Redes LAN

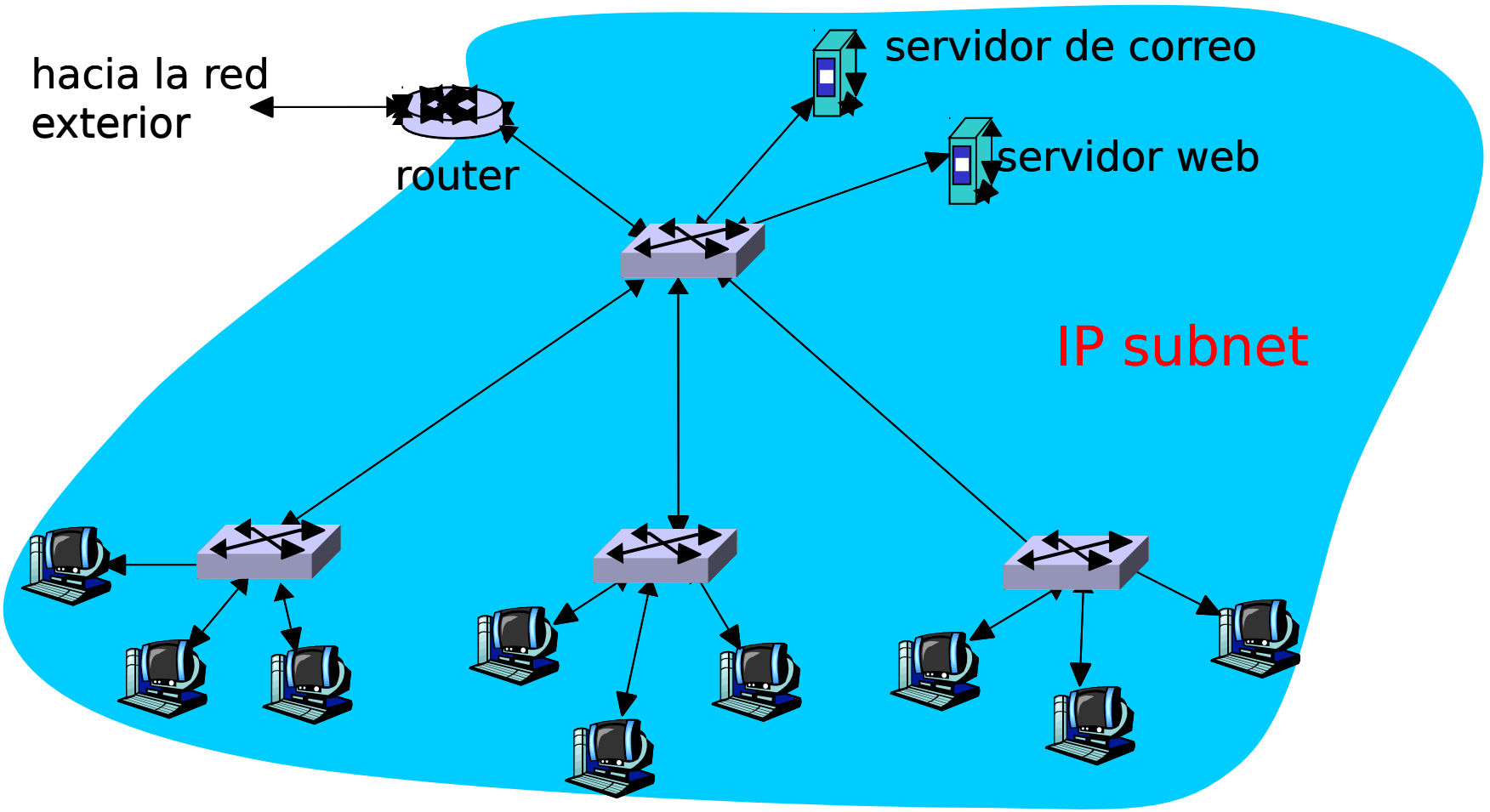
Tipo de red clasificada por:

- Distancia máxima entre dispositivos inferior a varios cientos de metros.
- Tecnología de acceso CSMA
- Medio compartido.
- Excepciones:
    - fibra óptica permite distancias mucho mayores
    - Interconexión de LAN a través de VPN
    - Ethernet conmutada el medio no es compartido
    - Wifi el medio es compartido.

Tecnologías:

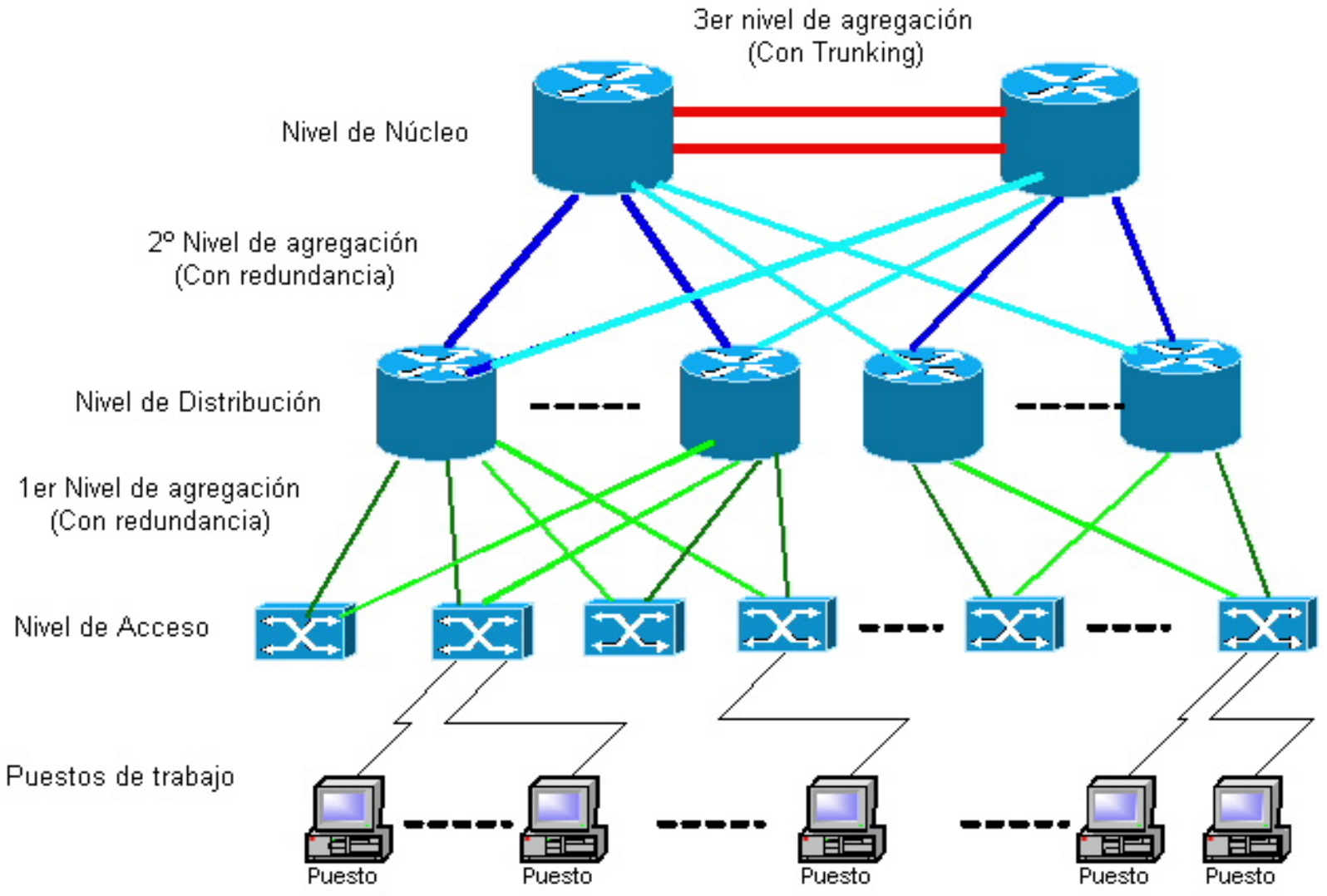
- Ethernet 802.3. Acceso CSMA/CD
- Ethernet VLAN 802.1q . Acceso CSMA/CD
- Wifi 802.11. Acceso CSMA/CA
- Redes PAN (Personal Area Networks)
    - Variantes del estándar 802
    - Bluetooth.
    - ZigBee (redes de sensores).

