# Protocolos y Redes

Profesor: Ing. Luis Manuel Morales Medina

Cel. 3317388741

## Temario

### Modulo 1

1. Modelo OSI
2. Justificacion de un modelo de referencia
3. Capa Fisica
4. Capa de enlace
5. Capa de red
6. Capa de transporte
7. Protocoles TCP
8. Protocolo UDP
9. Analisis Comparativo TCP y UDP
10. Capa de que sision
11. Capa de presentacion
12. Capa de aplicacion

### Modulo 2

1. Modelo TCP IP
2. Capa de red
3. Capa de internet
4. Capa de transporte
5. Capa de aplicacion
6. Comparativa con el modelo OSI

### Modulo 3

1. Desarrollo de aplicaciones en red
2. Arquitectura cliente - servidor
3. Caracteristicas y responsabilidades del servidor
4. Implementacion de un servidor TCP
5. Caracteristicas y responsabilidades del cliente
6. Implementacion de un cliente TCP
7. Extendiendo el modelo para multiples clientes
8. Manejo de multiples estados
9. Arquitectura Peer to Peer (P2P)
10. Funcion del servidor en P2P
11. Caracteristicas de los clientes P2P

### Modulo 4

1. Desarrollo de juegos en red
2. Diferencias de diseño con un juego local
3. Planeacion de un juego en red
4. Diseño del protocolo a utilizar
5. Serializacion del estado
6. Sincronizacion del estado
7. Diseño de un servidor para multiplayer
8. Manejo de sesiones
9. Diseño de los clientes
10. Pruebas de un juego en red

# Evaluacion

- Parcial 1: Modulo 1 y 2
- Parcial 2: Modulo 3
- Parcial 3: Modulo 4
- Examen 30%
- Proyecto 30%
- Tareas 30%
- Ejercicios 10%

---

# Tema 1: Justificacion del modelo de referencia

La primera forma de comunicacione fue el telegrafo, el cual funcionaba por medio de pulsos, este solo podia ser utilizado de una persona a la vez ya que si no, los pulsos se distorcionaban.

La ISO (Organizacion Mundial de estandares) creo un modelo de referencia llamado OSI, este modelo funciona por medio de 7 capas que estan establecidas para el funcionamiento del mismo.

La justificacion es que simplemente se esta abstrayendo la manera de comunicacion para plasmarlo en una computadora.

### TAREA 1:

### Modelo OSI

Que es una red?

Se le llama red, a un conjunto de dispositivos o computadoras que estan conectados entre si, su finalidad es poder compartir recursos entre ellos que facilitan y optimizan las tareas del usuario.

Por los años 80 las redes crecian sin control, no existian ningun estandar para estas redes. Por lo tanto surge el modelo OSI, este modelo es creado por la ISO (Organizacion Internacional de estandarizacion), esta misma creo un estandar que se debe de seguir para que todas la empresas se puedan comunicar sin redes independientes.

En el modelo OSI existen 7 capas:

1. **Aplicacion:** Procesos de red a aplicaciones
    - Proporciona servicios de red a procesos de aplicacion (mail, ftp, ...)

2. **Presentacion:** Representacion de datos
    - Asegura que el sistema receptor pueda leer los datos.
    - Formato de los datos.
    - Estructuras de los datos
    - Negociar la sintacis de transferencia de datos de la capa de aplicacion
3. **Sesión:** Comunicacion entre host (equipos)
4. **Transporte:** Comunicacion de extremo a extremo
    - Segmenta la infromacion en pequeños paquetes de datos TCP u UDP.
5. **Red:** Direccionamiento y mejor ruta
6. **Enlace de datos:** Acceso a los medios
7. **Física:** Transmisión binaria

Se lee desde la capa superior hacia la inferior cuando el mensaje va a salir y desde la inferior a la superior cuando el mensaje va a entrar.

Este modela representa el conjunto de pasos que hace posible la comunicacion entre dispositivos.

## Proyecto Arpanet

En 1968 el departamento de defensa de los estados unidos fue encargado de crear una red militar ya que temian que rusia los atacase y robara su informacion. Asi que se cre un departamento especial llamado "ARPA", esta crearia una red solida para proteger su informacion.

