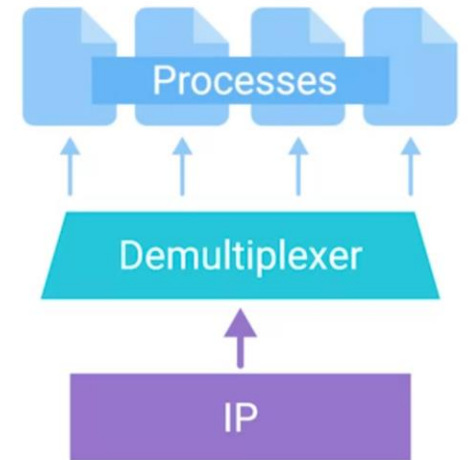
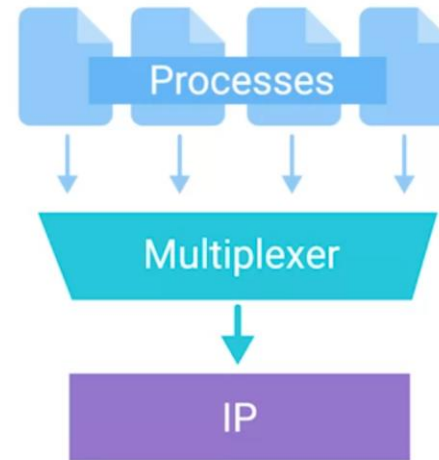
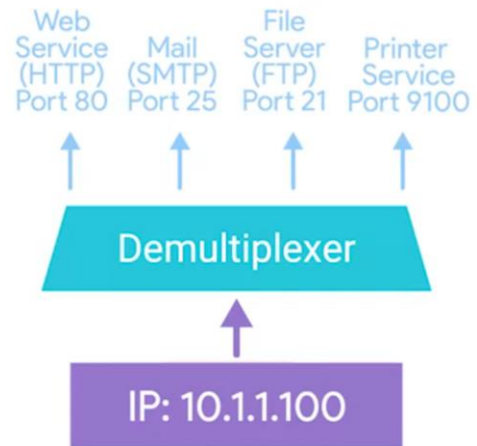
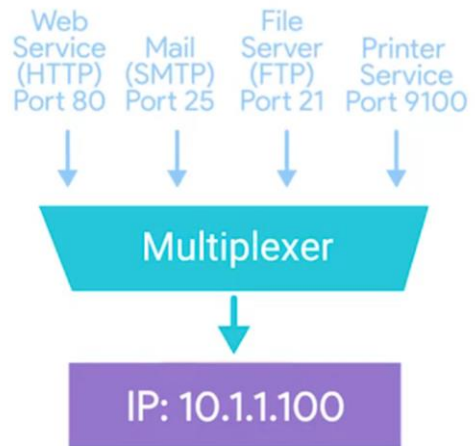


Application layer

Allows these applications to communicate in a way they understand

Transport layer

Allows traffic to be directed to specific network applications



10.1.1.100:80
Socket number or
socket port

Port

A 16-bit number that's used to direct traffic to specific services running on a networked computer

