Modulo 1
Componentes de Red

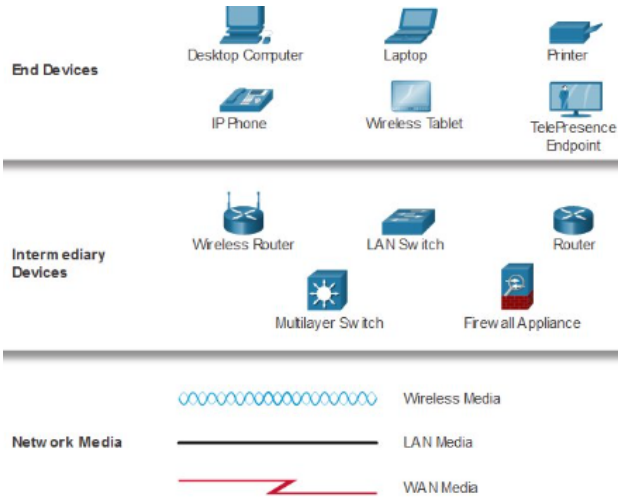
- Roles de host -> cada PC en una red -> host / dispositivo final
    - **Servidores** -> proporcionan info a dispositivos finales
        - de correo electronico
        - web
        - de archivos
    - **Clientes** -> envian solicitudes a los servidores para recuperar info
        - Pagina web desde un server web
        - correo desde un server correo
    - en de archivos -> server almacena archivos y cliente accede a archivos
- **Punto a Punto** -> 1 dispositivo sea servidor y cliente en 1 red -> para redes pequeñas

Ventajas	**Desventajas**
facil de configurar	admin no centralizada
menos complejo	no tan segura
reduce costos	no escalable
tareas simples -> transferir archivos y compartir impresoras	rendimiento mas lento

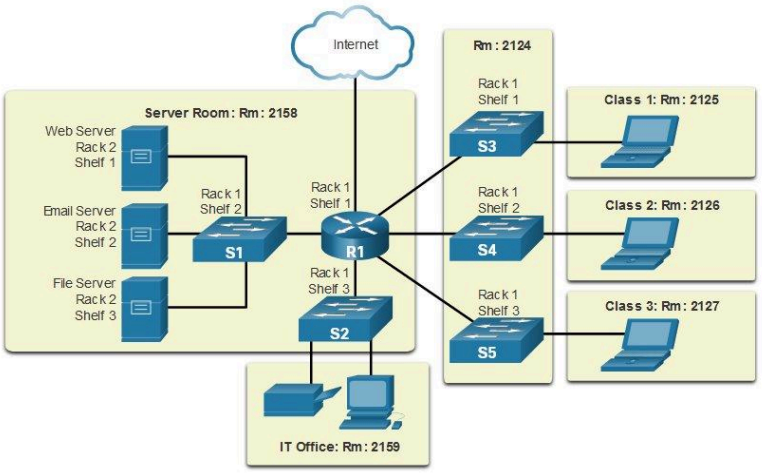
- **Dispositivos finales**
    - el punto donde un mensaje se origina o se recibe
    - datos -> se originan con un dispositivo final, fluyen por la red y llegan a un dispositivo final
- **Dispositivos de red Intermedios** -> interconecta dispositivos finales
    - gestionan datos a medida que fluyen a traves de una red
        - volver a generar y transmitir las señales de datos
        - mantener info -> qué vias existen en la red
        - notificar a otros dispositivos -> errores y fallas de comunicacion
- **Medios de Red** -> permite que un mensaje viaje de origen a destino
    - **Alambres de metal dentro de cables**
        - utiliza impulsos electricos
    - Fibras de vidrio o plastico dentro de los cables (**cable de fibra optica**)
        - usa pulsos de luz
    - **Transmision Inalambrica**
        - usa modulacion de frecuencias especificas de ondas electromagneticas

Representaciones de Red y Topologias

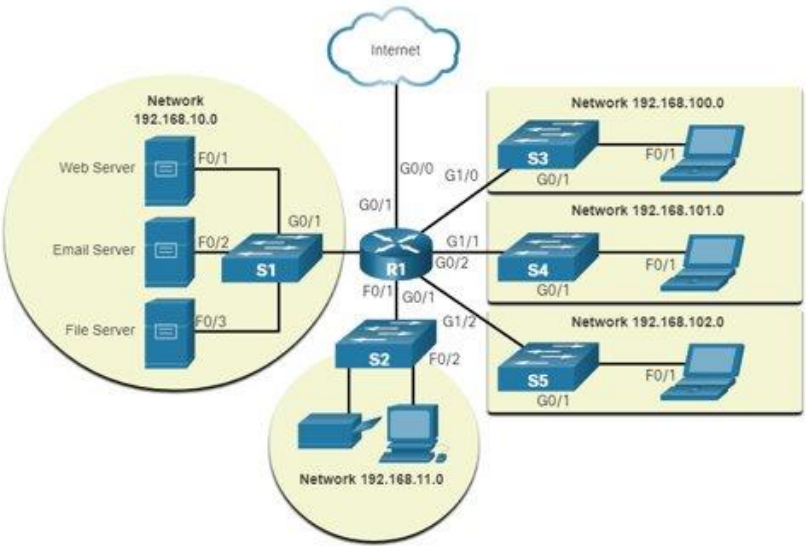
- Representaciones de Red
    - Terminos importantes
        - tarjeta de interfaz de red (NIC)
        - puerto fisico
        - interfaz



- **Diagramas de Topologia**
  - **Fisicos** -> ilustran la ubicacion fisica de los dispositivos intermedios y la instalacion de cables



  - **Lógicos** -> ilustran dispositivos, puertos y el esquema de direccionamiento de red



Tipos de Red -> Las **infra de red varian segun:**

- tamaño area a abarcar
- cant de usuarios conectados
- cant y tipos de servicios disponibles
- area de responsabilidad

LAN vs WAN

LAN	**WAN**
area geografica pequeña	area geografica extensa
interconecta dispositivos finales en un area limitada	interconecta LAN en amplias areas geograficas
admin por 1 sola org/individuo	Admin por +1 proveedores de servicios
proporciona ancho de banda de alta velocidad a dispositivos internos	proporciona enlaces de menor velocidad entre LANs

Internet -> coleccion mundial de LAN y WAN interconectadas

- LAN se conectran entre si mediante WAN
- WAN pueden usar
    - cables de cobre
    - fibra optica
    - transmisiones inalambricas

Intranet y Extranet

- **Intranet** -> coleccion privada de LAN y WAN internas de una org que debe ser accesible solo para los miembros de la org u otros con autorizacion
- **Extranet** -> proporciona acceso seguro a la red privada de una org por parte de personas que trabajan para otra org y que necesitan tener acceso a datos en su red

Conexiones a Internet

Tecnologias de Acceso a Internet

- servicios + usados x usuarios domesticos y pequeñas oficinas
    - **banda ancha pro cable**
    - **banda ancha por linea de suscriptor digital (DSL)**
    - **redes WAN inalambricas**
    - **servicios moviles**
- Organizaciones -> conexiones + rapidas para admitir los telefonos IP, las videoconferencias y el almacenamiento central de datos
- Proveedores de servicios -> proporcionan interconexiones de nivel empresarial y pueden incluir DSL empresarial, lineas arrendadas y Metro Ethernet

Home and Small Office

- Conexiones
    - **Cable** ->
        - internet de alto ancho de banda,

        - siempre encendido,
        - ofrecido por los proveedores de servicios de television por cable
    - **DSL**
        - ancho de banda alto,
        - siempre conectado
        - conexion a internet -> se ejecuta -> a traves de linea telefonica
    - **Red Celular**
        - red de telefonia celular para conectarse a internet
    - **Satelite**
        - beneficio para zonas rurales sin proveedores de servicio de internet
    - **telefono de marcacion**
        - opcion economica de bajo ancho de banda que utiliza un modem

Negocios

- Pueden requerir:
    - mayor ancho de banda
    - conexiones dedicadas
    - servicios gestionados
- Tipo de conexion
    - **Linea dedicada arrendada** -> circuitos reservados dentro de la red del proveedor de servicios que conectan oficinas distantes con redes privadas de voz y o datos
    - **WAN Ethernet** -> extiende logica de acceso LAN a la WAN
    - **DSL -> Business DSL -> SDSL (linea de suscriptor digital simetrico)**
    - **Satelite** -> proporciona una conexion cuando una solucion cableada no esta disponible

Red Convergente

- transportan multiples servicios en un enlace que incluyen: datos, voz, video -> a traves de la misma infraestructura de red -> usa el mismo conjunto de reglas y normas

Redes Confiables

Arquitectura de Red

- tecnologias que admiten la infra que mueve los datos a traves de la red
- **4 caracteristicas basicas**
    - **Tolerancia a fallas**
        - disminuye impacto de falla -> limita cant de dispositivos afectados
        - redes confiables -> proporcionan redundancia al implementar una red de paquetes conmutados
            - conmutacion x paquetes -> divide el trafico en paquetes que se enrutan a traves de una red
            - cada paquete puede tomar una ruta diferente hacia el destino -> no es posible con redes conmutadas x circuitos q establecen circuitos dedicados.

- **Escalabilidad** -> puede expandirse facil y rapido para admitir nuevos usuarios y nuevas apps sin afectar el rendimiento de los servicios de los users actuales.
- **Calidad de Servicio (QoS)**
  - ppal mecanismo q se usa para garantizar -> entrega confiable de contenido a los users
  - APlicando politica de QOS -> router admin facilmente el flujo de trafico de voz y de datos
- **Seguridad de la Red**
  - 2 tipos ppales:
    - **Seguridad de la infra de la red**
      - seguridad fisica de los dispositivos de red
      - Prevenir el acceso no autorizado a los dispositivos
    - **Seguridad de la info**
      - proteccion de la info o de los datos transmitidos a traves de la red
  - 3 objetivos de seguridad de la red
    - **Confidencialidad** .> solo destinatarios pueden leer los datos
    - **Integridad** - >garantia que no hubo modificacion de datos durante la transmision
    - **Disponibilidad** -> garantia del acceso confiable y oportuno a los datos x parte de los users autorizados

Tendencias de Red

- **BYOD** (bring your own device) -> users -> libertad de usar herramientas personales para comunicarse y acceder a info mediante dispositivos como: notebook, tablet, celu, kindle
- **Computacion en la Nube** -> gracias a los centros de datos
  - **Nubes Publicas** -> disponible para publico general -> gratis o paga
  - **Nubes Privadas** -> destinado a una org o entidad especifica como el gob
  - **Nubes Hibridas** -> compuesto por 2 o mas tipos de nubes -> cada parte es 1 objeto distinto pero conectadas con la misma arq
  - **Nubes Personalizadas** -> creado para satisfacer necesidades de una industria especifica -> privado o publico
- Redes de Linea Electrica
  - permiten que los dispositivos se conecten a una red LAN donde -> cables de red de datos o las comunicaciones inalambricas no son una opcion viable
- Banda Ancha Inalambrica

