Contents

1 introduccion

- internet surge de las investigaciones de la *advanced research projects agency* (ARPA), que incluye los estandares de redes y de como se comunican las computadoras
- los protocolos proveen la sintaxis y semantica de las comunicaciones, y permite separarla del hardware subyacente
- aplicaciones mas populares de internet: *world wide web*, mail, transmision de archivos, acceso remoto
- dos tipos de servicios: sin y con conexion

1.1 hardware

- dos tipos de tecnologia: broadcast y punto a punto
- unicasting: punto a punto con un solo emisor y receptor
- broadcast permite enviar a todos mediante un codigo especial en el campo de direccion
- multicast: algunos sistemas permiten enviar a un conjunto de receptores
- segun la escala: red de area personal, de area local, metropolitana y amplia
- interred: conexion de dos o mas redes (internet)

1.1.1 redes de area personal

- comunicacion dentro del rango de una persona, como una computadora con perifericos
- bluetooth, rfid

1.1.2 redes de area local

- redes de propiedad privada que operan dentro de un edificio
- todos se conectan a un *access point* (AP) para comunicarse
- cable de cobre, fibra optica
- ieee 802.3 ethernet
- vlan: dividir virtualmente una lan en varias
- colisiones ethernet clasica: se envia cuando el canal esta inactivo. si hay colision, se espera un tiempo aleatorio y se prueba de nuevo

- la asignacion del canal puede ser estatica, por ejemplo division por tiempo, o dinamica. la mayoria usa dinamica
- para asignacion dinamica se puede manejar de forma centralizada o no
- ethernet original
  - la ethernet original usaba cable coaxial
  - la conexion entre una computadora y el cable requiere un hardware especial llamado transreceptor
  - la otra parte era un adaptador que iba conectado a la computadora
- thin-wire ethernet
  - la original usaba componentes caros y dificiles de instalar
  - se creo un nuevo cable mas fino y mas barato
  - cubria menor distancia y no era tan resistente a interferencias
  - conexion directa con los hosts, y posibilidad de conectar computadoras directamente
- ethernet de par trenzado
  - con este tipo de cable no hace falta usar cables protegidos
  - mas baratos
  - cada host se conecta a un hub central que distribuye la señal
- fast ethernet: aumento de la velocidad de transmision con mejores cables
- 10/100 ethernet: puede operar a 10 o 100 mbps adaptandose en cada caso
- gigabit ethernet
- propiedades de ethernet
  - tecnologia de bus compartido
  - semantica de envio con el mejor esfuerzo
  - el control de acceso es distribuido porque no hay una autoridad central
  - esquema de acceso: csma/cd
- deteccion de colisiones y recuperacion
  - cuando se detecta una colision se espera un tiempo y se envia de nuevo
  - el tiempo es aleatorio y el rango se va duplicando cada vez que se detectan colisiones consecutivas
- direcciones
  - direcciones de 48 bits
  - *media access address* (mac)
  - unicast, multicast o broadcast

1.1.3 redes de area metropolitana

- cubren toda una ciudad
- redes de television por cable
- wimax

1.1.4 redes de a area amplia

- pais o continente
- empresa con sucursales repartidas en distintas ciudades

1.1.5 ethernet

1.2 sofware de red

1.2.1 jerarquia de protocolos

- organizacion por capas. cada capa tiene una funcion diferenciada e independiente
- intercambio de mensajes segun el protocolo de cada capa
- en realidad los mensajes bajan hasta la capa inferior (medio fisico), donde se realiza la comunicacion
- interfaz bien definida para comunicacion entre capas
- arquitectura de red: conjunto de capas y protocolos
- pila de protocolos: lista de protocolos usados por una arquitectura

1.2.2 aspectos de diseño para cada capa

- codigos de deteccion (y posible correccion) de errores
- enrutamiento: eleccion de una ruta para enviar informacion
- distribucion de protocolos en capas
- mecanismos para embalar, desembalar y transmitir
- escalabilidad
- asignacion eficiente de recursos
- uso del ancho de banda (multiplexado estadistico, fraccion fija)
- control de flujo
- confidencialidad, autenticacion e integridad

1.2.3 tipos de servicios

1. orientados a la conexion
   - se establece la conexion, se usa y se libera
   - en la mayoria de los casos se preserva el orden
   - como una linea telefonica
2. no orientados a la conexion
   - cada mensaje lleva la direccion de destino completa
   - cada mensaje es enrutado en forma independiente
   - como el sistema postal
3. confiables
   - nunca pierden datos
   - acuse de recibo
   - introduccion de sobrecarga y retardos
4. no confiables

	confiable	no confiable
conexion	secuencia de mensajes flujo de bytes	voz sobre ip
no conexion	mensajes de texto	mails

1.2.4 relacion entre servicios y protocolos

- un servicio se define como un conjunto de primitivas que una capa proporciona a la que esta encima de ella
- el servicio define el que pero no el como
- protocolo son las reglas de formato y significado de los paquetes o mensajes que se intercambian en la misma capa
- servicio se relaciona con las interfaces entre capas
- protocolo se relaciona con los paquetes que se envian entre distintas maquinas

1.3 modelos de referencia

1.3.1 modelo osi

1. capa fisica
   - transmision de bits puros a traves de un canal de transmision
   - busca que lleguen los mismos bits que salieron

- señales electricas para representar un bit
- como se establece y se termina una comunicacion

2. capa de enlace de datos
   - transforma los bits puros en una linea que este libre de errores para la capa de red
   - divide los datos en tramos
   - control de transmision para emisores rapidos y receptores lentos
3. capa de red
   - como se encaminan los paquetes del origen al destino
   - las rutas se basan en tablas estaticas o dinamicas
   - manejo de congestion
   - solucionar problemas para conectar redes heterogeneas
4. capa de transporte
   - aceptar datos de la capa superior, dividirlos en unidades mas pequeñas, pasar los datos a la capa de red y asegurar que las piezas lleguen al otro extremo
   - es una verdadera capa de extremo a extremo, a diferencia de las mas bajas
5. capa de sesion
   - control de dialogo
   - manejo de tokens
   - sincronizacion
6. capa de presentacion
   - se enfoca en la sintaxis y la semantica de la informacion transmitida
   - maneja estructuras abstractas para intercambiar datos entre computadoras con diferentes representaciones de datos
7. capa de aplicacion
   - protocolos que los usuarios necesitan

1.3.2 modelo tcp/ip

1. capa de enlace
   - capa sin conexion que opera a traves de distintas redes
   - describe que enlaces se deben llevar a cabo para cumplir con las necesidades de esta capa
2. capa de interred
   - permite que los host inyecten paquetes en cualquier red y que viajen independientemente a su destino

- analogo al sistema de correo
- define un formato de paquete y un protocolo oficial llamado ip y uno complementario llamado icmp
- el ruteo de paquetes es el principal aspecto, y la congestion

3. capa de transporte
   - permite que entidades en la misma capa mantengan una conversacion
   - tcp, udp
4. capa de aplicacion
   - reemplaza las capas de presentacion, sesion y aplicacion del modelo osi
   - telnet, ftp, smtp, dns, http

1.3.3 comparacion tcp/ip osi

- osi fue inventado antes que los protocolos, por eso es mas general. pero los diseñadores no sabian que funcionalidades colocar en cada capa
- con tcp/ip paso al reves. los protocolos encajaron perfectamente, pero no era util para describir redes que no fueran tcp/ip
- osi tiene 7 capas, tcp/ip tiene 4

1.3.4 defectos de osi

- mala sicronizacion: para cuando se desarrollaron los protocolos osi, tcp/ip ya se estaba usando lo suficiente como para que los distribuidores no quisieran apoyar otra pila
- mala tecnologia: el modelo es muy complejo. las capas de sesion y presentacion estan casi vacias, las de red y enlace llenas. son dificiles de implementar e ineficientes.
- malas implementaciones: por su complejidad las primeras implementaciones eran lentas y pesadas. despues mejoraron pero la imagen quedo
- malas politicas: osi se asocio con el gobierno estadounidense y tcp/ip con unix

