

TCP/IP Layers

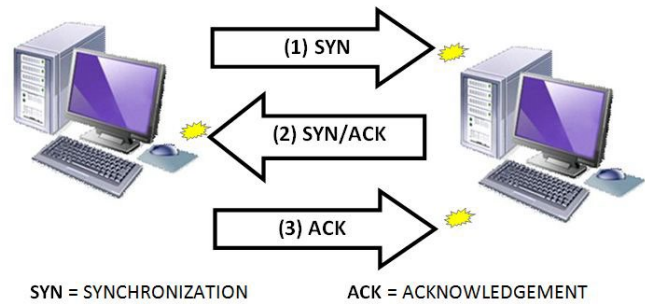
Application layer

This layer represents an interface through a variety of protocols that enable services to be applied to end-user application processes. These services include handling high-level protocols, issuing of representation, encoding, and dialog control.

- **Simple Mail Transfer Protocol (SMTP):** It refers to a TCP/IP protocol that specifies a reliable and efficient transfer of electronic mail service on the Internet.
- **Post Office Protocol, version 3 (POP3):** It refers to a TCP/IP protocol that is designed to allow a workstation to retrieve mail that the server is holding for it.
- **Trivial File Transfer Protocol (TFTP):** It is a small and simple alternative to FTP that uses UDP to transfer files between systems.
- **File Transfer Protocol (FTP):** It refers to a TCP/IP protocol that enables the sharing of computer programs and/or data between hosts over a TCP/IP network. It uses TCP to create a virtual connection for control information and then creates a separate TCP connection for data transfer.
- **Network File System (NFS):** It refers to a TCP/IP protocol that enables computers to mount drives on remote hosts and operate them as if they were local drives.
- **Domain Name System (DNS):** It refers to a TCP/IP protocol that is used on the Internet for translating names of domains and their publicly advertised network nodes into IP addresses.
- **Simple Network Management Protocol (SNMP):** It refers to a TCP/IP protocol that monitors and controls the exchange of management information between networks and network components; it enables network administrators to manage configurations, statistics collection, network performance, and security. SNMP model includes three (3) components:
 - **Managed devices** collect and store management information and make this information available to NMSs using SNMP.
 - An **agent** has local knowledge of management information and translates that information into a form compatible with SNMP.
 - **NMS** executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management.
- **Terminal Emulation Protocol Network (Telnet):** It refers to a TCP/IP protocol that uses the TCP as the transport protocol to establish a connection between server and client. This general-purpose client-server program enables users to log in to remote systems and use resources as if they were connected to a local system. It uses special software called a **daemon**, is referred to as a remote host. A connection using Telnet is called a **Virtual Terminal (VTY) session, or connection**.
- **Remote login application (rlogin):** This is a UNIX command that allows authorized users to log in to other UNIX machines (hosts) on a network and to interact as if the user were physically at the host computer. Once the user is logged into the host, the user can do anything that the host has permitted, such as read, edit, or delete files.
- **Hypertext Transfer Protocol (HTTP):** It refers to an application-level protocol service and an Internet standard developed by the IETF that supports the exchange of information on the World Wide Web, as well as on internal networks.
- **HTTPS (Hypertext Transfer Protocol over Secure Socket Layer):** This is a secure message-oriented communications protocol designed for use in conjunction with HTTP.
 - **Secure Sockets Layer (SSL)** – It is a security protocol that works at a socket level. This layer exists between the TCP layer and the application layer to encrypt/decode data and authenticate concerned entities.

Transport layer

This layer is responsible for reliable end-to-end data delivery from the source host to the destination host. A **three-way handshake** is a method, in which the sender and the receiver inform their respective operating systems that a connection will be initiated before the actual data communication begins.



1. Once the sender transmits a packet, it starts a timer and waits for an acknowledgment from the receiver before sending the next packet. This flow control mechanism that requires the sender to receive an acknowledgment from the receiver after transmitting a certain amount of data is known as the **windowing**.
2. The receiver acknowledges the receipt of data as it arrives. When the buffers on the receiving device are full, a “not ready” indicator/message is sent to the sending device so that the transmission will be suspended until the data in the buffers has been processed.
3. On the other hand, when the receiver can handle additional data, the receiver sends a “ready” transport indicator. When this indicator is received, the sender can resume the segment transmission.
4. This flow control mechanism that requires a receiver to communicate with the sender and send back an acknowledgment message when the data is received is simply known as the **acknowledgment**.

