CAPÍTULO 18. IP Networks

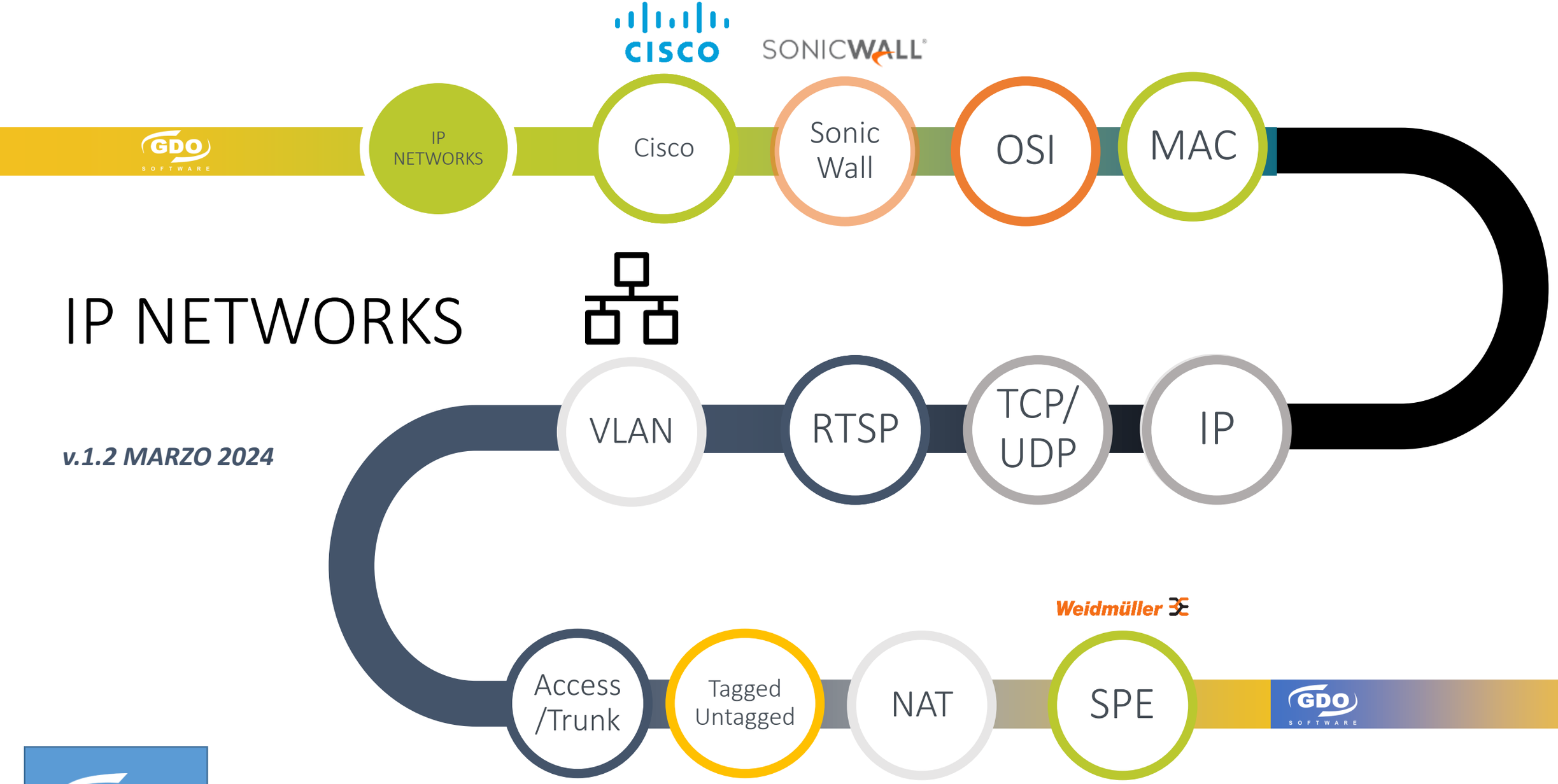
v.1.2 MARZO 2024

Ricardo Moraleda Gareta

[Director departamento de software de GDO Software]

IP NETWORKS

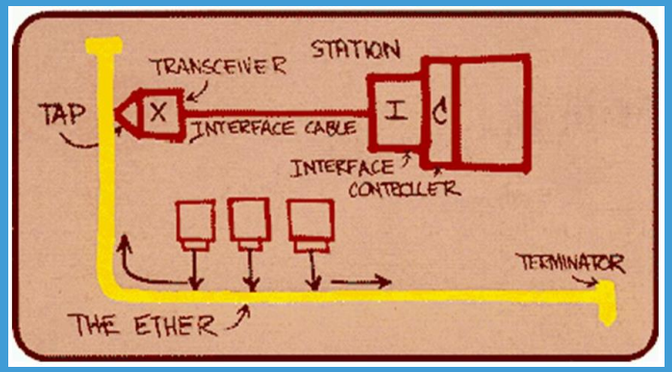
v.1.2 MARZO 2024



IP NETWORKS

Historia de Ethernet

Allá por 1976, Robert "Bob" Metcalfe y David Boggs inventaron / describieron Ethernet.



- La red Ethernet fue llamada así debido a que hacía referencia a la teoría de la física hoy ya abandonada según la cual las ondas electromagnéticas viajaban por un fluido denominado éter que se suponía llenaba todo el espacio (para Metcalfe el 'éter' era el cable coaxial por el que iba la señal)
- **Ethernet es un estándar de redes de área local para ordenadores**.

Historia de Ethernet

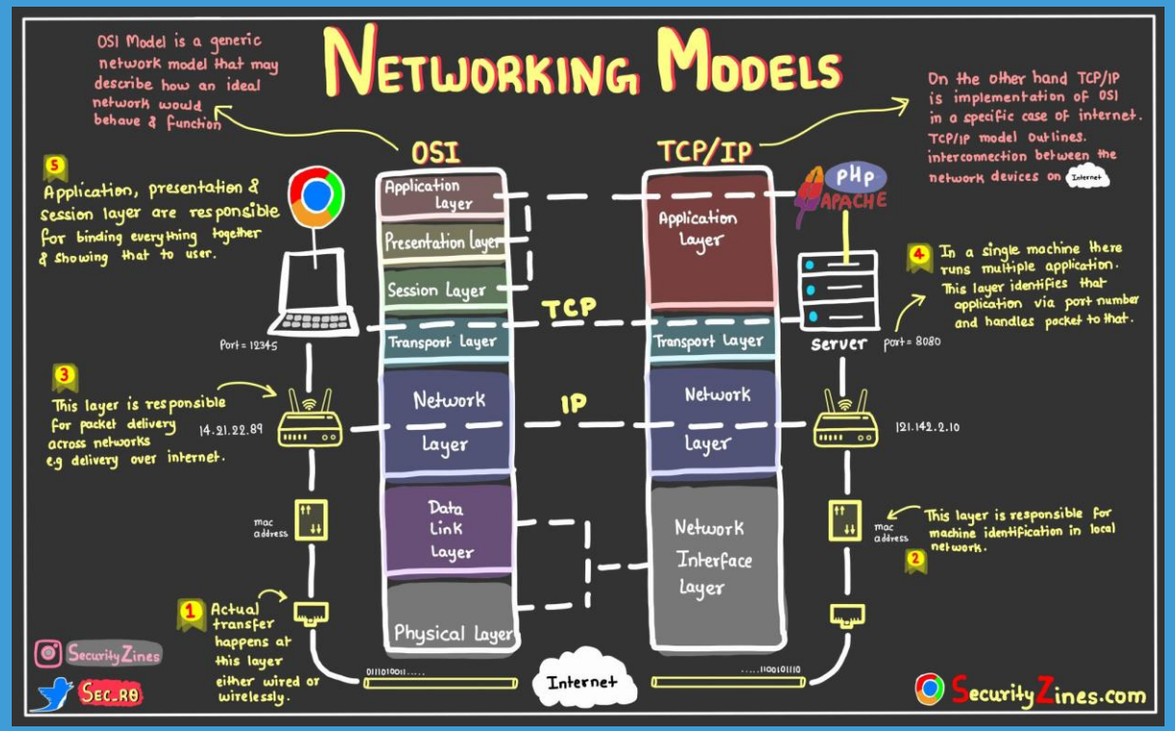
En 1975 Metcalfe y Boggs describieron Ethernet en un artículo que enviaron a Communications of the ACM (Association for Computing Machinery), publicado en 1976. En él ya describían el uso de repetidores para aumentar el alcance de la red. En 1977 Metcalfe, Boggs y otros dos ingenieros de Xerox recibieron una patente por la tecnología básica de Ethernet, y en 1978 Metcalfe y Boggs recibieron otra por el repetidor. En esta época todo el sistema Ethernet era propiedad de Xerox.