1.3.5 defectos de tcp/ip

- no se diferencian bien los conceptos de servicio, interfaz y protocolo
- el modelo no es para nada general
- la capa de enlace no es una capa sino una interfaz
- no distingue la capa de enlace y la fisica

2 capa fisica

2.1 conceptos

- serie de fourier
- ancho de banda
- banda base: desde 0 hasta una frecuencia maxima, pasa-banda: se desplazan para ocupar un rango mas alto
- teorema de nyquist: tasa de datos maxima de un canal sin ruido. tasa de muestreo
- teorema de shannon: tasa de datos maxima incluyendo la relacion señal ruido S/N

2.2 medios de transmision guiados

2.2.1 medios magneticos

- guardar la informacion en una cinta o medio removible y mandarlo fisicamente
- *nunca subestime el ancho de banda de una camioneta repleta de cintas que viaje a toda velocidad por la carretera*

2.2.2 par trenzado

- dos cables de cobre aislados
- trenzados porque en paralelo forman una antena
- la señal se transmite como la diferencia de voltaje entre los dos cables
- el ruido afecta a los dos cables por igual, el diferencial se mantiene
- sistema telefonico
- informacion analogica o digital
- el ancho de banda depende del grosor de los cables y la distancia. hasta varios mbps
- ethernet usa cuatro, uno para cada direccion
- hasta cat 6: utp (unshielded twisted pair). cat 7: stp

2.2.3 cable coaxial

- mejor blindaje y mayor ancho de banda que los tp, pero mas caro

2.2.4 lineas electricas

- las compañias las han utilizado para comunicacion de baja velocidad
- uso en el hogar para controlar dispositivos
- dificil porque el cableado de las casas no esta hecho para enviar señales a alta frecuencia

2.2.5 fibra optica

- lan, internet y ftth
- un pulso de luz indica 1, la ausencia 0
- cuando la luz pasa de un medio a otro (silice a aire) se refracta. el grado depende de los indices de refraccion de los medios. y para cualquier angulo mayor a un angulo critico la luz rebota completamente en el silice
- fibra multimodal: varios rayos de luz en una fibra
- fibra monomodo: un solo rayo de luz por fibra que es mucho mas angosta
- tres bandas: 0.85 1.3 y 1.55 micras. anchos de banda de 25000 a 30000 ghz. la primera tiene mas atenuacion
- fuentes: led y laser

2.3 transmision inalambrica

2.3.1 espectro electromagnetico

- los electrones se mueven y crean ondas electromagneticas
- las ondas viajan siempre a la velocidad de la luz
- $\lambda f = c$ relacion entre frecuencia f, longitud de onda λ y velocidad de la luz c
- espectro directo con salto de frecuencia: transmision dificil de detectar y bloquear. militares, bluetooth, versiones anteriores de 802.11
- espectro disperso de secuencia directa: multiples señales comparten ancho de banda. cdma (barker codes), gps, 802.11b
- uwb (banda ultra ancha)

2.3.2 radiotransmision

- las ondas de radio son faciles de generar, recorren largas distancias y penetran edificios
- son omnidireccionales
- las propiedades dependen de la frecuencia. baja frecuencia: cruzan obstaculos pero se reduce la potencia rapidamente. alta frecuencia: viajan en linea recta y rebotan en obstaculos
- ondas de alta frecuencia son absorbidas por la lluvia y otros obstaculos
- como recorren grandes distancia la interferencia es un problema
- estan reguladas por los gobiernos
- vlf, lf y mf siguen la curvatura de la tierra. hf van en linea recta y rebotan en la ionosfera, tambien son absorbidas por la tierra

2.3.3 transmision por microondas

- relacion S/N alta, pero las antenas deben estar alineadas
- microondas no atraviesan bien los edificios
- comunicacion telefonica, celulares, television. lo que provoco escasez de espectro

2.3.4 transmision infrarroja

- comunicacion de corto alcance
- no atraviesan objetos

2.3.5 tranmision por ondas de luz

- señalizacion optica mediante laser
- gran ancho de banda a bajo costo y seguro. pero muy dificil de apuntar

2.4 satelites de comunicacion

- un satelite es un enorme repetidor de microondas con varios transpondedores. transmite en modo **tublo doblado**
- posicion de los satelites limitadas por el cinturon de van allen

2.4.1 satelites geoestacionarios

- satelites que orbitan a la misma velocidad de la que rota la tierra. parecen inmoviles desde el suelo
- los primeros tenian un solo haz de luz que iluminaba la tierra, lo que se conoce como huella
- actualmente tienen multiples haces que se enfocan en una pequeña area geografica. estos son los haces puntuales
- vsat: terminales muy pequeñas que se utilizan para la transmision de tv
- los vsat no se pueden comunicar entre ellos por su baja potencia. para ello usan de intermediario potentes estaciones en la tierra
- aunque las señales viajen a la velocidad de la luz, dada las distancias tienen mas retardo que las comunicaciones terrestres
- los satelites son medios de difusion por naturaleza

2.4.2 ventajas de los satelites sobre la fibra optica

- cuando se requiere un despliegue rapido, ganan los satelites
- los satelites pueden enviar a cualquier parte del mundo
- un mensaje que envia un satelite lo pueden recibir miles de estaciones al mismo tiempo

2.5 modulacion digital y multiplexacion

- modulacion digital: proceso de convertir bits en la señal que los representan
- transmision en banda base: la señal ocupa una frecuencia desde 0 hasta un valor maximo que depende de la tasa de señalizacion. comun en cables
- transmision pasa-banda: la señal ocupa una banda de frecuencias alrededor de la frecuencia de la señal portadora. comun en inalambrico y optico
- multiplexacion: a compartir varias señales por un mismo canal

2.5.1 transmision en banda base

- NRZ(non-return-to-zero): voltaje positivo para el 1 y uno nulo para el 0
- el receptor muestrea a intervalos regulares y convierte de nuevo a bits. la señal no se vera igual a la que se envio por el ruido y el canal
- eficiencia del ancho de banda
  - con nrz la señal puede alternar entre positivo y negativo hasta cada 2 bits. necesita un ancho de banda B/2hz pasa tasa de B bps
  - una estategia es usar mas de 2 niveles de señalizacion. por ejemplo 4 voltajes para representar 2 bits a la vez como un simbolo
  - tasa de bits=tasa de simbolo*bits por simbolo
  - requiere una potencia mayor en el receptor para diferenciar los niveles
- recuperacion del reloj
  - el receptor debe saber cuando termina un simbolo y empieza otro
  - existe un limite en la precision de un reloj para muestrear señales
  - se podria enviar una señal del reloj por otra linea separada, pero seria mejor que si hubiera otra linea se usara para enviar datos
  - un truco seria usar xor entre las dos lineas para enviarlas en una sola. esta es la codificacion manchester y se usaba en ethernet clasico. lo malo es que requiere el doble de ancho de banda
  - una estrategia distinta es codificar los datos para que haya suficientes transiciones en la señal. ya que los problemas suceden en largas sucesiones de 0 o 1
  - nrzi: 1 como una transicion y 0 como no hay transicion. usb usa este metodo. largas sucesiones de 1 no tienen problemas, pero de 0 si
  - 4b/5b: se asocian grupos de 4 bits a 5 bits segun una tabla fija, de manera que nunca haya tres 0 seguidos. agrega 25% de sobrecarga. sobran 16 numeros de 5 bits, algunos se usan para control
  - para asegurar transiciones se puede hacer xor con una secuencia pseudoaleatoria. el receptor decodifica con la misma secuencia. esta debe ser facil de generar

  - pero la aleatorizacion no garantiza transiciones

- señales balanceadas
  - señales que tienen misma cantidad de voltajes positivos como negativos
  - ayuda a proveer transiciones para la recuperacion del reloj
  - codificacion bipolar: se alterna +1 y -1 voltios para el 1 y 0 voltios para el 0. en redes telefonicas ami
  - 8b/10b tambien para codigo balanceado

