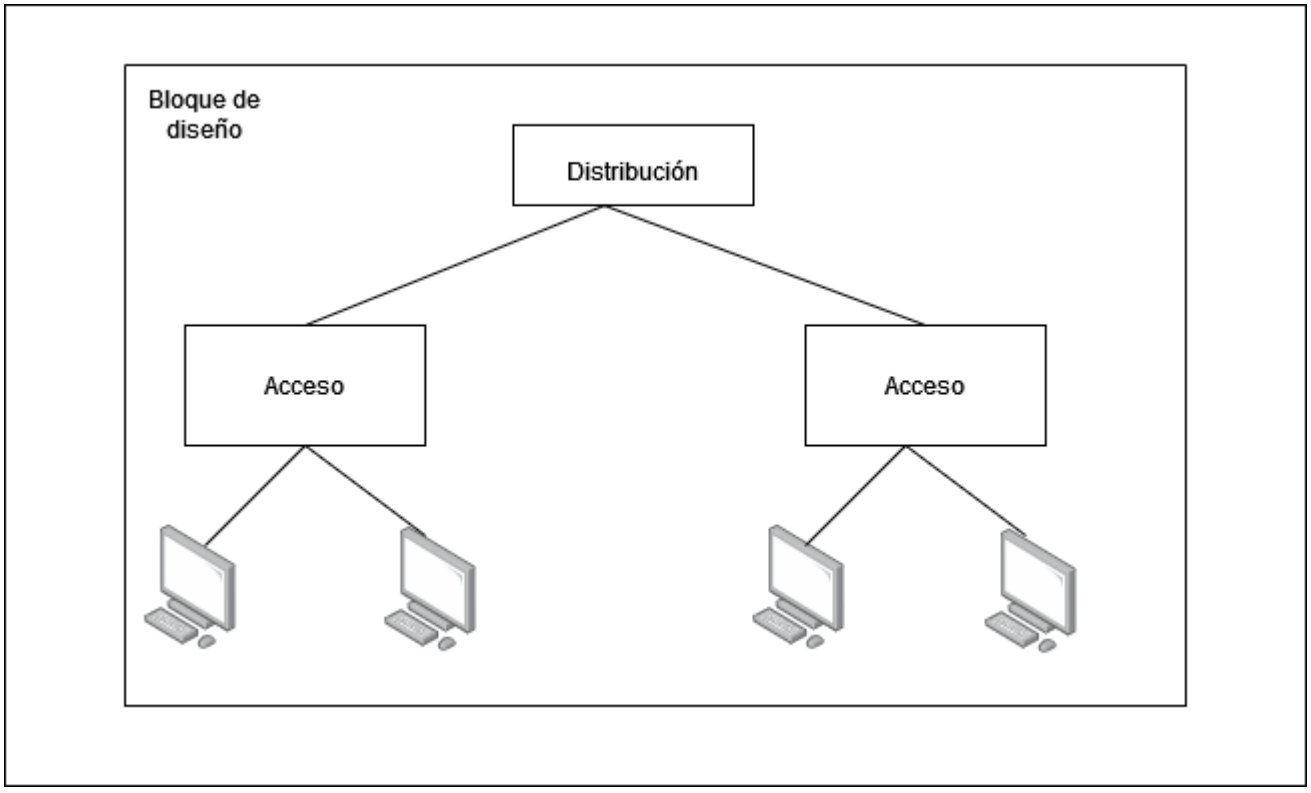
Diseño de Redes Seguras

Modelos de diseño de red básicos

Modelo Jerárquico



Se basa en la división de la red en capas:

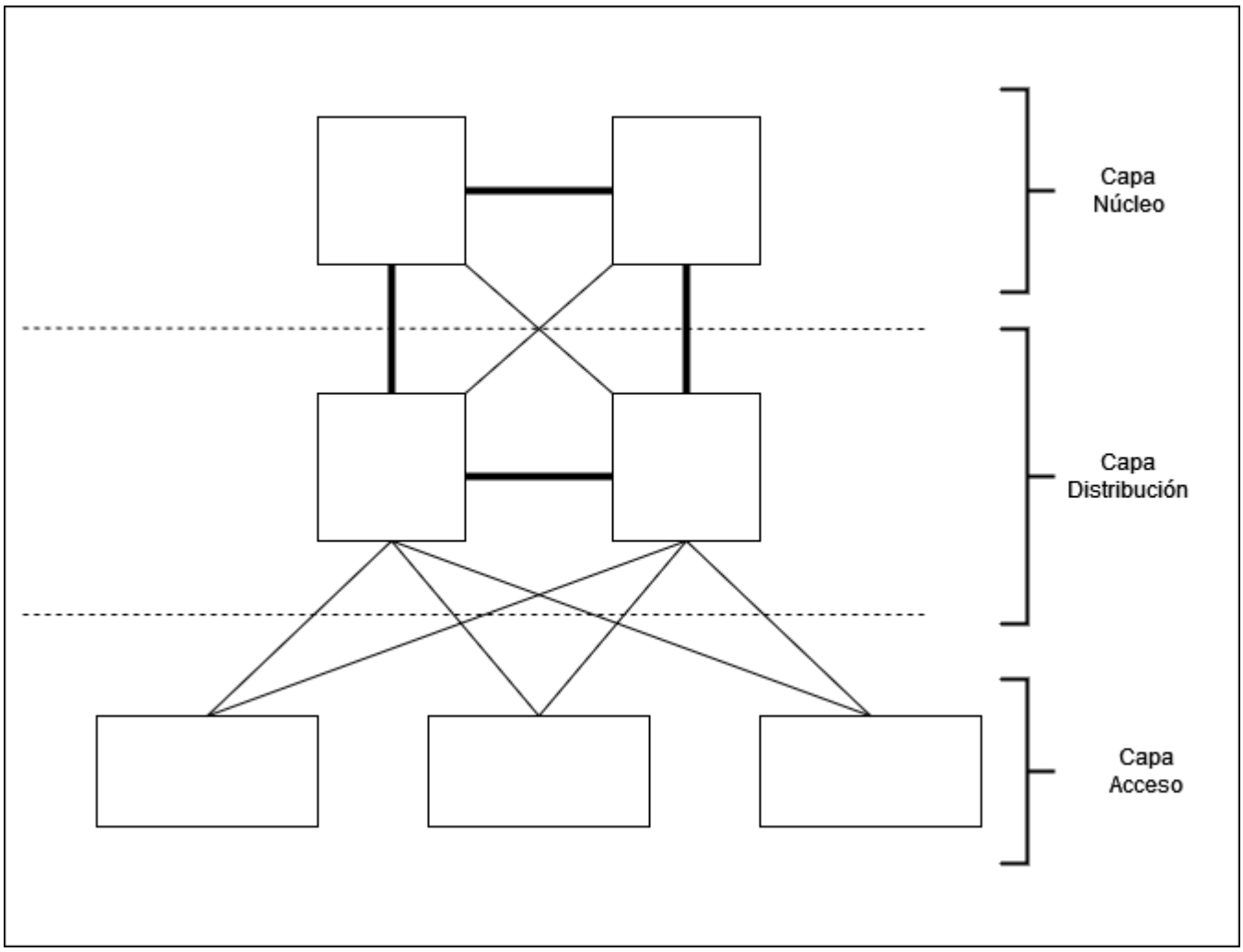
- Cada capa se especializa en una serie de funcionalidades
- Se basa en la estructura jerárquica de una organización
- Facilita la selección de desipositivos, configuración y mantenimiento
- Se puede aplicar en LAN y WAN

Ventajas

- Fácil de comprender: cada elemento implementa una serue de funciones limitadas y la monitorización y sistemas de gestión se estructuran por capas
- Permite el crecimiento modular: Reutilización de bloques de diseño y reducción del área de impacto de los cambios.
- Mejora la capacidad para determinar el ámbito de fallo
- En entornos corporativos, bien aplicado para ahorrar costes. Capacidad de control del ancho de banda. Mejora de la gestión de stocks de equipos de respaldo, así como las tareas de gestión de copias de seguridad.

Capas del modelo Jerárquico

- Capa de núcleo: Transporte a la mayor velocidad posible
- Capa de distribución: Conectividad basada en directivas
- Capa de acceso: Acceso a la red por parte de los usuarios.