Seguridad de la Red

- Amenazas
  - Externas
    - Virus, gusanos y caballos de Troya
    - Spyware y adware
    - Ataques de dia 0
    - ataques de actores de amenazas
    - ataques por denegacion de servicios
    - Intercepcion y robo de datos

        - robo de identidad
    - Internas
        - dispositivos perdidos o robados
        - uso indebido accidental por parte de los empleados
        - empleados malintencionados
- Soluciones de Seguridad
    - En hogar o pequeñas oficinas
        - instalar antivirus y antispyware
        - filtrado de firewall para bloquear accesos no autorizados
    - Redes mas grandes
        - sistemas de firewall dedicado
        - listas de control de acceso **ACL**
        - sistemas de prevención de intrusiones **IPS**
        - redes privadas virtuales **VPN**

Modulo 2

Acceso a Cisco IOS
Sistemas Operativos

- Shell -> interfaz de user que permite a los users solicitar tareas especificas del equipo -> a traves de interfaces CLI o GUI
- Kernel -> establece com entre HW y SW -> admin uso de recursos de HW para SW
- HW -> parte fisica de una pc

CLI -> consola de comandos
GUI -> windows

- permite a user -> interactuar con el sistema usando un entorno de iconos graficos menus y ventanas
- no se suelen usar para acceder a los dispositivos de red

Metodos de Acceso

- COnsola
- Secure Shell (SSH) -> establece conexion CLI remota -> metodo recomendado
- Telnet -> establece conexion CLI insegura

Navegacion del IOS
Modos de comando ppales

- Modo EXEC de user
    - permite acceso solo a una cant limitada de comandos basicos de monitoreo
    - se identifica con “>”
- Priviliged EXEC mode:
    - permite acceso a todos los comandos
    - se identifica con “#”

Modo de Configuracion y de subconfig

- Modo de subconfig global -> para acceder a las opciones de config de dispositivo
- Modo de config de linea -> para config el acceso a la consola, SSH, Telnet o AUX
- Modo de config de interfaz -> para un puerto de switch o una interfaz de router

Estructura de comandos: palabra clave y argumentos

Modulo 3

Aspectos basicos de la comunicacion
- Remitente -> fuente
- Destino -> receptor
- Canal -> medio

Protocolos de Comunicacion
- todas las comunicaciones -> se rigen por protocolos
- protocolos -> reglas que seguiran las comunicaciones

Establecimiento de reglas
Requisitos de protocolos:
- emisor y receptor identificados
- idioma y gramatica en comun
- velocidad y momento de entrega
- req de info o acuse de recibo

Requisitos de protocolos informaticos (comunes):
- **codificacion de los mensajes**
  - proceso -> info se convierte en -> otra forma aceptable para la transmision
  - decodificacion -> revierte el proceso
- **formato y encapsulamiento del mensaje**
  - al transferir mensaje -> formato especifico
  - dependen de:
    - tipo de mensaje
    - canal de envio de mensaje
- **tamaño del mensaje**
- **sincronizacion del mensaje (temporizacion) incluye:**
  - **control de flujo**: admin velocidad de transmision de datos y define cant de info y velocidad a la que se puede entregar
  - **tiempo de espera de rta**: admin el tiempo que espera un dispositivo cuando no escucha una rta del destino
  - **metodo de acceso**: determina en que momento se puede enviar un mensaje
    - colisiones -> +1 dispositivo envia trafico al mismo tiempo -> se dañan los mensajes
    - metodo activo -> evitar colision
    - metodo reactivo -> recuperar de colision
- opciones de entrega del mensaje -> para IPv4 no IPv6
  - **unidifusion** -> 1 a 1
  - **multidifusion** -> 1 a muchos (no todos)
  - **difusion** -> 1 a todos

Protocolos
Se pueden implementar en hw, sw o ambos
Tienen sus propios:
- funcion

- formato
- medicion

Tipos:

- **Comunicaciones de red**: permitir q 2 o + dispositivos se comuniquen a traves de una o mas redes
- **Seguridad de redes**: datos seguros para proporcionar autenticacion, integridad de datos y cifrado de datos
- **tabla**: permitir que los routers intercambien info de ruta, comparen info de ruta y seleccionen la mejor ruta
- **deteccion de servicios**: usado para la deteccion automatica de dispositivos o servicios

Funciones:

- pueden tener 1 o mas
- los dispositivos usan protocolos acordados para comunicarse

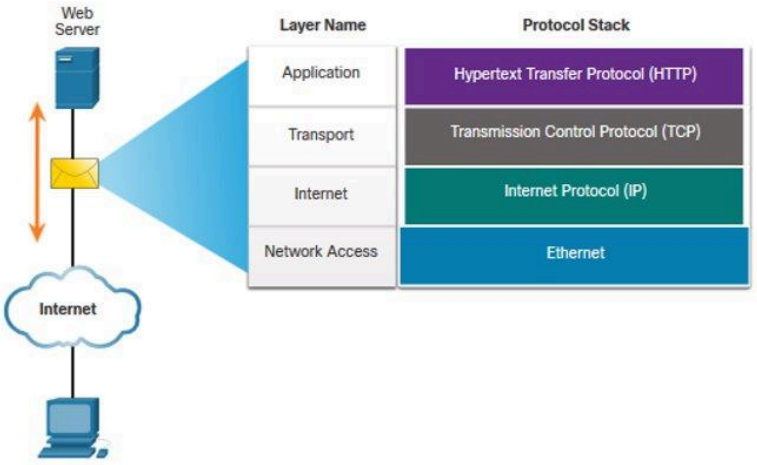
Funcion	**Descripcion**
direccionamiento	un emisor y receptor identificados
confianza	proporciona entrega garantizada
control de flujo	garantiza flujos de datos a una velocidad eficiente
secuenciacion	etiqueta de forma exclusiva cada segmento de datos transmitido
deteccion de errores	determina si los datos se dañaron durante la transmision
interfaz de la aplicacion	comunicaciones de proceso a proceso entre aplicaciones de red

Interaccion de Protocolos

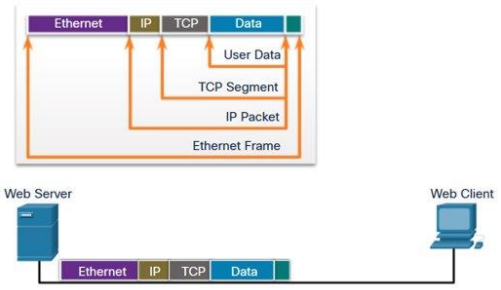
- redes -> requieren el uso de varios protocolos
- **de Internet:**
    - **Protocolo de transferencia de hipertexto (http)**
        - rige la manera en q interactuan un servidor web y un cliente
        - define contenido y formato
    - **Protocolo de control de transmision (TCP)**
        - seguimiento de conversaciones individuales
        - proporciona entrega garantizada
        - administra el control de flujo
    - **Protocolo de Internet (IP)**
        - entrega mensajes globalmente desde el remitente al receptor
    - **Ethernet**
        - entrega mensajes de una NIC a otra en la misma red de area local LAN

Suite de protocolos

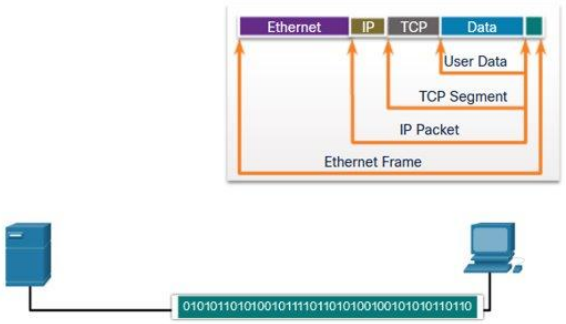
de Red Conjuntos de protocolos

- los protocolos deben poder trabajar con otros protocolos
- suite:
    - grupo de protocolos interrelacionados necesarios para realizar una funcion de comunicacion
    - conj de reglas q funcionan conjuntamente para ayudar a resolver un problema
- los protocolos se ven en terminos de capas:
    - capas superiores
    - capas inferiores: se preocupan por mover datos y proporcionar servicios a las capas superiores
- **Suite de Protocolo TCP/IP**
    - conj de protocolos utilizado por internet estandar abierto -> disponible gratuitamente para el publico y q puede usar cualquier proveedor
    - basado en estándares
    - operan en las capas: aplicacion, transporte e internet
    - 

    - proceso de comunicacion
        - un server web encapsulando y enviando uan pag web a su cliente:



- un cliente desencapsula:



Estandares:

- ISOC sociedad de internet -> desarrollo y evolucion del uso de internet en el mundo
- Consejo de Arquitectura de Internet IAB -> admin y desarrollo de estandares de internet
- Grupo de Trabajo de Ingenieria de Internet -IETF > todo de TCP/IP
- Gruppo de trabajo de investigacion de internet IRTF -> investigacion de TCP/IP

Modelos de Referencia

Beneficios de modelo en capas:

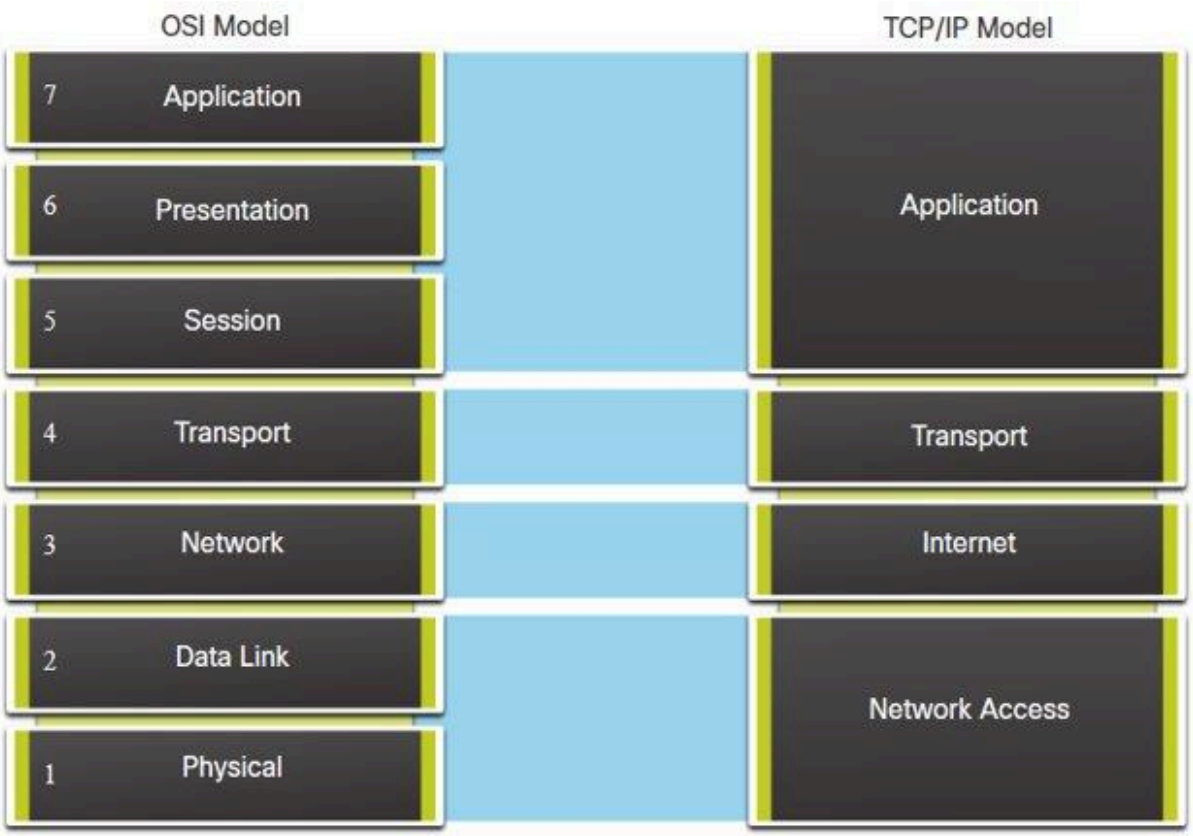
- ayuda en diseño de protocolos -> **operan en una capa especifica** -> interfaz definida para capas superiores e inferiores
- **fomenta competencia** -> distintos proveedores -> trabajar en conjunto
- Evita q cambios en tecnologia o en func de una capa afecten otras
- **proporciona -> lenguaje comun** -> describir funciones y capacidades de red
- **estandariza** -> para crear dispositivos de hw -> todos usan lo mismo

Modelo OSI

1. **Fisica**: describe medios para activar, mantener y desactivar conexiones fisicas
2. **Enlace de datos**: describe metodos para intercambiar marcos de datos entre dispositivos en un medio comun
3. **Red**: proporciona servicios para intercambiar las porciones de datos individuales en la red
4. **Transporte**: define servicios para segmentar, transferir y reensamblar los datos para las comunicaciones individuales
5. **Sesion**: proporciona servicios a la capa de presentacion y administra el intercambio de datos
6. **Presentacion**: proporciona una representacion comun de los datos transferidos entre los servicios de la capa de aplicacion
7. **Aplicacion**: contiene -> protocolos de -> comunicaciones proceso a proceso

Modelo TCP/IP

- **Acceso a la red**: controla los dispositivos del hw y los medios que forman la red
- **Internet**: determina el mejor camino a traves de una red
- **Transporte**: admite la comunicacion entre distintos dispositivos a traves de diversas redes
- **Aplicacion**: representa datos para el usuario mas el control de codificacion y de dialogo



- Modelo OSI -> divide la capa de acceso a la red y de aplicacion en varias capas
- El conjunto de protocolos TCP/IP no especifica qu protocolos utilizar al transmitir a traves de un medio fisico
- Capas 1 y 2 de OSI -> tratan los proc para acceder a los medios y las maneras fisicas de enviar datos por la red

Encapsulamiento de datos

Segmentacion del mensaje

- proceso de dividir mensajes en unidades mas pequeñas
- **Multiplexacion** -> proceso de tomar multiples fluhjos de datos segmentados y entrelazarlos
- Beneficios
    - **aumenta la velocidad** -> se puede enviar grandes cant de datos a traves de la red sin atar un enlace de comunicaciones
    - **AUmenta la eficiencia** -> solo los segmentos q no llegan se retransmiten

Secuenciacion

- **numerar** los **segmentos** para dps ensamblar mensaje -> **TCP** es el **responsable**

Unidades de datos del protocolo PDU

- encapsulacion -> proceso -> protocolos agregan su info a los datos
- en cada etapa -> una PDU tiene -> nombre distinto -> reflejar sus funciones nuevas
- se denominan acorde a TCP/IP -> no es universal
- PDU que pasan por la pila:
    1. datos -> corriente de datos

2. segmento
3. paquete
4. trama
5. bits -> secuencia de bits

Acceso a datos
Direcciones de Red

- **direcciones de origen y de destino de la capa de red** -> responsables de enviar el paquete IP desde el dispositivo de origen hasta el final -> en la misma red o en una remota
- **direcciones de origen y de destino de la capa de enlace de datos** -> responsables de enviar la trama de enlace de datos desde una NIC a otra en la misma red

Direccion logica de capa 3 (red)
los paquetes de IP contienen 2 direcciones:

- Direccion IP origen: del dispositivo emisor
- Direccion IP destion: dispositivo receptor

un paquete IP contiene 2 partes:

1. Parte de Red (IPv4) o Prefijo (IPv6)
    a. seccion de la izquierda -> indica de que red es miembro la direccion IP
    b. Cada LAN o WAN tendra la misma porcion de red
2. Parte del Host (IPv4) o ID de interfaz (IPv6)
    a. parte restante -> id un dispositivo especifico dentro del grupo
    b. seccion de hosts -> unica para cada dispositivo en la red

Si estan en la misma red tienen el mismo numero en la parte de red:

- PC1: 192.168.1.110
- Servidor FTP: 192.168.1.9

Rol de Acceso
Rol de las direcciones de la capa de enlace de datos: misma red IP

- cuando -> dispositivos en la misma red Ethernet -> marco de datos usa direccion MAC real de la NIC de destino
- Direcciones MAC -> integradas fisicamente a la NIC de Ethernet -> son direcciones locales
- La direccion MAC
    - de origen -> sera la del iniciador del enlace
    - de destino -> siempre en el mismo enlace que el origen -> en remoto tmb

Rol de las direcciones de la capa de enlace de datos: distinta red IP

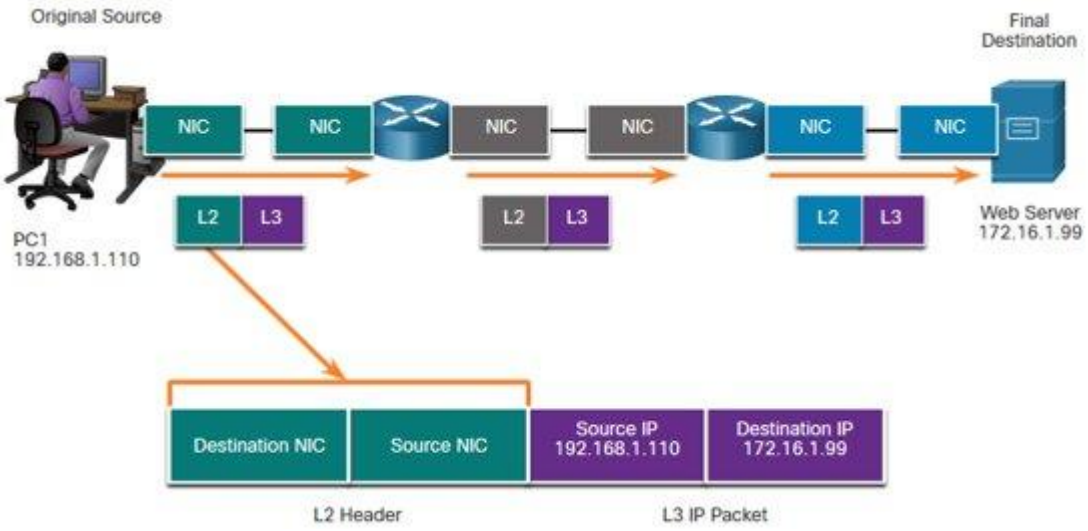
- cuando -> destino final remoto -> capa 3 -> proporciona a capa 2 direccion IP predeterminada local de la puerta de enlace, tmb conocida como direccion del router
- puerta del enlace predeterminada (DGW) es la direccion IP de la interfaz del router que forma parte de esta LAN y sera la puerta de enlace a todas las ubicaciones remotas
- todos los dispositivos LAN -> necesitan recibir info sobre esta direccion -> sino se limita su trafico a solo LAN

- una vez q la capa 2 en PC1 se reenvia a la puerta de enlace predeterminada (Router), el router puede iniciar el proceso de enrutamiento para obtener la info al destino real
- el direccionamiento de enlace de datos es direc local, tiene un origen y destino para cada enlace
- direccionamiento MAC para el primer segmento es:
    - origen -> AA-AA-AA ????? -> envia la trama
    - destino -> 11- 11-11-11-11 ?? -> recibe la trama

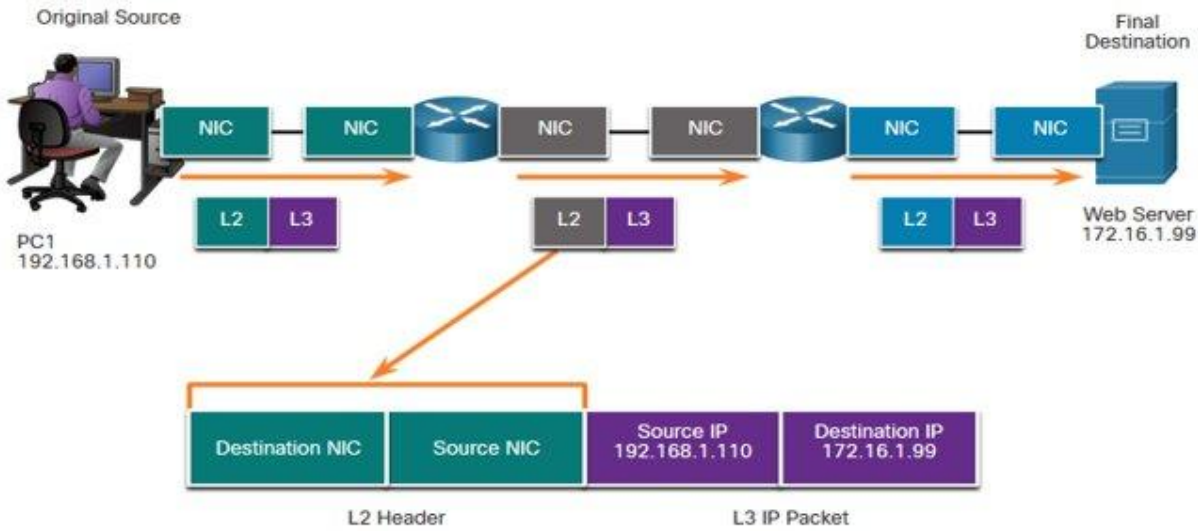
NO ENTENDI NADA DE ESTO DE ARRIBA

Direcciones de enlace de datos:

- es local -> tiene origen y destino para cada segmento o salto del viaje a destino
- direccionamiento MAC para el primer segmento es:
    - origen NIC PC1 envia tramas
    - Destino primer router - interfaz DGW recibe trama

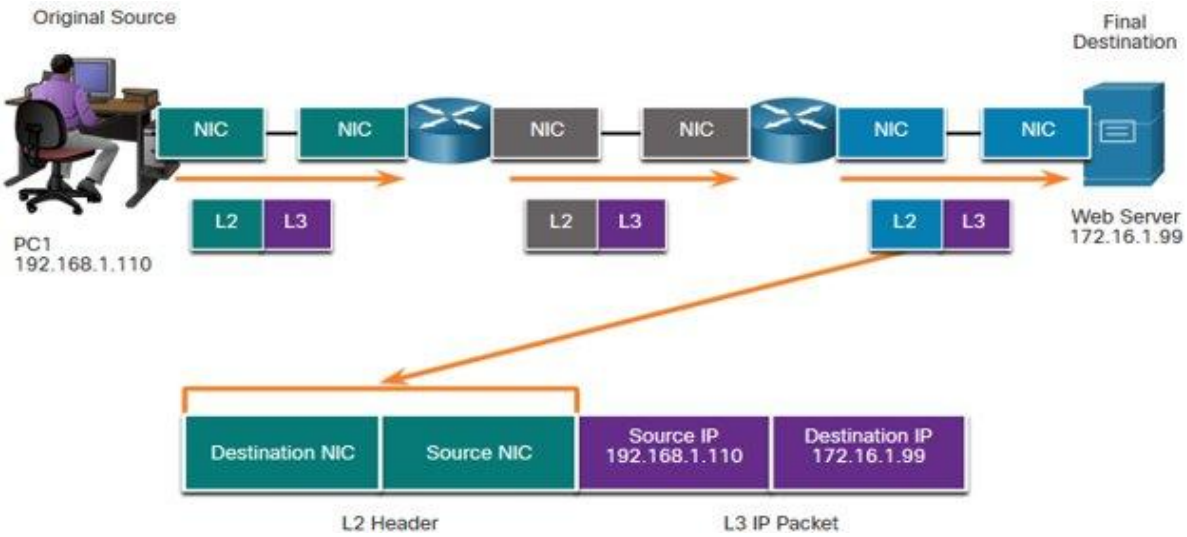


- para el segundo salto es:
    -



- para el ultimo segmento es:

-



- el paquete no se modifica pero el marco se cambia -> el direc IP L3 no cambia segm a segm como el MAC L2
- el direc L3 sigue siendo el mismo ya que es global y el destino final sigue siendo servidor web

Modulo 4

Capa Fisica

- transporta bits a traves los medios de red
- acepta una trama completa de -> capa 2 -> la codifica como una serie de señales q se transmietn a los medios locales
- ultimo paso en el proceso de encapsulacion
- Estandares -> implementados en HW -> abordan 3 areas funcionales
    - componentes fisicos -> dispositivos, medios y conectores q transmiten las señales
    - codificacion
    - señalizacion
- Codificacion -> convierte -> secuencia de bits -> formato reconocible x el siguiente dispositivo en la ruta de red
- Señalizacion ->
    - como se representan los valores de los bits en el medio fisico
    - varia en funcion del metodo q se use
- Ancho de banda
    - capacidad a la q un medio puede transportar datos
    - digital -> mide cant de datos q pueden fluir de un lugar a otro en un periodo -> bits x segundo
    - Latencia -> cant tiempo (incluye retrasos) -> datos viajan de un punto a otro
    - Rendimiento -> medida de transferencia de bits a traves de los medios -> en un periodo
    - Capacidad de transferencia util- >medida de datos utilizables en un periodo -> goodput = rendimiento - sobrecarga de trafico

Cables

- Cableado de cobre
    - + comun, economico, facil de instalar, baja resistencia al flujo de corriente electrica
    - limitaciones
        - atenuacion -> + tiempo viajan las señales, + debiles son
        - señal electrica susceptible a interferencias de
            - Interferencia Electromagnetica EMI
            - Interferencia de Radiofrecuencia RFI
    - mitigacion
        - para atenuacion -> restriccion de longitud de cable
        - para EMI y RFI -> blindaje metalico y conexion a tierra
        - diafonia -> girando cables de par de circuitos opuestos juntos
    - Tipos de cableado
        - Par trenzado sin blindaje (UTP)
            - medio de red + comun
            - interconecta hosts con dispositivos de red intermediarios
            - cubierta exterior -> protege cable de daño fisico
            - pares trenzados -> protegen la señal de interferencia
            - aislamiento de plastico codificado x colores -> aisla los cables entre si y los identifica
        - Par trenzado con blindaje (STP)
            - + proteccion contra el ruid q UTP
            - + caro q UTP
            - interconecta = q UTP
            - cubierta exterior -> protege cable de daño fisico
            - escudo trenzado o de lamina -> proteccion de EMI/RFI
            - escudo de alumnio para cada par de cables -> proteccion de EMI/RFI
            - aislamiento de plastico codificado x colores -> aisla los cables entre si y los identifica
        - Cable Coaxial
            - cubierta exterior -> protege cable de daño fisico
            - trenza de cobre tejida, o lamina metalica -> escudo para el conductor interno
            - capa de aislamiento de plastico flexible
            - conductor de cobre para las señales
    - Propiedades del Cableado UTP para limitar diafonia
        - cancelacion -> cables opuestos para cancelar EMI/RFI
        - variacion en giros por pie de cada cable
    - Estandares de cableado UTP

        - Fibra optica
            - + caro q UTP
            - - susceptible a atenuacion
            - inmune a EMI/RFI
            - guia de onda para transmitir luz entre los 2 extremos con una minima perdida de señal
            - Tipos

        - Fibra monomodo
            - nucleo pequeño
            - costosos lasers
            - aplicaciones a larga distancia
        - Fibra de modos multiples
            - nucleo mas grande
            - leds menos caros
    - Se usa en:
        - Redes empresariales
        - Fibra hasta el hogar
        - Redes de larga distancia
        - Redes de cable submarino

Medios Inalambricos
- usan frecuencias de rados
- limitaciones
    - area de cobertura
    - interferencia
    - seguridad
    - las WLAN de medio compartido -> semiduplex
- estandares
    - wifi -> IEEE 802.11
    - Bluetooth -> IEEE 802.15
    - WiMAX ->IEEE 802.16
    - Zigbee -> IEEE 802.15.4
- LAN Inalambrica
    - requiere:
        - Punto de acceso inalambrico (AP) -> concentra señales inalambricas de los users y conectese a la infra de red basada en cobre ya existente
        - Adaptadores NIC inalambricos -> brindan capacidad de comunicaciones inalambricas a los hosts de red

Modulo 5
Direcciones Binarias e IPv4
- binaria -> 0 y 1
- IPv4
    - 4 objetos
    - cada uno representa 1 numero binario
    - routers y pcs solo entienden binario entonces se convierte el IPv4 de decimal a binario

Notacion posicion binaria y conversion no va, pero como representamos la posicion del numero si, o sea los valores de las posiciones en binario:
1 2 4 8 16 32 64 128 -> potencias de 2

Direcciones hexadecimales e IPv6

- de 0 a 9 y de A a F
- tiene 16 numeros (hexa jaja!!)
- direccion MAC -> direccion de capa 2 -> es como el DNI -> lo tienen todos los dispositivos de red
- IP direccion de capa 3

conversion de hexa no se ve

NOTA: PROTOCOLOS PROPIETARIOS -> una firma los tiene ej cisco, los NO propietarios son publicos

Modulo 6: Capa de enlace de datos (2)

Proposito
- provee conexion con capa 3 y capa 1
- tiene q establecer emtodos de codificacion para q la info pueda seguir con las capas sup
- en la capa fisica viene la info como bits
- aca estan las direcciones MAC
- detecta errores y tramas corruptas -> permiti retransmitir datos o no
- trama -> info que circula en capa 2
- Proporciona acceso a los medios -> router realiza 4 funciones basicas
    - acepta una trama del medio de red
    - desencapsula la trama para exponer el paquete encapsulado
    - vuelve a encapsular el paquete en una nueva trama
    - reenvia la nueva trama en el medio del siguiente segmento de red

NOTA: en cada capa al paquete encapsulado se agrega una cabecera en cada capa

Estandar
- IEEE -> estandares para los metodos q se usan para recibir y transmitir de capa 2
    - WPAN -> red de corto alcance ej bluetooth infrarojo -> tienen estandar -> IEEE802.15
    - WLAN -> + extenso que WPAN -> IEEE 802.11
    - todo lo q es cableado -> IEEE 802.3
- **QUE SE YO**

SubCapas de capa 2
- Control de enlaces logicos -> LLC
    - se comunica entre el sw de red y AAAAAAAAAAAA
- Control de acceso a medios -> MAC
    - **ESTO NI LLEGUE**
    - Encapsulamiento de datos -> IEEE 802.3
        1. trama de ethernet -> estructura interna de trama Ethernet
        2. Direccionamiento Ethernet -> la trama Eth incluye -> direc MAC de origen y destino para entregar la trama Eth de NIC Eth a NIC Eth en la misma LAN

3. Deteccion de errores Ethernet -> la trama Eth incluye -> remolque de secuencia de comprobacion de fotogramas (FCS) utilizado para la deteccion de errores

-

Nota importante: tamaño min de una trama es 64 bytes -> para descartar las q tienen menos -> tam max 1518 bytes -> se descartan mayores -> se llaman jumbos

Topologias -> es como un mapa

- Fisica -> muestra conexiones fisicas y como los dispositivos estan interconectados -> estan cableados o inalambricos? en que placa de red, en que puerto etc
- Logica -> id las conexiones virtuales entre dispositivos mediante interfaces de dispositivos y esquemas de direccionamiento IP
- WAN tiene 3 fisicas comunes
    - Punto a Punto -> + simple y comun -> enlace permanente entre 2 puntos finales
    - Hub and spoke -> 1 sitio central interconecta sitios de sucursal a traves de enlaces puntoa a punto
    - Malla -> alta disponibilidad pero requiere que cada sistema final este conectado a cualquier otro sistema final -> hay parcial y completa
- LAN
    - Bus
    - Estrella
    - Estrella extendida
    - Anillo -> se usa hoy en dia -> en fibra optica
        - usan token para permitir recibir o transmitir info -> cuando 1 tiene l token no lo puede usar otro

Comunicacion semiduplex

- inalambricas
- solo permite q 1 dispositivo envie o reciba a la vez en un medio compartido
- se usa WLAN y topologias de bus heredadas con hubs Ethernet

Comunicacion Duplex completo

- permite q ambos dispositivos transmitan y reciban simult en medio compartido
- los switches Ethernet funcionan en modo full-duplex

