

Unit 2–Computer Network Fundamentals

Preface

Over the past several years, home computer networks have become increasingly popular in the U.S. Home networks are used to share Internet access and other computing resources, support sophisticated home entertainment and security systems, and more. In response to ever-growing demand, the electronics industry has introduced a wide variety of consumer-grade networking components, which are inexpensive and easy to use.

This unit the fundamental concepts of computer networking, using the TCP/IP model as a framework, with a focus on Ethernet and 802.11g. By the end of this unit, students will be conversant with the five layers of the TCP/IP model and the star topology. They will be able to build simple Ethernet networks, using hubs and switches and private IPv4 addresses; make their own patch cables; and troubleshoot connectivity problems. They will also be able to build wireless networks of a similar scale, using inexpensive 802.11g routers and adapters. Throughout this unit, students will use packet tracing exercises to help them visualize and apply the TCP/IP networking model to the networks they actually build.

Concepts & Processes

1. Computer networks allow users to share data and hardware. They also allow people from all over the world to communicate and collaborate in a variety of ways.
2. The TCP/IP protocol suite drives the Internet and is very well supported by all modern computing systems. TCP/IP uses an easy-to-understand model to describe how network systems work and the ways in which the various protocol layers work together.
3. A variety of Open Source software tools--including Linux, Ethereal, and many others--are available to support the study and understanding of networks.
4. Using simple, affordable components, it is possible to build robust, secure wired and wireless networks to accomplish virtually any task for which a networking solution is appropriate.
5. There exists a worldwide community of computing and networking enthusiasts, who are involved in literally thousands of projects to develop and share software and hardware solutions to a wide range of problems and opportunities.

Essential Questions

1. What is a computer network and why is it useful?
2. What do networks look like and how do they work?
3. What sorts of (hardware and software) tools are required to build a network?
4. What are hubs, switches, routers and how do they work?
5. What are the security implications of setting up a wired or wireless home network?
6. How can I use home networking to share resources, such as an Internet connection, media and data, and other resources?

Lessons

1. Network definition, types, and uses (1 day)
2. Network models: TCP/IP (1 day)
3. Internet Protocol (IP) addresses (1 day)
4. Ethernet LANs (1 day)
5. Network cabling (1 day)
6. Wired local area networks (2 days)
7. Sharing Resources with Samba (1 day)
8. Wireless LANs (2 days)

Unit Evaluation

- Classroom observation
- Practical exercises: making patch cables, creating wired and wireless LANs, and implementing security controls on wireless LANs.

Lesson 2.1—Network definition, types & uses

Background

In the early 21st century, most Americans encounter and use data and communications networks of many different types every day. We use them to communicate with friends, family and colleagues; to transact business of all types; to acquire information and exchange data; for entertainment and many other purposes. The networks we use are constructed and organized in different ways. For anyone interested in making more than casual use of networks, it's important to understand some of the basic terms and concepts that define the various kinds of networks.

Concepts

1. Networks enable computer systems to communicate with one another, over distances of a few meters to thousands of kilometers.
2. We use communications and data networks in a wide variety of ways.
3. Computer networks can be categorized in many different ways, such as their scale, topology, the functional relationship among nodes, and the protocols that govern their operation.

Student Learning Objectives

1. To describe what data and communications networks are and to give examples of how they are used in everyday life.
2. To define some basic terms used to describe and discuss networks.
3. To be able to categorize computer networks in terms of their scale, the functional relationships among hosts, topology, and communications protocols.

Key Terms

Bluetooth	Ethernet	TCP/IP
protocol	local area network (LAN)	personal area network (PAN)
metropolitan area network (MAN)	campus area network (CAN)	wide area network (WAN)
peer-to-peer (P2p)	client	server
client-server network	network topology	bus topology
star topology	ring topology	tree topology

Activities

1. Ask students to define the term “network,” and discuss some various contexts in which the word is used in everyday conversation.
2. Begin to focus on computer (data) networks, seeking to apply some attributes of networks in a broader sense to their understanding of computer networks. Ask students to list examples of computer networks they may encounter on a regular basis, both the obvious ones (like computer networks in their school) and less obvious networks, like automatic teller machine (ATM)

networks, etc.

3. Ask students to explain why computer networks were developed. What are the advantages and disadvantages of computer networking.
4. Explain that computer networks can be classified in various ways, in terms of their scale, the arrangement of network nodes (topology), the functional relationship among network nodes, and the protocols that govern their operation.
5. Distribute the Networking terms worksheet and discuss/explain the terms on it to help students develop a networking vocabulary that they can use to describe computer networks.

Supply List

Networking terms worksheet

Resources

Computer networking: http://en.wikipedia.org/wiki/Computer_networking

Name_____

Date_____

Worksheet: Networking terms

Fill in the definitions for the following terms, as we discuss them in class.

Network scales

personal area network (PAN)

local area network (LAN)

campus area network (CAN)

metropolitan area network (MAN)

Functional relationships

client

server

peer-to-peer (P2P)

client-server network

Network topologies

ring

bus

star

tree

Network protocols

protocol

Bluetooth

Ethernet

Transmission Control Protocol (TCP)

Internet Protocol (IP)

Lesson 2.2—Network Models: TCP/IP

Background

From the late 1980s through the 1990s, computer networks used a number of different, mostly incompatible, protocols developed and fielded by the makers of different computer and network operating systems. Examples include Appletalk, IPX/SPX, NeuBEUI, and DECNet, among others. With the growing popularity of the Internet beginning in the mid-1990s, most of these protocols have been deprecated in favor of the Internet protocol suite, known as TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP is now supported by virtually every modern operating system, and is usually the default networking protocol. Since TCP/IP is platform independent, computer systems of virtually all types, running just about any operating system, are able to communicate without difficulty. TCP/IP uses a four-layer architecture, which serves as a useful model for understanding how computer networks function. In recent years, it has largely displaced the seven-layer Open Systems Communication (OSI) as the standard networking model.