Topologías LAN



Topologías corporativas

Topologías LAN



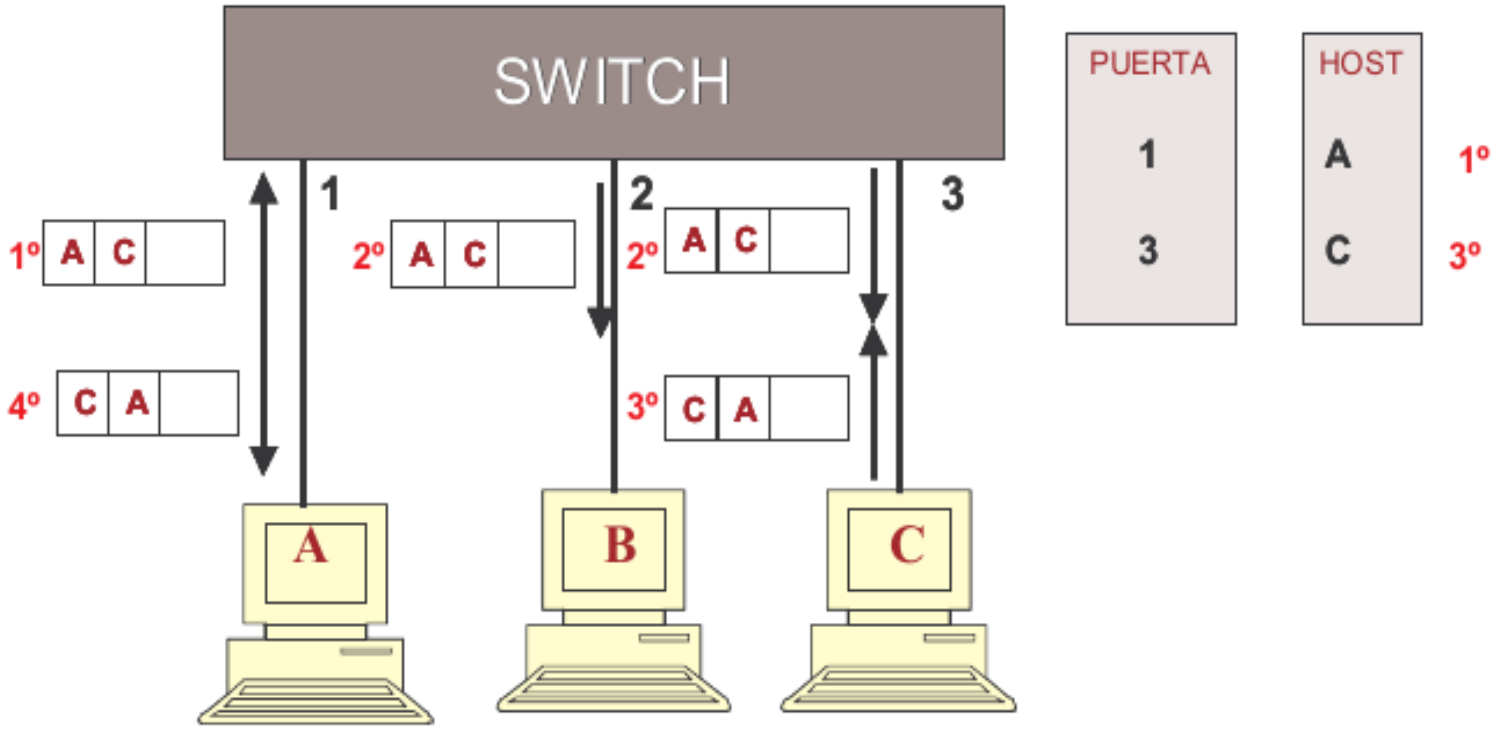
Ethernet

Grupo de trabajo IEEE 802

Estándar	Tecnología	Observaciones
IEEE 802.1	Bridging (networking) and Network Management	Incluye las tecnologías VLAN (802.1q)
IEEE 802.2	Logical link control (upper part of data link layer)	
IEEE 802.3	Ethernet (CSMA/CD)	
IEEE 802.4	Token bus	(disbanded)
IEEE 802.5	Defines the MAC layer for a Token Ring	(inactive)
IEEE 802.6	Metropolitan Area Networks	(disbanded)
IEEE 802.7	Broadband LAN using Coaxial Cable	(disbanded)
IEEE 802.8	Fiber Optic TAG	(disbanded)
IEEE 802.9	Integrated Services LAN	(disbanded)
IEEE 802.10	Interoperable LAN Security	(disbanded)
IEEE 802.11	Wireless LAN & Mesh	(Wi-Fi certification)
IEEE 802.12	demand priority (disbanded)	
IEEE 802.13	Not Used	
IEEE 802.14	Cable modems	(disbanded)
IEEE 802.15	Wireless PAN	
IEEE 802.15.1	(Bluetooth certification)	
IEEE 802.15.4	(ZigBee certification)	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16e	(Mobile) Broadband Wireless Access	WiMAX
IEEE 802.17	Resilient packet ring	
IEEE 802.18	Radio Regulatory TAG	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	
IEEE 802.24	Smart Grid TAG	New (November, 2012)
IEEE 802.25	Omni-Range Area Network	No ratificada

Ethernet conmutada

Switch - Conmutador



Medio semi-compartido o no compartido

Ethernet conmutada

Conmutadores-Switches

Cuando el conmutador aprende las direcciones de sus nodos, reenvia las tramas mediante un procedimiento de reenvio. Hay cuatro procedimientos fundamentales, entre puertos que tienen la misma velocidad:

1. Store and forward: el conmutador bufferiza y verifica cada trama completa antes de reenviarla.

2. Cut through: el conmutador solo lee en serie la trama hasta conocer la dirección de destino. Si el puerto donde se encuentra el destino está ocupado, almacena la trama hasta que esté libre. Si el puerto destino está desocupado, reenvía o redirige la trama directamente hacia ese puerto. Con este procedimiento el conmutador no comprueba errores, pero mejora la velocidad de conmutación.

3. Fragment free: el conmutador checkea los primeros 64 octetos de la trama, donde se encuentra la información de direccionamiento. Esto permite detectar colisiones previas en la trama, en cuyo caso no se reenvía.

4. Adaptive switching: permite seleccionar automáticamente el modo de reenvio entre los tres anteriores. Lo hace por estadística y mediante un algoritmo. Mantiene el cut throgh hasta que es informado de errores o de colisiones.

Ethernet conmutada

Cabecera Ethernet

802.3 Ethernet frame structure

Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interframe gap
7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	42[note 2]–1500 octets	4 octets	12 octets
	← 64–1518 octets (64-1522 octets for 802.1Q tagged frames) →							
← 84–1538 octets (88-1542 octets for 802.1Q tagged frames) →								

- **Preámbulo: 7 bytes de sincronización (unos y ceros alternados).**
- **Delimitador del comienzo de trama (SFD). Secuencia 10101011, indica el comienzo.**
- **Dirección de destino. 6 bytes. Puede ser a un grupo (FF:FF.....FF)**
- **Dirección de origen:**
- **Longitud/Tipo (2 Bytes): Longitud del campo LLC ó el tipo de Ethernet (ARP, DoD IP, etc). Valores por encima de 0x05DC indican Tipo.**
- **Datos LLC**
- **Relleno y secuencia de comprobación.**

