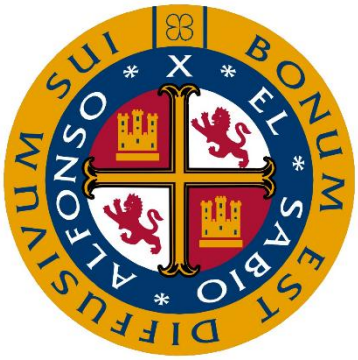


UNIVERSIDAD
ALFONSO X EL SABIO

Sistema de Videoconferencia Seguro en una Empresa Global

María Díaz, Juan Pablo Lobato, Mauricio Murillo, Cintia Santillán, Jiachen Ye

INDICE

1. Diseño de Arquitectura (Modelos OSI/TCP-IP y Comunicación)

1.1 Revisión de Modelos

Modelo OSI

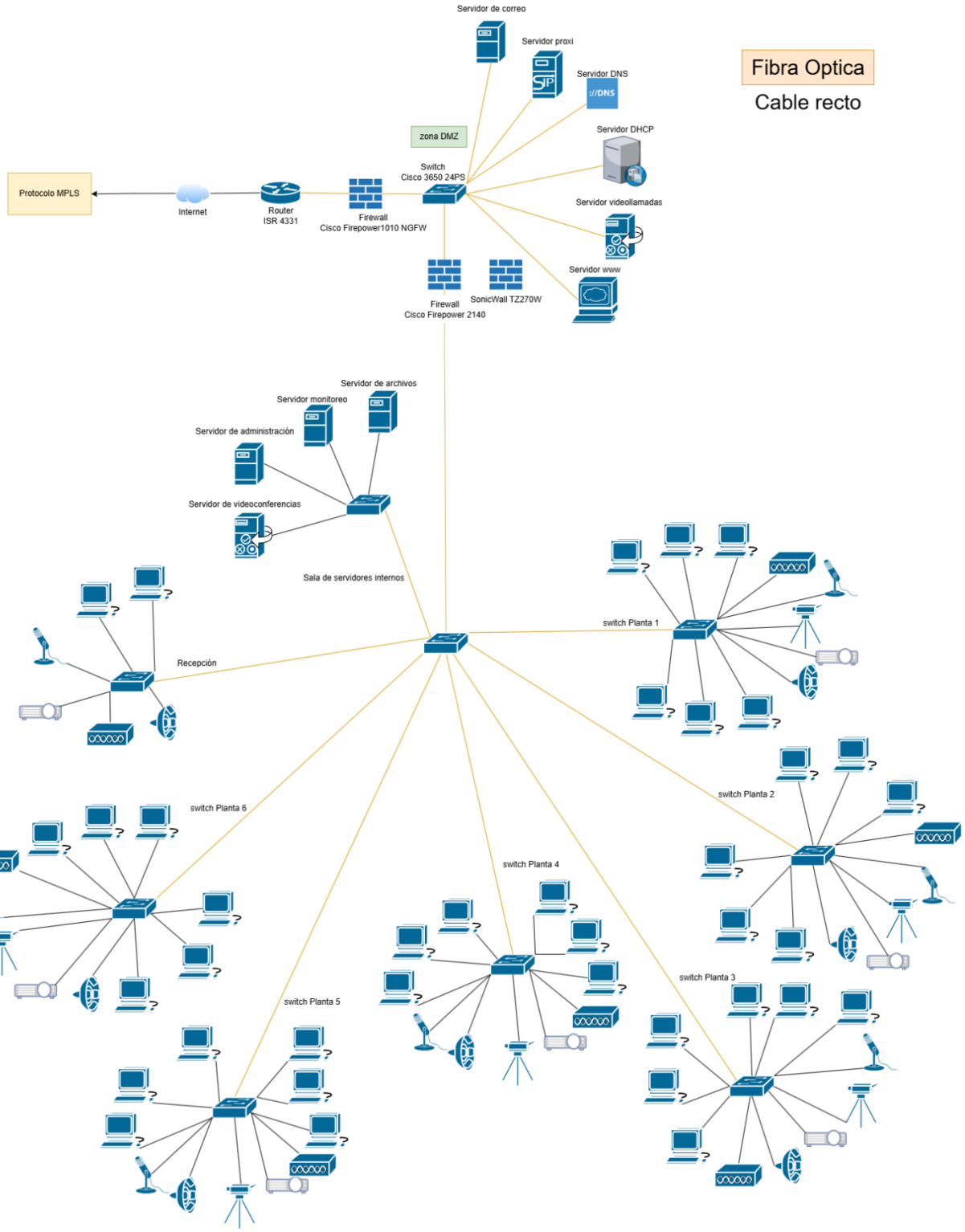
OSI	Función	Tecnologías
7 - Aplicación	Proporciona servicios de red a las aplicaciones del usuario, como videoconferencia.	Aplicaciones de videoconferencia (Zoom, Teams, Webex)
6 - Presentación	Codifica, comprime y cifra los datos para la transmisión segura.	Códecs de video (H.264, H.265), TLS/SSL
5 - Sesión	Gestiona la apertura, mantenimiento y cierre de sesiones de comunicación.	Protocolos SIP, H.323, WebRTC
4 - Transporte	Garantiza la entrega de datos de extremo a extremo con TCP o UDP.	TCP y UDP
3 - Red	Encamina los paquetes a través de la red usando direcciones IP.	IP, BGP, OSPF
2 - Enlace de Datos	Controla el acceso al medio y corrige errores de transmisión.	Ethernet, VLANs, Wi-Fi
1 - Física	Define los medios físicos de transmisión, como fibra óptica o cable Ethernet.	Fibra óptica, cables Ethernet, Wi-Fi 6