La primera versión del **IEEE 802.3** fue un intento de estandarizar Ethernet. Posteriormente ha habido ampliaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y el de 10 Gigabit), redes virtuales, hubs, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial).

Modelo OSI _TCP/IP

OSI (Open Systems Interconnection)

OSI es un marco conceptual para entender cómo los ordenadores se comunican entre sí.



OSI _ TCP/IP

El modelo OSI consta de 7 capas:

- Capa Física (Capa 1) → hardware de red
- Capa Enlace (Capa 2) → @MAC, tramas (Ethernet)
- Capa Red (Capa 3) → @ IP (Internet Protocol)
- Capa Transporte (Capa 4) → puertos. Ej 80, 443 HTTP, HTTPS
- Capa Sesión (Capa 5)
- Capa Presentación (Capa 6)
- Capa Aplicación (Capa 7) → Seguridad TLS, Aplicaciones. Ej. web browser.

El modelo TCP/IP (Transmission Control Protocol/Internet Protocol) es otro modelo usado para networking como implementación de OSI.

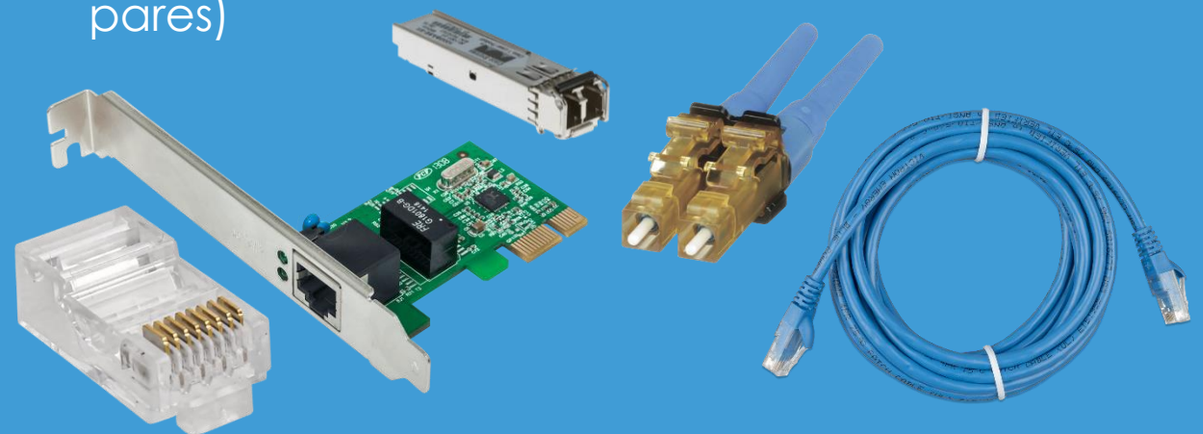
- Interfaz de red (Capa 1). Combina la capa física y de enlace de OSI
- Internet (Capa 2). Es la capa de red de OSI
- Transporte (Capa 3). Combina la capa de transporte y sesión de OSI
- Aplicación (Capa 4). Combina la capa de presentación y aplicación de OSI.

Capa 1/2 Física-Enlace

Capa 1/2 Física/Enlace

En la capa física/enlace interviene:

- Cables de red (par trenzado). Conector RJ45 (cobre) o SFP LC (fibra óptica) o sin cables (Wireless – WiFi, Lora, Bluetooth..).
- Tarjeta de red (NIC) con dirección MAC (Medium Access Control)
- RJ45 (categorías 5, 5e, 6, 6a y 8.1). 8 pines (4 pares)



MAC

La dirección MAC o **dirección física** es un identificador único que cada fabricante le asigna a la tarjeta de red de sus dispositivos conectados, desde un ordenador o móvil hasta routers, impresoras u otros dispositivos.

Las direcciones MAC están formadas por 48 bits representados generalmente por dígitos hexadecimales. Como cada hexadecimal equivale a cuatro binarios (48:4=12), la dirección acaba siendo formada por 12 dígitos agrupados en seis parejas separadas generalmente por dos puntos, aunque también puede haber un guión o nada en absoluto. De esta manera, un ejemplo de dirección MAC podría ser:

C8-D9-D2-82-1A-C7

Los 6 primeros denotan al fabricante → HP. Por aquí se puede saber el fabricante:https://maclookup.app/macaddress/C8D9D2

Como son identificadores únicos, las MAC pueden ser utilizadas por un administrador de red para permitir o denegar el acceso de determinados dispositivos a una red.

Capa 1/2 Física-Enlace

Capa 1/2 Física/Enlace

La capa 2 (Enlace) es responsable de la transferencia fiable de información a través de un circuito de transmisión de datos. Recibe peticiones de la capa de red (3) y utiliza los servicios de la capa física (1).

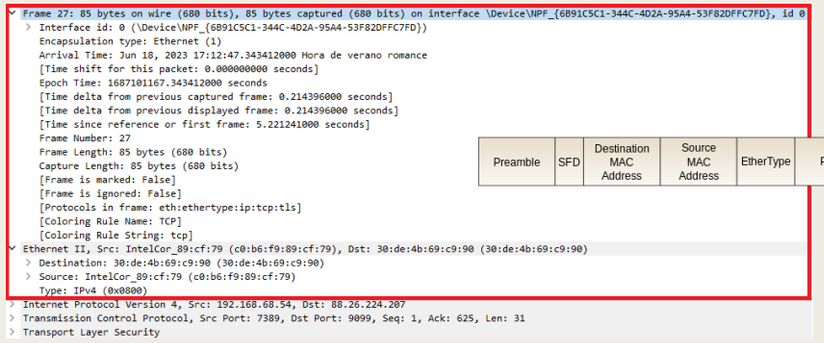
El objetivo de la capa de enlace es conseguir que la información fluya, libre de errores, entre dos máquinas que estén conectadas directamente (servicio orientado a la conexión). Para lograr este objetivo tiene que montar bloques de información (llamados **tramas** en esta capa), dotarles de una dirección de capa de enlace (Dirección MAC), gestionar la detección o corrección de errores, y ocuparse del "control de flujo" entre equipos (para evitar que un equipo más rápido desborde a uno más lento).

Cuando el medio de comunicación está compartido entre más de dos equipos es necesario arbitrar el uso del mismo. Esta tarea se realiza en la subcapa de control de acceso al medio → algoritmo **CSMA / CD** (Carrier Sense Multiple Access with Collision Detection)

Trama Ethernet

Estructura interna de la trama Ethernet IEEE 802.3. Carga útil de datos hasta 1.500 bytes + cabeceras.

