Diseño, Administración y Seguridad de Redes
Grado en Ingeniería Informática
Universidad de Valladolid

Jesús M. Vegas Hernández

Curso 2018-2019

Resumen

Material docente de la asignatura *Diseño, Administración y Seguridad de Redes* que se imparte en el Grado en Ingeniería Informática de la Universidad de Valladolid. El contenido se basa en los libros de texto de Priscilla Oppenheimer *Top-Down Network Design* (Cisco Press, 3/e, 2011), de James D. McCabe, *Network Analysis, Architecture, and Design* (3/e. Morgan Kaufmann, 2007) y de Kevin Dooley *Designing large-scale LANs* (O'Reilly, 2002)..La mayoría de las figuras están tomadas de estas fuentes o son de creación propia. Cuando no sea así se indicará explícitamente la fuente o se tratará de imágenes de dominio público sin restricciones conocidas.

Índice

Parte I
Identificar Necesidades y Objetivos del Cliente

1. Análisis de Objetivos y Restricciones del Negocio

Requisitos del Negocio

- Diseño de una red como un proceso que pone en correspondencia las necesidades del negocio con la tecnología disponible para maximizar las posibilidades de éxito de una organización

1.1. Metodología Descendente de Diseño de Red

Metodología Descendente de Diseño de Red

- No *unir puntos*
- Diseño descendente comienza por las capas superiores del modelo OSI para después descender
- Metodología diseño descendente es iterativa
- Modularidad → Modelo Jerárquico:
  - Core
  - Distribución
  - Acceso

Pila Protocolos OSI

N	*Nombre*	*Cometido*	*Ejemplos*
7	**Aplicación**	Usuario y aplicaciones	Web, email, dns
6	**Presentación**	Formato de datos, encriptación, codificación	ASCII vs EBCDIC encriptación flujo de datos
5	**Sesión**	Negocia y mantiene conexiones	Correlación nombres-direcciones
4	**Transporte**	Secuencia de paquetes entre extremos, fiabilidad	UDP, TCP, SPX
3	**Red**	Encaminamiento, control flujo	IP, IPX
2	**Enlace de datos (MAC)**	Fragmentación básica, detección errores, control de transmisión	Ethernet y control de colisiones
1	**Física**	Señales eléctricas y ópticas	Cableado y pulsos eléctricos

1.1.1. Proceso de Diseño Estructurado

Diseño Estructurado

- Flujo de datos, su tipo y los procesos que acceden a datos
- Localización y necesidades de las comunidades de usuarios
- Técnicas y Modelos para caracterizar el sistema existente y los nuevos requisitos
- Modelo lógico previo al modelo físico
    - Modelo lógico: bloques básicos, dependiendo de su función y la estructura del sistema
    - Modelo físico: dispositivos y tecnologías y sus implementaciones

1.1.2. Ciclo de Vida del Diseño

Ciclo de Vida del Diseño de Sistemas

- Análisis de Requisitos
- Desarrollo del Diseño Lógico
- Desarrollo del Diseño Físico
- Pruebas, Optimización y Documentación

Análisis de Requisitos

- Analizar objetivos del negocio y restricciones
- Analizar objetivos técnicos y compromisos
- Caracterizar la red existente
- Caracterizar el tráfico existente y futuro

Diseño Lógico

- Diseñar topología de red
- Diseñar modelos para nombrar y asignar direcciones
- Seleccionar protocolos de conmutación y encaminamiento
- Desarrollar estrategias de seguridad
- Desarrollar estrategias de administración

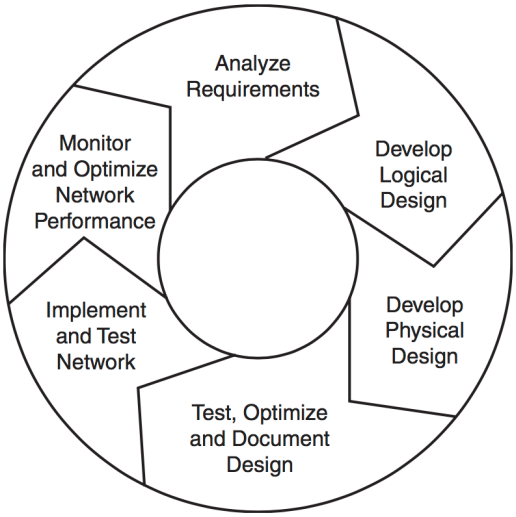
Diseño Físico

- Seleccionar las tecnologías y dispositivos
- Completar el estudio de proveedores de servicios

Pruebas, Optimización y Documentación

- Escribir e implementar un plan de pruebas
- Construir un piloto de la red
- Optimizar el diseño de la red
- Documentar el diseño

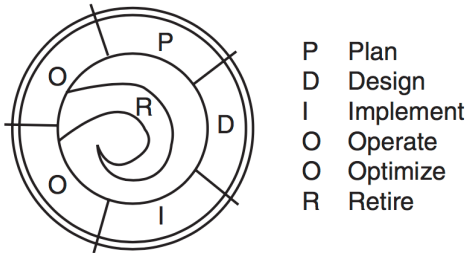
Ciclo de Vida del Diseño de Sistemas



Ciclo de Vida de una Red: PDIOOr

- ***P**lanificar* identificando los requisitos, áreas, usuarios y servicios de red
- ***D**iseñar* tanto lógica como físicamente la red
- ***I**mplementar* de acuerdo a las especificaciones del diseño
- ***O**perar* monitorizando la red detectando problemas y fallos
- ***O**ptimizar* identificando problemas antes de que provoquen paradas
- ***R**etirar* partes de la red o elementos obsoletos y fuera de uso

Ciclo de Vida de una Red: PDIOOr



1.2. Análisis de los Objetivos del Negocio

Objetivos del Negocio

- Incrementar beneficios
- Reducir costes operativos
- Mejorar las comunicaciones
- Reducir el ciclo de desarrollo de producto
- Expandirse en mercados globales
- Establecer alianzas con otras compañías
- Ofrecer mejor soporte a los clientes o nuevos servicios

1.2.1. Trabajar con el Cliente

Reuniones con el Cliente

- Recabar información previa
  - Servicios y productos
  - Viabilidad financiera
  - Clientes, proveedores, competidores
  - Ventaja competitiva
- Tratar de definir concisamente los objetivos del proyecto
  - Cuál es el problema que intentan resolver?
  - Cómo ayudará la tecnología?
  - Qué define el éxito del proyecto?

Reuniones con el Cliente

- Qué ocurre si fracasa el proyecto?
  - Es crítico para el negocio?
  - Es visible para los gestores o ejecutivos?
  - Quién está de tu lado?
- Descubrir cualquier condicionante
  - Sólo se utiliza software de una compañía?
  - Evitan ciertas tecnologías?
  - $\rightarrow$ Contactar con el personal técnico y de mantenimiento.

Reuniones con el Cliente

- Obtener una copia del organigrama
- Acceder a las políticas de seguridad
  - Catalogar los elementos de la red que deberían protegerse

1.2.2. Analizar Objetivos del Negocio

Prioridades Actuales para el Negocio

- Redes deben ofrecer un servicio al negocio
  - *IT Service Management*, ITSM
  - *Information Technology Infraestructure Library*, ITIL
- Gobernanza y Cumplimiento
  - *Gobernanza*, proteger organización de la mala administración o actividades ilegales de usuarios de servicios IT
  - *Cumplimiento*, adhesión a normas y regulaciones sobre fraude y mal uso de datos de clientes privados
- Soportar movilidad usuarios
- Seguridad
  - *Resiliencia*, continuidad del negocio tras un desastre

1.2.3. Alcance del Proyecto

Alcance del Proyecto

- Diseñar un nuevo segmento de red, o una red completa para la empresa
- Preocupaciones técnicas y del negocio relacionadas con el alcance
- Utilizar el modelo OSI para especificar la nueva funcionalidad

Alcance del Proyecto

- *Segmento*: red simple limitada por un switch o un router y basada en un protocolo concreto de nivel 1 y 2 (p.e. Ethernet)
- *LAN*: un conjunto de segmentos conmutados basados en un protocolo particular de nivel 2 (p.e. Fast Ethernet), y un protocolo de trucking entre switches (p.e. 802.1Q)
- *Red de edificio*: Múltiples LANs en un edificio, normalmente conectadas a una red troncal del edificio
- *Red de campus*: Múltiples redes de edificios limitados a un área geográfica de unos pocos kilómetros, normalmente conectadas a una red troncal de campus

Alcance del Proyecto

- *Acceso Remoto*: Soluciones de red que permiten que usuarios individuales o pequeñas sucursales accedan a la red
- *WAN*: Red geográficamente dispersa que incluye conexiones punto a punto, Frame Relay, ATM u otras conexiones de larga distancia
- *Red Inalámbrica*: LAN o WAN que utiliza el aire como medio de transmisión, en lugar de un cable
- *Red Empresarial*: Red grande y dispersa, formada por varios campus, servicios de acceso remoto, y una o más WANs o LANs de gran tamaño También es llamada *internerwork*

1.2.4. Identificar las Aplicaciones en Red del Cliente

Identificar las Aplicaciones en Red del Cliente

- Aplicaciones
  - Usuario
  - Sistema
- Criticidad

- 1. Extremamente crítica
- 2. Moderadamente crítica
- 3. No crítica

Aplicaciones en Red

Nombre Aplicación	Tipo	Nueva (S/N)	Crítica	Comentarios

1.3. Análisis de las Restricciones del Negocio

Restricciones del Negocio

- Políticas y Normas
- Presupuesto y Plantilla
- Planificación

Políticas y Normas
Restricciones del Negocio

- Detectar si existen razones por las que podría fracasar el proyecto
  - Hubo intentos anteriores de poner en marcha este proyecto?
- Problemas de personal, a favor y en contra
  - El proyecto puede provocar eliminación de puestos de trabajo?
- Tolerancia al riesgo y prejuicios sobre ciertas tecnologías (prohibidas?)
- Abierto vs cerrado, acuerdos con proveedores

Presupuesto y Plantilla
Restricciones del Negocio

- El proyecto de red debe ajustarse al presupuesto disponible
  - La mejor solución o la más asequible
- Equipamiento, software, mantenimiento y soporte, formación y personal
- Control del presupuesto
- Estudiar y presentar el ROI al cliente

Planificación
Restricciones del Negocio

- Cuál es la fecha de finalización?
- Incluir hitos intermedios facilita detectar desviaciones
- Documentar las distintas etapas
- Plazos vs calidad/alcance del proyecto

1.4. Resumen

Resumen

- Proceso descendente de diseño de la red, partiendo de los objetivos de la organización
- Importancia de sistematizar el diseño de la red
- Analizar el estado del negocio, tolerancia al riesgo y experiencia técnica
- Entender el presupuesto y plazos para el proyecto
- Entender la estructura organizativa de la organización
    - Toma de decisiones
    - Flujo de datos y topología

2. Análisis de Objetivos Técnicos y Compromisos

Análisis de Objetivos Técnicos

- Técnicas para analizar objetivos técnicos de un diseño de red (nueva o modificación)
- Compromisos entre objetivos contrapuestos

Objetivos Técnicos

- Técnicas y terminología para analizar objetivos técnicos de un diseño de red (nueva o modificación)
    - Escalabilidad
    - Disponibilidad
    - Prestaciones
    - Seguridad
    - Gestionabilidad

    - Usabilidad
    - Adaptabilidad
    - Asequibilidad
- Compromisos

2.1. Escalabilidad

Escalabilidad

- *Escalabilidad* se refiere a la capacidad de crecimiento
- Planes de expansión a corto y medio plazo
- Expansión en el acceso a los datos
    - 1970's mainframes $\rightarrow$ 1990's servidores en red departamental $\rightarrow$ 2010's centro de datos en la nube
    - Intranets, extranets
    - $\rightarrow$ rotura de la regla 80/20
- Atención!! algunas tecnologías no soportan bien el crecimiento

Escalabilidad

- Actualizar redes empresariales para hacerlas más escalables
    - Conectar LANs departamentales separadas
    - Resolver cuellos de botella en red corporativa
    - Agrupar servidores centralizados en centros de datos
    - Hacer los datos en mainframes accesibles a la red IP
    - Añadir redes para oficinas dispersas o teletrabajo
    - Añadir redes y servicios para comunicaciones seguras con clientes, proveedores y otros socios

2.2. Disponibilidad

Disponibilidad

- *Disponibilidad*, porcentaje de tiempo en el que la red está operativa
    - Capacidad insuficiente?
- Redundancia como medio para conseguir alta disponibilidad
- Resiliencia, cuánto estrés puede soportar y cuánto tiempo para volver a estar operativa tras un desastre
- Plan de recuperación ante desastres

Tiempo de caída en minutos según la disponibilidad

Disponibilidad	por Hora	por Día	por Semana	por Año
99,999 %	0,0006	0,01	0,10	5
99,98 %	0,012	0,29	2	105
99,95 %	0,03	0,72	5	263
99,90 %	0,06	1,44	10	526
99,70 %	0,18	4,32	30	1577

Especificación de Requisitos de Disponibilidad

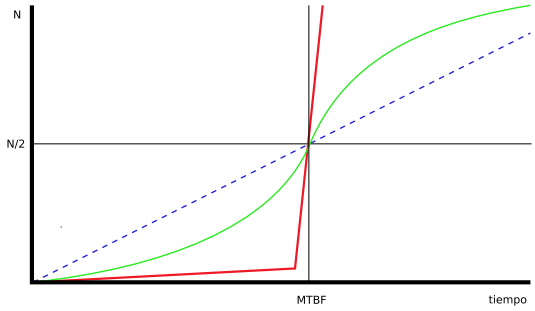
- Periodo, momento, concentrado o distribuído
- *Cinco nueves*, mantenimiento?
  - *En caliente*
  - Triple redundancia

Disponibilidad

- Disponibilidad = MTBF / (MTBF + MTTR)
- MTBF, Tiempo medio entre fallos
- MTTR, Tiempo medio de reparación
  - Si la red no debería caerse más de una vez cada 4000h (166 días) y tardar 1h en levantarse de nuevo,
  - 4000 / 4001 = 99,98 % disponibilidad
- Coste de caída (dinero / hora de caída)

Tiempo Medio entre Fallos
Disponibilidad

- MTBF, significa que la mitad de los dispositivos de este tipo no funcionarán una vez transcurrido ese tiempo
- Indica la probabilidad de fallo por unidad de tiempo
- Los fallos se irán sucediendo con ese valor medio, pero sin indicar nada sobre la curva



2.3. Prestaciones

Prestaciones

- *"La red debe funcionar sin quejas por parte de los usuarios"*
- *Capacidad* (ancho de banda): la capacidad de transporte de datos de un circuito o red (bps)
- *Utilización*: Porcentaje de la capacidad utilizada
- *Utilización óptima*: Utilización media máxima antes de considerar la red saturada
- *Productividad* (*throughput*): Cantidad de datos transferidos sin error entre nodos por unidad de tiempo, bps.
- *Carga ofrecida*: Suma de los datos que todos los nodos tienen listos para enviar en un instante particular

Prestaciones
Cont.

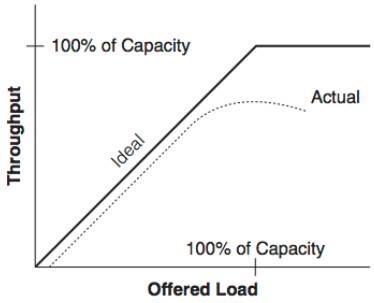
- *Precisión*: Cantidad de tráfico útil que se transmite correctamente, relativo al tráfico total
- *Eficiencia*: Análisis de cuánto esfuerzo se requiere para producir una cierta productividad
- *Retardo* (latencia): Tiempo entre que un marco está listo para enviar por un nodo y su entrega en cualquier otro sitio de la red
- *Variación del retardo* (*jitter*): Cantidad de tiempo que varía el retardo medio
- *Tiempo de respuesta*: Cantidad de tiempo entre una solicitud de un servicio de red y la respuesta a la solicitud

Utilización Óptima
Prestaciones

- Utilización calculada en un periodo de tiempo, no instantánea
- Utilización media máxima en un segmento: es una restricción
- Si se supera en un segmento
  - Dividir segmento en varios
  - Más ancho de banda
- La utilización media óptima es del 70 %
  - Permite soportar picos en el tráfico sin degradación prestaciones
- Especialmente crítica en WANs, no tanto en LANs
  - Características avanzadas en protocolos encaminamiento
  - Comprensión

Throughput y Ancho de Banda
Prestaciones

- Ancho de banda, es dado y constante
- Throughput, es medido y depende las prestaciones de la red



Throughput
Prestaciones

- Throughput vs. *Goodput*
  - Tamaño paquetes y sobrecarga cabeceras
  - Espacios relleno en paquetes
- Otros factores

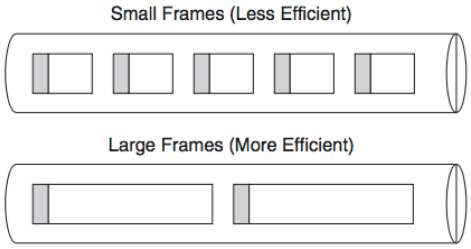
- Tasas de reenvío de paquetes
- Velocidad clientes y servidores
- Diseño de red
- Protocolos
- Distancia
- Errores

Precisión
Prestaciones

- Los datos recibidos en el destino deberían ser los mismos enviados por el origen
  - Picos de tensión, problemas de impedancia, ruido, ...
- Marcos con error han de ser retransmitidos (TCP), afectando throughput
- *Bit Error Rate*, BER
  - WAN,
    - analógicas, 1 en 10^5
    - cobre, 1 en 10^6
    - fibra óptica, 1 en 10^{11}
  - LAN, aproximados por marcos con error por bytes totales
    - 1 marco mal por 10^6 bytes de datos
- Colisiones
  - Dominio colisión Ethernet compartido
    - menos de 0.1 % de los marcos deberían ser colisiones (legales)
  - No colisiones en Ethernet Full Duplex, Serial, WAN
- Considerar también paquetes en desorden

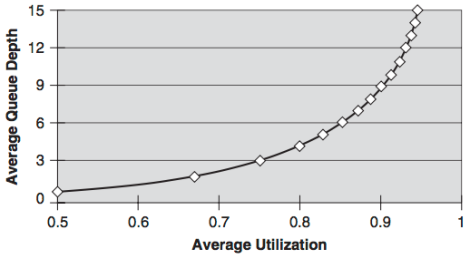
Eficiencia
Prestaciones

- Afectada por colisiones, paso de token, errores, encaminamiento, ACKs, cabeceras grandes, etc.
- Tamaño paquete óptimo? vs. BER
- Paquetes grandes en enlaces lentos (WAN), *retardo de serialización*



Retardo y su Variación
Prestaciones

- Afecta especialmente a usuarios de aplicaciones interactivas (video, audio)
- Causas
  - Retardo propagación, 270 ms en satélite, 1 ms / 200 km en cable
  - Retardo serialización
  - Conmutación paquetes, 5 - 20 μs en switches, más en routers
    - Colas de paquetes



Retardo y su Variación
Prestaciones

Paquetes en cola = Utilización / (1 - Utilización)

- Si 5 usuarios, transmitiendo 10 pps de 1024 bits sobre un enlace WAN de 56 kbps
  - Carga = $5 \times 10 \times 1024$ = 51200 bps
  - Utilización = $51200/56000$ = 91,4 %
  - Núm. medio paquetes en la cola = $0,914/(1-0,914)$ = 10,63 paquetes
- Aumentar ancho de banda
- Colas con prioridad

Retardo y su Variación
Prestaciones

- Tráfico en ráfaga produce variación en el retardo, afectando otras apps
- Minimizar jitter con buffer
  - Si jitter es menor que tamaño buffer
- Aceptable si variación es menor del 1 % - 2 % del retardo

Tiempo Respuesta
Prestaciones

- Usuarios perciben el tiempo de espera de una respuesta de la red (app) y su variación
- Límite 100 ms en apps interactivas
- Valor típico para temporizadores de retransmisión paquetes no reconocidos (TCP)

2.4. Seguridad

Seguridad

- Objetivo técnico clave, problemas de *seguridad* no impidan la actividad de la organización
- Planificación: identificación bienes a proteger, análisis de riesgos
- Compromisos:
  - Aumentar coste implantación y operación
  - Disminución productividad
  - Disgustar usuarios
  - Afectar redundancia
- Objetivo práctico: el coste de implementar seguridad no exceda del de recuperarse de incidentes de seguridad

Identificar Bienes
Seguridad

- Qué proteger? Cuál es su valor? Cuál el coste de perderlos?
  - Hardware
  - Software
  - Aplicaciones

    - Datos
    - Propiedad intelectual
    - Secretos industriales
    - Reputación

Riesgos
Seguridad

- Proceso continuo: análisis de riesgos, establecer políticas de seguridad, diseño de seguridad en la red
- Hackeo dispositivos de red
    - Interceptación datos
    - Cambio contraseñas administración
    - Cambios en configuración para alterar rutas
- Ataques de Reconocimiento
- Denegación de Servicio, DoS
- Considerar atacantes externos e internos

Requisitos
Seguridad

1. No se interumpa la capacidad de mantener el negocio
2. Proteger activos
    - *Confidencialidad*
    - *Integridad*
    - *Disponibilidad*

2.5. Gestionabilidad

Gestionabilidad

- *Gestionabilidad* es la capacidad de la red de ser administrada para conseguir los objetivos de disponibilidad, prestaciones y seguridad
- Distintos objetivos en cada organización
- Modelo *FCAPS* (ISO):
    - Gestión de *F*allos
    - Gestión de *C*onfiguración
    - Gestión de Cont*A*ble
    - Gestión de *P*restaciones
    - Gestión de *S*eguridad

2.6. Usabilidad

Usabilidad

- *Usabilidad* se refiere a la facilidad del uso de la red y sus servicios por parte de los usuarios.
- Algunos diseño de red tienen efectos negativos en la usabilidad (p.e. seguridad)
- Debe tenerse en cuenta la movilidad de los usuarios
  - VPN
  - WiFi

2.7. Adaptabilidad

Adaptabilidad

- La *adaptabilidad* permite incorporar a la red nuevas tecnologías y realizar cambios en el futuro
  - Nuevos protocolos
  - Nuevos patrones de tráfico
  - Nuevos modos de conexión
  - Nuevos segmentos de red
- Adaptación a problemas y actualizaciones

2.8. Asequibilidad

Asequibilidad

- Para que una red sea *asequible* debe transportar la máxima cantidad de tráfico a un coste financiero dado
  - Campus: suele primar el bajo coste a disponibilidad y prestaciones
  - Corporativa: la disponibilidad suele ser más importante que el coste bajo
- Costes principales
  1. Enlaces WAN
  2. Personal
- Técnicas de reducción de tráfico WAN y facilidad de gestión de la red

Requisitos Técnicos de las Aplicaciones en Red

Aplicación	Nueva? (S/N)	Crítica	Coste si Caída	MTBF Aceptable	MTTR Aceptable

2.9. Compromisos entre Objetivos

Compromisos entre Objetivos

- Cuánto está dispuesto a invertir el cliente en cada objetivo?

