TCP/IP Stack Protocols

Connection-Oriented vs Connectionless

Connection-Oriented

A connection-oriented protocol is the TCP protocol.

During the conversation with the destination computer, both the source and destination share information about each other and the progress of the data transfer.

TCP establishes a connection with the other computer using a three-way handshake.

Connectionless

A connectionless protocol is the UDP protocol.

During the transfer with the destination computer, neither the source nor the destination knows the progress of the data transfer.

That statement does not imply that the data transfer is unknown—it is only unknown at the Transport layer. Upper-layer protocols that use UDP might keep track of the data transfer depending on the application.

Key Differences

TCP	UDP
Sequenced	Unsequenced
Reliable	Unreliable
Connection-oriented	Connectionless
Virtual circuit	Low overhead
Acknowledgments	No acknowledgments
Windowing flow control	No windowing or flow control of any type

ICMP

Internet Control Message Protocol (ICMP) is a support protocol for TCP/IP.

It is used by networking devices to identify operation problems.

ICMP operates at layer 3 of the OSI.

IPv6

In IPv6, the ICMP protocol has a much larger role than it does in IPv4.

ICMP in IPv6 is responsible for the Neighbor Discovery Protocol (NDP), which is the equivalent of the Address Resolution Protocol (ARP) in IPv4.

ICMP in IPv6 is also responsible for the discovery of the network gateway(s) with ICMP Router Solicitation (RS) and Router Advertisement (RA) packets so that hosts can find a way out of the network.

In addition, ICMP in IPv6 performs duplicate address detection (DAD) so that hosts do not duplicate IPv6 addressing.

UDP

The User Datagram Protocol (UDP) is a transport protocol for TCP/IP.

UDP is a connectionless, non-sequenced, and non-acknowledged protocol.

Real-time protocols use UDP because the segments are time-sensitive.

TCP

Transmission Control Protocol (TCP) is another transport protocol for TCP/IP.

TCP is a connection-oriented, sequenced, and acknowledged protocol.

Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec) is a combination of two protocols that encrypt data (Encapsulating Security Payload [ESP]) and assure that data has not been altered in transit (Authentication Header [AH]).

IPSec allows private tunnels to be created that are impervious to eavesdropping or tampering.

IPSec is a Network layer protocol, and it's addressed at the network layer with a protocol number of 50 and 51.

IPSec operates in either transport mode or tunnel mode.

The main different between the two modes is what is being protected in IPSec.

In transport mode the data originating from the transport protocol is protected with IPSec and then it is sent to the Network layer for IP transit.

In transport mode the originating IP header itself is not protected, and therefore it can be modified in transit.

In tunnel mode the IPSec protocol will protect the originating IP header by adding an additional IP header to protect the original IP header.

In both modes the payload of data is protected.

Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) is one of two protocols in the IPSec protocol suite.

ESP encrypts the payload using either a shared key (symmetrical encryption) or a private and public keypair (asymmetrical encryption).

Authentication Header (AH)

Authentication Header (AH) is the other protocol in the IPSec protocol suite.

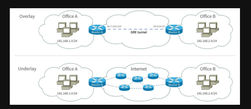
Authentication Header allows for the detection of payload tampering, and because of time stamps, it can prevent replay attacks.

The main difference is that AH authenticates the entire packet rather than just the ESP data and ESP tail, such as the case with just ESP alone.

Both ESP and AH can be used together

Generic Routing Encapsulation (GRE)

Generic Router Encapsulation (GRE) is a layer 3 protocol that allows you to create tunnels over an Internetwork, such as the Internet.



Office A and Office B believe they are directly connected by Router A and Router B, even though there are several Internet routers between them.

The GRE tunnel itself is considered an overlay network because it travels over an underlay network like the Internet.

Without GRE, using a routing protocol such as Open Shortest Path First (OSPF) between two offices separated by the Internet would be impossible.

GRE performs this by encapsulating the original packet with a GRE header, then sending the GRE packet to the destination router in a regular IP packet.

GRE is a Network layer protocol and inside the IP packet the protocol number is 47.

Be warned: GRE is a clear-text protocol.