Capa	Preámbulo	Delimitador del inicio de la trama	MAC Destino	MAC Fuente	802.1Q etiqueta (opcional)	Ethertype (Ethernet II) o longitud (IEEE 802.3)	Carga útil	Secuencia de control de trama (CRC de 32 bits)	Interpacket Vacío
	7 bytes	1 byte	6 bytes	6 bytes	(4 bytes)	2 bytes	46-1500 bytes	4 bytes	12 bytes
Capa 2 marco de Ethernet			← 64–1522 bytes →						
Capa 1 paquete de Ethernet & IPG	← 72–1530 bytes →								← 12 bytes →



Capa 3 Red

Capa 3 Red o IP

La capa 3 (Red) proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace.

Para la consecución de su tarea, puede asignar direcciones de red únicas, interconectar subredes distintas, encaminar **paquetes**, utilizar un control de congestión y control de errores.

Lo más importante de esta capa es la dirección IP. Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa "protocolo de Internet", que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.

Direcciones IPv4

Las direcciones IPv4 se expresan como un conjunto de cuatro números, por ejemplo, 192.158.1.38. Cada número del conjunto puede variar de 0 a 255. Por lo tanto, el rango completo de direcciones IP va desde 0.0.0.0 hasta 255.255.255.255. Permiten un espacio de direcciones de hasta 4.294.967.296 (2^{32}) direcciones posibles.

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los *hosts*,[8] de modo que la cantidad máxima de *hosts* es 2^{24} - 2 (se excluyen la dirección reservada para *broadcast* (últimos octetos a 1) y de red (últimos octetos a 0)), es decir, 16 777 214 *hosts*.
- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los *hosts*,[8] de modo que la cantidad máxima de *hosts* por cada red es 2^{16} - 2, o 65 534 *hosts*.
- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los *hosts*,[8] de modo que la cantidad máxima de hosts por cada red es 2^{8} - 2, o 254 *hosts*.

Clase	Bits iniciales	Intervalo (*)	N.º de redes	N.º de direcciones por red	N.º de hosts por red(‡)	Máscara de red	Dirección de *broadcast*
A	0	0.0.0.0 (**) - 127.255.255.255 (†)	128	16 777 216	16 777 214	255.0.0.0	x.255.255.255
B	10	128.0.0.0 - 191.255.255.255	16 382	65 536	65 534	255.255.0.0	x.x.255.255
C	110	192.0.0.0 - 223.255.255.255	2 097 150	256	254	255.255.255.0	x.x.x.255
D (Multicast)	1110	224.0.0.0 - 239.255.255.255					
E (experimental)	1111	240.0.0.0 - 255.255.255.254					

- (*) La dirección que tiene los bits de host iguales a 0 sirve para definir la red en la que se ubica. Se denomina **dirección de red**. La dirección que tiene los bits correspondientes a *host* iguales a 1,[1] sirve para enviar paquetes a todos los *hosts* de la red en la que se ubica. Se denomina **dirección de *broadcast***.
- (**) La dirección 0.0.0.0 es reservada por la IANA para identificación local.
- (†) Las direcciones 127.x.x.x se reservan para designar la propia máquina. Se denomina **dirección de bucle local** o ***loopback***.
- (‡) La primera dirección se reserva para identificar la red (p.ej. 18.0.0.0), mientras que la última dirección se emplea como dirección de difusión o *broadcast* (p.ej. 18.255.255.255). Ese es el motivo por el que el número máximo de *hosts* en una red es siempre igual al número de direcciones disponibles en un rango específico menos dos.

Capa 3 Red

Capa 3 Red o IP

Redes privadas. De los aproximadamente cuatro mil millones de direcciones definidas en IPv4, cerca de 18 millones de direcciones en tres rangos están reservadas para su uso en redes privadas. **Las direcciones de paquetes en estos rangos no son enrutables en la Internet pública; son ignorados por todos los enrutadores públicos**. Por lo tanto, los hosts privados no pueden comunicarse directamente con las redes públicas y requieren la traducción de direcciones de red en una puerta de enlace de enrutamiento para este propósito.

Rangos de red IPv4 reservados para redes privadas[11]

Nombre	Bloque CIDR	Rango de direcciones	Número de direcciones	Clase
bloque de 24-bit	10.0.0.0/8	10.0.0.0 – 10.255.255.255	16 777 216	Clase A.
bloque de 20-bit	172.16.0.0/12	172.16.0.0 – 172.31.255.255	1 048 576	Rango contiguo de 16 bloques de clase B.
bloque de 16-bit	192.168.0.0/16	192.168.0.0 – 192.168.255.255	65 536	Rango contiguo de 256 bloques de clase C.

Máscara de red

La máscara de red permite distinguir dentro de la dirección IP, los **bits que identifican a la red y los bits que identifican al host**. En una dirección IPv4, de los 32 bits que se tienen en total, se definen por defecto para una dirección clase A, que los primeros ocho (8) bits son para la red y los restantes 24 para host, en una dirección de clase B, los primeros 16 bits son la parte de red y la de host son los siguientes 16, y para una dirección de clase C, los primeros 24 bits son la parte de red y los ocho (8) restantes son la parte de host. Por ejemplo, de la dirección de clase A 10.2.1.2 sabemos que pertenece a la red 10.0.0.0 y el anfitrión o host al que se refiere es el 2.1.2 dentro de la misma.

La máscara se forma poniendo en 1 los bits que identifican la red y en 0 los bits que identifican al host. De esta forma una dirección de clase A tendrá una máscara por defecto de 255.0.0.0, una de clase B 255.255.0.0 y una de clase C 255.255.255.0. Los dispositivos de red realizan un AND entre la dirección IP y la máscara de red para obtener la dirección de red a la que pertenece el host identificado por la dirección IP dada

Dirección IP: 196.5.4.44

Máscara de red (por defecto): 255.255.255.0

AND (en binario):

`11000100.00000101.00000100.00101100` (196.5.4.44) Dirección ip

`11111111.11111111.11111111.00000000` (255.255.255.0) Máscara de red

`11000100.00000101.00000100.00000000` (196.5.4.0) Resultado del AND

Capa 4 Transporte

Capa 4 Transporte

La capa 4 (transporte) es la encargada de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red.

Las primitivas de un transporte sencillo serían:

- LISTEN: Se bloquea hasta que algún proceso intenta el contacto.

- CONNECT: Intenta activamente establecer una conexión.

- SEND: Envía información.

- RECEIVE: Se bloquea hasta que llegue una TPDU de DATOS.

- DISCONNECT: Este lado quiere liberar la conexión.

Y con estas primitivas podemos hacer un esquema sencillo de manejo de conexiones.

Protocolo UDP

Internet tiene dos protocolos principales en la capa de transporte, uno no orientado a la conexión, **UDP** (Protocolo de Datagramas de Usuario), y otro orientado a la conexión, el **TCP** (Protocolo de Control de Transmisión).

El protocolo UDP proporciona una forma para que las aplicaciones envíen datagramas IP encapsulados sin tener una conexión, descrito en la RFC 768.

Algunas características de este protocolo son:

Genera pocos gastos y se utiliza para aplicaciones que no requieren envío de datos confiable → STREAM de VIDEO. Rápido si pierdo paquetes no pasa nada, puedo perder alguna imagen pero prima la velocidad.

No orientado a la conexión, descrito en la RFC 768, sólo posee 8 bytes de carga. No rastrea la recepción de datagramas en el destino, sólo envía los datagramas recibidos a la capa de aplicación a medida que llega y no reenvía datagramas perdidos. Por esto es más rápido y ligero. Proporciona un servicio de datagramas poco fiable.