Capa de acceso

La tecnología base es Ethernet que decide como operan las redes cableadas y por otro lado está el WiFi para conexión inalámbrica, pero nos vamos a centrar en ethernet. Esta capa proporciona acceso a los usuarios del segmento local de la red(Ethernet):

- Conmutación de capa 2
- Alta disponibilidad
- Seguridad de Puerto
- Limitación del tráfico de broadcast
- QoS: Clasifiación, etiquetado y establecimiento de límites de confianza
- Limitación del ratio de transferencia
- ARP inspection
- Virtal Access Control Sit
- Spanning Tree
- Power Over Ethernet

- VLANs: VLANS auxiliares
- Network Access Control (NAC)

Capa de distribución

- Centraliza la conectividad de red en un edificio
- Sirve como punto de aislamiento entre la capa de acceso y la capa de distribución
- Es uno de los puntos clave a tener en cuenta para el diseño de redes seguras

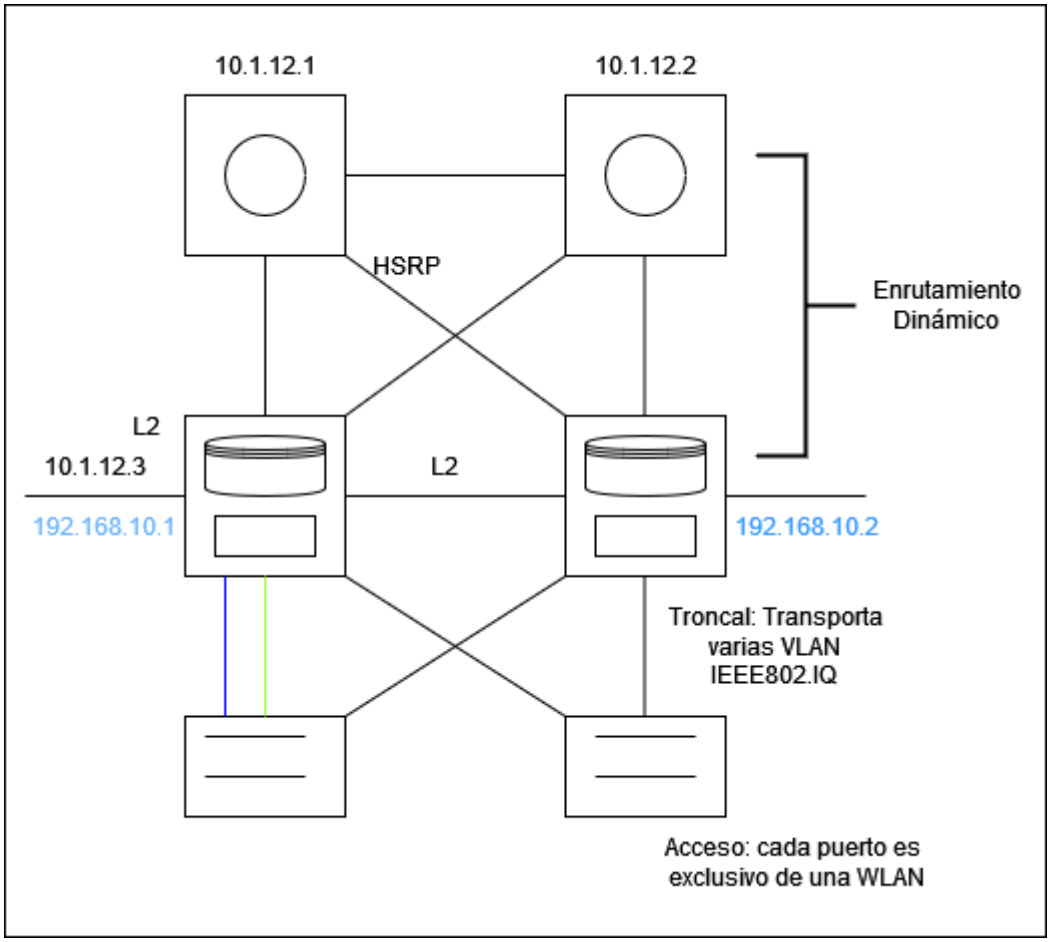
Funcionalidades de la capa de desitribución:

- Conectividad basada en políticas: Define la conectividad entre grupos de dispositivos, se aplican las reglas que definen los flujos de tráfico permitidos.
- Se pueden implementar mediante ACLs
- Balanceo de carga y redundancia
- Agregación de conexiones de planta (LAN) o enlaces (WAN)
- Aplicación de QoS

Capa de núcleo

- Es la parte central de la rez que se encarga de conmutar paquetes de datos a alta velocidad
- Recibe los nombres de núcleo, core o backbone.

