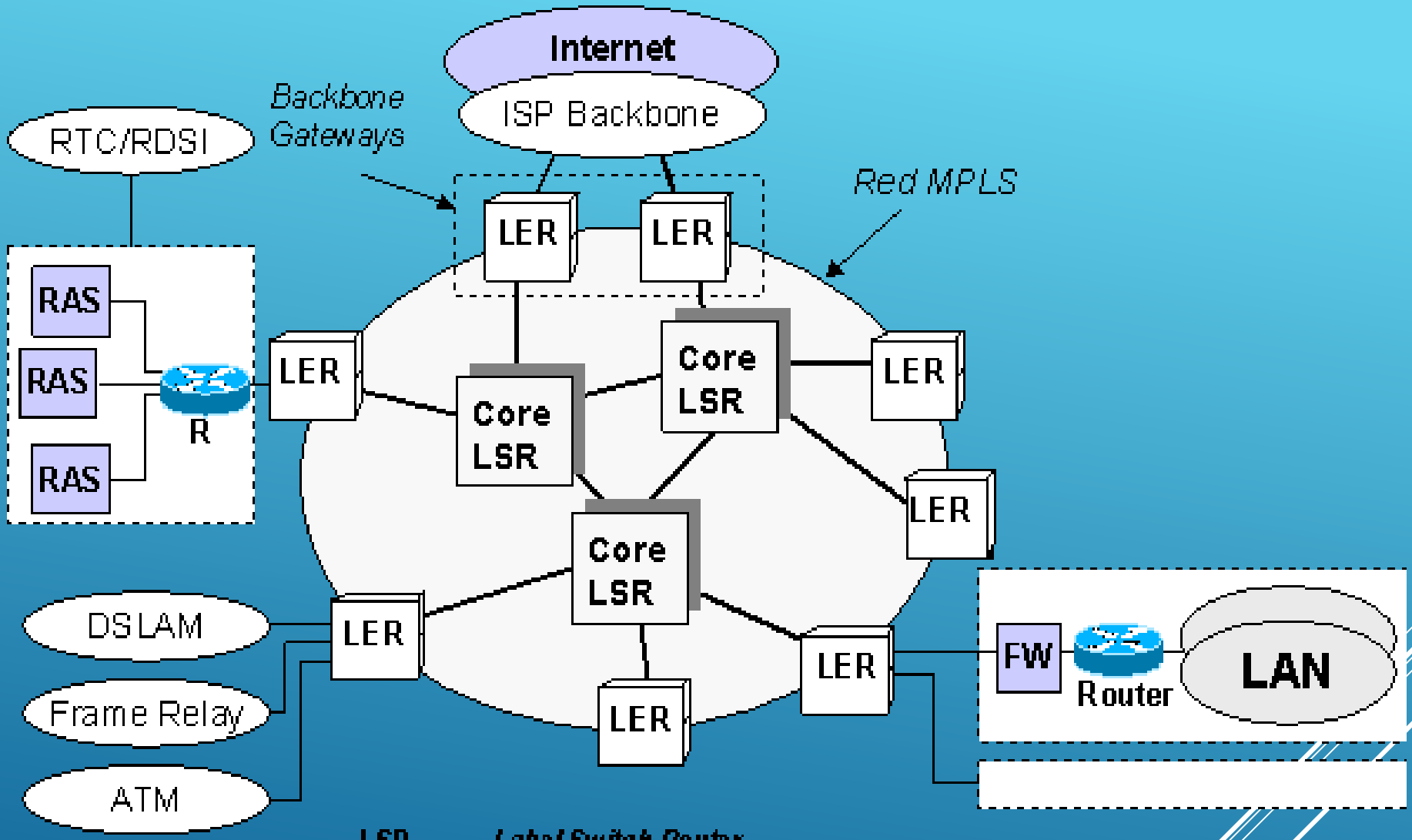
# MPLS

## MULTIPROTOCOL LABEL SWITCHING

# INTRODUCCION

MPLS es una tecnología de conmutación de datagramas basada en etiquetas (labels) que tuvo su origen en la combinación de IP y ATM en una única tecnología (tag switching).




| | |
|---|---|
| **LSR** | ***Label Switch Router*** |
| **LER** | ***Label Edge Router*** |
| **RAS** | ***Remote Access Server*** **(dial-in)** |
| **FW** | ***Firewall*** |
| **DSLAM** | ***Digital Subscriber Line Access Module*** **(ADSL)** |

Es la Integración de los Niveles 3 y 2 del modelo OSI, o sea un protocolo “Ruteable” ( IP ) y uno de “Enlace” ( ATM )

# IP

- *No orientado a la conexión.*
- *Sin control de flujo extremo a extremo.*
- *Sin recuperación de error.*
- *Sin calidad de servicio.*

# ATM

- *Orientado a la conexión.*
- *Apto servicio sincrono.*
- *Apto servicio datos.*
- *Diámetro de red ilimitado.*
- *Tasa de bits garantizada.*
- *Con calidad de servicio.*
- *Servicio sin colisión.*
- *Gran ancho de banda.*

# SERVICIOS EN ATM
# MODO DE TRANSFERENCIA ASINCRÓNICO

| | Class A | Class B | Class C | Class D |
|---|---|---|---|---|
| **Characteristics** | Constant bit rate | Variable bit rate | Connection oriented data | Connection less data |
| **Synchronization between Source and Destination** | Required | | Not Required | |
| **Bit rate** | Constant | Variable | | |
| **Connection Type** | Connection Oriented | | | Conn. less |
| **Adaption Layer** | AAL 1 | AAL 2 | AAL 5 | AAL 3/4 |

# MPLS

Los routers del backbone de la red IP-MPLS no necesitan examinar la cabecera IP para tomar una decisión respecto al reenvío del paquete, sino que lo hacen a través de la **etiqueta** que lleva incorporado el paquete IP.

En MPLS la asignación de etiquetas a los paquetes IP se realiza de acuerdo con una gran variedad de criterios (interfaz/subinterfaz de acceso, dirección IP, puerto y protocolo).

# Características de MPLS

PROTOCOLO NO ORIENTADO A LA CONEXIÓN.

OFRECE CONTROL DE TRÁFICO (SEGURIDAD)

OFRECE CONTROL DE ANCHO DE BANDA

ADAPTABILIDAD DE CALIDAD DE SERVICIO

TIENE LA FACULTAD DE OPERAR CON CUALQUIER PROTOCOLO DE RED (IP, IPX, ETC.)

# MPLS

Crea circuitos virtuales, para unir redes distribuidas entre lugares físicamente distantes.

Estos circuitos virtuales se denominan LSP (Label Switched Paths)

# COMPONENTES DE MPLS

- **LSR (Label Switching Router):** son nodos internos de la red, analiza el label del paquete recibido y a partir de su tabla de ruteo interno, determina:
  - Camino a seguir (puerto de salida)
  - Nuevo label, que reemplazara al actual

- **LER (Label Edge Router**): son nodos que están en la periferia de la red, y son los que se unen a las distintas redes IP externas.

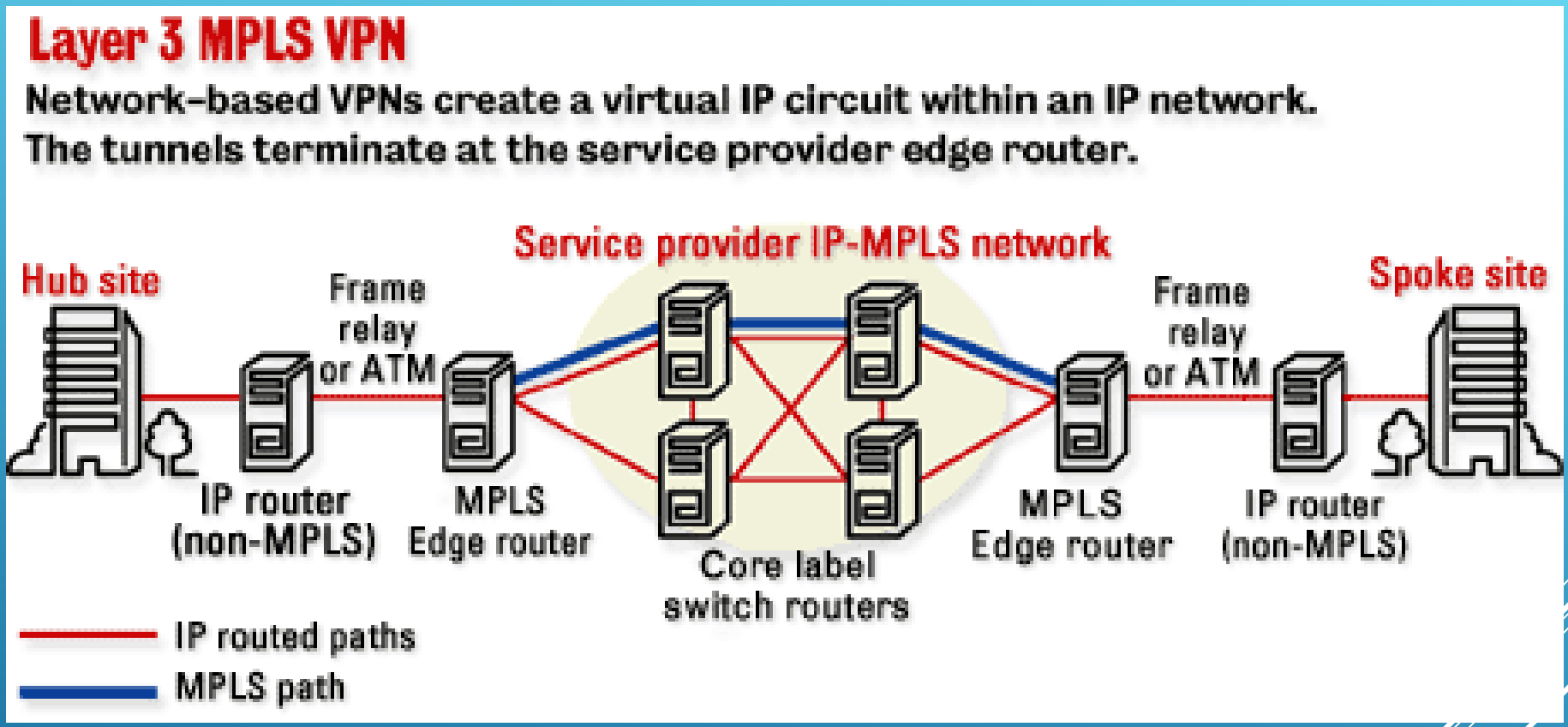
- **LSP**: son la concatenación de un LER de ingreso, una serie de combinaciones de LSR y finalmente un LER de egreso.

# COMPONENTES DE MPLS

- LER DE INGRESO: hace el mayor trabajo, este observa la dirección IP del paquete, entonces determina la ruta a seguir internamente asignando un LSP, y él agrega un label como encabezado

- LER DE EGRESO: simplemente remueve el label del paquete y se lo entrega a la red IP correspondiente

# TOPOLOGÍA MPLS




Topología clásica de una red IP distribuida interconectada a través de un VPN utilizando MPLS[12]

# CONCEPTOS BÁSICOS

- El único análisis de enrutamiento que se realiza en el router LER de ingreso. Los siguientes routers LSR o LER de egreso simplemente siguen el enrutamiento en base a los label y sus tablas internas.
- En MPLS, el label es usado para establecer la ruta, y por lo tanto no es necesario llevar información adicional sobre la ruta a seguir en cada paquete.
- El label asignado representa una combinación ***de enrutamiento, prioridad y calidad de servicio.***

# COMPONENTES MPLS (RESUMEN)

- Label Edge Router (LER)
- Label Switching Router (LSR)
- Forward Equivalence Class (FEC)
- Label
- Label-Switched Path (LSP)
- Label Distribution Protocol (LDP)

# MODO DE OPERACIÓN DE MPLS

- Creación de la etiqueta y distribución
- Creación de la tabla en cada router
- Creación de un label switched path
- Inserción de la etiqueta / lookup en la tabla
- Forwarding del paquete

# FEC - Forwarding Equivalence Class

- Trafico clasificado en el mismo FEC en un nodo sigue el mismo camino

- En forwarding IP convencional
  - El FEC viene determinado por el longest prefix match (*)
  - Cada salto reexamina y asigna el paquete a un FEC

– El nodo de entrada a la red (ingress router) hace la asignación de cada paquete a un FEC
– El FEC se indica mediante una etiqueta que viaja con el paquete
– En saltos siguientes no hay necesidad de identificar el FEC pues se tiene la etiqueta
– La etiqueta se emplea como índice en una tabla que especifica un siguiente salto y una nueva etiqueta
– La etiqueta que traía el paquete se sustituye por la nueva
– Reenvío MPLS no requiere que los nodos sepan procesar la cabecera del nivel de red (u otro protocolo encapsulado)

(*) La coincidencia de máxima longitud de prefijo es un algoritmo utilizado por los routers en la red de IP para seleccionar una entrada de una tabla de reenvío.