Modelo TCP/IP

Capa TCP/IP	Función	Tecnologías
Aplicación	Comunicación de video/audio.	SIP, H.323, WebRTC, TLS, SRTP
Transporte	Maneja la confiabilidad del envío de datos mediante TCP o UDP.	TCP (señalización), UDP (video/audio en tiempo real)
Internet	Direccionamiento y enrutamiento de paquetes.	IPv4, IPv6, QoS, VPNs
Acceso a Red	Conectividad física y lógica.	Ethernet, Wi-Fi 6, VLANs, SD-WAN

1.2 Diseño Lógico de la Red

Diagrama Conceptual



En esta imagen se muestra la red del sistema de videoconferencia que tendría un edificio modelo de la empresa, ajustable para cualquiera de sus tres sedes.

Las sedes se conectan a través de Internet con el protocolo MPLS. En esta red, la entrada a Internet llega por un primer router Cisco ISR 4331, se filtra por un firewall perimetral Cisco

Firepower 2140 que filtrar la mayor parte de los datos, después llega a un switch que conecta con los servidores de correo, proxy, DNS, DHCP, VoIP y web, todos estos servidores están la zona desmilitarizada (DMZ), obteniendo una mayor seguridad.

Inmediatamente de la zona desmilitarizada, se encuentra un firewall interno de la misma marca que filtra los servidores https y otro firewall en paralelo de una marca diferente SonicWall TZ270 menos potente para utilizar en caso puntuales por si una actualización de la marca Cisco u otra cosa vulnerabiliza el firewall.

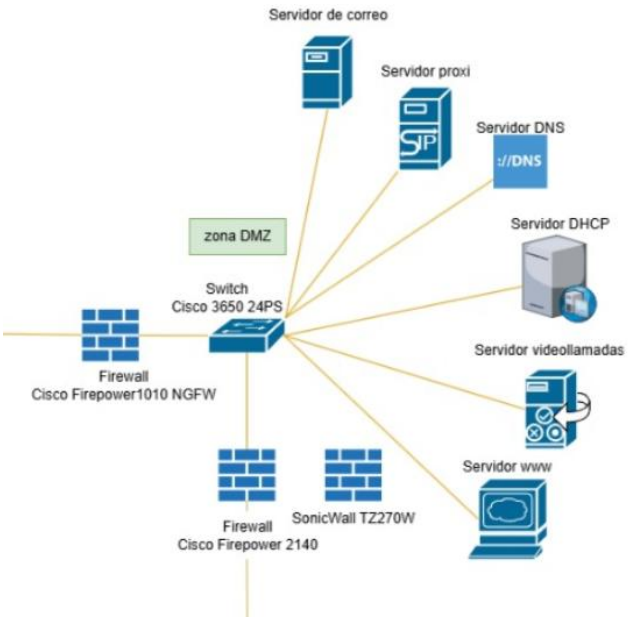
Seguido de estos firewalls se encuentra la red interna, en la cual se encontrará un switch central que se distribuye la conexión a cada segmento de la sede, como el switch de los servidores archivo, administración, videoconferencia y monitoreo o los switches que conectan con los ordenadores, cámaras, proyectores, altavoces y modelo ap. En cuanto a la estructura de cableado todo está compuesto de fibra hasta los switches, después a partir de cada switch de cada apartado y sus componentes está compuesto de cable recto ethernet, Cat 6a debido a que el Cat 7 es parecido, pero más costoso.