Implementación tradicional

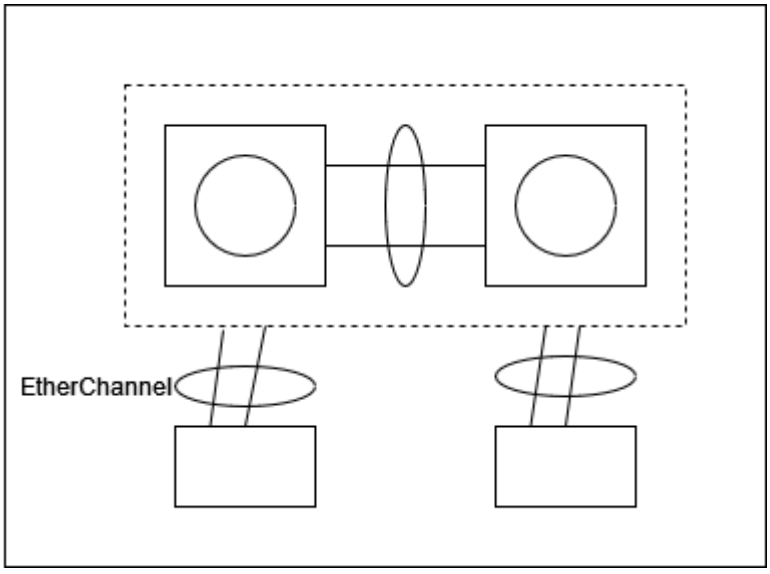


- Enlace des ce capa 3 enrutados entre distribución y núcleo.
- Entre distribución y acceso, y en acceso: enlaces de capa conmutados.
- Se usa Span Entry

Implementación Capa 3 hasta acceso

- Evita el uso de STP → balanceo de carga desde acceos
- Aumenta el coste de la instalación

Implementación de Virtual Switches



- Evita el uso de STP y HSRP
- VRRP → Balanceo de carga desde acceso
- Lo malo es que aumenta el coste de instalación y las tecnologías no son compatibles entre fabricantes.
- Aunque tengamos una topología física, esto operará como 2 switches de acceso conectados a un swtich. Se obtienen enlaces etherchannel.

Modelo Jerárquico en WAN

- Hub y Spoke o estrella extendida: Estabilidad, Rápida convergencia, redes corporativas, facilita las políticas de seguridad
- Anillo: Redes de transporte
- Malla: Tolerancia a fallos.

Frontera Corporativa

Conectividad con otras sedes de una organización

- Modelo de hub and spoke
- Tecnologías WAN más Actuales: SD-WAN, Mutiprotocolo Label Switching, Metro Ethernet, Lineas dedcadas imolementadas mediante diferentes tecnologías
- Site to site VPNs

Acceso remoto mediante VPNs

- Proporciona servicios de acceso remoto a la infraestructura
- Técnicas de tunneling criptográfico y mecanismos de autenticación

Aproximaciones de seguridad perimetral

Zonning

División en zonas o seguridad preimetral. Se agrupan los dispositivos con las mismas políticas. Se puede hacer de forma física o de forma lógica. Hay varios tipos de zonas básicas

- Zona pública: es una zona externa que no está controlada por la organización
- DMZ: Alberga los servicios públicos de la organización.
- Zona restringida: Zona interna que contiene datos y servicios críticos.

Para esto se utilizarán diferentes mecanismos de filtrado.

Además de la división en zonas y la utilización de dispositivos de seguridad como firewalls, es necesario usar conficuraciones de seguridad como:

- VPN: acceso remoto a la red corporativa.
- Acceso segura a la red
- Protección de la infraestructura: Limitar y controlar el acceso para que no todo el mundo pueda acceder a todos los dispositivos
- Gestión de red y seguridad: Herramientas de monitorización que permitan gestión centralizada de las políticas de seguridad.