

Aspectos básicos de redes



Introducción

- Con el desarrollo de Internet, siguen surgiendo ataques a las redes y la seguridad de la red se vuelve todavía más importante. La aplicación de tecnologías de seguridad a la comunicación de datos es una extensión de las tecnologías de comunicación de datos. Antes de aprender sobre las tecnologías de seguridad, tener conocimientos básicos de redes, tales como principios básicos de comunicación de redes, infraestructura de redes y protocolos de red común pueden ayudarle a entender mejor los principios operativos y los escenarios de aplicación de diferentes tecnologías de seguridad.
- Este capítulo describe la arquitectura de la red empresarial típica, dispositivos de red comunes y sus principios operativos, así como los modos de configuración del firewall basado en una interfaz gráfica de usuario (GUI) o una interfaz de línea de comandos (CLI).

Objetivos

- Una vez que finalice este curso, podrá hacer lo siguiente:
 - Comprender la definición de datos y el proceso de transmisión.
 - Describir los principios básicos de la pila de protocolos TCP/IP.
 - Describir los principios operativos de los protocolos comunes.
 - Describir dispositivos de red comunes y sus principios operativos.

Índice

1. Modelo de referencia de red

- Modelo de referencia OSI y modelo de referencia TCP/IP
 - Capa de aplicación
 - Capa de transporte
 - Capa de red
 - Capa de enlace de datos

2. Dispositivos de red comunes

Aplicaciones y datos

- Las aplicaciones se desarrollan para cumplir con los diferentes requisitos de los usuarios, tales como acceso de página web, juegos en línea y reproducción de videos en línea. La información se genera junto con las aplicaciones, y se la presenta de diversas maneras, como texto, imágenes y videos.
- Para los ingenieros de red, las aplicaciones pueden generar datos. Los datos transportan todo tipo de información y el símbolo físico o la combinación de varios símbolos físicos que registran la naturaleza, estado y relaciones de objetos. Los datos pueden ser símbolos, textos, dígitos, voces, imágenes y videos.
- Los datos que generan la mayoría de las aplicaciones necesitan ser transmitidos entre dispositivos. Los ingenieros de red necesitan prestarle más atención al proceso de transmisión de datos de extremo a extremo.



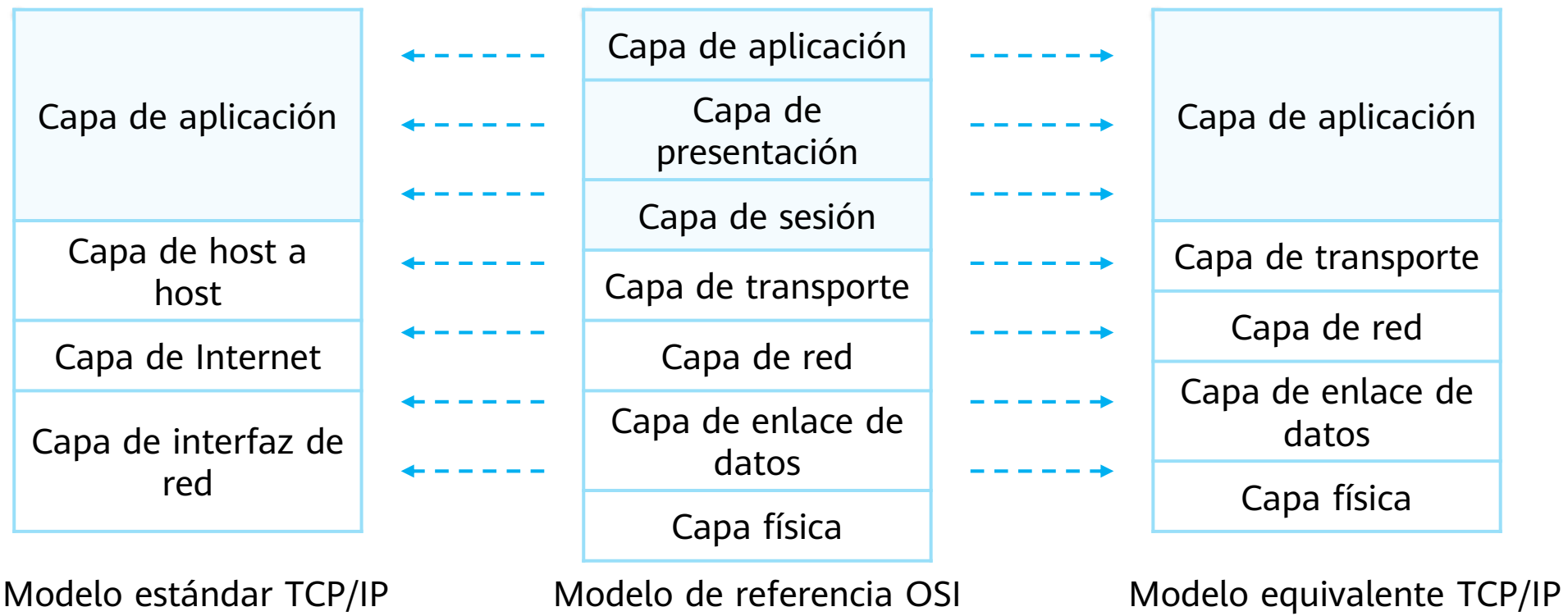
Modelo de referencia OSI

- El modelo de referencia de la interconexión de sistemas abiertos (OSI) fue propuesto por la Organización Internacional para la Normalización (ISO) en 1984 para la interconexión de redes. El modelo de referencia OSI tiene una arquitectura de siete niveles.

Capa	Función
Capa de aplicación	Provee interfaces de red para aplicaciones.
Capa de presentación	Convierte formatos de datos para garantizar que los datos de la capa de aplicación de un sistema puedan ser identificados y comprendidos por la capa de aplicación de otro sistema.
Capa de sesión	Crea, gestiona y finaliza sesiones entre las partes comunicantes.
Capa de transporte	Crea, mantiene y cancela el proceso de transmisión de datos de extremo a extremo. Controla la velocidad de transmisión y ajusta las secuencias de datos.
Capa de red	Define direcciones lógicas y transfiere información del origen al punto de destino.
Capa de enlace de datos	Encapsula paquetes en tramas, transmite tramas en modos de punto a punto o punto a multipunto e implementa la detección de errores.
Capa física	Transmite flujos de bits a través de un medio de transmisión y define las especificaciones eléctricas y físicas.

Modelo de referencia TCP/IP

- El modelo de referencia OSI es complejo y los protocolos TCP/IP se utilizan ampliamente en la industria. Por lo tanto, el modelo de referencia TCP/IP se ha convertido en el modelo de referencia real de Internet.



Protocolos comunes de la pila de protocolos TCP/IP

- La pila de protocolos TCP/IP define una serie de protocolos estándar.

Capa de aplicación	Telnet	FTP	TFTP	SNMP
	HTTP	SMTP	DNS	DHCP
Capa de transporte	TCP		UDP	
Capa de red	ICMP		IGMP	
	IP			
Capa de enlace de datos	PPPoE			
	Ethernet		PPP	
Capa física	...			

Índice

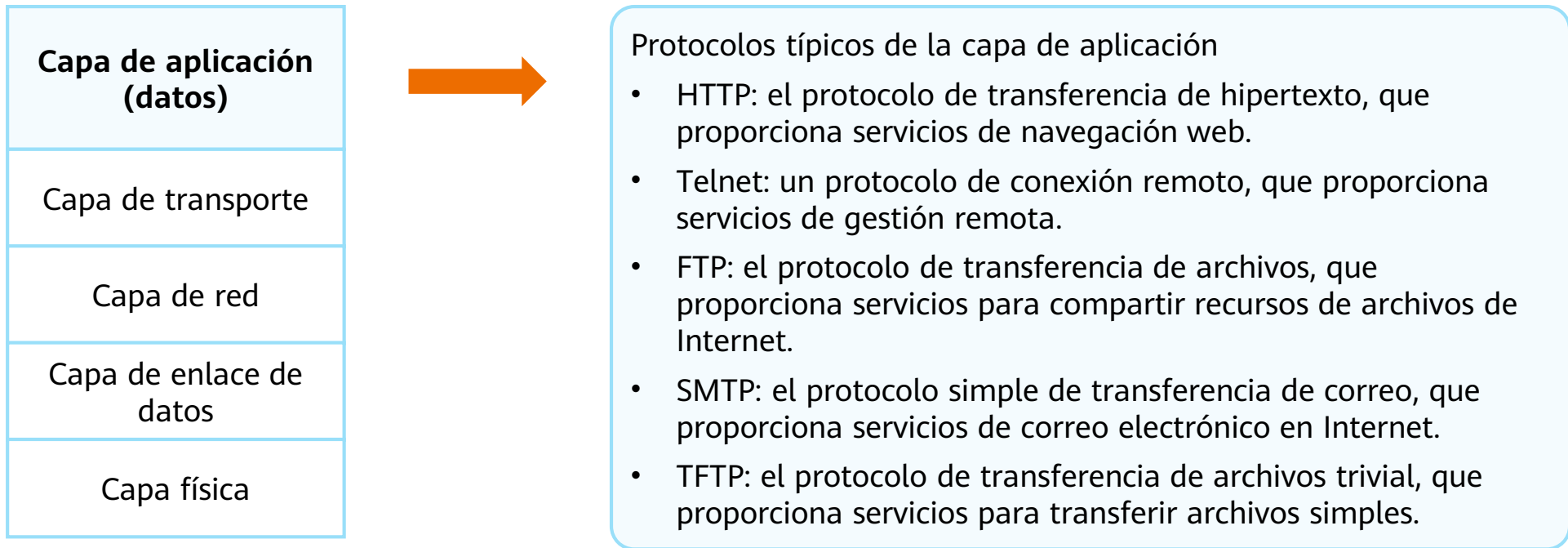
1. Modelo de referencia de red

- Modelo de referencia OSI y modelo de referencia TCP/IP
- Capa de aplicación
- Capa de transporte
- Capa de red
- Capa de enlace de datos

2. Dispositivos de red comunes

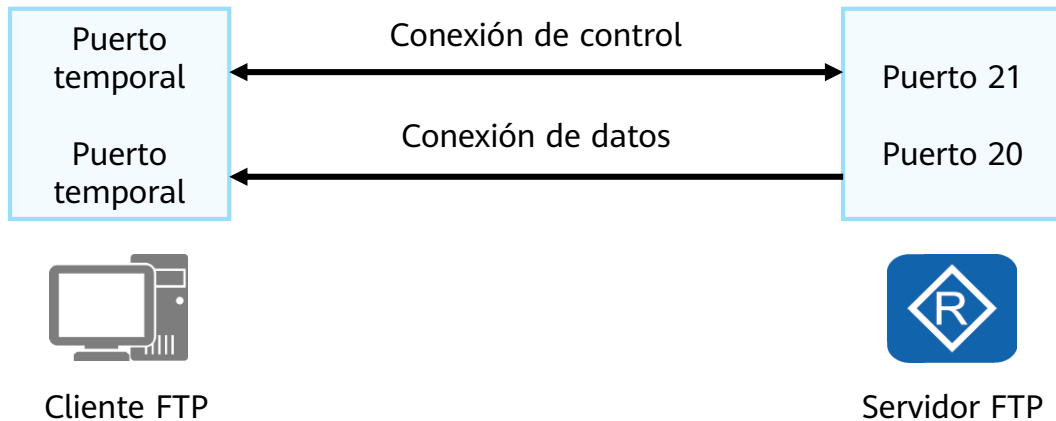
Capa de aplicación

- La capa de aplicación proporciona interfaces para la aplicación de software de modo que las aplicaciones puedan utilizar los servicios de red. Con base en un protocolo de la capa de transporte, las aplicaciones definen el número de puerto utilizado en la capa de transporte.

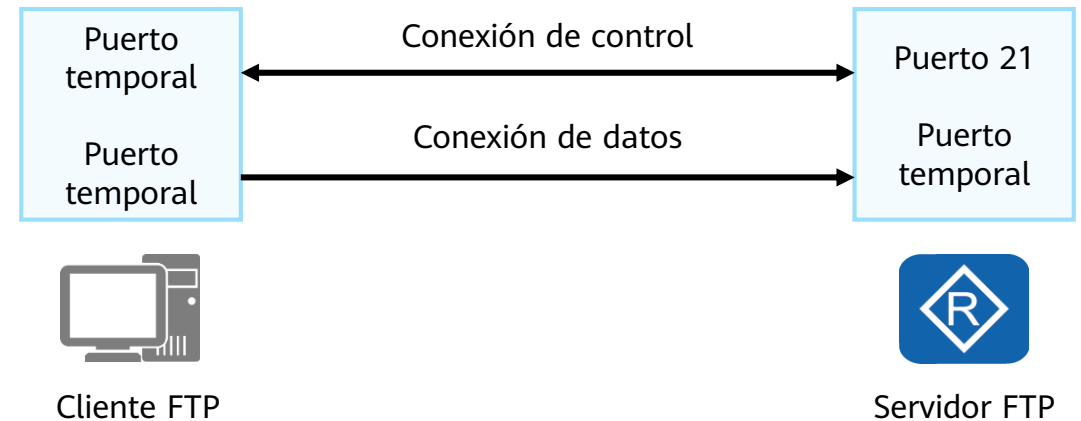


FTP

- El protocolo de transferencia de archivos (FTP) transfiere archivos de un host a otro para implementar la descarga y carga de archivos. Este protocolo adopta la estructura cliente/servidor (C/S). Cuando se utiliza FTP para la transmisión de datos, se establece la conexión de control y conexión de datos entre el servidor y el cliente.
- La conexión FTP se puede configurar en modo pasivo o proactivo. La diferencia entre los dos modos está en quien inicia la conexión de datos, ya sea el servidor o el cliente. Por defecto, se usa el modo proactivo. Los usuarios pueden cambiar al modo pasivo usando comandos.



