Module 14: Transport Layer

Instructor Materials

Introduction to Networks v7.0
(ITN)

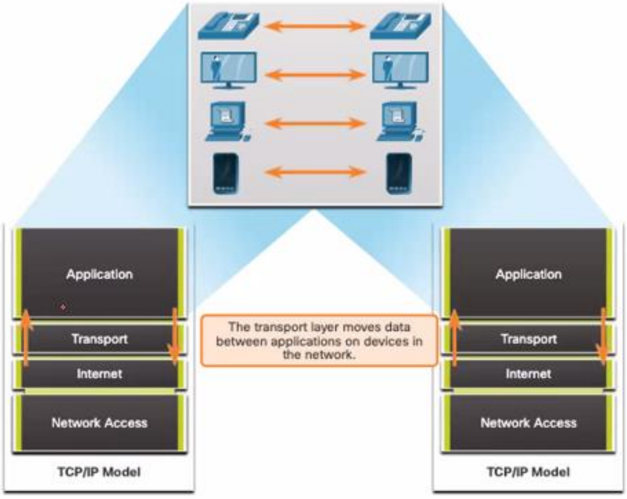
14.1 Transportation of Data

Transportation of Data

Role of the Transport Layer

The transport layer is:

- responsible for logical communications between applications running on different hosts.
- The link between the application layer and the lower layers that are responsible for network transmission.



The transport layer moves data between applications on devices in the network.

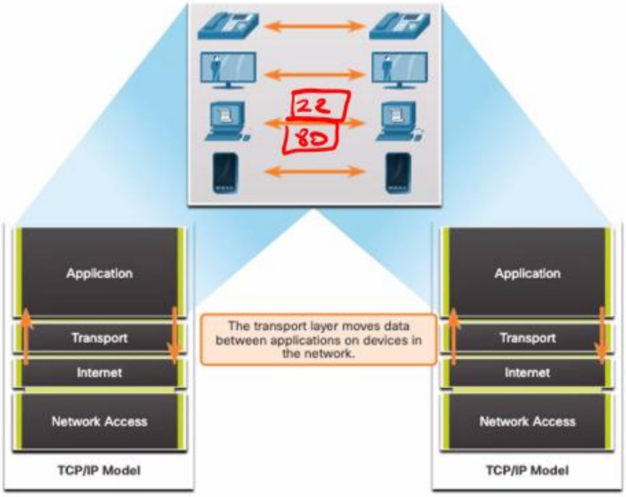
Transportation of Data

Role of the Transport Layer

22 = è un pacchetto SSH
80: è un pacchetto http

The transport layer is: L4

- responsible for logical communications between applications running on different hosts.
- The link between the application layer and the lower layers that are responsible for network transmission.



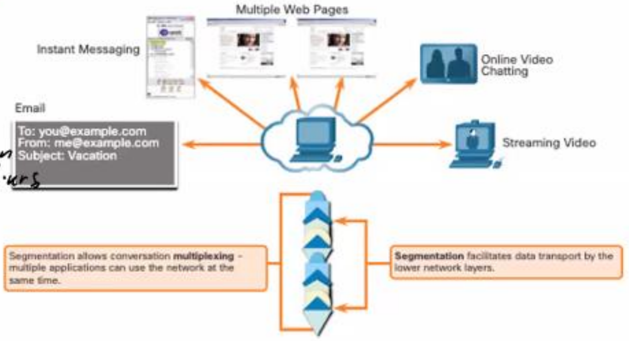
The transport layer moves data between applications on devices in the network.

Transportation of Data

Transport Layer Responsibilities

The transport layer has the following responsibilities:

- Tracking individual conversations
- Segmenting data and reassembling segments
- Adds header information TCP e UDP usano un header
- Identify, separate, and manage multiple conversations
- Uses segmentation and multiplexing to enable different communication conversations to be interleaved on the same network



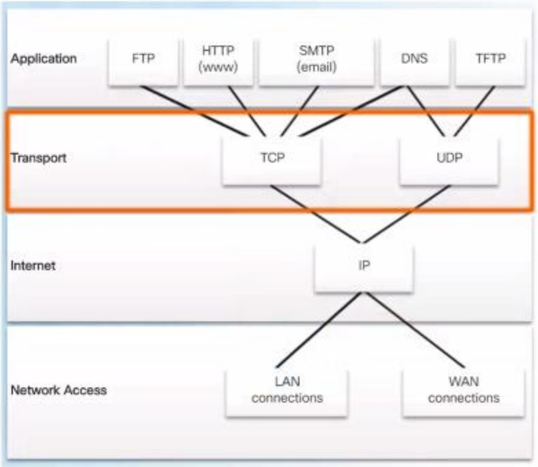
Segmentation allows conversation **multiplexing** - multiple applications can use the network at the same time.

Segmentation facilitates data transport by the lower network layers.

Transportation of Data

Transport Layer Protocols

- IP does not specify how the delivery or transportation of the packets takes place.
- Transport layer protocols specify how to transfer messages between hosts, and are responsible for managing reliability requirements of a conversation.
- The transport layer includes the TCP and UDP protocols.



Transportation of Data

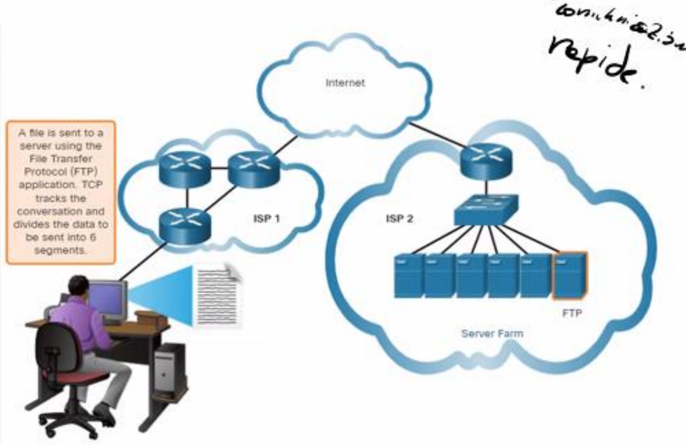
Transmission Control Protocol

Tcp ← per comunicazioni affidabile

UDP
↓
per comunicazione rapide.

TCP provides reliability and flow control. TCP basic operations:

- Number and track data segments transmitted to a specific host from a specific application
- Acknowledge received data
- Retransmit any unacknowledged data after a certain amount of time
- Sequence data that might arrive in wrong order
- Send data at an efficient rate that is acceptable by the receiver



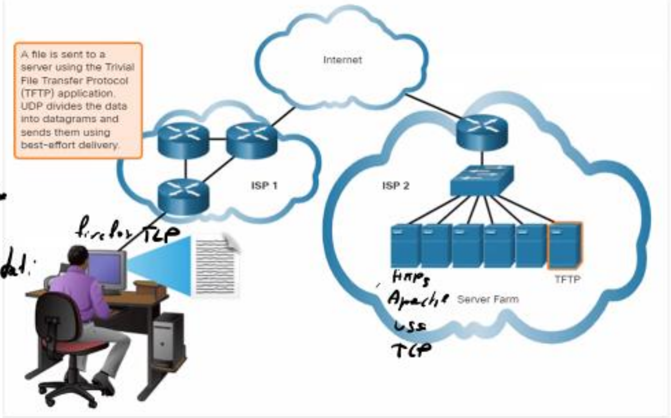
A file is sent to a server using the File Transfer Protocol (FTP) application. TCP tracks the conversation and divides the data to be sent into 6 segments.

Transportation of Data

User Datagram Protocol (UDP)

UDP provides the basic functions for delivering datagrams between the appropriate applications, with very little overhead and data checking.

- UDP is a connectionless protocol. ← non fa una connessione PRIMA di inviare i dati
- UDP is known as a best-effort delivery protocol because there is no acknowledgment that the data is received at the destination.



