Workshop Topics:

- Fundamentals
- Network Protocols
- Home Network Components
- Diagnostics

Outline of Workshop:

1. Fundamentals
   a. What is a computer network?
   b. Local Area Networks (LANs)
   c. Wide Area Networks (WANs)
   d. Virtual Private Network (VPN – AKA Tunneling)
   e. The Internet
   f. Peer-to-Peer Networks
   g. Server-based Networks
   h. Wireless Local Area Networks (WLANs)

2. Network Protocols
   a. TCP/IP
   b. Ethernet
   c. Ethernet Standards (802.3, 10BaseT, 100BaseT)
   d. Wireless Protocols (802.11xxx)

3. Home Network Components - Hardware
   a. PC/Laptop with Network interface Card (NIC)
   b. Cable Modem
   c. Router, Switch, Hub
   d. LAN Cabling
   e. Network Printer

4. Home Network Components – Software
   a. Peer-to-peer
   b. Domain Name Server (DNS)
   c. Dynamic Host Configuration Protocol (DHCP)
   d. Firewall

5. Network Diagnostics
   a. ipconfig command
   b. ping command
   c. Command to identify all active network components
   d. Wireshark
Fundamentals

What is a computer network?

A computer network consists of a collection of computers, printers and other devices that are connected together so that they can talk to each other. Local Area Networks (LANs), Wide Area Networks (WANs) and Virtual Private Networks (VPNs) are all examples of computer networks.

Local Area Networks (LANs)

LANs connect computers and other devices that are located physically close to each other. A computer network in a house or office is an example of a LAN. LAN connections can be either wired or wireless (more on this later).

Wide Area Networks (WANs)

WANs connect components that are geographically far apart (across cities and countries and internationally). The Internet is a WAN.

Virtual Private Networks (VPNs)

A VPN uses a public network to convey private information. VPN is sometimes called Tunneling. With VPN, a connection is established between two endpoints over a public network (such as the Internet). In a typical example, VPN allows a company’s employees to connect from their homes to the company’s internal private network, while protecting the security of the information that is passed back and forth. Refer to the figure below:

The Internet

The Internet is a worldwide system of interconnected computer networks. The Internet uses a standard internet protocol called TCP/IP. Internet users can access web pages, email systems and various forms of media.

Peer-to-Peer Network

A peer-to-peer network connects a number of nodes that all act as peers (equals). Tasks are shared among the peers, and include disk storage, computer processing, and print services.
This kind of network is simple to configure and relatively inexpensive. Most home networks are peer-to-peer configurations. The figure below is an example of a peer-to-peer network.

**Server-based Network**

In a server-based network (or client-server network) there are providers of resources (servers) and consumers of resources (clients). This kind of network is generally more expensive and more complicated to configure. However, it is much more scalable to large configurations than a peer-to-peer network. And it is much easier to administer. The figure below shows an example of a server-based network.
### Relative Advantages of Peer-to-Peer versus Server-based Networks

<table>
<thead>
<tr>
<th>Peer-to-Peer Network</th>
<th>Server-based Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy to configure</td>
<td>Scalable to large configurations</td>
</tr>
<tr>
<td>Less expensive hardware and software – any PC can perform server functions</td>
<td>Simpler to administer</td>
</tr>
<tr>
<td>More flexible</td>
<td>More secure – restricted access to servers &amp; more rigorous backups</td>
</tr>
<tr>
<td>No administrator required</td>
<td>Higher performance due to dedicated servers</td>
</tr>
<tr>
<td></td>
<td>More redundancy – servers have redundant disks and power supplies.</td>
</tr>
</tbody>
</table>

### Wireless Local Area Network

A WLAN uses radio communication, instead of physical wires, to interconnect the nodes of the network. Many home LANs today include a combination of physically wired and wireless devices.
Network Protocols

A network protocol defines how the network will operate. It defines the procedures and the physical connections that are used in the network.

The US postal system provides an analogy. Imagine you are mailing a letter. In the postal system, the data being sent is the contents of your letter. Delivery is ensured by placing the letter in an envelope, applying a stamp, and adding the destination and source addresses. In addition, a return receipt can be requested.

A network protocol defines similar function.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Also known as the Internet protocol suite, TCP/IP is the protocol used to communicate over the Internet. The diagram below shows the TCP/IP architecture.