Como cada entrada en una tabla de reenvío puede especificar una subred, una dirección de destino puede coincidir con más de una entrada de la tabla de reenvío.

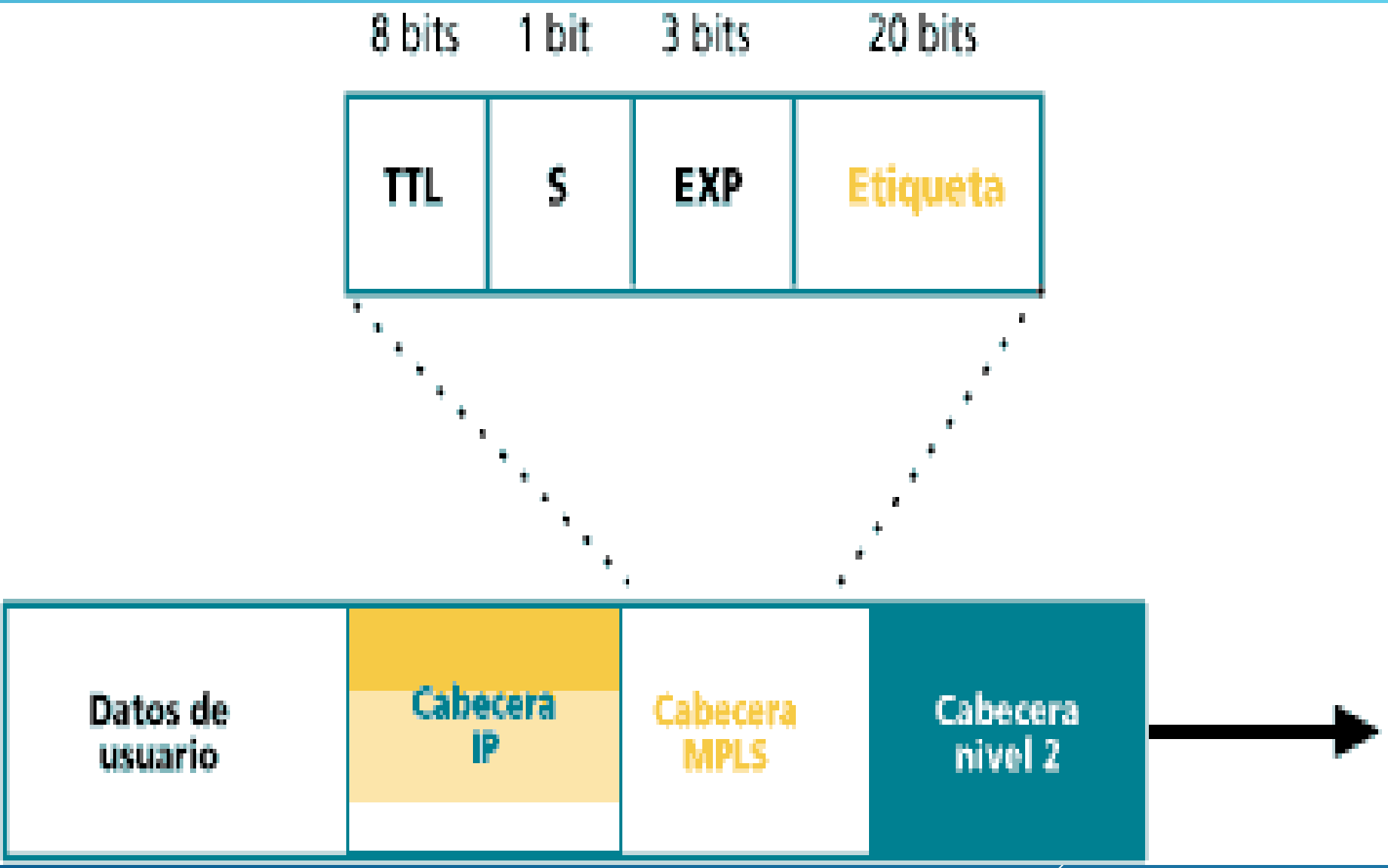
La más específica de las entradas de tabla coincidentes, ***la que tiene la máscara de subred más larga***, se denomina coincidencia de prefijo más larga. Se llama así porque también es la entrada donde el mayor número de bits de dirección principales de la dirección de destino coinciden con los de la entrada de la tabla.

Ejemplo, considere esta tabla de reenvío IPv4

192.168.20.16/28
192.168.0.0/16

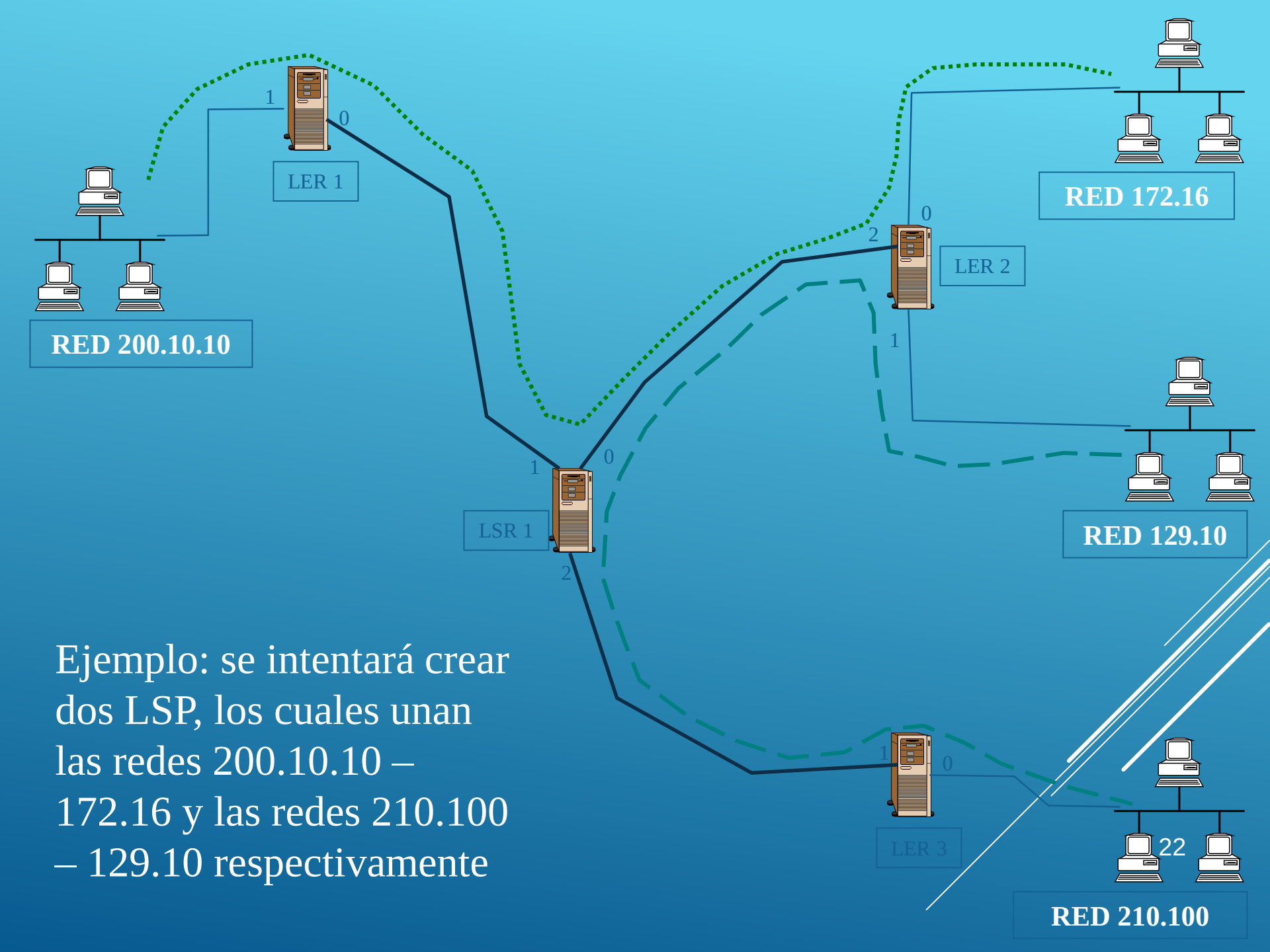
Se necesita buscar la dirección 192.168.20.19 , ambas entradas en la tabla de reenvío "coinciden".
Ambas entradas contienen la dirección buscada.
El prefijo más largo de las rutas candidatas es 192.168.20.16/28 , ya que su máscara de subred (/ 28) es más larga que la máscara de la otra entrada (/ 16), por lo que la ruta es más específica.

# ETIQUETA MPLS



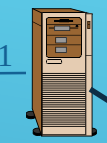
# CABECERA GENÉRICA MPLS Y SU RELACIÓN CON LAS CABECERAS DE LOS OTROS NIVELES

- **Los 32 bits de la cabecera MPLS se reparten en:**
- **20 bits para la etiqueta MPLS,**
- **3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS),**
- **1 bit de stack para poder apilar etiquetas de forma jerárquica (S),**
- **8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.**

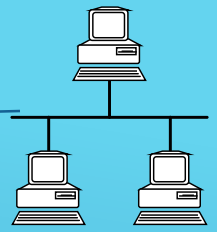



Ejemplo: se intentará crear dos LSP, los cuales unan las redes 200.10.10 – 172.16 y las redes 210.100 – 129.10 respectivamente

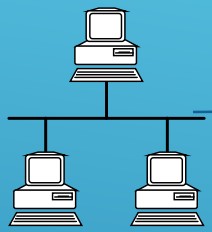
| TABLA RUTEO INTERNA | | | | |
|---|---|---|---|---|
| IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT |
| 2 | 9 | 172.16 | - | 0 |
| 2 | 10 | 129.10 | - | 1 |
| | | | | |




LER 1



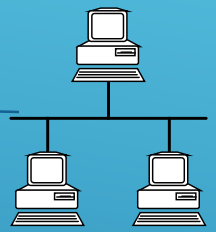
RED 172.16



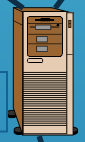
RED 200.10.10


LER 2

| TABLA RUTEO INTERNA | | | | |
|---|---|---|---|---|
| IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT |
| 0 | 21 | 200.10.10 | - | 1 |
| | | | | |
| | | | | |



RED 129.10



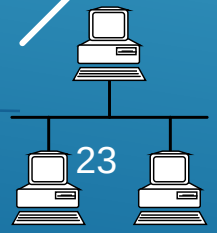

LSR 1

| TABLA RUTEO INTERNA | | | | |
|---|---|---|---|---|
| IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT |
| | | | | |
| | | | | |
| | | | | |