A file is sent to a server using the Trivial File Transfer Protocol (TFTP) application. UDP divides the data into datagrams and sends them using best-effort delivery.

firefox TCP

Https
Apache
uss
TCP

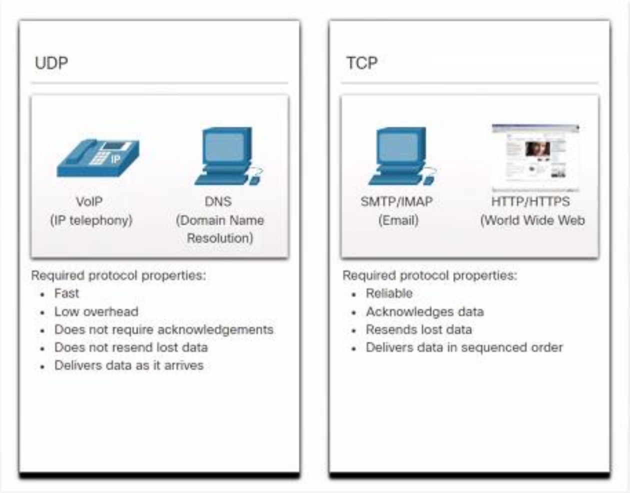
Transportation of Data

The Right Transport Layer Protocol for the Right Application

UDP → comunicazioni voce/video

UDP is also used by request-and-reply applications where the data is minimal, and retransmission can be done quickly.

If it is important that all the data arrives and that it can be processed in its proper sequence, TCP is used as the transport protocol.



UDP

VoIP (IP telephony)

DNS (Domain Name Resolution)

Required protocol properties:

- Fast
- Low overhead
- Does not require acknowledgements
- Does not resend lost data
- Delivers data as it arrives

TCP

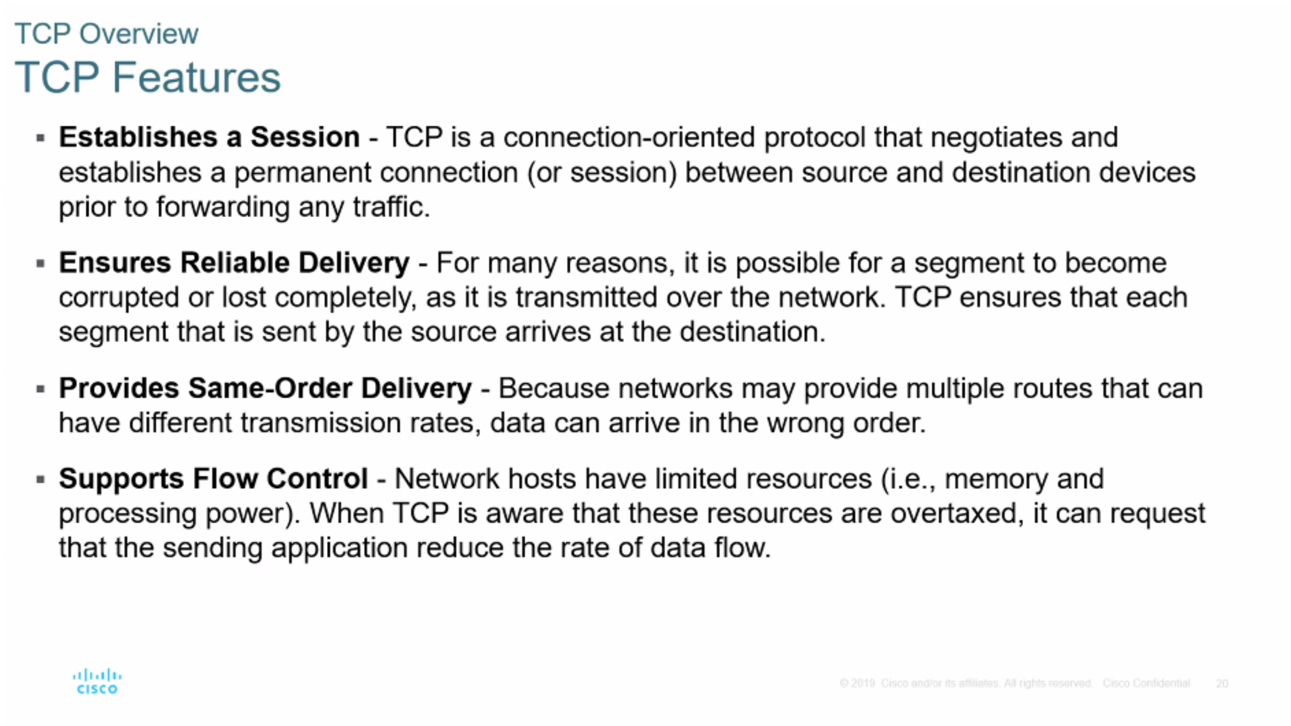
SMTP/IMAP (Email)

HTTP/HTTPS (World Wide Web

Required protocol properties:

- Reliable
- Acknowledges data
- Resends lost data
- Delivers data in sequenced order

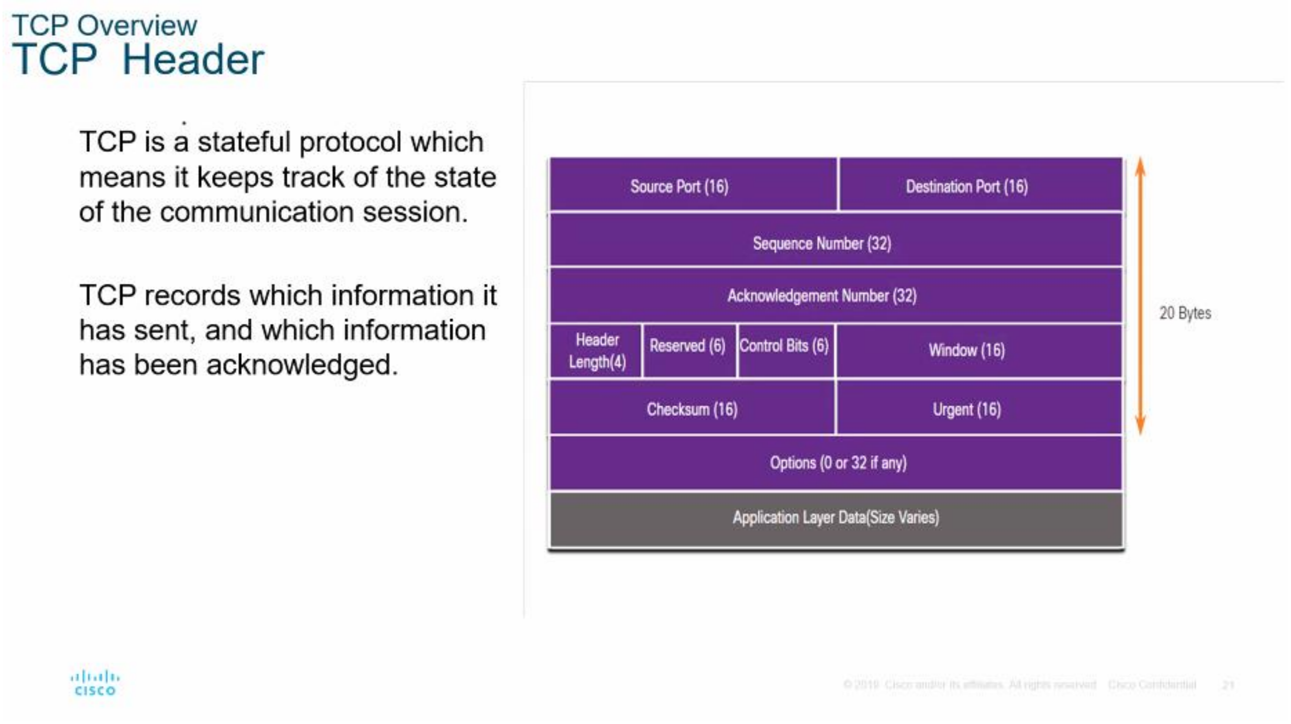
14.2 TCP Overview



TCP Overview

TCP Features

- **Establishes a Session** - TCP is a connection-oriented protocol that negotiates and establishes a permanent connection (or session) between source and destination devices prior to forwarding any traffic.
- **Ensures Reliable Delivery** - For many reasons, it is possible for a segment to become corrupted or lost completely, as it is transmitted over the network. TCP ensures that each segment that is sent by the source arrives at the destination.
- **Provides Same-Order Delivery** - Because networks may provide multiple routes that can have different transmission rates, data can arrive in the wrong order.
- **Supports Flow Control** - Network hosts have limited resources (i.e., memory and processing power). When TCP is aware that these resources are overtaxed, it can request that the sending application reduce the rate of data flow.



