

1º parcial - Redes II

Temas :	Ruteo estático / dinámico ✓	✓	STP / VLAN / Ethernet ✓
	OSPF ✓		NAT ✓
	BGP ✓		VoIP ✓
	WAN ✓		SIP / SDP / RTP ✓
	MPLS ✓		wifi ✓
	VRF & VPN ✓		FDMA vs. OFDMA vs. OFDMA ✓
	IPsec ✓		DHCP / DNS / HTTP ✓
	ACLs ✓		

Resumen:

- Redes: sistemas interconectados

En una red digital se distribuyen datos
(redes IP)

medios de red ↗ cobre (Ethernet)

satélite

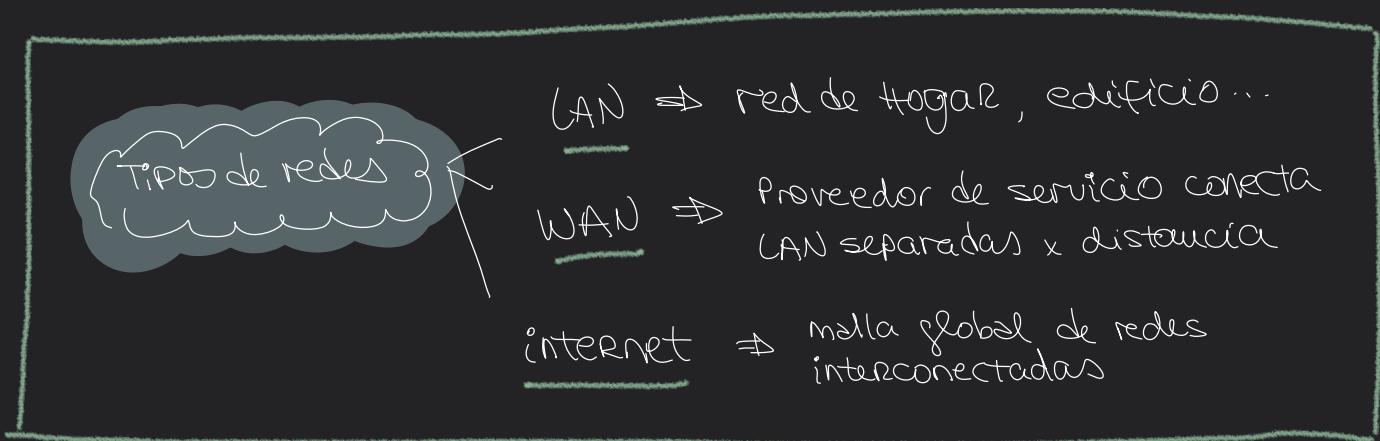
fibra óptica

medios inalámbricos (wifi)

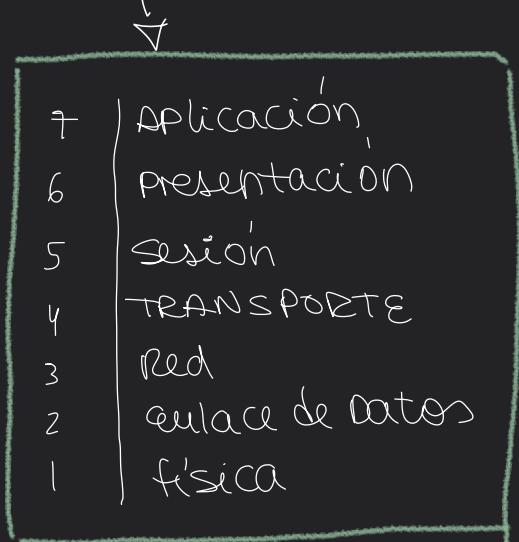
• Dispositivos de Red:

{

- Routers : en comunicaciones WAN
- switches : en comunicaciones LAN
- Gateway : conversores de medios
(ej: señales de cobre a fibra)

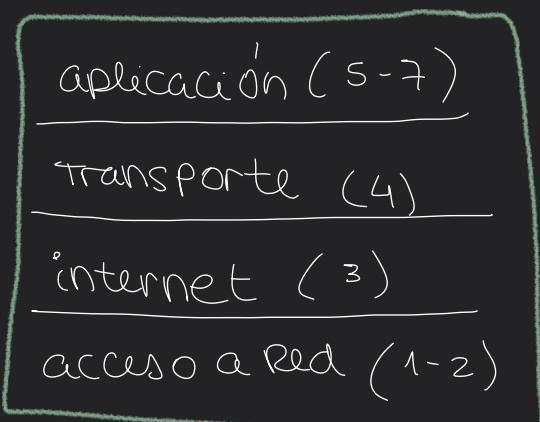


• Modelo OSI: modelo teórico que divide funciones de redes de comunicación en capas



→ Modelo TCP / IP ;

simplificación del modelo OSI
en 4 capas :



L2

→ Host tiene Dirección MAC / física que identifica de manera única un dispositivo de red a nivel físico

L1 → Capa física / capa de HW
maneja señales a nivel físico (potencia, electricidad)

L2 → Capa enlace de Datos
Responsable de Transferencia fiable x circuito eléctrico
(-) paquete en tramas (+) pequeñas y puede
bloquearlas en caso de colisión o error

L3 → Host tiene **DIRECCIÓN IP** que identifica dispositivo en Red

L3 → Red / Internet - crea Datagrama Ethernet
Mediante Ruteo, el router elige el mejor camino x el
cuál se enviará el paquete IP según tabla de
enrutamiento (almacena rutas a (+) routers de red)

L4 → Transporte
Soporta comunicación entre (+) dispositivos y (+) redes
Responsable de transferencia extremo a extremo
Usa puertos pl direccional paquetes

3 servicios

- Segmentación : divide datos en bloques
- Reensamblaje : reensambla segmentos al llegar a destino
- Multiplexación : identifica APPS o servicios y los vincula a puertos

2 protocolos

- [TCP → establece sesiones (+) ACK
(+ ACUSE DE REIBO)
- [UDP → rápido pero no asegura orden

L5-7

Aplicación /

Define y provee los servicios requeridos x el programa del usuario

Protocolos : Telnet, FTP, SMTP... .