Metodos de control de acceso

Acceso basado en la contencion -> como se gestionan los datos en diferentes dispositivos

- CSMA/CD -> multiples accesos con deteccion de colisiones -> en Ethernet de topologia de bus heredada
    - funciona en semiduplex
    - deteccion de colision -> controla cuando puede enviar un dispositivo y q pasa si varios envian al mismo tiempo
        1. dispositivos transmiten simultaneamente provocan colision de señal en medio compartido
        2. dispositivos detectan colision

3. dispositivos esperan un periodo aleatorio de tiempo y retransmiten datos

- CSMA/CA -> multiples accesos con avoidance de colisiones -> en LAN inalambricas
    - usado por WLAN IEEE 802.11
    - funciona en semiduplex
    - prevencion de colisiones -> determina cuando puede enviar un dispositivo y q pasa si varios mandan al mismo tiempo
        1. al transmitir los dispositivos incluyen el tiempo necesario !=#=ljej8daj
        2. **FALTA ESTO**

Acceso Controlado

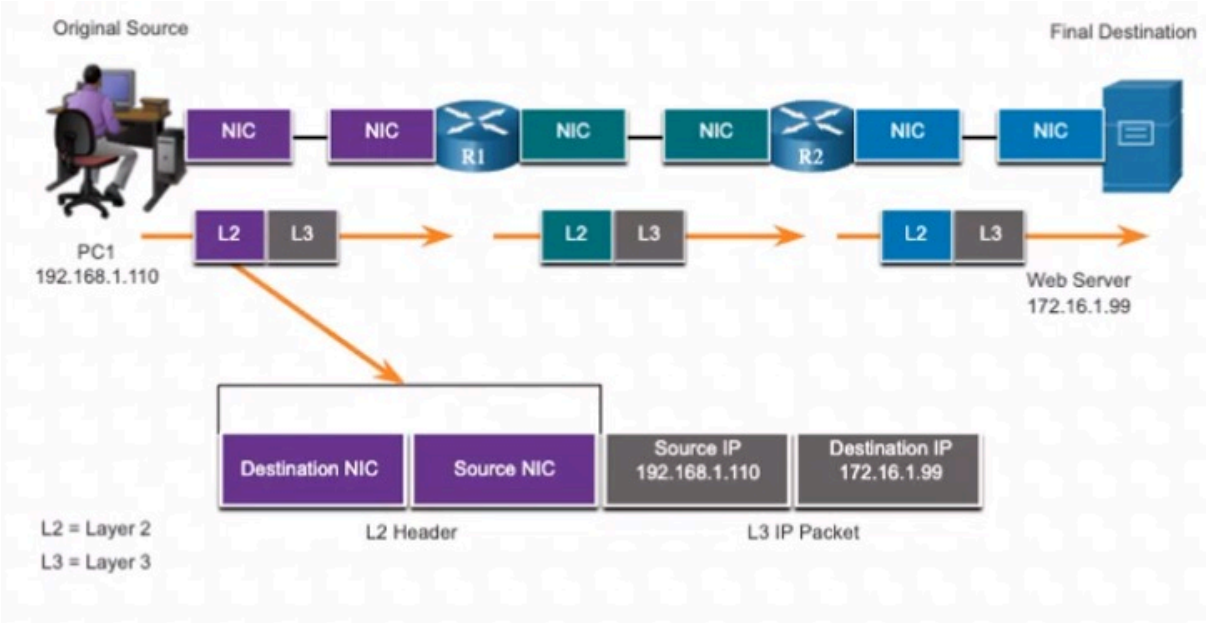
- acceso determinista donde cada nodo tiene su propio tiempo en el medio
- es usa en redes heredadas como Token Ring y ARCNET

Trama de capa 2 -> es la PDU de capa 2 (en capa 3 es paquete)

- datos -> encapsulados por la capa de enlace de datos con un encabezado y un remolque para formar una trama
- consta de 3 partes
    - encabezado
    - datos
    - trailer
    - **PONER FOTOOOO**
    - **esta parte parece importante xd**

Direcciones de Capa 2

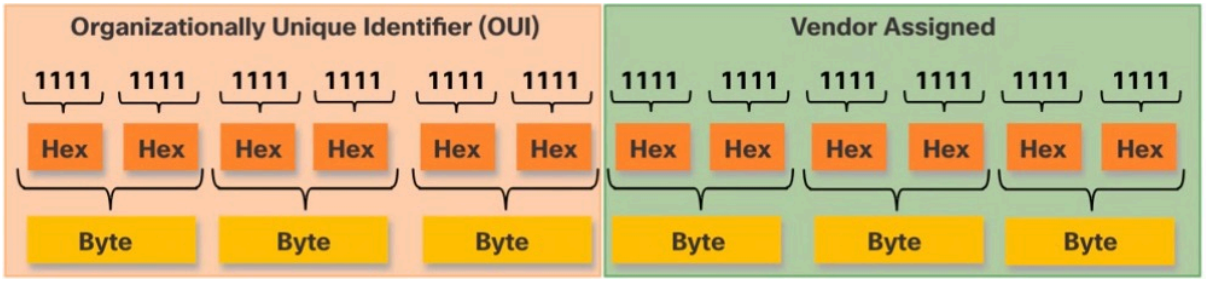
- tmb conocido como direccion fisica -> direccion MAC -> hexadecimal
- contenido en el encabezado de la trama
- se usa solo para la entrega local de una trama en el enlace
- actualizado por cada dispositivo q reenvia la trama
- si estoy en la mimsa red me comunico por capa 2 pero si tengo q comunicar a otra red con algo como un router, se adquiere otra direccion de capa 2, pero en capa 3 no cambia. Por eso se necesita la direc de capa 3 ademas de la MAC -> la MAC cambia porq es propia de cada dispositivo, ES FISICA



Protocolos de capa 2

- Ethernet
- 802.11 inalambrico
- PPP point to point
- control de enlace de datos de alto nivel (HDLC)
- frame-relay

Direccion MAC

- en hexa decimal
- si tiene 0s iniciales no se tienen en cuenta -> son para completar bits y q haya menos errores en la transmision
- de 48 bits
- 

- cuando es todo FF en la MAC -> broadcast -> se inundan todos los puertos menos el de origen **IMPORTANTE**

Procesamiento de tramas

- se envia a todos los destinos pero las q no lo necesitan lo ignoran
- conmutar -> se manda a todos la primera vez porq no se cual es y dps se guarda q es ese el destino entonces se ocnmuta O SEA NO ES CONMUTAR MIRA GPT -> o sea hace broadcast, pero cuando ya conoce hace unidifusion

Nociones Basicas de Switches

- diferencia con hub -> hub ancho de banda compartido -> switch ancho de banda
- toma decisiones de reenvio -> en q puerto envia la info
- examina la tabla de direcciones MAC,
- **esta parte seguila en casa campeon**
- la tabla de direcciones MAC -> se refresca cada 5 mins -> personalizable
- examina la direccion de origen
- busca la direccion de destino -> reenviar
- Metodos de reenvio de tramas
    - conmutacion de almacenamiento y reenvio -> recibe la trama y garantiza q es valida si la CRC es valida -> switch busca direccion de destino -> determina la interfaz de salida -> trama se reenvia desde el puerto correcto -> antes de enviar verifica si hay errores -> la descarta -> reduce el ancho de banda
    - conmutacion de corte -> reenvia la trama antes de q se reciba por completo -> no verifica si hay errores -> se debe leer la trama de destino antes de enviar
        - de avance rapido -> tiene menos latencia -> siwtching rapido -> poca integridad?
        - sin fragmentos -> punto intermedio de latencia y de integridad -> se verifiacan los primeros 64 bytes
- Memoria intermedia -.> SE LO PASOOOO UESAAAAA
- Config Duplex y velocidad
    - forma automatica -> autonegociacion-> funcion optativa -> permite q 2 dispositivos negocien automaticamente las mejores capacidades de velocidad y duplex
    - si hay dispositivos con distinta config y velocidad -> no se pueden comunicar

Auto-MDIX -> **completalo bobo**

Nota: Escalo a capa 3 cuandome conectoa algo remotooooooooo, si es local me quedo en la capa 2 ;)

Modulo 9

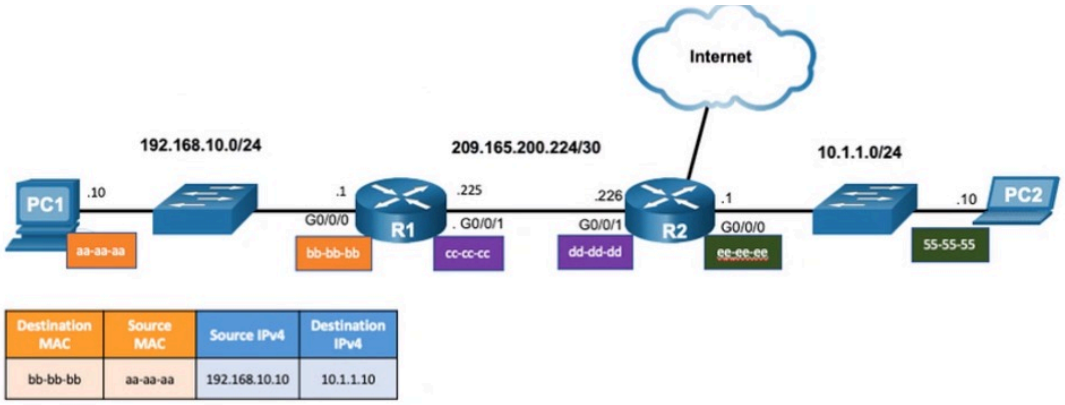
MAC e IP

- Direccion fisica de capa 2 -> para comunicaciones NIC a NIC en la misma red Ethernet
- Direccion logica de capa 3 IP -> enviar paquete desde el dispositivo de origen al de destino

Destino en una red Remota

- cuando la direc ip de destino esta en una red remota -> la direc mac de destino es la de la puerta de enlace predeterminada
- ARP -> IP + MAC -> asocia en Ipv4
    - a traves de la direcion IP de destino consigue la direccion MAC de destino (en red local para no pasar a capa 3)

    - tiene una tabla ARP con asignaciones de direcciones IP a MAC
        - no son permanentes las entradas se eliminan por temporizador
- ICMPv6 -> para IPv6



Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

Problemas ARP

- como se si un dispositivo es susceptible a ataques -> si tengo la OUI de la MAC puedo saber q vulnerabilidades tiene
- ARP Spoofing -> suplantar un cliente con la direccion MAC
- envenenamiento -> inyectan solicitudes ARP para hacer que se caiga -> ataque de denegacion de ervicio -> inhabilito una red
- lo sswitches de nivel empresarial estan preparados para este tipo de ataque