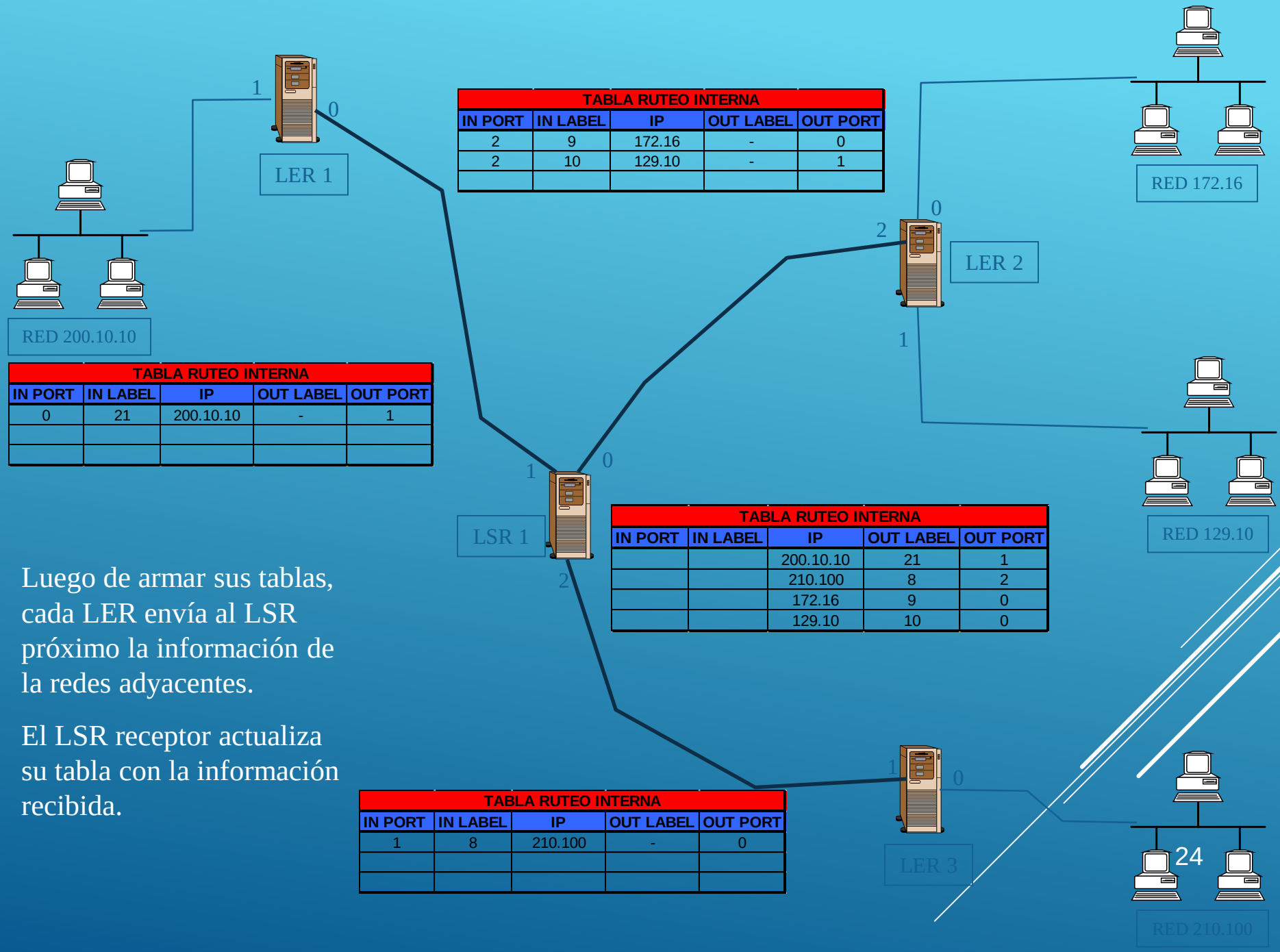
Al comienzo, cada red conectada a un LER es detectada por este, luego agrega un registro en su tabla interna por cada red

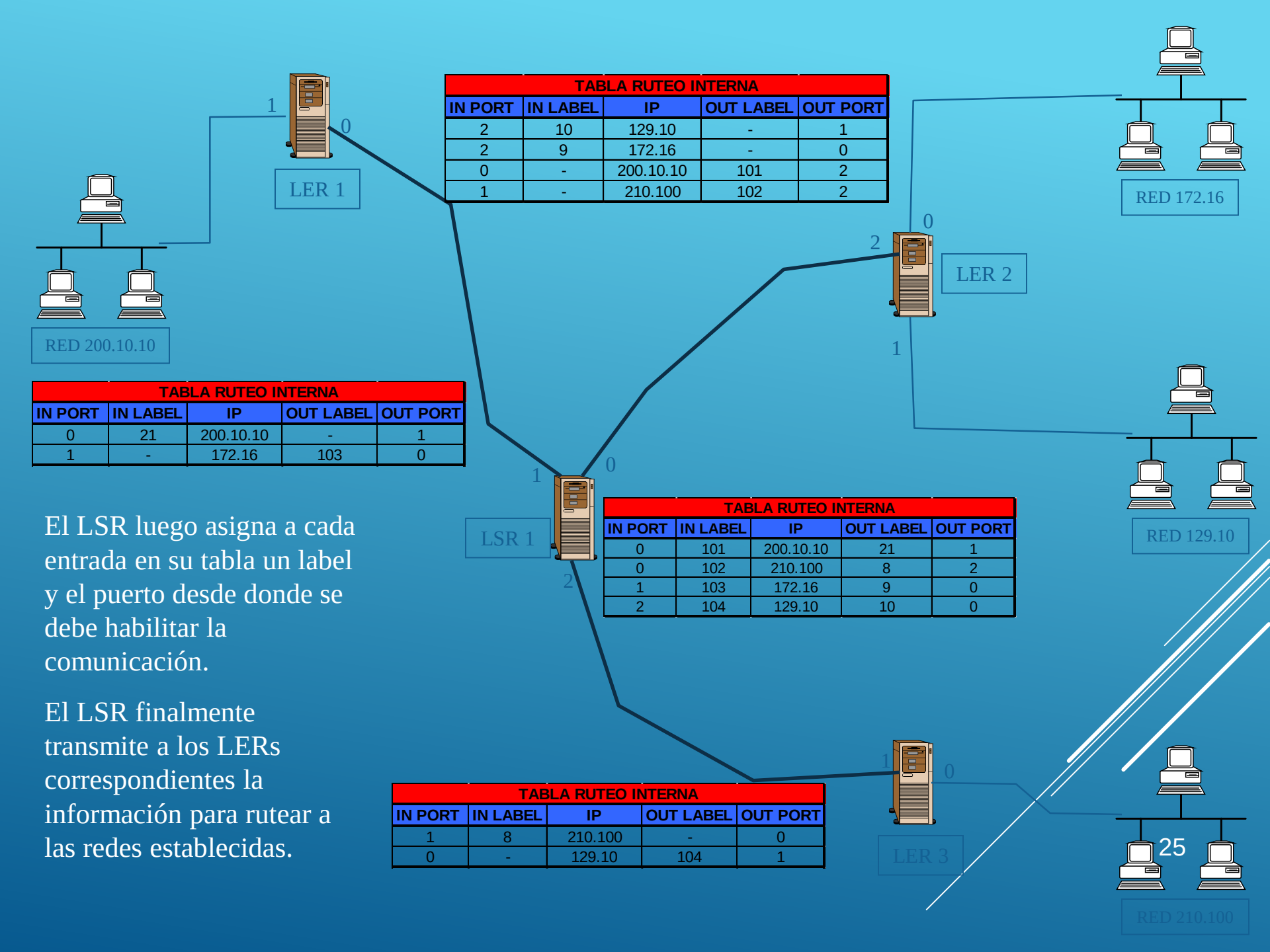
| TABLA RUTEO INTERNA | | | | |
|---|---|---|---|---|
| IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT |
| 1 | 8 | 210.100 | - | 0 |
| | | | | |
| | | | | |


LER 3

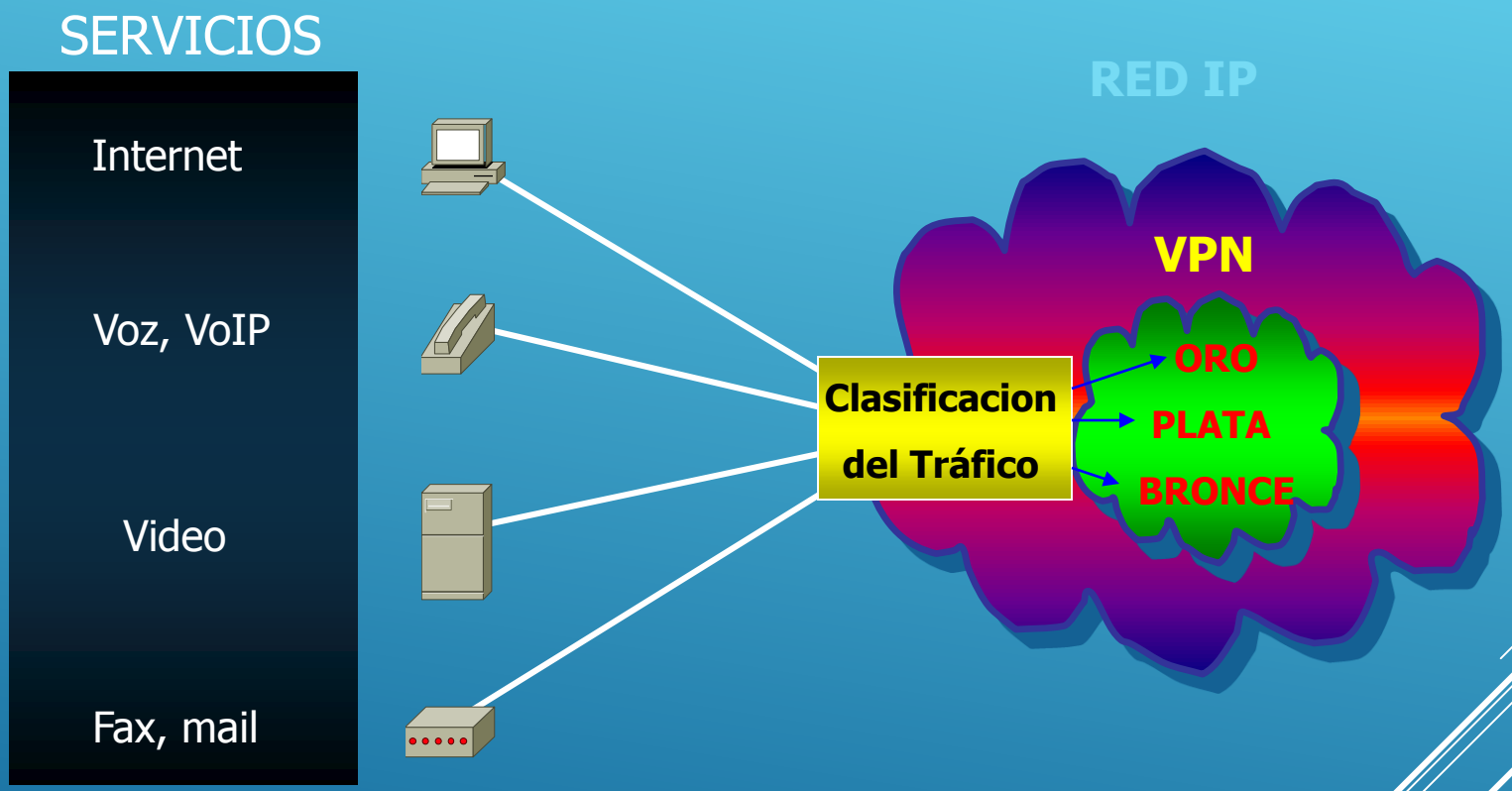


RED 210.100


1
0
LER 1
RED 200.10.10
TABLA RUTEO INTERNA
IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT
0 | 21 | 200.10.10 | - | 1
TABLA RUTEO INTERNA
IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT
2 | 9 | 172.16 | - | 0
2 | 10 | 129.10 | - | 1
0
2
LER 2
1
RED 172.16
RED 129.10
1
0
LSR 1
2
TABLA RUTEO INTERNA
IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT
200.10.10 | 21 | 1
210.100 | 8 | 2
172.16 | 9 | 0
129.10 | 10 | 0
Luego de armar sus tablas, cada LER envía al LSR próximo la información de la redes adyacentes.
El LSR receptor actualiza su tabla con la información recibida.
TABLA RUTEO INTERNA
IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT
1 | 8 | 210.100 | - | 0
1
0
LER 3
RED 210.100