Representa datos pl user \oplus codificación

TCP
~~~

vs.

UDP  
~~~

- ✓ orientado a la conexión
- ✓ emisor puede enviar múltiples paquetes antes de recibir ACK
- ✓ retransmite
- ✓ asegura orden paquetes
- ✗ \oplus lento

- ✓ no orientado a conexión (simplemente envia paquetes)
- ✗ no retransmite
- ✗ no asegura orden
- ✓ \oplus rápido

Ruteo

Estático \rightarrow

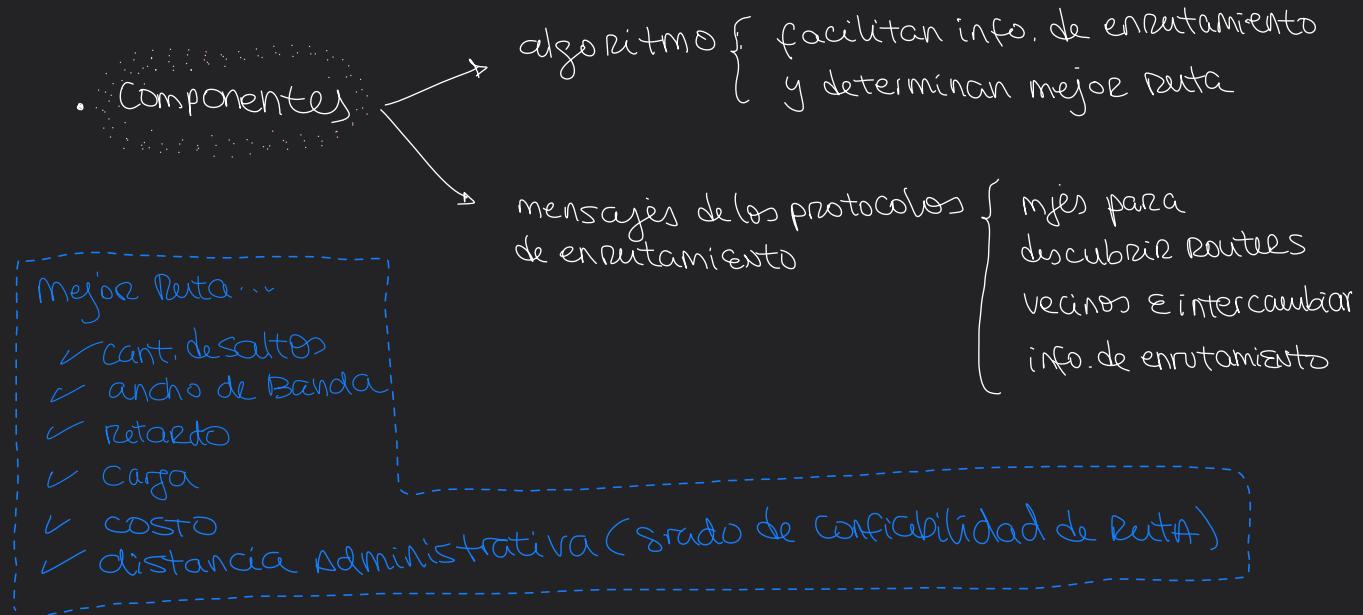
Tabla de enrutamiento (L3)
es config. manualmente x admin. de Red

No consume CPU ni ancho de banda
pero no es escalable \oplus seyta a errores de admin

Dinámico \rightarrow

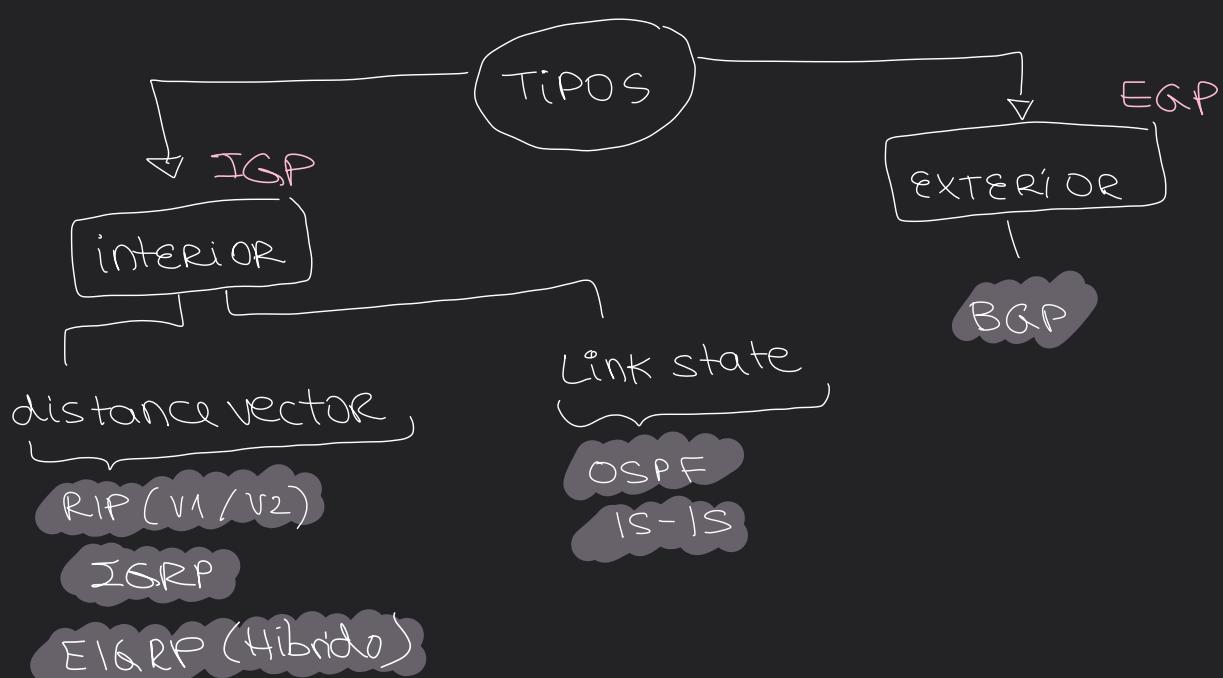
Tabla de enrutamiento config x protocolos
de enrutamiento dinámicos
selección de mejor ruta y mejor adaptacion a cambios

Protocolos de Ruteo Dinámico:



Ventajas vs. Desventajas

- | Ventajas | vs. | Desventajas |
|--|-----|--|
| <ul style="list-style-type: none">✓ adaptación a cambios de red✓ tolerancia a fallos✓ escalabilidad✓ equilibrio de carga✓ ing. de tráfico✓ prevención de bucles✓ convergencia rápida✓ reducción de tareas admin | | <ul style="list-style-type: none">✓ + complejo de config✓ (+) consumo de recursos (CPU y mem) - HW + potente✓ Usa ancho de banda pl. comunicación entre routers✓ Posibles riesgos de seguridad si no se configura bien✓ costo capacitación |



• Protocolos de enrutamiento gateway INTERIOR (IGP)

→ se usan para enrutamiento y comunicación dentro del mismo sistema Autónomo (AS)

↳ conj. de redes interconectadas a través de routers - organizan internet

1) Vector de distancia :



- * RIP, ISGRP, EIGRP
- * routers se anuncian como vectores
- * mejor camino se calcula x cantidad de saltos
- * no construye mapa topológico
- * actualizaciones periódicas
- * misma tabla de ruteo