Ethernet conmutada

Ethernet Types

EtherType	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on-LAN[3]
0x22F3	IETF TRILL Protocol
0x6003	DECnet Phase IV
0x8035	Reverse Address Resolution Protocol
0x809B	AppleTalk (Ethertalk)
0x80F3	AppleTalk Address Resolution Protocol (AARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q) & Shortest Path Bridging IEEE 802.1aq[4]
0x8137	IPX
0x8138	IPX
0x8204	QNX Qnet
0x86DD	Internet Protocol Version 6 (IPv6)
0x8808	Ethernet flow control
0x8809	Slow Protocols (IEEE 802.3)
0x8819	CobraNet
0x8847	MPLS unicast
0x8848	MPLS multicast
0x8863	PPPoE Discovery Stage
0x8864	PPPoE Session Stage
0x8870	Jumbo Frames[2]
0x887B	HomePlug 1.0 MME
0x888E	EAP over LAN (IEEE 802.1X)
0x8892	PROFINET Protocol
0x889A	HyperSCSI (SCSI over Ethernet)
0x88A2	ATA over Ethernet
0x88A4	EtherCAT Protocol
0x88A8	Provider Bridging (IEEE 802.1ad) & Shortest Path Bridging IEEE 802.1aq[5]
0x88AB	Ethernet Powerlink[*citation needed*]
0x88CC	Link Layer Discovery Protocol (LLDP)
0x88CD	SERCOS III
0x88E1	HomePlug AV MME[*citation needed*]
0x88E3	Media Redundancy Protocol (IEC62439-2)
0x88E5	MAC security (IEEE 802.1AE)
0x88F7	Precision Time Protocol (IEEE 1588)
0x8902	IEEE 802.1ag Connectivity Fault Management (CFM) Protocol / ITU-T Recommendation Y.1731 (OAM)
0x8906	Fibre Channel over Ethernet (FCoE)
0x8914	FCoE Initialization Protocol
0x8915	RDMA over Converged Ethernet (RoCE)

Ethernet conmutada

Acceso al medio CSMA/CD

En LAN's, el tiempo de retardo de propagación es pequeño en comparación con el de transmisión de trama. Así apareció el protocolo **CSMA/CD (Carrier Sense Multiple Access / Colission Detect).** EL hecho de que el tiempo de retardo sea pequeño, permite a todos los hosts saber si hay transmisión o no casi al momento.

El protocolo CSMA/CD escucha el medio de la siguiente forma:

1. Si el medio se encuentra libre, transmite; si no, se aplica la regla 2.
2. Si el medio está ocupado, sigue escuchando hasta que esté libre, tras lo cual transmite inmediatamente.
3. Si se detecta colisión durante la transmisión, las estaciones transmiten una señal corta de alerta para que todos dejen de transmitir.
4. Después de la alerta, las estaciones esperan aleatoriamente (el tiempo de espera sigue el algoritmo de retroceso exponencial binario), tras lo cual pasan al punto 1.

La eficiencia de CSMA/CD es alta, solo desaprovecha el tiempo que se tarda en detectar la colisión que es dos veces el retardo de propagación extremo a extremo.

Ethernet inalámbrica

Acceso al medio CSMA/CA

En LAN's inalámbricas existe el problema del **nodo oculto**: cuando una estación A que forma parte de la red no está en el alcance de una estación B pero sí de otra C (A <-----> C <-----> B) y la estación A no puede detectar la ocupación del medio entre B y C. En ese caso, se produciría colisión, pero A no lo detecta.

En ese caso el proceso sería:

1. A emite un RTS (Request to Send) al medio y espera un periodo de tiempo por una confirmación (CTS).

2. En modo infraestructure el AP (nodo C) gestiona si el medio está desocupado y envia un CTS (Clear to Send) a A, o no envía nada si sabe que hay otra estación transmitiendo. El CTS es escuchado por todas las estaciones y así evitan enviar un RTS durante un tiempo.

3. A transmite datos a B (a través de C) y espera un ACK de B (a través de C). Si no lo recibe en un tiempo vuelve a empezar.

Este método consume bastante capacidad de canal y no es muy eficiente, por lo que en muchos casos se utiliza una variante del mismo llamada DCF (Distributed Coordination Function). Este consiste en que todas las estaciones asignan un tiempo DIFS a escuchar el canal. Si está libre esperan un añadido BackoffTime aleatorio para solicitar el RTS y evitar que otra estación transmita al mismo tiempo.