TCP segment

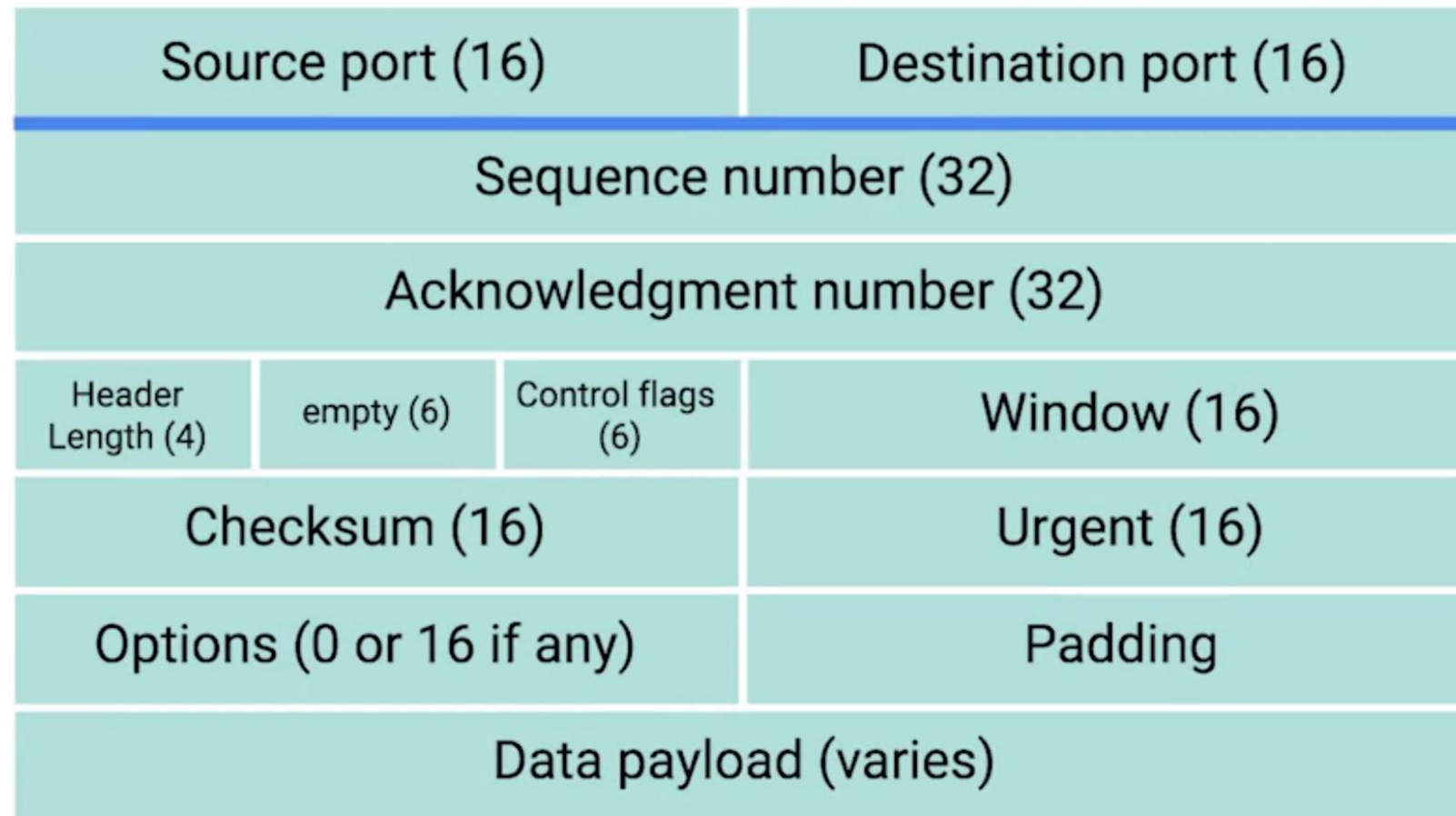
Made up of a TCP header and a data section

Bit 0

Bit 15

Bit 16

Bit 31



20
Bytes

Destination port

The port of the service the traffic is intended for

Source port

A high-numbered port chosen from a special section of ports known as ephemeral ports

