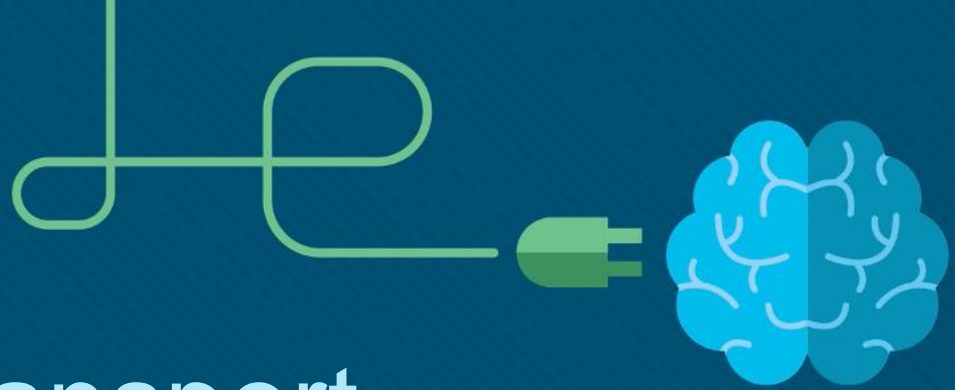




Module 11: Transport Layer Services

Networking Essentials (NETESS)



Module Objective

Module Title: Transport Layer Services

Module Objective: Explain how clients access internet services.

Topic Title	Topic Objective
The Client Server Relationship	Explain client and server interaction.
TCP and UDP	Compare TCP and UDP transport layer functions.
Port Numbers	Explain how TCP and UDP use port numbers.

11.1 The Client Server Relationship

The Client Server Relationship

Client and Server Interaction

- We use network services available over networks and the internet to communicate with others and to perform routine tasks
- A server is a host running a software application (or server service) that provides services to other hosts (clients)
- There are millions of servers on the internet. Clients and servers interact following agreed upon standards and protocols

Type	Description
Email	The email server runs email server software. Clients use mail client software, such as Microsoft Outlook, to access email on the server.
Web	The web server runs web server software. Clients use browser software, such as Windows Internet Explorer, to access web pages on the server.
File	The file server stores corporate and user files in a central location. The client devices access these files with client software such as the Windows File Explorer.

The Client Server Relationship

Video - Web Traffic in Packet Tracer



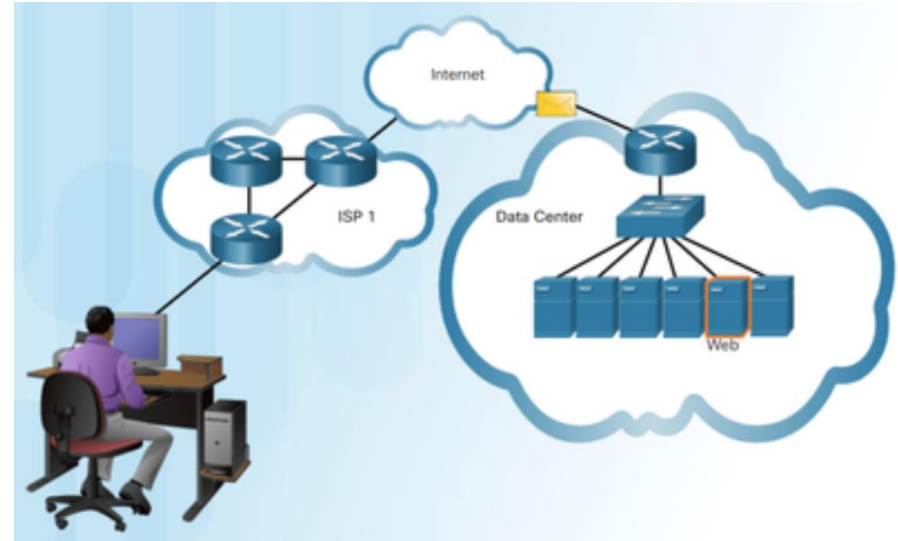
The Client Server Relationship

Client Requests a Web Page

A client/server system is illustrated by the interaction between a web client and a web server:

1. A person uses a web browser to access a web server by sending a request, for example, requesting a web page.
2. The server receives the request and responds by sending the requested web page back to the client.

A web server is usually in a part of the network with other servers called a server farm, or within a data center.



The Client Server Relationship

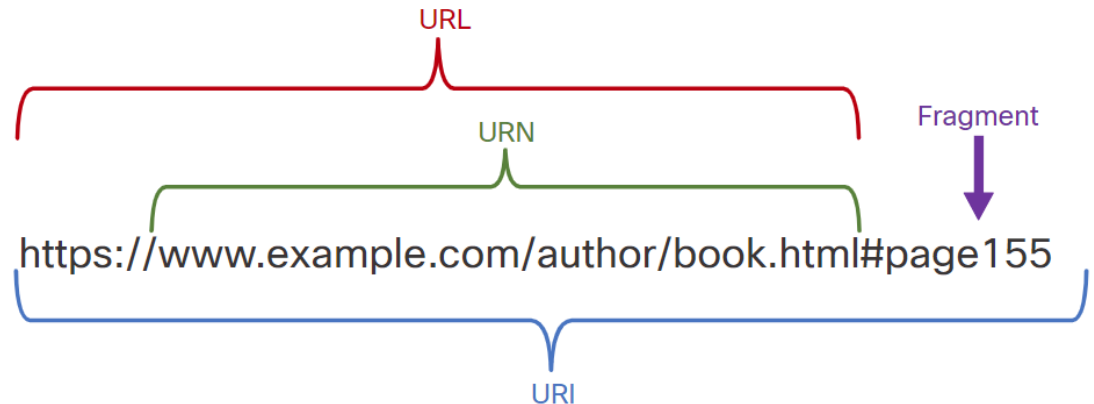
URI, URN, and URL

Uniform Resource Name (URN) - identifies only the namespace of the resource without reference to the protocol

Uniform Resource Locator (URL) - defines the network location of a specific resource on the network.

Components in the example URL:

- **Protocol/scheme** - HTTPS or other protocols such as FTP, SFTP, mailto, and NNTP
- **Hostname** - www.example.com
- **Path and file name** - /author/book.html
- **Fragment** - #page155



The Client Server Relationship

Video - Web Server and Client IP Interactions



Packet Tracer - The Client Interaction

In this activity, you will observe the client interaction between the server and PC.

11.2 TCP and UDP

Protocol Operations

A web server and a web client use specific protocols and standards in the process of exchanging information to ensure that the messages are received and understood. The various protocols necessary to deliver a web page function at the four different layers of the TCP/IP model are as follows:

- **Application Layer Protocol** - Hypertext Transfer Protocol (HTTP) governs the way that a web server and a web client interact.
- **Transport Layer Protocol** - Transmission Control Protocol (TCP) ensures that IP packets are sent reliably, and any missing packets are resent.
- **Internetwork Layer Protocol** - The most common internetwork protocol is Internet Protocol (IP) which is used to identify end hosts and to route packets to destination host.
- **Network Access Layer** - The specific protocol at the network access layer, such as Ethernet, depends on the type of media and transmission methods used in the physical network.

TCP and UDP

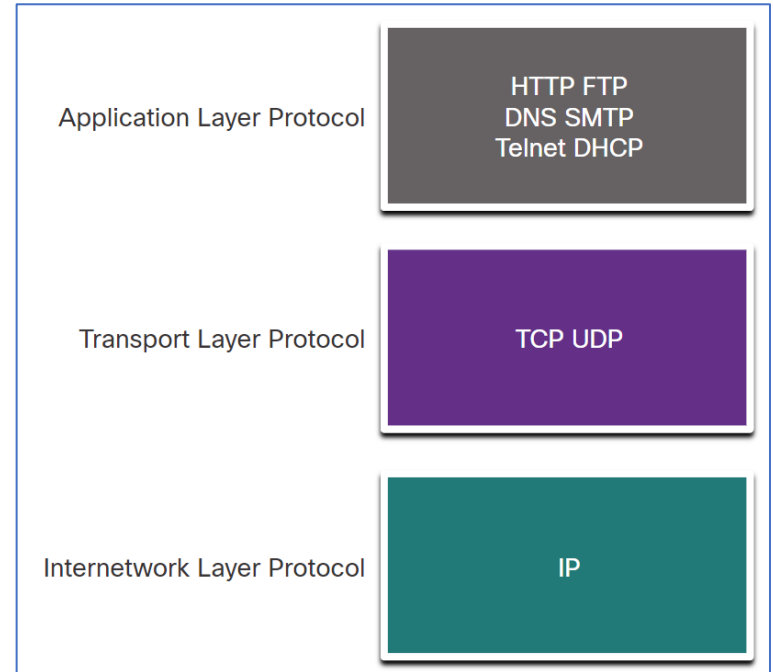
Video - TCP and UDP Operation



TCP and UDP

TCP and UDP

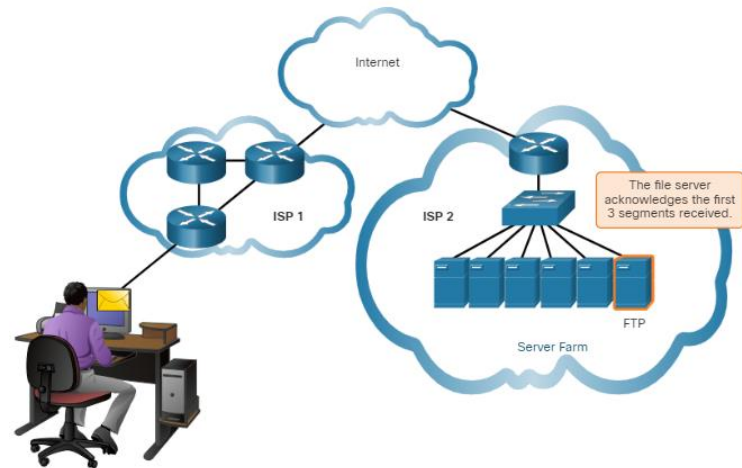
- Each service has its own application protocols that are implemented in the server and client software.
- All the common internet services use Internet Protocol (IP) to address and route messages between source and destination hosts.
- The service application decides which transport protocol to use. Transport protocols specify how to manage the transfer of messages between hosts.
- The two most common transport protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).



TCP Reliability

Transmission Control Protocol (TCP) helps ensure reliable delivery of data packets:

- TCP breaks up a message into small pieces (segments)
- Segments are numbered in sequence and passed to the IP process for assembly into packets.
- TCP tracks the number of segments that have been sent.
- If the sender does not receive an acknowledgment within a certain period, it assumes that the segments were lost and retransmits only the missing portion of the message.



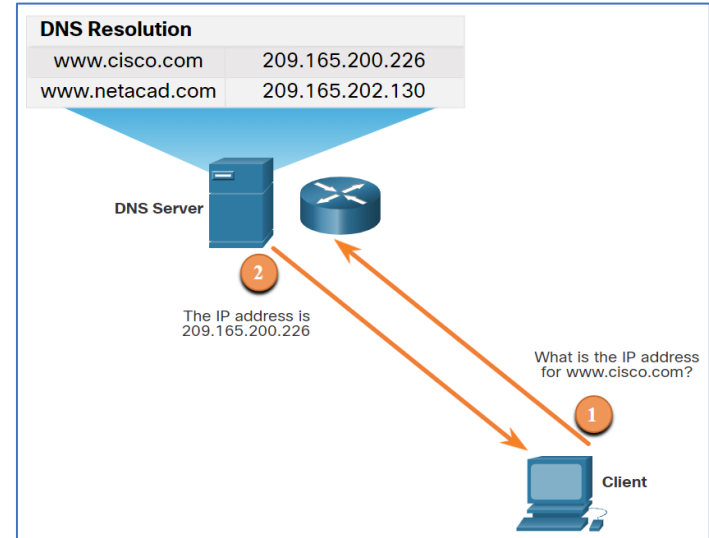
On the receiving host, TCP is responsible for reassembling the message segments in order and passing them to the application.

TCP and UDP

UDP Best Effort Delivery

In some applications, reliable delivery is not required, UDP may be an appropriate transport protocol.

- UDP is a 'best effort' delivery system that does not require acknowledgment of receipt.
- UDP is preferable with applications that use time sensitive technology such as streaming audio and voice over IP (VoIP).
- Acknowledgments would slow down delivery and retransmissions are undesirable.



11.3 Port Numbers

Video - Transport Layer Port Numbers



TCP and UDP Port Numbers

- When a message is delivered using either TCP or UDP, the protocols and services requested are identified by a port number.
- A port is a numeric identifier within each segment that is used to keep track of specific conversations between a client and server.
- Every message that a host sends contains both a source and destination port.
- Ports are assigned and managed by an organization known as the Internet Corporation for Assigned Names and Numbers (ICANN). Ports are broken into three categories and range in number from 1 to 65,535:
 - **Well-Known Ports** - Destination ports that are associated with common network applications. These ports are in the range of 1 to 1023.
 - **Registered Ports** - Ports 1024 through 49151 can be used as either source or destination ports.
 - **Private Ports** - Ports 49152 through 65535 are often used as source ports. These ports can be used by any application.

TCP and UDP Port Numbers (Cont.)

Some Common Well-Known Port Numbers

Port Number	Transport	Application Protocol
20	TCP	File Transfer Protocol (FTP) - Data
21	TCP	File Transfer Protocol (FTP) - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP, TCP	Domain Name Service (DNS)
67	UDP	Dynamic Host Configuration Protocol (DHCP) – Server
68	UDP	Dynamic Host Configuration Protocol - Client

TCP and UDP Port Numbers (Cont.)

Some Common Well-Known Port Numbers

Port Number	Transport	Application Protocol
68	UDP	Dynamic Host Configuration Protocol - Client
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol version 3 (POP3)
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)

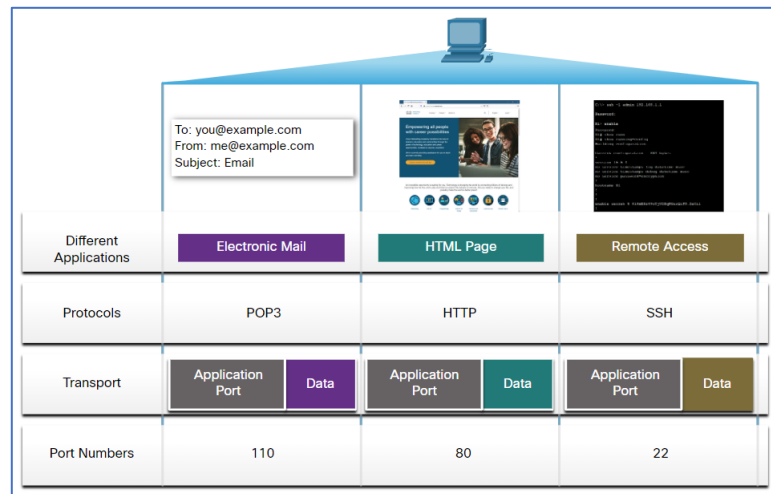
Port Numbers

Destination and Source Port Numbers

The source port number is associated with the originating application on the local sending host. The destination port number is associated with the destination application on the remote host.

Source Port - dynamically generated by the sending device to identify a conversation between two devices. This process allows multiple conversations to occur simultaneously.

Destination Port - The client places a destination port number in the segment to tell the destination server what service is being requested. The server responds to the request and sends information back to the sending device using the source port.

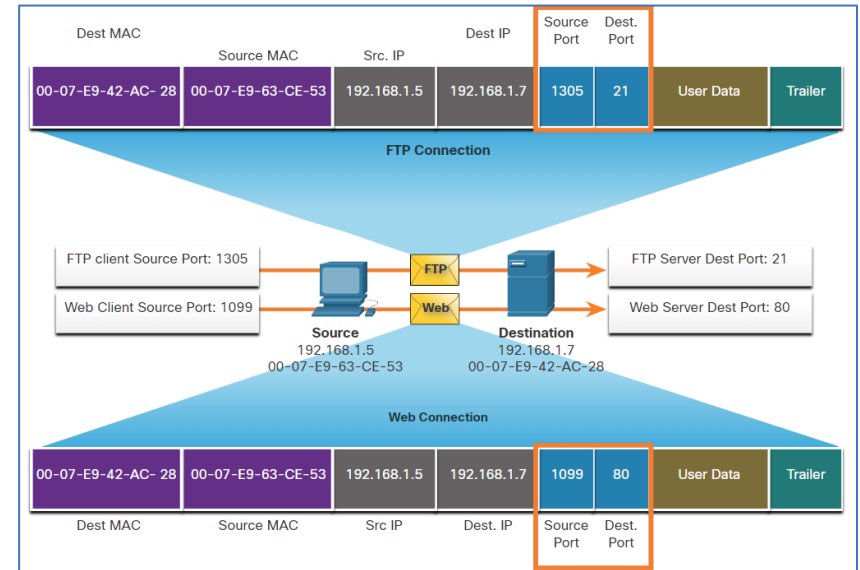


Port Numbers

Socket Pairs

The source and destination ports are placed within the segment PDU. It is encapsulated within an IP packet which contains the IP address of the source and destination. The combination of the source IP address and source port number, or the destination IP address and destination port number is known as a **socket**.

- In the example, the socket is used to identify the server and service being requested by the client. A client socket might look like 192.168.1.5:1099. The socket on a web server might be 192.168.1.7:80
- Together, these two sockets combine to form a socket pair: 192.168.1.5:1099, 192.168.1.7:80
- The source port number acts as a return address for the requesting application.



The netstat Command

- Unexplained TCP connections can pose a major security threat.
- On a PC, the command **netstat** lists the protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state.

In the example, the two lines highlighted with the red block indicate that the PC opens two web requests with the same web server. Notice that the PC generates two different source ports to maintain these two web sessions.

```
C:\> netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP   192.168.1.124:3126      192.168.0.2:netbios-ssn ESTABLISHED
TCP   192.168.1.124:3158      207.138.126.152:http    ESTABLISHED
TCP   192.168.1.124:3159      207.138.126.169:http    ESTABLISHED
TCP   192.168.1.124:3160      207.138.126.169:http    ESTABLISHED
TCP   192.168.1.124:3161      sc.msn.com:http         ESTABLISHED
TCP   192.168.1.124:3166      www.cisco.com:http      ESTABLISHED
```

11.4 Transport Layer Services Summary

What Did I Learn in this Module?

- In the client/server model, the term server refers to a host running a software application that provides information or services to other hosts connected to the network. The client refers to a host running a software application makes a service request to a server.
- TCP and UDP are two network protocols operating at the Transport Layer.
- TCP provides mechanisms to ensure reliable data packets delivery with sequencing and acknowledgement. However, the acknowledgement slows down the packet delivery process.
- UDP is a 'best effort' delivery system that does not require acknowledgment of receipt.
- A port is a numeric identifier within each segment that is used to keep track of specific conversations between a client and server.
- Source port number is dynamically generated by the sending device as a return address.
- Destination port identifies the intended service requested by a client.
- Port numbers are in three categories: well-known ports, registered ports, and private ports.
- Command **netstat** lists the protocols in use, the local address and port numbers, the foreign address and port numbers, and the connection state.

Module 11 - Transport Layer Services

New Terms and Commands

- transport layer protocols
- URI, URN, and URL
- Transport Control Protocol (TCP)
- User Datagram Protocol (UDP)
- reliable delivery system (TCP)
- sequencing and acknowledgement
- best-effort delivery system (UDP)
- TCP and UDP port numbers
- source and destination port numbers
- well-known ports
- registered ports
- private ports
- socket
- socket pair
- netstat command