Módulos

-Módulo internet

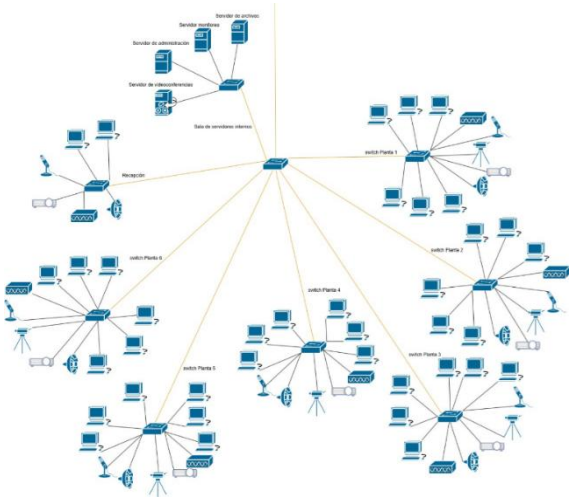
Este módulo provee internet a la red

-Módulo zona DMZ y servidores



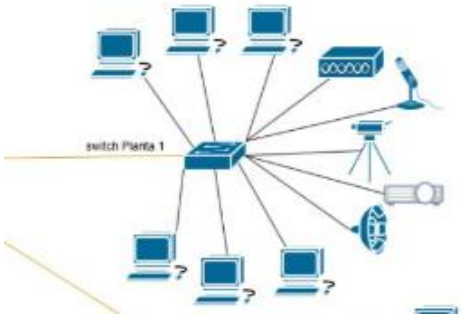
Este módulo aloja los servidores, además de proteger la red interna de amenazas externas

-Módulo red interna



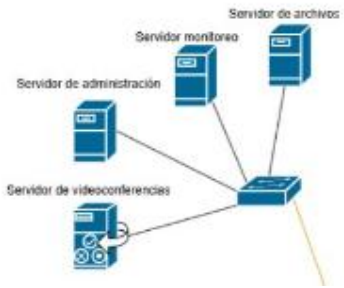
Este módulo consiste en el switch central y como distribuye la información por las diferentes plantas.

-Módulo oficina



En este módulo se muestra los dispositivos de cada planta

-Módulo servidores internos



Aquí se alojan los servidores internos de forma segura

Dispositivos Utilizados

A continuación, se describe los componentes de la red en detalle, como los routers, firewalls, switches, servidores y el cableado, así como los protocolos de seguridad implementados para proteger y optimizar la transmisión de datos entre las sedes.

Router: Cisco ISR 4331

Se ha seleccionado este modelo ya que gestiona múltiples sucursales, actúa como router de borde **MPLS** de tal forma que inicia y finaliza las etiquetas MPLS de los paquetes que entran y salen de la red. Además, permite la optimización de tráfico y firewall integrado.

Con precio aproximado entre $2,500 - $3,500 USD, cuenta con las siguientes especificaciones:

- Mejora la conectividad entres redes y optimiza el tráfico mediante QoS.
- Facilita una comunicación segura y eficiente con filtrado de tráfico.
- Se evitan pérdidas de paquetes y latencia.
- Se facilita la administración y escalabilidad al permitir módulos de expansión.

Switch: Cisco 3650-24PS

Este modelo de swicth se ha seleccionado por su capacidad para manejar altos volúmenes de tráfico, compatibilidad con VLANs y soporte para alimentación PoE+, permitiendo la conexión de dispositivos como teléfonos IP y puntos de acceso Wi-Fi.

Con precio aproximado entre $2,000 - $3,000 USD, cuenta con las siguientes especificaciones:

- Evita la congestión mejorando la segmentación de tráfico con VLANs.
- Permite una mejor gestión del ancho de banda mediante QoS.
- Evita cuellos de botella en la transmisión de datos.
- Impide interferencia y latencia de red.