2.5.2 transmision pasa-banda

- en canales inalambricos no es practico usar rango de frecuencias que empiecen en 0
- se puede tomar una señal en banda base que ocupe de 0 a b hz y desplazarla a otra pasa-banda que ocupe de s a s+b hz
- se puede modular la amplitud (ask), la frecuencia (fsk) o la fase (psk)
- psk puede ser bpsk (binaria) o qpsk (cuadratura)
- se pueden combinar y usar mas niveles, comunmente amplitud y fase
- diagrama de constelacion: forma de visualizar la modulacion combinada ask y psk. qpsk, qam-16, qam-64
- simbolos adyacentes no deben diferir en muchos bits, porque serian mas suceptibles al ruido. para eso se usa codigo gray

2.5.3 multiplexacion por division de frecuencia

- fdm: divide el espectro en bandas. cada usuario tiene posesion exclusiva de la banda
- banda de guarda: exceso de banda que mantiene a los canales separados
- ofdm: el ancho de banda del canal se divide en muchas subportadoras que envian de manera independiente. cada subportadora esta diseñada para ser 0 en el centro de las adyacentes. 802.11

2.5.4 multiplexacion por division de tiempo

- tdm: los usuarios toman turnos y usan todo el ancho de banda, se toman los datos y se agregan al flujo agregado
- para que funcione debe haber sincronizacion. se puede agregar tiempo de guarda

2.5.5 multiplexacion por division de codigo

- cdm: forma de comunicacion de espectro diverso. una señal de banda estrecha se dispersa en una mas amplia. cdma
- hace la señal mas tolerante a interferencias y permite que señales compartan la misma banda de frecuencia
- cdma es extraer la señal deseada mientras lo demas se rechaza como ruido
- cada tiempo de bit de divide en m intervalos llamados chips. en general 64 o 128 chips cada bit. a cada estacion se le asigna una secuencia de chip, un codigo de m bits. para transmitir un 1 envia la secuencia de chip, para el 0 la negacion
- todas las secuencias de chip son ortogonales por pares
- si varias estaciones envian al mismo tiempo se suman

3 capa de enlace

3.1 cuestiones de diseño

- funciones: dar a la capa de red una interfaz de servicios bien definida. manejar errores. controlar flujo
- toma los datos que obtiene de la capa de red y los encapsula en tramas

3.1.1 servicios dados a la capa de red

- transferir datos de la maquina de origen a la de destino
- 3 servicios razonables
  - sin conexion ni confirmacion de recepcion: tasa de error baja. trafico en tiempo real. ethernet
  - sin conexion con confirmacion: canales no confiables. 802.11 (wifi)
  - con conexion y confirmacion: cada trama esta enumerada. se garantiza que lleguen solo una vez y en orden. canales largos y no confiables. satelites y red telefonia larga

3.1.2 entramado

- la capa fisica no garantiza que el flujo de bits este libre de errores
- un metodo es dividir el flujo en tramas discretas y agregarles una suma de verificacion
- division de tramas
  - conteo de bytes: agrega en el encabezado la cantidad de bytes en la trama. si se altera este valor se pierde la sincronia. rara vez se usa solo

  - bytes bandera con relleno de bytes: cada trama inicia y termina con bytes especiales. si aparece la bandera en los datos se antecede un escape. y si aparece un escape se pone otro escape adelante. simplificacion de ppp
  - bits bandera con relleno de bits: igual a bytes pero sin la restriccion de 1 byte=8 bits. hdlc. usb. se usan 6 bits en 1 para delimitar. cada vez que se ven 5 bits en 1 se agrega un 0
  - violaciones de codificacion de la capa fisica: si se usa por ejemplo 4b/5b en la capa fisica se pueden usar los codigos no utilizados para el inicio y fin de trama

3.1.3 control de errores

- asegurar la entrega de datos confiable: retroalimentacion al emisor de lo que esta ocurriendo del otro lado. positiva y negativa
- puede desaparecer la trama por completo, o la de retroalimentacion. para eso tambien se usan temporizadores para enviar nuevamente
- ahora puede que se reciba la misma trama dos veces. para eso se usan numeros de secuencia

3.1.4 control de flujo

- que hacer cuando un emisor envia mas tramas de las que el receptor puede aceptar. ejemplo telefono y sitio web
- control de flujo basado en retroalimentacion: el receptor envia cuando puede aceptar mas datos
- control de flujo basado en tasa: el protocolo tiene un mecanismo integrado que limita la tasa de envio

3.2 deteccion y correccion de errores

- estategia: incluir redundancia en los datos.
- codigo de correccion de errores: para que el receptor pueda deducir que datos se quisieron enviar. fec
- codigo de deteccion de errores: para que sepa que hubo un error pero nada mas y solicite retransmision
- en fibra optica conviene la deteccion porque es rapido reenviar. en canales inalambricos es mejor correccion
- los bits de redundancia tambien pueden llegar mal. asi que nunca se podran manejar todos los errores
- los errores en rafaga tienen sus ventajas y desventajas

3.3 protocolos de enlace de datos

3.3.1 paquetes sobre sonet

- sonet se utiliza sobre canales de fibra optica de area amplia
- ppp se usa para diferenciar paquetes ocasionales del flujo continuo en el que se transportan

3.3.2 ppp

- ppp orientado a bytes, hdlc a bits
- metodo de entramado sin ambiguedades, tambien maneja deteccion de errores
- protocolo para activar lineas, probarlas, negociar y desactivarlas. lcp
- mecanismo para negociar opciones de capa de red independientemente del protocolo de red usado
- uso de banderas como delimitacion y bytes de escape
- la carga util se mezcla aleatoriamente antes de insertarla en sonet para garantizar mas transiciones que necesita sonet
- configuracion enlace ppp
  - muerto
  - establecer (cuando hay conexion en la capa fisica): intercambio de paquetes lcp
  - autentificar (si lo anterior fue exitoso): se verifican identidades
  - red: paquetes ncp para configurar la capa de red
  - abrir: intercambio de datos
  - terminar

4 subcapa control acceso al medio

- los enlaces de red pueden ser punto a punto o difusion
- subcapa mac es la parte inferior de la de enlace de datos

4.1 problema de asignacion de canal

- asignar un solo canal de difusion entre varios usuarios competidores

4.1.1 asignacion estatica

- dividir la capacidad mediante el uso de multiplexacion. cuando hay una pequeña cantidad de usuarios constantes
- si varia el numero de emisores y ese numero es grande se vuelve ineficiente
- lo mismo sucede con otras formas estaticas de dividir un canal

4.1.2 supuestos para la asignacion dinamica

- trafico independiente: las estaciones son independientes
- canal unico: hay un solo canal para todas las comunicaciones
- colisiones observables: todas las estaciones pueden detectar colisiones. que seran enviadas luego
- tiempo continuo o ranurado: se puede considerar de las dos maneras
- deteccion de portadora o sin deteccion: si hay deteccion las estaciones pueden saber si el canal esta en uso. sino mandan y despues determinan si tuvo exito

4.2 protocolos de acceso multiple

4.2.1 aloha

- aloha puro
  - despues de enviar su trama a la computadora central, esta difunde la trama a todas las estaciones. asi el emisor sabe si llego su trama
  - si la trama fue destruida espera un tiempo aleatorio y manda de nuevo
  - cada vez que dos tramas intenten ocupar el canal al mismo tiempo habra colision, por mas que sea un solapamiento pequeño
- aloha ranurado
  - como el metodo puro pero el tiempo se divide en ranuras discretas
  - sincronizacion por medio de una estacion que emita una señal al comienzo de cada intervalo

4.2.2 protocolos de acceso multiple con deteccion de portadora

- csma persistente-1
  - la estacion escucha el canal para ver si alguien esta enviando, sino envia. si ocurre una colision espera y manda de nuevo
  - el retardo de propagacion tiene un efecto importante en las colisiones. esta posibilidad depende del numero de tramas que quepan, o producto de ancho de banda-retardo
  - en lan como el retardo es pequeño, no habra muchas colisiones
- csma no persistente
  - a diferencia del persistente-1 si el canal esta en uso espera un tiempo y repite el proceso. no se queda escuchando constantemente
  - mejor uso del canal pero mayor retardo
- csma persistente-p

  - para canales ranurados
  - si el canal esta inactivo, envia con probabilidad p y espera a la siguiente ranura con probabilidad 1-p

