

Contents

Capa de Red	21
Generalidades:	21
El propósito de la capa de red es	21
Asuntos de los que se encarga la capa de red:	21
Hardware subyacente de la capa de red es:	21
No puede pasar un paquete tal cual de una red a otra. ¿Por qué?	21
Enfoques para mandar un conjunto de paquetes desde un host de origen a un host de destino:	22
Servicio no orientado a la conexión:	22
Nomenclatura	22
Paquetes =	22
Subredes =	22
¿Cómo diseñar la tabla de un enrutador?	22
La entrada de tabla de enrutador está formada por	22
Dirección de red: sirve para	22
Número de máquina: sirve para	22
¿Qué se hace cuando llega un paquete a un enrutador?	22
Servicio orientado a la conexión:	23
Todos los paquetes se	23
Trabajo a realizar antes de mandar paquetes:	23
Circuito virtual (CV) =	23
Cada paquete lleva un	23
Cuando no se necesita enviar más paquetes se	23
Enrutamiento Jerárquico	23
¿Cómo hacer para que las tablas de enrutamiento no crezcan demasiado	23
Los enrutadores se	23
Un enrutador	23
sabe cómo	23
Pero no sabe nada de	23
Precio a pagar	23
arquitectura de un enrutador:	23
Funciones clave	23
Conmutación descentralizada:	24
Dado un paquete, éste	24
meta:	24
encolado:	24
Encolado:	24
Los paquetes pueden perderse debido a	24
Disciplina de planificación:	24
Conceptos básicos para el algoritmos de enrutamiento:	24
Tenemos que evitar los siguientes efectos indeseados:	24
Algunos enrutadores pueden	24
Los caminos pueden ser	24

Se pueden sobrecargar algunas de	24
La causa es que	24
algoritmos de enrutamiento	24
Un algoritmo de enrutamiento se	24
es responsable de	24
Algoritmo de enrutamiento de caminos más cortos:	25
usando algoritmo de Dijkstra.	25
Inundación usando registro de paquetes difundidos	25
Algoritmos de enrutamiento:	25
conjunto de rutas se puede definir por	25
se preocupan de	25
idea	25
Implementación:	25
¿Cómo se puede evitar que las listas enlazadas crezcan sin límites?	25
¿Qué tiene que pasar para que tenga que actualizar la tabla de registros/paquetes difundidos?	26
Enrutamiento de vector de distancia	26
Cada enrutador mantiene una	26
A partir de su tabla de enrutamiento	26
El retardo de un enrutador a un vecino suyo, puede medirlo con	26
Enrutamiento de Estado de Enlace	26
En cada enrutador usar	26
La topología y retardos en	26
Este algoritmo es valioso porque	26
¿Qué tareas debe hacer un enrutador LSR?	26
¿Cómo se puede averiguar quiénes son los vecinos de un enrutador?	27
¿Cómo se puede hacer para que el enrutador conozca retardo a sus vecinos?	27
paquete de estado de enlace (LSP)	27
¿Qué datos poner en el LSP?	27
¿Cuándo se pueden construir los LSP?	27
Distribución confiable de los LSP.	27
usar	27
se lleva registro de	27
Cada paquete contiene un	27
Los enrutadores llevan el registro de	28
Cuando llega un LSP a un enrutador, ¿Que se hace con él?	28
comparar el	28
Si es nuevo	28
Si es un duplicado	28
número de secuencia menor que el mayor visto hasta el momento,	28
¿Cuándo se puede construir la tabla de enrutamiento de un en- rutador?	28
Construir el grafo de la subred completa.	28
Se ejecuta el algoritmo de Dijkstra para	28

Inundación:	28
contador de saltos:	28
¿Cómo se determina el contador de saltos?	29
Inundación Selectiva:	29
Los enrutadores no envían	29
¿Qué tipo de información necesita almacenar un enrutador	29
problemas	29
Si los números de secuencia vuelven a comenzar,	29
Si llega a corromperse un número de secuencia	29
Como protección contra los errores en las líneas enrutador-	
enrutador, se	29
Si llega a caerse un enrutador (de origen),	29
¿Cuándo se puede detectar que un enrutador está caído? .	29
¿Una vez identificado que un enrutador está caído cómo	
proceder?	29
¿Cómo hacer para asegurar que no pueda perderse ningún	
paquete y sobrevivir durante un período indefinido? 30	
Algoritmo de inundación de paquetes de estado de enlace más	
eficiente:	30
Una vez que un paquete de estado del enlace llega a un	
enrutador	30
Si antes de transmitirlo, llega	30
El buffer de paquetes para un enrutador contiene	30
Una fila de la tabla del búfer de paquetes de un enrutador contiene:	30
Banderas	30
de confirmación de recepción:	30
de envío:	30
Si llega un duplicado mientras	30
Control de congestión	31
meta	31
Problemas de los algoritmos de control de congestión de TCP . .	31
El host de destino	31
Los hosts solo se enteran de	31
Formas de disminuir la carga en la subred:	31
Regulación del tráfico:	31
Desprendimiento de carga:	31
Cómo identificar la congestión	31
Regulación de tráfico	31
¿Cómo se puede enterar un host de que hay congestión?	31
Método de paquetes reguladores:	31
cuando se satura una línea de salida de un enrutador, se .	32
evitar la pérdida descontrolada de paquetes.	32
La primera solución es	32
criterios para escoger qué paquetes descartar	32
Estrategia Vino:	32
Estrategia Leche:	32

Según la importancia de los paquetes.	32
desprendimiento de carga junto con reducción de tráfico.	32
Algoritmo de detección temprana aleatoria (RED):	33
Para detectar cuándo comenzar a descartar paquetes, los	
enrutadores	33
Cuando este promedio de una cola C sobrepasa el umbral	33
Las consecuencias de elegir paquetes al azar	33
Complementos de Control de Congestión	33
si los enrutadores tienen infinita memoria,	33
Los procesadores lentos	33
Las líneas de poco	33
Subredes de Circuitos Virtuales:	33
Idea 1: Usar una técnica de control de admisión	33
Idea 2: permitir el establecimiento de nuevos	33
Idea 3: negociar un acuerdo	33
Este arreglo normalmente especifica el	33
Para cumplir con su parte del acuerdo, la subred	34
recursos pueden incluir	34
De este modo es poco probable que	34
Método de bit de advertencia.	34
Cuando el paquete llega a su destino,	34
A continuación el origen	34
Mientras el enrutador está en estado de advertencia,	34
El origen monitorea la fracción de confirmaciones de recepción con	34
En tanto los bits de advertencia continúan fluyendo, el origen . .	34
Cuando la tasa de transmisión disminuye lo suficiente, el origen .	34
el tráfico se incrementa solo cuando	34
implementación de bit de advertencia usada por TCP	34
Se marcan 2 bits en el encabezado IP con distintos fines: .	35
Si ambos extremos soportan ECN	35
Se usan dos banderas en encabezado TCP para soportar	
ECN:	35
Secuencia de ejecución de ECN típica:	35
problema del método de paquetes reguladores	35
La solución es	36
Protocolo de capa de Red IP	36
propósito:	36
Datagramas IP	36
IHL :	36
Total Length :	36
Type of service :	36
Protocol :	36
identificación :	36
tiempo de vida :	36
Header checksum :	36
Direcciones IPv4:	36

direcciones de origen y de destino:	36
Consecuencias:	37
Cada host y enrutador en la internet tiene	37
Una máquina puede tener	37
Conceptos fundamentales	37
Una red corresponde a un	37
Prefijos	37
Ejemplo: ¿Qué significa el prefijo 128.208.0.0/24?	37
Máscara:	37
¿Cuál es la máscara de 128.208.0.0/24?	37
Subredes:	38
Asignaciones de redes a organizaciones	38
Evitar tablas de reenvío demasiado grandes:	38
solución:	38
Implementación	38
Tablas de enrutamiento	38
¿ Cómo definir las tablas de enrutamiento ?	38
El enrutamiento es	38
sólo se representan redes de	38
Cada entrada de tabla de enrutamiento se	38
Tabla de enrutamiento para todas las redes tiene entradas:	38
¿ Cómo se usa la tabla de enrutamiento cuando llega un paquete?	38
Control de tamaño de tablas de enrutamiento	39
CIDR	39
se combinan varios	39
Racionamiento de uso de direcciones IPv4	39
¿Cómo aumentar la cantidad de máquinas?	39
Asignar un solo N° de	39
Dentro de la organización cada computadora tiene	39
Cuando un paquete sale de la organización	39
implementación:	39
Para hacer posible este esquema	39
La única regla es que	39
3 rangos reservados	39
PUERTOS:	39
Cada mensaje TCP saliente contiene	39
uso de los puertos cuando un proceso quiere establecer una conexión TCP	40
se asocia a un	40
Problema:	40
Como sabe ahora la caja NAT con que dirección se reemplaza?	40
Solución 1: Guardar asociación en la caja NAT de número	40
Solución 2: Distinguir entre el número de puerto	40
Tabla de traducción de la caja NAT	40
Los índices en la tabla son	40
Una entrada de la tabla contiene	40

¿ Cómo tratar un paquete que llega a la caja NAT desde el ISP?	40
El puerto de origen en el encabezado TCP se	40
Desde la entrada localizada la	40
¿Cómo tratar un paquete saliente de la caja NAT ?	40
La dirección de origen	40
el campo puerto de origen TCP se	40
Críticas a NAT:	41
Protocolo IP	41
Campo tiempo de vida en los paquetes:	41
Debe ser	41
Cuando llega a 0	41
Previene que un	41
Subredes	41
Permiten que una red sea	41
Cada subred puede ser una	41
Los enrutadores de una subred se conectan a	41
no visibles por	41
Cuando un paquete entra al enrutador principal, ¿cómo saber a	
qué subred pasarlo?	41
¿Cómo expresar subredes?	42
El enrutador principal usa una	42
La máscara es una	42
Tabla de enrutamiento en un enrutador cuando hay subredes . .	42
Si se tienen entradas de la forma (dirección IP inicio subred,	
máscara) se hace	42
La cantidad máxima de hosts se da por	42
Complementos a IP	42
IPv6	42
Encabezado de longitud	42
Capacidad de direccionamiento	42
Etiquetado de flujos:	42
Consecuencia de etiquetado de flujos:	42
Etiqueta de flujo:	42
Prioridad	42
Longitud de carga útil:	43
Límite de saltos:	43
Próximo encabezado:	43
DHCP:	43
Meta:	43
DHCP puede retornar	43
es ampliamente usado en redes de	43
UPnP:	43
Problema:	43
Una aplicación ejecutada en un host puede pedir un mapeo	
NAT entre su	43
¿Si se acepta el pedido	44

ARP	44
Problema:	44
Solución:	44
difusión	44
Optimizaciones	44
Una vez que una máquina ha ejecutado ARP,	44
Cuando la difusión de ARP llega al host de destino,	44
cada máquina	44
sistema autónomo (SA)	44
consiste en	44
Generalmente distribuidos por	45
A veces los ISP dividen su	45
Los enrutadores dentro de un SA	45
Internet es un conjunto de	45
¿Por qué se necesita definir un protocolo intra-SA especial para	
internet?	45
Los protocolos de enrutamiento estudiados	45
A veces hay más de un	45
OSPF	45
Es un protocolo de	45
Se considera una adaptación del	45
Es compatible con	45
En OSPF el modelo de grafo asociado a un SA es	45
Para permitir los SA grandes, OSPF organiza un SA como	46
para un destino se puede considerar más de	46
Tipos de conexiones y redes soportadas	46
Representación de la red en un grafo	46
Los enrutadores se representan con	46
a cada arco se le asigna	46
Una conexión punto-punto entre dos enrutadores se repre-	
senta por	46
Una red de multiacceso se representa con un	46
organizar un SA muy grande?	46
áreas numeradas.	46
Un área puede contener	46
Cada enrutador está configurado para	46
Las áreas no	47
Tipos de áreas:	47
Clasificación de los enrutadores de un SA:	47
Enrutadores internos:	47
Enrutadores dorsales:	47
Enrutador de borde de área (EBA).	47
Aviso de estado de enlace (AEE)	47
contiene	47
Los EBA resumen	47
¿Cómo definir la información resumida de un área no dorsal? . .	47

Un EBA E recibe avisos de estado de enlace de	47
La información resumida de A contiene el	47
¿Cómo definir la información resumida de un área dorsal?	47
Por medio de un grafo donde:	47
Al ejecutarse OSPF	48
los enrutadores dentro de un área ejecutan	48
Cuando un enrutador se inicia,	48
envía mensajes Hello a:	48
Los enrutadores en la misma LAN son	48
OSPF no fija una política de cómo	48
trabaja intercambiando	48
Cada enrutador tiene	48
La BDEE	48
contiene	48
debe ser	48
Dentro de un área	49
Consecuencias	49
Tipos de paquetes usados para intercambio de información entre enrutadores adyacentes:	49
Paquete de actualización de estado de enlace	49
Paquete de confirmación de estado de enlace	49
Paquete de descripción de base de datos	49
Paquete de pedido de estado de enlace	49
¿Cómo actualizan sus BDEE los enrutadores?	49
Dos enrutadores vecinos deben	49
Un vecino es el	49
enrutador designado,	50
Usando inundación cada enrutador	50
Para un enrutador R dentro de un área se puede ejecutar el OSPF calcula todos los caminos más cortos entre	50
Interredes	50
Para enviar paquetes a una red con distinto protocolo:	50
Las puertas de enlace	50
Se construye una	50
Enrutamiento en interredes	50
Una vez construido el grafo de la interred pueden aplicarse En cada red se usa	50
Entre las redes se usa	50
Cada red puede usar distintos	50
Fragmentación	51
Ocurre cuando	51
Se fragmenta el paquete en	51
Para recuperar el paquete original, se puede:	51
Dirigir todos los fragmentos a	51
Tratar cada fragmento como	51
Entunelamiento	51

EGP/PPEE(External	51
Para enrutamiento inter-SA es	51
Requisitos	51
Los PPEE suelen implementarse sobre	51
Un EBSA:	51
Relaciones entre SA	52
Proveedor-Consumidor:	52
Compañerismo:	52
Multihoming:	52
BGP	52
Es el PPEE usado por	52
Provee a cada SA un medio para:	52
Obtener información de	52
Propagar esta información dentro del	52
Determinar buenas rutas a	52
Que cada red publique	52
En BGP los destinos son	52
Cada prefijo representa una	52
Un SA es identificado por	52
se incluye con el prefijo una	52
Atributos BGP:	53
AS-PATH:	53
NEXT-HOP:	53
Propagar información de rutas en BGP	53
Sesiones BGP	53
Es la conexión TCP con todos los	53
Una sesión BGP entre enrutadores de dos SA se llama	53
Una sesión BGP entre enrutadores del mismo SA se llama	53
Aviso de rutas	53
Cuando una puerta de enlace P recibe rutas:	53
La mejor ruta a un prefijo se guarda en	53
Base de información de Enrutamiento (BIE)	53
reglas:	53
Mensajes de actualización son usados para:	54
Un enrutador BGP no tiene la obligación de	54
Política de Importación	54
Cuando una puerta de enlace recibe aviso de ruta	54
Si un enlace falla o cambia una política, los enrutadores	
BGP pueden	54
Capa de Enlace de Datos	54
Generalidades	54
La CED toma de la CR	54
Las tramas tienen una	54
Cada paquete de la CR se	54
En la CR de la máquina de origen hay	54