Concepts

1. A networking protocol is a set of standards that governs communications among computing systems.
2. Since the mid-1990s, the Transmission Control Protocol/Internet Protocol (TCP/IP) suite has become the dominant protocol in computer networking.
3. TCP/IP uses a four-layer architecture, consisting of (from the top down) the Application layer, Host-to-host transport layer, internetwork layer, and network access layer. This model is useful for understanding how TCP/IP networks function.
4. TCP/IP uses encapsulation to provide abstraction of protocols and services between the layers.

Student Learning Objectives

1. To list the four layers of the TCP/IP protocol stack.
2. To define basic networking terms including TCP, IP, UDP, protocol, encapsulation, checksum, datagram, connection-oriented protocol, connectionless protocol, best-effort delivery, packet, and error correction.
3. To be able to describe how data moves from point to point through the TCP/IP protocol stack.
4. To be able to describe how to send a simple email message via telnet.

Key Terms

encapsulation	protocol stack	TCP
UDP	IP	packet
segment	datagram	frame
guaranteed delivery	“best effort” delivery	circuit-switching
packet-switching	connection-oriented	connectionless
checksum	error correction	application layer
host-to-host transport layer	internetwork layer	network access layer

Activities

1. Instructor introduces TCP/IP protocol stack and model, including some background and history.
2. Instructor introduces and describes each layer of the TCP/IP stack.
3. Instructor briefly describes how the TCP/IP model works, using encapsulation.
4. Instructor and students complete the TCP/IP activity, using a mail server and a telnet client.

Supply List

Worksheet--TCP/IP Network Model

Activity—Sending Email via Telnet

Resources

Internet Protocol Suite: http://en.wikipedia.org/wiki/TCP_IP

Understanding TCP/IP:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ap1.htm>

IP over Avian Carriers: http://en.wikipedia.org/wiki/IP_over_Avian_Carriers

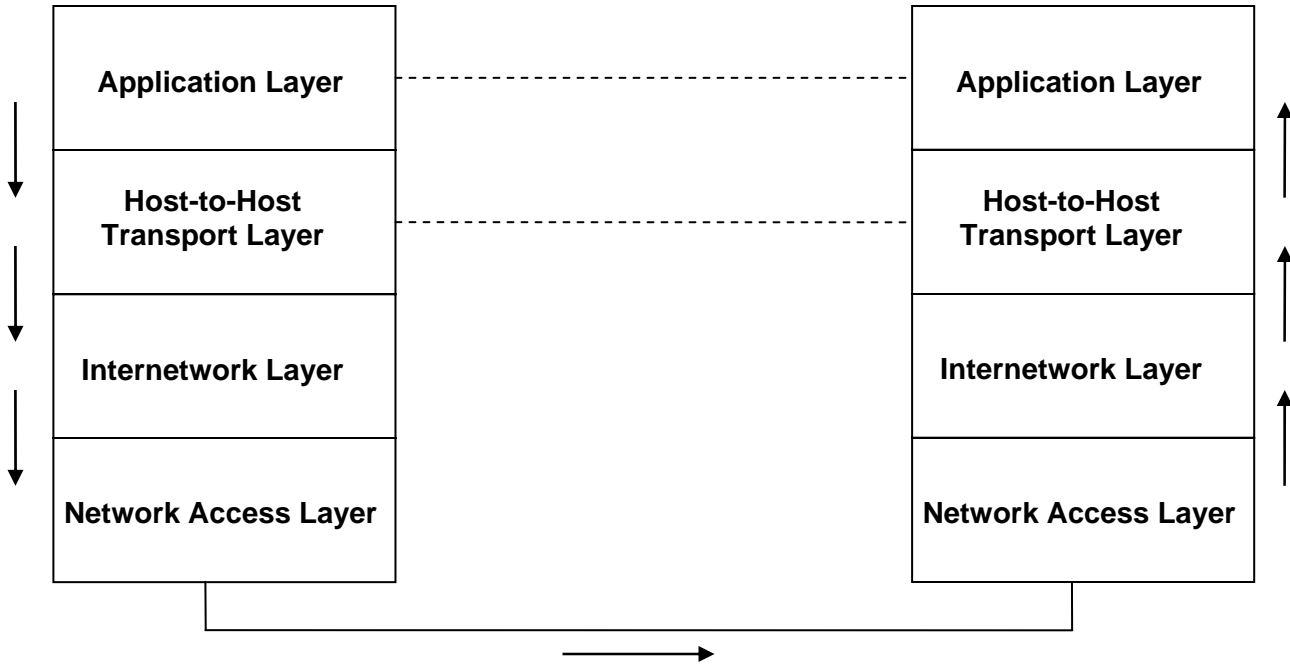
Notes

Consider configuring an email server on each computer to allow the student groups to send emails to the other group and to read the emails they receive on their own computer(s).

