TCP/IP Core Protocols

The TCP/IP protocol component that is installed in your network operating system is a series of interconnected protocols called the core protocols of TCP/IP. All other applications and other protocols in the TCP/IP protocol suite rely on the basic services provided by the following protocols: IP, ARP, ICMP, IGMP, TCP, and UDP.

IP

IP is a connectionless, unreliable datagram protocol primarily responsible for addressing and routing packets between hosts. Connectionless means that a session is not established before exchanging data. Unreliable means that delivery is not guaranteed. IP always makes a "best effort" attempt to deliver a packet. An IP packet might be lost, delivered out of sequence, duplicated, or delayed. IP does not attempt to recover from these types of errors. The acknowledgment of packets delivered and the recovery of lost packets is the responsibility of a higher-layer protocol, such as TCP. IP is defined in RFC 791.

An IP packet consists of an IP header and an IP payload. Table 1.3 describes the key fields in the IP header.

Table 1.3 Key Fields in the IP Header

IP Header Field	Function
Source IP Address	The IP address of the original source of the IP datagram.
Destination IP Address	The IP address of the final destination of the IP datagram.
Identification	Used to identify a specific IP datagram and to identify all fragments of a specific IP datagram if fragmentation occurs.
Protocol	Informs IP at the destination host whether to pass the packet up to TCP, UDP, ICMP, or other protocols.
Checksum	A simple mathematical computation used to verify the integrity of the IP header.
Time-to-Live (TTL)	Designates the number of networks on which the datagram is allowed to travel before being discarded by a router. The TTL is set by the sending host and is used to prevent packets from endlessly circulating on an IP internetwork. When forwarding an IP packet, routers are required to decrease the TTL by at least one.

Top Of Page

Fragmentation and Reassembly

If a router receives an IP packet that is too large for the network to which the packet is being forwarded, IP fragments the original packet into smaller packets that fit on the downstream network. When the packets arrive at their final destination, IP on the destination host reassembles the fragments into the original payload. This process is referred to as *fragmentation and reassembly* . Fragmentation can occur in environments that have a mix of networking technologies, such as Ethernet or Token Ring.

The fragmentation and reassembly works as follows:

- When an IP packet is sent by the source, it places a unique value in the Identification field.

- The IP packet is received at the router. The IP router notes that the maximum transmission unit (MTU) of the network onto which the packet is to be forwarded is smaller than the size of the IP packet.
- IP divides the original IP payload into fragments that fit on the next network. Each fragment is sent with its own IP header that contains:
    - The original Identification field identifying all fragments that belong together.
    - The More Fragments Flag indicating that other fragments follow. The More Fragments Flag is not set on the last fragment, because no other fragments follow it.
    - The Fragment Offset field indicating the position of the fragment relative to the original IP payload.

When the fragments are received by IP at the remote host, they are identified by the Identification field as belonging together. The Fragment Offset field is then used to reassemble the fragments into the original IP payload.

Top Of Page

ARP

When IP packets are sent on shared access, broadcast-based networking technologies such as Ethernet or Token Ring, the media access control (MAC) address corresponding to a forwarding IP address must be resolved. ARP uses MAC-level broadcasts to resolve a known forwarding IP address to its MAC address. ARP is defined in RFC 826.

For more information about ARP, see "Physical Address Resolution" later in this chapter.

Top Of Page

ICMP

Internet Control Message Protocol (ICMP) provides troubleshooting facilities and error reporting for packets that are undeliverable. For example, if IP is unable to deliver a packet to the destination host, ICMP sends a Destination Unreachable message to the source host. Table 1.4 shows the most common ICMP messages.