Capa 4 Transporte

Protocolo TCP

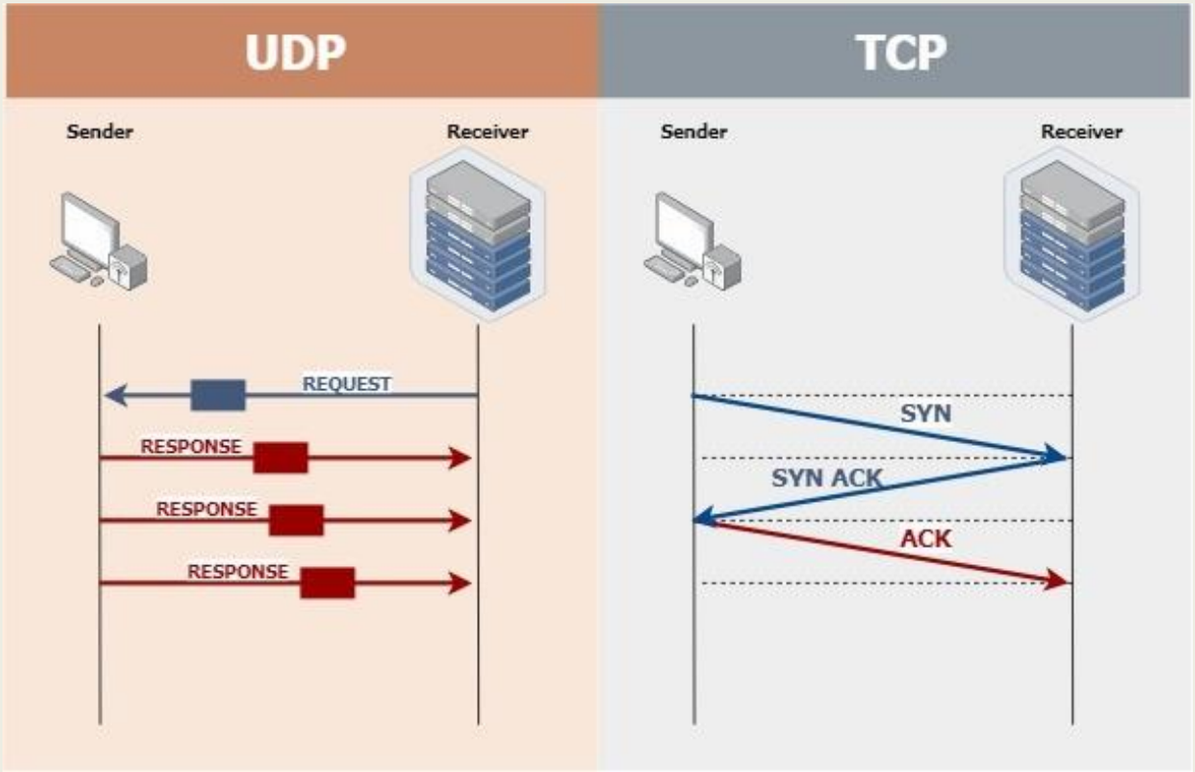
El protocolo TCP (protocolo de control de transmisión) se diseñó específicamente para proporcionar un flujo de bytes confiable de extremo a extremo a través de una interred no confiable. Una interred difiere de una sola red debido a que diversas partes podrían tener diferentes topologías, anchos de banda, retardos, tamaños de paquete… TCP tiene un diseño que se adapta de manera dinámica a las propiedades de la interred y que se sobrepone a muchos tipos de situaciones.

El protocolo TCP proporciona un servicio completo y fiable, descrito en la RFC 793/1323. Cada segmento de TCP posee 20 bytes de carga en el encabezado.

Algunas características del protocolo TCP son:

- Es un protocolo orientado a la conexión.
- Entrega confiable → Envío de un e-mail, p.ej.
- Control de flujo.
- Utiliza mecanismos de enlace, temporizadores, acuses de recibo y uso dinámico de ventanas.
- Su confiabilidad implica cierta sobrecarga en el tamaño de los encabezados y mayor tráfico entre el origen y el destino.

UDP vs TCP

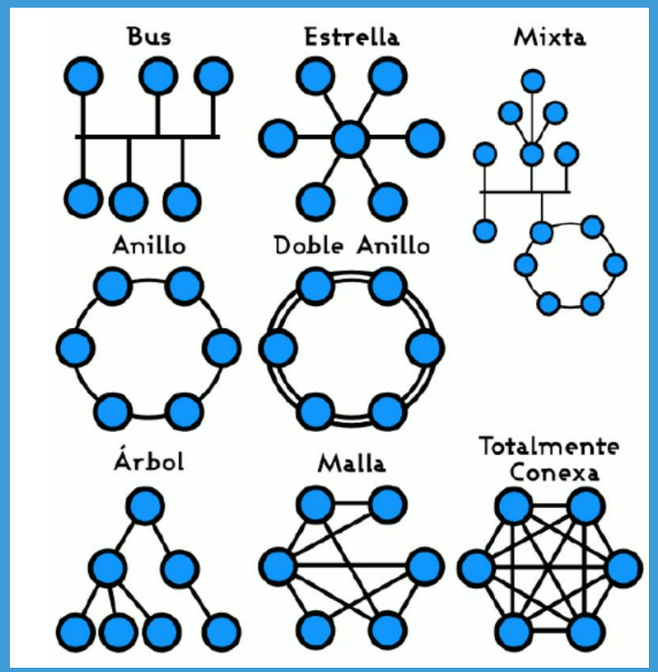


https://www.redeszone.net/tutoriales/configuracion-puertos/puertos-tcp-udp/

Topologías de redes IP

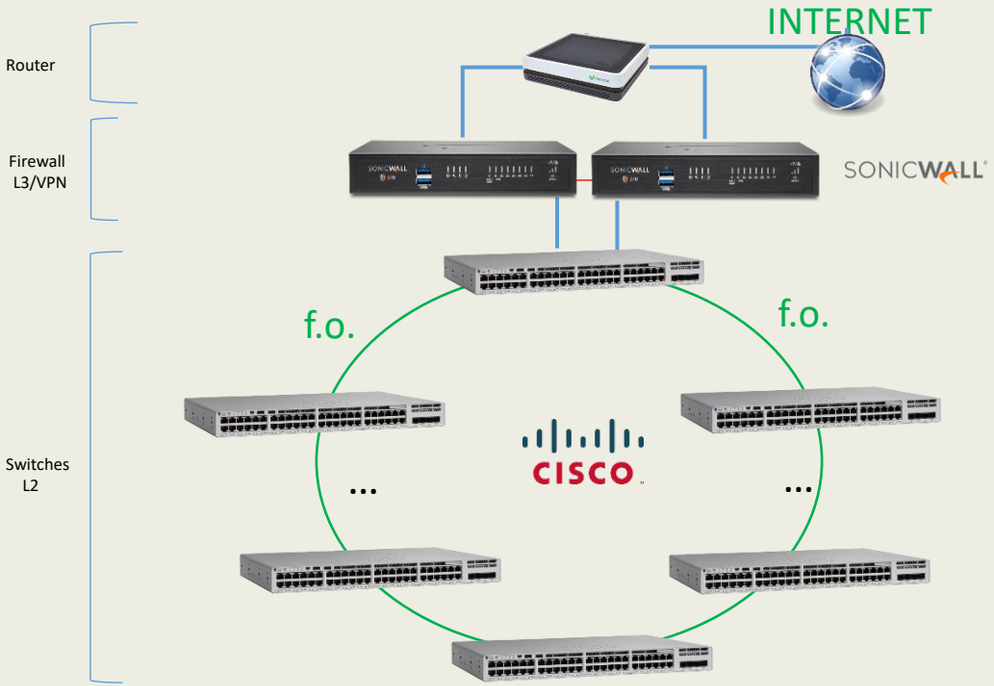
Diferentes topologías

La topología de red es la disposición física en la que se conecta una red de ordenadores. Si una red tiene diversas topologías se le llama mixta.