El trabajo de la CED es	54
Limitaciones de los canales de comunicación	55
Cometen	55
Tienen una	55
Hay	55
Meta	55
Lograr una	55
Un protocolo de CED hace que	55
Funciones	55
Control de flujo	55
Evitar que un	55
Uso de	55
Control de buffer receptor	55
Se da entre un nodo	55
Entramado (flaming)	55
En el canal de difusión solo hay	55
¿Cómo detectar el inicio y fin de cada trama?	55
Detección y corrección de errores	56
Se agrega a los mensajes de CED (tramas)	56
Manejo de colisiones	56
Ocurren en	56
Cuando dos máquinas intentan	56
Informaciones que debería contener una trama	56
encabezado:	56
campo de carga útil	56
un terminador final	56
información	56
Fundamentos de la comunicación	56
Se trabaja con:	56
Confirmaciones de	56
Temporización de	56
Retransmisiones de	56
Uso de	56
Llevar a	57
Control de	57
Flujo entre enrutadores	57
Canales de Difusión:	57
Es costoso e incómodo hacer que	57
En un canal de difusión están	57
Tipos	57
Inalámbricos	57
Cableados	57
Mediante el uso de	57
Necesidad de Control de Colisiones:	58
Si dos tramas se transmiten	58
¿Cómo evitar colisiones	58

Definir una	58
En una red de difusión el asunto clave es	58
protocolos de acceso múltiple	58
Soluciones	58
Inalámbricas	58
Cableadas	58
Control de colisiones en redes cableadas	58
Modelo de Estaciones	58
Una vez generada una trama, la	58
Suposición de canal único:	59
Propiedades de los canales de difusión modernos:	59
Fenómenos sucediendo en un canal que una estación podría detectar	59
Detectar que el canal está	59
Detectar que hay una	59
En las LAN actuales	59
cada estación puede detectar si	59
El hardware de una estación	59
¿Qué hacer si se detecta una colisión?	59
Ventajas de la detección de colisiones	59
Ahorra	59
Si no se detectan,	59
para definir PAMs conviene que	59
CSMA con Detección de Colisiones (PAM CSMA/CD):	60
el emisor:	60
Antes de transmitir una trama	60
Si el canal está libre	60
Si el emisor detecta una colisión,	60
el receptor:	60
Recibe una	60
Al mandar una	60
Evaluación del uso del canal:	60
el canal puede estar en 3 estados.	60
Se dice que una estación ha tomado el canal cuando	60
El tiempo mínimo en detectar la colisión es	60
El peor caso de demora de una estación en enterarse que ha habido	
una colisión es	61
Cómo ocurre una colisión	61
En el peor caso una estación no puede estar segura de que ha	
tomado el canal hasta que	61
las tramas tienen un requisito de	61
Ethernet (IEEE 802.3):	61
Hardware	61
Transceptor:	61
Tarjeta controladora:	61
Tipos de cableado	61
Cada cableado de Ethernet tiene una	61

concepto de segmento,	61
Una señal a medida que se va propagando por un cable se va	61
Llega un punto a partir del cual la señal es	62
Para que una señal pueda viajar más	62
repetidor	62
introducen un	62
Para permitir redes mayores que un segmento	62
Restricción	62
ningún par de	62
ninguna ruta	62
A medida que aumente la velocidad de la red,	62
Ethernet Conmutada:	62
conmutador (switch)	62
contiene una	62
Tarea	62
Transparencia:	62
aprenden	62
Si dos máquinas conectadas a la misma tarjeta de conexión trans-	
miten tramas al mismo tiempo y si todos los puertos de la	
tarjeta forman una LAN local dentro de la tarjeta:	63
Las colisiones en esta LAN en tarjeta se	63
Las tarjetas pueden estar	63
Si cada puerto de entrada se almacena en un búfer	63
todos los puertos de entrada	63
Cada puerto es	63
tabla de conmutador:	63
Un conmutador aprende	63
Cuando el conmutador recibe	63
Reenvío de una trama recibida por el conmutador:	63
La ventaja de usar conmutadores es	64
Problemas al diseñar protocolo de CED:	64
¿Cómo asegurar que una trama se entregue?	64
Regresar tramas de control con	64
Método que usa temporizador de retransmisiones	64
Al enviarse una trama,	64
Si la trama o la confirmación de recepción se pierden	64
Si la confirmación de recepción llega	64
¿Cómo hacer para evitar entregar a la CR tramas repetidas?	64
Método que	64
El receptor tiene una	64
¿Qué hacer con un emisor que quiere transmitir tramas a mayor	
velocidad que aquellas con que puede aceptarlos el receptor?	64
Solución basada en	64
¿Cómo transmitir datos entre dos máquinas y en ambas direcciones	
eficientemente?	64
Solución	64

La confirmación de recepción se	65
¿Qué pasa si la CED espera demasiado por una trama a la cual superponer el ack?	65
PAM: ALOHA puro	65
emisor:	65
Transmite cuando	65
Escucha el canal por	65
Si se escucha un ack en ese tiempo,	65
Si se falla en recibir un	65
receptor:	65
Al recibir una trama	65
Si la trama es inválida	65
Evaluación	65
Este método bajo carga baja es	65
En ALOHA puro una estación	65
el número de colisiones crece	66
la máxima utilización del canal es	66
CSMA persistente 1	66
emisor:	66
Si una estación tiene datos por enviar,	66
Si el canal está ocupado,	66
Cuando la estación detecta un canal inactivo,	66
Si ocurre una colisión,	66
Comportamiento luego que emisor envió una trama	66
La estación	66
Si no recibe ack	66
receptor:	66
Al recibir una trama	66
Si la trama es inválida	66
retardo de propagación	66
tiene un	66
Caso de que justo después de que una estación comienza a transmitir, otra estación está lista para enviar,	67
Aun si el retardo de propagación es cero,	67
Ethernet	67
Direcciones	67
Se usan direcciones de	67
Se escriben como	67
El bit de orden mayor de la dirección de destino es	67
Una trama que consiste únicamente de bits 1 en el campo de destino	67
Campo Tipo	67
Longitud de trama mínima	67
Las tramas deben tener al menos	67
Cuando los datos más el encabezado ocupan menos de 64 bytes.	67

Suma de verificación	68
Se usa un método de	68
cambios al formato DIX	68
Reducir el	68
Cambiar el campo de Tipo por	68
Poner un	68
Diferentes modos de cablear un edificio:	68
Un cable pasa entre	68
Una columna vertical	68
Topología de árbol	68
Algoritmo de retroceso exponencial binario	68
Algoritmo que determina	68
Tras una colisión	68
El tiempo de ranura es	69
las estaciones afectadas por la colisión	69
algoritmo	69
Tras i colisiones se escoge un número aleatorio entre	69
Tras haberse alcanzado 10 colisiones	69
Tras 16 colisiones el controlador	69
Evaluación	69
El algoritmo asegura un	69
El algoritmo asegura que la colisión	69
Ethernet Rápida:	69
Fast Ethernet (o 802.3u)	69
Cableado	69
100BASE-T	69
100BASE-TX	70
100BASE-FX	70
Interconectando conmutadores:	70
Conmutadores pueden	70
(se trabaja	70
Redes Inalámbricas	70
Señales:	70
Intensidad decreciente de la señal	70
Interferencias de otros orígenes	70
Propagación multi-camino	70
Mayor tendencia a	70
SNR y BER:	70
Necesario 1) sensibilidad del receptor (RSSI)	70
Necesario 2) relación señal a ruido (SNR)	71
Esquema de Modulación	71
Tasa de error (BER)	71
Modulación SNR y BER:	71
cuanto mayor es la SNR,	71
Para una SNR dada, una modulación	71
Problemas de la comunicación inalámbrica:	71

Los nodos inalámbricos usualmente no pueden	71
La potencia generada por el emisor es	71
Las redes inalámbricas no pueden	71
Se usa	71
Problema de la estación oculta	71
Problema de la estación expuesta	71
Canales y Asociación:	72
Cada host necesita	72
Puede haber más de 1	72
Se crea un	72
AP \rightarrow	72
Escaneo Activo:	72
Re asociación	72
Escaneo Pasivo:	72
Otras responsabilidades de AP:	72
Asociación :	72
Reasociación :	73
Desasociación :	73
Subcapa MAC 802.11:	73
Soporta dos modos	73
DCF	73
PCF	73
DCF:	73
En ethernet no existe	73
Colisiones:	73
Emisores esperan	73
Estación oculta:	73
PCF:	73
Hay una relación uno a uno entre hosts y AP (asociación) \rightarrow BSS	73
El tiempo en el medio se divide en:	74
Período sin (contention) disputa (PCF)	74
Período en (contention) disputa (DCF)	74
Beacon (baliza):	74
Poll (sondeo):	74
Tiempos Entre Tramas:	74
SIFS	74
PIFS	74
DIFS	74
SIFS:	75
Dentro de un	75
Hacen falta los SIFS para cosas como	75
Una estación usando SIFS para determinar la oportunidad de transmisión tiene	75
Hay solo una estación que puede responder luego de un intervalo SIFS,	75
PIFS:	75

Entre dos	75
Luego de un PIFS	75
Dentro de un PIFS se	75
El AP puede hacer sondeo	75
en forma	75
Cuando se emite un sondeo,	75
Si el AP recibe una respuesta a un poll,	75
Si no se recibe respuesta al poll,	75
DIFS:	75
Luego de un período de PCF, viene un	75
Si el AP no tiene nada que decir	76
Capa Física	76
se encarga de	76
medios físicos	76
se conectan entre sí usando	76
Señales Digitales y Analógicas	76
Señales analógicas:	76
Señales digitales:	76
Señales digitales vs señales analógicas	76
Las señales digitales generalmente son	76
Las señales digitales sufren más de	76
Ondas Sinusoidales	76
Son producidas por	76
ejemplo,	76
Onda sinusoidal	77
Propiedades	77
Frecuencia =	77
Amplitud =	77
Fase =	77
período (T) =	77
Los sistemas de comunicación usan	77
Señales Compuestas	77
Señales simples:	77
Señales compuestas:	77
Una señal electromagnética va a ser	77
Descubrimiento de Fourier	77
Señales periódicas:	77
Señales aperiódicas	78
Si una señal compuesta es periódica,	78
La mayoría de los sistemas usan	78
Una señal compuesta es creada en	78
Representaciones Gráficas De Las Señales	78
Representación de dominio de tiempo	78
Representación de dominio de frecuencia	78
Representación De Dominio De Frecuencias	78

La representación de dominio de frecuencia es	78
El espectro de una señal =	78
El ancho de banda analógica =	78
Señales Digitales	79
Las señales digitales usan	79
Mecanismos de transmisión físicos usan	79
Usar 2^n niveles para	79
Baudios y Bits por Segundo	79
El hardware coloca límites en	79
Si la señal no permanece en un nivel por superficie tiempo, . . .	79
La cantidad de veces que una señal puede cambiar por segundo se mide en	79
baud y número de niveles de señal controlan la	79
Relación entre baudios, niveles de señal y tasa de bits	79
La Tasa De Datos Máxima De Un Canal	79
Teorema de Nyquist	79
Si la señal consiste de V niveles de voltaje, el teorema de Nyquist (1924) establece:	79
cantidad de ruido térmico	80
se mide por	80
Si indicamos la potencia de una señal con S y la potencia del ruido con una N, la relación señal a ruido es	80
Resultado de Shannon (1948)	80
La tasa de datos máxima de un canal ruidoso cuyo ancho de banda es H Hz y cuya relación señal a ruido es S/N, está dada por:	80
La fórmula solo da un	80
Cálculo de niveles distinguibles de voltaje que valen la pena . . .	80
Modems, portadora,	80
Módem:	80
Un módem permite	80
Todos los módems modernos transmiten	80
Muchos sistemas de comunicación de larga distancia usan	80
Modulación:	81
El emisor debe cambiar	81
Portadora de onda senoidal =	81
de amplitud (b)	81
Se usan	81
de frecuencia (c)	81
Se usan	81
Si la señal es más fuerte,	81
si la señal es más débil,	81
Es más	81
de fase (DF)	81
Es posible usar	81
El DF se mide por	81

de fase (d)	81
Al requerir el	81
Detección de cambio de fase	81
Un receptor puede	81
Usualmente los sistemas están diseñados para para usar	82
Diagramas De Constelación	82
El eje horizontal se refiere a	82
el eje vertical a	82
Los diagramas de constelación también pueden usarse para	82
Los ejes del plano del diagrama suelen ser llamados	82
El módulo viene dado por	82
La fase es el	82
Multiplexado	82
¿Cómo hacer para poner muchas señales en un mismo canal?	82
Multiplexado:	82
Demultiplexado:	82
FDM (multiplexado por división de frecuencia):	83
El espectro de frecuencias se divide en	83
cada usuario posee	83
Funcionamiento de un multiplexor	83
Funcionamiento de un demultiplexor	83
Utilidad	83
TDM (multiplexado por división de tiempo):	83
Los bits de cada una de las	83
puede manejarse por completo mediante	83
Aplicación	83
Principio de Superposición de Ondas	84
CDM (multiplexado por división de código):	84
Permite	84
Varios usuarios pueden	84
a menudo se lo llama	84
las tramas que colisionan	84
cada tiempo de bit se	84
A cada estación se le asigna un	84
Notación bipolar:	84
Transmisión en un tiempo de bit	84
Requisito	85
Notación	85
¿Cómo hacer para que un receptor pueda recuperar la señal enviada por una estación de manera sencilla?	85
Todas las secuencias de chips deben ser	85
Para recuperar el flujo de bits de una estación, el receptor:	85
Calcula el	85
Si la secuencia de chips recibida es S y el receptor está tratando de escuchar una estación cuya secuencia de chips es C,	85