Arpanet significa Red de la agencia de proyector de investigacion avancazada, BMN se encargo de realizar este proyecto mandando un mensaje de la universidad de california a la universidad de stanford ("Login"), tras dos años ya existian mas de 40 computadoras conectadas, para 1971 Ray Tomlinson crea un softer de envio - recepcion de correos electronicos, a las computadoras se les llamo procesadores de interfaz de mensajes (IMB), en 1972 arpanet se cambia el nombre a DARPA y se realiza la primera demostracion publica, en 1976 se establece el protocolo llamado x25 para la transmision de paquetes conmutados en redes oublicas, en 1981 IMB prensenta las primeras computadoras personales, vendiendo mas de 4000 computadoras en el primer mes.

En 1991 Robert Kaiju, quien ayudo con la realizacion de Arpanet decide ponerle al proyecto World Wide Web (WWW), en 1990 la sociedad se estaba conectando a arpanet pero no estaba diseñado para eso, por lo que se creo el protocolo TCP IP, despues de esto Arpanet se transformo en Internet, el cual facilito las interconecciones y dio origen a las graficas simple (imagenes), este nuevo protocolo hizo que creciera exponencialmente.

Arpanet esta creada principalmente para la proteccion de la informacion, sin embargo, se creo un beneficio mundial ya que fue el pionero de internet.

## Implicaciones de la guerra fria y de la Segunda Guerra Mundial en la tecnologia

- Colossus: Fueron los primeros dispositivos calculadores electronicos usados por los britanicos para leer las comunicaciones cifradas de los alemananes. (Segunda Guerra)
- Cintan transportadora de papel: La maquina de Lorenz fue utilizada para cifrar comunicaciones militares alemandas de alto nivel durante la segunda guerra mundial.
- ENIAC (Electronic Numerical Integrator And Computer): Utilizada por el laboratorio de investigacion Balistica del ejercito de los Estados Unidos. Se considera la primera computadora de proposito general junto con colossus.

- Sputnik 1: Es el primer satelite artificial de la historia, crado por la union sovietica en 1957.
- NASA: Se crea en 1958 para la investigacion aeroespacial.

## TAREA 2:

## IEEE: Protocolo 802

IEEE (Institute of Electrical and Electronics Engineers) 802 es un proyecto que se identifica tambien por las siglas LMSC (LAN/MAN standard committee). Este se encarga de desarrollar estandares de red en area local (LAN) y redes de area metropolitana (MAN), este se encuentra en las dos capas inferiores del sistema OSI.

IEEE se manifiesta principalmente sobre las rede de computadora. Se refiere a IEEE 802 para referirse al estandar que se propone, algunos son:

- Ethernet (IEEE 802.3)
- Wi - Fi (IEEE 802.11)
- Bluetooth (IEEE 802.15), se esta intentando estandarizar.

Este se centra en subdividir el sugundo nivel, el de enlace, en dos sub niveles:

1. Enlace logico (LLC 802.2)
2. Control de acceso medio (MAC)

El resto de los estandares actuan en la capa fisica, como en el subnivel de acceso al medio.

En febrero de 1980 se formó en el IEEE un comité de redes locales con la intención de estandarizar un sistema de 1 o 2 Mbps que básicamente era Ethernet (el de la época). Le tocó el número 802. Decidieron estandarizar el nivel físico, el de enlace y superiores. Dividieron el nivel de enlace en dos subniveles: el de enlace lógico, encargado de la lógica de re-envíos, control de flujo y comprobación de errores, y el subnivel de acceso al medio, encargado de arbitrar los conflictos de acceso simultáneo a la red por parte de las estaciones.

Para final de año ya se había ampliado el estándar para incluir el **Token Ring** (red en anillo con paso de testigo) de IBM y un año después, y por presiones de grupos industriales, se incluyó Token Bus (red en bus con paso de testigo), que incluía opciones de tiempo real y redundancia, y que se suponía idóneo para ambientes de fábrica.

Cada uno de estos tres "estándares" tenía un nivel físico diferente, un subnivel de acceso al medio distinto pero con algún rasgo común (espacio de direcciones y comprobación de errores), y un nivel de enlace lógico único para todos ellos.