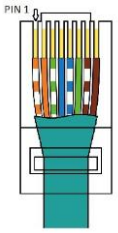
Firewall: Cisco Firepower 2140

Se ha elegido este firewall debido a su alto rendimiento en la inspección de tráfico, su capacidad para detectar amenazas y herramientas de ciberseguridad avanzada. Sumado a esto disponemos del Firewall FortiGate 200F que complementa al Cisco Firepower 2140 brindando una seguridad multicapa, seguridad avanzada, inspección de tráfico y control de amenazas en redes empresariales.
Con precio aproximado entre $41.200 - $48,000 USD para el Cisco Firepower 2140 y $5.000 - $6.300 USD para el **Firewall FortiGate 200F**, cuenta con las siguientes especificaciones:

- Proporciona una capa de seguridad perimetral, filtrando tráfico malicioso antes de que llegue a la red interna.
- Mejora la protección contra ataques de denegación de servicio (DDoS).
- Protege contra Intrusiones y ataques cibernéticos dirigidos a la infraestructura de la empresa.
- Se evitan problemas de fuga de información o ataques de malware en las comunicaciones.

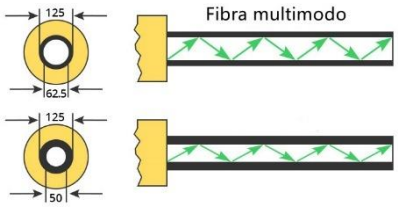
Cableado: Cat 6A y Fibra Óptica

El cableado Cat 6A se usa dentro de cada edificio para conectar dispositivos finales a los switches, mientras que para la fibra óptica se empleará el OM5 en enlaces troncales entre pisos y sedes por su alta capacidad, baja latencia, la capacidad para soportar distancias para redes de empresa y centros de datos a un precio inferior que la fibra monomodo, de este modo la información llegará a su destino sin interferencias ni cambios.



Con precio aproximado entre $0.25 - $1.00 USD por metro para el cableado Cat 6A y $3.00 - $9.00 USD por metro para el cableado de Fibra Óptica OM5, cuenta con:

- Mejora la velocidad y estabilidad de la red.
- Reduce la latencia en la transmisión de datos, fundamental para la videoconferencia.
- Se protege en caso de interferencias electromagnéticas en redes de cobre tradicionales.
- Se evita pérdida de señal en largas distancias, solucionado con fibra óptica.



2.Capa Física – Cálculos y Selección de Tecnologías

2.1 Cálculo de la Tasa de Transmisión según la Fórmula de Shannon

La capacidad máxima teórica del canal se obtiene con la fórmula:

$$C = B \times \log_2 (1+SNR)$$

Donde:

- B = 500 MHz (Ancho de banda disponible) (500MHz para Cat 6a)
- *SNR* = 23 dB (Relación señal a ruido en decibeles)

Conversión de SNR de dB a escala lineal

La conversión se realiza con la ecuación:

SNR linear =10^ (23 /10)

SNR linear =10^ (20/10) =199.52

Cálculo de la tasa de transmisión C

$C = 500 \times 10^6 \times \log_2 (1+199.52)$

$C \approx 3.823$ Gbps

La tasa de transmisión máxima teórica según el teorema Shannon es **3.823 Gbps.**

2.2 Selección de Modulación

Para seleccionar la modulación más adecuada en la red, se han evaluado diferentes opciones considerando la eficiencia espectral y la robustez ante interferencias. Se han definido los siguientes tipos de enlaces:

Enlaces Cableados (Ethernet y Fibra Óptica)

- **Cableado Cat 6A (Ethernet, 10 Gbps)**: Se utiliza PAM-4, ya que permite transmitir 2 bits por símbolo, mejorando la eficiencia espectral sin aumentar la frecuencia de la señal.
- **Fibra Óptica**: Se emplea PAM-4, optimizando la transmisión en enlaces de alta velocidad (40/100 Gbps), permitiendo mayor capacidad con menor ancho de banda en comparación con NRZ.

