8. Introducción a los sistemas en red. Direccionamiento IP

Autor	Xerach Casanova
Clase	Sistemas Informáticos
Fecha	@Feb 22, 2021 7:40 PM

1. Redes. Características y clasificación

Se define una red informática como dos o más dispositivos conectados que comparten componentes de su red e información que se pueda almacenar en todos ellos. Según Andrew S. Tanenbaum es un conjunto de equipos

informáticos conectados entre sí, por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con el fin de compartir información y recursos.

Redes de ordenadores. Ventajas.

Conectando dos ordenadores entre sí ya tenemos una red. A medida que vamos añadiendo más ordenadores, impresoras, o salimos a internet, conseguimos que la red cada vez sea más potente.

Las principales ventajas son:

- Posibilidad de compartir recursos.
- Posibilidad de compartir información.
- Aumentar posibilidades de colaboración.
- Facilitar la gestión centralizada.
- Reducir costes.

Clasificación de redes. Tipos de redes.

Se clasifican según diferentes conceptos:

- **Por alcance o extensión:**
  - **Red de área local o LAN (local area network),** es una red que se limita a un área especial, relativamente pequeña: un cuarto, un aula, un solo edificio, una nave o un avión. Suelen tener mayores velocidades y la unión de ellas crean redes más grandes.
  - **Red de área metropolitana o MAN (metropolitan area network).** Red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa. Define redes que abarcan extensiones relativamente grandes y necesitan recursos adicionales a los que ofrece una red local.
  - **Red de área amplia o WAN (wide area network).** Redes informáticas extendidas sobre un área geográfica extensa. Encontramos redes de telecomunicaciones que permiten el uso de internet. Internet se considera una gigantesca red WAN.
- **Según las funciones de sus componentes.**
  - **Redes de igual a igual entre iguales o peer-to-peer,** redes donde ningún ordenador está a cargo del funcionamiento de la red. Cada

ordenador controla su propia información y funciona como cliente o servidor según lo necesite. Los S.O. más utilizados posibilitan trabajar de esta manera.

- **Redes cliente - servidor.** Se basan en la existencia de uno ovarios servidores que dan servicio al resto de ordenadores, considerados clientes. Facilitan la gestión centralizada. Para ello se necesitan S.O. de tipo servidor como Windows Server o GNU-Linux.
- **Según el tipo de conexión.**
  - Redes cableadas: se utilizan diferentes tipos de cables para conectar los ordenadores.
  - Redes inalámbricas: no necesitan cables para comunicarse.
- **Según el grado de difusión.**
  - **Internet.** Un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única de alcance mundial.
  - **Intranet.** Es una red de ordenadores que utiliza alguna tecnología de red para usos comerciales, educativos o de otra índole de forma privada. No comparte sus recursos o su información con otras redes. Aunque la intranet no está conectada a internet, también utiliza protocolos TCP/IP.

2. Arquitectura de la red. Modelos OSI y TCP/IP

La arquitectura de una red se refiere a como está construida con el hardware (cables, equipos y conexiones) y el software utilizado.

Aparte de decidir que equipos se van a utilizar para la conexión, también se van a definir unos protocolos en la comunicación. Estos protocolos marcan la forma de comunicarse de dos dispositivos físicos.

La arquitectura de red tiene en cuenta tres factores:

- **Topología.** La forma en que se conectan los distintos nodos de una red.
- **Método de acceso:** medio utilizado para transmisión de datos: cable, aire.

- **Protocolos de comunicación.**

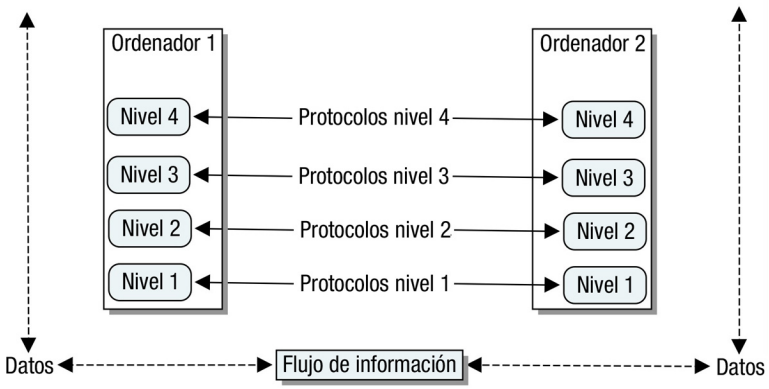
Protocolo de comunicación.

Es un conjunto de reglas normalizadas para la representación, señalización, autenticación y detección de errores necesario para enviar información a través de un canal de comunicación.

Se necesitan distintos protocolos para:

- Identificar el emisor y el receptor.
- Definir el medio o canal que se puede utilizar en la comunicación.
- Definir el lenguaje común a utilizar.
- Definir la forma y estructura de los mensajes.
- Establecer la velocidad y temporización de los mensajes.
- Definir la codificación y encapsulación del mensaje.

Modelos por capas o niveles



La arquitectura de red se divide en niveles o capas para reducir la complejidad de su diseño. Las capaz están jerarquizadas y tienen sus servicios y funciones asignadas, para lo que se utilizan los protocolos necesarios. Cada nivel solo se comunica con el nivel superior o el inferior.

En la figura, supongamos que el primer ordenador quiere realizar una transferencia al segundo ordenador. La capa superior es donde se ordena realizar la transferencia, pero no se fija en los detalles de como llegar al otro PC, su dirección, ruta, medio de transmisión etc..., los cuales se definen en las capas inferiores. El recorrido es el siguiente: Se va pasando desde la capa superior hasta la inferior, donde cada capa realiza sus funciones. Desde la

primera capa se pasa información al ordenador de destino a su primera capa, y ya en el ordenador destino se sigue la secuencia contraria, subiendo de capa en capa, para que la capa superior solo conozca los datos recibidos y no los detalles de como le llegó la información.

En este tipo de arquitectura cada nivel genera su propio conjunto de datos que se pasa con los datos originales a la siguiente capa. Facilitan compatibilidades, tanto de software como de hardware, pues no es necesario cambiar todas las capas cuando se mejora el sistema, basta con modificar los protocolos.

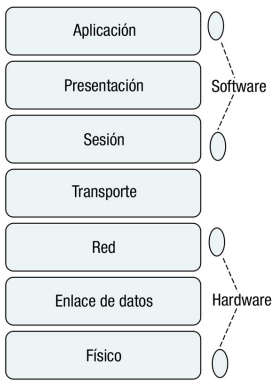
2.1. Modelo OSI.

Open System Interconnection (interconexión de sistemas abiertos), es el modelo de red creado por la Organización Internacional para la Normalización (ISO) en el año 84.

Agrupa procesos de comunicación en siete capas que realizan tareas diferentes. Es conveniente tener en cuenta que el modelo OSI no es una arquitectura desarrollada en ningún sistema, solo una referencia para desarrollar arquitecturas de red, para que los protocolos que se desarrollen puedan ser conocidos por todos.

Los niveles o capas OSI son:

- **Capa 1 - capa física.** Se encarga de las conexiones físicas, incluye cableado y componentes necesarios para transmitir señal.
- **Capa 2 - capa de enlace de datos.** Empaqueta los datos para transmitirlos a través de la capa física. En esta capa se define el direccionamiento físico utilizando direcciones MAC. Además se encarga del acceso al medio, el control de enlace lógico y detección de errores de transmisión.
- **Capa 3 - capa de red.** Separa datos en paquetes, determina la ruta que tomarán los datos y define el direccionamiento.
- **Capa 4 - capa de transporte.** Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar errores.