IPv6 mensajes de deteccions d vecinos IPv6

- Neighbor discovery (ND)
    - resolucion de direccion
    - descubrimiento de router
    - servicios de redireccion
    - los mensajes de solicitud de vecino y anuncio de vecino se usan para mensajes de dispositivo a dispositivo, como la resolucion de direcciones
    - **los mensajes ICMTPV6 Router Solicitation Y NO SONFAONJEAJUHOIYFDSHGPOUDSAJFSAIULFH**
    - Descubrimiento de vecinos - resolucion de direcciones
        - los disp ipv6 usan ND para resolver la direccion MAC de una direc ipv6 conocida
        - los mensajes de solicitud de vecinos se envian usando direcciones multidifusion Ethernet e ipv6

Modulo 10: config de router

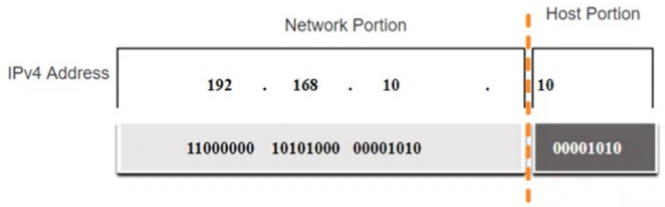
Puerta de enlace predeterminada en un host ->

- Gateway -> gral el 1er router disponible
- se usa cuando un host envia un parquet a otra red
- switch -> debe tener una direccion de puerta de enlace predet config par aadmoin el conmutador de forma remota desde otra red

Modulo 11: Direccionamiento

Estructura de una direc IPv4
Porciones de redy host

- IPv4 tiene porcion de red y porcion de host
- se usa mascara de subred para determinar estas porciones



-
- de 0 a 255 -> 0 se usa para red y 255 para broadcast -> se usan los demas
- cuando se empieza a subnetear -> puede haber un (ej) 3 en vez de 0 en red

Mascara de subred

- se compara mascara con direc bit por bit para determinar parte host y parte red

Longitud de prefijo

- metodo usado para id una direc de mascara de subred
- es el numero de bits establecido en 1 en la mascara de subred

Determinacion de la red: AND logica

- ???

Direccion de red, host y difusion

- dentro de cada red hay 3 tipos de direc ip
  - red
  - host
  - broadcast

	Porción de red	Porción de host	Bits de host
Máscara de subred **255.255.255.**0 o **/24**	255 255 255 11111111 111111 1111 1111	0 00000000	
Dirección de red **192.168.10.**0 o**/24**	192 168 10 11000000 10100000 00001010	0 00000000	All 0s
Primera dirección **192.168.10.**1 o **/24**	192 168 10 11000000 10100000 00001010	1 00000001	All 0s and a 1
Last address **192.168.10.**254 o **/24**	192 168 10 11000000 10100000 00001010	254 11111110	All 1s and a 0
Dirección de broadcast **192.168.10.**255 o **/24**	192 168 10 11000000 10100000 00001010	255 11111111	All 1s

-

Direcciones publicas y privadas

- las publicas se enrutan globalmente entre routers de proveedores de servicio de internet (ISP)
- las privadas -> bloques comunes de direccs usadas por la mayoria de las orgs para signar direc IPv4 a hosts internos
  - no exclusivas

    - cualquier red interna puede ??
    - no son enrutables globalmente

Enrutamiento a Internet

- NAT -> traduccion de direcciones privadas a publicas y **viceversa chequear**
    - habilitado en el router perimetral q se conecta a internet

Direcc publis y privadas

Direcciones de loopback

- se usa en un host para probar si TCP/IP esta operativo
- 127.0.0.0

Direcciones de enlace local

- direcciones de direccionamiento IP privado automatico -> **APIPA**
- no sirven para nada
- no hay config estatica -> la dinamica no me da una direc ip -> se usa una APIPA
- si aparecen -> hay algo mal -> ej no funciona TCP/IP

Direccionamiento con clase antigua

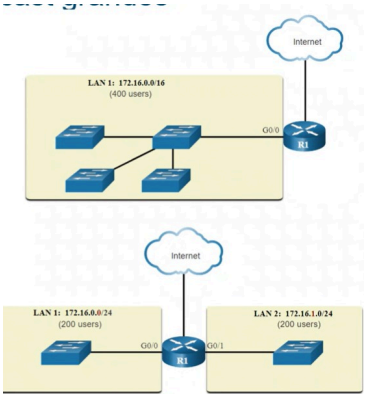
- Clase A -> 0.0.0.0 a 127.0.0.0
- Clase B -> 128.0.0.0 a 191.255.0.0
- Clase C -> 192.0.0.0 a 223.255.255.0
- Clase D -> 224.0.0.0 a 239.0.0.0
- Clase E -> 240.0.0.0 a 255.0.0.0

Asignacion de direcciones IP

- Autoridad de Numeros Asignados de Internet (**IANA**) -> admin y asigna bloques de direcciones IPv4 y 6 -> hay orgs regionales para la admin

Nota: Multicast se usa mucho para streaming como privilegios especificos de latencia

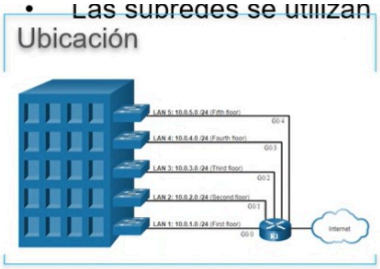
Segmentacion de la red

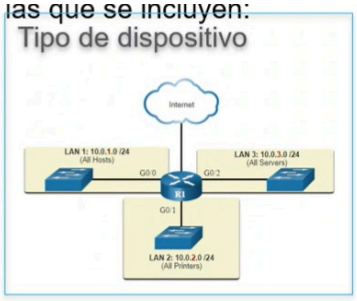
- dividir una red para que sea mas eficiente -> se limitan los broadcast de red para que no sea un broadcast enorme
- 

Motivos para dividir en subredes

- disminuye el trafico de red general y mejora su rendimiento
- se usa para implementar directivas de seguridad entre subredes
- reduce el numero de dispositivos afectados por el trafico de broadcast anormal
- Otros motivos:

- ubicacion
- grupo o funcion
- tipo de dispositivo
    - Las subredes se utilizan por una variedad de razones, entre las que se incluyen:





-

nota: subredes es fisica y subnetting es logica

SUBNETEO PAAA
Division en subredes en el limite del octeto

- las mas faciles son /8 /16 y /24

Longitud de prefijo	Máscara de subred	Máscara de subred en sistema binario (n = red, h= host)	Cantidad de hosts
/8	255.0.0.0	**nnnnnnnn**.hhhhhhhh.hhhhhhhh.hhhhhhhh **11111111**.00000000.00000000.00000000	16777214
/16	255.255.0.0	**nnnnnnnn.nnnnnnnn**.hhhhhhhh.hhhhhhhh **11111111.11111111**.00000000.00000000	65534
/24	255.255.255.0	**nnnnnnnn.nnnnnnnn.nnnnnnnn**.hhhhhhhh **11111111.11111111.11111111**.00000000	254

-
- si el prefijo es mas grande -> menos direcciones disponibles
- lo q mas vamos a ver:

Longitud de prefijo	Máscara de subred	Máscara de subred en sistema binario (n = red, h = host)	Cantidad de subredes	Cantidad de hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

Modulo 12: Direccionamiento IPv6

- esquema de coexistencia -> IPv4 e IPv6
    - **tecnicas de migracion**: -> se pasa de una a otra a medida q se migra
        - **dual stack** -> e ejecutan pilas de protocolos IPv4 e IPv6 -> conviven de forma simultanea
        - **tunneling** -> transporta paquete IPv6 sobre una red IPv4

        - **translation** -> usa **NAT64** -> dispositivos IPv6 se comunican con dispositivos IPv4
    - dps hay esquema puro de IPv6

Nota: nat traduce direcciones

Representacion de direcciones
IPv6 formatos de direcciones IPv6

- 128 bits
- hexadecimal
- tmb denominada hexteto
- **reglas -> para simplificar**
    1. **omitir el cero inicial**: se omite el cero inicial en cada tramo de la direccion. ej: si es 01ab -> 1ab, 001a -> 1a.
    2. **Dos punto**s -> si hay conjuntos de ceros seguidos -> 01ab:0000:ab12 -> se pone como dos puntos ese tramo -> 01ab::ab12 -> SOLO SE PUEDE HACER UNA VEZ
- Unicast, multicast y anycast
    - Unicast
        - **GUA global unicast address**-> direc publicas q todos pueden tener -> enrutables en internet
            - estructura-> global routing prefix, subnet id, interface id
                - global routing prefix + subnet id -> primeros 64 bits
                - **global routing prefix** -> direccion asignada por el ISP -> varia segun politicas de ISP
                - **ID de Subred** -> para id subredes dentro de su ubicacion
        - **LLA Link local address** -> direc local -> se enruta la publica, la local no (es como la MAC) para comunicarse de forma local -> es de capa 3 -> x seguridad
            - de fc00::/7 a fdff::/7
            - cada interfaz de red IPv6 tiene q tener LLA
            - si no se configura manualmente -> se crea automaticamente la direc de LLA
- **Longitud de prefijo de IPv6** -> la mayoria de direc usa /64
    - 64 bits primeros -> **prefijo de red**
    - 64 bits seguidos -> **id de interfaz**

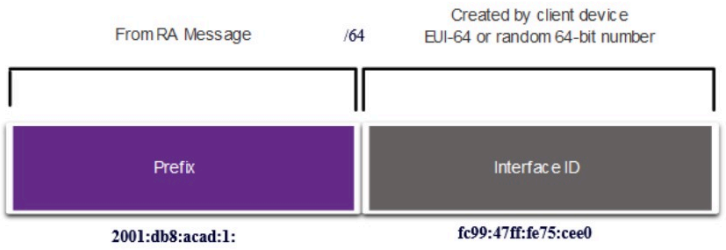
Confoiguraciones estaticas
Configuracion Estatica de GUA en un Router

- igual q IPv4 pero el comando cambia por ipv6 address

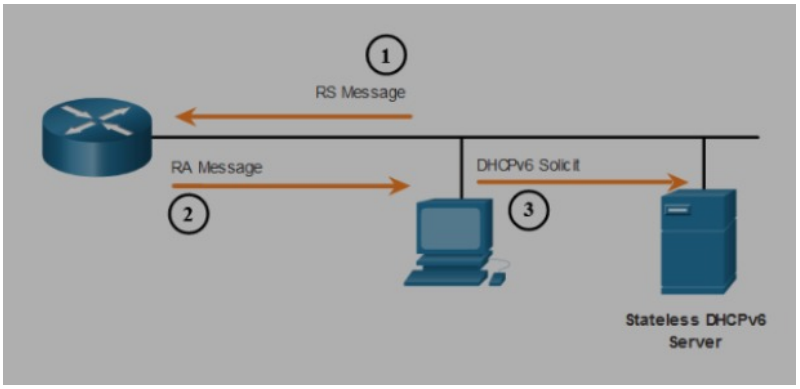
Configuracion Dinamiga

- **a traves de ICMPv6**
    - **mensaje de solicitud de router (RS)** -> enviados x dispositivos host para descubrir routers IPv6