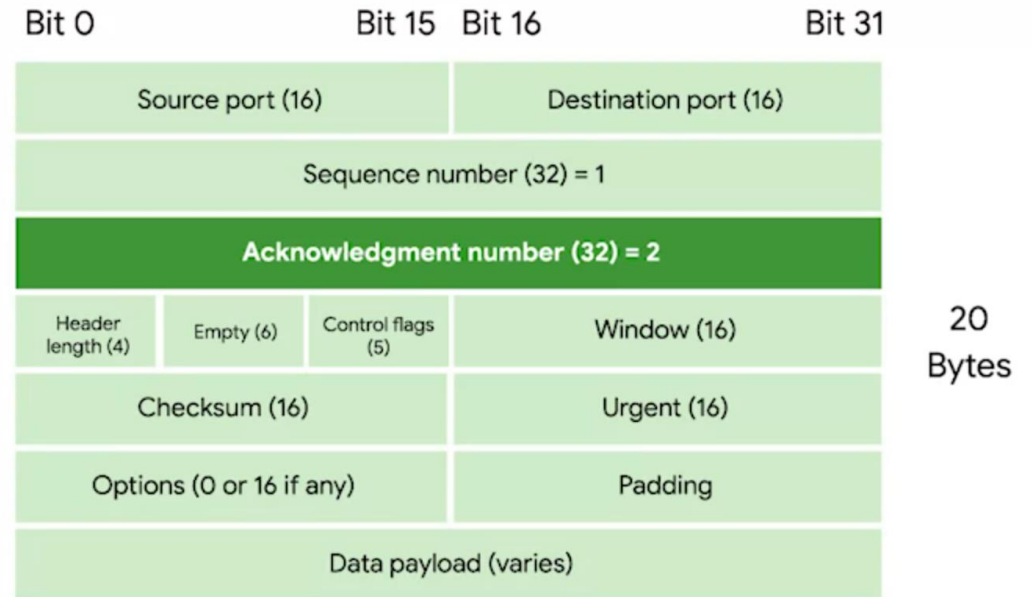
Sequence number

A 32-bit number that's used to keep track of where in a sequence of TCP segments this one is expected to be

Acknowledgement number

The number of the next expected segment

TCP header



TCP checksum

Operates just like the checksum fields at the IP and ethernet level

Data offset field

A 4-bit number that communicates how long the TCP header for this segment is

TCP window

Specifies the range of sequence numbers that might be sent before an acknowledgement is required

Urgent pointer field

Used in conjunction with one of the TCP control flags to point out particular segments that might be more important than others

TCP Flags

RST (reset)

One of the sides in a TCP connection hasn't been able to properly recover from a series of missing or malformed segments

ACK (acknowledged)

A value of one in this field means that the acknowledgement number field should be examined

URG (urgent)

A value of one here indicates that the segment is considered urgent and that the urgent pointer field has more data about this

PSH (push)

The transmitting device wants the receiving device to push currently-buffered data to the application on the receiving end as soon as possible

SYN (synchronize)

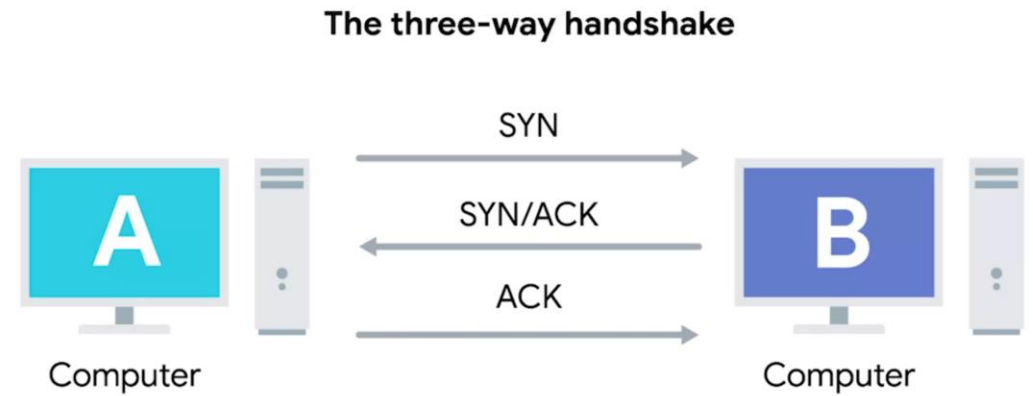
It's used when first establishing a TCP connection and makes sure the receiving end knows to examine the sequence number field

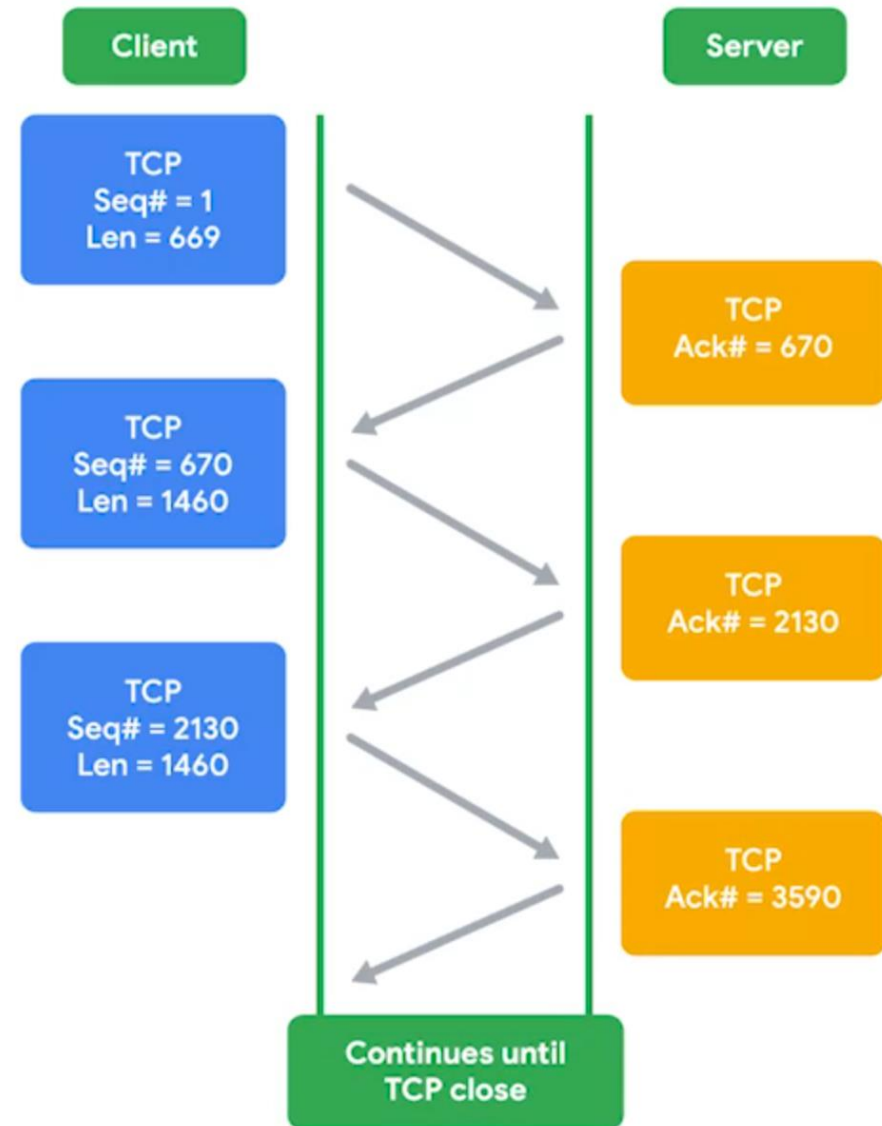
FIN (finish)

When this flag is set to one, it means the transmitting computer doesn't have any more data to send and the connection can be closed

Handshake

A way for two devices to ensure that they're speaking the same protocol and will be able to understand each other





Socket

The instantiation of an end-point in a potential TCP connection

All TCP socket States

CLOSE_WAIT

The connection has been closed at the TCP layer, but that the application that opened the socket hasn't released its hold on the socket yet

SYN-RECEIVED

A socket previously in a LISTEN state has received a synchronization request and sent a SYN/ACK back

LISTEN

A TCP socket is ready and listening for incoming connections

CLOSED

The connection has been fully terminated and that no further communication is possible