Después se fueron ampliando los campos de trabajo, se incluyeron redes de área metropolitana (alguna decena de kilómetros), personal (unos pocos metros) y regional (algún centenar de kilómetros), se incluyeron redes inalámbricas (WLAN), métodos de seguridad, comodidad, etc.

**Grupos de Trabajo**

| | | |
|---|---|---|
| Nombre | Descripción | Nota |
| IEEE 802.1 | Normalización de interfaz | |
| 802.1d | *Spanning Tree Protocol* | |
| 802.1p | Asignación de Prioridades de tráfico | |
| 802.1q | *Virtual Local Area Networks* (VLAN) | |
| 802.1x | Autenticación en redes LAN | |
| 802.1aq | *Shortest Path Bridging* (SPB) | |
| IEEE 802.2 | Control de enlace lógico (LLC) | Activo |
| IEEE 802.3 | CSMA / CD (ETHERNET) | |
| IEEE 802.3a | Ethernet delgada 10Base2 | |
| IEEE 802.3c | Especificaciones de Repetidor en Ethernet a 10 Mbps | |
| IEEE 802.3i | Ethernet de par trenzado 10BaseT | |
| IEEE 802.3j | Ethernet de fibra óptica 10BaseF | |
| IEEE 802.3u | Fast Ethernet 100BaseT | |
| IEEE 802.3z | Gigabit Ethernet parámetros para 1000 Mbps | |
| IEEE 802.3ab | Gigabit Ethernet sobre 4 pares de cable UTP Cat5e o superior | |
| IEEE 802.3ae | 10 Gigabit Ethernet | |
| IEEE 802.4 | Token bus LAN | Disuelto |
| IEEE 802.5 | Token ring LAN (topología en anillo) | Inactivo |

| | | |
|---|---|---|
| IEEE 802.6 | Redes de Área Metropolitana (MAN) (ciudad) (fibra óptica) | Disuelto |
| IEEE 802.7 | Grupo Asesor en Banda ancha | Disuelto |
| IEEE 802.8 | Grupo Asesor en Fibras Ópticas | Disuelto |
| IEEE 802.9 | Servicios Integrados de red de Área Local (redes con voz y datos integrados) | Disuelto |
| IEEE 802.10 | Seguridad de red | Disuelto |
| IEEE 802.11 | Redes inalámbricas WLAN. (Wi-Fi) | |
| IEEE 802.12 | Acceso de Prioridad por demanda 100 Base VG-Any Lan | Disuelto |
| IEEE 802.13 | Se ha evitado su uso por superstición2 | Sin uso |
| IEEE 802.14 | Módems de cable | Disuelto |
| IEEE 802.15 | WPAN (Bluetooth) | |
| IEEE 802.16 | Redes de acceso metropolitanas sin hilos de banda ancha (WIMAX) | |
| IEEE 802.17 | Anillo de paquete elástico script | |
| IEEE 802.18 | Grupo de Asesoría Técnica sobre Normativas de Radio | En desarrollo a día de hoy |
| IEEE 802.19 | Grupo de Asesoría Técnica sobre Coexistencia | |
| IEEE 802.20 | *Mobile Broadband Wireless Access* | |
| IEEE 802.21 | Media Independent Handoff | |
| IEEE 802.22 | *Wireless Regional Area Network* | |

## Porque no se estaba de acuerdo con el protocolo 802?

Salio al mismo tiempo que la OSI.

## Que es VPN?

VPN (Virtual Private Network), **una privada virtual capaz de conectar varios dispositivos como si se encontrasen físicamente en el mismo lugar**, emulando las conexiones de redes locales. Virtual, porque conecta dos redes físicas; y privada, porque solo los equipos que forman parte de una red local de uno de los lados de la VPN pueden acceder.

Funcion

Al conectarnos a una VPN, lo haremos utilizando **una suerte de túnel**, un vocablo que se emplea para indicar que los datos se encuentran cifrados en todo momento, desde que entran hasta que salen de la VPN, y que se lleva a cabo mediante distintos protocolos que los protegen. Ahora bien, existe una excepción con el PPTP –utiliza una combinación de algoritmos inseguros como MS-CHAP v1/2-.

