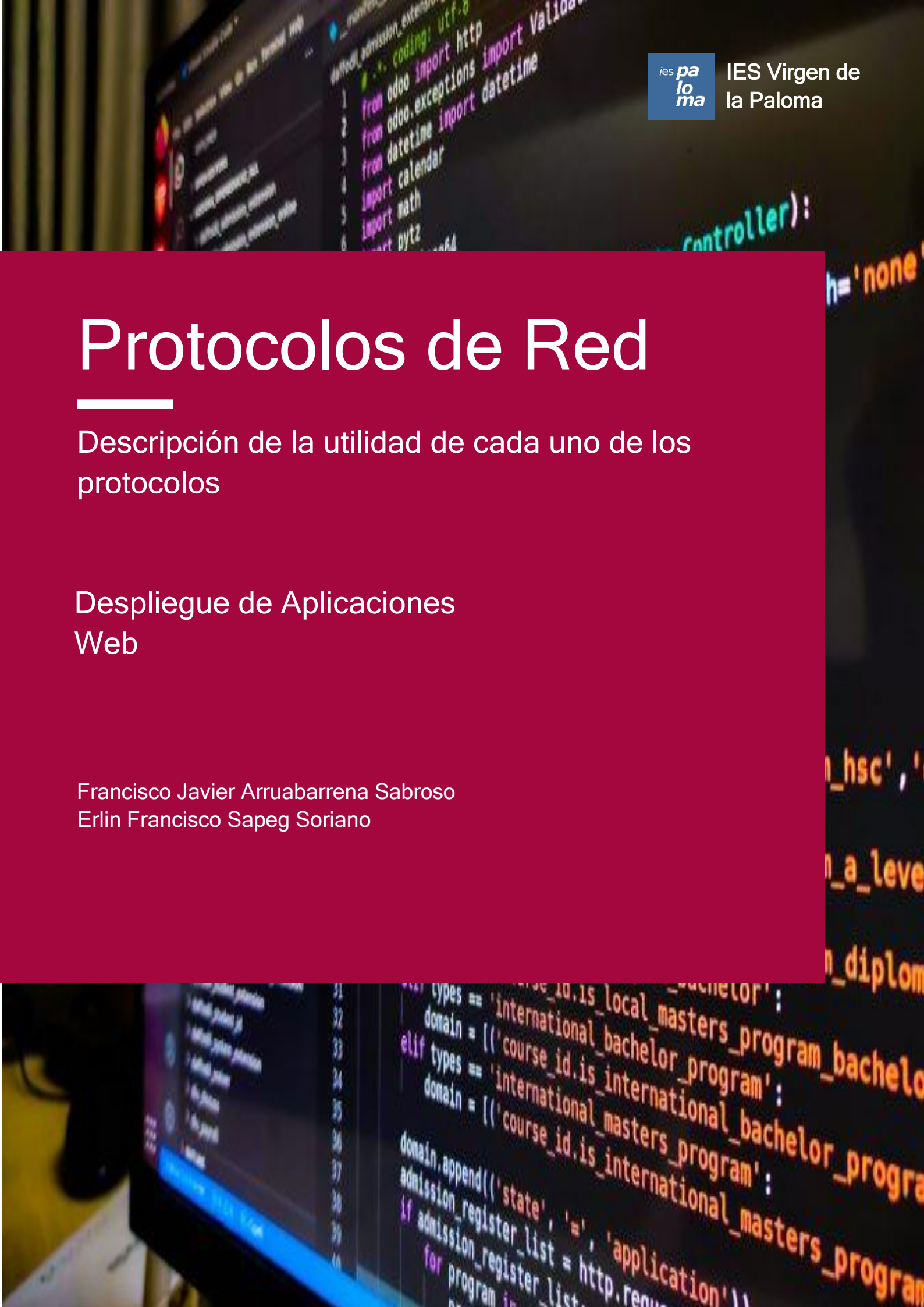


IES Virgen de la Paloma

Protocolos de Red

Descripción de la utilidad de cada uno de los protocolos

Despliegue de Aplicaciones Web

Francisco Javier Arruabarrena Sabroso
Erlin Francisco Sapeg Soriano

Índice

HTTP

Funciones principales

Transferencia de datos

HTTP permite la transferencia de diversos tipos de datos entre clientes y servidores web. Esto incluye texto, imágenes, videos y otros recursos multimedia.

Solicitudes y respuestas

El protocolo se basa en un modelo de solicitud-respuesta. El cliente (generalmente un navegador web) envía una solicitud HTTP al servidor, y este responde con los datos solicitados.

Métodos de solicitud

HTTP define varios métodos de solicitud como GET, POST, PUT y DELETE, que indican la acción deseada sobre el recurso.