- csma con deteccion de colisiones (csma/cd)
  - base de la clasica ethernet
  - el hardware escucha a la vez que envia. si la señal que recibe es distinta a la que envia, esta ocurriendo una colision
  - periodos alternantes de contencion y transmision con periodos de inactividad que ocurriran cuando todas las estaciones esten en reposo

4.2.3 protocolos libres de colisiones

- protocolo de mapa de bits
  - cada periodo de contencion consiste en n ranuras
  - las estaciones envian 1 si tienen tramas para enviar en ese periodo pero solo en su ranura correspondiente
  - luego cuando ya hay conocimiento de quien va a mandar mandan las tramas en orden
  - protocolos de revervacion

- paso de token
  - pasa un pequeño mensaje llamado token de una estacion a otra en un orden determinado. token ring
  - solo puede enviar la que tenga el token
  - cuando la estacion que envio recibe su misma trama la elimina para terminar el ciclo
  - no hace falta que sea un anillo. token bus

- conteo descendente binario
  - anteriores no escalan a redes con miles de estaciones
  - las estaciones que quieren usar el canal envian su direccion binaria y hacen or de todo lo que reciben
  - tan pronto como una estacion ve que una posicion de bit de orden alto, cuya direccion es 0, ha sido sobreescrita por un 1, se da por vencida

4.2.4 protocolos de contencion limitada

- en condicion de carga ligera es preferible contencion
- al reves para libres de colision
- protocolos de contencion limitada combinan los dos anteriores
- protocolo de recorrido de arbol adaptable

  - en la ranura 0 todas las estaciones intentan adquirir el canal. si una lo logra bien y sino se dividen en dos grupos y se va formando un arbol de decision
  - a mayor carga la busqueda debe iniciar mas abajo en el arbol

4.2.5 protocolos de lan inalambrica

- problema de la terminal oculta
- problema de la terminal expuesta
- maca (acceso multiple con prevencion de colisiones)
  - el emisor estimula al receptor para que envie una trama corta. las estaciones cercanas tambien escuchan y evitan enviar a la vez
  - rts/cts
  - en caso de colision un transmisor espera un tiempo y vuelve a intentar de nuevo

4.3 ethernet

- 802.3
- ethernet clasica (visto hasta ahora) y conmutada (switches)

4.3.1 capa fisica de ethernet clasica

- un solo cable de donde se conectaban todas las maquinas
- ethernet gruesa 500m y 100 maquinas
- ethernet delgada 185m y 30 maquinas
- longitud maxima por segmento conectada con repetidores

4.3.2 protocolo de subcapa mac para ethernet clasica

- multidifusion (a un grupo de estaciones) y difusion (a todas)
- direcciones globalmente unicas
- el tipo especifica a que proceso darle la trama
- campos tipo y longitud en conflicto. despues se usaron los dos: se interpreta segun si es mayor a la maxima longitud
- tamaño de trama maximo y minimo. se puede rellenar
- csma/cd
  - tras una colision el tiempo se divide en ranuras discretas de longitud igual a la ida y vuelta para el peor caso del cable
  - retroceso exponencial binario: despues de la colision n cada estacion espera de 0 a 2^n-1 ranuras para enviar de nuevo

4.3.3 ethernet conmutada

- se empezaron a usar hubs en vez de un solo cable
- las redes se podian saturar porque los hubs no incrementan la capacidad. de ahi se empezaron a usar los switch
- los switches envian tramas solo a los puertos para los que estan destinadas
- en un switch cada puerto es su dominio de colision independiente
- si el cable es full duplex (comun) no hay colisiones. si es half duplex se usa csma/cd
- en un hub las tramas se envian a todos, aumentando la probabilidad de intrusos
- un switch puede tener conectado un hub, asi actua como un concentrador

4.3.4 fast ethernet

- se mantuvo la ethernet anterior pero mas rapida
- se permiten tres medios: par trenzado categoria 3 y 5, fibra optica
- casi todos los switches pueden manejar 10mbps (anterior) o 100mbps (fast)

4.3.5 gigabit ethernet

- en half duplex se usa csma/cd, en full duplex no
- con 1gbps una trama minima que es enviada no llegaria a recorrer el cable antes que termine de enviar, por eso de limito la longitud a 200m
- extension de portadora: el hardware agrega datos para hacer la trama de 512 bytes. no hay que hacer cambios de software
- rafaga de tramas: el emisor envia una secuencia de tramas concatenadas en una sola transmision. si hay suficientes tramas, es preferible a la extension de portadora
- en la actualidad la mayoria de las interfaces ethernet soportan los 3 tipos

4.3.6 10 gigabit ethernet

4.4 redes lan inalambricas

- medio de comunicacion ondas electromagneticas
- tres tipos de redes: wpan, wlan, wwan
- modelos basados en pila: osi, tcp/ip, otros

4.4.1 wi-fi o wlan

- capa fisica y enlace de osi
- 802.11
- arquitectura celular: el sistema se subdivide en celdas. cada celda (bss) se controla por una estacion (ap)
- la capa fisica
  - funciones
    - codificacion/decodificacion de las señales
    - generacion/remocion de cabeceras
    - transmision/recepcion de bits
    - especificaciones del medio de transmision
  - fhss(espectro disperso con salto de frecuencia): transmision en intervalos de tiempo a frecuencias distintas que el emisor y el receptor conocen. resistente al ruido y mas seguro
  - dsss(espectro disperso con secuencia directa): transmitir con una secuencia de bits de alta velocidad llamados chips. secuencia de barker
  - mimo(multiple entrada/multiple salida): aparatos con varias antenas para generar subcanales de transmision
- capa de enlace
  - funciones
    - capa control acceso al medio
      - transmision: ensamblado de datos en tramas con campos de direccionamiento y deteccion de errores
      - recepcion: desensamblado de tramas, reconocimiento de direcciones y deteccione de errores
      - administra acceso al medio de transmision
    - capa control de enlace logico
      - interface a las capas superiores, control de errores y flujo
  - a diferencia de ethernet para wifi debe haber acuse de recibo
  - puede darle el problema de que una estacion no llegue a escuchar cuando otra en la misma red este mandando y se produzcan colisiones. estacion oculta
  - rts/cts
  - dcf: mecanismo basico de csma/ca. primero se verifica que nadie use el canal. las estaciones retardan aleatoriamente las tramas y luego escuchan para evitar colisiones. a veces usan rts/cts
  - pcf: tecnica de interrogacion circular desde el ap. servicios de tipo sincrono
- funciones de deteccion de portadoras

  - para deetrminar si el medio se encuentra disponible
  - dos tipos: de la capa fisica y deteccion de portadoras virtuales(nav)
- espaciamiento intertrama: cuatro diferentes espaciamientos para diferentes prioridades
- tres tipos de trama: datos, control y gestion
- control de enlace logico
  - direccionamiento de estaciones conectadas al medio y control de flujo
  - basado en el protocolo hdlc
  - 3 tipos de servicios: sin conexion y sin reconocimiento, con y sin, sin y con

4.4.2 wpan

- dispositivos perifericos
- bluetooth, homerf, zigbee, infrarrojo
- bluetooth
  - clase 1, 2 y 3 segun la potencia
  - piconet
    * un nodo maestro y hasta 7 nodos esclavos activos. hasta 255 en total
    * puede haber varias piconets conectadas de un nodo esclavo puente(scatternet)
    * capa fisica
      · sistema de baja potencia. pocos metros
      · 79 canales de 1mhz. modulacion desplazamiento de frecuencia
      · misma banda que 802.11 pero es mas problable que bluetooth interfiera con 802.11 que al reves
    * capa banda base
      · perecido a la capa mac
      · multiplexion por division de tiempo: el maestro transmite en ranuras pares y los esclavos en impares
      · enlace acl: capa l2cap. mejor esfuerzo
      · enlace sco: datos en tiempo real. se asigna una ranura fija a cada direccion. no se retransmiten datos
    * administrador de enlace
    * capa adaptacion y control de enlace logico(l2cap)
      · acepta paquetes de capa superior y los divide en tramas
      · maneja la multiplexion
      · se encarga de la calidad de los requerimientos de servicio. establece enlaces, negocia el tamaño de carga util
- bluetooth smart(ble)