Objetivo	Inversión
Escalabilidad	20
Disponibilidad	30
Prestaciones	15
Seguridad	5
Gestionabilidad	5
Usabilidad	5
Adaptabilidad	5
Asequibilidad	15
Total (máx. 100)	100

2.10. Resumen

Resumen

- Llegados a este punto tendremos los objetivos de negocio y técnicos del negocio para construir una red
- Ordenar objetivos: importantes, críticos, menos críticos
- Listar opciones y correlacionar con los objetivos
- Eliminar cualquier opción que no responda a un objetivo
- Seleccionar componentes que cumplan con los requisitos del cliente

3. Caracterización de la Red Existente

Caracterización de la Red Existente

- Caracterizar la red existente
    - estructura lógica

    - estructura física
- Nomenclatura
- Cableado y medios
- Restricciones arquitectónicas y ambientales (WiFi)
- Diagnosticar red saludable, umbrales

3.1. Caracterizar la Infraestructura de la Red

Caracterizar la Infraestructura de Red

- Descubrir la localización de los principales elementos y desarrollar un conjunto de mapas de dispositivos y segmentos
- Métodos de denominación y numeración
- Tipos y longitudes del cableado
- Restricciones arquitectónicas y ambientales

3.1.1. Hacer un Mapa de la Red

Hacer un Mapa de la Red

- Localizar los hosts, dispositivos y segmentos principales para entender cómo fluye el tráfico y dónde están los usuarios
- Partir de los mapas y diagramas existentes
- Pueden ser de utilidad herramientas descubrimiento de red
    - Tivoli, WhatsUp, Network Topology Mapper (aka LANsurveyor), MS Visio, inSSIDer, Netcrunch, etc.
    - Spiceworks Network Monitor

Redes Grandes
Hacer un Mapa de la Red

- Varios mapas, uno por localización
- Método descendente
    - Información de alto nivel
        - Información geográfica
        - Conexiones WAN entre países, ciudades
        - Conexiones WAN, LAN entre edificios, campus

- Detalles de cada campus
  - Edificios, plantas, y si se puede espacios
  - Localización de servidores o granjas de servidores
  - Localización de routers y switches
  - Localización NAT, Firewalls, IDS
  - Localización de estaciones de gestión de la red
  - Localización y alcance de VLANs
  - Localización y número de estaciones de trabajo

Redes Grandes
Hacer un Mapa de la Red

- Basado en modelo OSI
  - Aplicaciones y servicios: web, email, FTP, impresión, archivos, internos y externos
  - Servicios de red: RADIUS, DNS, DHCP, SNMP, VPN
  - Capa 3: routers, enlaces lógicos entre ellos, protocolos encaminamiento (OSPF), HSRP, filtrado, NAT, IDS
  - Enlaces y dispositivos LAN e interfaces conectadas a WANs (topología física): tecnología LAN/WAN, proveedores servicio, STP, VLANs y VTP

Diagrama de Estructura de la Red

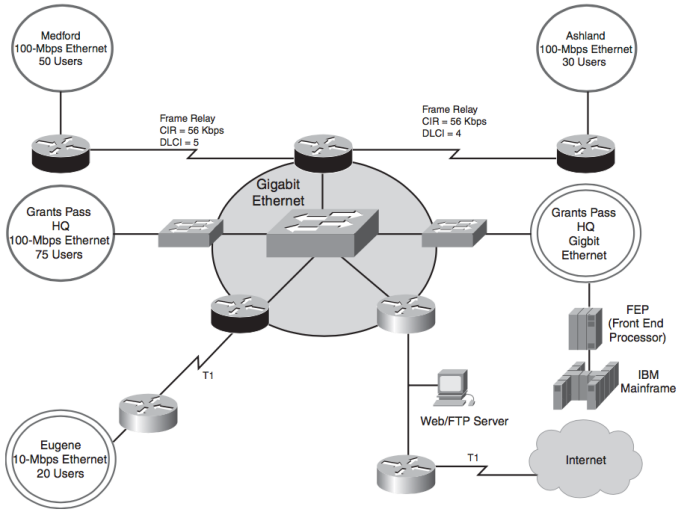
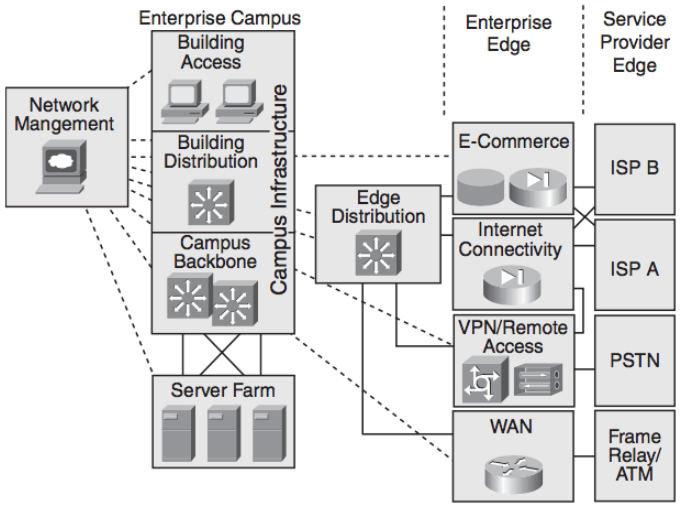


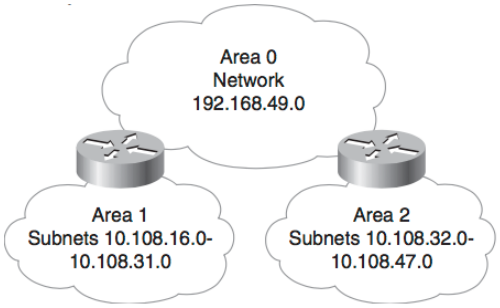
Diagrama de Bloques de la Red



3.1.2. Caracterización de Direcciones y Nombres

Caracterización de Direcciones y Nombres

- Identificar los nombres de las principales localizaciones, segmentos de red, servidores
- Existe estrategia de nomenclatura?
- Uso de direcciones de red
  - Agregación de rutas (*supernetting*), rutas resumibles
  - *Subredes discontinuas* cuando una subred ha sido dividida en dos áreas separadas por otra



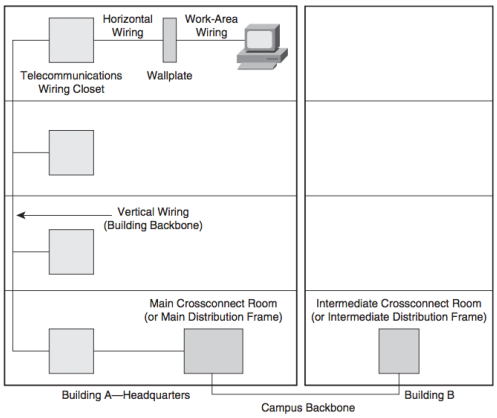
3.1.3. Caracterización del Cableado y Medio

Caracterización del Cableado y Medios

- Tipos de cable y distancias
- Etiquetado?
- Probables tipos de cable entre edificios
    - Fibra monomodo
    - Fibra multimodo
    - Cobre en par trenzado apantallado (STP)
    - Cobre en par trenzado no apantallado (UTP)
    - Cable coaxial
    - Microondas
    - Laser
    - Radio
    - Infrarrojos

Caracterización del Cableado y Medios

- En edificios
    - Armarios de comunicaciones, laboratorios, salas ordenadores
    - Cableado *vertical*, *horizontal* y latiguillos



3.1.4. Restricciones Arquitectónicas y Ambientales

Consideraciones Arquitectónicas

- Determinar circunstancias físicas que pudieran dañar el cable
- Restricciones legales para tender cables
- Obstáculo en la línea de visión de tecnologías inalámbricas
- Dentro de edificios, elementos necesarios:
  - Climatización
  - Alimentación eléctrica
  - Protección interferencias electromagnéticas
  - Espacio suficiente para conductos de cables, paneles conexión, racks, áreas de trabajo

Instalación Inalámbricas
Consideraciones Arquitectónicas

- Analizar si el lugar es apropiado para la transmisión inalámbrica
- Determinar el mejor emplazamiento de los puntos de acceso, APs, (WLAN)
- Problemas
  - Reflexión
  - Absorción
  - Refracción
  - Difracción
- *Margen de atenuación*, aumento de potencia de señal respecto a la necesaria si no hubiera obstáculos

3.2. Comprobar la Salud de la Red Existente

Comprobar la Salud de la Red existente

- Linea de partida para las nuevas prestaciones esperadas
- Analizador de tráfico y protocolos
- Periodos de carga normal, pico o ambos
  - Utilización, % carga en un periodo
  - Precisión, BER y colisiones
  - Eficiencia, MTU
  - Retardo y tiempo de respuesta, RTT

3.2.1. Utilización

Utilización

- *Utilización* de la red es la cantidad de ancho de banda en uso durante un periodo de tiempo
- Granularidad suficiente, intervalo
  - Resolución problemas, 1 minuto o segundos
  - Análisis de prestaciones, 1 a 5 minutos
  - Análisis de carga a largo plazo, 10 minutos
- Analizar 1 o 2 días al menos
- Por protocolo: *unicast* vs *broadcast*
  - *Utilización relativa*, respecto a la utilización del segmento
  - *Utilización absoluta*, respecto a la capacidad del segmento

3.2.2. Precisión

Precisión

- Líneas serie, BER
- Redes conmutación paquetes, marcos con error CRC y perdidos
  - Marcos con error, CRC, cada hora durante 1 o 2 días
  - No más de 1 marco con error por MB de datos
  - Analizar pérdidas: necesidad incrementar ancho banda, decrementar errores CRC o actualizar dispositivos de red (pérdidas en las colas)

Ethernet Conmutada
Precisión

- Switches semi-duplex
  - CSMA/CD
  - Que se produzca colisión, dependerá de lo que esté conectado al puerto
  - Si medio compartido, pueden darse colisiones
- Colisiones $< 0,1\,\%$ de marcos
- Colisiones tardías, después de que un puerto o interfaz ha enviado sus primeros 64 bits
- Cableado mal
  - > 100 m
  - Tarjeta defectuosa
  - Fallo detección duplex

Ethernet Conmutada
Precisión

- Si a un puerto se conecta un único dispositivo (switch, PC) entonces full-duplex
  - No CSMA/CD
  - Enlace punto a punto sin colisiones
- Velocidad, normalmente la autonegociación no es problema
  - Posible ajustar manualmente
  - Cat 3, 10 Mbps, errores si se excede

Ethernet Conmutada
Precisión

- Autonegociación no exenta de problemas
  - Incompatibilidad hardware
  - Software no conforme a IEEE 802.3u
- Detectar problemas negociación duplex
  - Analizar los errores y su tipo, asimetría
  - Lado full-duplex, errores CRC
  - Lado semi-duplex, colisiones
- Confiar en la autonegociación duplex (error humano)

3.2.3. Eficiencia

Eficiencia

- Maximizar núm. de bytes de datos respecto bytes de cabeceras y de ACKs
  - Incrementar ventana recepción, aceptar más marcos antes de responder con ACK
  - Incrementar MTU, necesario en routers con túneles pero malo para retardo de serialización en app interactivas con bajo ancho de banda (serialización)
- Analizar con analizador de protocolos
  - ≤ 64 bytes
  - entre 64 y 1500 bytes
  - ≥ 1500 bytes
- Calcular valor medio tamaño marco (MB/marcos), distribución bimodal
- Si excesivos marcos < 64 bytes, demasiadas colisiones

3.2.4. Retardo y Tiempo de Respuesta

Retardo y Tiempo de Respuesta

- Medir tiempo de respuesta antes y después de actuar sobre la red
  - Analizador protocolos
  - `ping` para calcular RTT (varianza)
  - Aplicación típica de usuario
  - Servicio de red
  - Arranque PCs

3.2.5. Comprobar Routers, Switches y Cortafuegos

Comprobar Routers, Switches y Cortafuegos

- No todos, sólo los principales
- Carga CPU? Paquetes procesados? Paquetes desechados? Espacio buffers y colas?
  - `show buffers`
  - `show cdp neighbors detail`
  - `show environment`
  - `show interfaces`
  - `show ip cache flow`
  - `show memory`
  - `show processes`
  - `show running-config`
  - `show startup-config`
  - `show version`

3.3. Lista de Comprobación

Lista de Comprobación

- Topología e infraestructura física bien documentadas
- Direcciones asignadas de forma estructurada y documentadas
- Cableado estructurado bien instalado y etiquetado
- Cableado testado y certificado
- PCs y armarios a menos de 100 m
- Disponibilidad cumple objetivos cliente
- Seguridad cumple objetivos cliente
- Sin segmentos LAN/WAN saturados ($< 70\,\%$ utilización durante 10 min)

Lista de Comprobación
Cont.

- Sin colisiones en segmentos full-duplex
- Trafico *broadcast* $< 20\,\%$ (o incluso $10\,\%$) del total por segmento
- Tamaño marcos optimizados (lo más grandes posible dependiendo del enlace)
- Sin routers saturados (utilización CPU $< 75\,\%$ durante 5 min)
- De media, routers desechando $< 1\,\%$ marcos (más en caso de sobresubscripción)
- Configuraciones routers y switches recolectadas, almacenadas y analizadas
- Tiempo de respuesta clientes/servidores < 100 ms

3.4. Resumen

Resumen

- Analizadas técnicas y herramientas para caracterizar una red antes de diseñar mejoras
- Verificar si los objetivos técnicos del cliente son realistas
- Comprender la topología y localización actual de segmentos y equipos
- Obtener una medida de referencia para comparar con las nuevas prestaciones, una vez implementado el diseño

4. Caracterización del Tráfico

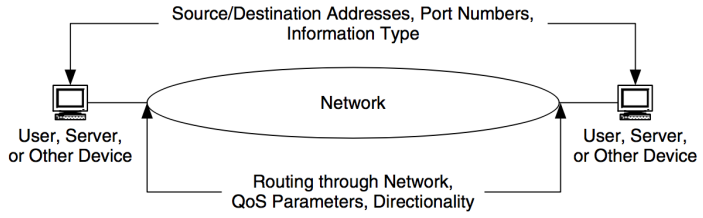
Caracterización del Tráfico

- Flujos de tráfico, fuentes y sumideros
- Volumen del tráfico
- Comportamiento de protocolos

4.1. Caracterización del Flujo

Caracterización del Fujo

- *Flujo* (flujo de tráfico, flujo de datos), es un conjunto de tráfico de red que tiene atributos comunes, como origen/destino, tipo de información, dirección, etc.
- Asociado a aplicación, dispositivo, red o usuario



Caracterización del Flujo

- Caracterizar el flujo de tráfico
  - Origen y destino
  - Dirección
  - Simetría
- Localización de generadores de tráfico (fuentes) y almacenes de datos (sumideros)
- Carga del tráfico
- Comportamiento del tráfico
- Calidad de Servicio, QoS

4.1.1. Identificando Fuentes y Almacenamiento

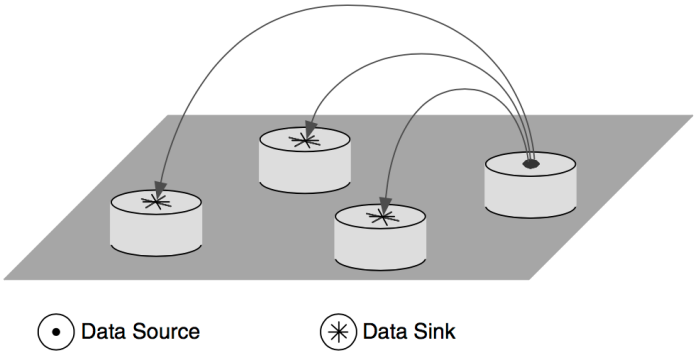
Fuentes y Sumideros

- *Comunidad de usuarios*, conjunto de usuarios que utilizan una aplicación o conjunto de aplicaciones
  - Intra/inter departamental
- *Almacén de datos*, Sumidero de datos, área de la red donde residen los datos de aplicación
  - Servidor,
  - Granja de servidores,
  - Unidad de backup

Fuentes y Sumideros

- Fuentes
  - Máquinas de cálculo generando gran cantidad información
  - Cámaras IP

- Sumideros
  - Almacenes de datos o archivos
  - Procesadores de imágen, pantallas



Fuentes y Sumideros

Almacén Datos	Localización	Aplicaciones	Usadas por Usuarios	Grupos

4.1.2. Documentar Flujos

Documentar Flujos

- Identificar y caracterizar flujos individuales entre fuentes y sumideros
- *Flujo de tráfico individual*, información transmitida entre entidades durante una sesión
  - Dirección, uni o bidireccional y su ruta
  - Simetria, si igual prestaciones o requisitos en ambos sentidos
  - Ruta
  - Núm. de paquetes
  - Núm. de bytes
  - Direcciones de los extremos
- Medir MBps durante 1 o 2 días, normalmente en el core

4.1.3. Caracterizar Tipos de Flujos

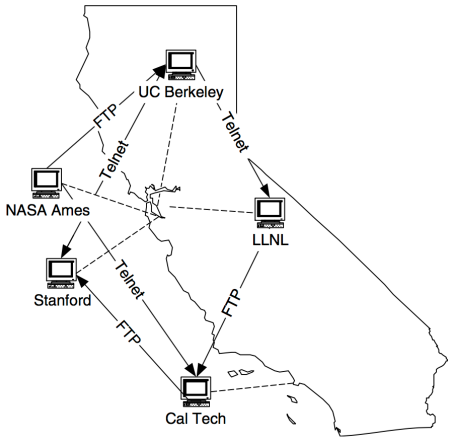
Caracterizar Tipos de Flujo

- Dirección y simetría
- Clasificar tráficos según patrones conocidos
  - Acceso a terminal
  - Ciente/servidor
  - Peer-to-peer, P2P
  - Servidor/servidor
  - Distribuido
  - VoIP

Acceso a terminal
Caracterizar Tipos de Flujo

- Asimétrico, cliente envía pocos caracteres, servidor responde con bastantes más
- `Telnet`
- Menos importante que antaño, pero aún presentes (en forma de cliente ligero)

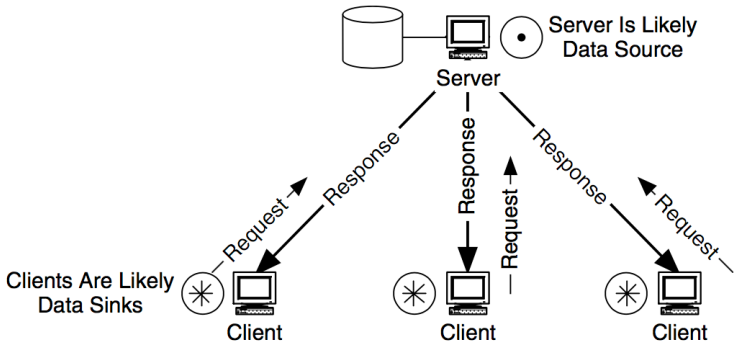
Acceso a terminal
Caracterizar Tipos de Flujo



Cliente/servidor
Caracterizar Tipos de Flujo

- Clientes confían en servidores para acceder a los recursos (almacenamiento, procesamiento)
- Cliente envía solicitudes que son atendidas por servidor
- Bidireccional y asimétrico
  - Cliente, normalmente marcos pequeños
  - Servidor, marcos grandes (hasta valor MTU)
- HTTP
  - No siempre tráfico entre cliente y servidor
  - Cachés multinivel
  - CDN

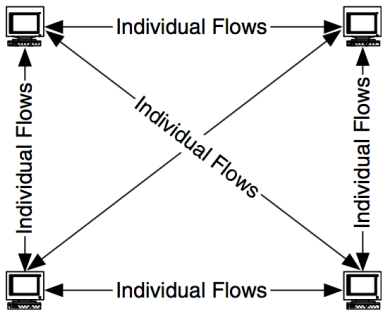
Cliente/servidor
Caracterizar Tipos de Flujo



Peer-to-Peer, P2P
Caracterizar Tipos de Flujo

- Bidireccional y simétrico
- No jerarquía
  - Compartir recursos (impresoras)
  - Distribución contenidos (multimedia, documentos)
  - Reuniones mediante videoconferencia
- Normalmente no permitido
  - Genera cantidad desmedida de tráfico
  - Infringe derechos usuario?

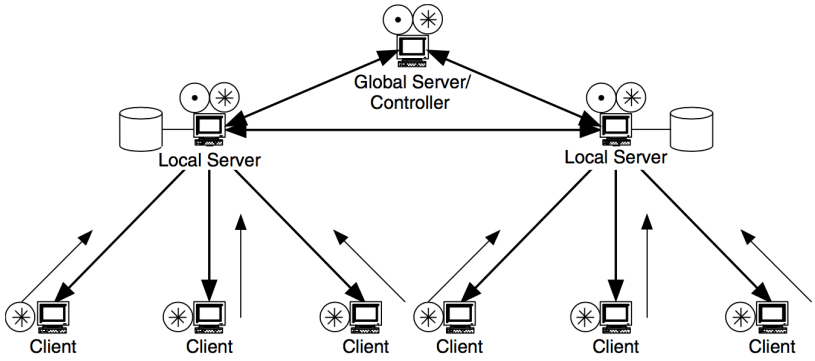
Peer-to-Peer, P2P
Caracterizar Tipos de Flujo



Servidor/servidor
Caracterizar Tipos de Flujo

- Transmisión entre servidores y también entre servidores y las aplicación de administración
  - Directorio, caché, espejado (*mirroring*)
- Bidireccional, simetría dependiendo de la aplicación
  - Servidor-servidor, normalmente simétrica
  - Si jerarquía servidores, puede ser asimétrica, algunos almacenan/gestionan más datos que otros

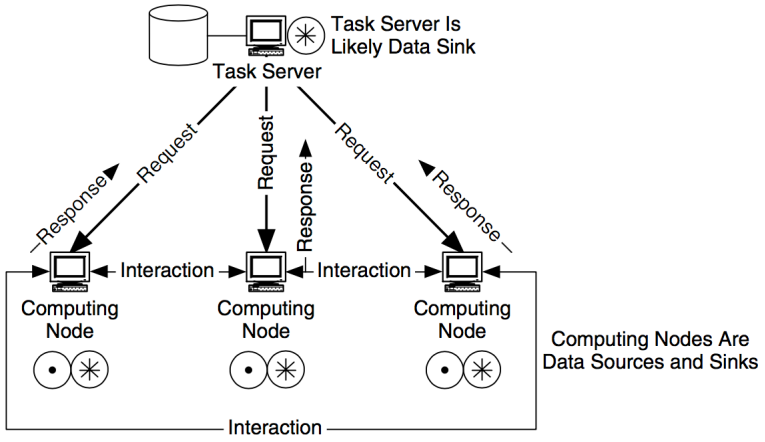
Servidor/servidor
Caracterizar Tipos de Flujo



Distribuido
Caracterizar Tipos de Flujo

- Aplicaciones que requieren de múltiples nodos para desarrollar su función
- Información fluye entre gestor de tareas y nodos procesamiento, y entre nodos
  - Fuertemente acoplados, transferencia frecuente de información
  - Débilmente acoplados, sin transferencia o poco frecuente
- Flujos de datos difíciles de predecir, dependientes de aplicación y de contexto

Distribuido
Caracterizar Tipos de Flujo



VoIP
Caracterizar Tipos de Flujo

- Dos flujos
  - Audio, tipo P2P
  - Establecimiento y mantenimiento de llamada, tipo cliente/servidor

4.1.4. Caracterizar Carga de Tráfico

Carga de Tráfico

- Caracterizar la carga de trabajo ayuda a diseñar redes con capacidad suficiente
- Múltiples factores afectan a la carga, estimación imprecisa
- Objetivo: evitar diseños con cuellos de botella críticos

- Análisis de aplicaciones
- Sobreaprovisionamiento de ancho de banda (barato en LAN, no tanto en WAN)

Cálculo de la Carga Teórica

- *Carga de tráfico* (*carga ofrecida*), suma de todos los datos que los nodos de una red están preparados para enviar en un instante dado
- La capacidad es suficiente?
  - Núm. estaciones
  - Tiempo medio inactividad entre envíos
  - Tiempo medio para transmitir un mensaje
- Analizador de protocolo para conseguir tiempos inactividad y tamaño medio de marco
- Mejora la precisión si se tiene en cuenta tipos de flujos
  - Cliente/Servidor: núm. clientes?, carga servidor?

Refinando la Estimación de Carga

- Investigar el tamaño de los objetos enviados por aplicación, sobrecarga de protocolos y cualquier sobrecarga debida a inicialización
- Comportamiento usuarios variable, difícil estimar el tamaño medio de los objetos
  - Pantalla de terminal: 4 KB
  - Email simple: 10 KB
  - Página web simple: 50 KB
  - Imagen de alta calidad: 50 MB
  - Backup de base de datos: 1 GB o más

Carga Debida a Protocolos de Encaminamiento

- Envío tabla en vector de distancias, cada medio minuto, puede consumir una significativa porción de ancho de banda
  - RIP envía uno o más paquetes de 532 bytes cada 30 segundos
- Protocolos más modernos (OSFP, EIGRP) usan menos ancho de banda
- OSPF
  - Sincronización BD cada 30 minutos (subdividir en areas para reducir)

    - `Hello` cada 10 seg.
- EIGRP
    - No sincronización periódica, solo cuando cambia la BD
    - `Hello` cada 5 seg.

4.2. Comportamiento del Tráfico

4.2.1. Broadcast/Multicast

Broadcast/Multicast
Comportamiento del Tráfico

- Broadcast
    - Marco que alcanza todas las estaciones en una LAN
    - `FF:FF:FF:FF:FF:FF`
- Multicast
    - Marco que alcanza un subconjunto de estaciones en una LAN
    - `01:xx:xx:xx:xx:xx`
    - Requiere protocolos encaminamiento multicast
- Usos
    - Compartir información (routers)
    - Anunciar servicios (servidores)
    - Encontrar servicios (clientes)

Broadcast/Multicast
Comportamiento del Tráfico

- Dispositivos L2 reenvían broadcast/multicast por todos los puertos, problemas escalabilidad en redes grandes planas
- Routers no reenvían broadcast, definen *dominio de difusión*
- VLANs limitan tamaño dominio difusión
- *Radiación de difusión*, efecto de difundir broadcast desde el emisor a todos los dispositivos en su dominio de difusión
- *Tormenta de difusión*, causado por interfaces mal configuradas o fallando
- Si broadcast/multicast $> 20\,\%$ del tráfico, segmentar (routers o VLANs)
- Tráfico de difusión es necesario e inevitable

4.2.2. Eficiencia de la Red

Eficiencia de la Red

- Uso eficiente del ancho de banda por aplicaciones y protocolos
  - Tamaño del marco
  - Interacción del protocolo
  - Control del flujo y ventanas
  - Mecanismos de recuperación de errores

Tamaño del Marco
Eficiencia de la Red

- Maximizar *Maximum Transmission Unit*, MTU, mejora las prestaciones, especialmente en las de transporte masivo de datos
- Cuidado no sobrepasar el máximo, fragmentación IP
- Mecanismos de descubrimiento de MTU para ajustar dinámicamente el tamaño de marcos

Control del Flujo y Ventanas
Eficiencia de la Red

- Comprender funcionamiento ventanas en el control de flujo
  - Emisor envía datos sin esperar ACK hasta que consume ventana emisión
  - Basada en la ventana recepción del receptor [1, 65KB]
  - Dependiendo de memoria disponible y cómo de rápido procesa los datos recibidos
- Tamaño ventana óptimo teórico = ancho de banda $*$ latencia
- Optimizar eficiencia incrementando memoria y capacidad procesamiento (CPU) de estaciones (mayores ventanas de recepción)
- Sólo en TCP, UDP no controla el flujo (lo hace la aplicación?)