Topología

Las más comunes son estrella, anillo y mixta. Dependiendo de la cantidad de elementos a conectar, su criticidad, velocidad, etc. Una de mis topologías preferidas para red troncal **industrial** OT redundante es:



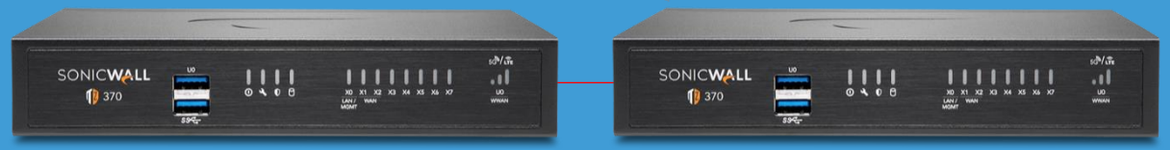
Red OT (Operational)

Equipos de red OT

En el diagrama de red anterior hablamos de una red **troncal** de nivel2 (switching) en anillo para redundancia de caminos con Firewall redundante con capacidades de nivel 3 (routing), accesos VPN, protección contra ataques y control de acceso.

Switches de la marca CISCO modelo 9200L series de 24 o 48 puertos de cobre (tanto PoE+ como normales) y con 4 de fibra.

Firewall de la marca SonicWall modelo TZ370 en alta disponibilidad.



Red OT (capa 2)

Los switches CISCO 9200L disponen de velocidad Gigabit/TenGigabit, soporta VLANs, hasta 4096, entorno web de gestión, también por CLI. Soporta SNMP como protocolo de gestión y los diferentes protocolos de enlace de datos y routing.

A destacar para redes en anillo el estándar **IEEE 802.1w** o protocolo **RSTP (RAPID SPANNING TREE PROTOCOL)**.

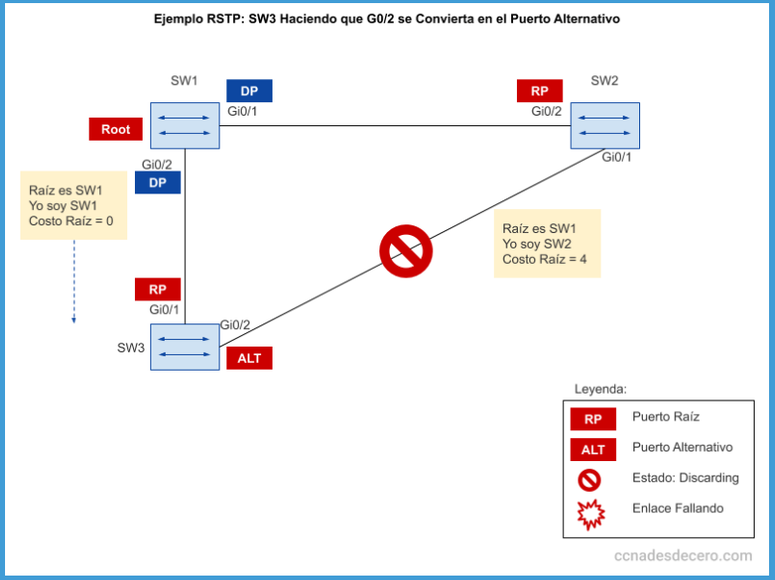
Como ya sabéis, en una red ethernet de nivel o capa 2 no se pueden hacer bucles (loops). Un bucle es cerrar un anillo entre 2 o más elementos, es decir, se produce cuando existe más de una ruta entre los dispositivos de origen y de destino. ¿Resultado? Tira la red abajo ya que los paquetes se reenvían indefinidamente, generando **tormentas de broadcast**.

¿Por qué funcionan los anillos para obtener redundancia de caminos? Gracias a los protocolos RSTP/MSTP (en switches gestionables)

IEEE 802.1w - RSTP

RAPID SPANNING TREE PROTOCOL

Rapid Spanning Tree Protocol (RSTP) es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos), que gestiona enlaces redundantes. Especificado en IEEE 802.1w, es una evolución del Spanning Tree Protocol (STP), reemplazándolo en la edición 2004 del 802.1d. RSTP reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología.

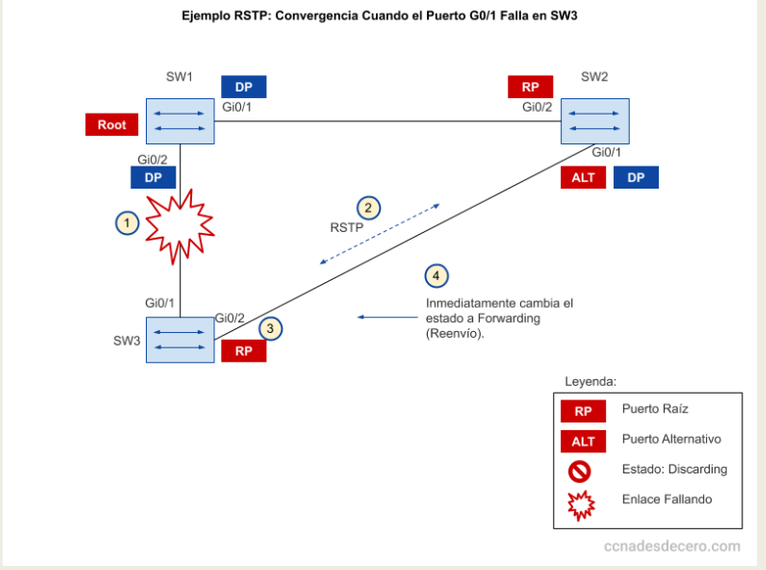


RSTP

Fuente: https://ccnadesdecero.com/curso/rstp/

Evita un doble camino lógico simultáneamente. En caso de fallo utiliza en camino alternativo haciendo converger la red.

Ver MSTP (Multiple Spanning Tree Protocol)



VLANs

VIRTUAL LANs

Las VLAN o también conocidas como «Virtual LAN» nos permite crear redes lógicamente independientes dentro de la misma red física, haciendo uso de switches gestionables que soportan VLANs para segmentar adecuadamente la red.

?Qué conseguimos con estas redes virtuales?

- Seguridad. Podemos crear redes lógicamente independientes, por tanto, podemos aislarlas.
- Segmentación. Las VLAN nos permite segmentar todos los equipos en diferentes subredes, a cada subred le asignaremos una VLAN diferente.
- Flexibilidad. Fácilmente gestionable el cambiar o asignar equipos a una VLAN con las políticas ya creadas.
- Optimización de la red. El uso de VLAN reduce la cantidad de routers necesarios, ya que las VLAN crean dominios de transmisión utilizando switches en lugar de routers.

VLANs

Fuente:https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Cuando creamos y configuramos las VLAN en un switch (L2) no se pueden comunicar entre ellas, la única forma de que se puedan comunicar las VLAN es ascendiendo a nivel de red (L3), esto lo podemos hacer de diferentes formas:

- Usar un router/**firewall** con soporte para el estándar de VLANs. El switch pasará un troncal con todas las VLANs y el router/firewall dará de alta en su firmware o sistema operativo las diferentes VLANs, y permitirán el enrutamiento inter-vlan. Es posible que, por defecto, este enrutamiento esté activado, pero por reglas en el firewall se deniegue la comunicación entre las VLAN, hasta que permitamos el acceso.
- Usar un switch gestionable L3. Los switches gestionables L3 nos permiten crear interfaces IPv4 y IPv6, por lo que podremos crear una interfaz por cada VLAN que tengamos configurada en el switch y activar el enrutamiento inter-vlan. Esto es una opción muy buena para intercomunicar las VLANs sin necesidad de que el router se encargue de todo, generalmente estos switches L3 están en el Core de la red.