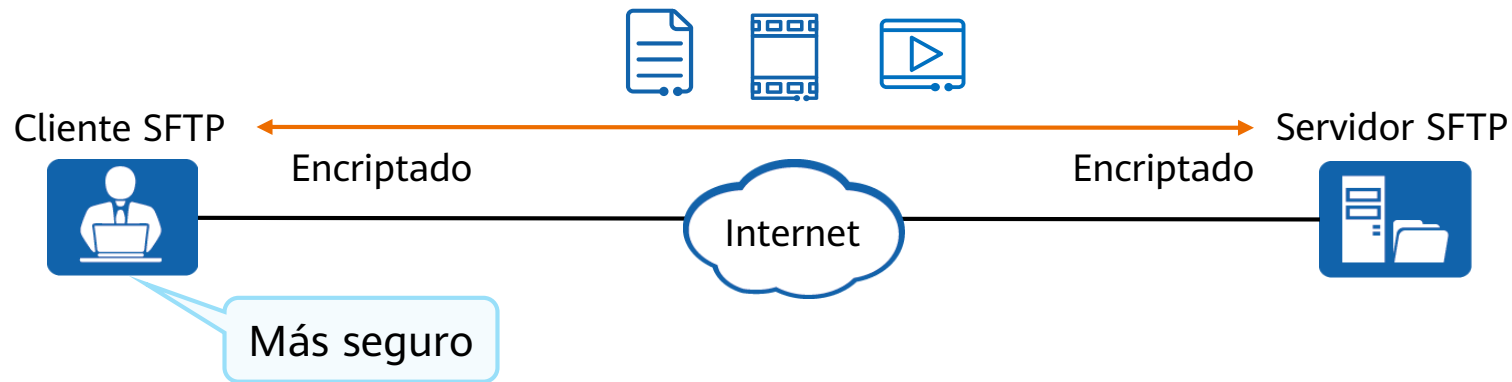
Modo proactivo



Modo pasivo

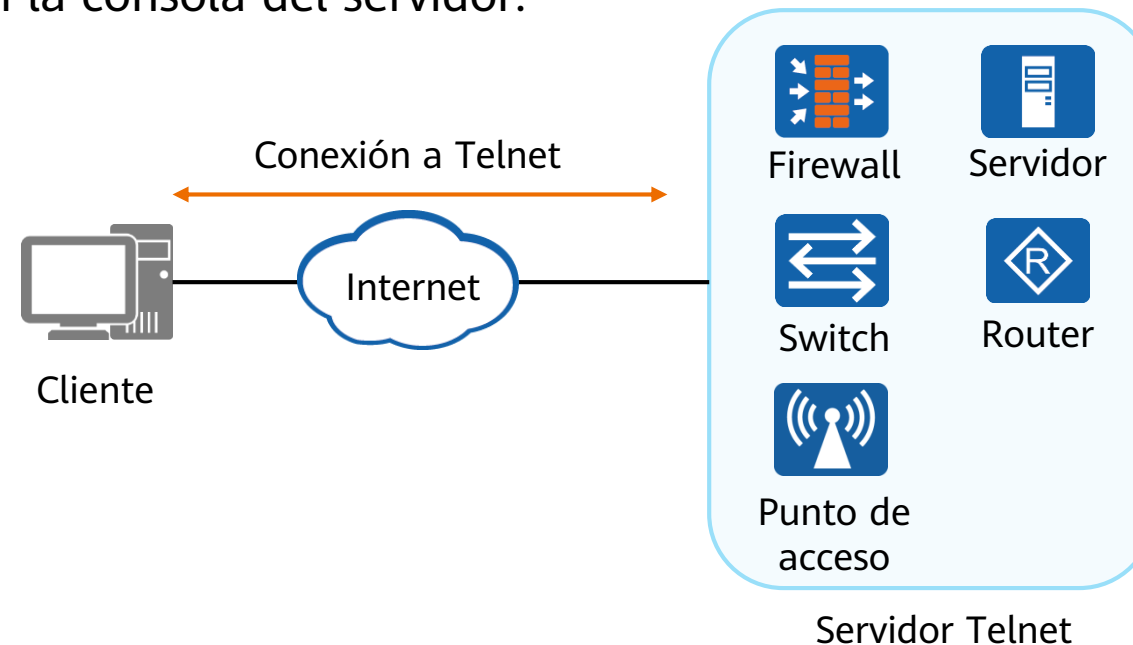
SFTP

- El protocolo de transferencia de archivos segura (SFTP) transmite archivos de manera segura basado en Secure Shell (SSH).
- FTP transmite datos en texto sin formato, lo cual no es seguro. SFTP encripta la información de autenticación y los datos para transmitir, con una nivel de seguridad más alto que FTP.
- SFTP es un protocolo de canal único y su número de puerto de destino por defecto es el 22. El cliente y el servidor se conectan de manera segura mediante la utilización de SSH para transferir archivos. FTP es un protocolo de dos canales, que incluye el canal de control y el canal de datos.



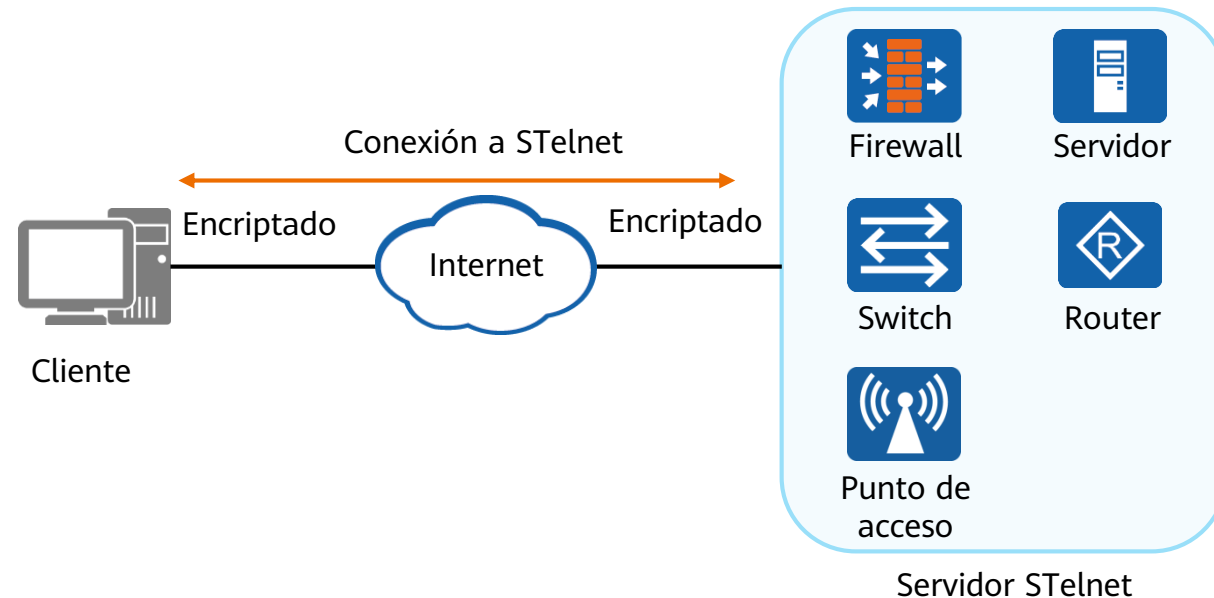
Telnet

- Telnet es un protocolo estándar que proporciona servicios de conexión remota para una red.
- Ayuda a los usuarios a manejar dispositivos remotos a través de PC locales.
- Los usuarios se conectan a un servidor Telnet a través de un programa del cliente Telnet. Los comandos que se ingresan en el cliente Telnet los ejecuta el servidor Telnet, como si los comandos se hubieran introducido en la consola del servidor.



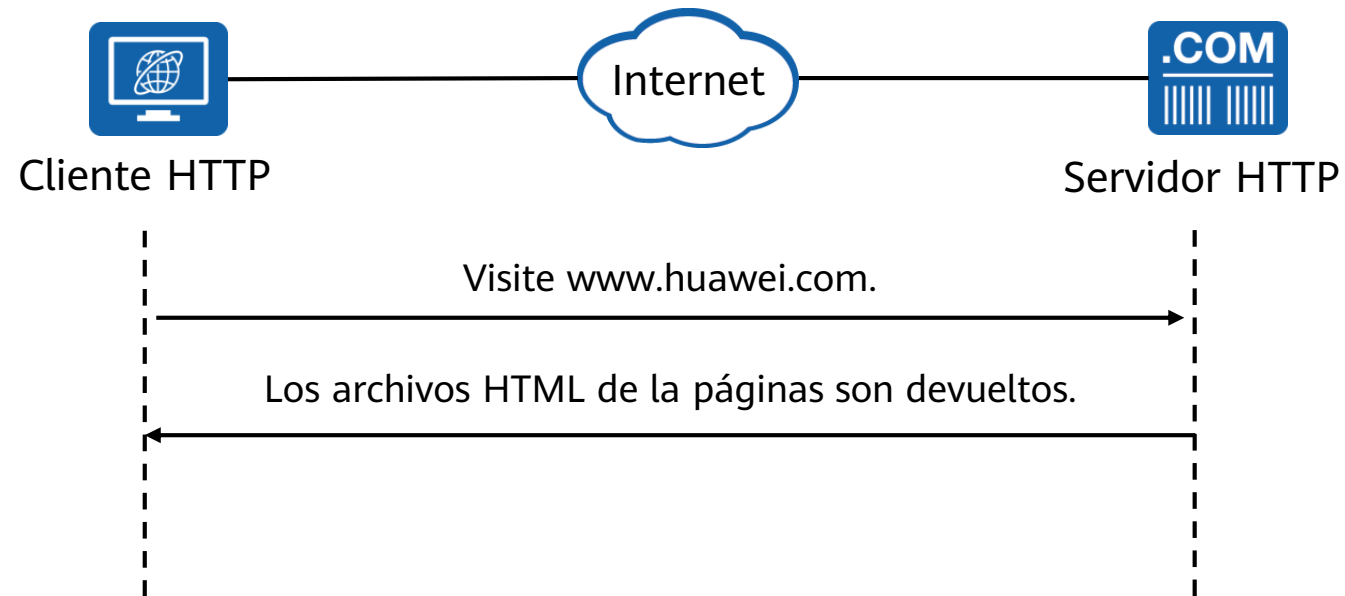
STelnet

- Secure Telnet (STelnet) es un servicio seguro de Telnet que le permite a los usuarios conectarse a dispositivos de manera remota y segura. A través de STelnet, todos los datos intercambiados se encriptan y además se implementan sesiones seguras. Telnet transmite datos en texto sin formato, lo cual no es seguro. La seguridad de la red puede mejorarse enormemente con el uso de STelnet.
- STelnet se implementa sobre la base de SSH y el número de puerto de destino es 22 por defecto. Las negociaciones entre un cliente STelnet y un servidor STelnet incluyen las siguientes etapas:
 - Negociación de versión
 - Negociación de algoritmo
 - Intercambio de claves
 - Autenticación de usuario
 - Interacción de sesión



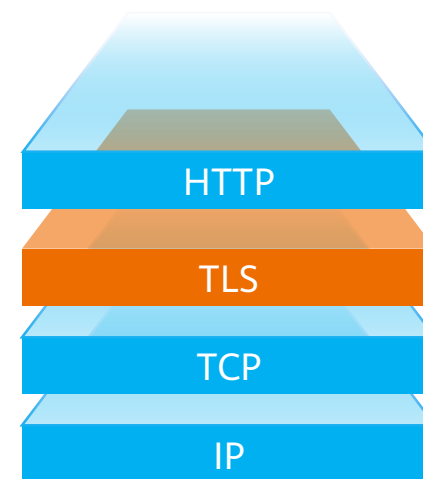
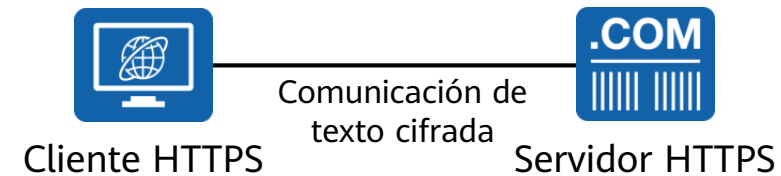
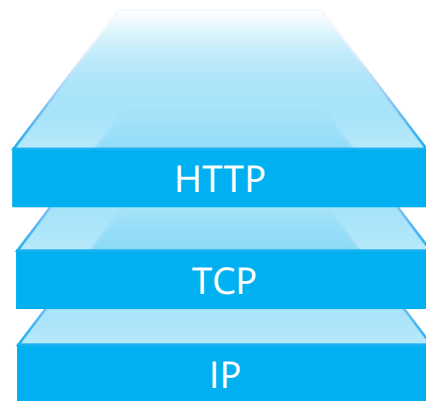
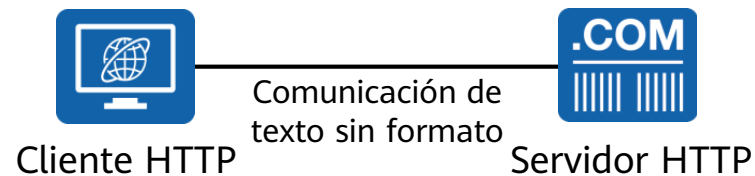
HTTP

- El protocolo de transferencia de hipertexto (HTTP) es uno de los protocolos de red más usados en Internet. HTTP se diseñó originalmente para proporcionar un método para publicar y recibir páginas (HTML) con lenguaje de marcas de hipertexto.



HTTPS

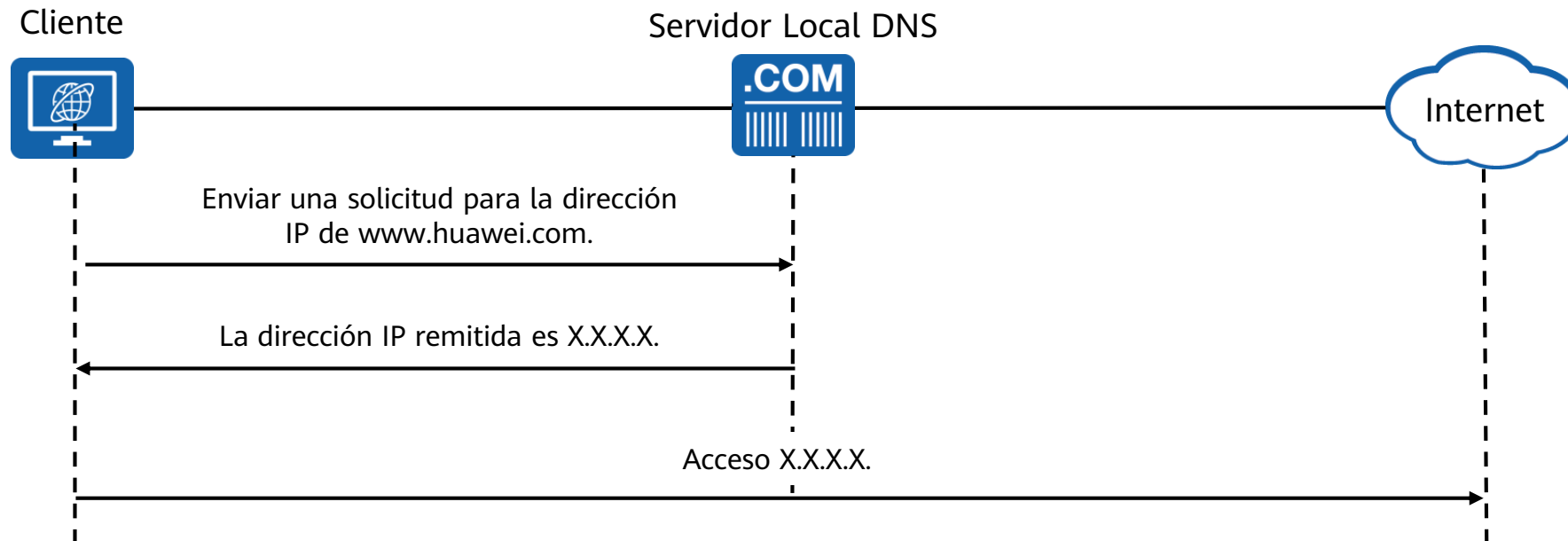
- Protocolo de transferencia de hipertexto (HTTPS): proporciona canales HTTP seguros.
- El protocolo de seguridad de la capa de transporte (TLS) se agrega a HTTPS basándose en HTTP para permitir la autenticación de identidad, la encriptación de datos y la verificación de integridad para la transmisión de datos. El número de puerto de destino de HTTPS es 443 y el número de puerto de destino de HTTP es 80 por defecto. Actualmente, la mayoría de los sitios web utiliza HTTPS para proporcionar una transmisión de datos segura.