SYN_SENT

A synchronization request has been sent, but the connection hasn't been established yet

FIN_WAIT

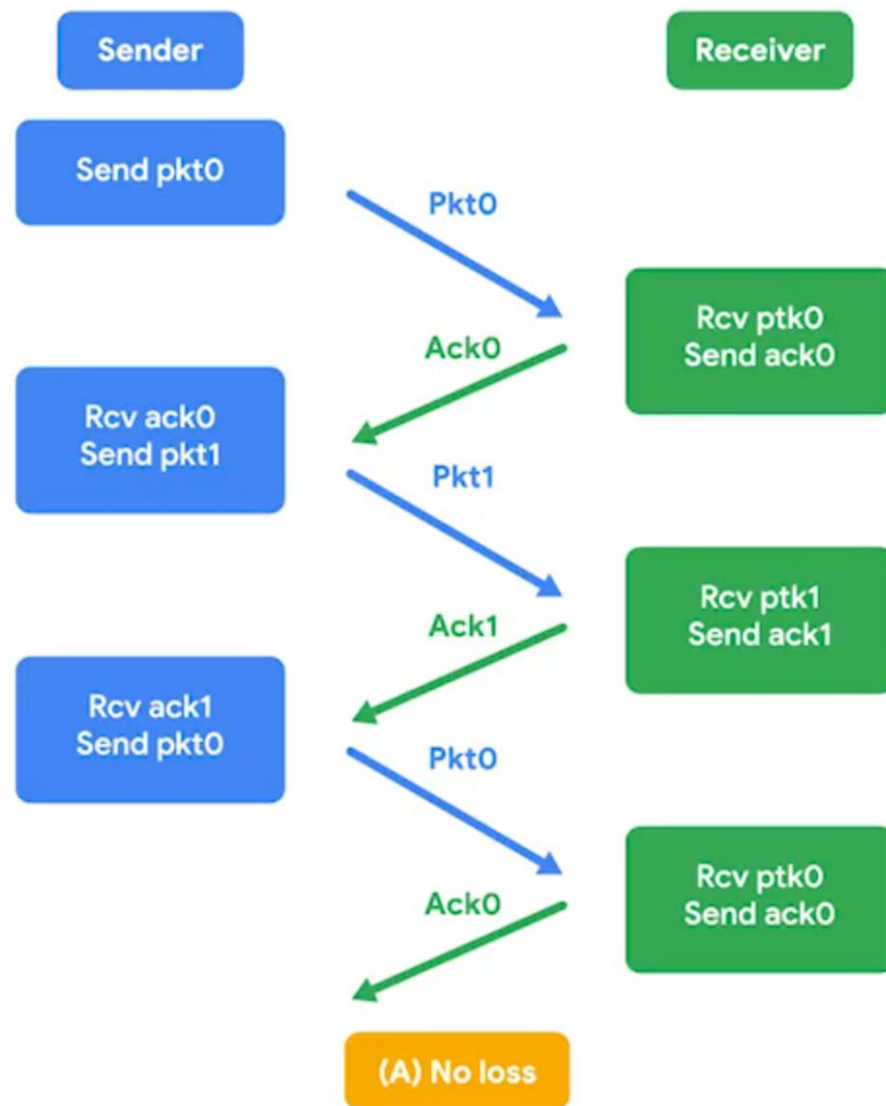