TCP Overview

TCP Header

TCP is a stateful protocol which means it keeps track of the state of the communication session.

TCP records which information it has sent, and which information has been acknowledged.

Source Port (16)		Destination Port (16)	
Sequence Number (32)			
Acknowledgement Number (32)			
Header Length(4)	Reserved (6)	Control Bits (6)	Window (16)
Checksum (16)		Urgent (16)	
Options (0 or 32 if any)			
Application Layer Data(Size Varies)			

Statefull: tiene traccia delle informazioni della comunicazione

TCP Overview

TCP Header Fields

1 dst: 80 src = 10120

PC A
dst-port = 80
src-port = 22110

1. dst: 10120 src = 80

2. dst = 22110 src = 80

TCP Header Field	Description
Source Port	A 16-bit field used to identify the source application by port number.
Destination Port	A 16-bit field used to identify the destination application by port number. 80, 22, 31
Sequence Number	A 32-bit field used for data reassembly purposes. ← riordina i pacchetti
Acknowledgment Number	A 32-bit field used to indicate that data has been received and the next byte expected from the source. quanto ho ricevuto e cosa mi aspetto
Header Length ← 20 byte	A 4-bit field known as "data offset" that indicates the length of the TCP segment header.
Reserved	A ~~6~~ 4-bit field that is reserved for future use. usi futuri
Control bits ←	A 6-bit field used that includes bit codes, or flags, which indicate the purpose and function of the TCP segment. 8 ~~[illegible]~~ danno delle funzioni e scopi particolari al pacchetto
Window size flow control	A 16-bit field used to indicate the number of bytes that can be accepted at one time.
Checksum ← controllo dell'errore	A 16-bit field used for error checking of the segment header and data.
Urgent	A 16-bit field used to indicate if the contained data is urgent.

Eth | IP | TCP | Dati | Eth ←

↑ controllo dell'errore

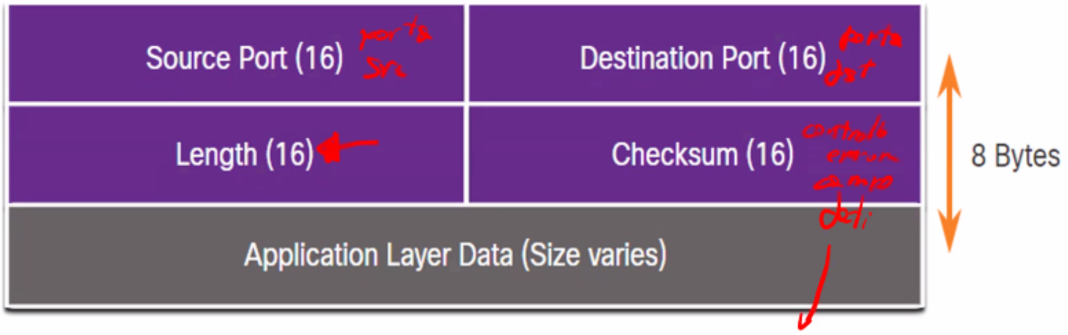
UDP Overview

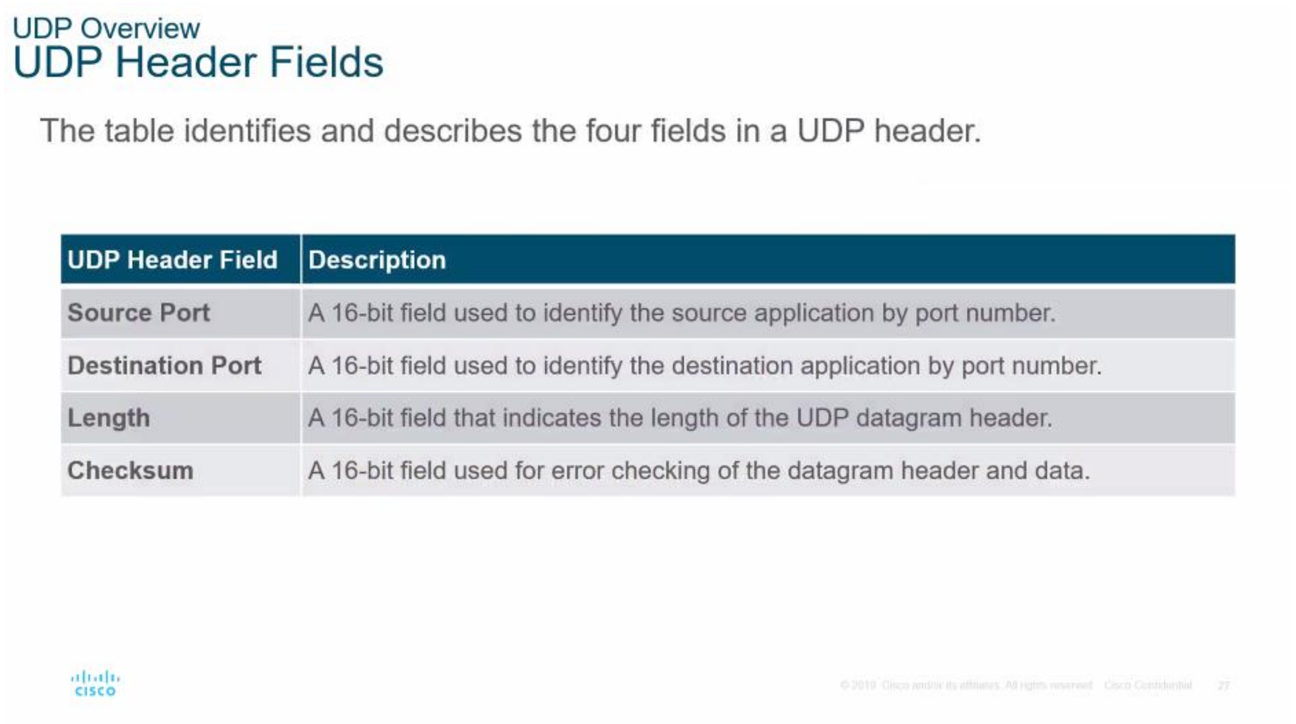
UDP Header

TCP = 20 bytes

UDP = 8 bytes

The UDP header is far simpler than the TCP header because it only has four fields and requires 8 bytes (i.e. 64 bits).