- Autenticación de identidad
- Encriptación de datos
- Verificación de integridad

DNS

- Para visitar un sitio web, los usuarios deben ingresar la cadena de caracteres de la dirección del sitio web. Sin embargo, una computadora necesita conocer la dirección IP correspondiente al nombre de dominio del sitio web para poder acceder a él. En este caso, se requiere un sistema de nombres de dominio (DNS).
- El DNS se clasifica en resolución de nombres de dominio dinámica y estática. La resolución de nombres de dominio estática se usa primero para averiguar un nombre de un dominio. Si falla, se usa la resolución de nombres de dominio dinámica.



Índice

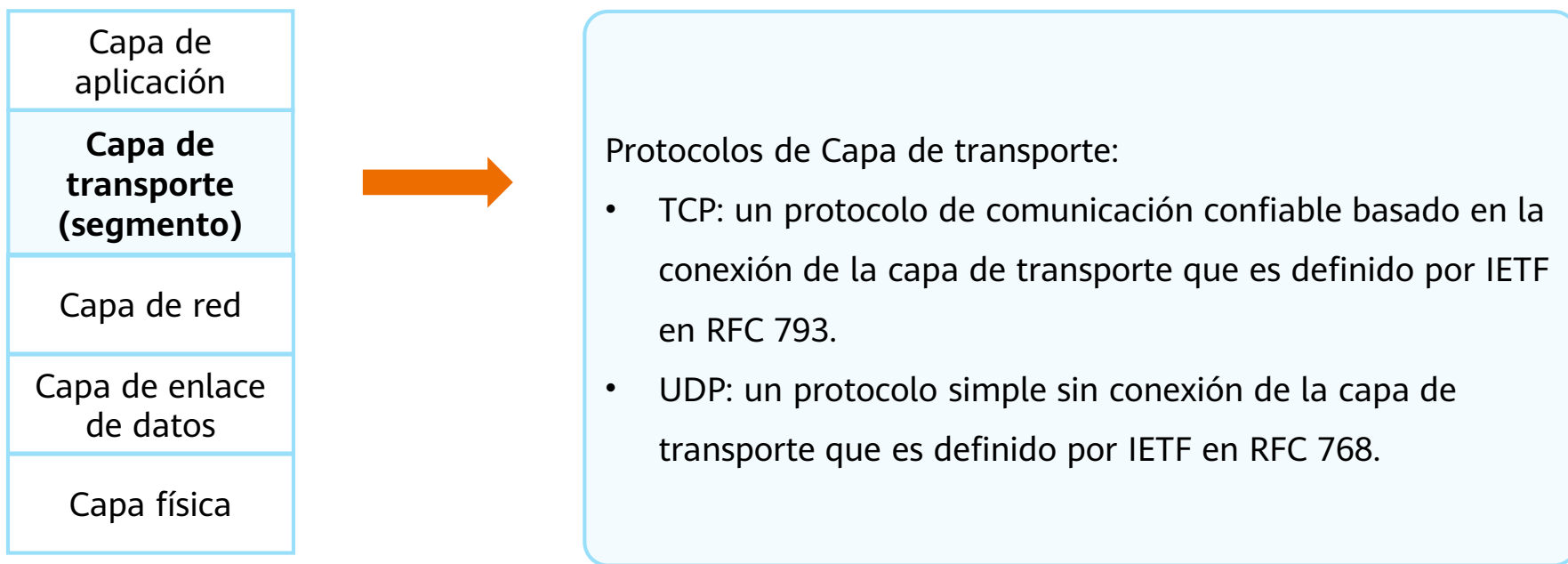
1. Modelo de referencia de red

- Modelo de referencia OSI y modelo de referencia TCP/IP
- Capa de aplicación
- Capa de transporte
- Capa de red
- Capa de enlace de datos

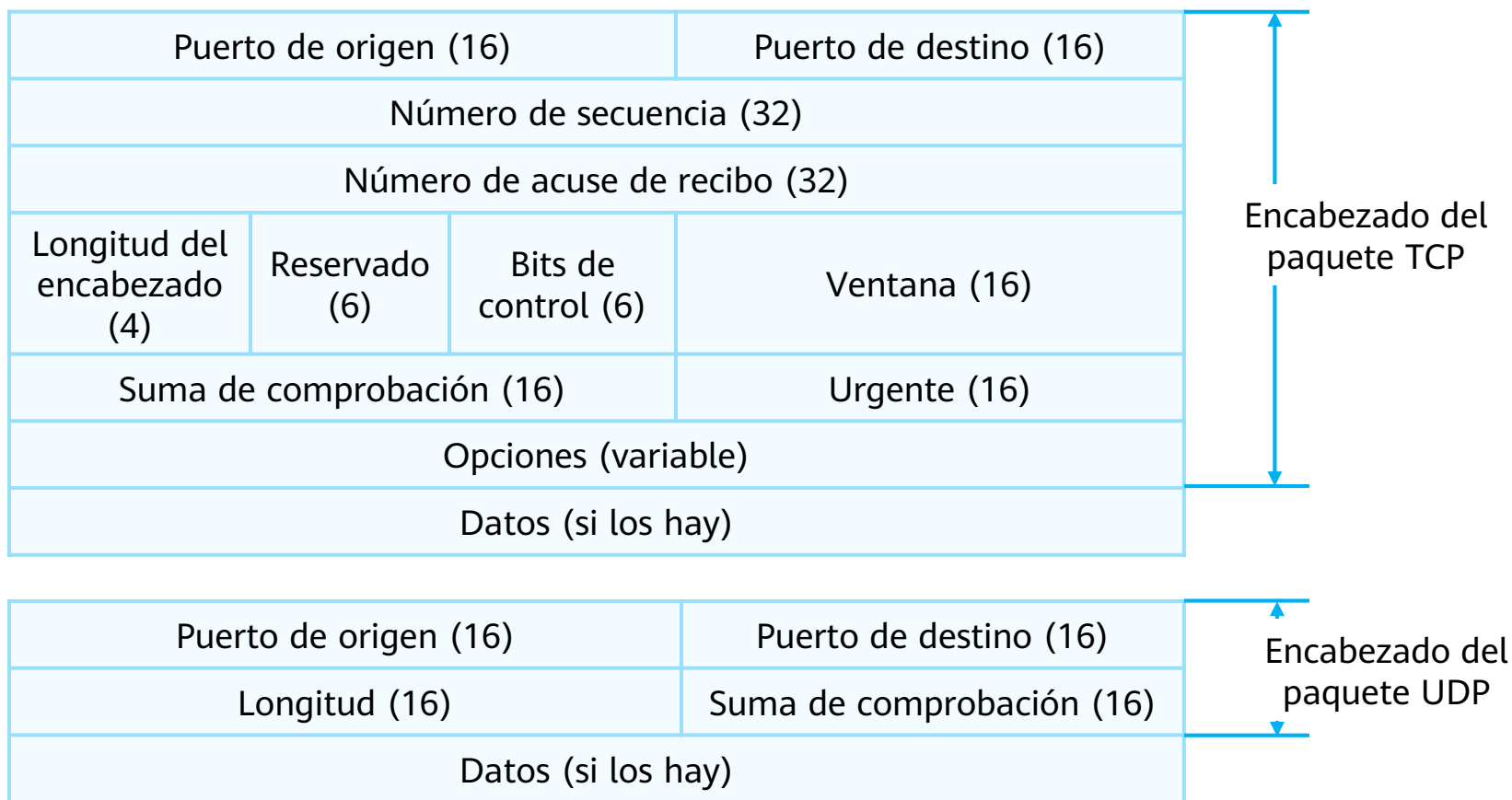
2. Dispositivos de red comunes

Capa de transporte

- Un protocolo de la capa de transporte recibe datos de un protocolo de la capa de aplicación, encapsula los datos con el correspondiente encabezado del protocolo de la capa de transporte y ayuda a establecer una conexión de extremo a extremo.

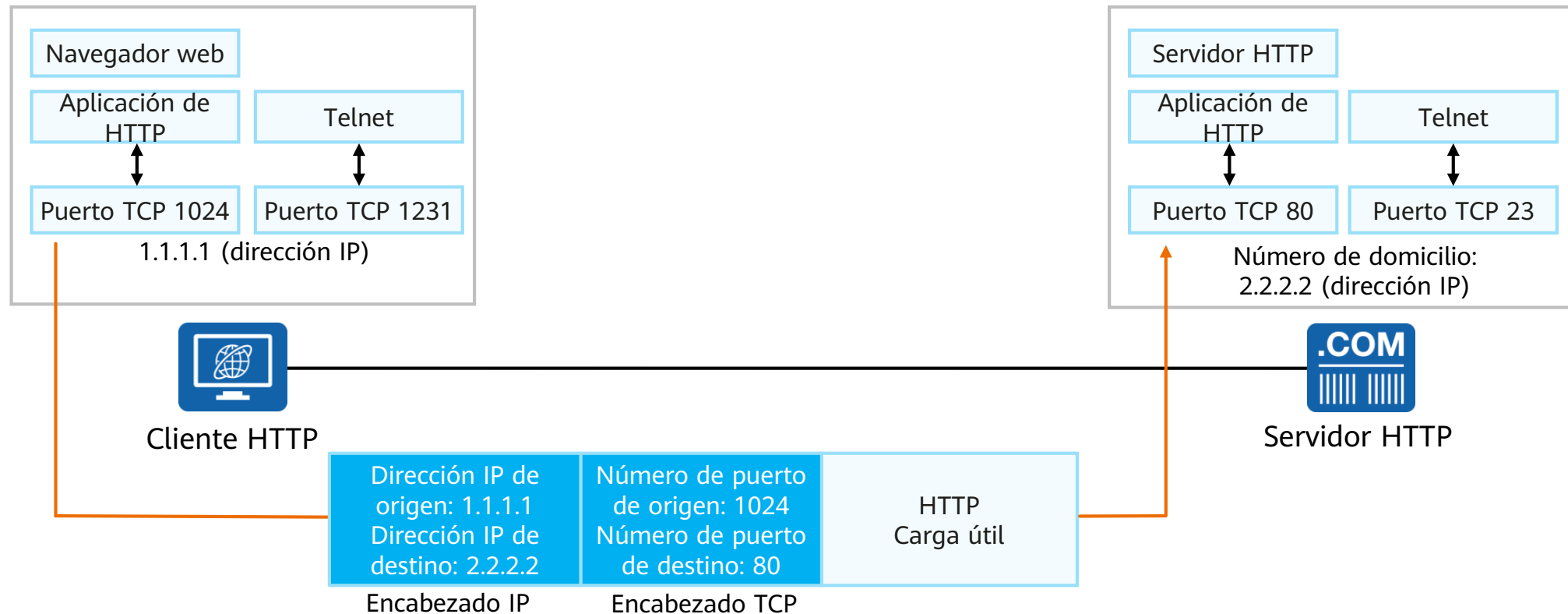


TCP y UDP: formatos de paquete



TCP y UDP: números de puerto

- TCP y UDP distinguen los diferentes servicios con el uso de diferentes números de puerto. Por lo general, el puerto de origen utilizado por un cliente se asigna aleatoriamente y al puerto de destino lo especifica la aplicación de un servidor. El número de puerto de origen es generalmente mayor que 1023 y no se encuentra en uso. El número de puerto de destino indica el número de puerto de escucha de la aplicación (servicio) habilitado en el servidor. Por ejemplo, el número de puerto HTTP por defecto es 80.



Índice

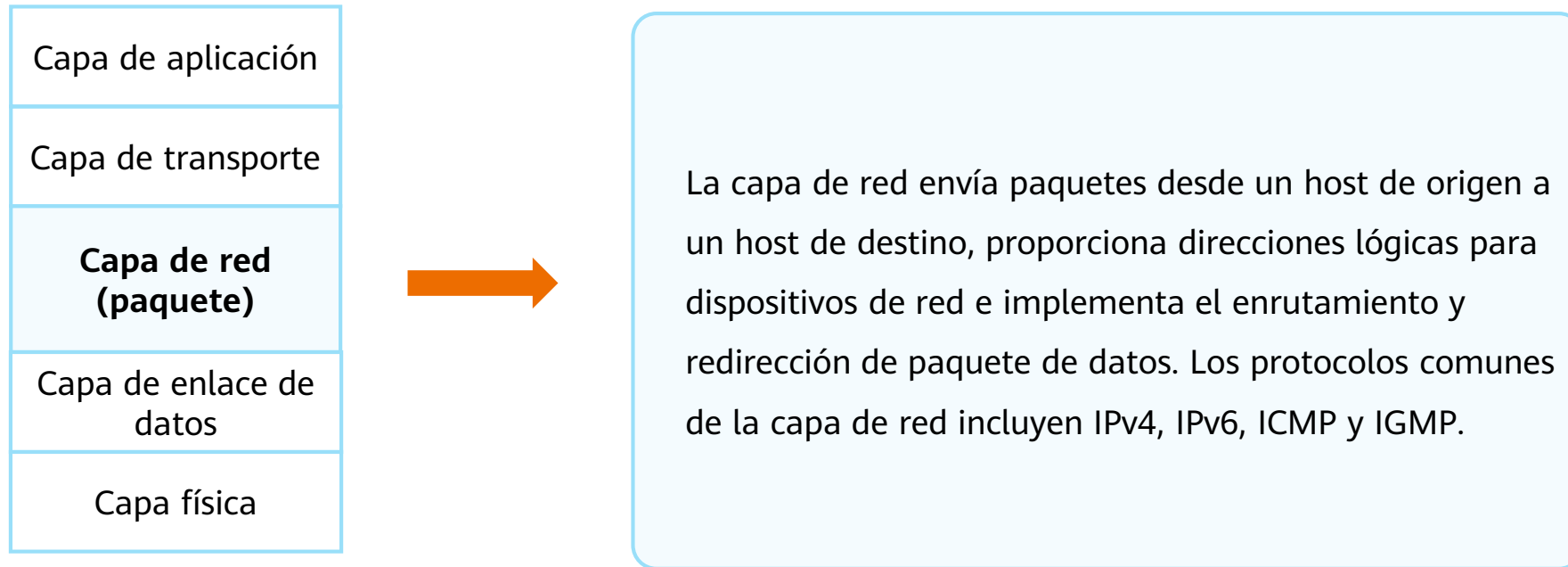
1. Modelo de referencia de red

- Modelo de referencia OSI y modelo de referencia TCP/IP
- Capa de aplicación
- Capa de transporte
- Capa de red
- Capa de enlace de datos

