ETSIIT
Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

Ingeniería Informática + ADE

Universidad de Granada (UGR)

Autor: Ismael Sallami Moreno

Asignatura: Tema 1 y Tema 2: Introducción y Capa de Red (FR)

Índice

Nota:*Se aconseja estudiar con ayuda de las diapositivas.*

1 Tema 1: Introducción a los fundamentos de las redes

1.1. Sistemas de comunicación y redes

Se define por un sistema de comunicación a la infraestructura (hard y soft) que permite el intercambio de la información. La información es el conjuntos de datos que tienen un significado. Y por red entendemos al sistema de comunicación con sistemas finales y autónomos, que tiene capacidad de procesar la información. facilitando el intercambio eficaz y transparente de información.

La motivación para usar redes es la posibilidad de compartir recursos, la escalabilidad, fiabilidad, robustez, duplicidad y el ahorro de costes.

Características de una red, ya sea de computadores, de móviles, etc es la autonomía, la interconexión y el intercambio de información de manera eficaz y transparente.

Los elementos de una red son:

- Hosts: sistemas finales, es decir, las terminales. Además son autónomos.
- Subred: es una infraestructura para el transporte de información. Esta consta de líneas de transmisión y nodos de elementos de comunicación, como pueden ser routers, switches, etc.

Ejemplos de medios de transmisión:

- Cable coaxial
- Cable por trenzado: UTP, STP, FTP
- Fibra óptica

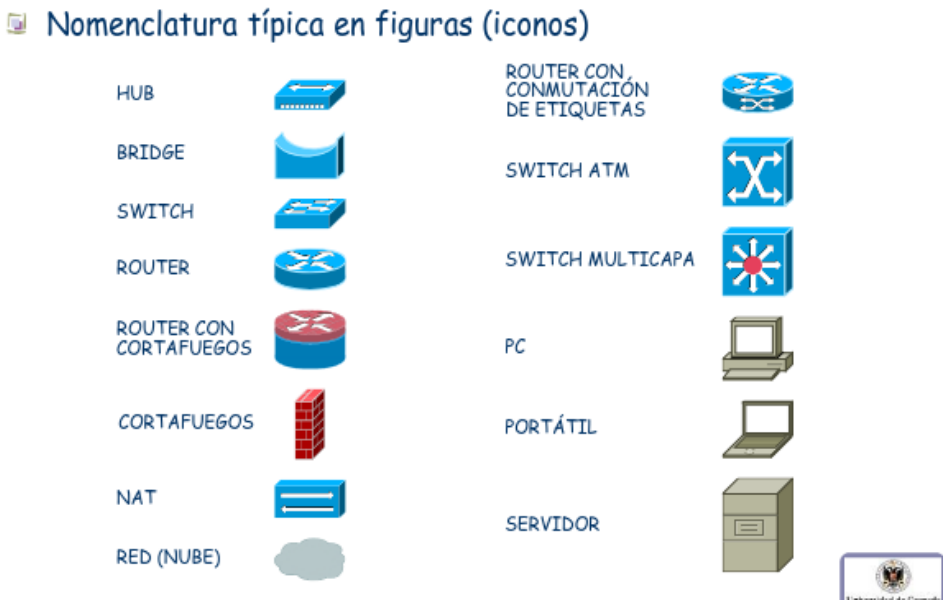
Topologías de redes: patrón de interconexión entre sus nodos

- Física vs lógica
- Tipos:
    - En bus
    - En anillo
    - En estrella
    - En malla
    - En árbol
    - En híbrida

1.2. Clasificación de las redes

- Según su tamaño: PAN (personal), LAN(local), MAN(m3tropolitano), WAN(wide):
  - PAN (Personal Area Network): Es una red utilizada para la comunicación entre dispositivos de una persona, típicamente en un rango de unos pocos metros. Ejemplos incluyen la conexión entre un teléfono móvil y un auricular Bluetooth.
  - LAN (Local Area Network): Es una red que cubre un área geográfica pequeña, como una casa, oficina o edificio. Permite la interconexión de dispositivos como computadoras, impresoras y otros equipos dentro de un área limitada.
  - MAN (Metropolitan Area Network): Es una red que abarca una ciudad o una gran área metropolitana. Se utiliza para conectar varias LANs dentro de una ciudad, proporcionando alta velocidad y conectividad eficiente.
  - WAN (Wide Area Network): Es una red que cubre un área geográfica extensa, como un país o incluso continentes. Las WANs permiten la comunicación y el intercambio de datos entre dispositivos ubicados en diferentes lugares geográficos. Internet es el ejemplo más conocido de una WAN.
- Según la tecnología de transmisión:
  - Difusión: En este tipo de red, un solo nodo transmite datos a todos los demás nodos en la red. Un ejemplo común es la red de televisión por aire.
  - Punto a punto: En este tipo de red, los datos se transmiten directamente entre dos nodos específicos. Un ejemplo común es una conexión telefónica.
- Según el tipo de transferencia entre datos:
  - **Simplex**: Es un modo de comunicación unidireccional, donde la información solo puede ser enviada en una dirección. Un ejemplo común es la transmisión de televisión.
  - **Half-duplex**: Es un modo de comunicación bidireccional, pero no simultánea. Esto significa que la información puede ser enviada en ambas direcciones, pero no al mismo tiempo. Un ejemplo es un walkie-talkie.
  - **Full-duplex**: Es un modo de comunicación bidireccional y simultánea. Esto significa que la información puede ser enviada y recibida al mismo tiempo. Un ejemplo es una llamada telefónica.

1.2.1. Nomenclatura típica en figuras



- **HUB**[1]: Dispositivo que conecta múltiples computadoras en una red local. Reenvía los datos recibidos a todos los dispositivos conectados.
- **ROUTER**: Encargado de dirigir paquetes de datos entre diferentes redes. Se utiliza para conectar redes locales a Internet o a otras redes.
- **SWITCH**: Dispositivo que conecta múltiples dispositivos en una red local, pero a diferencia de un HUB, envía los datos solo al dispositivo destinatario, mejorando la eficiencia.
- **BRIDGE**: Permite conectar dos redes locales separadas y filtrar el tráfico entre ellas en función de la dirección MAC.
- **SWITCH ATM**: Diseñado para redes que usan la tecnología de Modo de Transferencia Asíncrona (ATM), que transporta datos en celdas de longitud fija.
- **SWITCH MULTICAPA**: Similar a un switch, pero con la capacidad de operar en varias capas del modelo OSI, como la capa de red (3) y la capa de enlace (2).
- **ROUTER CON CORTAFUEGOS**: Combina las funciones de un router y un cortafuegos para proporcionar seguridad y dirigir tráfico en redes.
- **RED (NUBE)**: Representación abstracta de una red o conjunto de redes, que típicamente se utiliza para denotar servicios en la nube o conexiones externas.
- **NAT (Network Address Translation)**: Tecnología que permite que varios dispositivos compartan una única dirección IP pública mediante la traducción de direcciones.

[1]Para la práctica, hay que saberse como mínimo HUB, SWITCH, ROUTER

- **PC**: Computadora personal que actúa como un host en una red.
- **SERVIDOR**: Computadora diseñada para proveer servicios a otros dispositivos en la red, como archivos, aplicaciones o datos.
- **PORTÁTIL**: Computadora portátil que también puede funcionar como host en una red.
- **CORTAFUEGOS**: Dispositivo o software diseñado para proteger redes bloqueando o permitiendo el tráfico en función de reglas predefinidas.
- **ROUTER CON CONMUTACIÓN DE ETIQUETAS**: Router que utiliza conmutación basada en etiquetas, como MPLS (Multiprotocol Label Switching), para optimizar el enrutamiento.

Los que debemos de saber dibujar son: **HUB, SWITCH, ROUTER.**

1.2.2. Estructura y Elementos de una Red según Kurose y Ross

La estructura y los elementos de una red están compuestos por diversos componentes que trabajan juntos para permitir la comunicación eficiente entre sistemas finales. Según Kurose y Ross, estos son los elementos principales:

- **Hosts (Sistemas finales)**: Dispositivos autónomos que actúan como origen o destino de la comunicación en una red. Los hosts pueden ser computadoras, servidores, dispositivos móviles o cualquier terminal que procese información.
- **Subred**: La infraestructura que permite el transporte de información entre los sistemas finales. Dentro de una subred, encontramos dos elementos clave:
  - **Líneas de transmisión**: Canales físicos o lógicos que transportan los datos entre los nodos de la red. Estos pueden ser cables de par trenzado, fibra óptica, enlaces inalámbricos, entre otros.
  - **Nodos o elementos de conmutación**: Dispositivos intermedios como *routers* o *switches*, que se encargan de redirigir y gestionar el tráfico de datos dentro de la subred.

Estos elementos se combinan para formar una red que facilita la interconexión y el intercambio de información de manera eficiente y transparente.

1.3. Diseño y estandarización de redes

Debemos de mencionar el *Modelo de referencia* que engloba la definición de capas y de las funcionalidades. Para el diseño se deben de seguir ciertos apéndices:

- Funcionalidades que son distintas deben de estar en capas distintas.
- Minimizar el flujo de información entre capas.

1.3.1. Modelos OSI, TCP/IP y el concepto de RFC

Modelos OSI y TCP/IP

- **OSI (Open Systems Interconnection)**: Este modelo, desarrollado por la *International Organization for Standardization (ISO)*, divide las comunicaciones de red en siete capas funcionales. Estas capas, que van desde la física hasta la aplicación, proporcionan un marco conceptual para la interoperabilidad entre sistemas.
- **TCP/IP (Transmission Control Protocol/Internet Protocol)**: Es el modelo práctico utilizado para las comunicaciones en Internet, desarrollado por el *Internet Engineering Task Force (IETF)*. Se compone de cuatro capas que se alinean funcionalmente con el modelo OSI.

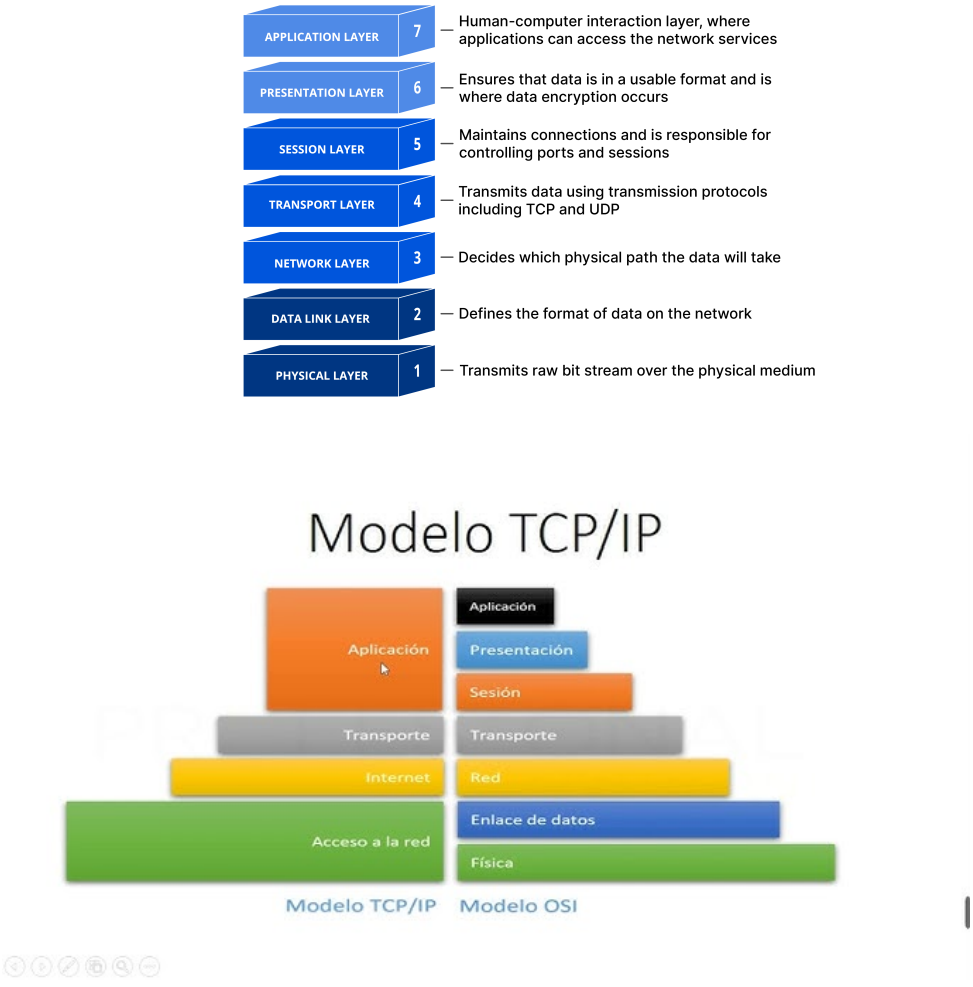


Figura 1: Comparación entre el modelo OSI (arriba) y el modelo TCP/IP (abajo).