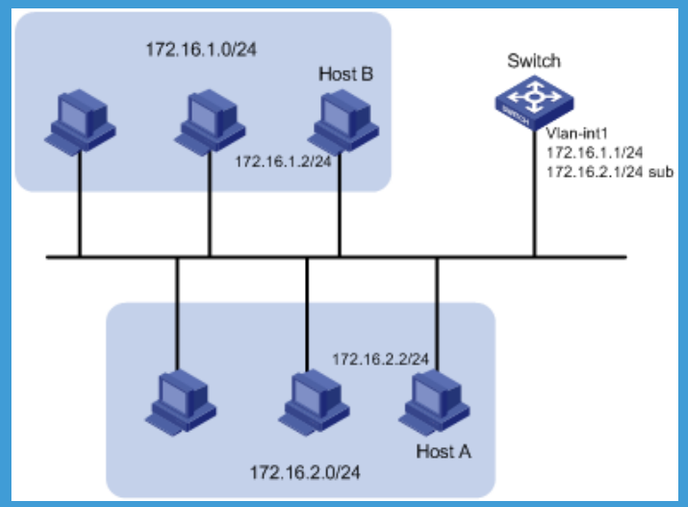
VLANs

VIRTUAL LANs

Por ejemplo una red privada de clase B (rango 172.16.x.x)

Establecemos una VLAN con ID 1 para el rango 172.16.1.0/24 y otra con ID 2 para el rango 172.16.2.0/24.

La puerta de enlace o Gateway a definir en cada equipo de cada VLAN tiene que estar definida en un elemento como Router o Firewall para enrutar los paquetes. Podemos asignar 172.16.1.1 para VLAN1 y 172.16.2.1 para la VLAN2.



VLANs

Actualmente existen varios tipos de VLANs que podemos utilizar en los diferentes equipos, es decir, en los switches y puntos de acceso WiFi. Las diferentes VLANs que existen son las basadas en el estándar **802.1Q VLAN Tagging basado en etiquetas**, las VLAN basadas en puerto, las VLAN basadas en MAC, las VLAN basadas en aplicaciones, aunque esta última no suele utilizarse habitualmente.

Lo normal es utilizar el estándar 802.1Q con VLANs basadas en etiquetas.

802.1q – PUERTOS

TAGGED / UNTAGGED

Cuando estamos usando el estándar 802.1Q y creamos las diferentes VLANs en un switch, podremos configurar los diferentes puertos como «tagged» o «untagged», es decir, con etiqueta o sin etiqueta.

- VLAN tagged: en las tramas Ethernet se incorpora el «tag» del VLAN ID que hayamos configurado, este tipo de VLANs son entendidas por todos los switches, por los puntos de acceso WiFi profesionales y por los routers. Se pueden configurar en modo «tagged» una o más VLANs en un determinado puerto. En los enlaces troncales (desde un router a un switch, de switch a switch y de switch a AP) se suelen configurar siempre como «tagged» para «enviarles» todas las VLANs.
- VLAN untagged: en las tramas Ethernet se retira el tag que hayamos configurado, este tipo de VLANs son entendidas por todos los dispositivos, pero principalmente se utilizan de cara a los equipos finales como ordenadores, portátiles, impresoras, cámaras IP y otro tipo de dispositivo. En un puerto en concreto solamente podremos configurar una VLAN como «untagged», no podemos poner dos VLANs como «untagged» porque el equipo final no «entendería» nada.

TRUNK / ACCESS

Fuente:https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Cuando estamos utilizando este estándar, los switches también permiten configurar los puertos físicos de diferentes formas:

- Access: son los puertos donde conectaremos los PC, impresoras, PLCs y los equipos finales. Este puerto de acceso tendrá configurada una VLAN como «untagged». Al seleccionar modo de acceso deberemos poner el VLAN ID configurado para quitar la etiqueta y pasarle al equipo final todos los datos.
- Trunk: lleva una o varias VLANs de un equipo a otro, por ejemplo, si queremos conectar un switch con otro switch y «pasarle» todas las VLANs o algunas de ellas, tendremos que configurarlo en modo troncal o trunk, y seleccionar las VLANs que queremos pasar como «tagged».

Los puertos configurados como «untagged» es sinónimo de un puerto configurado en modo acceso, y un puerto configurado como «tagged» es sinónimo de puerto en modo trunk donde le pasemos una o varias VLANs.

802.1q – ENLACES TRUNK

ENLACES TRUNK

En una red troncal definimos los enlaces que hacen el anillo como TRUNK (**IEEE 802.1Q → etiqueta de la trama con el ID de la VLAN**).

Es un enlace que se configura en uno o más puertos de un switch para permitir el paso del tráfico de las distintas VLANs que hemos configurado. Este enlace puede funcionar en una conexión de switch a otro switch o bien, de un switch a un router, de un switch a un firewall para «pasarle» varias VLANs simultáneamente.

En definitiva, por estos caminos debe pasar TODO el tráfico. En un anillo de fibra serán los puertos de fibra SFP y si además el firewall enruta VLANs los puertos de cobre que conectan el Switch al Firewall.

No hay dudas respecto a su eficacia, pues ahorra la necesidad de utilizar un enlace físico para cada VLAN, algo fundamental cuando tenemos decenas de VLANs configuradas y en uso, ya que, de lo contrario, necesitaríamos routers con decenas de puertos RJ45 o SFP disponibles para intercomunicar las diferentes VLANs, o bien disponer de un switch Multicapa L3.

Frame tagging (802.1Q)

Fuente:https://www.redeszone.net/tutoriales/redes-cable/configurar-enlace-troncal-switch/

Los puertos TRUNK se configurarán como "tagged" lo que permitirá etiquetar las tramas ethernet con el VLAN ID. De esta manera el enrutador sabrá cuál es cuál ya que por el enlace trunk pasan múltiples subredes virtuales.

Este estándar consiste en introducir una cabecera 802.1Q dentro de la trama Ethernet que todos conocemos, con el objetivo de diferenciar las diferentes VLANs que tengamos configuradas. Este estándar no encapsula la trama original de Ethernet, sino que añade 4 bytes al encabezado Ethernet original, además, el cambio de «EtherType» se cambia al valor 0x8100 para señalar que se ha cambiado el formato de la trama.

Ejemplo

TAGGED / UNTAGGED

Desde telnet con el CLI de CISCO y con la VLAN 10 ya creada.

- (izquierda) Configuramos el puerto 1 del SW1 y 2 en modo Access y le asignamos la VLAN 10.
- (derecha) Configuramos el puerto 24 del SW1 y 2 en modo Trunk (con todas las VLANs).

```
SW1(config)#interface fa0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
```

```
SW2(config)#interface fa0/1
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 10
```

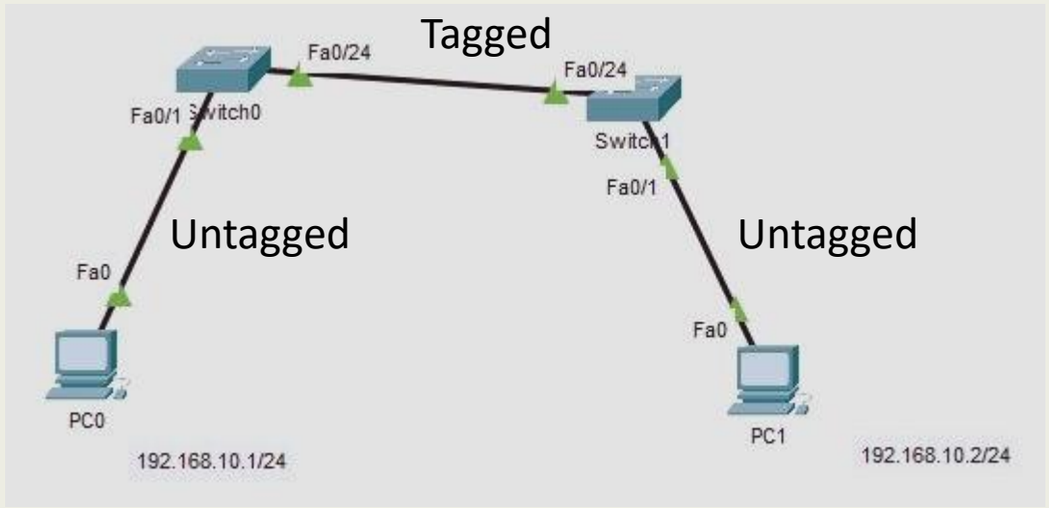
ACCESS (EQUIPO FINAL)

```
SW1(config)#interface fa0/24
SW1(config-if)#switchport mode trunk
```

```
SW2(config)#interface fa0/24
SW2(config-if)#switchport mode trunk
```