Name _____

Date _____

Worksheet: TCP/IP Network Model



Notes:

Application Layer

Host-to-Host Transport Layer

UDP:

TCP:

Internetwork Layer

Network Access Layer

Name _____

Date _____

Activity: Sending Email via Telnet

Purpose

Simple Mail Transport Protocol is the primary application layer protocol for electronic mail. The protocol's name is very descriptive. SMTP is a very simple protocol! In this activity, you will play the part of an email client program, doing everything email programs do to send email across the Internet.

Procedure

1. Using the Internet address provided by your instructor, make a telnet connection to the email server on the SMTP port (25).

If everything goes as it should, the server will respond with:

```
220 tux.net ESMTP Sendmail 8.14.1/8.14.1...
```

Now press Enter to ensure the server is ready to accept commands.

2. Send a HELO command, followed by an Internet name, to establish a mail session. Any name will work. For example:
3. To start an email message, send the MAIL FROM: command, followed by the sender's email address:

```
MAIL FROM: owensjp@clarkson.edu
```

Wait for a few moments to receive an acknowledgment.

```
250 2.1.0 owensjp@clarkson.edu... Sender ok
```

4. Now, send the recipient's email address, using the RCPT TO: command:

```
RCPT TO: jim@tux.net
```

```
250 2.1.5 jim@tux.net... Recipient ok
```

5. Next, send the DATA command to start entering the text of your message:

```
DATA
```

```
354 Enter mail, end with "." on a line by itself
```

```
Subject: Hello!
```

This is a hand-crafted email message from your friend at Clarkson University.

Regards,

Jim

6. To send your message, press the Enter key, followed by a period, and then the Enter key again. The server will respond with the message number.

250 2.0.0.0 19TBNOqp004826 Message accepted for delivery

7. To end your session, enter QUIT. The server will say, "Bye" and close the connection.

QUIT

221 Bye

Connection closed by foreign host.

Lesson 2.3—Internet Protocol (IP) Addresses

Background

Every computer or device connected to the Internet has assigned to it a unique address, called an *IP address*, which functions something like a telephone number, allowing other Internet-connected devices to communicate with it. Internet Protocol version 4, or IPv4 for short, is the version currently in use on the Internet. Within the next five years, or so, IPv4 will be succeeded by IPv6, a protocol which supports many times the number of unique addresses available with IPv4, among other changes and enhancements.

IPv4 uses 32-bit addresses, creating an address space of 4,294,967,296 unique addresses. IP addresses are normally represented using dot-decimal notation, four octets (values between 0 and 255) separated by “dots,” for example 68.236.159.234. IP addresses are grouped into three classes (A, B, and C), based on the value of the leading octet. The class of an IP address originally determined which portion of an IP address identified the network, with the remaining portion identifying a particular host on the network. Classless Inter-Domain Routing (CIDR) was introduced in the early 1990s to make more efficient use of the IPv4 address space. Subnet masks are now used to designate the portion of an IP address that identifies the network.

Several address ranges within the IPv4 address space are reserved for special purposes, such as private network spaces, local loopback, multicast, etc.

Concepts

1. Every Internet-connected device must have a unique address, called an IP address.
2. Internet Protocol version 4, called IPv4 for short, is the current standard. IPv4 uses 32-bit addressing, allowing for 4,294,967,296 unique addresses.
3. IPv4 addresses are divided into classes, which loosely identify the number of hosts or devices that a network can support. These classes can be further subdivided using subnet masks, under a system called Classless Inter-Domain Routing (CIDR), creating smaller networks.
4. The IPv4 address space contains a number of address ranges that are reserved for specialized uses, such as creating private networks.

Student Learning Objectives

1. To explain what an IP address is and how it is formed.
2. Given an IP address, to identify its class, the network number and the rest.
3. Given an IP address and a subnet mask or a classless address, to identify the network number and the rest.
4. To describe the difference between static and dynamic IP addresses.
5. To list some special address ranges in the IPv4 address and explain how they are used.

Key Terms

IP address	dotted-decimal notation	octet
subnet mask	Classless Inter-Domain Routing	static address
dynamic address	Dynamic Host Control Protocol	DHCP server
loopback address	private network	network address translation

Activities

IP addressing lecture/discussion

Supply List

- Worksheet: Internet Protocol (IP) Addresses
- Fact Sheet: Internet Protocol (IP) Addresses

Resources

IP address: http://en.wikipedia.org/wiki/Ip_address

IPv4: <http://en.wikipedia.org/wiki/IPv4>

IPv6: <http://en.wikipedia.org/wiki/IPv6>

Notes

Bring a Linksys wired firewall/router to pass around during the discussion, pointing out the WAN and switch ports. This may make the concept clearer, along with a diagram drawn on the board.

Name_____

Date_____

Worksheet: Internet Protocol (IP) Addresses

Fill in the definitions for the following terms, as we discuss them in class.