¿Qué es un RFC?

El término **RFC (Request for Comments)** se refiere a una serie de documentos que contienen especificaciones, estándares y directrices sobre cómo funciona Internet y sus

protocolos asociados. Estos documentos son gestionados por el *RFC Editor* bajo la supervisión del *Internet Engineering Task Force (IETF)*.

- Los RFC pueden describir protocolos como HTTP, TCP, IP, entre otros.
- También incluyen métodos, tecnologías y recomendaciones para la evolución de la arquitectura de Internet.

Por ejemplo, el **RFC 2026** detalla el procedimiento de normalización para los estándares de Internet. Los RFC son esenciales para asegurar que dispositivos y sistemas de diferentes fabricantes puedan comunicarse de forma eficiente y uniforme.

1.4. Terminología, conceptos y servicios

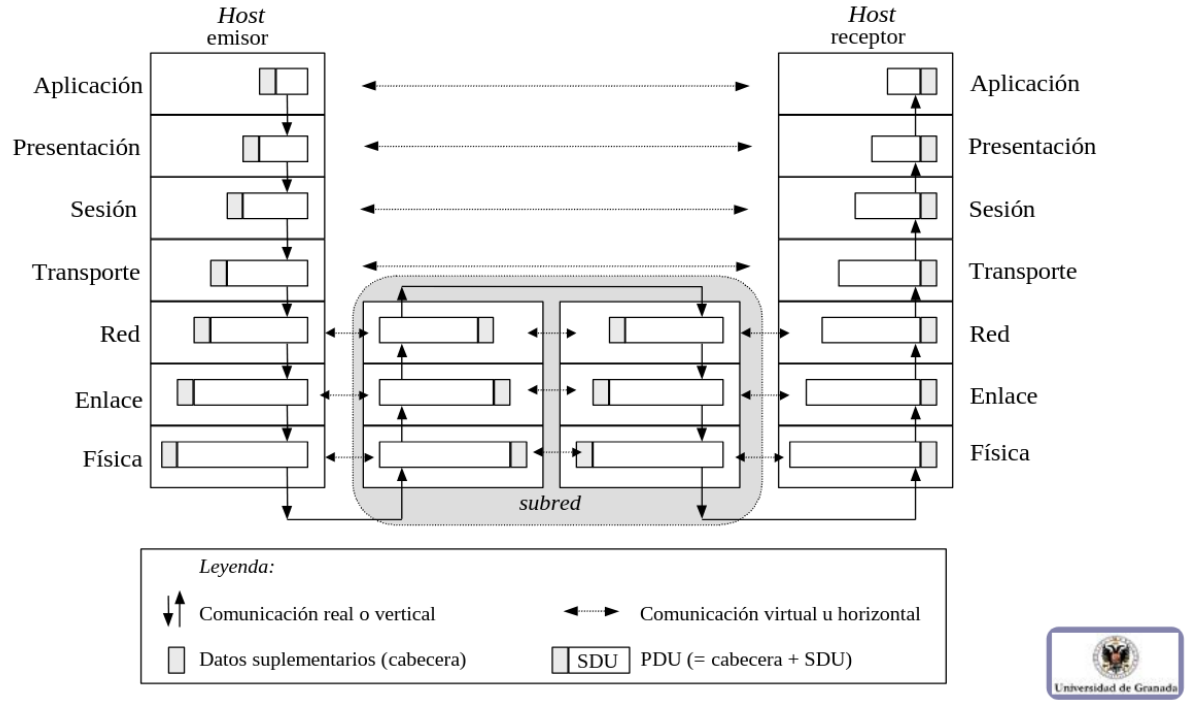


Figura 2: Terminología y conceptos básicos en redes de computadoras.

Terminología, Conceptos y Servicios

La terminología y los conceptos relacionados con las redes son esenciales para comprender cómo los dispositivos interactúan y cómo se estructuran las comunicaciones. A continuación, se detallan los términos principales:

Comunicación real (vertical): Es el intercambio de datos que ocurre entre capas adyacentes dentro de un dispositivo. Esta comunicación sigue un flujo descendente (del emisor) y ascendente (del receptor), en función del modelo de referencia utilizado.

Comunicación virtual (horizontal): Es la interacción lógica entre entidades pares en capas equivalentes de los dispositivos emisores y receptores. Aunque esta comunicación es conceptual, es facilitada por las capas inferiores.

Entidad del nivel N: Se refiere a una unidad funcional en la capa N del modelo OSI o similar. Por ejemplo, una entidad de la capa de transporte podría ser el protocolo TCP.

Entidades pares: Son entidades ubicadas en la misma capa de distintos dispositivos que se comunican mediante protocolos.

Protocolo: Es un conjunto de reglas que define cómo las entidades pares deben comunicarse. Incluye formatos, tiempos y secuencias de mensajes.

Interfaz: Es el punto de contacto entre capas adyacentes dentro de un dispositivo. Define cómo una capa accede a los servicios ofrecidos por la capa inferior.

Servicio: Es la funcionalidad que una capa provee a la capa superior. Por ejemplo, la capa de transporte ofrece servicios de entrega confiable a la capa de aplicación.

Capa proveedora y capa usuaria: La capa proveedora es aquella que ofrece un servicio, mientras que la capa usuaria lo consume. Por ejemplo, la capa de red es proveedora de la capa de transporte.

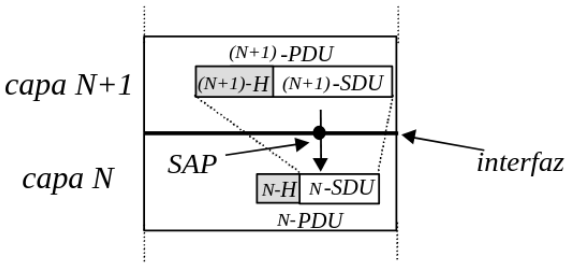
Pila de protocolos: Es la implementación de los protocolos en cada capa, que trabaja conjuntamente para permitir la comunicación de extremo a extremo.

Arquitectura de red: Es la combinación de un modelo de referencia (como OSI) y una pila de protocolos que define cómo funciona la red.

SAP (Service Access Point): Es un punto en la interfaz entre capas donde una capa accede a los servicios de otra. Se usa para identificar el punto de interacción.

SDU (Service Data Unit): Es la unidad de datos que una capa recibe de la capa superior para procesar y transmitir.

PDU (Protocol Data Unit): Es la unidad de datos intercambiada entre entidades pares en una capa. Incluye la SDU y cualquier información de encabezado o pie agregada por la capa.



Estos conceptos son fundamentales para garantizar el *intercambio de información transparente* entre los hosts, proporcionando una base sólida para entender cómo operan las redes modernas.

1.4.1. Retardos en la comunicación

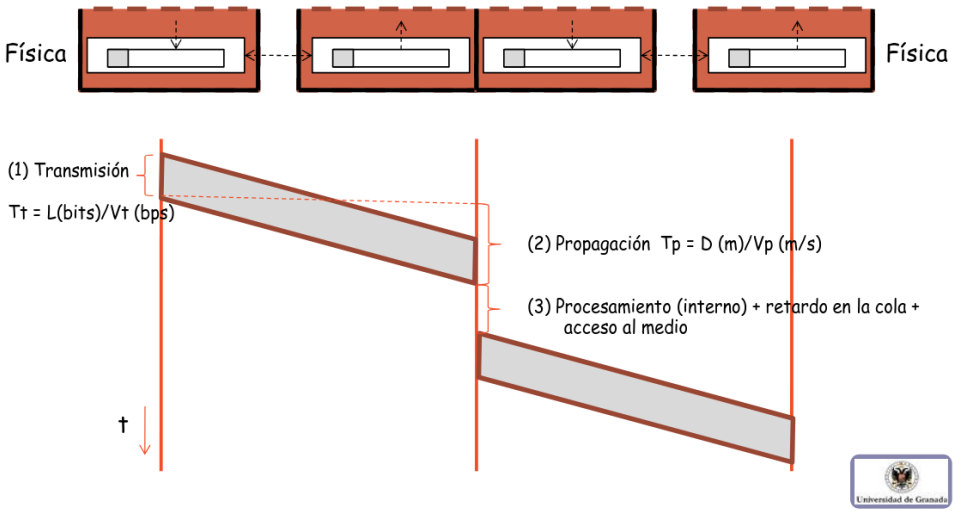
Fórmulas

Tiempo de transmisión:

$$T_t = \frac{L}{V_t} \tag{1}$$

Tiempo de propagación:

$$T_p = \frac{D(m)}{V_t(m/s)} \tag{2}$$



Nota

Si usamos la orden **ping** de una dirección, como por ejemplo de *www.google.com*, podemos obtener el tiempo de ida y vuelta de los paquetes.

Pregunta de Examen

¿Qué es la congestión de red? Podemos explicarlo mediante un caso práctico, como es, por ejemplo, mis routers tienen paquetes en cola, pues si salen pocos y entran muchos, descartan paquetes, y además conlleva que se reduzca la velocidad y por ende, se manden menos datos.

1.4.2. Tipos de servicios

- Orientado a conexión (SOC): Se establece una conexión antes de enviar los datos.
- No orientado a conexión (SNOC): Se envían los datos sin establecer una conexión previa.
- Confirmado (fiable): Se garantiza la entrega de los datos. Además, lleva un control de errores, de congestión, entrega ordenada.
- No confirmado (no fiable): No se garantiza la entrega de los datos.

1.5. Internet: topología y direccionamiento

Internet es una red global de redes interconectadas que permite la comunicación y el intercambio de información entre millones de dispositivos. Su diseño combina aspectos topológicos y de direccionamiento que aseguran su escalabilidad, eficiencia y robustez. A continuación, se resumen los aspectos clave:

1.5.1. Topología de Internet

La topología de Internet sigue una estructura jerárquica dividida en tres niveles principales:

- **Intranets:** Redes privadas de los usuarios que incluyen tecnologías como Ethernet y WiFi. Estas redes están divididas en una zona pública y una zona privada para gestionar la seguridad y el acceso.
- **Redes de acceso:** Conectan a los usuarios finales con los Proveedores de Servicios de Internet (ISP). Algunos ejemplos de tecnologías utilizadas son xDSL, FTTH y RDSI.
- **Redes troncales:** Son infraestructuras de alta capacidad operadas por grandes proveedores de telecomunicaciones. Utilizan tecnologías como ATM, SDH, SONET o MPLS.

Además, los acuerdos entre estas redes, conocidos como *peering* y conexiones de tránsito, permiten la comunicación entre operadores a nivel global. En este contexto, se diferencian las siguientes categorías:

- **Redes Tier 1:** Operadores globales interconectados que forman el *backbone* de Internet.