Control del Flujo y Ventanas
Eficiencia de la Red

- TCP
  - File Transfer Protocol (FTP), puerto 20 (datos), puerto 21 (control)
  - Secure Shell (ssh): puerto 22
  - Telnet: puerto 23

    - Simple Mail Transfer Protocol (SMTP): puerto 25
    - Hypertext Transfer Protocol (HTTP): puerto 80
- UDP
    - Domain Name System (DNS): puerto 53
    - Dinamic Host Configuration Protocol (DHCP): servidor puerto 67, cliente puerto 68
    - Trivial File Transfer Protocol (TFTP): puerto 69
    - Remote Procedure Call (RPC): puerto 111
    - Simple Network Management Protocol (SNMP): puertos 161 y 162

Mecanismos de Recuperación de Errores
Eficiencia de la Red

- Recuperación de error puede desperdiciar ancho de banda
    - Retransmisiones innecesarias por fallos prematuros
    - ACKs en distintas capas
- TCP usa retransmisiones adaptativas: disminuye la tasa de retransmisión con red congestionada, optimiza uso ancho de banda
- Repetición selectiva (vs. GBN)
- Configurar temporizadores de retransmisión o actualizar a mejor implementación de protocolos

4.3. Requisitos de QoS

Requisitos QoS

- Conocer los flujos y carga no es suficiente, hay que caracterizar requisitos de calidad
    - Flexible o inflexible?
    - Tomar ancho de banda de apps flexibles para mantener apps inflexibles?
- Voz, inflexible respecto a retardo, flexible con pérdidas
- Enfoques *Quality of Service*, QoS
    - ATM
    - IETF

4.3.1. QoS en ATM

Especificación QoS en ATM

- *Asynchronous Transfer Mode*, ATM, identifica los parámetros para especificar cierto tipo de QoS, y define categorías de servicio
  - CBR, *Constant bit rate*
  - rt-VBR, *Real-Time variable bit rate*
  - nrt-VBR, *Non-Real-Time variable bit rate*
  - UBR, *Unspecified bit rate*
  - ABR, *Available bit rate*
  - GFR, *Guaranteed frame rate*

4.3.2. QoS en IETF

IETF

- Servicios Integrados
  - *Resource Reservation Protocol*, RSVP, solicitar calidad de servicio a la red para una app
    - Clasificación de paquetes
    - Control de admisión
    - Planificador
  - *Servicio de carga controlada*, como si red descargada
  - *Servicio garantizado*, ancho de banda y retardo, limitando retardo debido a colas (cubeta agujereada)

IETF

- Servicios Diferenciados
  - Arquitectura para implementar una diferenciación servicios escalable
  - Paquetes marcados con códigos de servicio diferenciados, para su uso en colas y decisiones descarte de paquetes
  - Menos granularidad que RSVP, pero más escalable

4.4. Grado de Servicio

GoS

- *Grado de Servicio*, GoS, en redes de voz, fracción de llamadas exitosamente completadas (también *Call completion rate*, CCR)
  - Componentes fiables
  - Redundancia, encaminamiento dinámico y STP

4.4.1. Documentar Requisitos QoS

Documentar Requisitos QoS

- Trabajar con el cliente para clasificar cada app en una categoría de servicio
- Utilizar terminología ATM o IETF
- Simplificación
  - *Inflexible*, app con requisitos específicos de ancho de banda constante, retardo y variación del retardo, precisión y throughput.
  - *Flexible*, app que simplemente espera *best effort* de la red (no multimedia)

Documentar Requisitos QoS

Aplicación	Tipo Flujo	Protocolos	Grupo Usuarios	Almacenes Datos (Servidor, host)	Ancho de Banda Estimado	Requisitos QoS

4.5. Resumen

Resumen

- Técnicas para analizar tráfico de red de apps y protocolos
- Métodos para identificar fuentes y sumideros, medir flujos y cargas
- Documentación

Resumen Parte 1

Resumen Parte 1

- Identificado apps de red y requisitos técnicos del diseño
- Metodología descendente
  - Objetivos del negocio y aplicaciones
  - Objetivos técnicos para aplicaciones
  - Caracterización de la red existente
  - Caracterización del tráfico de red existente
- Análisis de requisitos fundamental para diseño descendente de redes

Parte II
Diseño Lógico

5. Diseño de la Topología de Red

Diseño de la Topología de la Red

- *Topología* como mapa que indica los segmentos, puntos de interconexión y comunidades de usuarios
- Mostrar la geometría de la red, no la localización física o implementaciones técnicas
- Previo a la elección de productos y tecnologías físicas

Aspectos a Tratar

- Jerarquía
- Redundancia
- Modularidad
- Entradas y salidas
- Perímetro protegido

5.1. Diseño Jerárquico

Topología Jerárquica

- Capa *núcleo*, routers y switches de alto nivel optimizados para disponibilidad y prestaciones
- Capa *distribución*, routers y switches que implementan políticas e interconectan toda la red
- Capa *acceso*, conecta usuarios mediante switches de bajo nivel y puntos de acceso inalámbricos

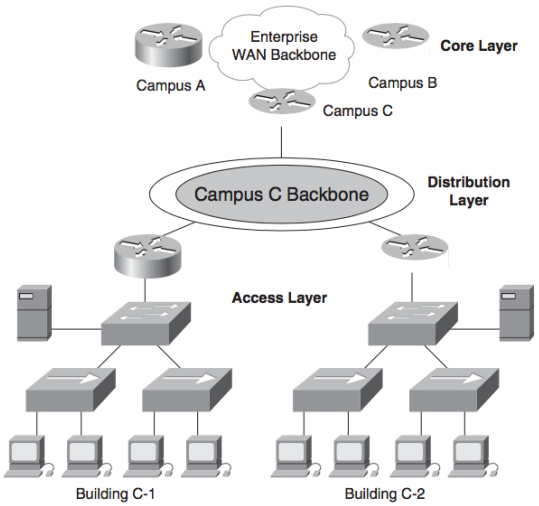
5.1.1. Por Qué un Diseño Jerárquico?

Por Qué un Diseño Jerárquico?

- Las redes no planificadas tienden a no tener estructura, *bolas de pelo*
- Reducir la carga en los dispositivos de red (routers!)

    - evita demasiados dispositivos comunicándose entre sí (reduce adyacencias de CPUs, dominios difusión)
- Minimizar costes ajustando las capacidades de los dispositivos a su cometido
- Cálculo preciso de las necesidades de ancho de banda
- Distribución de las responsabilidades de gestionabilidad
- Mantener un diseño sencillo y fácil de entender
- Facilita los cambios y la escalabilidad

Topología Jerárquica



Cuándo se Sabe que un Diseño es Bueno?

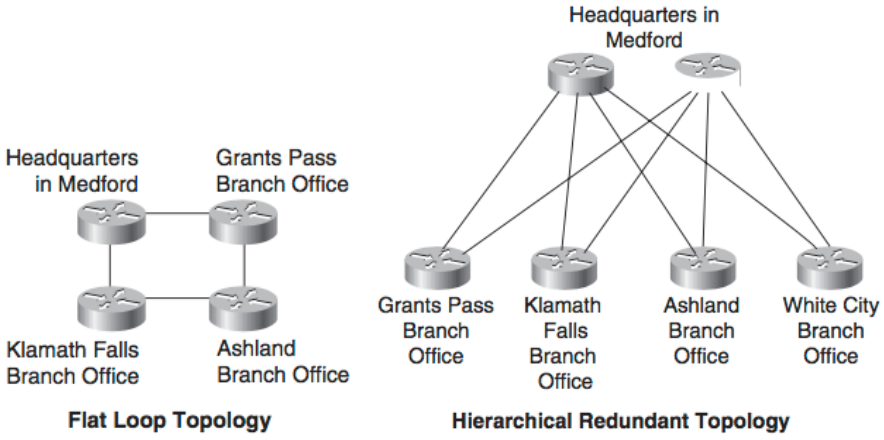
- Cuando ya se sabe cómo añadir un edificio, planta, enlace WAN, sitio remoto, etc.
- Cuando nuevas incorporaciones sólo producen cambios locales en los dispositivos directamente conectados
- Cuando la red puede crecer duplicándose o triplicándose sin mayores cambios en el diseño
- Cuando la solución de problemas es sencilla porque no hay interacciones complejas entre protocolos que tener en cuenta

5.1.2. Topologías Planas vs. Jerárquicas

Topologías Planas vs. Jerárquicas

- Topología plana adecuadas para redes pequeñas
- Fáciles de diseñar e implementar
- Dificultan resolución problemas cuando crecen

Topología plana WAN



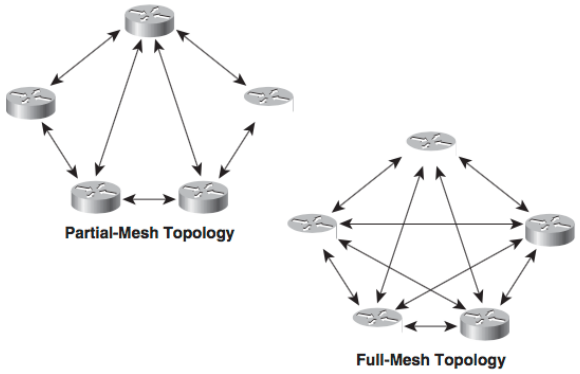
Topología plana LAN

- 1990's, hosts conectados mediante hubs en una topología plana
  - Todos compartían mismo dominio colisión (ancho de banda) afectando negativamente a retardo y throughput
- Cambio recomendado: usar switches para segmentar dominios de colisión
  - Dominio de difusión compartido
- Utilizar routers para segmentar y aislar tráfico difusión (a unos pocos cientos de dispositivos)
- Diseño jerárquico coloca dispositivos de red donde hacen mejor su trabajo
  - Routers aislando broadcast
  - Switches alta capacidad máximizando ancho de banda
  - Switches multipuerto para acceso

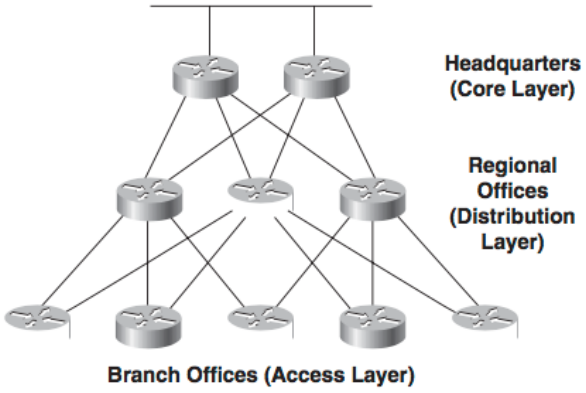
5.1.3. Topología Malla vs. Jerárquica

Topología Malla vs. Jerárquica

- Buenas prestaciones y fiabilidad
- Coste implantación y mantenimiento $(n \cdot (n-1)/2$ enlaces)
- Problemas escalabilidad en mensajes broadcast (regla: $\leq 20\,\%$ del tráfico)

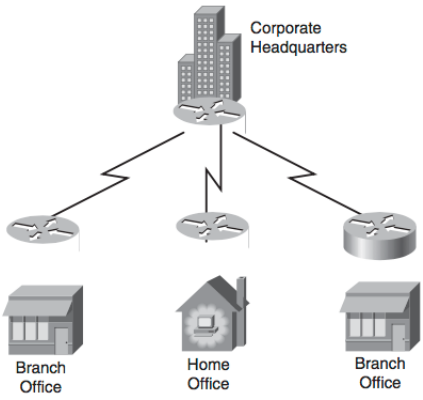


Topología Jerárquica con Mallado Parcial



Topología Jerárquica Radial

- Compañías pequeñas o medianas, topología radial
- Oficina central o centro de datos como eje

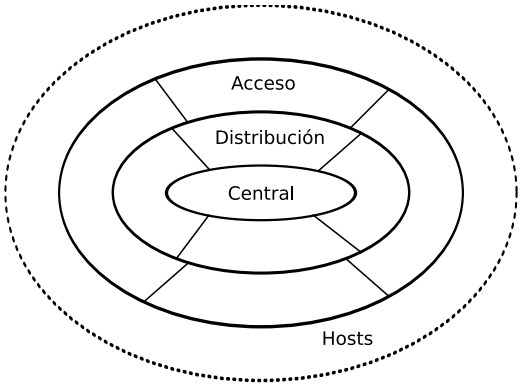


5.1.4. Modelo Jerárquico Clásico de Tres Capas

Modelo Jerárquico Clásico de Tres Capas

- Permite agregación y filtrado del tráfico en tres niveles sucesivos de encaminamiento o conmutación
- Escalable hasta grandes redes
- *Núcleo*, transporte óptimo entre sitios
- *Distribución*, conecta los servicios de red con la capa de acceso e implementa políticas de seguridad, carga de tráfico y encaminamiento
- *Acceso*, proporciona switches para la conexión de hosts de usuario (si WAN, consiste en los routers en el límite de la red del campus)

Concepto
Modelo Jerárquico Clásico de Tres Capas



Núcleo
Modelo Jerárquico Clásico de Tres Capas

- Troncal alta velocidad crítica para la red
- Optimizar throughput, evitando filtrado u otras operaciones que afecten a latencia y gestionabilidad
- Altamente fiable (redundancia) y adaptable
- Diámetro limitado proporciona prestaciones predecibles y facilita solución problemas
- Incluye enlaces a redes externas, mejorando seguridad

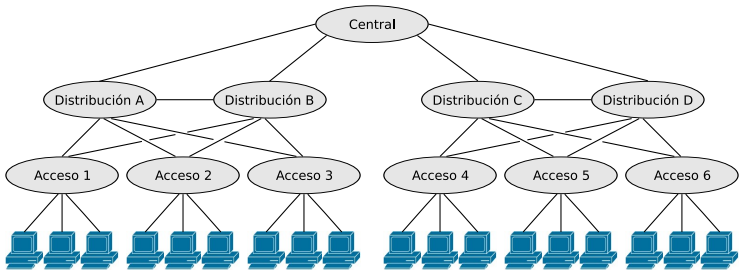
Distribución
Modelo Jerárquico Clásico de Tres Capas

- Límite entre núcleo y acceso
- Controla el acceso a recursos por seguridad, y el tráfico que cruza la red por prestaciones
- Límite de los dominios de difusión
- Si VLANs, puede encaminar entre VLANs
- Ocultar información entre routers núcleo y acceso
    - Resumir varios destinos hacia acceso en unos pocos anuncios en el núcleo
    - Resumir rutas hacia el núcleo ofreciendo una única ruta por defecto
    - Proveer de ruta al núcleo a través del router distribución más cercano

Acceso
Modelo Jerárquico Clásico de Tres Capas

- Segmentos de red locales con acceso a la red
- Constituidos por switches, APs (y routers)
- Si pequeñas sucursales o teletrabajo, incorpora enlaces WAN (ISDN, Frame Relay, DSL)

Modelo Jerárquico Clásico de Tres Capas



Modelo Jerárquico Clásico de Tres Capas

- Cada dispositivo de acceso conectado a 2 dispositivos del nivel de distribución
- Mejorar la productividad y la fiabilidad.
- Regla 80/20: ciertos grupos de usuarios usan ciertos servicios, agruparlos en la misma VLAN, y además en los mismos grupos de distribución

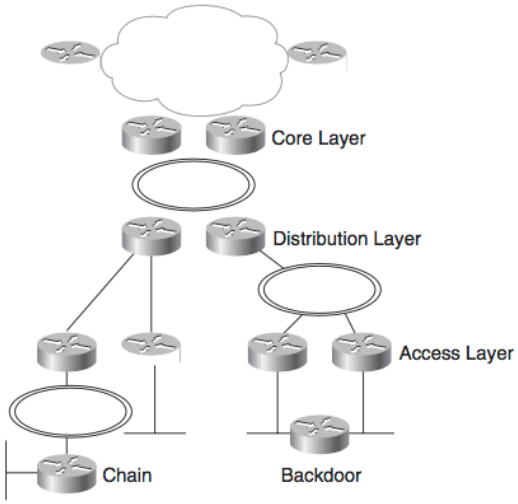
5.1.5. Directrices de Diseño Jerárquico

Directrices Diseño Jerárquico

- Controlar el diámetro de la topología
  - Tres capas serán suficientes
  - Latencia baja y predecible
- Control estricto de la capa de acceso
  - Evitar encadenamiento (añadir redes inapropiadamente) y puertas traseras (conexión entre dispositivos de la misma capa)
  - Problemas encaminamiento y conmutación, dificulta solución problemas
- Comenzar el diseño por la capa de acceso, luego distribución y núcleo
  - Facilita planificación de capacidades en distribución y núcleo

Diseñar cada capa de modo modular y jerárquico, después las interconexiones (según carga, flujo y comportamiento del tráfico)

Directrices Diseño Jerárquico



5.2. Diseño de Topologías Redundantes

Diseño de Topologías Redundantes

- Conseguir disponibilidad redundando elementos en la red
- Eliminar “cualquier” punto de fallo único redundando “cualquier” componente cuyo fallo afecte a aplicaciones críticas
  - Router, switch, enlace, fuente alimentación, enlace WAN, conexión Internet, . . .
- Caro de implantar y mantener, añade complejidad
  - Redundancia vs coste bajo
  - Complejidad vs simplicidad

Analizar objetivos técnicos del cliente, identificar aplicaciones críticas y consultar la tolerancia al riesgo

5.2.1. Camino Redundante

Camino Redundante

- Las redes redundantes incluyen camino de backup en caso de problemas en el primario (*high availability*, HA)
  - Routers, switches y enlaces extra

- Capacidad
  - Normalmente de menos capacidad que el principal
- Rapidez de activación
  - Activación manual o automática
  - Necesidad de ser testados
  - También para reparto de carga

5.2.2. Reparto de Carga

Reparto de Carga, LS

- Mejorar prestaciones repartiendo la carga entre varios enlaces o interfaces paralelas (también conocido como *load balancing*, LB)
- En WAN, agregación de canales permite establecer múltiples canales según se incremente el ancho de banda.
  - *Multilink Point-To-Point Protocol*, MPPP
  - Encaminamiento dinámico sobre enlaces paralelos con igual coste (congestión ojo de aguja)
  - EIGRP `variance`, permite hasta 6 caminos paralelos con distinto coste

5.3. Diseño Modular

Diseño Modular

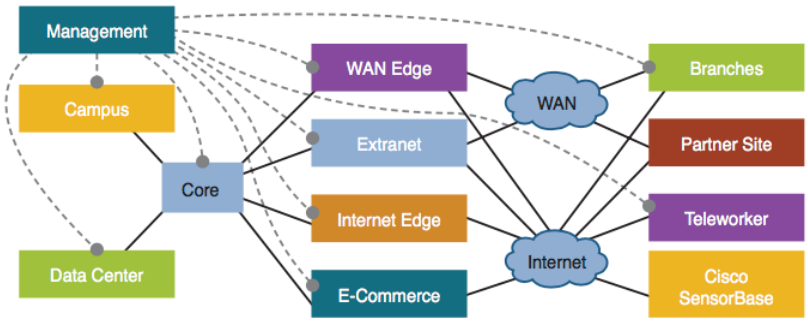
- Jerarquía, redundancia y modularidad
- Red grande consistente en distintas áreas o módulos
- SAFE, Arquitectura de referencia de seguridad Cisco

5.3.1. Arquitectura CISCO de Seguridad SAFE

Arquitectura CISCO de Seguridad SAFE

- Diseño modular, simplificando la complejidad de una red grande
- Arquitectura SAFE especialmente concernida con la seguridad
  - Defensa en profundidad multicapa

Arquitectura CISCO de Seguridad SAFE



Módulos
Arquitectura CISCO de Seguridad SAFE

- *Núcleo*
  - Une todos los demás módulos
  - Alta velocidad y escalable (L2 y L3)
  - Implementado como switches redundantes que agregan las conexiones de otros módulos
- *Centro de Datos*
  - Servidores, aplicaciones, almacenamiento para usuarios internos
  - Incorpora la infraestructura de red para esos dispositivos
    - Repartidores de carga, SW, RTR
  - No directamente accesible a usuarios externos en Internet

Módulos
Arquitectura CISCO de Seguridad SAFE

- *Campus*
  - Red de acceso para usuarios y dispositivos en una localización geográfica
  - Desde una o varias plantas de un edificio hasta varios edificios
  - Servicios locales de datos, voz y video
  - Permitir acceso seguro al centro de datos e Internet
- *Administración*
  - Monitorización, análisis, autenticación y registro
    - RADIUS, KERBEROS, NTP, SNMP
  - Combina gestión en banda y fuera de banda sobre todos los módulos
  - Si fuera de banda, switches dedicados o VLAN aislada

Módulos
Arquitectura CISCO de Seguridad SAFE

- *Extremo WAN*
  - Agregación de enlaces WAN hacia sucursales o central regional
  - Propio o alquilado a proveedor
- *Extremo Internet*
  - Conexión a Internet, *gateway* entre empresa y resto mundo
  - DMZ, acceso corporativo a Internet y acceso remoto mediante VPN

Módulos
Arquitectura CISCO de Seguridad SAFE

- *Sucursales*
  - Usuarios y dispositivos en localización remotas
  - Una o varias LANs conectadas a la central mediante WAN privada o Internet con VPN
  - Datos locales y servicios de voz y video
- *Extranet*
  - Permite que redes de socios, clientes y proveedores accedan a determinada porción de la red mediante protolos seguros
  - VPN, detección de amenazas, caída segura de servidores y dispositivos de red, topología redundante

Módulos
Arquitectura CISCO de Seguridad SAFE

- *Socios*
  - Redes de socios, clientes y proveedores
  - Acceden a servicios en la extranet mediante WAN o Internet segura
- *Comercio Electrónico*
  - Aplicaciones, servidores y datos utilizados para vender o comprar
  - Granjas de servidores, seguridad de L2 a L7, filtrado de tráfico, reparto de carga en servidores
  - Segmentación y ejecución de políticas servidor a servidor

Módulos
Arquitectura CISCO de Seguridad SAFE

- *Teletrabajo*
  - Casa del teletrabajador
  - VPN de acceso remoto, seguridad de escritorio e inalámbrica
  - Telefonía IP, video
- *Sensores*
  - Servidores que recolectan amenazas
  - Sistemas de prevención de intrusión

5.4. Diseño de una Topología de Red de Campus

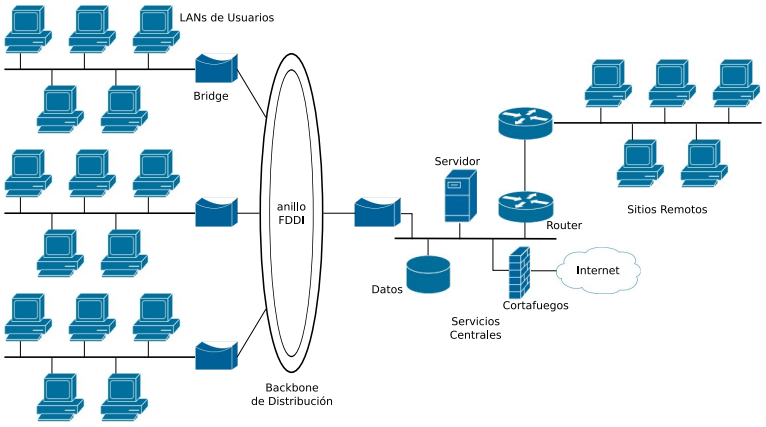
Topología de Red de Campus

- Diseñada para cumplir objetivos de disponibilidad y prestaciones
  - dominios de colisiones pequeños
  - dominios de difusión pequeños
  - redundancia con servidores espejados y múltiples caminos host-router
- Utilizar diseño jerárquico y modular para ofrecer buenas prestaciones, mantenibilidad y escalabilidad

Topología de Red de Campus

- Capa acceso de campus:
  - Estaciones de trabajo usuarios y teléfonos IP conectados a switches y APs
  - Servicios: acceso a red, control difusión, filtrado protocolos, marcado de paquetes para QoS
- Capa distribución de campus:
  - Agregación de armarios de cableado dentro de edificios y conectividad con el núcleo del campus
  - Servicios: encaminamiento, QoS y control acceso para seguridad y prestaciones
  - Recomendado redundancia y reparto de carga (enlaces duplicados con el núcleo)
- Capa núcleo de campus:
  - Interconexión acceso y distribución con el centro de datos, la administración de la red y los módulos fronterizos de forma rápida
  - Redundancia y recuperación rápida
  - Servicios: QoS y seguridad

LANs Campus al estilo antiguo
Ejemplo



LANs Campus al estilo antiguo

- Gigantesca red plana en capa 3
- Cada paquete de difusión es enviado a todos los nodos de la red
- Conmutación válida entre usuarios y servidores
- Conexión de los remotos con menor ancho de banda que los elementos en la LAN
  - Hecho cierto: el ancho de banda cuesta dinero, la distancia también
- Regla (modificada): conmutar donde el ancho de banda sea barato, encaminar donde sea caro

Estilo Antiguo Modernizado

- No conviene conmutar siempre en la LAN:
  - Muchos más dispositivos conectados.
  - Ráfagas de tráfico mas cortas que necesitan más ancho de banda
- Se necesita priorizar el tráfico y modelar las ráfagas de tráfico

5.4.1. Protocolo de Árbol de Expansión

Protocolo de Árbol de Expansión, STP

- STP (*Spanning Tree Protocol*), determina la topología de la red podando dinámicamente enlaces del nivel 2 para definir el árbol de expansión (IEEE 802.1D)

- STP crea un árbol lógico sin redundancia a partir de una malla de conexiones entre switches
  - Switch raiz y puertos en resto de bridges que reenvían tráfico hacia el raíz
  - BPDU, *Bridge Protocol Data Unit*
  - Calcula el camino de menor costo (mayor ancho de banda) al switch raíz

Protocolo de Árbol de Expansión Rápido, RSTP

- 802.1w, reconfiguración rápida del árbol de expansión
  - 802.1D, $\approx$ 1 min
  - 802.1w, $\approx$ 0,1 s
- Estados de puerto:
  - *Descartando*, no aprende dir. MAC ni reenvía
  - *Aprendizaje*, dir. MACs para poblar tabla MAC, pero aún no reenvía paquetes
  - *Reenvío*, aprendiendo MACs y reenviando paquetes
- Mecanismo sincronización, no dependiente de temporizadores
- Switch raíz, aquel con menor ID
- Cada switch tiene un costo asociado con el camino hacia el raíz
  - 0 para el raíz
  - Para los demás switches, suma de los costes del camino de puertos en el trayecto de menor coste

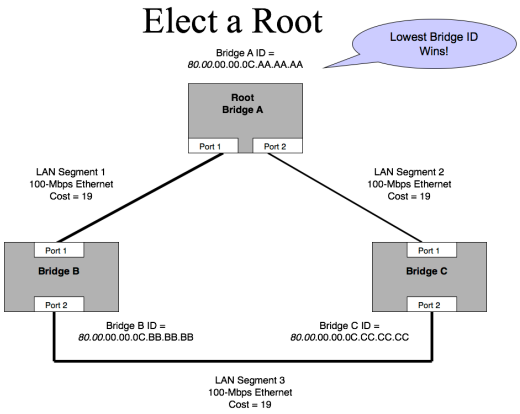
Protocolo de Árbol de Expansión Rápido, RSTP

- Cuando una red ha convergido, cada puerto de switch está en estado
  - *Raíz*, en el camino menor coste hacia raíz (reenvío)
  - *Designado*, puerto camino menor coste para toda una LAN (reenvío)
  - *Alternativo*, otro camino hacia raíz (descartando)
  - *Reserva*, backup de un puerto designado en dirección a las hojas (descartando)
  - *Desactivado*, no operativo (descartando)
- Puerto terminal, conectado a LAN sin más SWs (reenvío)
- Cada LAN sólo un puerto designado, y cada switch no raíz un único puerto root conectado a una LAN $\rightarrow$ no ciclos entre LANs, un árbol de expansión
- Elegir con cuidado el switch raíz: rápido y en el centro de la topología

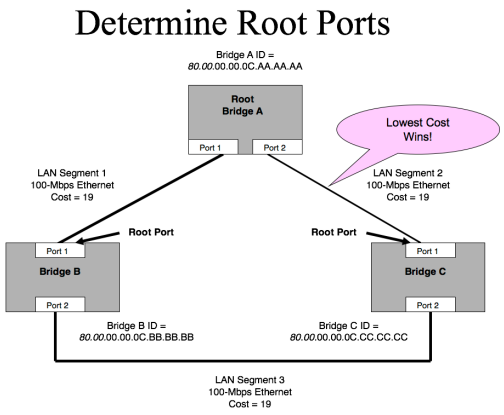
Switches Ejecutando RSTP

- Participan en la elección de un único switch que será el raíz.
- Calculan la distancia del camino más corto al SW raíz y eligen un puerto (puerto raíz) que conduce a ese camino más corto hacia el raíz
- Para cada segmento LAN, elegir un SW designado y un puerto designado en ese SW. El puerto designado en el segmento LAN es el que está más cerca del SW raíz (todos los puertos en el SW raíz son designados)
- Los puertos raíz y designados participarán en el STP, reenviando tráfico. El resto bloquearán el tráfico