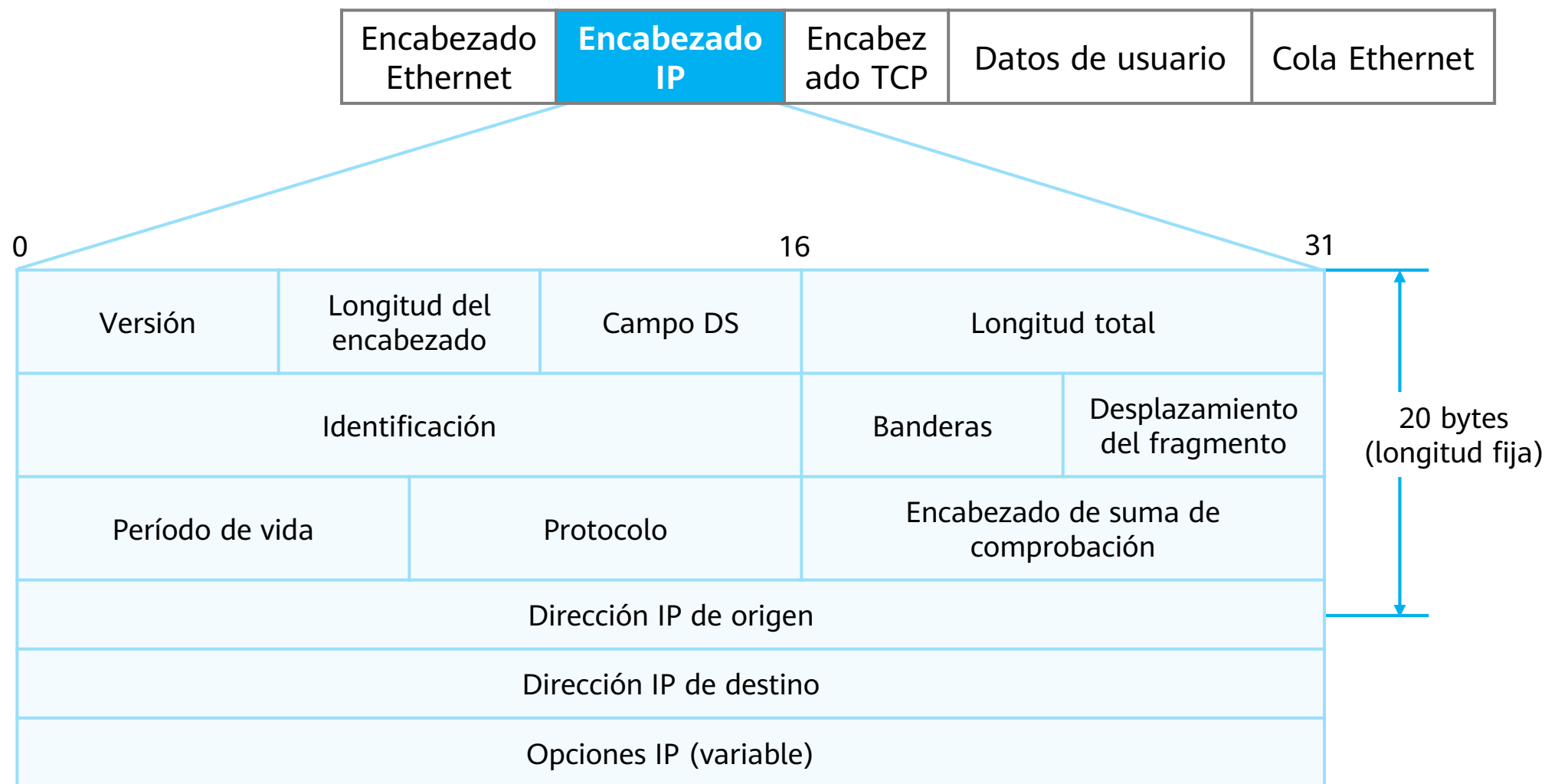
2. Dispositivos de red comunes

Capa de red

- La capa de transporte establece conexiones entre procesos en diferentes hosts y la capa de red transmite datos de un host a otro.

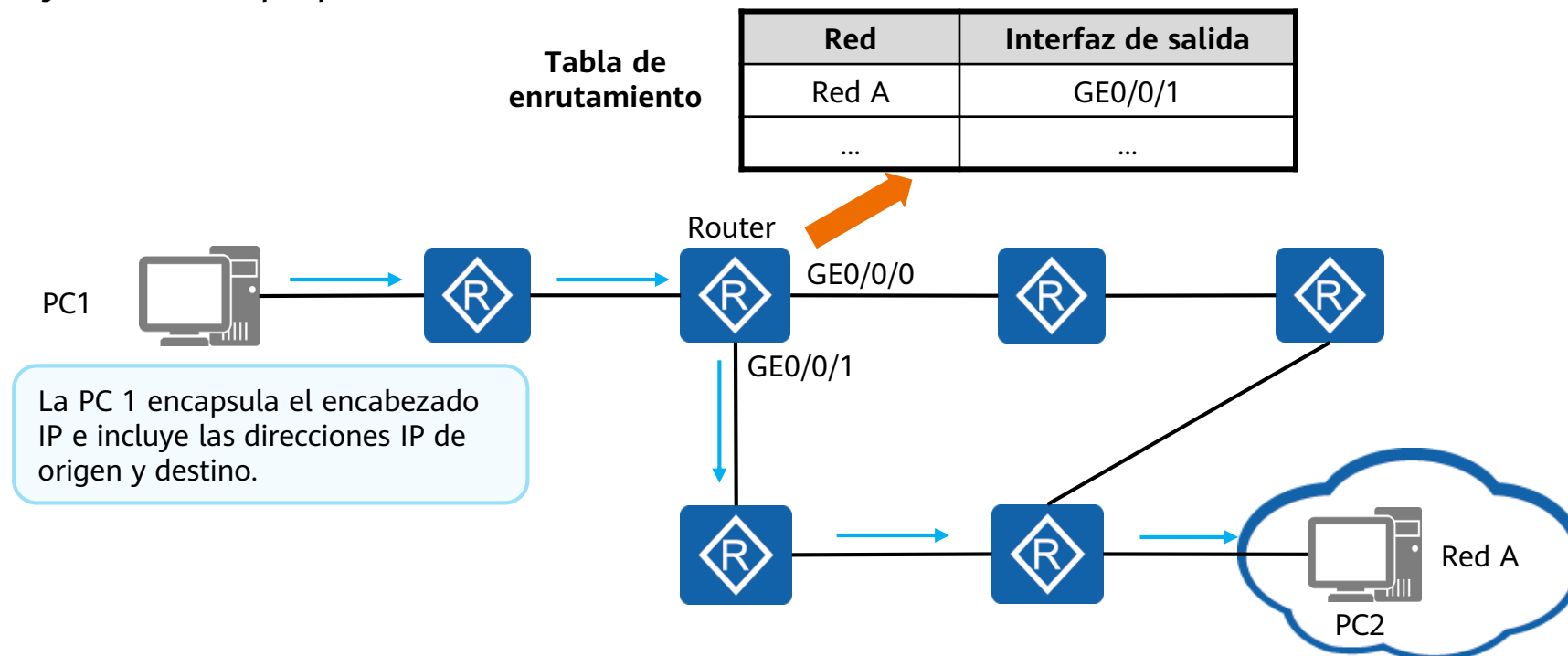


Encabezado del paquete IP



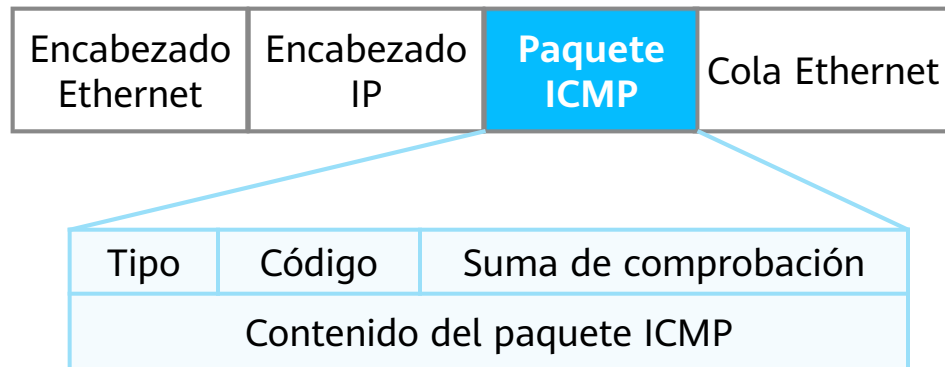
Redirección de paquete IP

- El encabezado de la capa de red de un paquete enviado por un dispositivo de origen lleva la dirección de la capa de red de los dispositivos de origen y de destino. Cada dispositivo de red (como un router) con funciones de enrutamiento cuenta con una tabla de enrutamiento. Luego de recibir un paquete, el dispositivo de red lee la dirección de destino de la capa de red del paquete, busca una coincidencia para la dirección en la tabla de enrutamiento y reenvía el paquete de acuerdo con las instrucciones de la coincidencia.



ICMP

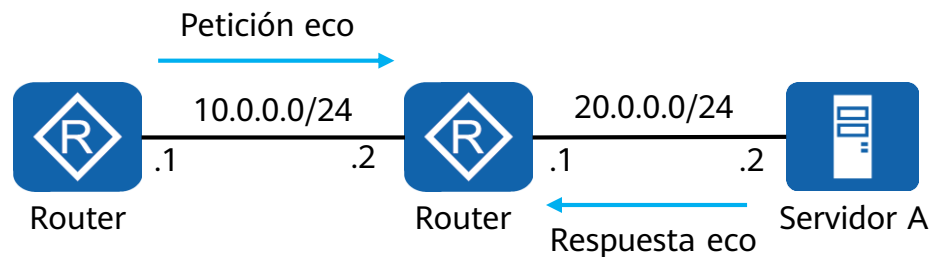
- El protocolo de mensajes de control de Internet (ICMP) es un protocolo IP auxiliar.
- El protocolo ICMP se usa para transmitir errores y controlar información entre dispositivos de red. Juega un papel importante en la obtención de información de red, así como de diagnóstico y rectificación de fallas de red.



Tipo	Código	Descripción
0	0	Respuesta eco
3	0	Red inalcanzable
3	1	Host inalcanzable
3	2	Protocolo inalcanzable
3	3	Puerto inalcanzable
5	0	Redirección
8	0	Petición eco

Comprobar errores de ICMP

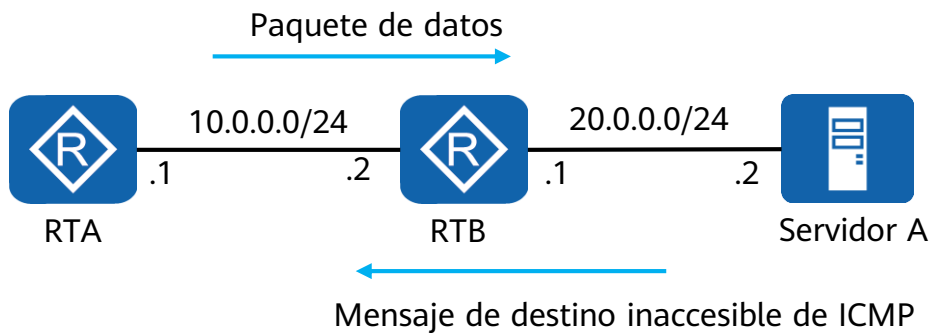
- El mensaje de petición eco ICMP y el mensaje de respuesta eco ICMP por lo general se utilizan para chequear la conectividad de la red entre las direcciones de origen y destino, y para proporcionar más información, tal como el retardo de ida y vuelta de paquetes.
- Una aplicación típica de ICMP es el comando ping. Ping es una herramienta común para chequear la conectividad de la red y para recopilar información relacionada. En el comando ping, los usuarios pueden asignar diferentes parámetros, tales como la longitud y el número de paquetes ICMP y el tiempo de espera para recibir una respuesta. Los dispositivos construyen y envían paquetes ICMP basados en parámetros para realizar pruebas de ping.



```
[RTA] ping 20.0.0.2
PING 20.0.0.2: 56 data bytes, press CTRL_C to break
Reply from 20.0.0.2: bytes=56 Sequence=1 ttl=254 time=70 ms
Reply from 20.0.0.2: bytes=56 Sequence=2 ttl=254 time=30 ms
Reply from 20.0.0.2: bytes=56 Sequence=3 ttl=254 time=30 ms
Reply from 20.0.0.2: bytes=56 Sequence=4 ttl=254 time=40 ms
Reply from 20.0.0.2: bytes=56 Sequence=5 ttl=254 time=30 ms
--- 20.0.0.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 30/40/70 ms
```

Informe de errores del protocolo ICMP

- El protocolo ICMP clasifica los diferentes mensajes de error para diagnosticar las fallas de conectividad de la red. Basado en los mensajes de error, el dispositivo de origen puede determinar la causa en la falla de transmisión de datos. Por ejemplo, cuando un dispositivo de red no puede acceder a una red de destino, automáticamente envía un mensaje de destino inaccesible ICMP al dispositivo de transmisión.
- Tracert rastrea la ruta de redirección del paquete salto a salto basándose en el valor del período de vida (TTL) del encabezado del paquete. Tiene un método efectivo para chequear la pérdida y demora del paquete y para ayudar a los administradores a encontrar bucles de enrutamiento en una red.



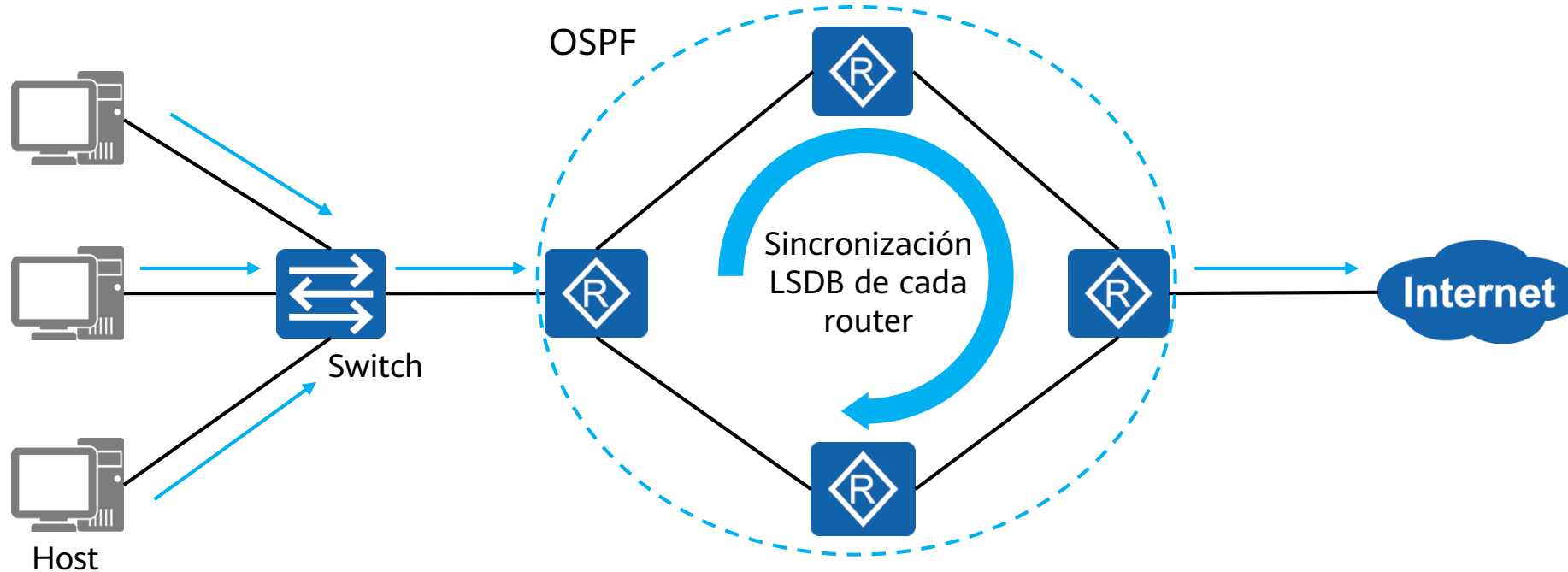
```
[RTA] tracert 20.0.0.2
```

```
tracert to 20.0.0.2(20.0.0.2), max hops: 30,packet length: 40,press  
CTRL_C to break
```

1	10.0.0.2	80 ms	10 ms	10 ms
2	20.0.0.2	30 ms	30 ms	20 ms

OSPF

- Las comunicaciones entre las diferentes redes se implementan a través de rutas. Hay tres tipos de rutas: directas, estáticas y dinámicas. Las rutas dinámicas han sido ampliamente utilizadas en redes para una mayor flexibilidad, confiabilidad y adaptabilidad.
- OSPF es el protocolo de enrutamiento dinámico mayormente utilizado en las redes empresariales.