- **Redes Tier 2:** Operadores regionales que necesitan conectarse a redes Tier 1 para alcanzar toda Internet.
- **Redes Tier 3:** ISPs locales que proveen conectividad a usuarios finales y empresas.

1.5.2. Direccionamiento en Internet

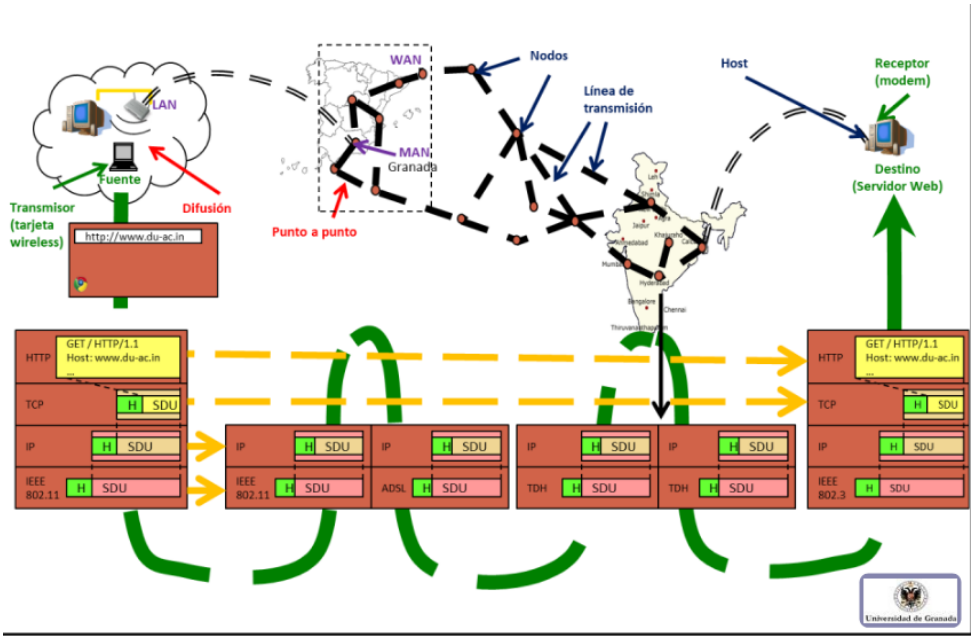


Figura 3: Estructura de Internet: topología y direccionamiento.

Explicación de la Imagen

La imagen muestra una representación gráfica del tema "Internet: topología y direccionamiento" como parte de la introducción a los fundamentos de redes. Esta imagen es relevante porque ilustra cómo se estructura y se direcciona la información en una red de Internet, desde la fuente hasta el destino. A continuación, se detallan los elementos presentes en la imagen:

- **Fuente y Transmisor**: La imagen comienza con una fuente de datos conectada a una red de área local (LAN) a través de un transmisor (tarjeta inalámbrica). Se muestra un ejemplo de una solicitud HTTP: `GET / HTTP/1.1 Host: www.dsc.uh.cu`.
- **Difusión y Punto a Punto**: La información se transmite desde la LAN a través de diferentes tipos de redes, incluyendo redes de área amplia (WAN) y redes de área metropolitana (MAN). Se destacan dos tipos de transmisión: difusión y punto a punto.
- **Nodos y Línea de Transmisión**: La información pasa a través de varios nodos y líneas de transmisión, representando la infraestructura física de Internet.

- **Receptor y Destino**: Finalmente, la información llega al receptor (modem) y al destino final, que es un servidor web. Se muestra otra solicitud HTTP similar a la inicial.
- **Capas del Modelo OSI**: La imagen también ilustra cómo los datos se encapsulan y desencapsulan a través de diferentes capas del modelo OSI (IEEE 802.11, IP, TCP, HTTP). Cada capa añade o quita su propio encabezado (H) y unidad de datos de servicio (SDU).

Esta imagen es interesante porque proporciona una visión clara y detallada de cómo se maneja y se dirige la información en una red de Internet, lo cual es fundamental para entender el funcionamiento de las redes de comunicación.

El direccionamiento en Internet se estructura en varios niveles, cada uno de los cuales cumple una función específica dentro de las diferentes capas del modelo TCP/IP:

- **URL (Uniform Resource Locator):** Utilizado en la capa de aplicación para identificar recursos específicos, como páginas web. Ejemplo: `http://www.du-ac.in/index.html`.
- **Puertos:** Identifican los procesos de origen y destino en la capa de transporte. Por ejemplo, el puerto 80 para HTTP.
- **Dirección IP:** Se utiliza en la capa de red para identificar de manera única a los hosts en Internet.

1.5.3. Otros elementos clave

En Internet también se destacan los siguientes componentes:

- **IXP (Internet Exchange Points):** Puntos de intercambio donde múltiples ISPs realizan *peering*.
- **Red IRIS:** Ejemplo de una red académica y de investigación en España.
- **Redes autónomas:** Identificadas mediante ASNs (Autonomous System Numbers), que gestionan bloques de direcciones IP y políticas de enrutamiento.

Esta estructura asegura que Internet pueda soportar la enorme cantidad de tráfico generado por sus usuarios, garantizando conectividad global y optimización en el intercambio de datos.

2 Tema 2: Capa de Red

2.1. Funcionalidades

2.1.1. Funciones y servicios en TCP/IP

- **Encaminamiento:** Proceso de seleccionar el camino más adecuado para enviar paquetes de datos desde el origen hasta el destino a través de una red. Ejemplo de protocolo: *OSPF (Open Shortest Path First)*.

- **Conmutación:** Técnica utilizada para enviar datos a través de una red mediante la creación de una ruta temporal entre el origen y el destino. Ejemplo de protocolo: *MPLS (Multiprotocol Label Switching)*.
- **Interconexión de redes:** Proceso de conectar diferentes redes para que puedan comunicarse entre sí, permitiendo el intercambio de datos. Ejemplo de protocolo: *IP (Internet Protocol)*.
- **En OSI: control de gestión:** Función que supervisa y controla el funcionamiento de la red, asegurando que los recursos se utilicen de manera eficiente y que se mantenga la calidad del servicio. Ejemplo de protocolo: *SNMP (Simple Network Management Protocol)*.
- **Ejemplos de protocolos de red:** Protocolos que operan en la capa de red para facilitar la comunicación entre dispositivos. Ejemplos incluyen *IP (Internet Protocol)*, *ICMP (Internet Control Message Protocol)*, y *ARP (Address Resolution Protocol)*.

2.2. Conmutación

La **conmutación** se refiere a la acción de establecer o determinar un camino que permita transmitir información de extremo a extremo en una red. A continuación, se describen los esquemas y conceptos principales asociados:

Esquemas de Conmutación

Existen diferentes esquemas para implementar la conmutación en redes:

- **Conmutación de Circuitos:** (Más adelante profundizaremos en este tema)
  - Es un servicio orientado a conexión, lo que significa que requiere el establecimiento previo de una conexión antes de transmitir los datos.
  - Ejemplo típico: redes telefónicas.
  - Los pasos del proceso incluyen:
    1. **Conexión:** Se establece un camino dedicado entre el emisor y el receptor.
    2. **Transmisión:** Los datos fluyen a través del circuito dedicado.
    3. **Desconexión:** El circuito se libera una vez finalizada la transmisión.
  - Ventajas:
    - Los recursos son dedicados, lo que facilita comunicaciones en tiempo real sin contención (es decir, sin competencia por el acceso al medio).
  - Inconvenientes:
    - Retraso significativo para el establecimiento de la conexión.
    - Baja flexibilidad para adaptarse a cambios en las condiciones de la red.
    - Poco tolerante a fallos.
- **Conmutación de Paquetes:** (Más adelante profundizaremos en este tema)

- Utiliza datagramas o circuitos virtuales para transmitir información.
- En este esquema, los datos se dividen en paquetes pequeños, que se transmiten de forma independiente a través de la red.
- Ofrece mayor flexibilidad y tolerancia a fallos en comparación con la conmutación de circuitos.

La elección entre conmutación de circuitos o de paquetes depende de las necesidades específicas de la red, como la prioridad de las comunicaciones en tiempo real frente a la adaptabilidad y tolerancia a fallos.

2.2.1. Conmutación de Circuitos

La **conmutación de circuitos** es un esquema de transmisión que establece un camino fijo entre los dispositivos de origen y destino antes de que ocurra la comunicación. Este enfoque presenta varias ventajas y desventajas, las cuales se detallan a continuación:

Ventajas

- **Transmisión en tiempo real:** Ideal para servicios sensibles al tiempo, como la comunicación de voz.
- **Uso permanente de recursos:** Una vez establecido, el circuito permanece activo durante toda la sesión, garantizando estabilidad.
- **Sin contención:** No hay competencia por el acceso al medio, ya que los recursos están dedicados.
- **Circuito fijo:** La ruta de comunicación no cambia una vez configurada, eliminando decisiones de encaminamiento durante la transmisión.
- **Simplicidad en la gestión de nodos intermedios:** La operación de los nodos es más sencilla porque no necesitan reevaluar las rutas.

Desventajas

- **Retraso en el inicio de la comunicación:** Es necesario establecer el circuito antes de comenzar la transmisión, lo que genera un tiempo de espera.
- **Uso no eficiente de recursos:** Si el circuito permanece inactivo durante parte de la sesión, los recursos se desperdician.
- **Falta de flexibilidad:** El circuito es fijo y no se puede ajustar en caso de fallos o cambios en la red.

Este esquema es adecuado para aplicaciones donde la calidad de servicio y la baja latencia son esenciales, pero puede no ser ideal en escenarios donde la eficiencia en el uso de recursos es prioritaria.

➢ Conmutación de circuitos

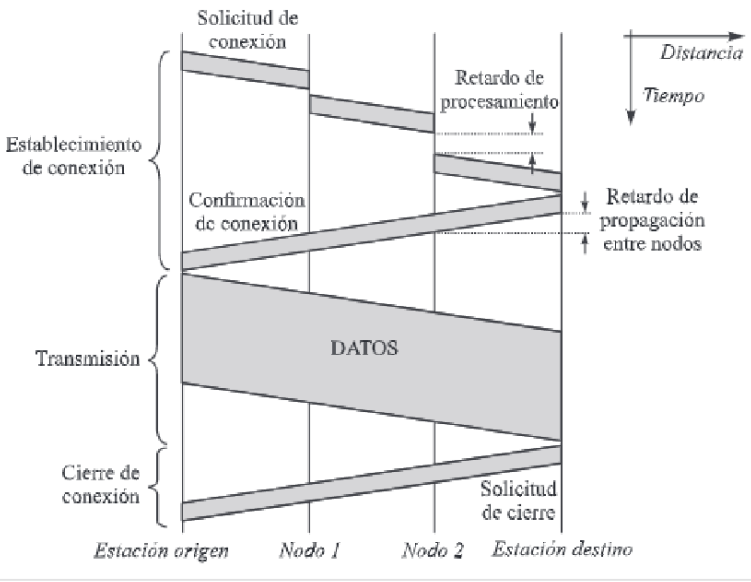


Figura 4: Ejemplo de conmutación de circuitos en una red telefónica.

2.2.2. Conmutación de Paquetes

La **conmutación de paquetes** es un esquema de transmisión en el que la información se divide en bloques denominados *paquetes*. Estos paquetes se envían de manera independiente a través de la red, permitiendo flexibilidad y eficiencia en el uso de los recursos.

Tipos de Conmutación de Paquetes

- **Conmutación mediante Datagramas:**
  - Ejemplo: El protocolo IP.
  - No requiere el establecimiento de una conexión previa.
  - Los paquetes se envían de manera independiente, y cada uno puede seguir rutas diferentes a través de la red.
  - En cada salto, los nodos intermedios realizan un proceso de *almacenamiento y envío* (*store-and-forward*), gestionando temporalmente los paquetes antes de retransmitirlos.
  - Cada paquete contiene las direcciones de origen y destino, lo que permite que los nodos intermedios determinen su ruta.
- **Conmutación de Paquetes con Circuitos Virtuales:**
  - Ejemplo: ATM (*Asynchronous Transfer Mode*), utilizado en redes troncales.
  - Este esquema combina características de la conmutación de circuitos y de la conmutación de paquetes.

- Los pasos típicos incluyen:
  1. **Conexión:** Se establece un circuito virtual antes de la transmisión.
  2. **Transmisión:** Los paquetes viajan a través del circuito virtual.
  3. **Desconexión:** El circuito virtual se libera al finalizar la transmisión.
- Los recursos no son dedicados, lo que permite mayor eficiencia en comparación con la conmutación de circuitos.

Ventajas de la Conmutación de Paquetes

- Flexibilidad en la ruta de los paquetes, lo que incrementa la tolerancia a fallos en la red.
- Uso más eficiente de los recursos en comparación con la conmutación de circuitos.
- Adecuado para datos no sensibles al tiempo, como correos electrónicos y descargas de archivos.

Desventajas de la Conmutación de Paquetes

- Latencia variable debido a los posibles retrasos en los nodos intermedios.
- Requiere mayor capacidad de procesamiento en los nodos para almacenar y decidir el envío de los paquetes.
- Pérdida potencial de paquetes, lo que puede requerir retransmisión en aplicaciones críticas.

La conmutación de paquetes es el mecanismo predominante en redes modernas, especialmente en Internet, debido a su capacidad de manejar tráfico de datos heterogéneo y adaptarse dinámicamente a las condiciones de la red.

2.2.3. Estimación del Tiempo de Transmisión en Conmutación de Paquetes mediante Datagramas

La pregunta plantea estimar el tiempo total involucrado en la transmisión de un mensaje de datos utilizando la técnica de conmutación de paquetes mediante datagramas (**CDP**). Los parámetros proporcionados son:

- M: Longitud en bits del mensaje a enviar.
- V: Velocidad de transmisión de las líneas en bits por segundo (*bps*).
- P: Longitud en bits de los paquetes.
- H: Bits de cabecera de los paquetes.
- N: Número de nodos intermedios entre las estaciones finales.
- D: Tiempo de procesamiento en segundos en cada nodo.
- R: Retardo de propagación en segundos asociado a cada enlace.

Solución Propuesta

Para resolver el problema, debemos considerar:

1. Dividir el mensaje en paquetes.
2. Calcular el tiempo de transmisión por paquete.
3. Incorporar los tiempos de procesamiento y propagación a lo largo de los nodos y enlaces.

Cálculo del Tiempo Total de Transmisión

$$\text{Número de paquetes: } N_p = \left\lceil \frac{M}{P-H} \right\rceil.$$

$$\text{Tiempo de transmisión de un paquete: } T_t = \frac{P}{V}.$$

$$\text{Tiempo total de transmisión: } T_{\text{total}} = N_p \cdot T_t + N_p \cdot N \cdot D + (N+1) \cdot R.$$

Donde:

- T_t: Tiempo de transmisión de un paquete, calculado como el cociente entre el tamaño del paquete P y la velocidad de transmisión V.
- T_{total}: Tiempo total de transmisión, que incluye:
  - La transmisión de todos los paquetes.
  - El procesamiento en cada nodo (D).
  - El retardo de propagación en los enlaces (R).

Análisis de Validez de las Soluciones

Solución Propuesta en las Diapositivas En el PDF[2] se menciona una fórmula similar basada en los mismos parámetros. La estructura general es válida, pero las diapositivas no siempre destacan la necesidad de sumar correctamente los retardos acumulados y los tiempos de procesamiento por cada paquete en nodos intermedios. Esto puede llevar a subestimar el tiempo total.

Solución Propuesta por ChatGPT La fórmula derivada en este documento, validada matemáticamente, considera cada paquete y su impacto en los tiempos de transmisión, procesamiento y propagación. Es válida y consistente con los principios de la conmutación de paquetes mediante datagramas.

[2]Como PDF se hace referencia a las diapositivas correspondientes al Temario 2, en específico, página 6/diapositiva 12

Conclusión

La solución propuesta aquí es válida, ya que incluye todos los retardos necesarios (transmisión, procesamiento y propagación) y maneja adecuadamente la fragmentación del mensaje en paquetes.

Si las soluciones del PDF no consideran alguno de estos elementos, pueden estar incompletas. Sin embargo, las presentaciones del PDF son útiles como referencia siempre que se ajusten a los detalles planteados en este análisis.

2.3. Protocolo IP

2.3.1. El Protocolo IP (IPv4)

El protocolo IP versión 4 (**IPv4**), especificado en el RFC 791, es el estándar fundamental para la interconexión de redes, también conocidas como subredes. Sus principales características y funciones se describen a continuación:

Características de IPv4

- **Interconexión de redes:** IPv4 permite la comunicación entre diferentes subredes, resolviendo el problema del direccionamiento en Internet.
- **Retransmisión salto a salto:** Gestiona el envío de paquetes desde el host de origen al destino final a través de routers intermedios.
- **Servicio no orientado a conexión:**
  - No realiza una negociación inicial o *handshake*, lo que significa que no establece una conexión lógica entre los extremos.
  - Es un protocolo *no fiable*, ya que no implementa control de errores ni control de flujo.
- **Unidad de datos:** Los paquetes enviados en IPv4 se denominan **datagramas**.
- **Protocolo de máximo esfuerzo (*best-effort*):**
  - No garantiza la entrega de los datagramas, que pueden perderse, duplicarse, retrasarse o llegar desordenados al destino.
- **Gestión de fragmentación:** IPv4 adapta el tamaño de los datagramas a las diferentes *Maximum Transfer Units* (MTUs) de las subredes, dividiendo los datagramas cuando es necesario.

Conclusión

IPv4 es un protocolo básico y ampliamente utilizado en Internet. Aunque no garantiza la fiabilidad ni el orden de los datos transmitidos, su simplicidad y diseño permiten la interoperabilidad entre redes heterogéneas, lo que ha facilitado la expansión de la conectividad global.

Ejemplos

- Hotmail con servidor webmail 130.206.192.39
- Youtube ...
- Google ...
- Facebook ...

Anotaciones Extra

- Las direcciones IP tienen 32 bits = 4 bytes
- No pueden ser mayores de 256 = 4 bytes
- Internet usa direccionamiento jerárquico, permitiendo clases, como la clase A, B, C, D, E, etc.
- Una de las máscaras que podemos tener es por ejemplo poniendo los 8 primeros bits a 1 y los 24 restantes a 0, es decir, 255.0.0.0
- ¿Que significa la red A?(podemos imaginar cualquier otra red). Pues significa que tenemos 128 redes de $2^{24} \approx 16$ millones.
- ¿Para que sirven las máscaras? Para ver la dirección IP que hay asociada a una red.

2.3.2. Direccionamiento Jerárquico y Máscaras de Red en IPv4

Internet adopta un esquema de **direccionamiento jerárquico** que simplifica el encaminamiento (*routing*) al dividir las direcciones IP en dos partes claramente diferenciadas. Este sistema permite identificar subredes y dispositivos dentro de cada subred.

Estructura de las Direcciones IP

Las direcciones IPv4 tienen un tamaño de **32 bits** y se dividen en dos componentes principales:

- **Identificador de subred:** Representa la subred a la que pertenece el dispositivo.
- **Identificador de dispositivo (host):** Identifica de manera única al dispositivo dentro de la subred.

Máscaras de Red

La **máscara de red** es un patrón que determina qué bits de una dirección IP corresponden al identificador de subred y cuáles al identificador del dispositivo. Se puede expresar de dos maneras:

- **Notación decimal con puntos:** Ejemplo: `255.255.255.0`.

- **Notación CIDR (Classless Inter-Domain Routing):** Ejemplo: `200.27.4.112/24`, donde el número después de la barra indica la cantidad de bits asignados al identificador de subred.

Ejemplo de Cálculo del Identificador de Subred

Dada una dirección IP y su máscara, el identificador de la subred se obtiene mediante una operación lógica AND:

```
Dirección IP:   200.27.4.112 = 11001000.00011011.00000100.01110000
Máscara:        255.255.255.0 = 11111111.11111111.11111111.00000000
-------------------------------------------------------------------
Subred:         200.27.4.0   = 11001000.00011011.00000100.00000000
```

Interpretación:

- **Dirección IP:** `200.27.4.112` identifica un dispositivo específico en la subred.
- **Máscara:** `255.255.255.0` indica que los primeros 24 bits (3 octetos) corresponden al identificador de subred.
- **Subred:** `200.27.4.0` es el identificador único de la subred a la que pertenece el dispositivo.

Ventajas del Direccionamiento Jerárquico

- **Simplificación del routing:** Reduce el tamaño de las tablas de encaminamiento al agrupar dispositivos en subredes.
- **Escalabilidad:** Permite gestionar redes de gran tamaño de manera eficiente.
- **Flexibilidad:** Las máscaras permiten subdividir redes en subredes más pequeñas para una asignación más granular de direcciones.

Conclusión

El uso de direccionamiento jerárquico y máscaras de red es esencial para la organización eficiente de Internet y la gestión de sus recursos. Estos conceptos son fundamentales para comprender cómo se realiza el encaminamiento y la interconexión de dispositivos en redes modernas.

Internet

Podemos considerar que Internet es un conjunto de subredes interconectadas. ¿Que es ... ?

- **Una subred:** Es una subdivisión lógica de una red IP. Las subredes permiten segmentar una red más grande en redes más pequeñas, lo que facilita la gestión y mejora la eficiencia del uso de direcciones IP.

- **Un switch:** Es un dispositivo de red que conecta múltiples dispositivos dentro de una misma red local (LAN). Los switches operan en la capa de enlace de datos (capa 2 del modelo OSI) y utilizan direcciones MAC para enviar datos al dispositivo de destino correcto.
- **Un router:** Es un dispositivo de red que dirige paquetes de datos entre diferentes redes. Los routers operan en la capa de red (capa 3 del modelo OSI) y utilizan direcciones IP para determinar la mejor ruta para enviar los datos a su destino final.

Para determinar las subredes debemos de separar la interfaz de los hosts de los routers, creando redes aisladas, estas correspondes con las subredes.

¿Quién tiene las direcciones IP?

Los hosts y los routers tienen 1 IP por cada interfaz, mientras que los switches no tienen direcciones.

2.3.3. Elección de la Máscara de Red

La elección de la máscara de red en una subred se basa en el número de dispositivos que se prevé alojar en dicha subred. Esto permite asignar direcciones IP de manera eficiente y evitar desperdiciar recursos.

Cálculo del Número de Dispositivos

El número de direcciones disponibles para dispositivos en una subred se calcula utilizando la fórmula:

$$\#\text{dispositivos} = 2^{\#\text{ceros en la máscara}} - 2$$

- El -2 se debe a que la primera dirección (todos ceros) está reservada para identificar la subred y la última dirección (todos unos) está reservada para difusión (*broadcast*).
- Por ejemplo, una máscara de `/24` (255.255.255.0) tiene 8 bits asignados al identificador de dispositivo, lo que permite $2^8 - 2 = 254$ dispositivos.

Ejemplo Práctico

Consideremos la dirección IP `200.27.4.112` con una máscara de red `255.255.255.0 (/24)`:

- Dirección IP: `200.27.4.112` = `11001000.00011011.00000100.01110000`.
- Máscara: `255.255.255.0` = `11111111.11111111.11111111.00000000`.
- Subred: Realizando una operación lógica AND entre la dirección IP y la máscara, obtenemos:

```
Dirección IP:   200.27.4.112 = 11001000.00011011.00000100.01110000
Máscara:        255.255.255.0 = 11111111.11111111.11111111.00000000
-----------------------------------------------------------------
Subred:         200.27.4.0   = 11001000.00011011.00000100.00000000
```

- Direcciones disponibles:
  - **Reservada para subred:** `200.27.4.0`.
  - **Primer dispositivo:** `200.27.4.1`.
  - **Último dispositivo:** `200.27.4.254`.
  - **Reservada para difusión:** `200.27.4.255`.

Resumen del Ejemplo

La máscara `/24` permite identificar una subred con hasta 254 dispositivos únicos. Este esquema asegura que cada subred tiene:

- Un identificador único dentro de la red mayor.
- Direcciones reservadas para subred y difusión.
- Direcciones suficientes para todos los dispositivos necesarios.

Conclusión

El uso de máscaras ajustadas al tamaño previsto de la subred optimiza la asignación de direcciones IP y facilita la gestión eficiente del espacio de direcciones disponible.

2.3.4. Tipos de direcciones

Para saber que es un *Intranet* pincha aquí.

- Direcciones Públicas: cada dirección se asigna solo a un dispositivo en Internet y se asigna de manera centralizada.
- Direcciones Privadas: solo en intranets, se pueden repetir en distintas intranets. Las asigna el usuario según su criterio.

2.3.5. Direcciones IP: Clases

Las direcciones IP, según el estándar IPv4, tienen un tamaño de **32 bits** y se representan en *notación decimal con puntos*. Cada dirección identifica un dispositivo o interfaz en una red.

Aspectos generales de las direcciones IP

- Cada **host** o **router** tiene una dirección IP para cada una de sus interfaces de red.
- Las direcciones IP están organizadas en **5 clases principales**, descritas en el **RFC 1166**.
- La estructura de las clases determina la jerarquía y el uso de las direcciones:
  - Clases **A**, **B**, y **C** son jerárquicas a dos niveles: *identificador de red* + *identificador de dispositivo*.
  - Clases **D** y **E** tienen propósitos específicos (multidifusión y uso futuro, respectivamente).

Descripción de las Clases

- **Clase A:**
  - Primer bit: 0.
  - Identificador de red: 7 bits.
  - Identificador de host: 24 bits.
  - Rango de direcciones: 0,0,0,0 a 127,255,255,255.
  - Uso: Redes muy grandes, con muchas direcciones de host disponibles.
- **Clase B:**
  - Primeros dos bits: 10.
  - Identificador de red: 14 bits.
  - Identificador de host: 16 bits.
  - Rango de direcciones: 128,0,0,0 a 191,255,255,255.
  - Uso: Redes medianas a grandes.
- **Clase C:**
  - Primeros tres bits: 110.
  - Identificador de red: 21 bits.
  - Identificador de host: 8 bits.
  - Rango de direcciones: 192,0,0,0 a 223,255,255,255.
  - Uso: Redes pequeñas, con pocos dispositivos por red.
- **Clase D:**
  - Primeros cuatro bits: 1110.
  - Rango de direcciones: 224,0,0,0 a 239,255,255,255.
  - Uso: Multidifusión (*multicast*).

- **Clase E:**
  - Primeros cinco bits: 11110.
  - Rango de direcciones: 240,0,0,0 a 255,255,255,255.
  - Uso: Reservadas para propósitos futuros.

Ejemplo

Una dirección IP en clase C, como `192.168.212.60`, tiene la siguiente estructura:

- Identificador de red: 192,168,212.
- Identificador de host: 60.

Para ver detalladamente el cáculo de los rangos pincha aquí.

2.3.6. Clases de Direcciones IP y Reglas Especiales

Las direcciones IPv4 están organizadas en cinco clases principales (A, B, C, D y E) según su propósito y estructura. A continuación, se describen sus rangos, usos y reglas especiales.

Rangos y Capacidad por Clase

- **Clase A:**
  - Rango: `0.0.0.0 - 127.255.255.255`.
  - Redes disponibles: 128 redes.
  - Capacidad: 16,777,216 hosts por red.
- **Clase B:**
  - Rango: `128.0.0.0 - 191.255.255.255`.
  - Redes disponibles: 16,384 redes.
  - Capacidad: 65,536 hosts por red.
- **Clase C:**
  - Rango: `192.0.0.0 - 223.255.255.255`.
  - Redes disponibles: 2,097,152 redes.
  - Capacidad: 256 hosts por red.
- **Clase D:**
  - Rango: `224.0.0.0 - 239.255.255.255`.
  - Uso: Reservado para **multidifusión (multicast)**.
- **Clase E:**
  - Rango: `240.0.0.0 - 255.255.255.255`.
  - Uso: Reservado para **fines futuros**.

Reglas Especiales

- Direcciones con el identificador de host 00 . . . 0:
  - Identifican una red.
  - Nunca se usan como dirección de origen ni se asignan a dispositivos.
- Direcciones con el identificador de host 11 . . . 1:
  - Se utilizan para difusión (**broadcast**) dentro de la red especificada.
  - Nunca se asignan a dispositivos.
- Dirección especial `127.0.0.0`:
  - Reservada para pruebas de **autobucle (loopback)**.
  - Utilizada para comprobar la configuración de red local.
- Restricción adicional:
  - Para evitar ambigüedades, el identificador de dispositivo no debe ser 255 ni 0.

Direcciones IP Privadas (RFC 1918)

El **RFC 1918** reserva rangos de direcciones IP para uso privado dentro de redes internas. Estas direcciones no se enrutan en Internet y se utilizan comúnmente en intranets.

- **Clase A:** `10.0.0.0` – 1 red privada.
- **Clase B:** `172.16.0.0 - 172.31.0.0` – 16 redes privadas.
- **Clase C:** `192.168.0.0 - 192.168.255.0` – 256 redes privadas.

Gestión de Direcciones IP

La asignación y gestión de direcciones IP está a cargo de la organización **IANA (Internet Assigned Numbers Authority)**. Actualmente, esta función es supervisada por **ICANN (Internet Corporation for Assigned Names and Numbers)**, que distribuye bloques de direcciones a organizaciones regionales (RIRs) y locales.

Para ver el cálculo de los hosts y demás pincha aquí.

2.3.7. Agotamiento de Direcciones IPv4 y Transición a IPv6

El agotamiento de las direcciones IPv4 y la implementación de IPv6 marcan un hito importante en la evolución de las redes de comunicación. A continuación, se describen los aspectos clave de este fenómeno.

Agotamiento de Direcciones IPv4 El espacio de direcciones IPv4, con un total de 2^{32} direcciones (4, 294, 967, 296), está prácticamente agotado. Desde noviembre de 2019:

- Sólo quedan disponibles bloques muy pequeños:
  - Bloques `/24`: 256 direcciones.
  - Bloques `/32`: 1 dirección.
- Las direcciones se recuperan de:
  - Sitios obsoletos.
  - Empresas que han desaparecido.
  - Proyectos terminados.
  - Hostings que ya no están en uso.

Este agotamiento ha generado la necesidad de una solución más escalable para manejar el creciente número de dispositivos conectados a Internet.

IPv6: El Futuro del Direccionamiento IPv6 es la versión más reciente del Protocolo de Internet y aborda las limitaciones de IPv4 mediante un esquema de direccionamiento más amplio y eficiente.

Características Principales de IPv6:

- **Longitud de las direcciones:** IPv6 utiliza direcciones de 128 bits, proporcionando un espacio de direccionamiento vastamente mayor.
- **Notación hexadecimal:** Las direcciones se expresan en 8 grupos de 4 dígitos hexadecimales, separados por dos puntos (`:`).
  - Ejemplo: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`.
  - Cada dígito hexadecimal corresponde a 4 bits en binario.
- **Rango de direcciones:**

  `0000:0000:0000:0000:0000:0000:0000:0000` a

  `FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF`.

  Esto equivale a un total de 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones (340 sextillones).
- **Compatibilidad con IPv4:** IPv6 puede coexistir con IPv4 mediante técnicas como el *tunneling* y el uso de direcciones mixtas (IPv4-mapeadas en IPv6).

Ventajas de IPv6

- **Espacio de direcciones prácticamente ilimitado:** Satisface las necesidades de crecimiento de dispositivos conectados.
- **Simplificación del routing:** Reduce la necesidad de NAT (Traducción de Direcciones de Red).
- **Mejoras en la seguridad y la calidad de servicio:** IPv6 incluye soporte nativo para IPSec y etiquetado de tráfico.

2.3.8. NAT(Network Address Translation)

Es un método encargado de reasignar las direcciones (normalmente suelen ser privadas) a otras (públicas) modificando la dirección IP de los paquetes mientras se retransmiten a través de un rooter.

Optimiza el uso de direcciones públicas mediante la utilización de direcciones privadas.

Reemplaza las direcciones privadas origen salientes por públicas y al reves con las reetrantes.

Posee un Tabla de Instrucciones.

Importante: No se puede implementar servidores detrás de un NAT, por ello tiene una zona pública (DMZ) y una privada.

2.3.9. Problema de Escasez de Direcciones IP

El problema de la escasez de direcciones IP surge cuando se necesitan m direcciones, pero solo se dispone de n, siendo $n < m$. Este escenario ha llevado al desarrollo de técnicas como el enmascaramiento y la traducción de direcciones de red (NAT) para optimizar el uso de las direcciones disponibles.

Enmascaramiento (Masquerading) Cuando $n = 1$, se utiliza el enmascaramiento, una técnica en la que una única dirección IP pública se comparte entre múltiples dispositivos en una red privada.

- Es comúnmente usado por los Proveedores de Servicios de Internet (ISPs) para ofrecer acceso a Internet a más usuarios de los que disponen de direcciones IP públicas.
- Supone que no todos los usuarios acceden simultáneamente.
- Las direcciones IP se asignan de forma dinámica a los usuarios a medida que las necesitan.

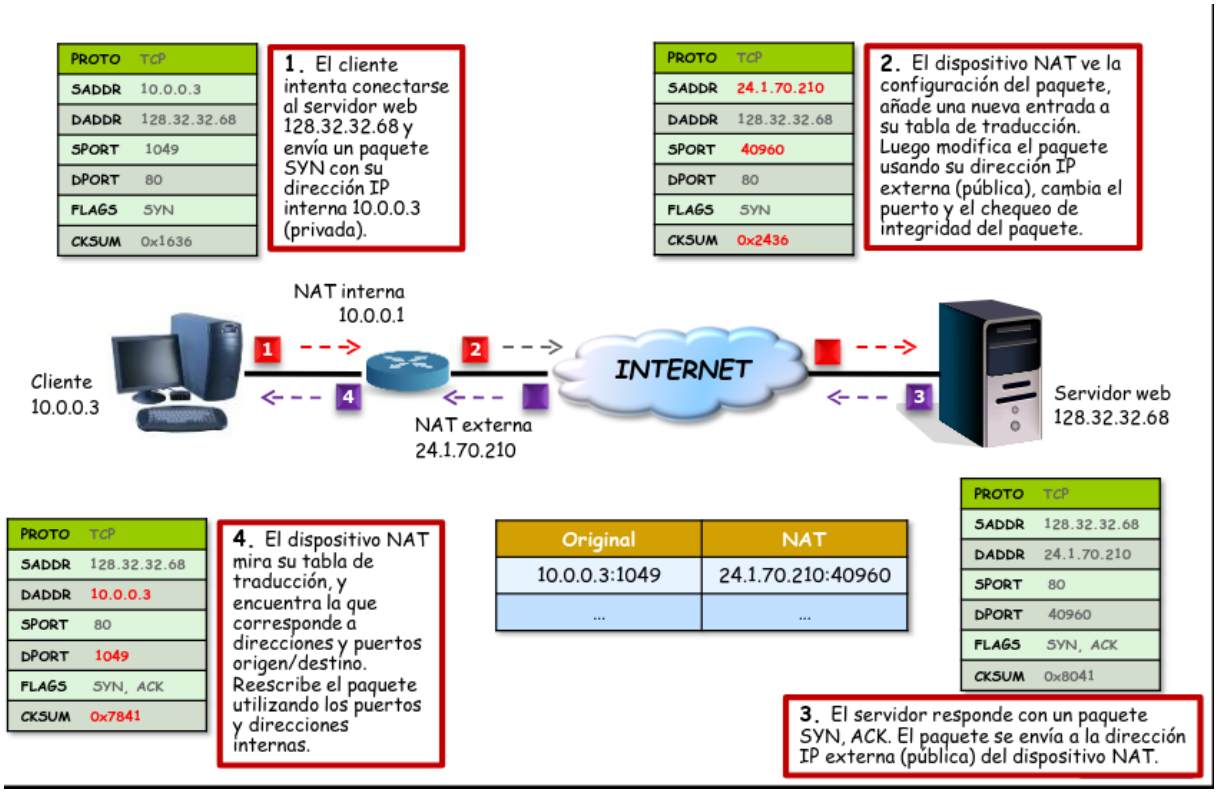
Traducción de Direcciones de Red (NAT) NAT (*Network Address Translation*) es una técnica que permite modificar las direcciones IP en los paquetes que atraviesan un router. Se utiliza para conectar redes privadas con la red pública (Internet). Existen dos tipos principales:

- **SNAT (Source NAT):**
  - Se aplica cuando el origen de los datos está en una red privada.
  - Cambia la dirección IP de origen en los paquetes.
  - Se realiza después del encaminamiento (*postrouting*).
- **DNAT (Destination NAT):**
  - Se aplica cuando el origen de los datos está en la red pública.
  - Cambia la dirección IP de destino en los paquetes.
  - Requiere configurar en el router qué puerto irá dirigido a qué máquina específica.
  - Se realiza antes del encaminamiento (*prerouting*).

Ejemplo de Uso de NAT

- **SNAT:** Un dispositivo en una red doméstica con dirección IP privada 192,168,1,10 envía un paquete a Internet. El router reemplaza la dirección de origen con la dirección IP pública 203,0,113,1.
- **DNAT:** Un paquete entrante desde Internet con destino al puerto 80 de la dirección pública 203,0,113,1 se redirige al servidor web interno con dirección IP 192,168,1,20.

Conclusión Las técnicas de enmascaramiento y NAT han sido fundamentales para mitigar el problema de la escasez de direcciones IPv4, permitiendo un uso más eficiente de las direcciones disponibles. Sin embargo, estas técnicas también introducen desafíos, como la complejidad en la configuración y la pérdida de visibilidad directa de los dispositivos internos en Internet.



2.3.10. Ejercicio de Asignar Direcciones

Enunciado

Vamos a suponer que tenemos redes corporativas con 30 dispositivos, direcciones privadas 192.168.0.0, y subred de acceso: dirección pública (ISP)

Resolución

- Red 1:
  - 30 dispositivos (suponemos que tenemos el router incluido, si no debemos de añadir una dirección para el router)
  - 30 + 1 dirección de red + 1 dirección de broadcast/difusión = 32 direcciones
  - $32 = 2^5$, por lo que necesitamos 5 bits para la subred(para cada equipo)
  - Máscara de red: 32 bits - 5 bits = 27 bits = /27
  - 192.168.0.0/27
    - red: **192.168.0.0**
    - broadcast: 192.168.0.31
- Red 2: **192.168.0.32**
- Red 3: **192.168.0.65**

Pregunta de Examen

¿Se puede varios servidores en un mismo punto en la zona privada? Sí, sin problema, porque lo que debe de ser distinto es el puerto externo.

2.3.11. Encaminamiento

Se tratade encontrar el mejor camino para transportar paquetes desde un origen a un destino. Se decide paquete a paquete y salto a salto en función de la IP destino del paquete y de las tablas de encaminamiento de cada uno de los routers.

Retransmisión salto a salto

Se puede hacer mediante la resolución local del camino o en el dispositivo origen y todos los intermediarios.

Modos de encaminamiento

- Directo: se conoce la dirección IP destino y se envía directamente.
- No Directo: se envía a un router que se encargará de enviarlo al destino.

Nota: Un router suele estar en varias redes distintas, mientras que un host solo está en una red. En caso de que hay un error a la hora de diriguir debido a la tabla de encamiento, se elige a ruta con máscara más larga.

Si no hay fragmentación ni traducción de direcciones (NAT), el datagrama IP no se modifica a lo largo de su recorrido (excepto por campos como el *TTL*, las opciones y el campo de comprobación). A continuación, se describe el proceso de encaminamiento salto a salto para cada datagrama IP:

Proceso de Encaminamiento

- Se extrae la dirección de destino (`IP_DESTINO`) del datagrama.
- Por cada entrada i ($i = 1, \ldots, N$) en la tabla de encaminamiento del nodo, se calcula:
$$\texttt{IPi} = \texttt{IP\_DESTINO}\ \text{AND}\ \texttt{MASCARA\_i}.$$
- Se verifica si `IPi` coincide con el identificador de destino (`Di`):
  - Si hay coincidencia y se trata de un **routing directo**, el datagrama se envía al destino final a través de la interfaz i.
  - Si hay coincidencia pero no es un **routing directo**, el datagrama se envía al siguiente salto (*next hop*) a través de la interfaz i.
- Si hay varias coincidencias, se selecciona la entrada con la máscara más larga (más específica).
- Si no hay coincidencias tras revisar toda la tabla, se genera un error, y es posible que se envíe un mensaje ICMP al origen del datagrama.

Encapsulación del Datagrama Para encapsular el datagrama en una trama física correspondiente (por ejemplo, Ethernet), se debe consultar la tabla ARP (*Address Resolution Protocol*) para obtener la dirección física del siguiente salto:

- Si la dirección física está disponible en la tabla ARP, se utiliza directamente.
- Si no se conoce la dirección física, se envía un mensaje de **broadcast ARP** solicitando la dirección física asociada a la dirección IP destino del enlace.

Resumen del Proceso El encaminamiento en un nodo IP involucra:

1. Determinar la interfaz de salida en función de la tabla de encaminamiento.
2. Encapsular el datagrama en una trama física usando ARP si es necesario.
3. Reenviar el datagrama al destino final (en routing directo) o al siguiente salto (en routing indirecto).

Este proceso se repite en cada nodo intermedio hasta que el datagrama llega a su destino final.

Comparación de Dirección de Destino y máscara

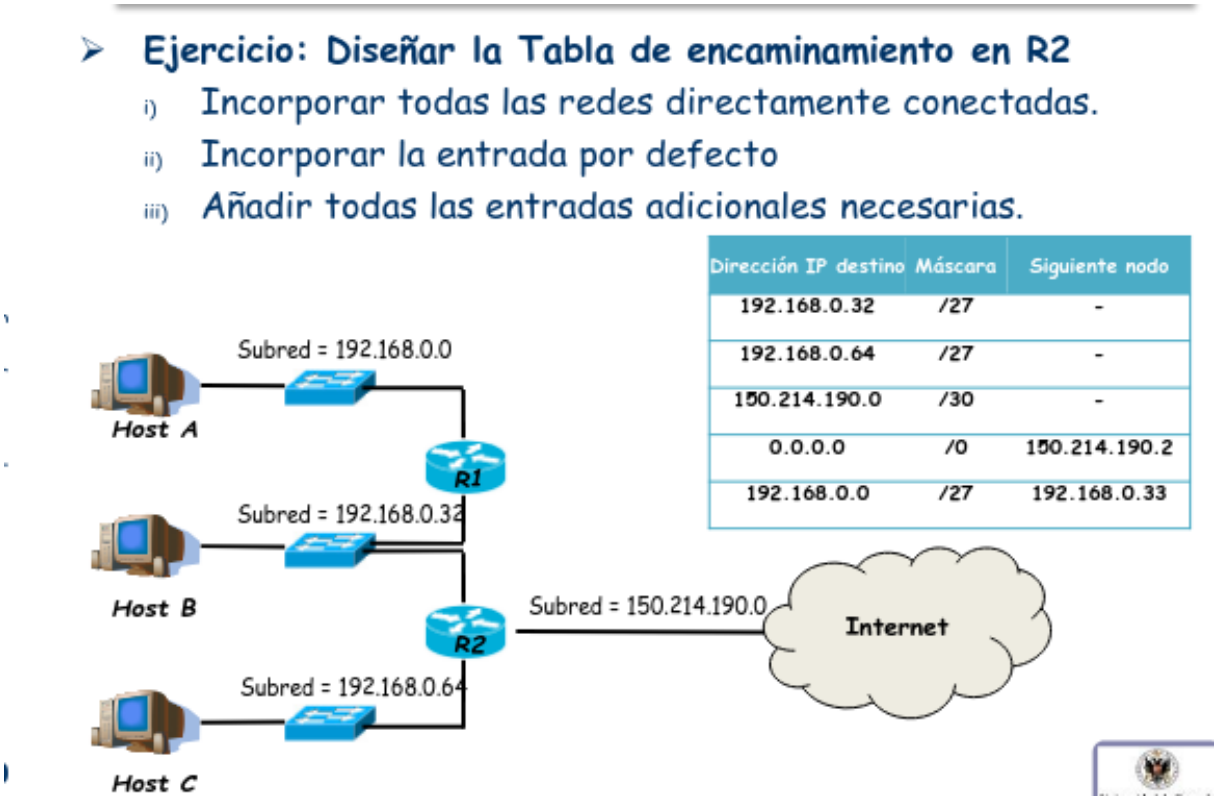
Para adivinar que dirección de destino se va a utilizar, se compara la dirección de destino and máscara con la dirección de la tabla de encaminamiento. Si la dirección de destino es igual a la dirección de la tabla de encaminamiento, se envía directamente, si no, se envía al siguiente salto. *Si hay más de una coincidencia(colisión) se elige la entrada de máscara más restrictiva.*

Problemas de la tabla de encaminamiento

Pueden presentar varios problemas como no direccionar algunos tipos de redes, como Internet y demás. Además, es recomendable usar la entrada por defecto que es la que posee la máscara `0.0.0.0`.

Ejercicio: Diseñar la tabla de encaminamiento de un router

En este caso vamos a diseñar la de R2:



Como podemos ver en esta imagen se trata de asignar en primer lugar las que están más cercanas con una máscara adecuada, luego la del internet, que como dirección de destino usamos la de por defecto ya que no sabemos cómo llegar a ella, y por último la red a la cual tenemos que poner como dirección de destino la más cercana a la red de destino, haciendo de esta manera que el switch haga su función.

Ejercicio

Enunciado

Imagine una situación donde hay cinco routers RA-RE, RA, RB y RC se conectan cada uno a una red local A, B y C, siendo cada router única puerta de enlace de cada red. RA, RB y RD están conectados entre sí a través de un switch. RC, RD y RE están conectados entre sí a través de un switch. RE conecta a Internet a través de la puerta de acceso especificada por el ISP. Especifique tablas de encaminamiento en los routers. Asigne a voluntad las direcciones IP e interfaces necesarias.

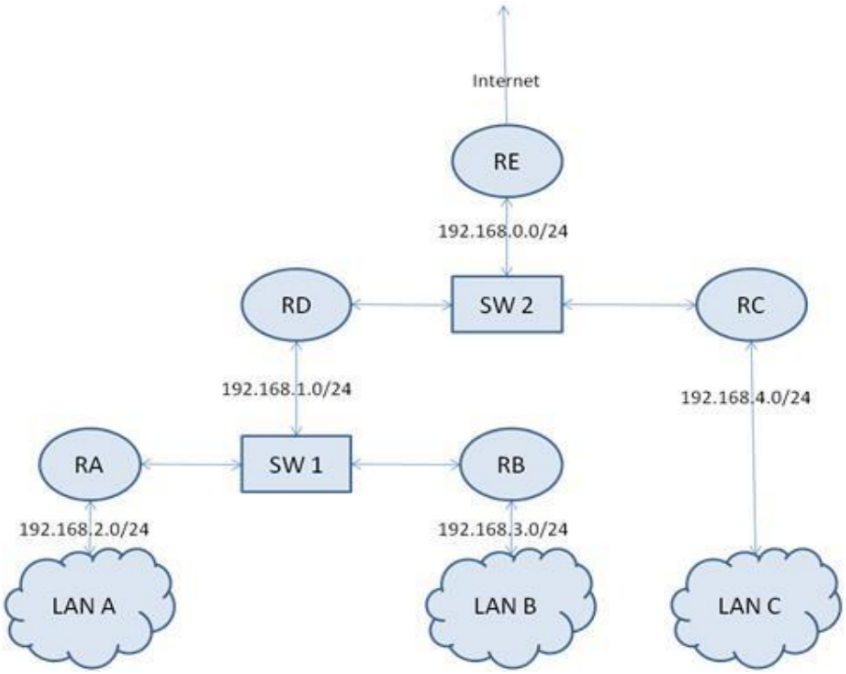


Figura 5: Diagrama de Red

Solución

Asignaremos direcciones IP e interfaces para cada red y router. Luego, especificaremos las tablas de encaminamiento necesarias para cada router.

Direcciones asignadas:

- Red A: 192.168.1.0/24 (RA conectado en interfaz `fa0/0`)
- Red B: 192.168.2.0/24 (RB conectado en interfaz `fa0/0`)
- Red C: 192.168.3.0/24 (RC conectado en interfaz `fa0/0`)
- Conexión RA-RB-RD: 192.168.4.0/24
- Conexión RC-RD-RE: 192.168.5.0/24
- Conexión RE-ISP: 203.0.113.0/24

Tablas de encaminamiento:

Router RA:

Red Destino	Máscara	Puerta de Enlace	Interfaz
192.168.2.0	255.255.255.0	192.168.4.2	`fa0/1`
192.168.3.0	255.255.255.0	192.168.4.3	`fa0/1`
203.0.113.0	255.255.255.0	192.168.4.3	`fa0/1`

Router RB:

Red Destino	Máscara	Puerta de Enlace	Interfaz
192.168.1.0	255.255.255.0	192.168.4.1	`fa0/1`
192.168.3.0	255.255.255.0	192.168.4.3	`fa0/1`
203.0.113.0	255.255.255.0	192.168.4.3	`fa0/1`

Router RC:

Red Destino	Máscara	Puerta de Enlace	Interfaz
192.168.1.0	255.255.255.0	192.168.5.2	`fa0/1`
192.168.2.0	255.255.255.0	192.168.5.2	`fa0/1`
203.0.113.0	255.255.255.0	192.168.5.3	`fa0/1`

Router RD:

Red Destino	Máscara	Puerta de Enlace	Interfaz
192.168.1.0	255.255.255.0	192.168.4.1	`fa0/0`
192.168.2.0	255.255.255.0	192.168.4.2	`fa0/0`
192.168.3.0	255.255.255.0	192.168.5.1	`fa0/1`
203.0.113.0	255.255.255.0	192.168.5.3	`fa0/1`

Router RE:

Red Destino	Máscara	Puerta de Enlace	Interfaz
192.168.1.0	255.255.255.0	192.168.5.1	`fa0/0`
192.168.2.0	255.255.255.0	192.168.5.1	`fa0/0`
192.168.3.0	255.255.255.0	192.168.5.1	`fa0/0`

Esto asegura que cada router pueda alcanzar las demás redes y enrutar tráfico hacia Internet a través de RE.

Aumento de escalabilidad y de administración

Internet se jerarquiza mediante Sistemas Autónomos(SA). Un SA es un conjunto de redes y de routers que son gestionados por una autoridad. Cada uno informa a otros SA de las redes accesibles, existen un router responsable de ello, llamado router exterior. Cada uno de los SA se identifica mediante un entero de 16 bits **pero, desde 2007 es de 32 bits**.

Niveles de Encaminamiento

- **Algoritmos IGP (Interior Gateway Protocol):**
  - Se utilizan dentro de un Sistema Autónomo (SA) para el encaminamiento de paquetes.
  - Los administradores de red tienen libertad para elegir el protocolo que mejor se adapte a sus necesidades.
  - Ejemplos comunes incluyen:
    - **OSPF (Open Shortest Path First):** Un protocolo de estado de enlace que utiliza el algoritmo de Dijkstra para calcular la ruta más corta.
    - **RIP (Routing Information Protocol):** Un protocolo de vector de distancia que utiliza el número de saltos como métrica.
    - **EIGRP (Enhanced Interior Gateway Routing Protocol):** Un protocolo híbrido desarrollado por Cisco que combina características de los protocolos de vector de distancia y de estado de enlace.
- **Algoritmos EGP (Exterior Gateway Protocol):**
  - Se utilizan para el encaminamiento de paquetes entre diferentes Sistemas Autónomos (SA).
  - En Internet, existe una norma única para el encaminamiento entre SA, que es el protocolo BGP.

- **BGP (Border Gateway Protocol):**
  - Es el protocolo estándar utilizado para el intercambio de información de encaminamiento entre Sistemas Autónomos.
  - Utiliza una tabla de encaminamiento para mantener la información de las rutas disponibles y toma decisiones basadas en políticas configuradas por los administradores de red.
  - BGP es un protocolo de vector de ruta que considera múltiples atributos para determinar la mejor ruta.

Diferentes protocolos

- RIP (Routing Information Protocol)

RIP ("Routing Information Protocol" RFC 1058, 2453, 4822)

- **Protocolo de la capa de aplicación:** Opera sobre UDP, puerto 520.
- **Algoritmo:** Vector-distancia (métrica basada en el número de saltos).
- **Funcionamiento:**
  - Periódicamente (por defecto cada 30 segundos), cada router RIP recibe de todos sus vecinos (usando la dirección multicast `224.0.0.9`) los vectores-distancia para todos los posibles destinos.
  - Para cada destino, se selecciona como siguiente salto el vecino que anuncie el menor coste. La métrica para ese destino se actualiza sumando uno al coste anunciado.
- **Problemas:**
  - **Convergencia lenta:** Las malas noticias tardan en propagarse.
  - **"Cuenta al infinito":** Los costos pueden incrementarse indefinidamente.
- **Soluciones:**
  - Split horizon.
  - Hold down.
  - Poison reverse.
- **Comando útil:** Para más detalles, consultar el manual del comando `routed` en sistemas Linux (`man routed`).

- OSPF

OSPF (RFC 2328)

- Basado en estado del enlace (*link state*), donde el coste es proporcional a 1/velocidad del enlace.
- Permite rutas alternativas y balanceo de carga.

- Gestión en base a áreas independientes.
- Minimiza difusión mediante routers designados (*Designated Routers, DR*).
- Mensajes utilizados:
  - Hello.
  - Database description.
  - Link status request, update y acknowledgment.

Enlace de imagen: `https://i0.wp.com/theosnews.com/wp-content/uploads/2015/05/2-Configuraci%C3%B3n-de-OSPF-Redes-directamente-conectadas.jpg?ssl=1`

Pregunta de Examen

Si R1 quiere ir a R3 por dos caminos con el mismo número de saltos pero con A=100Mbps y B=10Mbps,¿Cuál cojo? Solo cojo un camino si mejora el primero que me dan.

2.3.12. Formato del Datagrama

Imagen: pincha aquí.

2.3.13. Fragmentación IPv4

La fragmentación en IPv4 es un mecanismo que permite dividir un datagrama en fragmentos más pequeños para que puedan adaptarse al tamaño máximo permitido por la Unidad Máxima de Transferencia (*MTU*) de las subredes por las que pasa. A continuación, se explican los aspectos más relevantes:

- **Tamaño máximo del datagrama:** El tamaño máximo permitido para un datagrama IPv4 es de 65535 bytes ($2^{16} - 1$), incluyendo el encabezado y los datos.
- **Adaptación a la MTU:** Cada enlace en una red puede tener una MTU diferente. Si el tamaño de un datagrama excede la MTU de una subred, debe ser fragmentado para poder ser transmitido.
- **Ensamblado en el destino final:** Los fragmentos de un datagrama solo pueden ser ensamblados en el destino final. Los nodos intermedios no realizan ensamblado, lo que evita complejidad adicional en el encaminamiento.
- **Desplazamiento (*offset*):** Cada fragmento incluye un campo que indica su posición relativa dentro del datagrama original. Esto permite que los fragmentos se ensamblen correctamente en el destino final.
- **Indicadores de control:**
  - **Don't Fragment (DF):** Si este indicador está activado, el datagrama no puede ser fragmentado. Si el datagrama excede la MTU, se descarta y se envía un mensaje ICMP al origen.
  - **More Fragments (MF):** Este indicador se activa para todos los fragmentos excepto el último, indicando que el datagrama original está dividido en partes.

Ejemplo de Fragmentación Supongamos un datagrama con un tamaño total de 4000 bytes que necesita ser transmitido a través de una subred con una MTU de 1500 bytes. La fragmentación se realiza de la siguiente manera:

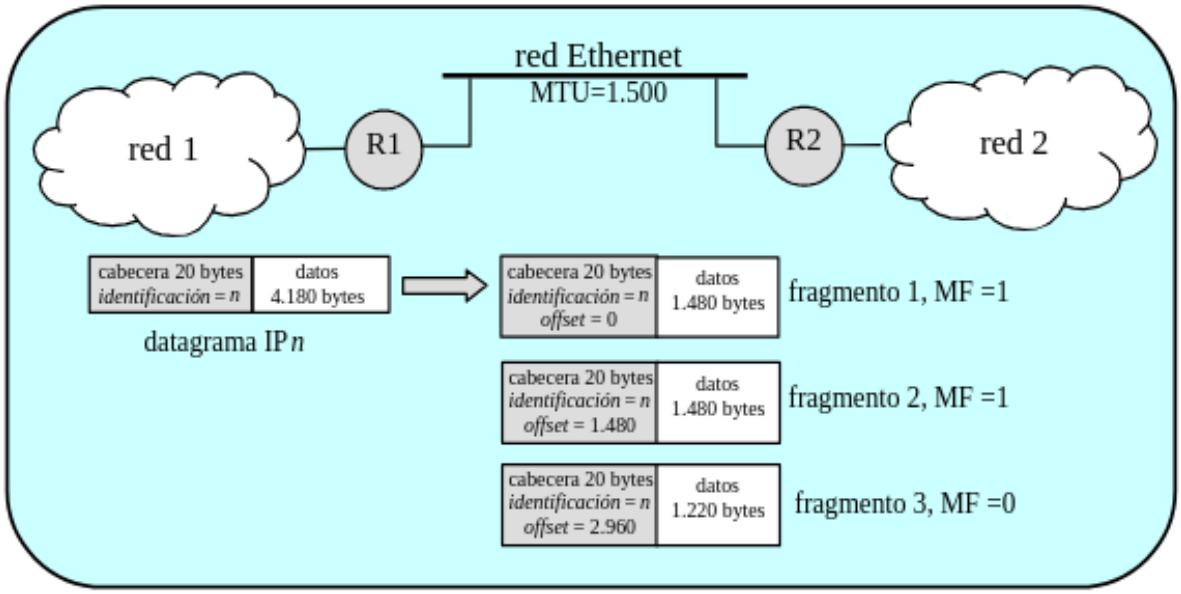
- El encabezado IP ocupa 20 bytes, dejando 1480 bytes para los datos en cada fragmento.
- Se generan los siguientes fragmentos:
  - **Fragmento 1:** Datos del byte 0 al byte 1479 (`offset = 0`).
  - **Fragmento 2:** Datos del byte 1480 al byte 2959 (`offset = 185`, ya que cada unidad de *offset* corresponde a 8 bytes).
  - **Fragmento 3:** Datos del byte 2960 al byte 3999 (`offset = 370`, último fragmento con `MF = 0`).

