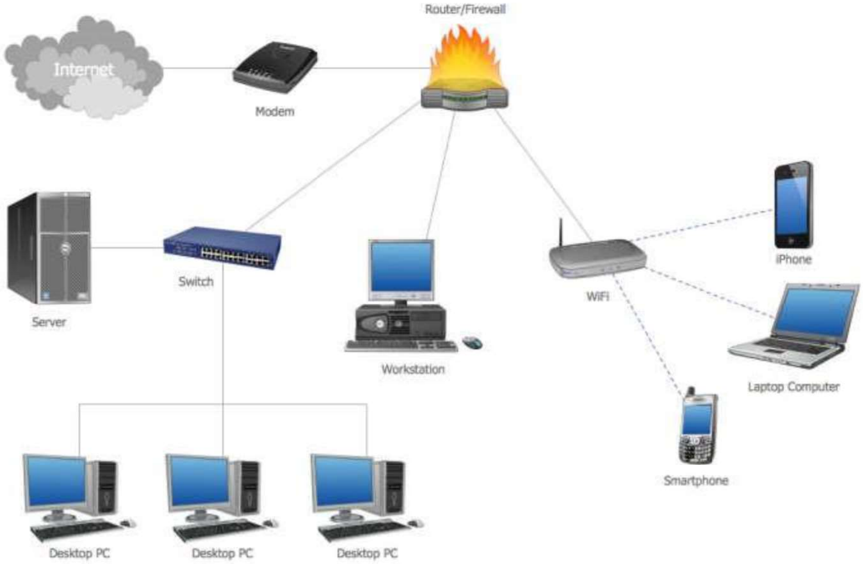
2015

A Practical Guide to Computer Network & Internet Technologies



,

Preface

Networking is a big domain under computer science and engineering. There are several streams and area of specializations under computer network in which students shall have their own choices for their future career. The course contents of computer network under bachelor degree level is very basics. It simply provides the overall theoretical knowledge on communication standards, protocols and network programming. Students have to learn about lots of new terms and technologies in computer network making this a bit hard to grab the knowledge the sufficient knowledge on computer. Hence, sufficient practical activities and tutorial practices are required under this subject to verify the concepts and strengthen the practical knowledge that shall be directly implemented in the real industries after graduation.

This lab manual on computer network is an attempt of my twelve+ years of experiences in teaching this subject. It helps course instructor for smooth lesson planning of his/her teaching and students to have more clarification on the theoretical knowledge achieved during the class hours. Students are instructed to do the lab tutorial step by step as an example first and then do given task after getting the practical concepts on each lab. This reduces the confusion for both instructor and students about what to do next in the lab.

There are fourteen lab sheets including case study and final exam designed to be completed within the specified academic period (one semester course) starting from the basic concepts of network hardware/software to advance level configuration up to routing, security implementation and different server systems deployment. I tried to cover the new networking technologies, tools, software/hardware on every lab with the objectives to provide sufficient latest knowledge on computer network to my valued readers. Students have to complete the tutorial steps during the lab hours and submit the task and exercise work on the next lab.

Table of Contents

Computer Network Lab

Lab Marks Distribution

Lab Reports	**Attendance/Viva**	**Final Exam**	**Total Full Marks**
40%	**20%**	**40%**	**100%**

Overall Objective:

The lab works in this course provides hands on training and knowledge about the analysis, design, troubleshooting, modeling, testing and evaluation of computer networks. Students shall have access to real test-bed networks, virtual and simulated network with the tools like tcpdump, wireshark, ip scanner, packet tracer, opnet, mininet, visio, Bosom, NetSim etc.. to fulfill the objectives set forth on each lab. At the end, student shall be able to perform the network and server administration like addressing management, switching (VLAN, VTP), routing and remote administration (SSH, Telnet, Hyperterminal), TCU/UDP/IP packet analysis, configuring of web, dns, dhcp and ftp servers over linux/unix OS. Students will gain the opportunity to design and develop networking model, simulation and testing with sufficient security measures.

For Students:

Students have to complete at least 10 to 12 lab activities throughout the semester to fulfill the objectives of the course Computer Network at Bachelor of engineering and computer science. Each lab manual is designed with lab objective, basic theoretical background, and sample example with necessary steps to operate with the networking tools and exercise. Before appearing into the lab, all are requested to learn the relevant activities in summary and explore theory/practical concepts of corresponding lab. Students have to do the exercise provided and submit the report into the next lab. Lab report to be submitted should include at least the following topics.