1
0
LER 1
RED 200.10.10
TABLA RUTEO INTERNA
IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT
2 | 10 | 129.10 | - | 1
2 | 9 | 172.16 | - | 0
0 | - | 200.10.10 | 101 | 2
1 | - | 210.100 | 102 | 2
0
2
LER 2
1
RED 172.16
TABLA RUTEO INTERNA
IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT
0 | 21 | 200.10.10 | - | 1
1 | - | 172.16 | 103 | 0
1
0
LSR 1
2
TABLA RUTEO INTERNA
IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT
0 | 101 | 200.10.10 | 21 | 1
0 | 102 | 210.100 | 8 | 2
1 | 103 | 172.16 | 9 | 0
2 | 104 | 129.10 | 10 | 0
RED 129.10
El LSR luego asigna a cada entrada en su tabla un label y el puerto desde donde se debe habilitar la comunicación.
El LSR finalmente transmite a los LERs correspondientes la información para rutear a las redes establecidas.
TABLA RUTEO INTERNA
IN PORT | IN LABEL | IP | OUT LABEL | OUT PORT
1 | 8 | 210.100 | - | 0
0 | - | 129.10 | 104 | 1
1
0
LER 3
RED 210.100
25

# DONDE SE APLICA :



# Niveles de QOS :

1. **El mejor esfuerzo** ( IP, IPX, Apple Talk )

Este es aquel nivel de QOS que es propio de la capa 3 cuya función es la de hacer el mayor esfuerzo por entregar un paquete pero sólo especifica eso , no informa con respecto al BW, Delay, Jitter, etc.

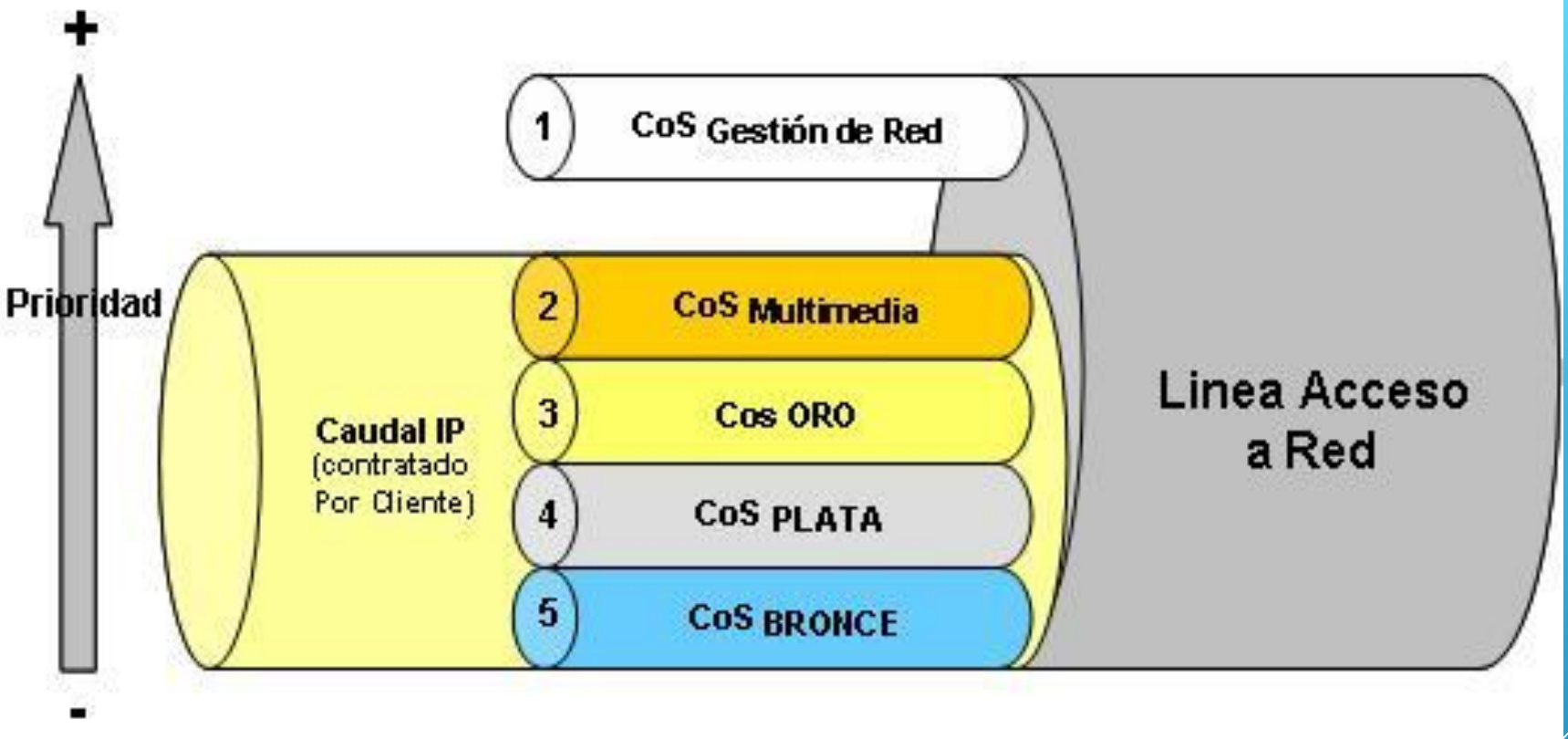
2. **Diferenciado - DIFFSERV** ( Primero, Clases, etc. )

En este nivel se le brinda un poco más al cliente, y es decir que en caso de congestión va a haber paquetes privilegiados, pero tampoco se puede garantizar nada.

3. **Garantizado** ( BW, Demora, Jitter )

En este nivel de QOS se puede especificar los parámetros de la calidad de servicio brindado, es el más serio y es el nivel más alto, es típico de ATM. ( Pero es el más caro. )

# CALIDAD DE SERVICIO




| Nº Co | Tipo Co | ToS | Descripcion de Clase de |
|---|---|---|---|
| 1 | Gestió | 6 | Tráfico Gestión: Gestión ED C's Red IP |
| 2 | Multimedi | 5 | Tráfico Multimedia: Voz Vide sobre IP |
| 3 | ORO | 3 | Tráfico Datos Alta Prioridad: SA , Base de |
| 4 | PLAT | 0 | Tráfico de Datos Estándar e |
| 5 | BRONCE | 1 | Tráfico Best : Datos Effort Internet. |

# QOS

| Parámetros QoS | Bronce | Plata | Oro | Multimedia |
|---|---|---|---|---|
| Pérdidas paquetes IP | - | X | X | X |
| Retardo ó Latencia | - | X | X | X |
| Variación de Retardo "Jitter" | - | - | - | X |

# DISPONIBILIDAD MENSUAL DEL SERVICIO

La Disponibilidad mensual del servicio corresponde al porcentaje de tiempo durante el cual el canal contratado está operativo y en correcto funcionamiento en un periodo de un (1) mes calendario. El tiempo es medido en horas.

$$\frac{\sum_{1}^{n}\left[\left(Ttot - Tnodisp_i\right)\right]}{Ttot} * 100$$

# *RETARDO DE TRÁNSITO (ROUND TRIP DELAY).*

- **El retardo de Tránsito Extremo a Extremo (RTD) es el tiempo de ida y vuelta (mseg) de un paquete de 100 bytes entre una sede origen y otra destino, pertenecientes a la misma VPN.**
- **Para cada una de las sedes pertenecientes a una VPN, el cliente deberá seleccionar una sede destino, es decir, la ruta sobre la que se realizarán las mediciones de los SLAs (Service Level Agreement) específicos (RTD, Perdida de Paquetes y Jitter).**

# JITTER Ó VARIACIÓN DE RETARDO.

- La Variación del Retardo o "Jitter" define con que regularidad llegan los paquetes al receptor. Un "jitter" muy pequeño indicaría que todos los paquetes llegan con un retardo muy similar (que puede ser bajo o alto, pero es más o menos constante), mientras que un "jitter" muy alto nos indicaría que las diferencias de retardo entre los distintos paquetes son considerables, es decir, unos paquetes llegan con un retardo muy bajo y otros con un retardo muy alto.
- El Jitter se expresa en milisegundos (mseg) y el periodo de observación es un mes de calendario.

| JITTER O VARIACIÓN DE RETARDO | |
|---|---|
| Calidad de Servicio | Valor de Jitter (%) |
| QoS Bronce | N/A |
| QoS Plata | N/A |
| QoS Oro | N/A |
| QoS Multimedia | < 30 mseg. |

# JITTER

- Parámetro muy importante para el tráfico Multimedia en Tiempo Real, pues las aplicaciones necesitan unas variaciones de retardo muy bajas, ya que mediante técnicas de "buffering" retrasan la reproducción de los flujos Multimedia precisamente en el valor estimado del "jitter" para asegurar con cierta certeza que van a poder reproducir la señal Multimedia sin cortes.
- Si un paquete llega con un retardo superior al "jitter" estimado, será descartado ya que no habrá llegado a tiempo para participar en la reconstrucción de la señal analógica real.

# PÉRDIDA DE PAQUETES

| Calidad de Servicio | Valor de Pérdida de Paquetes (%) |
|---|---|
| QoS Bronce | NA |
| QoS Plata | < 1 % |
| QoS Oro | < 1 % |
| QoS Multimedia | < 0,5 % |

# TIEMPO MEDIO DE REPARACIÓN MTTR

| Zona | Horas |
|---|---|
| Capital Federal y AMBA | 4 |
| Capitales Provinciales | 6 |
| Resto del País | 10 |

# TECNOLOGÍA DE LA RED

- Tecnológicamente, la red multiservicio es una red basada en tecnología ATM que permite el transporte de flujos de información Frame Relay y ATM.

