Data Communications Concepts—Layer by Layer

Dana E. Madison
Aaron D. Sanders

Clarion University of Pennsylvania
Computer Information Science Department
130 Becker Hall
Clarion, Pennsylvania, 16214, USA

Abstract

This paper presents an approach to hands-on data communications exercises using the layers of the Open Systems Interconnect model as the organizing mechanism. A greater understanding of the physical, data-link, and network layers of the Open Systems Interconnect model is possible for students as a result of this approach.

Keywords: Data communications, computer lab, OSI model

One of the more difficult concepts in computing to present is the Open Systems Interconnect (OSI) Model of networking. The largely theoretical nature of the OSI model tends to cause confusion for students, as they attempt to grasp the concept. The OSI model is difficult for instructors also, as lectures and diagrams can only go so far in presenting the conceptuality and usage of the layers, and the direct and virtual communication between those layers. A dynamically configurable computer lab is the perfect foil for rounding out the presentation of these concepts. Of the seven layers of the OSI model (Application, Presentation, Session, Transport, Network, Data Link, and Physical), the bottom three (Network, Data Link, and Physical) are easily demonstrated though the use of a dynamic computer lab.

1. DYNAMIC DATA COMMUNICATIONS LABS USING A MODULAR CONFIGURATION

One approach to reinforcing data communications concepts is proposed that provides a dynamically configurable computer lab that can be adapted to the requirements of the course in a matter of minutes. This concept uses a modular configuration of equipment that requires relatively small funding increments and permits a computer lab to evolve in size as funding becomes available. The precise configuration of a module depends on the purposes that it is used for, but the basic configuration is shown in Figure 1.

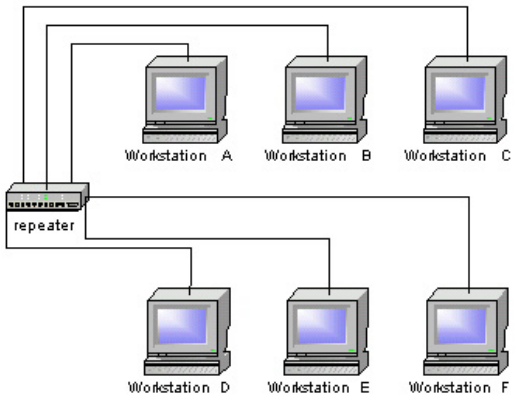

Figure 1

The Physical Layer—Connecting Nodes Together
The *physical* layer of the OSI Model defines the mechanical and the electrical requirements of the network medium, and the interface to that medium. The job of devices that are categorized into the Physical layer (for example network interface cards, hubs, repeaters, and cabling) is to make the physical connection between two nodes on a network.

Two of the most prevalent sources of network problems are faulty network interface cards (NICs) and cabling. A dynamically configurable lab provides an ideal means for identifying and categorizing these problems.

In the first exercise, the exterior coating of a Category 5 cable was cut and removed near the RJ-45 connector to reveal the wire pairs. The orange and brown wires were then cut in half to render the cable inoperable. This should be done so that it is not observable that the cable has been tampered with. Another option would be to take a cable that has not been terminated, and mix up the order of the wires before crimping the RJ-45 connector to the end. The cable was then used to connect the Workstation A to the repeater, as depicted in Figure 1. The task for the student is to determine why Workstation A cannot connect to any of the other workstations, by determining the scope of the problem. It must be determined whether the problem lies in the cable, the network card, network settings, or hardware devices.

The first step is to inspect the network settings on Workstation A. The next step is a visual inspection of the link and activity lights on the NIC on Workstation A. It is a good indicator that the cable is bad if both lights are off (which they most likely will be in this scenario). The ends of the cable should also be checked to make sure that both ends of the cable are plugged in snugly. The next step is to run the **ping** command from the Disk Operating System (DOS) prompt to determine where the break in connectivity is occurring. The first attempt is to ping another workstation. If that attempt fails, then the next step is to **ping localhost**. This will test to see if the TCP protocol is running correctly on Workstation A. In this exercise, Workstation A is unable to ping another workstation, but the **ping localhost** command shows that TCP is correctly configured on Workstation A. This leaves the repeater or the cable as the main possible sources of a problem. To identify the cable as the problem, a cable can be used from a workstation that is known to be working properly, and used to connected Workstation A to the repeater, making sure to use the same port in the repeater as before. At this point Workstation A should have resumed connectivity. A cable tester is used to make the final verification that the cable is bad. On a simple cable tester, the cable with cut wires tested as an open connection, and deemed unusable by the cable tester. On a cable tester with more extensive testing abilities, the cable failed the impedance and resistance tests, and also tested as an open connection.