Las secuencias ortogonales de chips para las estaciones se pueden generar utilizando un método conocido como	85
propiedades	85
Si $S * T = 0$, entonces	85
El producto normalizado de cualquier secuencia de chips por si mismo es	86
sistema CDMA	86
Aplicación	86
OFDM	86
El ancho de banda del canal es	86
Estas portadoras son	86
Las portadoras pueden ser	86
es usada en	86
WDM	86
Se refiere a	87
Las entradas y salidas de WDM son	87
Un multiplexor acepta	87
Un demultiplexor usa un	87
Medios De Transmisión	87
se clasifican en:	87
guiados	87
no guiados	87
magnéticos	87
Cable de par trenzado de cobre:	87
Evaluación:	87
Cable coaxial:	88
Evaluación:	88
Fibra Óptica:	88
Se dice que cada rayo tiene	88
una fibra que tenga esta propiedad se llama	88
Fibra monomodo:	88
¿Cómo hacer para aprovechar la fibra óptica si los hosts no usan señales ópticas?	88
Transmisión inalámbrica:	88
Ondas electromagnéticas:	88
Cuando los electrones se mueven,	88
Frecuencia f de una onda electromagnética =	89
Longitud de onda λ =	89
Principio:	89
En el vacío, todas las ondas electromagnéticas viajan a	89
En el cobre o la fibra óptica, la velocidad es aproximadamente	89
Ley: La relación entre λ , f y c en el vacío es de	89
La red telefonía pública conmutada	89
Para enviar datos digitales de una PC sobre una línea analógica	89
Módem telefónico:	89
Los datos se convierten a formato digital en	89

Codec:	89
En el extremo receptor	89
DSL (Digital Subscriber Line):	89
DMT (multitono discreto) divide el	89
Multiplexado	89
El canal 0 se usa para	90
Los canales 1 a 5	90
De los 250 canales restantes,	90
1 se usa para	90
El resto está disponible para	90
ADSL	90
El proveedor determina	90
La mayoría de los proveedores asigna	90
Dentro de cada canal,	90
la velocidad del flujo descendente es de	90
El módem ADSL funciona como	90
Internet Por Cable	90
Hay segmentos de	90
Sistema	91
Los convertidores electro-ópticos se llaman	91
un nodo de fibra puede	91
¿Cómo son los módems de internet por cable?	91
Para el flujo descendente cada canal descendente de 6 MHz	
se lo modula con:	91
¿Cómo se hace multiplexado en un cable coaxial?	91
El uso de canales para flujo descendente de 6 Mhz o de 8	
MHz es	91
TDM se usa para	91
Redes celulares:	91
Generaciones:	91
Modelo de hexagono:	91
las celdas se conectan a un	91
Categorías en la que se dividen los canales de la red:	92
canales de control	92
canales de localizacion	92
canales de acceso	92
canales de datos	92
1G	92
Tanto 1G como 2G están diseñados para el envío de	92
Características:	92
2G	92
Incluye el	92
GSM: Global system for mobile comm(Ete	92
Datos :	93
FDM	93
TDM	93

	Canal de control de difusión	93
	Canal de control dedicado	93
	Canal de control común	93
3G		93
	El principal objetivo ahora es	93
4G		93
	Capa de APP y TRANSPORTE	93
	Red IP	93
Gestión de movilidad:		94
	HOME NETWORK:	94
	FOREIGN NETWORK:	94
	CORRESPONSAL:	94
	CORE OF ADDRESS(CoA):	94
	El home agent controla	94
	Enrutamiento indirecto:	94
	Enrutamiento directo:	94
	Se necesita un	94

Capa de Red

Generalidades:

El propósito de la capa de red es

llevar paquetes de un host de origen a uno de destino siguiendo una ruta conveniente.

Asuntos de los que se encarga la capa de red:

Almacenamiento y reenvío

Enrutamiento

Control de congestión

Conectar redes de distintas tecnologías (Interredes)

Fragmentación

Hardware subyacente de la capa de red es:

Subred: formada por enrutadores interconectados

Hosts o LANs conectadas a subred

Varias subredes de distinta tecnología unidas entre sí usando puertas de enlace

No puede pasar un paquete tal cual de una red a otra. ¿Por qué?

Formatos de paquetes y tamaños máximos difieren de una red a otra.

Enfoques para mandar un conjunto de paquetes desde un host de origen a un host de destino:

Usar una ruta fija para mandar todos los paquetes (servicio orientado a la conexión).

La ruta puede cambiar, por lo que distintos paquetes pueden seguir distintos caminos (servicio no orientado a la conexión).

Servicio no orientado a la conexión:

Los paquetes se enrutan de manera independiente.

La ruta a usar entre los hosts va a cambiar cada cierto tiempo.

Nomenclatura

Paquetes =
datagramas

Subredes =
subredes de datagramas

¿Cómo diseñar la tabla de un enrutador?

para armar la tabla de enrutamiento solo necesita entradas para los enrutadores de la subred.

La entrada de tabla de enrutador está formada por

filas: <enrutador de destino, línea de salida> (La línea de salida es la dirección de un enrutador).

Dirección de red: sirve para

identificar una red.

Número de máquina: sirve para

identificar una máquina dentro de la red.

¿Qué se hace cuando llega un paquete a un enrutador?

1. Se lo almacena y se comprueba que llegó bien.
2. Se determina el enrutador de destino asociado al host de destino.
3. Se usa la fila de ese enrutador de destino para reenviar el paquete por la línea de salida de esa fila.

Servicio orientado a la conexión:

Todos los paquetes se
mandan por la misma ruta.

Trabajo a realizar antes de mandar paquetes:
configurar una ruta del host de origen al de destino (crear una conexión).

Circuito virtual (CV) =
conexión.

Cada paquete lleva un
identificador que indica a qué CV pertenece.

Cuando no se necesita enviar más paquetes se
libera la conexión. Al hacer eso también se termina el CV.

Enrutamiento Jerárquico

¿Cómo hacer para que las tablas de enrutamiento no crezcan demasiado

Los enrutadores se
dividen en regiones.

Un enrutador
sabe cómo
enrutar paquetes a destinos en su región.
También sabe cómo enrutar a otras regiones.

Pero no sabe nada de
la estructura interna de las regiones en las que no está.

Precio a pagar
una longitud de ruta mayor (no se puede aspirar a encontrar la mejor ruta).

arquitectura de un enrutador:

Funciones clave
Ejecutar algoritmos de enrutamiento/protocolos (RIP, OSPF, BGP)
Enviar paquetes de enlaces de ingreso a enlaces de salida

Conmutación descentralizada:

Dado un paquete, éste

busca un puerto de salida usando la tabla del enrutador.

meta:

procesamiento completo del input a la “velocidad de la línea”.

encolado:

si los paquetes arriban más rápido que la tasa de envío en la fábrica de conmutación.

Encolado:

requerido cuando los paquetes llegan de la fábrica de conmutación más rápido que la tasa de transmisión.

Los paquetes pueden perderse debido a

congestión, carencia de búferes.

Disciplina de planificación:

elige entre los paquetes encolados para transmisión.

Conceptos básicos para el algoritmos de enrutamiento:

Tenemos que evitar los siguientes efectos indeseados:

Algunos enrutadores pueden

quedar inactivos.

Los caminos pueden ser

innecesariamente largos.

Se pueden sobrecargar algunas de

las líneas de comunicación y los enrutadores asociados a ellas.

La causa es que

la capa de red elige mal las rutas para enviar paquetes.

algoritmos de enrutamiento

Un algoritmo de enrutamiento se

ejecuta en los enrutadores de la subred;

es responsable de

llenar y actualizar las tablas de enrutamiento.

Algoritmo de enrutamiento de caminos más cortos:

usando algoritmo de Dijkstra.

1. Construir grafo de la subred con costos.
2. Ingresar grafo de la subred con costos en los enrutadores.
3. En cada enrutador construir tabla de enrutamiento;
 - a. Ejecutar algoritmo de Dijkstra en el enrutador
 - b. A partir de un árbol de caminos más cortos con la raíz en el enrutador obtenido, generar la tabla de reenvío del enrutador.

Inundación usando registro de paquetes difundidos

Algoritmos de enrutamiento:

buscan determinar las rutas a seguir para enviar paquetes de un origen a un destino.

conjunto de rutas se puede definir por
medio de un conjunto de reglas a respetar.

se preocupan de
actualizar las tablas de reenvío de mensajes en los enrutadores.

idea

El enrutador de origen pone un número de secuencia en cada paquete que recibe de sus hosts

Un enrutador recuerda para cada enrutador de origen los números de secuencia recibidos

Si llega un paquete a un enrutador con par recibido antes, no se lo reenvía

Implementación:

para cada enrutador usar tabla de registro de paquetes difundidos.

¿Cómo se puede evitar que las listas enlazadas crezcan sin límites?

Agregar una columna contador que indica el mayor número de secuencia tal que llegaron paquetes con todos los números de secuencia anteriores desde ese enrutador de origen.

¿Qué tiene que pasar para que tenga que actualizar la tabla de registros/paquetes difundidos?

Que llegue un paquete para re-transmitir con el número de secuencia mayor que el contador y que no esté en la lista, o que llegue un paquete para un enrutador de origen que nunca mandó nada, y me obligue a crear una fila nueva.

Enrutamiento de vector de distancia

Cada enrutador mantiene una

tabla de enrutamiento indexada por cada enrutador en la subred.

Cada entrada (Cada fila) comprende la línea preferida de salida hacia ese destino y una estimación del tiempo o distancia a ese destino.

A partir de su tabla de enrutamiento

un enrutador E puede obtener un vector de distancia que contiene una lista de pares <destino, retardo estimado>

El retardo de un enrutador a un vecino suyo, puede medirlo con

paquetes de ECO que el receptor simplemente marca con la hora y los regresa tan rápido como puede.

Enrutamiento de Estado de Enlace

En cada enrutador usar

algoritmo de Dijkstra para encontrar la ruta más corta de un enrutador a los demás enrutadores.

La topología y retardos en

las líneas se distribuyen a cada enrutador.

Este algoritmo es valioso porque

responde rápido frente a cambios en la topología de la red, y es ampliamente usado en Internet (como parte del protocolo OSPF).

¿Qué tareas debe hacer un enrutador LSR?

1. Descubrir sus vecinos
2. Medir el costo a cada uno de sus vecinos
3. Construir un paquete diciendo lo que ha aprendido
4. Enviar este paquete a todos los demás enrutadores

5. Computar el camino más corto a cada uno de los otros enrutadores

¿Cómo se puede averiguar quiénes son los vecinos de un enrutador?

Se envía paquete Hello a cada línea punto a punto

Se espera que el enrutador del otro extremo regrese una respuesta indicando quién es.

¿Cómo se puede hacer para que el enrutador conozca retardo a sus vecinos?

Enviar un paquete ECHO especial a través de la línea

Una vez que llegue al otro extremo, éste debe regresar inmediatamente

Se mide el tiempo de ida y vuelta y se divide por 2.

paquete de estado de enlace (LSP)

¿Qué datos poner en el LSP?

Identidad del emisor

Número de secuencia

Edad

Lista de <vecino, retardo al vecino>

¿Cuándo se pueden construir los LSP?

Construirlos a intervalos regulares.

Construirlos cuando ocurra un evento significativo, como la caída o la reactivación de la línea o de un vecino,

Distribución confiable de los LSP.

usar

inundación para distribuir los LSP.

se lleva registro de

los paquetes difundidos.

Cada paquete contiene un

número de secuencia que se incrementa con cada paquete nuevo enviado (desde su enrutador de origen).

Los enrutadores llevan el registro de
todos los pares <enrutador de origen, secuencia> que ven.

Cuando llega un LSP a un enrutador, ¿Que se hace con él?

comparar el
valor de su número de secuencia con el que figura en la tabla (de paquetes difundidos) para el enrutador que lo mandó.

Si es nuevo
(nuevo número de secuencia mayor que los anteriores),
se reenvía a través de todas las líneas, excepto aquella por la que llegó.

Si es un duplicado
(número de secuencia mayor visto, pero repetido),
se descarta.

número de secuencia menor que el mayor visto hasta el momento,

se rechaza como obsoleto debido a que el enrutador tiene datos más recientes.

¿Cuándo se puede construir la tabla de enrutamiento de un enrutador?
Una vez que el enrutador ha acumulado un grupo completo de paquetes de estado del enlace

Construir el grafo de la subred completa.
Cada enlace se representa dos veces, una para cada dirección.
Los dos valores pueden promediarse o usarse por separado.

Se ejecuta el algoritmo de Dijkstra para
construir la ruta más corta a todos los destinos posibles.
Con los resultados del mismo se actualiza la tabla de enrutamiento.

Inundación:

contador de saltos:

integrar un contador de saltos en el encabezado de cada paquete, que disminuye con cada salto y el paquete se descarta cuando el contador llega a 0.

¿Cómo se determina el contador de saltos?

inicializar el contador de saltos a la longitud de la ruta entre el origen y el destino.

Si el emisor desconoce el tamaño de la ruta, puede inicializar el contador al diámetro total de la subred.

Inundación Selectiva:

Los enrutadores no envían

cada paquete de entrada por todas las líneas, sino sólo por aquellas que van aproximadamente en la dirección correcta.

¿Qué tipo de información necesita almacenar un enrutador

Se necesita saber en qué dirección va cada línea y en qué dirección está el destino.

problemas

Si los números de secuencia vuelven a comenzar,

reinará la confusión: Tenemos que usar un número de secuencia de longitud suficiente

Si llega a corromperse un número de secuencia

paquetes serán rechazados como obsoletos,

Como protección contra los errores en las líneas enrutador-enrutador, se

confirma la recepción de todos los paquetes de estado del enlace.

Si llega a caerse un enrutador (de origen),

perderá el registro de su número de secuencia. Si comienza nuevamente en 0, se rechazará el siguiente paquete:

¿Cuándo se puede detectar que un enrutador está caído?

Cuando se actualicen las tablas de enrutamiento y se mandan los paquetes Hello,

¿Una vez identificado que un enrutador está caído cómo proceder?

Se propaga la información de este hecho por toda la red.

Se hace que la información asociada al enrutador caído expire

cuando ese enrutador vuelva a la vida, puede comenzar con número de secuencia 0.

¿Cómo hacer para asegurar que no pueda perderse ningún paquete y sobrevivir durante un período indefinido?

Incluir un campo de edad en cada paquete:

Disminuir la edad una vez cada segundo.

Los enrutadores también decrementan el campo de edad

Se descarta el paquete cuya edad sea 0.

Algoritmo de inundación de paquetes de estado de enlace más eficiente:

Una vez que un paquete de estado del enlace llega a un enrutador
entra en un búfer de almacenamiento donde espera un tiempo breve.

Si antes de transmitirlo, llega

otro paquete de estado del enlace proveniente del mismo origen, se comparan sus números de secuencia.

Si son iguales, se descarta el duplicado.

Si son diferentes, se desecha el más viejo.

El buffer de paquetes para un enrutador contiene

una celda por cada paquete de estado de enlace recién llegado, pero aún no procesado por completo.

Una fila de la tabla del búfer de paquetes de un enrutador contiene:

Origen del paquete, número de secuencia, edad, datos de los estados de enlaces.