Área OSPF

- El ID de un área OSPF se usa para identificar un área OSPF.
- Se considera a un área OSPF como un grupo lógico de dispositivos.
- La conexión de redes de área única o múltiple puede ser utilizada en empresas que se basan en escalas y requisitos.

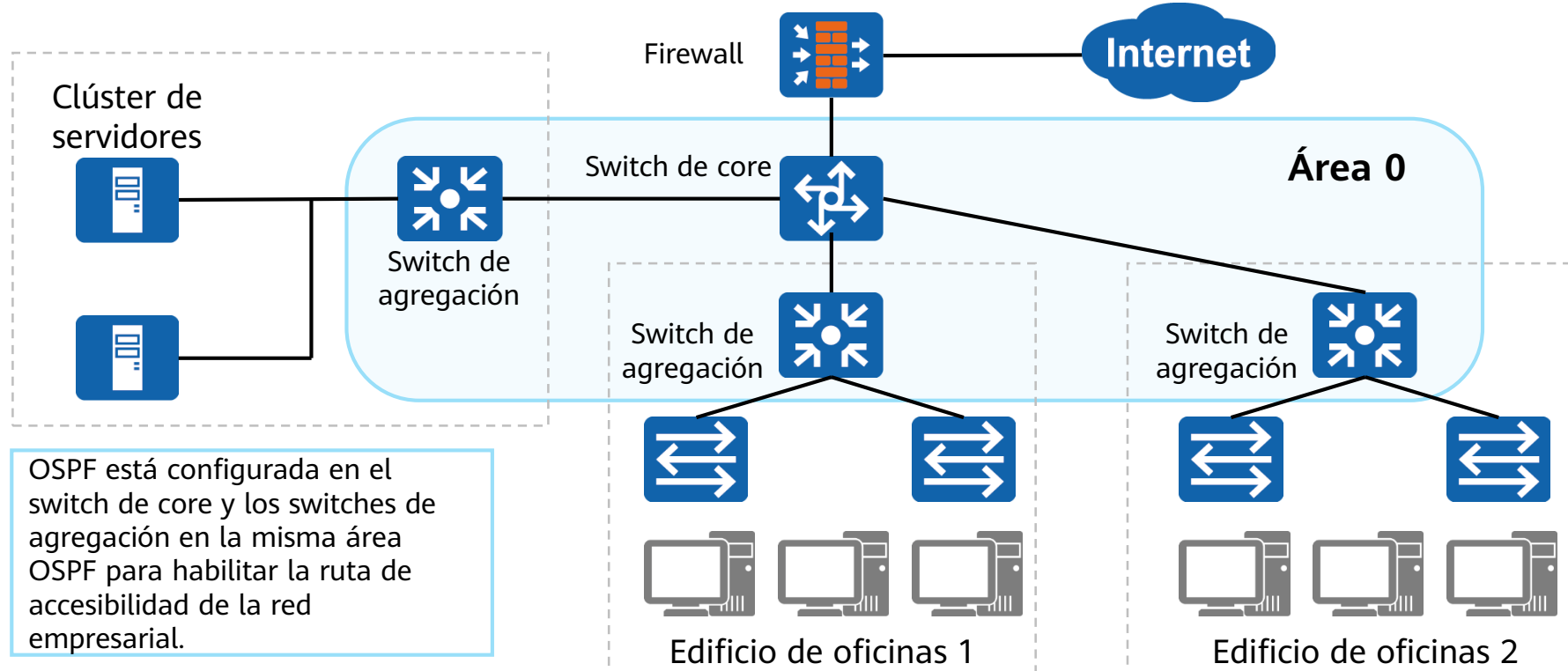


Tabla de enrutamiento OSPF

- Lo que debe saber sobre las tablas de enrutamiento OSPF:
 - Una tabla de enrutamiento OSPF contiene la información utilizada para guiar la retransmisión de paquetes, incluyendo la dirección de destino, costo y el siguiente salto.
 - Puede ejecutar el comando **display ospf routing** para verificar la información sobre la tabla de enrutamiento OSPF.

[R1]display ospf routing



ID del router: 1.1.1.1

ID del router: 2.2.2.2



GE1/0/0

Router 1 10.1.1.1/30

GE1/0/0

10.1.1.2/30



Router 2

```
<R1> display ospf routing
OSPF Process 1 with Router ID 1.1.1.1
Routing Tables
Routing for Network
Destination      Cost  Type   NextHop   AdvRouter   Area
1.1.1.1/32       0    stub   1.1.1.1    1.1.1.1     0.0.0.0
10.1.1.0/20      1    Transit 10.1.1.1    1.1.1.1     0.0.0.0
2.2.2.2/32       1    stub   10.1.1.2    2.2.2.2     0.0.0.0

Total Nets: 3
Intra Area: 3  Inter Area: 0  ASE: 0  NSSA: 0
```

Índice

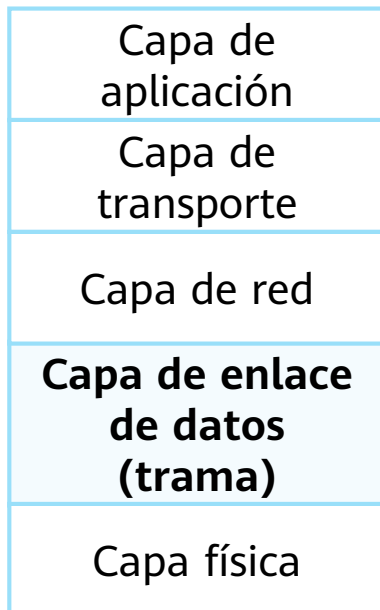
1. Modelo de referencia de red

- Modelo de referencia OSI y modelo de referencia TCP/IP
- Capa de aplicación
- Capa de transporte
- Capa de red
- Capa de enlace de datos

2. Dispositivos de red comunes

Capa de enlace de datos

- La capa de enlace de datos se localiza entre la capa de red y la capa física y provee servicios para protocolos como IP e IPv6 en la capa de red.
- Ethernet es el protocolo de la capa de enlace de datos más común.

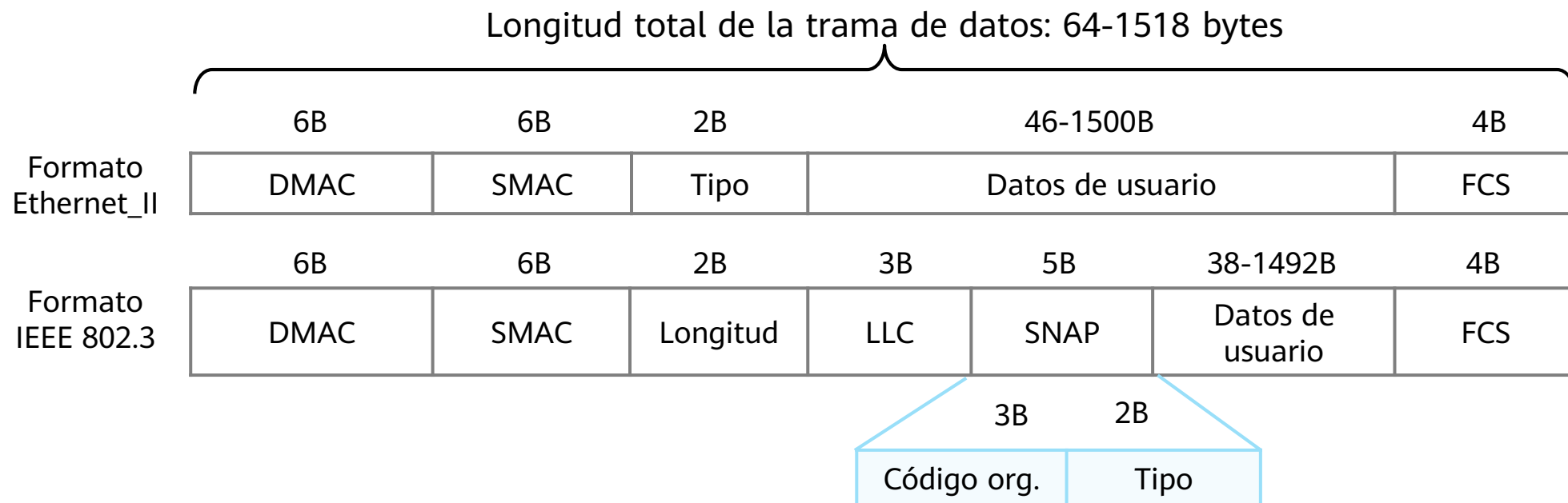


La capa de enlace de datos está localizada entre la capa de red y la capa física.

- La capa de enlace de datos proporciona comunicación intrasegmento para la capa de red.
- Las funciones de la capa de enlace de datos incluyen entramado, dirección física y control de errores.
- Los protocolos comunes de capa de enlace de datos incluyen Ethernet, PPPoE y PPP.

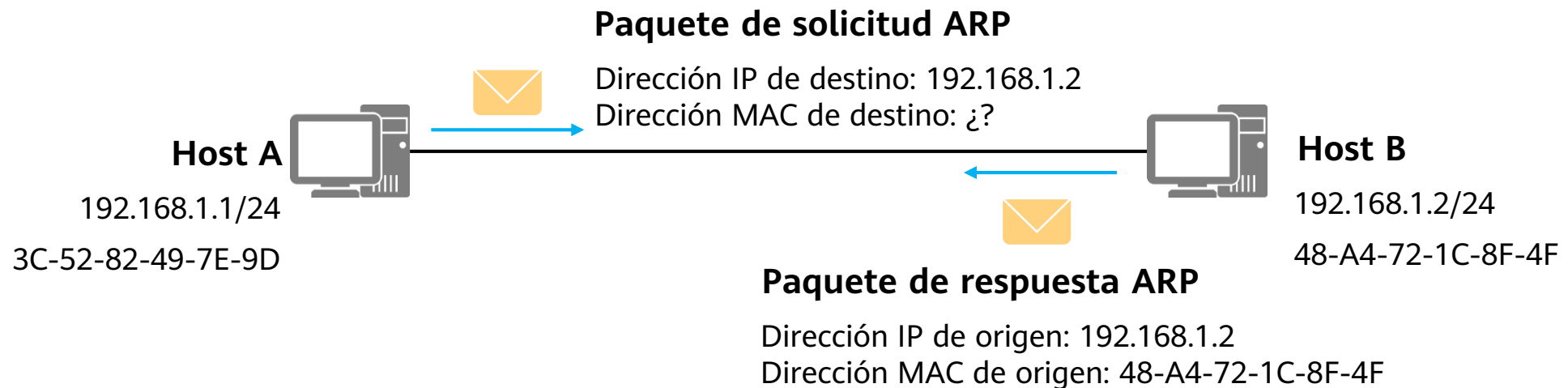
Estructura de trama Ethernet

- Las tramas utilizadas por la tecnología Ethernet son conocidas como tramas Ethernet. Las tramas Ethernet tienen dos formatos, específicamente Ethernet II e IEEE 802.3.
- Una dirección de control de acceso a medios (MAC) identifica exclusivamente una tarjeta de interfaz de red (NIC). Las direcciones MAC son utilizadas para la comunicación intrasegmento, con 48 bits de longitud, tales como 00-1E-10-DD-DD-02.

