Platzi

Curso de
Pentesting

Juan Pablo Caro

Introducción

¿Qué es Pentesting?

¿Qué es Pentesting?

“Acceso legal y autorizado a sistemas de información, con el objetivo de hacerlos más seguros, a través de herramientas para la identificación y explotación de vulnerabilidades”.

¿Qué es Pentesting?

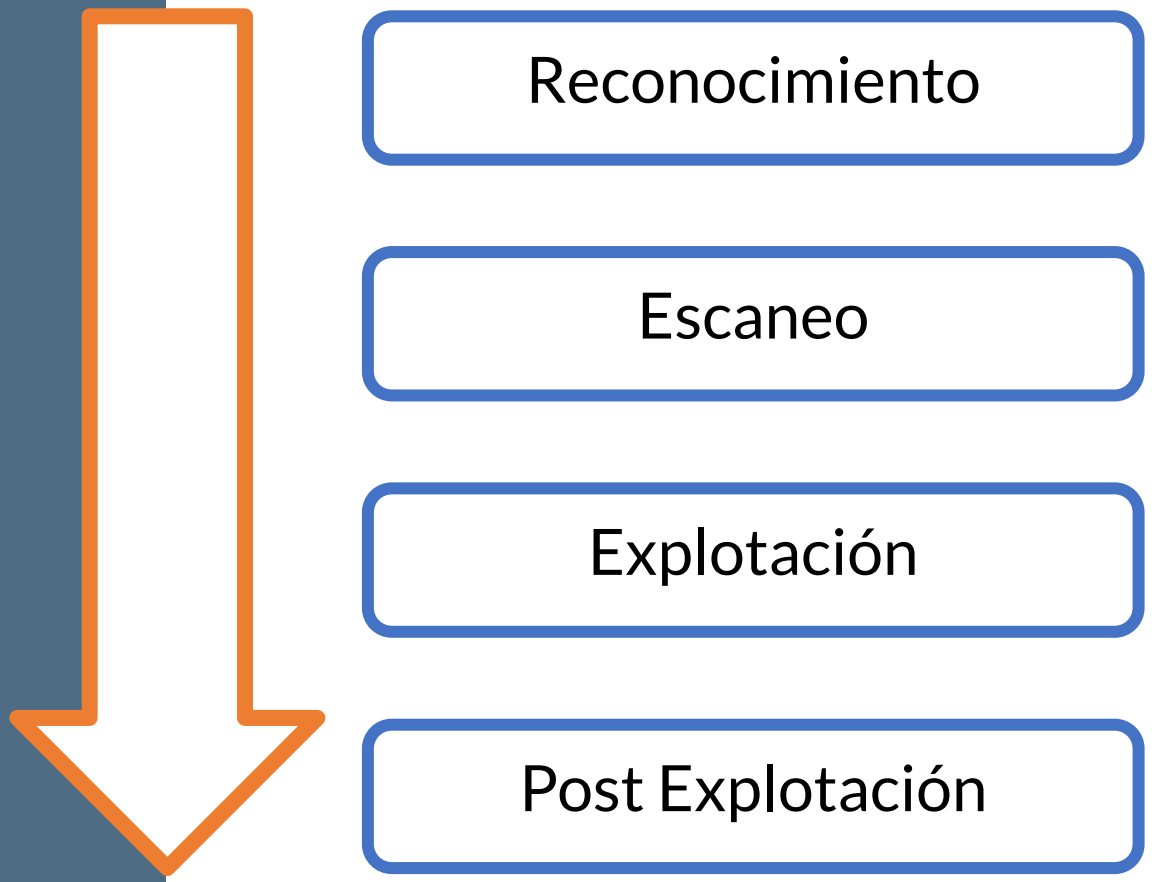
"Acceso **legal** y **autorizado** a sistemas de información, con el objetivo de hacerlos más seguros, a través de herramientas para la identificación y explotación de vulnerabilidades".

¿Qué es Pentesting?

"Acceso legal y autorizado a sistemas de información, con el objetivo de **hacerlos más seguros**, a través de herramientas para la identificación y explotación de vulnerabilidades".

¿Qué es Pentesting?

"Acceso legal y autorizado a sistemas de información, con el objetivo de hacerlos más seguros, a través de herramientas para la identificación y explotación de **vulnerabilidades**".


Reconocimiento
Escaneo
Explotación
Post Explotación

Reconocimiento

Escaneo

Explotación

Post Explotación

- Definir nuestros objetivos.
- Recolectar datos relevantes.
- Identificar información clave sobre nuestros objetivos.
- ¡Aquí ya hay vulnerabilidades!

Reconocimiento

Escaneo

Explotación

Post Explotación

- Escaneo para diferentes protocolos.
- Identificación de vulnerabilidades.
- Análisis de potenciales riesgos.

Reconocimiento

Escaneo

Explotación

Post Explotación

- Acceder a sistemas vulnerables.
- Obtener privilegios.
- Obtener información o accesos relevantes.
- Tenemos que darle un valor agregado al cliente.

Reconocimiento

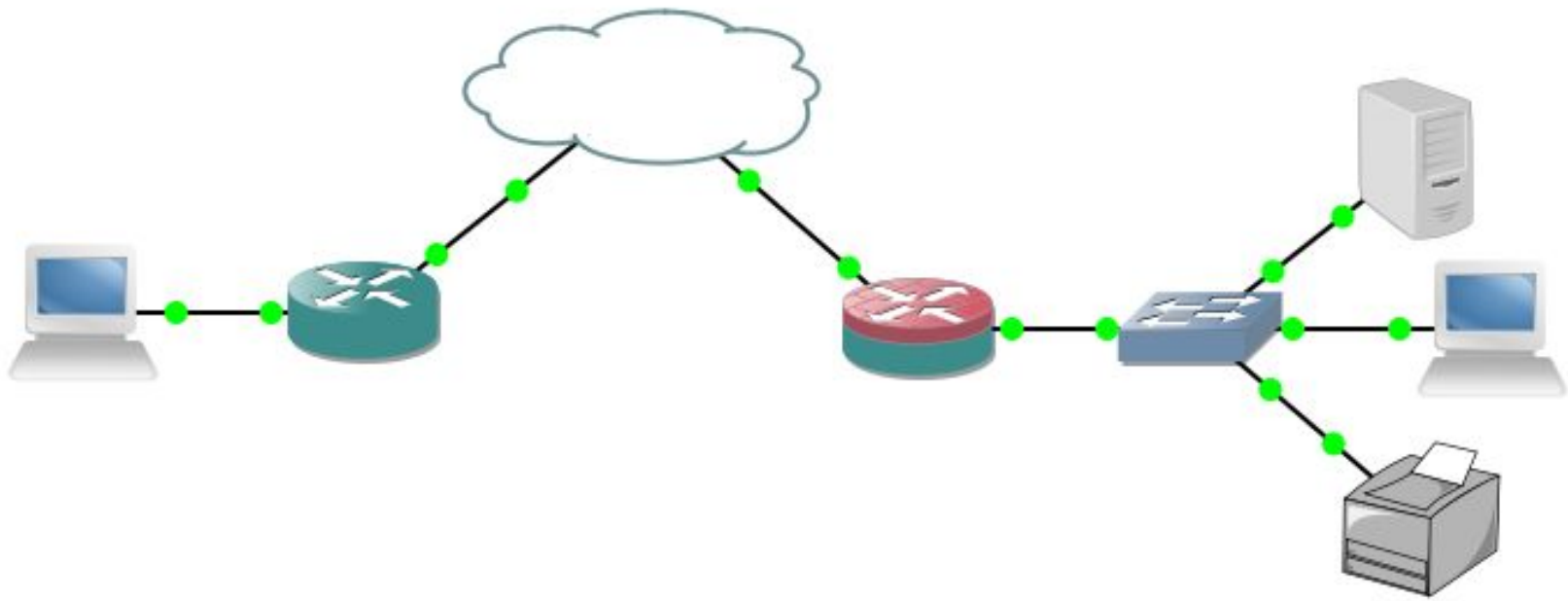
Escaneo

Explotación

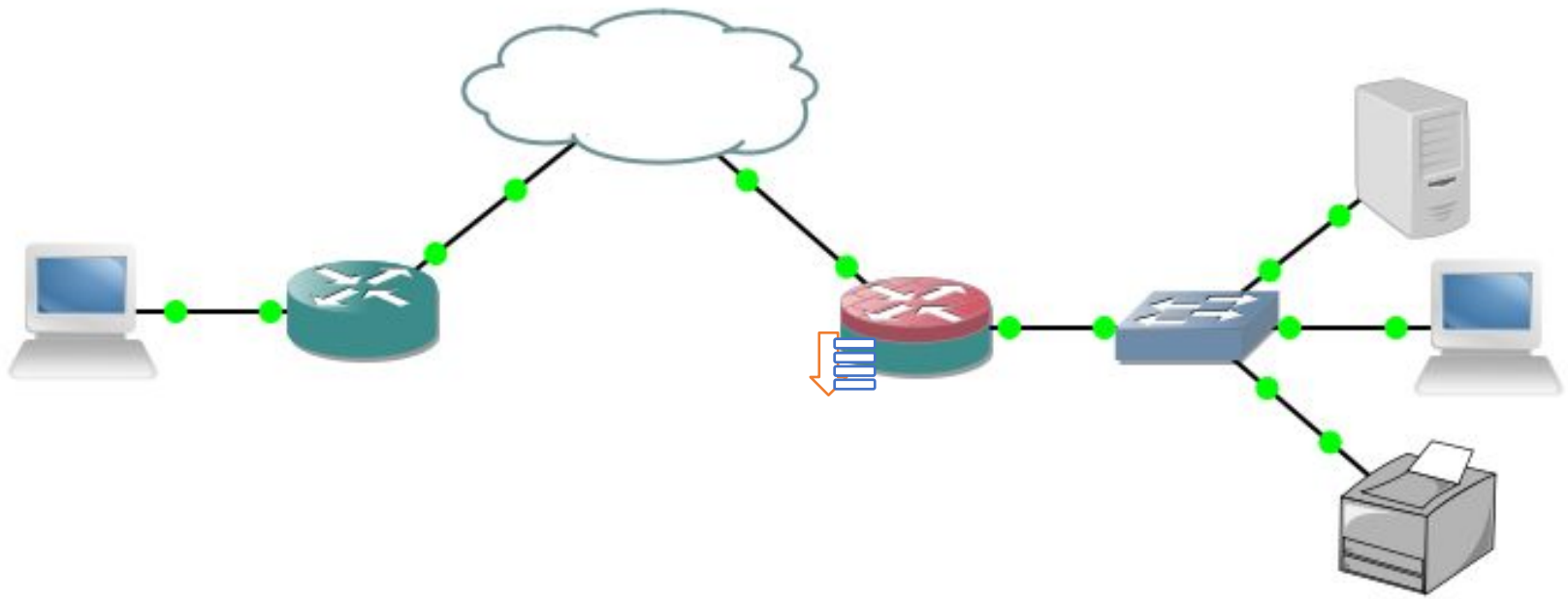
Post Explotación

- Mantener o conservar el acceso o privilegios.
- Generar nuevos accesos.

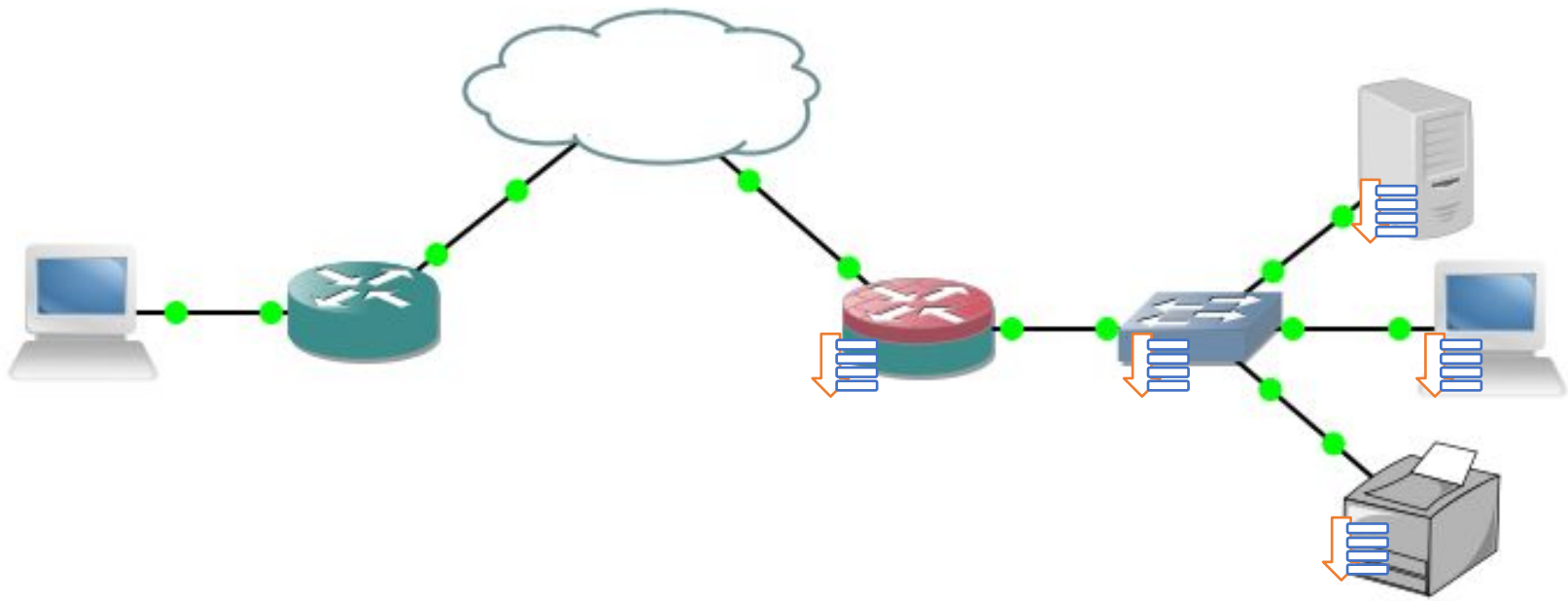
“Pivoting”



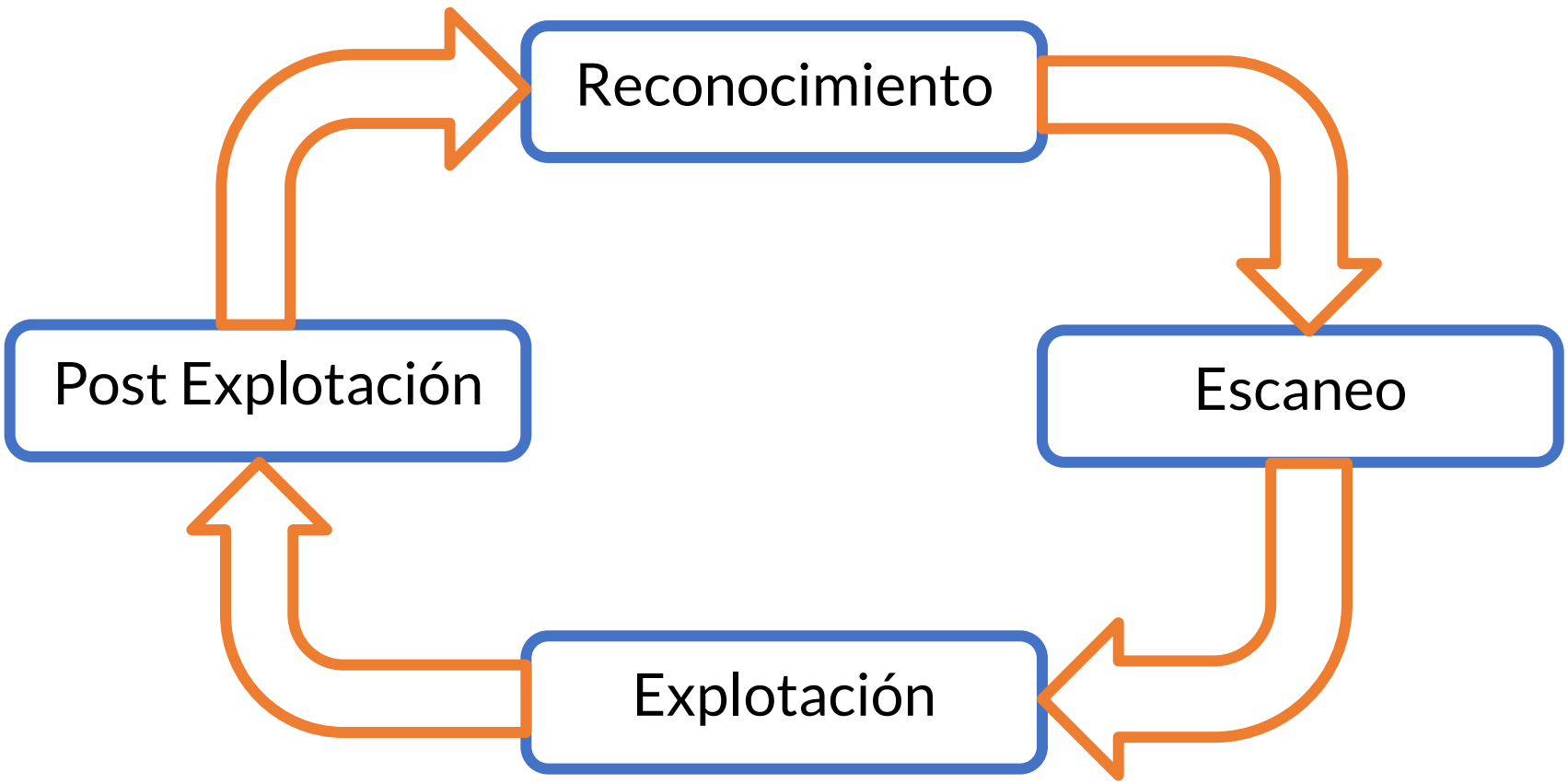
“Pivoting”



“Pivoting”



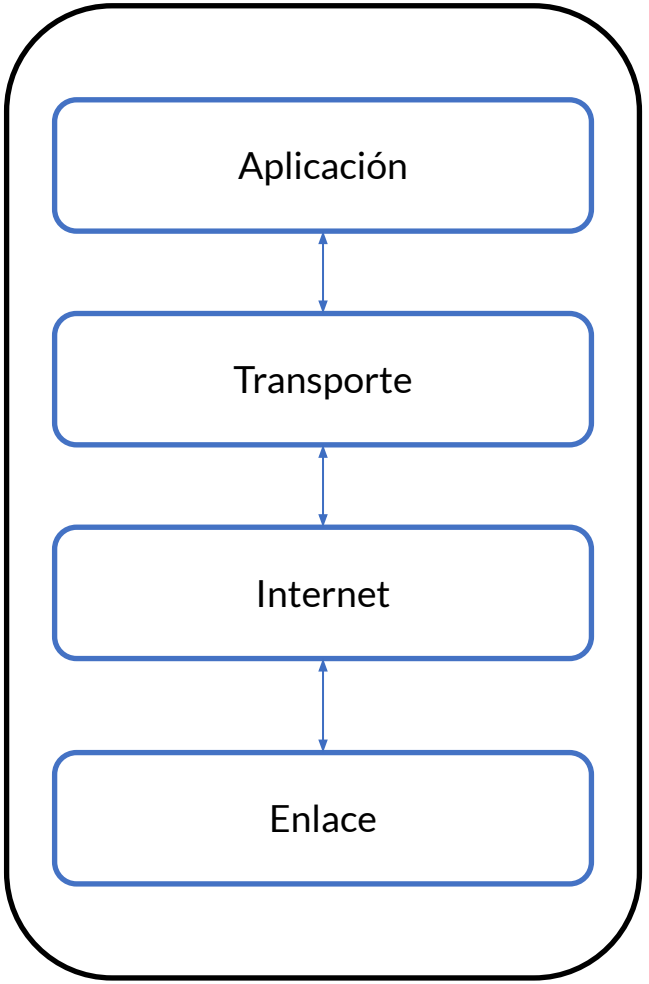
“Pivoting”



Conceptos generales de redes

Modelo TCP/IP

Modelo TCP/IP



Protocolos correspondientes a cada una de las aplicaciones que usan recursos de red.