: RIPv2 : comparte info. de sus tablas completas cl sus vecinos y se actualiza con vecinos cl 30"

cuenta con mecanismos de prevención de bucles :

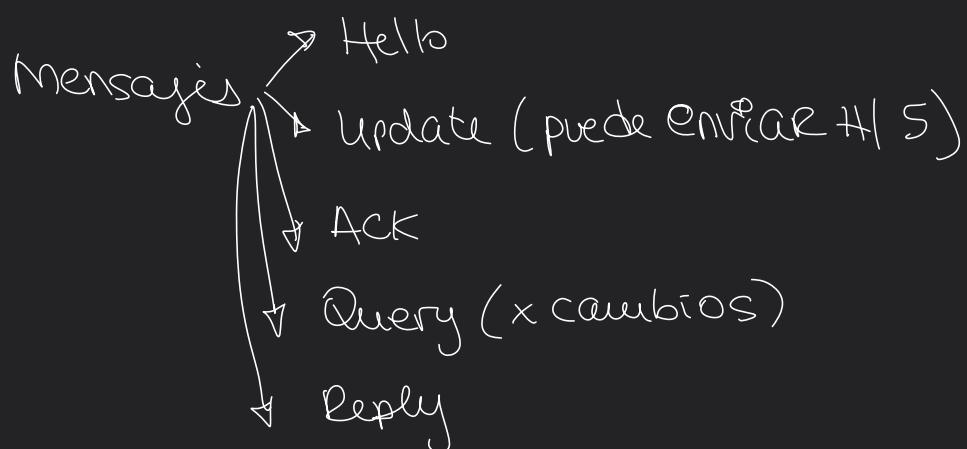
- { Split Horizon : no puede anunciar una ruta al vecino x el cual CONOCÍ ESA RUTA
- { Route Poisoning : cuando una red se convierte en inalcanzable se genera actualización cl métrica ∞ (160+)

Poison Reverse : Router anuncia la red como inalcanzable hacia router que le anuncio esa ruta - rompe split horizon .

• EIGRP: Es sucesor de IGRP (en desuso) - Cisco

Al habilitarlo se envía "Hello" cada 5 segs

Solo actualiza nueva red que se agregó o la red que se spitió en una actualización limitada



2) Estado de Enlace

- * creavista completa de la topología de red
- * actualizaciones no son periódicas
- * Algoritmo de Dijkstra (SPF)
- * Necesitan Θ memoria / procesamiento / ancho de banda p/ intercambio de mjes & convergencia



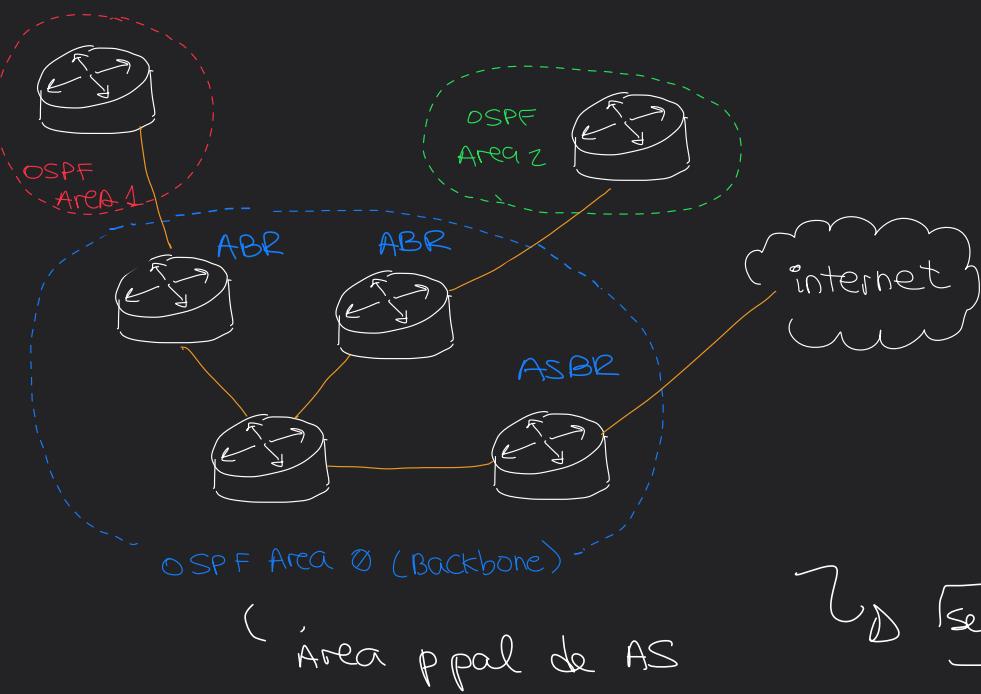
• OSPF: Open shortest path first - IETF '87

- Funciona con áreas
 - ↳ Área 0 o Backbone es obligatoria
 - ↳ otras áreas se conectan a 0
- No están fácil de configurar como EIGRP / RIPv2

Pasos:

- ① Descubre a sus vecinos y completa DB de adyacencia
- ② c/ router crea su propio LSP (paquete de estado de enlace) con info de sus interfaces y vecinos
- ③ Combina + LSP para mapa topológico
- ④ Corre algoritmo de Dijkstra sobre mapa topológico para crear Tabla de enrutamiento

- Se basa en costo total de la ruta & Ancho de banda para calcular mejor camino
- c/ router OSPF transmite info. sobre sus Rutas + costos que escuchó de vecinos
- los tipos de mensajes OSPF: Hello, descripción de DB (DBD), solicitud estado de enlace (LSR), actualización de estado de enlace (LSU) y ACK.
- se usa en Redes + grandes xq al ./ la red en áreas y correr OSPF evitamos tablas de enrutamiento $\Rightarrow \uparrow$ Escalabilidad
- Comparado con RIP v2 - converge + rápido ante cambios en topología de red debido a su actualización incremental de la DB del estado de enlace



- ABR: Área border router (El / Áreas)
- ASBR: AS Border router (El mire e internet)

↑ maneja cl 3 DB

• Protocodos de enrutamiento gateway exterior (EGP):