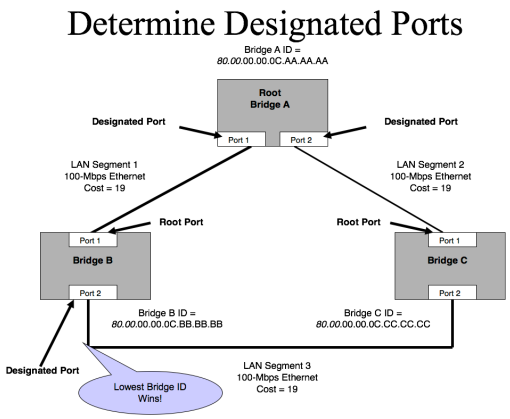
Protocolo de Árbol de Expansión Rápido, RSTP



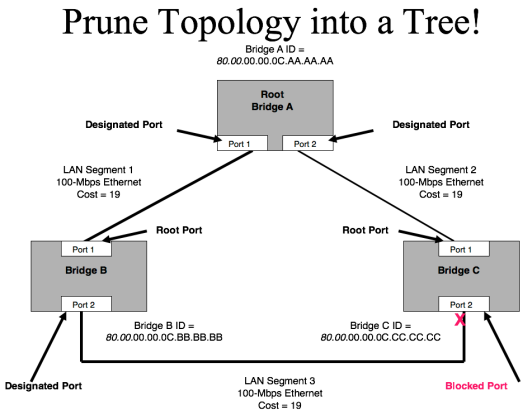
Protocolo de Árbol de Expansión Rápido, RSTP



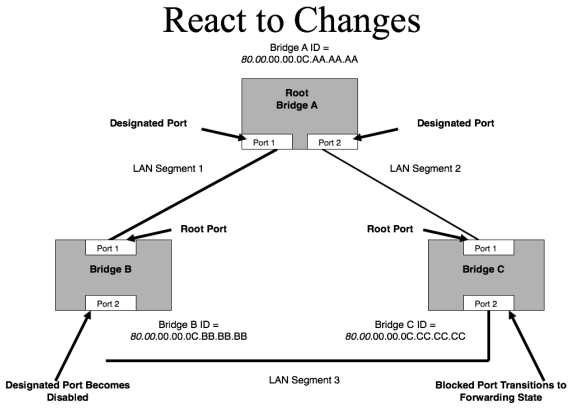
Protocolo de Árbol de Expansión Rápido, RSTP



Protocolo de Árbol de Expansión Rápido, RSTP



Protocolo de Árbol de Expansión Rápido, RSTP



Escala del Protocolo de Árbol de Expansión

- STP converge mejor en redes conmutadas relativamente pequeñas (no más de 7 SW) y con suficiente capacidad en CPU y memoria para procesar los paquetes STP
- RSTP (IEEE 802.1w) converge en cientos de ms
- Las redes se diseñan en su topología de nivel 2 como árboles, STP sólo para eliminar bucles inadvertidos
- Los routers y los protocolos de encaminamiento considerados en el diseño de distribución y núcleo

5.4.2. LAN Virtuales, VLANs

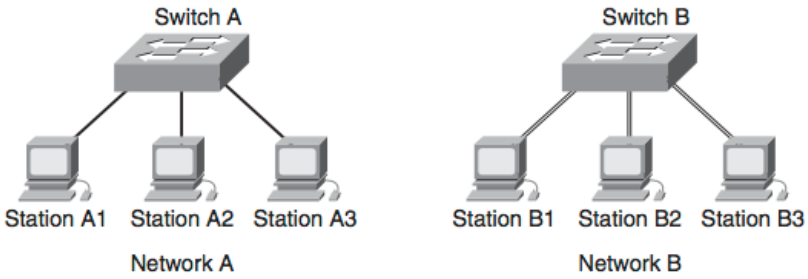
LAN Virtuales, VLANs

- Una red debería diseñarse con dominios de difusión y de colisión pequeños
  - *Dominio de colisión* - dispositivos que comparten el ancho de banda y compiten por acceder a él (colisiones)
  - *Dominio de difusión* - dispositivos que pueden oír los paquetes de difusión del resto
- VLAN emula una LAN que permite la transferencia de datos sin las restricciones físicas de una red
- Los dispositivos en una misma (distinta) VLAN se comunican entre ellos como si estuvieran en un mismo (distinto) cable, aunque estén en distintos segmentos físicos de red (en el mismo SW físico)
- Basadas en conexiones lógicas, no físicas $\rightarrow$ LANs muy flexibles

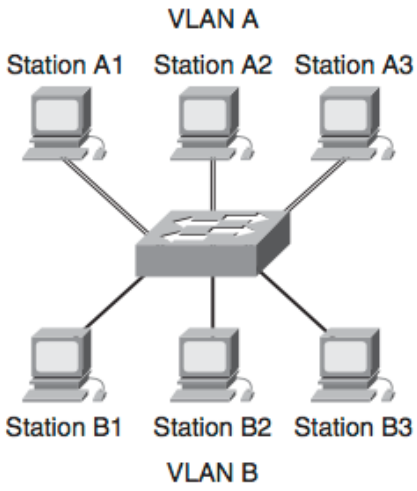
VLANs

- Mediados 1990's, no importa la localización física de un usuario, incluso pudiendo cambiar
  - VLANs dispersas cruzando varias LANs necesita que el tráfico alcance todas esas redes, afectando al rendimiento
  - Redes espagueti, difíciles de gestionar y optimizar
- Actualmente, VLANs como forma de dividir redes físicas basadas en SW en varias redes lógicas
  - Rompen dominios de difusión
  - Necesario router para comunicación inter-VLAN
  - En redes IP, VLAN implementada como una subred separada

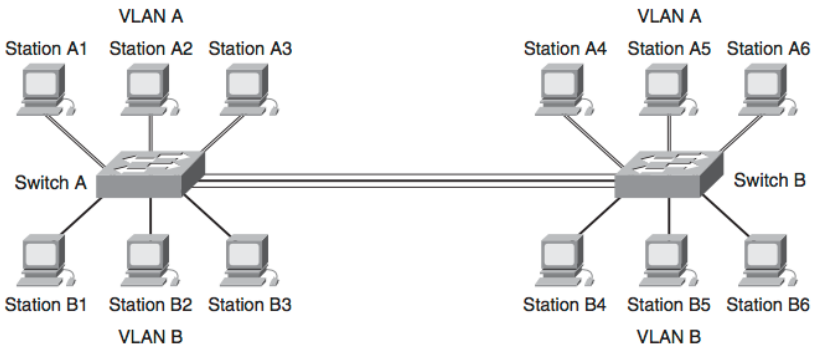
VLANs



VLANs



VLANs



Evitar VLAN Espagueti
VLANs

- Diseños físicos perfectos arruinados por un lío de VLANs
  - Cada puerto de cada switch se puede asignar a una VLAN
  - Todas las VLANs están activas a la vez
- Problemas
  - Oculta los problemas de comunicación
  - Incremento de latencia y congestión en la troncal
- Usarlas con mesura y cuidadosamente
- Cuidado con la asignación de VLANs según el protocolo, mejor basado en puerto

Regla 80/20
VLANs

- El 80 % del tráfico es local y sólo el 20 % necesita cruzar el centro de la red
- Intenta mantener baja la carga de los routers
- Útil en la construcción de VLANs, al decidir cómo agrupar los usuarios mediante VLANs
  - Demasiados dispositivos en una VLAN
  - Presencia de cada VLAN en todos los switch (espagueti)
- Sacrificar regla 80/20 frente a la fiabilidad y la manejabilidad

VLANs

- IEEE 802.1Q, o ISL de Cisco
- Cuando un paquete abandona un SW, se le añade una ID, etiqueta VLAN
- Enlaces troncal, *trunk* permiten extender VLANs por varios SW
- Enlaces de *acceso* permiten la conexión de host al SW en una VLAN
- Mantener alcance VLANs controlado a unos cientos de dispositivos (mismo dominio difusión)

5.4.3. LANs inalámbricas, WLANs

LANs inalámbricas, WLANs

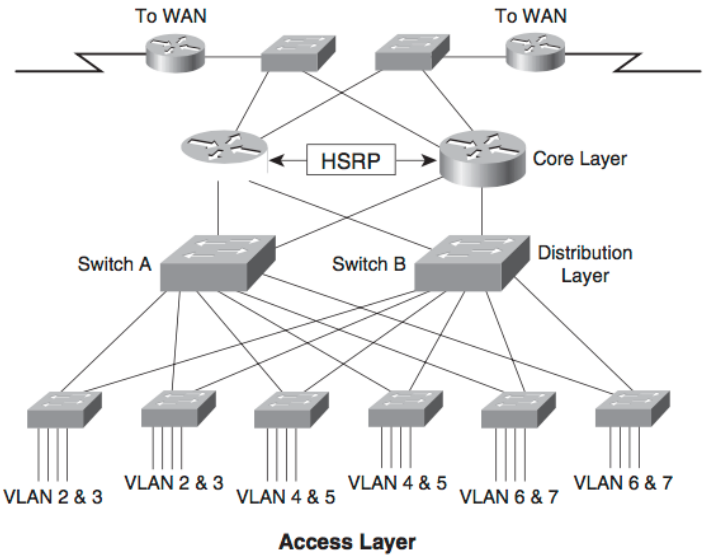
- Ofrecen acceso Internet/Intranet en áreas abiertas o donde no es posible el cableado
- Topologías WLAN determinando la cobertura en cada célula inalámbrica para posicionar APs
  - Tasa de datos, potencia, tipo de antena y posicionamiento
  - Células demasiado grandes implican muchos dispositivos en el dominio de colisión (802.11)
  - Células más pequeñas mejoran las prestaciones para los clientes a costa de más APs
- WLAN como una VLAN, misma subred IP, facilita *roaming* y filtrado (seguridad)
- Redundancia, dos APs con el mismo canal en el mismo área de cobertura, primario y secundario (HA)

5.4.4. Redundancia y Reparto de Carga en LANs

Redundancia y Reparto de Carga en LANs

- STP bueno para redundancia, no para reparto de carga
- Un STP por VLAN, un SW raíz para una VLAN puede ser backup para el raíz de otra VLAN
  - Cisco PVST+, construye un árbol de expansión por VLAN (escalabilidad limitada)
  - MST, *Multiple Spanning Tree*, IEEE 802.1s y Cisco MISTP permite agrupar VLANs en un ST

Redundancia y Reparto de Carga en LANs



Redundancia y Reparto de Carga en LANs

1. SW A raíz para VLANs 2, 4 y 6 (SW B backup de SW A)
2. SW B raíz para VLANs 3, 5 y 7 (SW A backup de SW B)
3. Ambos enlaces de SW de acceso llevan tráfico, y el cambio a un nuevo SW raíz es automático si cae el SW de distribución
4. LS y HA
5. Escalable a una red de campus grande
    - Probado hasta 8000 usuarios
    - 80 SWs de acceso
    - 14 SWs distribución
    - 4 RTRs en el núcleo

Redundancia de Servidor

- Archivos, web, DHCP, nombres, DB, VoIP (núm. telf. a dir. IP)
- DHCP redundantes, en capa de acceso o núcleo dependiendo tamaño de la red
    - DHCP no necesariamente en el mismo segmento que clientes, Cisco IP Helper Address

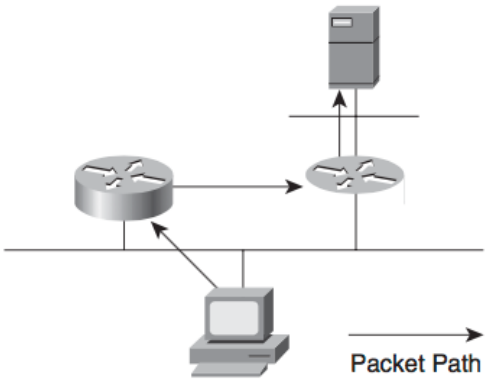
- Nombres (DNS, WINS, NBNS) redundantes, acceso o núcleo según tamaño red
- Servidores espejados (*mirrored*) con datos idénticos y actualizaciones sincronizadas, en redes y proveedores de electricidad distintos
    - HA con duplicado de discos, Storage Area Network (SAN)
    - LS con CDN, multiples direcciones en DNS, multiples servidores DNS

5.4.5. Redundancia Comunicación Estación de Trabajo - Router

Redundancia Estación de Trabajo - Router

- Computadoras en red necesitan acceder a su *router por defecto* para alcanzar servicios remotos (*gateway*, GW)
- Router ejecutando proxy ARP
    - No estandarizado
    - Problemas de seguridad
- Asignar router por defecto mediante DHCP o manualmente
    - Problema de salto extra: router por defecto no siempre es la mejor ruta
    - Resuelto con rutas estáticas o protocolo encaminamiento (añade redundancia)
- Descubrimiento mediante *Router Discovery Protocol*, RDP (RFC 1256)
    - Extensión de ICMP
    - RTR difunde anuncios periódicos (7 a 10 min.)
    - Solicitudes de WS a demanda
    - Soportado por RTR, no tanto por WS (poco usado)
    - DHCP (RFC 2131) puede ofrecer también IP del GW
- Punto único de fallo

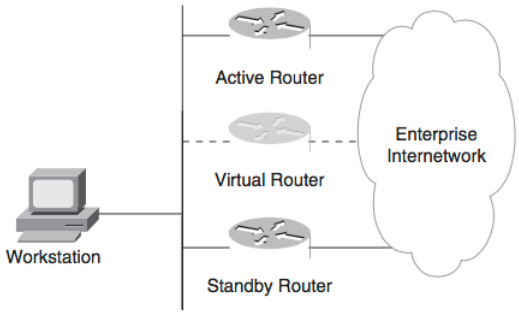
Problema Salto Extra
Redundancia Host-Router



HSRP/VRRP
Redundancia Estación de Trabajo - Router

- Redundancia mediante Cisco *Hot Standby Router Protocol*, HSRP (Cisco) o *Virtual Router Redundancy Protocol*, VRRP (RFC 2338)
  - Router virtual o fantasma, IP y MAC virtuales
  - WS configuradas con el router virtual como su GW
  - ARP respondido por RTR HSRP activo, o por el secundario si activo caído (también Proxy ARP)
  - Mensajes `hello`, temporizador
  - Tambien en el lado del router con varias interfaces WAN (*standby tracking*))
  - Preserva información NAT y túneles IPsec (VPNs) en el cambio entre routers
- LS con Cisco *Gateway Load Balancing Protocol*, GBLP
  - Una dirección IP virtual y varias MAC virtuales

HSRP
Redundancia Estación de Trabajo - Router



5.5. Diseño de una Topología para el Límite de la Red Empresarial

Límite de la Red Empresarial

- *WAN*, conectar oficinas remotas
- *Internet*, acceso a internet pública, ISP
- *Extranet*, conexiones con socios
- *Comercio Electrónico*, ofrecer y acceder a servicios y productos

5.5.1. Segmentos WAN Redundantes

Segmentos WAN Redundantes
Límite de la Red Empresarial

- Normalmente suficiente con una topología de malla parcial jerárquica
- Asegurarse de conseguir *diversidad de circuitos*
  - Difícil de asegurar por encaminamiento dinámico, alquileres entre proveedores
- Atención al cableado hasta el proveedor, normalmente más propenso a fallos

5.5.2. Conexiones Internet Redundantes

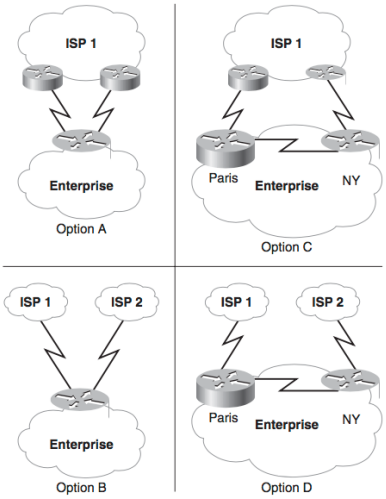
Conexiones Internet Redundantes, *multihoming*
Límite de la Red Empresarial

- *Multihoming* proveer a un sistema de más de una conexión para acceder y ofrecer servicios de red
- Dotar a la red de más de una conexión a Internet
- Redundancia, tolerancia a fallos

- Distintas opciones según objetivos
- Riesgo de convertirse en *red de tránsito*
    - RTR publica sólo su propia ruta

Los incrementos incontrolados de la redundancia conducen a incrementos incontrolados de la complejidad y, en realidad, pueden llegar a reducir la disponibilidad

Conexiones Internet Redundantes, *multihoming*
Límite de la Red Empresarial



Conexiones Internet Redundantes, *multihoming*
Límite de la Red Empresarial

	RTR	Conex	ISP	Pros	Cons
A	1	2	1	Coste bajo, coordinación ISPs	Sin redundancia ISP, RTR puf, ISP con dos conexiones cerca
B	1	2	2	Coste bajo, redundancia ISP	RTR puf, aplicar políticas con 2 ISPs
C	2	2	1	Coste medio, dispersión geográfica, coordinación ISPs	Sin redundancia ISP
D	2	2	2	Dispersión geográfica, redundancia ISPs	Coste alto, aplicar políticas con 2 ISPs

5.5.3. Redes Privadas Virtuales, VPNs

VPN
Límite de la Red Empresarial

- Red Privada Virtual, VPN, permite conexiones seguras privadas sobre una red de terceros o Internet
  - *Tunelización* (encapsular paquetes de un protocolo en otro) + *Encriptación*
  - Conexión punto a punto sobre una red IP no orientada a conexión, con capacidades de seguridad avanzadas
- Conectar sitios remotos, usuarios móviles o teletrabajadores

VPN
Límite de la Red Empresarial

- Capa 2 OSI
  - *Point-to-Point Tunneling Protocol*, PPTP
  - *Layer 2 Forwarding*, L2F
  - *Multiprotocol Label Switching*, MPLS VPNs
  - *Layer 2 Tunneling Protocol*, L2TP (RFC 2661), usado en mayoría soluciones VPN
- Capa 3 OSI
  - *Internet Protocol Security*, IPsec, si únicamente IP unicast
  - Cisco *Generic Routing Encapsulation*, GRE, si broadcast IP o no IP
- Aplicaciones VPN
  - Sitio-a-Sitio, (*extranet*)
  - Acceso Remoto

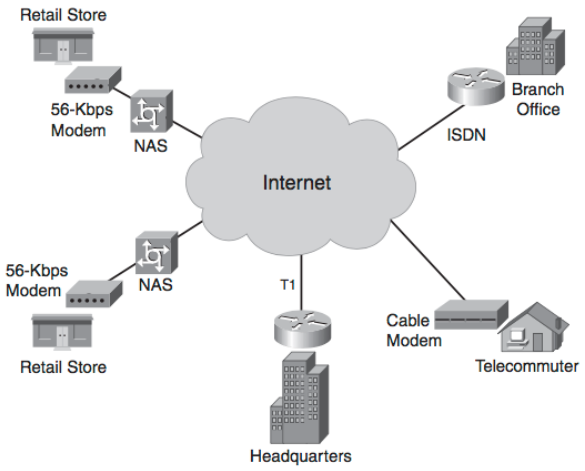
Aplicación VPN Sitio-a-Sitio
Límite de la Red Empresarial

- Medio asequible y fácil de gestionar para conectar sucursales remotas u oficinas domésticas vía ISP (en lugar de WAN)
- Topología (alta disponibilidad, recuperación fallos automática, prestaciones, seguridad, escalabilidad)
  - Radial
    - Un servidor VPN con un túnel IPsec o GRE con cada remoto
    - No apto si mucho tráfico, o redundancia (varios routers en central)
  - Malla
    - Conexiones VPN entre todos (o parcial)
    - OK si pocas localizaciones con mucho tráfico entre ellas
  - Jerárquica
    - Híbrido, malla entre regionales y radial con periféricos

Aplicación VPN Acceso Remoto
Límite de la Red Empresarial

- Conexiones bajo demanda para usuarios móviles o domésticos, que no siempre necesitan estar conectados
- Dónde se inicia el túnel?
  - En el cliente: seguridad en toda la conexión, pero software que gestionar en el cliente
  - Servidor de acceso a red, NAS: VPN reside en el ISP, sin software, pero sin seguridad en la conexión al NAS
- Según SAFE, conexiones VPN terminan en una sección VPN en el módulo de Internet
  - Uno o más concentradores de VPN entre router acceso a VPN y el de acceso a la red del campus
  - También Autenticación, Autorización y ContAbilidad (AAA), IDS e IPS en esa sección

Aplicación VPN Acceso Remoto
Límite de la Red Empresarial



Proveedor de Servicio
Límite de la Red Empresarial

- La red empresarial se conectará al módulo límite del proveedor servicio
- Aunque no diseñaremos ese módulo, entenderlo y seleccionar al proveedor adecuado

    - Pequeños, normalmente ofreciendo conexiones inalámbricas a usuarios finales
    - Especializados en hosting, sin usuarios finales
    - Interconectar ISPs en lugar de empresas o usuarios finales
- ISP Nivel 1 - 5 (*Tier*): globales - locales
- Tránsito pagado o libre
- Analizar requisitos y topología a extender para elegir el nivel de ISP necesario, y disponibilidad

5.6. Diseño de Topologías de Red Seguras

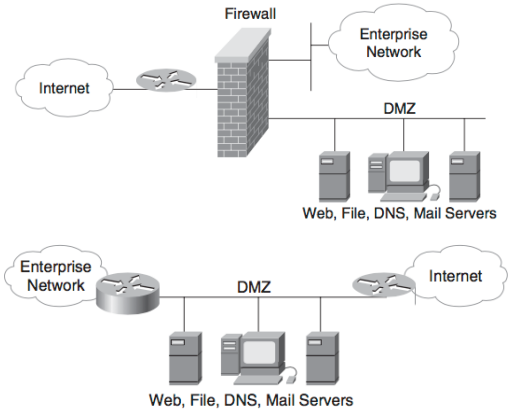
Topologías de Diseño de Red Seguras

- Poner la seguridad en relación con las topologías
- La seguridad física puede afectar al diseño lógico
    - Instalaciones de acceso restringido para el CPD

Topologías de Cortafuegos
Topologías de Diseño de Red Seguras

- *Cortafuegos* es un sistema o combinación de ellos que establece un límite entre redes
    - Colocado en la topología de red de forma que el tráfico exterior deba atravesarlo para llegar a la red protegida
- *Política de seguridad* determina el tráfico autorizado a atravesar el cortafuegos
- Router en la conexión WAN - LAN, util con políticas de seguridad sencillas implementables con ACLs
- *Bastión*, sistema seguro que soporta un número limitado de aplicaciones para usuarios externos
- DMZ con bastiones para servidores (HTTP, SMTP, DNS, FTP) para proteger datos privados y ofrecer datos públicos
    - Router - Firewall - (DMZ, LAN)
    - Router - DMZ - Router

Topologías de Cortafuegos
Topologías de Diseño de Red Seguras



6. Modelos de Diseño para Direcciones y Nombres

Asignación de Direcciones y Nombres

- Asignar nombre y dirección de red a cada dispositivo
- Modelo estructurado de direcciones y nombres
- Políticas y procedimientos
  - Fijar procedimiento y distribuir autoridad
- Dependencias
  - Estructura organización (departamentos, sedes, . . .)
  - Topología y jerarquía (límite de subredes)
- Puede afectar a los protocolos de encaminamiento a elegir

6.1. Guía para Asignar Direcciones de Red

Líneas Guía para Asignar Direcciones de Red

- Procedimiento asignación direcciones planeado, gestionado y documentado
  - Modelo estructurado
  - Dejar espacio para crecer
  - Asignar bloques en modo jerárquico
  - Según red física, no por pertenencia a grupos

- Si fuera posible, delegar autoridad
- Direccionamiento dinámico para sistemas finales
- Direcciones privadas + NAT

Modelo Estructurado

- *Modelo estructurado para direcciones*: las direcciones son significativas, jerárquicas y planeadas
- *Subnetting*
- Facilita gestión, resolución de problemas, optimización y seguridad
  - `a.b.c.d` → host `d`, departamento `c`, sede `b`, organización `a`
- Sin modelo estructurado
  - Direcciones duplicadas
  - Direcciones ilegales sin encaminamiento posible
  - Sin direcciones suficientes
  - Direcciones no asignables, desperdiciadas

Autoridad Central

- Modelo global de asignación de direcciones
  - Números de red para core
  - Bloques o subredes para distribución y acceso
- Direcciones públicas o privadas
  - Cuántos hosts necesitan ser visibles en la red pública?
  - Cuántos hosts sólo acceden a la red privada?
  - Dónde se realizará la traducción?
  - Dónde estará el límite entre red pública/privada
- *Internet Assigned Numbers Authority* IANA, *Regional Internet Registries*, RIR (ARIN, RIPE NCC, APNIC, LACNIC, AfriNIC)
- *Espacio de direcciones independiente de proveedor* asignado directamente por un RIR, si justificado por número hosts
- *Espacio de direcciones dependiente de proveedor* para hosts accesibles públicamente (resto dir. privadas)

Distribución Autoridad Direcciones

- Quién implementará el modelo?
- Si administradores inexpertos
  - Sencillez y minimizar esfuerzo configuración (DHCP)
  - No delegar autoridad para asignar direcciones y nombres
- Mantener el control ayuda a evitar errores que causen fallos en la red
  - Direcciones IP duplicadas

Direcciones Dinámicas para Hosts

- Asignación dinámica de direcciones reduce esfuerzo configuración
- Host puede aprender automáticamente sobre el segmento de red
- Combinación direcciones estáticas y dinámicas
  - Estáticas: servidores, routers, sistemas administración, switches, módulos e-commerce, Internet, VPN/acceso remoto y WAN
  - Dinámicas: estaciones de trabajo, teléfonos IP
- Criterios
  - Si número de hosts > 30
  - Renumeración
  - Alta disponibilidad
  - Seguridad
  - Seguimiento direcciones
  - Parámetros adicionales

DHCP

- Cliente/servidor (*broadcast*, dominio difusión)
- Métodos
  - Asignación dinámica de cualquier IP de un rango por un tiempo
  - Asignación automática de la misma IP de un rango a un cliente
  - Asignación manual (estática) de IP según administrador
- Asigna una dirección a un cliente por un periodo de tiempo extensible (*lease*), reutilización

- Detectar asignaciones duplicadas
  - Servidor envía `ping`
  - Cliente ARP gratuito
- Router como agente *relay* (Cisco *Ip Helper*)
- Alternativas:
  - Autoconfiguración IPv6
  - Zeroconf