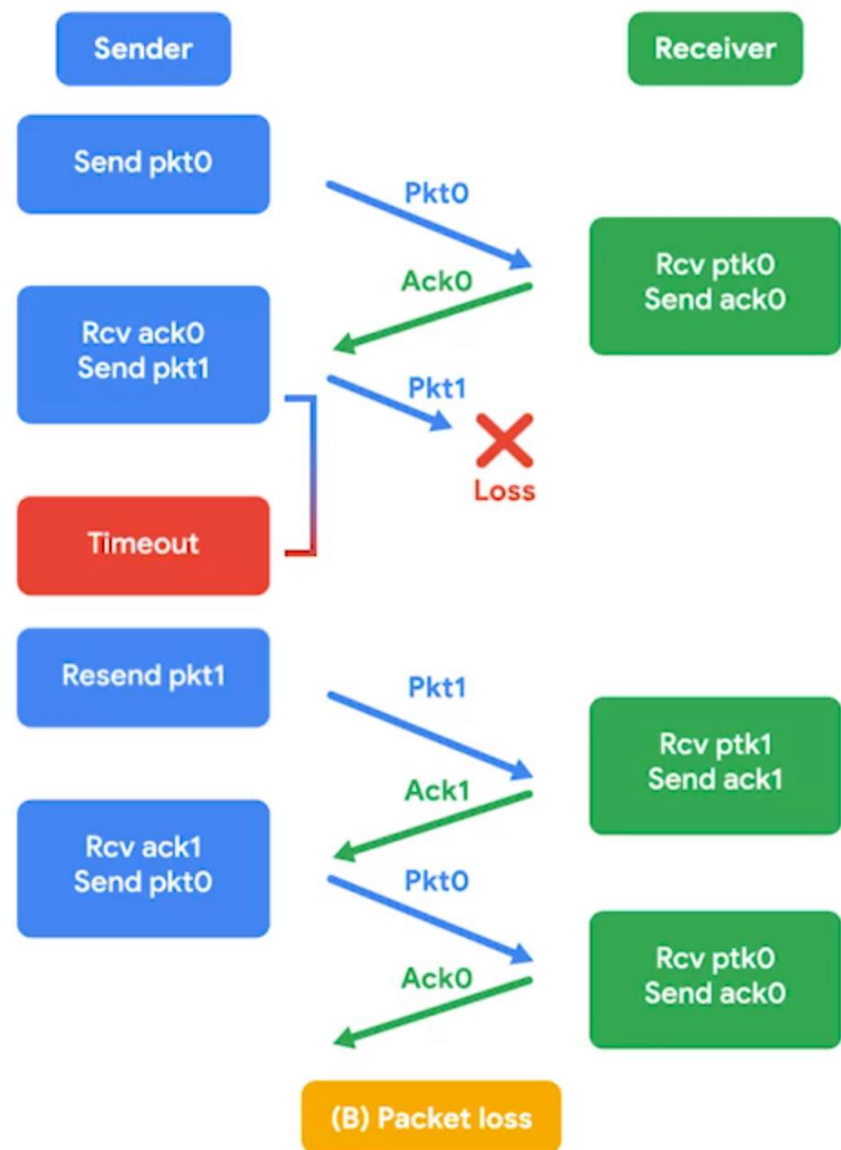
A FIN has been sent, but the corresponding ACK from the other end hasn't been received yet