- **Capa 5 - capa de sesión.** Mantiene y controla el enlace entre los dos extremos de la comunicación.
- **Capa 6 - capa de presentación.** Determina el formato de las comunicaciones, así como adaptar la información al protocolo que se está usando.
- **Capa 7 - capa de aplicación.** Define los protocolos que utilizan cada una de las aplicaciones para poder se utilizadas en red.

La capa 4 es una capa intermedia, la 1, 2 y 3 se relacionan con el hardware, mientras que la 5, 6 y 7 se relacionan con el software.

2.2. Modelo TCP

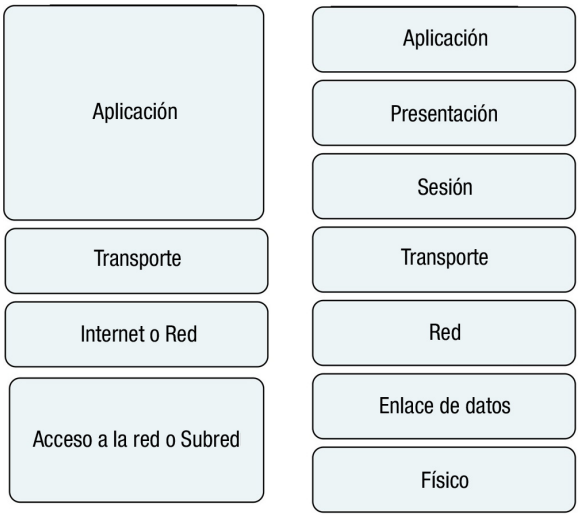
Es la arquitectura de redes más utilizada y la base de comunicaciones de internet y de los sistemas operativos modernos.

Es un conjunto de reglas generales de diseño e implementación de protocolos de red, permiten la comunicación entre ordenadores. Su nombre equivale a los dos protocoles más importantes que utiliza:

TCP (Protocolo de control de transmisión) y protocolo IP (Protocolo de internet).

Está compuesto por cuatro capas o niveles:

- **Nivel de subred, nivel de acceso a la red o nivel de alcance:** Se encarga del acceso al medio de transmisión (similar a los niveles 1 y 2 del modelo OSI). Permite y define el uso de direcciones físicas con direcciones MAC.
- **Nivel de red o nivel de internet:** equivale a la capa 3 del modelo OSI, se encarga de estructurar la información en paquetes y determinar la ruta del PC origen al destino que tomarán los paquetes.
- **Nivel de transporte.** Equivale a la capa 4 del modelo OSI, se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar errores. Los protocolos más importantes de esta capa son TCP y UDP, el protocolo orientado a conexión y fiable y el protocolo UDP es un protocolo no orientado a conexión y no fiable.
- **Nivel de aplicación.** Engloba las capas 5, 6 y 7 del modelo OSI e incluye todos los protocolos de alto nivel relacionados con las aplicaciones que se utilizan en internet.



2.2.1. Nivel 1. Nivel de enlace o acceso

Convierte la información suministrada por el nivel de red en señales que se puedan transmitir por el medio físico al destino y viceversa.

En este nivel se tienen en cuenta las conexiones físicas definidas por el estándar IEEE 802.3.

El aspecto más importante de este nivel es el direccionamiento físico, conocido como acceso al medio (MAC). Es un identificador de 48 bits, que se representa con 12 dígitos hexadecimales: FF:FF:FF:FF:FF:FF

Todas las tarjetas de red tienen una dirección física o dirección MAC única en el mundo, los seis primeros dígitos hexadecimales corresponden al fabricante de la tarjeta de red.

En este nivel hay dos protocolos relacionados con el direccionamiento físico:

- ARP (Address Resolution Protocol). Se encarga de relacionar la dirección MAC con la correspondiente dirección lógica (IP). La dirección física trabaja a nivel subred y la lógica a nivel red.
- RARP (Reverse ARP, protocolo de resolución de nombres inverso), realiza la función contraria.

2.2.2. Nivel 2. Nivel de red

El objetivo principal del nivel de red es encaminar los paquetes desde el nodo de origen hasta el nodo destino, aunque estén en redes distintas. La capa de red no se preocupa de la ordenación de los paquetes, esto es servicio no orientado a conexión. Cada paquete recibe el nombre de datagrama.

Las funciones más importantes de la capa de red son:

- **Direccionamiento lógico.** Permite identificar de forma única cada nodo de red. Reciben el nombre de IP.
- **El enrutamiento** o encaminamiento. Los protocolos de esta capa deben ser capaces de encontrar el mejor camino entre dos nodos.

Para realizar estas funciones el nivel de red utiliza como protocolos:

- **IP:** Internet Protocol, proporciona un enrutamiento de paquetes no orientado a conexión y es usado tanto por el origen como por el destino para comunicación de datos. También proporciona direcciones IP, que es la dirección lógica que identifica dentro de una red a un nodo o tarjeta de red. Hay dos versiones: IPv4 e IPv6 y se diferencian en el número de bits (32 y 128 respectivamente).
- **ARP y RARP.** También se utiliza en la capa de subred de datos y relaciona direcciones IP con direcciones MAC y viceversa.
- **ICMP.** Protocolo de mensajes de control en internet. Suministra capacidades de control y envío de mensajes. Se considera también protocolo del nivel de transporte y herramientas como ping y tracert lo utilizan para funcionar.

2.2.3. Nivel 3. Nivel de transporte

Crea reglas necesarias para establecer una conexión entre dos dispositivos remotos.

En este nivel se cuidan los detalles de la transferencia libre de errores entre el emisor y el receptor.

La información que maneja esta capa también tiene su propio nombre y se llama segmento. La capa de transporte se encarga de unir múltiples segmentos del mismo flujo de datos.

Los dos protocolos más importantes son:

TCP es un protocolo orientado a conexión y fiable. Está diseñado específicamente para proporcionar un flujo de bytes confiable de extremo a extremo a través de redes no fiables. TCP tiene un diseño que se adapta de manera dinámica a las propiedades de las distintas redes y situaciones.

UDP es un protocolo no orientado a conexión y no fiable. Proporciona lo necesario para que las aps envíen datagramas IP encapsulados sin tener una conexión establecida. Se utiliza en transmisión de audio y video en tiempo real.

2.2.4. Nivel 4. Nivel de aplicación

En este nivel se incluyen los protocolos de alto nivel que utilizan los programas o servicios para comunicarse:

- **HTTP**. Protocolo de transferencia de hiper texto, utilizado en páginas web. Es un protocolo orientado a transacciones y sigue esquema de petición - respuesta entre cliente y servidor. Tiene una versión segura llamada HTTPS.
- **FTP.** Protocolo utilizado en transferencia de ficheros entre dos ordenadores.
- **DNS.** Servicio de nombres de dominio. Convierte nombres de los nodos de red en direcciones red.
- **SMTP y POP.** Protocolos para correo electrónico. SMTP es protocolo simple de transferencia de correo, basado en texto para el envío de mensajes. POP es el protocolo de oficina de correo, para obtener mensajes de correos almacenados en servidor.
- **SNMP:** Protocolo de administración de redes, permite monitorizar y controlar dispositivos de red, administrar configuraciones y seguridad.

Puerto y socket

A cada aplicación se le asigna una dirección de transporte llamada puerto.

