Topic 05 (TCP/ IP)

Objectives

Describe the purpose of network protocol and the layers in the TCP/ IP architecture.

Describe TCP/ IP Application-layer protocols.

Describe TCP/ IP Transport-layer protocols.

Describe TCP/ IP Internetwork-layers protocols.

Describe TCP/ IP Network access-layer protocols.

TCP/ IP’s layered architecture

* A set of protocol working cooperatively is called protocol suite.
* Most common protocol suite is Transmission Control Protocol/ Internet Protocol (TCP/ IP)
* It is composed of more than dozens of protocols operating at different levels of communication process.

A close-up of a computer

Description automatically generated with low confidence

How the layers work together:

- Web browser starts and user opens home page e.g. <http://www.cengage.com>

- Web browser formats request for home page by using Application-layer protocol HTTP

- Unit of information Application-layer works with is called “data”

- Application-layer protocol passes the request down to the transport layer protocol

- TCP adds a header request

- Unit of information the Transport layer works with is called a segment

- TCP passes the segment to the Internetwork layer protocol (IP)

- IP places its header on the segment

- The unit of information is now called a packet

- Packet is passed down to Network access layer, where the NIC operates

- A frame header and trailer are added

- The frame is delivered to the network medium as bits

- The web server processes it and returns a webpage

- The data part of an Ethernet packet can hold up to 1500 bytes. MAC-addresses (48bits) are 6 bytes wide each and the number of bytes field is 2 bytes wide. That gives the max size of an Ethernet frame to be 1514 bytes.

Remote Desktop Protocol (RDP)

* RDP is used to access a Windows computer remotely by using the Windows GUI

Used to run Windows applications remotely and network administrator use it to manage Windows workstations and servers remotely.

Telnet and Secure Shell (SSH)

* Telnet and Secure Shell (SSH)

Used to connect a device across a network via a command-line interface. E.g. connecting a managed switch or router.

* Telnet uses TCP port 23 (not a secure protocol)
* SSH uses TCP port 22 (provides an encrypted channel between the client and server)

Domain Name Server

* DNS is a name-to-address resolution protocol that keeps a list of computer names and their IP addresses
* Using DNS a user can use a computer’s name instead of using it’s IP address. E.g. when you enter [www.cengage.com](http://www.cengage.com) in your Web browser, the DNS Client service contacts the DNS server specified in your OS’s IP configuration and requests that the name be resolved to an IP address, once the IP address for the website is, returned, your computer can contact Web server to request for Web page
* DNS uses UDP(TCP transport-layer) because DNS messages usually consists of a single packet of data

A picture containing text, screenshot

Description automatically generated

Transport-Layer Protocols

* Transport-layer protocols are used with most Application-layer protocols because they:

1. Supply a header field to identify the Application layer.
2. Provide reliability and flow control for applications that typically transfer a large amount of data.

* TCP Header

A screenshot of a computer

Description automatically generated with low confidence

Role of the Transport Layer

* Transport layer has two protocols:

1. Transmission Control Protocol (TCP)

Connection oriented and designed for reliable transfer of information in complex internetworks.

1. User Datagram Protocol (UDP)

Connectionless and designed for efficient communication of generally small amounts of data.

* TCP vs UDP

Both: Works with segments or datagrams.

Provide a means to identify the source and destination applications involved in a communication.

Protect data with checksum.

Working with Segments and Datagrams

* Transport-layer protocols works with units of data called segments (TCP) or datagrams (UDP)
* Both TCP and UDP add a header to data
* The Transport-layer protocol then passes the segment to the Internetwork protocol (IP)
* With incoming data, the Transport-layer receives the segment from the Internetwork protocol, processes it, de-encapsulates it and send the resulting data to the Application layer

Identifying Source and Destination Applications

* How do computers keep track of incoming data when a Web browser, email application, chat and a word processing program are all running at the same time?
* TCP and UDP use port numbers to specify the source and destination Application-layer protocols
* Port numbers are 16-bit values assigned to specific applications running on a computer or network device

Common port Numbers

* The Internet Assigned Number Authority (IANA) is responsible for global coordination of the DNS Root, IP addressing and other Internet protocol resources. This includes the registration of commonly used port numbers for well-known Internet services.
* Port numbers are divided into three ranges: well-known, registered ports, dynamic ports, or private ports.
* The well-known ports (also known as system ports) are those from – through 1023. The requirements for new assignments in this range are stricter than for other registrations.

Protecting Data with a Checksum

* TCP and UDP provide a checksum similar to the CRC (**an error-detecting code commonly used in digital networks and storage devices)** to protect data integrity.
* Intermediate devices don’t recalculate the checksum in the Transport layer so if data corruption occurs during the transmission, the final receiving station detects the checksum error and discards the data.

TCP: The Reliable Transport Layer

* TCP is used as the Transport-layer protocol if an application requires reliable data transfer.
* TCP provides reliability by:

1. Establishing a connection.
2. Segmenting large chunks of data.
3. Ensuring flow control with acknowledgments.

* TCP is connection-oriented protocol.

It is establishing a connection with the destination; data is transferred and connection is broken.

Establishing a Connection: The TCP Handshake

* A client sends a TCP synchronization (SYN) segment to the destination device, usually a server.

A destination port is specified, and a source port is assigned dynamically.

* When the server receives the SYN segment, it responds by sending either an acknowledgement-synchronization (ACK-SYN) segment or a reset connection (RST) segment.

RST is sent when the server refuses the request to open the session.

If an ACK-SYN is returned, the client completes the three-way handshake by sending an ACK segment back to the server.

Segmenting Data

* When TCP receives data from the Application layer, the size might be too large to send in one piece.
* TCP breaks the data into smaller segments (max frame sent by Ethernet is 1518 bytes)
* Each segment is labeled with a sequence number so that if segments arrive out of order they can be reassembled in the correct order.

Segmentation

A picture containing text, screenshot, number, font

Description automatically generated

Ensuring Flow Control with Acknowledgements

* Flow control prevents a destination from becoming overwhelmed by data, resulting in dropped packets.
* TCP establishes a maximum number of bytes, called the “window size”, that can be sent before the destination mut acknowledge the receipt of data.
* If no acknowledgement is received within a specified period of time, the sending station will retransmit from the point at which an acknowledgment was last received.

Internetwork-Layer Protocols

* The Internetwork layer is where administrators usually do the most network configuration.
* Where the IP protocol operates and is the heart of the TCP/ IP protocol suite
* Responsible for four main tasks:

1. Defines and verifies IP addresses.
2. Routes packets through an internetwork
3. Resolves MAC addresses from IP addresses.
4. Delivers packets efficiently.

Data link layer

* Layer 2 is the Data Link layer. This layer uses a Media Access Controller (MAC) to generate the frames that will be transmitted. MAC controls physical transmission media.
* When transmitting data, this layer adds a header containing the source and destination MAC addresses to the packet received from the Network layer. The frame it creates will then be forwarded to the Physical layer.

Physical Layer

* Layer 1 is the Physical layer. It sends and receives the signal on the physical wire or antenna to transmit the bits found in frames.
* There is a Physical layer found at the end of every network interface.

Data Encapsulation

* When a protocol on the sending system adds data to the packet header, the process is called data encapsulation.

Summary

* TCP/ IP is the main protocol suite used in networks.
* The Application layer consists of protocols such as HTTP and DNS and provides an interface for applications to access network services.
* The Transport layer provides reliability and works with segments (TCP) and datagrams (UDP).
* The Internetwork layer is where most network configuration occurs and is composed of IP, ICMP, and ARP.
* The Network access layer is composed of network technologies, such as Ethernet and WAN technologies.