![TCP/IP Architecture Diagram]

The left hand application (such as an email client) passes data (such as the email you are sending) to TCP/IP’s Application layer. As the data moves down the protocol stack, headers and a footer are added. These add-ons ensure that the data will reach its destination successfully. At the bottom of the protocol stack is the hardware that interfaces to the wires and other media that connect the two TCP/IP endpoints. When the information reaches the right hand protocol stack, it is processed in reverse order. Data integrity is checked, headers and footers are stripped off, and the data (email message) is delivered to the right hand application (email server).
Each node in a TCP/IP network has a 32 bit “IP address”. This address is divided into four, 8-bit octets as follows:

xxx.xxx.xxx.xxx

TCP/IP Information is carried over the physical connection in containers called packets or frames. Each frame includes:

- application data
- physical source media access control (MAC) address
- physical destination MAC address
- error detection.
**Computer Networking 101 (HH – rev1)**

**Ethernet**

Ethernet is a lower layer network protocol is commonly used with TCP/IP and over LANs. Ethernet was originally developed by Xerox. The figure below shows the Ethernet protocol stack in relation to the TCP/IP protocol stack:

![Ethernet Protocol Stack](image)

**Ethernet Standards**

In 1985, Ethernet was established as an international standard called 802.3. Within this standard, there are a number of hardware designations for 802.3 over telephone twisted pair (TTP) wiring. The most common standards are:

- **10BaseT** (10 megabit/second signaling rate)
- **100BaseTX** (100 megabit/second signaling rate)
- **1000BaseT** (1 gigabit/second signaling rate)

Network interface cards usually support one or more of these standards. In a mixed LAN (e.g. 10BaseT and 100BaseT NICs), the network can negotiate down to the lower speed interface. These 3 variations all use the same physical connector, called 8P8C. The image below shows a cable with an 8P8C connector:
The 10BaseT and 100BaseT standards require 4 wires (2 twisted pairs). The 1000BaseT standard uses 8 wires (4 twisted pairs). Standard LAN cables come with 8 wires.

**Wireless Protocols**

The 802.11 standard defines the MAC and physical layers that are used in wireless local area networks (WLANs). These networks are used by products labeled with the “WI-FI” brand. The most common wireless protocols are:

802.11b (11 megabit/second signaling rate)

802.11g (54 megabit/second signaling rate)

LANs can mix wireless and wired components. For example, one can combine wired and wireless routers with wired or wireless PCs.
Home Network Components - Hardware

Most home networks consist of at least the following components:

1. A PC or laptop with a network interface card (NIC). **Note** – PCs and laptops usually come with a network interface card built in.
2. An Ethernet router, switch or hub.
   a. A router passes packets between separate networks (e.g. between your LAN and the Internet).
   b. A switch filters and forwards packets between separate segments of a LAN.
   c. A hub passes packets on to all LAN segments without any filtering.

   **Note** – a LAN that connects to an Internet Service Provider (ISP) requires a least one router with a WAN port. This router is also called the Default Gateway as it is the portal to the Internet. This router will usually include a firewall (more about firewalls later).

3. The physical wires that interconnect these components (unless the network is completely wireless). Category 5 (CAT 5) LAN cables support 10BaseT, 100BaseTX and 1000BaseT versions of Ethernet.

The following additional components are often included in a home LAN:

1. A cable modem (e.g. Xfinity) or optical network terminal (e.g. FIOS) that supports connection to the Internet (and optional TV service) through an Internet Service Provider (ISP).
2. Additional PC(s) or laptop(s) with NIC(s)
3. A printer – historically, printers were connected directly to the PC (usually over USB), and were shared over the network using software. However, network printers are connected directly to the LAN (either wired or wireless).
4. A Smart Phone – these devices connect to the internet through a wireless router using WI-FI.

The diagram below shows a typical home network from a cable TV provider:
The diagram below shows a more complex network with wireless components:

This diagram shows the same complex network with FIOS:
Home Network Components - Software

Peer-to-peer

Windows software supports peer-to-peer networking between PCs on a LAN. Windows peer-to-peer networking requires that each PC in the network be configured in the same Workgroup. However, each PC must be assigned a unique name. Computer names and Workgroup names are assigned when Windows is first installed on the PC. The following steps describe how to configure each PC in Windows XP:

1. Right-click on My Computer on the desktop.
2. Select Properties.
3. Click on the Computer Name tab.
4. Click on the Change button.
5. Ensure that the Computer name is unique in your network.
6. Enter a Workgroup name that will be common to all the PCs in your network.
7. Click on OK, then restart the PC.

Once the PCs are on a common Workgroup, PC resources (files, printers) can be shared.
Domain Name Server (DNS)

The DNS function converts Internet website names into IP addresses. The DNS also locates these websites. The DNS function is activated when you type a uniform resource locator (URL) such as www.google.com into your web browser address field. The URL is converted into an IP address and the website is accessed. Note Google supports a range of IP addresses (64.233.160.0 - 64.233.191.255). The DNS in a home network is often located in the primary router. The ipconfig /all command identifies the location of the DNS server in your network (more on this later).

Dynamic Host Configuration Protocol (DHCP)

The IP address of each network component can be fixed (configured manually, by the user) or it can be configured automatically by DHCP. When activated, DHCP also configures a default route and the DNS server IP address into each LAN component. Most home networks use dynamic IP addresses. The IP address of the DHCP server in your network can be displayed by using the ipconfig /all command.