HTTP utiliza el puerto 80, por eso un servidor de páginas web está siempre abierto o en escucha ese puerto. HTTPS utiliza el 443.

FTP utiliza 20 y 21

DNS utiliza el 53.

Un socket es una conexión única, formada por la unión de la IP más el puerto. Por ejemplo, si una DNS tiene asignada la IP 192.168.1.11 sería equivalente a decir 192.168.1.11:80

2.3. Versiones de Ethernet. Estándar IEEE 802.3

Desde los años 80 se han estandarizado muchas versiones. Las velocidades alcanzadas más importantes son :

- Ethernet: velocidad de 10 Megabit/seg..
- Fast-Ethernet: velocidad de 100 Megabit/seg.

- Gigabit-Ethernet. Velocidad de 1 Gigabit/seg.
- 10 Gigabit-Ethernet: velocidad de 10 Gigabit/seg.

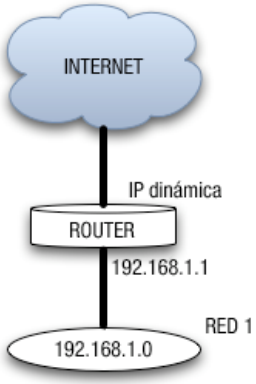
En redes locales lo más habitual es encontrarnos con Fast-Ethernet y Gigabit-Ethernet. Cuando incorporamos un ordenador a la red, debemos tener en cuenta la compatibilidad de la tarjeta con la velocidad de la LAN. También se debe tener en cuenta el cableado y sus velocidades máximas.

3. Topologías de red y modos de conexión

Topologías de red

La topología de red desde un punto físico es la forma en que se conectan los ordenadores de una red: bus, anillo y estrella.

La topología desde el punto de vista lógico nos muestra el uso de la red, nombre de los ordenadores, direcciones, aplicaciones, etc....

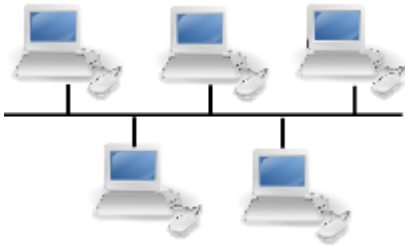


En el esquema la red la red se representa con un óvalo que tiene la dirección de red y fuera el nombre de la red.

En redes wifi o inalámbrica se habla de modo de conexión y se definen dos: modo infraestructura (necesita punto de acceso) y modo ad-hoc (no necesita punto de acceso).

Topología en bus

Un único cable troncal con terminaciones en los extremos, todos los ordenadores se conectan con la red troncal. las primeras redes utilizaban esta topología con cable coaxial. Poca flexibilidad ante fallos. Una rotura de un punto de la red deja toda la red inutilizable.



Topología en anillo

Conecta a cada ordenador o nodo con el siguiente y este último con el primero. Cada estación hace de receptor y transmisor y funciona a modo de repetidor. Las redes locales Token-ring emplean esta topología aunque la conexión física sea en anillo.

Los datos se envían en ambas direcciones y crean redundancia y tolerancia a fallos. Con un único punto de ruptura la red sigue operativa. Se utiliza actualmente en redes FDDI (Fiber Distributed Data Interface) como parte de una red troncal que distribuye datos por fibra óptica.

Topología en estrella

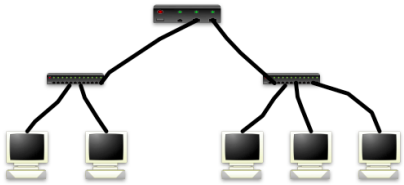
Conecta todos los ordenadores a un nodo central, llamado equipo de interconexión: router, switch o hub. Las redes modernas utilizan eta topología.

La interconexión central canaliza toda la información y por él pasan todos los paquetes de usuarios. Debe estar siempre activo y si falla, falla toda la red. Es tolerante a fallos porque una ruptura de cable solo deja inoperativo un nodo.

También permite incorporación de nuevos ordenadores si hay conexiones libres.

Lo habitual en un edificio es una estrella extendida o árbol, donde las redes en estrella se conectan entre sí con switch.

La estrella extendida habitualmente es jerárquica. Un nodo marca el inicio de la estructura. Suele ser un router que sirve de comunicación al exterior con internet.



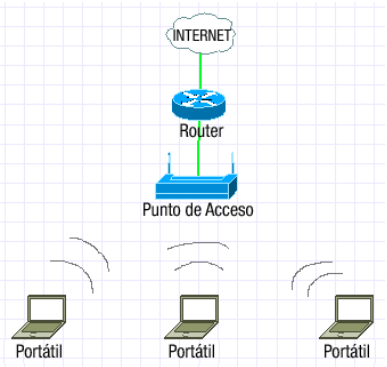
Este crea una red de área local que da servicios a redes locales más pequeñas. Tiene la ventaja que a partir de una única conexión a internet se da servicio a varias redes o subredes locales.

3.1. Redes inalámbricas. Modo de conexión: infraestructura y ad-hoc

En redes inalámbricas o wifi se sigue el estándar IEEE 802.11 y se introduce un concepto diferente al de topología, que es el modo de conexión.

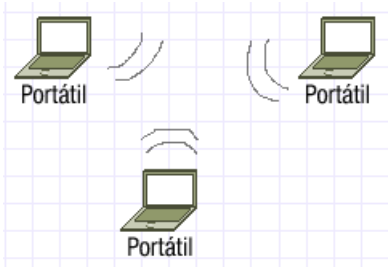
Modo infraestructura

Se utiliza para conectar equipos inalámbricos a una red cableada ya existente. Un equipo de interconexión como puente entre la red inalámbrica y cableada. Este equipo es el Punto de acceso.



Modo ad-hoc

Permite conectar dispositivos inalámbricos entre sí, sin utilizar punto de acceso. Cada dispositivo de la red forma parte de una red de igual a igual o peer to peer. Permite compartir información entre equipos de forma puntual y a poca velocidad, por ejemplo el bluetooth.



4. Componentes físicos de las redes informáticas

Medios de transmisión.

Los propios ordenadores con sus sistemas operativos, hardware y software se consideran componentes de la red. Algunos de ellos son:

- Cableado de red y conectores.
- El rack o armario de conexiones.
- Los patch panel (paneles de parcheo) que organizan el cableado del rack.
- Tarjetas de red.
- Conmutadores o switches que permiten conexión entre ordenadores o segmentos de la red.
- Puntos de acceso que permiten interconexión de dispositivos inalámbricos.
- Cortafuegos que pueden ser hardware o software especifico.
- Servidores.
- Nodos de red.

Clasificación de los medios de transmisión.

El medio de transmisor es un canal que transmite información entre nodos. Estas se realizan con ondas electromagnéticas, susceptibles de ser transmitidas por el vacío.

- **Medios guiados:** camino físico: cables (par trenzado, coaxial y fibra óptica).
- **Medios no guiados:** soporte para que las ondas se transmitan pero no las dirigen. A través del aire o del vacío.

Cable coaxial

Compuesto de un hilo conductor llamado núcleo y de un mallazo externo separados por un dieléctrico o aislante. Los conectores suelen ser BNC y el tipo N. Actualmente solo se utiliza para distribución de señal de tv, internet por cable, etc.

Cable de par trenzado

Es el más utilizado en redes de área local, es un trenzado de ocho hilos de colores distintos y se utiliza bajo el estándar IEEE 802.3. Los colores son: blanco-naranja, naranja, blanco-verde, verde, blanco-azul, azul, blanco-marrón y marrón.