IP address

Domain name system (DNS)

name resolution

dynamic IP address

Dynamic Host Control Protocol (DHCP)

static IP address

IPv4

IPv6

IPv4 addressing

subnet mask

private network

Internet gateway

Network Address Translation (NAT)

Fact Sheet: Internet Protocol (IP) Addresses

- Definition
- Domain name system and name resolution
- Dynamic vs. static IPs
- Current versions (IPv4 and IPv6)
 - IPv4 uses 32-bit addresses and provides 4,294,967,296 (2^{32}) unique addresses of the form 192.168.10.101.
 - IPv6 uses 128-bit addresses and provides about 3.403×10^{38} unique addresses of the form 2001:0db8:85a3:08d3:1319:8a2e:0370:7334.
 - It is anticipated that IPv6 will replace IPv4 within the next five years.
- IPv4 addressing
 - IP addresses are normally rendered in dotted decimal notation, four octets (values between 0 and 255) separated by dots.
 - IP addresses consist of two parts: the first part identifies a particular network, and the second part identifies a specific host on the network.
 - With *classful* addressing, the number of bits used to identify the network is determined by the value of the first octet, as shown in the table below:

<i>Class</i>	<i>Start</i>	<i>End</i>	<i>Networks</i>	<i>Hosts/network</i>
Class A	0.0.0.0	127.255.255.255	126	16,777,214
Class B	128.0.0.0	191.255.255.255	16,384	65,534
Class C	192.0.0.0	223.255.255.255	2,097,152	254

- Large network classes can be subdivided through the use of *subnet masks*, which identify the network portion of the IP address. Another method, called Classless Inter-Domain Routing (CIDR) is also commonly used to subdivide larger network blocks.
- About 589 million of the available IPv4 addresses are in reserved special ranges. Among these are 17,891,328 *private* network addresses. These ranges are not routable outside of a private network, and machines with private addresses cannot directly communicate with public networks. They can, however, do so through *network address translation*.

<i>Address range</i>	<i>Number of IPs</i>
10.0.0.0 – 10.255.255.255	16,777,215
172.16.0.0 – 172.31.255.255	1,048,576
192.168.0.0 – 192.168.255.255	65,535

- Computer hosts on private networks can communicate with public networks if they are connected to an Internet gateway that is assigned a public IP address and configured to translate private network addresses into its own public address.

Lesson 2.4—Ethernet LANs

Background

By the late 20th century, the term *Ethernet* had become synonymous with *local area network*. In fact, Ethernet is a proprietary set of technologies for local area networking, one of a number of competing approaches developed during the late-1970s and early-1980s. Although theoretically inferior to some other approaches, Ethernet proved superior in actual use and has become the de facto standard for LANs.

Ethernet operates at the Network Access layer in the TCP/IP model. It uses the star networking topology, which has proved more robust than either the bus or ring topologies. At the physical layer, Ethernet uses unshielded twisted pair cabling primarily. The current standard for UTP is Category 5 Enhanced, or Cat5e, supporting speeds of up to 1000 megabits per second, also known as Gigabit Ethernet.

To support multiple users on a network, Ethernet uses a scheme called CSMA/CD, for carrier sense multiple access with collision detection. Ethernet hosts are connected via cables to network hubs or switches. Hubs are half-duplex devices that broadcast all network traffic to all connected devices. Thus, hubbed networks are much more prone to collisions, quickly degrading network performance. Switches are smarter devices, capable of “learning” the locations of connected hosts. Switches are therefore able to limit traffic based on the actual destination MAC (media access control) addresses of traffic, greatly reducing the number of collisions and making full duplex communications possible.

Concepts

1. The Ethernet networking protocols have become the de facto standard at the Link layer.
2. Ethernet uses the star networking topology and a carrier sense multiple access with collision detection scheme.
3. The Ethernet physical layer is comprised of cabling, primarily unshielded twisted pair; hubs; and switches.
4. Switches are “smarter” devices than hubs, supporting higher networking speeds, particularly on busy networks.

Student Learning Objectives

1. List the most common network topologies and some advantages and disadvantages of each.
2. Briefly describe the Ethernet LAN protocol in terms of its topology, communications scheme, and list the equipment required to create a simple Ethernet LAN.
3. Explain how Ethernet's carrier sense multiple access with collision detection (CSMA/CD) works.
4. Describe the differences between Ethernet hubs and switches, and explain why switches are preferred.

Key Terms

CSMA/CD	hub	switch
half duplex	full duplex	Ethernet
unshielded twisted pair (UTP)	star topology	bus topology
ring topology	media access control (MAC) address	

Activities

1. Ethernet lecture/discussion
2. Ethernet equipment “Show and Tell”

Supply List

- Worksheet: Ethernet
- Ethernet equipment (network adaptor, hub, switch, patch cables)

Resources

Ethernet: <http://en.wikipedia.org/wiki/Ethernet>

Name_____

Date_____

Worksheet: Ethernet

Fill in the definitions for the following concepts and terms, as we discuss them in class.

Ethernet

star topology

bus topology

ring topology

unshielded twisted pair (UTP)

Ethernet hub

Ethernet switch

carrier sense multiple access with collision detection (CSMA/CD)

media access control (MAC) address

half duplex

full duplex

Name_____

Date_____

Quiz: Networking terms

Fill in short definitions for the following terms.

Network scales

personal area network (PAN)

local area network (LAN)

campus area network (CAN)

metropolitan area network (MAN)

Functional relationships

client

server

peer-to-peer (P2P)

Network topologies

Draw a small model showing the layout of each of the following network topologies. Show and label each of the parts you remember, including hosts, hubs, terminating resistors, etc.

ring

bus

star

tree

Lesson 2.5—Network Cabling

Background

In Ethernet's star topology, computers and other network devices are connected together using cables. Unshielded twisted pair, or UTP for short, is the most common cable used for local area networks. The current standard for UTP cables is Category 5 Enhanced, better known as Cat5e. Cat5e cable is available in a number of varieties, suitable for different wiring applications. Cable runs are terminated with RJ45 connectors. Making network cables is a relatively simple process. In addition to cable and connectors, only a crimper wire trimmer, and perhaps a pair of scissors is required. Two standards for the arrangement of UTP pairs have been defined: TIA/EIA 568A and TIA/EIA 568B.