→ Se usan para el enrutamiento entre los sistemas autónomos

• BGP: Border Gateway Protocol

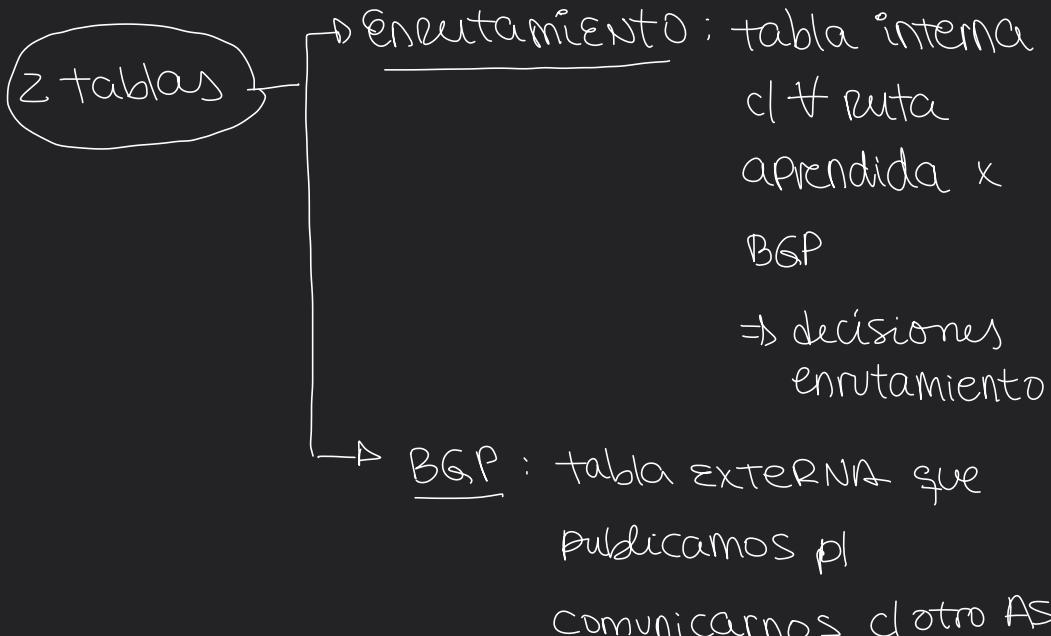
Protocolo que conecta varios AS que calcula mejor camino usando Atributos (no métricas)

(ej: ignorar la ruta cuyo siguiente salto es inaccesible / prioriza AS-Path más corto)

Necesita protocolo de ruteo subyacente (ej: OSPF) para tabla de enrutamiento -

-]- Cómo funciona:
- 2 routers vecinos usando BGP se comunican x TCP
- Son BGP neighbors
- Luego de establecer sesión x TCP, se intercambian full BGP table
- cambios se disparan x triggers

-]- Atributos BGP (*):
 - 1) Well Known:
 - obligatorios pl procezar & enviar
 - 2) Optional:
 - Transitivos NO
 - AS-Path
 - Next-Hop
 - Origin
 - Local Preference
 - (...)



- 4 mensajes
 - OPEN (establecer vecindad)
 - UPDATE (intercambio prefijos)
 - KEEPALIVE (cl 60" auto.)
 - NOTIFICATION

Redes WAN :

- Las redes WAN son aquellas que se extienden x área extensa
- (Capa 2) - Brinda tecno- necesarias p/ cubrir grandes DISTANCIAS & lograr las conexiones físicas

- MPLS →
- utilizada x proveedores de internet
 - Multiprotocol label switching (Protocolos de capa 2.5)
 - Marco de trabajo que agiliza enrutamiento basándose EN ETIQUETAS de relevancia local
 - Proceso de router seleccionando best path
 - x tabla de enrutamiento es costoso EN ALMACENAMIENTO !
 - Dentro de red MPLS corren ⊕ protocolos de routing (tanto estáticos como dinámicos)
 - Oculta info de L3 a proveedor de SVC
 - Routers ya no MIRAN la tabla de enrutamiento ⇒ MIRAN ETIQUETAS y decisión deja de ESTAR en capa 3 (pasa a 2.5)

- FEC : clase de equivalencia de reenvío
grupo de prefijos cl la misma ruta
- LSP : camino computado x ETIQUETAS
Ruta salto a salto ⊕ ETIQUETAS para llegar a destino

Protocolo de intercambio de labels

Hace mapeos de label a destino

vs. LSP
(label switched path) que es el camino switchado de los labels

• Pasos:

- 1) Antes de entrar a la red MPLS, Router de BORDE le **ASIGNA UNA ETIQUETA A PAQUETE IP**
- 2) El Router mira su tabla de enrutamiento y **ASOCIA PREFIJOS (direcciones IP)** a **ETIQUETAS**
- 3) Con **LDP** (label distribution protocol) los vecinos se **INTERCAMBIAN LAS ETIQUETAS** y se crea **LIB** (label info. base), DB que relaciona **ETIQUETAS** a **PREFIJOS**
- 4) LIB + tabla de enrutamiento (RIB) = **LFIB** (label forwarding info. base) que indica **QUE ETIQUETA USAR PARA LLEGAR A DESTINO**
- 5) Antes de salir de red MPLS, Router de borde le **SACA LA ETIQUETA A PAQUETE**

VPN: Tunneling + Encryption

- Enlace PPP: point-to-point protocol es un protocolo de capa 2 que establece una conexión directa entre 2 nodos de la red
- las VPN proporcionan la misma conectividad de red que un enlace PPP pero pueden pasar por un enlace de internet
 - ⇒ TECNO que permite realizar caminos virtuales en la red WAN

- incluyen
 - Autenticación
 - integridad
 - confidencialidad
- } forma de ,
comunicación
segura !



- Site-to-Site
- conectan sucursales corporativas / vinculan a clientes, proveedores o partners sobre una infra pública

- Remote Access
- conectan a usuarios remotos a EMPRESA .

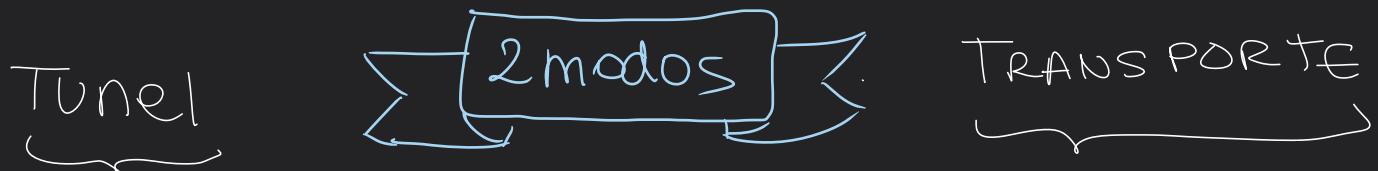
- Engral: Usamos internet para hacer conexión y creamos túnel VPN p/ que viaje info.
 - ✓ barato
 - ✓ flexible
 - ✓ conexión desde + lado
- utilizan IKE (internet key EXCHANGE) como protocolo de gestión de llaves y negociación de parámetros de seguridad en una conexión IPsec .
- IPSec: framework de seguridad comúnmente utilizado c/ VPNs que asegura las comunicaciones conj. de protocolos en capa 3

