Connecting and setting up a network

### Understanding TCP/IP and Windows Networking

TCP/IP is a set of rules that governs the connection of computer systems to the internet.

Communications between computers happens on three levels:

-Hardware level communication

-OS level communication

-Application level communication

Steps involved in the communication process

* One computer finds another
* Both computers agree on the method and rules for communicating
* One computer takes the role of the client and one thales the role of the server, client/server mode.

### Layers of network communication

* When two devices communicate, they must use the same protocol(language)
* Almost all networks today use a group or a suite of protocols known as TCP/IP (Transmission Communication Protocol/ Internet Protocol)
* Data is broken up into segments and each segment is put into packet
* A packet contains the data and information that identifies the type of data, where it came from, and where it is going.

| Header | Senders ip address  Receivers ip address  Protocol  Packet number | 96 bits |
| --- | --- | --- |
| payload | data | 896 bits |
| trailer | Data to show end of packet  Error connection | 32 bits |

### Level 1: Hardware Level

Root level of communication

* Wireless or network cables
* Phone lines or TV cable lines

Includes the network adapter and mac address

* MAC (media access control 48-bit hexadecimal number hard coded on the card by the manufacturer)
* Also known as hardware / physical / adapter address
* Only used on local networks

### Level 2: Operating system level

* Manages commu=unication between itself and another computer using TCP/IP
* Uses IP addressing - a 32 bit (IPv4) or 128 (IPv6) bit string that is assigned to a network connection is first made
* Used to find computers anywhere on
* The internet, Intranets (any private network that uses TCP/IP)

### Level 3: Application level

* Most applications used on the internet or a local network are client/server applications
* Client applications such as (internet explorer, google chrome, outlook)
* Communicate with server applications such as a web server an Email server

Port number

uniquely identifies computer application

Each client and server application installed on a computer listens at a predetermined address that uniquely identifies the application on the computer.

Eg. inbound email port 25

Internet port 80

Socket: an IP address followed by a Colon and a port number

Eg email example: 136.60.30.5**:**25

Webserver example 136.60.30.5**:**80

How IP addresses get assigned

A MAC address is embedded on a network adapter at a factory

Ip addresses are assigned manually or by software

Static IP manually and permanently to a computer or device

Dynamic IP assigned by a server each time the device connects to the network

A DHCP (dynamic host configuration protocol) server assigns addresses to a DHCP client that is requesting an address

IPv6 was created partly due to the shortage of IPv4 addresses

Internet Assigned Numbers Authority (IANA) is responsible for keeping track of assigned IP addresses

IPv4 32 bits long Made of 4 groups each 8 bits long

Four decimal numbers separated by period (decimal = Base 10)

Ex. 72.56.105.12

Octet each of the four decimal numbers 0 to 255 4.8 billion possible IP addresses

### How IP addresses are used

It identifies network and host

Classes are based on the number of possible IP addresses in each network within each data class

Class A addresses

First Octet identifies the network and the last three can be used to identify the host

The second third and fourth octets are used to identify clients on the network or subnets

Using 87 as the network octet

A client address would be 87.0.0.1

Class B Addresses

First two Octets identify The network and last two can be used to identify the host or subnets

The third and fourth octets are used to identify the clients on the network or subnets which means 65 thousand IP addresses on this network

Using 84.24 as the network octets

A client address would be 87.24.0.1

A few IP addresses are reserved for special use by TCP/IP and should not be assigned to a device

255.255.255.255 Used for broadcast messages by TCP/IP background processes

0.0.0.0 currently unassigned IP address

127.0.0.1 Indicates your own computer and is called the loopback address

Subnets using IPv4

Large networks can and should be divided into smaller networks called subnetwork

To divide a network into subnets, you designate a part of the host portion of the IP address as a subnet

The subnet mask identifies which part of an IP address id the network id and which part is the host Id

Subnets masks help a device know if an IP address is part of a network or belongs to another

If you don't divide the network into subnets the default subnet mask is used

Public IP addresses : available to the internet

Private IP addresses used on private networks (not allowed on the internet)

A computer using a private IP address on a private network can still access the internet if

The router or other device that stands between the network and the internet is using NAT (network address translation)

NAT is a TCP/IP control that substitutes the public IP Address of the router for the private IP address of the other computer when these computers need to communicate on the internet

IPv6

Each block is 16 bits

Leading 0s in a 4 character block can be eliminated

0B80 – B80

If block contains all 0 then it can be written as double colons

Character based names identify computers and networks

* Character based names: substitute for IP addresses
* (Host name (computer name) name of a computer
* (workgroup name : identifies a work group or peer to peer networks
* Domain name : identifies a network

TCP/IP protocol used by HTTP- that is the protocol used for the world wide web and used by web browsers and web servers to communicate

HTTPS (HTTP secure) protocol Port 443

HTTP protocol working with a security protocol such as Secure Socket Layer or Transport Layer Security (which is better than SSL) to create a secured socket

Used by web browsers and servers to encrypt the data before it is sent and decrypt the data before it is processed

SMTP Simple Mail transfer protocol port 25

Used to authenticate a user to an email server when the email client first tries to connect to email server to send email

Then send email

SMTP AUTH (authentication) is used.

POP and IMAp is used Port 110 (POP103)

Delivery of email message

Telnet - port 23

Remotely control a computer (not considered secure)

FTP (file transfer Protocol) port 20

SSH (Secure shell) port 22

FTPS ftp secure

Follow these steps to verify and change a TCP/IP wired connection

Click change adapter settings

In networks and sharing

Right click Local area connections and select properties

Select TCP/IPv4 and click properties

Default is Dynamic IP addressing

To change static select use the following IP address

Enter IP mask, subnet and gateway

Wireless network types

Unsecured public hotspots or secured private hotspot

If network is unsecured verify that the windows has configured the network as a public network

Test the connection

Wireless networks are created using access points

Methods used by access points to secure wireless network

* A security key is required
* SSID is not broadcasted
* Only computers with registered MAC addresses are allowed to connect