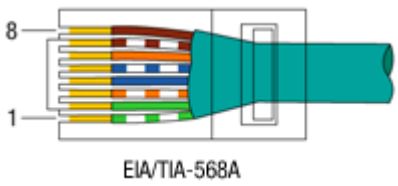
La distribución de estos colores conectados en el conector está estandarizada para que las conexiones sean fácilmente reconocibles.

Existen distintas categorías para las redes actuales:

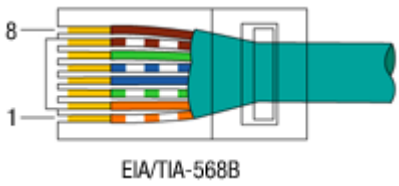
- **Categoría 5:** solo transferencias de 100 Megabit por seg. Válidos para redes Fast-Ethernet.
- **Categoría 5e, 6 y 7** alcanzan los 1000 Megabit por seg. (1 Gigabit).

El conector utilizado es el RJ-45. Un macho para cada extremo del cable. Se unen bajo una herramienta llamada crimpadora.

Para la conexión de 8 hilos al conector se realiza según los estándares ANSI/EIA/TIA 568 A y B. En las conexiones de red utilizamos cables directos y se recomienda usar 568B. En el caso de querer hacer cable cruzado se usa la norma 568A en un extremo y la norma 568B en otro. Los cables cruzados se usan para conectar dos equipos del mismo tipo (que no es lo habitual)



EIA/TIA-568A



EIA/TIA-568B

Pin	568-A	568-B
1	Blanco-verde	Blanco-naranja
2	Verde	Naranja
3	Blanco-naranja	Blanco-verde
4	Azul	Azul
5	Blanco-azul	Blanco-azul
6	Naranja	Verde
7	Blanco-marrón	Blanco-marrón
8	Marrón	Marrón

Fibra óptica

Es un hilo muy fino, de material transparente, vidrio o materiales plásticos en el que se envían pulsos de luz. La fuente de luz es láser o led y es inmune a interferencias electromagnéticas. Es fiable y permite transmitir gran cantidad de datos a gran distancia y velocidad.

Existen dos tipos: multimodo y monomodo. CLos conectores son FC y FFDI.

Cableado estructurado

Es la infraestructura de telecomunicaciones necesaria para conectar un edificio o conjunto de edificios:

- Armarios de distribución de donde confluyen cables, rack y paneles de parcheo.
- Cableado horizonal (de planta)
- Cableado troncal o vertical (entre plantas).
- Sala de equipamiento. Donde se distribuyen las conexiones del edificio.
- Entrada del edificio por donde se conectan los cables exteriores con los interiores.
- Cableado de interconexión de edificios.

Los estándares de cableado estructurados especifican cómo organizar la instalación del cableado.

4.1. Elementos de interconexión

Se refieren a los equipos que permiten conectar equipos en una red local o extensa. Se clasifican teniendo en cuenta el nivel en el que trabajan tomando como referencia del modelo OSI:

- **En el nivel 1 o físico:**

  Tarjetas de red: cableadas o inalámbricas.

  Concentradores o hubs: Son dispositivos que permiten conectar varios ordenadores, pero lo realiza de forma no inteligente, ya que se envía la información a todos los ordenadores, sin regular el tráfico. Los hubs pierden importancia a favor de los switchs por su eficiencia y bajo coste.

  Repetidores: pueden ser locales o remotos y su función es repetir la señal, regenerarla y/o amplificarla.

- **En el nivel 2 o de enlace de datos:**

  Conmutadores o switches: permite conectar varios ordenadores de forma inteligente. El tráfico es más rápido que en un hub, también conecta segmentos y ordenadores de la misma red.

  Puentes o bridges: conectan subredes, transmitiendo de una a otra el tráfico generado no local.

  Puntos de acceso: se encarga de conectar elementos inalámbricos entre sí, permite el acceso de dispositivos inalámbricos a redes cableadas.

- **En el nivel 3 o nivel de red:**

  Enrutadores o routers: Conectan redes distintas, su principal uso está en la conexión a internet. Al unir redes distintas se necesitan al menos dos direcciones IP, una para cada red. Los routers trabajan con la IP externa con la que nos ven desde fuera y la IP interna.

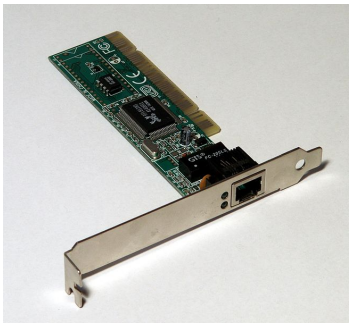
- **En los niveles superiores:**

  Pasarelas: son los equipos de interconexión que trabajan en niveles superiores del modelo OSI. Existen distintos tipos de pasarelas: Las que se encargan de conectar redes con tecnologías diferentes, las que facilitan el control de acceso a una red, las que controla accesos no autorizados. Pueden ser servidores, cortafuegos, etc...

Tarjetas de red y direccionamiento MAC

Trabaja en nivel 1 de OSI o nivel físico, también se les llaman NIC (network interface card). Todas

tienen la dirección MAC de 48 bits o 12 cifras hexadecimales y es única en el mundo.



Tiene una velocidad máxima, siendo las actuales de 100 o 1000 megabits por segundos. Estas velocidades coinciden con las velocidades con las de los cables de par trenzado categoría 5 y 5e.

Conmutadores o switches

Trabajan en capa 2, conecta dos o más segmentos de red. El conmutador permite conectar diferentes ordenadores para que puedan conectarse entre sí y que éstos tengan acceso a otros segmentos de red. Funciona almacenando las direcciones MAC de ordenadores conectados a él y de dispositivos que se encuentran en cada segmento. Gracias a ello es capaz de conectar un ordenador con otro de forma eficiente, sin necesidad de enviar la información a toda la red.

Enrutadores o routers

Trabaja en capa 3, es el equipo de interconexión que se encarga de conectar dos o más redes diferentes.

Los routers dirigen el tráfico de red, buscando el mejor camino para llegar al destino. Cada interfaz del router se conecta con una red distinta. Necesitan una configuración inicial para guardar la IP de cada interfaz o puerto y su máscara de red. También se pueden configurar servidores DNS y si se admiten direcciones IP dinámicas (protocolo DHCP).

Para realizar sus funciones un router guarda información de las redes a las que puede acceder, a través de la tabla de enrutamiento, que es donde se guarda

como se llega de una a otra red y que servicios permiten.

Un router profesional, si tiene 10 tomas RJ45 es para unir 10 redes diferentes, los routers caseros solo unen dos redes: la externa y la interna. Suelen tener conexión inalámbrico y varios puertos RJ45 que son un switch, ya que todos los equipos conectados a ellos están en la red interna. Estos routers son básicos pero tienen varias capas OSI: la 2 o de red, la 2 o de enlace y la 1 o punto de acceso.

Cable directo o cable cruzado entre equipos de interconexión.

Lo habitual es realizar conexiones entre dispositivos de un nivel y otro de nivel inmediato, por ejemplo, los ordenadores con sus tarjetas de red (n.1) se unen con los switch (n.2), que a su vez se unen con el router (n.3). En estos casos se usa un cable directo.

5. Redes inalámbricas

Las redes WLAN (Wifi Lan) basan su funcionamiento en el estándar IEEE 802.11 y es similar al funcionamiento de una red local cableada.

