EFA
MORATALAZ

1º CFGS Desarrollo de Aplicaciones Web

SISTEMAS INFORMÁTICOS

DANIEL CUENCA ARANDA

UT6 – SISTEMAS INFORMÁTICOS EN RED

EFA MORATALAZ

1º CFGS Desarrollo de Aplicaciones Web

SISTEMAS INFORMÁTICOS

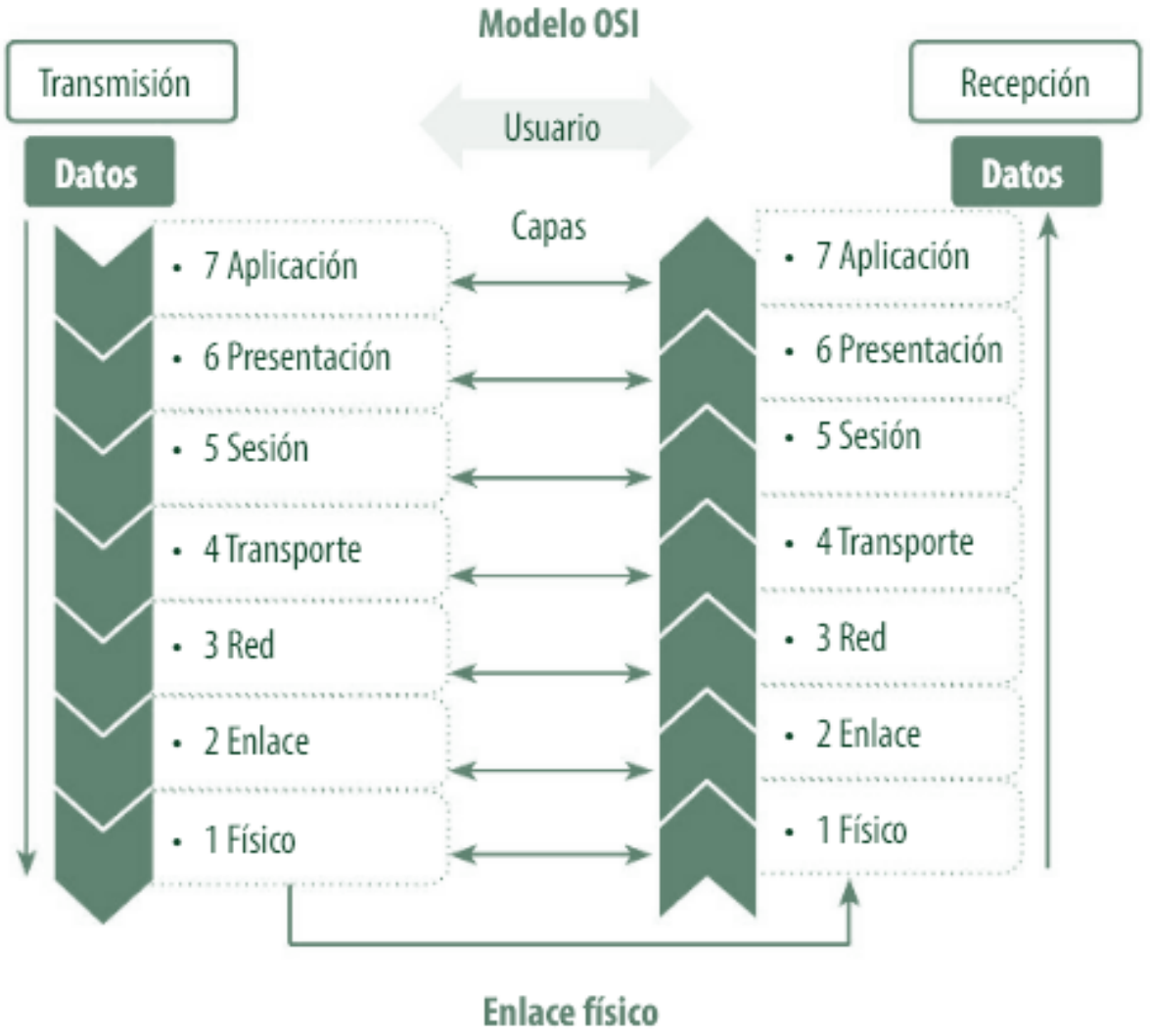
INDICE

UT6 – SISTEMAS INFORMÁTICOS EN RED

PROTOCOLOS PRINCIPALES DE RED

Los ***sistemas informáticos*** actuales prácticamente son ***sistemas en red***

Cualquier sistema operativo que trabaje con hardware específico de red y conectado a otros elementos de red compartiendo información, forma parte de una red de comunicaciones



Los sistemas informáticos se basan en modelos de referencia que establecen características y especificaciones necesarias para comunicarse entre diferentes entidades e intercambiar información.

Las arquitecturas de red que se apoyan en estos modelos de referencia descomponen sus funciones en carios niveles para definir protocolos y estándares encaminados a reducir la complejidad, controlar los flujos de comunicación y facilitar la evolución del modelo

La comunicación del modelo OSI transcurre en niveles con una capa que se comunica con su inmediata superior e inferior, de tal forma que el proceso de comunicación entre un emisor y un receptor sigue un recorrido permitiendo trazar con metainformación el camino entre el emisor y el receptor.

A este proceso es el denominado encapsulamiento, en el que a cada capa añade datos de la capa superior asociada al protocolo que representa, constituyendo unidades de paquetes de datos (PDU).

Pulsar para ver las funciones de cada una de las capas del modelo OSI

El modelo TCP/IP constituye el estándar abierto de Internet.

Dicho modelo se adapta al modelo OSI conceptual

Correspondencia entre modelo OSI y modelo TCP/IP

Modelo OSI	Modelo TCP/IP
7. Aplicación	a) Aplicación
6. Presentación	
5. Sesión	
4. Transporte	b) Transporte
3. Red	c) Internet
2. Enlace de datos	d) Acceso a red
1. Física	

Protocolos destacados del modelo TCP/IP

Protocolo	Utilidad	Capa
HTTP (Hypertext Transfer Protocol)	Web	APLICACIÓN
HTTPS (Hypertext Transfer Protocol Secure)		
SMTP (Simple Mail Transfer Protocol)	Correo electrónico	
POP3 (Post Office Protocol 3)		
IMAP (Internet Message Access Protocol)		
DHCP (Dynamic Host Configuration Protocol)	Obtención de direcciones IP	
DNS (Domain Name System)	Traducción de nombres de dominio a direcciones IP	
FTP (File Transfer Protocol)	Transferencia de archivos	
FTPS (File Transfer Protocol Secure)		
TLS (Transport Layer Security)	Encriptación	
SSL (Secure Sockets Layer)		

Protocolos destacados del modelo TCP/IP

Protocolo	Utilidad	Capa
UDP (User Datagram Protocol)	Conexión y envío de información entre hosts	TRANSPORTE
TCP (Transmission Control Protocol)		
IP (Internet Protocol)	Enrutamiento de paquetes	INTERNET
NAT (Network Address Translation)	Traducción de direcciones IP privadas a públicas	
ARP (Address Resolution Protocol)	Correspondencia entre direcciones MAC e IP	ACCESO A LA RED
RARP (Reverse Address Resolution Protocol)		
ETHERNET	Transmisión por cableado	
WLAN (Wireless Local Area Network)	Transmisión por Wi-Fi	
FDDI (Fiber Distributed Data Interface)	Transmisión por fibra óptica	

Protocolo Ethernet

Establece la forma de conexión y transmisión de datos por cable donde se especifican las características del cableado y su señalización, así como el formato de las tramas de datos

Emplea el mecanismo CSMA/CD, Acceso Múltiple por Detección de Portadora y Detección de Colisiones, en un medio compartido por varios hosts.

Cuando un host desea transmitir tiene que escuchar previamente el medio, de forma que si está ocupado el canal, espera un tiempo antes de volver a intentarlo.

En el caso de que dos hosts transmitan a la vez, se produciría la colisión y ambos detendrían la transmisión.

Su ventaja principal es el bajo coste, flexibilidad y facilidad de implementación segura ante accesos no permitidos.

Corresponde al estándar IEEE 802.3 y ampliamente utilizado en redes de área local (LAN).

Protocolo Wi-Fi

Define el conjunto de especificaciones para redes de área local inalámbricas.

Corresponde al estándar IEEE 802.11 estableciendo multitud de estándares de transmisión de datos por radiofrecuencia en las bandas ISM de fines no comerciales.

Emplea el mecanismo CSMA/CA, Acceso Múltiple por Detección de Portadora y Prevención de Colisiones, en un medio compartido por varios hosts.

Cuando un host desea transmitir antes de hacerlo envía una notificación sobre su intención de hacerlo y, si recibe la autorización correspondiente por parte del receptor, lo hace.

Se reduce la probabilidad de colisiones en el medio.

Su ventaja principal su facilidad de instalación y movilidad, sin embargo es más insegura que el protocolo Ethernet debido al medio de transmisión abierto y la saturación de los canales, bandas 2,4 GHz y 5 GHz, creando interferencias y aumentando la latencia de las comunicaciones.

Protocolo Wi-Fi

Estándar	Banda	Ancho de banda máximo
802.11a	5 GHz	54 Mbps
802.11b	2,4 GHz	11 Mbps
802.11g	2,4 GHz	54 Mbps
802.11n (Wi-Fi 4)	2,4 GHz y 5 GHz	600 Mbps
802.11ac (Wi-Fi 5)	5 GHz	7 Gbps
802.11ax (Wi-Fi 6)	2,4 GHz y 5 GHz	11 Gbps

Protocolo IPv4 e IPv6

El protocolo IP se encarga del enrutamiento de los paquetes de datos. De esta forma decide que ruta es la más adecuada para transportar los paquetes desde un origen a un destino pasando por distintos nodos intermedios. Hace uso del direccionamiento a hosts, denominado asignación de direcciones IP a interfaces de red) para poder enrutar los paquetes.

Este protocolo no garantiza si un paquete llega a su destino y en qué orden, por lo que no es fiable, sin embargo, la labor la pueden realizar otros protocolos de capas superiores como el protocolo TCP.

La dirección IP también denominada dirección lógica.

Asigna a cada controlador o interfaz de red de un equipo que utilice el protocolo IP una dirección IP.

La dirección IP identifica de forma unívoca cada dispositivo de red. No es posible la repetición de dos direcciones IP dentro de la misma red, ya que provoca conflictos de red, ocasionando el error en la recepción o el envío de los datos.

Las dos versión del protocolo IP son la 4 y la 6.

Protocolo IPv4 e IPv6

El Protocolo IPv4 hace uso de 32 bits desglasados en octetos conformando un total de 4 separados por puntos.

Cada bloque puede representar un número comprendido entre el 0 y 255.

El protocolo establece la necesidad de uso de ***una máscara de red*** *(similar a cuando establecíamos una máscara de permisos en Sistemas Operativos Linux).*

El formato de esta máscara es similar al de una dirección IP asociándola con la misma.

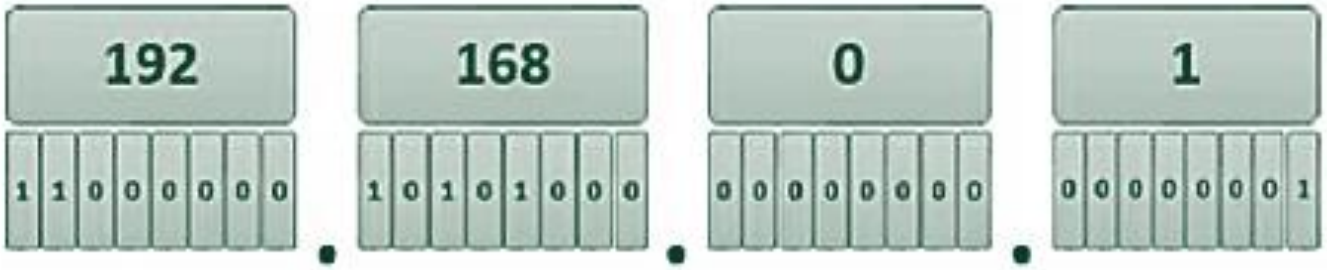
Permite identificar la red a la que pertenece la dirección IP.

La dirección IP se divide una porción correspondiente a la red y una porción correspondiente a al host.

La máscara de red es la encargada de determinar el número de bits de la dirección IP que corresponden con la red a la que pertenece y cuales al host dentro de dicha red.

Protocolo IPv4 e IPv6

IPv4

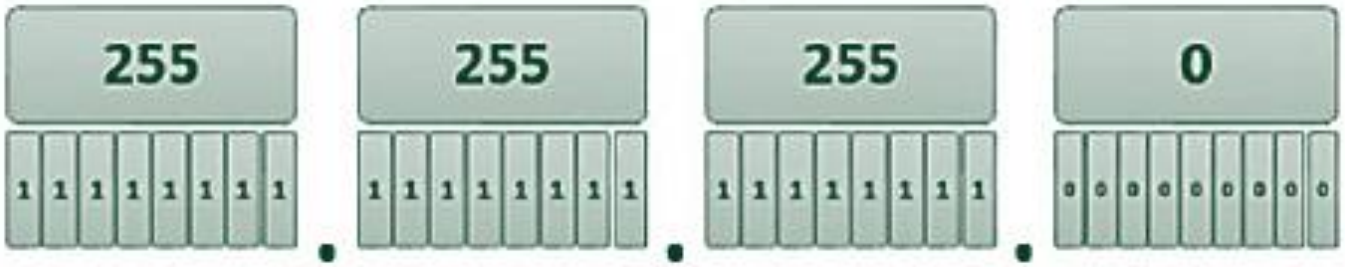


Los bits de la máscara de red que tienen valor 1 corresponden a la porción de red.

Los bits de la máscara de red que tienen el valor 0 corresponde a la porción de host.

Ejemplo de dirección IP

Ejemplo de máscara de red



Protocolo IPv4 e IPv6

IPv4

Codificación en binario ⟷ ***Codificación en decimal***

Otra forma de representar la máscara de red es mediante la notación CIDR intercalando el carácter / entre la dirección IP y número de unos que tiene la máscara, de forma que determina el número de bits que corresponde a la porción de red de la IP.

192.168.0.1/24

El sufijo 24 corresponde la máscara de red 255.255.255.0

11111111.11111111.11111111.00000000

Protocolo IPv4 e IPv6

IPv4

El administrador de la red es el encargado de establecer las distintas redes y rango de direcciones IP de cada una.

Antes de asignar la dirección IP y máscara de red a cada adaptador o interfaz de red se debe diseñar la organización lógica de la red mediante un mapa topológico donde se especifiquen los dispositivos y el esquema de direccionamiento IP.

Dentro del rango de direcciones de cada red se diferencian varios tipos de direcciones:

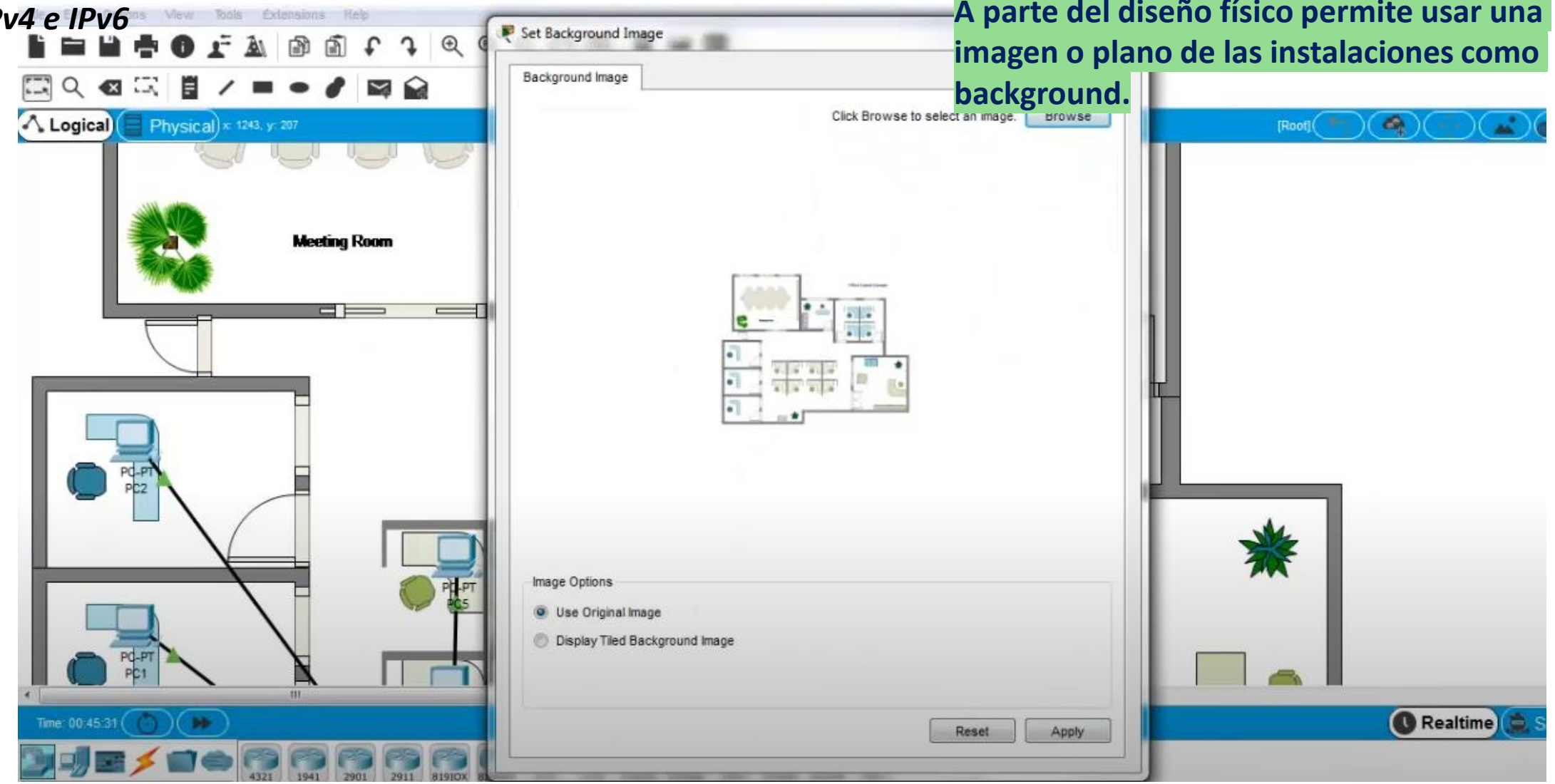
- **Dirección de red:** Especifica la red y se identifica por la primera dirección del rango de direcciones de red, es decir, todos los bits de la porción de host se encuentran en 0. Para determinarla simplemente se aplica un operador lógico tipo AND bit a bit entre la dirección IP y la máscara de red.
- **Dirección de broadcast:** Se emplea para enviar paquetes a todos los hosts de la red a la vez. Se identifica por la última dirección del rango de direcciones de red, es decir, todos los bits de la porción del hosts se encuentran en 1.
- **Direcciones de hosts:** Son la mayoría de las IP de la red que se usan para asignar a los hosts dentro de ella. Se comprenden entre la dirección de red y la dirección del broadcast.

Uso de herramientas como Packet Tracer

Protocolo IPv4 e IPv6

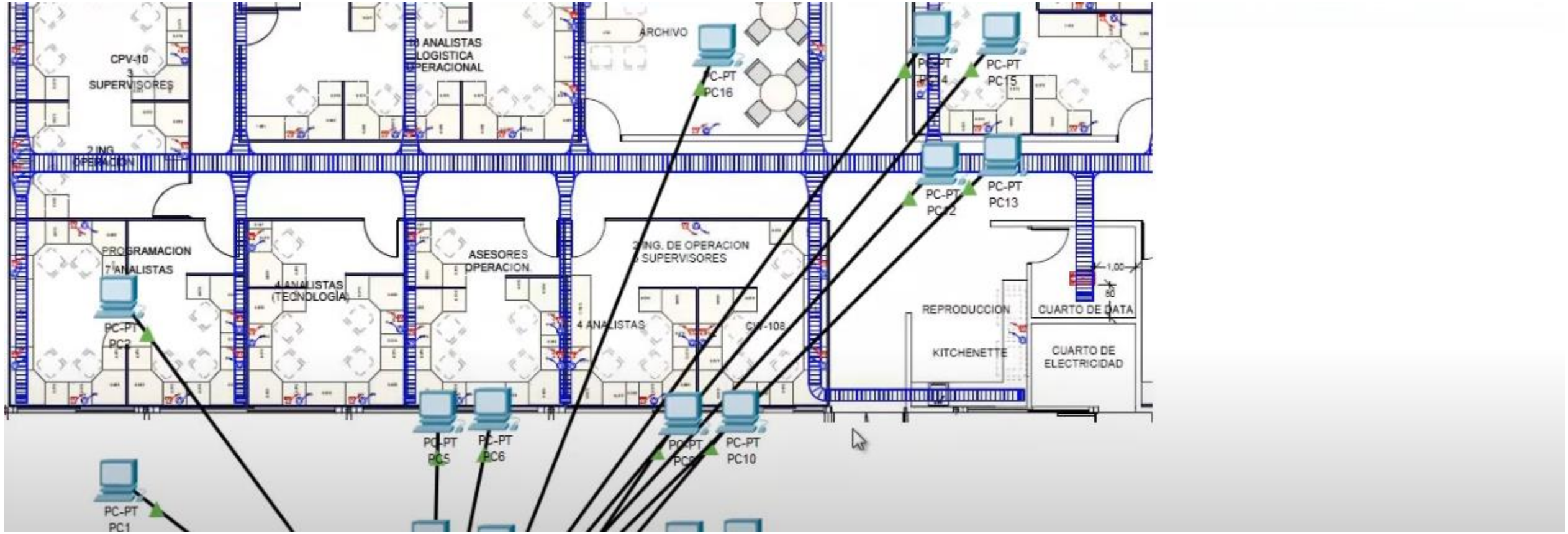
IPv4

A parte del diseño físico permite usar una imagen o plano de las instalaciones como background.



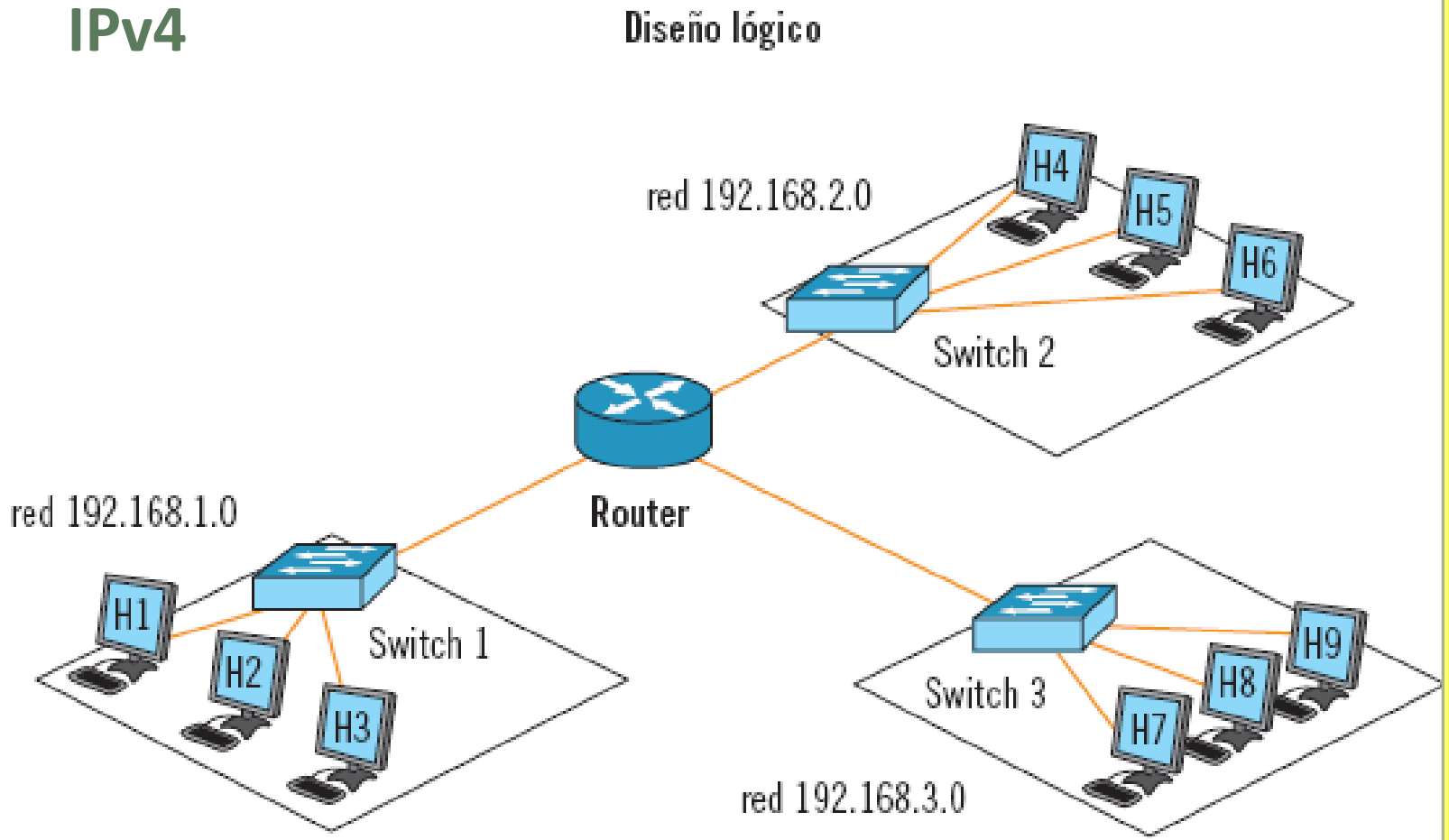
Protocolo IPv4 e IPv6

IPv4



Protocolo IPv4 e IPv6

IPv4



La direcciones IP se pueden clasificar en Públicas y Privadas.

Pública: Se usa con Internet y son únicas a nivel mundial gestionadas por entidades como IANA o RIPE NCC.

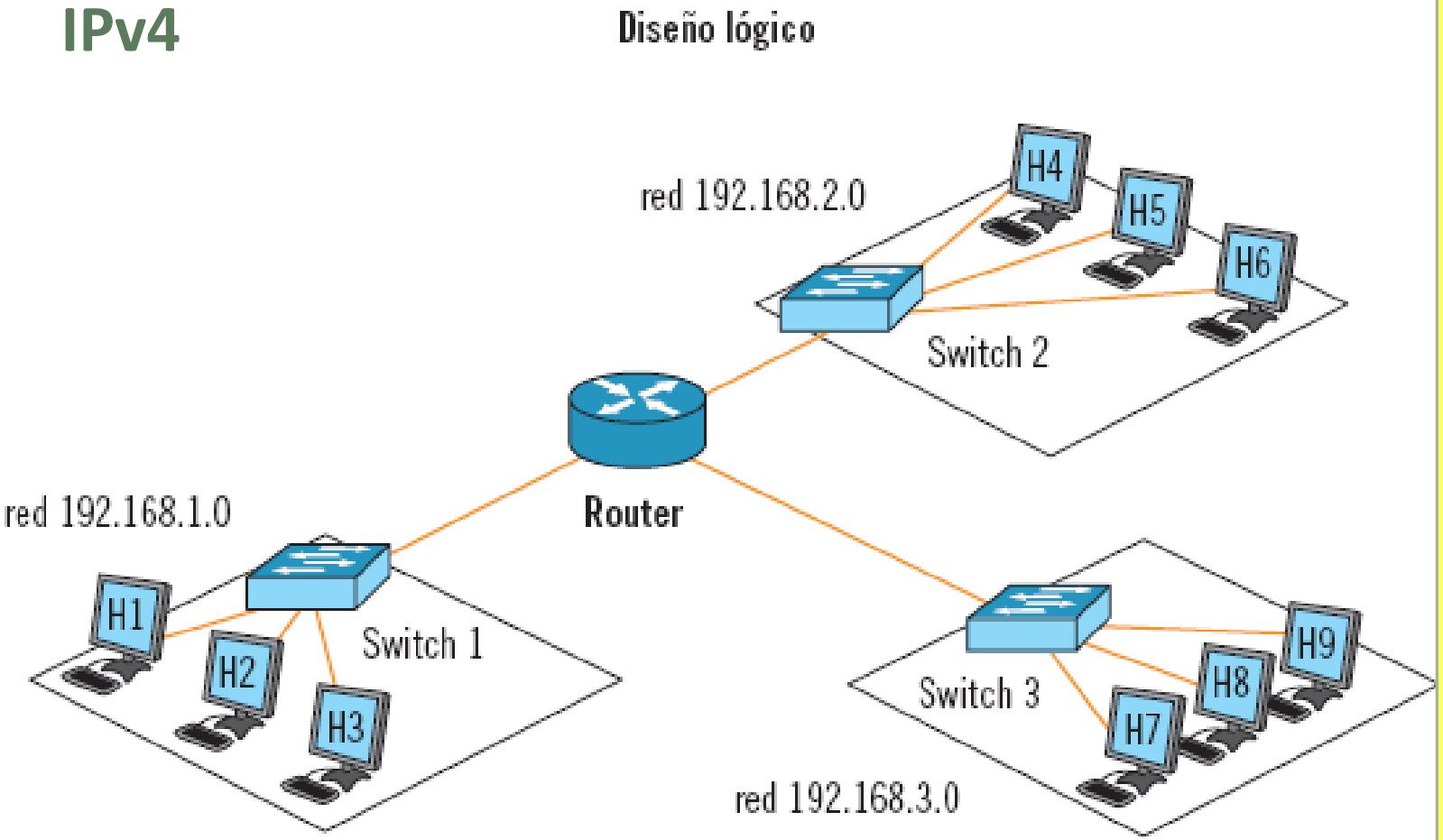
Privada: Se usa para redes con acceso restringido o nulo a Internet. No son asignables a Internet:

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

Estas redes ***para tener acceso a Internet debe hacer uso de un router*** que si tiene ***acceso a Internet gracias a un proveedor de servicios de Internet*** (ej: Vodafone, Orange, Movistar, etc).

Protocolo IPv4 e IPv6

IPv4



El router es el encargado de traducir las direcciones IP privadas a públicas gracias al protocolo bidireccional NAT.

Los adaptadores de red disponen de una dirección física llamada dirección MAC que asocia cada interfaz de red con el fabricante.

Esta dirección está formada por 48 bits en formato hexadecimal del tipo:

A1-EE-15-18-F4-AA

Se usa para que el protocolo Ethernet establezca el origen y el destino de cada trama dentro de la capa de enlace de datos del modelo OSI.

Protocolo IPv4 e IPv6

IPv6

El protocolo permite aumentar la seguridad de las comunicaciones, mejorar el tratamiento de los paquetes, incrementar el número de direcciones IP asignables y permite implantar el Internet de Todo (IoE).

Esta versión del protocolo IP hace uso de 128 bits representados en forma hexadecimal en bloques de 2 bytes con formato del tipo:

3D6A:1DD1:1FF0:4788:FF30:A1BB:CA51:1235D

Protocolo TCP y UDP

El protocolo TCP es el denominado Protocolo de Control de la Transmisión: Garantiza que todos los segmentos lleguen al destino. Hace un seguimiento de todos los datos transmitidos y recibidos. Si un segmento no se recibe se vuelve a enviar.

El protocolo UDP es el denominado Protocolo de Datagramas de Usuario: Envía los segmentos entre aplicaciones de manera rápida sin importar su confiabilidad, ya que la pérdida de algunos segmentos no compromete la comunicación ente las aplicaciones.

El protocolo TCP es más confiable pero más lento que el UDP.

Por esta razón protocolos como FTP o HTTP hacen uso del TCP, mientras que aplicaciones de streaming de vídeo y audio suelen hacer uso del UDP

CONFIGURACIÓN DEL PROTOCOLO TCP/IP

La asignación de la dirección IP a un adaptador de red se puede realizar de dos maneras, de **forma estática** o **dinámica**.

Este adaptador de red puede corresponder a cualquier host, es decir: un ordenador de sobremesa, un ordenador portátil, un smartphone, una Tablet, un smartwatch, un televisor con SmartTV, una cámara de videovigilancia IP, una bombilla LED con funciones de red, etc…

Estática

Hace uso de una dirección IP fija para cada host de forma que se mantiene sin modificar con el paso del tiempo.

Este tipo de configuración se usa para servidores de Internet o que deban mantener dirección IP para ofrecer servicios de impresión, HTTP, FTP, etc…

La asignación de una dirección IP estática se puede realizar manualmente a través del administrador del sistema configurando el adaptador de red.

Para configurarlo en Microsoft Windows (*para otros sistemas operativos es similar*) se debe establecer (*dentro del protocolo TCP/IPv4*):

- Dirección IP
- Máscara de subred
- Puerta de enlace o Gateway: en este caso se trata del router a través del cual accedemos a Internet

La asignación de la dirección IP a un adaptador de red se puede realizar de dos maneras, de **forma estática** o **dinámica**.

Este adaptador de red puede corresponder a cualquier host, es decir: un ordenador de sobremesa, un ordenador portátil, un smartphone, una Tablet, un smartwatch, un televisor con SmartTV, una cámara de videovigilancia IP, una bombilla LED con funciones de red, etc…

Estática

Hace uso de una dirección IP fija para cada host de forma que se mantiene sin modificar con el paso del tiempo.

Este tipo de configuración se usa para servidores de Internet o que deban mantener dirección IP para ofrecer servicios de impresión, HTTP, FTP, etc…

También se debe configurar las **direcciones de servidor** o **DNS**. Se trata de una dirección IP de un servidor DNS que traduce las direcciones de dominio a direcciones IP.

Por ejemplo los de Google públicos son el 8.8.8.8 o 8.8.4.4 o de OpenDNS son el 208.67.222.222 y 208.67.220220

En Microsoft Windows:

- Servidor DNS preferido
- Servidor DNS alternativo

La asignación de la dirección IP a un adaptador de red se puede realizar de dos maneras, de **forma estática** o **dinámica**.

Este adaptador de red puede corresponder a cualquier host, es decir: un ordenador de sobremesa, un ordenador portátil, un smartphone, una Tablet, un smartwatch, un televisor con SmartTV, una cámara de videovigilancia IP, una bombilla LED con funciones de red, etc…

Dinámica

Hace uso de una dirección IP fija para cada host de forma que se mantiene sin modificar con el paso del tiempo.

Este tipo de configuración se usa para servidores de Internet o que deban mantener dirección IP para ofrecer servicios de impresión, HTTP, FTP, etc…

La asignación de la dirección IP cambia con el paso del tiempo.

En la mayoría de los equipos informáticos se hace uso del **protocolo DCHP**.

Se hace uso de un servidor DHCP que provee de la configuración específica a los clientes DHCP.

La asignación de la dirección IP a un adaptador de red se puede realizar de dos maneras, de **forma estática** o **dinámica**.

Este adaptador de red puede corresponder a cualquier host, es decir: un ordenador de sobremesa, un ordenador portátil, un smartphone, una Tablet, un smartwatch, un televisor con SmartTV, una cámara de videovigilancia IP, una bombilla LED con funciones de red, etc…

Dinámica

Hace uso de una dirección IP fija para cada host de forma que se mantiene sin modificar con el paso del tiempo.

Este tipo de configuración se usa para servidores de Internet o que deban mantener dirección IP para ofrecer servicios de impresión, HTTP, FTP, etc…

El protocolo DHCP asigna de forma automática la dirección IP, la máscara de red, la puerta de enlace y servidores DNS.

Los routers domésticos (**router SoHo**) habilitan este servidor por defecto y por ello cuando nos conectamos a una red en una casa normalmente lo hacemos de forma automática sin tener que configurar nada más que indicar el nombre de la red e insertar la passwd.

La asignación de la dirección IP a un adaptador de red se puede realizar de dos maneras, de **forma estática** o **dinámica**.

Este adaptador de red puede corresponder a cualquier host, es decir: un ordenador de sobremesa, un ordenador portátil, un smartphone, una Tablet, un smartwatch, un televisor con SmartTV, una cámara de videovigilancia IP, una bombilla LED con funciones de red, etc…

Dinámica

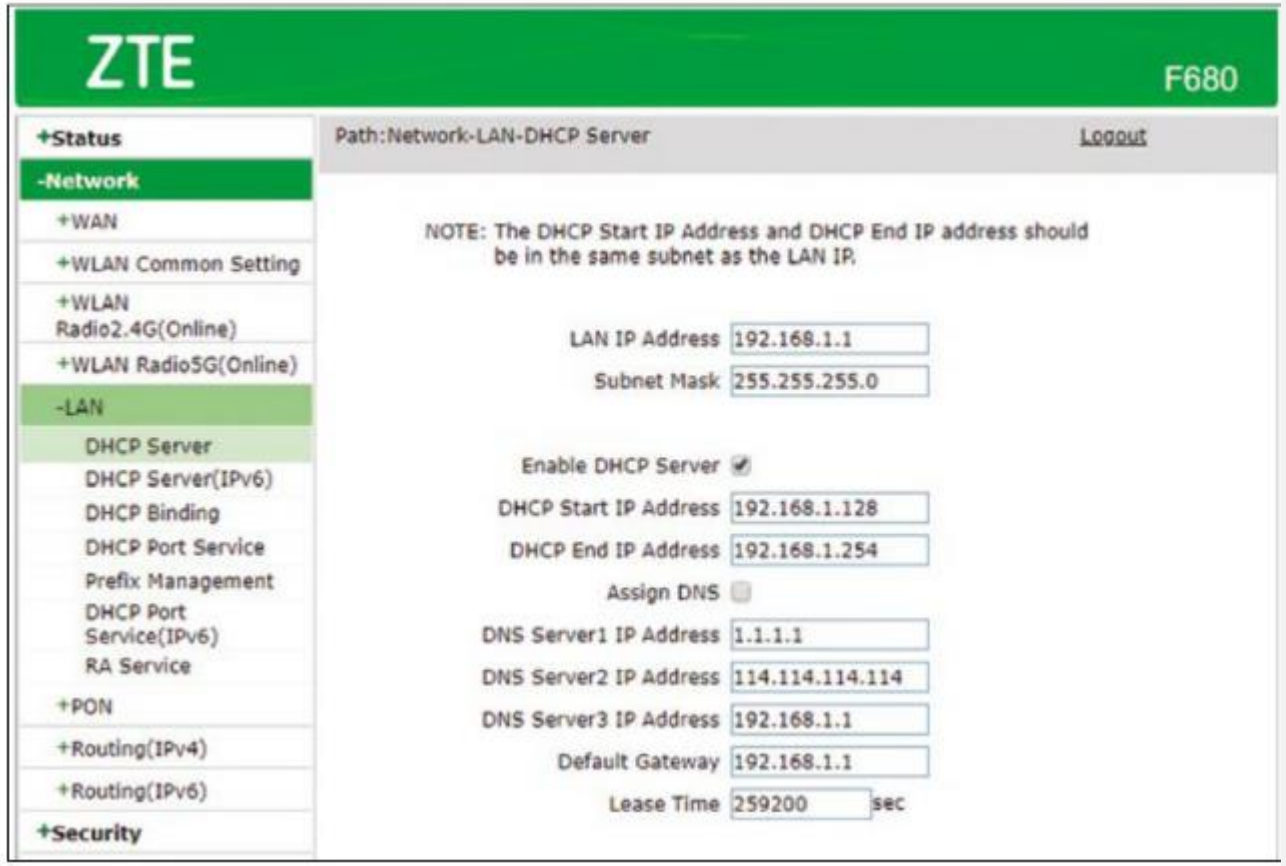
Hace uso de una dirección IP fija para cada host de forma que se mantiene sin modificar con el paso del tiempo.

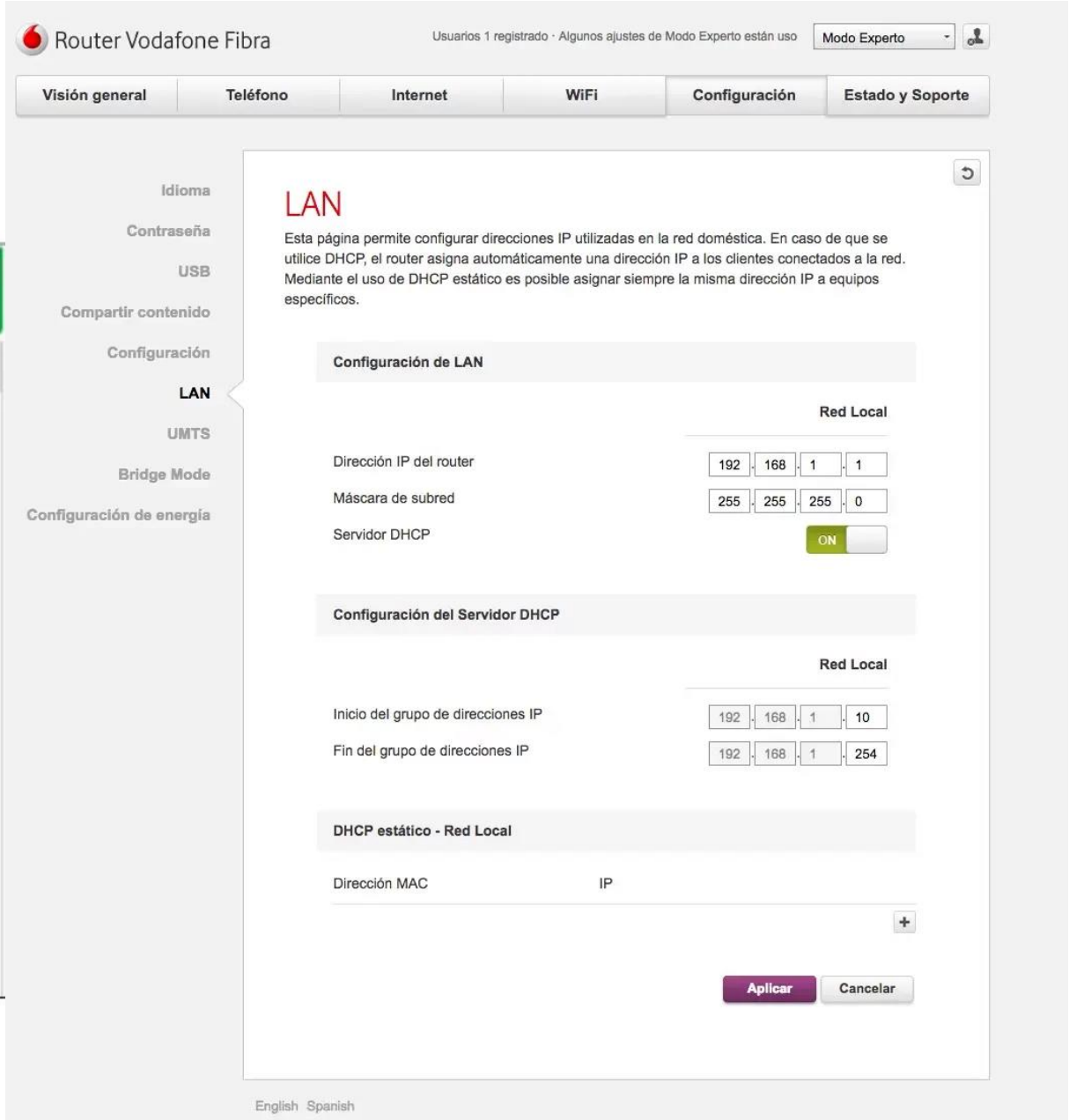
Este tipo de configuración se usa para servidores de Internet o que deban mantener dirección IP para ofrecer servicios de impresión, HTTP, FTP, etc…

Los servidores DHCP permiten establecer el rango de direcciones asignables por este protocolo, el resto se reservan para el direccionamiento estático.

Para configurar este protocolo en Microsoft Windows, simplemente se ha de mantener automático el protocolo TCP/IPv4.

2. CONFIGURACIÓN DEL PROTOCOLO TCP/IP





INTERCONEXIÓN DE REDES Y COMPONENTES

Capa	Dispositivo	Función
Física	Repetidor	Regenera la señal entre dos puntos de una red. Existen inalámbricos o cableados.
	Hub	Replica la información entrante por uno de sus puertos al resto de puertos.
Enlace de datos	Switch	Conecta la información entrante por uno de sus puertos al puerto de destino únicamente.
	Punto de acceso	Extiende la red cableada mediante un medio inalámbrico. Pertenece a las capas 1 y 2 del modelo OSI.
Red	Router	Conecta redes diferentes.

SWITCH

ROUTER

Tipos de routers:

- **Rackeable: son empleado para entornos empresariales, se conectan y configuran a través de armarios racks.**

- **SoHo: son los suministrados por los proveedores de acceso a Internet. Son para uso doméstico y permiten conectar la red local de nuestra casa con Internet. Integran los dispositivos como el switch, punto de acceso Wi-Fi y firewall.**

ARMARIO RACK

Tipos de routers:

- **Rackeable: son empleado para entornos empresariales, se conectan y configuran a través de armarios racks.**

- **SoHo: son los suministrados por los proveedores de acceso a Internet. Son para uso doméstico y permiten conectar la red local de nuestra casa con Internet. Integran los dispositivos como el switch, punto de acceso Wi-Fi y firewall.**

ARMARIO RACK MONTADO Y CONFIGURADO

Los routers y los hosts utilizan **tablas de enrutamiento** para encaminar paquetes a otros dispositivos de una red local o una red remota. Cuando dos hosts se encuentran en la misma red local, en la comunicación no interviene el router.

Cuando la comunicación es remota, es decir entre distintas redes, si son necesarios.

En dichas tablas de enrutamiento se almacenan:

- Direcciones de host de él mismo.
- Direcciones a un host local.
- Direcciones a un host remoto.

La tabla de enrutamiento en un host de Microsoft Windows se puede observar con el comando *netstat –r*

En GNU/Linux mediante el comando *ip route show*.

```
IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      192.168.0.1     192.168.0.10     35
        127.0.0.0        255.0.0.0      En vínculo        127.0.0.1    331
        127.0.0.1  255.255.255.255      En vínculo        127.0.0.1    331
  127.255.255.255  255.255.255.255      En vínculo        127.0.0.1    331
      192.168.0.0    255.255.255.0      En vínculo      192.168.0.10    291
     192.168.0.10  255.255.255.255      En vínculo      192.168.0.10    291
    192.168.0.255  255.255.255.255      En vínculo      192.168.0.10    291
     192.168.56.0    255.255.255.0      En vínculo      192.168.56.1    281
     192.168.56.1  255.255.255.255      En vínculo      192.168.56.1    281
   192.168.56.255  255.255.255.255      En vínculo      192.168.56.1    281
        224.0.0.0        240.0.0.0      En vínculo        127.0.0.1    331
        224.0.0.0        240.0.0.0      En vínculo      192.168.56.1    281
        224.0.0.0        240.0.0.0      En vínculo      192.168.0.10    291
  255.255.255.255  255.255.255.255      En vínculo        127.0.0.1    331
  255.255.255.255  255.255.255.255      En vínculo      192.168.56.1    281
  255.255.255.255  255.255.255.255      En vínculo      192.168.0.10    291
===========================================================================
```

Topologías de red

Este mapa ilustra la organización de los componentes y conexiones físicas entre elementos de una red. Se distinguen:

- **Inalámbricas:**

✓ Distribuida: emplea puntos de acceso para que los clientes se conecten a red y puedan moverse libremente saltando de un punto de acceso a otro.

✓ Centralizada: se utilizan puntos de acceso sin capacidad de gestión conectados entre ellos a switches WLAN controlando y gestionando la red Wi-Fi.

- **Cableadas:**

✓ De área extensa (WAN): pueden ser de punto a punto, en estrella o en malla.

✓ De área metropolitana (MAN): pueden ser en estrella o en estrella extendida.

✓ De área local (LAN): pueden ser en bus, en anillo, en estrella o en estrella extendida.

Topología lógica

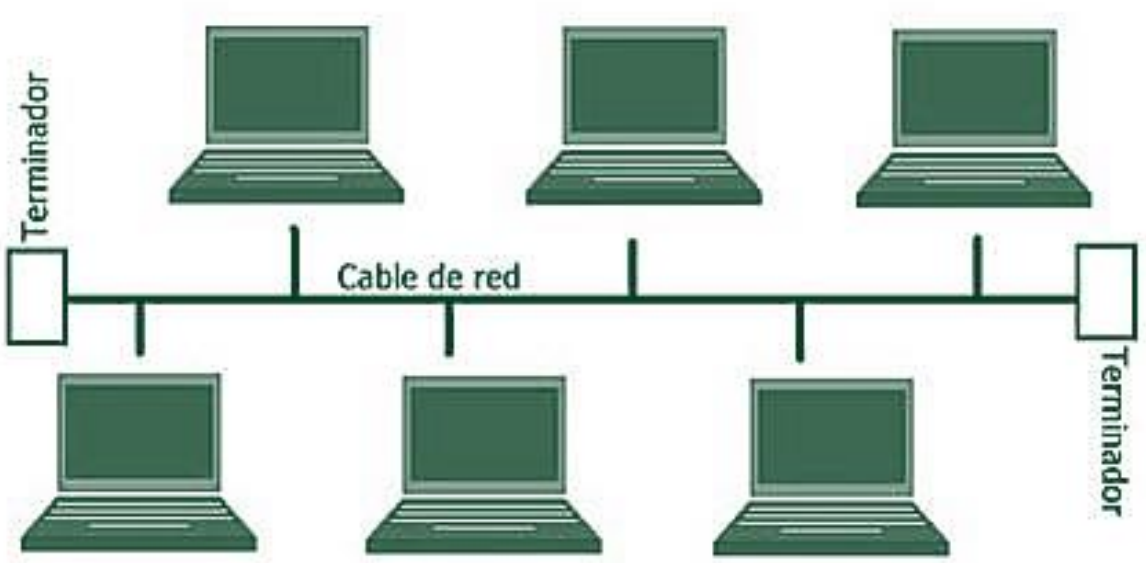
Topología de bus

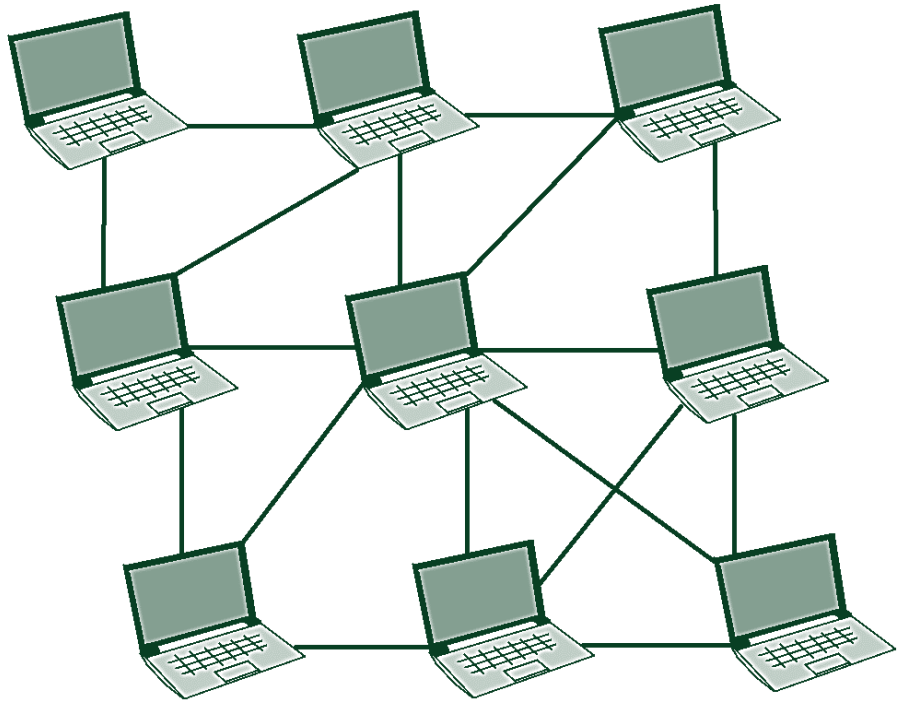
Topología de anillo

Topología en estrella

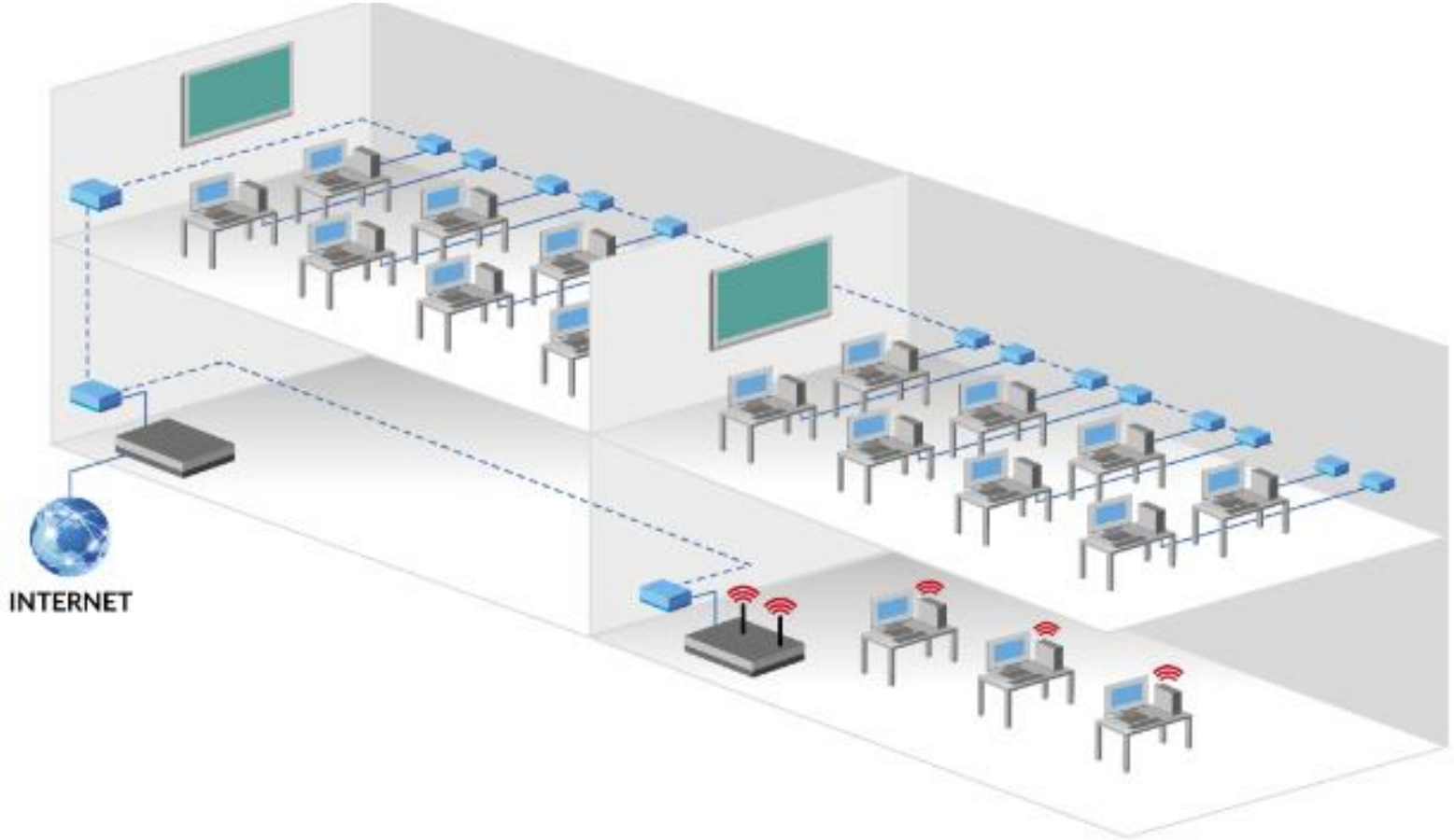
Topología en estrella extendida

Topología en malla





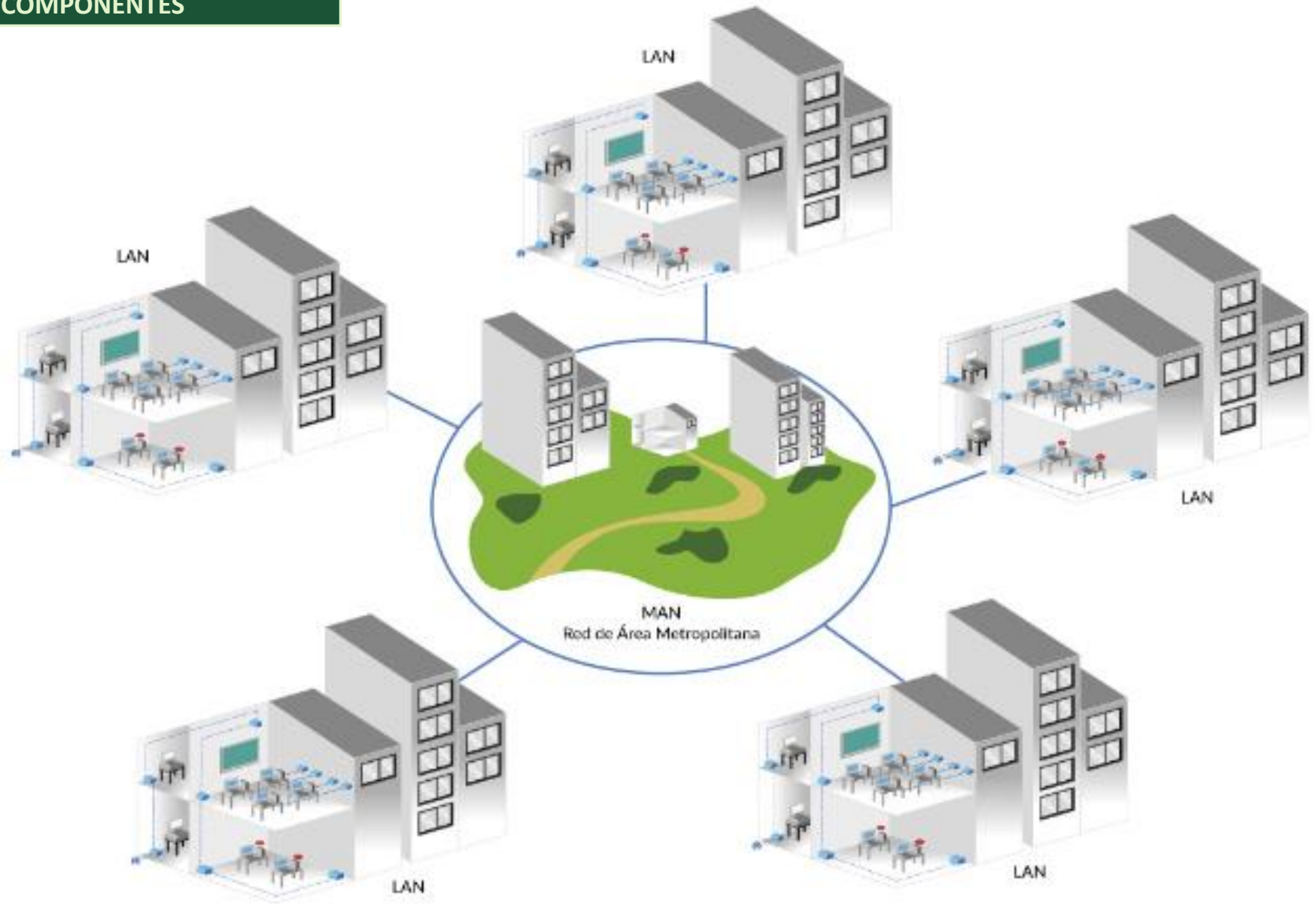
Topología lógica



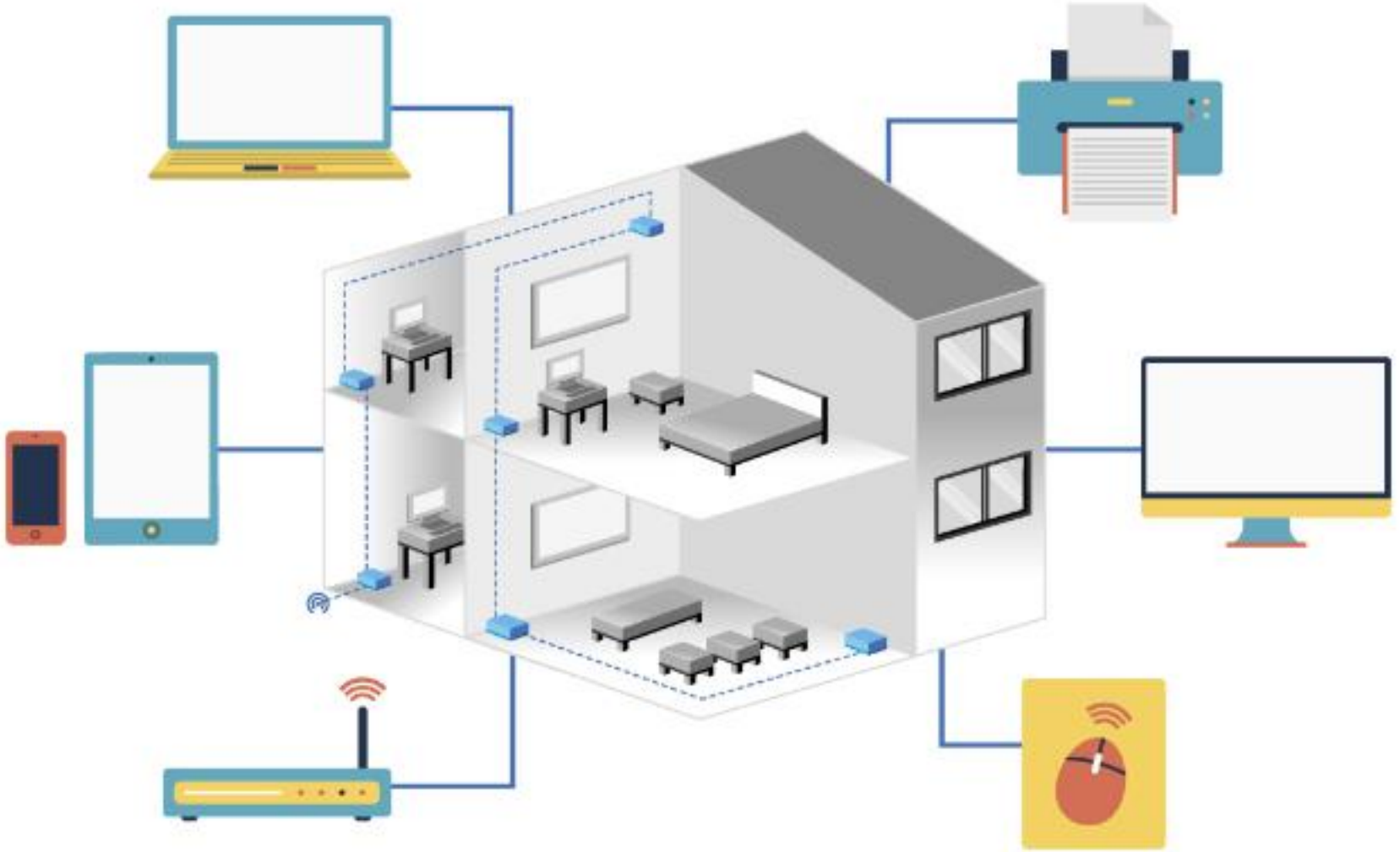
Red LAN

Topología lógica

Red MAN

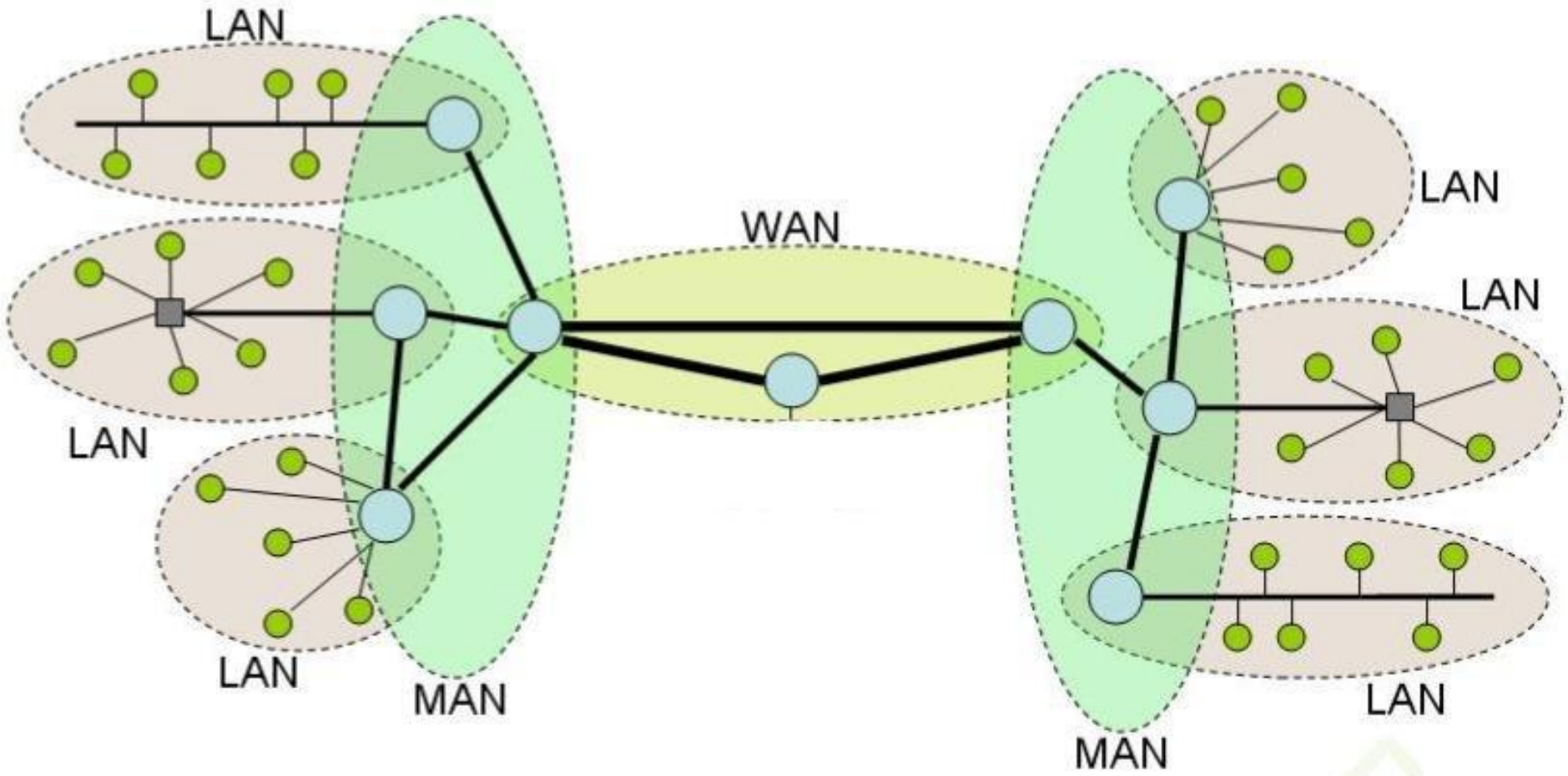


Topología lógica

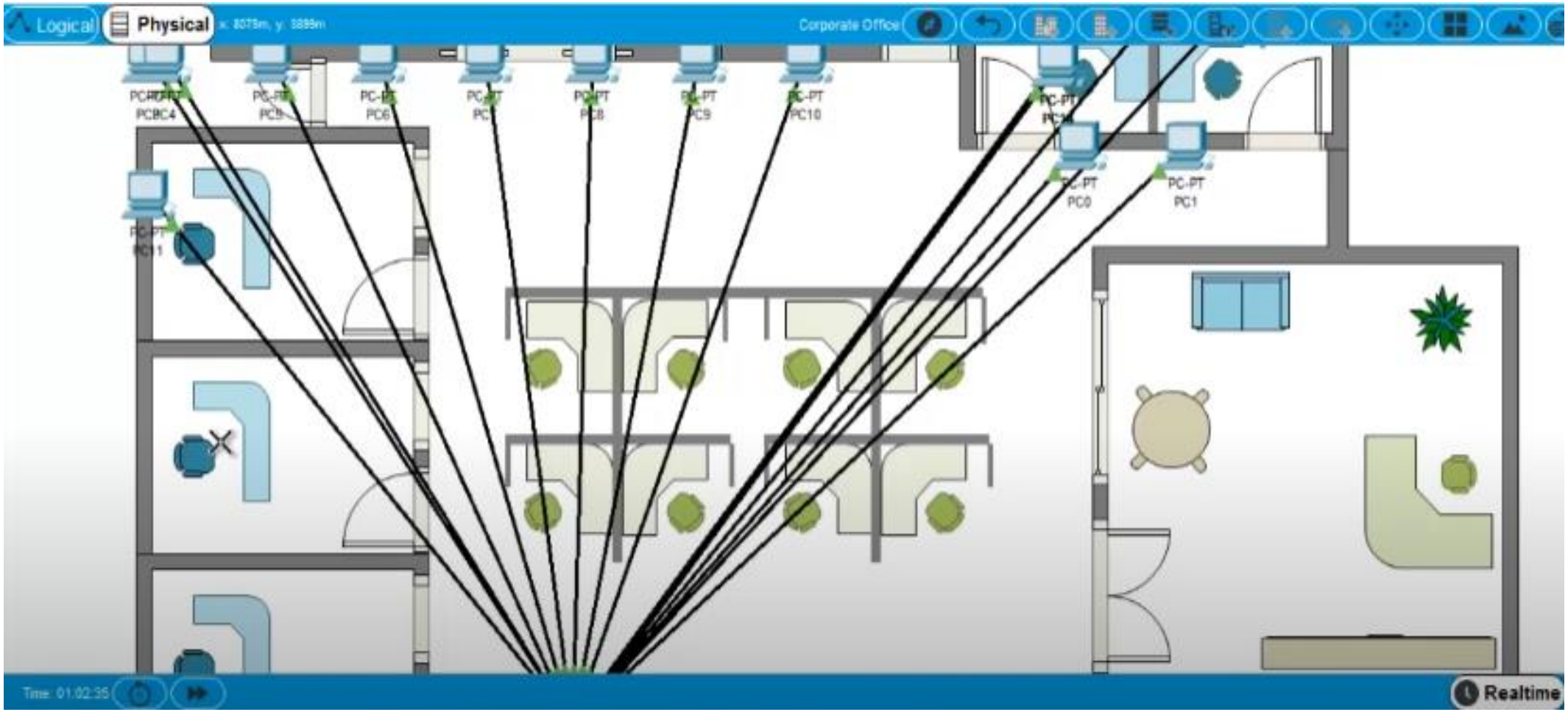


Red PAN

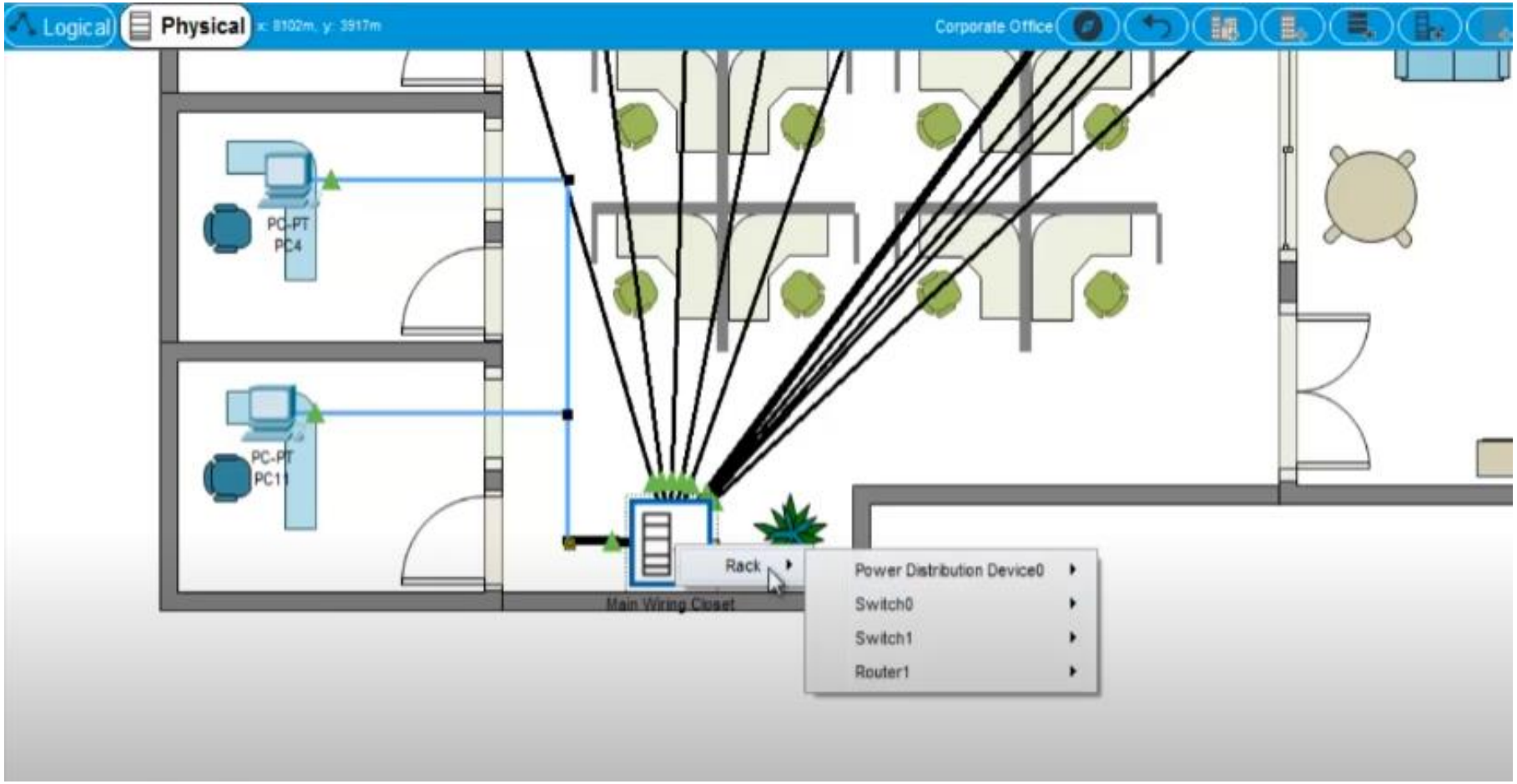
Topología lógica



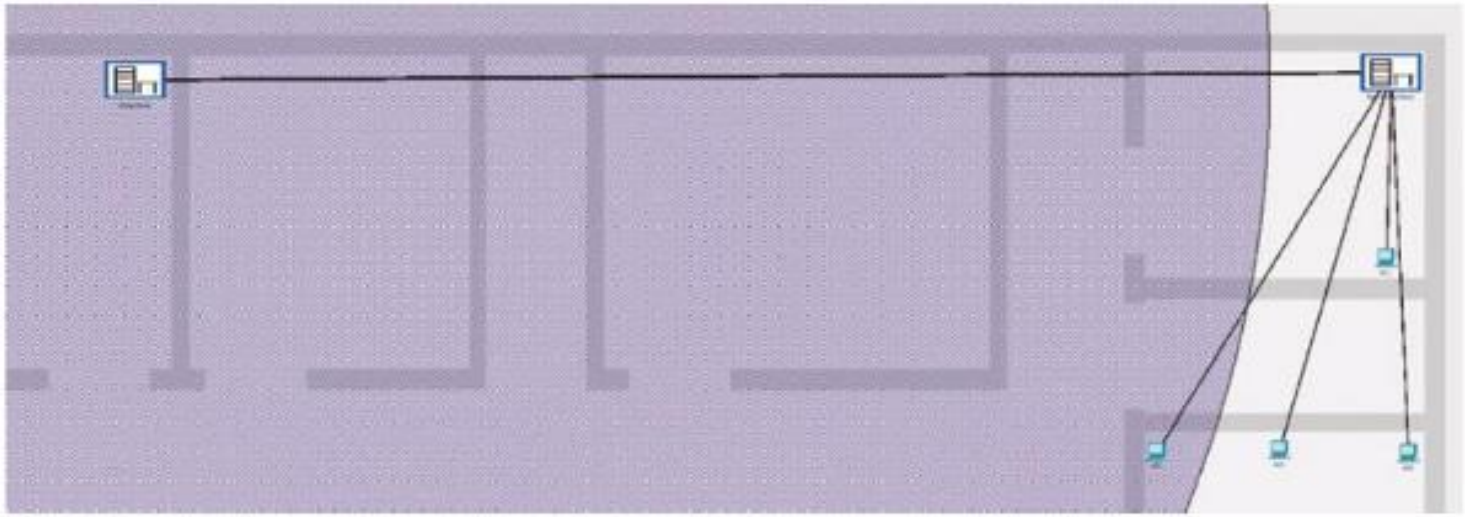
Topología física



Topología física



Topología física



Dominios de colisión y difusión

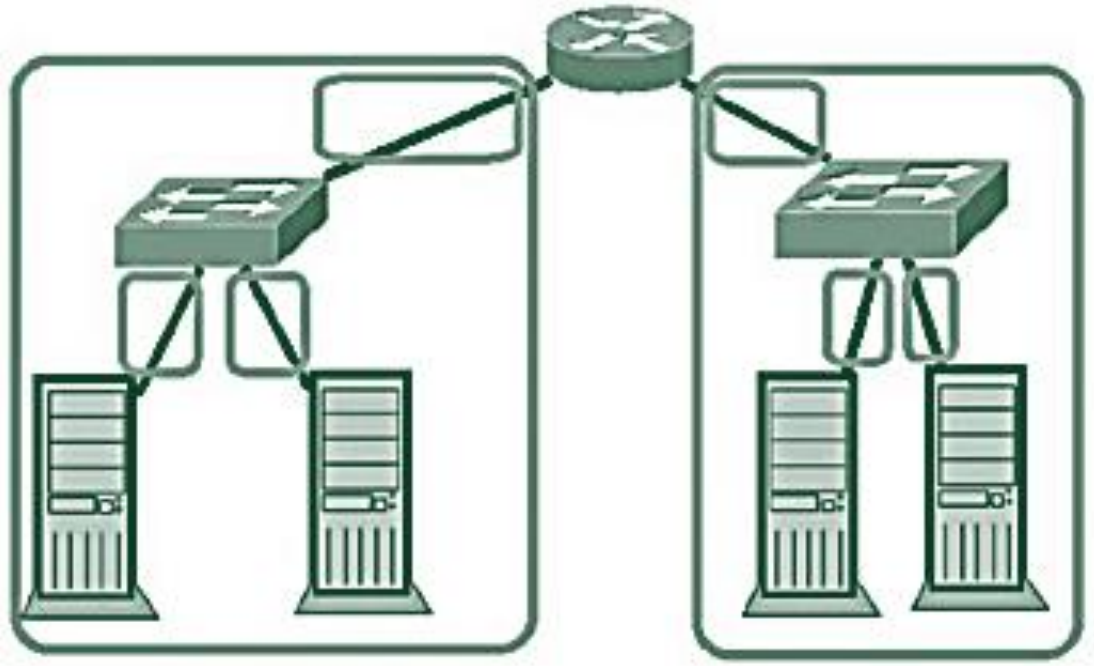
Para los dispositivos que trabajan en la capa 2 o superiores como routers y switches dividen los dominios de colisión, es decir, área donde pueden colisionar dos paquetes.

Adicionalmente en los dispositivos de capa 3 o superior como los routers dividen los dominios de difusión, es decir, áreas donde reciben tramas de broadcasts.

La segmentación de una red en dominios de colisión y dominios de difusión mejoran la eficiencia de la red y aumentan el ancho de banda.

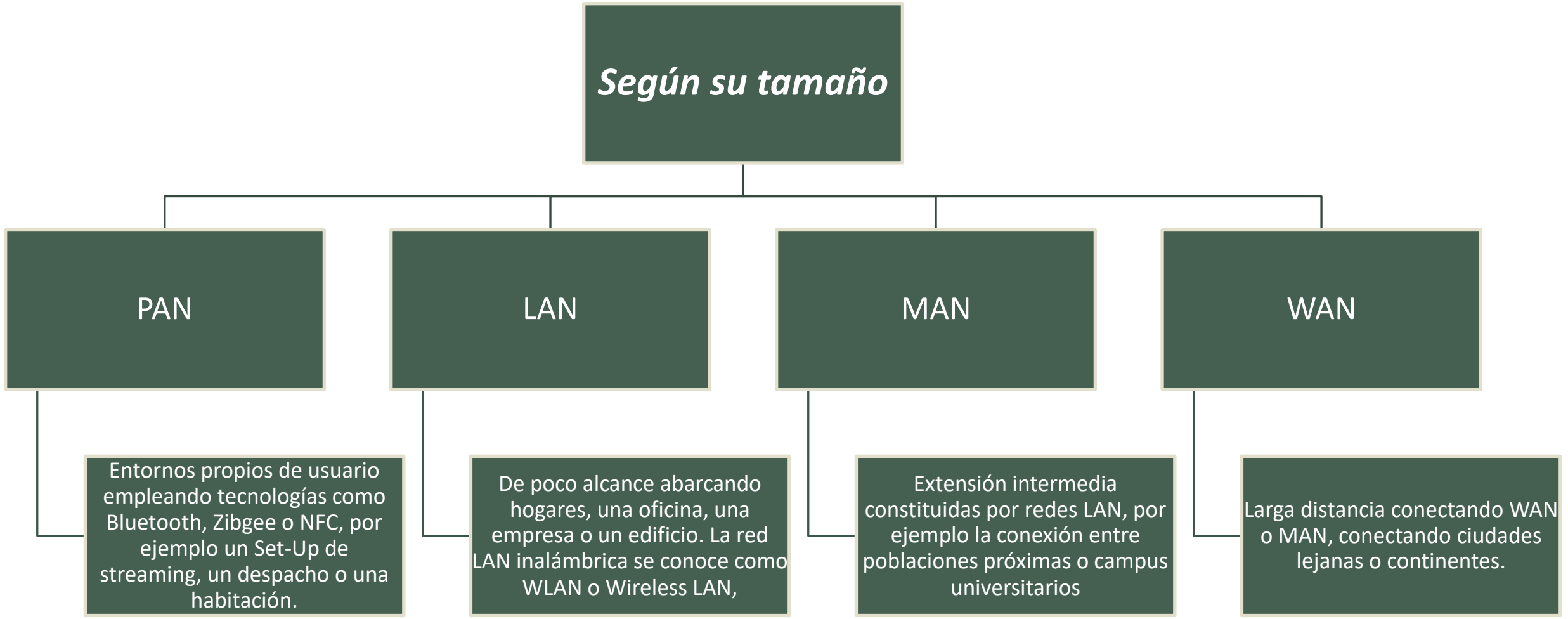
Dominios de colisión y difusión

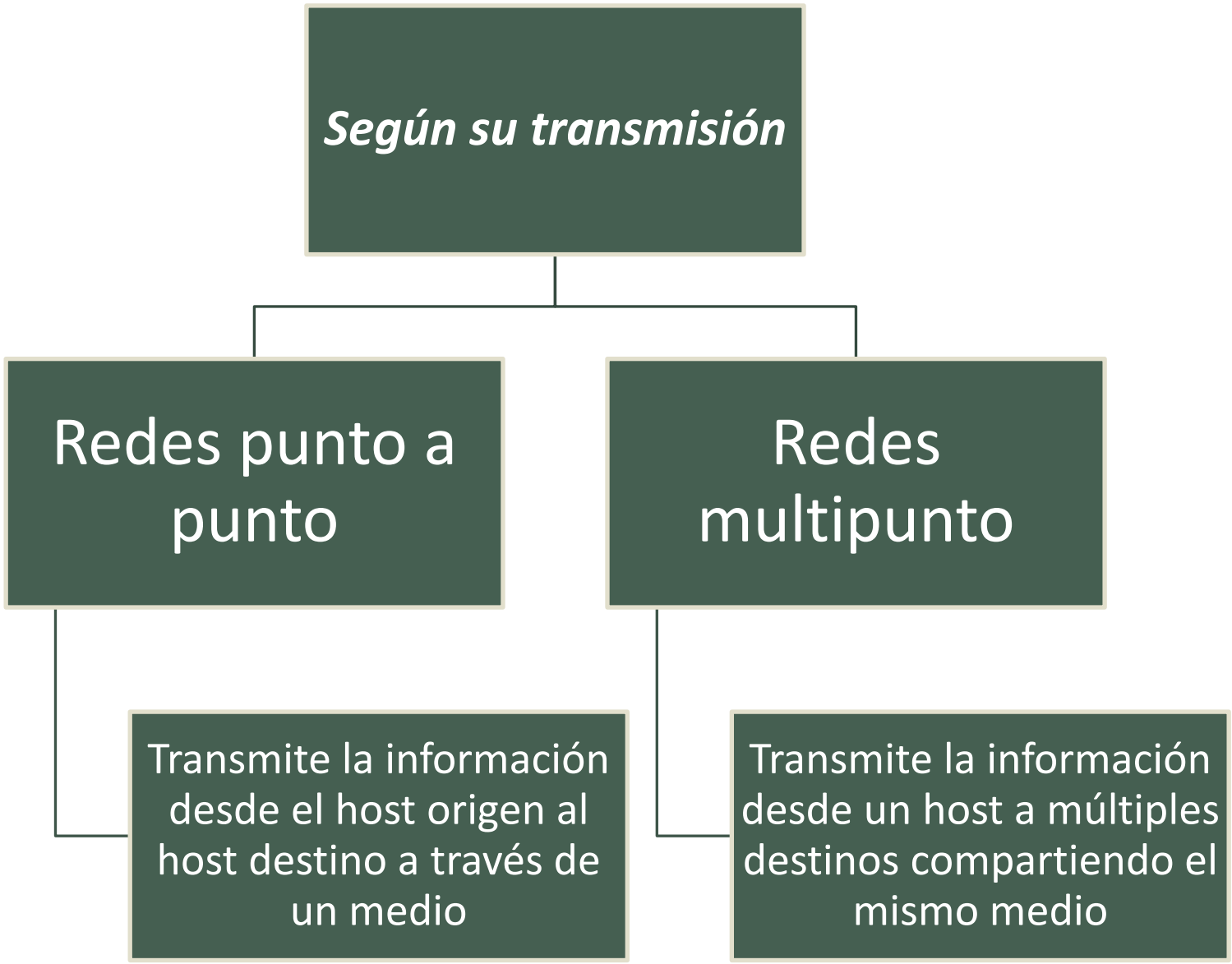
5 dominios de colisión

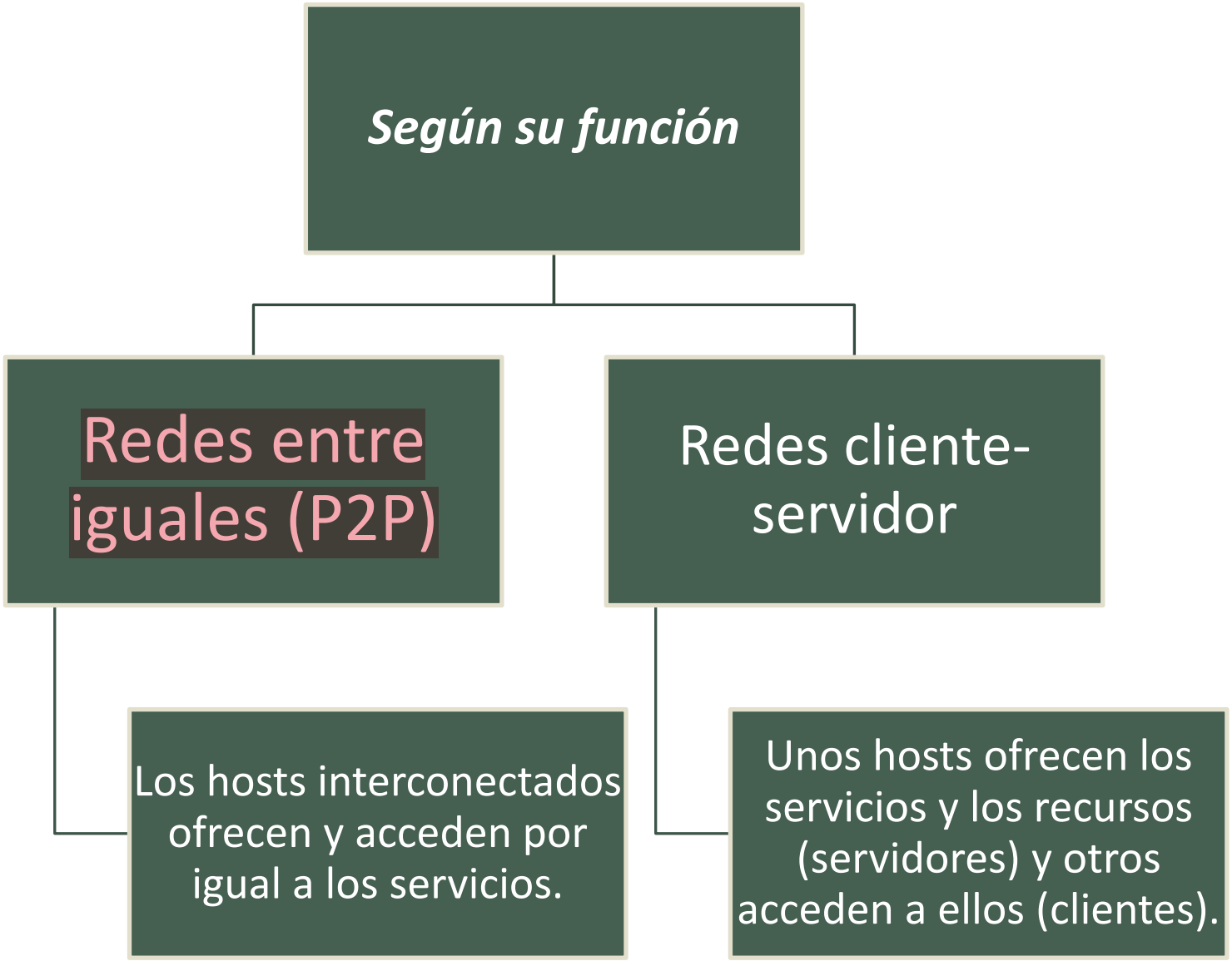


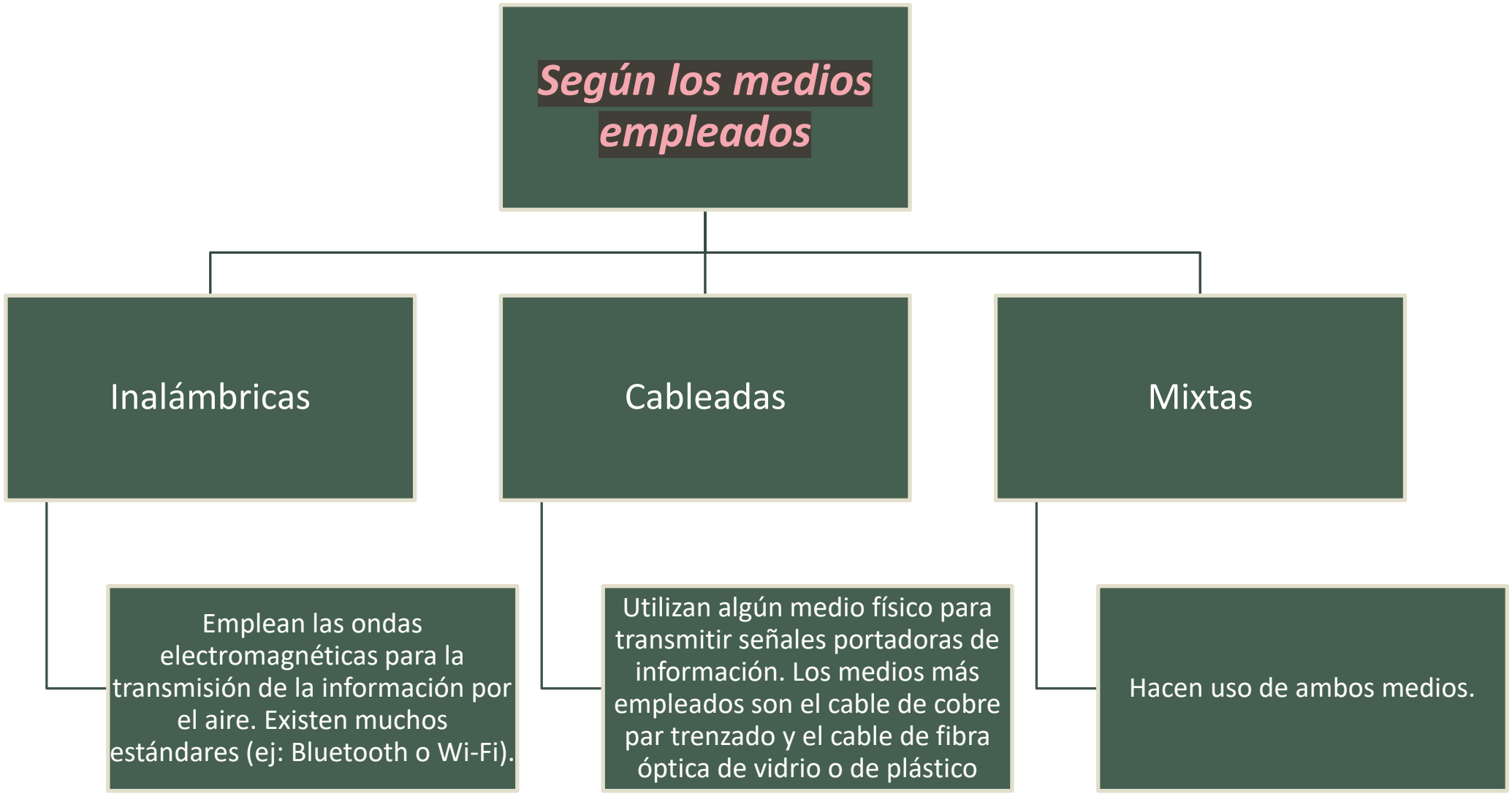
2 dominios de difusión + 3 dominios de colisión

TIPOS DE REDES


Según su tamaño
PAN
LAN
MAN
WAN
Entornos propios de usuario empleando tecnologías como Bluetooth, Zibgee o NFC, por ejemplo un Set-Up de streaming, un despacho o una habitación.
De poco alcance abarcando hogares, una oficina, una empresa o un edificio. La red LAN inalámbrica se conoce como WLAN o Wireless LAN,
Extensión intermedia constituidas por redes LAN, por ejemplo la conexión entre poblaciones próximas o campus universitarios
Larga distancia conectando WAN o MAN, conectando ciudades lejanas o continentes.


Según su transmisión
Redes punto a punto
Redes multipunto
Transmite la información desde el host origen al host destino a través de un medio
Transmite la información desde un host a múltiples destinos compartiendo el mismo medio


Según su función
Redes entre iguales (P2P)
Redes cliente-servidor
Los hosts interconectados ofrecen y acceden por igual a los servicios.
Unos hosts ofrecen los servicios y los recursos (servidores) y otros acceden a ellos (clientes).


Según los medios empleados
Inalámbricas
Cableadas
Mixtas
Emplean las ondas electromagnéticas para la transmisión de la información por el aire. Existen muchos estándares (ej: Bluetooth o Wi-Fi).
Utilizan algún medio físico para transmitir señales portadoras de información. Los medios más empleados son el cable de cobre par trenzado y el cable de fibra óptica de vidrio o de plástico
Hacen uso de ambos medios.

ACCESO A REDES WAN Y TECNOLOGÍAS

La conexión de redes LAN a largas distancias se lleva a cabo mediante el uso de redes WAN.

Mientras que las redes LAN son propiedad de particulares (por ejemplo tu hogar), la conexión con otra red LAN es inalcanzable geográficamente mientras no hagan uso de la suscripción a un proveedor de servicios de red o proveedor de Internet (denominado ISP).

Las redes de área extensa (WAN) requieren de estándares y tecnologías a las redes LAN principalmente debido a las largas distancias con las que trabajan.

Conexiones WAN privadas

Conexiones WAN públicas

Conexiones WAN privadas

Existen distintos tipos de conexiones WAN privadas entre las que destacan:

- Conmutación de circuitos: se requiere que se establezca un circuito o canal dedicado entre los nodos y terminales antes de que se comuniquen los usuarios. Uno de los ejemplos más habituales de este tipo de conexiones son la red telefónica conmutada tradicional. El canal es compartido por varias conversaciones gracias a la multiplexación por división temporal o TDM. Reparte el tiempo de conexiones por turnos. Algunos ejemplos de este tipo de comunicaciones son PSTN e ISDN (RDSI).

- Conmutación de paquetes: hace uso de la división de los datos para transmitir en paquetes a través de una red compartida. No es necesario que se establezca un circuito previamente. La red compartida facilita la comunicación entre multitud de pares de nodos a través de un mismo canal. Son más económicas que la conmutación de circuitos pero tienen latencias superiores. Algunos ejemplos de este tipo de conexiones son *Frame Relay*, x. 25 y ATM.

- Dedicada: su empleo se usa para establecer una conexión directa y permanente entre dos nodos de la red WAN del proveedor de servicios. Se conectan diferentes localizaciones del cliente entre un origen y un destino remoto. Suponen un coste elevado y se reducen tiempos de latencia. Se usan para aplicaciones de voz sobre IP (VoIP) y vídeo sobre IP.

Conexiones WAN públicas

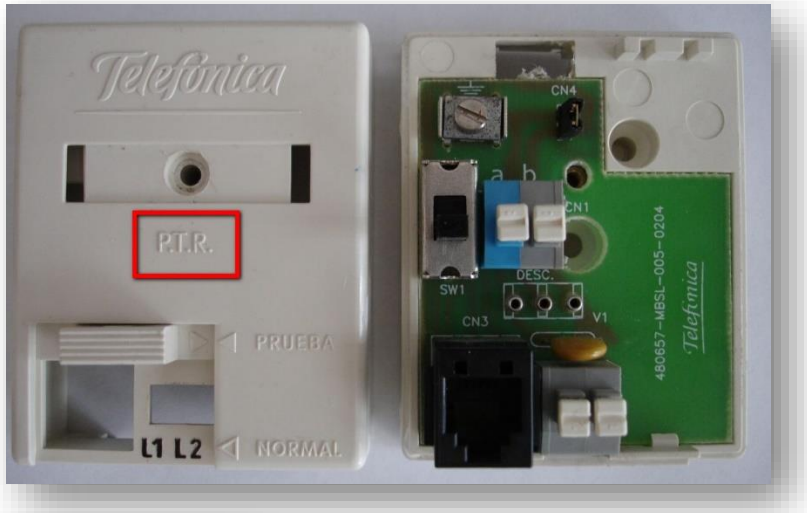
Existen distintos tipos de conexiones WAN públicas entre las que destacan:

- DSL o *Digital Subscriber Line*: corresponde a la familia de tecnologías SDSL, IDSL, HDSL, **VDSL** y **ASDSL** (*estos dos últimos son los más conocidos*). Permiten el acceso a Internet mediante **cables de cobre de par trenzado a través de la red telefónica** con un ancho de banda aceptable (entre los 20 MG/s y los 30 MG/s).
- FTTH o fibra óptica hasta el hogar: corresponde al uso de **tecnología óptica para transmitir la señal**. Permite alcanzar velocidades muy superiores a la tecnologías DSL (100 MG/s, 300 MG/s o 600 MG/s). Emplea fibra óptica desde la red troncal hasta los clientes.

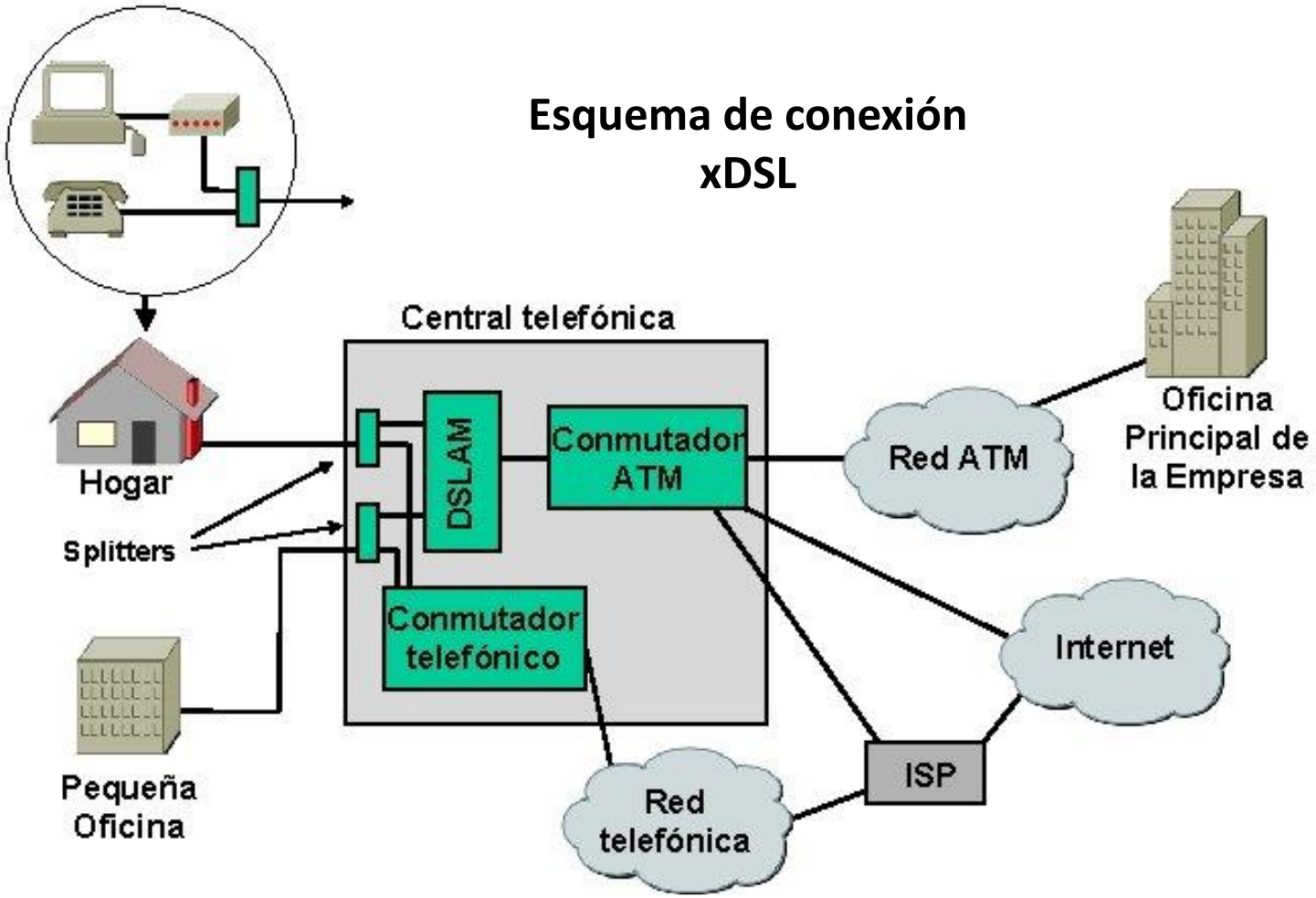
  Hacen uso de equipos con tecnologías GPON (*Gigabit-capable Passive Optical Network*):

  - OLT (Optical Line Termination): se trata de un dispositivo activo del que parten las fibras a los diferentes usuarios.
  - Divisor óptico o splitter: divide la señal óptica entrante en partes iguales de menor potencia a diferentes ramas o usuarios.
  - ONT (Optical Network Terminal): convierte las señales ópticas en señales eléctricas, y viceversa. Actualmente se integra en los routers SoHo.

Conexiones WAN públicas

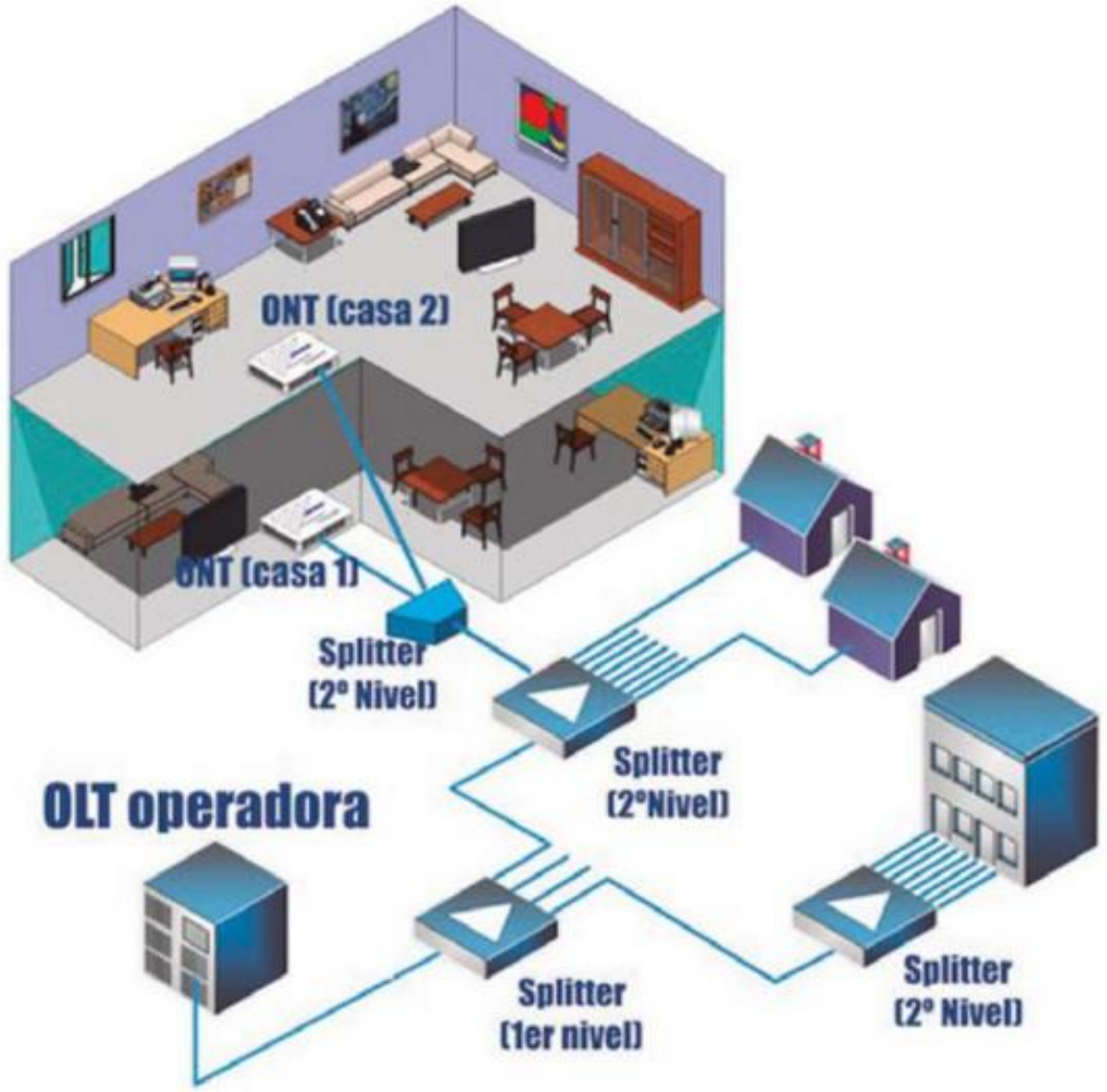


Esquema de conexión xDSL



Conexiones WAN públicas

Esquema de conexión FTTH



Conexiones WAN públicas

Existen distintos tipos de conexiones WAN públicas entre las que destacan:

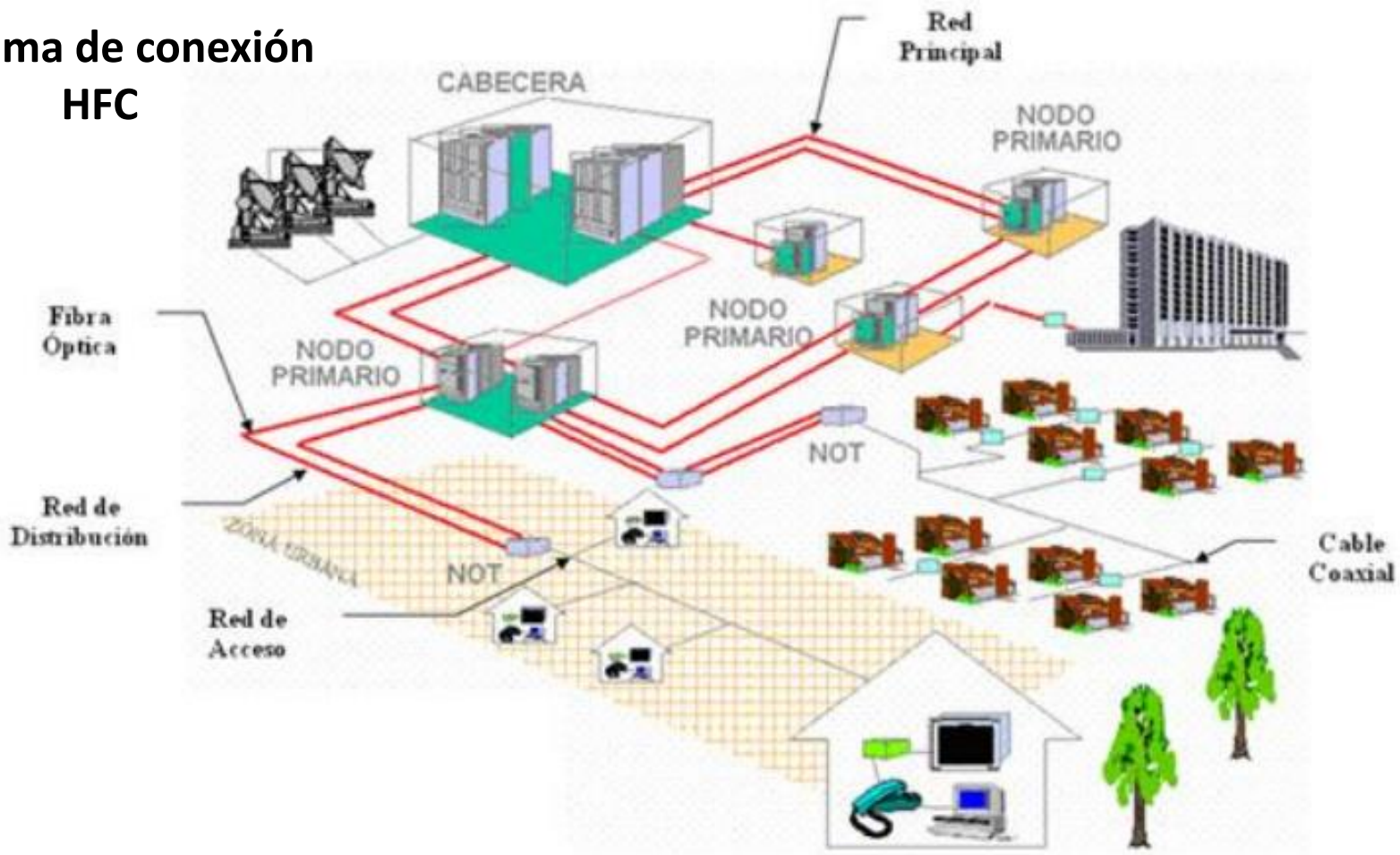
- HFC o híbrido fibra-coaxial: emplea la **fibra óptica en la red troncal** y el **cable coaxial en la red de distribución hasta los hogares**.

- Inalámbricas: **hacen uso de ondas electromagnéticas para la transmisión de datos**. No requieren de cableado. Se diferencian las distintas tecnologías inalámbricas en la longitud de onda y frecuencia de las que hacen uso. Las más habituales a día de hoy son:

    - WiMAX: permite un alcance alrededor de 60 km a la redonda, pudiendo alcanzar velocidades de 1GBps. Es muy utilizada en aquellas zonas geográficas que no dispongan de cobertura por cable (por ejemplo zonas rústicas, aldeas y diseminados, etc..)
    - LTE-A (4G) y 5G: permiten una gran movilidad de los terminales inalámbricos llegando a alcanzar varias Gbps.

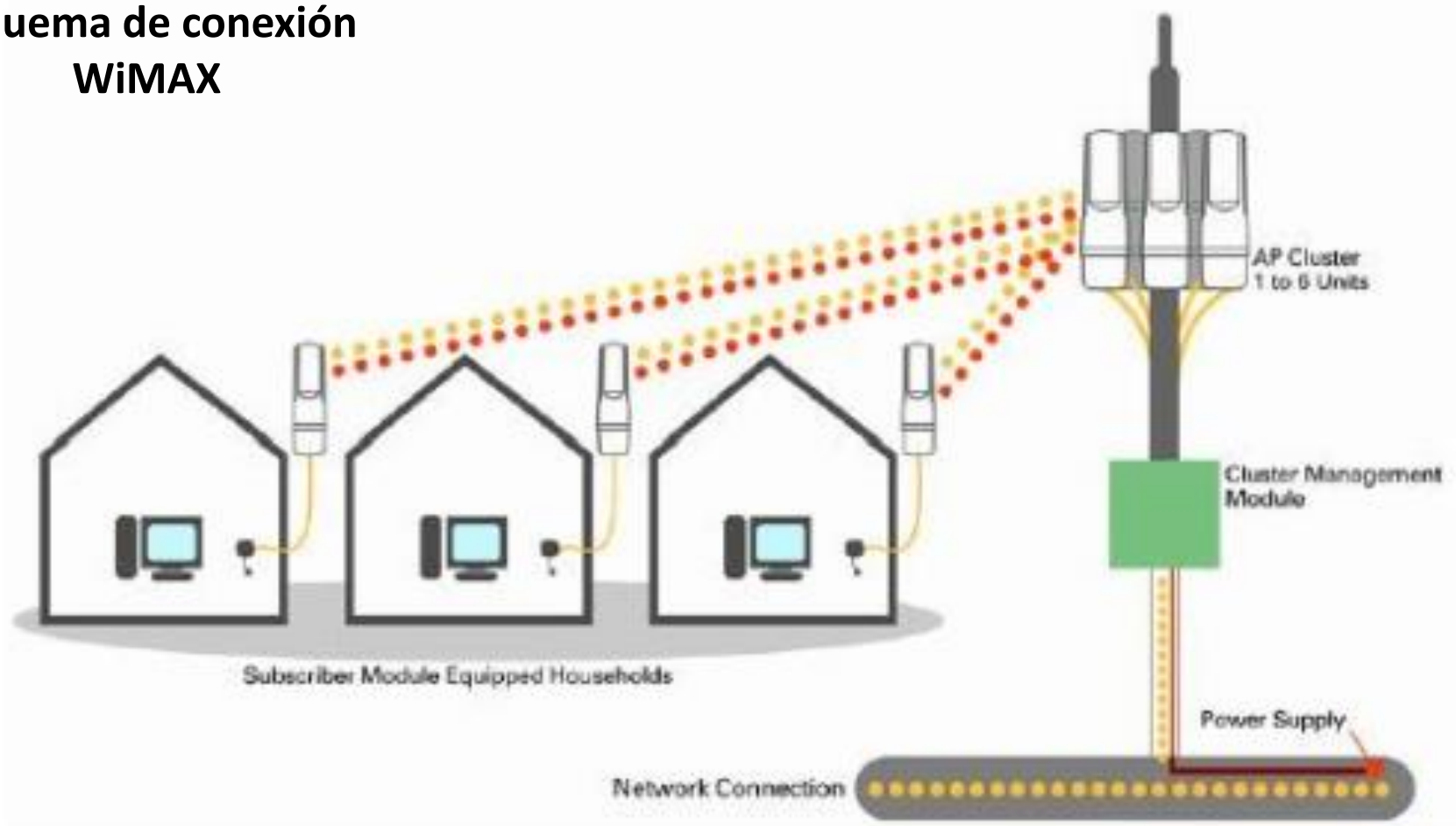
Conexiones WAN públicas

Esquema de conexión HFC



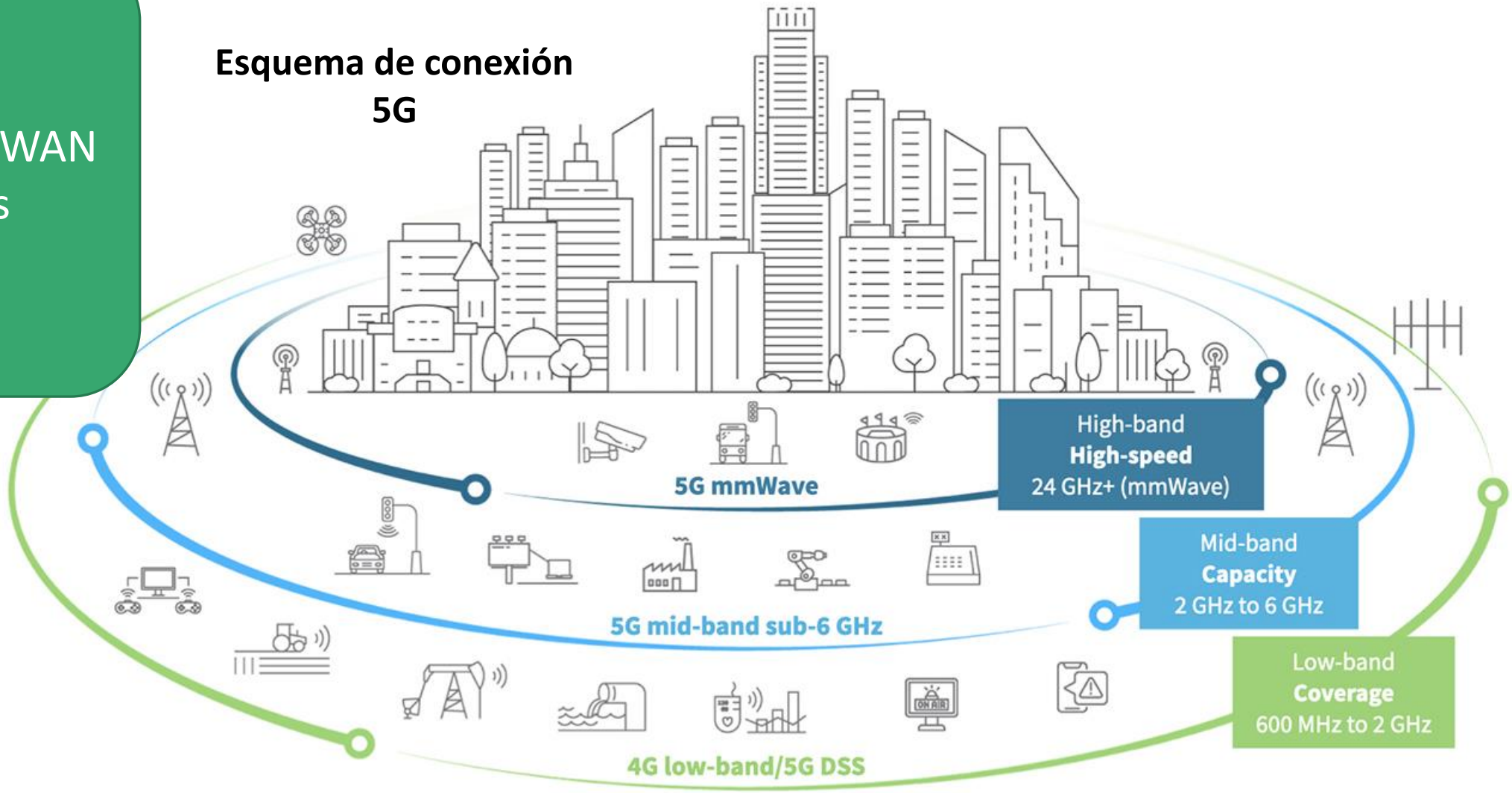
Conexiones WAN públicas

Esquema de conexión WiMAX



Conexiones WAN públicas

Esquema de conexión 5G



REDES CABLEADAS

Este tipo de redes conllevan las comunicaciones cableadas. Los medios de transmisión son guiados mediante el uso de cables de cobre o de fibra óptica.

Cable de cobre par trenzado:

Está recubierto por una cubierta de PVC. Dispone en su interior de 8 cables de cobre aislados y entrelazados identificados por un color individual en su cubierta. Los cables se trenzan siguiente el siguiente esquema:

- Azul – Blanco/Azul
- Naranja – Blanco/Naranja
- Verde – Blanco/Verde
- Marrón – Blanco/Marrón.

Para proteger los cables contra interferencias electromagnéticas externas y aportarle consistencia y rigidez se suelen hacer uso de blindajes en los pares o en el cable.

Tipos de blindajes en los cables de cobre par trenzado

U/FTP	Pantalla de aluminio en los pares	
F/FTP	Pantalla de aluminio en los pares y en el cable	
S/FTP	Pantalla de aluminio en los pares y malla de aluminio en el cable	
F/UTP	Pantalla de aluminio en el cable	
SF/UTP	Pantalla y malla de aluminio en el cable	

Tipos de blindajes en los cables de cobre par trenzado

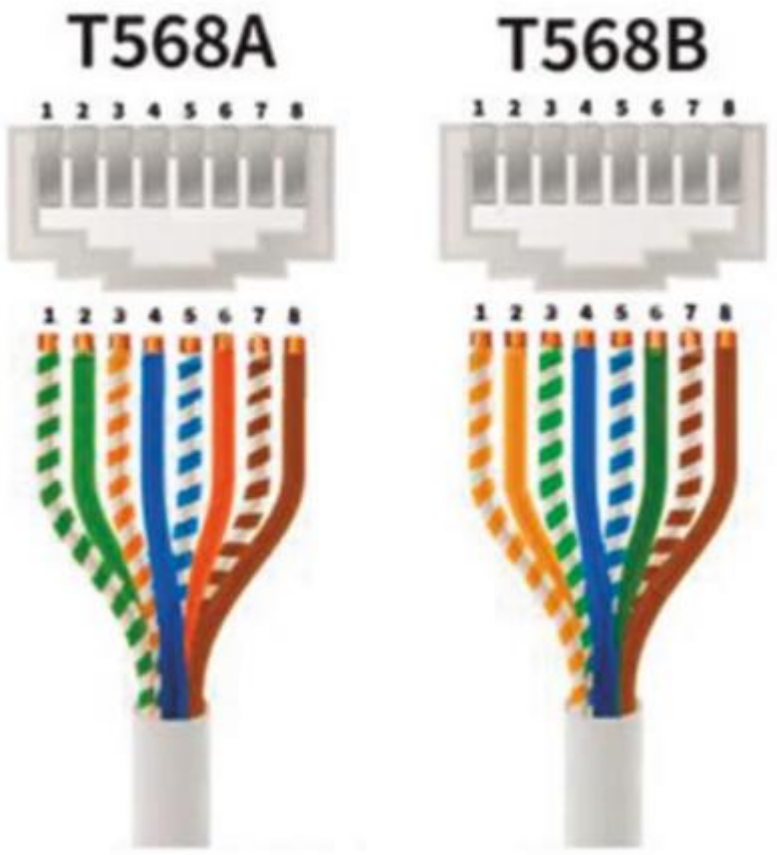
U/FTP	Pantalla de aluminio en los pares	
F/FTP	Pantalla de aluminio en los pares y en el cable	
S/FTP	Pantalla de aluminio en los pares y malla de aluminio en el cable	
F/UTP	Pantalla de aluminio en el cable	
SF/UTP	Pantalla y malla de aluminio en el cable	

Conectores empleados, tipo RJ 45

RJ45 para cables UTP

RJ45 apantallado para cables con blindaje

La terminación de los cables debe de llevar un orden regulado por la norma TIA/EIA-568-B, estableciendo dos tipos de configuraciones, la T-568ª (*directo*) y la T-568B (*cruzado*):



Dicho estándar también establece las categorías de cable par trenzado según sus características detallando aspectos como frecuencia de funcionamiento y velocidad máxima.

Este tipo de cables presentan un gran ancho de banda siendo muy económicos y de fácil instalación.

Cable de fibra óptica:

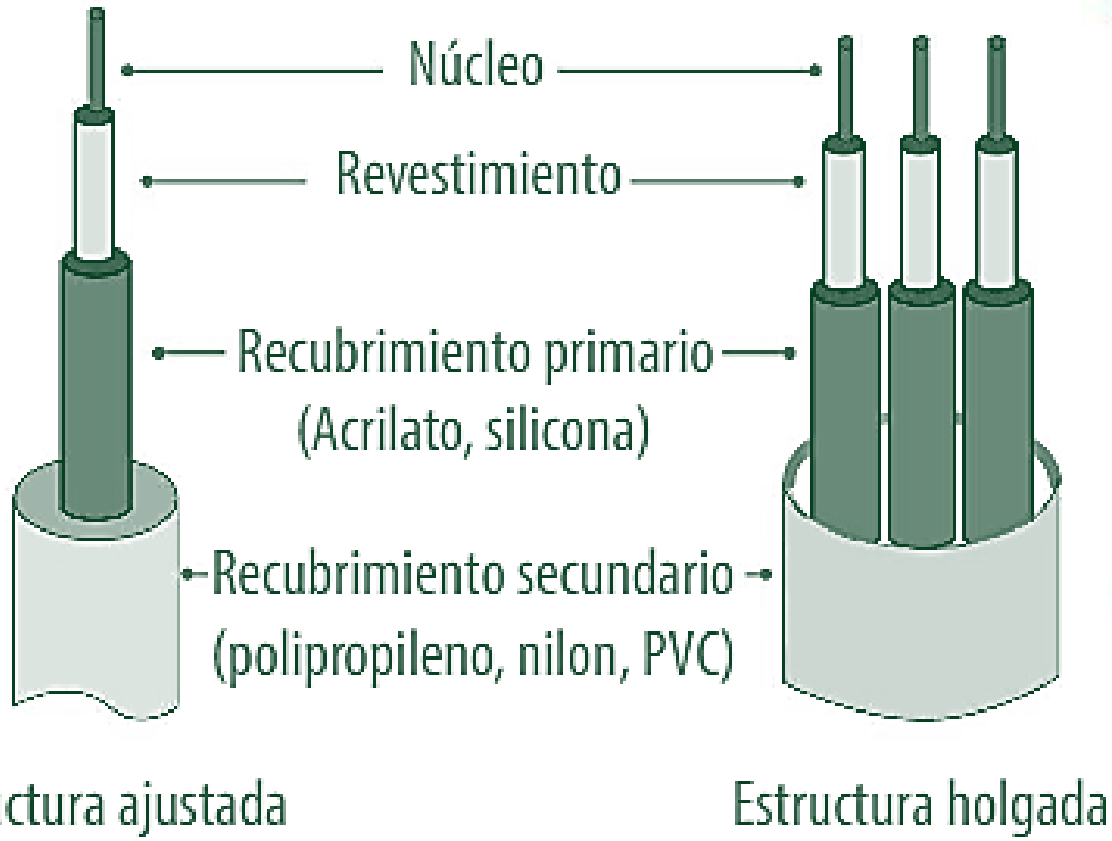
Estos cables están formados por uno o más hilos de fibra de vidrio o plástico cubierto por varias capas diferentes que le aportan protección y rigidez.

Según su estructura interna existen:

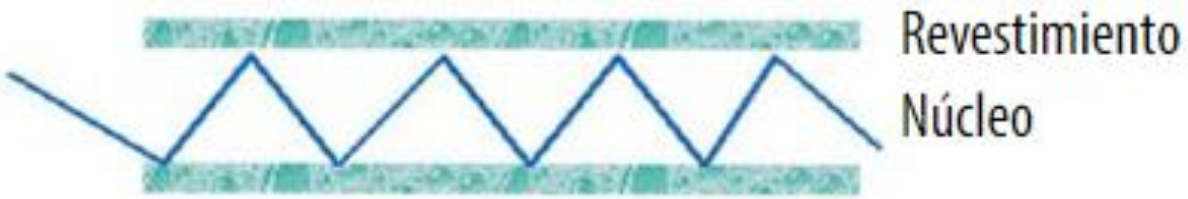
- Estructura holgada: los hilos de fibra se encuentran con cierta libertad en tubos dentro del cable de fibra óptica. Se usan en redes LAN o MAN
- Estructura ajustada: los hilos de fibra no presentan libertad de movimiento debido a un recubrimiento secundario. Se emplea para redes MAN o WAN.

Según el modo de transmisión:

- Monomodo (SM): se emite un único haz de luz por el interior del hilo. Es empleado principalmente para largas distancias.
- Multimodo (MM): transmite varios haces de luz con diferentes trayectorias. Se utiliza para distancias cortas, por ejemplo en manzanas de edificios o en el interior del edificio.



Monomodo



Multimodo

Conector LC

Conector SC

Conector MT-RJ

Conector MPO

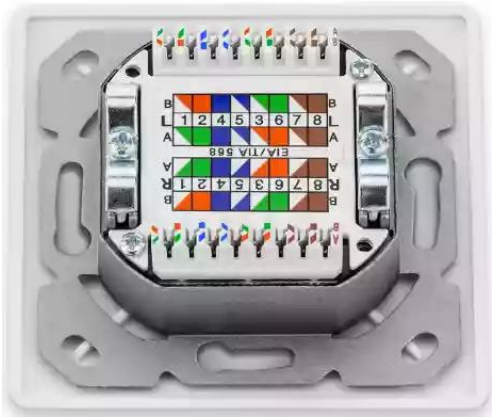
El estándar mencionado anteriormente también define el diseño e implementación del cableado en un edificio o entre varios, estableciendo una topología de red en estrella con nodos y hosts conectados a un nodo centra que conmuta y controla el flujo de datos entre todos ellos.

Los elementos electrónicos de red empleados para conectar cables de par trenzado como nodo central son principalmente los **switches** y los **routers,** que normalmente se instalan en el interior de armarios racks.

Los armarios racks o armarios de distribución suelen alojar multitud de dispositivos y elementos dependiendo la envergadura de la infraestructura de red.

Suelen contener los dispositivos electrónicos anteriormente mencionados, paneles de parcheo, regletas eléctricas, bandejas, organizadores de cables, etc…

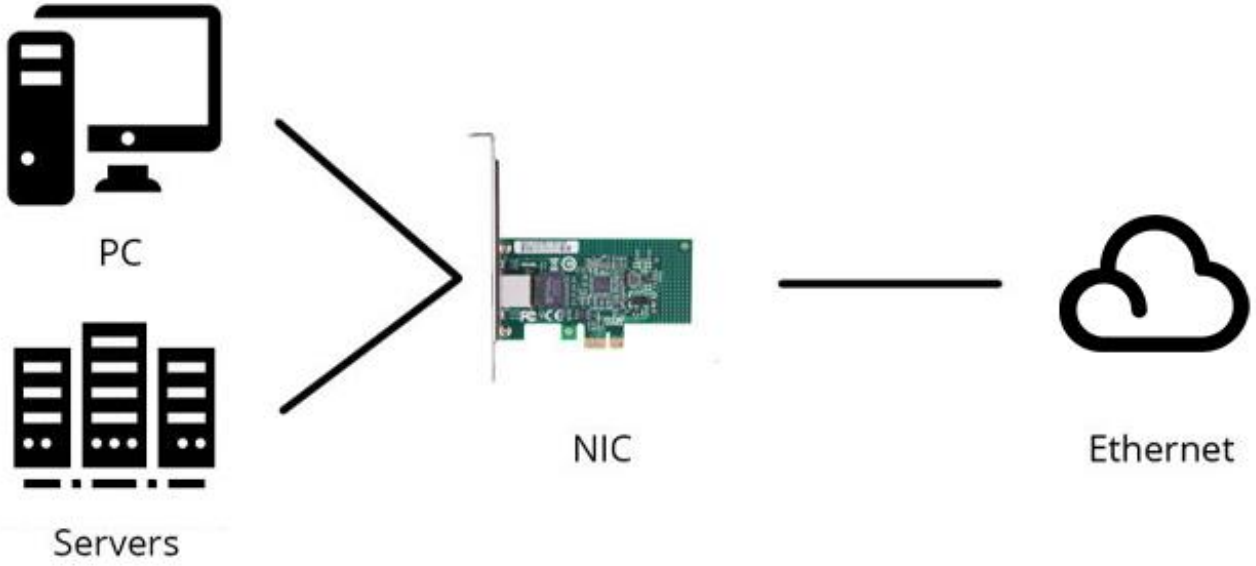
También existen dispositivos de interconexión y adaptadores de red en fibra óptica y en par trenzado.



Roseta empotrable en pared RJ - 45

Panel de parcheo o *patch panel* en armario rack

Las tarjetas de red o adaptadores de red de los equipos informáticos también se denominan **NIC** o ***Network Interfaz Controller*** y son necesarios para que los hosts puedan conectarse a la red.

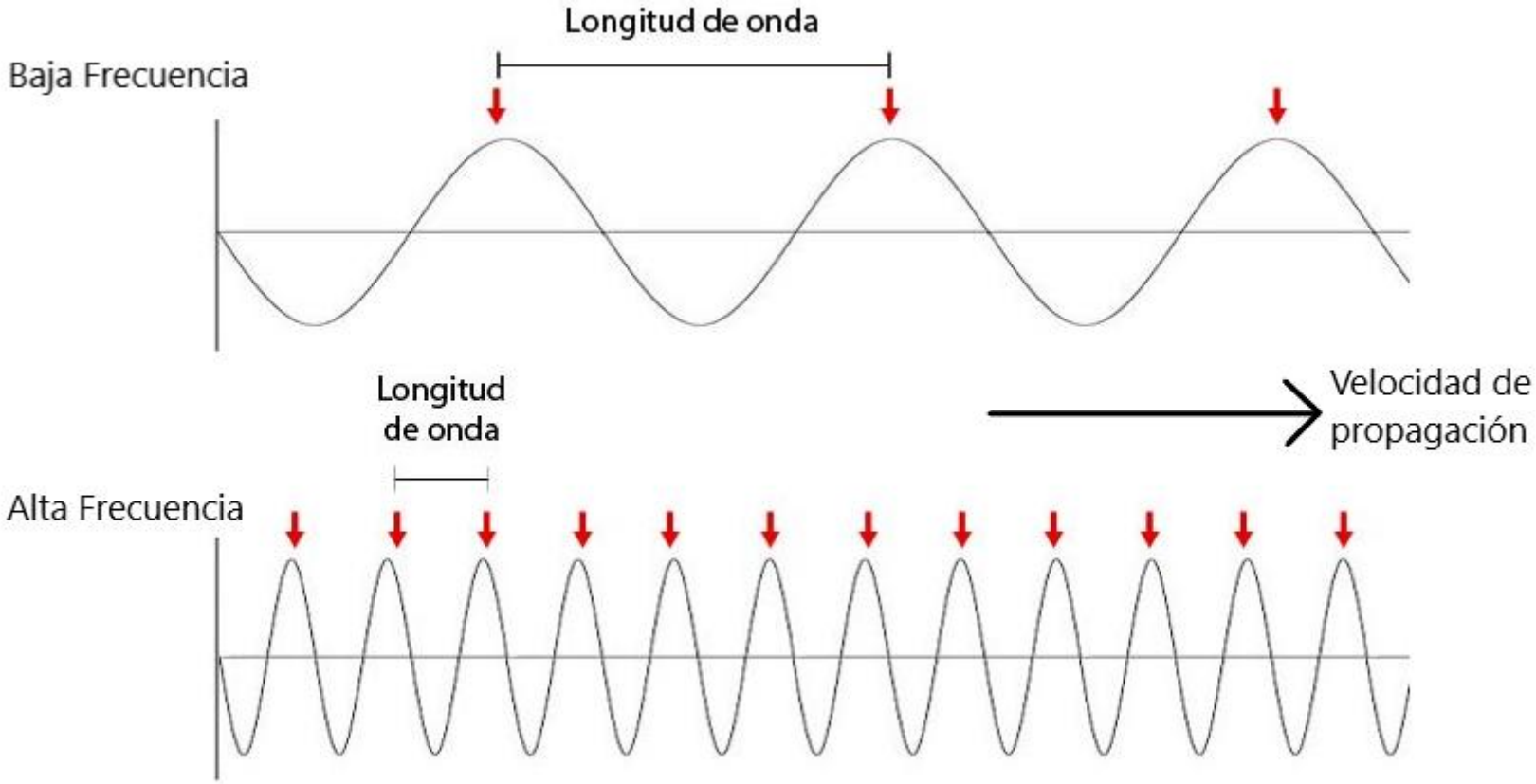


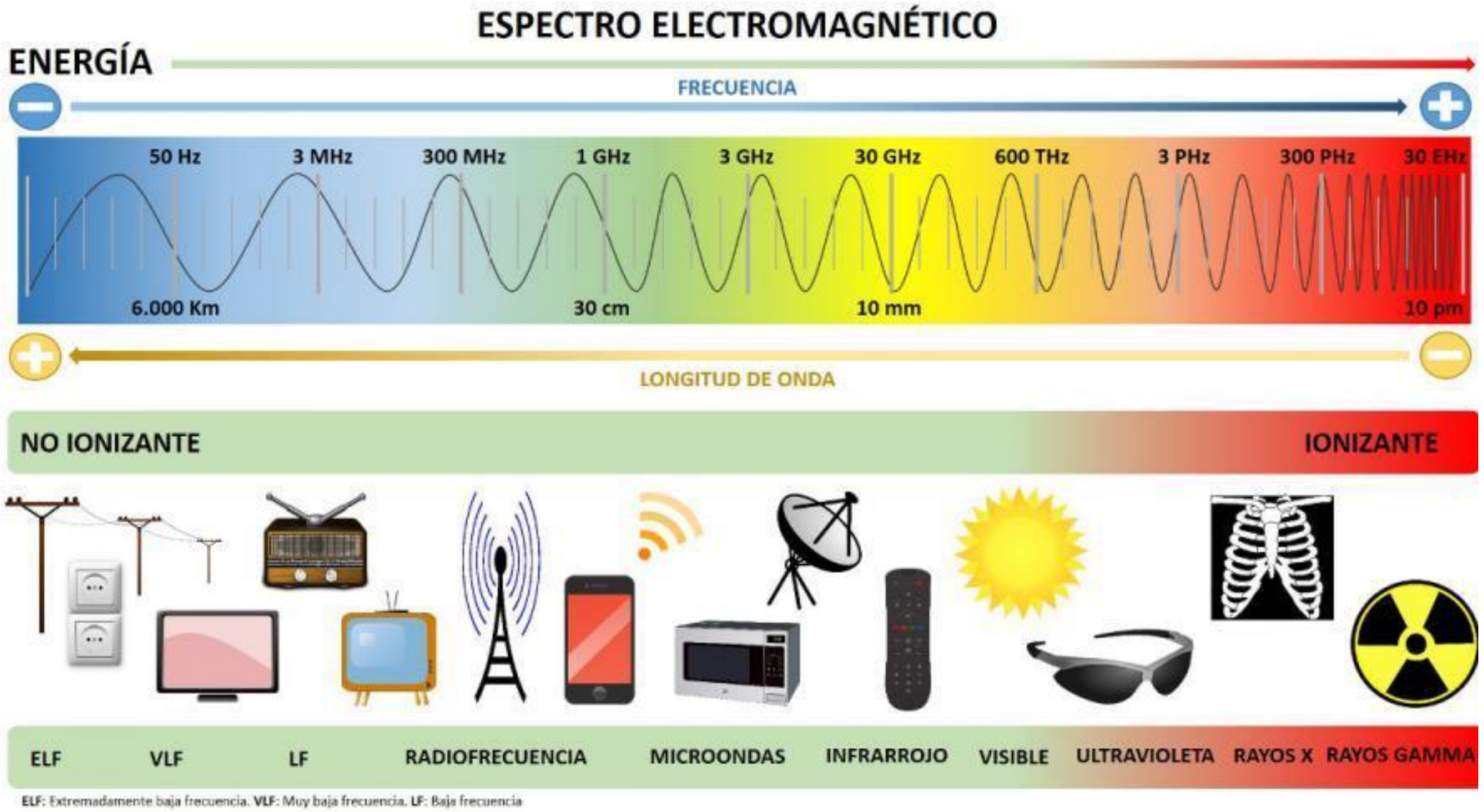
Tarjeta de red con conector RJ45

REDES INALÁMBRICAS

Algunas de las ventajas que aportan las redes inalámbricas respecto a las cableadas es la movilidad, la flexibilidad y la facilidad de instalación.

Como se indicó anteriormente hacen uso de ondas electromagnéticas para transmitir datos y su transmisión depende de la longitud de onda y de la frecuencia.





ELF: Extremadamente baja frecuencia. **VLF**: Muy baja frecuencia. **LF**: Baja frecuencia

Redes Wi-Fi

Transmiten datos a gran velocidad en un área de red local (LAN).

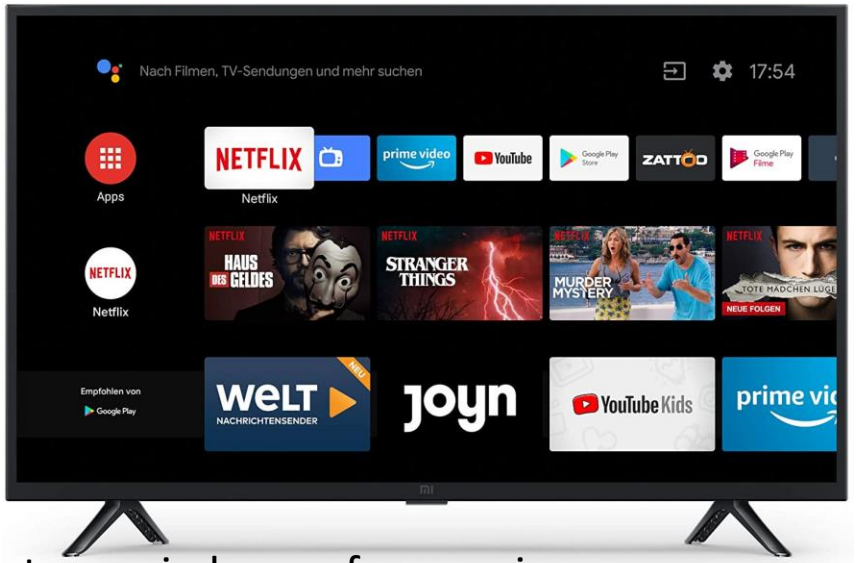
Esta tecnología se basa en el conjunto de estándares IEEE 802.11.

Trabajan en bandas de frecuencia entre los 2,4 GHz y los 5 GHz.

Cada estándar posee un rango de acción y un ancho de banda diferente asociado a su frecuencia.

A mayor frecuencia mayor ancho de banda pero menor alcance.

Requieren de puntos de acceso Wi-Fi para conectar los diferentes terminales NIC



Smart TV

Smartphone

Tarjeta Wi-Fi portátil

Tarjeta Wi-Fi PC sobremesa

Redes WiMAX

Establecen redes de comunicación de alta velocidad con alcance de decenas de kilómetros.

Se basa en el estándar IEEE 802.16.

Redes 4G y 5G

Son tecnologías de comunicación móvil para rede WMAN y WWAM.

Se basan en el estándar LTE-Advanced para la 4 generación o 4G.

Se basan en el estándar G NR para la 5 generación o 5G.

Este último es objeto de desarrollo ideal para aplicaciones a tiempo real e IoT (Internet de las Cosas).

Redes WPAN

Se suelen utilizar para áreas de red personal inalámbricas con comunicaciones directas entre dispositivos sin usar dispositivos intermedios.

Los más conocidos son:

Zigbee: definido por el estándar IEEE 802.15.4. Se usa para el control y monitorización a muy bajo coste en aplicaciones que requieran baja tasa de transferencia de datos.

Bluetooth: definido por el estándar IEEE 802.15.1. Se usa para la transmisión de datos y voz entre dispositivos muy cercanos, sincronización y eliminando la conexión por medio de cables. Se usa por ejemplo para conectar un smartphone al sistema operativo de un vehículo modero.

NFC: se trata de un estándar en si usado para comunicaciones entre dispositivos a muy pocos centímetros de distancia. Por ejemplo, el pago den cajero de supermercado mediante el uso de un smartphone con al tecnología NFC implantada y habilitada.

Dispositivos de interconexión

Los dispositivos de interconexión de una red inalámbrica depende del tipo de red y del estándar que defina dicha red.

En redes WiMAX, 54G o 5G, las estaciones base están provistas con equipos de telecomunicaciones y antenas para aportar la cobertura necesaria a los dispositivos creando la red inalámbrica.

Se pueden diferencia distintas topologías de red:

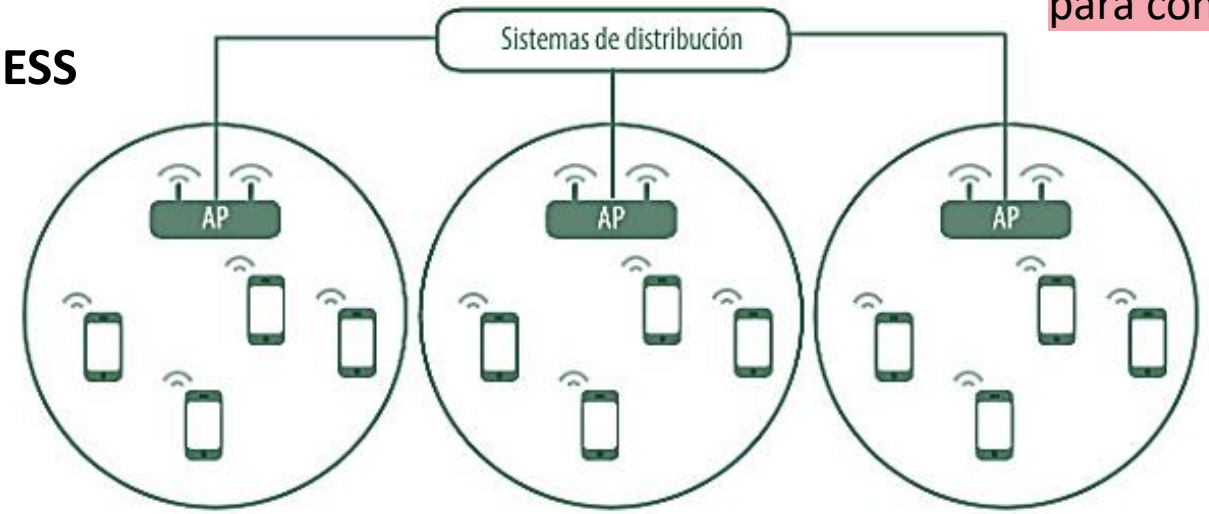
- Modo ad hoc (IBSS): dos clientes se conectan directamente sin emplear ningún dispositivo de infraestructura.

- Modo infraestructura: los clientes se conectan mediante un dispositivo de infraestructura, normalmente un punto de acceso inalámbrico. Los puntos de acceso Wi-Fi se conecta al sistema de distribución destacando:

  - ❑ Conjunto de servicios básicos (BSS).
  - ❑ Conjunto de servicios extendidos (ESS).

Dispositivos de interconexión

ESS



Configuración del APN

Nombre del punto de acceso (depende de la operadora para configurar el módem de Internet)

Parámetros de red Wi-Fi:

SSID: Nombre de red

Método (WPA2) y (WPA3) y contraseña de autenticación

FICHEROS DE CONFIGURACIÓN DE RED

En Ubuntu se emplea la herramienta NetPlan para gestionar y administrar la configuración de red.

Las interfaces del sistema podemos identificarlas mediante el comando **ip a** y el comando **lshw –class network**

El directorio */etc/netplan* contiene los archivos de configuración de NetPlan: *01-network-manager-all.yaml*.

Para realizar la configuración debe escribirse el fichero respetando la sintaxis en todo momento incluyendo los caracteres de espaciado (*no usar el tabulador*).

Para establecer los cambios usamos el comando **netplan apply** y comprobamos los cambios mediante el comando **ip address show**

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
      enp0s3:
            dhcp4: no
            addresses: [192.168.1.8/24]
            gateway4: 192.168.1.1
            nameservers:
                  addresses: [8.8.8.8, 8.8.8.4]
```

IP estática

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
      enp0s3:
            dhcp4: yes
```

IP dinámica

```
usuario@usuario-VirtualBox:~$ cd /etc/netplan
usuario@usuario-VirtualBox:/etc/netplan$ ls
01-network-manager-all.yaml
usuario@usuario-VirtualBox:/e
```

```
 GNU nano 4.8                 01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager

                          [ 4 líneas leídas ]
^G Ver ayuda ^O Guardar   ^W Buscar     ^K Cortar Tex^J Justificar^C Posición
^X Salir     ^R Leer fich.^\ Reemplazar^U Pegar      ^T Ortografía^  Ir a línea
```

```
usuario@usuario-VirtualBox:/etc/netplan$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:e0:9f:ad brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86246sec preferred_lft 86246sec
    inet6 fe80::171c:9564:5e0b:a02f/64 scope link noprefixroute
       valid_lft f
```

```
  GNU nano 4.8                01-network-manager-all.yaml                Modificado
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
      enp0s3:
            dhcp4: yes
```

```
usuario@usuario-VirtualBox:/etc/netplan$ sudo netplan apply
usuario@usuario-VirtualBox:/etc/netplan$ ip address show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:e0:9f:ad brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86384sec preferred_lft 86384sec
    inet6 fe80::a00:27ff:fee0:9fad/64 scope link
       valid lft forever preferred lft forever
```

MONITORIZACIÓN Y VERIFICACIÓN DE UNA RED MEDIANTE COMANDOS

```
usuario@usuario-VirtualBox:~$ sudo lshw
usuario-virtualbox
    descripción: Project-Id-Version: lshwReport-Msgid-Bugs-To: FULL NAME <EMAIL@
ADDRESS>PO-Revision-Date: 2012-03-14 06:38+0000Last-Translator: Paco Molinero <p
aco@byasl.com>Language-Team: Spanish <es@li.org>MIME-Version: 1.0Content-Type: t
ext/plain; charset=UTF-8Content-Transfer-Encoding: 8bitX-Launchpad-Export-Date:
2022-02-11 15:39+0000X-Generator: Launchpad (build fb383037dc57f48cc5195c1eb2676
319fbdf7e33)
    producto: VirtualBox
    fabricante: innotek GmbH
    versión: 1.2
    serie: 0
    anchura: 64 bits
    capacidades: smbios-2.5 dmi-2.5 vsyscall32
    configuración: family=Virtual Machine uuid=AA348146-BF7E-E14F-BFEF-88D0D94B8
E52
  *-core
       descripción: Placa base
       producto: VirtualBox
       fabricante: Oracle Corporation
       id físico: 0
       versión: 1.2
       serie: 0
     *-firmware
```

Este comando permite identificar multitud de detalles de las interfaces de red.

En Ubuntu 20.04.4 LTS

```
usuario@usuario-VirtualBox:~$ arp
Dirección                TipoHW  DirecciónHW         Indic Máscara         Interfaz
10.0.2.2                 ether   52:54:00:12:35:02   C                     enp0s3
```

En Microsoft Windows 10

```
C:\Users\Usuario>arp -a

Interfaz: 192.168.56.1 --- 0x9
  Dirección de Internet          Dirección física      Tipo
  192.168.56.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.251            01-00-5e-00-00-fb     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático
  255.255.255.255        ff-ff-ff-ff-ff-ff     estático

Interfaz: 192.168.0.11 --- 0xa
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1            78-b2-13-3c-cf-e0     dinámico
  192.168.0.10           60-1d-9d-ad-46-c7     dinámico
  192.168.0.255          ff-ff-ff-ff-ff-ff     estático
  224.0.0.2              01-00-5e-00-00-02     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.251            01-00-5e-00-00-fb     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático
  255.255.255.255        ff-ff-ff-ff-ff-ff     estático
```

Este comando mostrar las asociaciones entre las direcciones físicas o MAC y las direcciones IP del segmento de red local en un equipo.

Estas asociaciones se almacenan en una tabla ARP o ARP caché (*en Microsoft Windows también existe dicha tabla*).

Este comando es el más extendido para monitorizar las interfaces de red.

En Ubuntu 20.04.4 LTS

```
usuario@usuario-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fee0:9fad  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e0:9f:ad  txqueuelen 1000  (Ethernet)
        RX packets 122720  bytes 183492638 (183.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15508  bytes 982906 (982.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Bucle local)
        RX packets 263  bytes 22943 (22.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 263  bytes 22943 (22.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

En Microsoft Windows 10

```
C:\Users\Usuario>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet 2:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet VirtualBox Host-Only Network:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::a194:11f1:d342:eb6c%9
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.56.1
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :

Adaptador de LAN inalámbrica Conexión de área local* 9:

   Estado de los medios. . . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 10:
```

Se usa para comprobar la conexión de red. Permite enviar paquetes de prueba a un destino especificado y nos informa del tiempo de respuesta.

En Ubuntu 20.04.4 LTS

```
usuario@usuario-VirtualBox:~$ ping www.google.es
PING www.google.es (142.250.200.99) 56(84) bytes of data.
64 bytes from mad41s13-in-f3.1e100.net (142.250.200.99): icmp_seq=1 ttl=116 time=12.4 ms
64 bytes from mad41s13-in-f3.1e100.net (142.250.200.99): icmp_seq=2 ttl=116 time=12.3 ms
64 bytes from mad41s13-in-f3.1e100.net (142.250.200.99): icmp_seq=3 ttl=116 time=12.3 ms
64 bytes from mad41s13-in-f3.1e100.net (142.250.200.99): icmp_seq=4 ttl=116 time=12.5 ms
64 bytes from mad41s13-in-f3.1e100.net (142.250.200.99): icmp_seq=5 ttl=116 time=12.4 ms
^C
--- www.google.es ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 12.342/12.397/12.472/0.048 ms
```

En Microsoft Windows 10

```
C:\Users\Usuario>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=11ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=11ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=12ms TTL=117
Respuesta desde 8.8.8.8: bytes=32 tiempo=11ms TTL=117

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 11ms, Máximo = 12ms, Media = 11ms
```

GESTIÓN DE PUERTOS

El término puerto en sistema informáticos en red hace mención a:

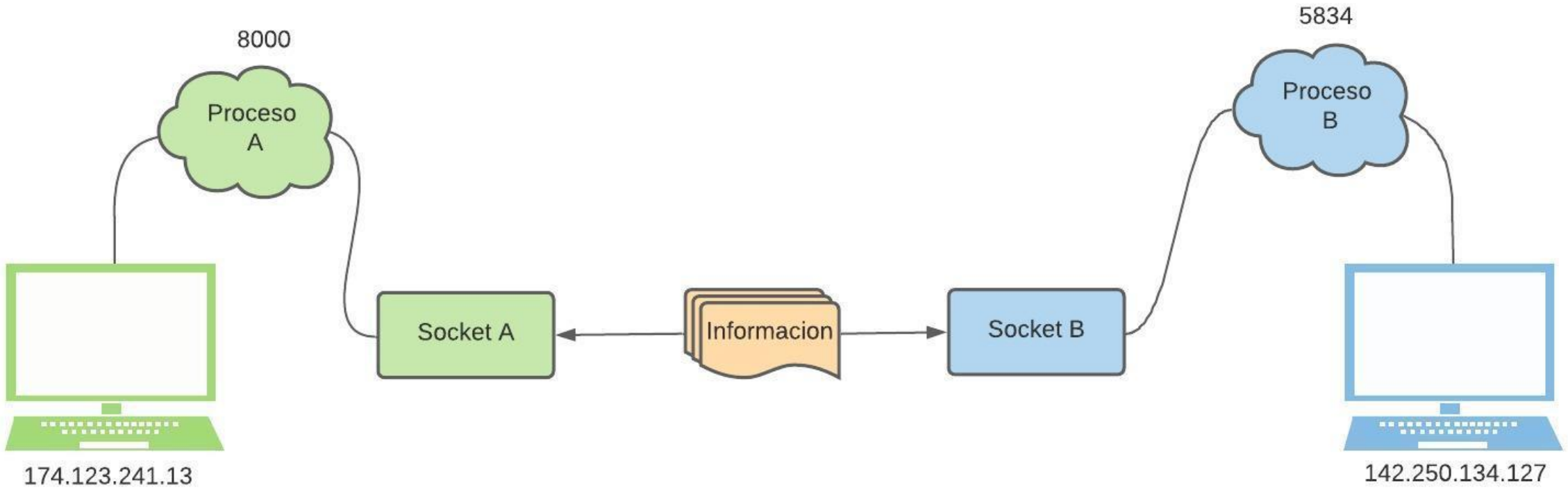
- ***Un puerto físico: por ejemplo un RJ – 45.***
- ***Un puerto lógico: un número que se asocia a la aplicación de origen o destino de una comunicación. Se usan en la capa de transporte.***

Los puertos lógicos pueden ser origen o destino.

Existen tres tipos de puertos lógicos asociados a su número:

1. Puertos conocidos: van del 0 al 1023 y son reservados para servicios y aplicaciones como HTTTP (80), FTP (20), HTTPS (443), SMTP (25), IMAP (143), etc.
2. Puertos registrados: van del 1024 al 49151 y son usados por aplicaciones de usuario cuando se conecta a servidores.
3. Puertos dinámicos, privados o efímeros: van del 49152 al 65535 y son usados por aplicaciones de intercambio de archivos punto a punto.

La combinación de una dirección IP y un puerto se denomina *socket*. La comunicación entre dos hosts se establece mediante una pareja de sockets.


8000
Proceso
A
5834
Proceso
B
Socket A
Informacion
Socket B
174.123.241.13
142.250.134.127

Para visualizar los puertos en Microsoft Windows se hace uso del comando **netstat**

```
C:\Users\Usuario>netstat -a

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:445            Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:1462           Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:5040           Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:7680           Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:49664          Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:49665          Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:49666          Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:49667          Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:49668          Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:49670          Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:60700          Dani-PC-Sobremesa:0    LISTENING
  TCP    0.0.0.0:60701          Dani-PC-Sobremesa:0    LISTENING
  TCP    127.0.0.1:14622        Dani-PC-Sobremesa:0    LISTENING
  TCP    127.0.0.1:14622        Dani-PC-Sobremesa:58033  ESTABLISHED
  TCP    127.0.0.1:26822        Dani-PC-Sobremesa:0    LISTENING
  TCP    127.0.0.1:32682        Dani-PC-Sobremesa:0    LISTENING
  TCP    127.0.0.1:57913        Dani-PC-Sobremesa:65001  ESTABLISHED
  TCP    127.0.0.1:57950        Dani-PC-Sobremesa:0    LISTENING
  TCP    127.0.0.1:57950        Dani-PC-Sobremesa:57969  ESTABLISHED
  TCP    127.0.0.1:57969        Dani-PC-Sobremesa:57950  ESTABLISHED
```

Para visualizar los puertos en Ubuntu se hace uso del comando

ss

```
usuario@usuario-VirtualBox:~$ ss
Netid State Recv-Q Send-Q                                  Local Address:Port   Peer Address:Port  Process
u_str ESTAB 0      0                                                   * 37818             * 37819
u_str ESTAB 0      0                                                   * 48826             * 48827
u_str ESTAB 0      0                                                   * 37740             * 37743
u_str ESTAB 0      0                        /run/systemd/journal/stdout 36110             * 36105
u_str ESTAB 0      0                                                   * 28261             * 28262
u_str ESTAB 0      0                                                   * 37247             * 37249
u_str ESTAB 0      0                        /run/systemd/journal/stdout 36442             * 36437
u_str ESTAB 0      0                                                   * 35983             * 35988
u_str ESTAB 0      0                                  /run/user/1000/bus 35516             * 35515
u_str ESTAB 0      0                                  /run/user/1000/bus 33684             * 33683
u_str ESTAB 0      0                        /run/dbus/system_bus_socket 25694             * 25693
u_str ESTAB 0      0                                                   * 52094             * 52095
u_str ESTAB 0      0                                  @/tmp/.X11-unix/X0 37426             * 37425
u_str ESTAB 0      0                                                   * 37374             * 37375
u_str ESTAB 0      0            @/home/usuario/.cache/ibus/dbus-T2WUrdIk 36023             * 36022
u_str ESTAB 0      0                                                   * 37516             * 37517
u_str ESTAB 0      0                                                   * 36527             * 36528
u_str ESTAB 0      0                                                   * 25196             * 25197
u_str ESTAB 0      0                                  /run/user/1000/bus 34094             * 34093
u_str ESTAB 0      0                                                   * 51440             * 51442
```