Ethernet inalámbrica

Modos de trabajo 802.11

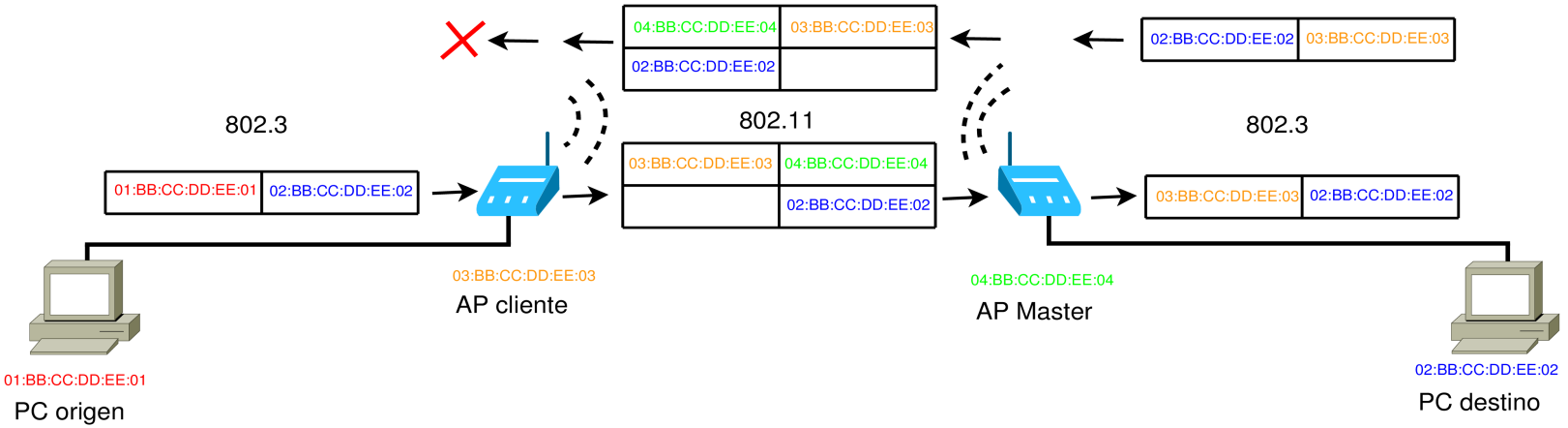
1. Modo **Ad-Hoc**: comunicación directa entre equipos. Problema del nodo oculto

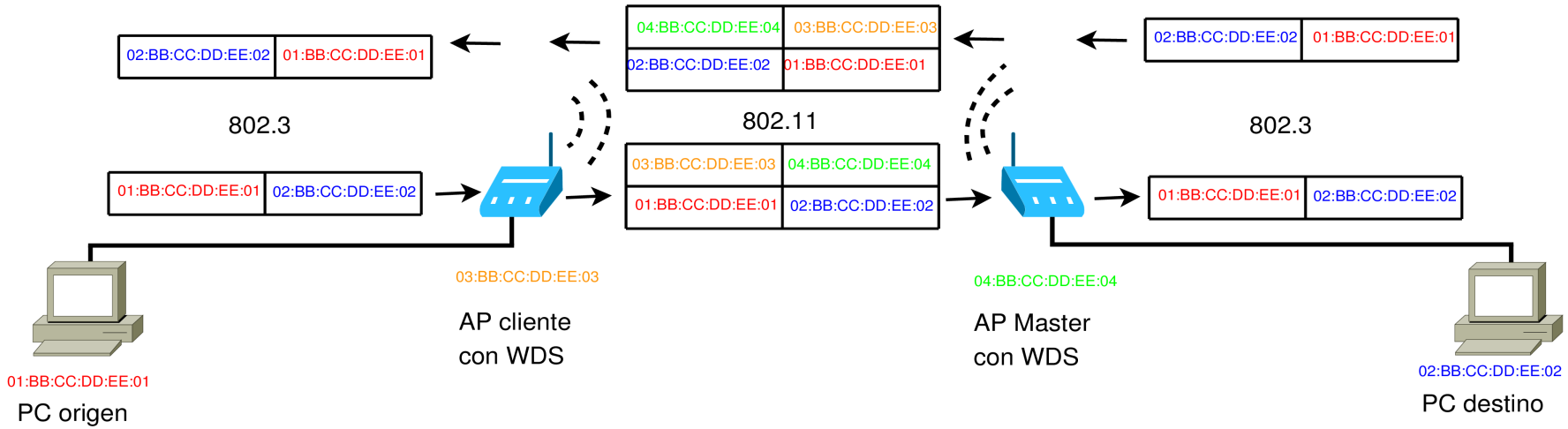
2. Modo **Infraestructure**: gestión del acceso al medio mediante modelo Maestro-Esclavo (solicitud de acceso al Maestro por RTS, confirmación del Maestro al esclavo por CTS). Comunicación de equipos hacia una red. Dos tipos de dispositivos:
   * Maestro, AP, Manager, Red
   * Esclavo, Estación, Managed, Equipo

3. Modo **WDS** (Wireless Distribution System): comunicación entre redes. Enlaces entre Aps. Utiliza los 4 campos de la cabecera 802.11