Enlaces Inalámbricos (Wi-Fi, Redes Celulares)

- **Wi-Fi**: Se utiliza 64-QAM, ya que con un SNR de 23 dB proporciona un equilibrio óptimo entre velocidad y resistencia a interferencias.
- **Alternativas**:
  - **16-QAM** en entornos con más ruido.
  - **256-QAM** descartado por requerir un SNR superior a 30 dB.

Conclusión

La red implementará PAM-4 en enlaces cableados (Ethernet y fibra óptica) para optimizar la transmisión de alta velocidad y 64-QAM en Wi-Fi para garantizar un rendimiento estable con el SNR disponible

3.Capa de Red – Direccionamiento y Enrutamiento

3.1 Esquema de Direccionamiento IP y Subneteo

Esquema de Direccionamiento para las Sedes

Sede	Red principal
Sede 1	192.168.10.0/23
Sede 2	192.168.20.0/23
Sede 3	192.168.30.0/23

Sede 1 - 192.168.10.0:

VLAN	Descripción	Red	Máscara	Host	Gateway
VLAN10	Recepción	192.168.10.0/28	255.255.255.240	14	192.168.10.1
VLAN20	Planta 1	192.168.10.16/26	255.255.255.192	62	192.168.10.17
VLAN30	Planta 2	192.168.10.80/26	255.255.255.192	62	192.168.10.81
VLAN40	Planta 3	192.168.10.144/26	255.255.255.192	62	192.168.10.145
VLAN50	Planta 4	192.168.11.0/26	255.255.255.192	62	192.168.11.1
VLAN60	Planta 5	190.168.11.64/26	255.255.255.192	62	192.168.11.65
VLAN70	Planta 6	192.168.11.128/26	255.255.255.192	62	192.168.11.129
VLAN80	Servidores Int.	192.168.11.192/24	255.255.255.0	254	192.168.11.193

Sede 2 - 192.168.20.0:

VLAN	Descripción	Red	Máscara	Host	Gateway
VLAN10	Recepción	192.168.20.0/28	255.255.255.240	14	192.168.20.1
VLAN20	Planta 1	192.168.20.16/26	255.255.255.192	62	192.168.20.17
VLAN30	Planta 2	192.168.20.80/26	255.255.255.192	62	192.168.20.81
VLAN40	Planta 3	192.168.20.144/26	255.255.255.192	62	192.168.20.145
VLAN50	Planta 4	192.168.21.0/26	255.255.255.192	62	192.168.21.1
VLAN60	Planta 5	190.168.21.64/26	255.255.255.192	62	192.168.21.65
VLAN70	Planta 6	192.168.21.128/26	255.255.255.192	62	192.168.21.129
VLAN80	Servidores Int.	192.168.21.192/24	255.255.255.0	254	192.168.21.193

Sede 3 – 192.168.30.0:

VLAN	Descripción	Red	Máscara	Host	Gateway
VLAN10	Recepción	192.168.30.0/28	255.255.255.240	14	192.168.30.1
VLAN20	Planta 1	192.168.30.16/26	255.255.255.192	62	192.168.30.17
VLAN30	Planta 2	192.168.30.80/26	255.255.255.192	62	192.168.30.81
VLAN40	Planta 3	192.168.30.144/26	255.255.255.192	62	192.168.30.145
VLAN50	Planta 4	192.168.31.0/26	255.255.255.192	62	192.168.31.1
VLAN60	Planta 5	190.168.31.64/26	255.255.255.192	62	192.168.31.65
VLAN70	Planta 6	192.168.31.128/26	255.255.255.192	62	192.168.31.129
VLAN80	Servidores Int.	192.168.31.192/24	255.255.255.0	254	192.168.31.193

Calculo con ejemplo de la sede 1

Dirección base de la sede 1: 192.168.10.0/23
Rango: 192.168.10.0 - 192.168.11.255
512 direcciones en total, que se reparten entre las VLANs.