Lo que hará nuestro sistema al tratar de visitar una página es **encapsular la petición** y mandarla a través de Internet a nuestro proveedor de VPN. Este los desencapsulará haciendo que sigan su curso habitual: saldrán por su router de red y, posteriormente, se reenviará el paquete.

Ventajas

Usar una VPN implica que podremos acceder a prácticamente cualquier lugar de la red sin ningún tipo de restricción geográfica, **sin importar dónde nos encontremos físicamente**. ¿La razón? Que nos permitirá acceder a través de varios servidores emplazados en otro lugar del mundo distinto al que nos hallamos.

La **seguridad y privacidad** son otros puntos a su favor, en especial si necesitamos enviar o recibir información de carácter sensible a través de la red. Y si bien siempre podemos decantarnos por servicios proxy y herramientas que ocultan la IP de nuestro dispositivo, al decantarnos por una VPN estamos escogiendo establecer una conexión segura entre el ordenador y el servidor.

Ya **en un contexto más empresarial**, hace posible que los empleados de una compañía **accedan remotamente a sus redes y servidores** sin que se vea comprometida la seguridad. Otra de sus virtudes es que no se trata de servicios demasiado caros y que incluso encontramos opciones que merecen la pena de manera gratuita.

## Zona desmilitarizada

Es un nivel de acceso, se esta ahislando un grupo de otro.

## Firewall

Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.

Un firewall puede ser hardware, software o ambos.

Tipos de FireWall

**Firewall proxy**

Un firewall proxy, uno de los primeros tipos de dispositivos de firewall, funciona como gateway de una red a otra para una aplicación específica. Los servidores proxy pueden brindar funcionalidad adicional, como seguridad y almacenamiento de contenido en caché, evitando las conexiones directas desde el exterior de la red. Sin embargo, esto también puede tener un impacto en la capacidad de procesamiento y las aplicaciones que pueden admitir.

**Firewall de inspección activa**

Un firewall de inspección activa, ahora considerado un firewall "tradicional", permite o bloquea el tráfico en función del estado, el puerto y el protocolo. Este firewall monitorea toda la actividad, desde la apertura de una conexión hasta su cierre. Las decisiones de filtrado se toman de acuerdo con las reglas definidas por el administrador y con el contexto, lo que refiere a usar información de conexiones anteriores y paquetes que pertenecen a la misma conexión.

**Firewall de administración unificada de amenazas (UTM)**

Un dispositivo UTM suele combinar en forma flexible las funciones de un firewall de inspección activa con prevención de intrusiones y antivirus. Además, puede incluir servicios adicionales y, a menudo, administración de la nube. Los UTM se centran en la simplicidad y la facilidad de uso.

**Firewall de próxima generación (NGFW)**

Los firewalls han evolucionado más allá de la inspección activa y el filtrado simple de paquetes. La mayoría de las empresas están implementando firewalls de próxima generación para bloquear las amenazas modernas, como los ataques de la capa de aplicación y el malware avanzado.

Según la definición de Gartner, Inc., un firewall de próxima generación debe incluir lo siguiente:

- Funcionalidades de firewall estándares, como la inspección con estado
- Prevención integrada de intrusiones
- Reconocimiento y control de aplicaciones para ver y bloquear las aplicaciones peligrosas
- Rutas de actualización para incluir fuentes de información futuras
- Técnicas para abordar las amenazas de seguridad en evolución

Si bien estas funcionalidades se están convirtiendo cada vez más en el estándar para la mayoría de las empresas, los NGFW pueden hacer más.