Direcciones IP Privadas

- Direcciones públicas necesarias para servidores accesibles desde el exterior, no para host o redes internas
- NAT permite el acceso desde el exterior a servidores con direcciones privadas
- No necesario coordinación con ISP o RIR
- IETF reserva redes privadas (RFC 1918)
  - `10.0.0.0` – `10.255.255.255`
  - `172.16.0.0` – `172.31.255.255`
  - `192.168.0.0` – `192.168.255.255`

Direcciones IP Privadas

Los beneficios pesan más que los inconvenientes

- Ventajas
  - Seguridad, dirs IP no anunciadas a Internet
  - Adaptabilidad cambios ISP
  - Permite anunciar a Internet sólo una dir IP
  - Reservar dirs IP públicas para servidores
- Inconvenientes
  - Dificulta administración remota
  - Dificulta comunicación con socios, extranets
  - Dificulta fusión entre compañías
  - Facilita olvidar el modelo estructurado y jerárquico

***Network Address Translation*, NAT**

- Traducción entre direcciones de red interna y externa (RFC 3022)
- Útil con direcciones privadas
- Asigna una dirección entre un *pool* de disponibles
- Si sólo una, entonces PAT (*Port Address Translation*)
- Todo el tráfico entre empresa e Internet cruza por pasarela NAT
  - Asegurar prestaciones suficientes (video o voz)
  - Comprobar funcionamiento correcto (prueba piloto)

6.2. Modelo Jerárquico de Asignación de Direcciones

Modelo de Asignación de Direcciones Jerárquico

- Aplicar estructura a la dirección de red
  - Parte izquierda, grupos de nodos
  - Parte derecha, nodos individuales
- Facilita el encaminamiento jerárquico, agregación de direcciones en el intercambio de tablas de encaminamiento, mejora prestaciones, estabilidad, consume menos recursos (CPU, memoria, ancho de banda)
- Facilita VLSM (*Variable–Length Subnet Masking*)

Encaminamiento Jerárquico

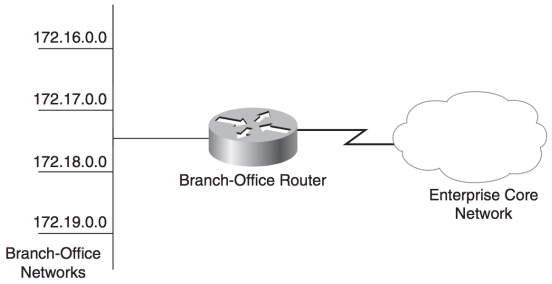
- Conocimiento de la topología y configuración de la red es local
- Ningún router conoce cómo alcanzar cualquier segmento de red
- Requiere de asignación jerárquica de direcciones
- Evolución hacia CIDR (*Classless InterDomain Routing*, `10.1.0.1/16`) desde el direccionamiento con clases (A, B o C)

Clase	Primeros bits	Prefijo
A	`0`	8 bits
B	`10`	16 bits
C	`110`	24 bits

- Protocolos encaminamiento soportan CIDR: RIPv2, EIGRP, OSPF, BGP, IS-IS
- RIPv1, IGRP sólo soportan direccionamiento con clases

Agregación de Rutas

- Si direcciones jerárquicas, CIDR agrega subredes a una única ruta reduciendo tamaño tablas encaminamiento y sobrecarga procesamiento, ancho de banda comunicación inter–routers



- Subredes resumidas como 172.16.0.0/14
  - `10101100 00010000`
  - `10101100 00010001`
  - `10101100 00010010`
  - `10101100 00010011`

Agregación Rutas

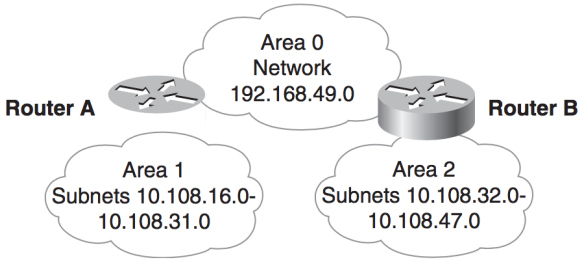
- Requisitos
  - Varias direcciones IP deben compartir los bits más a la izquierda
  - Routers deben basar su decisiones encaminamiento en la dirección de 32 bits y un prefijo de hasta 32 bits de longitud
  - Protocolos de encaminamiento deben poder transportar tanto las direcciones IP como el prefijo
- Pueden agregarse si
  - El número de subredes a resumir debe ser potencia de 2
  - El byte relevante en la primera dirección de red en el bloque a resumir debe ser un múltiplo del número de subredes

Agregación Rutas

Subredes	Byte 3	Máscara	Ruta resumida
192.168.32.0	00100000	22	192.168.32.0/22
192.168.33.0	00100001	22	
192.168.34.0	00100010	22	
192.168.35.0	00100011	22	
192.168.36.0	00100100	22	192.168.36.0/24

Subredes No Contiguas

- La agregación obliga que las subredes sean contiguas
- Con RIP v1 tanto A como B anuncian 10.0.0.0 y se ignoran
- Utilizar protocolos encaminamiento sin clases (OSPF, EIGRP)



6.3. Diseño de un Modelo de Nombres

Diseño de un Modelo de Nombres

- Múltiples tipos de recursos en una red: routers, servidores, hosts, impresoras, etc. accesibles por nombre, no por dirección de red
- Diseñar modelos de nombres que cumplan con los objetivos de usabilidad, gestionabilidad, prestaciones y disponibilidad
- Relación dirección–nombre, ya bien dinámica (protocolo) o estática (archivo)
- Consideraciones
  - Tipos de entidades a nombrar
  - Estructura del nombre
  - Cómo se almacenan, gestionan y acceden?
  - Quién los asigna?
  - Cómo aprender los host su nombre?
  - Si servidores, redundancia necesaria?

Autoridad de Nombres Distribuida

- Quién asignará nombres?
  - Espacio nombres controlado por una autoridad central o algunos nombres dados por agentes (descentralizadamente)?
  - Departamento IS dará nombres para oficinas regionales o sucursales, o los administradores departamentales darán nombres en esos sitios?

    - Usuarios darán nombres a sus sistemas o serán fijados por administradores de red?
- Si se comparten políticas, la asignación distribuida de nombres tiene ventajas

Guía para Asignar Nombres

- Nombres cortos, unívocos, distintivos y con significado
- Incluir prefijo o sufijo indicando el tipo: rtr, sw, svr, etc.
- Código de localización: va, pa, sg, so
- Evitar caracteres especiales, con posible significado para algún protocolo
- No distinguir MAYUSCULAS/minúsculas, ya que dificulta memorización
- Sin espacios
- 8 caracteres
- Nombre único aunque varias interfaces de red/direcciones IP
- Excepción: nombres fácilmente reconocibles por usuarios, también por atacantes

Asignación de Nombres en Entorno IP

- Archivos `/etc/host.conf`, `/etc/hosts`, servidores DNS y NIS (*Network Information Service*)
- Tanto NIS como DNS permiten gestión centralizada de nombres con servidores distribuidos
- DNS es una base de datos distribuida para un sistema de nombres jerárquico: `hostname.domainname`
    - Cliente/Servidor
    - Cada nivel jerárquico tiene delegada la autoridad y es gestionado autónomamente en cada nivel
    - DDNS, DNS dinámico, permite asignar un nombre estático a una dirección IP dinámica

7. Selección de Protocolos de Encaminamiento y Conmutación

Selección de Protocolos de Encaminamiento y Conmutación

- Seleccionar los protocolos adecuados según
  - Características de tráfico
  - Uso de CPU, memoria y ancho de banda
  - Número de routers o switches
  - Capacidad adaptación a cambios
  - Características de seguridad
- Idea aproximada de topología de red y dónde estarán routers y switches, pero sin determinar detalles
- Conocer protocolos ayuda a seleccionar el mejor producto

7.1. Decisiones en el Proceso de Diseño Descendente

Decisiones en el Proceso de Diseño Descendente

- Para tomar una buena decisión, hay que tener una lista de objetivos
- Tabla de decisión, enfrentando protocolos con los objetivos
- Seleccionada una opción, qué puede salir mal?
- Plan contingencia?

Tabla de Decisión
Decisiones en el Proceso de Diseño Descendente

	Objetivos Críticos			**Otros Objetivos**		
	Obj 1	Obj 2	Obj 3	Obj 4	Obj 5	Obj 6
BGP	X	X	X	8	7	7
OSPF	X	X	X	8	8	8
IGRP	X	X		8	6	5
RIP			X			

- Marcar cumplimiento Objetivos
  - Totalmente, X
  - Parcialmente, 0-10

7.2. Selección de Protocolos de Conmutación

Selección de Protocolos de Conmutación

- Switches, dos modos de funcionamiento
  - *almacenamiento y reenvío*, *store–and–forward*, recibe paquete, lo procesa y reenvía
  - *directo*, *cut–through*, conmuta paquete según se recibe, más rápido pero puede propagar paquetes ilegales (con errores CRC o diminutos)
  - algunos switches pueden combinar ambos: *cut–through* adaptativo dependiendo de la tasa de errores
- Múltiples caminos de conmutación simultaneos, dependiendo de la malla de interconexión
- Estados: bloqueado, escucha, aprendizaje, reenvio

Almacenamiento y Reenvío

- Dispositivo almacenamiento–y–reenvío
  - Recibir completamente el marco
  - Determinar el puerto de salida
  - Preparar el marco para el puerto de salida
  - Calcular CRC
  - Transmitir el marco por el puerto de salida cuando el medio de transmisión esté libre

Conmutación y las Capas OSI

- Conmutador, *switch*, se refiere a un dispositivo que opera en las capas OSI 1 y 2
- *Conmutar*: mover datos de una interfaz a otra
  - *Hub* ethernet, repetidor que conmuta bits de una interfaz a todas las demás
  - Switch ethernet, *bridge* multipuerto de alta velocidad que conmuta marcos basado en la dirección destino de la capa 2
  - *Router*, conmutador de paquetes (datagramas) basado en la dirección destino de la capa 3
  - Switch de capa 3, router de alta velocidad que incluye interfaces que pueden tomar decisiones de reenvío basadas únicamente en información de la capa 2 (dispositivo de las capas 2 y 3)

Conmutación Transparente

- *Conmutación transparente* conecta dos o más segmentos LAN de modo que hosts se comunican sin percibir la presencia del switch
- Aprendizaje localización hosts basada en MAC origen de los marcos, *Tabla Conmutación MAC*
- *Filtrado* y *reenvio*
- *Inundación*, reenvio del marco recibido por todos los puertos excepto por el de entrada
    - MAC destino desconocida
    - MAC destino FF-FF-FF-FF-FF-FF (broadcast)
- Segmentan dominios de colisión, pero no de difusión
    - Problemas de escalabilidad si encadenamiento switches
    - Utilizar routers o VLANs para segmentar

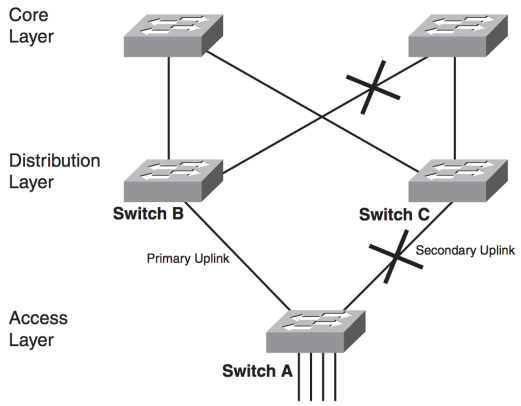
Mejoras en Spanning Tree

- RSTP, IEEE 802.1w, incluído ya en IEEE 802.1D
- Agregación VLANs sobre STP, IEEE 802.1s
- *PortFast*
    - Sólo en *puertos límite* del switch, sin otros switches conectados
        - Automáticamente a estado reenvio, sin pasar por estados previos (bloqueo, escucha, aprendizaje)
        - Riesgo de que se conecte otro switch, y deje de ser el último
        - `BPDU Guard`, deshabilita PortFast si detecta BPDUs

Mejoras en Spanning Tree

- *UplinkFast, BackboneFast* mejora la convergencia de STP si falla enlace redundante en switch acceso hacia distribución
    - UplinkFast se recupera en 1 seg, mientras STP por defecto, 30 - 50 s
    - UplinkFast sólo en switches de acceso
    - BackboneFast recorta en hasta 20 s la recuperación de un switch de un fallo indirecto en un puerto no local (pasar a estado escucha inmediatamente, sin esperar temporizadores)
- Detección de enlaces unidireccionales, *Unidirectional Link Detection*, UDLD
    - Fallos en cable conexión
    - SW A ve SW B, pero SW B no ve SW A (BPDUs)
    - Produce ciclos

Switch acceso con 2 UpLinks



Mejoras en Spanning Tree

- *LoopGuard*
  - Protección adicional anti-ciclos
  - Evita que un puerto bloqueado pase a estado aprendizaje y reenvío por error, al dejar de recibir BPDUs
  - Pasa a un estado añadido llamado estado-inconsistente-por-ciclo, del que sale cuando recibe BPDUs de nuevo
- STP LoopGuard o UDLD, o ambos

Protocolos Transporte Información VLAN

- Con VLANs, asegurarse de que el tráfico intraVLAN alcanza las interfaces correctas
  - IEEE 802.1Q, añade campos al marco IEEE 802.3
  - ISL encapsula el marco IEEE 802.3 en uno nuevo
  - Interacción con STP (802.1Q un árbol para todas las VLANs, ISL uno por VLAN)
- *Dynamic Trunk Protocol* permite SW negociar 802.1Q con otro extremo
  - Problemas si un lado en trunk y el otro no
  - Estados `on`, `off`, `desirable`, `auto`, `nonegotiate`
  - Si los dos SWs soportan DTP, poner ambos lados `desirable`

Protocolos Transporte Información VLAN

- Configuración y gestión de VLANs, *VLAN Trunking Protocol*, VTP
  - Gestiona adición, borrado y renombrado de VLANs en una red de campus de forma automática
  - 3 modos: servidor (por defecto), cliente y transparente
    - servidor (por defecto), actulaliza BD VLANs y reenvía
    - cliente, aprende, reenvía pero no modifica BD
    - transparente, no aprende, pero reenvía anuncios VTP
  - Dominios VTP para redes grandes

7.3. Selección de Protocolos de Encaminamiento

Selección de Protocolos de Encaminamiento

- Objetivo general: compartir información sobre accesibilidad entre routers
- Diferentes enfoques, tipo información intercambiada, dinamismo, eficiencia, escalabilidad
- Dos grandes clases:
  - Vector de distancias: RIP v1, RIP v2, IGRP, EIGRP, BGP
  - Estado de enlace: OSPF

7.3.1. Protocolos Vector de Distancias

Protocolos Vector de Distancias

- Envía su tabla encaminamiento completa (o actualizaciones) a sus vecinos (broadcast)
- Contador de saltos (*hop count*), número de routers (a veces son enlaces) a atravesar para alcanzar destino

Red	Distancia (saltos)	Enviar a (siguiente salto)
10.0.0.0	0	Puerto 1
172.16.0.0	0	Puerto 2
172.17.0.0	1	172.16.0.2
172.18.0.0	2	172.16.0.2
192.168.1.0	1	10.0.0.2
192.168.2.0	2	10.0.0.2

Horizonte Dividido

- *Horizonte dividido*, *Split-Horizont*, router sólo envía rutas que son accesibles vía otros puertos
  - Reduce tamaño tablas compartidas
  - Mejora la precisión de la información
- No envía información a otros routers que pueden aprender por si mismos

Horizonte Dividido

- *Bloqueo*, *Hold-Down*, no añadir una ruta o actualizar información de una ruta recién eliminada hasta que expire un temporizador (*count-to-infinity*)
  - Evita ciclos durante *convergencia*

Router A's Routing Table

Network	Distance	Send To
172.16.0.0	0	Port 1
192.168.2.0	1	Router B

Router B's Routing Table

Network	Distance	Send To
192.168.2.0	0	Port 1
172.16.0.0	1	Router A

Envenamiento de Ruta

- *Envenenamiento de ruta*, *route poisoning*, envía un anuncio a indicando un número de saltos infinito (16 en RIP) hacia ese destino
- Evita ciclos y acelera convergencia
  - Cuando un router aprende una ruta de otro router, le responde devolviéndole una actualización determina que una ruta ya no es válida (evita problema cuenta al infinito)
  - Si un router cae, su vecino avisa al resto

7.3.2. Protocolos de Estado de Enlace

Protocolos de Estado de Enlace

- Intercambian información sobre los enlaces a los que está conectado un router
- Los routers aprenden a partir de la información de sus vecinos
  - No intercambian tablas de encaminamento

    - Hello entre vecinos, *adyacencia*
    - Todos los routers acaban teniendo el mismo conocimiento de la red, grafo
- Algoritmo Dijkstra, camino más corto
- Consumen más CPU y memoria que los de vectores de distancias
- Menos propensos a bucles, y convergencia más rápida

7.3.3. Selección de Protocolos de Encaminamiento

Selección de Protocolos de Encaminamiento

- Utilizar protocolos vector de distancias:
    - Red sencilla, topología plana sin diseño jerárquico
    - Topología sencilla con concentrador único
    - Administrador sin conocimientos para algoritmo de estado de enlace
    - Tiempos de convergencia no son un problema

Selección de Protocolos de Encaminamiento

- Utilizar protocolos estado de enlace:
    - Redes grandes según diseño jerárquico
    - Administrador con conocimientos para algoritmo de estado de enlace
    - La convergencia rápida es requisito

Métricas

- Las métricas son utilizadas para determinar la ruta preferida
    - número de saltos
    - retardo, ancho de banda, fiabilidad, etc.
- Afectan a la escalabilidad y las prestaciones

Jerárquicos vs No Jerárquicos

- Sin jerarquía, todos los routers con las mismas tareas
- Jerárquicos, agrupan routers según tareas (AS, dominios)
- Resumen de rutas, estabilidad, independencia de problemas en otras áreas

Interior vs Exterior

- Interior, dentro de un AS: RIP, OSPF, EIGRP
- Exterior, entre ASs: BGP

Con Clases vs Sin Clases

- Con clases (RIP, IGRP) siempre se tiene en cuenta la clase para resumir rutas, cuidado con subredes discontiguas o VLSM
- Sin clases, la máscara se traslada con la dirección IP, soportando subredes discontinuas y VLSM

Espacio direcciones IP debería ser distribuido de modo que subredes ocupen bloques contiguos, permitiendo su resumen en los límites de las áreas

Dinámico vs Estático y por Defecto

- *Ruta estática* configurada de forma manual, no se actualiza por ningún protocolo encaminamiento
  - Cuando no es necesario protocolo encaminamiento: red que no permite ir más allá (*stub*), pe. compañía conectada internet con un único enlace
  - Requiere trabajo administrativo, manual, reduce consumo recursos y son fáciles de arreglar pero pierde información sobre encaminamiento (fallos, caídas) y no optimiza
  - Control sobre la ruta que sigue el tráfico, seguridad
  - Precedencia sobre rutas dinámicas hacia mismo destino
- *Ruta estática flotante*, mayor distancia administrativa que rutas dinámicas, se emplea cuando no hay información dinámica
- *Ruta por defecto*, si no existe ruta hacia un destino, último recurso, pe. salida a internet

Restricciones de Escalabilidad

- Existen límites a la métrica?
- Rapidez de convergencia ante cambios?
- Frecuencia de transmisión de actualización en tablas o anuncios de estado de enlace?
- Cantidad de datos transmitidos en una tabla de encaminamiento?
- Ancho de banda consumido para enviar tablas?

- Alcance de distribución de las tablas?
- CPU necesaria para procesar tablas o anuncios de estado de enlace?
- Soportadas rutas estáticas y por defecto?
- Soportado el resumen de rutas?

Convergencia

- *Convergencia* es el tiempo que tardan los routers en entender consistentemente la topología tras un cambio
- Durante la convergencia, paquetes pueden no ser encaminados correctamente al destino
- Frecuencia de los cambios (caídas)?
- Aplicaciones sensibles al tiempo (VoIP)?
- Protocolos estado de enlace convergen más rápidamente que los de vectores de distancia
- Mensajes *keepalive*, *hello*
- Con reparto de carga mejora la convergencia

7.4. Encaminamiento IP

Encaminamiento IP

- RIP
- EIGRP
- OSPF
- IS-IS
- BGP

7.4.1. RIP

Routing Information Protocol, RIP

- Primer protocolo encaminamiento en TCP/IP (1980's)
- En redes antiguas y por su simplicidad y la facilidad para resolver problemas
- Difunde tabla cada 30 s., con hasta 25 rutas por paquete, problemas si red grande y enlaces pequeños

- Número saltos como métrica única (≤ 15) para distancia a destino
- RIPv1 con clases, RIPv2 sin clases
- RIPv2
  - Añade campos a la tabla de encaminamiento v1
    - *route tag*, facilita combinar RIP y no-RIP
    - máscara de subred
    - siguiente salto, IP del siguiente salto en dirección al destino (`0.0.0.0`)
  - Autenticación simple mediante contraseña en texto plano

7.4.2. EIGRP

Enhanced Interior Gateway Routing Protocol, EIGRP

- IGRP, vector de distancias alternativa a RIP
- (1990s) EIGRP métrica compuesta
  - Ancho de banda
  - Retardo
  - Fiabilidad
  - Carga
- Equilibrado de carga sobre caminos con métrica igual y desigual (tráfico proporcional a la métrica)
- Mejor selección de la ruta por defecto
- Convergencia mejorada mediante actualizaciones por *triggers*, olas de actualizaciones
- Anuncios de vectores de distancia no periódicos, parciales y de alcance limitado
- Menos consumo ancho de banda

7.4.3. OSPF

Open Shortest Path First, OSPF

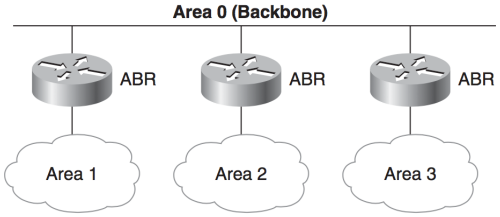
- Protocolo estado enlace para superar limitaciones RIP
  - Estándar abierto
  - Convergencia rápida
  - Protocolo autenticación
  - Soporta redes discontiguas y VLSM

    - Multidifusión

- Minimiza consumo ancho de banda enviando anuncios estado enlace sólo ante cambios (sincro BD/30 m., Hellos/10 s.)
- Coste de ruta asignado a mano (100 Mbps/ancho de banda)
- Si varias rutas con el menor coste, distribución de tráfico entre ellas
- Buena elección por bajo consumo de ancho de banda, escalabilidad y compatibilidad entre fabricantes

Arquitectura OSPF

- OSPF permite agrupar redes en áreas, ocultándose los detalles entre sí (resumibles)
- Reducción del tráfico de encaminamiento, uso memoria y CPU en routers
- Area O, a la que se conectan el resto mediante *Area Border Router* (ABR)
- Conexión a otro AS o red no OSPF mediante *Autonomous System Boundary Router* (ASBR)



7.4.4. IS-IS

Intermediate System-to-Intermediate System, IS-IS

- Protocolo estado enlace no muy popular OSI-IP para grandes redes jerárquicas (ISP)
- Similar a OSPF, también jerárquico.
    - Routers Nivel 1, encaminan intra área
    - Routers Nivel 2, encaminan entre áreas
- El límite área en el enlace, todas interfaces de un router en el mismo área (diferencia con OSPF)

7.4.5. BGP

Border Gateway Protocol, BGP

- Reemplaza a Exterior Gateway Protocol, EGP
  - Internal BGP (iBGP), gran compañía para encaminar entre dominios
  - External BGP (eBGP), encaminar entre compañías y participar en el encaminamiento global de Internet
- eBGP utilizado en conexión *multihomed*
- Su uso requiere del conocimiento de la complejidad de Internet
- eBGP sólo en routers con mucha memoria, CPUs rápidas y una conexión de alta capacidad a Internet

7.4.6. Combinación Múltiples Protocolos en una Misma Red

Protocolos de Encaminamiento en Modelo Jerárquico

- Núcleo: EIGRP, OSPF, IS-IS
  - OSPF impone diseño jerárquico estricto y correspondencia areas – dir. IP
  - EIGRP es propietario Cisco
- Distribución: RIPv2, EIGRP, OSPF, IS-IS
  - Distribución entre protocolos encaminamiento núcleo y acceso
- Acceso: RIPv2, EIGRP, OSPF
  - OSFP supera normalmente las capacidades de los dispositivos en esta capa
  - También encaminamiento estático

Redistribución entre Protocolos Encaminamiento

- Permite que los routers ejecuten más de un protocolo de encaminamiento y compartir rutas entre protocolos
- Puede produce ciclos y dificultar resolución problemas
- Util para conectar distintas capas, migrar a nuevos protocolos, entornos mixtos
- Configurar especificando qué protocolos deberían insertar información en tablas encaminamiento de otros protocolos
- Determinar los protocolos a utilizar en cada *dominio de encaminamiento* (routers que comparten información mediante un protocolo de encaminamiento) y los límites

Redistribución entre Protocolos Encaminamiento

- Redistribución en uno o dos sentidos
  - Un sentido, apoyado por ruta por defecto o estáticas (jerárquico)
  - Dos sentidos, filtrado para limitar el alcance de la información
- Métricas incompatibles, conversión
- Distancias administrativas
  - Un router aprenda una ruta a través de más de un protocolo
  - *Distancia administrativa* indica preferencia de rutas entre protocolos
- Ruta estática flotante

Distancias Administrativas

Origen de la Ruta	Valor Distancia por Defecto
Interfaz conectada	0
Ruta estática	1
Ruta resumida EIGRP	5
eBGP	20
EIGRP interna	90
OSPF	110
IS-IS	115
RIP	120
EIGRP externa	140
iBGP	200
Desconocido	255

7.5. Resumen Protocolos Encaminamiento

Resumen Protocolos Encaminamiento

	VD/EE	Int/Ext	Clases	Métrica	Escala	Conv	Recursos	Seg	Dific
RIPv1	VD	Int	Clases	Contador saltos	15 saltos	Puede ser grande	Mem y CPU: bajo, AdBanda: grande	No	Fácil
RIPv2	VD	Int	CIDR	Contador saltos	15 saltos	Puede ser grande	Mem y CPU: bajo, AdBanda: grande	Si	Fácil
IGRP	VD	Int	Clases	AdBanda, retardo, fiabilidad, carga	255 saltos	Rápido	Mem y CPU: bajo, AdBanda: grande	No	Fácil
EIGRP	VD	Int	CIDR	AdBanda, retardo, fiabilidad,carga	1000s routers	Muy rápido	Mem: moderado, CPU y AdBanda: bajo	Si	Fácil