Ethernet inalámbrica

Modo WDS. Justificación de uso de los campos de dirección de la cabecera



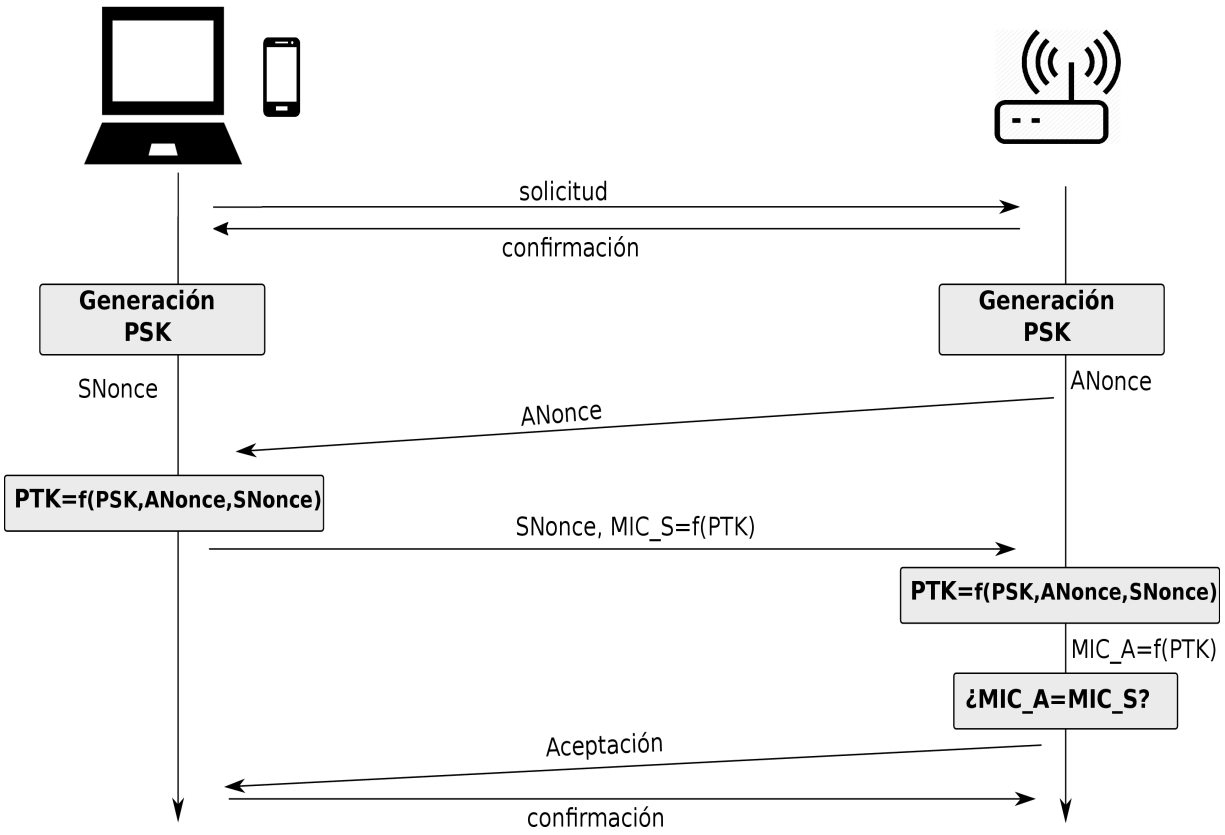


Ethernet inalámbrica. Seguridad WPA

Wireless Protected Access

- Personal Mode (estático) o Enterprise Mode (Dinámico → Radius)
- Autenticación:
  - Palabra clave → *PSK = PBKDF2(PalClav, SSID, LSSID, N, S)*
  - N=número de iteraciones. S, habitualmente 256.
  - El cliente envía una solicitud de acceso -> el AP le envía un número aleatorio llamado ANonce.
  - El cliente genera otro número aleatorio SNonce y envía un mensaje de autenticación compuesto por el SNonce y un hash (llamado MIC y del cual no puede deducirse la palabra clave) generado con el ANonce y la clave PSK.
  - En ambos extremos se genera una clave transitoria llamada PTK (Pairwise Transient Key) que está compuesta por una función del ANonce, el SNonce y el MIC, y esta clave debe coincidir en ambos extremos para finalizar la autenticación.
- Transmisión:
  - Protocolo TKIP que emplea claves dinámicas diferentes en cada trama de datos enviada.

Ethernet inalámbrica. Seguridad WPA



Es importante resaltar que la clave PSK no se envía nunca al otro extremo, por lo que no puede ser capturada por un atacante, y además, cada cliente genera una PTK diferente, pues para ello se utilizan números aleatorios.

VLAN

VLAN – Redes Virtuales

Se pueden definir las redes virtuales como la segmentación lógica de la red Ethernet, esto es, crear segmentos lógicos para proporcionar:

- Seguridad al segmento de red
- Contención del Broadcast al tener segmentos mas pequeños, esto hace que los dominios de broadcast sean menores.
- Hacer mas eficiente la administración en cuanto a movimientos, adiciones y cambios del usuario dentro de la empresa ya que si un departamento se desplaza a otro edificio dentro de la fabrica, este cambio físico será transparente gracias a la visión lógica de la red virtual.

Tipos de VLAN

- Basada en puertos (capa 1):Consiste en una agrupación de puertos físicos que puede tener lugar sobre un conmutador o varios. La asignación de los usuarios a la VLAN se hace en base a los puertos a los que están conectados físicamente.

- Basada en MAC (capa 2):Operan agrupando estaciones finales en una VLAN en base a sus direcciones MAC.

- VLAN de capa 3:Toman en cuenta el tipo de protocolo o direcciones de la capa de red, para determinar la pertenencia a una VLAN

- VLAN basadas en reglas (Policy Based).Permite crear VLANs adaptadas a necesidades especificas del gestor de red utilizando una combinación de reglas, como pueden ser de acceso.

Membresía

Método utilizado para indicar la membresía cuando un paquete viaja entre conmutadores, es decir, cómo identificar que determinado paquete de datos “pertenece” a una VLAN u otra.