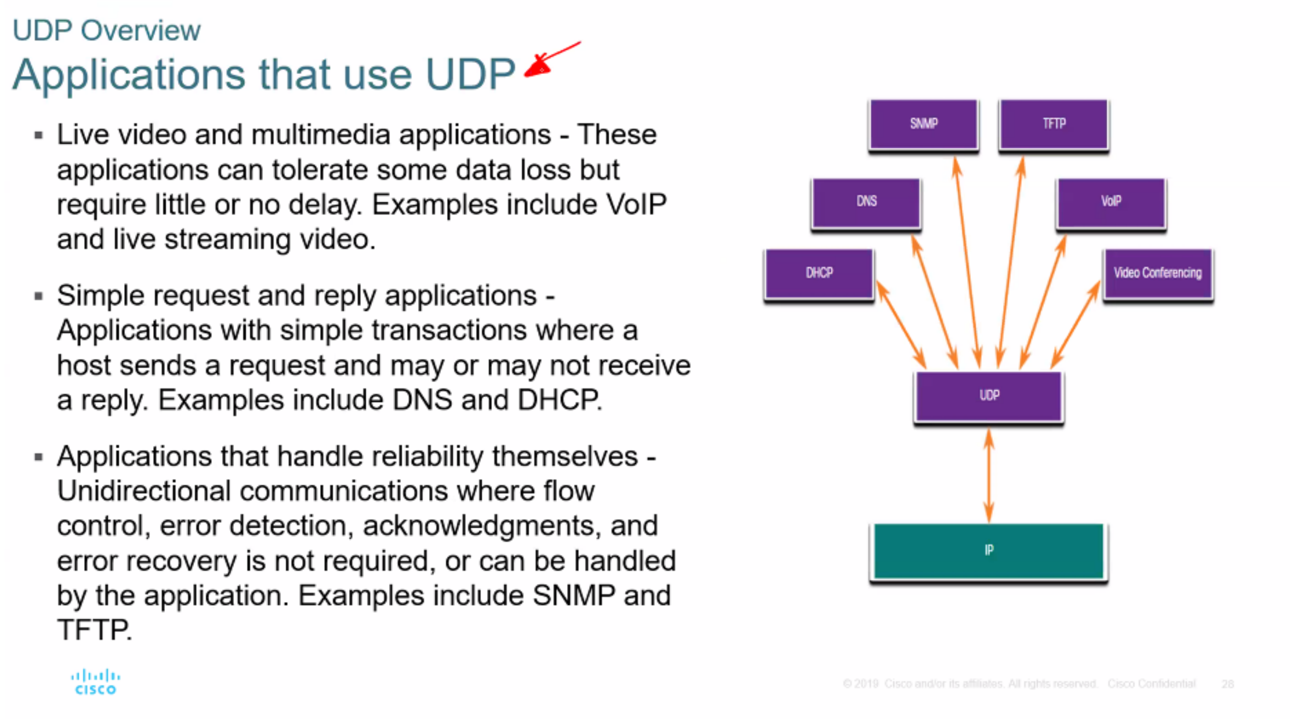


UDP Overview

UDP Header Fields

The table identifies and describes the four fields in a UDP header.

UDP Header Field	Description
Source Port	A 16-bit field used to identify the source application by port number.
Destination Port	A 16-bit field used to identify the destination application by port number.
Length	A 16-bit field that indicates the length of the UDP datagram header.
Checksum	A 16-bit field used for error checking of the datagram header and data.



UDP Overview

Applications that use UDP

- Live video and multimedia applications - These applications can tolerate some data loss but require little or no delay. Examples include VoIP and live streaming video.
- Simple request and reply applications - Applications with simple transactions where a host sends a request and may or may not receive a reply. Examples include DNS and DHCP.
- Applications that handle reliability themselves - Unidirectional communications where flow control, error detection, acknowledgments, and error recovery is not required, or can be handled by the application. Examples include SNMP and TFTP.

Port Numbers
Multiple Separate Communications

TCP and UDP transport layer protocols use port numbers to manage multiple, simultaneous conversations.

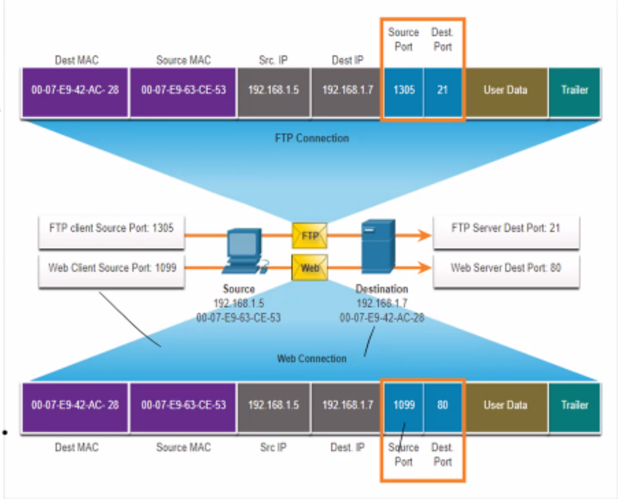
The source port number is associated with the originating application on the local host whereas the destination port number is associated with the destination application on the remote host.

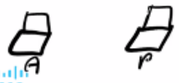
Source Port (16)
Destination Port (16)

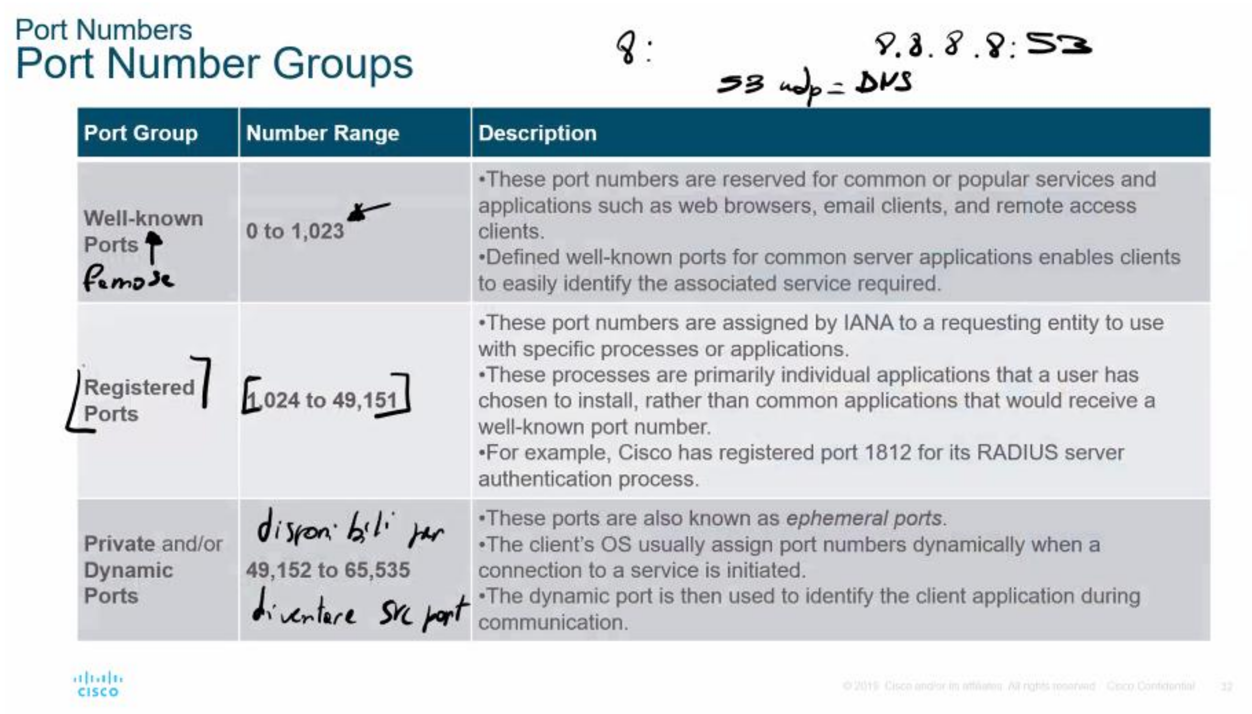
Port numbers
Socket Pairs

1.[192.168.1.5:1035] ,[192.168.1.7:21] Server A
ospite inerto

- The source and destination ports are placed within the segment.
- The segments are then encapsulated within an IP packet.
- 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. [socket]
- Sockets enable multiple processes, running on a client, to distinguish themselves from each other, and multiple connections to a server process to be distinguished from each other.