- router -> envia **mensaje de anuncio de router (RA)** -> informa hosts como obtener un GUA IPv6 -> proporcionar info util de red
    - 1 prefijo de red y longitud de prefijo
    - 2 direc gateway predeterminado
    - 3 direc dns y nombre de dominio
- **RA puede proporcionar 3 metodos para configurar GUA (en orden de complejidad)**
    - **SLAAC** -> state less address auto config
        - permite a un dispositivo conif GUA sin serv DHCPv6
        - dispositivos obtienen info nec para config GUA a partir de los mensajes **RA** ICMPv6 del router local
        - el prefijo -> lo proporciona el RA -> dispositivo usa metodo **EUI-64** o de generacion aleatoria para crear un **ID de interfaz** -> en base a la direc mac



        - **SLAAC con servidor DHCPv6 stateless**
            - router provee -> direccionamiento -> direc link local, gateway
            - servidor DHCPv6 provee -> DNS



        - **Stateful DHCPv6 (no SLAAC)**
            - el direccionamiento lo jace el DHCPv6 -> link local, DNS, gateway -> todo lo provee el servidor
- Proceso EUI-64 vs Generado aleatoriamente
    - si el RA es SLAAC o SLAAC stateless -> cliente -> genera su propia interface id -> se pued ecrear con EUI-64 o aleatoriamente en 64bits
        - **EUI-64**
            - EUI -> id unico extendido
            - valor de 16 bits de fffe -> se inserta en el centro de la direc MAC Ethernet de 48 bits del cliente
            - 7mo bit de la direc MAC del cliente se invierte del binario 0 al 1

MAC de 48 bits	fc: 99:47:75:ce:e0
Id. de interfaz EUI-64	fe: 99:47:ff:fe:75:ce:e0

-
    - Aleatorio
- **en stateful -> no depende del cliente -> todo servidor**

creo q eso fue para gua ahora vamos con LLAS

LLAs Dinamicas

- todas las interfaces IPv6 -> tienen LLA IPv6
- **se crea auto cuando se configura una GUA**

Direcciones Multicast -> misma func q Ipv4 pero con prefijo distinto

- grupos de multicas con direcs especificas
- jaja xd lo re paso eso no??

Division en subredes para IPv6

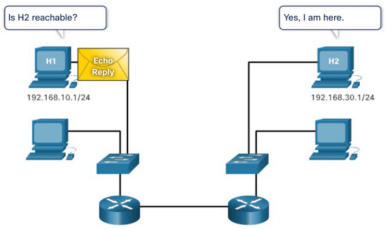
- **primeros 64 bits -> ultimos 16 bits -> subnet id -> es par asubnetear**

Asignacion de Subred IPv6

Modulo 13: ICMP

Mensajes ICMPv4 e ICMPv6

- internet control message protocol
- para saber q dispositivo final esta encendido o apagado
- los **mensajes icmp 4 y 6 incluyen**
    - **accesibilidad al host**
        - **Echo message** -> para probar accesibilidad



-
    - **gestion o servicio inaccesible**
        - **codigos de destino inalcanzable:**
            - imcp 4 ->
                - 0 red inalcanzable
                - 1 host inalcanzable
                - 2 protocolo inalcanzable
                - 3 puerto inalcanzable
            - icmp 6
                - 0 no hay ruta para el destino
                - 1 comunicacion con destion prohibida

        - 2 mas alla del alcance de la direc de origen
        - 3 no se puede alcanzar la direc
        - 4 puerto inalcanzable
    - **tiempo superado**
        - cuando TTL de un paquete -> reduce a 0 -> se envia mensaje icmp4 -> al host de origen
        - Limite de salto en icmpv6 -> determina si un paquete expiro
- icmp 4 -> no se suelen permitir en una red x seguridad

Mensajes ICMPv6

- **entre router y dispositivo IPv6 ->** SLAAC y los otros 2
    - **RS ->** determina como recibir dinamicamente su info de direc IPv6
    - **RA** -> puede incluir info de
        - direccionamiento para el host
            - prefijo
            - long prefijo
            - direc dns
            - nombre dominio
        - SLAAC o DHCP establece su puerta de enlace pred en la direc de enlace local del router -> la envia RA
        - envia mensaje en respuesta a mensaje RS
- **Entre dispositivos IPv6** -> para detectar direcciones duplicadas y resolucion de direccion
    - **NS -> mensaje d esolicitud de vecino ->** se fija por **DAD -> deteccion de direcciones duplicadas** -> envia un mensaje con su propia IPv6 para ver si hay duplicado
    - **NA -> mensaje de anuncios de vecino** -> si hay duplicado -> devuelve la direccion MAC de Ethernet
    - **NS manda un objetivo ->** si encuentra, **NA** devuelve la direc mac del objetivo -> de paso se puede usar para encontrar duplicados si NS objetivo = direc ip de origen
- se envian cada 200 seg -> se puede modificar

Modulo 14: **Capa de Transporte**

Funciones

- ultima capa con direcciones de origen y destino
- **gestiona sesiones q se abren**
- **responsable de** -> comunicaciones logicas entre aplicaciones q se ejecutan en diferentes hosts -> mueve data entre aplicaciones en los dispositivos en la red.
- e**nlace entre capas de aplicacion y capas inferiores** q se encargan de la transmision a traves de la red

nota: creo q la trama aca son conversaciones

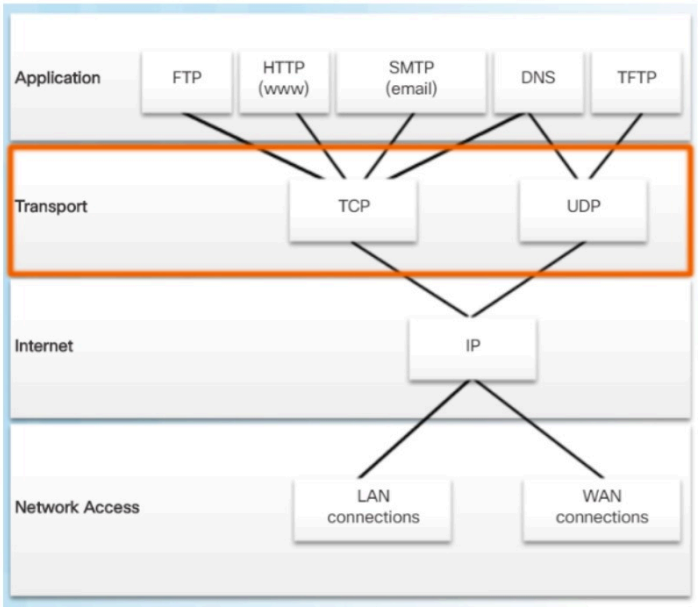
Tareas

- seguimiento de conversaciones individuales

- **segmentacion** -> de datos y rearmado de segmentos -> permite conversation **multiplexing** -> muchas aplicaciones pueden usar la red al mismo tiempo
- agregar info de encabezado
- id, separar y admin -> multiples conversaciones

Protocolos de la capa

- especifican **como transferir mensajes entre hosts** y son responsables de **admin los reqs de fiabilidad de una conver**



- **TCP -> transmission control protocol -> FIABILIDAD**
  - **Segmento**
  - provee confiabilidad y control de flujo de operaciones basicas TCP
    - numere y rastree segmentos de datos transmitidos a un host especifico desde una app especifica
    - confirmar datos recibidos
    - vuelva a transmitir info no reconocida dps de un tiempo
    - datos de secuencia -> llegan en orden incorrecto
    - enviar datos a velocidad eficiente
  - **SMTP y HTTP lo usan**
  - **Caracteristicas**
    - **Establece una sesion** -> negocia y establece conexion permanente (sesion) entre dispositivos de origen y destino -> antes de reenviar trafico
    - **Garantiza entrega confiable**
    - **Proporciona entrega en el mismo pedido** -> es posible -> datos lleguen en orden incorrecto -> redes proporcionan multiples redes con diferentes velociddades de transmision
    - **Admite control de flujo** -> cuando una app sobrecarga recursos -> se le pide q reduzca la velocidad de flujo de datos
  - **Encabezado**
    - puertos -> origen y destino
    - secuencia de numeros

        - **numero de respuesta -> numero ack** -> para gestionar conversaciones
        - campos reservados -> porq dps se amplia
        - **ventana** -> tamaño de mensaje q se puede aceptar
        - urgente -> ver si es urgente
        - **checksum** -> suma de comprobaciones -> comprobación de errores del encabezado y los datos
    - Apps que usan TCP
        - HTTP
        - FTP
        - SMTP
        - SSH
- **UDP -> protocolo de datagramas de usuario de datos -> VELOCIDAD**
    - **Datagrama**
    - entrega segmentos de datos con poca sobrecarga y revision de datos
    - protocolo sin conexion -> no se controla si se conecta o no
    - el orden de los paquetes enviados -> no se controlan en el receptor
    - si no se transmite un paquete -> no se vuelve a transmitir?
    - **DNS lo usa**
    - **Caracteristicas**
        - **datos** -> se **reconstruyen** en el **orden** en q se **recibieron**
        - **segmentos perdidos** -> no se vuelven a enviar
        - **no** se establece **sesion**
        - **envío** -> **no informado** sobre la **disponibilidad** de **recursos**
    - **Encabezado**
        - puertos -> origen y destino
        - longitud (del encabezado mismo)
        - **checksum** -> comprobación de errores del encabezado y los datos del datagrama
    - Apps que usan UDP
        - DHCP
        - DNS
        - SNMP
        - TFTP
        - VoIP
        - Video Conference

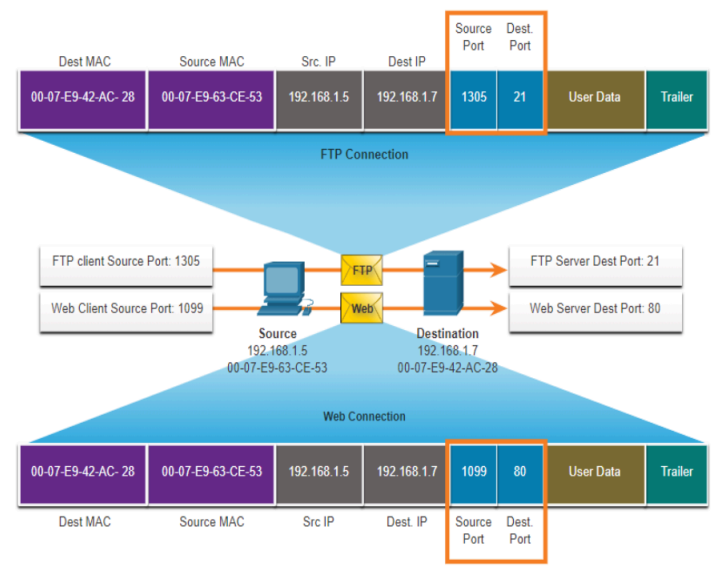
nota: en conmutacion por circuito se puede desperdiciar ancho de banda al haber 1 solo circuito