**NGFW centrado en amenazas**

Estos firewalls incluyen todas las funcionalidades de un NGFW tradicional y también brindan funciones de detección y corrección de amenazas avanzadas. Con un NGFW centrado en amenazas, puede hacer lo siguiente:

- Estar al tanto de cuáles son los activos que corren mayor riesgo con reconocimiento del contexto completo
- Reaccionar rápidamente ante los ataques con automatización de seguridad inteligente que establece políticas y fortalece las defensas en forma dinámica
- Detectar mejor la actividad sospechosa o evasiva con correlación de eventos de terminales y la red
- Reducir significativamente el tiempo necesario desde la detección hasta la eliminación de la amenaza con seguridad retrospectiva que monitorea continuamente la presencia de actividad y comportamiento sospechosos, incluso después de la inspección inicial

- Facilitar la administración y reducir la complejidad con políticas unificadas que brindan protección en toda la secuencia del ataque

## EJERCICIO 1

**IPV4**

IPV4 (Protocolo de Internet nivel 4), es un protocolo de interconexión de redes basados en internet y fue la primera versión implementada para la producción de Arpanet, en 1983. IPv4 usa direcciones de 32 bits, limitándola a

$$2^{32}$$

= 4 294 967 296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LAN).

**IPV6**

IPV6, posee direcciones con una longitud de 128 bits, es decir 2^128 posibles direcciones (340.282.366.920.938.463.463.374.607.431.768.211.456), o dicho de otro modo, 340 sextillones.

El despliegue de IPv6 se irá realizando gradualmente, en una coexistencia ordenada con IPv4, al que irá desplazando a medida que dispositivos de cliente, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet.

**IP Publica**

Una dirección IP está formada por **cuatro grupos de entre 1 y tres dígitos separados por puntos**, tienen una longitud de 32 bits y constan de dos campos, uno que es el identificador de red y corresponde con el primer grupo de números, y el identificador de host, que son los otros tres grupos restantes.

La **pública** es el identificador de nuestra red desde el exterior, es decir, la de nuestro router de casa, que es el que es visible desde fuera, mientras que la **privada** es la que identifica a cada uno de los dispositivos conectados a nuestra red, por lo tanto, cada una de las direcciones IP que el router asigna a nuestro ordenador, móvil, tablet o cualquier otro dispositivo que se esté conectado a él.

**Mac Address**

La Mac Address o dirección Mac **es una identificador único de 48 bits para identificar la totalidad de dispositivos de red** como por ejemplo tarjetas de red Ethernet, tarjetas de red wifi o inalambricas, Switch de red, Routers, impresoras, etc.

**La totalidad de fabricantes en el momento de fabricar el hardware**, como por ejemplo una tarjeta de red wifi, **graban la Mac Address en formato binario en una memoria ROM** del dispositivo que están fabricando. Como la memoria ROM es solo de lectura es totalmente imposible modificarla y **por lo tanto** esto implica que **la Mac address o identificador de un dispositivo nunca lo podremos modificar**. **No obstante** en futuros post veremos que **es posible hacer creer a otras personas o a integrantes de la red que nuestra MAC Address es otra diferente a la real.

El motivo por el cual es posible modificar la MAC de la tarjeta de red de nuestro ordenador es simple. Cuando se arranca nuestro ordenador la tarjeta de red copia la dirección MAC a nuestra memoria RAM. Una vez copiada la Mac Address a la memoria RAM la totalidad de veces que se requiere de la Mac Address se usará la Mac Address almacenada en la memoria RAM. Por lo tanto si queremos cambiar nuestra Mac Address tan solo tenemos que modificar la Mac Address almacenada en nuestra memoria RAM y esto si que es posible.

**Que es un puerto?**

Punto por donde se conecta la unidad central de la computadora con otros periféricos o aparatos externos, como la impresora, el módem, etc.

**Topologia de red**

La topología es el arreglo (físico o lógico) donde los dispositivos o nodos de una red, se interconectan sobre un medio de comunicación. La topología en una red determina la forma de comunicación entre sus nodos.La topología en una red determina la forma de comunicación entre sus nodos. Existen topologías donde la intercomunicación entre sus nodos es sencilla y otras donde es compleja. La mala elección de una topología puede ocasionar que la red no opere de manera eficiente. Una topología determina el número de nodos que se conectarán, el método de acceso múltiple, tiempo de respuesta, velocidad de la información, costo, tipo de aplicaciones, etcétera.