Concepts

1. Of the available cable types, unshielded twisted pair cabling is most commonly used in local area networks.
2. UTP cabling consists of four twisted pairs of insulated conductors, wrapped in an insulating sheath.
3. Several distinct categories of UTP cabling have been defined, based on their construction and specifications. Category 5 Enhanced (Cat5e) is the current standard for LANs.
4. Cat5e is manufactured in several varieties, suitable for different cabling applications.
5. Cable runs are terminated with RJ45 connectors.
6. Making up patch cables is a relatively simple process, requiring only a few simple tools.

Student Learning Objectives

1. List common cable types used in networking.
2. Describe how UTP cables are made.
3. Explain how UTP cables are used in Ethernet networks.
4. Demonstrate the ability to make a working patch cable.
5. Name the two wiring standards used for wired Ethernet networks and their uses.

Key Terms

Cat5e	RJ45	crimping tool / crimper
patch cable	wiring standard	TIA/EIA 568A standard
TIA/EIA 568B standard		

Activities

1. Cabling lecture/discussion with slide show
2. Cable making activity

Supply List

- Cat5e patch cable and RJ45 connectors
- Crimpers, cable trimmers, scissors
- Computers and Ethernet hubs or switches (for testing cables)
- Network Cabling slide show
- Activity sheet: Making Ethernet patch cables

Resources

Ethernet: <http://en.wikipedia.org/wiki/Ethernet>

Notes

Some students were able to fashion working cables, while others needed more practice.

Name_____

Date_____

Activity: Making Ethernet patch cables

Purpose

Ethernet patch cables provide the links between network devices (such as hubs and switches) and our computers. During this activity, you will learn to make your own patch cables in a way that helps to ensure reliable network connections.

Procedure

Make two patch cables in your group, one 568A and one 568B

1. Strip cable end (about 1")
2. Untwist wire ends
3. Arrange wires into desired pattern
568A: GW-G OW-BI BIW-O BrW-Br
568B: OW-O GW-BI BIW-G BrW-Br
4. Trim wires to size (about ½")
5. Attach RJ45 connector (with tab facing down)
6. Check wire ends and insulating sheath positions
7. Crimp firmly
8. Test cable by connecting PC to hub

Conclusion Questions

1. Did your cables make good connections?

2. What is the difference between the two wiring standards? Do you think one is preferable to the other?

3. If a newly-made patch cable fails testing, describe some likely causes for the failure.

4. In planning a network installation for a small business, would it be better to make your own patch cables or to purchase pre-made cables from a vendor? Explain your reasoning.

Lesson 2.6—Wired Local Area Networks

Background

Small wired local area networks (LANs) are easy to set up and maintain, using inexpensive components that are readily available in most office supply stores. Small networks can serve a variety of purposes in the small office/home office (SOHO) environment, making it possible to share resources such as an Internet connection, printers, scanners, and other devices among several computers. In addition, simple peer-to-peer networks can facilitate collaboration by making it easy to share and back up files across the network.

When implemented using Ethernet and TCP/IP networking protocols, networks can link virtually any type of computer system, including those running Windows, Linux and Unix, Macintosh, and other systems. Small networks can be as simple as two computers linked directly with a crossover cable, or they can link a larger number of systems using an Ethernet hub or switch. To share an Internet connection, a network router is also required, to connect the local network to the wide area network, the Internet.

Depending on the needs and skill level of the network's users, a simple peer-to-peer, or workgroup, may be recommended. Greater security and streamlined management of network resources is a feature of client-server networks. A variety of software systems are available for setting up client-server networks, a number of which are Open Source systems available at no cost. While these network systems can be more secure and robust, set up and management of client-server networks requires a higher level of skill than peer-to-peer networks.

Concepts

1. Small peer-to-peer networks can be constructed using a few inexpensive, readily available components.
2. Two computers can be networked using only a crossover network cable.
3. Three or more computers can be networked using an Ethernet hub or switch and standard UTP patch cables. Assignment of static IP addresses is normally required with networks of this type.
4. Dynamic assignment of IP addresses in simple networks can be accomplished by using an inexpensive router in place of a hub or switch. In this case, computers are networked using the Ethernet switch that is usually included in these devices.
5. Network connectivity can be tested using ping, which sends a series of ICMP (Internet Control Message Protocol) packets to another host on the network.
6. The use of ping and other network tools that generate ICMP packets may be restricted by local network policies or packet-filtering software and devices.

Student Learning Objectives

1. Set up a simple peer-to-peer network using dynamic IP addresses.
2. Determine a networked computer's MAC and IP addresses, netmask, gateway, and DNS settings using network software tools available in Windows and Linux.
3. Set up a simple peer-to-peer network using static IP addresses, using network software tools available in Windows and Linux.
4. Test a computer's network connectivity using ping.
5. Discuss some possible limitations on the use of ping within local or between local and distant networks.

