Connecting and setting up network

find out how to connect to a virtual machine from a different location using a VPN

[Understanding TCP/IP and Windows Networking](#_50spbuogrncl)

[Layers of network communication](#_3782xaemczzc)

[Level 1: Hardware level](#_q2f9ndijsay4)

[Level 2: Operating system level](#_vnu7yq39fcrh)

[Level 3: Application level](#_i39e7tt2rsdp)

[How IP addresses get assigned](#_u1bnjn36w1r)

[How IPv4 addresses are used](#_pa1g6792w6js)

[How IPv6 addresses are used](#_54kfjr1nji4z)

[Character based names identify computers and networks](#_a6fbch9lbxru)

[TCP/IP protocols used by applications](#_k3wh2a54ow9f)

[Connect to a wired network](#_awcz803sam0y)

## Understanding TCP/IP and Windows Networking

* Communications between computers happens on three different levels

1. Hardware
2. OS
3. Application

* Steps involved in the communication process

1. One computer finds another
2. Both computers agree on the methods and rules for communication (protocols)
3. One computer takes on the role of the client and the other of the server, client/server mode.

## Layers of network communication

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

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

## Level 1: Hardware level

* Root level of communication
  + Wireless or network cables
  + Phone liens or TV cable lines
* Includes the network adapter ad the MAC address
  + MAC (media access control) address is a unique 48-bit hexadecimal number hard coded on the card by the manufacturer
  + Also known as hardware address, physical address, adapter address or ethernet address
  + Only used on local networks

## Level 2: Operating system level

* Manages communication 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 when the connection is first made
* Used to find computers anywhere on
  + the internet
  + intranets - any private network that uses TCP/IP protocols
  + subnets

## 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 browser
  + E-mail 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
  + Examples
    - Port 25 is inbound e-mail
    - Port 80 is internet
* Socket
  + IP address followed by a colon and port number
  + Email example: 136.60.30.5:25
  + Web server example: 136.60.30.5:80

## How IP addresses get assigned

* Static IP address: manually and permanently assigned to a computer or device
* Dynamic IP address: 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
* An IP address has 32 or 128 bits
* Internet protocol version 4 (IPv4) – uses a 32 bit address to identify a network connection
  + Currently a shortage of ipv4 addresses
* Internet protocol version 6 (IPv6) was created partly due to the shortage of IPv4 addresses
  + Uses 128 bit IP address
* Internet assigned numbers authority (IANA) is responsible for keeping track of assigned IP addresses

## How IPv4 addresses are used

* IP address: 32 bits long, made up of 4 groups, each 8 bits long
  + Four decimal numbers separated by periods
    - 72.56.105.12
  + Largest possible 8-bit number
    - 11111111 (255 decimal)
  + Largest possible decimal IP address
    - 255.255.255.255
    - 11111111.11111111.11111111.11111111
  + Octet: each of the four decimal numbers
    - 0 to 255
* IP address identifies network and host
  + Classes are based on the number of possible IP addresses in each network within each class
* Class A addresses:
  + First octet identifies the network and the last three can be used to identify the host
    - The second third and forth octets are used to identify clients on the network or subnets which means that there can be up to 16 million IP address on this network
  + 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 clients on the network or subnets which means there can be up to 65 thousand IP address on this network
  + Using 87.24 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
* Public IP addresses: available to the internet
* Private IP addresses: used on private network (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 protocol 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
* Subnets using IPv4
  + Large networks can and should be divided into smaller networks called subnetworks or subnets
  + To divide a network into subnets you designate part of the host portion of the IP address as a subnet
* The subnet mask identifies which part of an IP address is part of its network or belongs to another network
* If you don't divide a network into subnets the default subnet mask is used

## How IPv6 addresses are used

* IPv6 address has 128 bits written as 8 blocks of hexadecimal numbers separated by colons
  + Example

2001:0000:0B80:0000:0000:00D3:9C5A:00CC

* + Each block is 16 bits
    - For example: the first block in the address above is 2001 in hex, which can be written as 0010000000000001 in binary
  + Leading 0s in a 4-character hex block can be eliminated. For example, the IP address above:
    - 2001:0000:B80:0000:0000:D3:9C5A:CC
  + If a block contains all 0s then it can be written as double colons
    - 2001:0000:B80::D3:9C5A:CC

## 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 workgroup on peer to peer networks
  + Domain name: identifies a network
    - Example mycompany.com

## TCP/IP protocols used by applications

* HTTP (hypertext transfer protocol) - is the protocol used for the World Wide Web and used by web browsers and web servers to communicated – port 80
* HTTPS (HTTP Secure) protocol – port 443
  + HTTP protocol working with a security protocol such as secure sockets layer (SSL) or transport layer security (TLS), 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 then decrypt it before the data 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 the email server to send email
  + Then send the e-mail message
  + SMTP AUTH (SMTP Authentication) is used
* POP and IMAP – port 110 (POP3)
  + Deliver of email message
* Telnet – port 23
  + Remotely control a computer
  + Not considered secure

FTP (file transfer protocol) port 20

SSH (Secure Shell)

## Connect to a wired network

* Steps
  + 1. Install network adapter
  + 2. Connect network able to ethernet RJ-45 port and network port
* Troubleshooting
  + Verify deceive manager recognizes adapter without errors
    - If errors, try updating NIC drivers
  + If adapter has no errors, open Network and Sharing Center
    - A red X indicates a problem
    - Click X to start windows network diagnostics
  + After windows has resolved the problem
    - Should see a clear path from the computer~~~~~~~
* Follow these steps to verify and change TCP/IP settings:
  + Click change adapter settings in the network and sharing center
    - In the network connections window, right click local area connection and select properties form the shortcut menu
  + Select TCP/IPv4 and click properties
  + Default setting is dynamic IP addressing
  + Tp change to static select use the following IP address
    - Enter IP address subnet mask and default gateway
* Wireless network types
  + Unsecured public hotspot or succeed private hotspots
* Steps to connect to a wireless network using windows 7:
* If network is unsecured verify that windows has configured the network as a public network
* Test the connection
  + For some hotspots a home page appears and you must enter a password
* Wireless networks are created using access points
* Methods used by access points to secure wireless networks
  + A security key is required
  + SSID is not broadcasted
    - SSID (service set identifier) = name
  + Only computers with registered mac addresses are allowed to connect