División de las VLANs, con diferentes mascaras:
Recepción /28 à 16 direcciones -2 son 14 hosts: 192.168.10.0/28
Cada planta /26, à 64 direcciones -2 son 62 hosts: 192.168.10.16/26, 192.168.10.80/26, etc...
Servidores /29 à 8 direcciones - 2 son 6 hosts: 192.168.11.192/29

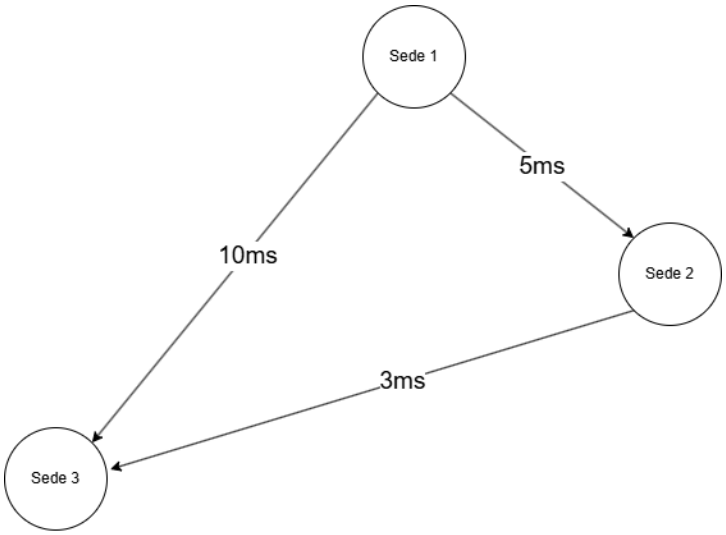
Otras explicaciones:

Las máscaras de VLAN20-VLAN70 serán de 255.255.255.192 a pesar de que actualmente hay un desperdicio de direcciones, hemos decidido poner esta máscara por si surge una futura expansión en la planta.

Mientras que VLAN10 hemos puesto una de 255.255.255.240 debido a que en la recepción habrá menos dispositivos. Y en la VLAN80 donde se alojan los servidores internos una de 255.255.255.248 ya que solo será necesario 4 direccionamientos, uno por cada servidor interno. En estos dos casos también hemos dejado un pequeño desperdició de direcciones por si en un futuro hace falta expandir el equipo no se tenga que tocar la red.

3.2 Enrutamiento

Rutas Óptimas Calculadas (Dijkstra)



Como podemos observar la ruta óptima para ir de la sede 1 a la sede 3 sería pasando por la sede 2 ya que nos dejaría 8ms (3ms+5ms) a diferencia de ir por la ruta directa que serían 10 ms.

Configuración del Enrutamiento por Inundación para Contingencias

El enrutamiento por inundación (flooding) se usa en contingencias cuando los protocolos de enrutamiento fallan. Consiste en enviar los paquetes por todas las rutas posibles, asegurando su entrega si existe un camino disponible. Aunque garantiza conectividad, genera alto tráfico y consumo de recursos, por lo que se limita a casos como descubrimiento de rutas o recuperación tras fallos. Para evitar congestión, se implementan mecanismos como TTL o filtrado de paquetes duplicados.

Pasos para Configurar el Enrutamiento por Inundación

1) Habilitar el reenvío de paquetes en los routers

Se activa la opción de reenvío de paquetes para permitir la transmisión a múltiples interfaces:

```
conf t
ip forwarding
exit
```

2) Configurar las interfaces de red

Se asignan direcciones IP y se habilitan las interfaces para enviar paquetes en todas direcciones posibles:

```
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
```

```
no shutdown
Exit
```

Repite para cada interfaz conectada.

3) Implementar rutas estáticas de respaldo.

Para mejorar la eficiencia, se configuran rutas estáticas en caso de fallo:

```
ip route 0.0.0.0 0.0.0.0 192.168.1.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

Esto envía los paquetes a todas las posibles rutas disponibles.

4) Configurar enrutamiento de contingencia (Flooding manual con ACLs y PBR)

Si el protocolo de enrutamiento principal falla, puedes forzar la inundación con listas de control de acceso y políticas de reenvío:

```
access-list 101 permit ip any any
route-map Flood permit 10
 match ip address 101
 set interface GigabitEthernet0/1 GigabitEthernet0/2
```

Esto permite que los paquetes se envíen por múltiples interfaces en caso de fallo.

¿Cuándo se debe utilizar?

- En caso de que un enlace principal falle y es necesario enviar tráfico por cada una de las rutas posibles.
- En redes pequeñas o incluso de emergencia, siempre que otros protocolos puedan tardar en coincidir.
- Como medida de contingencia en redes críticas (bancos, hospitales, etc.).

Se debe tener en cuenta que la inundación suele generar una gran sobrecarga, por ello no es lo ideal en redes de gran tamaño.