TRUNK (SWITCHES)

Ejemplo

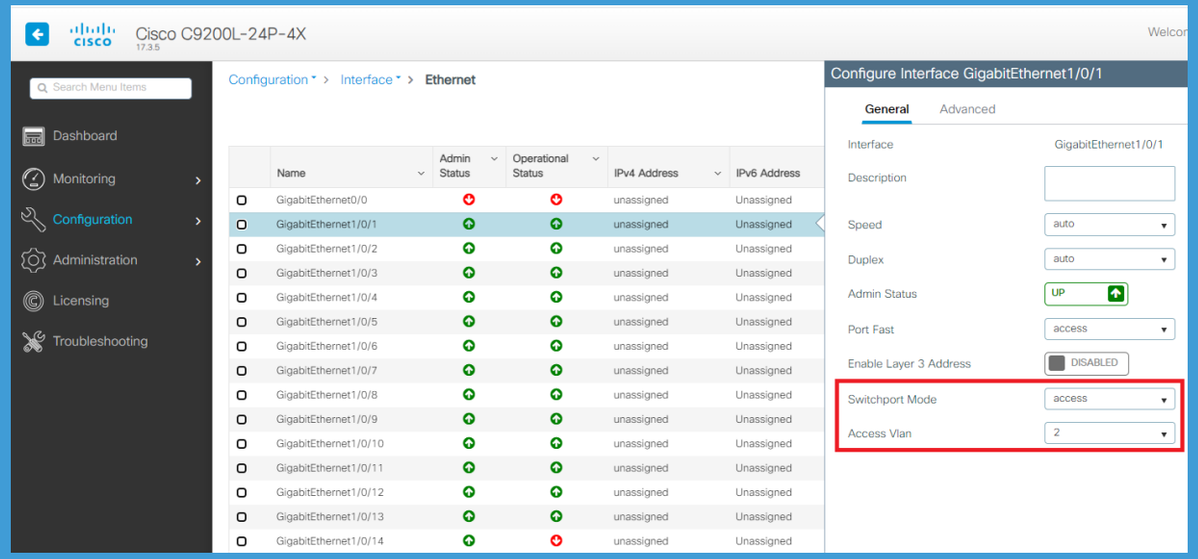


Equipos finales en VLAN 10 (192.168.10.x) y en el puerto 1 de cada switch.
Ambos switches se conectan entre sí por el puerto 24 (enlace troncal).

Ejemplo

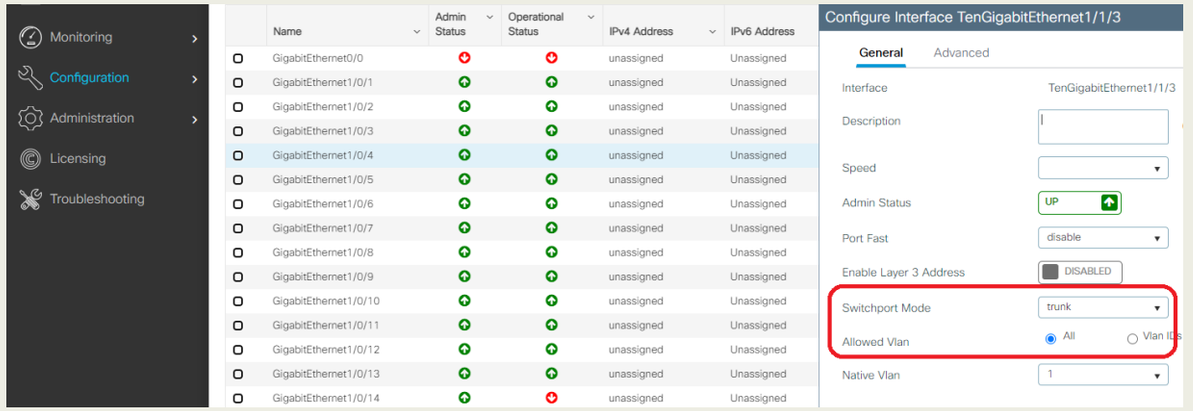
Mode access + vlan id

Ejemplo en entorno web de configuración de un puerto gigabit para un equipo final en la vlan 2 (mode access).



Mode trunk + all vlan

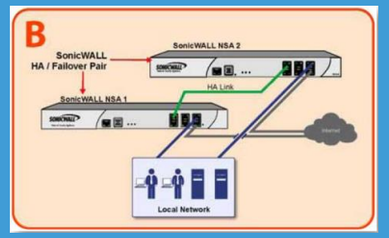
Ejemplo en entorno web de configuración de un puerto 10 gigabit para un enlace troncal para todas las vlan (mode trunk).



Routing VLANs

Enrutamiento VLANs

Para hacer el enrutamiento de las VLANs utilizaremos el Firewall SonicWall TZ370 HA (alta disponibilidad).



X0: LAN
X1: WAN
X7: High Availability

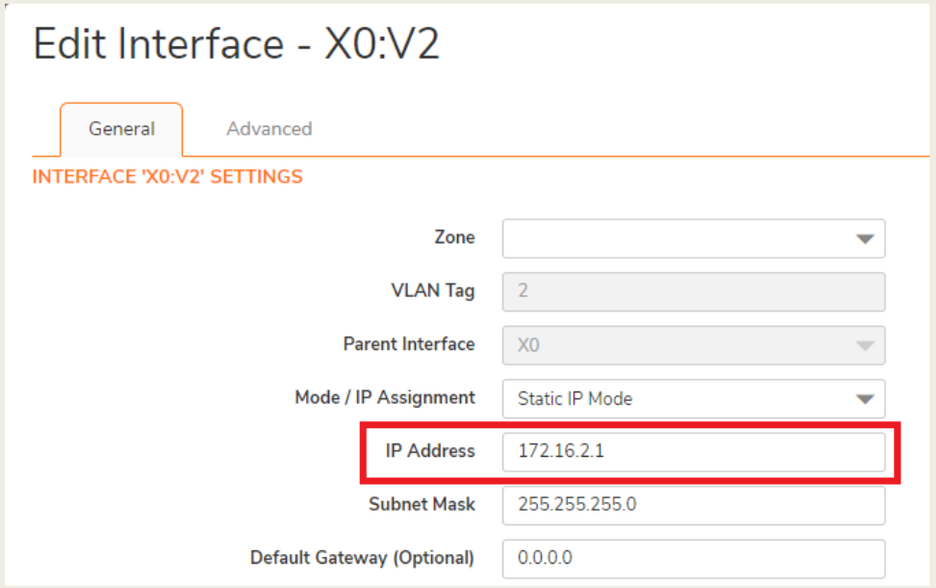
NAME	ZONE	GROUP	IP ADDRESS	SUBNET MASK	IP ASSIGNMENT	STATUS
X0	LAN	N/A	172.16.0.1	255.255.255.0	Static IP	1 Gbps Full Duplex
X0:V2		N/A	172.16.2.1	255.255.255.0	Static IP	VLAN Sub-Interface
X0:V3		N/A	192.168.1.1	255.255.255.0	Static IP	VLAN Sub-Interface

Dentro de la interfaz X0/LAN creo 2 subinterfaces para cada VLAN (V2/V3)

Red OT (capa 3)

Configuro la @IP del default Gateway de la VLAN 2 y de las N que tenga.