Banderas

de confirmación de recepción:

indica a dónde tiene que enviarse la confirmación de recepción del paquete.

de envío:

significan que el paquete debe enviarse a través de las líneas indicadas.

Si llega un duplicado mientras

el original aún está en el búfer, los bits de las banderas tienen que cambiar.

Control de congestión

meta

asegurar que la subred sea capaz de transportar el tráfico ofrecido.

Problemas de los algoritmos de control de congestión de TCP

El host de destino

demora demasiado en enterarse de la congestión

Los hosts solo se enteran de

pérdidas de paquetes, no pueden controlar qué paquetes perder y cuáles no.

Formas de disminuir la carga en la subred:

Regulación del tráfico:

hacer que hosts responsables de la congestión se enteren más rápido de la congestión y reduzcan su tasa de transferencia.

Desprendimiento de carga:

los enrutadores descartan paquetes inteligentemente antes que se saturen búferes.

Cómo identificar la congestión

Siempre que la demora reciente de cola de esta línea rebasa un umbral, la línea de salida entra en un estado de advertencia. Cada paquete nuevo que llega se revisa para ver si su línea de salida está en estado de advertencia. Si es así, se realiza alguna acción.

Regulación de tráfico

es cuando los emisores ajustan sus transmisiones para enviar un tráfico que la red pueda soportar.

¿Cómo se puede enterar un host de que hay congestión?

Se le avisa de la congestión.

Método de paquetes reguladores:

1. Usar paquetes reguladores si la línea de salida está en estado de advertencia, el enrutador regresa un paquete regulador (PR) al host de origen, proporcionándole el destino encontrado en el paquete.
- 2.
3. El PR le pide al host de origen que reduzca en un porcentaje X el tráfico enviado al destino especificado.

4. El host ignora los PR que se refieran a ese destino por un intervalo fijo.
5. Una vez que haya expirado ese tiempo, el host escucha más PR durante un intervalo.

Si llega alguno el host reduce el flujo aún más y comienza a ignorar nuevamente los PR.

Si no llega ningún PR durante el host incrementa el flujo.

cuando se satura una línea de salida de un enrutador, se pierden paquetes indiscriminadamente.

evitar la pérdida descontrolada de paquetes.

La primera solución es

descartar paquetes inteligentemente antes de que se ocupe todo el espacio de búfer cuando hay estado de advertencia en una línea de salida.

criterios para escoger qué paquetes descartar

Estrategia Vino:

Descartar primero los paquetes más nuevos.

P.ej. en la transferencia de archivos.

Estrategia Leche:

Descartar primero los paquetes más viejos.

P.ej. en multimedia.

Según la importancia de los paquetes.

Marcar los paquetes con clases de prioridades.

Los enrutadores primero se desprenden de paquetes de la clase más baja,

desprendimiento de carga junto con reducción de tráfico.

La respuesta a paquetes perdidos por desprendimiento de carga es que el origen disminuya su tasa de transferencia.

Si expira el temporizador de retransmisiones, el emisor lo toma como pérdida de paquete.

Algoritmo de detección temprana aleatoria (RED):

Para detectar cuándo comenzar a descartar paquetes, los enrutadores mantienen un promedio móvil de sus longitudes de cola.

Cuando este promedio de una cola C sobrepasa el umbral una pequeña fracción de los paquetes son descartados al azar.

Las consecuencias de elegir paquetes al azar hace más probable que los hosts emisores más rápidos pierdan un paquete, lo noten, y reduzcan su tasa de transferencia.

Complementos de Control de Congestión

si los enrutadores tienen infinita memoria,

la congestión empeora en lugar de mejorar,

ya que para cuando los paquetes llegan al principio de la cola su temporizador ha terminado (repetidamente) y se han enviado duplicados.

Los procesadores lentos

pueden causar congestión.

Las líneas de poco

ancho de banda también pueden causar congestión.

Subredes de Circuitos Virtuales:

Idea 1: Usar una técnica de control de admisión

una vez que se ha detectado la congestión no se establecen CVs nuevos hasta que ha desaparecido el problema.

Idea 2: permitir el establecimiento de nuevos

CV, pero enrutando cuidadosamente los circuitos nuevos por otras rutas que no tengan problemas.

Idea 3: negociar un acuerdo

entre el host y la subred cuando se establece un CV.

Este arreglo normalmente especifica el

volumen y la forma del tráfico, la calidad de servicio requerido y otros parámetros.

Para cumplir con su parte del acuerdo, la subred
reservará recursos a lo largo de la ruta cuando se establezca el circuito.

recursos pueden incluir
espacio en tablas y en búfer en los enrutadores y ancho de banda en las líneas.

De este modo es poco probable que
ocurran congestiones en los CV nuevos.

Método de bit de advertencia.

Señalar el estado de advertencia activando un bit especial en el encabezado del paquete.

Cuando el paquete llega a su destino,
la entidad transportadora copia el bit en la siguiente confirmación de recepción que se regresa al origen.

A continuación el origen
reduce el tráfico.

Mientras el enrutador está en estado de advertencia,
continúa activando el bit de advertencia, lo que significa que el origen continúa obteniendo confirmaciones de recepción con dicho bit activado.

El origen monitorea la fracción de confirmaciones de recepción con
el bit activado y ajusta su tasa de transmisión de manera acorde.

En tanto los bits de advertencia continúan fluyendo, el origen
continúa disminuyendo su tasa de transmisión.

Cuando la tasa de transmisión disminuye lo suficiente, el origen
incrementa su tasa de transmisión.

el tráfico se incrementa solo cuando
no haya enrutadores con problemas.

implementación de bit de advertencia usada por TCP
es ECN (Explicit Congestion Notification):

Se marcan 2 bits en el encabezado IP con distintos fines:

00: transporte no capaz de ECN

10: transporte capaz de ECN, ECT(0)

01: transporte capaz de ECN, ECT(1)

11: congestión encontrada, CE

Si ambos extremos soportan ECN

mandan sus paquetes con ECT(0) y ECT(1) respectivamente.

Si el paquete atraviesa la cola congestionada y el enrutador soporta ECN, se cambia código en el paquete a CE para avisar al receptor de la congestión.

Se usan dos banderas en encabezado TCP para soportar ECN:

ECE (ECN echo): se usa para mandar indicación de congestión al emisor.

CWR (ventana de congestión reducida): es usada para confirmar que la indicación ECE fue recibida.

Secuencia de ejecución de ECN típica:

Se negocia ECN en conexión TCP

Emisor manda un paquete IP “P” con ECT(0)

“P” llega a un enrutador congestionado que soporta ECN y enrutador marca “P” con CE.

Receptor recibe “P” con CE y manda segmento “Q” (con ACK de “P”) de vuelta usando bandera ECE prendida.

Emisor recibe “Q” con ECE prendido, entonces emisor reduce ventana de congestión.

El emisor manda el siguiente segmento al otro extremo usando bandera CWR prendida para confirmar la recepción de aviso de congestión.

Nota: Se continúa transmitiendo segmentos con ECE prendido hasta recibirse segmento con CWR prendido.

problema del método de paquetes reguladores

a altas velocidades o distancias grandes, el envío de un paquete regulador a los hosts de origen no funciona bien porque la reacción es muy lenta.

La solución es

usar el método de salto por salto, hacer que el paquete regulador ejerza su efecto en cada salto que da.

Protocolo de capa de Red IP

propósito:

Explicar formato de datagramas.

Definición de direcciones IP.

Definición de redes.

Definición y uso de tablas de reenvío.

Manejo de fragmentación de paquetes.

Datagramas IP

IHL :

Longitud del encabezado en palabras de 32 bits

Total Length :

2B de encabezado + datos ≤ 65535 B

Type of service :

Los 6 primeros bits se usan para indicar clase de servicio

Protocol :

(8b) dice a cuál proceso de transporte (p.ej. TCP, UDP, etc.) entregar el paquete

identificación :

se usa para que el host de destino determine a qué paquete un fragmento pertenece

tiempo de vida :

tiempo de vida de un paquete

Header checksum :

se usa para detectar errores cuando el paquete viaja a lo largo de la red.

Direcciones IPv4:

direcciones de origen y de destino:

Cada una tiene 32 b.

indican el número de red y el número de máquina.

Consecuencias:

uso números IP diferentes para distinguir las máquinas de una red.

Las direcciones IP son jerárquicas.

Cada host y enrutador en la internet tiene
una dirección IP.

Una máquina puede tener
más de un IP

Una máquina tiene un IP por cada red a la que está conectada

Conceptos fundamentales

Una red corresponde a un

bloque contiguo del espacio de direcciones IP llamado prefijo.

Prefijos

se escriben dando la dirección IP más baja en el bloque y la cantidad de bits usadas para la dirección de la red.

Ejemplo: ¿Qué significa el prefijo 128.208.0.0/24?

La porción de la red es de 24 bits

Que tengo 2^8 máquinas en la red

La dirección IP más baja en el bloque es 128.208.0.0.

Máscara:

está formada de 1's para identificar la red, seguido de 0's para identificar las máquinas

¿Cuál es la máscara de 128.208.0.0/24?

255.255.255.0

Subredes:

Conjunto de interfaces de dispositivos con la misma parte de red de la dirección IP

Asignaciones de redes a organizaciones**Evitar tablas de reenvío demasiado grandes:****solución:**

Alojar las direcciones IP de una red en un bloque contiguo que permite 2^k máquinas

Implementación

CIDR (Classless Inter Domain Routing).

En todas las máquinas de la red, la parte de la dirección IP para identificar la red es la misma.

Se representa la red asignada con un único prefijo.

Tablas de enrutamiento**¿ Cómo definir las tablas de enrutamiento ?**

El enrutamiento es
jerárquico

sólo se representan redes de
organismos.

Cada entrada de tabla de enrutamiento se

Tabla de enrutamiento para todas las redes tiene entradas:

(dirección IP inicio subred, máscara, línea de salida.)

¿ Cómo se usa la tabla de enrutamiento cuando llega un paquete?

1. Extraer dirección de destino IP.
2. Luego analizar la tabla entrada por entrada,

Hacer AND de la máscara de la entrada con la dirección de destino y comparar el resultado con la dirección IP de inicio de la subred de la entrada.

3. Si coinciden entradas múltiples se usa la máscara más larga (la red más pequeña).

Control de tamaño de tablas de enrutamiento

CIDR

se combinan varios

prefijos en un prefijo único más grande (conocido como superred).

A esto se le llama agregación de prefijos.

Racionamiento de uso de direcciones IPv4

¿Cómo aumentar la cantidad de máquinas?

traducción de dirección de red (NAT).

Asignar un solo N° de

IP a cada organización para el tráfico de internet.

Dentro de la organización cada computadora tiene

una dirección IP única que se usa para el tráfico interno(o

Cuando un paquete sale de la organización

va al ISP, se presenta una traducción de dirección (de la dirección de la computadora en la organización a la dirección IP usada por la organización en internet
)

implementación:

Para hacer posible este esquema

3 rangos de direcciones IP se han declarado como privados

La única regla es que

ningún paquete que contiene estas direcciones puede aparecer en internet.

3 rangos reservados

1.0.0.0 – 10.255.255.255/8 (16,777,216hosts)

172.16.0.0 – 172.31.255.255/12 (1,048,576hosts)

192.168.0.0 – 192.168.255.255/16 (65,536hosts)

PUERTOS:

Cada mensaje TCP saliente contiene

puertos de origen y destino que sirven para identificar los procesos que usan la conexión en ambos extremos

uso de los puertos cuando un proceso quiere establecer una conexión TCP

se asocia a un

puerto TCP sin usar en su máquina conocido como puerto de origen

el proceso otorga también un puerto destino para indicar a quién dar los mensajes del lado remoto

Problema:

Cuando la respuesta vuelve, se dirige a la dirección IP de la compañía

Como sabe ahora la caja NAT con que dirección se reemplaza?

Solución 1: Guardar asociación en la caja NAT de número

IP al puerto de origen que viene en el mensaje TCP/UDP dentro del paquete

Solución 2: Distinguir entre el número de puerto

usado para identificar la máquina (osea IPs en la red interna) y el número de puerto usado por TCP/UDP para identificar la conexión

Tabla de traducción de la caja NAT

Los índices en la tabla son

números de puertos para identificar la máquina

Una entrada de la tabla contiene

un par (número de puerto para identificar la conexión , dirección IP)

¿ Cómo tratar un paquete que llega a la caja NAT desde el ISP?

El puerto de origen en el encabezado TCP se

Desde la entrada localizada la

dirección IP interna y el puerto TCP se extraen e insertan en el paquete

Entonces el paquete se pasa al enrutador de la compañía para su entrega

¿Cómo tratar un paquete saliente de la caja NAT ?

La dirección de origen

se reemplaza por la verdadera dirección IP de la compañía

el campo puerto de origen TCP se

reemplaza por un índice en la tabla de traducción de la caja NAT

Críticas a NAT:

Viola el modelo de IP que dice que cada número IP pertenece solo a una máquina

Si la caja Nat se cae, se pierde toda su traducción y por lo tanto toda la conexiones TCP se destruyen

Retrasa la adopción de IPv6

Protocolo IP

Campo tiempo de vida en los paquetes:

Contador para limitar el tiempo de vida de un paquete

Debe ser

Cuando llega a 0

Previene que un

Subredes

Permiten que una red sea

dividida en varias partes para uso interno pero que actúe como una red simple para el mundo externo.

Cada subred puede ser una

LAN que tiene un enrutador

Los enrutadores de una subred se conectan a

un enrutador principal

no visibles por

fuera de la red

Cuando un paquete entra al enrutador principal, ¿cómo saber a qué subred pasarlo?

Eliminar algunos bits del N° de host para crear un número de subred

¿Cómo expresar subredes?

El enrutador principal usa una

máscara de subred que indica la división entre el número de red + número de subred y el host.

La máscara es una

información resumida de la red que me permite saber cuántos bits tiene la dirección de red y cuántos bits tenemos para las máquinas

Tabla de enrutamiento en un enrutador cuando hay subredes

Si se tienen entradas de la forma (dirección IP inicio subred, máscara) se hace

AND booleano con la dirección de destino del paquete y cada máscara de subred para deshacerse del número de host y buscar la dirección resultante en sus tablas

La cantidad máxima de hosts se da por

la cantidad de 0's a la derecha del último 1 en la dirección de origen.

Complementos a IP

IPv6

Encabezado de longitud

fija de 40 bytes para procesamiento más rápido de datagramas

Capacidad de direccionamiento

expandida: direcciones de 128 bits.

Etiquetado de flujos:

se etiquetan paquetes que pertenecen a un mismo flujo para los cuales el emisor requiere manejo especial.