# TECNOLOGÍA DE LA RED

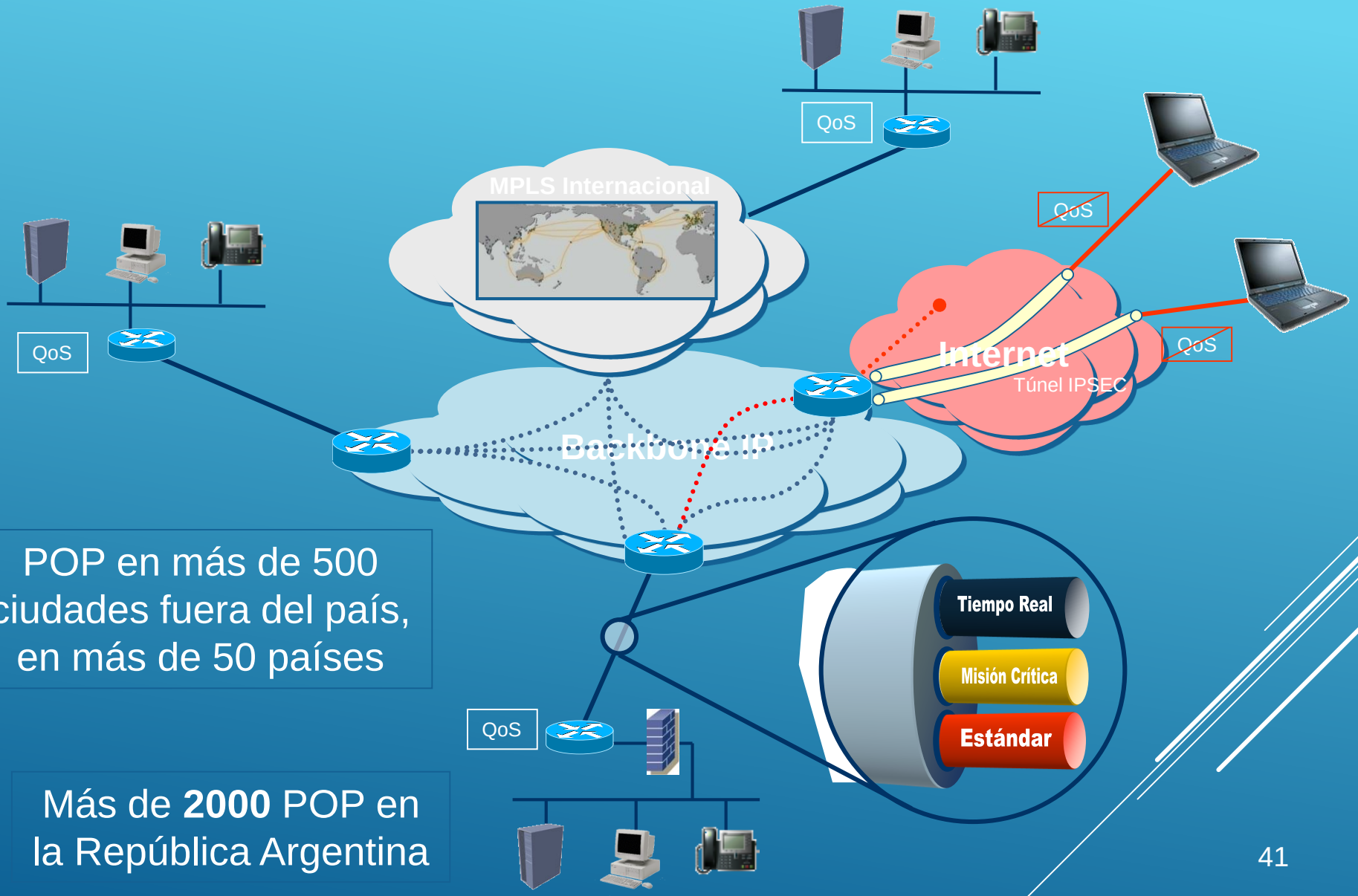
- La capa externa de acceso esta conformada por routers marca Cisco de las líneas ESR (10000), OSR (7600) y 7500. El core de dicha red, de conmutación exclusiva de paquetes MPLS, está formada por equipos de la misma marca, de la línea GSR (12000).
- La capacidad de conmutación instalada es de cientos de gigabits por segundo, con enlaces disponibles para entregar hasta veinte gigabits por segundo y capacidad de crecimiento de acuerdo a la demanda.
- Se puede acceder a esta red desde cualquiera de los nodos de la red multiservicio, extendiéndose su alcance a todo el territorio nacional.

# TECNOLOGÍA DE LA RED

- Los equipos de acceso a la red IP permiten la conexión de enlaces de cliente de entre 64 kbps y 622 Mbps en arquitecturas tipo WAN, y de entre 10 Mbps y 10 Gbps en arquitecturas tipo LAN. Los protocolos de acceso a la red que se pueden utilizar son todos los que permite el protocolo IP y la red multiservicio; por ejemplo: PPP, HDLC (Cisco), Frame Relay, ATM, IEEE 802.3.

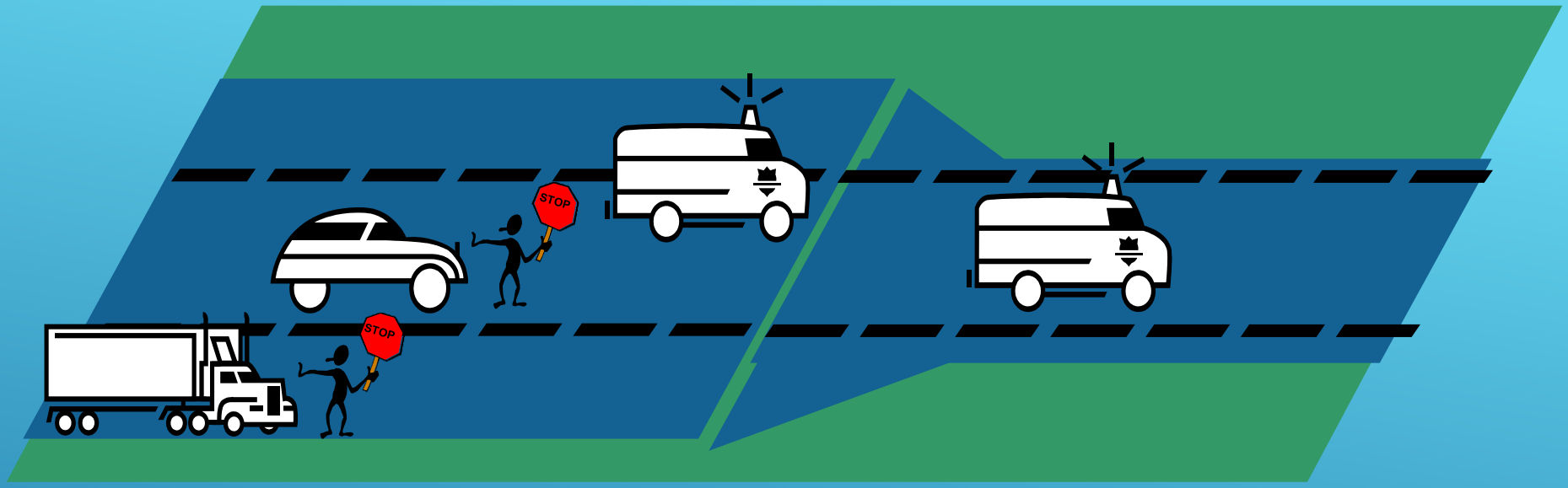
# VPN IP MPLS

# VPN IP MPLS – ESQUEMA




POP en más de 500 ciudades fuera del país, en más de 50 países

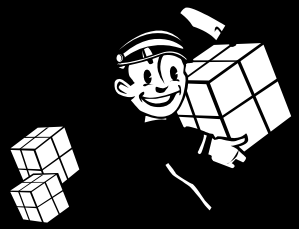
Más de **2000** POP en la República Argentina




Latencia (Delay)



Variación de la latencia (Jitter)



Tasa de pérdida de paquetes (Paquet Loss Ratio)


## Configuración del acceso en función de las QoS

%TR + %MC + %ES = BW Acceso [Kbps]

El precio del servicio será dependiente de esta configuración

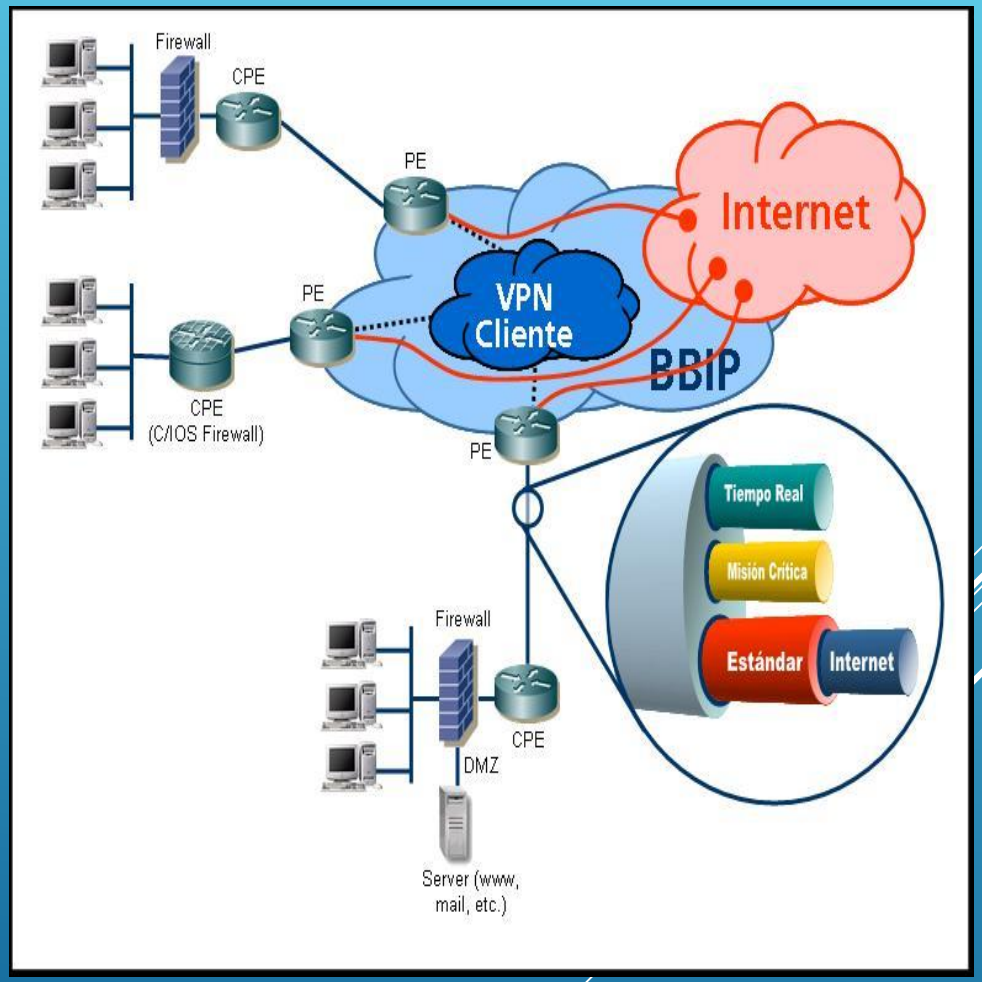
| QoS | Delay | Jitter | Packet Loss | Aplicaciones comunes |
|---|---|---|---|---|
| **Tiempo Real** | <60 mseg (Nac)<br><185 mseg (Int)* | <10 mseg (Nac)<br><20 mseg (Int)* | <0,30 % | Voz / Video Interactivo |
| **Misión Crítica** | - | - | <0,50 % | Aplicaciones corporativas (ERP, SAP, Vantive, etc.) |
| **Estándar** | - | - | <1 % | Correo Electrónico /<br>File Transfer / Servicios WEB |