Las redes ad-hoc permiten conectarse entre sí pero a velocidades bajas y con seguridad mínima.

El modo infraestructura, donde se utiliza un punto de acceso para que actúe como canalizador de todas las conexiones mejora la velocidad y seguridad.

El punto de acceso se conecta a una red de área local a través de cable normalmente, con la idea de dar acceso a internet.

Ventajas de redes Wi-Fi

- Movilidad
- Escalabilidad: fáciles de ampliar
- Flexibilidad: alto grado de conectividad.
- Menor tiempo de instalación.

Desventajas:

- Seguridad: es difícil garantizar un alto grado de seguridad.
- Interferencias.

Tipos de redes 802.11 y características

El estándar IEEE 802.11 define estas versiones:

IEEE 802.11a: opera en la banda 5 Ghz. con velocidad máxima de 54 Mbps.

IEEE 802.11b: opera en la banda de 2,4 Ghz. con una velocidad máxima de 11 Mbps.

IEE802.11g: opera en la banda de 2,4 Ghz, por lo que es compatible con la versión b, pero ofrece las mismas tasas que la versión a con máximas de 54 Mbps. Se recomienda usar versión g sobre versión b, porque si se conecta un dispositivo versión b en un acceso g, baja la velocidad de toda el área de cobertura.

IEEE 802.11n opera simultáneamente bandas de 5 Ghz. y 2.4 Ghz. Es compatible con otras versiones, y es útil que trabaje con banda 5 Ghz. que está menos congestionada y sufre menos interferencias. Tiene velocidad máxima de 600 Mbps.

IEEE 802.11ac. Opera la banda 5 Ghz con velocidad máxima de 1,3 Gbps, doblando la velocidad de IEEE 802.11n

Las velocidades indicadas son las máximas, pero las reales son bastante menores. las más utilizadas actualmente son g, n y ac por sus altas velocidades. 5Ghz tiene mayor calidad, menos ruido pero tiene un alcance un 10% menor y es más sensible a muros .

El SSID de una red 802.11

Identificador de conjunto de servicio, es una cadena alfanumérica de 32 caracteres de longitud que distingue mayúsculas y minúsculas para identificar una red. Los nombres de las redes cuando nos conectamos a una red son los SSID de las distintas redes WLAN.

Los dispositivos inalámbricos de una red se deben configurar con el mismo SSID.

Cada punto de acceso que su área de cobertura se solape con el de otro punto de acceso debe usar canales distintos. En el estándar IEEE 802.117g implica usar canales de diferencia de 5.

Si el punto de acceso no consigue cobertura necesaria se pueden conectar varios puntos de acceso entre sí, con un canal distinto pero el mismo SSID.

Seguridad en 802.11

Las redes wifi son vulnerables a interceptación de paquetes y usuarios no autorizados, es conveniente implementar medidas de seguridad que prevengan

el uso indebido de la red.

Tipos de cifrado

Las medidas habituales son encriptar o codificar la información con:

- WEP (Privacidad equivalente a cableado), método débil y fácilmente descifrable.
- WPA (Acceso Wi-Fi protegido). Relativamente seguro por su cifrado.
- WPA2 Se recomienda utilizarlo con el algoritmo AES. El más seguro hoy en día.

Ocultar SSID

No proporciona seguridad pero si dificulta a los clientes conectarse. De esta manera los ordenadores deben configurar manualmente la SSID.

Deshabilitar WPS

Facilitan la conexión a distintos dispositivos sin utilizar contraseña, pero compromete la seguridad de la conexión. Es aconsejable desconectarla del router o punto de acceso.

Filtrado de direcciones MAC

Es una buena medida de seguridad adicional, se recomienda utilizarla como complemento de algunos métodos de encriptación. Consiste en configurar el punto de acceso o router de tal forma que tenga un listado de direcciones MAC autorizados a conectarse a la red inalámbrica. Filtrar por direcciones MAC es una buena medida de seguridad.

6. Sistema binario. Conversión decimal - binario

Sistema binario.

Para entender las direcciones lógicas de una red es necesario conocer los cálculos binarios.

En nuestro lenguaje, para referirnos a los números utilizamos sistema decimal, es decir, 10 cifras distintas del 0 al 9.

El sistema binario utiliza dos cifras distintas: 0 y 1. Los ordenadores solo utilizan este sistema.

Bit y byte

Un bit es un número binario con una única cifra. En un bit solo cabe un cero o un uno. Hay 2^1 = 2 números distintos (del 0 al 1). Un byte es un conjunto de 8 bits

- Con 2 bits se pueden escribir 00, 01, 10, 11. Hay 2^2 = 4 números distintos: del 0 al 3.
- Con 3 bit se puede escribir: 000, 001, 010, 011, 100, 101, 110, 111. Hay 2^3 = 8 números distintos (del 0 al 7).
- Por cada bit se doblan los números posibles a escribir. Así pues el byte es un número binario de 8 cifras y se anota por B. Al ser 8 cifras se pueden escribir 2^8 = 256 números distintos (del 0 al 255).

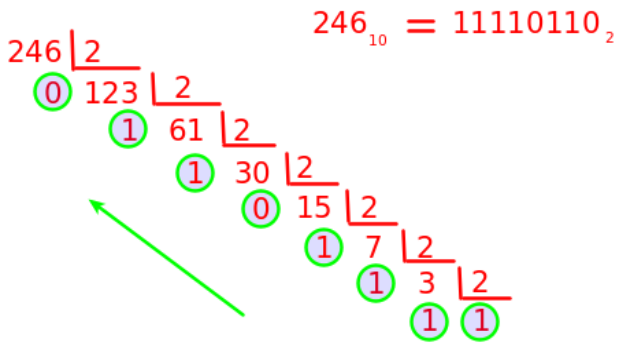
Con un byte se pueden representar 256 caracteres alfanuméricos distintos, los necesarios para escribir cualquier texto en nuestro lenguaje. Si guardamos en el bloc de notas un documento llamado prueba.txt que tenga la palabra hola, observamos que ocupa 4 bytes, una para cada letra (código ascii extendido).

Con vistas al cálculo de direcciones IP, en las redes es importante recordar la idea de la potencia explicada anteriormente.

- Con 1 byte u 8 bits se representan 256 números distintos, del 0 al 255 (del 00000000 al 11111111).
- Con 16 bits se representan 65536 números distintos (2 elevado a 16, del 0 al 65535 o del 0000000000000000 al 1111111111111111).

Conversión decimal binario

Para convertir un decimal en binario se realizan divisiones enteras por dos, utilizando el cociente entero para dividir de nuevo por 2, hasta que el cociente sea 0 o 1. Para obtener el número binario, se coge como cifra significativa el último cociente y después todos los restos empezando por el último.