Resumen Protocolos Encaminamiento

	VD/EE	Int/Ext	Clases	Métrica	Escala	Conv	Recursos	Seg	Dific
OSPF	EE	Int	CIDR	Coste (100M/Mbps)	100s routers/área, 100s áreas	Rápido	Mem y CPU: alto, AdBanda: bajo	Si	Moderado
BGP	VC	Ext	CIDR	Configurable	1000s routers	Rápido	Mem y CPU: alto, AdBanda: bajo	Si	Moderado
IS-IS	EE	Int	CIDR	Camino, retardo, precio y errores	100s routers/área, 100s áreas	Rápido	Mem y CPU: alto, AdBanda: bajo	Si	Moderado

7.6. Resumen

Resumen

- Selección del protocolo adecuado para conmutación y encaminamiento
- Ayuda a la posterior selección del dispositivo concreto
- Repaso de STP y combinación con VLANs
- Distintos protocolos de encaminamieto

8. Estrategias de Seguridad

Estrategias de Seguridad

- Proteger todas las partes de una red sin limitar la facilidad de uso y las prestaciones
- Servidores públicos, extranet para socios, acceso remoto desde casa
- Enfoque descendente sistemático que establece la planificación y la política antes que los productos de seguridad
- La seguridad como un objetivo transversal

8.1. Diseño de Seguridad de Red

Diseño de la Seguridad de la Red

1. Identificar activos de red
2. Analizar riesgos
3. Analizar requisitos y compromisos
4. Desarrollar un plan seguridad
5. Definir política seguridad
6. Procedimientos para aplicar políticas

7. Desarrollar e implementar estrategia técnica y procedimientos seguros
8. Aceptación usuarios, gestores y técnicos
9. Formación
10. Implementación
11. Probar y actualizar
12. Mantenimiento

Identificar Activos de Red

- Identificar los *activos de red*, el riesgo de sabotaje o acceso inapropiado y sus efectos
    - Hosts, dispositivos de red (routers, switches), datos que atraviesan la red, propiedad intelectual, secretos, reputación

Analizar Riesgos

- Riesgos, desde intrusos hostiles hasta usuarios descuidados y no formados
- Robo de datos, modificación de datos, denegación de servicio (*Denial-of-Service*, DoS)

Analizar Requisitos y Compromisos

- Seguridad como requisito ya considerado en el análisis hecho
- En general, considera la protección de activos
    - Confidencialidad de los datos
    - Integridad de los datos
    - Disponibilidad de sistema y datos
- El *coste* de protegerse contra amenazas no debería superar al de recuperarse de un ataque
- Compromisos: objetivos seguridad vs asequibilidad, usabilidad, rendimiento y disponibilidad
    - Incremento tareas administrativas
    - Reducción prestaciones
    - Limitación redundancia y balanceo de carga

Desarrollar un Plan

- *Plan de seguridad* documento de alto nivel que propone el modo en que una organización va a cumplir con los requisitos de seguridad
- Debe referirse a la topología de red y los servicios proporcionados
- Especifica tiempo, personal y otros recursos requeridos para desarrollar e implementar una política de seguridad
- Decidir qué servicios son necesarios
- Evitar estrategias seguridad complejas, difíciles de implementar y acarrean agujeros inesperados
- Implicación universal

Definir Política Seguridad

- *Política de seguridad* reglas que deben cumplir las personas a las que se les da acceso a la tecnología y a los activos de información de una organización
- Informa a usuarios, gestores y técnicos de sus obligaciones para proteger los activos (datos y tecnología)
- Especifica los mecanismos por los que se alcanzarán esas obligaciones
- Aceptación universal
- Documento vivo en respuesta a cambios en la organización
    - Política de acceso, que defina derechos de acceso y privilegios
    - Política de responsabilidad, qué hacer y a quién contactar
    - Política de autenticación, establecimiento contraseñas efectivas, acceso remoto
    - Política de privacidad, respecto a monitorización comunicaciones y acceso a archivos
    - Política de adquisición y configuración, de equipamiento de acuerdo a política de seguridad

Procedimientos de Seguridad

- Procedimientos para implementar las políticas de seguridad
    - Configuración
    - Acceso
    - Auditoría
    - Mantenimiento

- Documento escrito
- Especificar cómo gestionar incidentes
- Difundidos en cursos de formación

Mantenimiento

- Revisar continuamente para ver si cumple con su objetivo
  - Auditorías, Registros
  - Respuesta a incidentes
  - Lectura de literatura y informes agencias de seguridad
  - Pruebas
  - Formación administradores seguridad
  - Actualización plan de seguridad
- *Rueda de la seguridad*

8.2. Mecanismos de Seguridad

Mecanismos de Seguridad

- Algunos componentes típicos en los diseños de redes seguras
  - Seguridad física
  - Autenticación
  - Autorización
  - Auditoría
  - Encriptación de datos
  - Filtrado de paquetes
  - Cortafuegos
  - Sistemas de detección y prevención de intrusión

Seguridad Física

- Limitar el acceso a elementos clave de la red guardándolos en armarios
  - routers núcleo, puntos de demarcación, cableado, modems, servidores, hosts, almacenamiento de backup
- Protegerlos de desastres naturales y provocados por humanos
- Alimentación ininterrumpida, detección de fuego y alarma, sistemas de extinción de incendios, evacuación de agua, instalación en racks sujetos a pared o suelo
- Considerar seguridad física desde el principio para prever la construcción o instalación de mecanismos de seguridad

Autenticación

- Identificar quién o qué está solicitando servicios de red
- Basada en tres pruebas, mejor si están combinadas
  - Algo que el usuario conoce: contraseña
  - Algo que el usuario tiene: tarjeta identificación
  - Algo que el usuario es: huella dactilar
- *Autenticación doble factor*, doble prueba de identidad

Autorización

- Controla qué puede acceder una vez se ha accedido a los recursos de red: privilegios a usuarios o procesos
- Principio de *menor privilegio posible*
  - Difícil de concretar
  - Grupos y usuarios

Auditoría

- Recoger datos de la actividad en la red para su análisis
- Incluir intentos de acceso (autenticación y autorización), incluidos *anonymous* y *guest*
- Intentos de cambio de derechos de acceso
- Registros con marcas de tiempo
- Nunca incluir contraseñas
- Reforzar con *evaluación de seguridad* periódica por parte de expertos

Encriptación de Datos

- Manipular los datos para protegerlos de lecturas por parte de cualquiera excepto su legítimo destinatario
- Texto *cifrado* / *plano*
- Criptografía clave simétrica o pública
- Básico para proporcionar confidencialidad, también puede servir para autenticación
- Valorar su efecto en las prestaciones

Filtrado de Paquetes

- Se establecen en routers, cortafuegos, servidores para aceptar o denegar paquetes dependiendo de su dirección o servicio
- Dos políticas
  - Denegar ciertos tipos de paquetes específicos y aceptar el resto
  - Aceptar ciertos tipos de paquetes concretos y denegar el resto
- La segunda opción es más fácil de implementar, más segura y sencilla de probar
- *Access Control Lists*, ACLs
  - `deny-all` implícita al final

Cortafuegos

- Refuerzo de las políticas de seguridad en el límite entre dos o más redes
- Especialmente importante entre la red empresarial e Internet
- Filtrado de paquetes con o sin estado
- Pasarelas de aplicación (*proxies*) para seguimiento de sesiones con servidores externos

Detección/Prevención de Intrusión

- Análisis del tráfico y detección de eventos maliciosos (firmas) y comunicación al administrador
- Protege incluyendo reglas en el cortafuegos o denegando paquetes
- En host o subred
- Tendencia a generar falsas alarmas

8.3. Diseño Modular de Seguridad

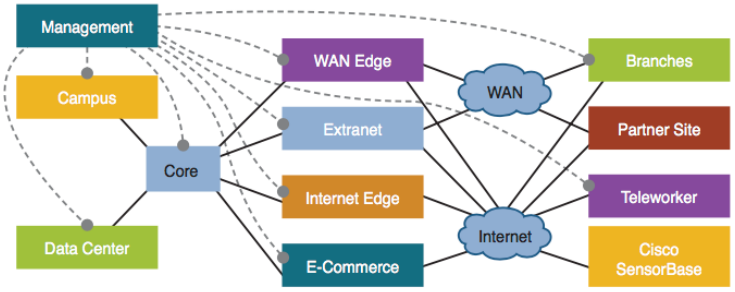
Diseño Modular de Seguridad

- Principio de *defensa en profundidad*
  - Multicapa, técnicas diferentes
  - Cada mecanismo debe tener su backup (*cinturón y tirantes*)
- El diseño de la seguridad además debe ser modular
  - Conexiones a Internet

- Acceso remoto y VPNs
- Servicios de red y gestión
- Granjas de servidores
- Servicios de usuarios
- Redes inalámbricas

Arquitectura CISCO de Seguridad SAFE

- El modelo de referencia CISCO SAFE trata la seguridad en cada módulo de la arquitectura de red



8.3.1. Conexión a Internet

Conexión a Internet

- Securizado con mecanismos solapados
  - Routers internet equipados con filtros
  - Apoyados por filtros en cortafuegos
- Monitorizada cuidadosamente
- Regla: una red empresarial debe tener entradas y salidas bien definidas
  - Mejor si sólo tiene una conexión a internet
  - Si varias por prestaciones o redundancia, sólo si están monitorizadas y gestionadas
- Bloquear conexiones entrantes, excepto hacia servicios en servidores públicos o si completan conexión iniciada por cliente interno
- Riesgos
  - Ataques de reconocimiento (filtrado, NAT)
  - Inyección de rutas (autenticación, rutas estáticas o por defecto)

8.3.2. Servidores Públicos

Servidores Públicos

- Servidores públicos: WWW, FTP, email, DNS, e-commerce
- En DMZ protegidos con cortafuegos
- Protección DoS, limitando el número de conexiones por periodo
- SOs fiables con los últimos parches de seguridad
- Manteniendo modularidad
    - En el host servidor Web (o FTP, email DNS, etc.) no corre ningún otro servicio
- E-Commerce
    - Gestionan información comercial y financiera sensible
    - Múltiples servidores
    - En DMZ propia separada

8.3.3. Acceso Remoto y VPNs

Acceso Remoto y VPNs

- Para permitir usuarios móviles, autenticación y autorización mediante RADIUS, CHAP
- RADIUS, el servidor de acceso es un cliente de BD con datos de autenticación y autorización
- Acceso mediante módem sobre líneas telefónicas debería estar muy restringido. Si es posible, siempre activar *callback*
- Para conectar sitios privados sobre redes públicas, usar VPNs
- Protegerse de la conexión de un cliente comprometido, para que el ataque no utilice la VPN
- Cliente con antivirus y cortafuegos personal
- Datos encriptados, normalmente mediante IPsec (confidencialidad, integridad de datos y autenticación)

8.3.4. Servicios de Red y de Gestión

Servicios de Red y de Gestión

- Proteger routers y switches
- Ejecutar sólo los servicios mínimos y conexiones con pares autenticados
- Necesario el uso de contraseñas para el acceso, sobre protocolos seguros (`ssh`), cambiando mensaje bienvenida por otro menos amistoso
- Limitar el uso de SNMP, especialmente si el comando `set` no es autenticado (sí lo es en SNMPv3)
- Hosts de administración especialmente protegidos ya que gestionan información sensible (SO reforzado con los últimos parches de seguridad, sin servicios innecesarios y con mecanismos de autenticación robustos)

8.3.5. Granjas de Servidores

Granjas de Servidores

- Soportan servicios y aplicaciones del negocio
- Accedidos por gran número de usuarios, priman prestaciones pueden limitar seguridad
- IDS en red y hosts para monitorizar redes y hosts individuales
- Filtros que limiten conectividad entre servidores
- SO con últimos parches de seguridad, clientes y servidores robustos
- Autenticación y autorización para acceso y administración de servidor
- Contraseña `root` de acceso controlado
- Evitar cuentas `guest`

8.3.6. Servicios de Usuario

Servicios de Usuario

- Política de seguridad estricta sobre qué aplicaciones se permiten instalar en los PC conectados a la red
- Cortafuegos y antivirus personal, actualizados
- Cerrar sesiones usuario cuando se abandone la mesa (apagar si fin jornada)
- Asegurarse que sólo se conectan interfaces de red permitidas a la red
- Protocolo 802.1X no permite la conexión a un puerto de un switch sin autenticación previa (y otros usos interesantes en redes inalámbricas)

8.3.7. Redes Inalámbricas

Redes Inalámbricas

- Colocar las redes inalámbricas en una subred y VLAN propias
  - Facilita movilidad, direcciones y filtrado
- Cortafuegos y antivirus personales y actualizados
- Pueden utilizar VPN para acceder a la red corporativa
- 802.1X, EAP, RADIUS, TLS, TTLS, PEAP, MD5, 802.11i (WPA), TKIP, WPA2

8.4. Resumen

Resumen

- Seguridad, preocupación principal en organizaciones cada vez más dependientes de la red y con incremento de ataques
- Seleccionar cuidadosamente tecnologías y productos, compromiso seguridad vs prestaciones
- Modularidad
- Defensa en profundidad, estrategias multicapa

9. Gestionabilidad de la Red

Gestionabilidad de la Red

- Gestionar la red es un requisito de diseño, no de operación
- Una red bien gestionada permite que alcance los requisitos de prestaciones, disponibilidad y seguridad
- Ayuda medir cómo se están consiguiendo los objetivos, y ajustar los parámetros de la red si no se alcanzan
- Facilita la escalabilidad
  - Ayuda a analizar el comportamiento actual de la red, aplicar actualizaciones de forma adecuada y resolver los problemas con actualizaciones

Visión General

Gestión de Redes
Conjunto de funciones para controlar, planificar, reservar, desplegar, coordinar y monitorizar recursos en redes de ordenadores

- Las redes son recursos cuya integridad debe ser medible y verificable
- Planificación de la arquitectura de gestión:
  - Elegir protocolo de gestión
  - Reconfiguración de la red para satisfacer requisitos
  - Monitorizar toda la red desde una localización o dispositivo
  - Monitorización proactiva
  - Acceso fuera-banda

9.1. Diseño de la Gestionabilidad de la Red

Diseño de la Gestionabilidad de la Red

- Considerar escalabilidad, patrones de tráfico, formato de datos y compromiso coste/beneficio: sistemas que pueden ser caros y afectar a las prestaciones
- El acto de observar puede alterar lo observado (*Principio de incertidumbre de Heisenberg*)
- Determinar qué recursos han de ser monitorizados
- Determinar las métricas para medir prestaciones
- Determinar qué y cuántos datos recolectar (y almacenar)

Gestión Proactiva de Red

- Comprobar la salud de la red durante funcionamiento normal, reconocer potenciales problemas, optimizar prestaciones y planear actualizaciones
- Los test pueden mostrar tendencias
- Requiere más herramientas y procesos de administración que la reactiva, a cambio de menores tiempos de caída

Modelo FCAPS de Gestión de Red

- ISO define los procesos de gestión de la red, *FCAPS*
  - Gestión de *F*allos
  - Gestión de *C*onfiguración
  - Gestión de cont*A*bilidad
  - Gestión de desem*P*eño
  - Gestión de *S*eguridad

Gestión de Fallos

- Detectar, aislar, diagnosticar y corregir problemas
- Informar del estado de fallo a usuarios y administradores
- Herramientas: monitorización, analizadores de protocolos, *help-desk*
- Simple Network Management Protocol, SMNP, y Remote Monitoring (RMON)

Gestión de Configuración

- Asiste al administrador en el seguimiento de los dispositivos de red y su configuración
- Inventario de activos, componentes hardware y versión de software
- Ayuda a la gestión del cambio

Gestión de Contabilidad

- Registra el uso de la red por parte de individuos o departamentos (incluso si no se factura)
- Facilita la asignación de costes asociados a la red
- Permite detectar abusos (intencionados o no)

Gestión de Desempeño

- Mide el comportamiento de la red y su efectividad
  - Extremo a extremo: prestaciones de la red (disponibilidad, capacidad, utilización, retardo y su variación, productividad, accesibilidad, tiempo de respuesta, errores y linealidad del tráfico)
  - Por componente: prestaciones de un dispositivo o enlace (productividad, uso de memoria y CPU, errores)
- Sondear localizaciones remotas para medir accesibilidad y tiempo de respuesta (ping)
- Medir flujos y volumen de tráfico
- Registrar cambios en rutas

Gestión de Seguridad

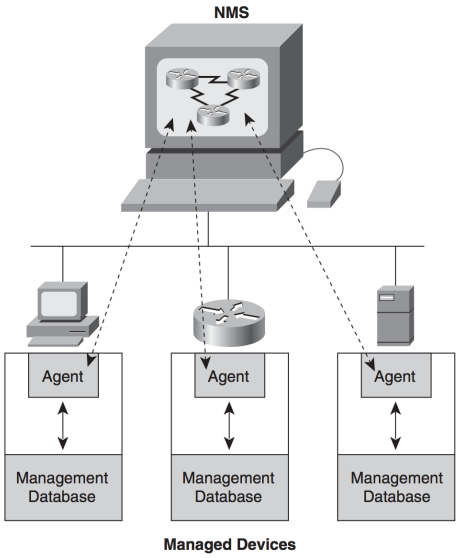
- Mantener y distribuir contraseñas y otra información de autenticación
- Generar, distribuir y almacenar claves de encriptación
- Recolectar, almacenar y examinar registros de auditoría de seguridad, *logs*
- Analizar configuraciones de routers y switches y comprobar que cumplen políticas de seguridad

9.2. Arquitectura de Gestión de Red

Arquitectura de Gestión de Red

- Una arquitectura de gestión de la red consiste en disponer dispositivos gestionados, agentes y sistemas de gestión dentro de la red
    - *Dispositivo gestionado*, nodo de la red que recoge y almacena información de gestión
    - *Agente*, software de gestión que reside en un dispositivo gestionado
    - *Sistema de Gestión de Red*, ejecuta aplicaciones que monitorizan y controlan dispositivos gestionados, comunicándose con los agentes y muestran la información de administración

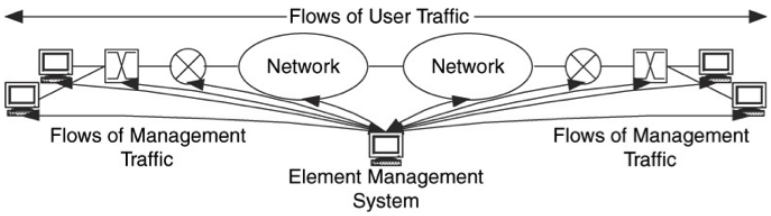
Componentes de Gestión de la Red



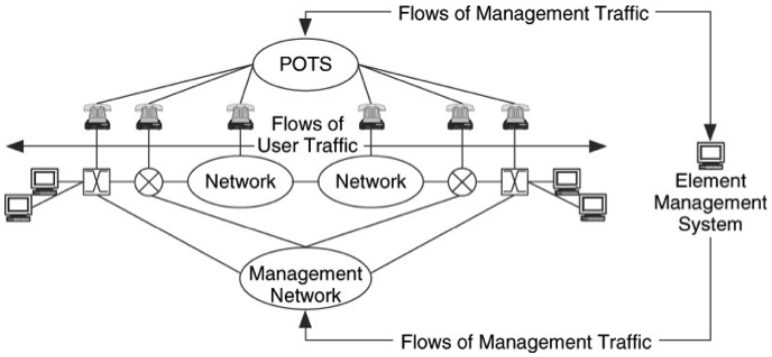
Cuestiones sobre la Arquitectura

- Monitorización *en banda* o *fuera de banda*
  - En banda es más fácil de desarrollar, pero afectada por los problemas de la red
  - Fuera de banda, compleja, cara y con riesgos para la seguridad
- Monitorización *centralizada* o *distribuída*
  - Centralizada, si un único NMS gestiona toda la red
  - Distribuida, cuando varios NMS se reparten la red
  - Jerárquica, varios NMS envían información a un gestor de gestores, filtrando y resumiendo datos, pero más complejidad y riesgo de seguridad
- Generalmente la mejor solución es una arquitectura de administación que no complique la administración de la red misma

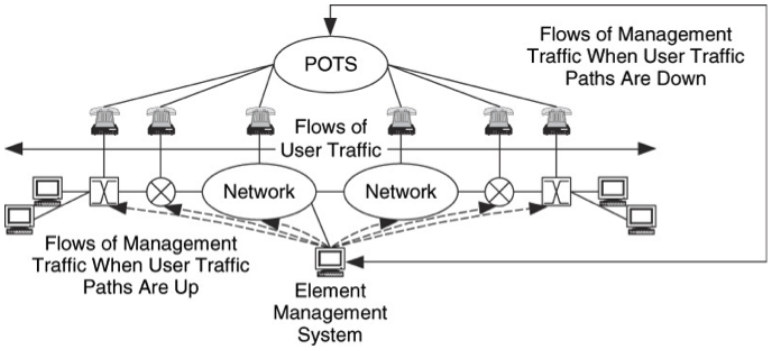
Flujos de Gestión En-Banda



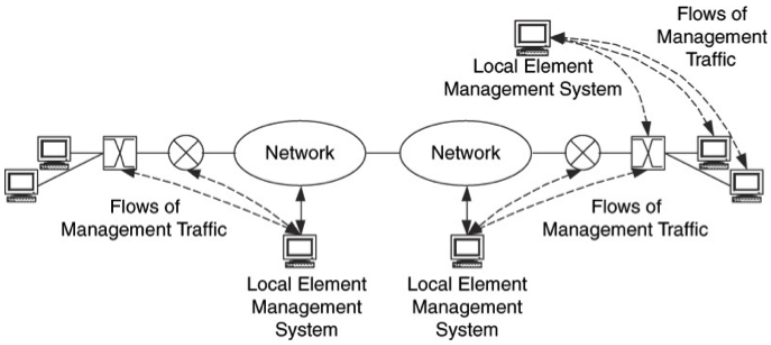
Flujos de Gestión Fuera-Banda



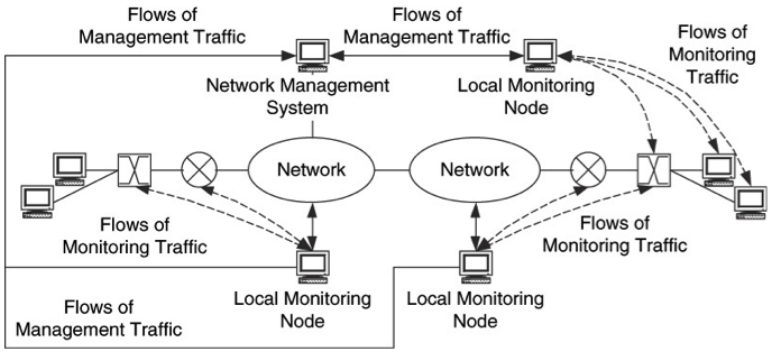
Combinación Flujos de Gestión En-Banda/Fuera-Banda



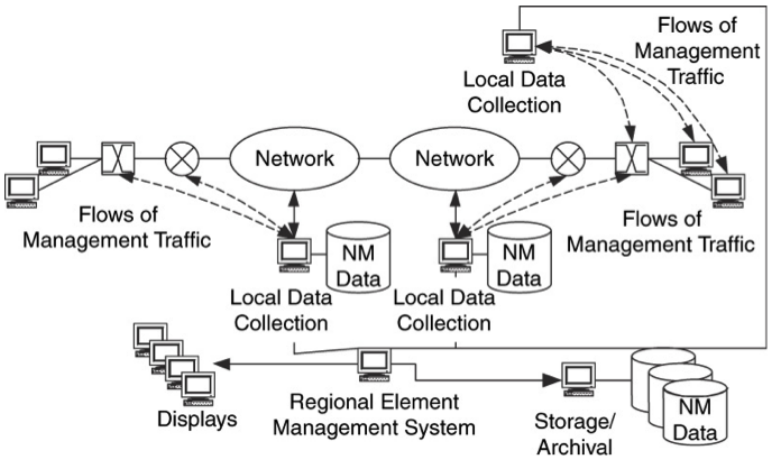
Dominios Administración Divididos



Monitorización Distribuida



Funciones Distribuidas



9.3. Mecanismos de Gestión de Red

Mecanismos de Gestión de Red

- Protocolos de gestión que permiten recuperar, cambiar y transportar datos de gestión por la red:
  - SNMP, Simple Network Management Protocol
    - v1-v3, SNMPv3
    - Comandos NMS a Agente: `get`, `get-next`, `get-bulk`, `set`
    - Comandos Agente a NMS: `response`, `trap`
    - Comandos NMS a NMS: `inform`
    - MIB, *Management Information Base*, con datos de información de gestión por objeto
  - CMIP, *Common Management Information Protocol* (CMOT en su versión TCP/IP)
- SNMP utilizado para
  - *Monitorización*
  - *Instrumentación*
  - *Configuración*

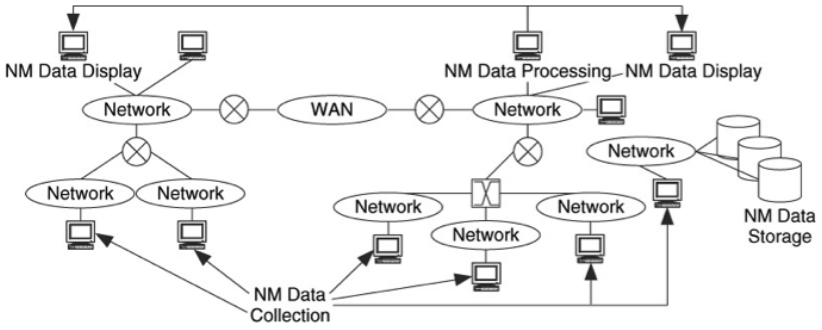
9.4. Mecanismos de Monitorización

Mecanismos de Monitorización

Monitorizar
Obtener valores de las características entre extremos, de enlace, red y elemento

- *Recolectar* mediante consulta activa, monitorización o servicio proxy
- *Procesar* datos en bruto para obtener otros que indiquen el estado
- *Mostrar* datos brutos o procesados a usuario o administrador
- *Archivar* datos o parte de ellos en almacenamiento primario (servidor de gestión), secundario o terciario (archivos de gestión)

Elementos de Monitorización



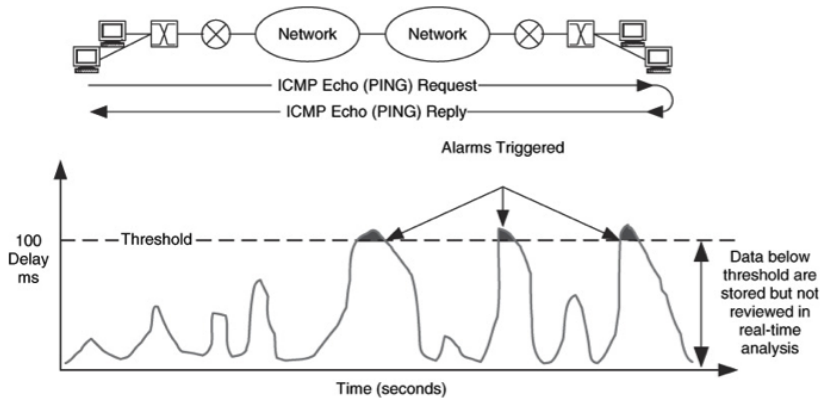
Notificación de Eventos
Monitorización

Evento
Algo que ocurre y que hay que tener en cuenta

- Problema, fallo de un dispositivo o una característica que supera un *umbral*
- Comunicación a usuario, administrador o gestor

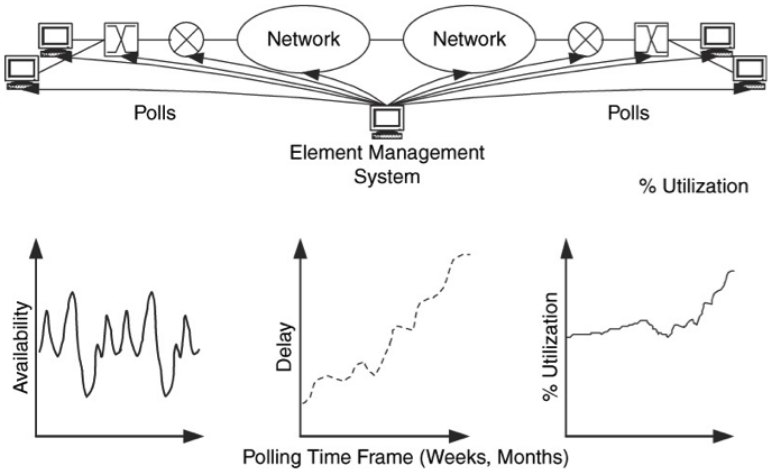
- Dependiendo del nivel de prioridad son registrados, mostrados o generan una alarma
- *Análisis en tiempo real* si los eventos o transitorios se notifican inmediatamente
  - Intervalo de muestreo
  - Número de características muestreadas
  - Atención al *impacto* del tráfico de gestión generado!!