Existen dos métodos:

• Implícito: La membresía a una VLAN está indicada por la dirección MAC. En este caso, todos los conmutadores que soportan una VLAN particular, deben compartir una tabla con las direcciones MAC de miembros. Esto permite independizar la ubicación física del equipo al conectarlo a un conmutador con soporte VLAN y con la tabla de miembros. Obliga al uso de un protocolo de transmisión de tablas VLAN-MAC.

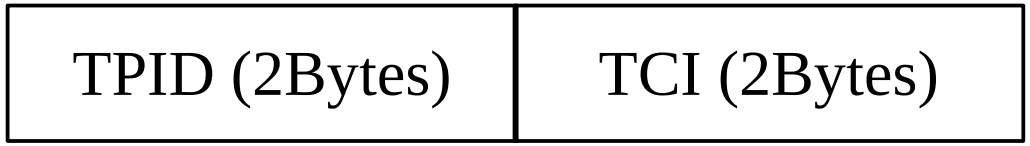
• Explicito: Se introduce una etiqueta al paquete para indicar a qué VLAN pertenece. Es el método utilizado por la especificación 802.1Q.

Como resumen, cuando un paquete entra al conmutador, la determinación de su pertenencia a una VLAN puede ser basada en puerto, en MAC o en protocolo. Cuando el paquete viaja hacia otro conmutador, la determinación de la pertenencia a una VLAN de este paquete puede ser Implícita (utilizando la dirección MAC) o Explicita (Utilizando una etiqueta que fue introducida por el primer conmutador).

Etiquetado

- El objetivo de la especificación 802.1Q es la utilización de VLANs basadas en puertos y etiquetado explicito.

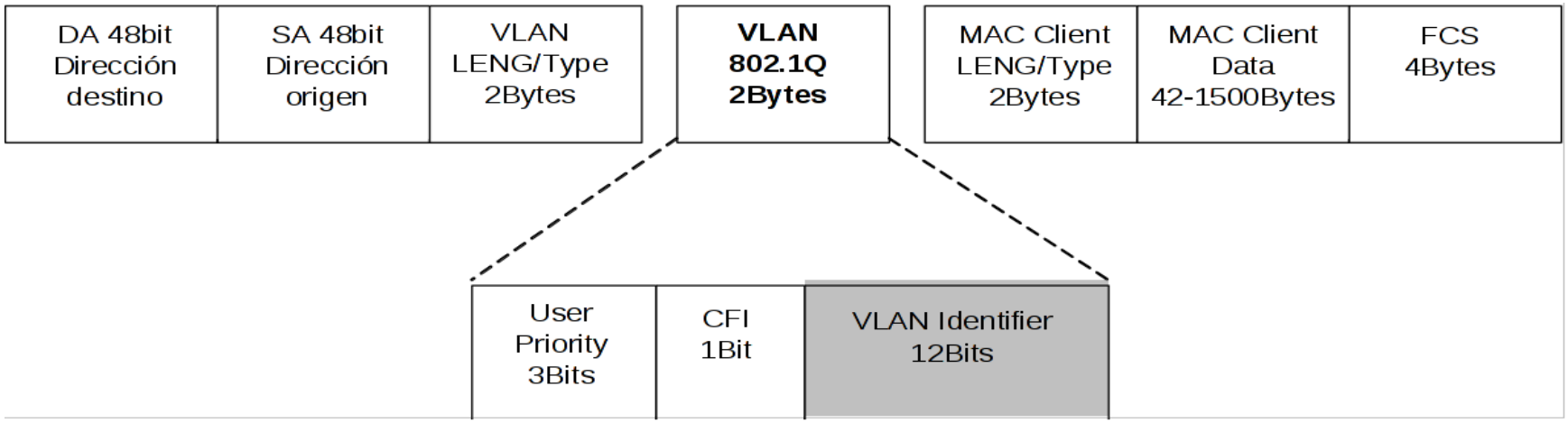
- 802.1Q añade dos campos de información a la trama MAC Ethernet original. Estos campos son empleados para identificar la VLAN de origen.



- TPID. Es la etiqueta de identificación de protocolo, que indica que sigue una etiqueta TCI (VLAN LENG/Type). Tiene siempre el valor 0x8100 que indica que lo que sigue es el TCI.

- TCI. Contiene el User Priority, indicador canónico de formato y VLAN ID (VLAN 802.1Q)

Trama Ethernet con extensión 802.1q



- VLAN identifier. Permite con sus 12 Bits distinguir hasta 4096 redes virtuales distintas. Informa sobre la VLAN de origen.
- Canonical Format Indicador CFI. Este bit no es empleado por los dispositivos Ethernet y siempre es puesto a 0. (Se utiliza para Token Ring).
- User Priority. Mediante estos tres bits, se establece el nivel de prioridad de tratamiento para la trama. Es posible distinguir hasta ocho niveles. La prioridad mas baja corresponde al 0. El uso de este campo está descrito en la norma 802.1p.

Es necesario tener en cuenta que los adaptadores de red de estaciones y servidores no precisan soportar 802.1Q. La etiqueta 802.1Q es colocada y eliminada por el conmutador.