1. Cover page
2. Title
3. Objective(s)

4. Apparatus
5. Procedure (steps), (Explanation, topology if any, setup, configuration)
6. Testing and verification (if any)
7. Discussion and Conclusion

LAB 1

Lab No	Description (Title)
1	**Overview of Networks and layered communications, understanding of Network equipment, wiring in details**
2	CAT6 UTP EIA/TIA 568A/B straight and cross-over wiring, testing

Objective(s):

- To understand layered communications and protocols
- To feel and know the networking equipment (repeater, hub, bridge, switch, router, crimper, UTP, Fiber cable, connectors, patch panel, cable managers, racks, CAT6 straight and crossover wiring standards, LAN meter/tester, RJ-45)

Network Hardware: Crimper/clamper, RJ-45 jack male/female, LAN/Cable tester, UTP, Fiber cable, HUB/Switch/Router/Bridge, patch panel, cable manager....

Repeaters are simple devices that work at the physical layer of the OSI. They regenerate signals (active hubs does that too).

Hubs are used to build a LAN by connecting different computers in a star/hierarchal network topology, the most common type on LANs now a day. A hub is a very simple (or dumb) device, once it gets bits of data sent from computer A to B, it does not check the destination, instead, it forwards that signal to all other computers (B, C, D…) within the network. B will then pick it up while other nodes discard it. This amplify that the traffic is shared.

There are mainly two types of hubs:

1. **Passive**: The signal is forwarded as it is (so it doesn't need power supply).
2. **Active**: The signal is amplified, so they work as repeaters. In fact they have been called multiport repeaters. Hub is a multiport repeater.

Hubs can be connected to other hubs using an uplink port to extend the network. Hubs work on the physical layer (lowest layer). That's the reason they can't deal with addressing or data filtering.

Switches on the other hand are more advanced. Instead of broadcasting the frames everywhere, a switch actually checks for the destination MAC address and forwards it to the relevant port to reach that computer only. This way, switches reduce traffic and divide the collision domain into segments, this is very sufficient for busy LANs and it also protects frames from being sniffed by other computers sharing the same segment.

They build a table of which MAC address belongs to which segment. If a destination MAC address is not in the table it forwards to all segments except the source segment. If the destination is same as the source, frame is discarded.

Switches have built-in hardware chips solely designed to perform switching capabilities, therefore they are fast and come with many ports. Sometimes they are referred to as intelligent bridges or multiport bridges.

Most common switching methods are:
1. **Cut-through**: Directly forward what the switch gets.
2. **Store and forward**: receive the full frame before retransmitting it.

Normal Switches are on the data link layer (just above physical layer), that's why they deal with frames instead of bits and filter them based on MAC addresses. Switches are known to be used for their filtering capabilities. Intelligent switches works as a router.

VLANs (Virtual LANs) and broadcast domains: Switches do not control broadcast domains by default, however, if a VLAN is configured in a switch it shall have its own broadcast domain.

VLAN is a logical group of network devices located on different LAN physical segments. However they are logically treated as if they were located on a single segment.

Bridges are used to extend networks by maintaining signals and traffic. Bridges are on the data link layer so in principle they are capable to do what switches do like data filtering and separating the collision domain, but they are less advanced. They are known to be used to extend distance capabilities of networks.

In a comparison with switches, bridges are slower because they use software to perform switching. They do not control broadcast domains and usually come with less number of ports. Multiport bridges are generally termed as switch.

Routers are used to connect different LANs or a LAN with a WAN (e.g. the internet). Routers control both collision domains and broadcast domains. If the packet's destination is on a different network, a router is used to pass it the right way, so without routers, the internet could not functions. Routers use NAT (Network Address Translation) in conjunction with IP Masquerading to provide the internet to multiple nodes in the LAN under a single IP address. Routers work on the network layer so they can filter data based on IP addresses. They have routing tables to store network addresses and forward packets to the right port.

Gateways are very intelligent devices or else can be a computer running the appropriate software to connect and translate data between networks with different protocols or architecture, so their work is much more complex than a normal router. For instance, allowing communication between TCP/IP clients and IPX/SPX or AppleTalk. Gateways operate at the network layer and above, but most of them at the application layer.

There is an important rule to obey while using repeaters/hubs to extend a local network and is called the 5-4-3. The rule forces that in a single collision domain there shouldn't be more than 5 segments, 4 repeaters between any two hosts in the network and only 3 of the segments can be populated (contain user connections). This rule ensures that a signal sent over the network will reach every part of it within an acceptable length of time. If the network is bigger, the collision domain can be divided into two parts or more using a switch or a bridge.

Exercise:

1. What are physical layer devices?
2. What are the differences between Repeater and Hub? Hub and Switch?, Bridge and Switch?, Switch and Router?
3. What is virtual LAN? Why do we need to create VLAN?
4. Discuss Different Network Topologies