  - 40 canales de 2mhz
  - no es directamente compatible con el anterior. si en modo dual(smart ready)
  - topologia broadcasting
    * enviar datos a cualquier dispositivo que este escuchando el medio
    * envia periodicamente paquetes de anuncio por canales especificos
  - topologia conexiones
    * conexion permanente y periodicamente se intercambian datos entre maestro y esclavo
  - un dispositivo puede ser maestro y esclavo. un maestro puede ser conectado a multiples esclavos. un esclavo a multiples maestros
  - perfiles genericos: perfil de acceso generico(gap), perfil de atributo generico(gatt)
  - capa de enlace
    * varios estados
      · espera: no transmite ni recibe. modo ahorro
      · anuncio: un esclavo envia paquetes en canales de anuncio. recibe tambien desde un maestro
      · exploracion: escucha los paquetes de anuncio que envian los dispositivos
      · inicializacion: usado por el maestro antes de iniciar una conexion. escucha hasta que recibe el anuncio de un esclavo deseado y se conecta

4.4.3 sistema de telefonia y comunicaciones moviles

- division celular: dividir en zonas pequeñas donde se reutilizan canales disponibles
- reutilizacion de frecuencias
  - se asigna a cada celda un grupo de frecuencias, de modo que no se compartan con celdas vecinas
  - el grupo de celdas que no comparten canales se llama cluster
- modo de funcionamiento
  - simplex: no se puede transmitir y recibir simultaneamente por enlaces de subida y bajada
  - duplex: los dos enlaces usan portadoras distintas y se pueden usar a la vez
- desde 1g hasta 4g+. 5g sin estandarizar
- arquitectura
  - equipo de usuario: contiene una tarjeta que le permita usar el servicio. se conecta a traves de una interfaz de radio
  - red de acceso: sustenta la transmision de radio con los usuarios para conectarlos con la red troncal
  - red troncal: control de acceso, gestion de movilidad, gestion de sesiones de datos, etc
- tipos de redes de acceso: gerand/utran(3g) y e-utran(lte)

- la red troncal se divide en tres
  - dominio de circuitos: todas las entidades que dan servicios basados en conmutacion de circuitos. accesible a traves de geran y utran, e-utran no usa
  - dominio de paquetes: basado en conmutacion de paquetes. dos implementaciones: gprs y epc. gprs fue la primera en contexto de las redes anteriores. epc es la nueva de lte
  - subsistema ims: provision de servicios ip basados en el protocolo sip. asociada a lo multimedia y utiliza servicios del dominio de paquetes
- arquitectura de lte
  - eps(evolved packet system), enteramente basada en paquetes ip, tanto servicios en tiempo real como transmision de datos
  - los componentes son: la red e-utran, el dominio de paquetes epc y el sistema ims
  - contempla el acceso al servicio de redes utran y geran, y otras redes que no pertenecen a la misma familia
  - la red de acceso se compone de una unica entidad enb, que proporciona conectividad entre usuarios y la red troncal
  - enb usa tres interfaces: e-utran uu(usuarios-enb), s1(enb-troncal) y x2(enb-enb)
- capa fisica
  - ofdma para enlace descendente y sc-fdma para ascendente
  - qpsk, 16qam y 64qam descendente, qpsk, 64qam ascendente
- interfaz de radio
  - tres tipos de transferencia: difusion de señalizacion de control, envio de paquetes ip y transferencia de señalizacion de control
- ofdma
  - diversidad multiusuario: la asignacion de subportadoras se realizan dinamicamente
  - diversidad frecuencial: es posible asignar al usuario subportadoras no contiguas, suficientemente separadas
  - robustez en la propagacion multicamino: fuerte a la interferencia intersimbolica por la propagacion por multiples caminos
  - flexibilidad de banda asignada: permite acomodar las velocidades a usuarios segun lo que requieran
  - granularidad en recursos asignables: para acomodar servicios con diferente calidad
  - elevada relacion entre potencia media e instantanea
  - suceptibilidad a errores de frecuencia: cuando hay desplazamientos de frecuencia hay interferencias. se requieren mecanismos de sincronizacion
- sc-fdma

- variaciones reducidas entre potencia media e instantanea
- posibilidad de llevar a cabo de forma sencilla mecanismos de ecualizacion en el dominio de la frecuencia
- capacidad de proporcionar asignacion de banda flexible

4.5 conmutacion de la capa de enlace de datos

- lan de lanes con puentes

4.5.1 usos de puentes

- universidades y departamentos tienen sus propias redes lan separadas, pero tambien requieren comunicarse entre ellas
- la organizacion puede estar separada geograficamente
- dividir una sola red lan en varias para alivianar la carga
- dos algoritmos para que los puentes sean transparentes

4.5.2 puentes de aprendizaje

- cada puerto del switch define un dominio de colision
- si una estacion se quiere comunicar con otra dentro del mismo segmento el switch debe descartar las tramas porque no es necesario reenviarlas
- mediante una tabla hash los switches saben a que segmento pertenecen las estaciones
- cuando llega una trama al puente se fija la hora y actualiza el puerto si cambio. por si se modificaran las topologias
- si no conoce por cual puerto enviar una trama. se envia a todos excepto por el que vino
- **conmutacion al vuelo**: es posible empezar a reenviar ni bien se lea la cabezera de una trama, que contiene la direccion

4.5.3 puentes con arbol de expansion

- enlaces redundantes. si se corta uno la red no se dividira en dos. pero crea ciclos en la topologia
- los puentes ejecutan un algoritmo distribuido para construir el arbol
- incluyen la distancia desde la raiz para recordar la ruta mas corta. desactivan los puertos que no formen parte de esa ruta

4.5.4 redes lan virtuales

- agrupar a los usuarios en diferentes lan para reflejar la estructura de la organizacion
- seguridad: por ejemplo separar servidores de computadoras de uso publico
- carga: algunas lan se usan mucho mas que otras
- trafico de difusion
- las redes vlan se basan en switches diseñados para este proposito. el administrador decide cuantas vlan habra y como se llamaran
- tablas de configuracion en los puentes. que vlan se puede acceder por un puerto
- estandar 802.1q
  - se cambio el encabezado de ethernet. tiene una nueva etiqueta vlan
  - los campos de vlan no los deben ver los usuarios, solo puntes y conmutadores
  - cuando una trama llega al primer switch con soporte para vlan agrega los campos y el ultimo los elimina

5 capa de red

5.1 aspecto de diseño

5.1.1 conmutacion de paquetes de almacenamiento y reenvio

5.1.2 servicios proporcionados a la capa de transporte

- independientes de la tecnologia del enrutador
- la capa de transporte debe estar aislada del tipo, cantidad y topologia de enrutadores
- plan de numeracion uniforme para las direcciones disponibles

5.1.3 implementacion del servicio sin conexion

- los paquetes se transmiten por separado y se enrutan de manera independiente
- datagramas
- ip

5.1.4 implementacion del servicio orientado a la conexion

- evitar la necesidad de elegir una nueva ruta para cada paquete enviado. cuando se establece una conexion se guarda la ruta
- mpls: usa vez que se establece el circuito virtual los enrutadores intermedios asignan identificadores diferentes para origenes diferentes para diferenciarlos en una misma ruta

5.2 algoritmos de enrutamiento

- un enrutador tiene dos procesos internos: uno maneja cada paquete conforme llega y busca en la tabla de ruteo la linea de salida. el otro es llenar y actualizar las tablas de ruteo, y ahi es donde entra el algoritmo de ruteo
- muchas redes intentan reducir el numero de saltos que debe dar un paquete
- no adaptativos: no basan sus decisiones en mediciones de trafico y topologia actuales. las rutas se elijen de antemano. enrutamiento estatico
- adaptativos: no no adaptativos. enrutamiento dinamico

5.2.1 principio de optimizacion

- si una ruta es optima para i->j->k, tambien es optima para j->k
- arbol sumidero: el conjunto de rutas optimas