Numeros de Puerto
Comunicaciones separadas multiples

- **TCP y UDP -> usan numeros de puerto -> para admin multiples conversaciones simultaneas**
- num de puerto de origen -> asociadon con la app de origen en el host local
- num de puerto de destino -> asociado con la app de destino en el host remoto
- cuando entramos a una IP vemos servicios disponibles -> cuando IP+puerto estamos entrando a un servicio especifico

Pares de sockets -> combinacion de **direc IP origen + nro puerto origen (tmb con destino)**

- dentro del segmento -> se encapsulan dentro de un paquete ip
- permiten ->
    - diversos proceso -> q se ejecutan en 1 cliente -> se distingan entre si
    - diferenciación nde diferentes conexiones a un proceso de servidor



Ej de Socket: 192.168.1.5:**1305** y 192.168.1.7:**21**

Cuando tengo un puerto abierto -> es un punto de entrada

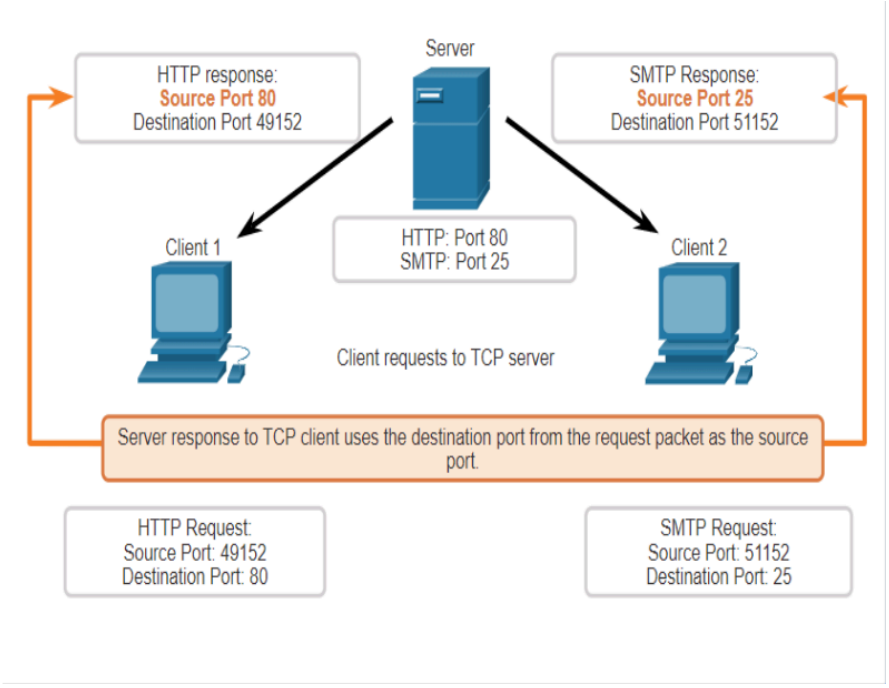
Grupos de Numeros de puerto

- Conocidos -> 0 a 1023 -> usados para determinados servicios
- Registrados -> 1024 a 49151 -> para procesos o apps especificos -> ej:cisco el 1812 para RADIUS -> para tener mayor seguridad en una red
- Privados y/o Dinamicos -> 49152 a 655535 -> son como puertos privados (como las direc ip privadas)

Proceso de comunicacion en TCP

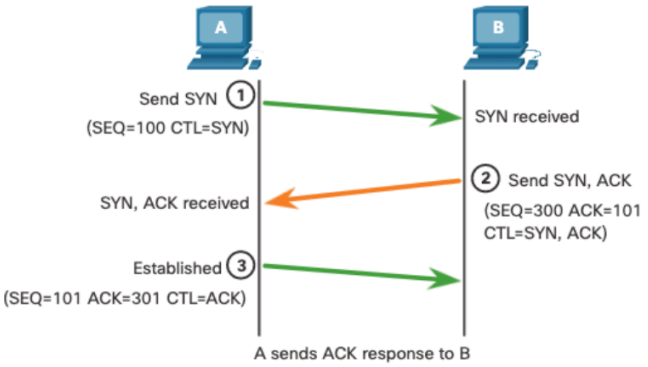
Proceso del Servidor TCP

- 1 server individual -> no puede tener -> 2 servicios asignados al mismo nro de puerto
- 1 app de servidor activa asignada a un puerto especifico -> abierta -> capa de transporte acepta y procesa los segmentos dirigidos a ese puerto
- solicitudes entrantes de un cliente direccionadas al socket correcto -> aceptadas -> datos se envian a la app del servidor



Establecimiento de conexion

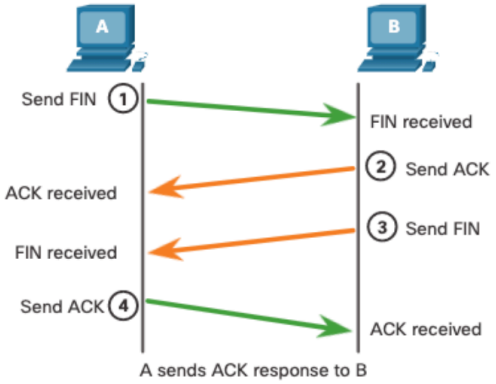
1. cliente de origen -> solicita sesion de comunicacion con el servidor
2. a
3. a



Finalizacion de la Sesion TCP

1. cliente no tiene + datos para enviar -> envia segmento con FIN
2. servidor envia

creo q lo importante es q envia mensajes ACK para inicio y fin CREO



Analisis de protocolo TCP de enlace de tres vias
funciones

- establece q el dispositivo de destino esta presente en la red
- veirfica q el dispositivo
- y algo mas

Analisis de protocolo de enlace TCP de 3 vias -> en el campo control bits del encabezado

- **URG -> campo indicador urgente importante**
- **ACK -> indicado de acuse de recibo utilizado en el establecimiento de la conexion y la terminacion de la sesion**
- hay mas

Comunicacion UDP
?

Modulo 15: **Capa de Aplicacion**
Aplicacion, Presentacion y sesion

- **la 5 y 6 proveen interfaz entre la aplicacion y las demas capas**
- **Presentacion** -> se encarga del **formato de los dato**s -> formato de archivos
  - **comprimir datos** para q pueda descompirmirlos el dispositivo de destino
  - **cifrar los datos** para transmitirlos
- **Sesion** -> **crear y mantener dialogos entre las apps** de origen y destino
  - maneja intercambio de info para
    - **iniciar los idalogos y mantenerlos activos**
    - **reiniciar sesiones q se interrumpieron o q estuvieron inactivas**

Protocolos de Capa de Aplicacion

- **DNS -> usa TCP y UDP**
  - traduce nombres de dominio a direcciones IP
- **DHCP -> UDP**
  - permite que las **direcciones vuelvan a utilizarse cuando ya no son necesarias**
- **HTTP -> TCP**
  - conj de **reglas para intercambiar datos en la World Wide web**

De punto a punto
Modelo Cliente-Servidor

- hay 2 canales de comunicacion
  - Subida
  - Bajada

Aplicaciones punto a punto

- permite q un dispositivo funcione como cliente y como servidor dentro de la misma comunicacion
- usan un sistema hibrido -> cada par accede a un servidor indice para obtener la ubi de un recurso almacenado en otro par

Protocolos web y de correo electronico

Protocolo HTTP

POP -> usado por una app para recuperar correo electronico de un servidor

- **IMAP** -> se descargan **copias** de los mensajes a la app cliente -> mensajes originales quedan en el servidor -> en cambio en POP -> se descarga el original

DNS -> como una guia telefonica

- **Jerarquia**
    - sistema jerarquico para crear una bd que proporcione la resolucion de nombres

DHCP -> dynamic host client protocol

- provee
    - direccion IP
    - puerta de enlace
    - DNS
- si no se usa DHCP se hace de manera estatica
- Proceso
    - cliente desencadena mensaje de descubrimiento -.> **DHCP discover** -> busca si hay un servidor -> como un broadcast
    - servidor devuelve un mensaje con un pool de direcs -> **DHCP offer**
    - cliente solicita con un mensaje -> **DHCP Request**
    - servidor devuelve un **DCHPACK** -> reconoce al cliente q se ha finalizado la concesion

NOTA: **pool de direcs -> conjunto de direcs ip**
NOTA: Transporte abre y cierra .Sesion mantiene abiertas

FTP

- proceso
    - cliente establece la primera conexion al server para controla el trafico en el puerto TCP
    - cliente establece segunda conexion al servidor para la transfer de datos reales usando el puerto TCP
    - transferencia de datos puede ocurrir en cualquier direc -> cliente puede descargar datos del servidor o subirlos

SMB -> server message block

- 3 funciones
    - **iniciar, autenticar y terminar sesiones**
    - **controlar acceso a los archivos y a las impresoras**
    - **autorizar una app para enviar o recibir mensajes para o de otro dispositivos**
- permite poner usuario y contraseña
- conexion a largo plazo con los servidores
- despues de establecer ocnexion -> cliente -> accede recursos de server como si fuera local

Modulo 16: **Fundamentos de Seguridad**

Tipos de amenazas
- Robo de info
- perdida y manipulacion de datos
- robo de id
- interrupcion del servicio

Seguridad Fisica
- Amenazas de HW
- Amenazas Ambientales
- Amenazas electricas
- Amenazas de mantenimiento

Tipos de Firewalls
- filtrado de
    - paquetes
    - aplicaciones
    - url
- Inspeccion de paquetes con estado SPI -> paquetes entrantes -> respuestas legitimas a -> solicitudes de los hosts internos. Paquetes no solicitados -> bloqueados

Cisco AutoSecure
- Contraseñas seguras
- Mantener actualizados los sistemas operativos

Habilitar SSH
1. Configurar nombre de host unico
2. Configurar nombre de dominio con ip-domain name
3. Generar clave para cifrar el trafico SSH
4. Comprobar o crear una entrada de base de datos local con comando username
5. Autenticar contra la base de datos local con Login para autenticar la linea vty
6. Habilitar las sesiones vty SSH entrantes mediante transport input [ssh | telnet]

Deshabilitar servicios que no se utilice