ESTABLISHED

The TCP connection is in working order and both sides are free to send each other data

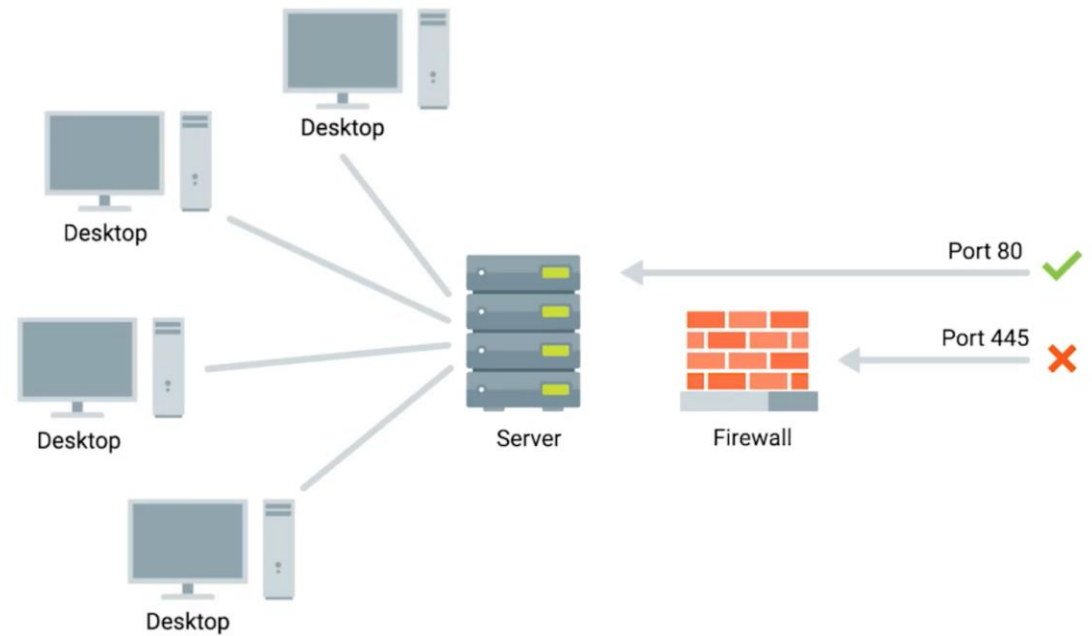
Connection-oriented protocol

Establishes a connection, and uses this to ensure that all data has been properly transmitted



Firewall

A device that blocks traffic that meets certain criteria



OSI Model

Application

Presentation

Session

Transport

Network

Data link

Physical

Presentation Layer

Responsible for making sure that the unencapsulated **application layer** data is able to be understood by the application in question

Session Layer

Facilitating the communication between actual **applications** and the **transport layer**

OSI Model

Application

Presentation

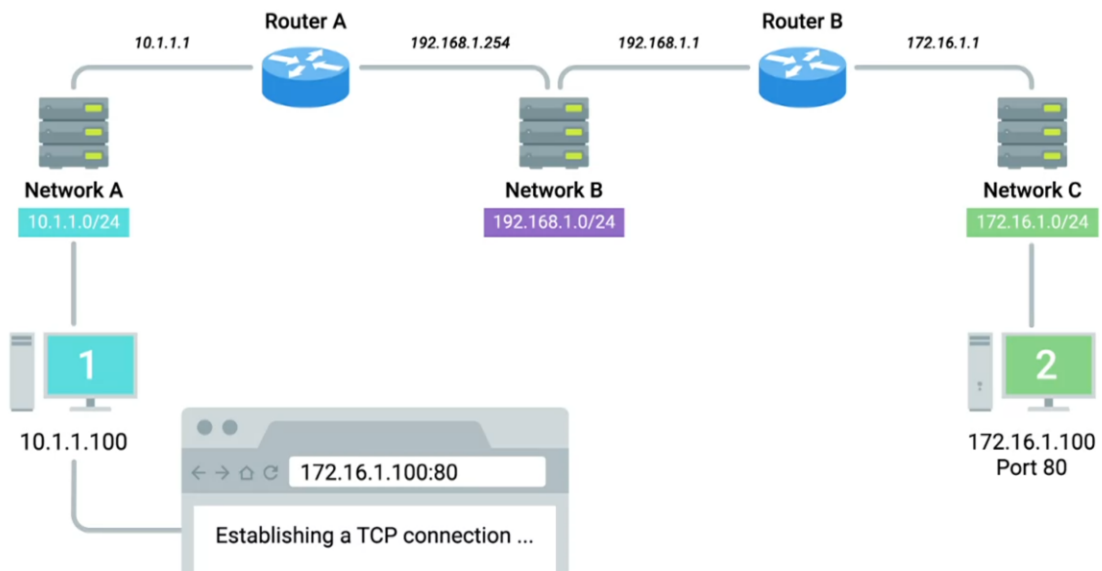
Session

Transport

Network

Data link

Physical



OSI Model



TCP/IP 5-Layer Model