(si encriptado) \Rightarrow Usa 2 protocolos principales

- \rightarrow AH (Authentication Header)
- \rightarrow ESP (Encapsulating Security Payload)

AH: provee autenticación e integridad pero no confidencialidad (cifrado). Transporta datos en texto plano y valida origen - garantiza no-modificación de datos
(protección débil \oplus problemas con NAT)

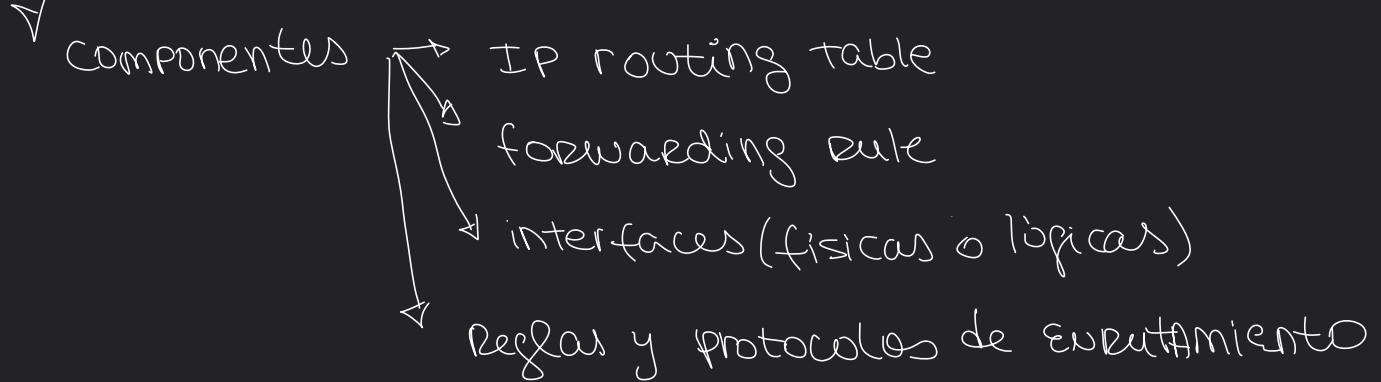
ESP: servicios de AH \oplus cifrado. Encapsula datos a ser protegidos



- Provee seguridad para todo el paquete IP (encripta \neq el paquete)
- P/I proteger tráfico entre 2 redes
- Encripta solo los datos (payload - ~~entero~~ paquete)
- NO Toca Header IP
- P/I proteger tráfico entre 2 hosts

VRF:

- Virtual Routing & Forwarding
- Técnica que permite tener instancias de ruteo múltiples y separadas funcionando en simultáneo en 1 dispositivo
- Router virtual que permite crear UPNs en misma infra — MPLS nos permite definirlo vía labels.



∴ En contexto de Redes de proveedores de servicio (WAN)
que usan MPLS ...

L VRF permite implementar MPLS L3 VPNs
que permiten a proveedores ofrecer servicios de red privada a múltiples clientes sobre infraestructura compartida

~~~~~ paso a paso ~~~~

① Routers (CE routers) del cliente → (PE routers) Routers de Borde de proveedor  
conexión

⚠ Tanto PE routers como P routers (routers centrales del proveedor) son label switching routers ⇒ MPLS

② En Routers PE se configuran instancias VRF para el cliente x separado ⇒ Aislado Ruteo

③ Info. de ruteo de los clientes se aprende en los PEs y luego se redistribuye el (los) PE de la red vía BGP

multiprotocolo (que soporta las direcciones VPNv4)



Prefijos de cliente  
únicos en MPLS  
del proveedor  
incluso si IP  
solapada



dirección IPv4  
del cliente



Route  
Distinguisher

- ④ Tráfico ingresado en PE se clasifica al FEC  
y se le imponen etiquetas MPLS
- ⑤ P routers intermedios reenvian tráfico solo viendo  
la etiqueta sin examinar header IP del cliente
- ⑥ Egress PE elimina etiquetas antes de enviar  
paquete a red del cliente de destino.

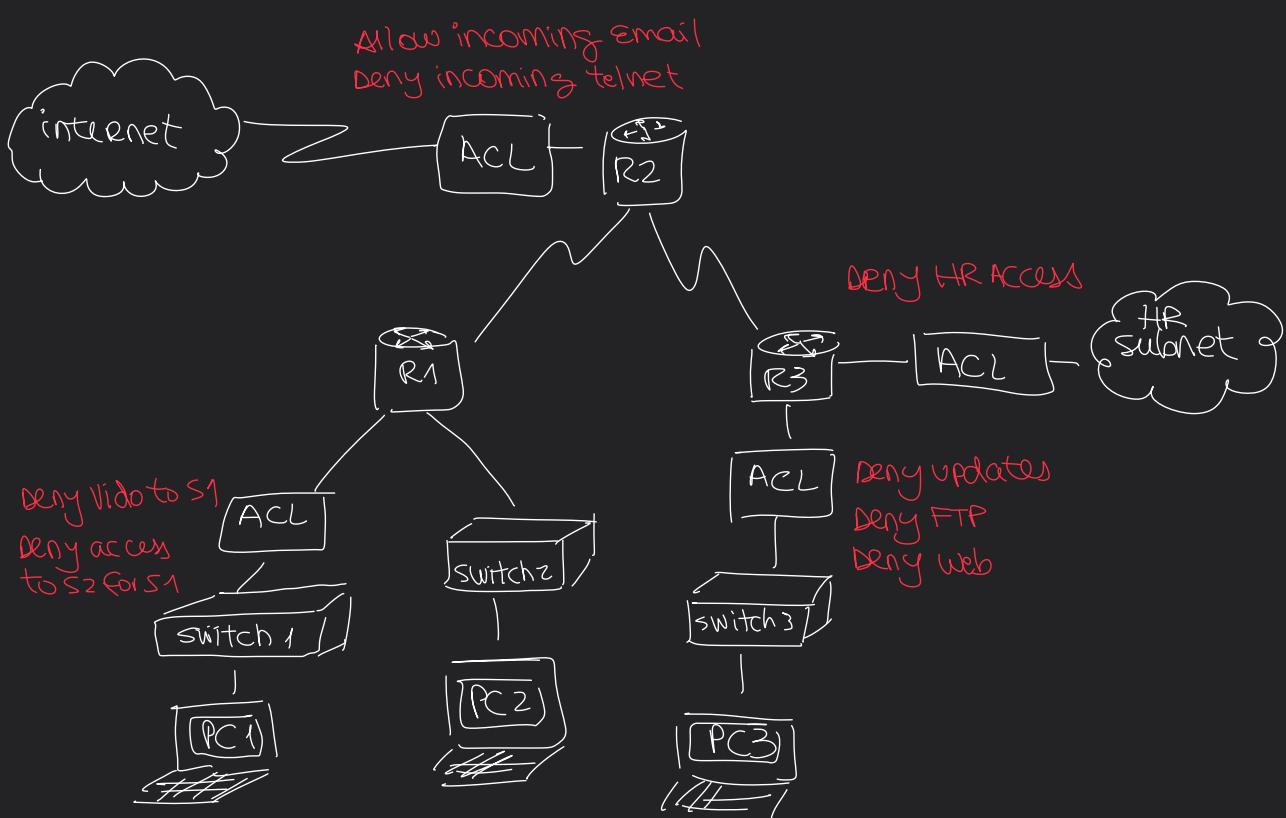
En resumen:

- VRF en los PE mantienen separación lógica  
de las redes de los clientes
- MPLS proporciona mecanismo de transporte  
eficiente y basado en labels a través  
de red central del proveedor
- Routers CE no necesitan participar en  
BGP ni MPLS de proveedor.

ACLs:

→ listas dentro de los routers para controlar acceso a red

- Cryptomap: en IPsec, refiere a una configuración que realiza 2 funciones
  - selecciona el tráfico a proteger
  - define las políticas para este tráfico y los "crypto peers" (los otros dispositivos con los que se establece la VPN)
- ACLs son parte central del Cryptomap ya que seleccionan tráfico que será protegido por criptografía ⇒ crypto ACLs
- Son stateless ⇒ no van a ver el contenido del paquete para tomar una decisión sobre si RECHAZARLO o ACEPTARLO
  - ~~~~~
  - Solo tiene en cuenta dirección IP de origen y destino
  - ⊕ puertos



