

Network+

Mega Guide

Prepare With Confidence

This PrepLogic Mega Guide was written by certified subject matter experts and published authors to provide you accurate, in-depth exam coverage. All exam objectives are covered in detail, giving you the knowledge and confidence you need to pass your exam.



PrepLogic

Be Prepared. Be Confident. Get Certified.



1.0 Network Technologies

1.1 Explain the Function of Common Networking Protocols

TCP

Transmission Control Protocol (TCP), a Transport layer protocol, is a host-to-host, connection-oriented protocol. It enables two hosts to establish a connection and exchange network data. Unlike IP, TCP guarantees data packet delivery and reassembles packets back into the same order in which they were sent.

TCP's connection-oriented properties set it apart from similar protocols, such as UDP (covered next). TCP provides error detection and recovery, flow control, and guaranteed, reliable delivery of data. Network applications that require reliable, guaranteed, error-free delivery use TCP. But TCP does this at a price. The TCP header contains 20 bytes, which means it has more overhead than UDP. Because it has more overhead, it's slower than UDP. To choose between TCP and UDP, decide whether you want speed (UDP) or reliability (TCP).

FTP

The File Transfer Protocol (FTP) is an Application layer protocol that allows a user to upload or download files between hosts. FTP is the simplest way to exchange files between computers on the Internet, and is used on the Web to download files. It's often compared to HTTP, which transfers Web pages, and to SMTP, which transfers e-mail.

FTP operates as a protocol when used by applications. However, FTP also can operate as a program. Users can use FTP to access directories and files and to perform directory operations such as relocating directories or files. FTP is limited to listing and manipulating directories, typing file contents, and transferring files between computers. FTP cannot execute remote files as programs. When paired with Telnet, FTP allows for seamless login to an FTP server for file transfers. FTP also offers authentication security.

UDP

User Datagram Protocol (UDP), also a Transport layer protocol, is a streamlined, economy class version of TCP, earning it the nickname "thin protocol," which means it doesn't take up much bandwidth on the network. UDP is a connectionless, unreliable, low overhead protocol but is faster than TCP. UDP doesn't offer the assurances of TCP, but does do a very good job of getting data from one host to another using lower bandwidth and fewer network resources to do so. It's a good choice to use if guaranteed delivery is not required. UDP is also used when it is paired with a service, such as Network File System (NFS), that contains its own reliability checks. You, for example, would choose UDP for transport for applications such as streaming audio and video. If a packet here or there is lost, by the time TCP retransmitted, it is a moot point.

DHCP

The Dynamic Host Configuration Protocol (DHCP) is used by devices to request an IP address and local network configuration parameters. These most common parameters include an IP address, default gateway, and the DNS server IP address(es). If there is no DHCP server in a network, devices are typically statically configured with this information.

TFTP

Trivial File Transfer Protocol (TFTP) is also similar to FTP in that it facilitates file transfer between computers. The difference between FTP and TFTP is speed. FTP uses TCP, which is reliable but has high overhead, and TFTP uses UDP, which uses much less bandwidth, offering greater speeds but less reliably.

TFTP is a more primitive, simpler version of FTP. TFTP only transfers files. It does not allow the user to browse files in a directory, and there is no security for authentication. TFTP is the protocol of choice for users who know the file location and exactly what files they want. Because TFTP lacks security, it is seldom-used by users. It is, however, used in other applications by system administrators for activities such as downloading a new Internetwork Operating System (IOS) to a Cisco Router.

DNS

The Domain Name Service (DNS) translates and resolves IP addresses into host names or the reverse: resolves host names to IP addresses.

HTTP(S)

Hypertext Transfer Protocol (HTTP) is a control protocol used on the Web to transfer files from a Web server or client PC to a Web browser. When you select a URL, HTTP is the protocol that opens a Web page, no matter where that document is located. HTTP resides in the Application layer of the OSI model, uses little bandwidth, and supports the use of both text and graphics

Hypertext Transfer Protocol Secure (HTTPS) is the secure version of HTTP. HTTPS was developed by Netscape using Netscape's implementation of SSL. HTTPS offers secure message-oriented communications and is designed for use with HTTP. HTTPS allows browsers and servers to sign, authenticate, and encrypt an HTTP network packet. HTTPS uses the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols for security. If you use Internet Explorer as your Web browser and a gold colored lock appears at the bottom of the Web page, you are visiting a secure Web site. If you use Firefox, the address field containing the URL is white with a yellow background. Also, Secure Web sites are also identified by a URL that begins with https:// instead of http://.

ARP

Address Resolution Protocol (ARP) is a Network layer protocol that resolves network (IP) addresses into hardware (MAC) addresses. ARP uses the address resolution cache table built into every network interface card (NIC). This table maps IP addresses to MAC addresses on the network. Whenever a node needs to send a packet, it checks the address resolution cache table to see if the MAC address information for the destination is there. If so, that destination address will be used. If not, an ARP broadcast request is issued. ARP is built into most network operating systems such as Windows, UNIX, and Novell and is executed at a command prompt.

Reverse Address Resolution Protocol (RARP) uses a host MAC address to discover its IP address. The host broadcasts its MAC physical address and a RARP server replies with the host's IP address.

SIP (VoIP)

The Session Initiation Protocol (SIP) is a VoIP call control protocol which is rising in popularity. SIP takes advantage of already used Internet schema; this is because SIP uses a URL to address a specific endpoint (i.e. sip:test@user.com). SIP supports not only VoIP services but also Video over IP, instant messaging and presence.

RTP (VoIP)

The Real-Time Transport Protocol (RTP) is used by most VoIP signaling protocols to transport voice traffic between endpoints. RTP uses UDP to transport this traffic but adds both time-stamping and packet sequencing which do not exist within UDP.

SSH

Secure Shell (SSH) is an application program used to log into another computer on a network, execute commands, and transfer files back and forth. SSH offers secure data transfers as compared to using rlogin, telnet or FTP. Actually, SSH is a suite of protocols; slogin, ssh and scp and requires that the server and client are both running SSH software. It uses strong authentication methods and secure communications. Because the entire session is encrypted, SSH protects against network attacks. SSH use the RSA public-key encryption technology authentication method and can be used on Windows, UNIX, and Mac computers.

POP3

Post Office Protocol version 3 (POP3) is an Application layer protocol used to retrieve e-mail files from an e-mail server. Whenever you connect to a POP3 e-mail server, all messages addressed to your e-mail address are downloaded into your e-mail application. Once e-mail files are downloaded, you can view, modify, and/or delete the messages without further assistance from the POP3 server. POP3 can be used with or without Simple Mail Transfer Protocol (SMTP).

NTP

Network Time Protocol (NTP) is an Internet standard application protocol that sets computer clocks to a standard time source, usually a nuclear clock maintained by the U.S. Naval Observatory Master Clocks. An NTP designated server on a LAN is often deployed to periodically connect to an NTP server on the Internet, assuring accurate synchronization of the LAN NTP server's time clock down to the millisecond. The LAN NTP server then checks and, if necessary, adjusts, all other servers and client computers time clocks assuring accurate time and date stamping of client files.

IMAP4

Internet Message Access Protocol version 4 (IMAP4) is similar to POP3, but supports additional features. IMAP4 allows you to download e-mail, look at or download the message header, store messages in hierarchical structure, and link to documents and Usenet newsgroups. It also provides search commands that allow you to locate messages based on their subject, header, or content. IMAP4 also allows users to manipulate their e-mail and e-mail folders while disconnected from their main messaging system and to synchronize to their message store once the connection is reestablished. IMAP4 also contains authentication components, which support the Kerberos authentication method.

Telnet

Telnet stands for Telephone Network, so called because most Telnet sessions occur over a dial-up network. Telnet is a terminal emulation program often used to connect a remote computer to a Web server but can connect to any kind of server. Once the connection is established, you enter and execute commands using a command prompt. Telnet depends on TCP for transport services and reliable delivery. To start a Telnet session using a Telnet client, you must log onto a Telnet server by entering a valid user name and password.

SMTP

As its name implies, SMTP is used to send e-mail. One thing to remember is how SMTP compares with POP3, which can be used with or without SMTP. SMTP sends e-mail whereas POP3 receives e-mail.

SMTP uses the spooled, or queued, method to deliver e-mail. An e-mail is sent to a destination and is spooled to a hard disk drive. The destination e-mail server regularly checks the spooled e-mail queue for new e-mails, and when it finds new e-mails, forwards or sends them to their destinations.

Most Internet-based e-mail services use SMTP to send e-mails along with either POP3 or IMAP to receive e-mails. SMTP is generally used to send messages between mail servers. This is why you need to specify both the POP3 and the SMTP server IP addresses when you configure your e-mail application.