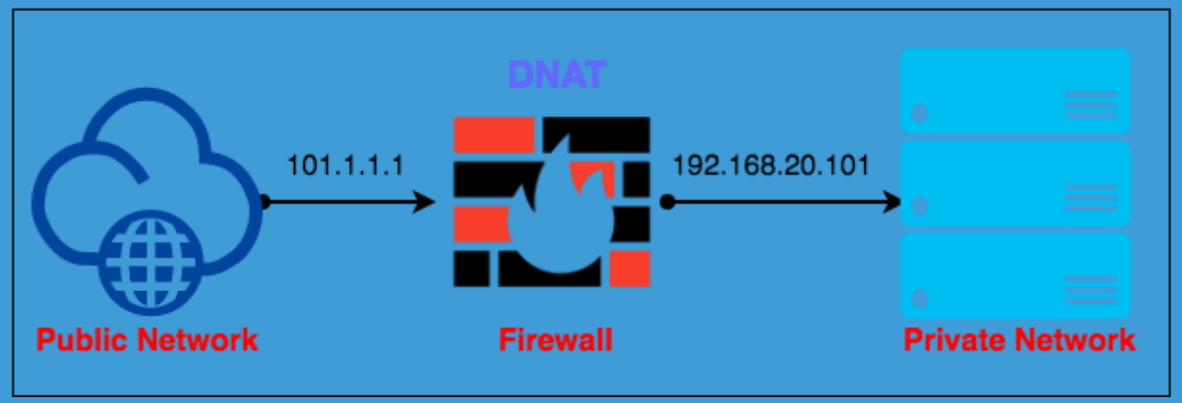
En este caso la subred 172.16.2.x acabando siempre en 1.



NAT

NAT (Network Addres Translation)

NAT significa traducción de direcciones IP. Es decir, su trabajo consiste en coger una dirección IP privada y traducirla a una dirección IP pública o viceversa.



Red OT (FW)

La función de NAT la puede hacer el propio firewall para exponer servicios de la red privada a la red pública.

Con reglas como:

- Cualquier IP que llame a la IP pública del FW por el puerto TCP expuesto obtiene el servicio.

- Permitiendo los puertos específicos de WAN a LAN (o red pública a red privada).

	GENERAL				ORIGINAL					TRANSLATED		
	P.	HITS	NAME	STA..	INGRESS INTERFACE	EGRESS INTERFACE	SOURCE	DESTINATION	SERVICE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE
	45	1.8k	NodeRed_34		Any	Any	Any	WAN Interface IP	TCP_9099	Original	NodeRed	Original
	46	1.9k	PortalInformesSSL_35		Any	Any	Any	WAN Interface IP	TCP_9092	Original	PortalInformes	Original

Bonus

SINGLE PAIR ETHERNET

Varios fabricantes de IoT industrial están desarrollando y estandarizando SPE (Single Pair Ethernet).

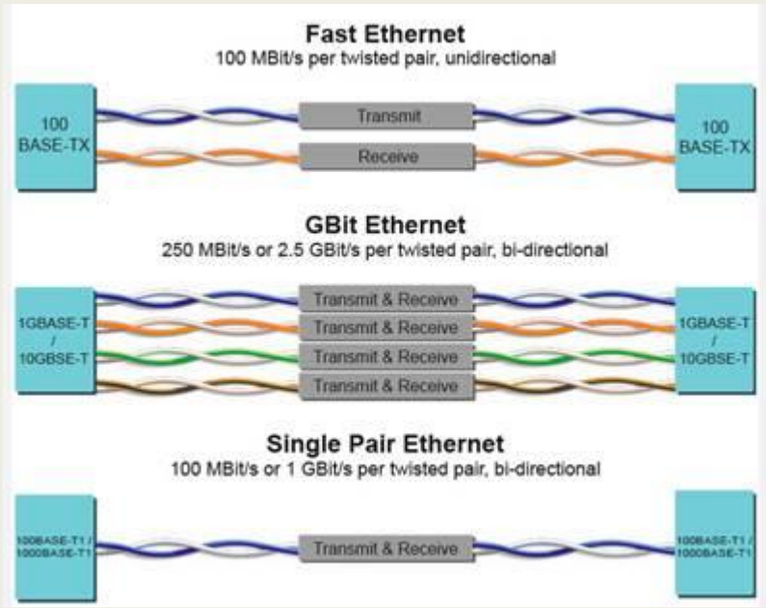
https://www.weidmuller.es/es/productos/connectivity/conectores/single_pair_ethernet.jsp

https://www.telcomanager.com/es/blog/que-es-la-tecnologia-single-pair-ethernet-spe/

SPE System Alliance es una asociación de empresas tecnológicas líderes de diferentes industrias y campos de aplicación que agrupan e intercambian sus conocimientos sobre Single Pair Ethernet. Todos los partners persiguen el objetivo común de promover la tecnología SPE para la IoT industrial y todo el resto de campos de aplicación. En la web se encuentran detalles y oportunidades para contactar con SPE System Alliance.

¿Qué es SPE?

Es un Ethernet de 2 hilos (single pair) para conectar sensores directamente a electrónica de red y que la conectividad sea 100% Ethernet. Consiguiendo más alcance (1 Km) a menos velocidad.



Bonus

SINGLE PAIR ETHERNET

Ventajas:

- Reducción del peso del cableado
- Alimentación de dispositivos mediante PoDL (tipo PoE)
- Alcance mayor
- Reducción de espacio en los racks / cuadros
- Miniaturización (diseño compacto)
- Simplicidad

El tema clave será la **compatibilidad** con redes Ethernet existentes.

¿Creéis que tendrá éxito? La verdad que tiene buena pinta.

Miniaturización

La siguiente imagen muestra un switch SPE y debajo un switch Ethernet normal con puertos RJ45.

Donde antes conectaba 5 dispositivos ahora puedo conectar el doble o más o bien reduciendo el espacio para conectar 5 dispositivos.

Enlaces recomendados

Enlaces recomendados

Redes

https://ccnadesdecero.com/curso/rstp/

https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

https://www.redeszone.net/tutoriales/redes-cable/configurar-enlace-troncal-switch/

https://maclookup.app/macaddress/

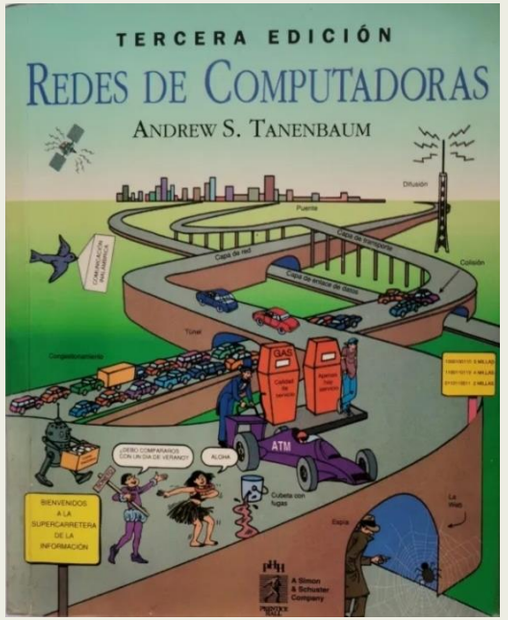
https://www.redeszone.net/tutoriales/configuracion-puertos/puertos-tcp-udp/

SPE (Single Pair Ethernet)

https://www.weidmuller.es/es/productos/connectivity/conectores/single_pair_ethernet.jsp

https://www.telcomanager.com/es/blog/que-es-la-tecnologia-single-pair-ethernet-spe/

Un libro de cuando estudié en la universidad.



Andrew S. Tanenbaum en 1987 creó el sistema operativo Minix, un sistema Unix-like gratuito con propósitos educativos, que posteriormente inspiró Linux.

IP NETWORKS
v.1.2 MARZO 2024

https://www.linkedin.com/in/ricardo-moraleda-gareta-9421099

https://www.linkedin.com/company/gdo-electric1996/

RICARDO MORALEDA GARETA

GDO SOFTWARE