5.2.2 algoritmo de la ruta mas corta

- ver la red como un grafo y buscar el camino mas corto
- corto puede ser el numero de saltos, distancia geografica, u otras metricas

5.2.3 inundacion

- tecnica local. el enrutador envia por todas las lineas excepto por la que vino el paquete
- gran cantidad de duplicados
- numero maximo de saltos en la cabecera
- numero de secuencia en paquetes para no enviarlos dos veces
- no es practico para la mayoria de envios. pero tienen usos importantes como la difusion, porque asegura que todas las estaciones reciban el paquete
- es en extremo robusta
- requiere poca configuracion
- siempre encuentra la ruta mas corta, sin contar el congestionamiento que provoca el algoritmo

5.2.4 enrutamiento por vector de distancia

- cada enrutador mantiene un vector (una tabla) con la mejor ruta para cada destino. esta tabla se va actualizando
- cada T ms cada enrutador manda a sus vecinos su tabla
- problema del conteo al infinito: la convergencia llega a la respuesta correcta, pero lo hace lentamente

5.2.5 enrutamiento por estados de enlace

- las variantes is-is y ospf son usadas en la actualidad en internet
- descrubrir a sus vecinos
  - cuando un enrutador se pone en funcionamiento envia paquetes por todas las lineas que son respondidos con informacion de los vecinos

5.2.6 enrutamiento jerarquico

5.2.7 enrutamiento por difusion

5.2.8 enrutamiento multidifusion

5.2.9 enrutamiento anycast

5.2.10 enrutamiento para hosts moviles

5.2.11 enrutamiento para redes ad hoc

5.3 algoritmos de control de congestion

- las capas de red y transposte manejan la congestion
- el control de congestion lo hace la red como conjunto. control de flujo se hace entre un emisor y receptor en particular

5.3.1 metodos para control de congestion

- la presencia de congestion significa que la carga es mayor que los recursos
- la manera mas basica es contruir una red que coincida con el trafico que transmita
- aprovisionamiento: enrutadores y enlaces que se utilicen mucho son los que se actualizan primero
- enrutamiento conciente de trafico: las rutas se pueden ajustar segun patrones de trafico
- cuando no es posible aumentar la capacidad hay que reducir la carga, como rechazar nuevas conexiones (control de admision)
- reconocer cuando empieza la congestion: para eso se monitorean la carga promedio, retardo de encolamiento y perdida de paquetes
- como avisar a las fuentes: debe haber retroalimentacion. hay que ajustar la escala de tiempo con cuidado
- si falla todo hay que empezar a descartar paquetes

5.3.2 enrutamiento conciente de trafico

5.3.3 control de admision

- usada en redes de circuitos virtuales
- no agregar conexiones a menos que no lleve a congestion de la red
- como saber cuando una conexion generara congestion?
- describir tasa de transmision de una forma simple pero significativa es dificil
- leaky bucket o token bucket: vincula la tasa promedio y el tamaño de la rafaga instantanea de trafico
- se puede usar el comportamiento pasado para estimar el numero de circuitos que admite una red

5.3.4 regulacion de trafico

- la red aspira a operar justo antes de que empiece la congestion
- los enrutadores deben determinar cuando se acerca. se puede usar enlaces de salida, **bufer de paquetes en cola**, numero de paquetes que se pierden
- tambien deben entregar una retroalimentacion a los que generan congestion
- paquetes reguladores: se avisa al origen que su paquete provoca congestion, con un bit en el encabezado. el emisor puede esperar un poco y reenviar
- notificacion explicita de congestion (ecn): el enrutador reenvia paquetes congestionados con el encabezado modificado. cualquiera que lo recibe sabe el estado de la red y actua
- contrapresion de salto por salto: los paquetes reguladores surten efecto en todos los puntos intermedios

5.3.5 desprendimiento de carga

- cual paquete tirar depende de la aplicacion
- un desprendimiento mas inteligente requiere cooperacion de los emisores. por ejemplo paquetes que mandan informacion de enrutamiento
- las aplicaciones pueden marcar que tan importante son los paquetes

5.4 calidad de servicio

- exceso de aprovisionamiento: contruir una red con la suficiente capacidad para el trafico que maneje. mas costoso. a veces no se puede predecir los cambios en la cantidad de trafico
- cuatro aspectos para asegurar la calidad de servicio:
  - lo que las aplicaciones necesitan de la red

  - como regular el trafico que entra en la red
  - como reservar recursos en los enrutadores para garantizar el desempeño
  - si la red puede aceptar mas trafico de forma segura

5.4.1 requerimientos de la aplicacion

- parametros que caracterizan las necesidades de cada flujo: ancho de banda, retardo, variacion de retardo, perdida

5.4.2 modelado de trafico

-

5.5 ipv4

- conmutacion de paquetes
- servicio sin conexion

5.5.1 objetivos

- funcion de ruteo
- transparencia en la red de redes
- reglas de entrega de paquetes no confiable
- unidad basica: datagrama

5.5.2 formato

- tamaño variable por posibilidad de incluir opciones
- campo type of service para informar como debe ser tratado el paquete

5.5.3 fragmentacion

- los datagramas pueden pasar por redes de mayor o menor mtu
- cada router intermedio fragmenta los datos de acuerdo con el mtu de salida
- los fragmentos son reensamblados una vez que llegan a destino
- la fragmentacion se controla con campos en la cabecera

5.5.4 otros campos

- ttl (time to live): cuanto tiempo en segundos un paquete puede estar en la red. si llega a 0 se envia un mensaje icmp de error al origen
- protocol: indica el protocolo de nivel superior que fue usado
- options: no estan incluidos en todos los datagramas

5.5.5 clases de direcciones

- a: r.h.h.h. 1.0.0.0 a 126.0.0.0
- b: r.r.h.h. 128.0.0.0 a 191.255.0.0
- c: r.r.r.h. 192.0.0.0 a 223.255.255.0
- d: multicast address. 224.0.0.0 a 239.255.255.255
- e: reservado. 240.0.0.0 a 255.255.255.255
- el primer octeto se da por el corrimiento del ultimo 1 de izquierda a derecha (0, 10, 110, 1110, 11110)

5.5.6 packet switching

- el paquete se divide en el origen en unidades manejables: datagramas
- los datagramas viajan al destino
- se ensamblan en el destino para lograr el mensaje original
- los paquetes se dividen segun los requisitos de cada punto intermedio (cada router)

5.5.7 ruteo

- proceso de seleccion del camino de un paquete
- entrega directa: transmision entre hosts de una misma red ip. no necesita del router. se encapsula el datagrama en una trama y se envia directamente
- entrega indirecta: los hosts se encuentran en redes separadas. se envia el datagrama a un ruteador de su red ip encapsulandolo en una trama
- se compara el netid del transmisor con el de destino. si son iguales es entrega directa
- sino usan las tablas de ruteo que indican por cada posible ip el siguiente salto que debe tomar en la ruta hasta el destino
- las tablas tambien se usan para entrega directa

5.5.8 direcciones privadas

- las ipv4 no alcanzan para todos los dispositivos del mundo
- cada red interna usa un conjunto de ip privadas que se repiten en cada red que no sale a internet
- por dentro la red se maneja con esas ip privadas, y desde afuera se ve una sola ip

5.5.9 subredes ip

- cuando se usan bits de la parte de host para crear subredes

5.6 icmp: internet control message protocol

- ip falla cuando el destino se desconecta de la red, cuando pasa el timeout para la respuesta o cuando router intermediarios estan muy congestionados
- icmp es requerido por ip y debe ser incluido en una implementacion del protocolo
- reporta errores, no corrige. aunque sugiere accioner a tomar

5.6.1 funciones

- error: un nodo que reconoce un error de transmision genera un paquete icmp. este se reporta a la fuente original, que es la que esta en la cabecera del paquete. no puede avisar a los routers intermedios. ni el origen saber que router tuvo el problema
- control: herramientas de diagnostico de la red (ping, traceroute)
- trama { ip { icmp {} } }

