

**TEMA 118. REDES DE ÁREA LOCAL.
ARQUITECTURA. TIPOLOGÍA. MEDIOS DE
TRANSMISIÓN. MÉTODOS DE ACCESO.
DISPOSITIVOS DE INTERCONEXIÓN. GESTIÓN DE
DISPOSITIVOS. ADMINISTRACIÓN DE REDES LAN.
GESTIÓN DE USUARIOS EN REDES LOCALES.
MONITORIZACIÓN Y CONTROL DE TRÁFICO.
GESTIÓN SNMP. CONFIGURACIÓN Y GESTIÓN DE
REDES VIRTUALES (VLAN). REDES DE ÁREA
EXTENSA.**

Actualizado a 12/09/2020

1. REDES DE AREA LOCAL

- Generalmente son de tipo BROADCAST
- Ejemplo red Ethernet: 10Mbps-10Gbps
- Estándares
 - Ethernet: 802.3
 - Token Bus: 802.4
 - Token Ring: 802.5

1.1. REDES DE ÁREA LOCAL

El estándar más conocido para redes de área local, Redes LAN Ethernet (802.3)

REDES LAN ETHERNET (802.3)

- Características
 - Topología física en ESTRELLA y topología lógica en BUS
 - Capa de enlace se divide en MAC y LLC
 - Método de acceso al medio: CSMA/CD
 - Tramas de 64-1518 bytes
 - Medios de transmisión: coaxial, UTP/STP, FO,...
 - Cada equipo tiene una dirección MAC única de 48 bits
 - Velocidades: 10 Mbps – 10 Gbps
- Especificaciones Ethernet según velocidad **[velocidad][modulación][medio de tx]**

10Mbps	100Mbps Fast Ethernet (802.3u)	1Gbps	10 Gbps	Medio de transmisión
10 BASE T	100 BASE TX	1000 BASE T	10 GBASE T	Cable UTP/STP > Cat5 UTP6 (10 Gbps)
	100 BASE FX	1000 BASE LX	10 GBASE LX4	Cable FO

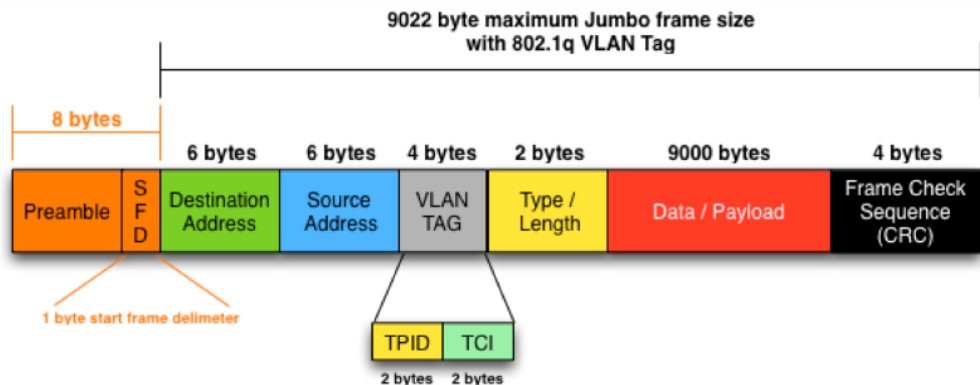
- Subniveles de enlace 802.3
 - **Capa LLC (Logical Link Control)**
 - Identifica el protocolo de la capa de red
 - Control de errores y control de flujo
 - Envía la trama al subnivel MAC
 - **Capa MAC (Media Access Control)**
 - Encapsulación de datos: delimitación de tramas, direccionamiento y detección de errores
 - Control de acceso al medio: gestiona la transmisión de info sobre el medio y la recuperación en caso de colisiones
- Trama Ethernet
 - Tamaño MÍN 64 bytes (sin preámbulo ni etiqueta)
 - Tamaño MÁX 1518 (sin preámbulo ni etiqueta)
 - Formato trama:
 - Preámbulo para sincronizar SFD (Start Frame Delimiter): 1B

- MAC destino: 6B
- MAC origen: 6B
- Tipo o Longitud: varias normas por lo que puede tomar valores distintos (tipo IP, trama etiquetada, ARP, IPv6,...)
- Payload (carga útil de datos): de 46 a 1500 bytes
- CRC de todo el datagrama: 4B
- Etiqueta opcional (4B): 802.1q
- Hay dos estilos de tramas de Ethernet: el estándar DIX Ethernet, que ahora es Ethernet II, y el estándar IEEE 802.3

Comparación del tamaño del campo y las estructuras de tramas de Ethernet y 802.3



- **JUMBO FRAMES** → MTU de 9000 bytes



- Dirección MAC
 - Tamaño 48 bits
 - Normas IEEE para identificar el fabricante en cada tarjeta MAC

TÉCNICAS DE ACCESO AL MEDIO

- **Técnicas por selección**
 - Sondeo (polling) (nodo que sondea al resto para ver quién transmitirá)
 - Paso de testigo (reserva distribuida)
- **Técnicas por contienda:**

- Aloha puro
- Aloha ranurado
- **Técnicas por contienda con escucha (CSMA)**
 - acceso múltiple con detección de portadora (**CSMA, Carrier Sense Multiple Access**)
 - Mecanismos para resolver las colisiones: CSMA/CD (Ethernet→detecta colisiones) y CSMA/CA (wifi)
 - **CSMA 1-Persistente:** si el canal está ocupado, espera escuchando el canal y transmite si está libre.
 - **CSMA NO PERSISTENTE:** si el canal está ocupado, espera un tiempo aleatorio para volver a escuchar
 - **CSMA p-PERSISTENTE:** si el canal está ocupado, transmite con una **probabilidad p** o espera con una **probabilidad (1-p)**

1.2. DISPOSITIVOS DE INTERCONEXIÓN

Conceptos:

- Dominio de colisión
- Dominio de difusión

INTERCONEXIÓN A NIVEL DE ENLACE. Puentes/BRIDGES

- Captura las tramas de un segmento de red y las reenvía selectivamente a otro segmento de la red
- Conecta dos segmentos de red y operan a nivel MAC
- Objetivos:
 - Interoperabilidad de redes heterogéneas (ejemplo: Red Ethernet y Token Ring)
 - Unión de dos tipos de medios físicos distintos (ejemplo: UTP y FO)
 - Fiabilidad
 - Seguridad, en una red local cq ordenador en modo PROMISCOUO puede ver todas las tramas → al segmentar evita que se vean fuera de la red
- Tipos de puentes
 - Puentes con encaminamiento desde el origen: las estaciones deben indicar el camino que seguirá la trama
 - Puentes transparentes: no requiere modificación alguna en las estaciones

PUENTES Transparentes

- Funcionan de manera transparente para el resto de los dispositivos.
- Funcionan en modo PROMISCOUO.
- Cada interfaz tiene una dirección MAC.
- El puente propiamente tiene una dirección propia → DIRECCIÓN CANÓNICA.
- Sólo reenvía una trama de un segmento a otro si:
 - Las tramas van a un segmento de red distinto de la estación origen
 - Las tramas tienen una dirección de grupo
 - Las tramas tienen un destino desconocido para el puente

CONMUTADORES/SWITCHES

- Interconecta múltiples segmentos a nivel de enlace.
- Formas de conmutación de tramas
 - **Almacenamiento y reenvío**
 - **Cut-through**
 - **Cut-through libre de fragmentos**
 - **Híbrido**: mira la frecuencia de envío de tramas erróneas. Si supera un umbral prefijado para a modo Almacenamiento y reenvío

REDES ETHERNET CONMUTADAS (SWITCHED LANS)

- Son redes basadas en switches , con mayor rendimiento que redes basadas en puentes
- Mejoras por el uso de switches en redes Ethernet: TRANSMISIÓN EN FULL-DUPLEX

1.3. CONFIGURACIÓN Y GESTIÓN DE REDES VIRTUALES (VLAN).

VLAN

Agrupación lógica, definida en uno o más switches conectados, de un conjunto de dispositivos y estaciones de red permite agrupación lógica, aunque las estaciones estén separadas físicamente.

Redes Ethernet Conmutadas → permiten crear REDES VIRTUALES/VLANs

Modos de definir VLAN:

- VLAN ESTÁTICA. Asignación de puertos.
- VLAN DINÁMICA. Se gestionan desde una aplicación, normalmente según la dirección MAC (también puede hacerse por dirección IP, tipo de protocolo,...) podrían conectarse estaciones de VLANs distintas a un mismo puerto
- VTP (VLAN Trunking Protocol) : protocolo propietario de CISCO que permite una gestión centralizada de todas las VLAN

ETIQUETADO

- Tramas de diferentes VLANs → añade etiqueta en cabecera de la trama MAC
- IEEE 802.1Q añade etiqueta de 4 bytes a trama Eth máximo de 1522 bytes
- IEEE 802.1Q define además protocolo MSTP (Multiple Spanning Tree Protocol) extensión de RSTP para usar en organizaciones donde hay definidas más de una VLAN.

TIPOS DE VLANs:

- **VLAN de nivel 1** (por puerto o “port switching”) : se especifica qué puertos del switch pertenecen a la VLAN. No permite la movilidad de los usuarios, habría que reconfigurar las VLAN si el usuario se mueve físicamente. Es lo común.

- **VLAN de nivel 2 por direcciones MAC:** se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar si por ejemplo el usuario se conecta a otro puerto. Pero hay que asignar los miembros uno a uno.
- **VLAN de nivel 2 por tipo de protocolo.** La VLAN queda determinada por el contenido del campo tipo de protocolo de la trama MAC. Por ejemplo, se asociaría VLAN 1 al protocolo IPv4, VLAN 2 al protocolo IPv6, VLAN 3 a AppleTalk, VLAN 4 a IPX...
- **VLAN de nivel 3 por direcciones de subred** (subred virtual).
- VLAN de niveles superiores. Se crea una VLAN para cada aplicación-

STP (SPANNING TREE PROTOCOL)

- Protocolo de Ethernet para VLAN. Estandarizado por IEEE 802.1d
- Protocolo de nivel 2 que gestiona la presencia de bucles por enlaces redundantes
- Se basan en la definición de un único camino entre dos nodos
- Se basa en el intercambio de BPDUs (Bridge Protocol Data Units)
- Estados de los puertos:
 - Bloqueo: en este estado se pueden recibir BPDU's pero no las enviará.
 - Escucha: los switches determinan si existe alguna otra ruta hacia el puente raíz. Se procesan las BPDU.
 - Aprendizaje: las tramas de datos se descartan pero ya se actualizan las tablas de direcciones MAC. Se procesan las BPDU.
 - Envío: en este estado el puerto puede enviar y recibir datos. Las tramas de datos se envían y se actualizan las tablas de direcciones MAC. Se procesan las BPDU.
 - Desactivado: a este estado se llega desde cualquier otro. Se produce cuando un administrador deshabilita el puerto o éste falla. No se procesan las BPDU.

RSTP (RAPID STP)

Estandarizado por IEEE 802.1w y mantiene la compatibilidad con STP

Reduce significativamente el tiempo de convergencia. Permite 2048-4096 puertos conectados

Estado de los puertos:

- **Learning:** Escucha BPDUs y guarda información relevante.
- **Forwarding:** Una vez ejecutado el algoritmo para evitar bucles, los puertos activos pasan a este estado.
- **Discarding:** No recibe BPDUs por lo cual no se encuentra participando en la instancia activa de STP

MSTP (MULTIPLE STP)

Estandarizado por IEEE 802.1s

Introduce el concepto de REGIÓN: grupo de switches con el mismo ID y VLAN asignada

INTERCONEXIÓN A NIVEL DE RED. ENCAMINADORES/ROUTERS

Características:

Permite la interconexión de redes de área local separadas físicamente



Separa DOMINIOS DE COLISIÓN y DOMINIOS DE BROADCAST

Utiliza esquema de direccionamiento IP

Ventajas sobre switches: opciones de filtrado y conmutación más potentes

1.4. ADMINISTRACIÓN. MODELO DE GESTIÓN DE REDES

FCAPS

- **Fault** Management
- **Configuration** Management
- **Accounting** Management
- **Performance** Management
- **Security** Management

GESTIÓN SNMP

Modelo de gestión de red de Internet (IETF)

Elementos:

- Lenguaje **SMI (Structure of Management Information)**:
 - **Basado en ASN.1**
- **MIB-I estándar, MIB-II de cada fabricante, MIB propietarias**
- **Protocolo SNMP (Simple Network Management Protocol)**

PROTOCOLO SNMP (Simple Network Management Protocol)

- Protocolo de capa de **APLICACIÓN**
- Define los mensajes entre agentes-gestores → **SOBRE UDP**
 - Puerto **UDP 161 y UDP 162 (Trap)**
- Versiones
 - **SNMP v1**
 - Modo pregunta-respuesta sobre protocolo de transporte NOC → UDP
 - También se permiten TRAPS desde el agente al gestor para notificar eventos
 - NO permite recuperar grandes bloques de info del agente
 - Operaciones:
 - GetRequest
 - GetNextRequest
 - Response
 - SetRequest
 - Trap
 - **SNMP v2**

- Nuevas operaciones:
 - GetBulk
 - Inform
 - Report
- **SNMP v3**
 - Nuevos mecanismos de seguridad:
 - Modelo de control de acceso basado en vistas o **VCAM** (Views-Based Access Control Model)
 - Seguridad basada en usuario (**USM**, User-based Security Model)

RMON (Remote MONitoring MIB):

- MIB que amplía las funcionalidades de la MIB-II sin necesidad de cambios en el protocolo SNMP
- MIB que permite al gestor delegar la monitorización en agentes especiales → **Sondas RMON** → reduciendo el tráfico de red
- Sonda RMON y RMON → comunicación mediante **mensajes SNMP**
- Versiones:
 - **RMON v1**, permite la monitorización a nivel físico y de enlace (MAC) → nivel 2
 - **RMON v2**, permite la monitorización de segmentos de redes LAN y el chequeo de tráfico a nivel de red (IP) y de aplicación → **monitorizar la red, no sólo los dispositivos (nivel 3)**
- Ventajas:
 - Funciona off-line
 - Disminuye tráfico de red
 - Detección y reporte de fallos
 - Datos con valor agregado
 - Múltiples Gestores de red
- SMON (Switched MONitoring)
 - capaz de gestionar los dispositivos de red y VPNs

MODELO DE GESTIÓN OSI/IEC

Recomendaciones del UIT-T X.700 y X.701

Elementos:

- **MIB** (Management Information Base)
 - Información sobre el objeto gestionado
 - Estructura en forma de árbol
- Servicios de gestión **CMIS** (Common Management Information Service)
- Protocolo **CMIP** (Common Management Information Protocol)
 - Equivalente OSI de SNMP pero más complejo
- Protocolo **CMOT** (Common Management Over TCP/IP) → intento de extender el modelo de gestión OSI a redes TCP/IP → fracaso

MODELO DE RED MTNM (MULTI-TECNOLOGY NETWORK MANAGEMENT)

Para gestión de redes de transporte PDH y SDH → se ha ampliado para redes ATM, DWDM, Ethernet

Recomendaciones M.3170.x

SOFTWARE DE GESTIÓN DE REDES Y SISTEMAS

- Nagios
- BMC Patrol
- Pandora FMS
- Zabbix
- DUDE
- Cisco Prime NCS (Network Control System)
- Solarwinds
- MRTG
- PRTG Network Monitor
- Zenoss
- Monitis
- OpenNMS
- Icinga (se basa en Nagios)
- Opsview
- IBM Tivoli Monitoring
- HP Systems Insight Manager
- ...