Conversión de binario a decimal

Cada bit se multiplica por una potencia de 2, comenzando desde el bit menos significativo (por la derecha). Ejemplo. Convertir 11110110 a decimal:

$$11110110 = 0*2^0 + 1*2^1 + 1*2^2 + 0*2^3 + 1*2^4 + 1*2^5 + 1*2^6 + 1*2^7 =$$
$$= 0*1 + 1*2 + 1*4 + 0*8 + 1*16 + 1*32 + 1*64 + 1*128 =$$
$$= 2 + 4 + 16 + 32 + 64 + 128 = 246$$

Se obtiene $11110110_2 = 246_{10}$

O lo que es lo mismo. Se suma la potencia de 2 correspondiente cuando el bit es 1 y no se suma nada cuando el bit es 0:

Binario	2^7 = 128	2^6 = 64	2^5 = 32	2^4 = 16	2^3 = 8	2^2 = 4	2^1 = 2	2^0 = 1	Suma	Decimal
00000000	0	0	0	0	0	0	0	0	0+0+0+0+0+0+0+0=0	0
10101100	1	0	1	0	1	1	0	0	128+32+8+4	172
00111110	0	0	1	1	1	1	1	0	32+16+8+4+2	62
11111111	1	1	1	1	1	1	1	1	128+64+32+16+8+4+2+1	255

Múltiplos del byte

Cuando hablamos de Megas solemos confundir el bit con el byte. Por eso, cuando hablamos e bytes lo hacemos con B y cuando hablamos de bits lo hacemos con b:

Nombre	Notación	Equivalencia
Bit	**b**	
Byte	**B**	8 b
Kilobyte	**KB**	1000 B = 10^3 B
Megabyte	**MB**	1000 KB = 10^3 KB = 10^6 B
Gigabyte	**GB**	1000 MB = 10^3MB = 10^9 B
Terabyte	**TB**	1000 GB = 10^3 GB = 10^{12} B
Petabyte	**PB**	1000 TB = 10^3 TB = 10^{15} B
Exabyte	**EB**	1000 PB = 10^3 PB = 10^{18} B

Diferencia entre Kilobyte y Kibibyte

1 kilobyte se considera desde siempre como 1024 bytes (2 elevado a 10 B).

Pero un kilo significa 1000 y no 1024, así pues, se normalizaron 2 notaciones distintas en el estándar IEC 80000-13 del año 2008.

Así pues, nos referimos a kilo, mega o gigas a los múltiplos de 1000 y a kibi, mebi y gibi a los múltiplos de 1024

7. Direccionamiento lógico. Clases de redes y división en subredes

Direcciones IP Versión 4. IPv4.

El direccionamiento IP se encarga de asignar de forma correcta a cada equipo una dirección IP, de esta manera se comunican correctamente entre sí.

Una dirección IP tiene 32 bits, de manera que una dirección IP tiene 4 bytes. Para mayor comodidad, a una dirección IP se le sustituyen los 8 bits por su valor decimal, separándola con puntos.

Ejemplo: La dirección IP 11010001 11011000 00110111 00000011 se escribe 209.216.55.3

Los equipos de la misma red tienen la misma dirección de red, llamado identificador de red (netid), después cada equipo tiene un número que le

identifica de forma única dentro de la red, llamado identificador de equipo o host (hostid).

Una dirección IP tiene ambas partes (netid) y (hostid). netID son los cuatro primeros números, hostID es el último.

En el ejemplo, netID corresponde a 209.216.55 y hostID corresponde a 3. Este número puede variar para identificar a cada equipo de la red, desde 0 a 255, pero 0 y 255 no se pueden usar.

La IP del ejemplo es de clase C, tiene 24 bits para la dirección de red y 8 para la de equipo, pero no siempre es así.

Direcciones específicas. Reglas y convenios.

- La dirección 0.0.0.0 identifica al host actual, no se puede utilizar para ninguna red.
- La dirección con el campo identificador de equipo to a ceros se utiliza para indicar la dirección red, por tanto no se puede utilizar para ningún equipo.
- Se conoce por broadcast o multidifusión o multicast, la posibilidad de enviar un mensaje a todos los equipos de la misma red, para eso se reservan algunas direcciones que no podrá tener ningún equipo de esa red. 255.255.255.255 es el broadcast de todas las redes, la dirección con el campo identificador de equipo todo a unos se utiliza como al dirección boradcast de la red indicado, no se puede utilizar para ningún equipo.
- Todas las redes tienen máscara de red, para calcularla se ponen todos los bits de la dirección a 1 y todos los del host a 0. El objetivo de la máscara es marcar los límites de la red. Todos los equipos de la misma red tienen la misma máscara.
- La dirección127.0.0.1 se utiliza para loopback. Cuando se envía un mensaje a esta IP, se devuelven a la dirección de origen todos los mensajes sin intentar enviarlos a ninguna parte. Se usa para probar la conectividad local.

Puerta de enlace

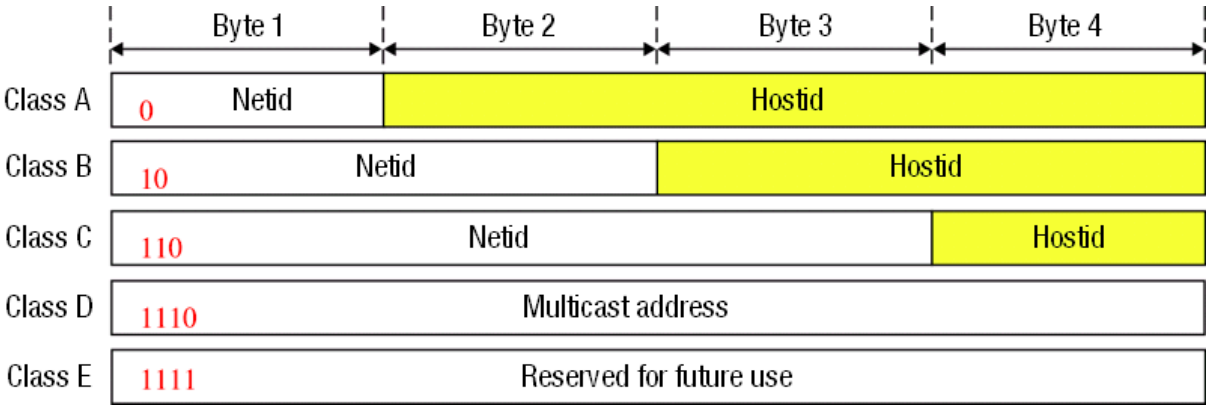
Cuando configuramos las IPs en los ordenadores, hay que configurar cual es la puerta de enlace, que es una IP de nuestra red y es el equipo por el que saldremos al exterior. Habitualmente es la dirección IP del router con el que nos conectamos a internet.

7.1 División de redes en clases

Hay 5 clases principales de redes: A, B,C, D, E.

- Las más normales son A, B y C.
- D son redes multicast o multidifusión.
- E son direcciones reservadas.

Se distinguen por los bits que se utilizan para el número de red y los valores de los primeros bits.



El objetivo es poder tener redes más grandes y redes más pequeñas, a más bits para equipo se puede tener una red más grande.

Clase A

Dirección de red: se utilizan 8 bits de red, con el primer bit a 0. El primer byte puede ir de 00000000 a 01111111 (de 0 a 127). Al ser siempre el primer bit 0, vienen dadas por 2^7 = 128. Las redes 0 y 127 no se pueden utilizar. 0 representa a todas las redes y el propio equipo se reconoce por la dirección 0 y 127 representa loopack. Solo hay disponibles 126 redes posibles de clase A.

Dirección de equipo o host.

La dirección de equipo la forman 24 bits (2 elevado a 24) = 16 millones de equipos aprox.

Ejemplo de clase A	
Dirección de red	126.0.0.0
Primer equipo	126.0.0.1
Último equipo	126.255.255.254
Broadcast red	126.255.255.255
Máscara de red	255.0.0.0

Clase B

Dirección de red: se utilizan 16 bits de red, con los dos primeros bits a 10. El primer byte puede ir de 10000000 a 10111111 (de 128 a 191). El segundo byte también es dirección red, así, de las 16 cifras para la red, las dos primeras son obligatorias (10), por tanto 2 elevado a 14 = 16384 redes.