5.6.2 tipos

- 8/0 ping: solicitud eco/respuesta
- 3 destination unreachable: cuando no puede entregar/direccionar un datagrama
- 4 source quench: congestionamiento
- 5 route change request: usado por el router directamente conectado host fuente para cambio de ruta
- 11 time exceeded
- 13/14: timestamp para sincronizacion, calculo de viaje redondo, etc
- 17/18: solicitud/respuesta de mascara

5.7 arp: address resolution protocol

- se usa para obtener direcciones mac, tanto para el ultimo paso (host destino) como para intermedios (routers)
- el pedido es broadcast, la respuesta es unicast
- el transmisor incluye su mac e ip para que los host actualicen
- trama { arp {} }
- dos partes: transforma direcciones ip en direcciones fisicas. responde pedidos de otras maquinas

- se mantiene una tabla con direcciones guardadas, que se actualizan cada cierto tiempo
- por que se usa un broadcast que alcanza al destino para despues enviar un mensaje al mismo destino?: los mensajes broadcast son mas costosos porque cada maquina debe procesar el mensaje

5.8 ipv6

- necesidad de mas direcciones porque las ipv4 no alcanzaban
- cabecera base simple, tamaño fijo, menos campos
- tamaño de direcciones de 128 bits

5.8.1 tipos de direcciones

- unicast global
  - como las publicas de ipv4
  - ruteables en internet
  - prefijo 2000::/3
  - rango desde 2000::/3 hasta 3000::/3
- unicast link local
  - alcance solo para enlace
  - no son ruteables
  - prefijo fe80::/64
- unicast unique local
  - solo validas dentro de una organizacion. como las privadas de ipv4
  - no son ruteables en internet
  - prefijo fc00::/7
- anycast
- multicast
  - prefijo ff0[1|2|5|14]::/8, [nodo local,link local,site local,global]
  - identificador de grupo: [1|2], [todos los nodos,todos los routers]

5.8.2 protocolos ipv6

- neighbor discovery (ND)
  - para encontrar otros nodos en la misma subred
  - se activa cuando la interfaz ipv6 se activa. no puede dejar de funcionar
- router discovery (RD)
  - lo usan los routers para anunciarse en la subred
  - los routers no responden RD
- duplicate address detection (DAD)
  - cuando se encuentra una direccion duplicada en una interfaz, se deshabilita hasta que se resuelve el problema
- icmpv6
- dhcpv6

6 capa de transporte

- las computadoras ejecutar muchos procesos a la vez, que serian los ultimos destinatarios de los mensajes enviados a traves de una red
- en vez de eso cada proceso puede acceder a puntos abstractos de destino llamados puertos
- los puertos se manejan de manera sincrona y con buffers
- ahora los mensajes deben tener direccion ip de destino y puerto. tambien puerto de origen para las respuestas

6.0.1 user data protocol (udp)

- cada datagrama udp posee direccion ip y puerto de origen y de destino
- sin conexion, sin acuses de recibo, no se ordenan los mensajes y tampoco se usa retroalimentacion para control de flujo
- todo lo que no tiene udp lo deberia dar la aplicacion
- para el calculo del checksum se usa un pseudoheader, que incluye la direccion ip no presente en el datagrama udp
- ip para diferenciar hosts, udp para diferenciar destinos dentro de un host
- para generar el pseudoheader el origen debe conocer el ip destino, por lo que debe haber averiguado antes donde mandar. esta interaccion entre udp e ip viola la filosofia de separacion del modelo de capas

- la multiplexacion y demultiplexacion se maneja con el sistema de puertos. las aplicaciones piden al sistema operativo un puerto
- cuando udp recibe un datagrama, se fija que el puerto este en uso, sino lo descarta y manda un icmp
- dos formas de asignar puertos: una autoridad central los elije y las aplicaciones usan segun esta eleccion *well-known ports*. otra forma es la dinamica, donde cada vez que una aplicacion necesita un puerto el software de red le asigna una, despues para conocer que puerto fue usado las otras computadoras consultan

6.0.2 reliable stream transport service (tcp)

- el programador no tiene que preocuparse por la confiabilidad de la red si el protocolo lo hace
- propiedades
  - los datos se piensan como un flujo de bytes. al receptor le llegan exactamente los mensajes enviados por el transmisor
  - conexion de circuito virtual. antes de la transferencia las dos aplicaciones se comunican para establecer los detalles de la conexion. durante la transferencia tambien hay intercambio de mensajes de exito o error
  - para hacer la transmision mas eficiente antes de enviar se acumulan datos hasta llenar un datagrama de cierto tamaño. tambien provee un servicio push
  - los datos enviados no tienen estructura
  - conexiones full duplex
- reconocimiento positivo y retransmision. el receptor envia un ack cada vez que le llegan datos. el emisor lleva cuenta de los paquetes enviados y si no recibe respuesta reenvia
- numero de secuencia a cada paquete para evitar duplicados. tambien son reenviados con el ack
- ventana semoviente (deslizante)
  - problema: el emisor no hace nada mientras espera el ack
  - mantener una ventana de mensajes: se envian una cantidad de mensajes determinado por el tamaño de la ventana
  - estos mensajes al principio no estan reconicidos (no se recibio el ack)
  - cuando se recibe el ack para el primer paquete la ventana se mueve
  - el emisor tambien mantiene una ventana
- tcp especifica el formato que los datos deben tener, los menajes de reconocimiento y el procedimiento que dos computadoras deben seguir para una comunicacion confiable
- usa puertos igual que udp, aunque mas complejos porque un solo puerto no corresponde a un solo objeto

- tcp usa la conexion como abstraccion y no los puertos. una conexion se identifica por un par de extremos
- se definen los extremos como un par (host,puerto) por lo que varios host pueden compartir el mismo puerto
- antes de iniciar la comunicacion, un host debe indicar al sistema operativo que esta abierto a aceptar conexiones (*passive open*). se le asigna un numero de puerto, generando uno de los extremos
- un host que se quiere comunicar debe requerirlo tambien mediante el sistema operativo
- los dos modulos tcp se intercambian datos para establecer y verificar la conexion
- tcp divide los datos en segmentos, que usualmente se transmite en un solo datagrama ip
- la ventana semoviente tambien sirve para el control de flujo, permitiendo al receptor esperar hasta que tenga espacio
- la ventana opera a nivel de octeto, no de segmento
- tcp permite variacion en el tamaño de la ventana en el tiempo. cada ack lleva tambien el tamaño del buffer, por lo que se puede ir acomodando el tamaño de la ventana
- los datos pueden ser marcados como urgentes, en caso de que se necesite que el receptor los procese apenas los reciba, por ejemplo interrupciones
- el checksum se calcula como en udp sobre un pseudoheader
- los ack especifican el numero de secuencia del octeto que se espera recibir (esquema acumulativo)
- retransmision y timeout
  - cuando se envia un paquete, se prende un temporizador hasta recibir respuesta. si termina el tiempo se retransmite
  - tcp monitorea cada conexion para deducir los temporizadores, ya que pueden variar bastante. tcp esta hecho para comunicacion en internet
  - se registra el tiempo que tarda desde que se envia un paquete hasta que se rebice el ack (tiempo en redondo). y se va ajustando segun una formula con el viejo rtt y el nuevo
- para evadir congestion, tcp usa dos tecnicas
  - multiplicative decrease: el tamaño de la ventana es el minimo del enviado en el ack y un tamaño de ventana de congestion. los dos inician iguales. cuando se pierde un segmento se reduce la ventana de congestion a la mitad
  - slow-start: cuando la congestion se alivia. por cada ack se aumenta el tamaño de segmento en 1. lo que no quiere decir que sea lento porque se por cada ack que se devuelve por cada segmento
- congestion

  - el modelo de capas no deja que haya comunicacion entre distintas capas
  - por ejemplo tcp puede llegar a reenviar paquetes creyendo que se perdieron cuando solo van lento en capas inferiores
  - la transmision se maneja con colas, por lo tanto se busca optimizar su uso
  - una politica es que si la cola esta llena cuando llega un datagrama lo descarta
  - como los datagramas son multiplexados, es mas probable que se descarte 1 de n host que n de un solo host (sincronizacion global)

