**What is TCP/IP?**

TCP/IP stands for Transmission Control Protocol / Internet Protocol. It defines how electronic devices (like computers) should be connected over the Internet, and how data should be transmitted between them. TCP/IP provides end-to-end connectivity. TCP/IP is the basic communication language or protocol of the Internet.

It can also be used as a communications protocol in a private network (either an [intranet](http://searchwindevelopment.techtarget.com/definition/intranet) or an [extranet](http://searchenterprisewan.techtarget.com/definition/extranet)). TCP/IP is a two-layer program. The higher [layer](http://searchsoftwarequality.techtarget.com/definition/layer), Transmission Control Protocol, manages the assembling of a message or file into smaller [packet](http://searchnetworking.techtarget.com/definition/packet)s that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, [Internet Protocol](http://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol), handles the [address](http://searchnetworking.techtarget.com/definition/address) part of each packet so that it gets to the right destination.

**TCP - Transmission Control Protocol**

TCP is responsible for breaking data down into small packets before they can be sent over a network, and for assembling the packets again when they arrive.

**IP - Internet Protocol**

IP is a "connection-less" communication protocol. IP takes care of the communication between computers. It is responsible for addressing, sending and receiving the data packets over the Internet. IP is rule for addressing of computer. IP is responsible for "routing" each packet to the correct destination.

## What is IP Addresses?

IP uses 32 bits, or four numbers between 0 and 255, to address a computer.

IP addresses are normally written as four numbers separated by a period, like this: 192.168.1.50.

Each computer must have an unique IP address before it can connect to the Internet.

Each IP packet must have an address before it can be sent to another computer.

In computer terms, TCP/IP uses 32 bits addressing. It uses 4 **bytes**. One byte is**8 bits**. One byte can contain 256 different values:

00000000, 00000001, 00000010, 00000011, 00000100, 00000101, 00000110, 00000111, 00001000 .......and all the way up to 11111111.

## Three of the most common TCP/IP protocols OR TCP/IP Protocols for the Web.

Web browsers and servers use TCP/IP protocols to connect to the Internet. Common TCP/IP protocols are:

**HTTP - Hyper Text Transfer Protocol**

HTTP takes care of the communication between a web server and a web browser. HTTP is used for sending requests from a web client (a browser) to a web server, returning web content (web pages) from the server back to the client.

**HTTPS - Secure HTTP**

HTTPS takes care of secure communication between a web server and a web browser. HTTPS typically handles credit card transactions and other sensitive data.

**FTP - File Transfer Protocol**

FTP takes care of transmission of files between computers. FTP is not just a protocol; it’s also a program.

## What is Domain Names Server?

A name is much easier to remember than a 12 digit number.

Names used for TCP/IP addresses are called domain names.

www.google.com is a domain name.

When you address a web site, like http:// www.google.com, the name is translated to a number by a Domain Name Server (DNS).

All over the world, DNS servers are connected to the Internet. DNS servers are responsible for translating domain names into TCP/IP addresses.

When a new domain name is registered together with a TCP/IP address, DNS servers all over the world are updated with this information.

## All TCP/IP Protocols

## TCP/IP Protocols for Email

E-mail programs use TCP/IP for sending and receiving e-mails. The TCP/IP protocols for email are:

**SMTP - Simple Mail Transfer Protocol**

SMTP takes care of sending emails. Often emails are sent to an email server (SMTP server), then to other servers, and finally to its destination. SMTP can only transmit pure text. It cannot transmit binary data like pictures, sounds or movies.

**MIME - Multi-purpose Internet Mail Extensions**

The MIME protocol lets SMTP transmit multimedia files including voice, audio, and binary data across TCP/IP networks. The MIME protocol converts binary data to pure text, before it is sent.

**POP - Post Office Protocol**

The POP protocol is used by email programs to retrieve emails from an email server. If your email program uses POP, all your emails are downloaded to your email program (also called email client), each time it connects to your email server.

**IMAP - Internet Message Access Protocol**

The IMAP protocol works much like the POP protocol. The main difference is that the IMAP protocol will not automatically download all your emails each time your email program connects to your email server.