Table 1.4 Common ICMP Messages

ICMP Message	Function
Echo Request	Troubleshooting message used to check IP connectivity to a desired host. The ping utility sends ICMP Echo Request messages.
Echo Reply	Response to an ICMP Echo Request.
Redirect	Sent by a router to inform a sending host of a better route to a destination IP address.
Source Quench	Sent by a router to inform a sending host that its IP datagrams are being dropped due to congestion at the router. The sending host then lowers its transmission rate. Source Quench is an elective ICMP message and is not commonly implemented.
Destination Unreachable	Sent by a router or the destination host to inform the sending host that the datagram cannot be delivered.

There are a series of defined Destination Unreachable ICMP messages. Table 1.5 describes the most common messages.

Table 1.5 Common ICMP Destination Unreachable Messages

Destination Unreachable Message	Description
Network Unreachable	Sent by an IP router when a route to the destination network can not be found. This message is obsolete.
Host Unreachable	Sent by an IP router when a route to the destination IP address can not be found.
Protocol Unreachable	Sent by the destination IP node when the Protocol field in the IP header cannot be matched with an IP client protocol currently loaded.
Port Unreachable	Sent by the destination IP node when the Destination Port in the UDP header cannot be matched with a process using that port.
Fragmentation Needed and DF Set	Sent by an IP router when fragmentation must occur but is not allowed due to the source node setting the Don't Fragment (DF) flag in the IP header.
Source Route Failed	Sent by an IP router when delivery of the IP packet using source route information (stored as source route option headers) fails.

ICMP does not make IP a reliable protocol. ICMP attempts to report errors and provide feedback on specific conditions. ICMP messages are carried as unacknowledged IP datagrams and are themselves unreliable. ICMP is defined in RFC 792.

Top Of Page

IGMP

Internet Group Management Protocol (IGMP) is a protocol that manages host membership in IP multicast groups. An *IP multicast group* , also known as a *host group* , is a set of hosts that listen for IP traffic destined for a specific IP multicast address. IP multicast traffic is sent to a single MAC address but processed by multiple IP hosts. A specific host listens on a specific IP multicast address and receives all packets to that IP address. The following are some of the additional aspects of IP multicasting:

- Host group membership is dynamic, hosts can join and leave the group at any time.
- A host group can be of any size.
- Members of a host group can span IP routers across multiple networks. This situation requires IP multicast support on the IP routers and the ability for hosts to register their group membership with local routers. Host registration is accomplished using IGMP.
- A host can send traffic to an IP multicast address without belonging to the corresponding host group.

For a host to receive IP multicasts, an application must inform IP that it will receive multicasts at a specified IP multicast address. If the network technology supports hardware-based multicasting, the network interface is told to pass up packets for a specific IP multicast address. In the case of Ethernet, the network adapter is programmed to respond to a multicast MAC address corresponding the specified IP multicast address.

A host supports IP multicast at one of the following levels:

- Level 0: No support to send or receive IP multicast traffic.
- Level 1: Support exists to send but not receive IP multicast traffic.

- Level 2: Support exists to both send and receive IP multicast traffic. Windows 2000 and Windows NT 3.5 and later TCP/IP supports level 2 IP multicasting.

The protocol to register host group information is IGMP, which is required on all hosts that support level 2 IP multicasting. IGMP packets are sent using an IP header.

IGMP messages take two forms:

- When a host joins a host group, it sends an IGMP Host Membership Report message to the all-hosts IP multicast address (224.0.0.1) or to the specified IP multicast address declaring its membership in a specific host group by referencing the IP multicast address.
- When a router polls a network to ensure that there are members of a specific host group, it sends an IGMP Host Membership Query message to the all-hosts IP multicast address. If no responses to the poll are received after several polls, the router assumes no membership in that group for that network and stops advertising that group-network information to other routers.

For IP multicasting to span routers across an internetwork, multicast routing protocols are used by routers to communicate host group information so that each router supporting multicast forwarding is aware of which networks contain members of which host groups.

IGMP is defined in RFCs 1112 and 2236.

Top Of Page

TCP

TCP is a reliable, connection-oriented delivery service. The data is transmitted in segments. *Connection-oriented* means that a connection must be established before hosts can exchange data. Reliability is achieved by assigning a sequence number to each segment transmitted. An acknowledgment is used to verify that the data was received by the other host. For each segment sent, the receiving host must return an acknowledgment (ACK) within a specified period for bytes received. If an ACK is not received, the data is retransmitted. TCP is defined in RFC 793.

TCP uses byte-stream communications, wherein data within the TCP segment is treated as a sequence of bytes with no record or field boundaries. Table 1.6 describes the key fields in the TCP header.

Table 1.6 Key Fields in the TCP Header

Field	Function
Source Port	TCP port of sending host.
Destination Port	TCP port of destination host.
Sequence Number	Sequence number of the first byte of data in the TCP segment.
Acknowledgment Number	Sequence number of the byte the sender expects to receive next from the other side of the connection.
Window	Current size of a TCP buffer on the host sending this TCP segment to store incoming segments.
TCP Checksum	Verifies the integrity of the TCP header and the TCP data.

Top Of Page

TCP Ports

A TCP port provides a specific location for delivery of TCP segments. Port numbers below 1024 are well-known ports and are assigned by the Internet Assigned Numbers Authority (IANA). Table 1.7 lists a few well-known TCP ports.

Table 1.7 Well-Known TCP Ports

TCP Port Number	Description
20	FTP (Data Channel)
21	FTP (Control Channel)
23	Telnet
80	HTTP used for the World Wide Web
139	NetBIOS session service

For a complete list of assigned TCP ports, see the Internet Assigned Numbers Authority (IANA) Port Numbers link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Top Of Page

TCP Three-Way Handshake

A TCP connection is initialized through a three-way handshake. The purpose of the three-way handshake is to synchronize the sequence number and acknowledgment numbers of both sides of the connection and exchange TCP Window sizes. The following steps outline the process:

1. The client sends a TCP segment to the server with an initial Sequence Number for the connection and a Window size indicating the size of a buffer on the client to store incoming segments from the server.
2. The server sends back a TCP segment containing its chosen initial Sequence Number, an acknowledgment of the client's Sequence Number, and a Window size indicating the size of a buffer on the server to store incoming segments from the client.
3. The client sends a TCP segment to the server containing an acknowledgment of the server's Sequence Number.

TCP uses a similar handshake process to end a connection. This guarantees that both hosts have finished transmitting and that all data was received.

Top Of Page

UDP

UDP provides a connectionless datagram service that offers unreliable, best-effort delivery of data transmitted in messages. This means that neither the arrival of datagrams nor the correct sequencing of delivered packets is guaranteed. UDP does not recover from lost data through retransmission. UDP is defined in RFC 768.

UDP is used by applications that do not require an acknowledgment of receipt of data and that typically transmit small amounts of data at one time. NetBIOS name service, NetBIOS datagram service, and SNMP are examples of services and applications that use UDP. Table 1.8 describes the key fields in the UDP header.

Table 1.8 Key Fields in the UDP Header

Field	Function

Source Port	UDP port of sending host.
Destination Port	UDP port of destination host.
UDP Checksum	Verifies the integrity of the UDP header and the UDP data.

Top Of Page

UDP Ports

To use UDP, an application must supply the IP address and UDP port number of the destination application. A port provides a location for sending messages. A port functions as a multiplexed message queue, meaning that it can receive multiple messages at a time. Each port is identified by a unique number. It is important to note that UDP ports are distinct and separate from TCP ports even though some of them use the same number. Table 1.9 lists well-known UDP ports.

Table 1.9 Well-Known UDP Ports

UDP Port Number	Description
53	Domain Name System (DNS) Name Queries
69	Trivial File Transfer Protocol (TFTP)
137	NetBIOS name service
138	NetBIOS datagram service
161	SNMP

For a complete list of assigned UDP ports, see the Internet Assigned Numbers Authority (IANA) Port Numbers link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Top Of Page

© 2018 Microsoft