Notificación de Eventos



Análisis de Tendencias y Planificación
Monitorización

- *Análisis de tendencias* utiliza los datos de gestión para determinar el comportamiento a largo plazo de la red
- Planificación del crecimiento futuro de la red
- Almacenamiento durante periodos grandes (semanas, meses, años) de datos muestreados a intervalos constantes (min., horas)



9.5. Mecanismos de Instrumentación

Mecanismos de Instrumentación

Instrumentación
Conjunto de herramientas y útiles necesarios para monitorizar y sondear la red en busca de datos de gestión

- SNMPv3 permite acceder a los datos sobre gestión de red en MIB
- Utilidades: `ping`, `traceroute`, `TCPdump`
- Acceso directo: `telnet`, FTP y conexiones vía consola

Ejemplo de Parámetros MIB-II

Parámetro	Significado
`ifOperStatus`	Estado de la interfaz
`ifInOctets`	Num. de bytes recibidos
`ifOutOctets`	Num. de bytes enviados
`ifInUcastPkts`	Num. de paquetes unicast recibidos
`ifOutUcastPkts`	Num. de paquetes unicast enviados
`ifInNUcastPkts`	Num. de paquetes multicast/broadcast recibidos
`ifOutNUcastPkts`	Num. de paquetes multicast/broadcast enviados
`ifInErrors`	Num. de paquetes con errores recibidos
`ifOutErrors`	Num. de paquetes con errores enviados

Mecanismos de Instrumentación

- La instrumentación debe ser *precisa*, *confiable* y *simple*
  - precisa: pruebas y toma de medidas alternativas
  - confiable: servidores de gestión robustos y jerarquía de componentes de gestión

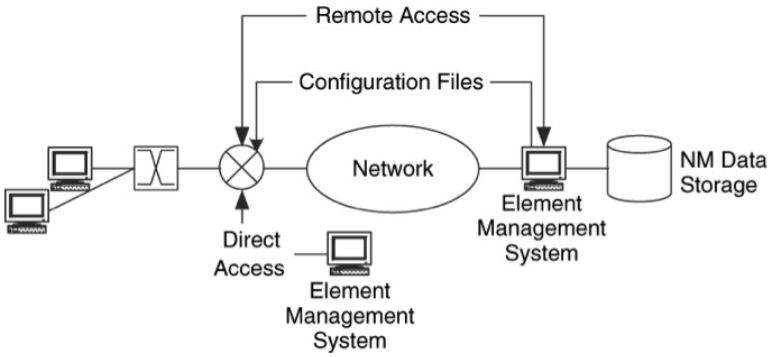
9.6. Mecanismos de Configuración

Mecanismos de Configuración

Configuración
Fijar los parámetros en un dispositivo de red para su funcionamiento y control

- Acceso directo o remoto al dispositivo y descarga de los archivos de configuración
- Comandos *set* de SNMP
- Acceso Telnet a la interfaz de comandos
- Acceso vía HTTP
- FTP/TFTP para descargar los archivos de configuración

Mecanismos de Configuración



Configuración y Resolución de Problemas

- Muchos dispositivos requieren cierto grado de configuración:
  - Tabla de parámetros
  - Método para configurar esos parámetros
  - Comprender los efectos en los cambios de los parámetros
- *Resolución de problemas*
  - Notificación del problema
  - Aislamiento
  - Identificación
  - Resolución
- Conocer los modos de fallo de la red, sus efectos y el modo de solucionarlos

Características de funcionamiento + configuración de parámetros + modos de fallo $\Rightarrow$ comprensión de la red

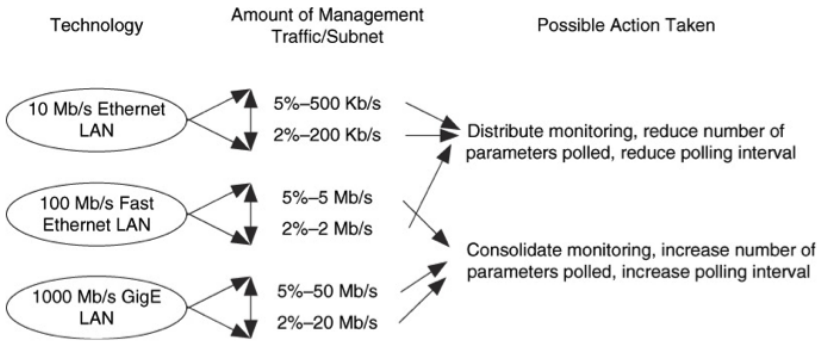
Incremento del Tráfico de Gestión

- Determinar y optimizar el tráfico de gestión
- Para LANs, un dispositivo de monitorización por subred IP

- Núm. dispositivos a encuestar
- Media de interfaces por dispositivo
- Núm. parámetros a recolectar
- Frecuencia de recolecta/encuesta

- El tráfico de gestión debe estar entre 2 % y 5 % de la capacidad de la LAN
  - Si >10 % de la capacidad de la LAN, considerar reducir el tráfico generado
  - Si <1 %, es posible incrementar una de las variables consideradas

Incremento del Tráfico de Gestión



Incremento del Tráfico de Gestión

- Para WANs, un dispositivo de monitorización por interfaz WAN-LAN
  - Permite monitorizar la red en cada localización
  - Medir, verificar y garantizar servicios y prestaciones a través de la WAN
- Añadido a la monitorización LAN
- Un mismo dispositivo puede monitorizar WAN-LAN

Comprobaciones y Balances

- Duplicar medidas para verificar y validar los datos de administración
- Normalizar datos entre distintos fabricantes y verificar datos de distintos orígenes
- Localizar e identificar:
  - Errores en datos almacenados o actuales
  - Vueltas a cero de contadores
  - Cambios en variables MIB entre versiones

9.6.1. Gestión de los Datos de Gestión de la Red

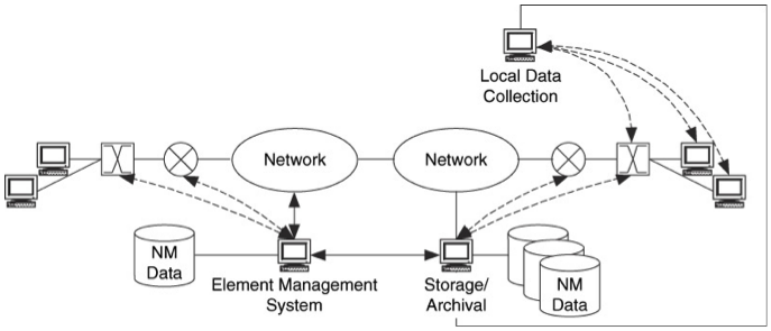
Gestión de los Datos de Gestión de la Red

- Comprender cómo se generan, transportan, procesan y muestran los datos de administración
  - consultas/respuestas o condiciones (*traps*)
  - intervalo de muestreo: sobrecarga dispositivo o congestionar red
  - análisis eventos en tiempo real o análisis de tendencias
- Almacenamiento local vs. archivado
- Copia selectiva
- Migración
- Metadatos

Almacenamiento Local y Archivado

- Almacenar localmente los datos para análisis de eventos y de corto plazo
- Archivar los datos para análisis de tendencias

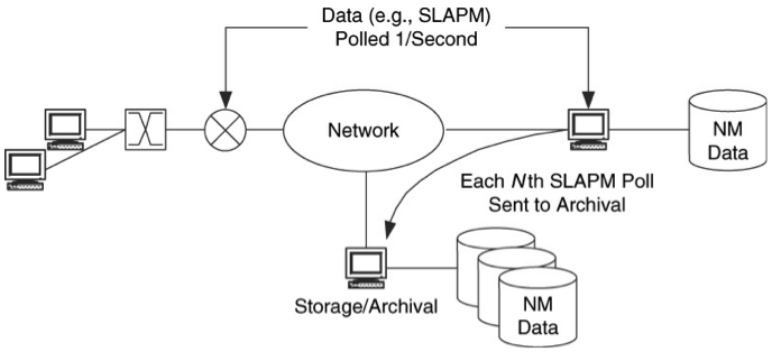
Almacenamiento Local y Archivado



Copia Selectiva de Datos

- Dato usado tanto para notificación de eventos como para análisis de tendencias
- Copiar la N-ésima iteración del parámetro en una BD separada
  - N suficiente grande para minimizar la cantidad de datos
  - N en rango $(10^2 \ldots 10^5)$
- Si riesgo de pérdida de datos entonces TCP o múltiples archivos

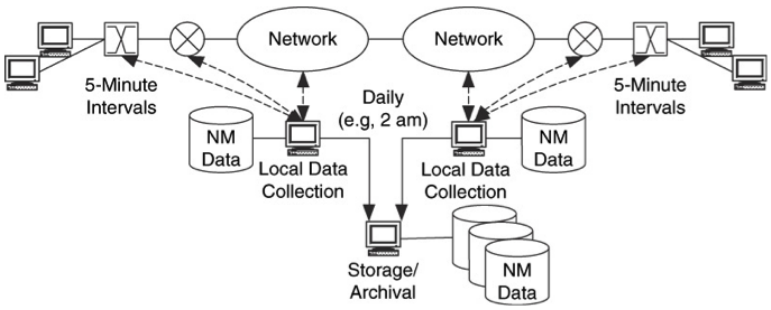
Copia Selectiva de Datos



- SLAPM, *Service Level Agreements (SLAs) for Preventive Maintenance*

Migración de Datos

- Datos almacenados localmente deben archivarse cuando no afecten al tráfico orgánico



Metadatos

- Información adicional sobre los datos recolectados:
  - tipos de datos
  - marca de tiempo
  - etc.
- El sistema de archivado debe proporcionar modo de acceder a los metadatos

9.6.2. Relaciones Externas

Relaciones Externas

- Compromisos, dependencias y restricciones entre la arquitectura de administración y otros componentes arquitectónicos:
  - Direccionamiento y encaminamiento
  - Prestaciones
  - Seguridad
  - Etc

Interacción entre Gestión y Direccionamiento/Encaminamiento

- Si en-banda, el tráfico de gestión debe gestionarse del mismo modo que el tráfico ordinario
- Si fuera-banda entonces el encaminamiento de los datos de gestión debe ser considerado por separado al de la red ordinaria

Interacción entre Gestión y Prestaciones

- La recolección de datos de gestión afectará al rendimiento de la red
- Las prestaciones también dependen de que la gestión aporte datos sobre la red
- Gestión de la red depende de las prestaciones: *Best-effort* o Prioridades

Interacción entre Gestión y Seguridad

- La gestión de la red debe considerar algún nivel de seguridad para ser utilizada
  - Nivel protocolo (SNMP)
  - Acceso seguro a los dispositivos de red
- Si fuera-banda, el acceso debe ser seguro (POTS?)
- Compromiso gestión/seguridad

9.7. Diseño de una Red Administrable

Diseño de una Red Administrable

- Requisito básico de diseño
- Cómo va a ser administrada?
- Dónde estarán los servidores y equipamiento de administración?
- Sonda: observador pasivo del tráfico
  - En una red conmutada cada dispositivo tienen su propio segmento LAN
  - Configurar un puerto del switch para replicar el tráfico de otro/s puertos
  - Monitorización centralizada
  - VLAN administración.

VLAN de administración

- No es deseable que el tráfico de administración se mezcle con el tráfico de usuarios
- Transferencia de software o configuración a dispositivos de la red sin interferencias
- Bloquear tráfico SNMP en VLANs de usuario reduce la posibilidad de ataques
- Facilita a los ingenieros el acceso a los dispositivos para resolver los problemas
- En distribución y núcleo, no necesaria en acceso

Diseño Físico

- Asegurarse de que la red es administrada con eficiencia:
  - Facilidad de acceso: equipamiento accedido frecuentemente el más accesible
  - Etiquetado claro: paneles (99A, 99B, 99V) y cables (número), documentación (con copia en el armario)
  - Disposición lógica: esquema etiquetado consistente con la disposición física
- VLAN administración lo más cerca del núcleo posible
  - Excepto si externalizada, entonces fuera-banda tras cortafuegos

9.8. Herramientas y Protocolos de Gestión de Red

SNMP
Simple Network Management Protocol

- Agente y Servidor, sobre UDP
- SNMPv1, v2 y v3 (Seguridad)
- Comandos: `set`, `get`, `trap`
- Utilizado principalmente para gestión de fallos, aunque también para gestión de prestaciones y de configuraciones (problemas de seguridad?)
- Management Information Base (MIB): árbol de parámetros monitorizados

9.8.1. Selección MIB

MIB

- *Management Information Base*
- MIB-II, segunda versión
- Sólo contiene objetos considerados esenciales
  - Partes específicas para distintos tipos de dispositivos
  - extensiones MIB de fabricante
- `mib-2`
  - `system`
  - `interfaces`
  - `ip`
  - `icmp`
  - `tcp`
  - `udp`
  - `egp`
  - `system`

Objetos grupo `System`
SNMP y MIB

Objeto	Sintaxis	Acceso	Descripción
`sysDescr`	`DisplayString (SIZE (0..255))`	RO	Descripción de la entidad: hardware, sistema operativo, etc
`sysObjectID`	`OBJECT IDENTIFIER`	RO	Identificación del fabricante del subsistema de administración contenido en la entidad
`sysUpTime`	`TimeTicks`	RO	Tiempo desde que el sistema de administración fue reiniciado

Objetos grupo `System`
SNMP y MIB

Objeto	Sintaxis	Acceso	Descripción
`sysContact`	`DisplayString (SIZE (0..255))`	RW	Identificación y datos contacto de la persona para este nodo
`sysName`	`DisplayString (SIZE (0..255))`	RW	Nombre administrativo asignado para el dispositivo
`sysLocation`	`DisplayString (SIZE (0..255))`	RW	Localización física del dispositivo
`sysServices`	`DisplayString (SIZE (0..255))`	RO	Valor que indica el conjunto de servicios que ofrece esta entidad

RMON
Remote Monitoring

- Desarrollado para resolver carencias de MIB para dar datos sobre enlaces y capa física
- Nueve grupos de datos para Ethernet
- Estadísticas sobre paquetes, bytes, distribución de tamaño de paquetes, difusión, colisiones, paquetes desechados, fragmentos, errores CRC y de alineación, paquetes demasiado pequeños y demasiado grandes

9.9. Cómo Monitorizar

Cómo Monitorizar

- Combinación de encuestas y *traps*
  - Traps para informar de eventos entre encuestas
  - Encuestas para detectar fallos que impiden llegar los traps
- Intervalo de encuesta?
  - Incremento tráfico de gestión
  - Dispositivos no responden bloquean encuesta a dispositivos funcionando
- Múltiples colas de encuesta
- Mostrar visualmente los errores, listarlos formato texto, abrir tickets automáticamente

9.10. Qué Monitorizar

Qué Monitorizar

- Dispositivos clave: switches y routers
  - ICMP: `ping`
  - SNMP: `sysUpTime`
  - Conflictos con cortafuegos, monitorizar fuera-banda
- Routers: estadísticas de buffers y colas
- Buscar en MIB el parámetro apropiado (extensiones específicas de fabricante)

Elementos a Monitorizar

Parámetro	Variable MIB	Test	Comentario
Accesibilidad	ICMP (no SMTP)	$t > N$, % sin respuesta	Todos dispositivos incluso no SMTP
Reboot	`coldStart`	trap	Indica que el agente SMTP se ha reiniciado
Activo	`sysUptime`	$t_{i+1} - t_i > 0$	Segundos desde que se inicio el agente SMTP
	`ifOperStatus`	$t_{i+1} - t_i \neq 0$	Cambio en el estado de la interfaz
	`ifInOctets`	Registro	Número bytes recibidos
	`ifInDiscards`	$t_{i+1} - t_i > N$	Paquetes entrantes desechados
	`ifInErrors`	$t_{i+1} - t_i > N$	Paquetes entrantes con error

Elementos a Monitorizar

Parámetro	Variable MIB	Test	Comentario
Estado	`ifOutOctets`	N	Número bytes enviados
	`ifOutDiscards`	$t_{i+1} - t_i > N$	Paquetes salientes desechados
	`ifOutErrors`	$t_{i+1} - t_i > N$	Paquetes salientes con error (debería ser 0)
	`ifInNUcastPkts`	$t_{i+1} - t_i > N$	Paquetes entrantes multi/broadcast
	`ifOutNUcastPkts`	$t_{i+1} - t_i > N$	Paquetes salientes multi/broadcast
	`linkDown`	trap	Indica que una interfaz se ha caído
	`linkUp`	trap	Indica que una interfaz se ha levantado

9.11. Actividades Automatizadas

Actividades Automatizadas

- Automatización de operaciones invasivas o no invasivas
- Recolecta automática de datos sobre el estado de dispositivos
- Descarga periódica de la configuración de los dispositivos

    - Necesario en caso de reemplazo de dispositivo roto
    - Útil para detectar cambios no legítimos
- Modificaciones de contraseñas en routers (supervisado)
- Reconfiguraciones en respuesta a incidentes (no recomendable en redes complejas!)

9.12. Resumen

Resumen

- Administrar una red es una tarea compleja con muchas dependencias de la arquitectura de la red
- Monitorización, instrumentación y gestión
- Qué monitorizar y administrar?
- Dónde localizar cada función?
- Cómo gestionar el flujo de tráfico de gestión?
- Protocolos y herramientas

Resumen Parte 2

Resumen Parte 2

- Diseño lógico de la red con un enfoque descendente
- Definir topología basada en el analisis de requisitos
- Concebir direcciones y nombres
- Seleccionar protocolos de conmutación y encaminamiento
- Oportunidad para centrarse en los objetivos de diseño sin entrar en detalles técnicos o de implementación física

Parte III
Diseño Físico

Diseño Físico

- En esta fase se tratará de cableado y activos (SW, RTR, AP)
- Múltiples opciones, elegir según escalabilidad, prestaciones, asequibilidad y gestionabilidad
- Campus primero, WAN y acceso remoto después
  - *Campus*, segmentos LAN y redes de edificio en una área $< 1,5$ Km

10. Tecnologías y Dispositivos para Redes de Campus

10.1. Diseño del Cableado de LAN

Diseño del Cableado de LAN

- Cableado es más un problema de implementación que de diseño, pero no menos importante
- Debe durar varios años, disponibilidad y escalabilidad
- Cableado existente? (← Caracterización de la red existente)
  - Topologías cableado campus/edificios
  - Localización armarios comunicaciones
  - Tipos y longitud
    - Cables entre edificios
    - Cableado vertical
    - Cableado horizontal
    - Latiguillos en áreas de trabajo

10.1.1. Topologías de Cableado

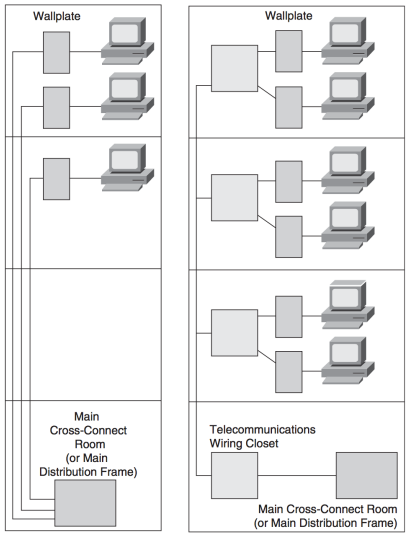
Topología de Cableado

- Guías y especificaciones cableado
  - EIA/TIA guía para cable e instalación UTP
  - Compañías (AT&T, IBM, DEC, HP, Northern Telecom)
- Dos esquemas de cableado posibles
  - *Centralizado*, la mayoría de los cables confluyen en un área (estrella)
  - *Descentralizado*, los cables discurren a través del entorno (bus, anillo, malla)

Topología Cableado en Edificio

- Depende del tamaño
  - Edificio pequeño, centralizada
  - Edificio grande (alto y plantas grandes), distribuido ($>$ 100 m entre áreas trabajo y armarios comunicaciones)

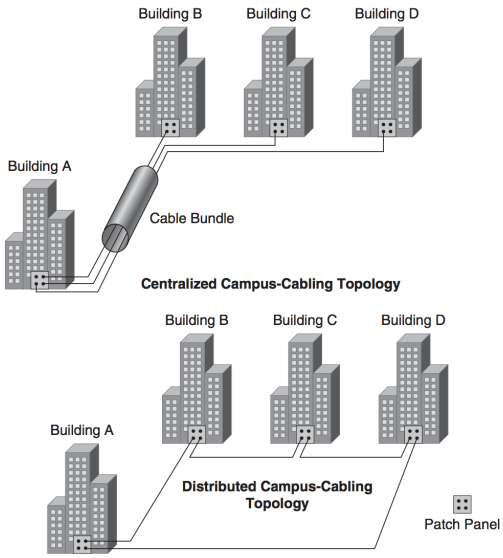
Topología Cableado en Edificio



Topología Cableado en Campus

- Exposición a riesgos físicos
- Seleccionar cables y topología con cuidado
- Cableado distribuido ofrece más disponibilidad que centralizado, pero es más difícil de gestionar
- Combinación cable e inalámbrico

Topología Cableado en Campus



10.1.2. Tipos de Cables

Tipos de Cables

- Cobre apantallado
  - STP, *Shielded Twited-Pair*, Token Ring (1980s-1990s)
  - Coaxial, cable grueso (10Base5) y fino (10Base2), bus, no recomendado para instalaciones nuevas
- Cobre no apantallado
  - UTP, *Unshielded Twister-Pair*, Ethernet 10BaseT y siguientes
  - Asequible, pero menos capacidad transmisión (diafonía, ruido, interferencias electromagnéticas), distancia
- Fibra óptica
  - Inmune a diafonía, ruido e interferencias electromagnéticas
  - Mayor capacidad de transmisión, > 40 Gbp con WDM (*Wavelength-Division Multiplexing*)
  - Cableado horizontal y vertical, raro en área de trabajo (coste NICs)

Categorías UTP

- Cat 1 y 2, no recomendados para datos
- Cat 3 (16 MHz), *cableado de voz* también para datos, Ethernet 10BaseT y Token Ring 4 Mbps

- Cat 4 (20 MHz), Token Ring 16 Mbps, obsoleto
- Cat 5 (100 MHz), Ethernet 100BaseT, FDDI (*Fiber Distributed Data Interface*), con 4 pares soporta Gigabit
- Cat 5e (100 MHz), Ethernet 100BaseT, Gigabit y ATM (*Asincronous Transfer Mode*), [*Mínimo*]
- Cat 6 (200 MHz), Ethernet 100BaseT, Gigabit* y ATM, mejor SNR (*Signal-to-Noise Ratio*) [*Recomendado*]
- Cat 7/a (1 GHz), Gigabit Ethernet (100m), Gigabit Ethernet 40 (50m) y Gigabit Ethernet 100 (15m)
- Cat 8 (2 GHz), 40GBaseT, sustitución fibra en data center (<30m)

Fibra Óptica

- Mayor coste y dificultad de instalación
  - Pérdidas en acoplamientos y conexiones
  - Reflexión en conectores
- Multimodo
  - Múltiples rayos de luz, distintas distancias, dispersión intermodal limita el ancho de banda
  - Más barato, núcleo mayor, LED
- Monomodo
  - Núcleo menor, único camino, sin dispersión intermodal (laser)
  - Mayor ancho de banda y distancia que multimodo
  - Dificultad de acoplamiento y conexión
  - Mayor coste instalación, componentes

10.2. Tecnologías LAN

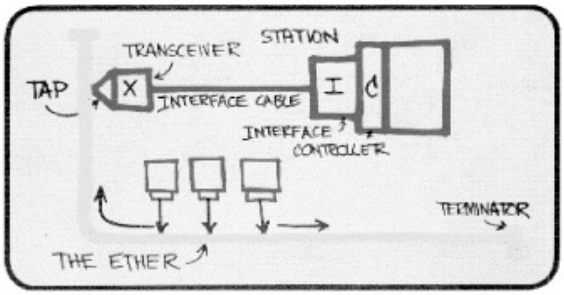
Tecnologías LAN

- Objetivos y restricciones del negocio
  - Sesgo tecnológico
  - Tecnologías aprobadas y proveedores
  - Tolerancia al riesgo
  - Experiencia tecnológica del personal
  - Presupuesto y planificación
- Objetivos técnicos (escalabilidad, disponibilidad, gestionabilidad, asequibilidad, adaptabilidad)
- Restricciones throughput, retardo, jitter, ancho de banda y QoS