Key Terms

netmask	gateway (address)	Domain Name Service (DNS)
peer-to-peer network	small office/home office (SOHO)	Internet Control Message Protocol (ICMP)
ping	denial of service attack	ping flooding
Ping of Death	Dynamic Host Control Protocol (DHCP)	localhost (IP address 127.0.0.1)

Activities

First day

- Instructor presentation
 - Networking with a DHCP server
 - Using ifconfig or ipconfig to verify network settings
 - Using ping to check network connectivity
- Students complete Peer-to-Peer Network with DHCP Activity

Second day

- Instructor presentation
 - Networking configuration using static IP addresses
 - Considerations on the use of ping and related ICMP tools
- Students complete Peer-to-Peer Network with Static IPs Activity

Supply List

1. Activity: Networking with DHCP
2. Activity: Networking with Static IPs
3. SOHO wired router, Ethernet hubs or switches, and patch cables
4. One laptop or desktop PC for each three students, with one Ubuntu Virtual Machine or LiveCD per computer

Resources

An Overview of ping: <http://www.linuxjournal.com/article/8605>

Notes

The networking setup for the DHCP activity consisted of a Linksys wired router, which includes a DHCP server and four-port switch, and two Linksys switches plugged into the router's switch.

Name_____

Date_____

Activity: Networking with DHCP

Purpose

Setting up a local area network with a Dynamic Host Control Protocol (DHCP) server is easy! The DHCP server provides all the information your computer needs to get up and running on the network. Once connected, you will check network connectivity with the router and at least one other peer on the network.

Procedure

Getting connected

1. Before connecting your PC to the network, be sure the Ubuntu virtual machine is running on your computer. You will use Ubuntu Linux throughout this activity.
2. Next, open a terminal window on your computer by clicking on **Applications->Accessories->Terminal**.
3. In the terminal window, type **ifconfig** and press Enter.
 - a. How many network devices are listed in the output? Record their names below.
 - b. Is there an IPv4 address listed for any of the network devices? If so, record your IP address(es) below.
4. Connect your computer to a network switch using a patch cable. Did you get a light on the switch? Record the port number you connected to in the space below.
5. Draw a diagram of the entire local area network in the space below, including the router, any switches or hubs, and all connected PCs.
6. Run **ifconfig** again. Do you see an IP address? If so, record it below.
7. In the terminal window, type **dhclient eth1** and press Enter. Describe what happens.

Checking your connection

1. Check connectivity with the router with the ping command. Type **ping -c4 10.0.1.1** and press Enter. Record the times listed in the last column of the output. What was the average round trip time (rtt) from your computer to the router and back?
2. Ask another group for their IP address. Check connectivity with that group's computer with ping. Run ping as shown above, substituting the new IP address for the one listed in the previous item. Record the times listed in the last column below. What was the average round trip time (rtt)?
3. When you have completed the activity, shut down your computer and return to your seat.

Conclusion Questions

1. How difficult is it to set up a small network? Do you think most people would be able to do it?
2. Can you think of any disadvantages of setting up a network of this sort at home or in a small office environment? Explain.

Name_____

Date_____

Activity: Networking with Static IPs

Purpose

While setting up a network with a Dynamic Host Control Protocol (DHCP) server is very convenient, it is sometimes preferable to use static IP addresses. In this activity, you will join the network using an IP address and netmask provided by your instructor. Once connected, you will check network connectivity with at least one other peer on the network.

Procedure

Getting connected

1. Before connecting your PC to the network, be sure the Ubuntu virtual machine is running on your computer. You will use Ubuntu Linux throughout this activity.
2. When the boot process is completed, connect your computer to the network switch using a patch cable. Did you get a light? What port number did you connect to on the switch?
3. Draw a diagram of the entire network in the space below.

4. To configure your network settings, click **System->Administration->Network**.
5. In the **Network settings** window, make sure the **Connections** tab is selected.
6. Click on **Wired connection**, and then click the **Properties** button.
7. In the **Interface properties** window, change the **Configuration** setting to **Static IP address**.
8. Enter the IP address provided by your instructor in the **IP address** field.
9. Enter **10.0.1.0** in the **Gateway address** field.
10. Finally, enter **255.255.255.0** in the **Subnet mask** field. Click **OK** to close the **Interface properties** window.
11. Click **OK** to close the **Network settings** window.

Checking your connection

1. Open a terminal window on your computer, if one is not already open, by clicking **Applications->Accessories->Terminal**.
2. Type **ifconfig** and press Enter. Are your network setting correct? If not, repeat the steps 4–11 in the previous section

3. Ask another group for their IP address. Check connectivity with that group's computer with ping. For example, `ping -c4 10.0.1.200`. Record the times listed in the last column below. What was the average round trip time?
4. Ask a second group for their IP address. Check connectivity to that group's computer with ping. Record the times listed in the last column below. What was the average round trip time?
5. When you have completed the activity, shut down your computer and return to your seat.

Conclusion Questions

1. How does setting up a network with static IP addresses compare with networking using DHCP?
2. Can you think of any advantages of setting up a network with static IP address instead of DHCP? Explain.

Lesson 2.7—Sharing Resources with Samba

Background

A primary reason for networking computers is to allow the sharing of resources, including files, printers and other hardware resources. While the open TCP/IP protocol suite has become the standard for networking, most operating systems continue to use proprietary or non-standard protocols to support file and hardware device sharing. This fact can make it difficult to share resources between computers running different operating systems. An effective solution to sharing resources among diverse computer systems is the Open Source Samba package. Samba provides its own implementation of Microsoft's SMB/CIFS (Server Message Block/Common Internet File System) protocols, which are used to support resource sharing over Windows networks. Versions of Samba have been developed for all the major desktop computer operating systems, and most systems come with the client-side Samba software installed and ready to use. Thus, Samba is an excellent choice for demonstrating file sharing among disparate computer systems on a network.