Consecuencia de etiquetado de flujos:

Cuando un paquete con una etiqueta de flujo distinta de cero aparece, los enrutadores pueden ver en tablas internas para ver qué tipo de tratamiento especial requiere

Etiqueta de flujo:

(20 b) para identificar datagramas en el mismo “flujo”

Prioridad

(pri) tiene dos usos:

dar prioridad a ciertos datagramas dentro de un flujo.

dar prioridad a datagramas de ciertas aplicaciones sobre datagramas de otras aplicaciones.

Longitud de carga útil:

(16 b) número de bytes en el datagrama IPv6 luego del encabezado (de 40 B).

Límite de saltos:

(8 bits) el contenido de este campo se decrementa en 1 por cada enrutador que entrega el datagrama. Si el contador alcanza 0, el datagrama se descarta.

Próximo encabezado:

(8 bits) significa:

Cuál de los 6 encabezados de extensión de opciones actuales le sigue al encabezado. Si este encabezado es el último encabezado IP, el campo dice a cuál protocolo de transporte entregar el datagrama. Los encabezados de opciones también tienen este campo.

DHCP:

Meta:

permitir a los hosts cuando se unen a una red obtener dinámicamente su dirección IP a partir de un servidor de red.

DHCP puede retornar

Dirección del enrutador del primer salto para el cliente

Nombre y dirección IP del servidor DNS

Máscara de red

es ampliamente usado en redes de
acceso a internet residenciales y en redes LAN inalámbricas.

UPnP:

Problema:

¿Cómo puede un host detrás de NAT permitir pedidos de conexiones entrantes?

Una aplicación ejecutada en un host puede pedir un mapeo NAT entre su
(IP privado, Port privado) y su (IP público, Port público).

¿Si se acepta el pedido

Nodos de afuera pueden iniciar conexiones TCP con el (IP público, Port público) asignado.

ARP

Problema:

¿cómo se convierten direcciones IP en direcciones de Ethernet?

Solución:

el host de origen da salida a un paquete de difusión hacia Ethernet preguntando: ¿quien posee una dirección IP w.x.y.z ?

difusión

la dirección de destino consiste solo de 1s. 1. La difusión llegará a cada máquina en Ethernet y cada una verificará su dirección IP. 2. Al host de destino le bastará con responder con su dirección de Ethernet E. 3. Así el host de origen aprende que la dirección IP de w.x.y.z está en el host con la dirección de Ethernet E.

Optimizaciones

Una vez que una máquina ha ejecutado ARP,

Cuando la difusión de ARP llega al host de destino,

cada máquina

difunde su correspondencia cuando arranca.

Esto se hace mediante un ARP que busca su propia dirección IP.

No debe haber una respuesta,

Si llega inesperadamente una respuesta, es que la misma dirección IP se ha asignado a dos máquinas.

La más reciente debe avisar al gerente de sistemas y no arrancar.

sistema autónomo (SA)

consiste en

un grupo de enrutadores bajo el mismo control administrativo.

Generalmente distribuidos por
los ISP

A veces los ISP dividen su
red en varios SA

Los enrutadores dentro de un SA
corren el mismo algoritmo de enrutamiento (protocolo de enrutamiento intra-SA)

Internet es un conjunto de
SAs

¿Por qué se necesita definir un protocolo intra-SA especial para inter-
net?

Los protocolos de enrutamiento estudiados
no son compatibles con IP por la forma de las tablas de enrutamiento que se usaban.

no son adecuados cuando un SA es demasiado grande

El modelo de grafo no es adecuado cuando se trabaja con IP

A veces hay más de un
camino más corto a un destino y no se saca provecho de esta situación para balancear la carga que tiene un enrutador.

OSPF

(Open Shortest Path First)

Es un protocolo de

puerta de enlace interior (IGP, hace referencia a los protocolos usados dentro de un SA).

Se considera una adaptación del
método de enrutamiento de estado de enlace

Es compatible con
IP.

En OSPF el modelo de grafo asociado a un SA es
más flexible que el usado para los protocolos de enrutamiento anteriores al considerar redes de distintos tipos.

Para permitir los SA grandes, OSPF organiza un SA como

una jerarquía de niveles.

para un destino se puede considerar más de

una línea de salida (cuando hay más de un camino óptimo) para balancear la carga en la red.

Tipos de conexiones y redes soportadas

Líneas punto a punto entre dos enrutadores
Redes multiacceso con difusión (la mayoría de las LAN)

Redes de multiacceso con muchos enrutadores, cada uno de los cuales se puede comunicar directamente con los otros.

Representación de la red en un grafo

Los enrutadores se representan con

nodos

a cada arco se le asigna

un costo o retardo.

Una conexión punto-punto entre dos enrutadores se representa por

un par de arcos, uno en cada dirección.

Sus pesos pueden ser diferentes.

Una red de multiacceso se representa con un

nodo para la red en sí.

Los arcos desde el nodo de la red a los enrutadores tienen peso 0.

organizar un SA muy grande?

Considerar un SA como una red jerárquica. OSPF divide los SAs en áreas numeradas.

áreas numeradas.

Un área puede contener

varias redes dentro de ella.

Cada enrutador está configurado para

conocer qué otros enrutadores están en su área.

Las áreas no
se traslapan

Tipos de áreas:

Red dorsal (backbone) que tiene número 0, cuya topología no es visible desde fuera.

Áreas conectadas a la red dorsal

Clasificación de los enrutadores de un SA:

Enrutadores internos:
yacen completamente dentro de un área.

Enrutadores dorsales:
enrutadores en un área dorsal

Enrutador de borde de área (EBA).
Es parte de una red dorsal y a la vez de una o más áreas.

Aviso de estado de enlace (AEE)
contiene
el costo de un enrutador a todos sus vecinos.

Los EBA resumen

información de enrutamiento aprendida de un área para hacerla disponible en sus AEE que envían a las otras áreas.

¿Cómo definir la información resumida de un área no dorsal?

Un EBA E recibe avisos de estado de enlace de
todos los enrutadores de una de sus áreas A y con esa información determina el costo de alcanzar cada LAN de A.

La información resumida de A contiene el
costo de alcanzar cada LAN de A. Este paquete es puesto por el EBA E en la red dorsal para que llegue a las demás áreas.

¿Cómo definir la información resumida de un área dorsal?

Por medio de un grafo donde:

Todos los arcos unen pares de EBA

El peso de cada uno de estos arcos es el costo de camino óptimo que une el par de EBAs.

Esto permite que todos los enrutadores del área dorsal aprendan el costo de alcanzar todas las redes de cada área.

Todos los enrutadores aprenden a alcanzar todas las redes en el SA.

Al ejecutarse OSPF

los enrutadores dentro de un área ejecutan
una adaptación del protocolo de estado de enlace.

Cuando un enrutador se inicia,
envía mensajes Hello a:

Todas las líneas punto a punto

El grupo de todos los otros enrutadores de una LAN

De las respuestas cada enrutador aprende quiénes son sus vecinos.

Los enrutadores en la misma LAN son
todos vecinos.

OSPF no fija una política de cómo
los pesos de los enlaces son fijados.
Este es el trabajo del administrador de la red.

trabaja intercambiando
información entre enrutadores adyacentes.

Cada enrutador tiene
base de datos de estado de enlace (BDEE).

La BDEE
contiene
todos los AEE que el enrutador ha recibido.

debe ser
creada, y luego mantenerse.

Dentro de un área

cada enrutador debe tener el mismo grafo (BDEE) para construir la tabla de reenvío.

Consecuencias

En la BDEE se guarda información que un enrutador puede intercambiar con sus vecinos.

La información de una BDEE puede ser actualizada luego que un enrutador recibe AEE de vecinos.

Tipos de paquetes usados para intercambio de información entre enrutadores adyacentes:**Paquete de actualización de estado de enlace**

(PAEE): para mandar AEE asociado al enrutador emisor. Estos AEE tienen número de secuencia. Usando dicho número de secuencia el receptor puede ver si un AEE es más nuevo o más viejo que el que ya tiene.

Paquete de confirmación de estado de enlace

(PCEE): para confirmar los PAEE.

Paquete de descripción de base de datos

(PDBD): llevan resumen de la descripción de todos los AEE de la BDEE del enrutador emisor,

o sea, números de secuencia de los AEE del enrutador emisor.

El receptor puede determinar cuáles AEE de ese grupo necesita, comparando número de secuencia de un AEE con número de secuencia de AEE (del mismo enrutador) que ya tiene.

Paquete de pedido de estado de enlace

(PPEE): se usan para solicitar AEEs.

¿Cómo actualizan sus BDEE los enrutadores?**Dos enrutadores vecinos deben**

sincronizar sus BDEE.

Un vecino es el

maestro y el otro es el esclavo. El maestro controla el intercambio de PDBD.

Se intercambian PDBD, PPEE, PAEE, PCEE para asegurar que ambos vecinos tienen igual información en sus BDEE.

enrutador designado,

intercambia mensajes con todos los enrutadores de la LAN mediante sincronización.

Usando inundación cada enrutador

informa a todos los demás (de su área) sus enlaces con otros enrutadores y sus respectivos costos.

Este intercambio se hace periódicamente, cuando una línea se cae o regresa y cuando cambia su costo.

Para un enrutador R dentro de un área se puede ejecutar el algoritmo de Dijkstra.

Para esto usar la BDEE de R.

Dijkstra calcula el camino más corto desde R a cualquier otro enrutador de su área y red en el SA entero.

OSPF calcula todos los caminos más cortos entre dos nodos, y por ello puede dividirse el tráfico de envío entre ellos.

Interredes

Para enviar paquetes a una red con distinto protocolo:

Las puertas de enlace

traducen o convierten paquetes de un protocolo a otro.

Se construye una

capa arriba de las diferentes redes que oculte las diferencias entre las distintas redes.

Enrutamiento en interredes

Una vez construido el grafo de la interred pueden aplicarse algoritmos de enrutamiento al grupo de enrutadores multiprotocolo.

En cada red se usa

un protocolo de puerta de enlace interior (IGP).

Entre las redes se usa

protocolo de puerta de enlace exterior (EGP) o (PPEE).

Cada red puede usar distintos

IGP pero el EGP debe ser uno solo.

Fragmentación

Ocurre cuando

un paquete de gran tamaño quiere viajar a través de una red cuyo tamaño máximo de paquete es bastante más pequeño.

Se fragmenta el paquete en

la puerta de enlace

Para recuperar el paquete original, se puede:

Dirigir todos los fragmentos a

la misma puerta de salida y recombinar allí.

Tratar cada fragmento como

el paquete original y recombinar en el host de destino.

Entunelamiento

Tenemos una red distinta entre dos redes de la misma clase. Para mandar el paquete de una red a otra de la misma clase los paquetes son encapsulados en la red del medio usando un encabezado.

EGP/PPEE(External

Para enrutamiento inter-SA es

imposible encontrar un camino óptimo, ya que cada SA corre su propio protocolo interno,

Requisitos

Encontrar algún camino de SAs sin ciclos.

Respetar las políticas de los SAs

Los PPEE suelen implementarse sobre

Enrutadores de Borde de Sistema Autónomos (EBSA)

Un EBSA:

Hace una elección de varias rutas a un destino

Elige la mejor acorde a sus políticas

Informa a sus vecinos el camino usado para cada destino.

Relaciones entre SA

Proveedor-Consumidor:

El proveedor debe dar publicidad de rutas al ISP consumidor sobre el enlace que los conecta. El consumidor publica rutas a los destinos en su red al proveedor.

Compañerismo:

los ISP no se cobran por mandarse mensajes.

Multihoming:

Un ISP está conectado a varios ISP,

BGP

Es el PPEE usado por

la internet.

Provee a cada SA un medio para:

Obtener información de

alcanzabilidad de las subredes desde SA vecinos

Propagar esta información dentro del SA

Determinar buenas rutas a

las subredes

Que cada red publique

su existencia al resto de la internet.

En BGP los destinos son

prefijos.

Cada prefijo representa una

subred o colección de subredes.

Un SA es identificado por

un número globalmente único ASN (Número de sistema autónomo)

se incluye con el prefijo una

ruta que pasa por varios SA, compuesta por un prefijo y atributos BGP.

Atributos BGP:**AS-PATH:**

contiene los ASN de los SA por los cuales el aviso de prefijo ha pasado

Se usa para detectar y prevenir ciclos.

También para elegir entre varios caminos al mismo prefijo.

NEXT-HOP:

IP de la interfaz del enrutador que comienza el AS-PATH hacia el destino.

Propagar información de rutas en BGP

Pares de enrutadores intercambian información de rutas sobre conexiones TCP semipermanentes en el puerto 179

Sesiones BGP

Es la conexión TCP con todos los
mensajes BGP enviados

Una sesión BGP entre enrutadores de dos SA se llama
sesión externa BGP (eBGP)

Una sesión BGP entre enrutadores del mismo SA se llama
sesión interna BGP (iBGP)

Aviso de rutas

Cuando una puerta de enlace P recibe rutas:

P usa las sesiones iBGP para distribuir rutas a otros enrutadores dentro de su SA

La mejor ruta a un prefijo se guarda en
la Base de información de Enrutamiento (BIE)

Base de información de Enrutamiento (BIE)

reglas:

Rutas con mayor valor de preferencia local son elegidas

De las restantes, la ruta con el camino AS-PATH más corto es elegida

De las restantes, la que tiene el NEXT-HOP más cercano es elegida

Si queda más de una se usan criterios adicionales

Mensajes de actualización son usados para:

Información acerca de una ruta a través de internet

Una lista de rutas previamente avisadas por el enrutador emisor, que no son más válidas

Un mensaje de actualización hace que la BIE se actualice y que se emitan mensajes de actualización hacia otros vecinos.

Un enrutador BGP no tiene la obligación de
avisar una ruta a destino

Política de Importación

Cuando una puerta de enlace recibe aviso de ruta
usa su política de importación para aceptar o filtrar la ruta.

Si un enlace falla o cambia una política, los enrutadores BGP pueden
cancelar caminos avisados previamente. (Avisa ruta removida)

Capa de Enlace de Datos

Generalidades

La CED toma de la CR
paquetes y los encapsulan en tramas.

Las tramas tienen una
longitud máxima impuesta.

Cada paquete de la CR se
divide en tramas.

En la CR de la máquina de origen hay
un proceso que entrega bits a la CED para transmitirlos a la máquina de destino.

El trabajo de la CED es
transmitir los bits a la máquina de destino para que puedan ser entregados a su CR.

Limitaciones de los canales de comunicación

Cometen

errores ocasionales

Tienen una

tasa de datos finita

Hay

retardo de propagación

Meta

Lograr una

comunicación confiable y eficiente entre dos máquinas conectadas por un canal de comunicaciones.

Un protocolo de CED hace que

las líneas de comunicación parezcan perfectas o al menos bastante buenas.