- random early dicard (red)
  - tecnica utilizada para evitar la sincronizacion global
  - se mantienen dos marcas en la cola: *tmin* y *tmax*
  - si la cola tiene menos de *tmin* datagramas agregarlo
  - si tiene mas de *tmax* descartarlo
  - si tiene entre *tmin* y *tmax* descartarlo con una probabilidad p

- estableciendo una conexion tcp
  - *three-way handshake*: envia SYN (seq=x) -> recibe SYN, envia SYN (seq=y) y ACK (seq=x+1) -> rebice SYN+ACK, envia ACK (seq=y+1) -> recibe ACK
  - una vez establecida la conexion, la informacion puede fluir en cualquier direccion, no hay maestro ni esclavo

- numeros de secuencia iniciales
  - los dos extremos elijen numeros de secuencia al azar al hacer el *twh*. no pueden ser siempre los mismos
  - siempre los ack siguen la convencion de enviar el numero de secuencia del siguiente octeto esperado

- cerrando una conexion tcp
  - *twh* modificado
  - como es full duplex, cualquiera de los dos puede terminar independientemente del otro
  - cuando termina de enviar, un host espera el ack para cerrar su mitad de la conexion enviando un fin
  - despues deja de enviar informacion, pero puede seguir recibiendo y enviando paquetes ack

- se puede resetear la conexion mediante el paquete rst

- forzando en envio
  - tcp acumula octetos para mandar los segmentos completos y asi hacer mas eficiente la comunicacion

  - esto puede interferir con ciertas aplicaciones, por ejemplo mandar caracteres que se presionan por teclado que necesitan verse de forma inmediata
  - tcp provee una operacion push que obliga a enviar aunque el buffer no este lleno
  - se prende el bit psh para que la aplicacion tambien lo reciba al toque
- sindrome de ventana tonta
  - cuando el receptor es mucho mas lento que el emisor
  - caso extremo: el emisor envia muchos datos que llenan el buffer del receptor. el receptor manda con el ack el tamaño disponible que es 1 octeto. el emisor sigue enviando de a un octeto pero tiene que pasar por todas las capas inferiores, lo que es muy ineficiente
  - para evitar esto se evita enviar pequeñas cantidades de datos por segmento, asi como tambien devolver tamaños disponibles pequeños
  - AQUI ESTOY

7 capa de aplicacion

7.1 dns

- traducir de nombre a direccion ip
- tambien puede hace al reves
- el recurso se convierte en critico. hay que tener mas de un servidor por si falla. servidores primarios, secundarios, etc
- necesidad de delegar la administracion de los registros por el aumento de la cantidad

7.1.1 conceptos e implementacion

- dominios y delegacion
  - estructura de arbol. la raiz, *top level domains* (TLD), los nombres de dominio y puede seguir
  - TLD puede ser gTLD (generic): .com .edu .net o ccTLD (country code): .ar .us .es
- autoridad y delegacion
  - la autoridad de la raiz la tiene la ICANN
  - gTLD los administra la ICANN y son delegados a registradores acreditados
  - ccTLD son delegados a los paises
  - cada nivel inferior puede delegar tambien
  - lo que esta mas a la izquierda es el host. www por convencion
  - el dueño puede delegar de la manera que quiera todo lo que esta a la izquierda de su dominio

- componentes
  - un dns tiene tres partes: datos que describen el dominio, uno o mas progamas Name Server, un resolver
  - los datos se definen en RR (resource recods), organizados en archivos de texto llamados archivos de zona
  - el programa NS responde los pedidos de hosts locales o remotos
  - el resolver esta en cada host y traduce cada peticion del usuario en una o mas peticiones al servidor por tcp o udp
- zonas y archivos de zonas
  - describen el dominio y sub-dominios
  - datos que describen propiedades generales del tope de la zona (soa record)
  - datos autoritativos para todos los nodos o host de la zona (a, aaaa)
  - informacion global para la zona (registros de mail mx, servidores de nombres NS)
  - en caso de delegacion a sub-dominio el nombre del servidor responsable (NS)
  - registros glue para cada sub-dominio
- consultas
  - recursivas: se recibe una respuesta completa. no son obligatorias
  - iterativas: se puede recibir una respuesta o una referencia de quien preguntar. son obligatorias
  - inversas: obsoletas
- consultas recursivas
  - da una respuesta o un error
  - se negocia con un bit en el header de la consulta
  - el resolver en representacion del cliente busca a traves del dns la respuesta
- consultas iterativas
  - en vez de encargarse el resolver de buscar la respuesta si no la tiene, le devuelve al cliente una referencia de a quien puede preguntar
  - son mas rapidas, dan mas control al cliente, son mejores para sacar diagnosticos
- actualizaciones de zonas: zone transfer (axfr) o incremental zone transfer (ixfr)
- axfr
  - los esclavos toman la informacion del maestro, el intervalo es determinado en el registro soa
  - se pide el registro soa, si el numero de serial es mayor al que tiene se inicia la transferencia
  - udp puerto 53

- ixfr
  - permite la actualizacion de registros en vez de la zona entera
  - el proceso es igual a axfr
  - tcp puerto 53
- notify: el maestro tambien puede notificar a los esclavos antes del tiempo de actualizacion
- actualizaciones dinamicas
  - la forma clasica de actualizar es manualmente cambiar los registros y reiniciar el servicio para que propague los cambios
  - cuando el sistema es grande puede traer problemas
  - dos soluciones: permitir actualizaciones de una aplicacion externa o tomar los datos de una base de datos que se pueda modificar dinamicamente

7.1.2 mapeo inverso

- usado por sistemas de mail
- diseñadores de dns usan el nombre de dominio especial in-addr.arpa o ip6.arpa
- las direcciones ip son divididas en bloques para varias regiones del mundo. cada una puede subdividirse, delegando la autoridad para el mapeo
- para los archivos de zona se invierte la direccion y se agrega in-addr.arpa. despues se listan lost hosts y los nombres completos terminados en punto
- TODO

7.1.3 tipos de dns

- maestro (primario)
  - define uno o mas archivos de zona donde es autoritativo. la zona fue delegada con un registro NS
  - un maestro de zona toma los datos de una fuente local, un esclavo de una fuente externa (usualmente un maestro)
  - el maestro puede notificar a los esclavos sobre cambios en el archivo de zona
  - puede estar oculto, alguno de los esclavos puede no saber de su existencia
- esclavo (secundario)
  - toma sus datos por transferencia
  - responde como autoritativo de la zona que le corresponde
  - no es posible saber si el resultado de una consulta vino de un maestro o esclavo
  - puede haber cualquier cantidad de esclavos en una zona

- un esclavo tambien puede ser maestro
  - puede ser usado si un maestro esta oculto, por cuestiones de seguridad para aislar un servidor (tomalo con pinza)
- resolver o servidores cache
  - obtiene los datos de otro servidor y guarda la respuesta para consultas posteriores
  - si devuelve un dato que trajo del maestro responde como autoritativo, si es de cache como no-autoritativo
  - dos configuraciones habituales: un servidor maestro o esclavo para alguna zona y como resolver para las demas consultas. un servidor solo como resolver (proxy/forwarding server)
- servidores forwarding
  - simplemente pasan consultas a otros servidores y guardan las respuestas en cache
  - util por si el servidor remoto es lento
  - puede ser parte de un servidor dividido para seguridad
- servidor oculto (*stealth*)
  - no aparece definido publicamente en ningun registro NS del dominio
  - por ejemplo una organizacion necesita un dns publico para acceder a servicios de mail, ftp, y no quiere que el exterior vea sus hosts internos
  - el servidor publico muestra solo los servicios publicos y no acepta transferencias del oculto
- servidor solo autoritativo
  - el termino se usa para describir un servidor que responde como autoritativo y no hace cache
  - configuraciones usuales: servidor externo de un oculto, servidores de alto rendimiento
- split horizon
  - devuelven distintas respuestas segun la direccion de origen, o alguna otra caracteristica
  - segun posicion geografica: para devolver direcciones que esten mas cerca
  - si ciertas direcciones tienen mas privilegios se les puede devolver una respuesta especial que al resto, pero las consultas siempre son con el mismo nombre de dominio
  - equilibrio de carga

7.2 firewall

7.2.1 iptables

-