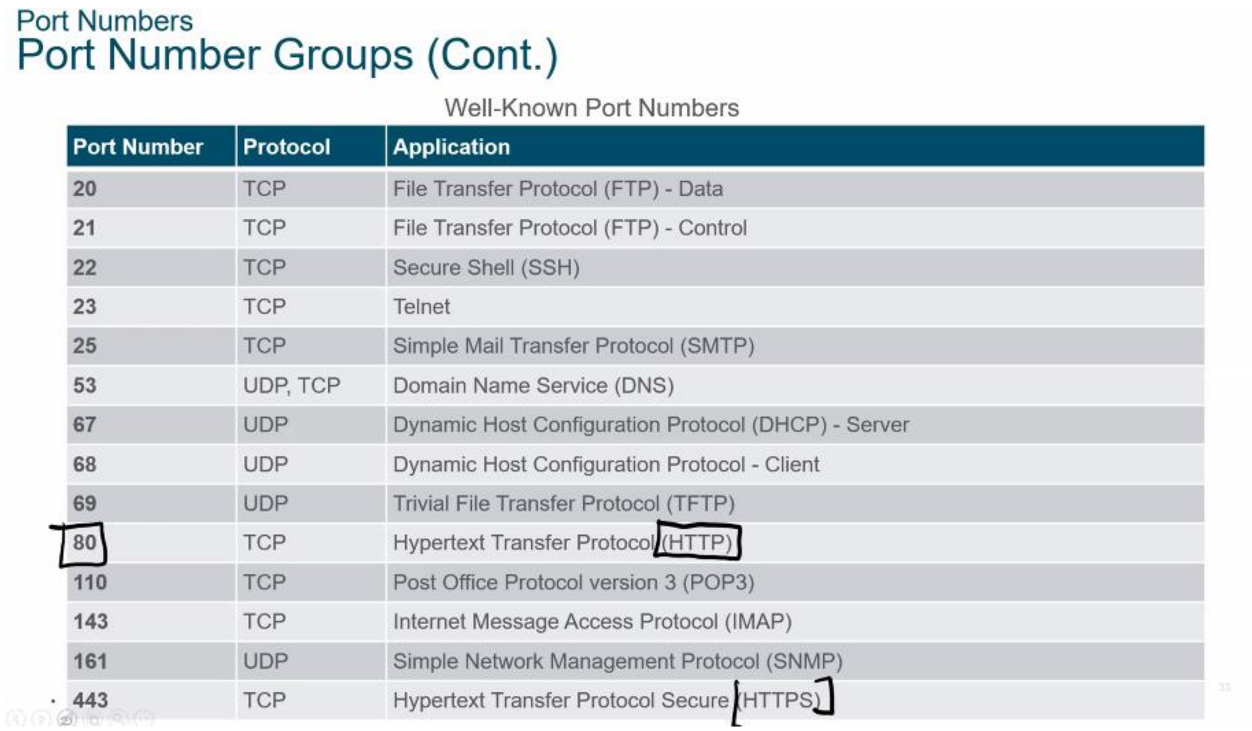
Port Numbers

Port Number Groups

8: 8.8.8.8:53

53 udp = DNS

Port Group	Number Range	Description
Well-known Ports ↑ Remote	0 to 1,023 ←	•These port numbers are reserved for common or popular services and applications such as web browsers, email clients, and remote access clients. •Defined well-known ports for common server applications enables clients to easily identify the associated service required.
Registered Ports	1,024 to 49,151	•These port numbers are assigned by IANA to a requesting entity to use with specific processes or applications. •These processes are primarily individual applications that a user has chosen to install, rather than common applications that would receive a well-known port number. •For example, Cisco has registered port 1812 for its RADIUS server authentication process.
Private and/or Dynamic Ports	disponibili per 49,152 to 65,535 diventare src port	•These ports are also known as *ephemeral ports*. •The client's OS usually assign port numbers dynamically when a connection to a service is initiated. •The dynamic port is then used to identify the client application during communication.

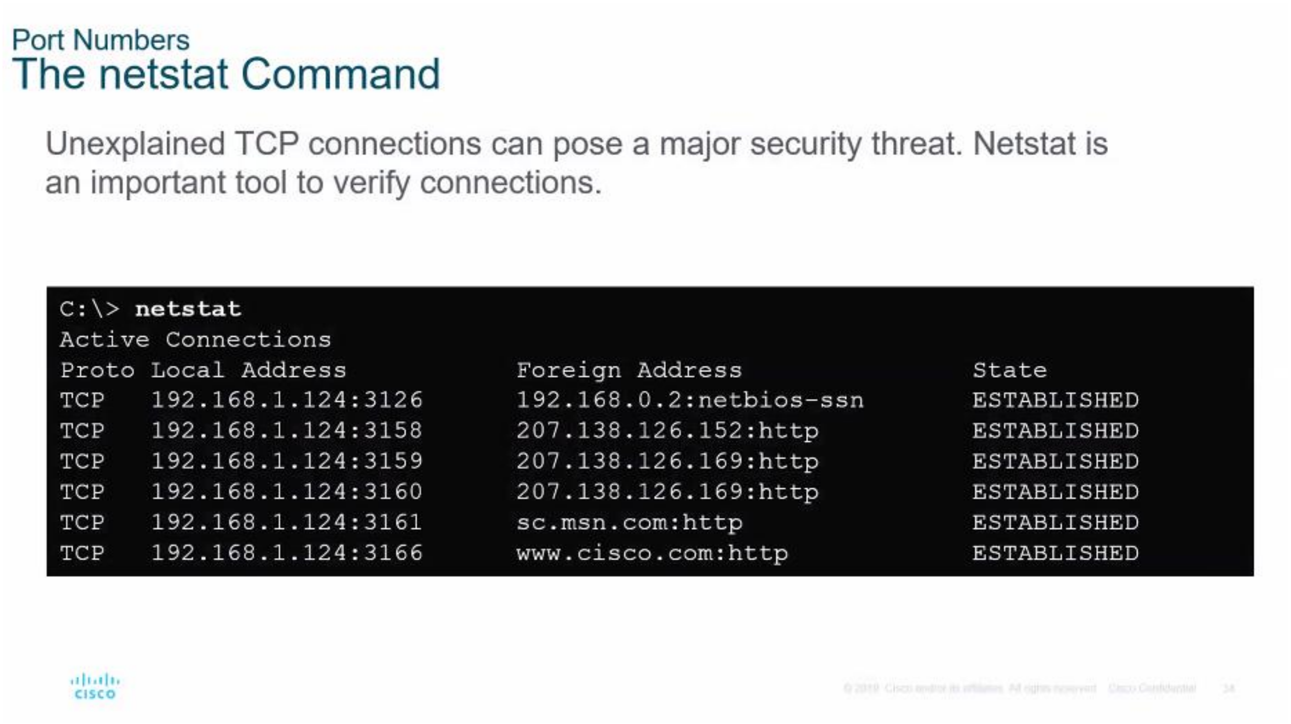


Port Numbers

Port Number Groups (Cont.)

Well-Known Port Numbers

Port Number	Protocol	Application
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
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)



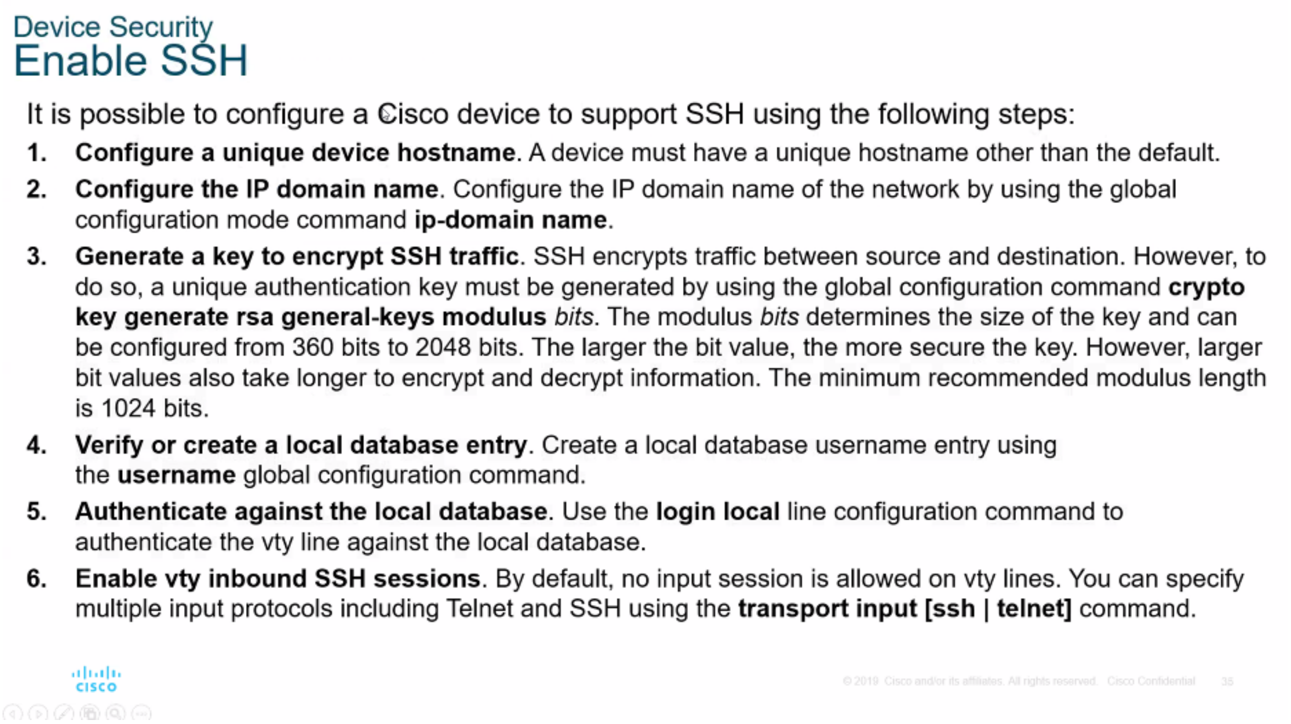
Port Numbers

The netstat Command

Unexplained TCP connections can pose a major security threat. Netstat is an important tool to verify connections.

```
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
```

Netstat -noa: mostra ip, processo e tutti i dati salvati



Device Security

Enable SSH

It is possible to configure a Cisco device to support SSH using the following steps:

1. **Configure a unique device hostname**. A device must have a unique hostname other than the default.
2. **Configure the IP domain name**. Configure the IP domain name of the network by using the global configuration mode command **ip-domain name**.
3. **Generate a key to encrypt SSH traffic**. SSH encrypts traffic between source and destination. However, to do so, a unique authentication key must be generated by using the global configuration command **crypto key generate rsa general-keys modulus** *bits*. The modulus *bits* determines the size of the key and can be configured from 360 bits to 2048 bits. The larger the bit value, the more secure the key. However, larger bit values also take longer to encrypt and decrypt information. The minimum recommended modulus length is 1024 bits.
4. **Verify or create a local database entry**. Create a local database username entry using the **username** global configuration command.
5. **Authenticate against the local database**. Use the **login local** line configuration command to authenticate the vty line against the local database.
6. **Enable vty inbound SSH sessions**. By default, no input session is allowed on vty lines. You can specify multiple input protocols including Telnet and SSH using the **transport input [ssh | telnet]** command.

Router e Switch CISCO condividono gli stessi comandi per SSH. Bisogna collegarsi alla porta Console (nella vita vera) e da PC ci colleghiamo allo switch tramite programma stile Putty da terminale.

Switch:

- Switch> Enable
- Switch(config)# Configure terminal

  (SSH richiede di settare l’hostname del dispositivo)
- Switch(config)# hostname S1

  (SSH richiede di settare il nome di dominio del dispositivo)
- S1(config)# ip domain-name example.com

  (Generare una chiave di cifratura del testo SSH)
- S1(config)# crypto key generate rsa general-keys modulus 1024
- S1(config)# crypto key generate rsa (poi specifico la dimensione della key)

  (Creazione di un user con associato username e password)
- S1(config)# username franco secret cisco1
- S1(config)# username ciccio secret cisco2

  (login local per fare in modo che user creato sopra possa fare l’accesso e usa un database dove confronta user-password in quanto ciascun user creato avrà associata una password)
- S1(config)# line vty 0 15
- S1(config-line)# login local

  (impone al dispositivo di accettare solo connessioni SSH e di rifiutare tutte le altre tipologie di connessione, ad esempio rifiuta telnet)
- S1(config-line)# transport input ssh

  (da PC do il comando [ssh – l username target] per accedere allo switch)

  (posso accedere solo al primo livello, per entrare in configuration-mode devo prima abilitare nello switch il “enable secret cisco”)

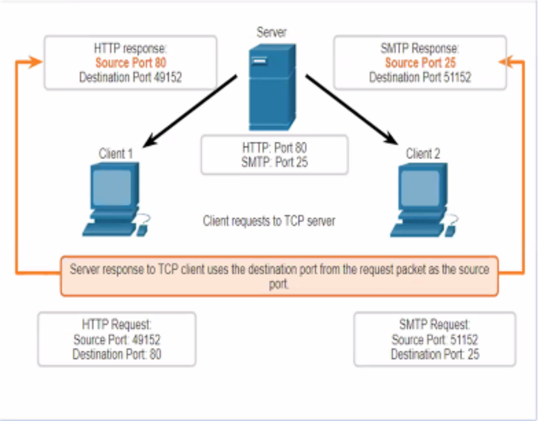
14.5 TCP Communication Process

TCP Communication Process

TCP Server Processes

Each application process running on a server is configured to use a port number.

- An individual server cannot have two services assigned to the same port number within the same transport layer services.
- An active server application assigned to a specific port is considered open, which means that the transport layer accepts, and processes segments addressed to that port.
- Any incoming client request addressed to the correct socket is accepted, and the data is passed to the server application.



TCP Communication Process

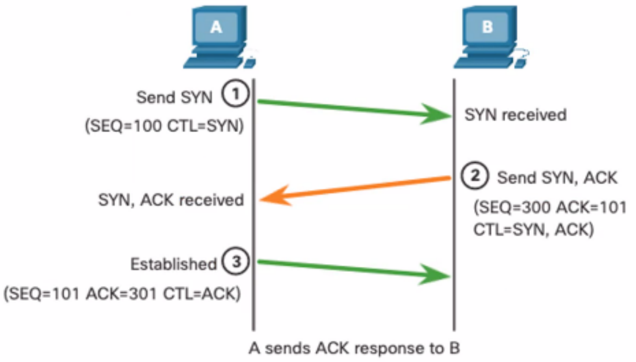
TCP Connection Establishment

PcA chiede a PcB se la porta x è aperta

Step 1: The initiating client requests a client-to-server communication session with the server. A->B

Step 2: The server acknowledges the client-to-server communication session and requests a server-to-client communication session.

Step 3: The initiating client acknowledges the server-to-client communication session.



TCP Communication Process

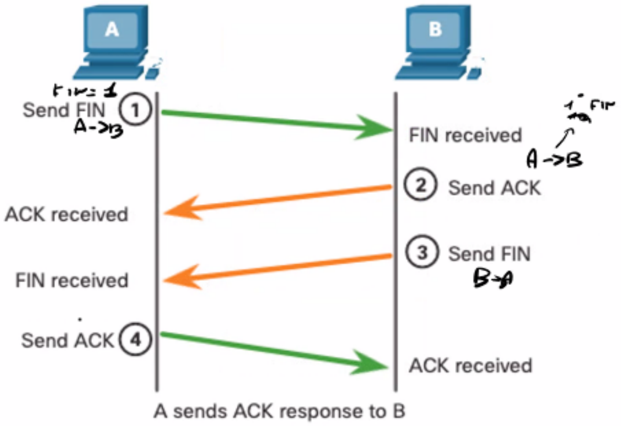
Session Termination

Step 1: When the client has no more data to send in the stream, it sends a segment with the FIN flag set.

Step 2: The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.

Step 3: The server sends a FIN to the client to terminate the server-to-client session.

Step 4: The client responds with an ACK to acknowledge the FIN from the server.



TCP Communication Process

TCP Three-Way Handshake Analysis

Functions of the Three-Way Handshake: → [illegible]

- It establishes that the destination device is present on the network.
- It verifies that the destination device has an active service and is accepting requests on the destination port number that the initiating client intends to use.
- It informs the destination device that the source client intends to establish a communication session on that port number.

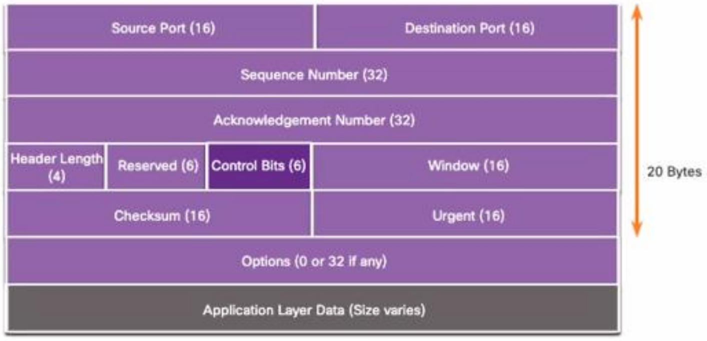
After the communication is completed the sessions are closed, and the connection is terminated. The connection and session mechanisms enable TCP reliability function.

TCP Communication Process

TCP Three-Way Handshake Analysis (Cont.)

The six control bit flags are as follows:

- **URG** - Urgent pointer field significant
- **ACK** - Acknowledgment flag used in connection establishment and session termination
- **PSH** - Push function
- **RST** - Reset the connection when an error or timeout occurs
- **SYN** - Synchronize sequence numbers used in connection establishment
- **FIN** - No more data from sender and used in session termination



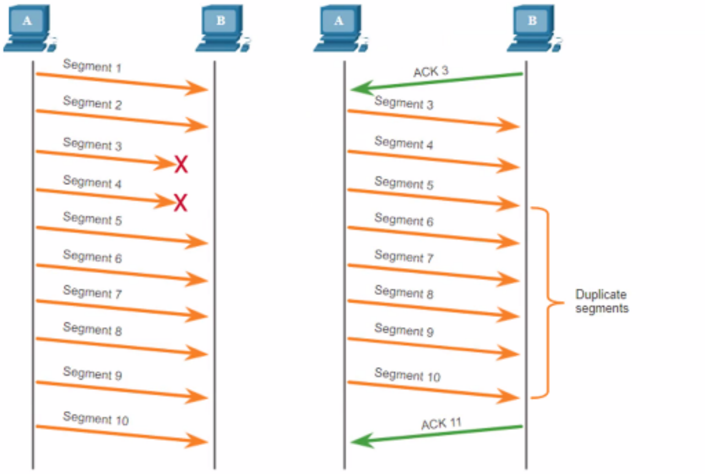
14.6 Reliability and Flow Control

Reliability and Flow Control

TCP Reliability – Data Loss and Retransmission

No matter how well designed a network is, data loss occasionally occurs.

TCP provides methods of managing these segment losses. Among these is a mechanism to retransmit segments for unacknowledged data.

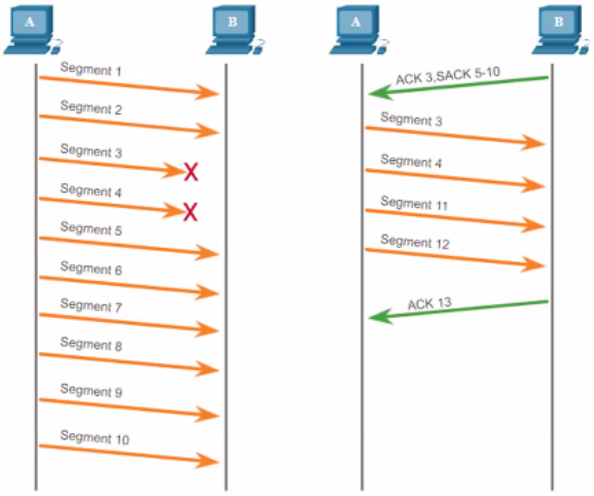


Reliability and Flow Control

TCP Reliability – Data Loss and Retransmission (Cont.)

Host operating systems today typically employ an optional TCP feature called selective acknowledgment (SACK), negotiated during the three-way handshake.

If both hosts support SACK, the receiver can explicitly acknowledge which segments (bytes) were received including any discontinuous segments.



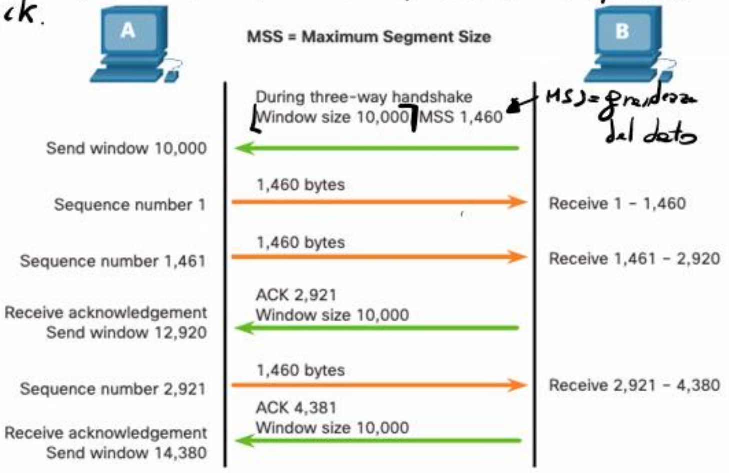
Reliability and Flow Control

TCP Flow Control – Window Size and Acknowledgments

Flow control → quanti pacchetti (bytes) posso mandare prima di aspettare un Ack.

TCP also provides mechanisms for flow control as follows:

- Flow control is the amount of data that the destination can receive and process reliably.
- Flow control helps maintain the reliability of TCP transmission by adjusting the rate of data flow between source and destination for a given session.



MSS = grandezza del dato

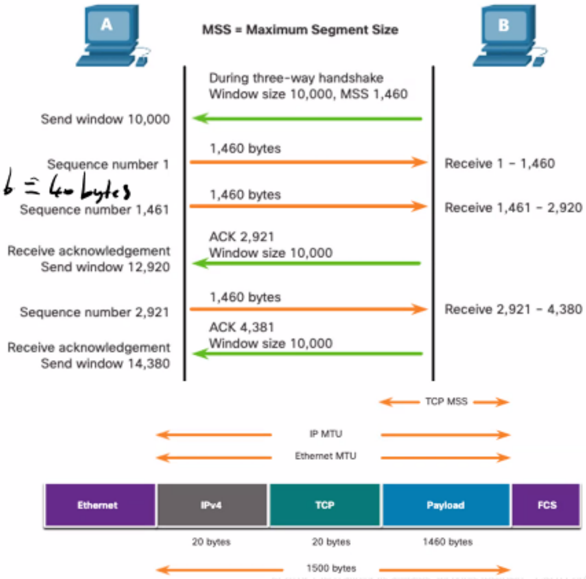
Reliability and Flow Control

TCP Flow Control – Maximum Segment Size

MTU

Maximum Segment Size (MSS) is the maximum amount of data that the destination device can receive.

- A common MSS is 1,460 bytes when using IPv4. IP + TCP = 20b + 20b = 40 bytes
- A host determines the value of its MSS field by subtracting the IP and TCP headers from the Ethernet maximum transmission unit (MTU), which is 1500 bytes be default. (+18 ethernet)
- 1500 minus 40 (20 bytes for the IPv4 header and 20 bytes for the TCP header) leaves 1460 bytes.

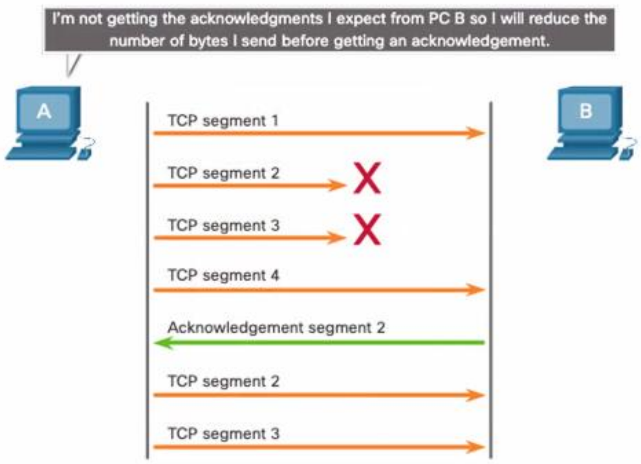


Reliability and Flow Control

TCP Flow Control – Congestion Avoidance

When congestion occurs on a network, it results in packets being discarded by the overloaded router.

To avoid and control congestion, TCP employs several congestion handling mechanisms, timers, and algorithms.



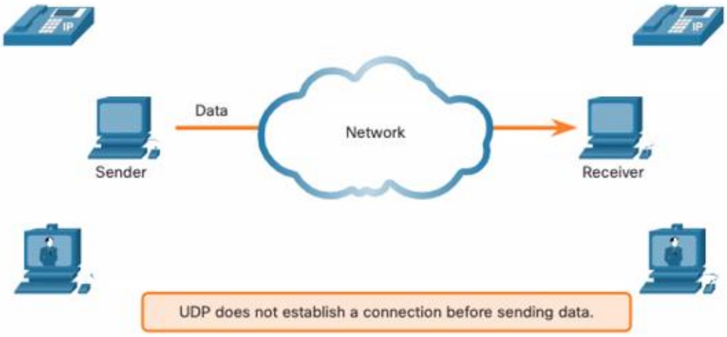
I'm not getting the acknowledgments I expect from PC B so I will reduce the number of bytes I send before getting an acknowledgement.

14.7 UDP Communication

UDP Communication

UDP Low Overhead versus Reliability

UDP does not establish a connection. UDP provides low overhead data transport because it has a small datagram header and no network management traffic.

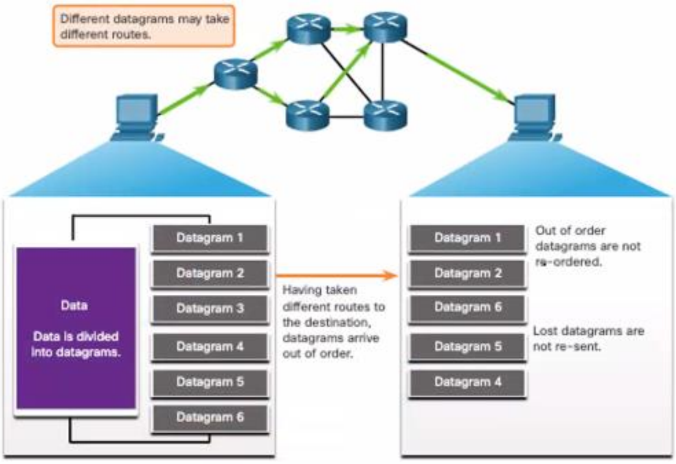


UDP does not establish a connection before sending data.

UDP Communication

UDP Datagram Reassembly

- UDP does not track sequence numbers the way TCP does.
- UDP has no way to reorder the datagrams into their transmission order.
- UDP simply reassembles the data in the order that it was received and forwards it to the application.



Different datagrams may take different routes.

Having taken different routes to the destination, datagrams arrive out of order.

Out of order datagrams are not re-ordered.

Lost datagrams are not re-sent.

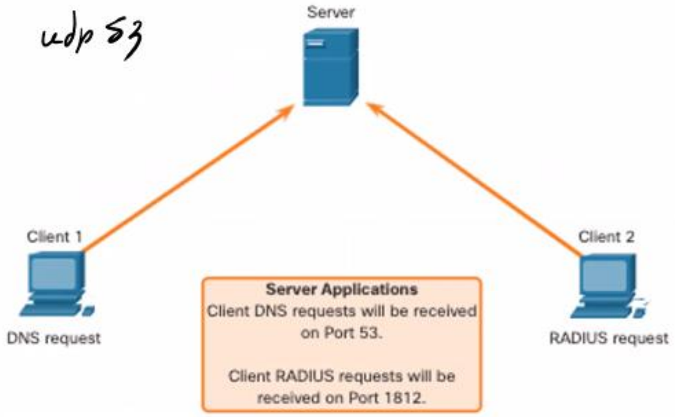
UDP Communication

UDP Server Processes and Requests

UDP-based server applications are assigned well-known or registered port numbers.

UDP receives a datagram destined for one of these ports, it forwards the application data to the appropriate application based on its port number.

udp 53



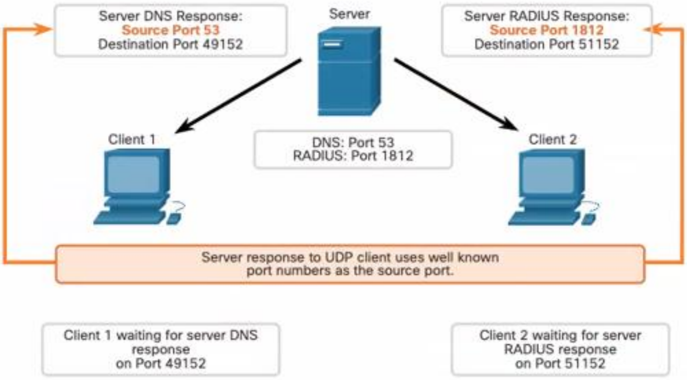
Server Applications
Client DNS requests will be received on Port 53.

Client RADIUS requests will be received on Port 1812.

UDP Communication

UDP Client Processes

- The UDP client process dynamically selects a port number from the range of port numbers and uses this as the source port for the conversation.
- The destination port is usually the well-known or registered port number assigned to the server process.
- After a client has selected the source and destination ports, the same pair of ports are used in the header of all datagrams in the transaction.



Server DNS Response:
Source Port 53
Destination Port 49152

Server RADIUS Response:
Source Port 1812
Destination Port 51152

Server response to UDP client uses well known port numbers as the source port.

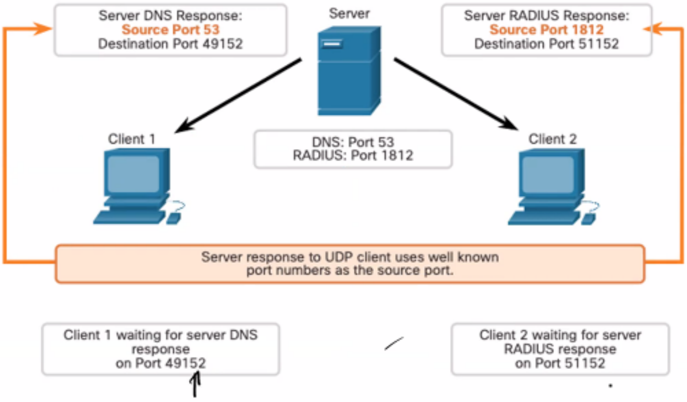
Client 1 waiting for server DNS response on Port 49152

Client 2 waiting for server RADIUS response on Port 51152

UDP Communication

UDP Client Processes

- The UDP client process dynamically selects a port number from the range of port numbers and uses this as the source port for the conversation.
- The destination port is usually the well-known or registered port number assigned to the server process.
- After a client has selected the source and destination ports, the same pair of ports are used in the header of all datagrams in the transaction.



Server DNS Response:
Source Port 53
Destination Port 49152

Server RADIUS Response:
Source Port 1812
Destination Port 51152

DNS: Port 53
RADIUS: Port 1812

Server response to UDP client uses well known port numbers as the source port.

Client 1 waiting for server DNS response on Port 49152

Client 2 waiting for server RADIUS response on Port 51152