Protocols used in TCP/IP

- **Transport Control Protocol (TCP):** It refers to a **connection-oriented** TCP/IP standard transport layer protocol that provides reliable data delivery, duplicate data suppression, congestion control, and flow control on which many application protocols depend.
- **User Datagram Protocol (UDP):** It refers to a **connectionless** TCP/IP standard transport layer protocol that provides unreliable, best-effort service.

Internet Layer

This layer is responsible for the delivery of service requests that respond from the transport layer and has them arrive at their destination through the “virtual network” image of the internet.

- **Internet Protocol (IP):** It performs the following operations:
 - Defines a packet and an addressing scheme
 - Transfers data between the Internet layer and network access layers
 - Routes packets to remote hosts
- **Internet Control Message Protocol (ICMP):** It refers to a TCP/IP protocol that handles error and controls the process of sending data between computers. Specifically, routers and hosts use ICMP to send reports of problems about packets that return to the original source that sent the packet. ICMP also includes an echo request/reply that is used to test whether a destination is reachable and responding.
- **Internet Group Management Protocol (IGMP):** It refers to a TCP/IP protocol that handles multicasting. Hosts use IGMP to keep local routers apprised of their membership in multicast groups. When all hosts leave a group, routers no longer forward packets that arrive for the group.

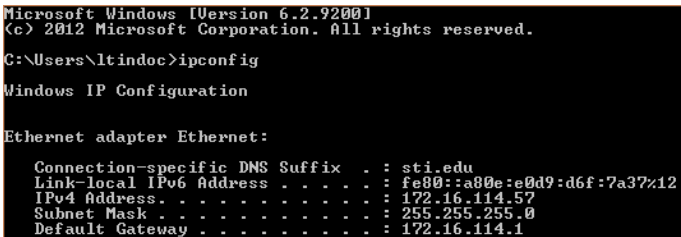
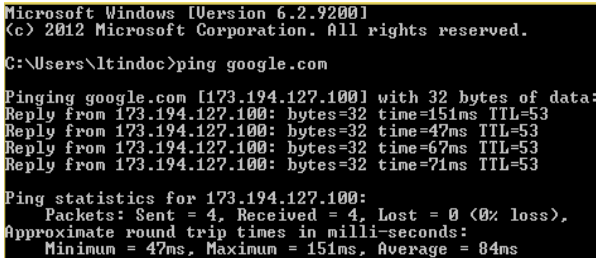
- **Address Resolution Protocol (ARP):** It refers to a TCP/IP protocol that obtains the physical address of a node from a specific IP number. It is used to dynamically bind a high-level IP address to a low-level physical hardware address and is used across a single physical network and is limited to networks that support hardware broadcast.
- **Reverse Address Resolution Protocol (RARP):** It refers to a TCP/IP protocol that allows a host with no local permanent data storage media to find its Internet address given its physical address.

Network Access Layer

This layer is also called the host-to-network layer, which is concerned with all of the issues that an IP packet requires to actually make a physical link to the network media. The network interface layer functions include mapping the IP addresses to physical hardware addresses and encapsulation of IP packets.

- **Ethernet:** It refers to a family of LAN, covered by a group of IEEE 802.3 standards. Ethernet is a best-effort delivery system that uses a CSMA/CD access method.
- **Point-to-Point Protocol (PPP):** This refers to the protocol used for data transfer across a serial line.
- **Fiber distributed data interface (FDDI):** This is a set of ANSI protocols for sending digital data over fiber optic cable.
- **Asynchronous Transfer Mode (ATM):** This refers to a wide area protocol that features high data rates and equal-sized packets/cells that is suitable for text, audio, and video data transfer.
- **Frame Relay:** This is a WAN protocol for LAN internetworking that provides a fast and efficient method of transmitting information from a user device to another across multiple switches and routers.
- **Address Resolution Protocol (ARP):** It refers to a TCP/IP protocol that performs mapping of an IP address to a physical machine that is recognized in the local network.
- **Proxy ARP:** This is used when one needs to move a device from one segment to another, but cannot change its current IP addressing information.
- **Reverse Address Resolution Protocol (RARP):** It refers to a TCP/IP protocol that allows a host with no local permanent data storage media to find its Internet address given its physical address.

Networking Tools

<p>IPCONFIG (IP Configuration tool) is a Console Command which can be issued to the Command Line Interpreter (or command prompt) to display the network settings (e. g. MAC address, IP address, and gateway) currently assigned to any or all network adapters in the machine. This command can be utilized to verify a network connection as well as to verify your network settings.</p>	 <pre> Microsoft Windows [Version 6.2.9200] (c) 2012 Microsoft Corporation. All rights reserved. C:\Users\ltindoc>ipconfig Windows IP Configuration Ethernet adapter Ethernet: Connection-specific DNS Suffix . : sti.edu Link-local IPv6 Address : fe80::a80e:e0d9:d6f:7a37%12 IPv4 Address. : 172.16.114.57 Subnet Mask : 255.255.255.0 Default Gateway : 172.16.114.1 </pre>
<p>PING (Packet Internet Groper) is a diagnostic utility used to determine the quality of your connection to devices/the Internet. It uses the ICMP Echo message and its response to test if a network device on an IP network is reachable. It sends out a packet to a designated internet host or network computer and measures its response time.</p>	 <pre> Microsoft Windows [Version 6.2.9200] (c) 2012 Microsoft Corporation. All rights reserved. C:\Users\ltindoc>ping google.com Pinging google.com [173.194.127.100] with 32 bytes of data: Reply from 173.194.127.100: bytes=32 time=151ms TTL=53 Reply from 173.194.127.100: bytes=32 time=47ms TTL=53 Reply from 173.194.127.100: bytes=32 time=67ms TTL=53 Reply from 173.194.127.100: bytes=32 time=71ms TTL=53 Ping statistics for 173.194.127.100: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 47ms, Maximum = 151ms, Average = 84ms </pre>

Response returned	Which means...
Ping Request could not find Host...	The address you have entered doesn't exist. Check your spelling and try again.
Reply From...	The address that you have entered is alive and is responding to pings.
Request Timed Out...	The address was found but it isn't responding to ping requests.
TTL Expired in Transit...	The TTL value determines the maximum amount of time an IP packet may live in the network without reaching its destination. The number of required hops exceeds TTL.
Destination Host Unreachable...	The host that you are trying to ping is down or is not operating on the network.

TRACERT (MS-DOS and Windows) is used to view the listing of how a network packet travels (sequence of segments or "hops" (i.e., the name of the intermediate hops/routers)) from the source to a remote destination host and where it may fail or slow down.

```
(c) 2012 Microsoft Corporation. All rights reserved.
C:\Users\ltindoc>tracert google.com

Tracing route to google.com [173.194.127.100]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  172.16.114.1
  1  <1 ms  <1 ms  <1 ms  172.16.200.100
  2  <1 ms  <1 ms  <1 ms  122.53.17.129.static.pldt.net [122.53.17.129]
  3  <1 ms  <1 ms  <1 ms  122.2.28.185.static.pldt.net [122.2.28.185]
  4  60 ms  41 ms  61 ms  122.2.28.185.static.pldt.net [122.2.28.185]
  5  54 ms  29 ms  56 ms  210.213.132.18.static.pldt.net [210.213.132.18]
  6  59 ms  61 ms  33 ms  122.2.175.34.static.pldt.net [122.2.175.34]
  7  17 ms  17 ms  18 ms  210.213.133.109.static.pldt.net [210.213.133.109]
  8  *      *      *      Request timed out.
  9  97 ms  81 ms  55 ms  72.14.196.249
 10  *      55 ms  51 ms  209.85.248.62
 11  81 ms  74 ms  53 ms  209.85.241.167
 12 116 ms  31 ms  28 ms  hkg03e12-in-f4.1e100.net [173.194.127.100]

Trace complete.
```

Message	Which means...
Unable to resolve target system <site name>	The name you entered doesn't exist.
Trace complete	Trace was successful.
Request timed out	Either the host or hops on the way didn't respond in the timeout period.
Destination network unreachable	This means that a device that the rest of the Internet is sending traffic to the host cannot connect to it or doesn't know where to send the traffic.