Para profundizar en el tema de offset picha aquí.

Ventajas y Desventajas de la Fragmentación

- **Ventajas:** Permite la transmisión de datagramas grandes a través de redes con diferentes MTUs.
- **Desventajas:** Introduce sobrecarga adicional en términos de encabezados y complica el ensamblado en el destino. Además, si un fragmento se pierde, el datagrama completo debe ser retransmitido.

2.3.14. Ejercicio Típico de Examen sobre la fragmentacion IPv4



Comentarios del Ejercicio

Para la realización del ejercicio debemos de seguir los siguientes pasos y repetirlos hasta que no se necesiten más fragmentos, es decir, hasta que el MF = 0. Debemos de

tener en cuenta que la cabecera ocupa siempre 20 bytes, por lo tanto, si nuestro MTU es 1500, solo podremos transportar el paquete en unidades de 1480 bytes, siendo esto el valor máximo. El offset mide el desplazamiento del paquete, en otras palabras, la suma total de los bytes que se han transmitido.

2.3.15. Diferencias entre IPv4 y IPv6

Característica	**IPv4**	**IPv6**
Longitud de la dirección	32 bits	128 bits
Espacio de direcciones	~4.3 mil millones	340 undecillones (casi ilimitado)
Formato	Decimal (ej. 192.168.0.1)	Hexadecimal (ej. 2001:0db8:8a2e:0370:7334)
Configuración	Manual o DHCP	Autoconfiguración sin estado (SLAAC)
Seguridad	Opcional (IPsec)	IPsec obligatorio
Fragmentación	Los routers pueden fragmentar	Solo el dispositivo emisor fragmenta
Encabezado de paquetes	Complejo y variable	Simplificado y fijo
QoS	Limitado (TOS)	Optimizado (Flow Label)
Compatibilidad	Amplia, pero limitado por direcciones	No compatible directamente con IPv4
Optimización para móviles	Menos eficiente	Mejor rendimiento en redes móviles

Tabla comentada

- **Longitud de la dirección:**
  - IPv4 utiliza direcciones de 32 bits, lo que limita el espacio de direcciones disponibles.
  - IPv6 expande las direcciones a 128 bits, proporcionando un espacio de direccionamiento prácticamente ilimitado.
- **Espacio de direcciones:**
  - IPv4 puede manejar aproximadamente 4.3 mil millones de direcciones únicas, un recurso que ya se ha agotado en gran medida.
  - IPv6 proporciona 340 undecillones de direcciones, suficientes para las necesidades actuales y futuras.
- **Formato:**
  - IPv4 utiliza un formato decimal, como `192.168.0.1`.

  - IPv6 adopta un formato hexadecimal, más eficiente para expresar direcciones largas, como `2001:0db8:8a2e:0370:7334`.

- **Configuración:**
  - IPv4 requiere configuración manual o el uso de DHCP.
  - IPv6 ofrece autoconfiguración sin estado mediante SLAAC, simplificando la gestión de redes.
- **Seguridad:**
  - IPv4 soporta IPsec de forma opcional.
  - IPv6 integra IPsec de manera obligatoria, mejorando la seguridad por defecto.
- **Fragmentación:**
  - En IPv4, los routers pueden fragmentar los paquetes.
  - En IPv6, la fragmentación solo se realiza en el dispositivo emisor, mejorando la eficiencia del encaminamiento.
- **Encabezado de paquetes:**
  - IPv4 tiene un encabezado complejo y variable, lo que puede aumentar la latencia.
  - IPv6 utiliza un encabezado simplificado y fijo, optimizando el procesamiento en los nodos.
- **Calidad de servicio (QoS):**
  - IPv4 ofrece un soporte limitado mediante el campo TOS (*Type of Service*).
  - IPv6 mejora la QoS mediante etiquetas de flujo (*Flow Label*), proporcionando mayor granularidad.
- **Compatibilidad:**
  - IPv4 es ampliamente compatible con sistemas y dispositivos existentes.
  - IPv6 no es directamente compatible con IPv4, lo que requiere mecanismos de transición como túneles o direcciones mixtas.
- **Optimización para móviles:**
  - IPv4 es menos eficiente en redes móviles.
  - IPv6 está diseñado para mejorar el rendimiento en estas redes, adaptándose a las necesidades modernas.

2.4. Asociación de la capa de enlace: protocolo ARP

2.4.1. Direcciones MAC

Las direcciones **MAC (Medium Access Control)** son identificadores únicos que se utilizan para direccionar paquetes a nivel de la capa de enlace en redes Ethernet (cableadas) y WiFi. Estas direcciones juegan un papel clave en el encaminamiento de datos dentro de una red local.

Uso de las Direcciones MAC Una vez que se realiza la redirección a nivel de IP, el paquete debe ser enviado a la dirección MAC del siguiente nodo en la ruta hacia el destino final. Este proceso asegura que los datos lleguen al nodo correcto dentro de la red local antes de ser enviados a la siguiente etapa.

Formato de las Direcciones MAC Las direcciones MAC tienen un formato estándar de 6 bytes (48 bits) representados en notación hexadecimal y separados por guiones:

```
HH-HH-HH-HH-HH-HH
```

Por ejemplo:

```
00-24-21-A8-F7-6A
```

Asignación de Direcciones MAC

- Cada dirección MAC es única y está asignada por la **IEEE (Institute of Electrical and Electronics Engineers)**.
- Las direcciones se asignan en lotes de 2^{24} direcciones para cada fabricante de dispositivos de red.

Dirección de Difusión (Broadcast) En las redes locales, la dirección **FF-FF-FF-FF-FF-FF** se utiliza para enviar paquetes a todos los dispositivos conectados en la red. Esto es útil para realizar descubrimientos, como en el caso del protocolo ARP (Address Resolution Protocol).

Para ver el formato ARP accede al siguiente enlace: `https://i.ytimg.com/vi/qJZzX0V8Opg/maxresdefault.jpg`

Resumen Las direcciones MAC son esenciales para la comunicación dentro de redes locales, permitiendo la identificación única de dispositivos y facilitando tanto la comunicación unicast (entre dos nodos específicos) como la difusión a todos los nodos de la red.

2.5. El Protocolo ICMP

El **ICMP (Internet Control Message Protocol)** es un protocolo de la capa de red utilizado para gestionar y reportar situaciones de error o eventos relacionados con el funcionamiento de IP. Se clasifica como un protocolo de señalización, ya que no transporta datos de usuario, sino información sobre el estado de la red.

Características del Protocolo ICMP

- **Propósito:** ICMP se utiliza para informar sobre errores en el funcionamiento de IP y para facilitar diagnósticos de red.
- **Dirección del mensaje:** Los mensajes ICMP suelen enviarse hacia el origen del datagrama IP que generó el evento, excepto en casos como solicitudes de eco (*ping*).
- **Encapsulación:** Los mensajes ICMP se encapsulan dentro de paquetes IP para su transmisión.
- **Cabecera:** La cabecera ICMP tiene un tamaño fijo de 32 bits y contiene la siguiente información:
  - **Tipo (8 bits):** Indica el tipo de mensaje ICMP.
  - **Código (8 bits):** Especifica el subtipo del mensaje, proporcionando mayor detalle.
  - **Comprobación (16 bits):** Un campo para la detección de errores en el mensaje ICMP.
- **Incluye información del datagrama original:** El mensaje ICMP incluye la cabecera del datagrama IP que disparó el evento, para que el origen pueda identificar el problema.

Tipos Comunes de Mensajes ICMP

- **Destino inalcanzable:** Informa al origen que un datagrama no pudo ser entregado.
- **Tiempo excedido:** Indica que un datagrama ha sido descartado porque excedió su tiempo de vida (*Time-to-Live, TTL*).
- **Redirección:** Notifica a un host que debe utilizar otra ruta para alcanzar un destino.
- **Solicitud y respuesta de eco (*Ping*):** Se utiliza para comprobar la conectividad y medir el tiempo de respuesta entre dos dispositivos.

Resumen

El protocolo ICMP es una herramienta esencial para la gestión de redes IP. Al proporcionar información sobre errores y diagnósticos, permite mantener la integridad y el rendimiento de la comunicación en la red. Aunque no transporta datos de usuario, su papel en la señalización lo convierte en un componente fundamental de la capa de red.

Para ver los mensajes ICMP, accede a este enlace: `https://w3.ual.es/~vruiz/Docencia/Apuntes/Networking/Protocols/Level-3/04-ICMP/mensajes_ICMP.png`

2.6. DHCP: Autoconfiguración de la capa de red

El **DHCP (Dynamic Host Configuration Protocol)** es un protocolo de red que permite a los dispositivos obtener automáticamente configuraciones esenciales para su conexión en una red IP. Es ampliamente utilizado para asignar dinámicamente direcciones IP, así como otros parámetros de configuración de red.

Funcionamiento del DHCP

El protocolo DHCP sigue un modelo cliente-servidor en el que los clientes solicitan información de configuración y el servidor responde con los datos necesarios. El proceso se compone de cuatro etapas principales:

1. **Discover:** El cliente envía un mensaje de difusión DHCP Discover buscando servidores DHCP disponibles en la red.
2. **Offer:** El servidor responde con un mensaje DHCP Offer, que incluye una dirección IP disponible y otros parámetros.
3. **Request:** El cliente envía un mensaje DHCP Request indicando su intención de usar la dirección IP ofrecida.
4. **Acknowledge:** El servidor confirma la asignación con un mensaje DHCP Acknowledge, y el cliente puede comenzar a usar la dirección IP.

Parámetros Configurados por DHCP

El servidor DHCP no solo asigna direcciones IP, sino que también puede proporcionar otros parámetros de configuración importantes, tales como:

- Máscara de subred.
- Puerta de enlace predeterminada (*default gateway*).
- Servidores DNS.
- Tiempo de arrendamiento (*lease time*) para la dirección IP asignada.
- Opciones específicas de la red, como rutas estáticas.

Ventajas del DHCP

- **Automatización:** Reduce la necesidad de configurar manualmente cada dispositivo en la red.
- **Eficiencia:** Permite reutilizar direcciones IP, lo que es especialmente útil en redes con un número limitado de direcciones disponibles.
- **Facilidad de gestión:** Centraliza la administración de la configuración de red.

Desventajas del DHCP

- **Dependencia del servidor:** Si el servidor DHCP falla, los nuevos dispositivos no podrán obtener configuración de red.
- **Falta de control fijo:** Aunque es posible asignar direcciones fijas, DHCP está diseñado principalmente para asignaciones dinámicas.

Ejemplo de Funcionamiento

Proceso de una sesión DHCP entre cliente y servidor: https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhyvPCPxrYJdM7ra-zKKv-9ptw5el9t7mQUvzKB6GGjV8I07_0URHw1aHtl652KsklN0Eac_Wr6-gvvJzzPccANoflbWWt0KkuT3zidC59Do4A8bCYHDoe/s1600/DHCP_Cliente_Servidor.png

Resumen

El protocolo DHCP es fundamental para la gestión dinámica y automatizada de redes IP. Su capacidad para asignar y gestionar parámetros de configuración de red de manera eficiente lo convierte en una herramienta esencial en redes modernas, tanto domésticas como empresariales.