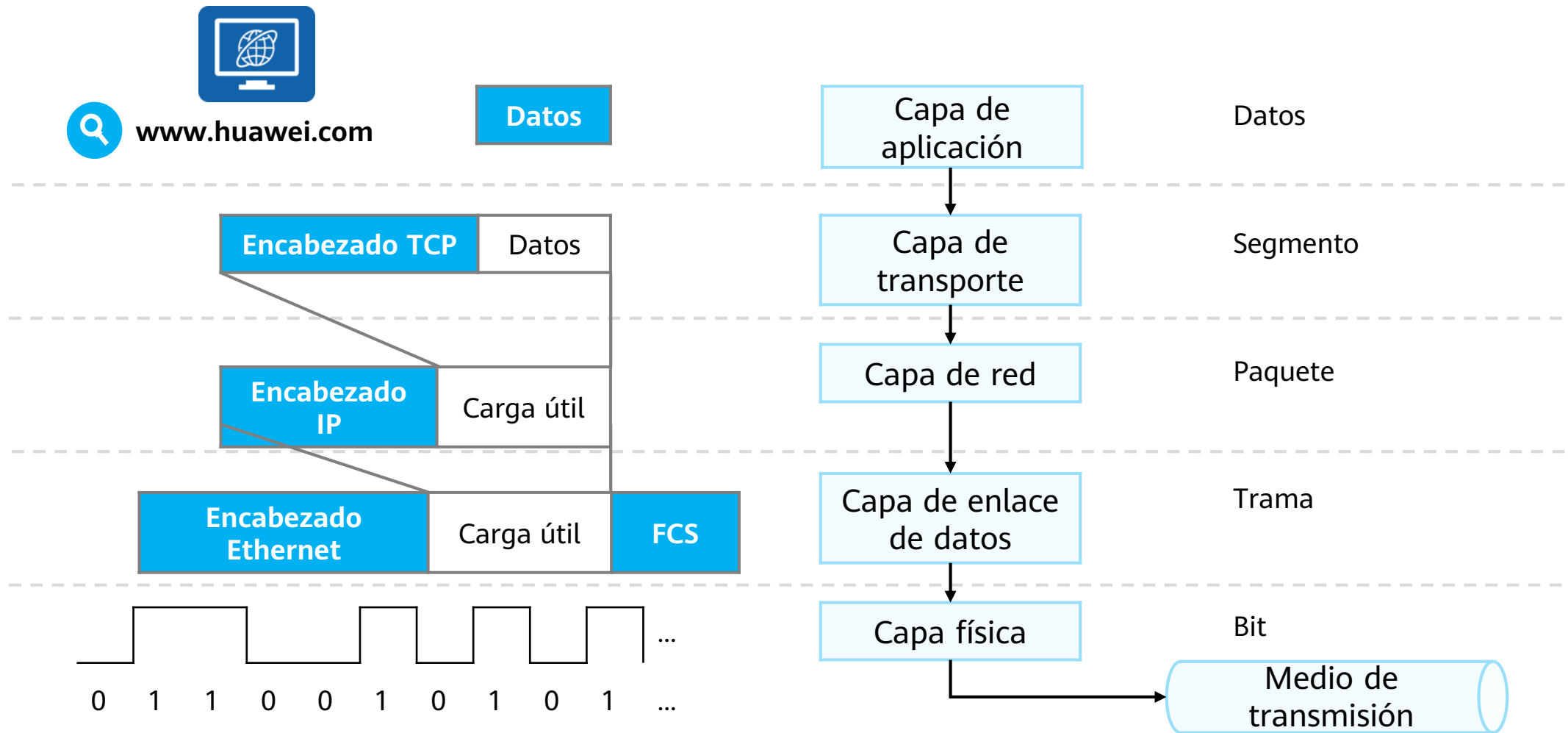


ARP

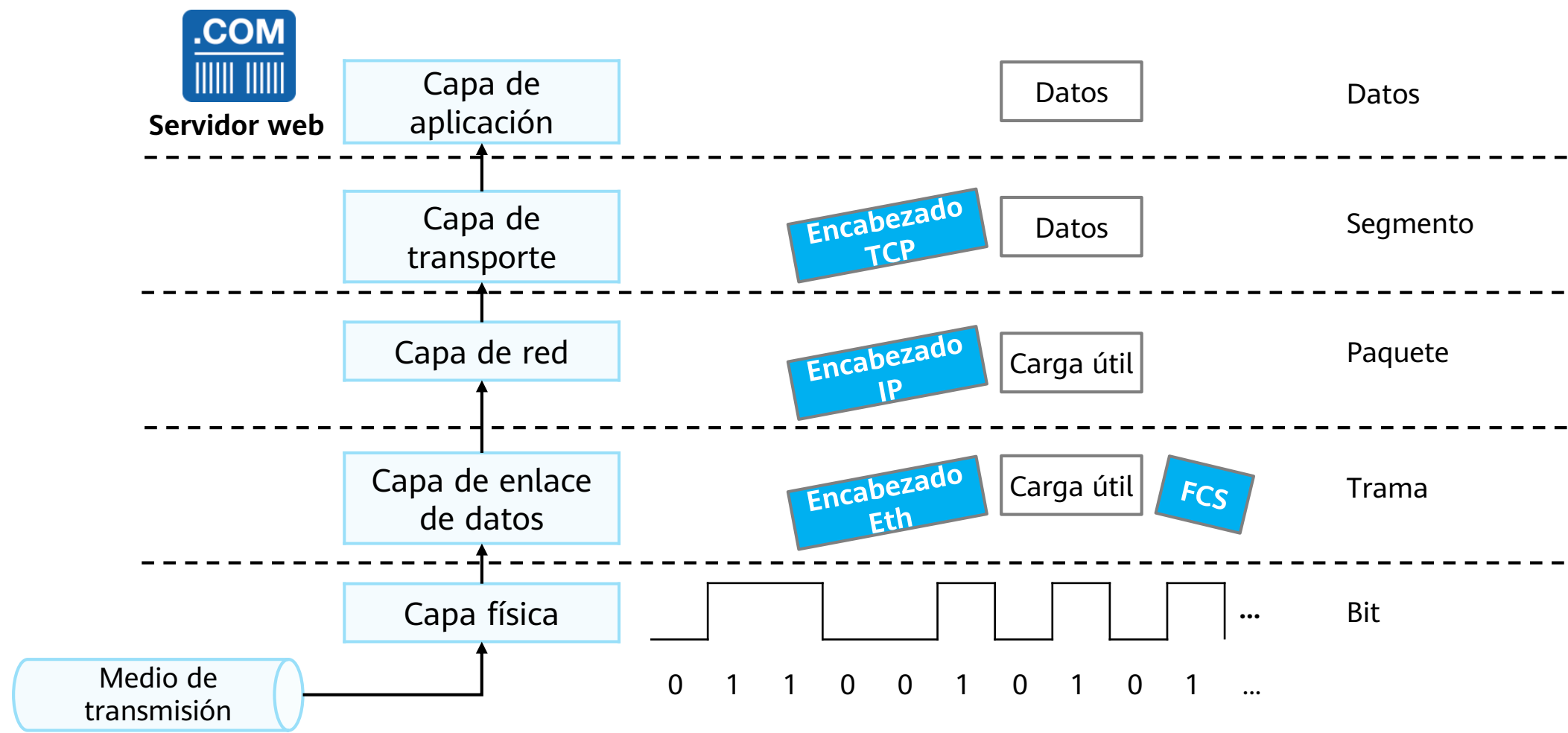
- Para habilitar el reenvío normal del paquete, debe obtenerse la dirección de destino o la dirección MAC de la gateway. Como tal, el protocolo de resolución de direcciones (ARP) se utiliza para obtener la dirección MAC correspondiente con base en la dirección IP conocida.



Encapsulación de datos de un remitente



Desencapsulación de datos de un receptor

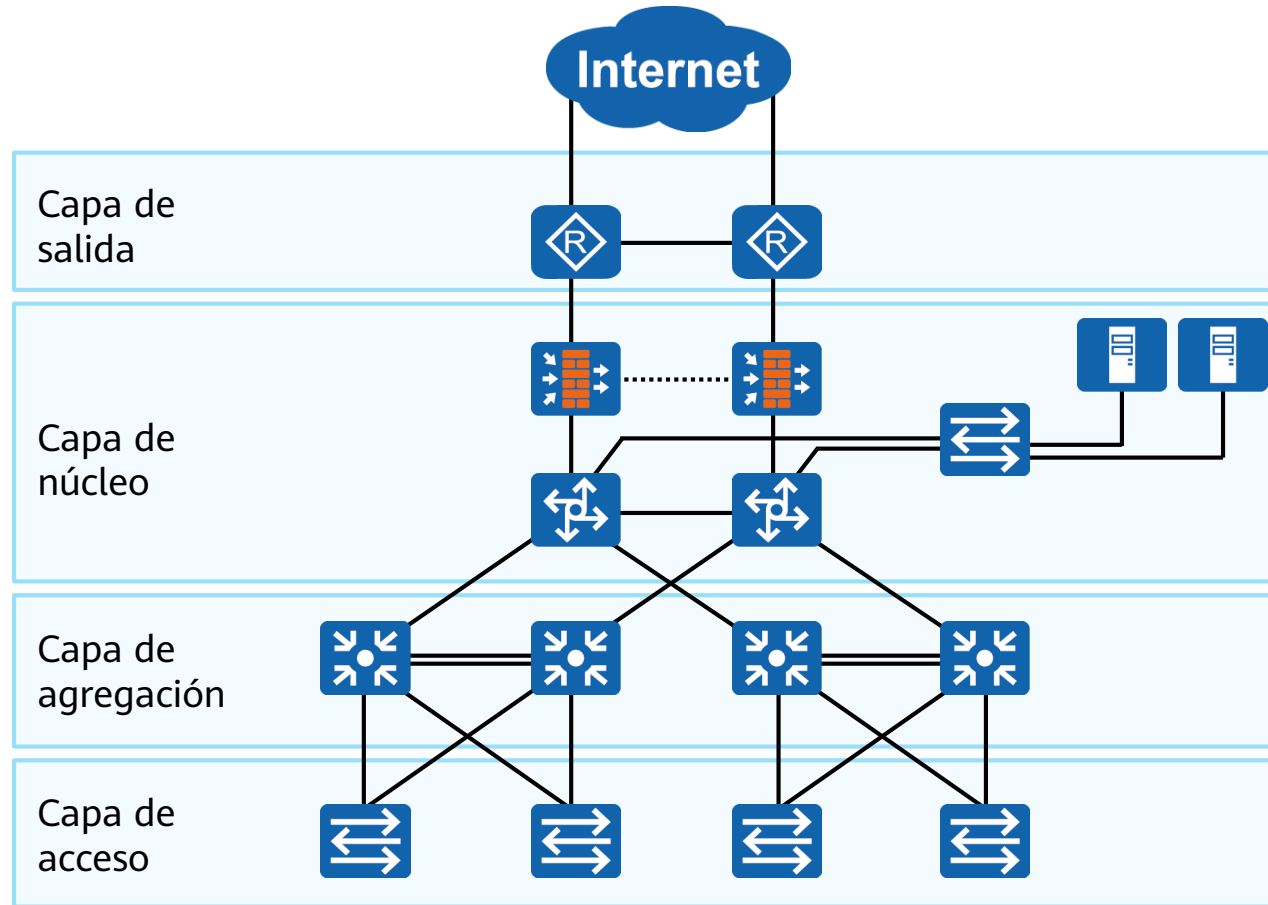


Índice

1. Modelo de referencia de red
- 2. Dispositivos de red comunes**

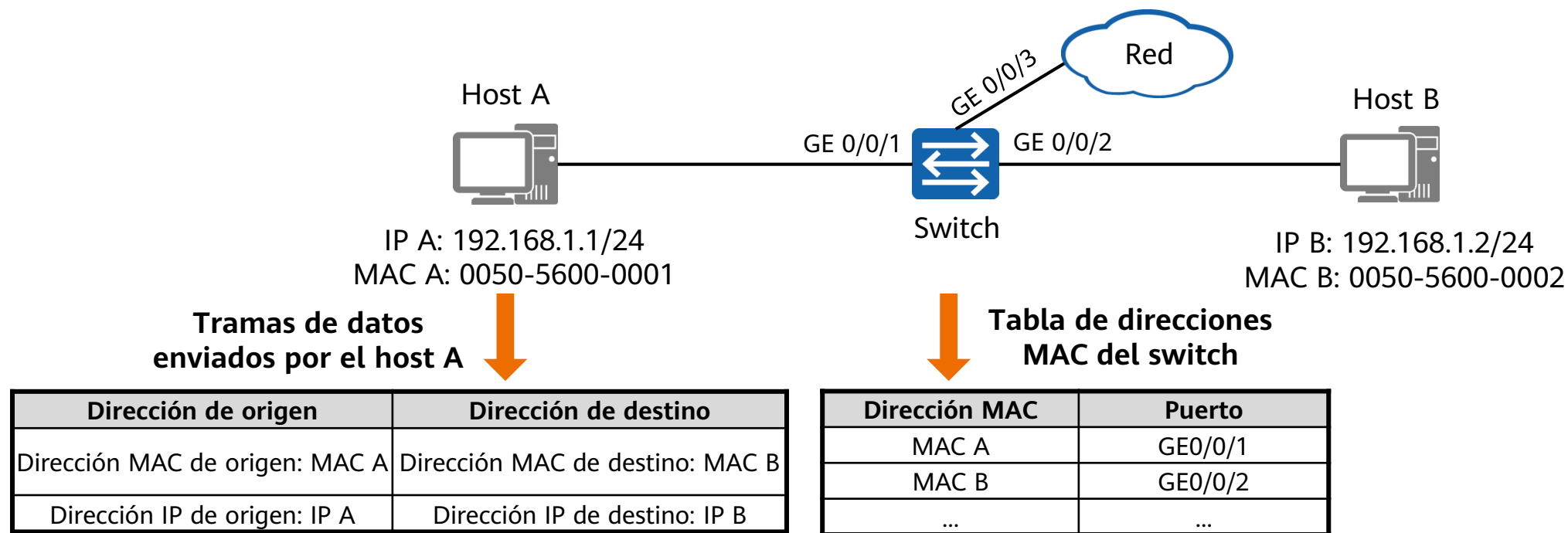
Arquitectura de la red de campus empresarial típica

- Una red de campus empresarial típica consta de switches, routers, firewalls y servidores.



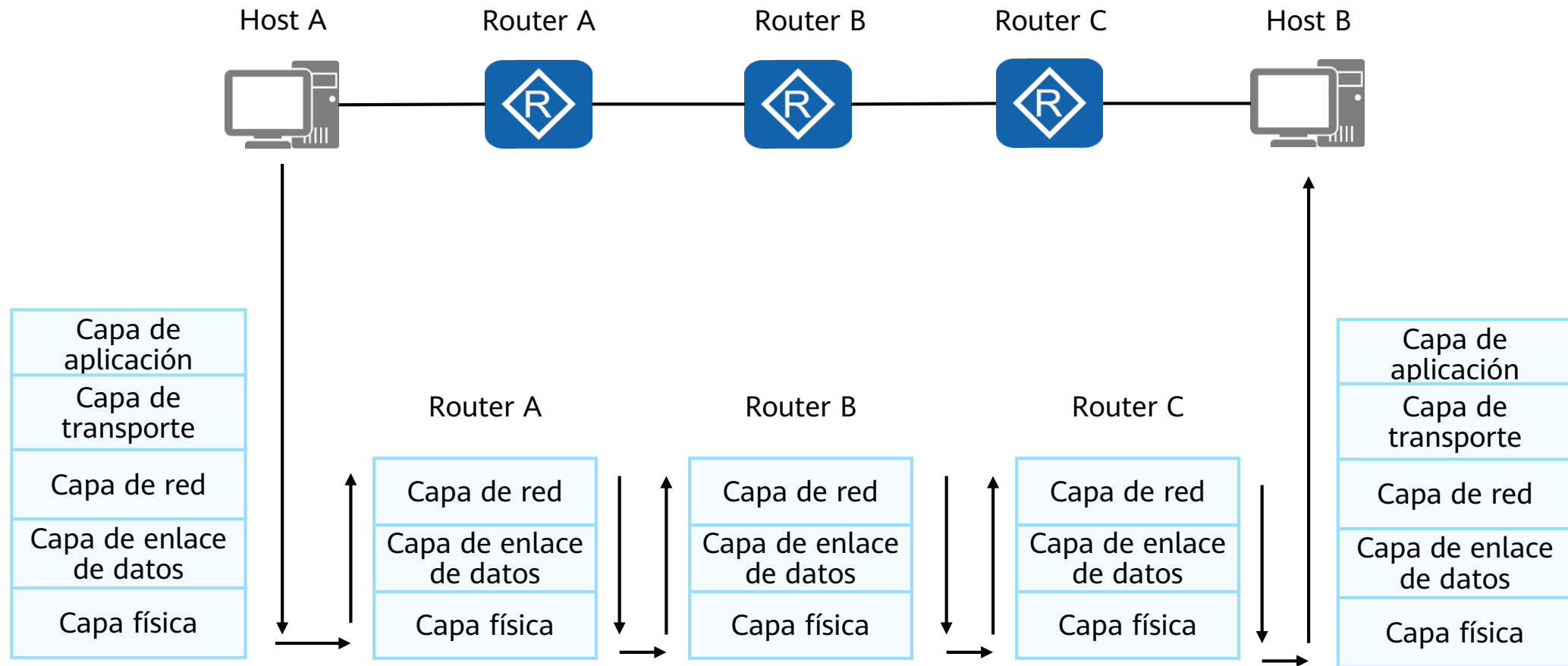
Switch

- Un switch es el dispositivo más próximo al usuario final y se usa para conectar terminales a la red y habilitar el reenvío de tramas de datos en el mismo segmento de red.
- Los switches funcionan en la capa de enlace de datos y reenvían tramas de datos basándose en tablas de dirección MAC que almacenan el mapeo entre las direcciones MAC y los puertos del switch.



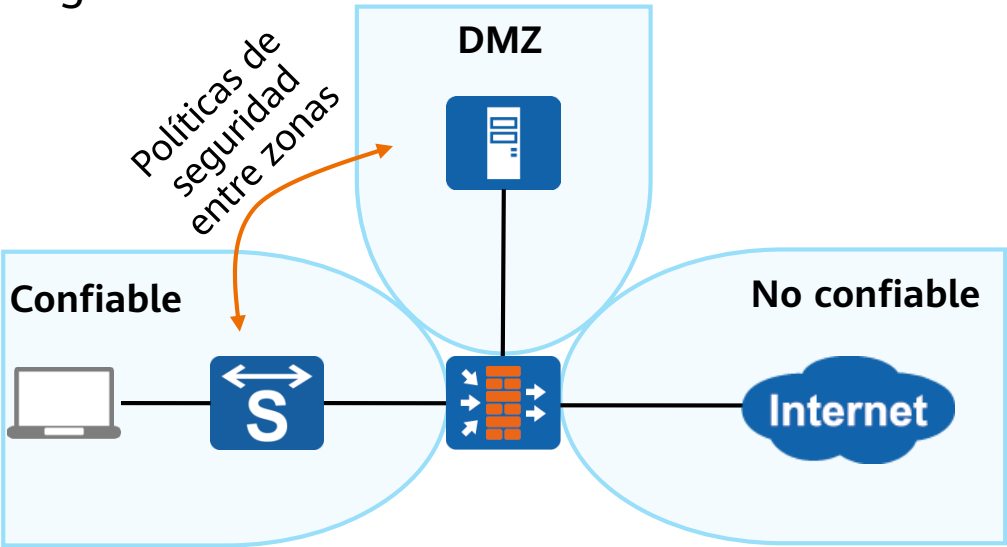
Router

- Los routers funcionan en la capa de red para garantizar que los paquetes puedan reenviarse entre las diferentes redes.



Firewall

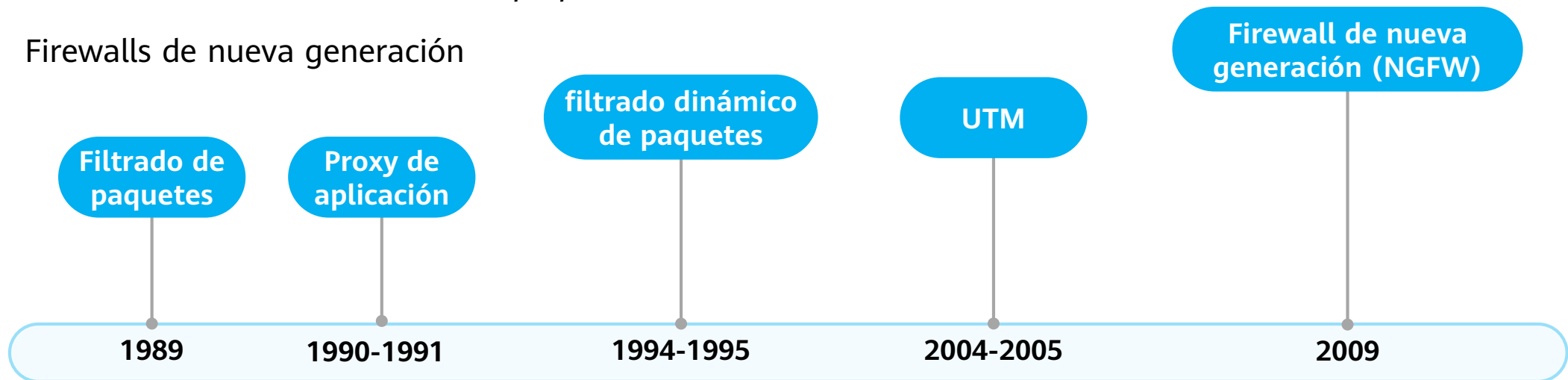
- Los firewalls se implementan mayoritariamente en las fronteras de la red para controlar los comportamientos de acceso a la red con protección de seguridad como característica principal.
- Los firewalls consideran que los flujos de datos en la misma zona de seguridad no presentan riesgos y no requieren política de seguridad. Las verificaciones de seguridad del dispositivo se desencadenan solamente cuando los datos circulan entre zonas de seguridad diferentes y se implementan políticas de seguridad.



Zona	Prioridad de seguridad predeterminada
Zona no confiable	5 (nivel de seguridad bajo)
DMZ	50 (nivel de seguridad medio)
Zona de confianza	85 (nivel de seguridad alto)
Zona local	100 (nivel de seguridad más alto). Una zona local define el dispositivo e incluye sus interfaces.

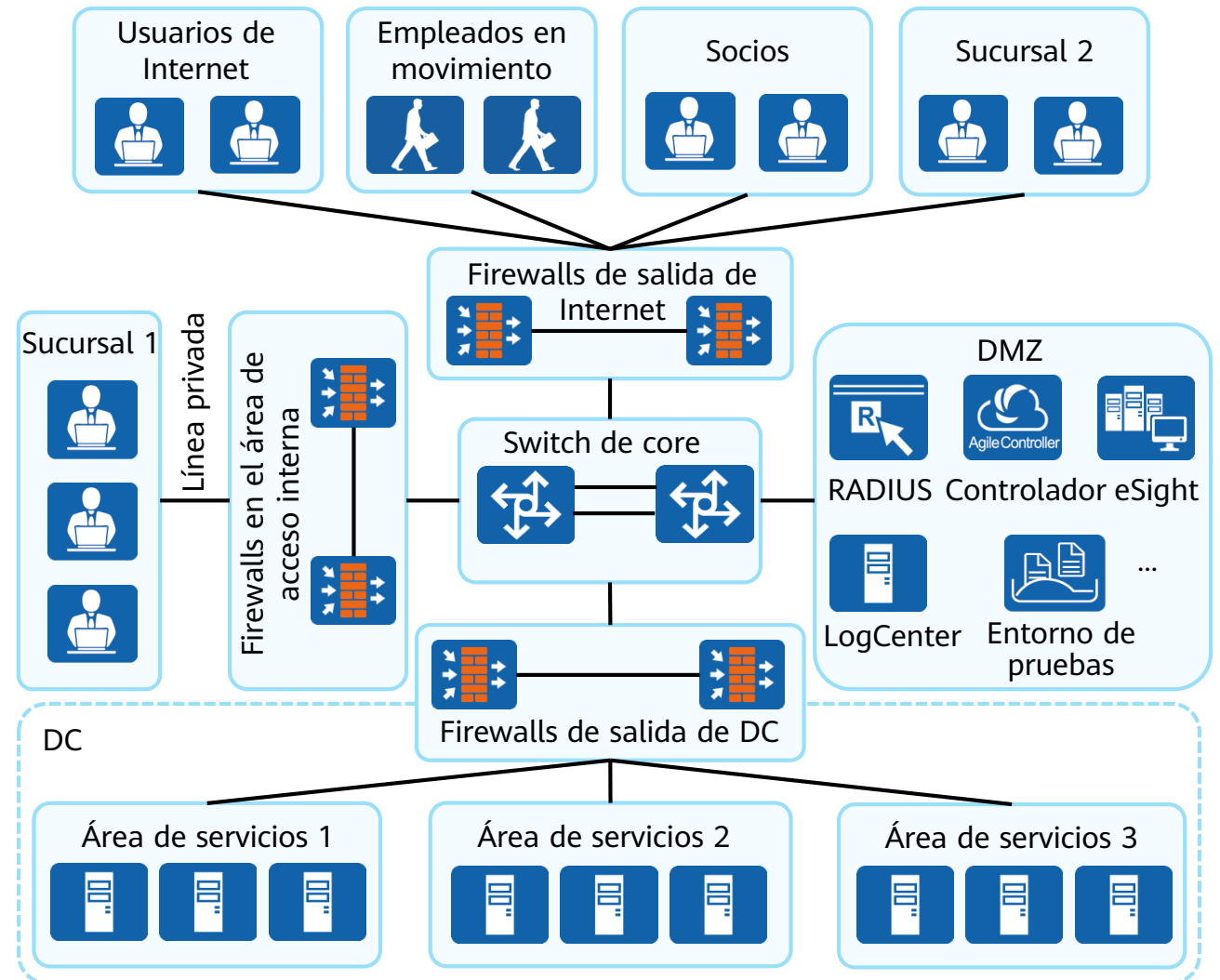
Historia del desarrollo de firewall

- Con el avance de las tecnologías, los firewalls han mejorado, desde un nivel bajo a un nivel alto, con funciones relacionadas que se desarrollan de una manera simple a compleja. El desarrollo de las tecnologías de red y la proliferación de demandas continúan promoviendo las mejoras de firewall.
- Basado en la historia de su desarrollo, los firewalls se pueden clasificar en los siguientes tipos:
 - Firewalls de filtrado de paquetes
 - Firewalls de filtrado dinámico de paquetes
 - Firewalls de nueva generación



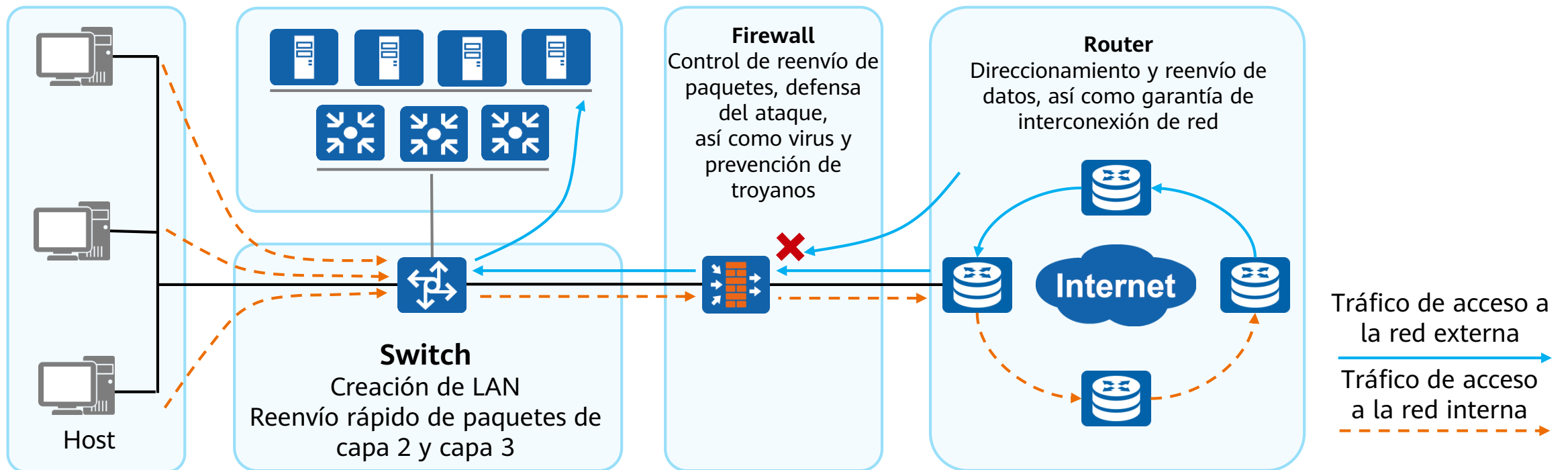
Funciones de firewall

- Los firewalls protegen a la red contra ataques e intrusiones de otra red. Con atributos de aislamiento y defensa, los firewalls se implementan en las subidas de red empresarial, fronteras de subred de redes de amplia escala y fronteras del centro de datos (DC).
- Las funciones del firewall se describen a continuación:
 - Aislar redes de diferentes niveles de seguridad
 - Implementar control de acceso (con el uso de políticas de seguridad) entre redes de diferentes niveles de seguridad
 - Implementar autenticación de identidad de usuario
 - Implementar acceso remoto
 - Implementar encriptación de datos y servicios VPN
 - Implementar traducción de direcciones de red
 - Implementar otras funciones de seguridad



Comparación entre firewalls, switches y routers

- Las principales funciones de los switches, routers y firewalls son diferentes, los switches crean LAN, los routers conectan diferentes redes y los firewalls se implementan en las fronteras de las redes.
- La función principal de los routers y switches es el reenvío de paquetes, mientras que la de los firewalls es el control de acceso a la red.



Inicio de sesión en el dispositivo de red y configuraciones

- Las configuraciones del dispositivo de red están involucradas en los procesos de implementación, operación y mantenimiento. Necesita iniciar sesión en un dispositivo antes de configurarlo.
- Los administradores pueden configurar dispositivos de red en la interfaz de usuario de la web o a través del CLI.

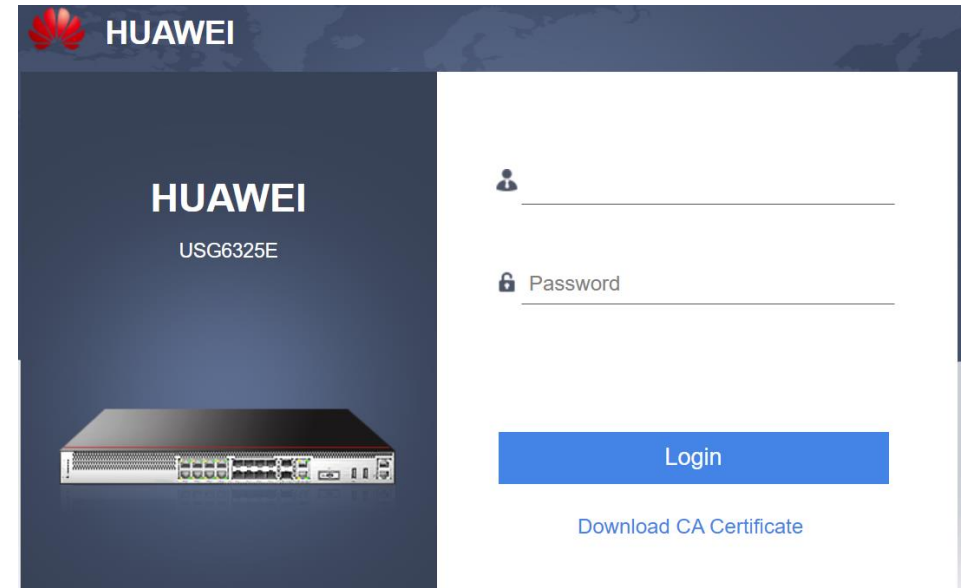
Inicio de sesión en la consola

```
Username: admin
Password: Admin@123
Info: The max number of VTY users is 21, the number of
current VTY users online is 0, and total number of terminal
users online is 1.
<FW> display this
#
sysname FW
#
command-privilege level 0 view system interface
#
Return
```

Inicio de sesión Telnet

Inicio de sesión SSH

Inicio de sesión web



Comandos de configuración básicos (1/2)

- Configurar una dirección IP de interfaz.

```
[FW] interface GigabitEthernet 0/0/1  
[FW-GigabitEthernet0/0/1] ip address 10.102.0.1 255.255.255.0
```

Este comando se usa para configurar una dirección IP para una interfaz física o lógica en un dispositivo.

- Ver las configuraciones actuales.

```
<FW> display current-configuration
```

- Guardar un archivo de configuración.

```
<FW> save
```

- Visualizar datos de configuración guardados.

```
<FW> display saved-configuration
```

Comandos de configuración básicos (2/2)

- Borrar datos de configuración guardados.

```
<FW> reset saved-configuration
```

- Ver los parámetros de configuración de puesta en marcha del sistema.

```
<FW> display startup
```

Este comando se utiliza para visualizar software de sistema relacionado, software de sistema de respaldo, archivos de configuración, archivos de la ruta y archivos de voz para la puesta en marcha actual y la siguiente.

- Configurar el archivo de configuración para la próxima puesta en marcha.

```
<FW> startup saved-configuration configuration-file
```

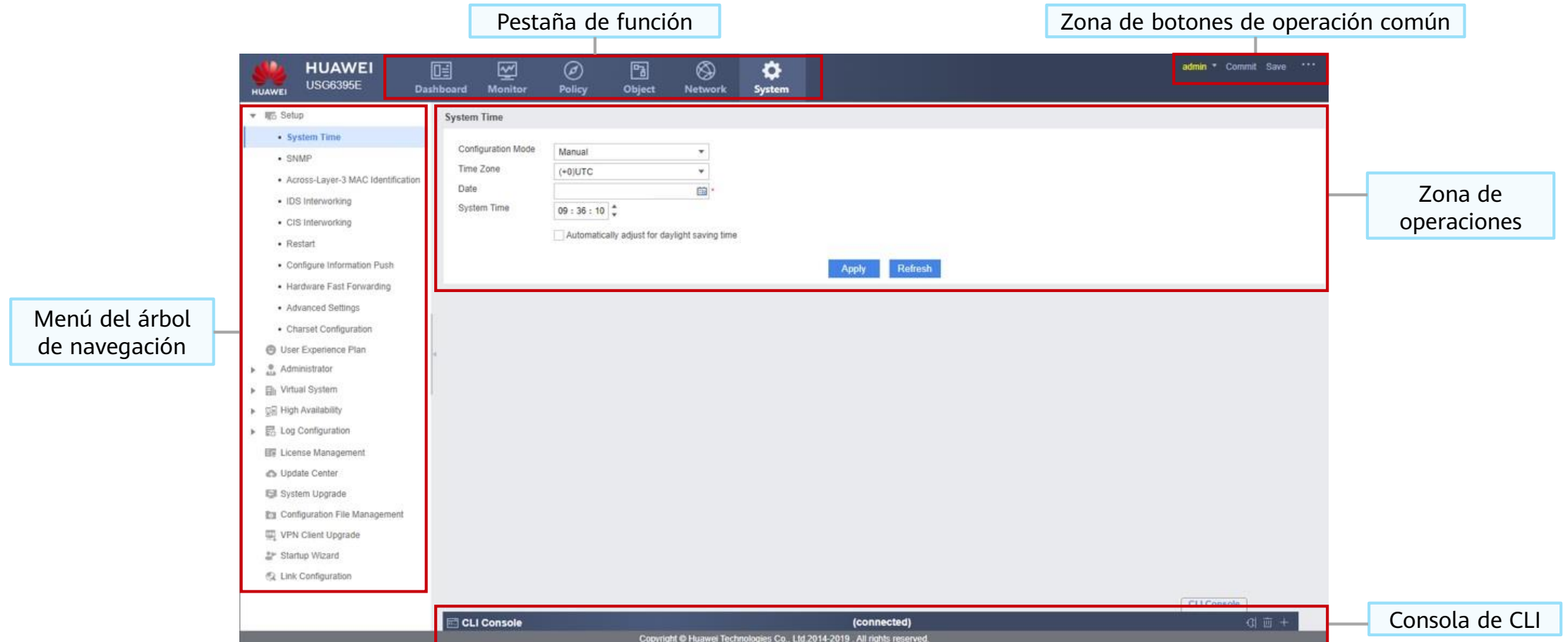
El dispositivo carga un archivo de configuración específico para la próxima puesta en marcha durante una actualización al ejecutar este comando.

- Reiniciar el dispositivo.

```
<FW> reboot
```


GUI (1/2)

- Las GUI de firewall incluyen la pestaña de función, el menú del árbol de navegación, la zona de operaciones, el área de botones de operación común y la consola de CLI.



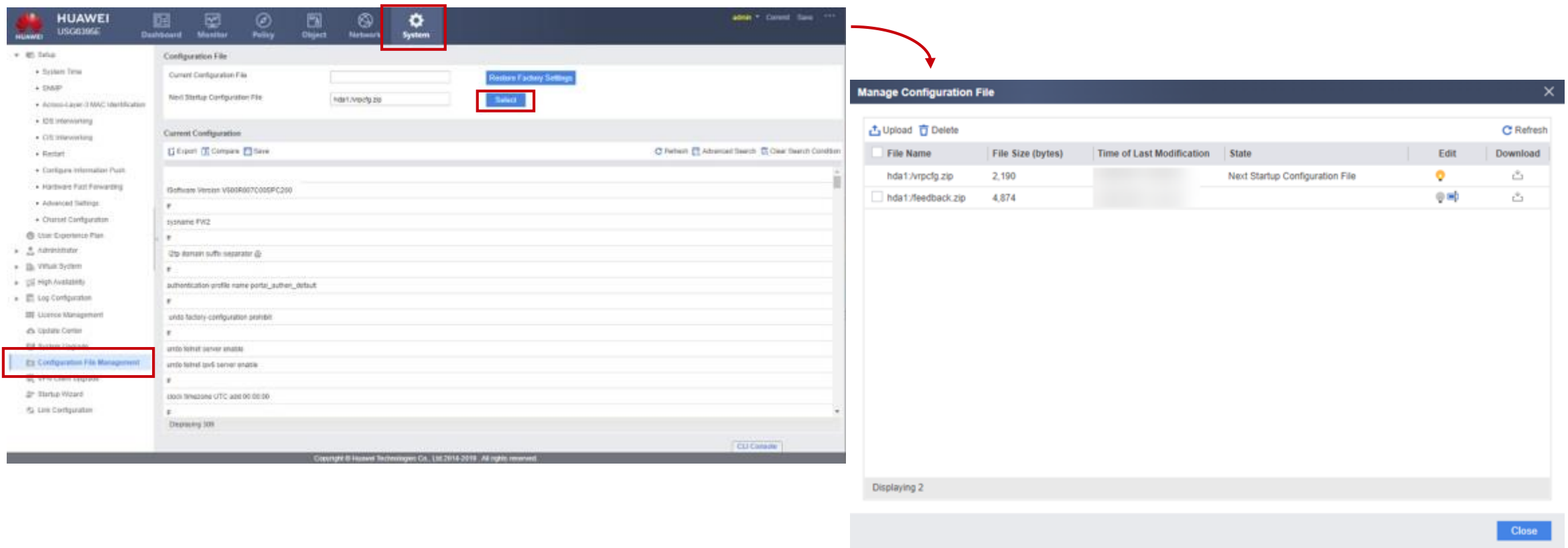
GUI (2/2)

- La pestaña de función en la GUI muestra funciones del firewall basadas en tipos y es generalmente usada durante las configuraciones de firewall en la interfaz de usuario de la web.

Pestaña de función	Descripción
Dashboard	Le permite ver el estado del dispositivo de manera rápida y monitorear el estado del sistema en ejecución.
Monitor	Proporciona métodos O&M completos y le permite ver registros y estadísticas, así como diagnosticar las fallas del dispositivo.
Policy	Le permite configurar políticas de servicio, tales como políticas de seguridad y políticas del ancho de banda para controlar el tráfico de retransmisión y defender contra las amenazas de red.
Objeto	Le permite configurar elementos comunes, tales como direcciones y servicios a los que se refieren las diferentes políticas de servicio, simplificando la configuración del servicio.
Red	Le permite configurar las funciones de comunicación de red, tales como interfaces, rutas y VPN, que son la base para que los dispositivos accedan a la red.
System	Le permite configurar funciones de gestión de dispositivos, tales como administrador, reloj, SNMP y actualización del sistema y proporciona una base para la ejecución normal del sistema.

Gestión de archivo de configuración

- Elija **System > Configuration File Management** para ver el archivo de configuración actual y especificar un archivo de configuración para la próxima puesta en marcha.




The screenshot displays the Huawei USG6300E web interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Policy', 'Object', 'Network', and 'System'. The 'System' menu is highlighted. The left sidebar shows the 'Configuration File Management' option. The main content area shows the 'Configuration File' section with fields for 'Current Configuration File' and 'Next Startup Configuration File'. The 'Current Configuration' section shows a list of configuration items. A red arrow points from the 'Select' button in the 'Current Configuration' section to the 'Manage Configuration File' dialog box. The dialog box shows a table of configuration files with columns for File Name, File Size (bytes), Time of Last Modification, State, Edit, and Download. The table lists two files: 'hda1/vrpcfg.zip' (2,190 bytes) and 'hda1/feedback.zip' (4,874 bytes). The 'hda1/vrpcfg.zip' file is highlighted as the 'Next Startup Configuration File'.

File Name	File Size (bytes)	Time of Last Modification	State	Edit	Download
hda1/vrpcfg.zip	2,190		Next Startup Configuration File		
hda1/feedback.zip	4,874				

Actualización de versiones

- Elija **System > System Upgrade** para actualizar el software del sistema, parchear archivos y presentar archivos de paquete.



HUAWEI

USG6395E

Dashboard

Monitor

Policy

Object

Network

System

Setup

- System Time
- SNMP
- Across-Layer-3 MAC Identification
- IDS Interworking
- CIS Interworking
- Restart
- Configure Information Push
- Hardware Fast Forwarding
- Advanced Settings
- Charset Configuration
- User Experience Plan

Administrator

Virtual System

High Availability

Log Configuration

License Management

Update Center

System Upgrade

Configuration File Management

VPN Client Upgrade

Startup Wizard

Link Configuration

System Upgrade

Current Version

USG6395E V600R007C00SPC200 (VRP (R) software, Version 5.179)

Details

System Upgrade File List

Server IP Address

sac.huawei.com

[\[Server Connectivity Test\]](#)

File Name	Current File	Startup File	Status	Operation
System File	hda1:/v500r007c00spc200.bin	hda1:/v500r007c00spc200.bin		[One-Click Upgrade] [Select]
Patch File				[One-Click Upgrade] [Select]
Content Security Con	hda1:/v500r007c00spc200_content...	hda1:/v500r007c00spc200_content...	Current file: Matched with the system so... Startup file: Matched with the system so...	[Online Upgrade] [Locally Upgrade] [Select] [Remove]
Content Security Con			Not loaded	[Online Upgrade] [Locally Upgrade] [Select]
URL Remote Query C			Not loaded	[Online Upgrade] [Locally Upgrade] [Select]
Cloud Sandbox C...			Not loaded	[Online Upgrade] [Locally Upgrade] [Select]

Displaying 6

CU Console

System Software Management

Upload

Delete

Refresh

<input type="checkbox"/>	File Name	File Size (bytes)	Last Modified	Status	Edit	Download
<input type="checkbox"/>	hda1:\v900r007c00spc200.bin	214,283,264		Run		

Displaying 1

Close

Cuestionario

1. (Pregunta de respuesta múltiple) ¿Cuál de los siguientes protocolos puede aplicarse a la capa de aplicación? ()
 - A. HTTP
 - B. DNS
 - C. FTP
 - D. OSPF
2. (Verdadero o falso) La conexión de datos la inicia el cliente en modo FTP activo. ()
 - A. Verdadero
 - B. Falso

Resumen

- Este curso describe el modelo de referencia TCP/IP, que consta de cinco capas: la capa de aplicación, la capa de transporte, la capa de red, la capa de enlace de datos y la capa física. Cada capa proporciona servicios para la capa superior, cada uno se aplica con protocolos diferentes. El curso también presenta protocolos comunes como ARP, ICMP, FTP y HTTPS.
- Este curso describe la arquitectura de la red empresarial típica, dispositivos de red comunes, como switches, routers y firewalls, y también los modos de configuración del firewall basado en una interfaz gráfica de usuario (GUI) o una interfaz de línea de comandos (CLI).

Recomendaciones

- Visite los sitios web oficiales de Huawei:
 - Servicio para empresas: <https://e.huawei.com/en/>
 - Soporte técnico: <https://support.huawei.com/enterprise/en/index.html>
 - Aprendizaje en línea: <https://learning.huawei.com/en/>

Acrónimos y abreviaturas (1/3)

Acrónimos y abreviaturas	Significado
ACK	Acuse de recibo
ARP	Protocolo de resolución de direcciones
C/S	Cliente/Servidor
CLI	Interfaz de línea de comando
FIN	Finalizar
FTP	Protocolo de transferencia de archivos
HTTP	Protocolo de transferencia de hipertexto
HTTPS	Protocolo de transferencia de hipertexto segura
ICMP	Protocolo de mensajes de control de Internet
IGMP	Protocolo de gestión de grupos de Internet
IP	Protocolo de Internet

Acrónimos y abreviaturas (2/3)

Acrónimos y abreviaturas	Significado
IS-IS	Sistema intermedio a sistema intermedio
MAC	Control de acceso al medio
OSI	Interconexión de sistemas abiertos
PPP	Protocolo punto a punto
PPPoE	Protocolo punto a punto sobre Ethernet
SFTP	Protocolo de transferencia de archivos segura
SMTP	Protocolo de transferencia de correo simple
SSH	Protocolo de Secure Shell
STelnet	Secure Telnet
SYN	Sincronización de número de secuencia
TCP	Protocolo de control de transmisión

Acrónimos y abreviaturas (3/3)

Acrónimos y abreviaturas	Significado
TFTP	Protocolo de transferencia de archivos trivial
TLS	Seguridad de la capa de transporte
TTL	Período de vida
UDP	Protocolo de datagramas de usuario
URL	Localizador universal de recursos
UTM	Gestión unificada de amenazas
VPN	Red privada virtual
WAF	Firewall de aplicaciones web
WWW	Red global mundial
OSPF	Abrir primero el trayecto más corto
LSDB	Base de datos del estado del enlace

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

**Copyright©2023 Huawei Technologies Co., Ltd.
All Rights Reserved.**

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