Funciones

Control de flujo

Evitar que un

emisor rápido sature a un receptor lento.

Uso de

protocolos de tubería.

Control de buffer receptor

Parada y espera, Go-back-N, Selectiva.

Se da entre un nodo

receptor y uno que transmite un flujo de datos que fluye a lo largo de toda la red → se da salto a salto.

Entramado (flaming)

En el canal de difusión solo hay

un stream de bits.

¿Cómo detectar el inicio y fin de cada trama?

Usualmente se usa un patrón especial de bits para ello (llamado bandera).

Inicio y fin de trama → Preámbulo, Bandera de inicio.

Detección y corrección de errores

Se agrega a los mensajes de CED (tramas)

bits adicionales, para detectar errores en la transmisión o para saber cuál es el error.

Checksum, CRC.

Manejo de colisiones

Ocurren en

canales de difusión usados por varias máquinas.

Cuando dos máquinas intentan

transmitir tramas al mismo tiempo ocurre una colisión.

Informaciones que debería contener una trama

encabezado:

suele contener direcciones del origen y del destino, a veces la longitud de la trama, etc.

campo de carga útil

(el contenido que se quiere enviar).

un terminador final

(para control de errores).

información

adicional para el entramado.

Fundamentos de la comunicación

Se trabaja con:

Confirmaciones de

recepción de tramas

Temporización de

reenvío

Retransmisiones de

tramas (perdidas o dañadas)

Uso de

números de secuencia en las tramas (para identificar tramas duplicadas).

Llevar a

caballito (piggybacking) para aprovechar mejor el canal de comunicaciones.

Control de

flujo (para evitar que emisor sature a receptor más lento)

Flujo entre enrutadores

1. Al llegar trama al enrutador el hardware verifica si está libre de errores.
2. La CED comprueba si esta es la trama esperada y de ser así, entrega el paquete dentro de la trama al software de enrutamiento.
3. El software de enrutamiento elige la línea de salida adecuada y entrega el paquete a la CED para enviarlo.

Canales de Difusión:**Es costoso e incómodo hacer que**

todo par de máquinas de una organización estén conectadas directamente entre sí por dos canales

En un canal de difusión están

conectadas varias máquinas que quieren transmitir tramas por el canal. Si una máquina envía un mensaje todas las demás lo reciben.

Tipos**Inalámbricos**

P.ej. por uso de señales de radio o de microondas.

Cableados

P.ej. De un cable coaxial salen cables a distintas máquinas.

P.ej. de un concentrador salen cables a distintas máquinas

Mediante el uso de

conmutadores

Necesidad de Control de Colisiones:

Si dos tramas se transmiten

en forma simultánea en un canal de difusión se traslapan en el tiempo y la señal resultante se altera. Este evento se llama colisión.

¿Cómo evitar colisiones

Definir una

subcapa de la CED que se encargue del control de colisiones.

Esta subcapa se llama subcapa de control de acceso al medio SCAM.

La subcapa MAC es una subcapa inferior de la CED.

En una red de difusión el asunto clave es

cómo determinar quién puede usar el canal cuando hay competencia por él.

protocolos de acceso múltiple

(PAM) determinan quién sigue en un canal de difusión.

Soluciones

Inalámbricas

Estación base (access point) que coordina la comunicación entre hosts.

Se usa protocolo 802.11 (WIFI).

Cableadas

Ethernet cuando varias máquinas se enchufan a un concentrador (Hub) o a un mismo cable (cable coaxial).

Ethernet usa protocolo CSMA/CD para control de colisiones.

Control de colisiones en redes cableadas

Modelo de Estaciones

Hay N estaciones independientes que genera tramas para transmisión

Una vez generada una trama, la

estación se bloquea hasta que la trama se haya transmitido con éxito.

Suposición de canal único:

Hay un solo canal disponible donde todas las estaciones pueden transmitir y recibir

Propiedades de los canales de difusión modernos:

Fenómenos sucediendo en un canal que una estación podría detectar

Detectar que el canal está

en uso (o sea, alguna estación está enviando una trama).

Detectar que hay una

colisión en el canal.

En las LAN actuales**cada estación puede detectar si**

el canal está en uso está ocurriendo una colisión

El hardware de una estación

escucha el cable mientras transmite.

Si lo que lee es distinto de lo que puso en él, sabe que está ocurriendo una colisión.

¿Qué hacer si se detecta una colisión?

Dejar de enviar la trama, abortar las transmisiones de la estación apenas se detecte una colisión.

Ventajas de la detección de colisiones**Ahorra**

tiempo y ancho de banda.

Si no se detectan,

la estación no va a recibir la confirmación de recepción (expira un temporizador) y va a tener que retransmitir la trama.

para definir PAMs conviene que

una estación pueda detectar lo que está pasando en el canal.

CSMA con Detección de Colisiones (PAM CSMA/CD):

el emisor:

Antes de transmitir una trama

detecta a la portadora (refiere a la frecuencia central donde se portan los datos).

Si el canal está libre

transmite. Si no, espera hasta que el canal se desocupe para transmitir.

Si el emisor detecta una colisión,

aborta la transmisión, espera un tiempo aleatorio, y una vez que pasó este tiempo: goto 1

el receptor:

Recibe una

trama buena si no hubo colisión y el medio no cometió errores.

En caso contrario, recibirá una trama dañada la cual será descartada.

Al mandar una

confirmación de recepción hace los pasos del emisor.

Evaluación del uso del canal:

Períodos alternantes de contención y transmisión, ocurriendo períodos de inactividad cuando todas las estaciones no necesitan enviar tramas.

el canal puede estar en 3 estados.

Período donde el canal está ocioso, ninguna estación está enviando ninguna trama.

Período donde se está enviando una trama exitosamente.

Período de contención, donde no se logró transmitir ninguna trama con éxito.
→ hubo colisiones durante las ranuras de contención.

Se dice que una estación ha tomado el canal cuando

todas las demás estaciones sabían que estaba transmitiendo y no interfirieron.

El tiempo mínimo en detectar la colisión es

el tiempo que tarda la señal para propagarse de una estación a otra.

El peor caso de demora de una estación en enterarse que ha habido una colisión es

cuando el ruido de la colisión recorre la mitad de la distancia para llegar.

Cómo ocurre una colisión

y cuándo se enteran las estaciones de ella:

1. A comienza a transmitir en $t = 0$.
2. En $\tau - \epsilon$ un instante antes de que la señal llegue a B, B comienza a transmitir.
3. B detecta la colisión casi de inmediato y se detiene.
4. La ráfaga de ruido causada por la colisión no regresa a A hasta pasados $2\tau - \epsilon$.

En el peor caso una estación no puede estar segura de que ha tomado el canal hasta que

ha transmitido durante 2τ sin detectar una colisión.

las tramas tienen un requisito de

tamaño mínimo \rightarrow 512 bits.

Ethernet (IEEE 802.3):

Hardware

Transceptor:

maneja detección de portadora y detección de colisiones.

Tarjeta controladora:

Se encarga de ensamblar los datos en el formato de trama adecuado, calcular terminador de las tramas de salida, comprobar las tramas de entrada

Tipos de cableado

Cada cableado de Ethernet tiene una

longitud máxima de cable por segmento.

concepto de segmento,

el segmento fija una limitación ya que su longitud determina la distancia máxima que puede haber entre dos máquinas.

Una señal a medida que se va propagando por un cable se va debilitando.

Llega un punto a partir del cual la señal es
demasiado débil como para continuar su viaje.

Para que una señal pueda viajar más
se usan repetidores:

repetidor

es un dispositivo de capa física que recibe, amplifica (regenera) y retransmite
señales en ambas direcciones

introducen un
retardo.

Para permitir redes mayores que un segmento
conectar múltiples cables mediante repetidores.

Restricción

ningún par de
transceptores puede estar separado por más de 2,5 km

ninguna ruta
entre dos transceptores puede atravesar más de 4 repetidores.

A medida que aumente la velocidad de la red,
la longitud mínima de la trama debe aumentar o la longitud máxima del cable
debe disminuir, de manera proporcional.

Ethernet Conmutada:

conmutador (switch)

contiene una
matriz de conmutación de alta velocidad de 4 a 32 tarjetas de línea, cada tarjeta
de línea contiene de 1 a 8 conectores.

Tarea

Almacenamiento y reenvío de tramas de Ethernet.

Transparencia:

Los hosts no son conscientes de la presencia de conmutadores.

aprenden

por sí solos no necesitan ser configurados.

Si dos máquinas conectadas a la misma tarjeta de conexión transmiten tramas al mismo tiempo y si todos los puertos de la tarjeta forman una LAN local dentro de la tarjeta:

Las colisiones en esta LAN en tarjeta se
detectan y manejan igual que en una red CSMA/CD.

Las tarjetas pueden estar
transmitiendo en paralelo.

Si cada puerto de entrada se almacena en un búfer

todos los puertos de entrada
reciben y transmiten tramas al mismo tiempo, para una operación en paralelo duplex.

Cada puerto es
un dominio de colisión independiente.

tabla de conmutador:

<dirección MAC del host, interfaz para alcanzar el host, estampilla de tiempo>

Un conmutador aprende
cuáles hosts pueden ser alcanzados a través de cuáles interfaces.

Cuando el conmutador recibe
una trama registra el par emisor /localización en la tabla del conmutador.

Reenvío de una trama recibida por el conmutador:

Registrar enlace de ingreso, dirección MAC del host emisor de la trama.

Identificación de la interfaz del destino:

Se busca en la tabla del conmutador la dirección MAC del destino:

if se encuentra la entrada para el destino then { if el destino está en el segmento por el cual vino la trama then descartar trama else enviar trama en la interfaz indicada por la entrada }

si no se encuentra una entrada para el destino:

else inundar /* enviar en todas las interfaces excepto aquella por la que llegó la trama */

La ventaja de usar conmutadores es

que se pueden enviar tantos datos por segundo como la capacidad de la matriz de conmutación de alta velocidad. un conmutador tiene varios buffers por tarjeta o por cada puerto → hay muchas menos colisiones.

Problemas al diseñar protocolo de CED:

¿Cómo asegurar que una trama se entregue?

Si una trama no se entregó, entonces el emisor la reenvía.

Regresar tramas de control con

confirmaciones de recepción positivas o negativas de las tramas que llegan.

Método que usa temporizador de retransmisiones

Al enviarse una trama,
se inicia un temporizador.

Si la trama o la confirmación de recepción se pierden

el temporizador expirará. Luego, se puede enviar la trama de nuevo.

Si la confirmación de recepción llega

antes que el temporizador expira, entonces el temporizador se cancela.

¿Cómo hacer para evitar entregar a la CR tramas repetidas?

Método que

asigna números de secuencia a las tramas que salen.

El receptor tiene una

función que dado un número de secuencia de la trama que llega decide si ella es duplicada.

¿Qué hacer con un emisor que quiere transmitir tramas a mayor velocidad que aquellas con que puede aceptarlos el receptor?

Solución basada en

retroalimentación el receptor autoriza al emisor a enviar más datos. (control de flujo).

¿Cómo transmitir datos entre dos máquinas y en ambas direcciones eficientemente?

Solución

llevar a caballito (piggybacking).

Cuando llega una trama de datos, el receptor se aguanta y espera hasta que la CR le pasa el siguiente paquete P.

La confirmación de recepción se
anexa a la trama de datos de salida con P

¿Qué pasa si la CED espera demasiado por una trama a la cual superponer el ack?

El temporizador del emisor expirará y la trama será retransmitida. ¿Cómo hacer para evitar que pase eso? Si llega en menos de x msecs un paquete, el ack se superpone a él sino, la CED manda trama de ack independiente.

PAM: ALOHA puro

emisor:

Transmite cuando
tiene datos para enviar.

Escucha el canal por
un tiempo igual a la demora de propagación de ida y vuelta máxima en la red más un incremento fijo de tiempo.

Si se escucha un ack en ese tiempo,
todo anduvo bien. Si no, se espera un tiempo aleatorio y la trama se manda de nuevo.

Si se falla en recibir un
ack luego de varias retransmisiones se tira la toalla.

receptor:

Al recibir una trama
chequea su validez y si lo es, inmediatamente manda un ack.

Si la trama es inválida
el receptor la ignora, la trama puede ser inválida por ruido o por colisión.

Evaluación

Este método bajo carga baja es
eficiente y tiene una demora baja.

En ALOHA puro una estación
no escucha el canal antes de transmitir esto generará probablemente muchas colisiones.

el número de colisiones crece
rápidamente a medida que aumenta la carga,

la máxima utilización del canal es
alrededor del 18%.

CSMA persistente 1

emisor:

Si una estación tiene datos por enviar,
primero escucha el canal para saber si otra está transmitiendo en ese momento.

Si el canal está ocupado,
entonces la estación espera hasta que se desocupe.

Cuando la estación detecta un canal inactivo,
transmite una trama.

Si ocurre una colisión,
la estación espera una cantidad aleatoria de tiempo y comienza de nuevo.

Comportamiento luego que emisor envió una trama

La estación
espera un tiempo razonable por un ack, teniendo en cuenta el tiempo de propagación de ida y vuelta máximo en la red

Si no recibe ack
la estación espera una cantidad aleatoria de tiempo y comienza de nuevo.

receptor:

Al recibir una trama
chequea su validez y si lo es, inmediatamente manda un ack.

Si la trama es inválida
el receptor la ignora, la trama puede ser inválida por ruido o por colisión.

retardo de propagación

tiene un
efecto importante en el desempeño de CSMA persistente 1.

Caso de que justo después de que una estación comienza a transmitir, otra estación está lista para enviar,
si la señal de la primera estación no ha llegado aún a la segunda, esta última detectará un canal inactivo y comenzará a enviar también, eso producirá una colisión.

Aun si el retardo de propagación es cero,
habrá colisiones dos estaciones quieren enviar y detectan que una tercera está transmitiendo. Luego que la tercera termine de transmitir las dos estaciones que quieren enviar detectarán un canal inactivo, por lo tanto enviarán y se producirá una colisión.

Ethernet

Direcciones

Se usan direcciones de
6 bytes

Se escriben como

6 pares de dígitos hexadecimales separados por '-'. → P.ej: 1A-23-F9-CD-06-9B

El bit de orden mayor de la dirección de destino es
0 para las direcciones ordinarias y de 1 para las direcciones de grupo.

Una trama que consiste únicamente de bits 1 en el campo de destino

se acepta en todas las estaciones de la red (broadcasting).

Campo Tipo

El campo de tipo indica al receptor a qué proceso entregarle la trama.

Longitud de trama mínima

Las tramas deben tener al menos
64 bytes de largo,

Cuando los datos más el encabezado ocupan menos de 64 bytes.

Uso del campo de relleno (para alcanzar los 64 B)

Suma de verificación

Tiene 32 bits de largo.