* Las mediciones internacionales se realizan contra nuestro POP Miami

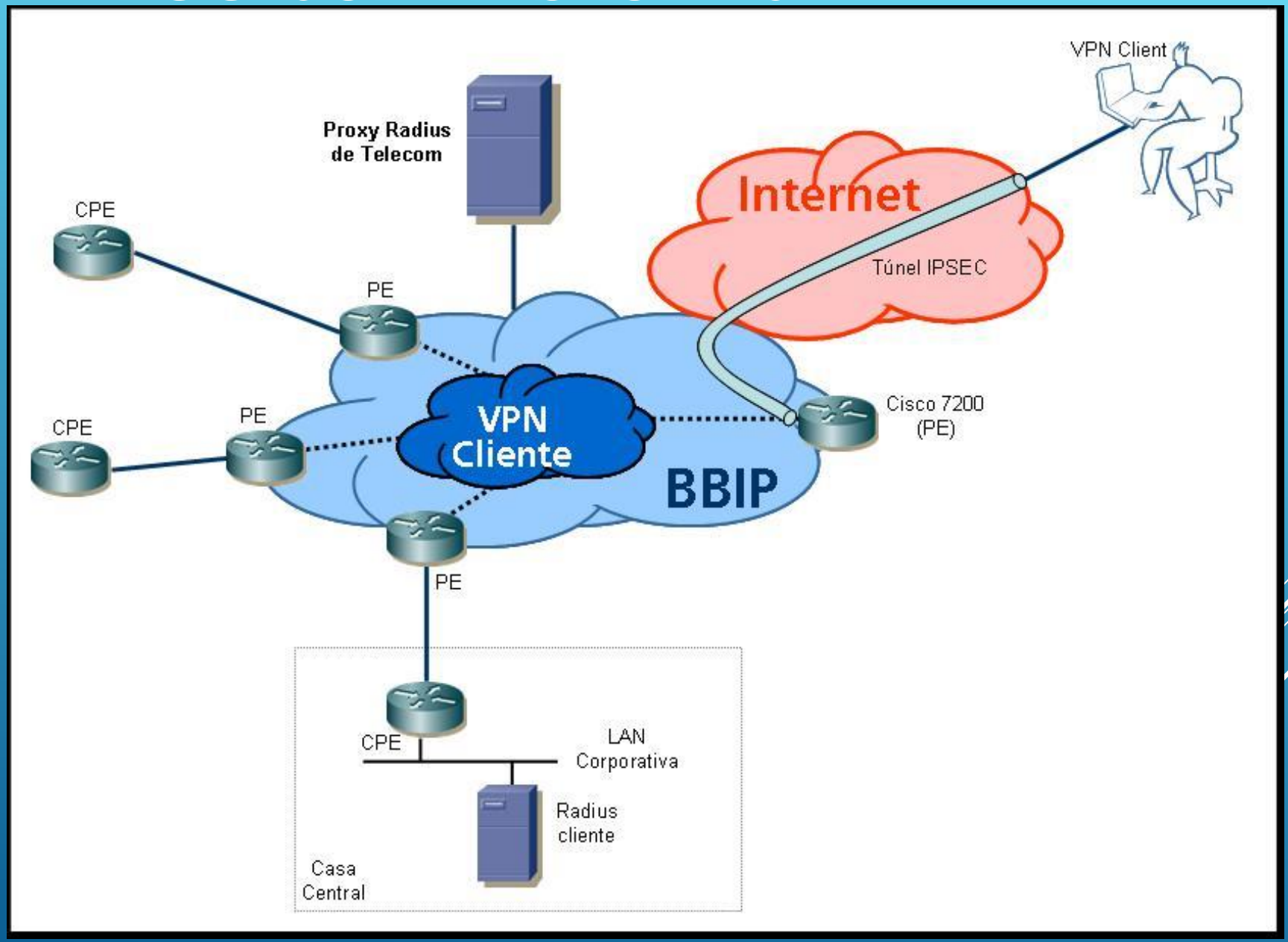
# ACCESO A INTERNET

- Como valor adicional a la VPN se incorpora en cada sitio la posibilidad de acceder a Internet, manteniendo las características de privacidad de la VPN, es decir que este adicional, **no** transforma a la VPN en una solución de Internet VPN



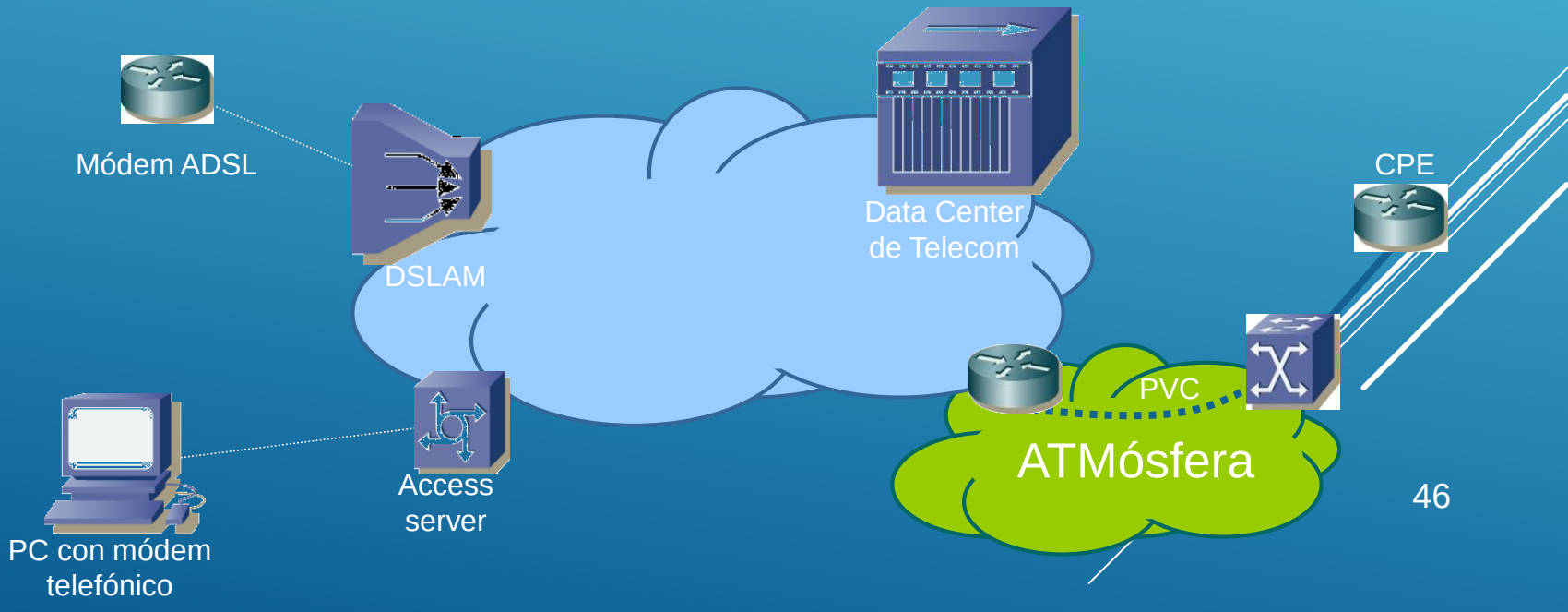

- El BW para tráfico de Internet debe estar considerado en el BW de QoS Estándar.
  - Sólo se puede configurar el BW de Internet hasta un 50% de la capacidad del vínculo de acceso y hasta el 100% de la QoS estándar

# ACCESO REMOTO DESDE INTERNET

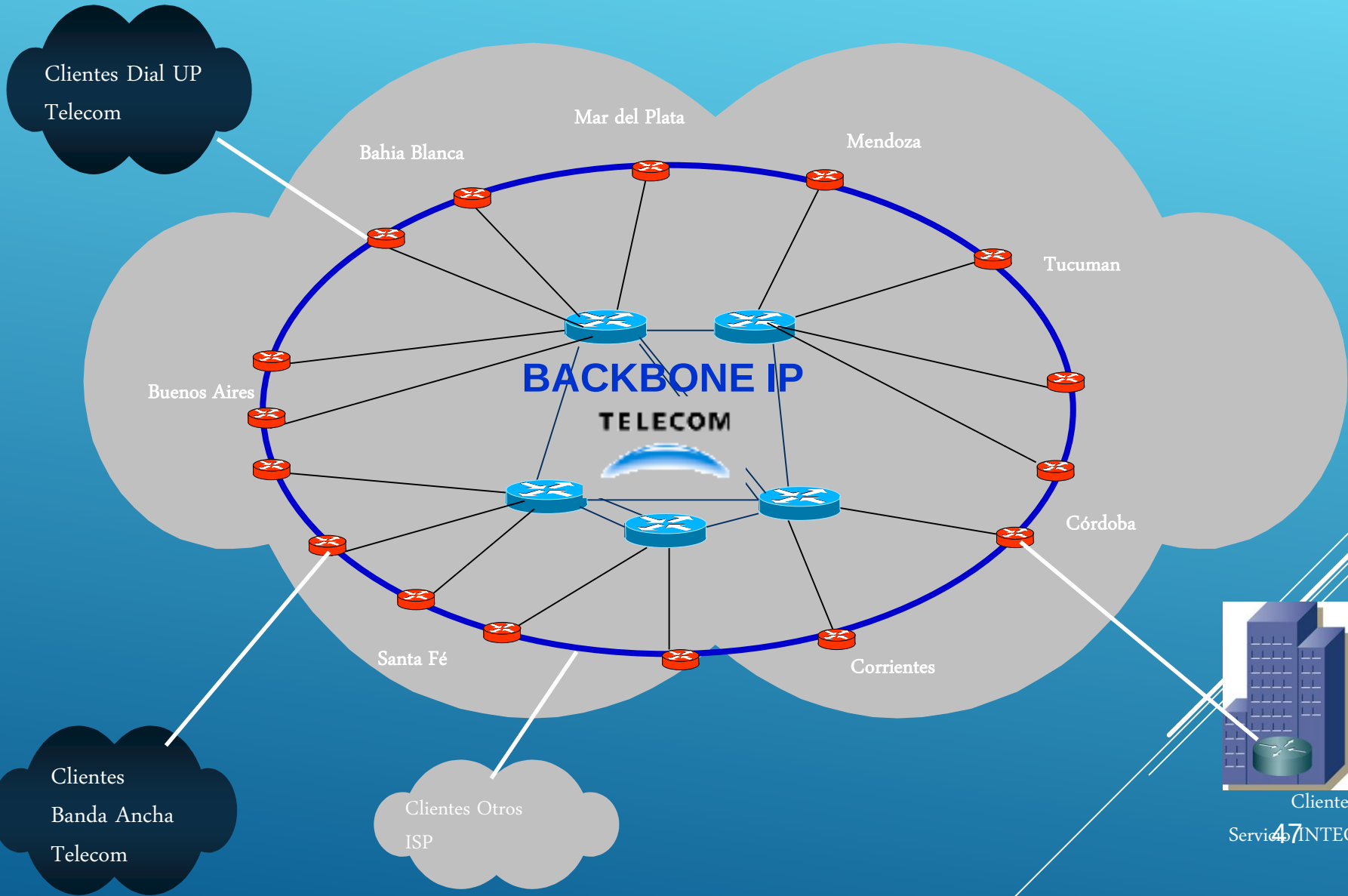


# INTEGRACIÓN DE TECNOLOGÍAS

- Múltiples tecnologías conviven en una misma red permitiendo el enrutamiento de los datos en forma óptima y sin congestión:
  - Data Center
  - Accesos dial up
  - Accesos ADSL
  - Interworking con ATM y frame relay



# Arquitectura de la Red IP



# CONCLUSIONES

- MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel (o conmutación IP). La idea básica de separar lo que es el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles 3 y 2, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura.

# CONCLUSIONES

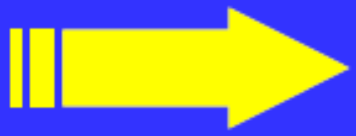
- Por otro lado, el hecho de que MPLS pueda funcionar sobre cualquier tecnología de transporte -no sólo sobre infraestructuras ATM- va a facilitar de modo significativo la migración para la próxima generación de la Internet óptica, en la que se acortará la distancia entre el nivel de red IP y la fibra.

# SEGURIDAD EN REDES

# CONCEPTOS GENERALES

- CONFIDENCIALIDAD O PRIVACIDAD
- AUTENTICIDAD
- INTEGRIDAD DE LOS DATOS

**ATAQUES INFORMÁTICOS**



- INTERCEPTACIÓN
- FABRICACIÓN
- MODIFICACIÓN
- DESTRUCCIÓN

# ALGUNOS MÉTODOS

- CLAVES DE ACCESO: AL SISTEMA O LOS RECURSOS
- ENCRIPTADO DE DATOS
- SEGURIDAD FÍSICA DE DISPOSITIVOS
- FIRMA DIGITAL
- FIREWALL
- CAPACITACIÓN DE USUARIOS Y ADMINISTRADORES
- PROTOCOLOS DE SEGURIDAD (IP SEC POR EJEMPLO)
- RED PRIVADA VIRTUAL (VPN)

# CRITERIOS PARA EVALUAR LOS SISTEMAS DE COMPUTADORAS

**CONFIABILIDAD**

**SEGURIDAD**

**DOD 5200-28-STD**

**NORMA DEL DEPARTAMENTO DE DEFENSA DE LOS EEUU**

**https://www.fas.org/irp/nsa/rainbow/std001.htm**

**CLASIFICACIÓN DE LOS SISTEMAS SEGÚN NIVELES**

# NIVELES

**IMPONEN LÍMITES Y CONDICIONES QUE DEBE REUNIR UN SISTEMA PARA ALCANZAR UN ESQUEMA DE SEGURIDAD RESPECTO DE SOFTWARE Y HARDWARE.**

**SON 4 NIVELES**

| | |
|---|---|
| D | PROTECCIÓN MÍNIMA |
| C C1 C2 | PROTECCIÓN DISCRECIONAL |
| B B1 B2 B3 | PROTECCIÓN DE MANDATARIO |
| A | PROTECCIÓN VERIFICADA |

# NIVELES

## NIVEL D: PROTECCIÓN MÍNIMA

- SISTEMAS QUE NO TIENEN CLASIFICACIÓN DE SEGURIDAD.
- NO REQUIERE PROTECCIÓN.

## NIVEL C: PROTECCIÓN DISCRECIONAL

- SISTEMAS CON CIERTA PROTECCIÓN.
- INCLUYE:
  - CAPACIDAD DE AUDITORÍA
  - RESPONSABILIZACIÓN DE SUJETOS Y SUS ACCIONES

## C1: PROTECCIÓN DE SEGURIDAD DISCRECIONAL

- SEPARACIÓN ENTRE USUARIOS Y DATOS.
- REGISTRO DE USUARIOS MEDIANTE NOMBRE Y CLAVE DE ACCESO.
- CUENTA DE ADMINISTRADOR DE SISTEMA SIN RESTRICCIONES.

## C2: PROTECCIÓN DE ACCESO CONTROLADO

- REFUERZA RESTRICCIONES DE USUARIOS.
- RESPONSABILIZA A LOS USUARIOS POR SUS ACCIONES MEDIANTE LOGIN, AUDITORÍA Y AISLACIÓN DE RECURSOS.
- ESPECIFICA NIVELES DE ACCESO. PERMISOS DE LECTURA, ESCRITURA O AMBOS.

**EJEMPLOS = UNIX, WINDOWS NT**

# NIVEL B: PROTECCIÓN DE MANDATARIO

•MAYOR IMPORTANCIA EN PRESERVAR LA INTEGRIDAD DE LA INFORMACIÓN SENSIBLE.

•USA REGLAS PARA EL CONTROL DE ACCESO DEL ADMINISTRADOR.

# B1: PROTECCIÓN DE SEGURIDAD CLASIFICADA

. REQUIERE LO INCLUIDO EN C2.

. ESTABLECE POLÍTICAS DE SEGURIDAD EN FUNCIÓN DE LA CLASIFICACIÓN DE SEGURIDAD QUE SE ASIGNE A LOS DATOS (RESERVADO, CONFIDENCIAL, SECRETO, ULTRA SECRETO).

. TRABAJA SOBRE EL CONTROL DE ACCESO A "OBJETOS". LOS CAMBIOS SÓLO PUEDEN SER REALIZADOS POR SU DUEÑO.

. SE APLICA SOBRE INFORMACIÓN QUE DEBE SER EXPORTADA Y SE DESEA MANTENER LOS DERECHOS DEL AUTOR.

## B2: PROTECCIÓN DE ESTRUCTURA

.IDENTIFICACIÓN DE OBJETO SEGÚN LA PROTECCIÓN NECESARIA.

.ESTABLECE PAUTAS DE COMUNICACIÓN ENTRE UN OBJETO DE NIVEL MÁS ELEVADO DE SEGURIDAD CON UNO DE MENOR NIVEL.

.INCREMENTO DE CONTROLES Y MECANISMOS DE AUTENTICACIÓN.

## B3: DOMINIOS DE SEGURIDAD

.EMPLEO DE HARDWARE DE SEGURIDAD.

.ALTA RESISTENCIA AL ACCESO NO AUTORIZADO.

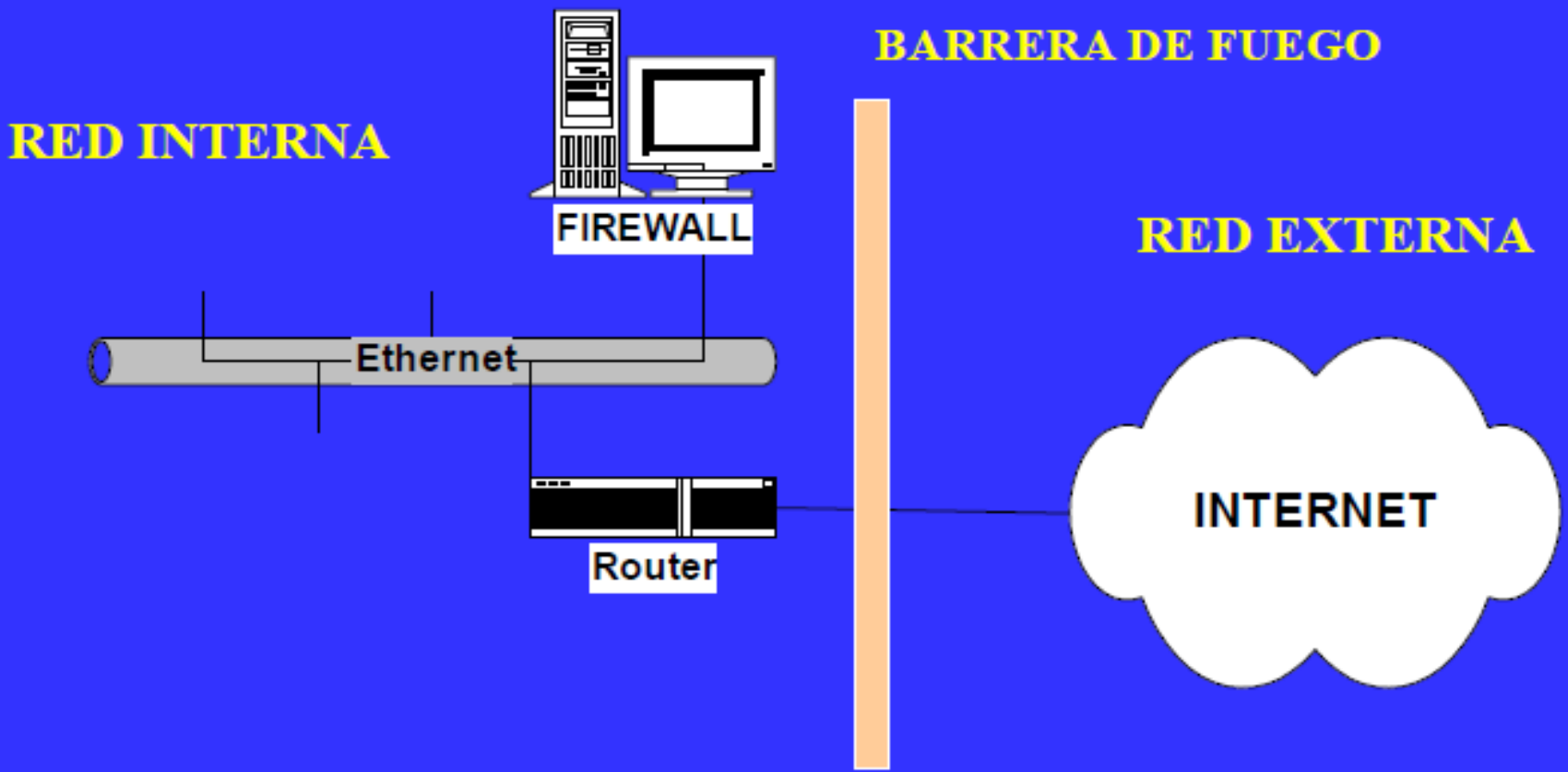
.ESTABLECIMIENTO DE RUTAS SEGURAS EN LA COMUNICACIÓN.

# NIVEL A: PROTECCIÓN VERIFICADA

- TAMBIÉN LLAMADO NIVEL DE DISEÑO VERIFICADO.
- ABARCA VERIFICACIONES EN EL DISEÑO, DESARROLLO E IMPLEMENTACIÓN DE HARDWARE Y SOFTWARE.
- PREVEE LA ADMINISTRACIÓN Y GESTIÓN DE LA SEGURIDAD DEL SISTEMA.

# FIREWALL

**ES UN SISTEMA QUE CREA UNA BARRERA SEGURA ENTRE DOS REDES. SE COMPONE DE HARDWARE Y SOFTWARE.**



# BENEFICIOS DE UN FIREWALL

- CONCENTRA SEGURIDAD EN UN ÚNICO PUNTO.
- CONTROLA ACCESO.
- REGULA EL USO DE LA RED EXTERIOR.
- REGISTRA EL EMPLEO DE LA RED INTERNA Y LA EXTERNA.
- PROTEGE DE ATAQUES EXTERNOS.
- LIMITA EL TRÁFICO DE SERVICIOS VULNERABLES.
- MEJORA LA PRIVACIDAD DEL SISTEMA. POR EJEMPLO OCULTAR DIRECCIONES IP INTERNAS O BLOQUEAR SERVICIOS.

# DECISIONES AL IMPLEMENTAR UN FIREWALL

## 1RO POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN.

- NEGACIÓN DE TODOS LOS SERVICIOS, EXCEPTO ALGUNOS AUTORIZADOS.
- PERMITIR LIBRE USO DE TODO, EXCEPTO LO EXPRESAMENTE PROHIBIDO.
- MEDIR Y AUDITAR EL USO DE LA RED.

## 2DO NIVEL DE SEGURIDAD DESEADO.

- ANÁLISIS DE NECESIDADES CON NIVELES DE RIESGO ACEPTABLES.
- NIVEL DE SEGURIDAD QUE SATISFACE. SOLUCIÓN DE COMPROMISO.

## 3RO EVALUACIÓN DE COSTOS.

- MEJOR RELACIÓN COSTO – BENEFICIO.

# FIREWALL

**ES UN COMPONENTE DE LA SEGURIDAD DE UNA RED. HAY QUE COMPLEMENTARLO CON OTRAS ACCIONES.**

**TIPOS DE FIREWALL**

**NIVEL DE RED**

**DIRECCIONES IP Y NÚMEROS DE PUERTO.**

**EJEMPLO = ROUTER.**

**NIVEL DE APLICACIÓN**

**NO PERMITEN TRÁFICO DIRECTO ENTRE LAS REDES.**

**EJEMPLO = SERVIDOR PROXY.**

# FIRMA DIGITAL

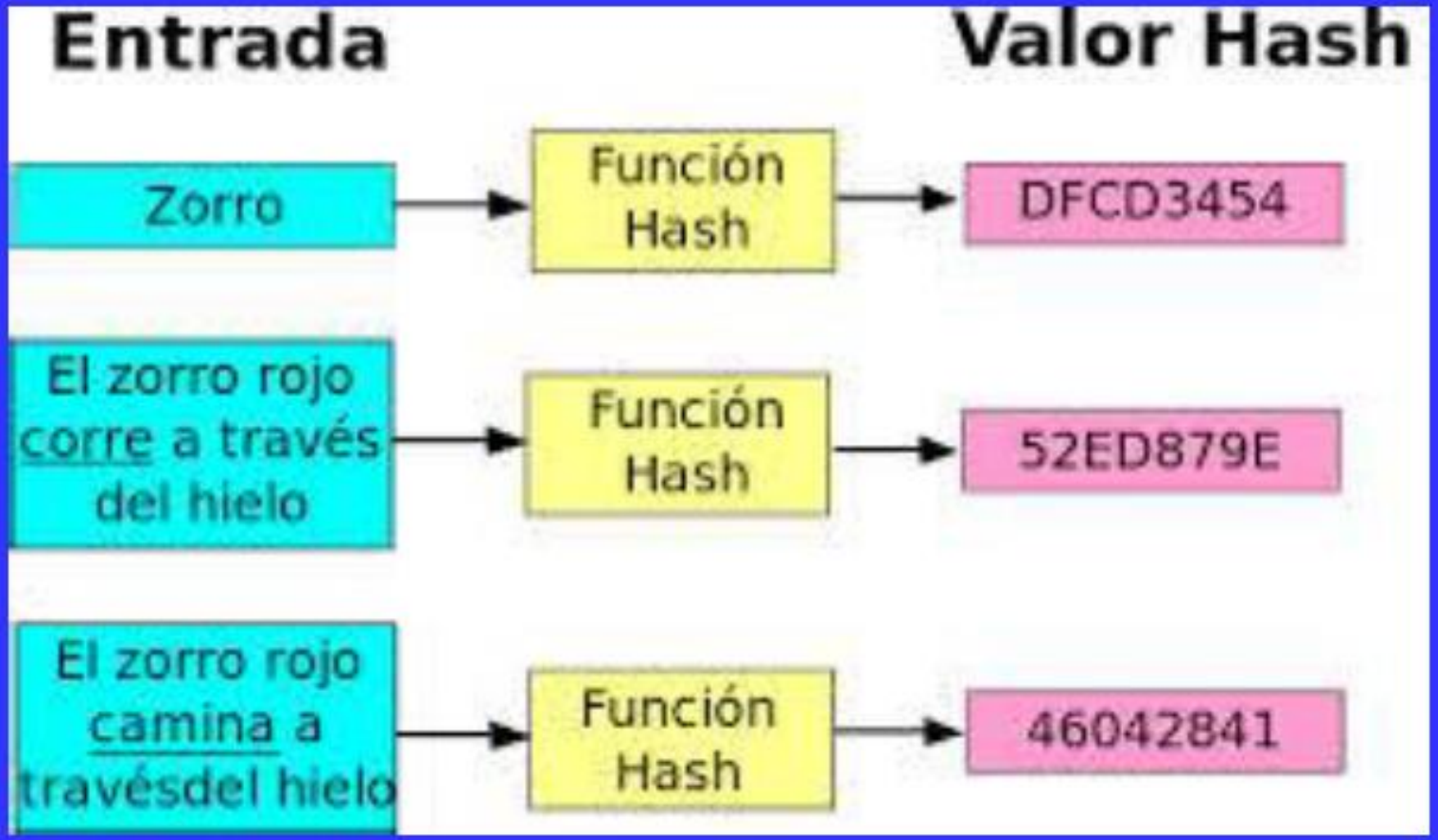
**ES LA TÉCNICA DE SEGURIDAD INFORMÁTICA APLICADA SOBRE LA INFORMACIÓN DIGITAL QUE SE INTERCAMBIA EN UNA RED, BASADA EN:**

- **CRIPTOSISTEMA ASIMÉTRICO**
  - **CLAVE PÚBLICA**
  - **CLAVE PRIVADA**
- **FUNCIÓN MATEMÁTICA (HASH). Salida long fija (DIGEST)**
- **AUTORIDAD CERTIFICANTE**

**PROVEE AUTENTICIDAD, INTEGRIDAD Y NO REPUDIO.**

**PUEDE ADICIONARSE EL ENCRIPTADO COMPLETO DE UN MENSAJE CON LO QUE SE PROVEE CONFIDENCIALIDAD (PRIVACIDAD)**

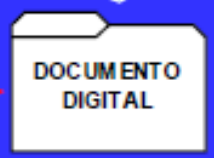
# FUNCIÓN HASH



# FIRMA DIGITAL


REGISTRA LAS CLAVES PÚBLICAS Y LAS DISTRIBUYE EN FORMA SEGURA

CLAVE PRIVADA A


CLAVE PUBLICA A

USUARIO A


USUARIO B

# IP SECURITY

# IP SEC

ES UN CONJUNTO DE PROTOCOLOS DE SEGURIDAD QUE PERMITEN AGREGAR ENCRIPTADO Y AUTENTICACIÓN A LA COMUNICACIÓN.

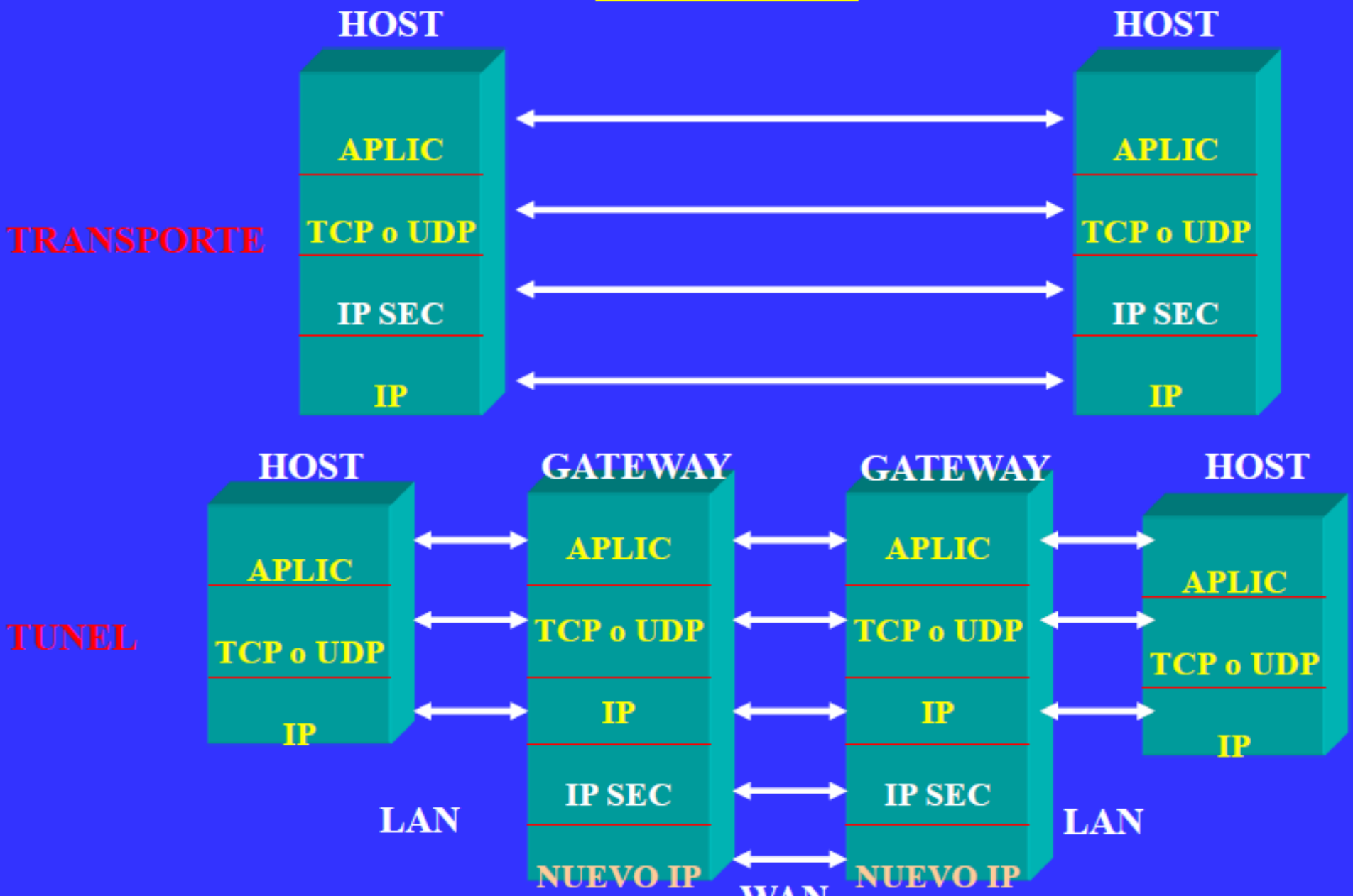
ES DE CAPA 3 RESULTANDO TOTALMENTE TRANSPARENTE PARA LAS APLICACIONES.

USO FRECUENTE EN VPN.

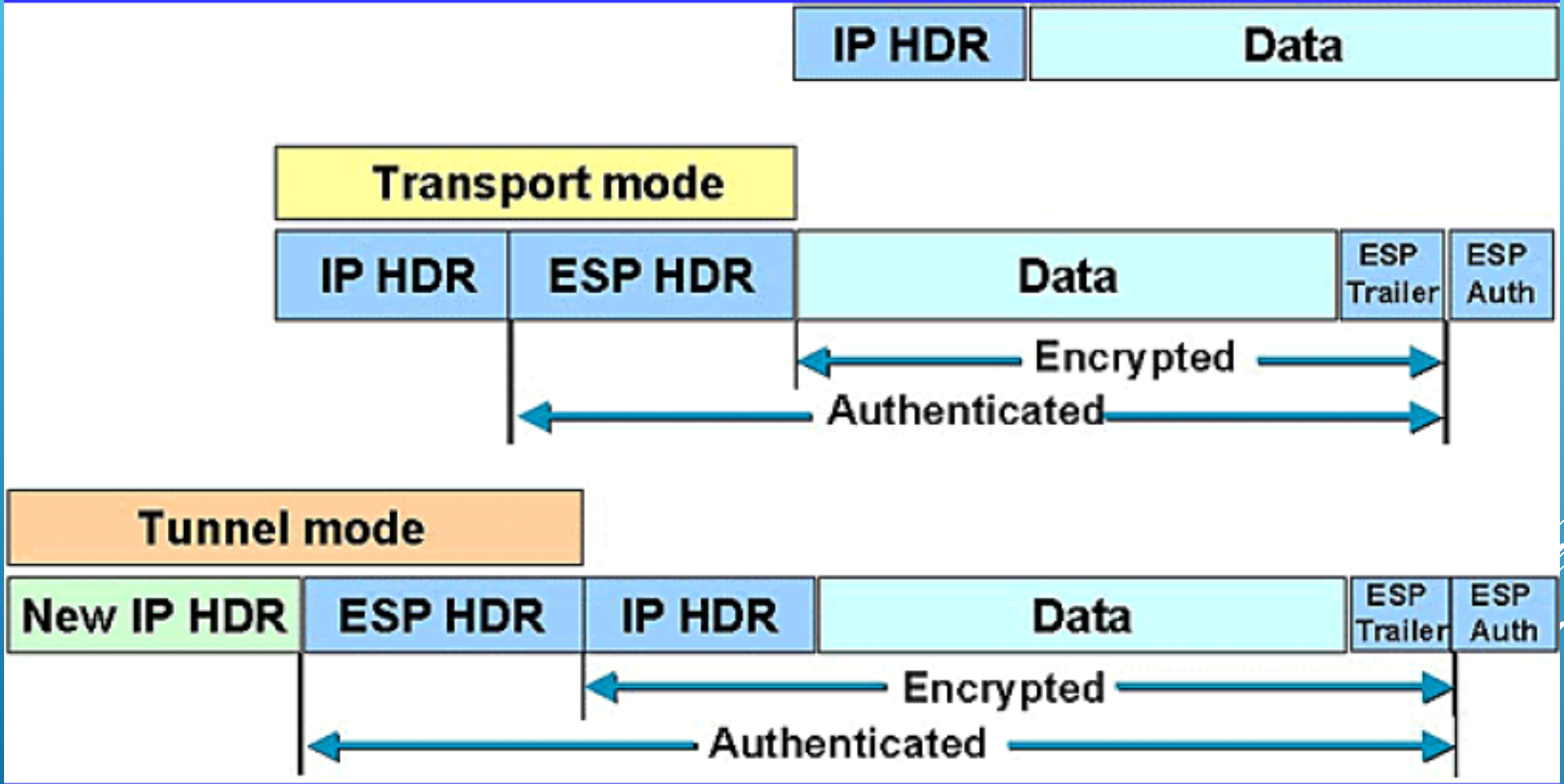
MODOS DE APLICACIÓN:

- TRANSPORTE
- TÚNEL

# IP SEC


HOST
HOST
APLIC
TCP o UDP
IP SEC
IP
APLIC
TCP o UDP
IP SEC
IP
TRANSPORTE
HOST
GATEWAY
GATEWAY
HOST
APLIC
TCP o UDP
IP
APLIC
TCP o UDP
IP
IP SEC
NUEVO IP
APLIC
TCP o UDP
IP
IP SEC
NUEVO IP
APLIC
TCP o UDP
IP
TUNEL
LAN
LAN
WAN

# MODOS IP SEC




Encapsulating Security Payload (ESP)