Las topologías pueden ser de dos tipos:

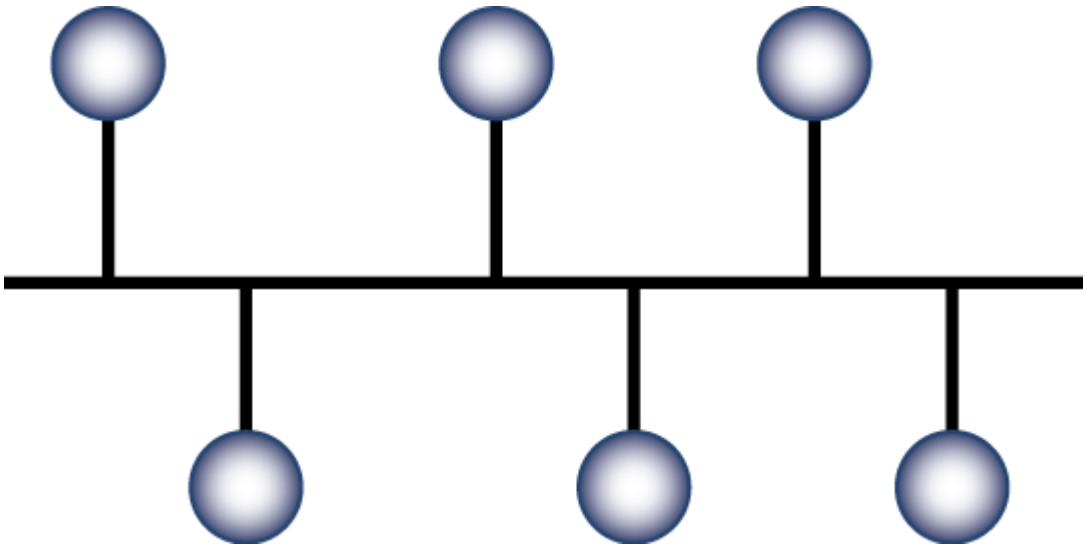
- *Topología física*: Se refiere al diseño actual del medio de transmisión de la red.
- *Topología lógica*: Se refiere a la trayectoria lógica que una señal a su paso por los nodos de la red.

**TOPOLOGÍA FÍSICAS** Las topologías físicas más comunes son: **ducto, estrella, anillo, malla y las híbridas**. Cada una de éstas tiene sus ventajas y desventajas, así como sus aplicaciones específicas.

**Topología de ducto (bus)**

Una topología de ducto o bus está caracterizada por una dorsal principal con dispositivos de red interconectados a lo largo de la dorsal. Las redes de ductos son consideradas como topologías pasivas. Las computadoras "escuchan" al ducto. Cuando éstas están listas para transmitir, ellas se aseguran que no haya nadie más transmitiendo en el ducto, y entonces ellas envían sus paquetes de información. Usualmente utilizan Ethernet.

En ambientes MAN (Metropolitan Area Network), las compañías de televisión por cable utilizan esta topología para extender sus redes.