Se usa un método de

detección de errores llamado código polinomial.

cambios al formato DIX**Reducir el**

preámbulo a 7 bytes y usar el último byte para un delimitador de inicio de trama.

Cambiar el campo de Tipo por

un campo de Longitud.

Poner un

pequeño encabezado a los datos para dar información de tipo.

Diferentes modos de cablear un edificio:**Un cable pasa entre**

cuarto y cuarto y cada estación se conecta a él en el punto más cercano.

Una columna vertical

corre del sótano a la azotea y en cada piso se conectan cables horizontales a dicha columna.

En cada piso conectar cable a columna con un repetidor entre ambos.

Topología de árbol

El medio de transmisión es un cable que se divide en ramas.

El árbol tiene puntos conocidos como headends donde uno o más cables comienzan

La transmisión desde una estación se propaga por el medio y puede ser recibida por todas las otras estaciones.

Algoritmo de retroceso exponencial binario**Algoritmo que determina**

en Ethernet el tiempo de espera del emisor cuando ocurre una colisión.

Tras una colisión

el tiempo se divide en ranuras cuya longitud es igual al tiempo de propagación de ida y vuelta en el peor caso en el cable 2τ .

El tiempo de ranura es

512 tiempos de bit o $5,12 \mu \text{ seg.}$

las estaciones afectadas por la colisión

eligen cada una aleatoriamente una cierta cantidad de ranuras a esperar.

algoritmo

Tras i colisiones se escoge un número aleatorio entre
0 y $(2^i - 1)$ y se salta ese número de ranuras.

Tras haberse alcanzado 10 colisiones

el intervalo de aleatorización se congela en un máximo de 1023 ranuras.

Tras 16 colisiones el controlador

tira la toalla y avisa de un fracaso a la computadora. La recuperación posterior es responsabilidad de las capas superiores.

Evaluación

El algoritmo asegura un

retardo pequeño cuando unas cuantas estaciones entran en colisión.

El algoritmo asegura que la colisión

se resuelva en un intervalo razonable cuando hay colisiones entre muchas estaciones.

Ethernet Rápida:

Fast Ethernet (o 802.3u)

es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps.

Cableado

Cable par trenzado de cobre con (Cat 5 UTP) domina el mercado.

100BASE-T

Se usan pares de cobre trenzado

2 tipos de dispositivos de interconexión: concentradores y conmutadores.

CSMA/CD y el algoritmo de retroceso exponencial binario.

Se usan dos pares de cable trenzado: uno para enviar y otro para recibir.

100BASE-TX

Se usan dos pares de cable trenzado uno para enviar y otro para recibir.

100BASE-FX

2 líneas de fibra óptica una para recepción (RX) y la otra para transmitir(TX).

La distancia entre una estación y el conmutador es de hasta 2 km.

Los cables 100BaseFX deben conectarse a conmutadores.

Interconectando conmutadores:

Conmutadores pueden

conectarse entre sí:

(se trabaja

exactamente de la misma manera que en el caso de un único conmutador).

Redes Inalámbricas

Señales:

Intensidad decreciente de la señal

Dispersión (A más lejos de la antena, menos intensidad en la señal de recepción),
atenuación (energía que se pierde en el cable a lo largo del tiempo).

Interferencias de otros orígenes

Ruido electromagnético, bandas abiertas ISM.

Propagación multi-camino

Rebotes en objetos.

Mayor tendencia a

errores en el bit que las redes cableadas por lo que usan técnicas de detección y
recuperación de errores más robustas.

SNR y BER:

Señal electromagnética (no eléctrica).

Necesario 1) sensibilidad del receptor (RSSI)

Que el receptor pueda detectar a señal.

Necesario 2) relación señal a ruido (SNR)

Que el receptor pueda entender la señal

Esquema de Modulación

(Propiedades de ondas, no se puede cargar 1 y 0 \rightarrow se deben traducir mediante modulación).

Tasa de error (BER)

Cada cuantos bits tengo un bit errado, depende el ruido y la potencia.

Modulación SNR y BER:

cuanto mayor es la SNR,
menor BER.

Para una SNR dada, una modulación

con tasa de bit más alta tendrá un mayor BER.

Problemas de la comunicación inalámbrica:

Los nodos inalámbricos usualmente no pueden
transmitir y recibir al mismo tiempo.

La potencia generada por el emisor es

mucho más alta que lo que probablemente será una señal recibida

Las redes inalámbricas no pueden

escuchar colisiones,

Se usa

CSMA/CA (Acceso Múltiple con Detección de Portadora y Evitación de Colisiones) (WiFi 802.11)

Problema de la estación oculta

La estación C transmite a la estación B. Si A detecta el canal no escuchará nada y concluirá erróneamente que ahora puede comenzar a transmitir a B. Si lo hace \rightarrow colisión!

Problema de la estación expuesta

Supongamos que B transmite a A, y que C desea enviar a D por lo que escucha el canal. Cuando C escucha una transmisión concluye erróneamente que no debería

transmitir a nadie porque escucha la transmisión de B. Pero no hay problema si C transmite a D, porque no va a interferir con la habilidad de A de recibir de B

Canales y Asociación:

Cada host necesita

asociarse con un AP antes de poder enviar o recibir datos de la capa de red.

Puede haber más de 1

AP.

Se crea un

“cable virtual” entre el host y el AP.

AP →

Identificador (SSID, Service Set Identifier)

Escaneo Activo:

iniciado por el host

1. El nodo manda una trama de prueba.
2. Los AP al alcance responden con una trama de respuesta.
3. El nodo elige el AP y envía trama de pedido de asociación.
4. El AP responde con una trama de respuesta de asociación.

Re asociación

el nuevo AP notifica al AP anterior del cambio. Si estos AP son partes del mismo sistema extendido hay un protocolo de comunicación entre APs que permite notificar que un nodo se ha dado de baja en uno y se ha dado de alta en otro.

Escaneo Pasivo:

iniciado por el AP

AP difunde una trama guía periódicamente

Capacidades (i.e., tasas de transmisión) e identificador del AP, la hora, cuánto falta para la próxima trama guía, etc.

El nodo elige el AP y envía trama de pedido de asociación.

El AP responde con una trama de respuesta de asociación.

Otras responsabilidades de AP:

Asociación :

establece asociación inicial entre nodo y AP.

Reasociación :

para transferir una asociación a otro AP (handoff)

Desasociación :

notificación por nodo o AP que una asociación existente terminó.

Subcapa MAC 802.11:**Soporta dos modos****DCF**

función de coordinación distribuida.→ para redes ad hoc

PCF

función de coordinación puntual → para redes basadas en infraestructura (AP)

DCF:**En ethernet no existe**

RTS ni CTS ya que no necesita evitar la colisión.

Colisiones:

Dos nodos pueden enviar RTS simultáneamente. Emisores asumen una colisión porque no reciben el CTS luego de un cierto intervalo de tiempo.

Emisores esperan

una cantidad de tiempo (algoritmo de retroceso exponencial binario) e intentan de nuevo.

Estación oculta:

CTS es escuchado por una estación oculta (establece el NAV) No envía nada (tiempo incluido en el RTS y CTS). Luego de ese tiempo más un pequeño intervalo el canal puede ser asumido disponible otra vez y otro nodo es libre de intentar enviar.

PCF:

Es opcional usarlo, tiene que haber un momento donde los nodos puedan “hablar” DCF ya que no todos “hablan” PCF.

Hay una relación uno a uno entre hosts y AP (asociación) → BSS

AP: responsable de enviar y recibir datos (i.e. paquetes) desde y hacia hosts asociados con el AP
AP: responsable para coordinar la transmisión de varios hosts inalámbricos asociados.
AP: sondea los nodos preguntándoles si tienen tramas para enviar
AP: → no ocurren colisiones

El tiempo en el medio se divide en:

Período sin (contention) disputa (PCF)

Implementada en AP,

Nodos transmiten sólo si lo pide el AP.

El AP tiene una lista de nodos “privilegiados”

Los nodos se registran para estar en la lista.

Período en (contention) disputa (DCF)

Implementado en los nodos

Los nodos compiten por el medio

Beacon (baliza):

el AP demarca el inicio de la trama.

Contiene información de cuánto esperar para el próximo.

Ese es el tiempo de un NAV, dentro del cual ocurren diálogos dentro del PCF.

Poll (sondeo):

el AP pide a la estación que transmita.

Cuando esa estación termina de transmitir, termina su turno y el derecho a transmitir pasa a la siguiente estación.

Tiempos Entre Tramas:

SIFS

(Short Inter Frame Space) de 28 us

Intervalo entre tramas en un mismo diálogo (ACK, CTS, datos).

PIFS

(Point Coordination IFS) de 78 us

Intervalo entre tramas asumido por el AP (PCF).

DIFS

(Distributed IFS) de 128 us

Intervalo entre tramas asumido por nodos (DCF).

SIFS:

Dentro de un
diálogo se usan intervalos SIFS

Hacen falta los SIFS para cosas como
calcular suma de verificación, entramado, de la próxima trama.

Una estación usando SIFS para determinar la oportunidad de transmisión tiene
la prioridad más alta.

Hay solo una estación que puede responder luego de un intervalo SIFS,
nodo el cual está transmitiendo o recibiendo en ese momento.

PIFS:

Entre dos
diálogos diferentes se usa un PIFS (dentro de PCF).

Luego de un PIFS
el AP puede mandar una trama beacon o poll.

Dentro de un PIFS se
impide el uso de DCF.

El AP puede hacer sondeo
en forma
round-robin a todas las estaciones:

Cuando se emite un sondeo,
la estación responde usando un SIFS.

Si el AP recibe una respuesta a un poll,
puede hacer otro poll usando PIFS.

Si no se recibe respuesta al poll,
el AP puede hacer otro poll.

DIFS:

Luego de un período de PCF, viene un
DCF (con CSMA/CA), cuyas conversaciones se rigen por un DIFS.

Si el AP no tiene nada que decir

y ocurre un tiempo DIFS, cualquier estación puede intentar adquirir el canal.

Capa Física

se encarga de

transportar un stream de datos de una máquina a otra usando medios físicos

medios físicos

Bit, enlace físico, par trenzado (TP), cable coaxial, cable de fibra óptica, radio link types, wide-area, satellite.

se conectan entre sí usando

dispositivos como codecs, modems, multiplexores, etc.

Señales Digitales y Analógicas

Señales analógicas:

Caracterizadas por función matemática continua

Señales digitales:

Con conjunto fijo de niveles válidos

Señales digitales vs señales analógicas

Las señales digitales generalmente son

más baratas que las señales analógicas y son menos susceptibles a interferencias de ruidos

Las señales digitales sufren más de

atenuación (reducción de fuerza de la señal) que las señales analógicas

Esta atenuación puede llevar rápidamente a la pérdida de información contenida en la señal

Ondas Sinusoidales

Son producidas por

fenómenos naturales,

ejemplo,

los tonos audibles suelen ser ondas sinusoidales

Onda sinusoidal

$s(t) = A \sin(\pi f t + \phi)$, t número real

Propiedades

Frecuencia =

número de oscilaciones por segundo $f = 1/T$ (cantidad de ciclos por segundo)

Amplitud =

diferencia entre las alturas máxima y mínima

Fase =

cuánto es desplazado el comienzo de la onda sinusoidal a partir de un tiempo de referencia

período (T) =

tiempo requerido por un ciclo

Los sistemas de comunicación usan

altas frecuencias (expresadas en millones de ciclos por segundo megahertz (MHz))

Señales Compuestas

Señales simples:

Una onda sinusoidal

Señales compuestas:

Puede descomponerse en un conjunto de ondas sinusoidales simples

Una señal electromagnética va a ser

compuesta;

además va a ser hecha de varias frecuencias

Descubrimiento de Fourier

Toda señal es hecha a partir de un conjunto de funciones sinusoidales (cada una con frecuencia, amplitud y fase)

Señales periódicas:

$s(t+T) = s(t)$ para todo $-\infty < t < \infty$.

Señales aperiódicas

(también no periódicas)

Si una señal compuesta es periódica,

entonces las partes constitutivas son también periódicas

La mayoría de los sistemas usan

señales compuestas para transportar información

Una señal compuesta es creada en

uno de los extremos y el receptor descompone la señal en sus componentes simples

Representaciones Gráficas De Las Señales

Representación de dominio de tiempo

Grafo de una señal como función del tiempo

Representación de dominio de frecuencia

Muestra conjunto de ondas sinusoidales simples que constituyen la función compuesta

A $\sin(2 \pi f t)$ es representada por una línea simple de altura A que se posiciona en $x = f$

Representación De Dominio De Frecuencias

La representación de dominio de frecuencia es

muy compacta

El espectro de una señal =

rango de frecuencias que contiene

Es el intervalo desde la frecuencia más chica a la frecuencia más grande

El ancho de banda analógica =

ancho del espectro

Diferencia entre las frecuencias más altas y la más bajas

Señales Digitales

Las señales digitales usan

voltajes para representar valores digitales

Mecanismos de transmisión físicos usan

dos o más niveles de voltaje para enviar señales digitales

Cada nivel representa un número binario

Usar 2^n niveles para

representar número de n bits.

Baudios y Bits por Segundo

El hardware coloca límites en

cuán corto el tiempo en un nivel debe ser

Si la señal no permanece en un nivel por suficiente tiempo,

el hardware receptor va a fallar en detectarlo

La cantidad de veces que una señal puede cambiar por segundo se mide en

baudios

baud y número de niveles de señal controlan la

tasa de bits

Relación entre baudios, niveles de señal y tasa de bits

bits por segundo = N° baudios * $\lceil \log_2(\text{niveles}) \rceil$

La Tasa De Datos Máxima De Un Canal

Teorema de Nyquist

Si la señal consiste de V niveles de voltaje, el teorema de Nyquist (1924) establece:

Tasa de datos máxima = $2H \log_2 V$ bps

cantidad de ruido térmico

se mide por

la relación entre la potencia del ruido, llamada radiación señal a ruido.

Si indicamos la potencia de una señal con S y la potencia del ruido con una N, la relación señal a ruido es
S/N

La relación misma no se expresa; en su lugar se da la cantidad $10 \log_{10} S/N$. Estas unidades se conocen como decibels (dB).

Resultado de Shannon (1948)

La tasa de datos máxima de un canal ruidoso cuyo ancho de banda es H Hz y cuya relación señal a ruido es S/N, está dada por:

$N^\circ \text{ máximo de bps} = H \log_2(1+S/N)$

La fórmula solo da un

límite superior y los sistemas reales rara vez lo alcanzan

Cálculo de niveles distinguibles de voltaje que valen la pena

Suponemos que conocemos la relación señal a ruido S/N. La cantidad de niveles de voltaje permitidos depende de S/N.