10.2.1. Aspectos Básicos de Ethernet

Aspectos Básicos de Ethernet

- *Ethernet* capa física y enlace para la transmisión de marcos en LANs
- 1970s Xerox Corporation (Bob Metcalfe y David Boggs)
- Estándar de facto



Ethernet y IEEE 802.3

- 1982, DEC, Intel y Xerox publican Ethernet II
- 1983, IEEE 802.3
- Sinónimos aunque con diferencias sutiles (en físico 802.3, en enlace ambos)

Field Name	Preamble	Destination Address	Source Address	Ether Type	Information	Frame Check Sequence
Size in Bytes	8	6	6	2	46-1500	4

Ethernet Version 2.0 Frame Format

					LLC Header				
Field Name	Preamble	Destination Address	Source Address	Length	DSAP	SSAP	Control	Information	Frame Check Sequence
Size in Bytes	8	6	6	2	1	1	1	43-1497	4

IEEE 802.3 Frame Format

10.2.2. Opciones de Tecnología Ethernet

Opciones de Tecnología Ethernet

- Escalable, adaptada al incremento de requisitos de capacidad
  - Ethernet semi-duplex, full-duplex
  - Ethernet 100 Mbps

    - Ethernet 1000 Mbps (1 Gbps, Gigabit)
    - Ethernet 10 Gbps
    - Metro Ethernet
    - Ethernet de largo alcance, *Long-Reach Ethernet*, (LRE)
    - EtherChanel Cisco
- Posibilidades para acceso, núcleo y distribución

Ethernet Semi-duplex, full-duplex

- Ethernet, medio compartido con CSMA/CD regulando envío de marcos y detección de colisiones
- Si semi-duplex, la estación o está transmitiendo o recibiendo (medio compartido)
- Regla diseño: RTT$_{dominio\ colision} <$ t$_{transmitir}$ (512 bits) (51,2 μs en 10 Mbps)
    - Tamaño dominio colisión debe asegurar que una estación enviando el paquete mínimo (64 bytes, o 512 bits) puede detectar el reflejo de una colisión desde el otro extremo mientras aún está enviando el marco
- Segmentos punto-a-punto son full-duplex (microsegmentación)
    - Host - Switch
    - Switch - Switch
- Full-duplex duplica la tasa transmisión de semi-duplex (teóricamente)

Ethernet 100 Mbps

- *Fast Ethernet*, 100BaseT, (originalmente IEEE 802.3u)
- Similar a 10 Mpbs, facilita la transisión entre tecnologías (parámetros diseño multiplicados o divididos por 10)
- Implementaciones físicas
    - *100BaseTX*, dos pares UTP Cat 5 (o superior) [*]
    - *100BaseT2*, dos pares UTP Cat 3 (o superior)
    - *100BaseT4*, cuatro pares UTP Cat 5 (o superior)
    - *100BaseFX*, dos fibras multimodo

Ethernet Gigabit

- Originalmente 802.3z, similar a Ethernet 100 Mbps, pero 10 veces más rápido
- Para evitar reducir el tamaño de un segmento semi-duplex a 1/10 del tamaño con 100 Mbps, modificar MAC
  - Mantener tamaño mínimo marco en 512 bits
  - Tiempo mínimo de envío equivalente a 4096 bits (512 bytes)
  - *Extensión de portadora* 0 - 4096 bits
  - Permitir envío de varios paquetes en ráfagas (sólo el primero con extensión de portadora) hasta *burstLimit* (8192 bytes)
- Apropiado para troncales de edificios y de campus
  - Agregando tráfico de segmentos 100 Mbps
  - Modo full-duplex, SW-SW o SVR-SW
- Sobre cableado UTP, twinax, fibra monomodo o multimodo

Ethernet Gigabit

	1000BaseSX	**1000BaseLX**	**1000BaseCX**	**1000BaseT**
Cable	multimodo 850 nm	multi/mono modo 1300 nm	Twinax 150 Ohm	UTP
Distancia (m)	200 - 550	550 multimodo, 5000 monomodo	25	100 entre nodo y hub (200 diámetro)
Uso	horizontal y troncal edificio	troncal edificio/campu	armario	horizontal/área trabajo (1 rep)

Ethernet 10 Gbps

- 2002, forma parte del estándar IEEE 802.3
- Diferencias con otras implementaciones Ethernet, manteniendo formato marco
- *Ether* omnipresente
  - Transacciones completamente transportadas por Ethernet
- SW y RTR, también NICs para SVR
- Troncal para ISPs, redes empresariales, granjas servidores
- Full-duplex sobre cobre o fibra, no soporta semi-duplex
- Normalmente transmisión serie
  - 10GBaseLX4 multiplexa en 4 bits con WWDM, *Wide wavelength-division multiplexing*

Ethernet 10 Gbps

	Long. Onda	Medio	Distancia
10GBaseLX4	1310 nm	62,5 μm multimodo	2 - 300 m
10GBaseLX4	1310 nm	10 μm monomodo	2 - 10 Km
10GBaseS	850 nm	50 μm multimodo	2 - 300 m
10GBaseL	1310 nm	10 μm monomodo	2 - 10 Km
10GBaseE	1550 nm	10 μm monomodo	2 - 30 (40) Km
10GBaseCX4	N/A	Twinax	15 m
10GBaseT	N/A	UTP/STP	100 m

Metro Ethernet

- Combina LAN con WAN
- Método interconectar redes campus a precio razonable
- Acceso al ISP mediante Ethernet 10 Mbps - 10 Gbps, mantenendo circuitos virtuales
- Soporta varios protocolos de transporte
  - SONET, *Synchronous Optical Network*
  - ATM, *Asynchronous Transfer Mode*
  - DWDM, *Dense-Mode Wavelenght-Division Multiplexing*
  - MPLS, *Multiprotocol Label Switching*
- Aplicaciones MAN

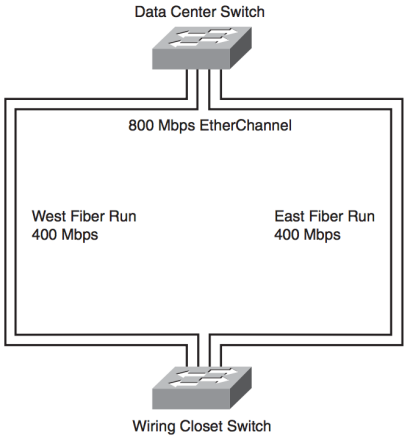
Ethernet de Largo Alcance

- Ethernet sobre cableado voz (Cat 1, 2 o 3)
- Enlace punto-a-punto hasta 1,6 Km con hasta 11,25 Mbps full-duplex simétricos
- Cohexistencia Ethernet-servicios telefónicos (ISDN, PBX)
- Codificación y modulación DSL, *Digital Susbcriber Line*
- Conexión edificios, o habitaciones en edificios
  - Áreas rurales
  - Centros históricos
  - Hoteles, complejos edificios
- Aplicaciones MAN

EtherChannel Cisco

- Tecnología troncal, agrupa varios enlaces Ethernet full-duplex
  - Prestaciones
  - Reparto de carga
  - Alta disponibilidad
- Hasta 4 enlaces 10 Mbps/100 Mbps/1 Gpbs/10 Gbps para conseguir 80 Mbps/800 Mbps/8 Gbps/80 Gbps agregados full-duplex
- Distribuye tráfico unicast, multicast y broadcast entre los enlaces del canal
  - XOR últimos 2 bits si 4 enlaces, último bit si 2 enlaces, de dir. origen y destino)
- Diversidad física en el tendido de fibra
- Recuperación fallos automática ($<$ 1 s)

EtherChannel Cisco



10.2.3. Dispositivos de Interconexión en Red de Campus

Dispositivos de Interconexión en Red de Campus

	Capa OSI	**Segmentación Dominos Colisión**	**Segmentación Dominios Difusión**	**Uso Típico**	**Características Adicionales**
Hub	1	Todos los puertos mismo dominio colisión	Todos los puertos en mismo dominio difusión	Conectar dispositivos individuales en pequeñas LANs	Autoparticionado o aislamiento nodos mal comportamiento
Bridge	1-2	Cada puerto un dominio colisión	Todos los puertos en mismo dominio difusión	Conectar redes	Filtrado de paquetes configurado por usuario

Dispositivos de Interconexión en Red de Campus

	Capa OSI	Segmentación Dominos Colisión	Segmentación Dominios Difusión	Uso Típico	Características Adicionales
Switch	1-2	Cada puerto un dominio colisión	Todos los puertos en mismo dominio difusión excepto si VLANs	Conectar dispositivos individuales o redes	Filtrado, procesamiento *cut-through*
Router	1-3	Cada puerto un dominio colisión	Cada puerto en un dominio difusión	Conexión de redes	Filtrado, cortafuegos, enlaces WANs alta velocidad, compresión, encolado y procesado avanzado

10.2.4. Optimización de Características Dispositivos Interconexión

Optimización de Características Dispositivos Interconexión

- QoS no sólo en WAN, también en LAN
  - Ancho de banda demandado excede el disponible
  - VoIP impone restricciones sobre retardo/jitter
- QoS en enlaces de subida
  - Distribución a núcleo
  - Acceso a Distribución
- QoS en acceso, información nivel 2
  - Puerto alta prioridad
- QoS en distribución y núcleo, información nivel 3
  - Direcciones IP
  - Número de puertos
  - En ambas direcciones del flujo de tráfico

10.2.5. Ejemplo de Diseño de Red de Campus

Ejemplo Diseño Red de Campus

Estudiar sección del capítulo 10 de TDND

10.3. Resumen

Resumen

- Primer paso en fase diseño físico (metodología descendente)
- Seleccionar tecnlogías y dispositivos para redes de campus
- Cables, implementaciones capa 2 y dispositivos de red
- Restringido por objetivos negocio, requisitos técnicos, tráfico
- Diseño cableado LAN y tecnologías: Ethernet, MetroEthernet, EtherChannel

11. Tecnologías y Dispositivos para Redes Empresariales

Tecnologías y Dispositivos para Redes Empresariales

- Acceso remoto
- Redes WAN
- Dispositivos
  - Servidores acceso remoto
  - Routers
  - Firewalls
  - Concentradores VPN

11.1. Tecnologías de Acceso Remoto

Tecnologías de Acceso Remoto

- Organizaciones más dispersas y móviles
- Acceso remoto para teletrabajadores, empleados en oficinas remotas y viajantes
  - Sucursales, oficinas de ventas, fábricas, almacenes, tiendas
- Teletrabajadores
  - Email, web, aplicaciones ventas, agendas
  - Descarga de archivos, demostraciones, teleconferencias, teleformación
- Modem analógicos 56 Kbps $\rightarrow$ modem DSL o cable en routers SOHO, *Small Office/Home Office*
- PPP, *Point to Point Protocol*

11.1.1. PPP

PPP

- Capa enlace para transportar varios protocolos capa de red sobre enlaces punto a punto serie
  - Síncronos, asíncronos, telefónicos y ISDN
- Servicios
  - Multiplexado de protocolos de capa de red
  - Configuración de enlace
  - Prueba de calidad del enlace
  - Negociación de opciones del enlace
  - Autenticación
  - Compresión de cabeceras
  - Detección de errores

PPP

- Capas funcionales
  - NCP, *Network Control Protocol*, para establecimiento y configuración de protocolos de red (IP, IPC, AppleTalk, DECnet)
  - LCP, *Link Control Protocol*, para establecimiento, configuración, autenticación, prueba y finalización de la conexión de enlace de datos
  - Encapsulación datagramas de capa de red utilizando protocolo HDLC, *High-Level Data Link Control*
  - Capa física, basada en estándares (RS-232-C, RS-422, V.24 y V.35)

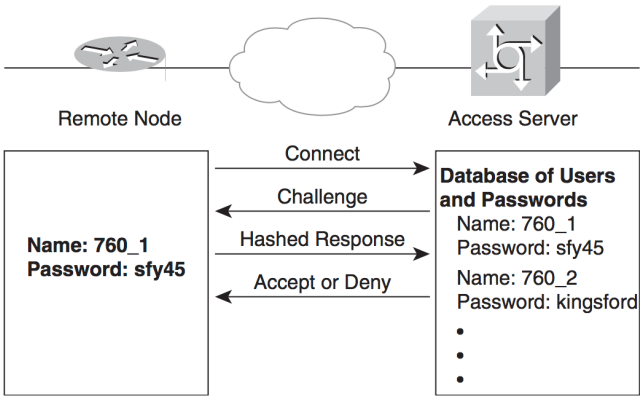
PPP Multienlace y Multichasis

- MPPP, *Multilink PPP*, soporta agregación de canales PPP
- Reparto de carga y ancho de banda extra
- Asegura que los paquetes llegan al destino en orden
  - Encapsulación datos en PPP y asignación número de secuencia
  - Ordenación en destino
- Múltiples enlaces aparecen como un único enlace para protocolos superiores

Autenticación PPP

- Dos métodos
  - PAP, *Password Authentication Protocol*
  - CHAP, *Challenge Handshake Authentication Protocol*
- PAP obsoleto, envío contraseña como texto plano
- CHAP
  - Conexión en tres paso con desafío basado en contraseña
  - Verificación en establecimiento y repetible durante la sesión

Autenticación PPP



11.1.2. Acceso Remoto vía Modem Cable

Acceso Remoto vía Modem Cable

- Utilizar la red de cable coaxial de TV para acceder a la red
- Mayores velocidades que la línea telefónica
- Siempre conectado, sin necesidad de marcar (lento)
- HFC, *Hybrid Fiber/Coax*
- 25 - 50 Mbps de bajada, 2 - 3 Mbps subida
  - Compartidos
  - Bajada visible para todos los modems, filtrado
  - Subida basada en ranuras de tiempo: reservadas o contienda

11.1.3. Acceso Remoto vía Línea de Subscriptor Digital

Línea de Subscriptor Digital

- DSL, *Digital Subscriber Line*
- Trafico de datos de alta velocidad sobre líneas telefónicas
- Velocidad dependiendo de distancia a centralita, calidad del cable, ruido
- Simétrico y Asimétrico
- ADSL, *Asymmetric DSL*
  - Canal de bajada, 1,5 - 12 Mbps
  - Canal de subida, 16 - 640 Kbps
  - Voz, POTS, *Plain Old Telephone Service*, 64 Kbps
- SDSL, *Symmetric DSL*
  - Dos canales datos de 1,5 Mbps
  - No voz

xDSL

- IDSL
  - ISDN + DSL
  - 128 Kbps bidireccional sobre un par de hilos
  - 4,6 - 5,5 Km
- HDSL, *High-Bit-Rate DSL*
  - 1,5 Mbps simétricos sobre 2 pares
  - 2,0 Mbps simétricos sobre 3 pares
  - 3,7 - 4,6 Km
  - Más barato que E1 o T1, soporta líneas poca calidad

xDSL

- HDSL-2
  - 1,5 Mbps simétricos sobre un par
  - No interfiere con ADSL
- G.SHDSL
  - Múltiples tasas como SDSL, con compatibilidad con HDSL-2

- VDSL, *Very-High-Bit-Rate DSL*
  - Datos y PSTN, *Plain Switched Telephone Network*
  - 52 Mbps bajada y 16 Mbps subida
  - Cerca de centralita
  - Usada por LRE, *Long Reach Ethernet*

PPP y ADSL

- ADSL utiliza dos implementaciones de PPP
- PPPoA, *PPP over ATM*
  - Equipo en cliente actúa como router Ethernet-WAN
  - Sesión PPP entre equipo cliente y concentrador nivel 3 del ISP
  - AAA
  - Usa ATM entre extremos
- PPPoE, *PPP over Ethernet*
  - Equipo en cliente actúa como puente Ethernet-WAN
  - Sesión PPP encapsulando marcos PPP en marcos MAC y pasándolos sobre ATM/DSL al router gateway en el ISP
  - Cliente recibe IP del ISP mediante negociación PPP

11.2. Selección Dispositivos Acceso Remoto

Dispositivos Acceso Remoto para Usuarios

- Compatibilidad con el operador
- Criterios selección
  - Características seguridad y VPN
  - Soporte de NAT
  - Fiabilidad
  - Coste
  - Capacidad para actuar como AP inalámbrico
  - Soporte para varias interfaces Ethernet/agregación canales
  - Capacidad QoS para soportar VoIP

Dispositivos Acceso Remoto para Central

- Conecta usuarios remotos que acceden a la red corporativa mediante modems cable o DSL y VPN
- Routers y firewalls actúan como punto de terminación de túneles VPN
  - Si $>$ 100, mejor concentrador VPN
- Interoperablidad VPN central y clientes
- Atención al número de túneles simultáneos y tráfico soportado
  - Procesador rápido
  - RAM alta velocidad
  - Redundancia fuente alimentación
  - Encriptación por hardware

Dispositivos Acceso Remoto para Central

- Capacidades software
  - Protocolos tunelado: IPSec, PPTP, L2TP
  - Algoritmos encriptación: DES 56 bits, Triple DES 168 bits, RC4 40-128 bits, AES 128-192-256 bits
  - Algoritmos autenticación: MD5, SHA-1, HMAC con MD5, HMAC con SHA-1
  - Protocolos de red: DNS, DHCP, RADIUS, Kerberos, LDAP
  - Protocolos encaminamiento
  - Soporte autoridades certificación: Entrust, VeriSign, Microsoft
  - Gestión utilizando SSH, HTTPS

11.3. Tecnologías WAN

Tecnologías WAN

- Diferentes alternativas disponibles
- Incremento en necesidades de ancho de banda
- Infraestructura SONET y ATM en operadoras
- Nuevos servicios
- En el futuro también WANs inalámbricas

11.3.1. Aprovisionamiento de Ancho de Banda

Aprovisionamiento de Ancho de Banda

- *Aprovisionamiento*, selección de capacidad necesaria para WAN
  - Análisis del tráfico
  - Objetivos de escalabilidad (2 o 3 años)
- Clasificaciones ancho de banda en cable de cobre
  - *North America Digital Hierarchy*, para USA y otros países
    - DS, *Digital Signal*, un canal en la jerarquía
    - Multiplexación para conseguir canales de mas velociad
    - DS1 y DS3 son los más comunes
  - *Committe of European Postal and Telephone Hierarchy*
    - Jerarquía Europea, *E system*
- *Synchronous Digital Hierarchy*, SDH, estándar internacional para transmisión sobre fibra óptica
  - Tasa estándar STS-1
  - Tasas equivalentes en SONET *Optical Carrier* (OC)

North America Digital Hierarchy

Señal	Capacidad	Núm. de DS-0s	Nombre
DS-0	64 Kbps	1	Canal
DS-1	1,544 Mbps	24	T1
DS-1C	3,152 Mbps	48	T1C
DS-2	6,312 Mbps	96	T2
DS-3	44,736 Mbps	672	T3
DS-4	274,176 Mbps	4032	T4
DS-5	400,352 Mbps	5760	T5

Committe of European Postal and Telephone Hierarchy

Señal	Capacidad	Número de E1s
E0	64 Kbps	N/A
E1	2,048 Mbps	1
E2	8,448 Mbps	4
E3	34,368 Mbps	16
E4	139,264 Mbps	64
E5	565,148 Mbps	256

***Synchronous Digital Hierarchy*, DSH**

Señal STS	Señal OC	Capacidad
STS-1	0C-1	51,84 Mbp
STS-3	0C-3	155,52 Mbps
STS-12	0C-12	622,344 Mbps
STS-24	0C-24	1.244,16 Mbps
STS-48	0C-48	2.488,32 Mbps
STS-96	0C-96	4.976,64 Mbps
STS-192	0C-192	9.953,28 Mbps

11.3.2. Líneas Alquiladas

Líneas Alquiladas

- *Línea alquilada*, circuito dedicado que se alquila a un operador por una cierta cantidad de tiempo
- Sólo transporta tráfico del cliente
- Punto a punto
- 64 Kbps (DS-0) - 45 Mbps (DS-3)
- Tanto voz como datos, encapsulados como PPP o HDLC
- Pros
  - Tecnología probada
  - No enlace compartido, punto a punto real
- Cons
  - Coste (aunque disminuyendo)
  - Para tráficos sin QoS avanzados

11.3.3. Synchronous Optical Network, SONET

***Synchronous Optical Network*, SONET**

- Especificación capa física para transmisiones de alta velocidad síncronas de paquetes o celdas sobre fibra óptica
- 1980s
- Redes internas de operadores, también en WAN o MAN
- Define velocidades más altas que sistemas T y E, compatibles con ambos

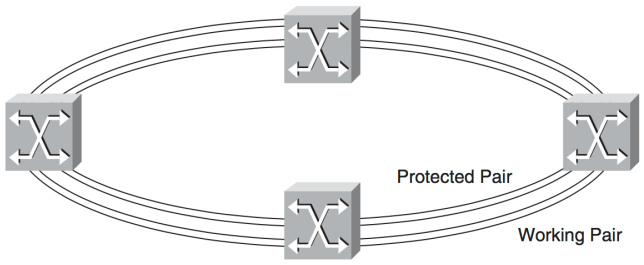
- Módulo STS-1

- Multiplexado y demultiplexado más eficiente
  - Jerarquías norteamericana y europea como redes *plesiócronas*, no completamente síncronas

Arquitectura SONET

- Protocolo con cuatro capas
  - Capa fotónica: características equipo óptico
  - Capa de sección: marco y conversión en señales ópticas
  - Capa de línea: sincronización y multiplexación de marcos
  - Capa de camino: transporte entre extremos
- Multiplexores (en SWs o RTRs) permiten acceder a red SONET
- Doble anillo, full-duplex
- Recuperación de cortes sin interrupción (ms)

Arquitectura SONET



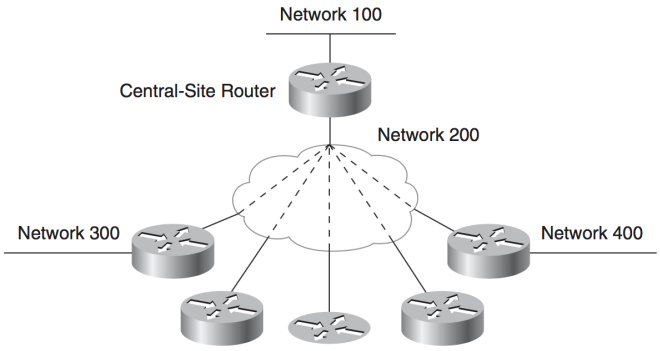
11.3.4. Frame Relay

Frame Relay

- Protocolo WAN altas prestaciones que opera en capas física y de enlace de datos
- 1990s, para mejorar otras alternativas como X.25
  - Supone que el canal no es tan propenso a errores
  - Eficiente, asignación de ancho de banda dinámico y baja latencia
  - 64 Kbps - 1,544 Mbps (algunos hasta T3)
- Servicio enlace de datos orientado a conexión entre equipamiento terminal de datos (DTE) dentro de una red de conmutación de paquetes, que puede pasar por varios equipos de terminación de circuitos (DCE)

- Control de congestión
- Control de tráfico
  - Tasa de acceso: múmero máximo de bps que un DTE puede transmitir en una red Frame Relay
  - Otros parámetros

Topología Frame Relay



Topología Frame Relay

- Radial, una conexión física, varias lógicas
- Limitado por *horizonte divido*, que en encaminamiento dinámico prohibe que un router publique una ruta por la interfaz por la que la aprendió
  - Anular horizonte dividido en EIGRP con Frame Relay
  - Subinterfaces, aunque más complejidad configuración routers y más números de redes
  - Red mallada, aunque más coste (x N)

11.3.5. ATM

ATM

- Buena opción para troncal WAN rápida y con QoS
  - T3 o más
  - OC-192 o más (10 Gbps)
- Soporta mejor compartición ancho banda entre aplicaciones (celdas vs paquetes)
- Interfaces red caras
- Complejidad
- *Ethernet over ATM*

11.3.6. Metro Ethernet

Metro Ethernet

- Combina capacidades y comportamiento WAN con Ethernet
- Interfaces Ethernet para acceder a la red
  - Opciones acho de banda
  - 1 Mbps
- Varios protocolos de transporte: SONET, ATM, MPLS
- Circuito Virtual Ethernet, EVC
  - E-linea: punto a punto
  - E-LAN: multipunto
  - E-árbol: punto a multipunto

11.3.7. Selección de Routers WAN

Selección de Routers WAN

- Selección cuidadosa para evitar problemas de prestaciones
  - Agregación de tráfico en la parte alta de la jerarquía
- Interfaces WAN apropiadas
- Memoria y CPU para reenviar paquetes y gestionar protocolos
- Características de optimización
  - Técnicas de comnutación y encolado avanzadas
  - Conformado de tráfico (*traffic shaping*)
  - RED, *Random Early Detection*
  - Reenvío exprés, Cisco *Express Forwarding*, CEF

11.3.8. Selección del Proveedor WAN

Selección del Proveedor WAN

- Además del coste, otros criterios
  - Servicios ofrecidos
  - Área geográfica
  - Fiabilidad y prestaciones de la red interna del proveedor
  - Nivel de seguridad

    - Nivel de soporte técnico
    - Probabilidad de continuación en el tiempo
    - Disposición a colaborar para alcanzar los objetivos
- Investigar la esctructura, seguridad y fiabilidad de la red interna del proveedor
- Acuerdo de nivel de servicio, *service-level agreement*, SLA

11.3.9. Ejemplo de Diseño de una WAN

Ejemplo Diseño Red Empresarial

Estudiar sección del capítulo 11 de TDND

11.4. Resumen

Resumen

- Diseño de la red en aquellos aspectos de acceso remoto y WAN
- Acceso remoto: PPP, modems cable y DSL
- Tecnologías WAN: NADH, Sistema E, SDH, líneas alquiladas, SONET, Frame Relay, ATM y Metro ethernet
- Criterios de selección routers y proveedores

Resumen Parte 3

Resumen Parte 3

- Diseño físico involucra la selección de medios, tecnologías y dispositivos para las redes de campus y empresa
- Trata de cables, protocolos capa 1 y 2, y dispositivos de red
- Depende de los objetivos del negocio, requisitos técnicos y características del tráfico (Parte 1)
- Se construye sobre el diseño lógico (Parte 2)
- Múltiples elecciones para la tecnología LAN y WAN, ninguna cubre todas las necesidades por si sola

12. Referencias

Referencias

[Dooley, 2002] Kevin Dooley *Designing Large-Scale LANs*. O'Reilly & Associates Inc., 2002.

[McCabe, 2007] James D. McCabe *Network Analysis, Architecture, and Design*. Elsevier, 3/ed 2007.

[Oppenheimer, 2002] Priscilla Oppenheimer *Top-Down Network Design*. Cisco Press, 3/ed 2011.

Hecho con...
LaTeX y BEAMER