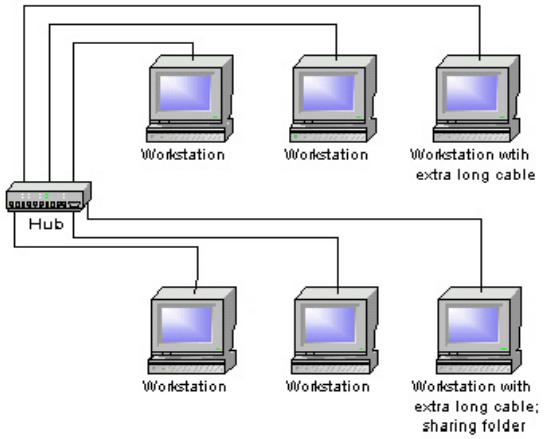

Figure 2

Hub devices, similar to the one depicted in Figure 2, are categorized into the Physical layer and could be demonstrated using a variety of similar setups. In the second exercise a general purpose hub device, one designed for home networking that provides no signal amplification or repeating service, is placed in the spot previously occupied by the repeater, as shown in Figure 2. Two special-length network cables were then hooked up, one from a workstation in one row to the hub, and the other from a workstation in the other row to the hub. The length of each of these cables is such that the total length of cable between the two workstations exceeds the one hundred meter limit of Category 5 cable. Software such as Network Associates' Sniffer or the Windows NT Network Monitor is used to monitor the packet activity over the connection between the two computers. The number of dropped packets and errors is monitored and recorded. The hub could then be replaced with the repeater, and the connection from workstation to workstation attempted, but this time the connection statistics are different, because the repeater amplifies the signal, nullifying the attenuation problem, and curing the dropped packets and errors.

The Data Link Layer—Making the Translation

The *data link* layer of the OSI Model passes data from the *physical* layer and the *network* layer. This job is more difficult than it might seem, because data must be translated before it is sent in either direction. The job of devices that are categorized into the Data Link layer (for example bridges, flow control, Media Access Control addressing, and error control) is to translate and pass frames between the Physical and Network layers. There are two specially designated sub-layers of the Data Link layer, and they are the Logical Link Control (LLC) and the Media Access Control (MAC) sub-layers. Flow control occurs at the LLC sub-layer, and MAC addresses are handled by the MAC sub-layer.

Using the configuration in Figure 1, one can access a shared folder on a computer on the other row because a

repeater does not perform any task other than amplifying signals. All traffic flows through a repeater without any hesitation. It is at this point that the dynamically configurable lab shows its strength. By replacing the repeater with a bridge that is set to not let any traffic cross from one side to the other, as in Figure 3, you now have segmented the network and created a fairly safe computing environment. This demonstrates how one can keep two parts of a corporation that should not have interaction with each other (such as employee salary information from the Payroll department to any other department), from being able to have any interaction with each other. This provides a nice path to segue into a protocol discussion. By running different protocols on each segment, one can drastically increase the security, and decrease the likelihood of anyone intercepting any traffic that is not meant for them. This serves as a lead in to the Network Layer, which will tie everything together, and really emphasize the importance of protocols.

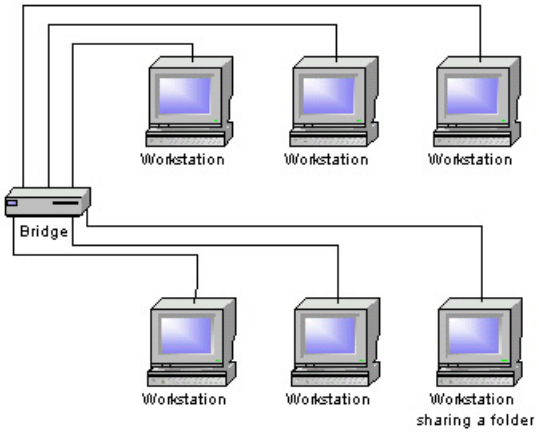

Figure 3

In the following exercise, hubs are connected to a switch, as shown in Figure 4. Computers are then connected to each of the hubs, and communication is initiated between the computers. Software products such as Network Associates' Sniffer and Windows NT Network Monitor can be used to measure the utilization percentage of the network at the hubs, and the number of packets passing through each hub. The switch is then replaced with a repeater, and the monitoring is repeated. When the repeater is used to connect the hubs, the utilization of the network decreases, and the number of packets flowing through each hub increases.