Concepts

1. Resource sharing is a primary purpose for computer networking.
2. The TCP/IP protocol suite has become the standard for networking among all major operating systems, yet most systems continue to use proprietary or non-standard protocols to support resource sharing. This lack of standardization can make it difficult to share resources among computers running different operating systems.
3. The Open Source Samba package, which is based on the Windows protocols for file and printer sharing, can be used to share files and printers among many different types of computers.
4. Most major operating systems now include the Samba client software necessary to use Windows file and printer shares by default. This software is quite simple to configure and use.
5. Samba server software is also available for all major operating systems. When properly configured, Samba makes it possible to share resources with virtually any kind of computing system to meet a variety of different needs, from simple file sharing at home, to sophisticated and secure systems on enterprise-level networks.

Student Learning Objectives

1. To discuss the advantages of resource sharing on computer networks.
2. To use ping to confirm connectivity on a computer network.
3. Given a username, password, and domain name, to be able to connect to a Samba share over a network.
4. To be able to retrieve a file from a secure Samba share and update it.
5. To briefly describe the differences between user-level and share-level security in Samba.
6. To briefly discuss the relative advantages and disadvantages of user-level and share-level security.

Key Terms

Service Message Block (SMB)	Common Internet File System (CIFS)
domain	workgroup
username	group

Activities

First day

- Instructor presentation
 - File and printer sharing on a network
 - Samba SMB/CIFS background
 - Share- and user-level shares
 - Workgroups and domains
- Students complete Sharing Resources with Samba Activity

Second day

- Instructor demonstration
 - Setting up a Samba share
 - Share-level security
- Students complete Setting Up a Samba Share Activity

Supply List

1. Activity: Sharing Resources with Samba
2. SOHO wired router, Ethernet hubs or switches, and patch cables
3. One laptop or desktop PC for each three students, with one Ubuntu LiveCD per computer

Resources

Samba (software): http://en.wikipedia.org/wiki/Samba_%28software%29

Name_____

Date_____

Activity: Sharing Resources with Samba

Purpose

Samba is an Open Source software program that mimics Windows networking protocols to allow users to share files and printers over a network with other users running almost any other operating system. In this activity, we will use Samba to share files between computers running Linux.

Procedure

1. Connect your PC to the network and boot it using the Ubuntu Live CD provided by your instructor. We will use a DHCP server to configure the network settings automatically.
2. Check your connectivity by pinging the router, with a command like the following:

```
ping -c 4 10.0.1.1
```

3. From the menu, click Places->Connect to Server.
4. In the **Connect to Server** window, change the Service type to **Windows share** and type **Norwood** into the **Server** field, then click **Connect**.
5. When the **Norwood** folder icon appears on your desktop, double-click on the icon to open it.
6. Find your group's share folder icon and double-click on it.
7. When the **Authentication Required** window appears, enter the information below to gain access to your folder.

Username: *group username*

Domain: *norwood*

Password: *group password*

8. Copy the group file onto your desktop, open it, and fill in the names of your group members. Then copy the updated file to the server by dragging and dropping it back into your group's share folder.
9. Try to access another group's files. Were you successful?
10. When you have completed this activity, shut down your computer and return to your seat.

Lesson 2.8—Wireless LANs

Background

While networking offers a number of advantages for sharing resources and information, wireless networking can offer even more advantages, in terms of mobility, flexibility, convenience and cost. In place of UTP cables and hubs or switches, wireless LANs use radio waves to connect computers, personal digital assistants (PDAs), telephones, and other devices to wireless access points (WAPs) or wireless routers. Wireless networking technologies can also be used to connect computers and similar devices directly, in ad hoc networks.

Wireless networking protocols have been standardized under several protocols: 802.11a/b/g and a newer standard still under development as of this writing, 802.11n. The individual standards are defined by the radio spectrum used for communications among hosts, throughput speed, encryption methods utilized, and other factors. The two most common standards as of late 2006 are 802.11b and 802.11g. A new standard, 802.11n is expected to be fielded by mid-2007.

Wireless LANs consist of one or more wireless access points (WAPs) and one or more clients. Wireless LANs resemble non-switched Ethernet networks in that all connected hosts compete for the same available bandwidth, using a carrier sense multiple access protocol with collision avoidance (CSMA/CA), as opposed to Ethernet's CSMA/CD protocol. This difference is necessitated by the fact that hosts on a wireless LAN may not be able to "hear" each other well enough to detect collisions. Therefore, collisions on wireless LANs must be avoided, rather than simply detected.

Wireless LANs offer a number of advantages over wired Ethernet LANs, primarily in terms of their ease of installation and flexibility. Wireless LANs also bring a number of disadvantages, including interference from mobile phones, microwave ovens, and other devices; limited range, and the vulnerability of messages passed over open networks or those with weak encryption.