NETSTAT is a utility that tells us what our machine is connected to at the moment the command is run. This makes it a very useful tool to see if spyware, adware, or Trojans have established connections that we do not know about. This tool can display the following information:

- Active TCP connections and ports on which the computer is listening.
- Ethernet statistics
- IP routing table
- IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols)
- IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols)

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.
C:\Users\ltindoc>netstat -an

Active Connections

 Proto Local Address           Foreign Address         State
 TCP   0.0.0.0:135              0.0.0.0:0              LISTENING
 TCP   0.0.0.0:445              0.0.0.0:0              LISTENING
 TCP   0.0.0.0:554              0.0.0.0:0              LISTENING
 TCP   0.0.0.0:2701             0.0.0.0:0              LISTENING
 TCP   0.0.0.0:2869             0.0.0.0:0              LISTENING
 TCP   0.0.0.0:10243            0.0.0.0:0              LISTENING
 TCP   0.0.0.0:49152            0.0.0.0:0              LISTENING
 TCP   0.0.0.0:49153            0.0.0.0:0              LISTENING
 TCP   0.0.0.0:49154            0.0.0.0:0              LISTENING
 TCP   0.0.0.0:49155            0.0.0.0:0              LISTENING
 TCP   0.0.0.0:49161            0.0.0.0:0              LISTENING
 TCP   0.0.0.0:49182            0.0.0.0:0              LISTENING
 TCP   0.0.0.0:49185            0.0.0.0:0              LISTENING
 TCP   127.0.0.1:50748           0.0.0.0:0              LISTENING
 TCP   172.16.114.57:139        0.0.0.0:0              LISTENING
 TCP   172.16.114.57:50690      192.168.0.42:445        ESTABLISHED
 TCP   172.16.114.57:50695      192.168.0.85:445        ESTABLISHED
```

Port State

State	Description
CLOSED	No connection is active or pending.
LISTEN	The server is waiting for an incoming call.
SYN RCVD	A connection request has arrived.
SYN SENT	The client has started to open a connection.
ESTABLISHED	Normal data transfer state.
FIN WAIT 1	Client has confirmed it is finished.
FIN WAIT 2	Server has agreed to release.
TIMED WAIT	Wait for pending packets ("2MSL wait state")
CLOSING	Both sides have tried to close simultaneously.
CLOSE WAIT	Server has initiated a release.
LAST ACK	Wait for pending packets

Netstat Syntaxes

	Displays
netstat	Active connections only, with the full domain name
netstat -a	Active connections and listening ports with full domain name
netstat -ao	Active connections and listening ports with full domain name and PID of the application using it*
netstat -an	Active connections and listening ports but in numeric form (no domain names)
netstat -ano	Active connections and listening ports but in numeric form (no domain names) and PID of the application using it*
netstat -<any of above> 30	Repeats the command, updating the statistics after the number of seconds indicated.
netstat -e	The statistics of the Ethernet
netstat -n	The numerical values of the IP addresses and ports used for active TCP connections
netstat -p <protocol>	The statistics for a specific protocol. The valid values for <protocol> include tcp, udp, ip, icmp

References:

- Mueller, S. (2013). *Upgrading and Repairing PC's 21st Edition*. Indianapolis, Ind.: Que
- Oliviero, A. (2014)., *Cabling: the complete guide to copper and fiber-optic networking, 5th ed*. Indianapolis, IN: John Wiley and Sons
- Sosinsky, B. (2009). *Networking bible*. Indianapolis, IN: Wiley Pub., Inc.
- Tanenbaum, A. (2011). *Computer Networks (5th Edition)*. Boston: Pearson Prentice Hall