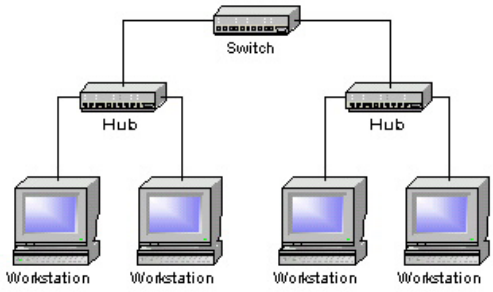

Figure 4

The Network Layer-Choosing the Correct Route

The *network* layer of the OSI Model defines how traffic is moved from segment to segment on a network. The job of devices that are categorized into the Network layer (for example routers, and node and logical segment addressing) is to move data from one segment or network to another. They do this by addressing messages and translating logical addresses and names into physical addresses.

Since all computers on a network or segment must have a unique Internet Protocol (IP) address, setting two computers with the same IP address, as in Figure 5, can demonstrate what happens when this occurs. Using the configuration detailed above, with a repeater between the two rows, setting one computer on each row to have the same IP address will provide a way for students troubleshoot IP addressing problems. The **winipcfg** command can be run to examine the IP and MAC address in use on a particular computer. The Address Resolution Protocol (ARP) can be run from the command prompt to associate IP address with MAC address for all of the computers connected to the repeater.

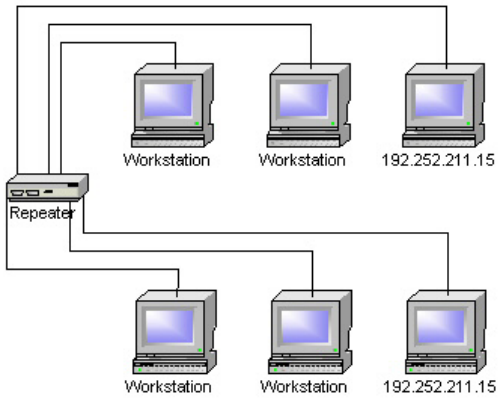

Figure 5

In the following exercise, computers were connected to a router, as shown in Figure 6, and the router was configured for dynamic updating of the routing table. The routing table was examined, and the entries were noted. Another computer was connected to the router,

and the routing table examined again to view the addition. A second set of computers was hooked to a second router, using the configuration shown in Figure 6. The routing table of the second router was examined, and the entries were noted. The two routers were then connected directly together. The routing tables of each router were then examined to determine if each router had detected the other, and passed its routing table to the other. Upon examination of the routing tables of each router, it was determined that the appropriate entries were added to each routing table, along with appropriate number of hops (one) to each computer.

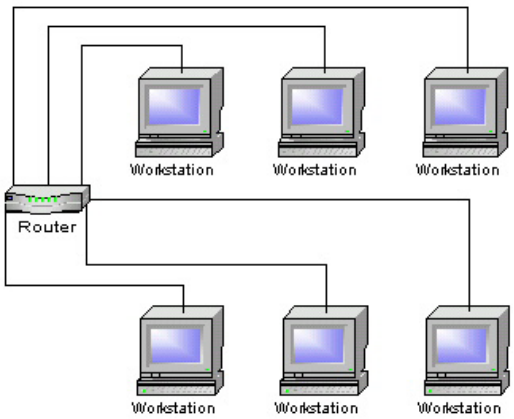

Figure 6

2. DIRECTIONS FOR FURTHER RESEARCH

The next phase of this work will involve detailing actual experiments that can be performed using the various network configurations proposed. Each of the module uses described in this paper will be analyzed and molded into a set of exercises supporting a semester-long course. The exercises will be tried in actual course settings and feedback obtained from the students and faculty involved. The long-term goals for this project will involve identifying other areas of computing for which this modular approach is suited. As each topic area is identified, sets of exercises will be developed supporting them.

3. CONCLUSION

Computer lab facilities for specialized areas of computing such as those described in this paper are hard to find in educational institutions. Meaningful exercises that reinforce networking concepts can make the difference between an ordinary course and one that students are eager to take on. The dynamic, modular computer lab concept proposed in this paper addresses both of these issues and integrates them into an environment that adds a whole new dimension to the learning experience for computing students. The concept is robust and will evolve as new technologies are developed and make their way into computing curricula.

4. REFERENCES

Craft, Poplar, Watts, & Willis, 1999, Network+ Exam Prep. Coriolis, Arizona.

Forouzan, Behroutz A., 2001, Data Communications and Networking, 2nd Edition. McGraw-Hill, New York.

Microsoft Corporation, 2000, Networking Essentials Plus 3rd Edition. Microsoft Press, Washington.

Palmer & Sinclair, 1999, A Guide to Designing and Implementing Local and Wide Area Networks. Course Technology, Massachusetts.

Tanenbaum, Andrew S., 1996, Computer Networks, 3rd Edition. Prentice-Hall, New Jersey.