# Redes LAN :

- Ethernet:
  - Tecnología de L1 y L2 estándar de redes LAN p/ transmisión de datos
  - Define estándares p/ los cables, conectores y protocolos
  - Capa 2 → se encarga del control de enlace lógico (LLC) que maneja comunicación con capas superiores y el SW de red + capa MAC que maneja la encapsulación de datos y el control de acceso al medio
  - Trama ethernet usa direcciones MAC
  - Comunicación
    - UNICAST : comunicación normal host a host
    - BROADCAST : envío a todos los hosts de la red
    - MULTICAST : envío a grupo seleccionado de host

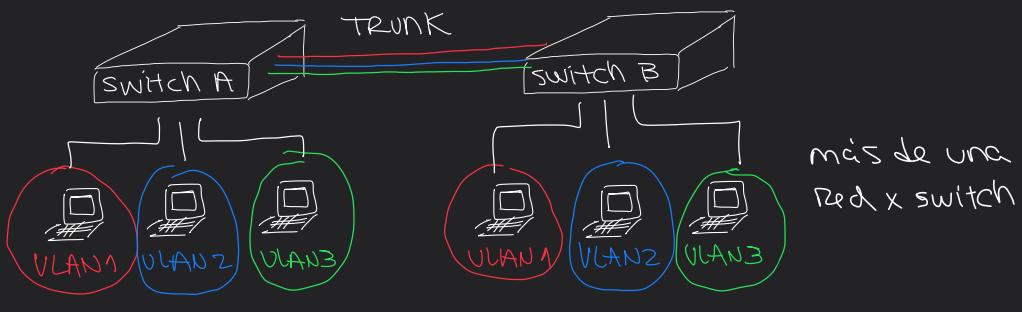
- Switch:
  - Dispositivos Capa 2 que interconectan dispositivos cableados de red LAN y reenvía tramas entre ellos
  - Usan direccionamiento MAC - c/ switch contable MAC
  - Ordenan la comunicación, habilitan interconexión y entre redes
  - Factores de forma → switch de config fija
    - switch modulares
    - switch de config aplicable
  - Resuelven colisiones : switch como centro de red (LAN) hace que c/ computadora tenga su propio dominio de colisión

## STP:

- Spanning Tree Protocol — Capa 2
- Se usa entre switches para eliminar loops ; Permite que dispositivos de interconexión activen / desactiven Auto, enlaces de conexión
- Designa un switch como Root y crea un árbol con menor cantidad de enlaces a un nodo  $\oplus$  Bloquea puertos redundantes
- Mensajes BPDU

## VLAN:

- Método utilizado para dividir una red física en varias redes lógicas en redes LAN
- Permiten que un grupo de dispositivos se comuniquen como si estuvieran conectados a misma red física  $\oplus$  evita que VLANs de un mismo switch accedan a la misma info
- switch etiqueta las VLANs con tags (vía protocolo 802.1q) y el tráfico se transporta x trunk ports.



## NAT:

→ Técnica utilizada para traducir direcciones IP privadas a públicas y viceversa (ej: para salir a internet)

→ Multiples dispositivos de red privada pueden usar misma public IP

→ Se implementa en dispositivos de borde (firewalls o routers)

- TIPOS
- estático: Admin de red asigna manualmente una dirección IP pública fija
  - Dinámico: Router de borde asigna auto. una dirección IP pública temporal disponible en un pool de direcciones

PAT (port access translation) o NAT overload:

permite q' multiples direcciones locales internas se traduzcan a única IP pública y q' conexión se diferencie x puerto.

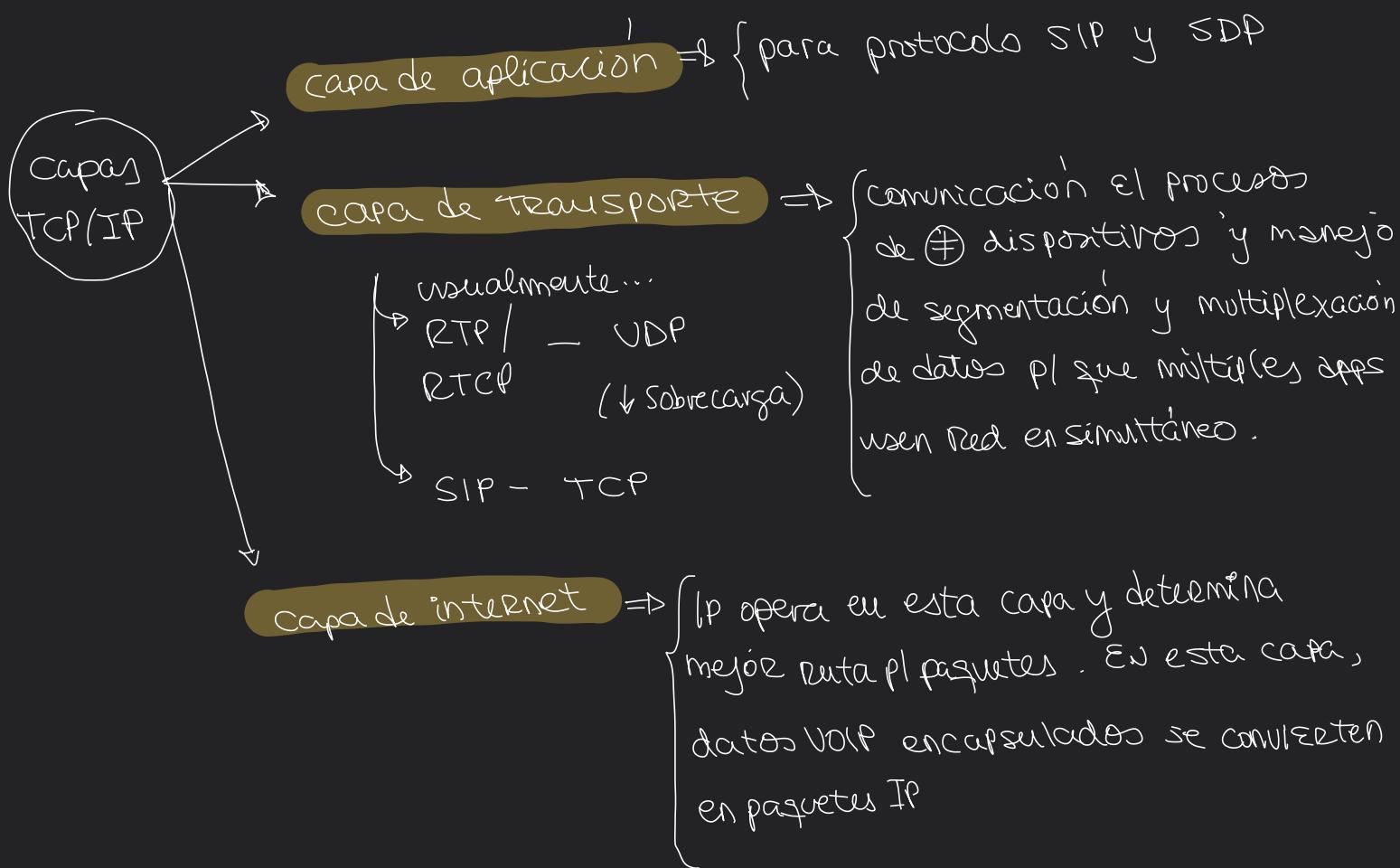
## VoIP:

→ Sistema que permite transportar voz sobre IP

→ sensible a calidad de red ⇒ cantidad de llamadas simultáneas x ancho de banda

- Protocolos
- SIP (session initiation)  
(protocolo de señalización)  
se establece, gestiona y finaliza llamadas  
sus direcciones usan formato URL similar a un email
  - SDP (session description)  
(protocolo de definición)  
se usa para negociación de la capacidad de los participantes - descripción de la sesión y los medios
  - RTP (real-time transport)  
⊕ RTCP (control)  
(protocolo de intercambio)  
maneja flujo de datos  
suele usar UDP

- Codecs: definen cómo se comprime y descomprime la voz  
paquetización del audio - Transfiere señales analógicas a digitales y viceversa



- Quality of Service (QoS): medio utilizado pl proteger y priorizar tráfico crítico e importante

Manejando bandwidth para dar performance deseada — controlar delay, pérdida de paquetes y jitter

ideal < 30ms para conexión aceptable

Variación del retardo / latencia El  $\oplus$  paquetes consecutivos pertenecientes a misma comunicación

Ocurre cuando paquetes no arriban a intervalos regulares o lo hacen fuera de orden

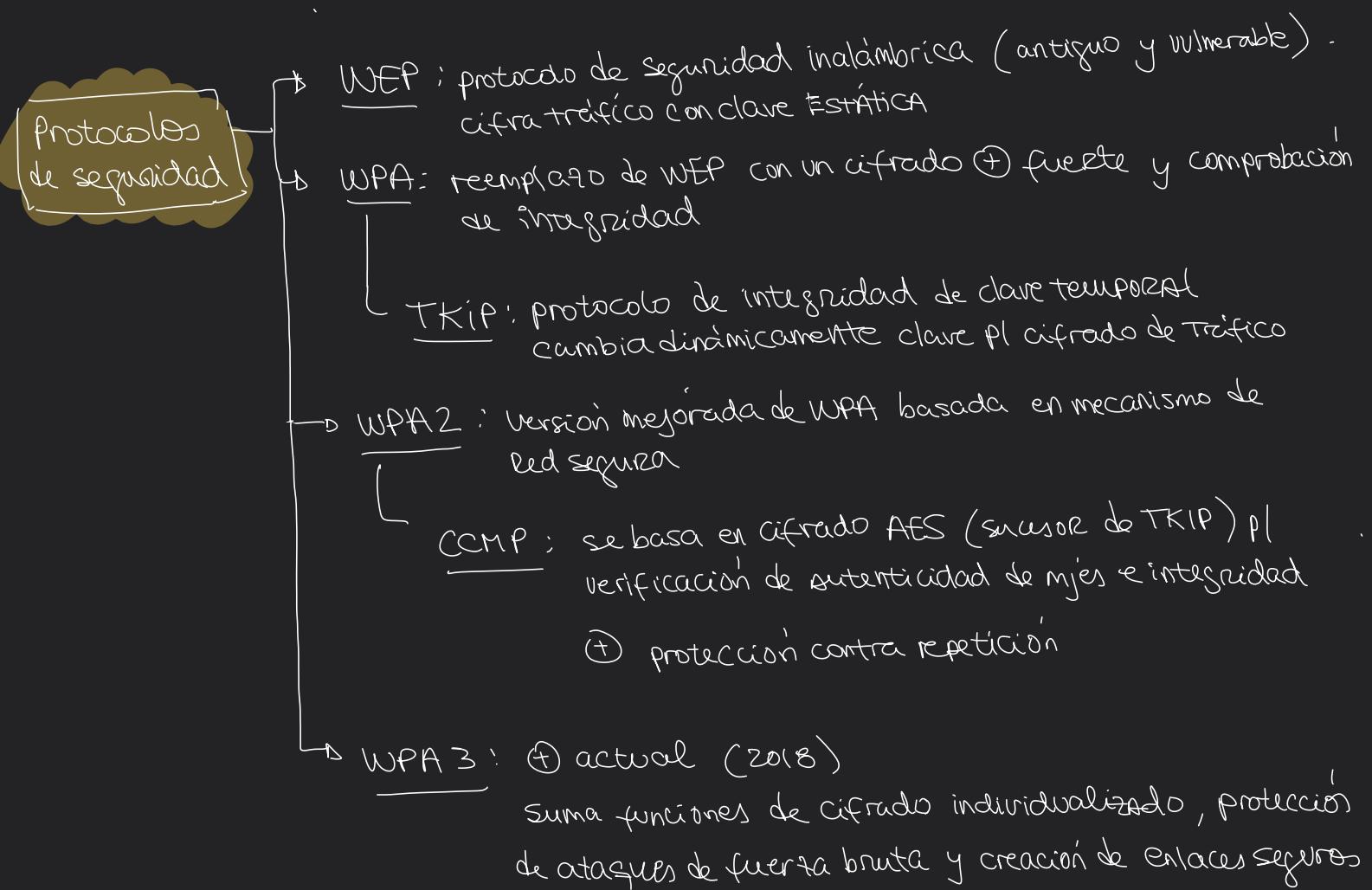
Pros VoIP: ↓ costo que cable dedicado

↓ desperdicio bandwidth

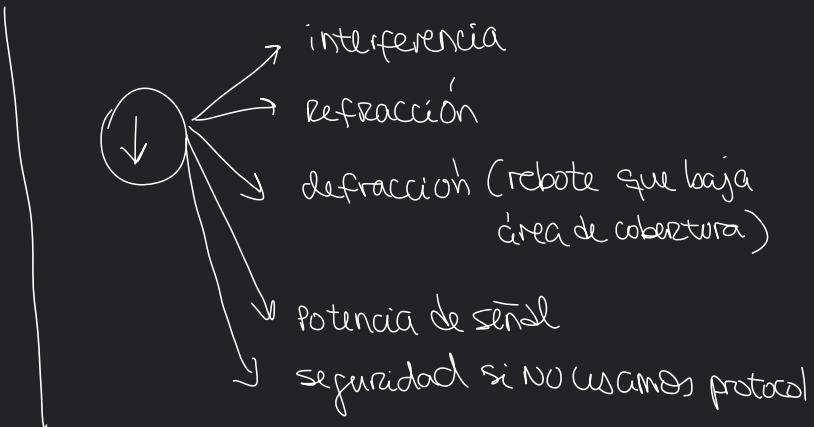
Cons VoIP: ↑ latencia  
↑ limitado BW  
↑ pérdida paquetes  
↑ jitter  
↑ eco

# Wifi:

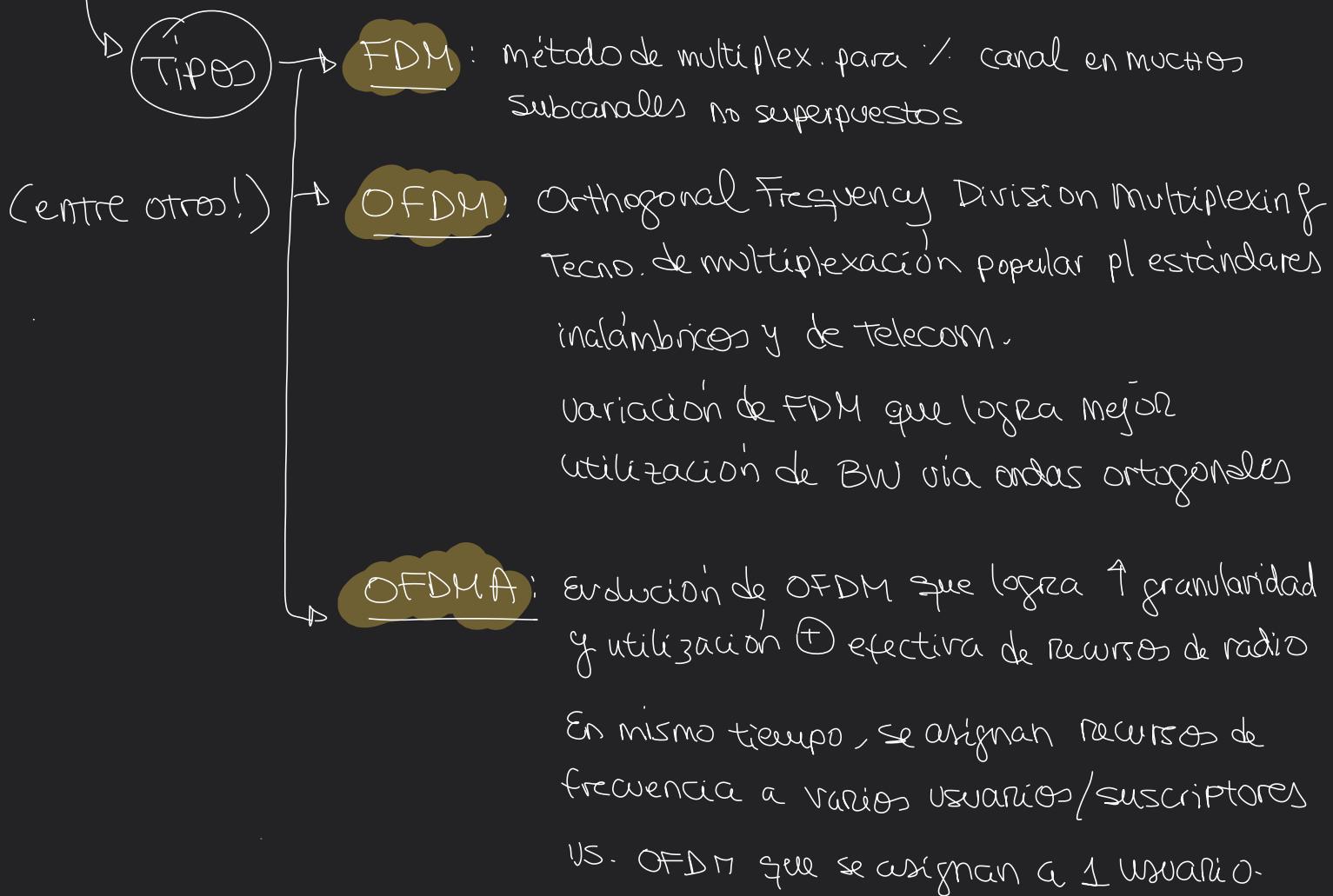
- Estándar de red inalámbrica que permite conexión a INTERNET
- Utiliza métodos de acceso al medio antes de transmitir datos
- Transmisión X onda de radio ⇒ fácil interceptar DATOS



① → conexión inalámbrica  
accesibilidad  
escalabilidad  
ahorro costos de cableado



• Multiplexación:   
 Combinación de varios canales de comunicación en un solo medio de transmisión  
 Objetivo: Varios usuarios compartiendo único enlace



### \* DHCP:

Dynamic Host Config. Protocol — se utiliza para config. de parámetros de red en dispositivos cliente

Permite configurar pools de direcciones IP que serán asignadas a clientes → Especificar

{ red (network)  
 router x defecto (default-router)  
 Servidor DNS (dns-server)

→ Sistema para traducción de nombres

## HTTP :

protocolo de capa de aplicación que típicamente interactúa con servidores web

Utiliza servicios de capa de Transporte (TCP)