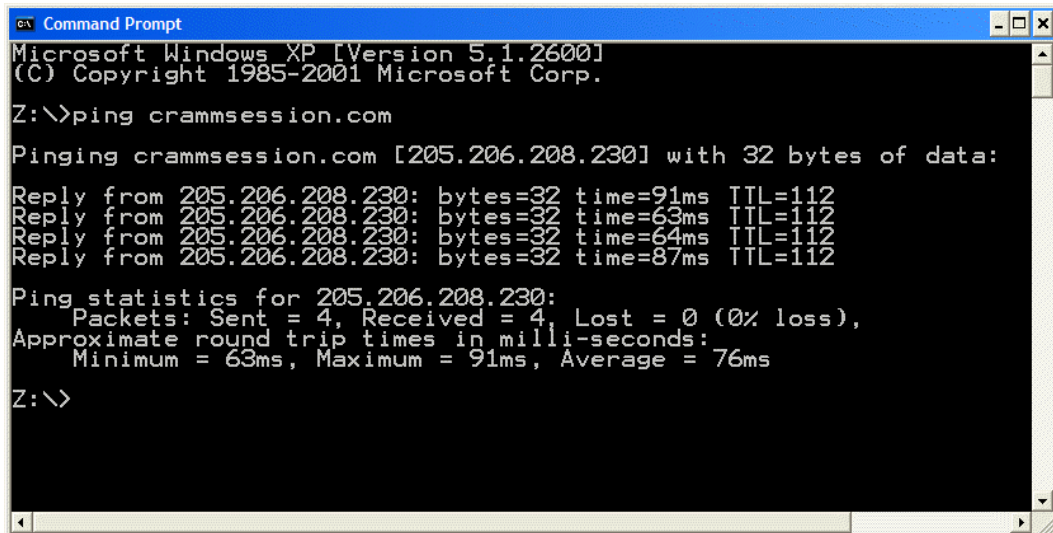
SNMP2/3

Simple Network Management Protocol version 2 and 3 (SNMP2/3) monitors the network and network devices. SNMP sends messages to different parts of a network. SNMP agents store and return data to the SNMP requesters. It uses Management Information [Data] Bases (MIB) to define what information is available from a managed network device.

ICMP

Internet Control Message Protocol (ICMP) works with IP at Layer 3 to provide Network layer management and control. Routers send ICMP control messages in response to undeliverable datagram's. The receiving router places an ICMP message into an IP datagram and sends the datagram back to the source.

ICMP provides feedback about network connectivity problems and the processing of datagram's but does not guarantee reliable delivery. ICMP is built into most network operating systems such as Windows, UNIX, and Novell, and can use packets containing error control. The ping command, for example, uses ICMP to test an Internet connection. When you ping a network device with an IP address, the ICMP part of that host's TCP/IP stack responds to the request.



```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

Z:\>ping crammsession.com

Pinging crammsession.com [205.206.208.230] with 32 bytes of data:

Reply from 205.206.208.230: bytes=32 time=91ms TTL=112
Reply from 205.206.208.230: bytes=32 time=63ms TTL=112
Reply from 205.206.208.230: bytes=32 time=64ms TTL=112
Reply from 205.206.208.230: bytes=32 time=87ms TTL=112

Ping statistics for 205.206.208.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 63ms, Maximum = 91ms, Average = 76ms

Z:\>
```

Figure 1 - Ping Command Results

IGMP

Internet Group Management Protocol (IGMP) is a Network layer protocol that is used by an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows an Internet computer to send content to multiple computers. Multicasting is used to send out company newsletters to an e-mail distribution list, and to broadcast high-bandwidth programs using streaming media to a multicast group membership audience.

TLS

Transport Layer Security (TLS) is the successor to Secure Sockets Layer (SSL) (HTTPS) in providing a secure method for transferring data from server to client. TLS works in a basically similar manner to SSL and supports several different encryption options.

1.2 Identify Commonly Used TCP and UDP Default Ports

Port Number	Services and Protocols	Transport Protocol	Function
20	FTP	TCP	Transfers FTP data when in active mode
21	FTP	TCP	Provides flow control and FTP signaling
22	SSH	TCP	Executes commands and moves files (Remote login protocol)
23	Telnet	TCP	Connects a remote computer to a server
25	SMTP	TCP	Delivers e-mail between e-mail servers
53	DNS	TCP/UDP	Translates host names into IP addresses
67	DHCP	UDP	Listens for DHCP address requests
68	DHCP	UDP	Responds to DHCP address requests
69	TFTP	UDP	Transfers data (simple FTP)
80	HTTP	TCP	Opens a browser connection to a Web page
110	POP3	TCP	Delivers e-mail between a mail server and client
119	NNTP	TCP	Views and writes news articles for various newsgroups
123	NTP	UDP	Sets computer clocks to a standard time
143	IMAP4	TCP	Downloads e-mail or e-mail headers; stores, searches messages from newsgroups
161	SNMP	TCP/UDP	Used to manage configured SNMP devices
443	HTTPS	TCP	Allows browsers and servers to sign, authenticate, and encrypt HTTP network packets (uses SSL)

Table 1 - Commonly used TCP/UDP ports