Mantenimiento de las conexiones y calidad en la transferencia de datos.

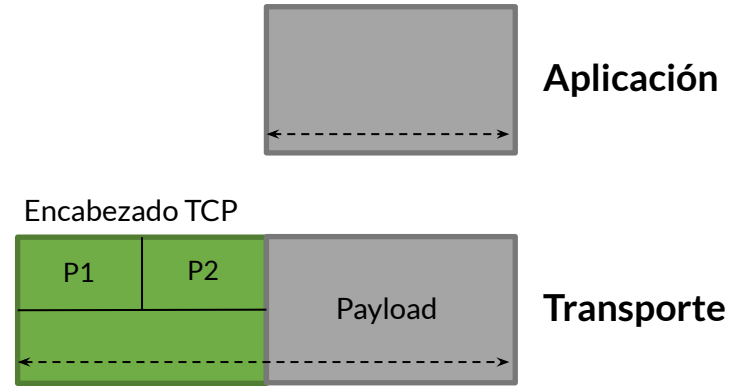
Recursos para conexión entre nodos que no están en el mismo segmento o sección.

Mecanismos físicos de conexión y comunicación.

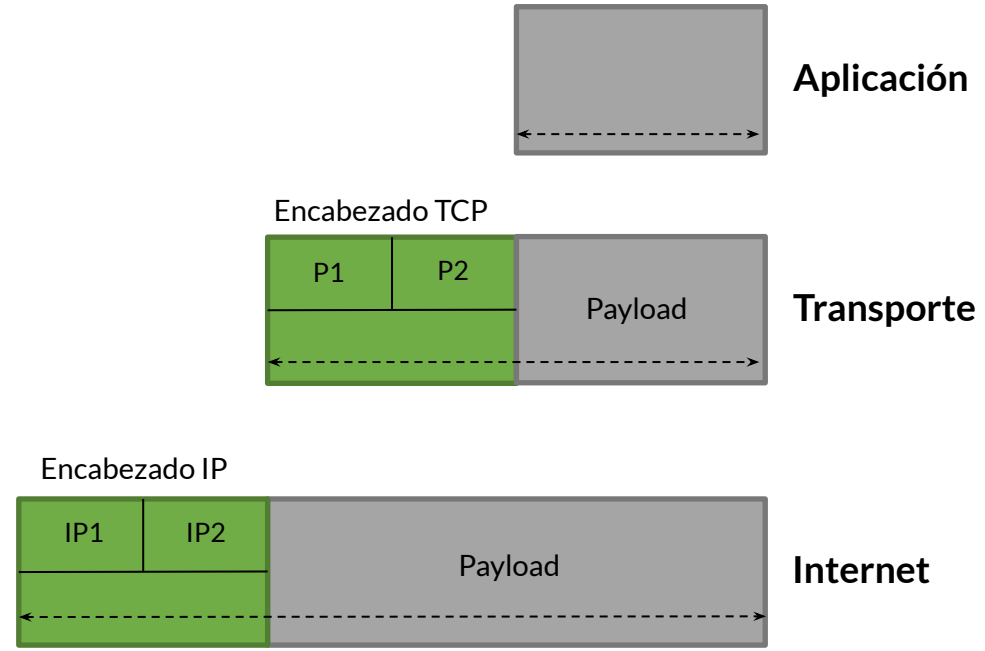
Encapsulado de datos

Aplicación

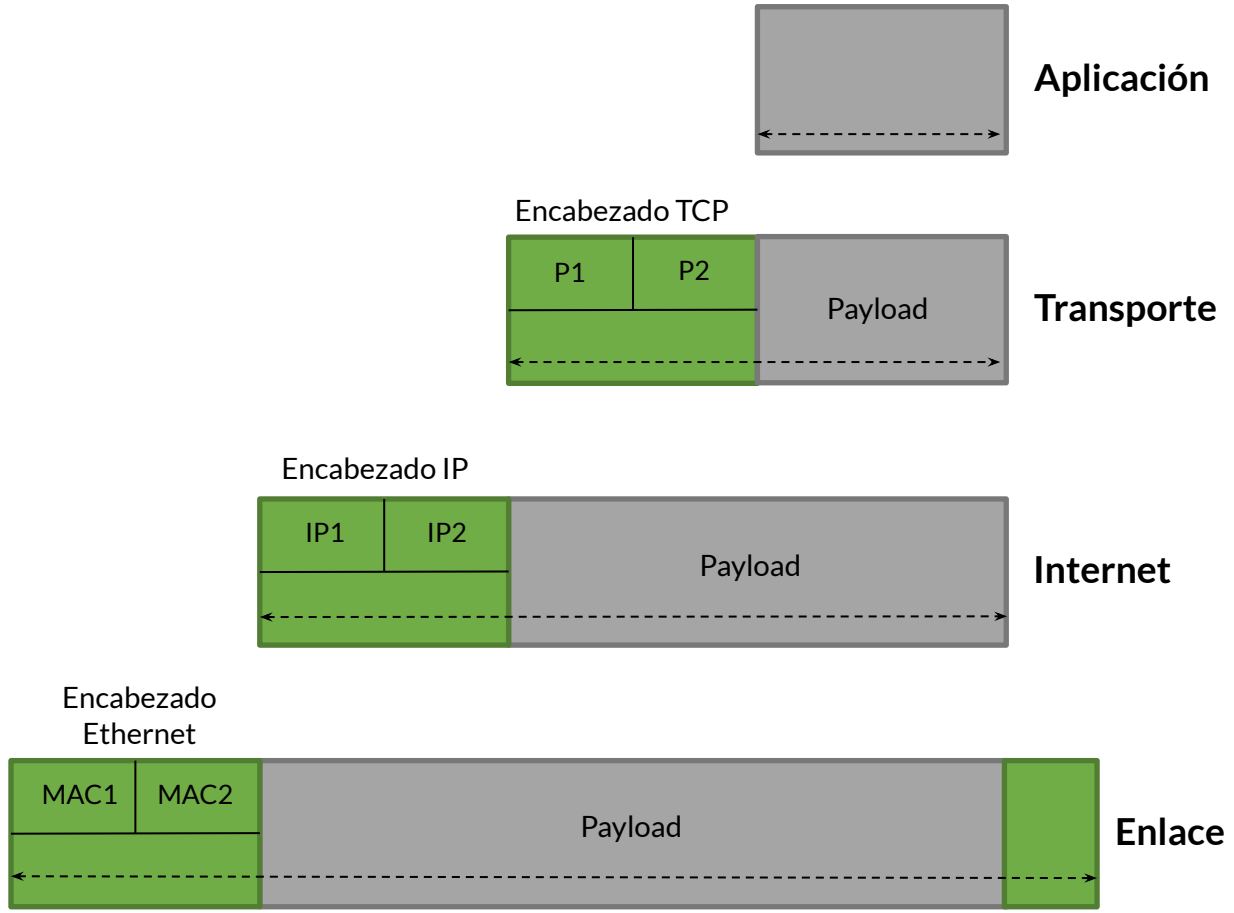
Encapsulado de datos



Encapsulado de datos



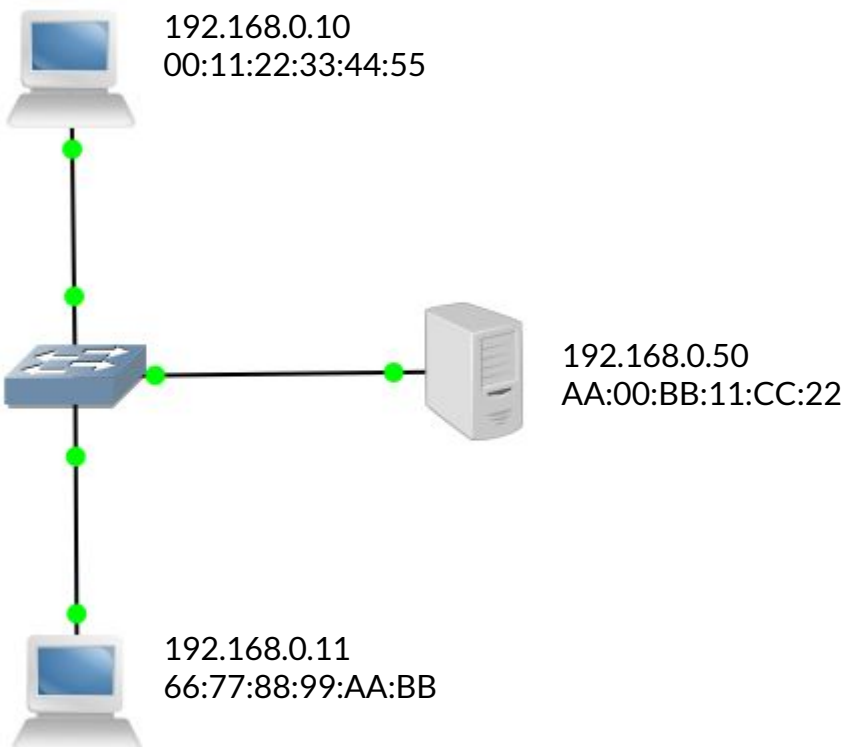
Encapsulado de datos



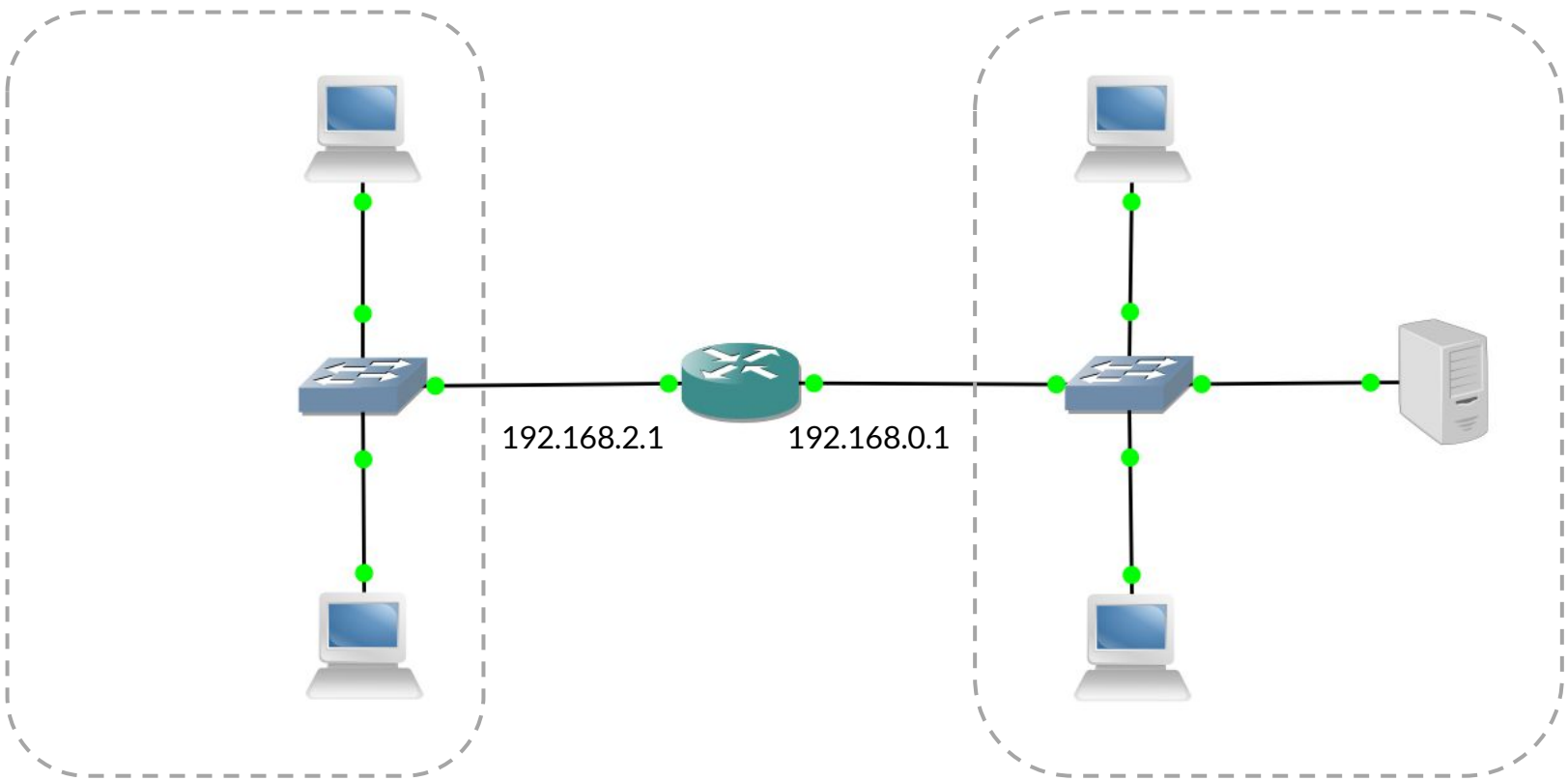
Conceptos generales de redes

Enrutamiento

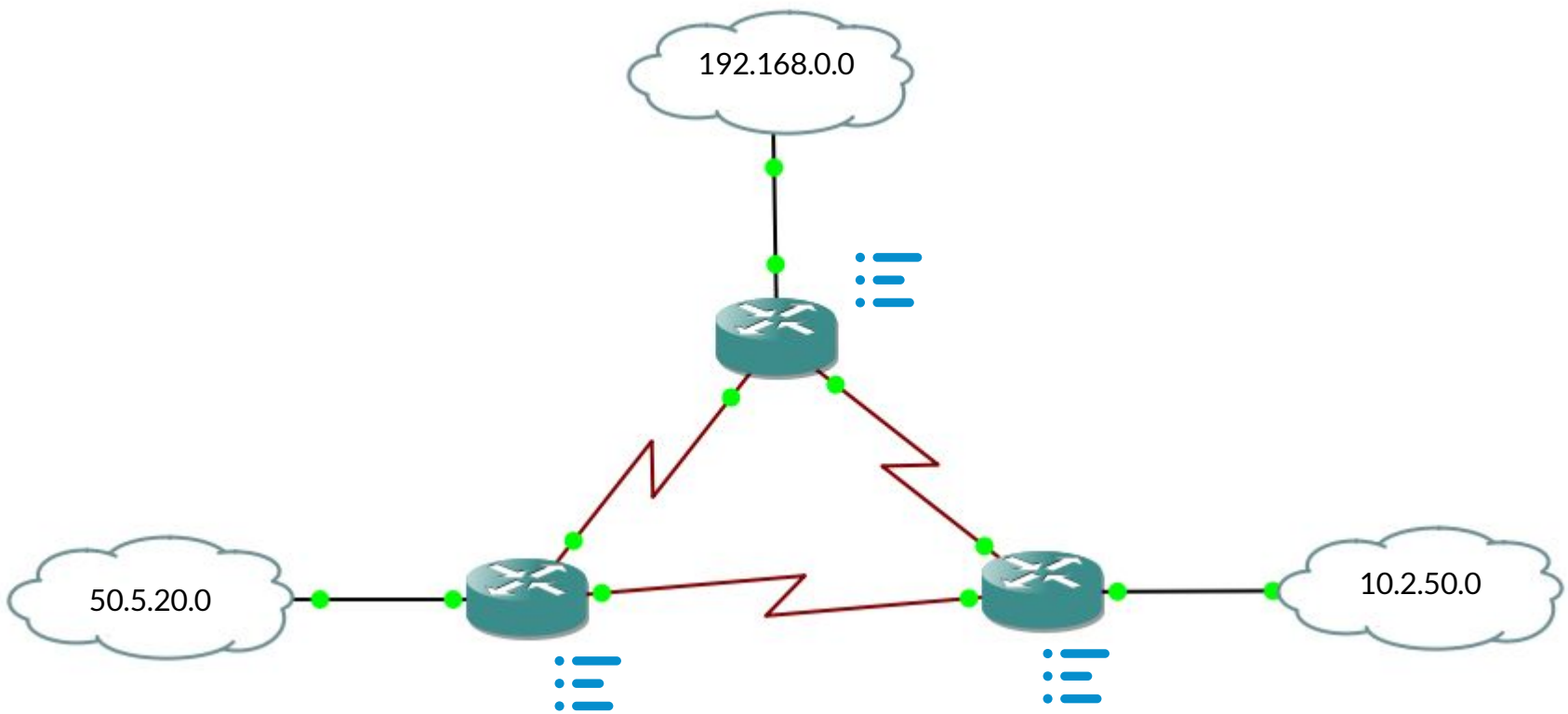
Enlace de datos



Enrutamiento entre segmentos



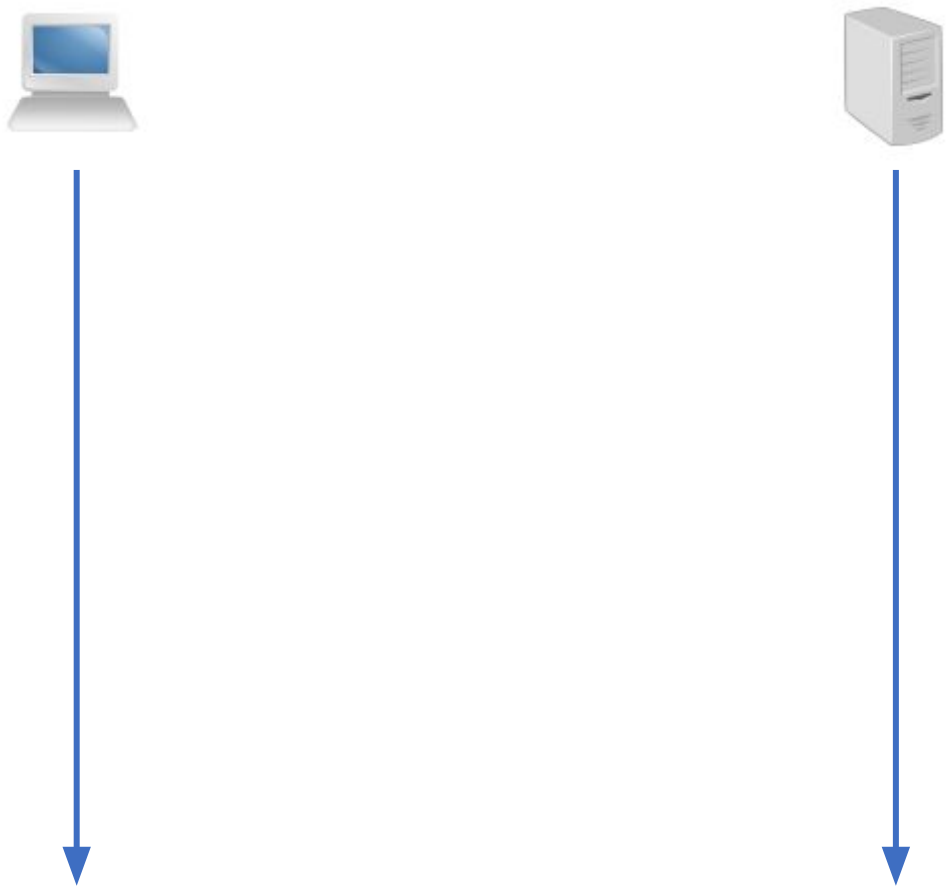
Tablas de enrutamiento



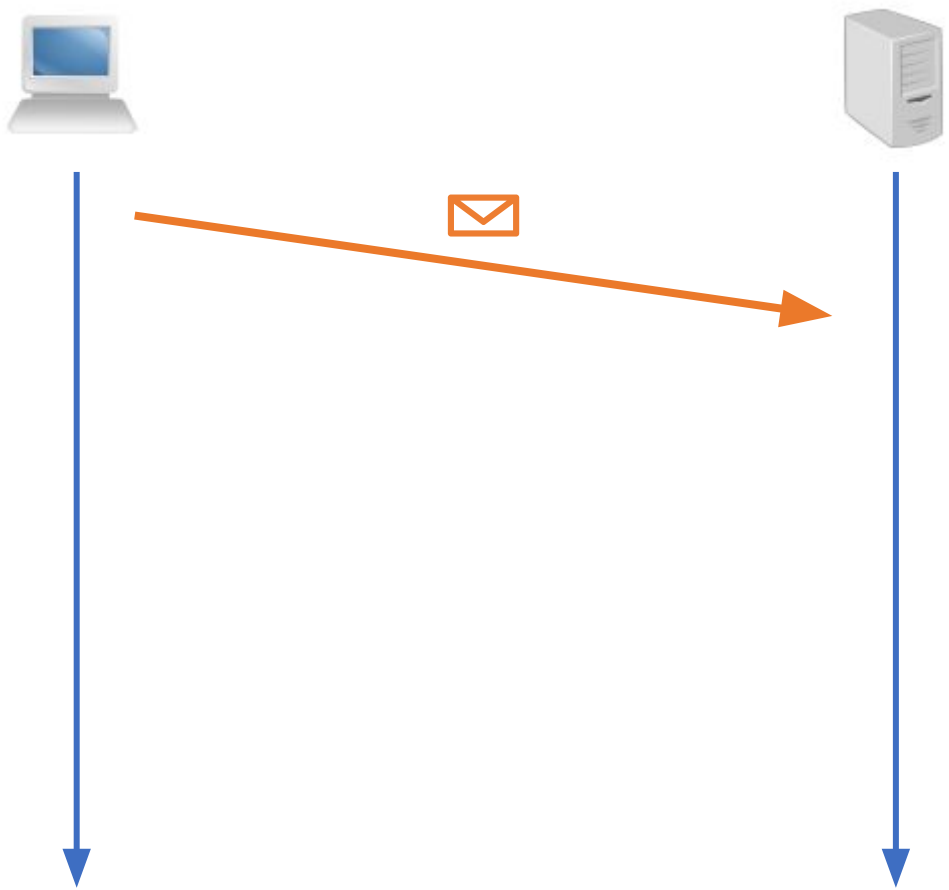
Escaneo y análisis de vulnerabilidades

Análisis de TCP y UDP

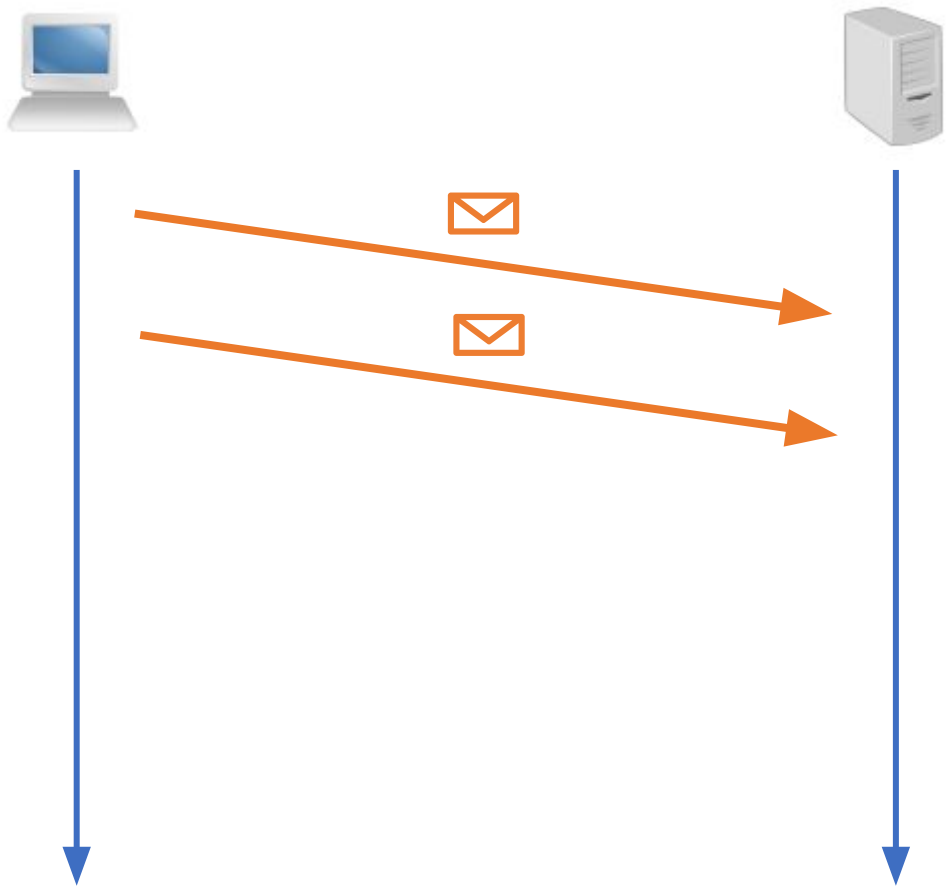
User Datagram Protocol (UDP)



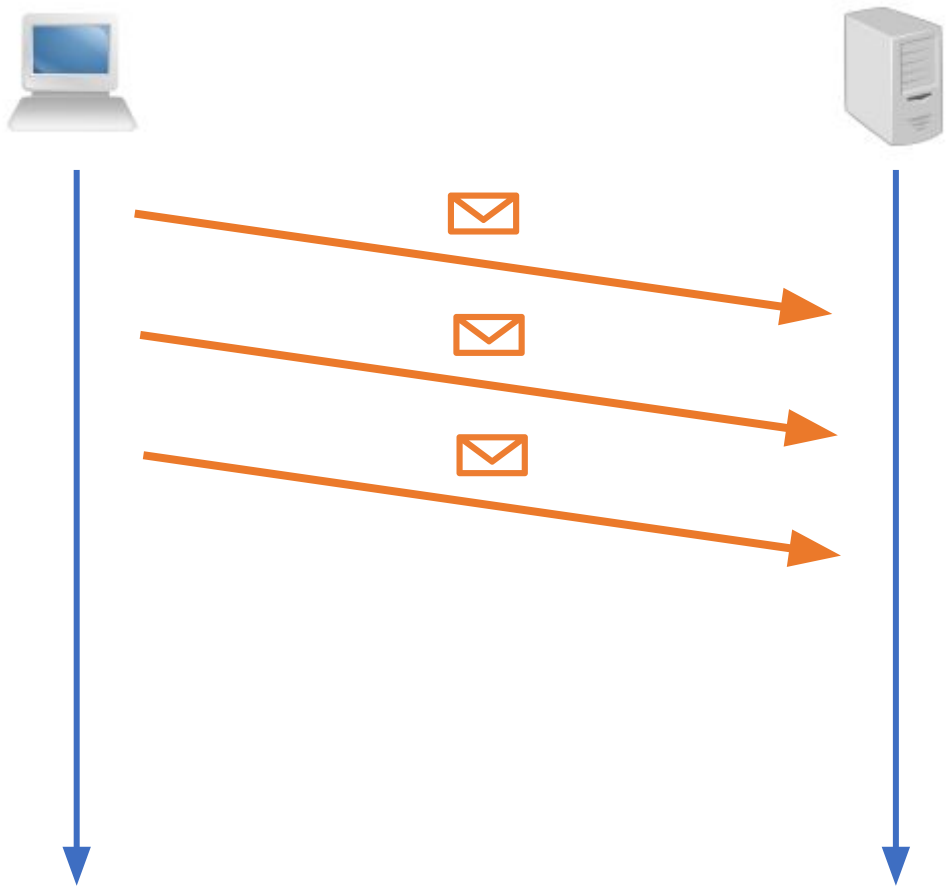
User Datagram Protocol (UDP)



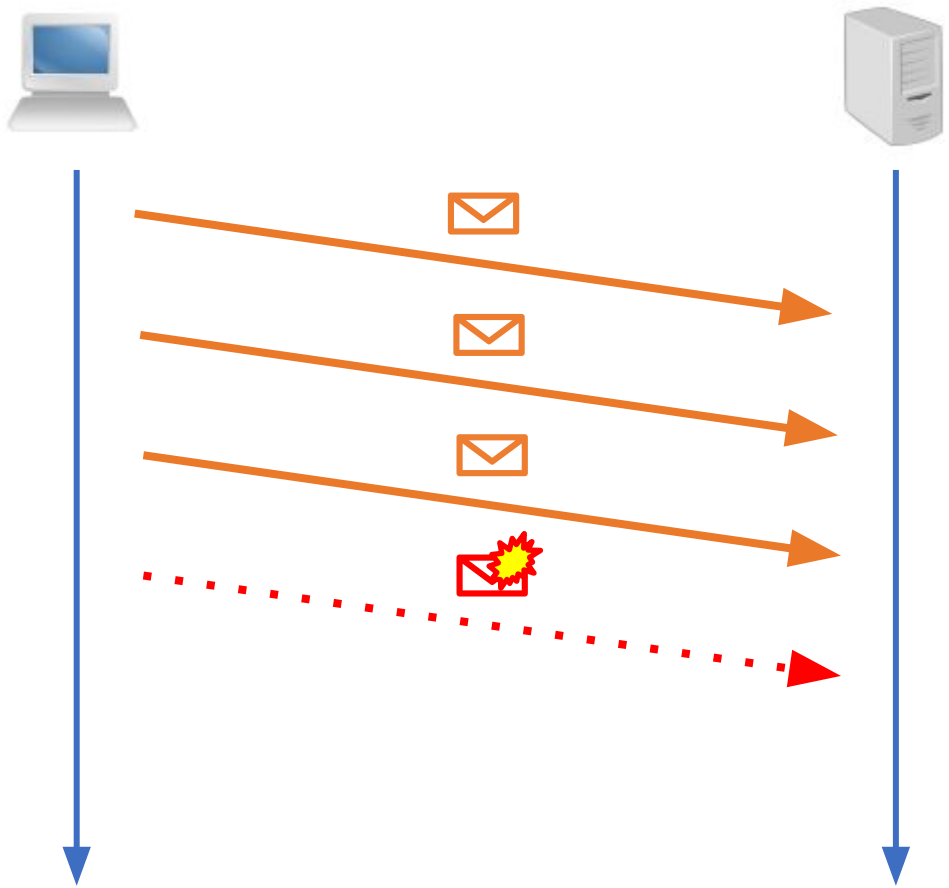
User Datagram Protocol (UDP)



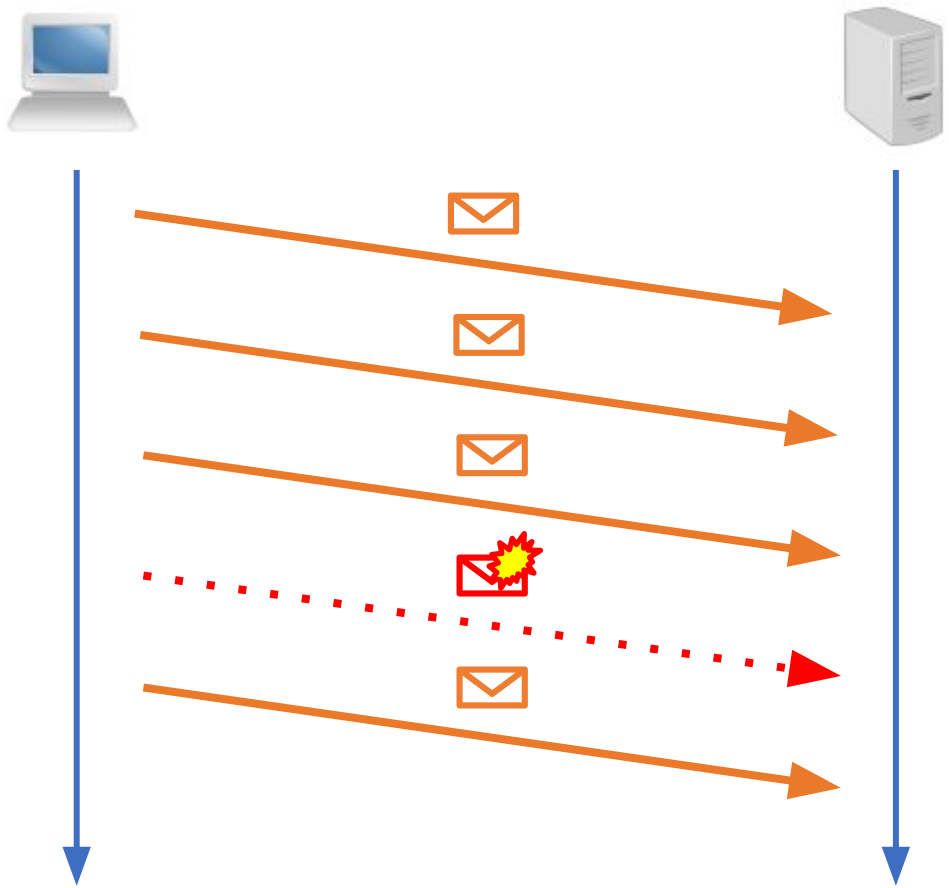
User Datagram Protocol (UDP)



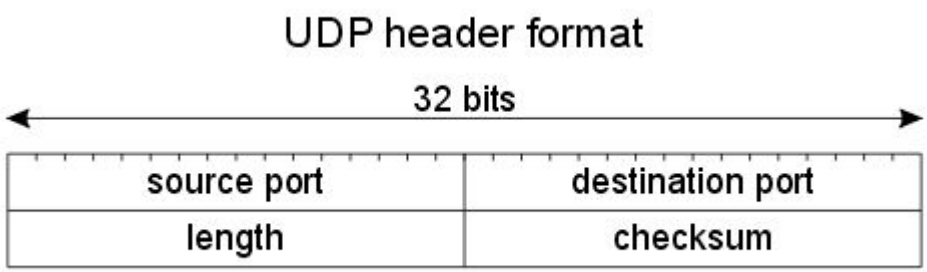
User Datagram Protocol (UDP)



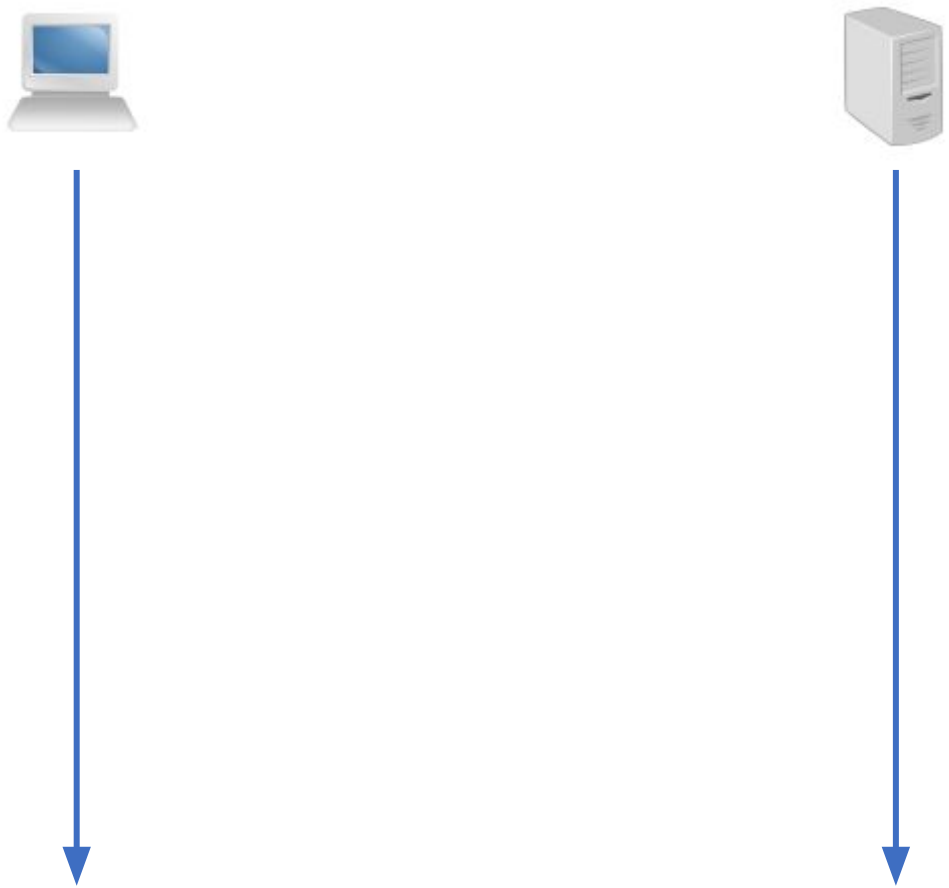
User Datagram Protocol (UDP)



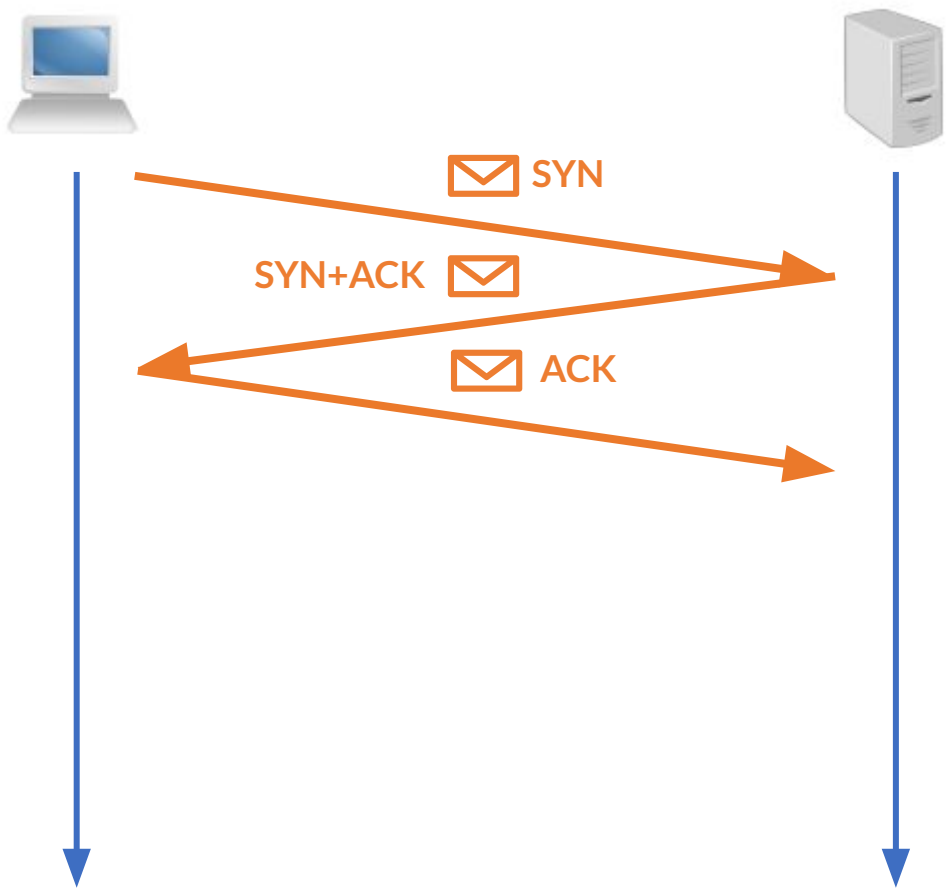
User Datagram Protocol (UDP)



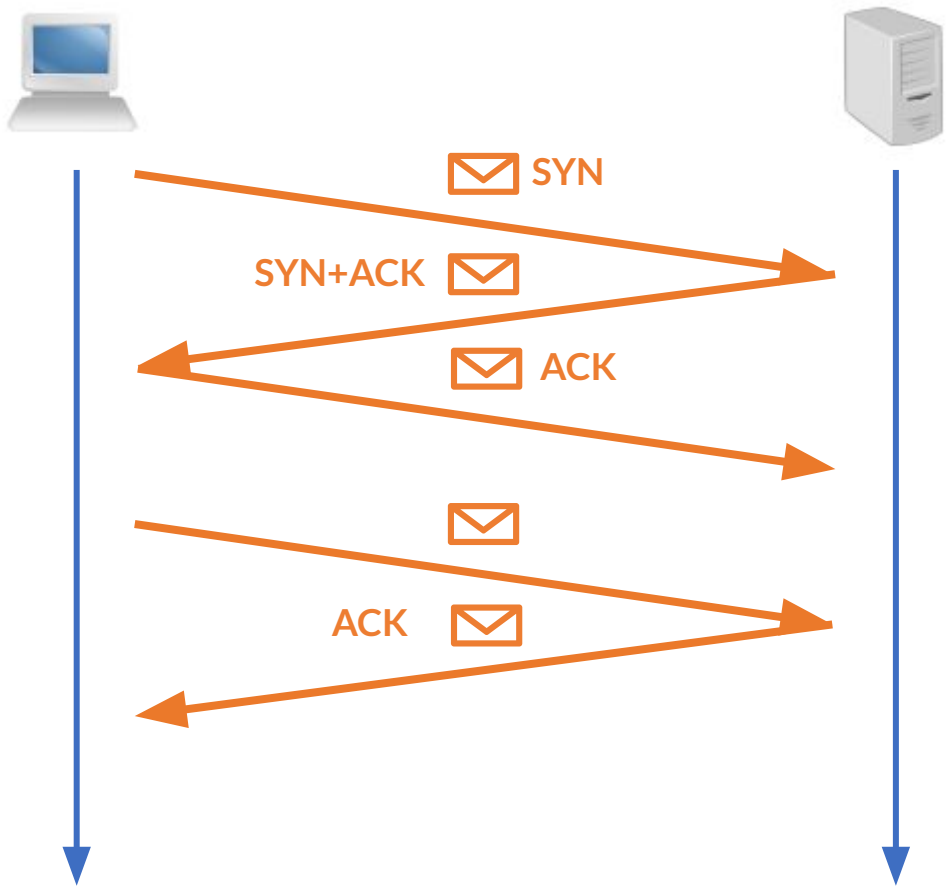
Transmission Control Protocol (TCP)



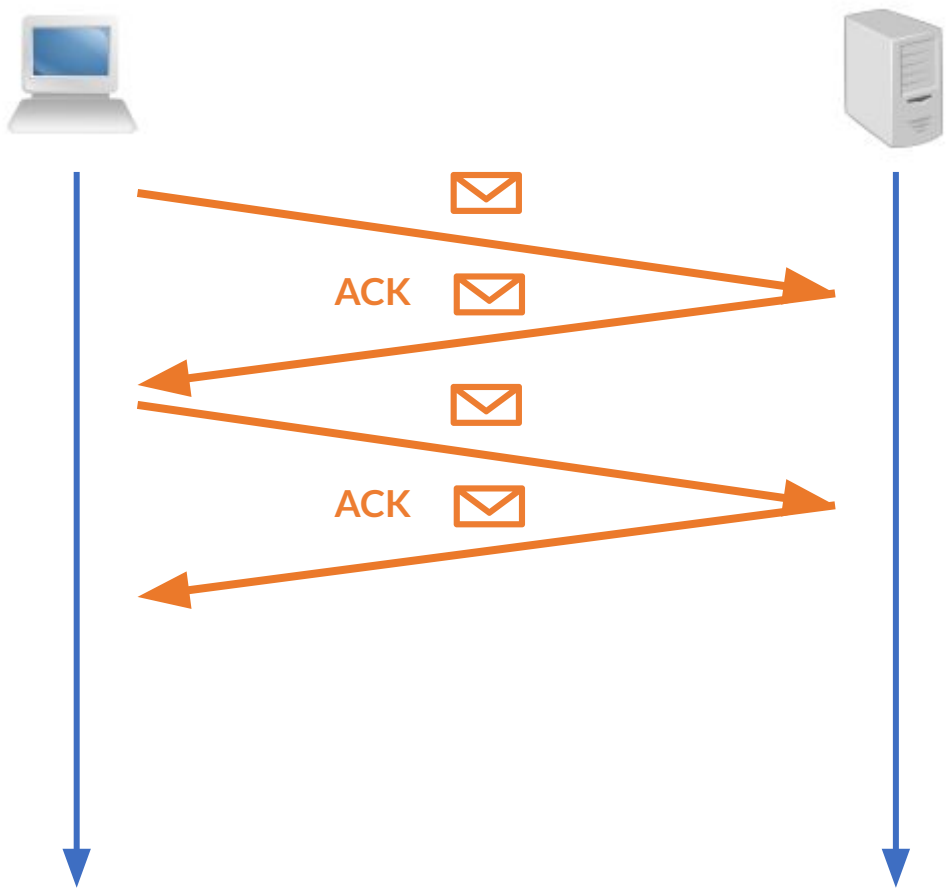
Transmission Control Protocol (TCP)



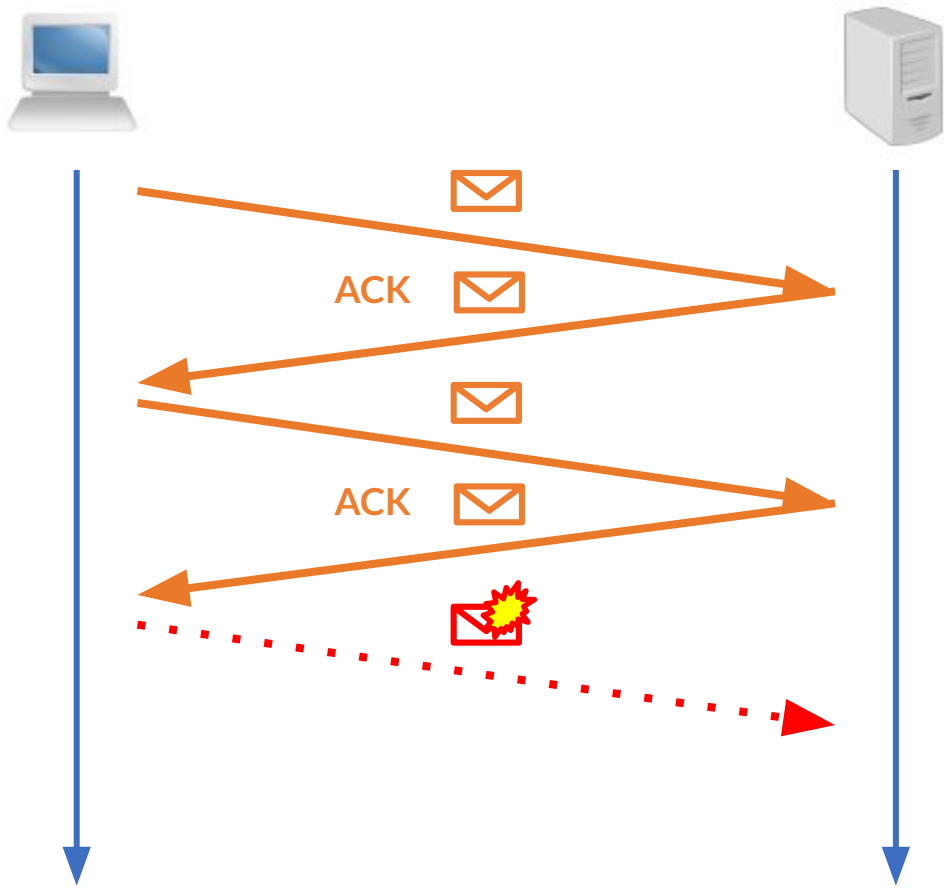
Transmission Control Protocol (TCP)



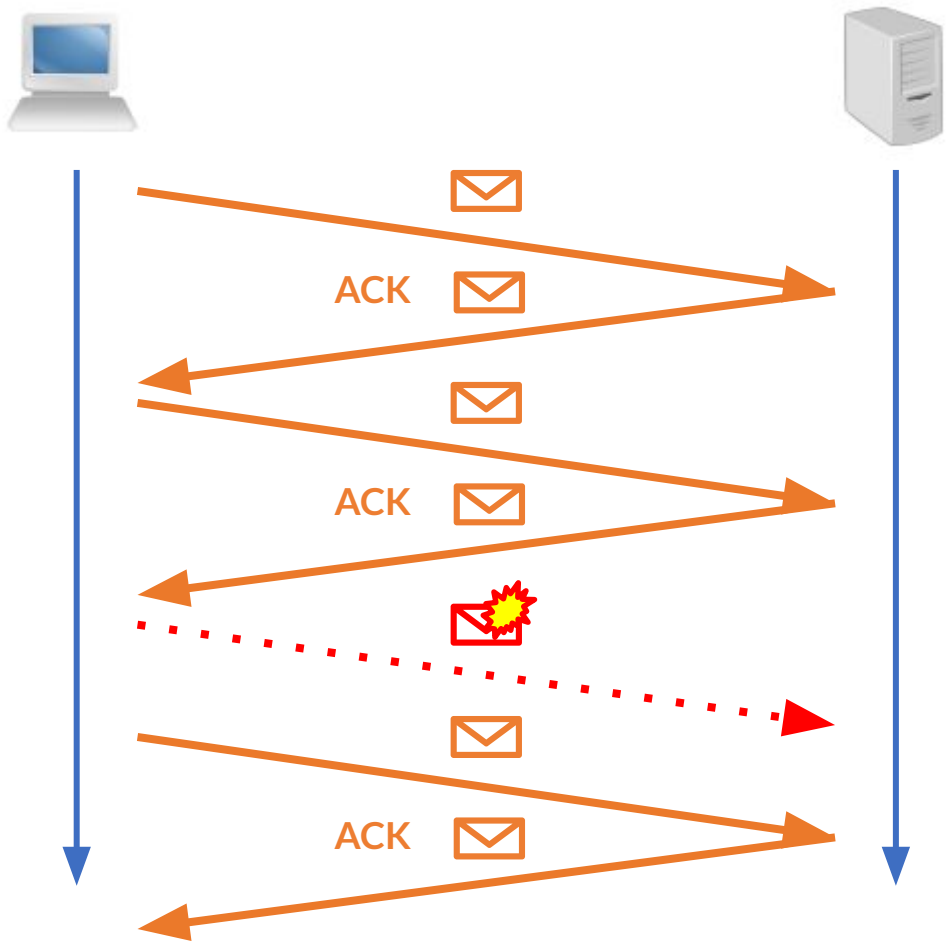
Transmission Control Protocol (TCP)



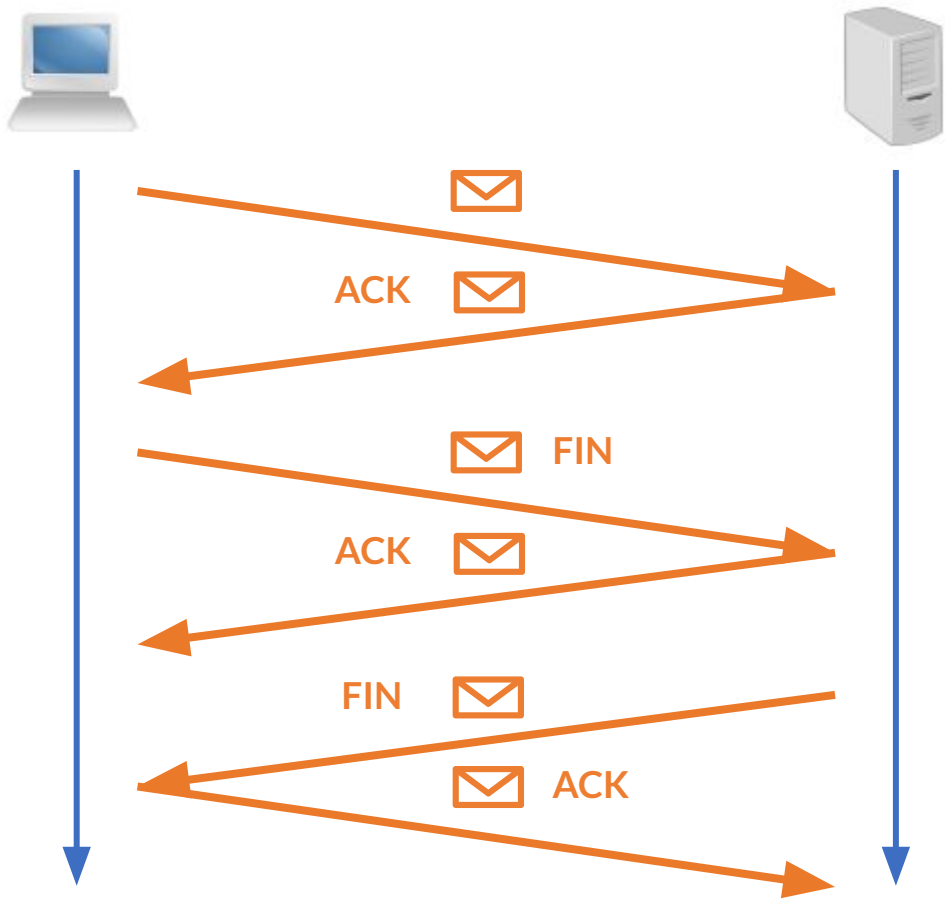
Transmission Control Protocol (TCP)



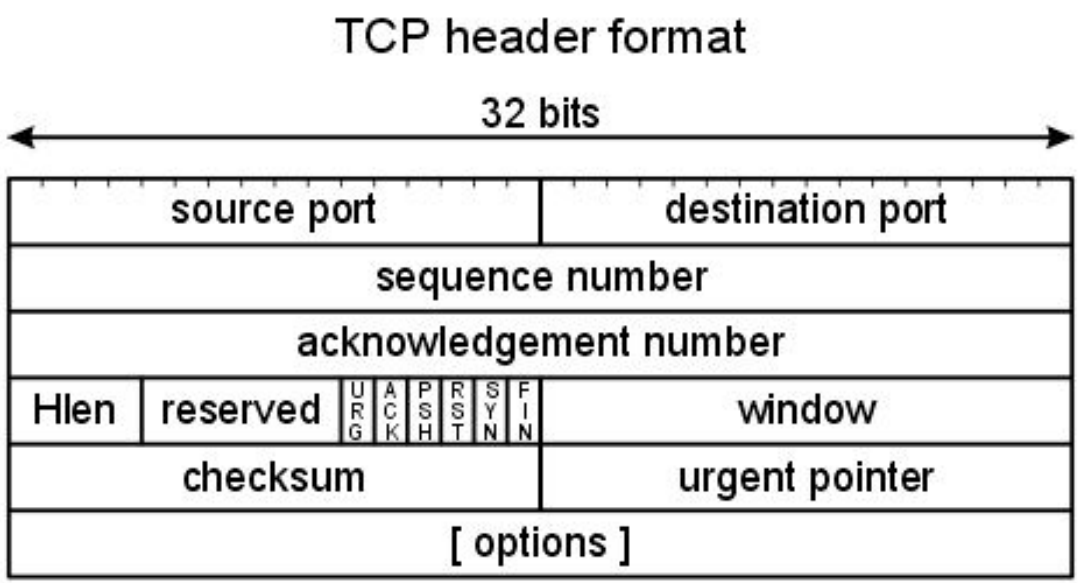
Transmission Control Protocol (TCP)



Transmission Control Protocol (TCP)



Transmission Control Protocol (TCP)



Algunos puertos comunes

Número de puerto	Servicio	Número de puerto	Servicio
20	Transferencia de FTP	443	HTTPS
21	Control de FTP	445	SMB
22	SSH	1433	MSSQL
23	Telnet	3306	MySQL
25	SMTP	3389	RDP
53	DNS	5800	VNC sobre HTTP
80	HTTP	5900	VNC
137 - 139	NetBIOS		