Concepts

1. Wireless networking, also called WiFi, uses radio waves instead of cables to connect hosts.
2. Several standards have been defined for wireless networking, under IEEE 802.11. The two most common standards are currently 802.11b and 802.11g. A new standard 802.11n, which promises much greater speed, is due out in mid-2007.
3. WLANs consist of one or more wireless access points, called WAPs, and clients such as desktop or laptop computers, personal digital assistants, and cell phones.
4. WLANs use a modified version of the Ethernet protocol, carrier sense multiple access with collision avoidance (CSMA/CA), for communications among network nodes.
5. WLANs can be easier and cheaper to set up than wired LANs. They also permit mobility and more flexibility than wired LANs. Disadvantages include potential interference from mobile phones, microwave ovens and other devices. WLANs also pose security challenges since open connections are subject to interception and unintentional use.

Student Learning Objectives

1. To briefly describe wireless networking and how it works.
2. To list and differentiate among the currently defined wireless networking standards.
3. To list the equipment required to set up a wireless LAN.
4. To demonstrate how to set up a wireless LAN, using a SOHO wireless router.
5. To discuss the advantages and disadvantages of wireless LANs.
6. To explain how the security problems often associated with wireless LANs can be mitigated.

Key Terms

wireless access point (WAP)	range extender
wireless router	wireless LAN (WLAN)
hot spot	Institute for Electronic and Electrical Engineers (IEEE)
wired equivalent privacy (WEP)	WiFi protected access (WPA)
IEEE 802.11	carrier sense multiple access with collision avoidance (CSMA/CA)
radio spectrum	service set identifier (SSID)
WiFi	personal digital assistant (PDA)

Activities

First day

- Instructor presentation
 - How WiFi works
 - Equipment
 - Set up
 - Advantages & disadvantages
- Students complete Setting up a Wireless LAN activity

Second day

- Instructor demonstration
 - Configuring wireless encryption (WEP and WPA)
 - Other wireless security measures
- Students complete Securing a Wireless LAN activity

Supply List

1. Slideshow: Wireless LANs
2. Activity: Setting up a Wireless LAN
3. Activity: Securing a Wireless LAN
4. SOHO wireless routers, one for every three or four students
5. One wireless-equipped laptop or desktop PC for each three students

Resources

IEEE 802.11: http://en.wikipedia.org/wiki/IEEE_802.11

Wi-Fi: <http://en.wikipedia.org/wiki/Wifi>

Carrier sense multiple access with collision avoidance: <http://en.wikipedia.org/wiki/CSMA/CA>

Notes

In a 40-minute period, there isn't enough time for students to actually implement all of the security measures discussed. The demonstration and discussion of not broadcasting the SSID and restricting access by MAC address may be sufficient, along with the caution that these measures can be readily defeated by a determined intruder, who is equipped with the right tools and a pretty good understanding of wireless networking.

Name _____

Date _____

Activity: Setting Up a Wireless LAN

Purpose

Wireless LANs are relatively simple to set up. Configuration of the wireless router is an important step in the process. In this activity, we will set up a simple local area network, which is open to any host within range.

Procedure

1. Connect your PC to the network and boot it using the Ubuntu Live CD provided by your instructor. We will use the wireless router's built-in switch and DHCP server to configure the network settings automatically.

2. Check your connectivity by pinging the router, with a command like the following:

```
ping -c 4 192.168.1.1
```

3. Point your browser at <http://192.168.1.1/start.htm>.

In the menu on the left side of the screen, under Maintenance, click on **Set Password**.

In the section **Set Password**, enter the following information:

Old Password: password
New Password: time2go
New Password: time2go

Click Apply. Once the settings are updated, you will have to log in:

Username: admin
Password: time2go

4. In the menu on the left side of the screen, under Setup, click on **Wireless Settings**.

In the section **Wireless Network**, enter the following information:

Name (SSID): *Pick a name* (Not NETGEAR)
Region: United States
Channel: Pick a channel different than the others
Mode: g and b

In the section **Security Options**, select Disable.
Click Apply.

5. In the menu on the left side of the screen, under **Setup**, click on **Basic Settings**.

In the section **Internet IP Address**, select **Use Static IP Address**, and enter the following information:

Name _____

Date _____

Activity: Securing a Wireless LAN

Purpose

Wireless LANs are easy to set up, as well as being convenient and flexible. Unsecured wireless networks are subject to monitoring and unintended use, however. In this activity, you will learn to encrypt wireless LAN communications and other measures that can restrict unintended use of wireless networks.

Procedure

1. Connect your PC to the network and boot it using the Ubuntu Live CD provided by your instructor. We will use the wireless router's built-in switch and DHCP server to configure the network settings automatically.

2. Check your connectivity by pinging the router, with a command like the following:

```
ping -c 4 192.168.1.1
```

3. Point your browser to the router's configuration screen at this address:

```
http://192.168.1.1/start.htm.
```

You will need to log in:

Username: admin

Password: time2go

Wireless Encryption

4. In the menu on the left side of the screen, click on **Wireless Settings**. In the section **Security Options**, make the following modifications:

Select WEP, and select **64bit** Encryption Strength.

Enter the **Passphrase** of your choice, and then click **Generate**.

Write down the hexadecimal **Key1** value.

Click Apply.

Try connecting to your router wirelessly, both without and with the key.

5. Repeat the previous activity, selecting **WPA-PSK** instead of **WEP**.

Encryption Settings

6. Before beginning this section, be sure to disconnect your computer from the wireless router.
7. In the menu on the left side of the screen, click on **Advanced Wireless Settings**. In the section **Wireless Router Settings**, make the following modifications:

