Introducción y conceptos básicos

Contenido

1. Funciones principales de routers y puertas de enlace
2. Componentes y arquitectura de un router
3. Protocolos de enrutamiento
4. Tipos de routers y puertas de enlace
5. Seguridad en routers y puertas de enlace
6. Desafios y tendencias actuales

Funciones de routers y puertas de enlace en una red

Concepto	Router	Puerta de enlace
Función	Enrutamiento de paquetes, conexión de redes, segmentación de tráfico, filtrado y control de tráfico	Conexión entre redes diferentes, traducción de direcciones de red (NAT), seguridad de la red, gestión de tráfico
Conectividad	Permite la interconexión de diferentes redes, como redes locales (LAN) y redes de área amplia (WAN)	Actúa como punto de entrada y salida para las comunicaciones entre redes diferentes
Enrutamiento	Toma decisiones sobre cómo dirigir los paquetes de datos a través de una red utilizando tablas de enrutamiento y protocolos de enrutamiento	No se encarga del enrutamiento propiamente dicho, sino de la traducción y gestión de las comunicaciones entre redes

Funciones de routers y puertas de enlace en una red

Concepto	Router	Puerta de enlace
Seguridad	Puede implementar funciones de filtrado de tráfico y control de acceso utilizando listas de control de acceso (ACL)	Puede implementar funciones de cortafuegos, proxy y VPN para proteger la red y controlar el acceso a recursos internos
Traducción de direcciones	No realiza la traducción de direcciones de red (NAT)	Puede realizar la traducción de direcciones de red (NAT) para permitir que varios dispositivos compartan una dirección IP pública
Gestión de tráfico	Puede realizar la gestión de tráfico, asignando ancho de banda y priorizando el tráfico	Puede realizar la gestión de tráfico, optimizando el rendimiento de la red y asignando recursos según las necesidades

Componentes y arquitectura de un router

Un router está compuesto por una combinación de componentes **físicos** y **lógicos** que trabajan juntos para permitir el enrutamiento y la conectividad en una red.

1. **CPU**: La CPU ejecuta las instrucciones y procesa los datos en el router.
2. **Interfaces de red**: Son los puertos físicos en el router que se utilizan para conectarlo a otros dispositivos o redes. Pueden incluir interfaces Ethernet, Wi-Fi, puertos serie, puertos USB, entre otros.
3. **RAM**: La memoria RAM del router almacena los datos y las instrucciones que se están utilizando en tiempo real.
4. **Memoria flash**: Se utiliza para almacenar el sistema operativo del router, así como otros archivos de configuración y firmware
5. **Interfaz de consola**: Permite la conexión de un dispositivo de administración al router a través de un puerto de consola para realizar tareas de configuración y monitoreo.
6. **Alimentación**: El router requiere una fuente de alimentación eléctrica para funcionar. Puede ser alimentado mediante una conexión eléctrica directa o a través de un adaptador de corriente.

¿Qué elementos son físicos y cuáles son lógicos? ¿Por qué?

Protocolos de enrutamiento

Existen diferentes tipos de protocolos de enrutamiento, cada uno se diferencia del resto por **tipo**, **algoritmo**, **escalabilidad**, **complejidad**, **convergencia** y los **casos de uso**.

- **Tipo**:
  - **Estado de enlace**: Es un enfoque de enrutamiento donde los routers intercambian información sobre el estado de los enlaces de red en la topología. Utilizan algoritmos como SPF (Shortest Path First) para calcular las rutas óptimas y construir una base de datos con la información de enrutamiento actualizada.
  - **Vector de distancia**: Es un enfoque de enrutamiento donde los routers intercambian información sobre la distancia o el costo de las rutas hacia diferentes destinos. Utilizan algoritmos como Bellman-Ford para seleccionar las rutas más cortas o largas y actualizar sus tablas de enrutamiento.
- **Algoritmo**: Procedimiento de desición
  - Ruta más larga o ruta más corta

Protocolos de enrutamiento

- **Escalabilidad**: Capacidad de un protocolo de enrutamiento para adaptarse y funcionar eficientemente en redes de diferentes tamaños y complejidades. Un protocolo escalable puede manejar redes grandes con miles de routers y un alto volumen de tráfico sin degradar su rendimiento.

- **Complejidad**: Dificultad y sofisticación del protocolo de enrutamiento en términos de su diseño, configuración y operación. Protocolos más complejos pueden requerir una mayor configuración y administración, mientras que protocolos más simples pueden ser más fáciles de implementar y mantener.

- **Convergencia**: Es el tiempo necesario para que todos los routers en una red actualicen y se ajusten a los cambios en la topología o en las tablas de enrutamiento. Una rápida convergencia implica que los routers pueden adaptarse rápidamente a los cambios y asegurar la conectividad sin interrupciones, mientras que una convergencia lenta puede resultar en una interrupción del servicio.

Protocolos de enrutamiento

Protocolo	Tipo	Algoritmo	Escalabilidad	Complejidad	Convergencia	Uso
OSPF	Estado de enlace	Rutas más cortas primero	Alta	Alta	Rápida	Redes grandes y complejas
BGP	Vector de distancia	Rutas más largas primero	Muy alta	Media	Lenta	Proveedores de servicios y enrutamiento entre dominios
RIP	Vector de distancia	Rutas más cortas primero	Media	Baja	Rápida	Pequeñas redes y entornos simples
EIGRP	Vector de distancia	Algoritmo propietario	Alta	Media	Rápida	Redes Cisco y entornos mixtos
IS-IS	Estado de enlace	Rutas más cortas	Alta	Alta	Rápida	ISP
Babel	Vector de distancia	Rutas más cortas primero	Alta	Media	Rápida	Redes inalámbricas ad hoc y de sensores

Protocolos de enrutamiento

Protocolo	Tipo	Algoritmo	Escalabilidad	Complejidad	Convergencia	Uso
RIPng	Vector de distancia	Rutas más cortas primero	Media	Baja	Rápida	IPv6 y entornos pequeños
OLSR	Estado de enlace	Multipunto optimizado	Media	Media	Rápida	Redes Móviles
ISIS	Estado de enlace	Rutas más cortas primero	Alta	Alta	Rápida	ISP
RIPv2	Vector de distancia	Rutas más cortas primero	Media	Baja	Rápida	Pequeñas redes y entornos simples
EGP	Vector de distancia	Rutas más largas	Media	Baja	Rápida	Enrutamiento entre dominios

Tipos de routers

Tipo de Router	Uso Principal	Escala	Funcionalidad	Ejemplo
Router de Servicios Integrados (ISR)	Redes empresariales	Pequeña a grande	Enrutamiento, servicios adicionales integrados como cortafuegos, VPN, voz y video	Cisco ISR Series, Juniper SRX Series, etc.
Router Inalámbrico	Conexión inalámbrica, acceso a Internet	Pequeña a mediana	Enrutamiento, funciones inalámbricas como Wi-Fi	Routers inalámbricos domésticos, routers empresariales con capacidades inalámbricas
Router de Servicio de Borde (PE router)	Proveedores de servicios, redes de área amplia	Grande	Conectividad entre proveedores de servicios, enrutamiento de nivel superior	Routers de proveedores de servicios como Cisco ASR, Juniper MX Series, etc.

Tipos de routers

Tipo de Router	Uso Principal	Escala	Funcionalidad	Ejemplos
Router de Acceso	Hogares, pequeñas empresas	Pequeña escala	Conectividad básica, funciones de red limitadas	Routers domésticos, routers para pequeñas empresas
Router de Borde	Conexión a Internet, protección de red	Mediana a grande	Enrutamiento, seguridad, gestión de tráfico	Routers para empresas, routers de seguridad de borde
Router de Distribución	Redes empresariales, proveedores de servicios	Mediana a grande	Enrutamiento, interconexión de redes, políticas de tráfico	Routers de distribución de Cisco, Juniper, etc.
Router de Núcleo	Proveedores de servicios, grandes empresas	Grande	Alto rendimiento de enrutamiento, interconexión de múltiples redes, escalabilidad	Routers de núcleo de Cisco CRS, Juniper MX Series, etc.

Tipos de puertas de enlace de red

Tipo de Puerta de Enlace	Uso Principal	Funcionalidad	Características
Puerta de Enlace de Red	Conexión entre redes diferentes	Encaminamiento de paquetes entre redes, traducción de direcciones de red (NAT), control de tráfico, seguridad de red	Punto de entrada y salida de datos entre redes, funciones de firewall, soporte para VPN
Puerta de Enlace de Firewall	Protección de la red contra amenazas externas	Control y filtrado de tráfico, inspección de paquetes, prevención de intrusiones, protección contra ataques de denegación de servicio (DoS)	Funcionalidades de cortafuegos, inspección profunda de paquetes, administración de políticas de seguridad
Puerta de Enlace de VPN	Acceso remoto seguro a una red privada	Establecimiento de túneles VPN, autenticación y cifrado de datos, encriptación de tráfico, seguridad de la conexión	Soporte para protocolos VPN, como IPSec, SSL/TLS, PPTP, L2TP

Tipos de puertas de enlace específicas

Tipo de Puerta de Enlace	Uso Principal	Funcionalidad
Puerta de Enlace de Proxy	Control y filtrado de contenido web	Caché de contenido, filtrado de URL, control de acceso, aceleración de tráfico, seguridad de navegación web
Puerta de Enlace de Seguridad	Protección contra amenazas de seguridad en la red	Detección y prevención de intrusiones (IDS/IPS), análisis de tráfico, inspección de contenido, protección contra malware
Puerta de Enlace de Voz y Video	Conexión de redes de comunicación de voz y video	Gestión y enrutamiento de llamadas, conversión entre protocolos de voz, priorización de tráfico de voz/video

Seguridad en routers

Aspecto de Seguridad	Descripción
Autenticación segura	Configuración de métodos de autenticación seguros, como contraseñas fuertes, autenticación de dos factores y autenticación basada en certificados.
Gestión de contraseñas	Uso de contraseñas robustas y únicas para el acceso a los routers. Considerar políticas de cambio periódico de contraseñas y almacenamiento seguro de contraseñas.
Actualizaciones de firmware	Mantenimiento y aplicación regular de actualizaciones de firmware para los routers para corregir vulnerabilidades conocidas y mejorar la seguridad.
Filtrado de tráfico	Configuración de reglas de filtrado de tráfico para permitir únicamente el tráfico necesario y bloquear o restringir el tráfico no autorizado o malicioso.
Seguridad inalámbrica	Configuración segura de conexiones inalámbricas en routers, como el uso de cifrado WPA2/WPA3, ocultación del SSID y configuración de contraseñas fuertes para evitar accesos no autorizados.

Seguridad en puertas de enlace

Aspecto de Seguridad	Descripción
Seguridad física	Protección física de las puertas de enlace para evitar acceso no autorizado o manipulación. Colocación en áreas seguras y restricción de acceso físico a los dispositivos.
Auditoría y monitoreo	Implementación de sistemas de auditoría y monitoreo para detectar y registrar eventos de seguridad, como intentos de acceso no autorizado o actividades sospechosas.
Copias de seguridad	Realización regular de copias de seguridad de la configuración de las puertas de enlace para facilitar la restauración en caso de incidentes o fallos.
Control de acceso	Configuración de listas de control de acceso (ACL) para limitar el acceso a los servicios y puertos de administración solo a las direcciones IP o rangos de IP autorizados.
Detección de intrusiones	Implementación de sistemas de detección de intrusiones (IDS) para monitorear y alertar sobre actividades sospechosas o intentos de intrusión en las puertas de enlace.

Desafios y tendencias actuales

Amenazas en routers

Amenaza	Descripción
Ataques de Fuerza Bruta	Intentos repetidos de adivinar o descifrar contraseñas de administración de routers mediante la prueba de múltiples combinaciones hasta encontrar la correcta.
Inyección de Comandos	Introducción de comandos maliciosos en el sistema operativo del router para obtener acceso no autorizado o realizar acciones destructivas.
Envenenamiento de Tabla de Enrutamiento	Modificación o manipulación de las tablas de enrutamiento del router para redirigir el tráfico a destinos incorrectos o maliciosos.
Ataques de Denegación de Servicio (DoS)	Sobrecarga del router con tráfico malicioso o solicitudes falsas para agotar sus recursos y hacer que deje de funcionar correctamente.
Explotación de Vulnerabilidades Conocidas	Aprovechamiento de debilidades y vulnerabilidades de seguridad en el firmware o en el sistema operativo del router para obtener acceso no autorizado o control sobre el dispositivo.

Amenazas en puertas de enlace

Amenaza	Descripción
Ataques de Denegación de Servicio (DoS)	Sobrecarga de la puerta de enlace con tráfico malicioso o solicitudes falsas para agotar sus recursos y hacer que deje de funcionar correctamente.
Ataques de Firewall Bypass	Intentos de evadir o superar las reglas de firewall de la puerta de enlace para permitir el acceso no autorizado a la red protegida.
Ataques de Explotación de Protocolos	Aprovechamiento de vulnerabilidades en los protocolos de red utilizados por la puerta de enlace para obtener acceso no autorizado o control sobre la red.
Ataques de Suplantación de Identidad (Spoofing)	Falsificación de direcciones IP o MAC para hacer que la puerta de enlace crea que el tráfico malicioso o no autorizado proviene de una fuente confiable.
Ataques de Acceso Remoto no Autorizado	Intentos de acceder a la puerta de enlace de forma remota sin la autenticación o autorización adecuadas para obtener control o realizar acciones maliciosas.

Ataques a Protocolos de Enrutamiento (Internos)

Ataque	Descripción
Envenenamiento de Tabla de Enrutamiento (Route Poisoning)	Modificación maliciosa de las tablas de enrutamiento enviando información falsa sobre rutas para redirigir el tráfico a destinos incorrectos o maliciosos.
Secuestro de Rutas (Route Hijacking)	Toma de control de las rutas legítimas de enrutamiento mediante el envío de actualizaciones de enrutamiento falsas para desviar el tráfico a través de un atacante.
Inundación de Protocolo (Protocol Flooding)	Saturación de los routers con paquetes de enrutamiento falsos o inútiles, lo que provoca una congestión en el tráfico de enrutamiento y puede afectar negativamente la operación de la red.
Ataques de Divulgación de Información (Information Disclosure)	Obtención de información confidencial, como la topología de la red o las tablas de enrutamiento, aprovechando debilidades en los protocolos de enrutamiento.
Ataques de Inyección de Rutas (Route Injection)	Introducción de rutas falsas o maliciosas en los protocolos de enrutamiento para redirigir el tráfico a través de rutas controladas por un atacante.

Ataques a Protocolos de Enrutamiento (Externos)

Ataque	Descripción
Ataques de Inundación de BGP (BGP Flooding)	Envío masivo de actualizaciones de enrutamiento falsas o redundantes en el protocolo BGP (Border Gateway Protocol), lo que puede causar interrupciones en el enrutamiento y saturación de los routers.
Ataques de Inyección de Rutas (Route Injection)	Introducción de rutas falsas en el protocolo BGP para desviar el tráfico a través de rutas controladas por un atacante y permitir el espionaje o el redireccionamiento malicioso.
Ataques de Suplantación de Identidad (BGP Hijacking)	Falsificación de la identidad de un sistema autónomo (AS) para interceptar y redirigir el tráfico a través de una ruta no autorizada o maliciosa.
Ataques de Divulgación de Información (Information Disclosure)	Obtención de información sensible sobre las políticas de enrutamiento y la topología de la red aprovechando las debilidades en los protocolos de enrutamiento exterior.
Ataques de Falsificación de Origen (Origin Spoofing)	Manipulación de la información de origen en las actualizaciones de enrutamiento BGP para hacer que el tráfico aparezca como si se originara en una entidad diferente, lo que puede permitir ataques de intercepción o redireccionamiento.