Dirección de equipo o host: La forman 16 bits (2 elevado a 16 = 65536), pero no se puede utilizar ni la primera (representa la dirección de red) ni la última (broadcast). Así que pueden haber 65534 equipos o hosts.

Ejemplo de clase B	
Dirección de red	150.85.0.0
Primer equipo	150.85.0.1
Último equipo	150.85.255.254
Broadcast red	150.85.255.255
Máscara de red	255.255.0.0

Clase C

Dirección de red

24 bits de red con los 3 primeros bit a 110. Esto significa que en decimal va de 192 a 223, pero 192 se reserva para redes privadas. Pueden haber 24 cifras para la red, las 3 primeras son obligatorias por tanto: 2 elevado a 21: aproximadamente 2 millones de redes.

Dirección de equipo o host: la forman 8 bits, 2 elevado a 8 = 256, pero no se utilizan ni la primera ni la última: 254 hosts.

Ejemplo de clase C	
Dirección de red	196.220.53.0
Primer equipo	196.220.53.1
Último equipo	196.220.53.254
Broadcast red	196.220.53.255
Máscara de red	255.255.255.0

Clases D y E

No se utilizan para configuración general de las redes. Clase D son las que comienzan por 1110 y van desde 224 a 239, para multidifusión. Clase E comienzan por 1111 y van desde 240 a 254, reservadas para uso futuro. La 255 es el broadcast general de todas las redes.

Redes privadas

Algunas direcciones IP se reservan para redes privadas, de manera que no se pueden asignar a ningún ordenador en internet.

Clase	Rango	Número de redes
A	10.x.x.x	1
B	172.16.x.x a 172.31.x.x	16
C	De 192.168.x.x a 192.168.255.x	256

Las redes privadas se utilizan para intranet.

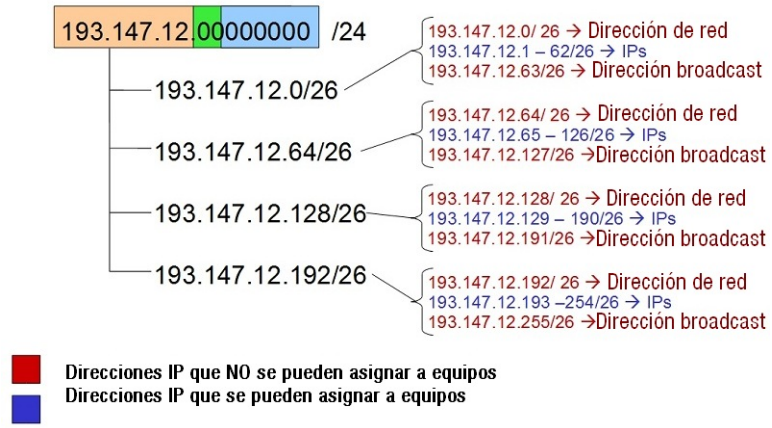
- La dirección IP pública es la que está conectada a internet y es única en internet.
- La dirección privada es la que está en la red del domicilio con el resto de aparatos. La IP de cada aparato es distinta.
- La privada de muchos routers suele ser 192.168.0.1, cada domicilio se ve desde fuera con su IP externa que es única en internet. La ip externa del router se puede ver en www.cualesmiip.es

7.2. División de redes en subredes

Cuando se diseña la red en una empresa hay que tener en cuenta la optimización del uso de las redes. y tener en cuenta si necesitamos crear subredes distintas para departamentos que tendrán equipos que solo serán visibles dentro de su propia subred.

El direccionamiento IP nos ayuda a crear subredes, cada una de ellas tendrá su dirección subred, su broadcast de subred y su rango de IP permitidas.

Si por ejemplo dividimos una red de clase C en 4 subredes, se obtienen 4 subredes de 64 equipos (62, por no poder utilizar la dirección de subred y la de broadcast.



En el ejemplo, 2 bits de identificador de equipo de la clase C pasan a ser dirección de subred, de forma que el identificador de subred son 26 bits y el de equipo son 6 bits. Al dividir la red en subredes, se calcula la máscara, la dirección de subred y broadcast con las mismas normas que en las redes.

8. Configuración de routers

Los routers se encargan de comunicar varias redes y permiten asegurar la red de la empresa. Para configurar un router se debe crear la tabla de enrutamiento o directivas firewall. Se utilizan los siguientes elementos:

- Interfaz de red donde se recibe la información.
- Origen / Destino del mensaje. Es una dirección o un conjunto de direcciones IP.
- Puerto: permitir y denegar acceso a los puertos, permite el tráfico de un servicio o lo deniega.
- Acción: especifica la acción que debe realizar el router:

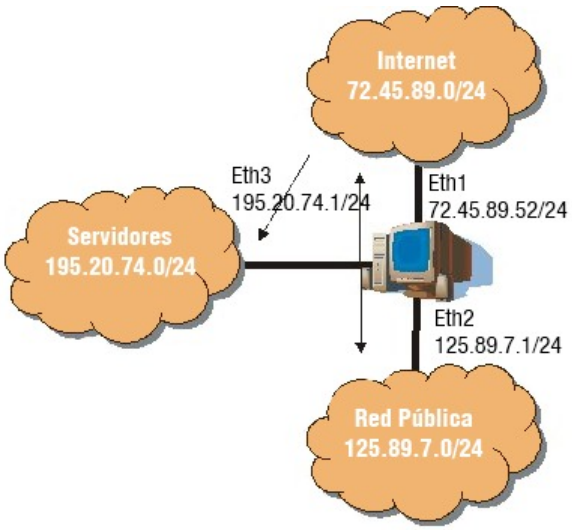
- Aceptar: dejar pasar información.
- Denegar.
- Reenviar: envía el paquete a una determinada dirección IP.

Es importante utilizar la máscara de red para indicar la dirección de origen o destino. Ejemplo:

Ejemplo	Comentario
192.165.2.23/32	Representa a un único ordenador
192.165.2.0./24	Representa a todas las direcciones IP del tipo 192.165.2.X
192.165.0.0/16	Representa a todas las direcciones IP del tipo 192.165.X.X
192.0.0.0/8	Representa a todas las direcciones IP del tipo 192.X.X.X
0.0.0.0/0	Representa a todas las direcciones IP del tipo X.X.X.X

Ejemplo de creación de unaa tabla de enrutado.

En la figura hay un ordenador con 3 interfaces o tarjetas de red (eth1, 2 y 3), realizando labores de router. También están reflejadas las IP de las tarjetas, que conectan a las 3 redes: internet, red pública y servidores.



Se deben crear el conjunto de reglas para permitir que la red pública se conecte a Internet y que los servidores sean accesibles desde Internet; el

servidor web se encuentra en la dirección 195.20.74.5 y el servidor de correo se encuentra en la dirección 195.20.74.7.

El conjunto de reglas está formado por seis reglas sencillas. La complejidad de las reglas tiene propósitos educativos para mostrar los conceptos del procesamiento de reglas (directiva) del filtrado de paquetes.

Las reglas están agrupadas en tres grandes grupos: las primeras tres reglas se aplican al tráfico que tiene como origen Internet y como destino la red de servidores. Las reglas 4 y 5 permiten la comunicación entre Internet y la red pública. Y la última regla, se utiliza siempre para indicar que el tráfico que no cumpla las reglas anteriores debe ser denegado.