The IMAP protocol allows you to look through your email messages at the email server before you download them. With IMAP you can choose to download your messages or just delete them. This way IMAP is perfect if you need to connect to your email server from different locations, but only want to download your messages when you are back in your office.

## Other TCP/IP Protocols

**ARP - Address Resolution Protocol**

ARP is used by IP to find the hardware address of a computer network card based on the IP address.

**BOOTP - Boot Protocol**

BOOTP (Boot Protocol) is a simple connection-less protocol, typically used by a disc less workstation to discover its Internet address and/or the name of its bootstrap file. BOOTP operates over UDP (User Datagram Protocol). BOOTP simply discovers the parameters needed for the bootstrap procedure. *BOOTP is used for booting (starting) computers from the network.*

**DHCP - Dynamic Host Configuration Protocol**

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. *DHCP is used for allocation of dynamic IP addresses to computers in a network.*

**ICMP - Internet Control Message Protocol**

The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. *ICMP takes care of error-handling in the network.*

**LDAP - Lightweight Directory Access Protocol**

LDAP is used for collecting information about users and e-mail addresses from the internet.

**NTP - Network Time Protocol**

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use. *NTP is used to synchronize the time (the clock) between computers.*

**PPTP - Point to Point Tunneling Protocol**

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. *PPTP is used for setting up a connection (tunnel) between private networks.*

**RARP - Reverse Address Resolution Protocol**

RARP is used by IP to find the IP address based on the hardware address of a computer network card.

**SNMP - Simple Network Management Protocol**

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. *SNMP is used for administration of computer networks.*

**SSL - Secure Sockets Layer**

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. *The SSL protocol is used to encrypt data for secure data transmission.*

**TLS - Transport Layer Security**

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). *The TLS protocol is a newer and more secure version of SSL.*

**Telnet**

Telnet is a network protocol that allows a user on one computer to log onto another computer that is part of the same network. It is an [application layer](https://en.wikipedia.org/wiki/Application_layer) protocol used on the [Internet](https://en.wikipedia.org/wiki/Internet) or [local area networks](https://en.wikipedia.org/wiki/Local_Area_Network).

**SFTP – Secure File Transfer Protocol**

In computing, the SSH File Transfer Protocol (also Secure File Transfer Protocol, or SFTP) is a network protocol that provides file access, file transfer, and file management over any reliable data stream.

**TFTP – Trivial File Transfer Protocol**

Trivial File Transfer Protocol (TFTP) is a simple, lockstep, File Transfer Protocol which allows a client to get from or put a file onto a remote host. One of its primary uses is in the early stages of nodes booting from a local area network.

IT pros and Sys Admins typically use TFTP configuration for:

* Transferring files
* Remote-booting without hard drives
* Upgrading codes
* Backing up network configurations
* Backing up router configuration files
* Saving IOS images
* Booting PCs without a disk

**RDP – Remote Desktop Protocol**

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

**SIP (VoIP) – Session Initiation Protocol**

The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging, over Internet Protocol (IP) networks.

**RTP (VoIP) – Real-time Transport Protocol**

The Real-time Transport Protocol (RTP) is a network protocol for delivering audio and video over IP networks. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications, television services and web-based push-to-talk features.

**SSH - Secure Shell**

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely.

**SCP - Secure Copy Protocol**

Secure copy or SCP is a means of securely transferring computer files between a local host and a remote host or between two remote hosts. It is based on the Secure Shell (SSH) protocol. "SCP" commonly refers to the: Secure Copy Protocol.

**IGMP – Internet Group Management Protocol**

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast.

**TCP – Transmission Control Protocol**

TCP is one of the main protocols in TCP/IP networks. Whereas the IPprotocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

**UDP – User Datagram Protocol**

UDP (User Datagram Protocol) is an alternative communications protocol to Transmission Control Protocol ([TCP](http://searchnetworking.techtarget.com/definition/TCP)) used primarily for establishing low-latency and loss tolerating connections between applications on the Internet. Both UDP and TCP run on top of the Internet Protocol (IP) and are sometimes referred to as UDP/IP or TCP/IP. Both protocols send short packets of data, called [datagrams](http://searchnetworking.techtarget.com/definition/datagram).