Escenario de uso típico

Imaginemos una aplicación web de comercio electrónico:

1. Un usuario navega por el catálogo de productos. Cada vez que carga una nueva página, el navegador envía una solicitud HTTP GET al servidor.
2. Al agregar un producto al carrito, se envía una solicitud HTTP POST con los detalles del producto.
3. Para actualizar la cantidad de un producto en el carrito, se podría usar una solicitud HTTP PUT.
4. Si el usuario decide eliminar un producto del carrito, se enviaría una solicitud HTTP DELETE.

HTTPS

Funciones principales

Cifrado de datos
HTTPS cifra toda la información transmitida entre el cliente y el servidor, protegiendo datos sensibles como contraseñas, información de tarjetas de crédito y datos personales.

Autenticación
El protocolo verifica la identidad del sitio web al que se está conectando el usuario, ayudando a prevenir ataques de phishing y suplantación de identidad.

Integridad de datos
HTTPS garantiza que los datos no sean modificados o corrompidos durante la transmisión.

Escenario de uso típico

Consideremos una aplicación web de banca online:

1. Un usuario accede a su cuenta bancaria online. El navegador establece una conexión HTTPS con el servidor del banco.
2. El servidor presenta un certificado SSL que autentica su identidad como el banco legítimo.
3. Se establece un canal de comunicación cifrado entre el navegador y el servidor.
4. El usuario introduce sus credenciales de inicio de sesión, que se transmiten de forma segura a través de la conexión cifrada.
5. Todas las transacciones posteriores, como consultas de saldo o transferencias, se realizan a través de esta conexión segura.

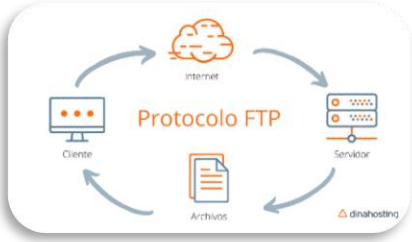
FTP

Funciones principales

Transferencia de archivos
FTP permite la transferencia bidireccional de archivos entre un cliente y un servidor a través de una red, independientemente del sistema operativo utilizado.

Gestión de archivos remotos
El protocolo facilita operaciones como crear, eliminar, renombrar y mover archivos y directorios en el servidor remoto.

Autenticación y control de acceso
FTP proporciona mecanismos de autenticación para controlar el acceso a los recursos del servidor, aunque también permite conexiones anónimas en algunos casos.



Escenario de uso típico

Consideremos una agencia de diseño web que mantiene varios sitios de clientes:

1. Un diseñador necesita actualizar el sitio web de un cliente. Utiliza un cliente FTP para conectarse al servidor web del cliente.
2. El diseñador sube nuevos archivos HTML y CSS que contienen las actualizaciones del diseño del sitio.
3. También transfiere imágenes y otros recursos multimedia actualizados al servidor.
4. El diseñador descarga los archivos de registro del servidor para analizar el tráfico del sitio.
5. Finalmente, actualiza algunos archivos de configuración del servidor web para reflejar los cambios realizados.

DNS

Funciones principales

Resolución de nombres

DNS traduce nombres de dominio legibles por humanos (como www.ejemplo.com) a direcciones IP numéricas (como 192.0.2.44) que las máquinas utilizan para comunicarse en redes.

Base de datos distribuida

DNS funciona como una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

Localización de servicios

Además de la resolución de nombres, DNS ayuda a localizar servicios específicos, como los servidores de correo electrónico correspondientes a cada dominio

Escenario de uso típico

Imaginemos un usuario que quiere acceder a un sitio web:

1. El usuario escribe "www.example.com" en su navegador web.
2. El navegador envía una solicitud al solucionador de DNS del proveedor de servicios de Internet (ISP) del usuario.
3. El solucionador de DNS consulta a los servidores de nombres raíz, luego a los servidores de nombres de dominio de nivel superior (.com), y finalmente a los servidores de nombres autoritativos para example.com.
4. El servidor DNS autoritativo responde con la dirección IP correspondiente a www.example.com.
5. El solucionador de DNS devuelve esta dirección IP al navegador del usuario.
6. El navegador establece una conexión con el servidor web en la dirección IP proporcionada y solicita la página web.

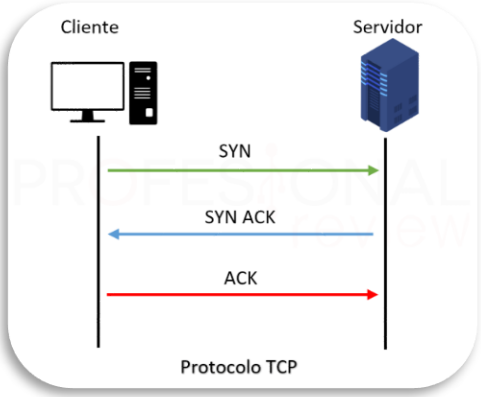
TCP

Funciones principales

Transmisión confiable de datos
TCP garantiza que los datos se entreguen de manera ordenada y sin errores entre aplicaciones en dispositivos conectados a una red.

Control de flujo
El protocolo implementa mecanismos para evitar la saturación de la red, ajustando la velocidad de transmisión según sea necesario.

Orientación a la conexión
TCP establece y mantiene una conexión entre el emisor y el receptor antes de iniciar la transferencia de datos.



Escenario de uso típico

Consideremos una situación de navegación web:

1. Un usuario ingresa la URL de un sitio web en su navegador.
2. El navegador inicia una conexión TCP con el servidor web (handshake de tres vías).
3. Una vez establecida la conexión, el navegador envía una solicitud HTTP al servidor.
4. El servidor responde enviando los datos de la página web en múltiples paquetes TCP.
5. TCP en el dispositivo del usuario recibe los paquetes, los ordena correctamente y confirma su recepción.
6. Si algún paquete se pierde, TCP solicita su retransmisión.
7. Una vez recibidos todos los datos, el navegador muestra la página web al usuario.
8. Finalmente, la conexión TCP se cierra cuando la transferencia se completa.

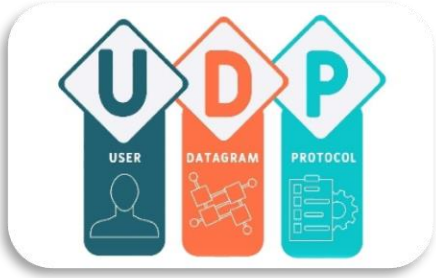
UDP

Funciones principales

Transmisión rápida de datos
UDP permite el envío de datagramas a través de la red sin establecer una conexión previa, priorizando la velocidad sobre la fiabilidad.

Comunicación sin conexión
Facilita el envío de datagramas incluso antes de que se haya establecido una conexión entre emisor y receptor.

Multiplexación de aplicaciones
Utiliza puertos para distinguir entre diferentes aplicaciones en el mismo dispositivo, permitiendo la comunicación simultánea de múltiples servicios.



Escenario de uso típico

Consideremos una aplicación de videoconferencia en tiempo real:

1. Un usuario inicia una llamada de video en su aplicación.
2. La aplicación comienza a enviar paquetes UDP con datos de audio y video.
3. Estos paquetes se envían rápidamente sin esperar confirmación de recepción.
4. El receptor recibe los paquetes y los reproduce inmediatamente.
5. Si algunos paquetes se pierden, la aplicación continúa con los siguientes sin intentar recuperarlos.
6. Esto resulta en una transmisión de baja latencia, aunque ocasionalmente puede haber pequeñas interrupciones en el audio o video

IP

Funciones principales

Direccionamiento
IP asigna direcciones únicas a cada dispositivo en una red, permitiendo la identificación y localización de hosts.

Encapsulamiento de datos
IP encapsula los datos en paquetes, incluyendo información de origen, destino y otros metadatos necesarios para el enrutamiento.

Enrutamiento
IP es responsable de dirigir los paquetes desde el origen hasta el destino a través de una o más redes IP.

Escenario de uso típico

Un usuario ingresa una URL en su navegador.

1. El navegador solicita la resolución del nombre de dominio a un servidor DNS.
2. Una vez obtenida la dirección IP del servidor web, el navegador crea paquetes IP con la solicitud HTTP.
3. Cada paquete IP contiene la dirección IP de origen (el dispositivo del usuario) y la dirección IP de destino (el servidor web).
4. Los paquetes se envían a través de la red, pasando por varios routers que utilizan la información de direccionamiento IP para dirigirlos.
5. Los paquetes llegan al servidor web de destino, que los procesa y envía una respuesta utilizando el mismo proceso IP.

ICMP

Funciones principales

Notificación de errores
ICMP se utiliza para enviar mensajes de error e información operativa, indicando por ejemplo que un host no puede ser localizado o que un servicio solicitado no está disponible.

Diagnóstico de red
Facilita herramientas de diagnóstico como ping y traceroute para evaluar la conectividad y el rendimiento de la red.

Control de flujo

Permite implementar mecanismos como el enfriamiento de fuente, informando a los clientes que deben reducir su velocidad de transferencia de datos.

Escenario de uso típico

Consideremos un escenario de diagnóstico de red:

1. Un administrador de red quiere verificar la conectividad con un servidor remoto.
2. Utiliza el comando ping, que envía paquetes ICMP de solicitud de eco al servidor.
3. Si el servidor es alcanzable, responde con paquetes ICMP de respuesta de eco.
4. El ping muestra el tiempo de ida y vuelta de los paquetes y si hubo pérdida de paquetes.
5. Si hay problemas, el administrador puede usar traceroute, que también utiliza ICMP.
6. Traceroute muestra la ruta que siguen los paquetes y dónde pueden estar ocurriendo retrasos o pérdidas.

ARP

Funciones principales

Resolución de direcciones
ARP traduce direcciones IP a direcciones MAC (Media Access Control) en redes locales.

Mantenimiento de caché
ARP mantiene una tabla de caché con mapeos de direcciones IP a MAC para reducir el tráfico de red.

Comunicación entre capas
ARP facilita la comunicación entre la capa de red (IP) y la capa de enlace de datos (Ethernet) del modelo OSI.

Escenario de uso típico

1. Consideremos una situación de comunicación en una red local:
2. El Host A quiere enviar un paquete al Host B en la misma red local.
3. El Host A conoce la dirección IP del Host B, pero necesita su dirección MAC.
4. El Host A verifica primero su caché ARP en busca de la dirección MAC del Host B.
5. Si no la encuentra, el Host A envía una solicitud ARP de difusión a toda la red.
6. La solicitud ARP contiene la dirección IP del Host B y se envía a la dirección MAC de difusión (FF:FF:FF:FF:FF:FF).
7. Todos los dispositivos en la red reciben la solicitud, pero solo el Host B responde.
8. El Host B envía una respuesta ARP directamente al Host A con su dirección MAC.
9. El Host A actualiza su caché ARP con la nueva información.
10. Ahora el Host A puede enviar el paquete al Host B utilizando la dirección MAC obtenida.

Ethernet

Funciones principales

Transmisión de datos
Ethernet permite la transmisión de datos entre dispositivos en una red local (LAN) utilizando tramas.

Direccionamiento
Utiliza direcciones MAC de 48 bits para identificar de manera única los dispositivos en la red.

Control de acceso al medio
Implementa mecanismos para gestionar el acceso al medio compartido y evitar colisiones.

Escenario de uso típico
Consideremos una red local de oficina:

1. Un empleado envía un correo electrónico con un archivo adjunto a un colega.
2. La tarjeta de red del ordenador del empleado crea una trama Ethernet.
3. La trama incluye la dirección MAC de destino (el ordenador del colega) y la dirección MAC de origen.
4. La trama también contiene un campo de tipo/longitud que indica el protocolo de capa superior (por ejemplo, IP).
5. Los datos del correo electrónico y el archivo adjunto se encapsulan en la sección de datos de la trama.
6. La trama se transmite a través del cable Ethernet o switch.
7. Otros dispositivos en la red reciben la trama, pero solo el ordenador de destino la procesa completamente.
8. El ordenador de destino extrae los datos y los pasa al protocolo de capa superior correspondiente.

Wi-Fi

Funciones principales

Conectividad inalámbrica
Wi-Fi permite la conexión inalámbrica de dispositivos a una red local, facilitando el acceso a internet y recursos compartidos sin necesidad de cables.

Transmisión de datos
Permite la transmisión de datos a alta velocidad entre dispositivos dentro del alcance de la red.

Compatibilidad
Asegura la interoperabilidad entre dispositivos de diferentes fabricantes que cumplen con el estándar.

Escenario de uso típico

Consideremos un entorno de oficina moderno:

1. Una empresa instala puntos de acceso Wi-Fi en sus instalaciones.
2. Los empleados llegan a la oficina con sus laptops, tablets y smartphones.
3. Los dispositivos detectan automáticamente la red Wi-Fi disponible.
4. Los empleados se conectan a la red introduciendo la contraseña correspondiente.
5. Una vez conectados, pueden acceder a internet, recursos compartidos en la red y servicios en la nube.
6. Durante una reunión, un empleado comparte su pantalla inalámbricamente con un proyector Wi-Fi.
7. Al moverse por la oficina, los dispositivos cambian automáticamente entre puntos de acceso para mantener la mejor señal.

Bibliografía

SSD Nodes → http
Wikipedia → http
Cloudflare → http
Isquaredsoftware → http
Dinahosting → https
Ryte → https
Wikipedia → https
Fortinet → ftp
Progress → ftp
Cdmon → ftp
Microsoft → dns
Amazon → dns
Alcancelibre → dns
Wikipedia → tcp
Nosololinux → tcp
Hostinger → tcp
Keepcoding → udp
Checkpoint → udp
Wikipedia → udp
Wikipedia → ip
Cloudfare → ip
Techtarget → ip
Wikipedia → icmp
Fortinet → icmp
Amazon → icmp
Study-ccna → arp
Geeksforgeeks → arp
Techtarget → arp
Uh → ethernet
Lantronix → ethernet
Freecodecamp → ethernet
Vadavo → Wi-Fi
Intel → Wi-Fi
Ymant → Wi-Fi