Reglas	Interfaz	Origen	Destino	Puerto	Acción
1	Eth1	0.0.0.0/0	195.20.74.5/32	80	Aceptar
2	Eth1	0.0.0.0/0	195.20.74.5/32	25,110	Aceptar
3	Eth1	0.0.0.0/0	195.20.74.0/24	-	Denegar
4	Eth1	0.0.0.0/0	125.89.7.0/24	-	Aceptar
5	Eth2	125.89.7.0/24	0.0.0.0/0	-	Aceptar
6	-	-	-	-	Denegar

- Regla 1. Esta regla permite el acceso entrante en el puerto 80, que es el servicio web. El host 195.20.74.5 es el servidor web. La organización no puede predecir quién quiere acceder a su sitio Web, por lo que no hay restricción en las direcciones IP de origen.
- Regla 2. Esta regla permite el acceso entrante a los puertos 25 y 110, que son los del correo electrónico. El servidor de correo está en la dirección 195.20.74.7. Al igual que en la regla anterior, no se restringen las direcciones IP de origen.
- Regla 3. Esta regla elimina todos los paquetes que tienen como destino la red donde se encuentran los servidores. Como la regla 1 y 2, se ejecutan antes, sí se permite el tráfico que va dirigido a los servidores web y correo electrónico. Si se pone esta regla al principio de la tabla de enrutamiento, no se podrá acceder a ningún servidor.
- Reglas 4 y 5. La cuarta regla deja pasar el tráfico que va desde Internet a la red pública. Y la quinta regla deja pasar el tráfico que va desde la red

pública a la red de Internet.

- Regla 6. Esta regla bloquea explícitamente todos los paquetes que no han coincidido con ningún criterio de las reglas anteriores. La mayoría de los dispositivos realizan este paso de forma predeterminada, pero es útil incluirla.

Para terminar, se muestra un ejemplo de configuración de un router con iptables, donde iptables es el servicio de enrutamiento en un servidor Linux.

```
[root@redhatserver root]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  10.0.0.0/24          anywhere           tcp dpt:http
ACCEPT     udp  --  10.0.0.0/24          anywhere           udp dpt:domain
ACCEPT     all  --  anywhere             anywhere           state ESTABLISHED

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
[root@redhatserver root]#
```

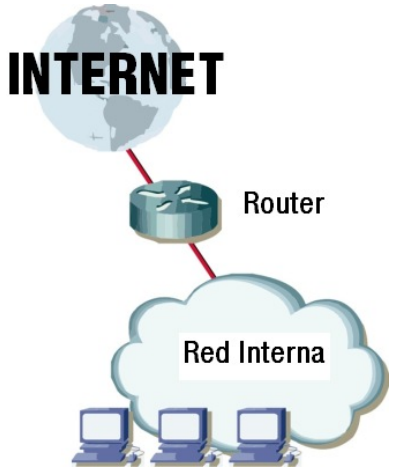
8.1. Seguridad en la arquitectura de una red

Las arquitecturas de seguridad se utilizan para en caso de intrusión, limitar el acceso al intruso. Los elementos básicos que intervienen en la arquitectura de cortafuegos son:

- Router: Permite o deniega comunicaciones, al ser intermediario debe estar protegido, con el enrutamiento, ya que puede ser objeto de ataque.
- Red interna: Dependiendo del nivel de seguridad que necesite la red se puede dividir en varias redes para permitir o denegar el tráfico de una a otra red.
- Zona neutra (red perimetral). Se añade una red entre dos redes para proporcionar mayor protección a una de ellas. En esta red se suelen ubicar los servidores de la empresa. Su objetivo es que ante una posible intrusión en uno de los servidores, esta se aísle y no permita el acceso a la red interna.

Esquema de red básico

Consiste en el empleo de un router para comunicar la red interna con internet. El router se encarga de permitir o denegar tráfico.

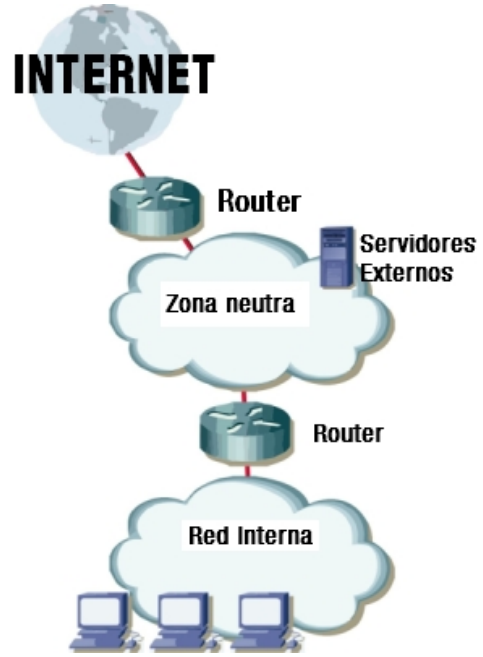


Es la más insegura, puesto que la seguridad reside solo en el router. Es usual en domicilios y pequeñas empresas.

Esquema de red con zona neutra

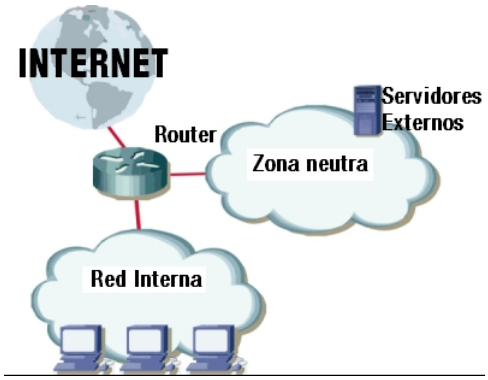
Un servidor ofrece servicios a internet. Es peligroso poner un servidor en una red interna, puesto que el router permite el tráfico al servidor, y en un fallo de seguridad el atacante tiene acceso completo a la red interna. Se soluciona el problema añadiendo una nueva red a la empresa llamada zona neutra o desmilitarizada.

Utiliza dos routers y permiten crear un perímetro de seguridad, donde se ubican los servidores accesibles desde el exterior, protegiendo la red local de atacantes externos.

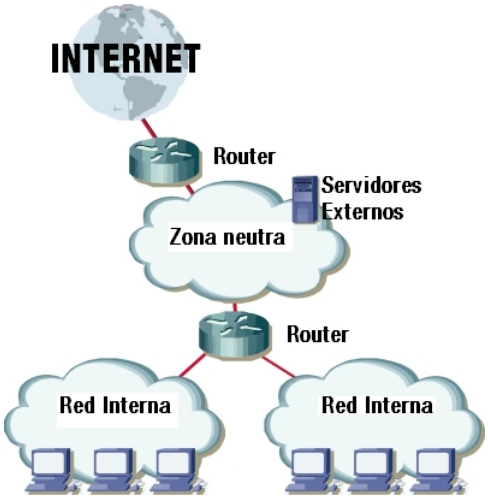


En este esquema, el router exterior permite acceso desde internet a los servidores de la zona neutra, especificando los puertos utilizados. El router interior solo permite tráfico saliente de la red interna al exterior. De esta forma nunca se podrá tener acceso a la red interna de la empresa.

Otras configuraciones con zona neutra sería utilizando un único router con tres interfaces (routers profesionales).



No es tan fiable, pero sí más que el modelo básico. En esta última imagen se muestra un esquema con 2 routers con zona neutra y varias redes internas.



Mapa conceptual