Firewall

A firewall is a network security system that prevents unauthorized Internet access to the components of your private LAN. A firewall monitors inbound and outbound traffic and restricts this traffic based on a set of rules. A LAN configuration may have multiple firewalls. Typically, the primary router includes a firewall. In addition, each PC may have its own firewall. Windows operating systems include configurable firewalls. Third party firewalls are also available.

- For Windows (XP or 7) the firewall settings are located in Control Panel
- Barracuda is an example of a 3rd party firewall
Computer Networking 101 (HH – rev1)

Diagnostics

ipconfig /all Command

ipconfig /all is a Windows command that returns the current TCP/IP network configuration of the PC. The ipconfig /all command is issued using the following steps:

1. Click on the Start button on the Windows task bar.
2. Click on run...
3. Type cmd <enter> (the DOS window is displayed)
4. Type ipconfig /all <enter>

The following image shows a typical response to the ipconfig /all command:

Note that the IP addresses of the PC issuing the command (192.168.1.6), the DHCP Server (192.168.1.1) and the DNS server (192.168.1.1) are all displayed. In this example, the latter three functions are all contained in the primary router.

“Lease Expires” refers to the IP address that the DHCP assigns to your PC. If you reboot your PC after the lease expiration date, the DHCP may assign a new IP address to your PC if the previous IP address is no longer available. In a home network, your PC’s assigned IP address almost never changes.
**ping Command**

The **ping** command is useful in resolving many network connectivity issues. This command verifies connectivity between the PC and the device addressed by a specific IP address. The ping command also indicates how long it takes (in milliseconds) for the device to respond. The **ping** command is issued using the following steps:

5. Click on the **Start** button on the **Windows task bar**.
6. Click on **run**…
7. Type **cmd** <enter> (the DOS window is displayed)
8. Type **ping** <IP Address> <enter>, where “<IP Address>” is the IP address of the device you wish to ping.

The following image shows the **ping** command when sent to the primary router in a home network:

![Ping Command Image](image)

**Command to identify all active network components**

The following command captures the IP addresses of all of the active components in your network:

```
FOR /L %i IN (1,1,254) DO ping -n 1 192.168.1.%i | FIND /i "Reply">>c:\ipaddresses.txt
```
Note this command may need to be adjusted to the range of addresses in your network. In this example, it is assumed that the addresses in your network are in the form 192.168.1.x, where x is in the range of 0 to 254. This is a common default range for home networks. The results of this command are stored in a text file called “ipaddresses.txt” in the root directory of the “C” hard disk. This command is issued using the following steps:

1. Copy the above command into the clipboard.
2. Click on the Start button on the Windows task bar.
3. Click on run…
4. Type cmd <enter> (the DOS window is displayed)
5. Right-click in the Command window to the right of the prompt and select Paste.
6. Modify the command if needed for your network.
7. Type <enter>
8. The Command window displays an entry as each IP address is tested. This test runs for an extended period of time. Note the test can be stopped at any time by typing <ctrl><c>
9. View the results by opening the c:\ipaddresses.txt file using Notepad. The IP addresses of the valid network components are displayed. Shown below is an example of the file:

```
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>54</td>
<td>42</td>
<td>28</td>
<td>31</td>
</tr>
</tbody>
</table>

In this case, 5 IP addresses were discovered (including address of the PC issuing the command – 192.168.1.6).

Wireshark
Wireshark is free network packet analyzer that can be downloaded off the internet. When executed, Wireshark displays detailed information about the network traffic visible from the PC. The user can view live traffic or the data can be stored in a file. The traffic can also be filtered. Using this tool requires a high degree of network expertise. The screen on the next page shows a sample Wireshark capture:
**Other Resources from CCLS:**

1. Network Your Computers & Devices Step by Step by Ciprian Adrian Rusen  
   CALL NO. 004.68 RUS
2. How Networks Work by Frank J. Derfler and Les Freed  
   CALL NO. 004.6 DER 7th EDITION
3. Wireless Home Networking for Dummies by Daniel D Briere  
   CALL NO. 004.68 BRI  2006, 2nd Ed.
4. The Wireless Networking Starter Kit : the Practical Guide to Wi-Fi Networks for  
   Windows and Macintosh by Adam Engst and Glenn Fleishman  
   CALL NO. 004.68 E
5. Sams Teach Yourself Network Troubleshooting in 24 Hours by Jonathan Feldman  
   CALL NO. 004.6 F
6. Network Security for Dummies by Chey Cobb  
   CALL NO. 005.8 SECURITY COB
7. Networking All-in-One Desk Reference for Dummies by Doug Lowe  
   CALL NO. 004.68 L
8. Networking Bible by Barrie Sosinsky  
   CALL NO. 004.6 S
9. Network Warrior by Gary A. Donahue  
   CALL NO. 004.6 D
    CALL NO. 004.6 R
11. Cisco Networking for Dummies by Ron Gilster  
    CALL NO. 004.68 G  2nd ed.
12. Wiring Home Networks by John Ross and the editors of Sunset Books  
    CALL NO. 004.68 R

Some of these titles are available from other libraries in the system.