Igualando Nyquist y Shannon: $V = (1+S/N)^{(1/2)}$

Modems, portadora,

Módem:

Un módem permite

convertir señales digitales en analógicas y recíprocamente.

Todos los módems modernos transmiten

tráfico en ambas direcciones al mismo tiempo (mediante el uso de frecuencias distintas para las diferentes direcciones).

Muchos sistemas de comunicación de larga distancia usan

una portadora (carrier) de orden sinusoidal. Los sistemas hacen pequeños cambios a la portadora para representar información siendo enviada.

Modulación:

El emisor debe cambiar

una de las características de la onda: amplitud, frecuencia, desplazamiento de fase.

Portadora de onda senoidal =

tono continuo en el rango de 1000 a 2000 HZ

de amplitud (b)

Se usan

dos niveles diferentes de amplitud para representar 0 y 1

de frecuencia (c)

Se usan

dos o más tonos diferentes

Si la señal es más fuerte,

la frecuencia del carrier aumenta y

si la señal es más débil,

la frecuencia del carrier disminuye

Es más

difícil de visualizar

de fase (DF)

Es posible usar

cambios en la fase para representar una señal

El DF se mide por

el ángulo de cambio

de fase (d)

Al requerir el

DF al final de cada intervalo, se facilita que el receptor reconozca los límites de los intervalos

Detección de cambio de fase

Un receptor puede

medir la cantidad portadora desplazada durante un DF

Usualmente los sistemas están diseñados para para usar
 2^n DF, así un emisor puede usar bits de datos para elegir entre los DF.

Diagramas De Constelación

El eje horizontal se refiere a

los componentes de símbolos que están en fase con la señal portadora y

el eje vertical a

los componentes en cuadratura (90°)

Los diagramas de constelación también pueden usarse para

reconocer el tipo de interferencia y distorsión en una señal

Los ejes del plano del diagrama suelen ser llamados

“I” (en fase) y “Q” (en cuadratura). En la constelación se representa la relación de amplitud y fase de una portadora modulada digitalmente

El módulo viene dado por

la distancia entre el origen de las coordenadas y el punto.

La fase es el

ángulo que una línea que une al origen con el punto hace con el eje horizontal.

Multiplexado

¿Cómo hacer para poner muchas señales en un mismo canal?

Usar multiplexores y demultiplexores

Multiplexado:

Un canal transportar varias señales

Multiplexor: Mecanismo que implementa el concepto anterior

Demultiplexado:

Separar la combinación de señales constitutivas

Demultiplexor: Mecanismo que implementa el concepto anterior

FDM (multiplexado por división de frecuencia):

El espectro de frecuencias se divide en
bandas de frecuencia

cada usuario posee
exclusivamente alguna banda.

Funcionamiento de un multiplexor

Primero se eleva la frecuencia de los canales de voz, cada uno en una cantidad diferente

Después de lo cual se pueden combinar, porque en ese momento no hay dos canales que ocupen la misma porción del espectro.

Funcionamiento de un demultiplexor

Se usan filtros para recuperar las señales originales

Utilidad

FDM aún se usa sobre cables o canales de microondas, requiere circuitos analógicos

TDM (multiplexado por división de tiempo):

Los usuarios esperan su turno (en round-robin), y cada uno obtiene en forma periódica toda la banda durante un breve lapso de tiempo.

Los bits de cada una de las

puede manejarse por completo mediante
dispositivos digitales y por ello es popular

Aplicación

TDM es ampliamente usado como parte de las redes de teléfonos y redes de celulares.

Principio de Superposición de Ondas

Si dos señales en un punto están en fase se agregan para sumar sus amplitudes, pero si están fuera de fase, se restan para dar una señal que es la diferencia de las amplitudes.

CDM (multiplexado por división de código):

Permite

varias señales de diferentes usuarios, compartir la misma banda de frecuencias.

Varios usuarios pueden

coexistir y transmitir simultáneamente con interferencia mínima

a menudo se lo llama

CDMA (Code Division Multiple Access)

las tramas que colisionan

no son distorsionadas; en cambio, se agregan múltiples señales en forma lineal

Esto es debido al principio de superposición de ondas

cada tiempo de bit se

subdivide en m intervalos cortos llamados chips

Hay 64 o 128 chips por bit

A cada estación se le asigna un

código único de m bits llamado secuencia de chips

Notación bipolar:

el 0 en binario es -1 y el 1 en binario es +1

Usamos la notación bipolar para la secuencia de chips y mostraremos la secuencia de chips entre paréntesis

Transmisión en un tiempo de bit

Una estación puede transmitir un 1 enviando su secuencia de chips en bipolar,

Puede transmitir un 0 enviando su negativo de su secuencia de chips

Requisito

Todas las estaciones están sincronizadas
todas las secuencias de chips comienzan al mismo tiempo

Notación

El símbolo S significa el vector de m chips para la estación S (en notación bipolar)
y \underline{S} para su negación (cambiar de signo cada componente de S)

Dos secuencias de chips S y T son ortogonales si y sólo si cumplen:

$$S * T \equiv \frac{1}{m} \sum_{i=1}^m S_i T_i = 0$$

o sea, el producto interno normalizado de S y T es 0

¿Cómo hacer para que un receptor pueda recuperar la señal enviada por una estación de manera sencilla?

Todas las secuencias de chips deben ser ortogonales dos a dos.

Para recuperar el flujo de bits de una estación, el receptor:

Calcula el

producto interno normalizado de la secuencia de chips recibida y la secuencia de chips de la estación cuyo flujo de bits se está tratando de recuperar

Si la secuencia de chips recibida es S y el receptor está tratando de escuchar una estación cuya secuencia de chips es C ,

simplemente calcula $S * C$

Las secuencias ortogonales de chips para las estaciones se pueden generar utilizando un método conocido como

código de walsh

propiedades

Si $S * T = 0$, entonces

$S * T = 0$

El producto normalizado de cualquier secuencia de chips por si mismo es

1.

$$S * S = \frac{1}{m} \sum_{i=1}^m S_i^2 = \frac{1}{m} \sum_{i=1}^m (\pm 1)^2 = 1$$

Además $S * S = -1$

sistema CDMA

sin ruido, el número de estaciones que envían concurrentemente puede ser hecho arbitrariamente grande usando secuencias de chip más largas

Aplicación

Además de que en las redes celulares, CDMA es usado por redes satelitales y de cable.

OFDM

(Orthogonal Frequency Division Multiplexing)

El ancho de banda del canal es

dividido en varias portadoras que independientemente envían datos (e.g., con QAM)

Estas portadoras son

empaquetadas juntas en el dominio de frecuencias, de modo que las señales de cada portadora se extienden a las adyacentes

Las portadoras pueden ser

muestreadas en sus frecuencias del centro sin interferencia de sus vecinos

Para hacer este trabajo, un tiempo guarda es necesitado para repetir una porción de los símbolos de señales en el tiempo de modo que tienen la respuesta de frecuencia deseada

es usada en

802.11 y redes de cable

WDM

(multiplexación por división de longitud de onda):

Se refiere a

la aplicación de FDM a la fibra óptica

Las entradas y salidas de WDM son

longitudes de onda de luz

Denotadas por la letra griega λ , e informalmente llamados colores

Un multiplexor acepta

rayos de luz en varias longitudes de onda y usa un prisma para combinarlos en un rayo único

Un demultiplexor usa un

prisma para separar las longitudes de onda

Medios De Transmisión

se clasifican en:

guiados

cable de cobre, fibra óptica

no guiados

radio

magnéticos

DVDs, Blu-ray, cintas magnéticas

Cable de par trenzado de cobre:

Son dos alambres de aproximadamente 1 mm de grueso se trenzan, logran alcanzar algunos km sin amplificación,

Evaluación:

El ancho de banda depende del ancho del cable y la distancia recorrida son ampliamente utilizados.

Cable coaxial:

Con mejor blindaje que los pares trenzados, puede recorrer distancias más largas a mayor velocidad

Evaluación:

buena combinación de alto ancho de banda y excelente inmunidad al ruido

Velocidad de propagación entre 66% y 90% de la velocidad de la luz

Fibra Óptica:

Con la tecnología de fibra óptica el ancho de banda alcanzable es de 50,000 Gbps (50 Tbps). El límite actual ronda a los 100 Gbps

Se dice que cada rayo tiene

un modo diferente,

una fibra que tenga esta propiedad se llama

fibra multimodo

Fibra monomodo:

El diámetro de la fibra se reduce a unas cuantas longitudes de onda de luz, la luz se propaga sólo en línea recta.

¿Cómo hacer para aprovechar la fibra óptica si los hosts no usan señales ópticas?

1. Fuentes de luz
 - a. Un pulso de luz indica un bit 1 y la ausencia de luz indica un bit 0
2. El medio de transmisión es una fibra de vidrio ultra delgada
3. El detector genera un pulso eléctrico cuando la luz incide en él

Transmisión inalámbrica:**Ondas electromagnéticas:****Cuando los electrones se mueven,**

crean ondas electromagnéticas que se pueden propagar por el espacio libre (aún en el vacío)

Frecuencia f de una onda electromagnética =
cantidad de oscilaciones por segundo (se mide en Hz)

Longitud de onda λ =
distancia entre dos puntos máximos o mínimos consecutivos

Principio:

En el vacío, todas las ondas electromagnéticas viajan a
la velocidad de la luz c y es de 30cm por nanosegundo.

En el cobre o la fibra óptica, la velocidad es aproximadamente
 $2/3 c$ y se vuelve ligeramente dependiente de la frecuencia.

Ley: La relación entre λ , f y c en el vacío es de
 $\lambda * f = c$

La red telefonía pública conmutada

Para enviar datos digitales de una PC sobre una línea analógica
es necesario convertir los datos a formato analógico.

Módem telefónico:
hace conversación

Los datos se convierten a formato digital en
la oficina central de la compañía telefónica para transmitirlos sobre las troncales

Codec:
es el dispositivo que hace esa conversación

En el extremo receptor
el stream de bits es usado para reconstruir los datos analógicos

DSL (Digital Subscriber Line):
DMT (multitono discreto) divide el
espectro de 1,1 MHz en el circuito local en 256 canales de 4312 Hz cada uno

Multiplexado
OFDM es usado

El canal 0 se usa para
el servicio telefónico convencional

Los canales 1 a 5
no se emplean, para evitar que las señales de voz y de datos interfieran entre sí

De los 250 canales restantes,
1 se usa para
control del flujo ascendente y 1 para el control del flujo descendente

El resto está disponible para
datos del usuario

ADSL

El proveedor determina
cuántos canales se utilizarán para el flujo ascendente y cuántos para el flujo descendente

La mayoría de los proveedores asigna
entre 80 y 90% del ancho de banda al canal descendente

Dentro de cada canal,
modulación QAM es usada a una tasa de alrededor de 4000 symbols/sec

la velocidad del flujo descendente es de
13,44 Mbps

En la práctica la relación señal a ruido nunca es suficientemente buena para alcanzar esa tasa

El módem ADSL funciona como
250 módems QAM operando en paralelo a diferentes frecuencias (implementa OFDM)

Internet Por Cable

Hay segmentos de
cable coaxial, a cada uno de ellos se conectan varias casas

Sistema

HFC(red híbrida de fibra óptica y cable coaxial)

Los convertidores electro-ópticos se llaman

nodos de fibra

un nodo de fibra puede

alimentar múltiples cables coaxiales

¿Cómo son los módems de internet por cable?

Para el flujo descendente cada canal descendente de 6 MHz se lo modula con:

QAM-64 (casi 36 Mbps de la cual se aprovecha 27 Mbps de carga útil), o

Si la calidad de cables es muy buena, QAM-256 (carga útil de 39 Mbps)

¿Cómo se hace multiplexado en un cable coaxial?

El uso de canales para flujo descendente de 6 Mhz o de 8 MHz es la parte FDM

TDM se usa para

compartir ancho de banda en el flujo ascendente entre varios suscriptores

El tiempo se divide en miniranas y diferentes suscriptores envían en las diferentes miniranas

Redes celulares:

Generaciones:

1G, 2G, 3G, 4G y 5G.

Modelo de hexagono:

Siendo las letras en el interior una frecuencia de señal, todas las celdas adyacentes tienen distintas frecuencias .

una terminal(smartphone/dispositivo) se conecta a una única celda a la vez, pero puede ir variando en el tiempo

las celdas se conectan a un

MSC(centro de conmutacion movil) multi-nivel que no se ve en detalle

Categorías en la que se dividen los canales de la red:

canales de control

(base a movil)

administracion

canales de localizacion

(base a movil)

aviso llamada

canales de acceso

(bidireccional)

llamadas

canales de datos

(bidireccional)

fax, datos

1G

Tanto 1G como 2G están diseñados para el envío de paquetes de voz, no para el envío de datos de red(o sea internet)

Características:

Analogica

Frequency division multiplex (FDM)

Simple electrónicamente

Full duplex(comunicación que puede dar y recibir en el mismo momento)

2G

Incluye el

GSM: Global system for mobile comm(Ete

número de tarjeta SIM. Se utiliza hasta hoy en día.

Datos :

voz → 900 1800 1900 MHZ más espectros, más usuarios.

FDM

Principio de división de canales por frecuencia

2 canales grandes de 124 canales c/u

TDM

dentro de cada canal tenemos una división por tiempo(tramas/T)

Canal de control de difusión

todos los nodos escuchan

Canal de control dedicado

a una celula en específico

Canal de control común

localización

acceso aleatorio concesión

3G**El principal objetivo ahora es**

el envío de Datos. la voz pasa a un segundo plano

CDMA: Acceso por división de código

En TDM o FDM no es posible asignar ranuras → en CDMA un usuario puede reducir su interferencia

4G

Core y voz completamente sobre IP

Capa de APP y TRANSPORTE

siguen igual

Red IP

Cambia

ip usa radio base, con IP y UDP (una mezcla)

túnel IP/UDP → arquitectura recursiva

Gestión de movilidad:

HOME NETWORK:

Red propia

Home agent: Gestiona la movilidad

FOREIGN NETWORK:

Red ajena o visitada

Foreign agent : Gestiona la movilidad

CORRESPONSAL:

El que se quiere comunicar con el móvil

CORE OF ADDRESS(CoA):

Parte de la red Foreign, asignada al dispositivo que la está visitando

El home agent controla

en qué red visitada esta el smartphone

Enrutamiento indirecto:

paso 1: Servidor envía los datos a la dirección permanente(Home Network)

paso 2: El Home Agent encapsula los datos dentro de un paquete más grande, y lo envía a CoA

paso 3: El Foreign agent desencapsula y le entrega los datos a el dispositivo

paso 4: El nodo móvil ahora envía directamente sus datos al Servidor

Enrutamiento directo:

Se necesita un

foreign agent, este se comunica con home agent y le aviso donde está(el dispositivo) luego, como enrutamiento indirecto