Tipos de conexiones

Los equipos en una red virtual (VLAN) se pueden conectar en base a dos criterios:

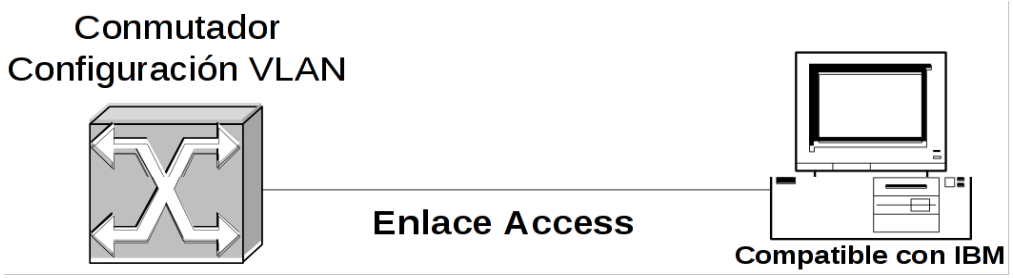
- Equipos que “entienden la pertenencia a una VLAN” como pueden ser los conmutadores y routers y

- equipos que “No entienden la pertenencia a una VLAN” como son las estaciones de trabajo, impresoras, servidores, etc.

Access vs Trunk

Enlace Trunk: Todos los equipos conectados mediante un trunk deben "entender VLAN" y es el enlace utilizado para conectar conmutadores entre si y/o Routers. Los paquetes que viajan entre ambos equipos están etiquetados con 802.1Q.

Enlace Access: Conecta un equipo que "no entiende VLAN" como un PC a un equipo con configuración de VLAN como un conmutador. Este último se encarga de quitar o poner la etiqueta 802.1Q dependiendo si el paquete viaja hacia el PC (La quita) o desde el PC (La Pone). También se puede conectar a un puerto ACCESS un segmento de red,



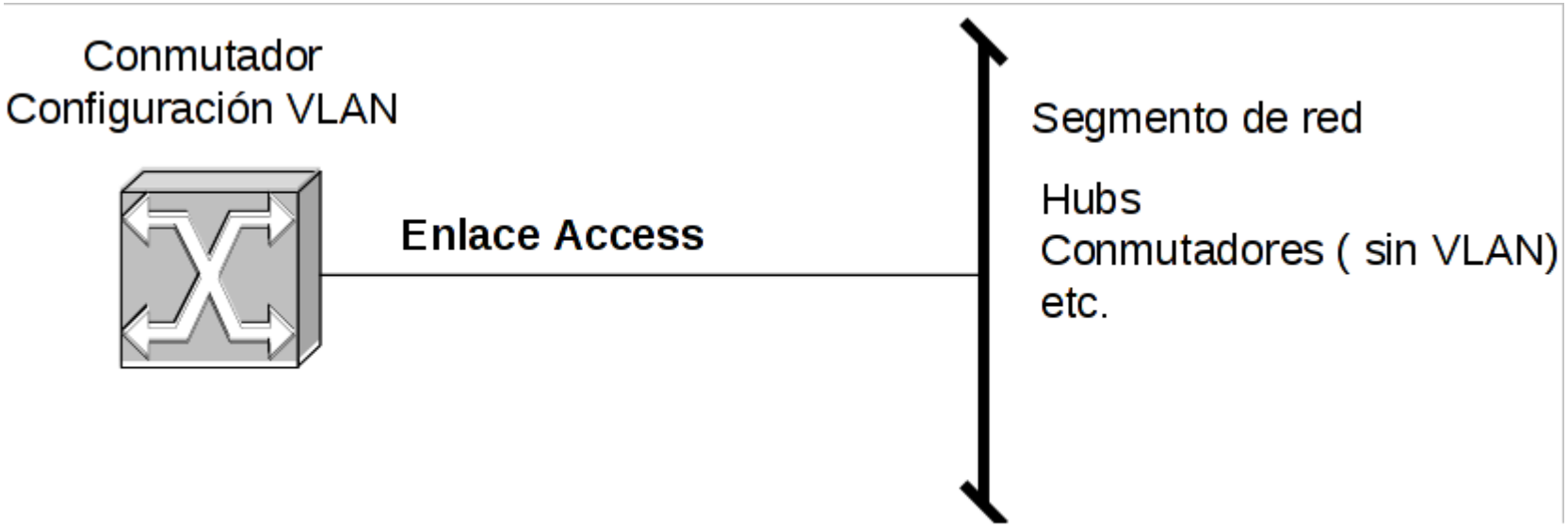
Características

Los puertos tipo access pueden tener varias VLANs, se suelen llamar “multi”.

Los puertos multi son incompatibles con los puertos Trunk.

También se puede conectar a un puerto ACCESS un segmento de red.

La VLAN con ID 1 está reservada como VLAN por defecto.



Características

- VLAN por defecto. Default VLAN es la VLAN en la que está asignada la CPU del propio conmutador. Este término suele confundirse con el PVID, aunque no son lo mismo, pues la VLAN por defecto está referida a todo el conmutador, y el PVID está referido a un puerto.

- PVID. El PVID es el VLAN_ID configurado para ese puerto específico. El valor del PVID dependerá del tipo de puerto al que se le asigne:

* *Puerto Access:* el PVID es el mismo que el VLAN_ID asignado a ese puerto.

* *Puerto Trunk:* el PVID se configurará manualmente para asignar un VLAN_ID a todas las tramas entrantes que no lleven etiqueta 802.1Q. Se considera una buena práctica que el PVID sea el mismo que la VLAN por defecto, o que este no se asigne.