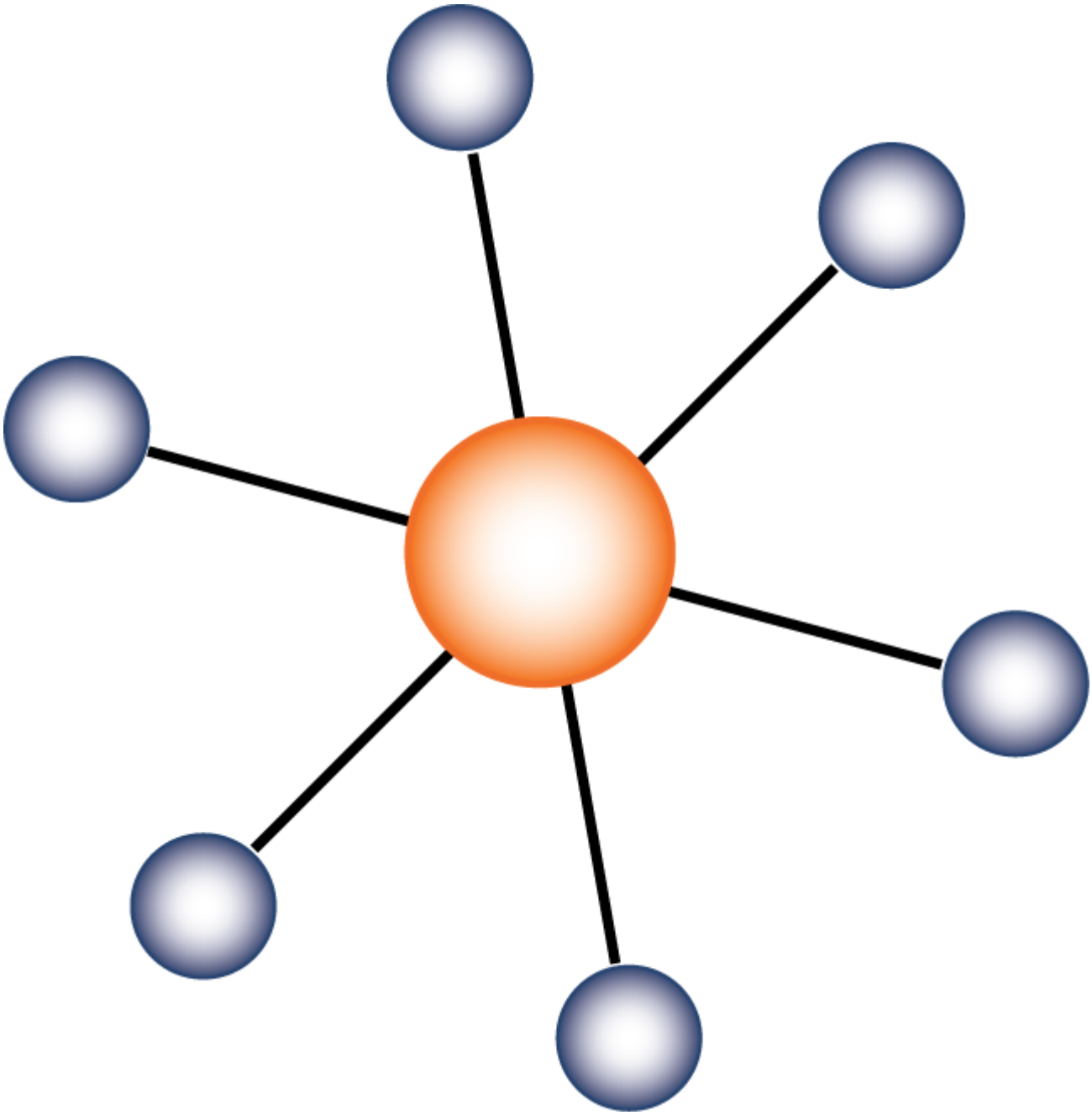


**Topología de estrella (star)**

En una topología de estrella, las computadoras en la red se conectan a un dispositivo central conocido como concentrador (hub en inglés) o a un conmutador de paquetes (swicth en inglés).

En un ambiente LAN cada computadora se conecta con su propio cable (típicamente par trenzado) a un puerto del hub o switch. Este tipo de red sigue siendo pasiva, utilizando un método basado en contensión, las computadoras escuchan el cable y contienden por un tiempo de transmisión.

Debido a que la topología estrella utiliza un cable de conexión para cada computadora, es muy fácil de expandir, sólo dependerá del número de puertos disponibles en el hub o switch (aunque se pueden conectar hubs o switchs en cadena para así incrementar el número de puertos). La desventaja de esta topología en la centralización de la comunicación, ya que si el hub falla, toda la red se cae.



La topología estrella extendida en un ambiente LAN es fácil de configurar, de costo accesible, y tiene más redundancia que la topología de ducto. En vez de conectar todos los dispositivos a un nodo central, los nodos se conectarán a otros dispositivos subcentrales, permitiendo más funcionalidad para establecer subredes y creando también más puntos de falla. Mientras la topología de estrella fue hecha para redes pequeñas, la topología estrella extendida se adapta mejor a redes grandes.

Un ejemplo aplicado de una **topología estrella extendida**, en un ambiente MAN, es la telefonía celular. El nodo central es el conmutador que se encarga de establecer la comunicación entre las terminales móviles. Al conmutador central se conectan vía enlace de microondas, las radiobases o antenas de telefonía celular. A su vez, las radiobases se conectan vía frecuencias de telefonía celular a las terminales móviles.

**Topología de anillo (ring)** Una topología de anillo conecta los dispositivos de red uno tras otro sobre el cable en un círculo físico. La topología de anillo mueve información sobre el cable en una dirección y es considerada como una topología activa. Las computadoras en la red retransmiten los paquetes que reciben y los envían a la siguiente computadora en la red. El acceso al medio de la red es otorgado a una computadora en particular en la red por un "token". El token circula alrededor del anillo y cuando una computadora desea enviar datos, espera al token y posiciona de él. La computadora entonces envía los datos sobre el cable. La computadora destino envía un mensaje (a la computadora que envió los datos) que de fueron recibidos correctamente. La computadora que transmitio los datos, crea un nuevo token y los envía a la siguiente computadora, empezando el ritual de paso de token o estafeta (token passing) nuevamente.

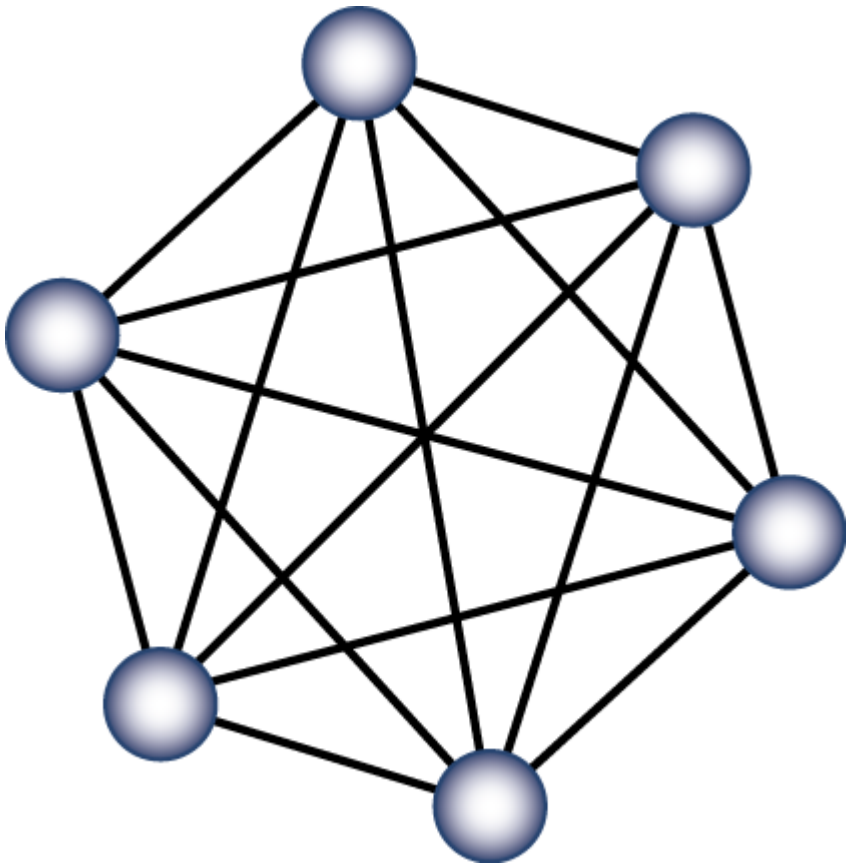
La topología de anillo es muy utlizada en redes CAN y MAN, en enlaces de fibra óptica SONET, SDH y FDDI en redes de campus.

**Topología de malla (mesh)**

La topología de malla (mesh) utiliza conexiones redundantes entre los dispositivos de la red aí como una estrategía de tolerancia a fallas. Cada dispositivo en la red está conectado a todos los demás (todos conectados con todos). Este tipo de tecnología requiere mucho cable (cuando se utiliza el cable como medio, pero puede ser inalámbrico también). Pero debido a la redundancia, la red puede seguir operando si una conexión se rompe.

Las redes de malla, obviamente, son mas difíciles y caras para instalar que las otras topologías de red debido al gran número de conexiones requeridas.

La red Internet utiliza esta topología para interconectar las diferentes compañías telefónicas y de proveedoras de Internet, mediante enlaces de fibra óptica.



## Tema 2: