FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

A LOS ASISTENTES A LOS CURSOS

Las autoridades de la Facultad de Ingeniería, por conducto del jefe de la División de Educación Continua, otorgan una constancia de asistencia a quienes cumplan con los requisitos establecidos para cada curso.

El control de asistencia se llevará a cabo a través de la persona que le entregó las notas. Las inasistencias serán computadas por las autoridades de la División, con el fin de entregarle constancia solamente a los alumnos que tengan un mínimo de 80% de asistencias.

Pedimos a los asistentes recoger su constancia el día de la clausura. Estas se retendrán por el periodo de un año, pasado este tiempo la DECFI no se hará responsable de este documento.

Se recomienda a los asistentes participar activamente con sus ideas y experiencias, pues los cursos que ofrece la División están planeados para que los profesores expongan una tesis, pero sobre todo, para que coordinen las opiniones de todos los interesados, constituyendo verdaderos seminarios.

Es muy importante que todos los asistentes llenen y entreguen su hoja de inscripción al inicio del curso, información que servirá para integrar un directorio de asistentes, que se entregará oportunamente.

Con el objeto de mejorar los servicios que la División de Educación Continua ofrece, al final del curso deberán entregar la evaluación a través de un cuestionario diseñado para emitir juicios anónimos.

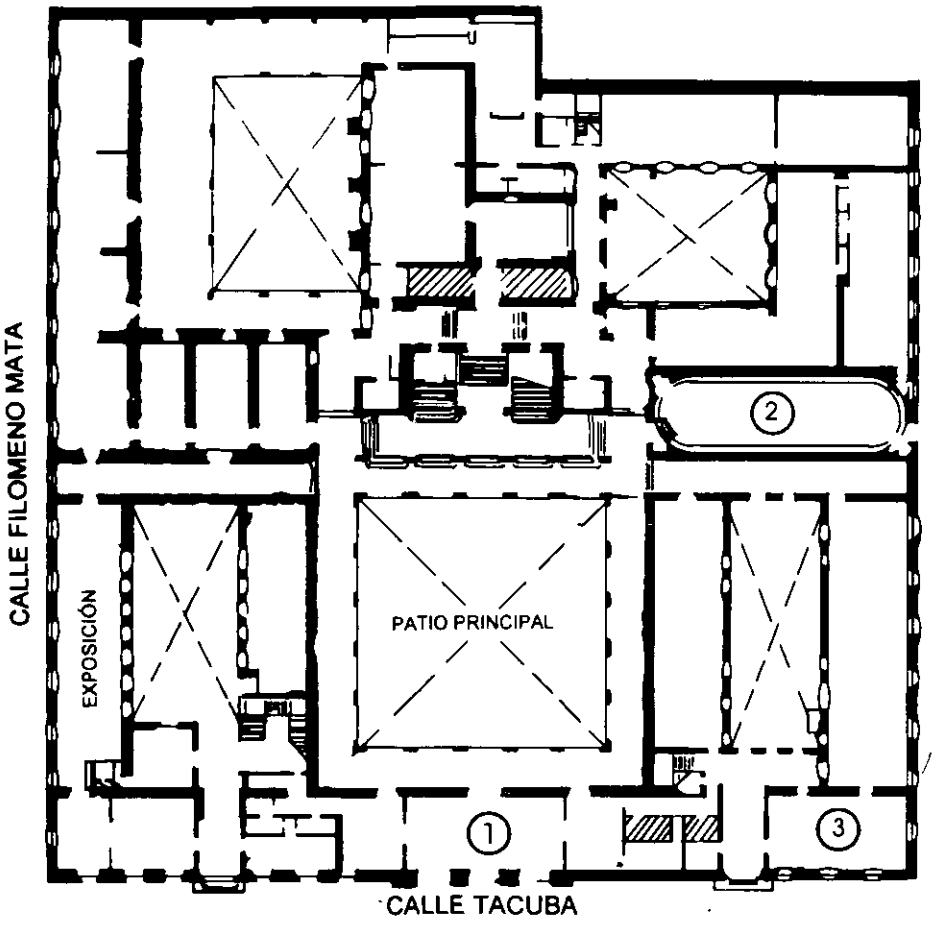
Se recomienda llenar dicha evaluación conforme los profesores impartan sus clases, a efecto de no llenar en la última sesión las evaluaciones y con esto sean más fehacientes sus apreciaciones.

Atentamente

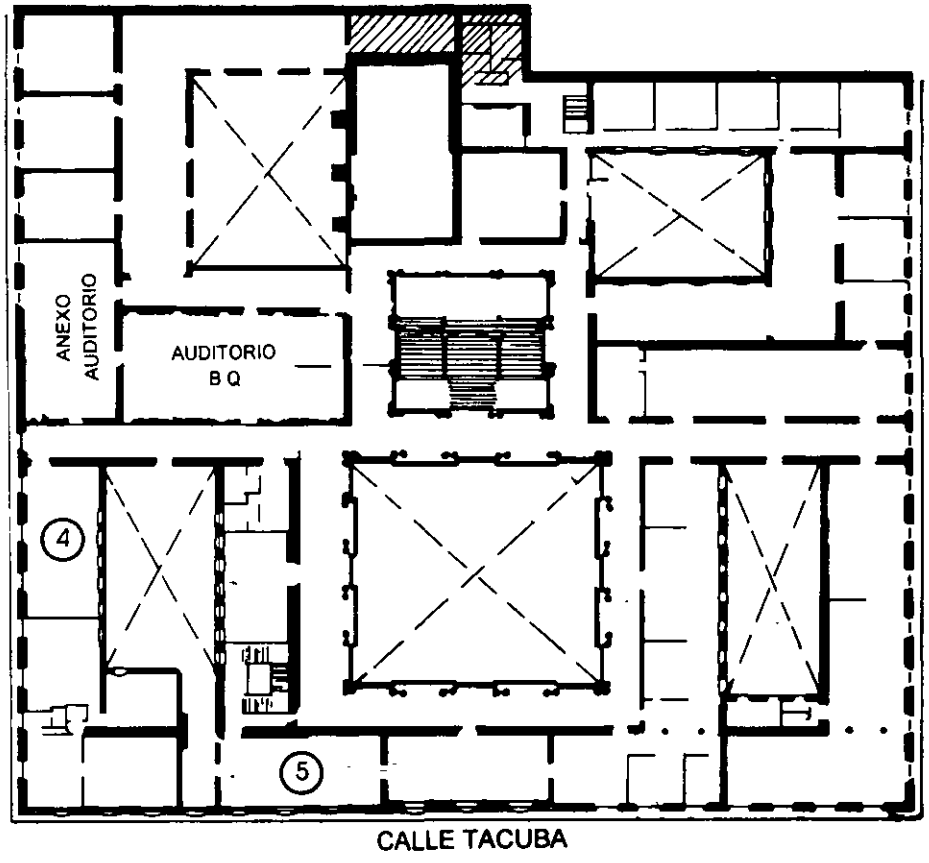
División de Educación Continua.

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg Cuauhtémoc 06000 México, D F. APDO. Postal M-2285
Teléfonos: 5512-8955 5512-5121 5521-7335 5521-1987 Fax 5510-0573 5521-4021 AL 25

PALACIO DE MINERIA

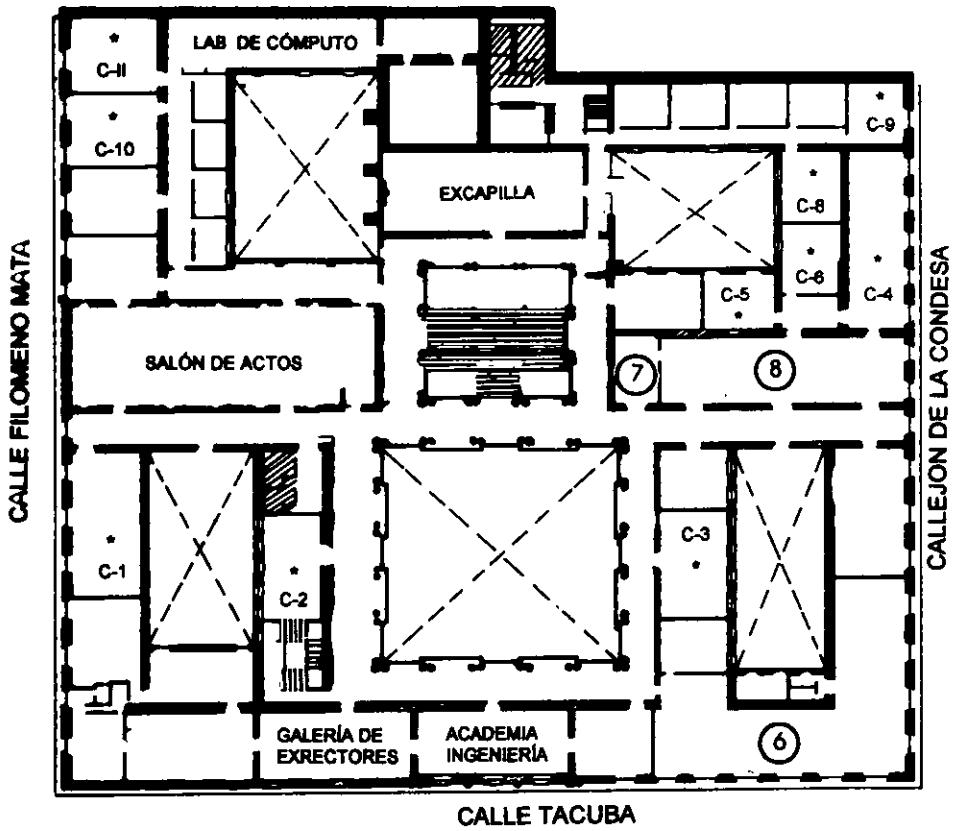


PLANTA BAJA



MEZZANINNE

PALACIO DE MINERIA



1er. PISO

GUÍA DE LOCALIZACIÓN

1. ACCESO
2. BIBLIOTECA HISTÓRICA
3. LIBRERÍA UNAM
4. CENTRO DE INFORMACIÓN Y DOCUMENTACIÓN "ING. BRUNO MASCANZONI"
5. PROGRAMA DE APOYO A LA TITULACIÓN
6. OFICINAS GENERALES
7. ENTREGA DE MATERIAL Y CONTROL DE ASISTENCIA
8. SALA DE DESCANSO

SANITARIOS

* AULAS

DIVISIÓN DE EDUCACIÓN CONTINUA
FACULTAD DE INGENIERÍA U.N.A.M.
CURSOS ABIERTOS

DIVISIÓN DE EDUCACIÓN CONTINUA
DEC

Módulo IV
REDES DIGITALES: actualidad y perspectivas

Temario

1. Introducción
1.1 Historias de las Redes Telefónicas
1.1.1 Objetivo
1.2 Modelo de Referencia OSI
1.2.1 Objetivo

2. Tecnología de Transporte
2.1 Modulación por Codificación de Pulsos PCM
2.1.1 Origen

3. Tecnologías LAN
3.1 Objetivo

4. Tecnologías WAN
4.1 Tipos de Conexiones
4.2 X.25

5. Conmutación de Paquetes
5.1 Introducción al Direccionamiento
5.2 VLSM
5.2.1 Variable Length Subnet Mask
5.2.2 Máscara de Subred Variable
5.3 Sumarización
5.4 CIDR
5.4.1 Classless InterDomain Routing
5.5 Protocolos de Enrutamiento

6. VLANs y LAN Emulation
6.1 Virtual LAN
6.1.1 Objetivos
6.2 Concentradores vs. Switches
6.2.1 Diferencias Técnicas y Económicas

7. VPN's y MPLS
7.1 MPLS-VPN Architecture Overview

FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

"Tres décadas de orgullosa excelencia" 1971 - 2001

CURSOS ABIERTOS

DIPLOMADO INTERNACIONAL EN TELECOMUNICACIONES

MODULO IV: REDES DIGITALES: ACTUALIDAD Y PERSPECTIVAS

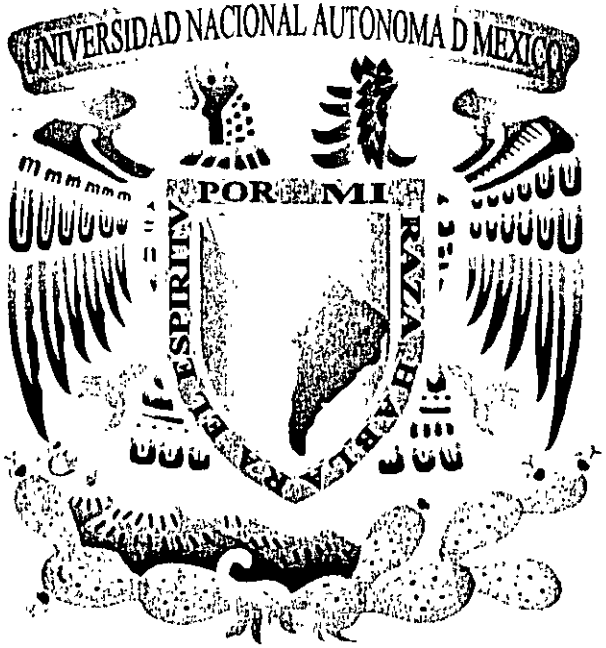
TEMA

TECNOLOGÍA DE TRANSPORTE

EXPOSITOR: ING. VICTOR OCTAVIO CID CASTILLO
PALACIO DE MINERIA
JUNIO 2001

2. Tecnología de Transporte

del 11 al 15 de junio de 2001



Diplomado Internacional en Telecomunicaciones

Módulo 4

Redes Virtuales

Actualidad y Perspectivas

del 11 al 15 de junio de 2001

1. Introducción

del 11 al 15 de junio de 2001

Historia de las Redes Telefónicas

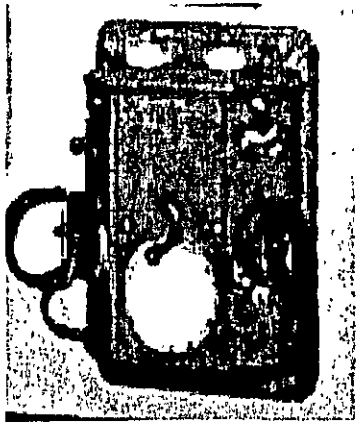
Objetivos:

- **Señalar puntos trascendentales de la historia de las redes telefónicas y de la redes de datos.**
- **Mencionar puntos importantes de la digitalización de la voz.**

De los años de 1876 a 1900:

- *Alexander Graham* Bell "Come here Mr. Watson, I want to see you!", Marzo 10 de 1876.
- En 1877 la tienda de *Charles Williams* hace los primeros teléfonos.
- 1878, Se funda el monopolio the *Bell System* a cargo de *Theodore Vail*.
- En estas mismas fechas se desarrollan las primera tarjetas de conmutación manual.

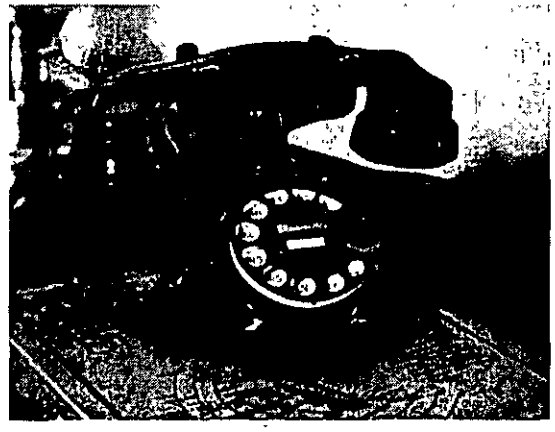
Historia de Redes Telefónicas



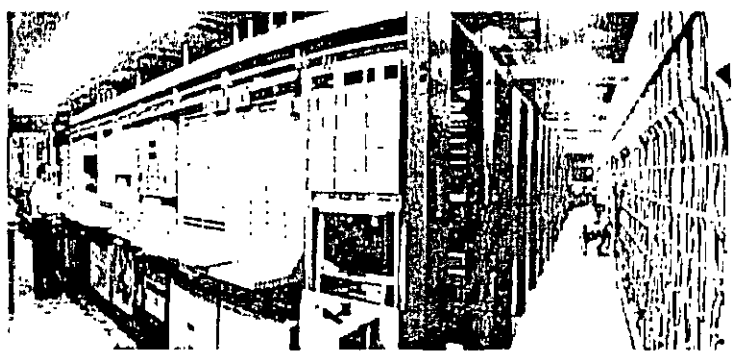
- 1879 La compañía *Western Union* cede todas sus patenetes y se forma *American Bell Company*.
- En los 1880 se instalaron los primeros circuitos metálicos.
- 1882 *Wetern Electric* comienza a ser la primera suministradora de las *Bell Companies.*
- *Automatica Strowger* 1891 inventa el teléfono de marcado automático.
- 1903 Bells enfrenta pequeñas compañías que se expanden en varios territorios.

De los años de 1901--1940

•La primera línea telefónica de costa a costa se tiende en 1915 de NY a San Francisco.
• El gobierno se hace cargo de los servicios telefónicos en 1918.
•En 1920 nace el Radio y Bell System se involucra en estos negocios.
•Para 1930 la condiciones económicas del país hacen que los servicios telefónicos y largas distancias tengan reducciones en sus ventas.



De los años de 1940—A nuestros días

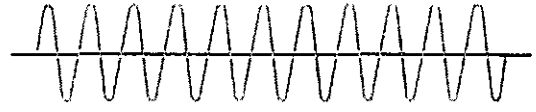


- La Segunda Guerra Mundial lleva a los Bell a realizar una serie de inovaciones tecnológicas en cuestion telefónica.
- Los primeros teléfonos móviles se instalan en 1946.
- 1947 se introduce a través de los *Bell Labs* el transistor y el curso de la historia cambió.
- 1949 viene la primera propuesta de separación de la compañía *Bell System.*
- El teléfono Princess se introduce en 1963.
- En los 60's se lanzan los primeros satélites de comunicaciones permitiendo dar servicio a millones de teléfonos.

Historia de Redes Telefónicas

- Para 1970 la FCC permite la libre competencia entre compañías.
- En 1983 se divide definitivamente la compañía *Bell System* en 7 unidades llamadas *Baby Bells.*
- En 1995 se empieza a desarrollar voz sobre IP.
- Para 1999 algunas compañías empiezan a tener tráfico de voz en redes IP.

Conversión Analógico/Digital

Como pasamos de una señal 

a una señal  **?**

R=

Modulación por pulsos codificados

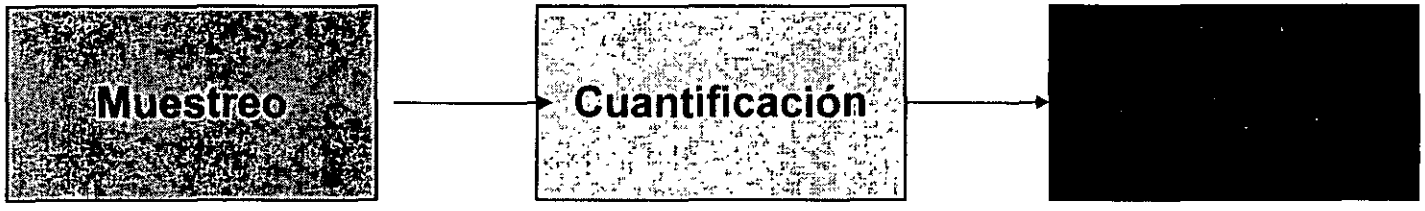
Pulse Code Modulation

PCM

Digitalización de la voz

PCM

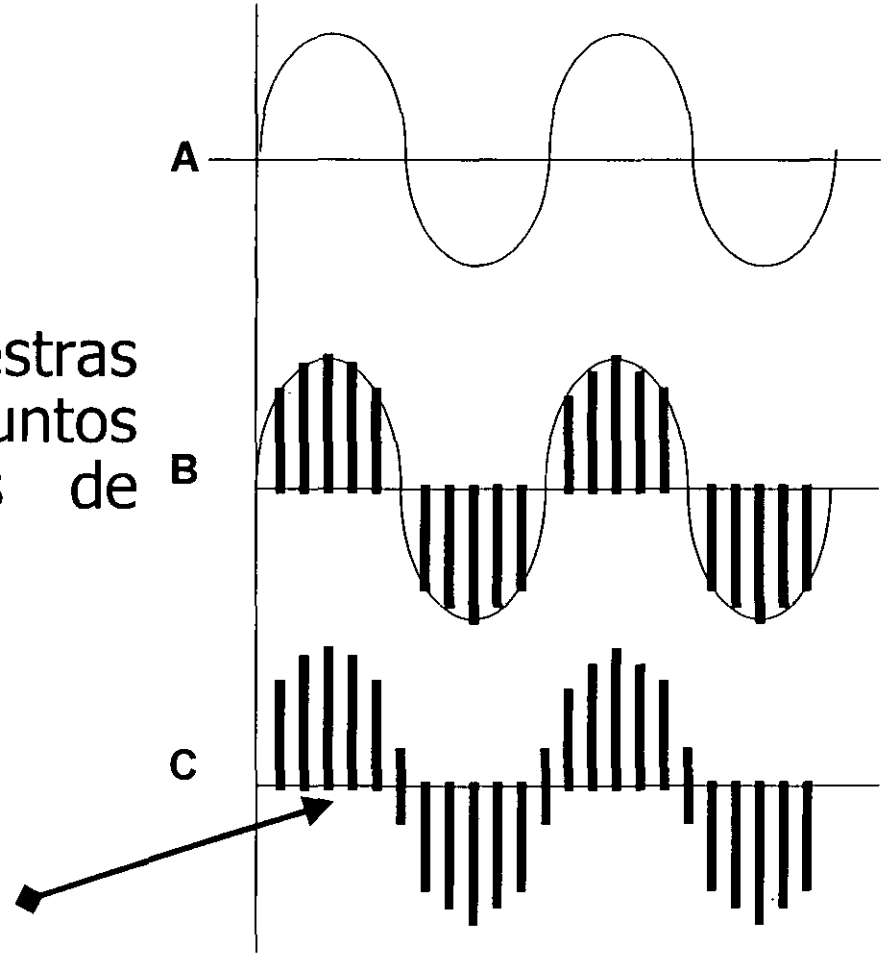
Es un método de conversión de señales analógicas a unos y ceros digitales, utilizado en la transmisión digital y consiste de tres pasos fundamentales:



Digitalización de la voz

Muestreo:

Se toman pequeñas muestras de voltaje en puntos discretos, a intervalos de tiempo predeterminados

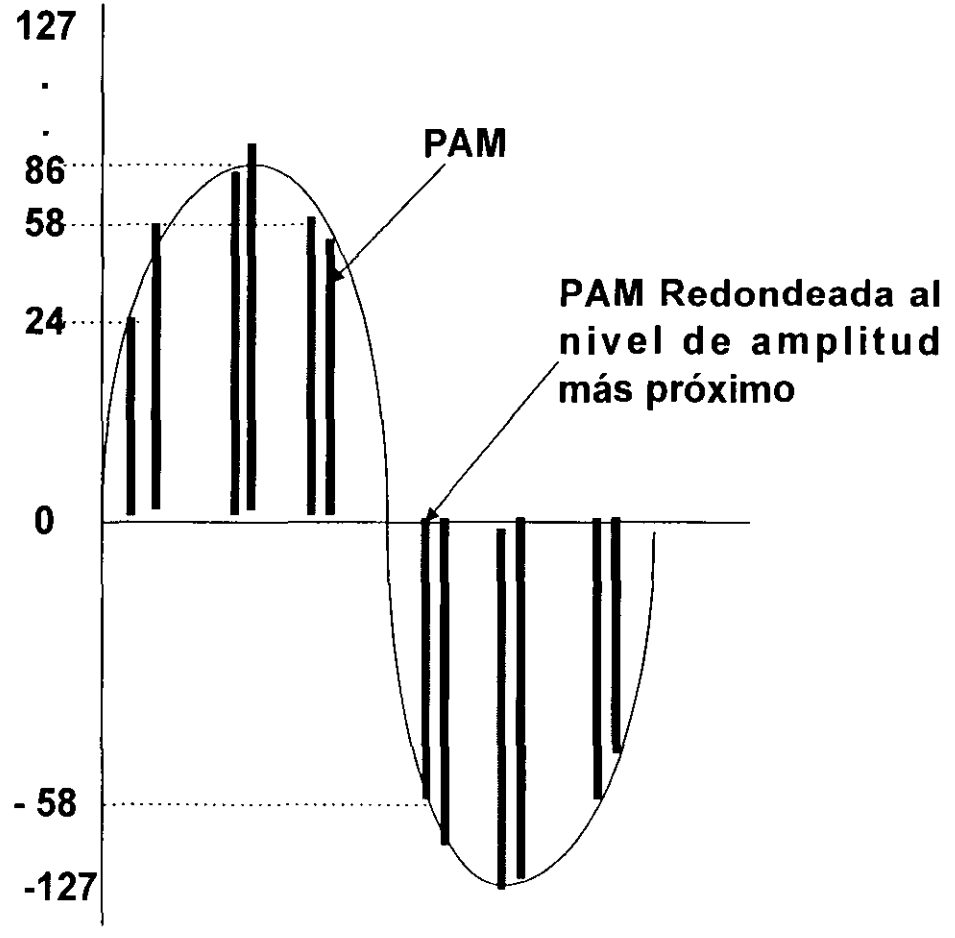


Digitalización de la voz

Cuantificación:

Cada muestra toma un valor de votaje cercano o próximo a los 256 niveles de amplitud.

Compresión con Ley A en Europa y con Ley μ en Estados Unidos y Japón, para que puedan ser representadas las ondas en su totalidad.



Codificación:

Convierte los 256 niveles de votaje de amplitud numérico posibles en códigos digitales binarios de 8 bits.

Voltaje	Código
1	00000000
2	00000000
.....	
128	00001111
.....	
256	11111111

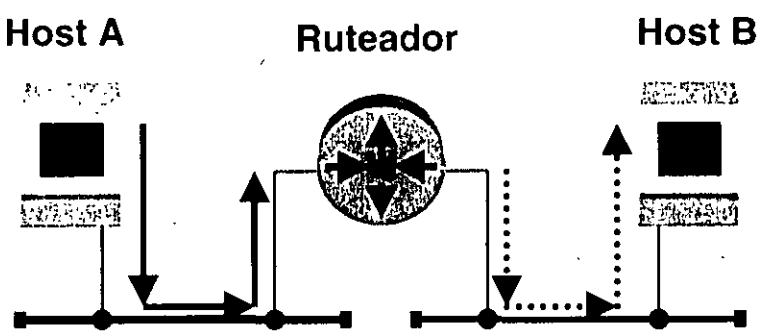
Modelo de Referencia OSI

Objetivo:

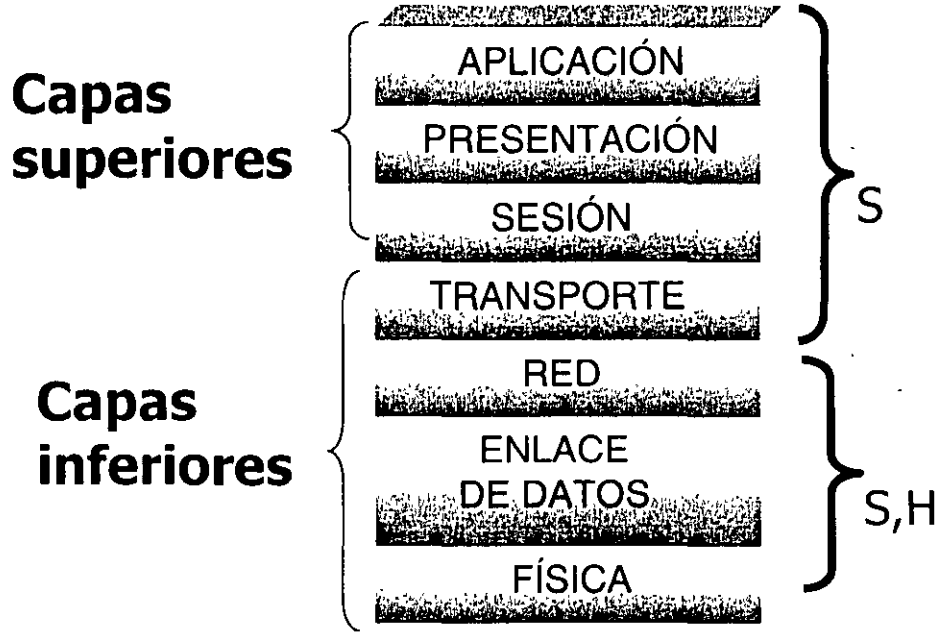
Definir el modelo de referencia OSI

Modelo de Referencia OSI

Describe como la información de una aplicación de software en una computadora se mueve a través de un medio de red y llega a otra computadora.



Modelo de Referencia OSI



- Desarrollado por ISO en 1984.
- Es un modelo conceptual de siete capas.
- Cada capa tiene tareas específicas.

S=software
H=hardware

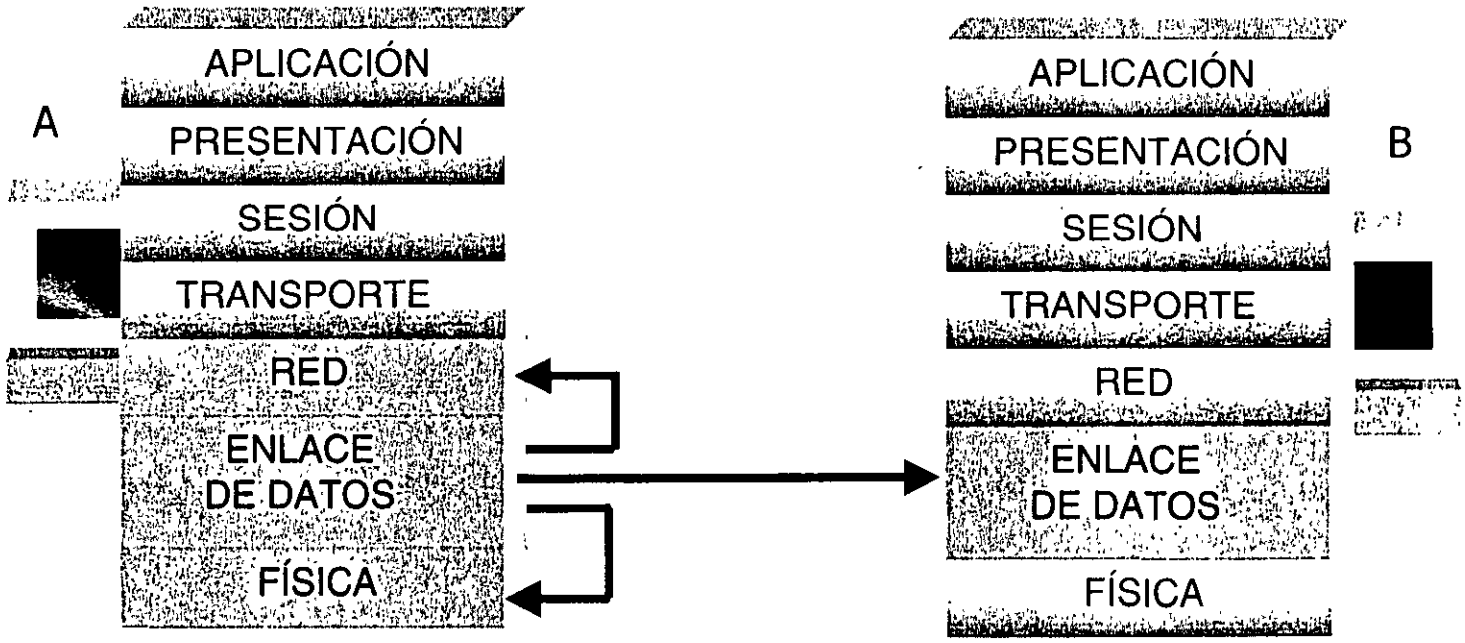
Protocolos

En el mundo de las redes de datos, un protocolo es un conjunto formal de reglas y convenios que determinan como las computadoras intercambian la información sobre un medio de redes.

- El modelo en si NO ES UN MÉTODO DE COMUNICACIÓN!.
- La comunicación se hace utilizando:
  - Protocolos LAN(capa 1 y 2)
  - Protocolos WAN(capa 1,2 y 3)
  - Protocolos de red(capas 5,6,7)
  - Protocolos de ruteo.(capa 3)

Modelo de Referencia OSI

Interacción entre capas

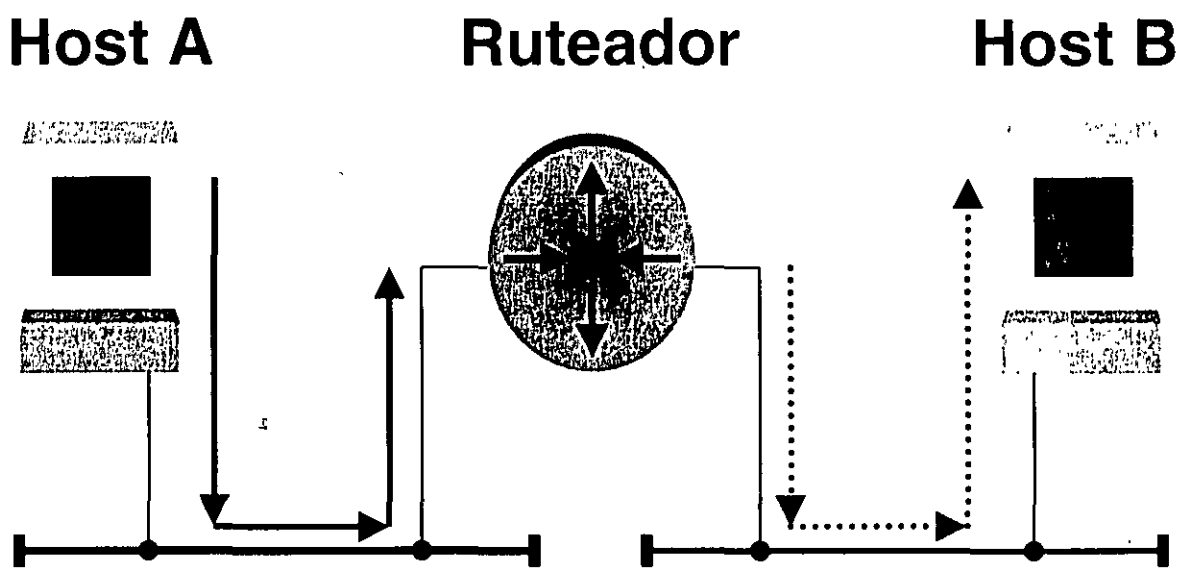


- Si una capa se quiere comunicar con otra, esta última da el servicio.
- Los servicios de las capas adyacentes le ayudan con la capa pareja.

Encapsulamiento

Consiste en agregar datos que han sido pasados hacia abajo por una capa superior, utilizando los *Headers* y *Trailers* .

La **Información de control** consiste de peticiones específicas y de Instrucciones que son intercambiadas entre las capas parejas de OSI



Formatos de la Información

FRAME

Es la unidad de información que se manejan entre las capas enlace de datos. Consta de HEADER, datos de las capas superiores y posiblemente Trailer.

PACKET

Es la unidad de información que se manejan entre las capas de red cuando se usa el servicio orientado a conexión. Consta de HEADER, datos de las capas superiores y Posiblemente Trailer.

DATAGRAM

Es la unidad de información que se manejan entre las capas de red cuando se usa el servicio no orientado a conexión. Consta de HEADER, datos de las capas superiores y Posiblemente Trailer.

SEGMENT

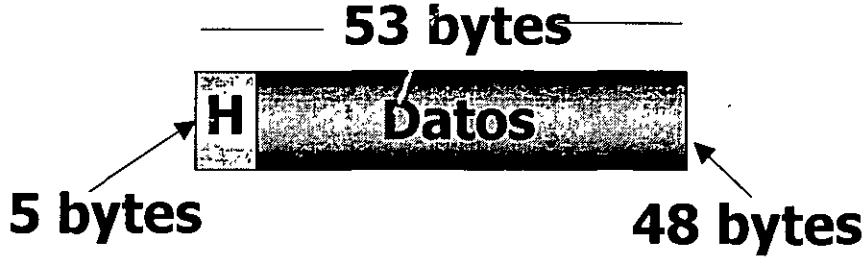
Se refiere a la unidad de información cuya fuente y destino son las capas de transporte.

MESSAGE

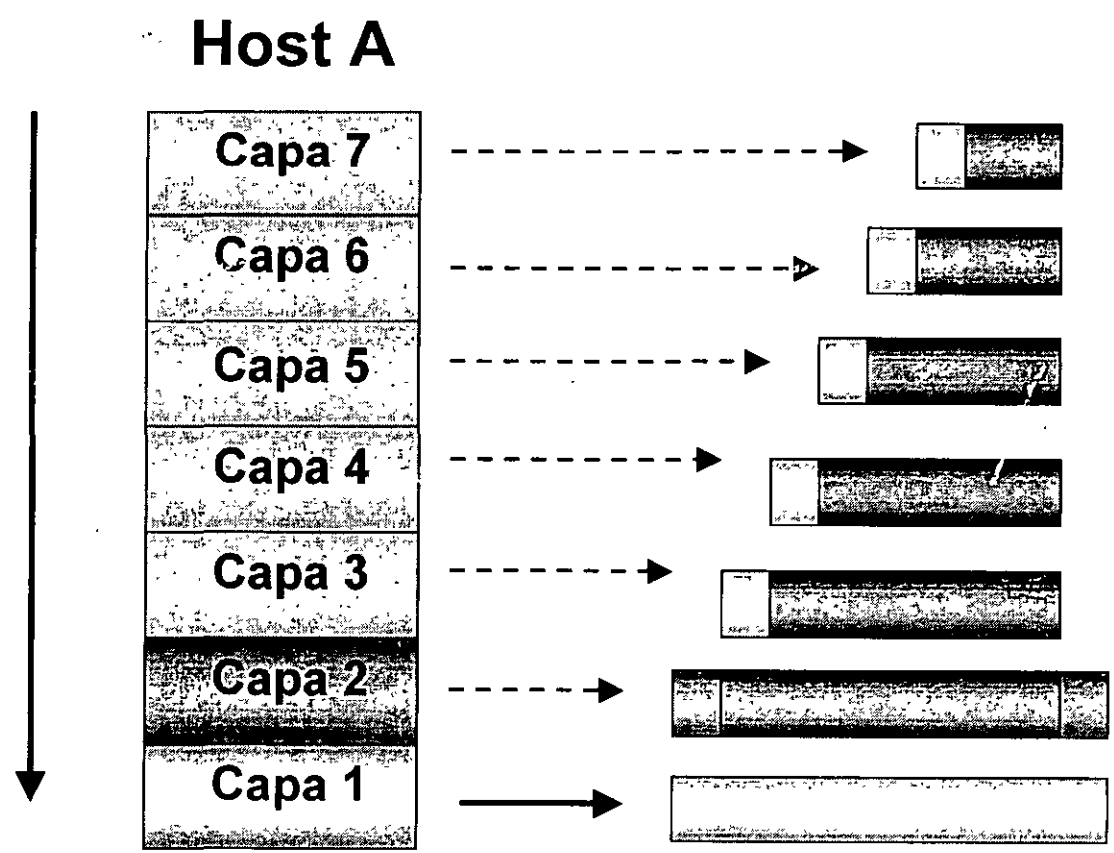
Es la unidad de información que se manejan entre las capas superiores a las de red.

Cell

Es la unidad de información de tamaño fijo que se manejan entre las capas de enlace de datos y son utilizadas en ambientes de redes switcheables como ATM.. Consta de HEADER y PAYLOAD.

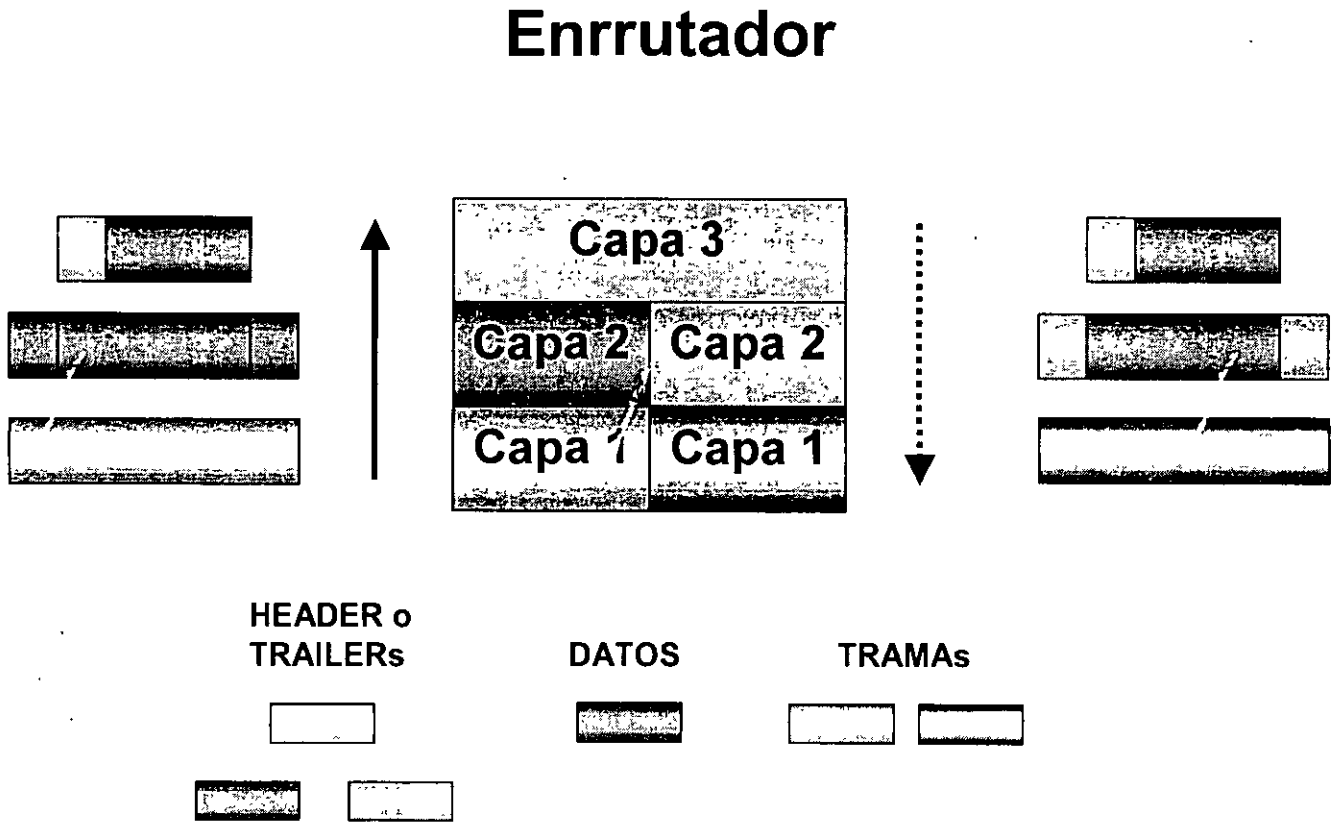


Encapsulamiento

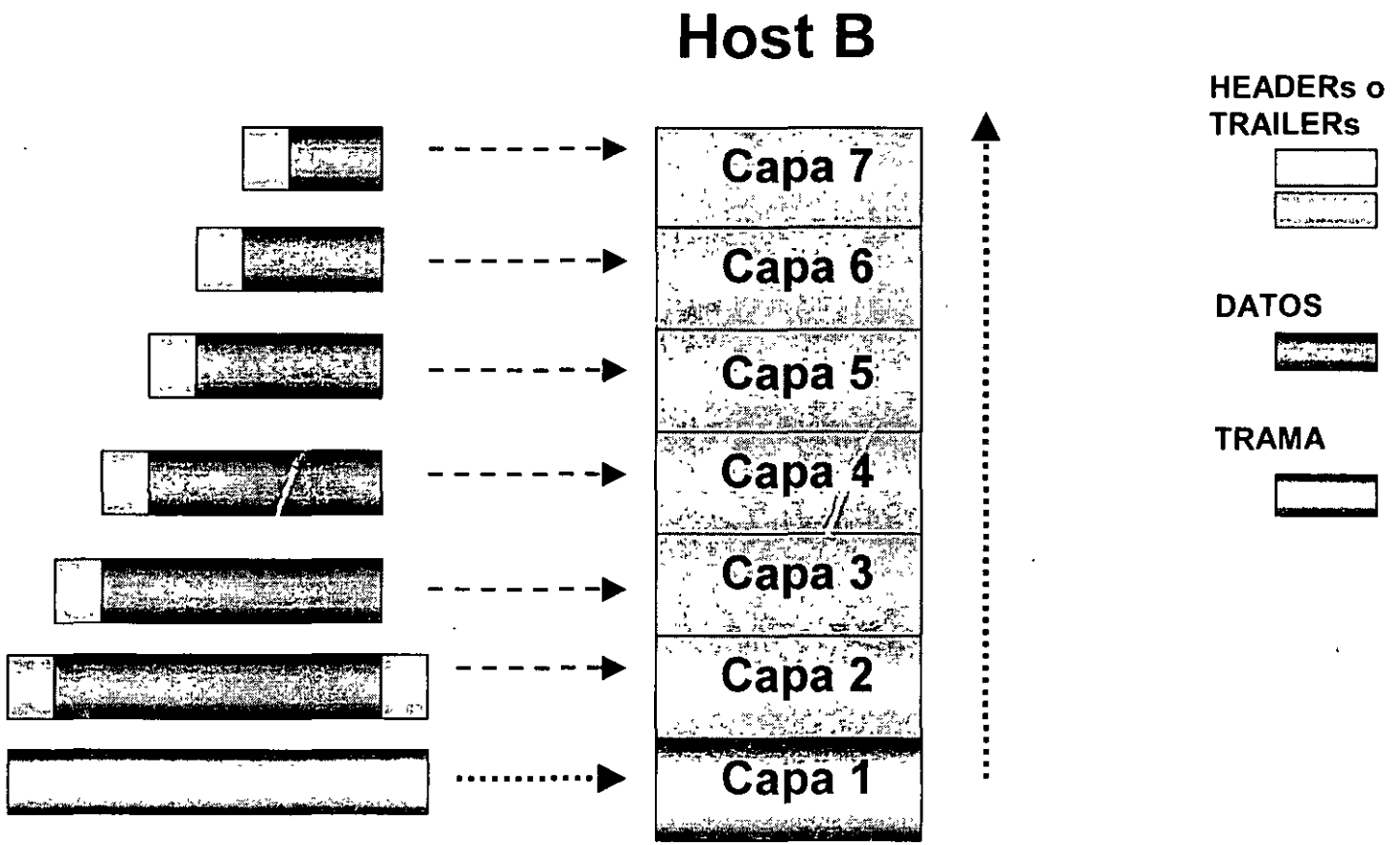


Modelo de Referencia OSI

Encapsulamiento



Encapsulamiento

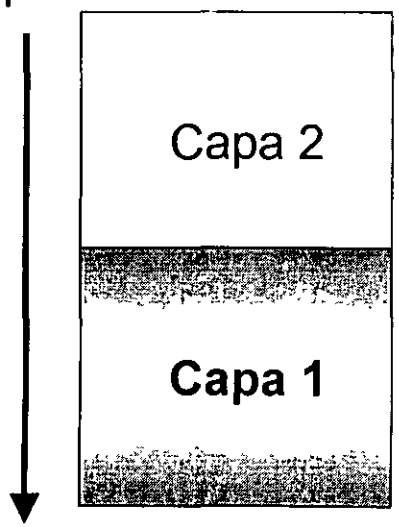


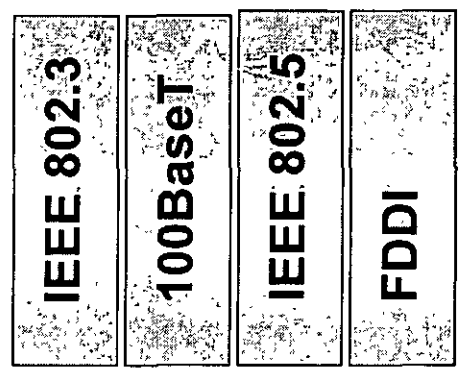
Capa Física

En ésta capa se define las especificaciones eléctricas, mecánicas, funcionales y de procedimiento para activar, mantener y desactivar el enlace físico de los sistemas de redes que se estén comunicando.

Por ejemplo:

- Relaciona propiedades físicas de la interfaz con el medio de transmisión.
- Niveles de voltaje de bits así como tasa de transmisión.
- Funciones entre los circuitos individuales de la interfaz y el medio de Tx.
- Especifica la secuencia de eventos por la cual se intercambia un flujo de bits.



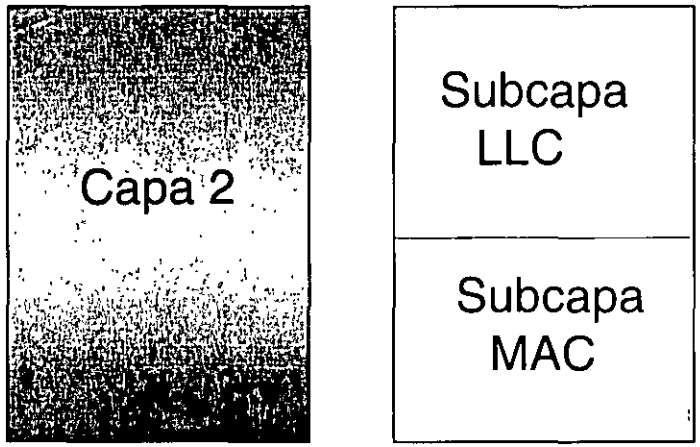


EIA-TIA 232
V.24 V.35
HSSI G703
EIA 530
X.21bis SIP

Capa de Enlace de Datos

Mientras la capa física proporciona solamente un servicio bruto de datos, la capa de enlace intenta hacer el enlace físico confiable.

- Notifica errores a las capas superiores cuando un error de transmisión a ocurrido.
- Maneja direccionamiento físico.
- Define como están lo equipos físicamente conectados, ej. bus o anillo.
- Sirve como moderador para el control de flujo.



LLC: Logical Link Control:

- Maneja la comunicación entre equipos sobre un solo enlace.
- Soporta servicios orientados y no orientados a conexión pedido por la capa superior.

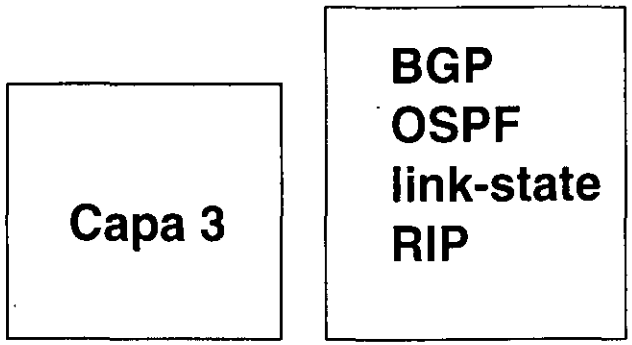
MAC: Media Access Control

- Maneja los protocolos de acceso al medio.
- Define MAC address.

Capa de Red

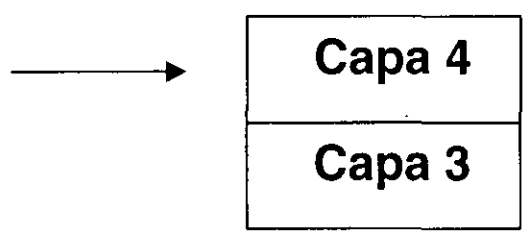
Proporciona los medios para transferencia de información entre sistemas finales a través de algún tipo de red de comunicación.

- Maneja direccionamiento lógico
- Realiza funciones de ruteo para especificar la dirección destino y solicitar ciertas facilidades de la red.
- Maneja varios enlaces a la vez
- Los protocolos que se manejan en esta capa generalmente son protocolos de ruteo.



Capa de Transporte

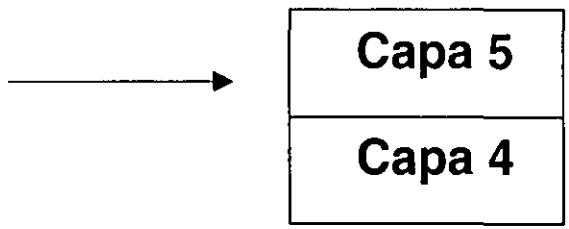
- Intercambia datos entre sistemas finales.
- El servicio de transporte orientado a conexión asegura que los datos lleguen libres de errores, en secuencia y sin pérdidas.
- Maneja el control de flujo entre sistemas finales.
- Multiplexa los datos para que varias aplicaciones sean envíadas por un solo enlace físico.
- Establece rutas virtuales(circuitos virtuales), las cuales establece, las mantiene y termina.
- Checa errores y los restablece haciendo uso de la retransmisión.



Capa de Sesión

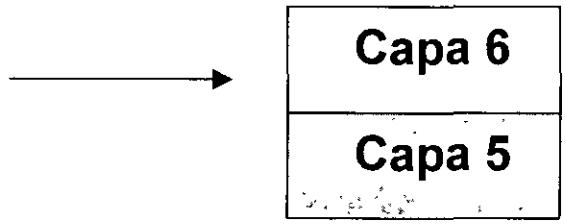
Controla el diálogo entre aplicaciones en los sistemas finales:

- Establece, mantiene y termina la sesión de comunicación entre las capas de presentación.
- Consta de Petición de servicios y Respuesta de servicios solicitados por las aplicaciones que se estén corriendo en los diferentes equipos.
- Define si el diálogo es full-duplex o semi-duplex.
- Agrupamiento marcando el flujo de datos.
- Recuperación proporcionando un mecanismo de comprobación.
- Casi no es utilizado en redes actuales.



Capa de Presentación

Define el formato de los datos que se van a intercambiar entre las aplicaciones y ofrece a los programas de aplicación un conjunto de servicios de conversión y codificación que son aplicados a la capa de aplicación asegurando que la información enviada por la capa de aplicación de un sistema sea entendida en el otro sistema.
Ejemplos:
MPEG,TIFF,JPEG,GIF..

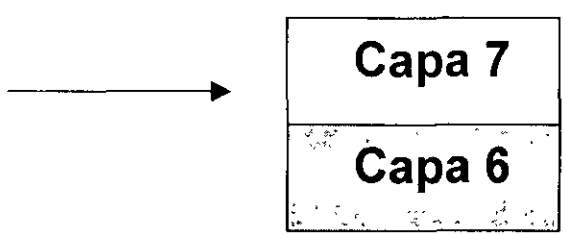


Capa de Aplicación

Proporciona un medio a los programas de aplicación para que accedan al entorno OSI.

- Es la capa más cercana al usuario final.
- La capa de aplicación y el usuario interactúan directamente con el software de aplicación.

Ejemplos:
Transferencia de archivos
Terminal virtual(VTP)
Protocolo de información de gestión común (CMIP)



FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

"Tres décadas de orgullosa excelencia" 1971 - 2001

CURSOS ABIERTOS

DIPLOMADO INTERNACIONAL EN TELECOMUNICACIONES

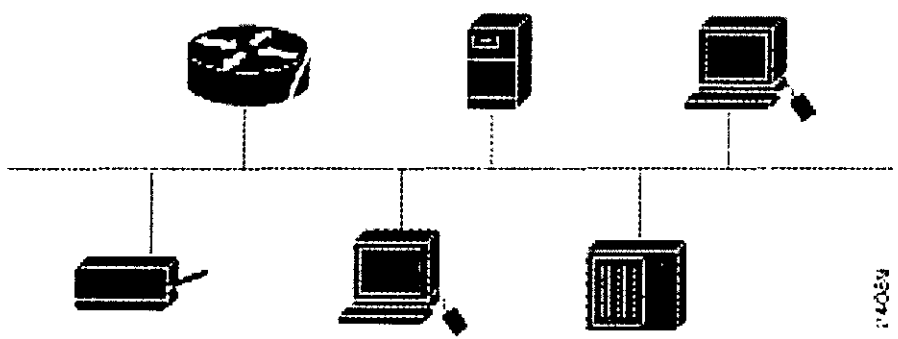
MODULO IV: REDES DIGITALES: ACTUALIDAD Y PERSPECTIVAS

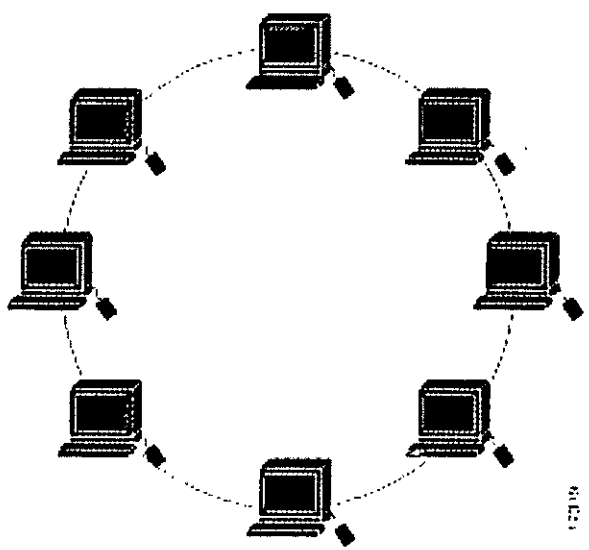
TEMA

TECNOLOGÍAS LAN

EXPOSITOR: ING. RODOLFO ARIAS VILLAVICENCIO
PALACIO DE MINERIA
JUNIO 2001

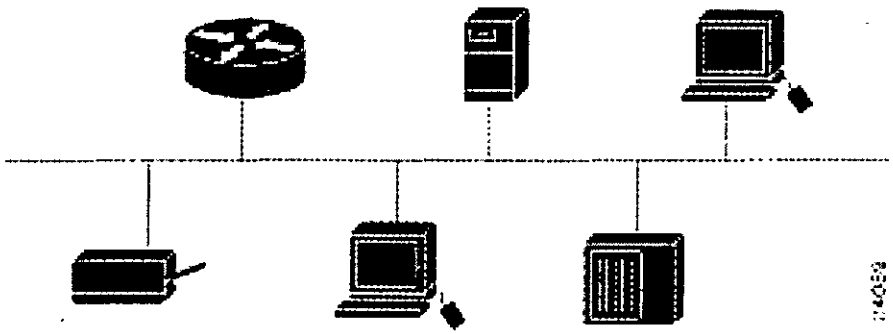
3. Tecnologías LAN

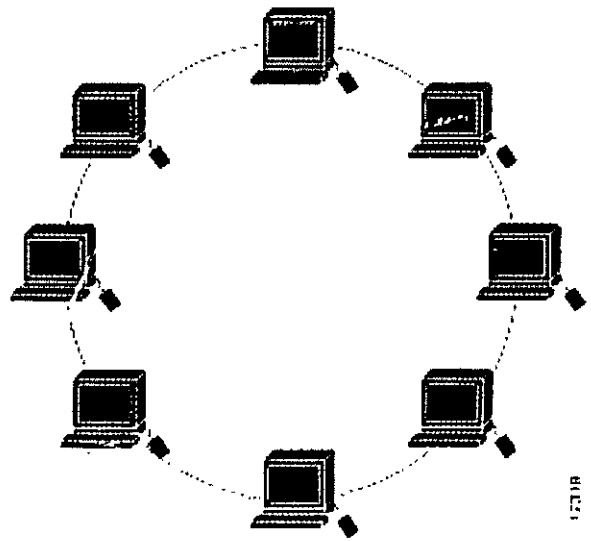




del 11 al 15 de junio de 2001

Tecnologías LAN





Objetivos

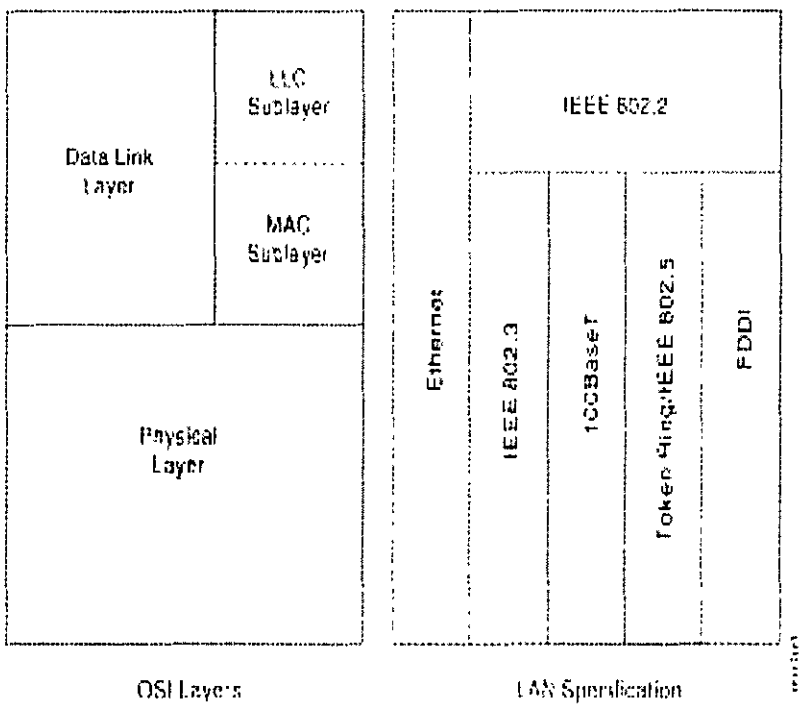
- Describir el modelo de referencia IEEE 802

- Describir las principales tecnologías LAN basadas en el modelo IEEE 802

Objetivos

- Describir el modelo de referencia IEEE 802
- Describir las principales tecnologías LAN basadas en el modelo IEEE 802

Arquitectura LAN 802



LLC 802.2:

- Define la aplicación fuente y destino
- Control de flujo
- Tipo de datagrama
- Transporta información de capas superiores.

Formato LLC

1	1	2	Variable	Octetos
DSAP	SSAP	Control	Información	

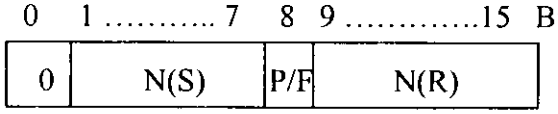
DSAP: Destination Service Access Point
SSAP: Source Service Access Point

Campo de Control

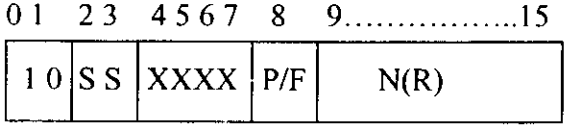
- Define el tipo de trama que se transmite
  - Información
    - Información de usuario
  - Supervisión
    - Control de la conexión
  - No numerada
    - Establecimiento, mantenimiento y terminación de la sesión

- Control de Flujo

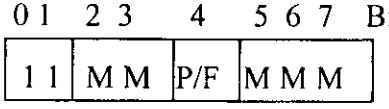
Campo de Control



Frame I

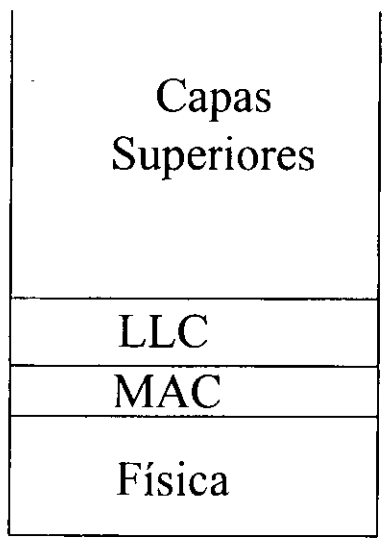


Frame S



Frame U

Arquitectura LAN 802



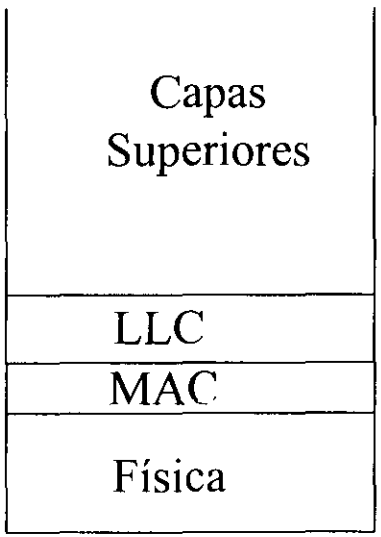
MAC

- Define el formato de trama
- Direccionamiento físico
- Detección y control de errores
- Control de acceso al medio
- Relacionado con la topología y medio de transmisión

Capa MAC

- Control de acceso al medio
- Direccionamiento físico
- Determina longitud máxima de datagrama, al interactuar con la capa física
- Detección de errores
- Control de errores al interactuar con la subcapa LLC

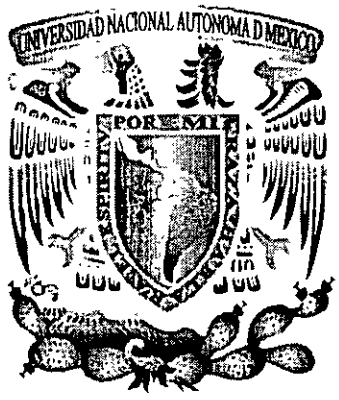
Arquitectura LAN 802



Física
- Topología
- Distancias mínimas y máximas del medio de transmisión
- Código de línea

Capa Física

- Define topología
- Define el medio de transmisión
- Código de línea
- Limites físicos
- Características eléctricas
- Sincronía



Ethernet

Características

Topología

CSMA/CD

Formato del frame

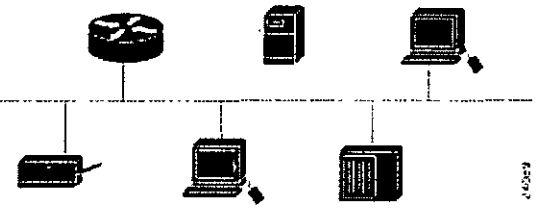
Implementación Física

Características

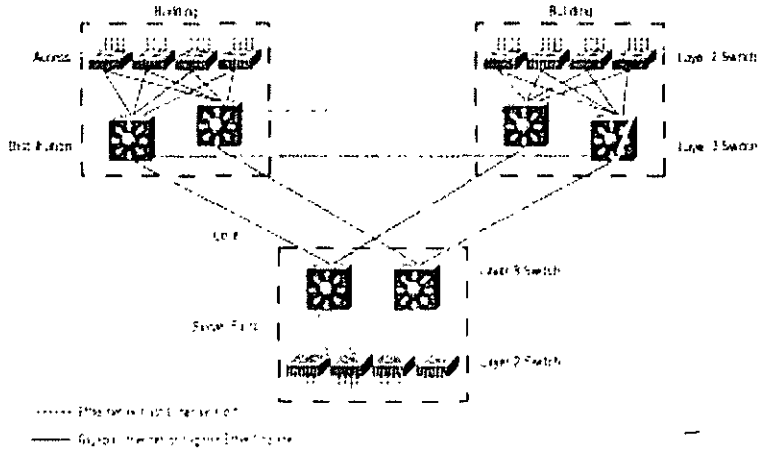
- **Extremadamente sencilla de implementar**
- **Técnica de acceso al medio tipo contención**
- **Red no determinística**
- **Bus lógico**
- **Tasas de transmisión de 10, 100 y 1000 Mbps**
- **Tamaño máximo de trama de 1518 bytes y mínimo de 64 bytes**
- **Diferentes medios de trasnmisión**
- **Es el tipo de red que tiene la mayor penetración en el mercado**

Topología

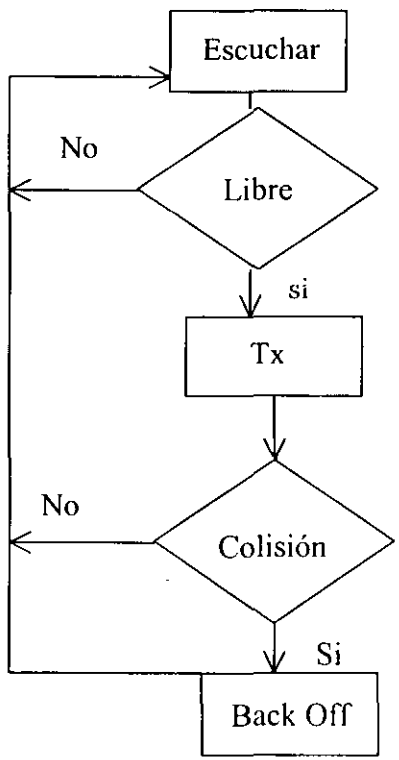
Lógica



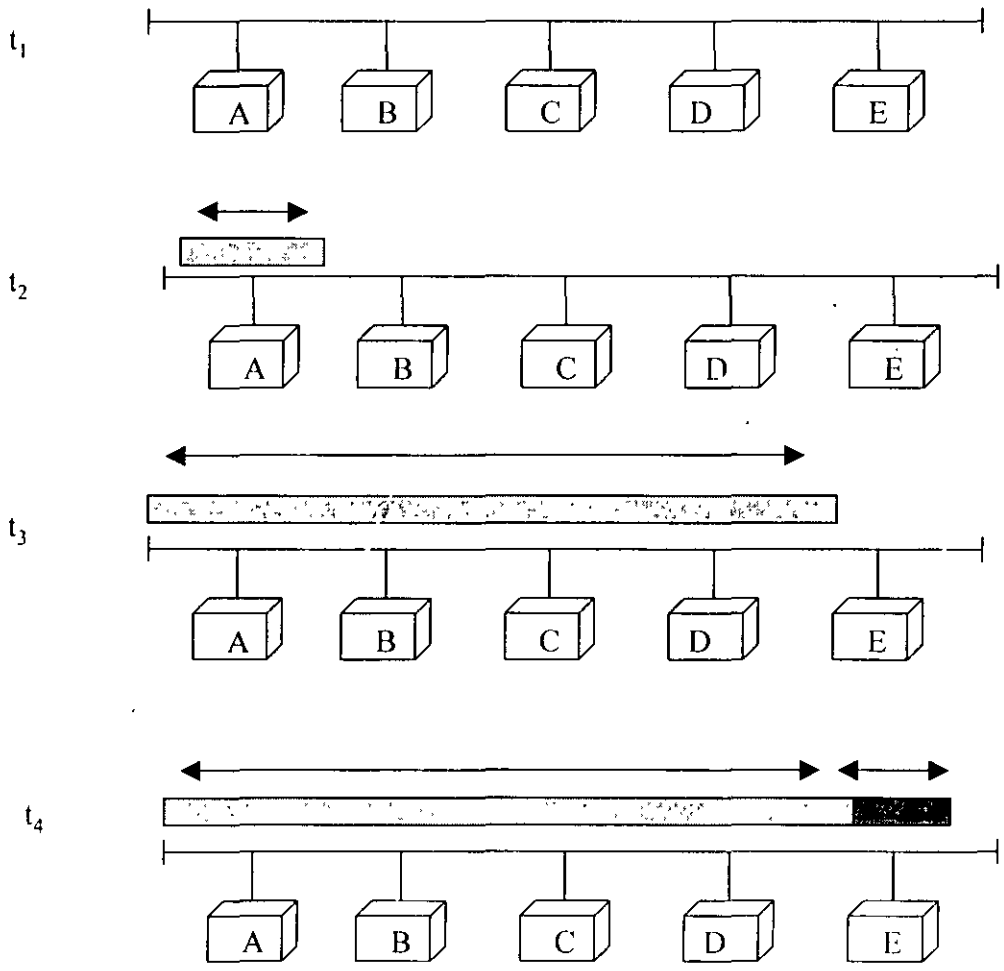
Física



CSMA/CD



Tecnologías LAN

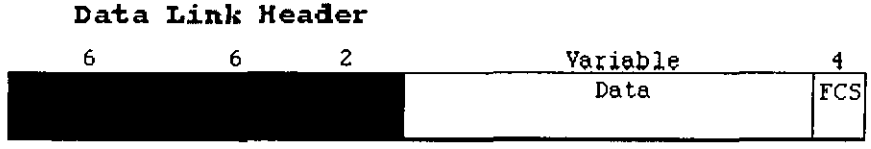


Algoritmo de Bakc Off

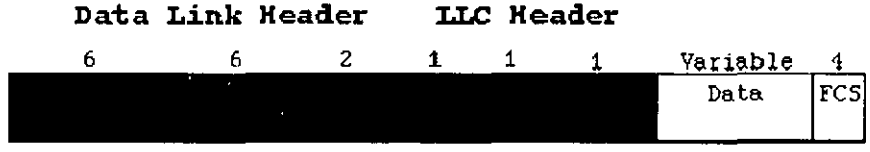
1. Selecciona un número aleatorio del rango 0 a 2^n - 1
   n = Número de colisiones detectadas para una transmisión determinada
2. Multiplica el número aleatorio x 51.2 μs
3. Incrementan hasta un valor de 10
4. Repite este valor 5 veces más
5. Si la colisión persiste manda un error de capas superiores

Formato del Frame

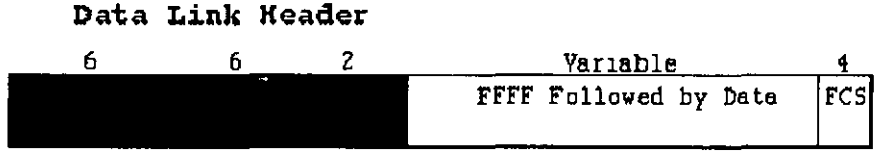
Versión 2



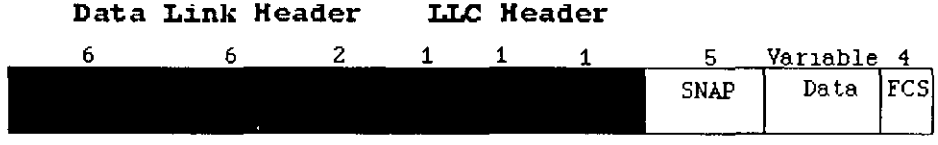
802.3



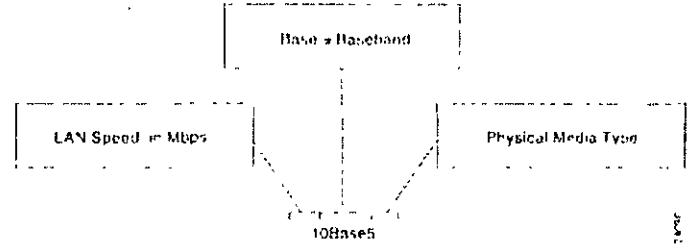
Novell



SNAP



Implementación Física



Característica	Ethernet Value	Valores IEEE 802.3				
		10Base5	10Base2	10BaseT	10BaseFL	100BaseT
Tasa de transmisión (Mbps)	10	10	10	10	10	100
Método de señalización	Baseband	Baseband	Baseband	Baseband	Baseband	Baseband
Máxima longitud de cable (m)	500	500	185	100	2,000	100
Medio	50-ohm coax (thick)	50-ohm coax (thick)	50-ohm coax (thin)	Unshielded twisted-pair	Fiber-optic	Unshielded twisted-pair
Topología física	Bus	Bus	Bus	Star	Point-to-point	Bus

10 Base 5

Coaxial grueso
Manchester
Bus lineal
Max. Longitud de segmento 500 m
Max. de segmentos 5
Distancia mínima entre estaciones 2.5 m
Max. de nodos por segmento 200

10 Base 2

Coaxial delgado
Manchester
Bus lineal
Max. Longitud de segmento 185 m
Max. de segmentos 5
Distancia mínima entre estaciones 0.5 m
Max. de nodos por segmento 370

10 Base T

UTP
Manchester
Estrella
Max. Longitud de segmento 100 m
Max. de segmentos 4

Evoluciones

- Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet

Fast Ethernet

Características	100BaseTX	100BaseFX	100BaseT4
Cable	UTP categoría 5, o STP Tipo 1 y 2	Fibra multimodo 62.5/125 micron	UTP categoría 3, 4, o 5
Número de pares o hilos	2 pares	2 hilos	4 pares
Conector	Conector ISO 8877 (RJ-45)	Conector Duplex SCmedia-interface (MIC) ST	Conector ISO 8877 (RJ-45) c
Máxima longitud del segmento	100 metros	400 metros	100 metros
Máxima longitud de la red	200 metros	400 metros	200 metros

Autonegociación

100BASE-TX full duplex

100BASE-T4

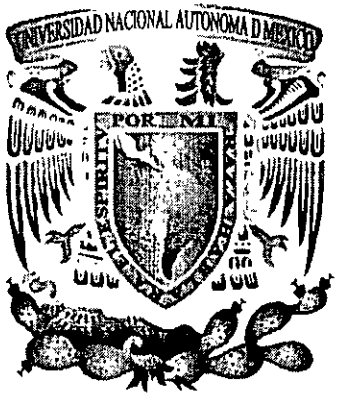
100BASE-TX

10BASE-T full duplex

10BASE-T

Gigabit Ethernet

1 Gbps
10 Gbps
MTU mínimo de 512 bytes
X3T11 en capa física
8B10B



Token Ring 802.5

Carácterísticas

Topología

Token passing

Formato del frame

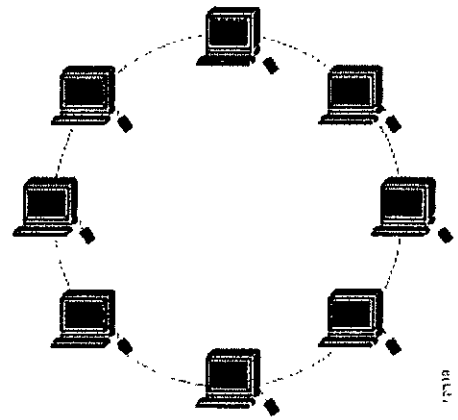
Funciones de supervisión

Características

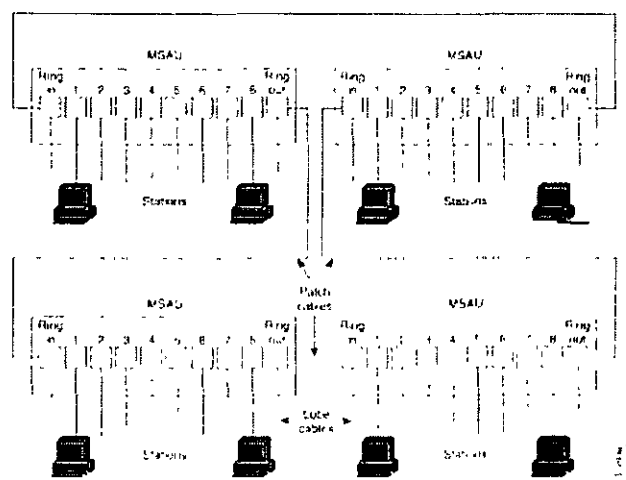
- **Esquema de acceso al medio round-robin con opciones de prioridad y reservación**
- **Red tipo determinística**
- **Velocidades de 4 y 16 Mbps**
- **Tamaño de trama de 4500 bytes como máximo**
- **Topología lógica tipo anillo**
- **Red de soporte para aplicaciones propietarias de IBM, como SNA**

Topología

Lógica



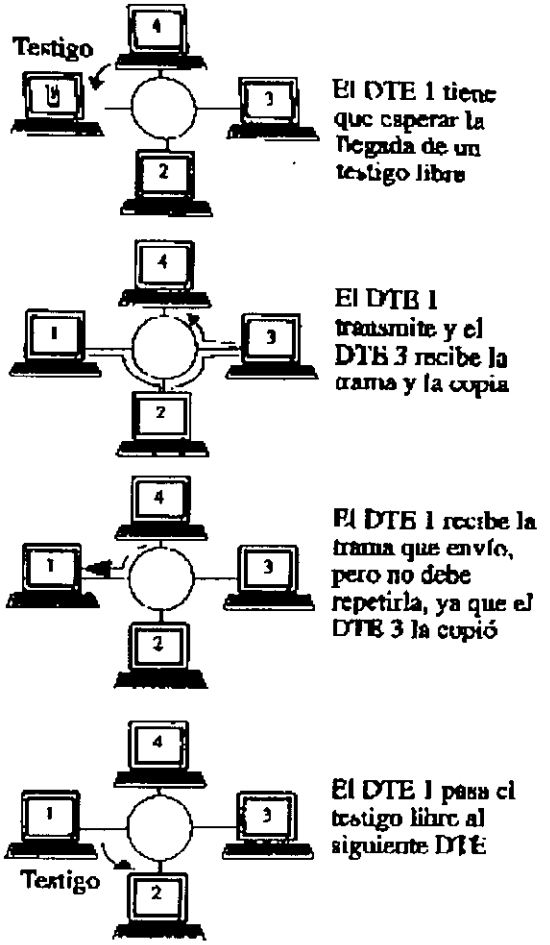
Física



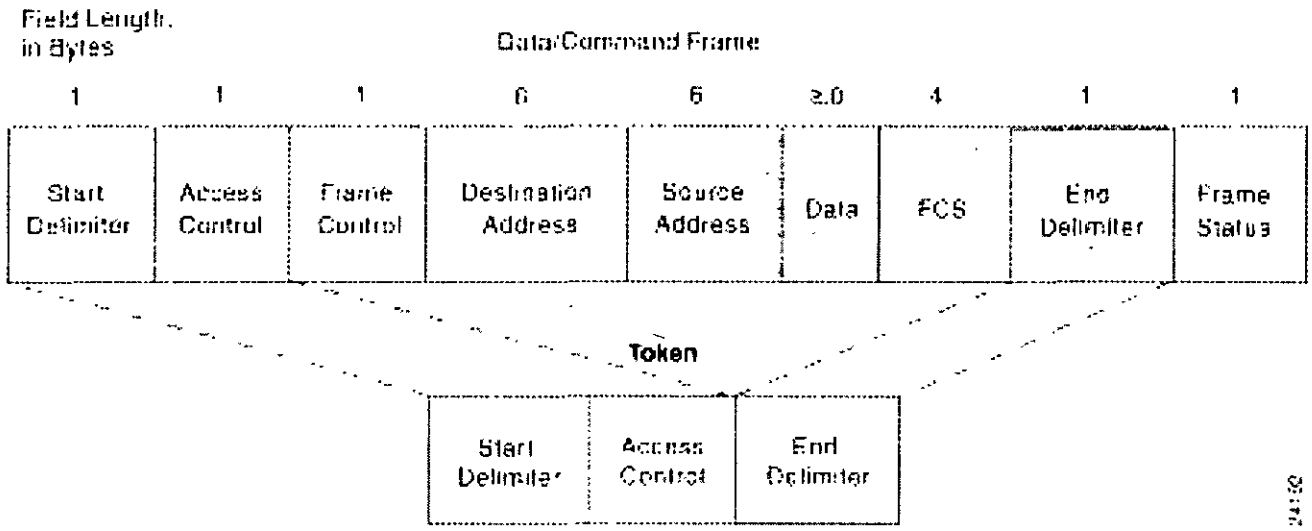
Token Passing

- **Uso de un frame especial llamado "token"**
- **Esquema Round Robin**
- **Opciones de prioridad y reservación para transmitir**

El DTE 1 desea enviar una trama al DTE 3



Formato del Frame



Funciones de Supervisión

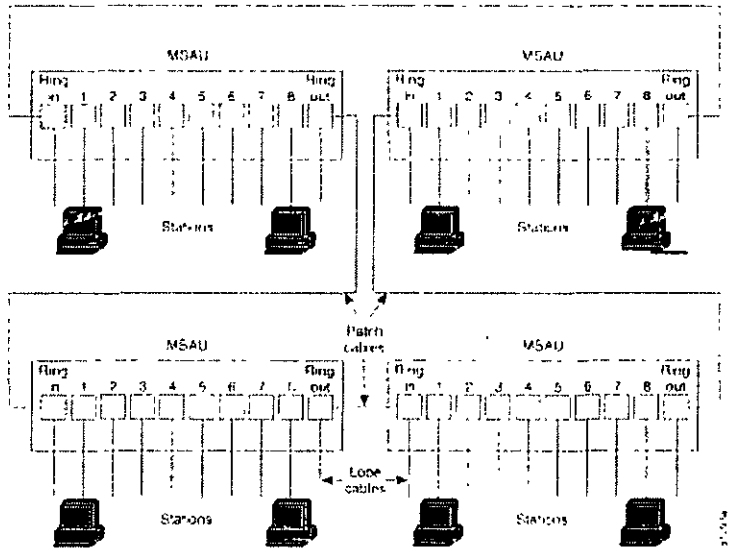
Monitor Activo

- **Frames no reclamados**
- **Generación del primer token**
- **Estabilización del anillo**

Monitor contention, selección del monitor activo

Implementación Física

	IBM Token Ring	IEE 802.5
Tasa de transmisión	4 ó 16 Mbps	4 ó 16 Mbps
Dispositivos por segmento	260 (STP) 72 (UTP)	250
Topología física	Estrella	Estrella
Medio	Par trenzado	Par trenzado
Metodo de acceso	Token passing	Token passing



FDDI

Características

Topología

Tipos de nodos

Arquitectura

Redundancia

Formato del frame

MAC

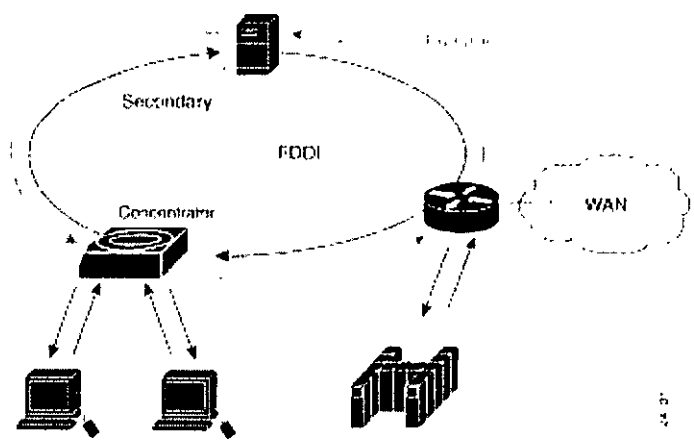
Características

- Red basada en fibra óptica.
- Utiliza un código 4B5B.
- Velocidad de datos de 100Mbps.
- Topología de anillo doble.
- Baja tasa de error (una en un billón).
- Conmutadores ópticos opcionales.
- Tamaño de paquete variable, máximo 4500 bytes.
- Eficiencia de un 80% con una frecuencia de 125 MHz

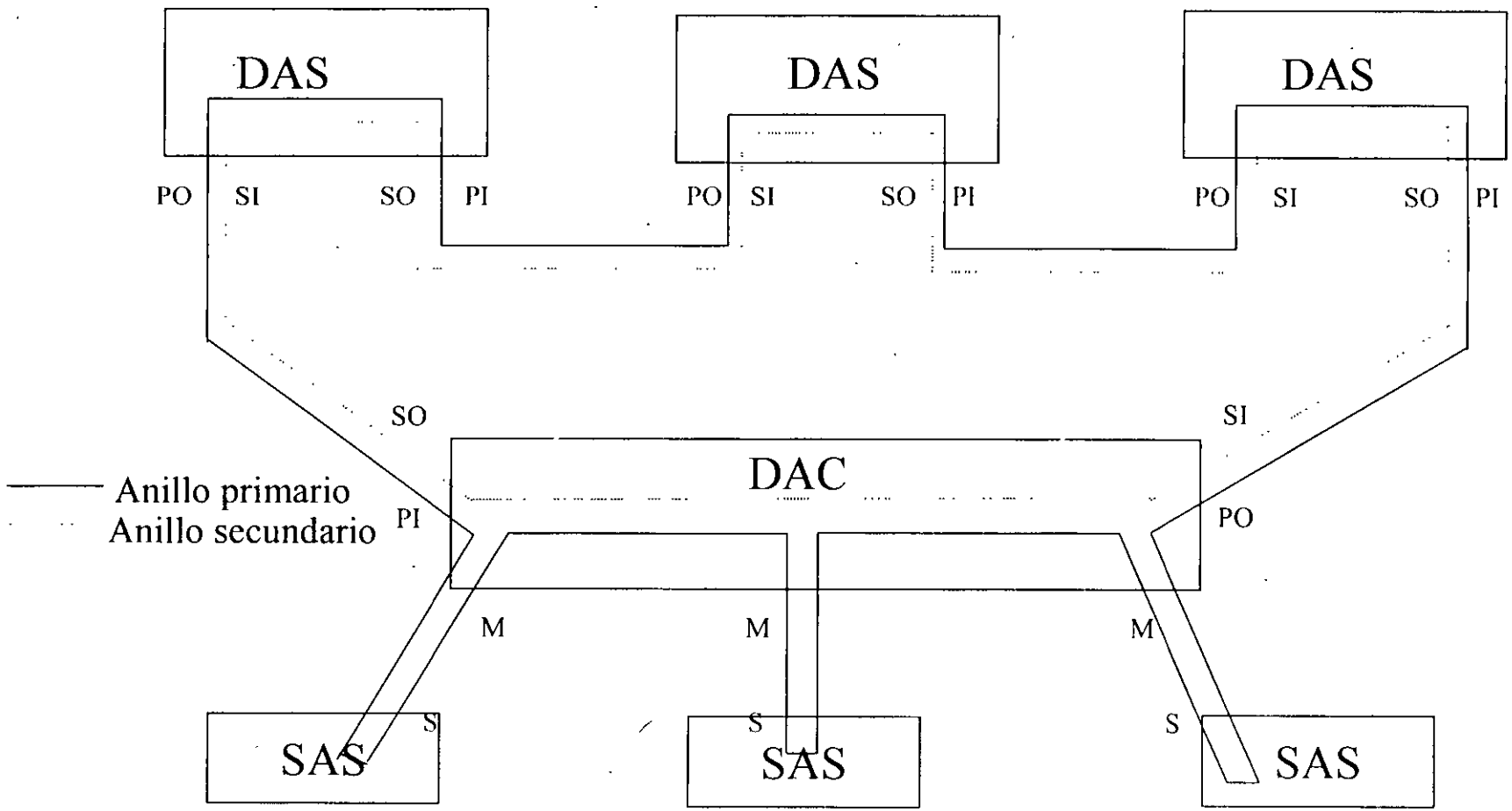
Topología

Lógica: Doble anillo

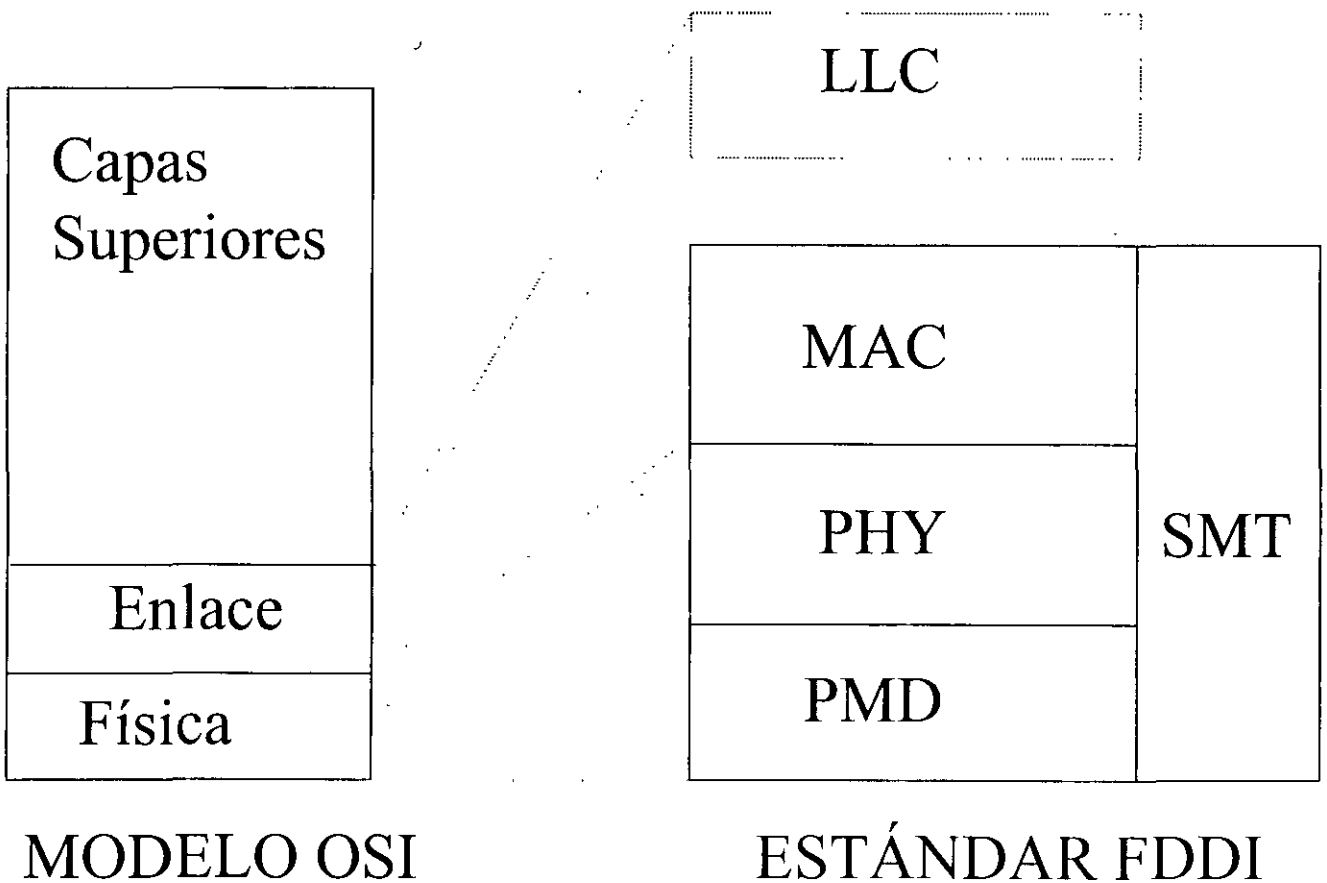
Física: Estrella y anillo



Tipos de Nodos



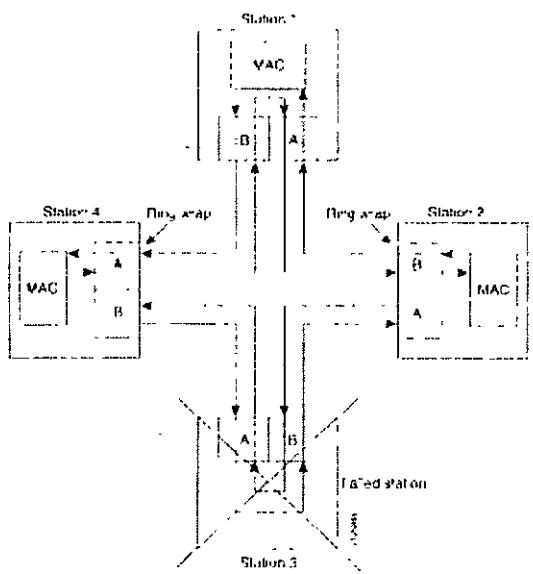
Arquitectura FDDI

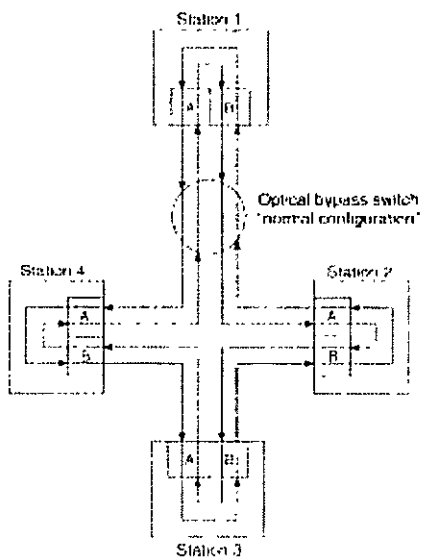


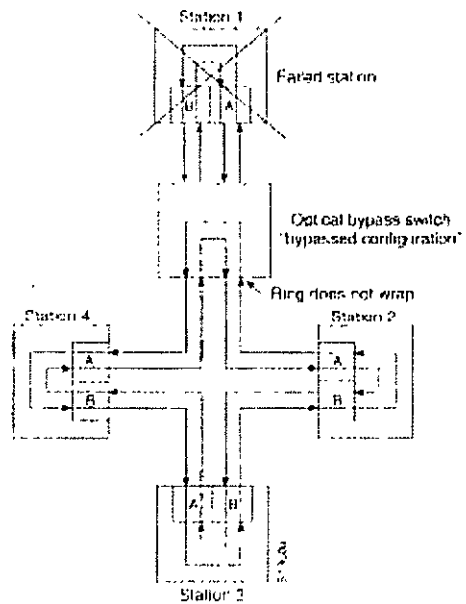
Características de Redundancia

- WRAP
- Estación bypass.- Aíslan una estación y permiten la operación continua del anillo.
- Dual Homing

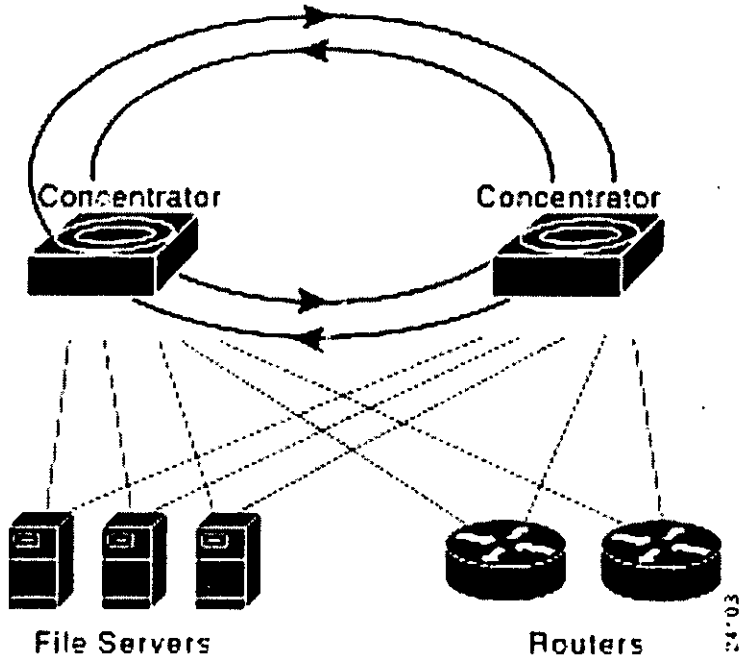
Wrap, bypass


VAC
MAC
Ring wrap
Ring wrap
Failed station

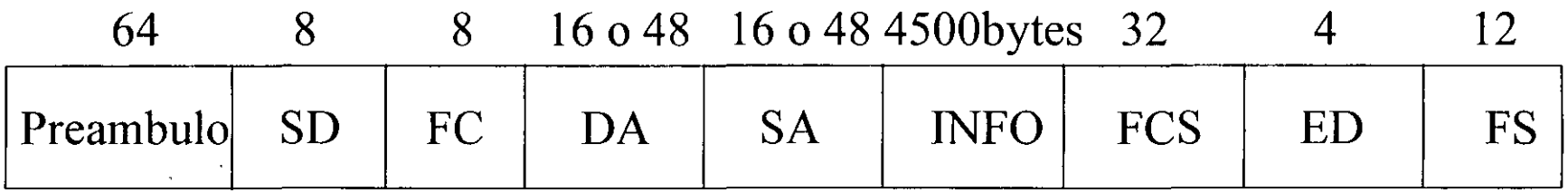

Station 1
Optical bypass switch
"normal configuration"
Station 4
Station 2
Station 3


Station 1
Failed station
Optical bypass switch
"bypassed configuration"
Ring does not wrap
Station 4
Station 2
Station 3

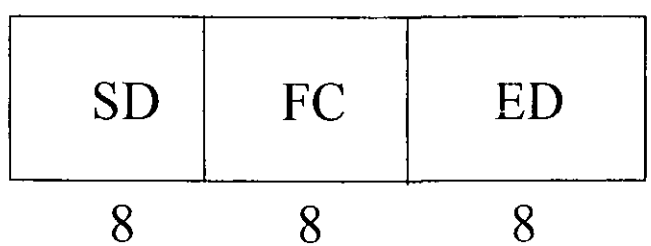
Dual homing



Formato de Trama FDDI

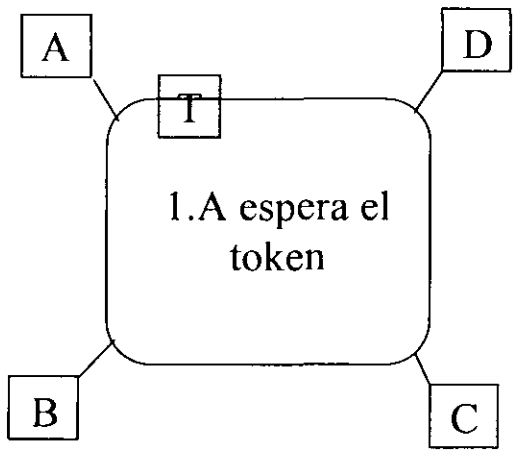


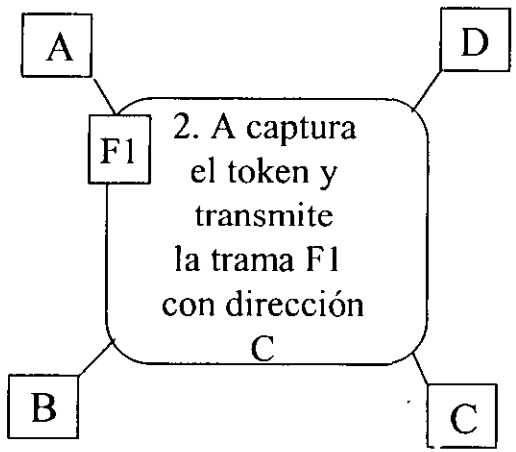
Formato de trama de Token

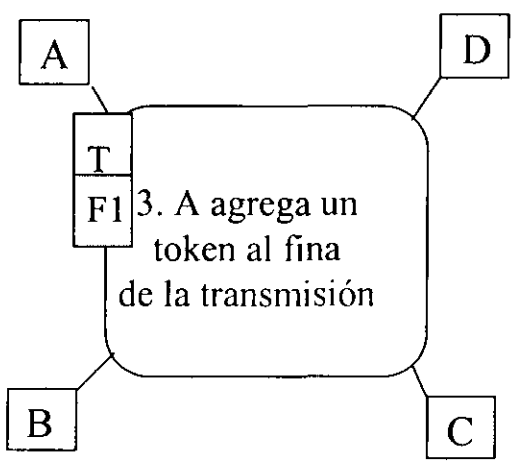


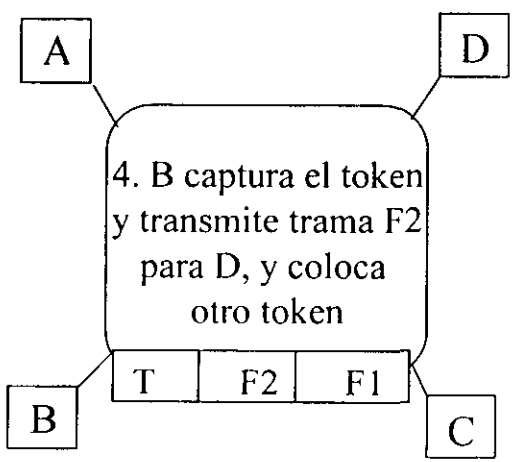
Se define la longitud de las tramas en bits

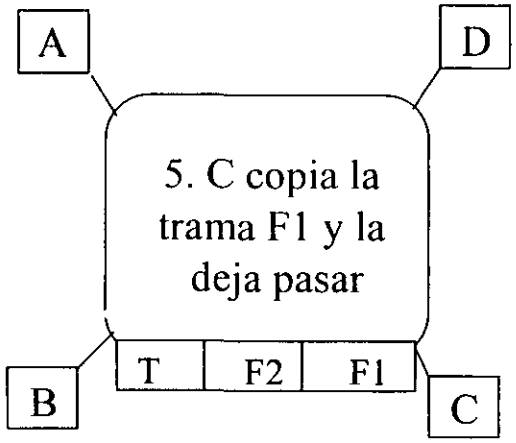
Protocolo MAC de FDDI

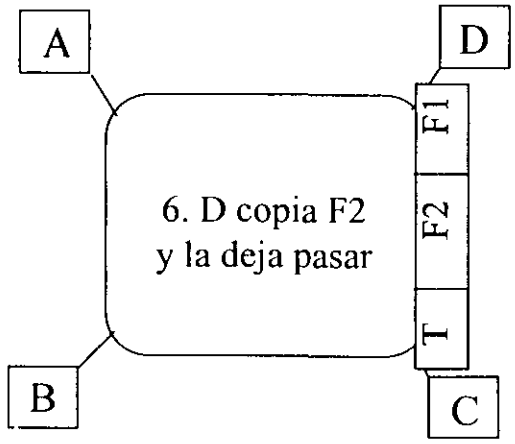


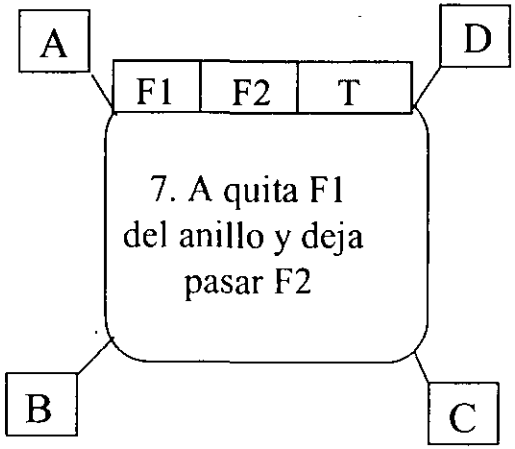


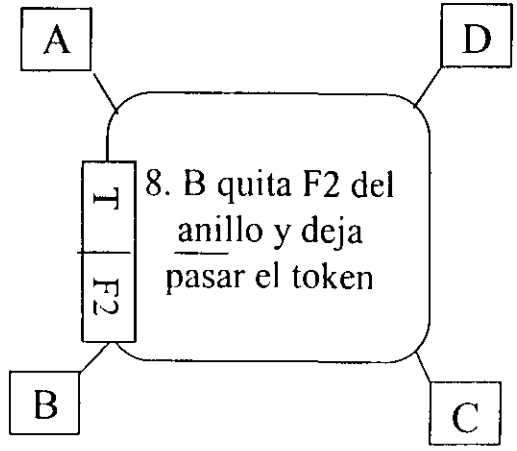





A
D
5. C copia la trama F1 y la deja pasar
T
F2
F1
B
C


A
D
6. D copia F2 y la deja pasar
F1
F2
T
B
C


A
D
F1
F2
T
7. A quita F1 del anillo y deja pasar F2
B
C


A
D
T
F2
8. B quita F2 del anillo y deja pasar el token
B
C

Tecnologías Relacionadas

- **CDDI**
- **FDDI II**
- **FFOL**

100VGAnyLAN

Características

Topología

Demand priority

Características

Diseñada para implementarse sobre cableado UTP categoria 3 de la planta telefónica ya instalada

Soporte de los frames tipo Ethernet y Token Ring

Velocidad de 100 Mbps

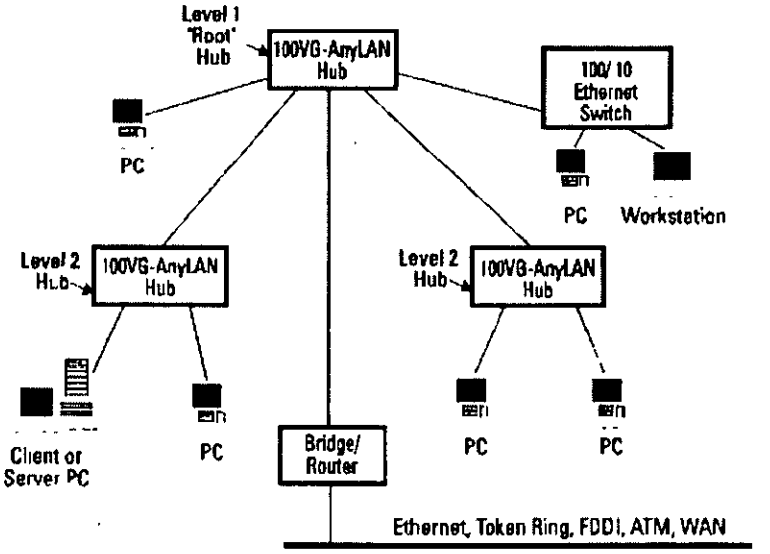
Topología jerárquica

Muy poca penetración en el mercado

Topología

Física: Jerárquica, estrella

Lógica: Anillo



Demand Priority

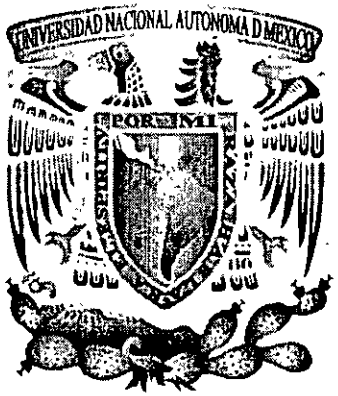
Sistema centralizado del control de acceso al medio

Esquema de acceso tipo round-robin

Se requiere de una petición de transmisión, la cual entra en una de dos colas de espera:

Prioridad normal

Prioridad alta



Resumen 802.x

802.1	Hiher Level Interface (HILI)
•802.2	Logical Link Control (LLC)
•802.3	CSMA/CD (Ethernet)
•802.4	Token Bus
•802.5	Token Ring
•802.6	Metropolitan Area Networks
•802.7	Broadband Technical Advisory Group (BBTAG)
•802.8	Fiber Optic Technical Advisory Group (FOTAG)
•802.9	Integrated Service LAN (ISLAN) Interface
•802.10	Estandar for Interoperable LAN Security (SILS)
•802.11	Wireless LAN (WLAN)
•802.12	Demand Priority (100VGanyLAN)
802.14	Cable-TV Based Broadband Communication Network.

Gracias!

Rodolfo Arias Villavicencio
ravillav@telmex.net

FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA

"Tres décadas de orgullosa excelencia" 1991 - 2001

CURSOS ABIERTOS

DIPLOMADO INTERNACIONAL EN TELECOMUNICACIONES

MODULO IV: REDES DIGITALES: ACTUALIDAD Y PERSPECTIVAS

TEMA

TECNOLOGÍAS WAN

EXPOSITOR: ING. JAVIER SOLIS GONZALEZ
PALACIO DE MINERIA
JUNIO 2001

Palacio de Minería Calle de Tacuba 5 Primer piso Deleg. Cuauhtémoc 06000 México, D.F. APDO. Postal M-2285
Teléfonos 5512-8955 5512-5121 5521-7335 5521-1987 Fax 5510-0573 5521-4021 AL 25

4. Tecnologías WAN

del 11 al 15 de junio de 2001

Tipos de Conexiones

- EIA/TIA-232D
- EIA/TIA-449
- V.35
- X.21
- G.703
- EIA-530
- HSSI

SDLC

- Creado por IBM a mediados de los 70's para uso sobre ambiente SNA.
- Primer protocolo orientado a bits y síncrono.
- Más eficiente, flexible y rápido.
- Predecesor de protocolos como HDLC, LAP, LAPB, IEEE 802.2

SDLC Tipos y Topologías

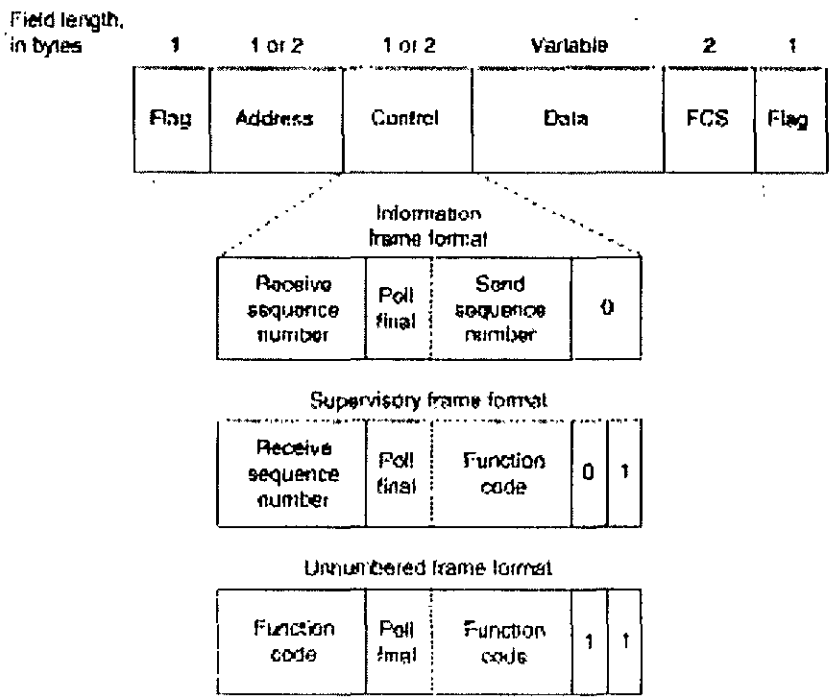
SDLC identifica dos tipos de nodos de red:

- Primario
- Secundario

Las topologías son:

- *Point-to-point*
- *Multipoint*
- *Loop*
- *Hub go-ahead*

Formato de la Trama SDLC



HDLC

- Comparte el formato de trama con SDLC.
- Soporta full-duplex y es síncrono.
- A diferencia de su predecesor, HDLC puede utilizar checksum de 32 bits.
- HDLC no soporta *loop* y *go-ahead.*
- SDLC soporta solo un modo de transmision, HDLC soporta 3 modos.

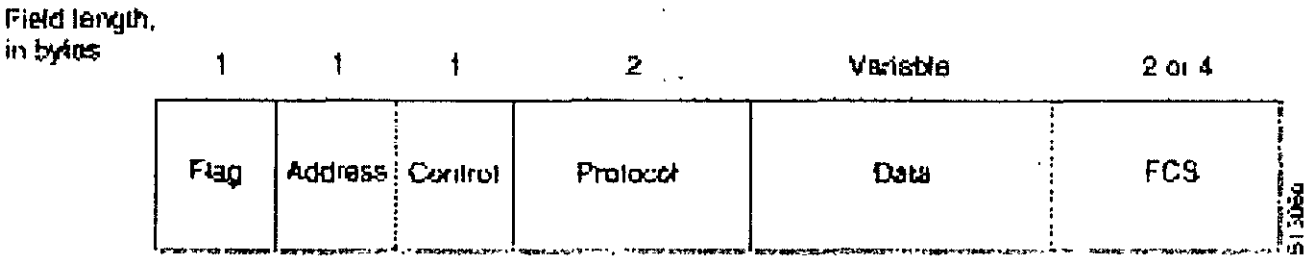
HDLC Tipos

- NRM *(Normal Response Mode)*.
- ARM *(Asynchronous Response Mode)* .
- ABM *(Asynchronous Balanced Mode)*.

PPP

- Surgió como protocolo de transporte para IP.
- Esta compuesta por tres componentes principales:
  - Método para encapsular datagramas multiprotocolo.
  - LCP *(Link Control Protocol)* para establecer y configurar la conexión a nivel enlace.
  - NCP *(Network Control Protocols)* para establecer y configurar diferentes protocolos de capa de red.

Formato de la Trama PPP



PPP LCP

LCP se realiza en cuatro etapas:

- Establecimiento de la conexión y negociación de la configuración.
- Determinación de la calidad del medio o enlace.
- Negociación a nivel protocolo de red.
- Fin de la conexión.

SLIP

- Originado por una implementación conocida como 3COM UNET TCP/IP.
- Define una forma de enviar paquetes de IP sobre líneas seriales en el estándar RS-232.
- Actualmente es utilizado para que computadoras remotas puedan accesar a redes (Dial-up).

Características en tramas SLIP

SLIP define dos caracteres especiales:

- END
- ESC

No existe un "estándar" en la especificación de SLIP, por lo que no hay un tamaño de paquete máximo para este protocolo. Sin embargo, se toma como norma el utilizado por los drivers Berkeley UNIX SLIP .

Deficiencias

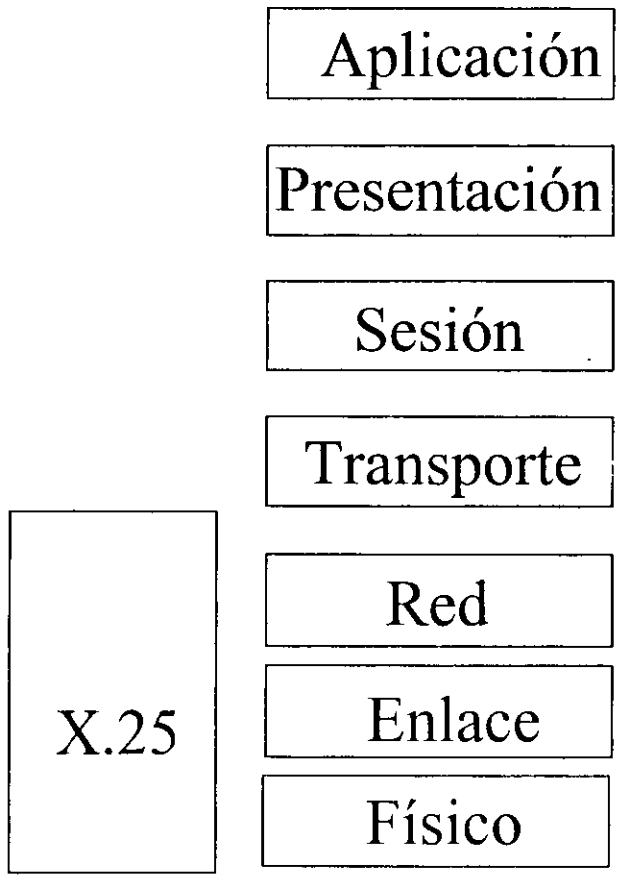
Debido a que SLIP es un protocolo realmente sencillo que fue diseñado hace tiempo no se tomaron en cuenta algunos puntos como:

- Direccionamiento
- Tipo de identificación
- Detección y corrección de errores.
- Compresión.

X.25

- Establecido por la CCITT en 1976
- Solo existía la infraestructura telefónica.
- Trata de mejorar la conmutación de Circuitos.
- Estándar solo para datos.
- Protocolo enfocado a tráfico de ráfagas
- Tecnología de conmutación de paquetes

Relación X.25 con de capas del modelo de referencia OSI



Capa Física:

Define las interfaces eléctricas y procedimientos para establecer la comunicación física entre el DTE y DCE

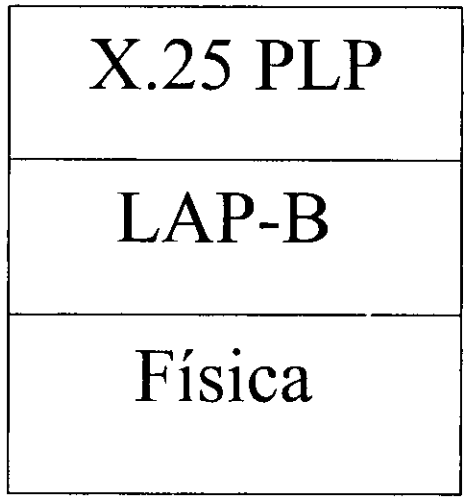
Capa de enlace:

Define los procedimientos de control de flujo de información entre el DTE y DCE y es responsable de la corrección de errores.

Capa de red:

Define los procedimientos de control para el intercambio de paquetes, en esta capa se establece la conexión virtual entre el punto fuente y el destino.

Arquitectura X.25

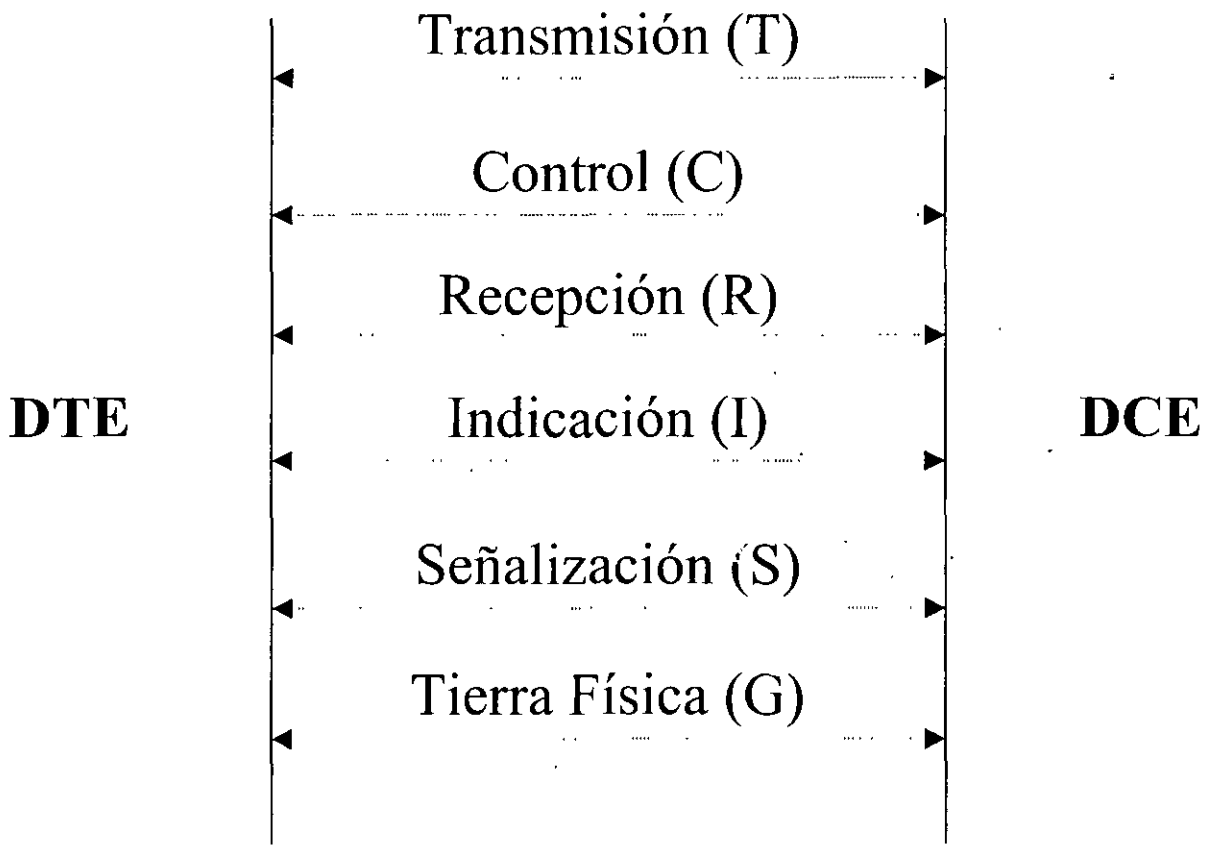


Capa Física:

Para la capa física X.25 refiere a la recomendación X.21 bis de la CCITT que específica la forma para establecer, mantener y desconectar la trayectoria física entre DTE/DCE.

X.21 bis define dos estándares: V.24 (RS-232-C) para velocidades de transmisión menores a 20Kbps y V.35 para velocidades hasta 48Kbps.

X.21 proporciona dos circuitos para transmisión de datos y dos circuitos de control, un circuito de señalización y un circuito de referencia.

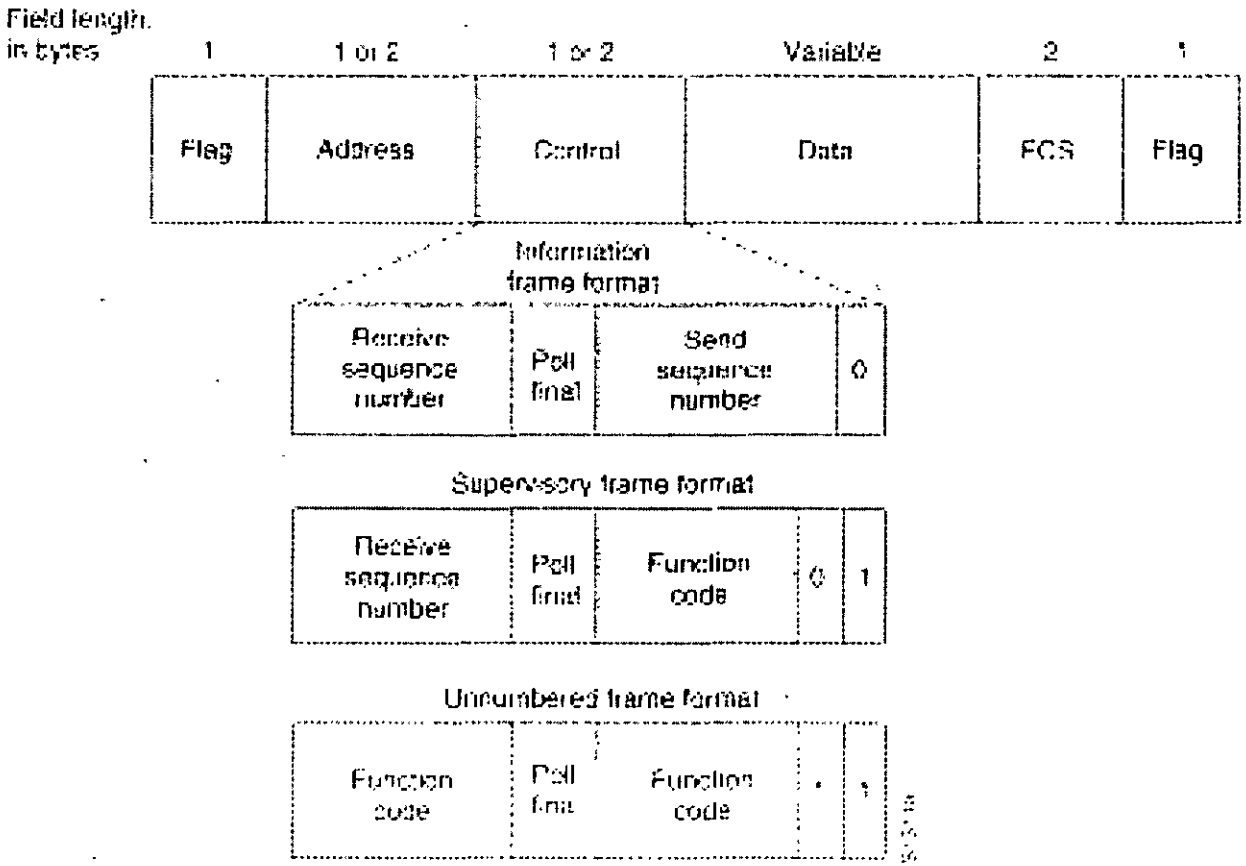

Transmisión (T)
Control (C)
Recepción (R)
DTE
Indicación (I)
DCE
Señalización (S)
Tierra Física (G)

Capa de enlace:

Las funciones de esta capa son las siguientes:

- Transferir los datos a través del enlace de manera eficiente.
- Sincroniza el enlace para asegurar que el receptor y transmisor estén en línea.
- Detecta errores de transmisión y realiza los procedimientos necesarios para la recuperación.
- Identifica y reporta los errores a las capas superiores a las capas superiores para la recuperación de datos.
- Informa a la capa de red el status del enlace.

Trama X.25


Field length, in bytes
1
1 or 2
1 or 2
Variable
2
1
Flag
Address
Control
Data
FCS
Flag
Information frame format
Receive sequence number
Poll final
Send sequence number
0
Supervisory frame format
Receive sequence number
Poll final
Function code
0
1
Unnumbered frame format
Function code
Poll final
Function code
1
1

Tipos de tramas X.25

- Tramas de Información: son utilizadas para la transferencias de paquetes. También lleva información de reconocimiento (acknowlegment) para el control de flujo.

- Tramas de supervisión: realiza funciones de supervisión como en reconocimiento de acknowlegment, retransmisión de tramas de información y responde a suspensiones temporales de transmisión.

- Tramas no numeradas: estas tramas realizan funciones de control y son utilizadas durante el establecimiento y la liberación del enlace.

LAP-B

Proporciona sincronía a nivel 2.

Direccionamiento físico.

Identifica el tipo de trama (I, S, U).

Proporciona control de flujo y control de errores.

Transporta información de capas superiores.

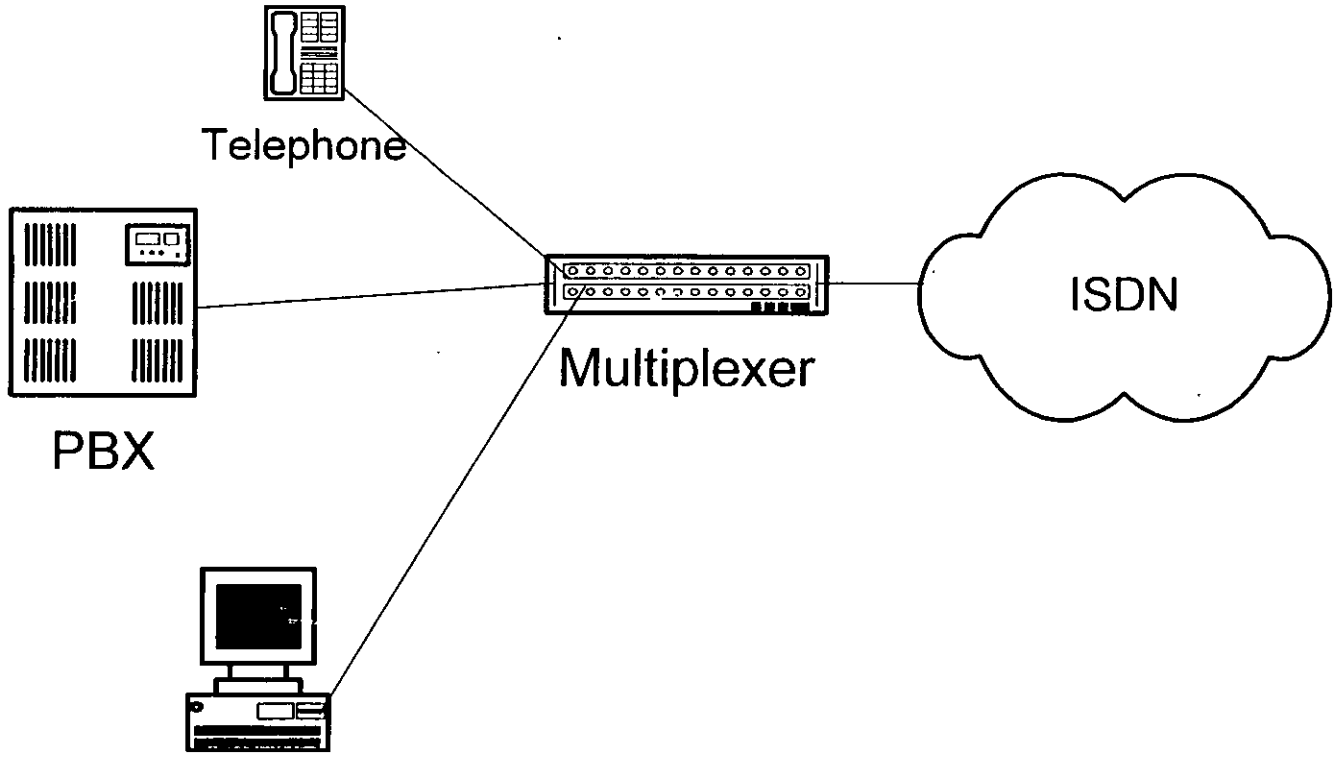
Formato del Frame LAP-B

F	ADD	CTRL	INFORMACIÓN	CRC	F
1	1	1	Variable	2	1

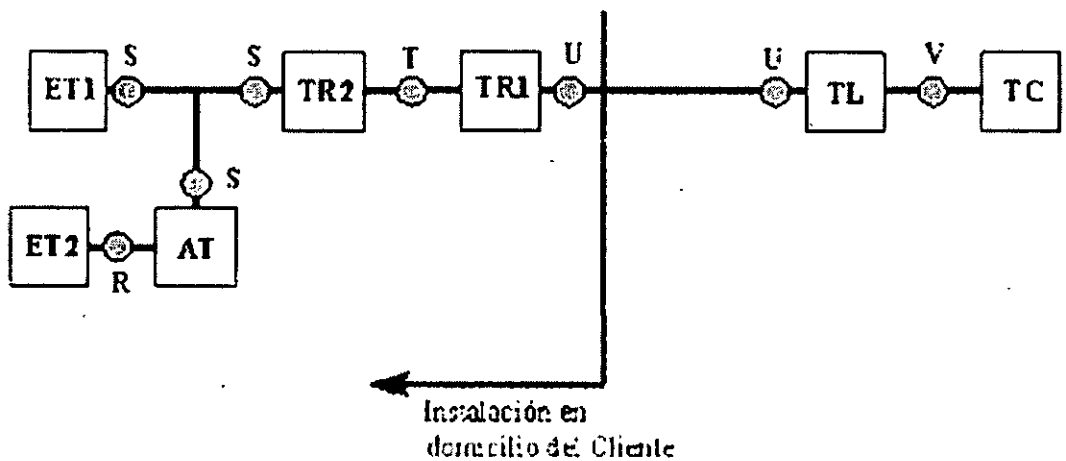
- F: Bandera de inicio.
- ADD: Dirección.
- CTRL: Identifican el tipo de trama y control de flujo.
- INF: Datos e información de capas superiores.
- CRC: Chequeo de la trama y control de errores en combinación con el campo de control.
- F: Bandera final.

- Integrated Services Digital Network
- Soporta aplicaciones de voz y no voz utilizando un conjunto de estándares
- Soporta aplicaciones conmutadas y no conmutadas
- Utiliza conexiones de 64 Kbps o múltiplos
- Implementa inteligencia en la red (SS7)
- Basado en una arquitectura de capas

Integración de Servicios



Agrupaciones Funcionales y Puntos de Referencia



Agrupación Funcional.

Punto de Referencia o Interfaz.

ISDN Estructura de Transmisión

Canales B a 64 Kbps
Canales D a 16 o 64 Kbps
Canales H a 384 (H0), 1536 (H11), o 1920 (H12) Kbps

3 conexiones diferentes en un canal B:

- Circuitos-conmutados
- Paquetes-conmutados
- Semipermanentes

Tipos de Acceso

Acceso Básico: 2B + D 144 (196) Kbps

Acceso Primario 30 B + D 1984 Kbps

Estos accesos se refieren a la capa física

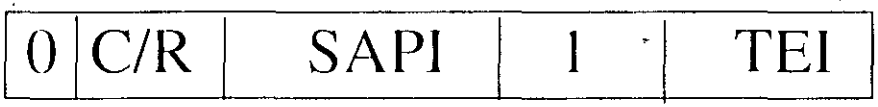
Acceso Básico

Full duplex
Código de línea Pseudoternario. 1 = 0V. 0 = +750 mV o -750 mV
Conector RJ45

Acceso Primario

Configuración punto a punto
1.544 o 2.048 Mbps
Código de línea 2B1Q. 10 = +3
11 = +1
01 = -1
00 = -3

LAP-D



Service Access Point Identifier (SAPI)
Terminal Endpoint Identifier (TEI)

Servicios de la ISDN

- **Servicios portadores**
  - **Modo circuito**
  - **Modo paquete**
- **Teleservicios**
- **Servicios suplementarios**

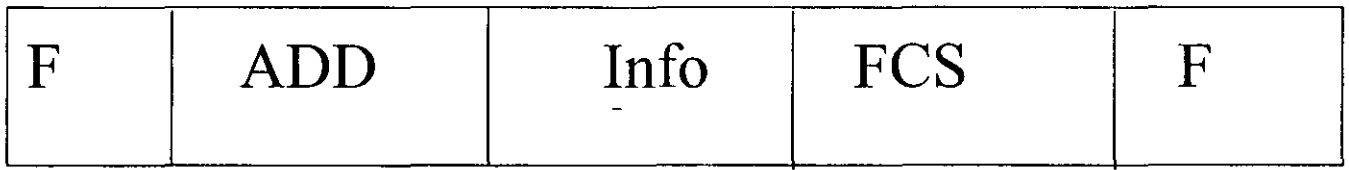
Frame Relay

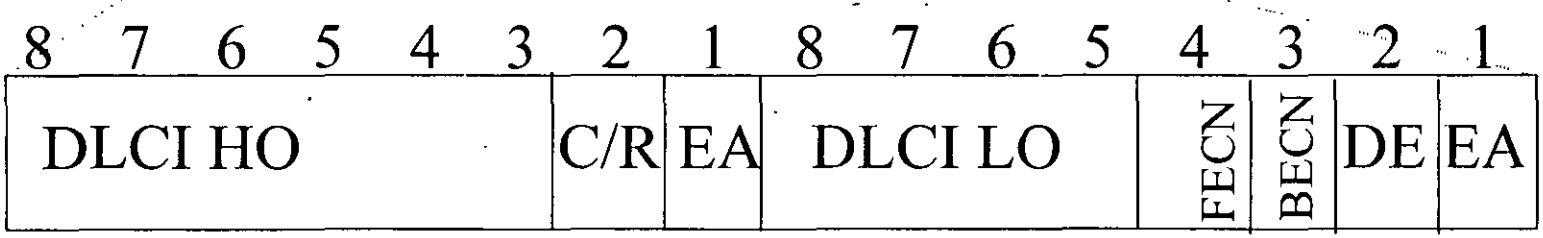
- Uso de circuitos virtuales.
- Utiliza las ventajas de los medios de transmisión digitales.
- Implementa identificadores de circuitos virtuales.
- Permite la conmutación de paquetes en la red a nivel 2.
- Implementa el multiplexaje estadístico.
- No efectúa corrección de errores.
- No realiza control de flujo.

Frame Relay

- Alta velocidad y bajo retardo.
- Soporte eficiente para tráficos o ráfagas.
- Flexibilidad.
- Eficiencia.
- Transporte de voz y datos.
- Conectividad.
- Simplicidad en gestión.
- Estándar.

LAP-F


F
ADD
Info
FCS
F

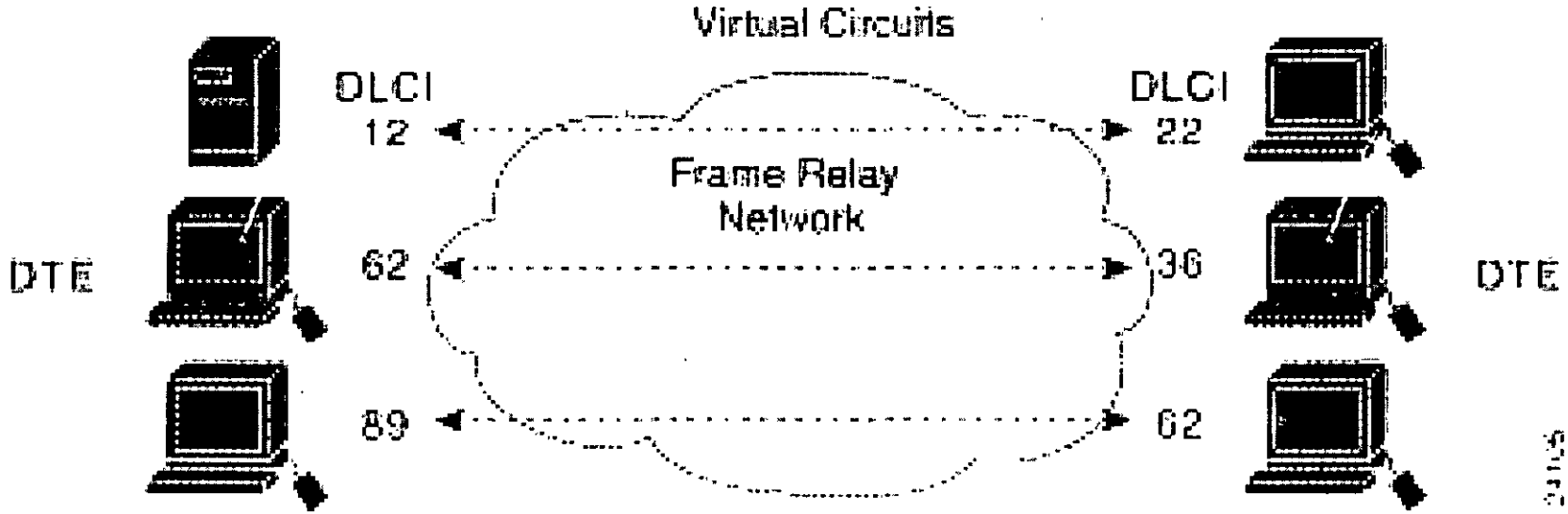

8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1
DLCI HO
C/R
EA
DLCI LO
FECN
BECN
DE
EA

LAP-F

- DLCI : Data Link Conection Identifier.
- C/R: Bit Comando Respuesta.
- EA: Extended Address (Dirección extendida).
- FECN: Forward Explicit Congestion Notification.
- BECN: Backward Explicit Congestion Notificatio.
- DE: Discard Elegibility.
- FCS: Frame Check Sequence.

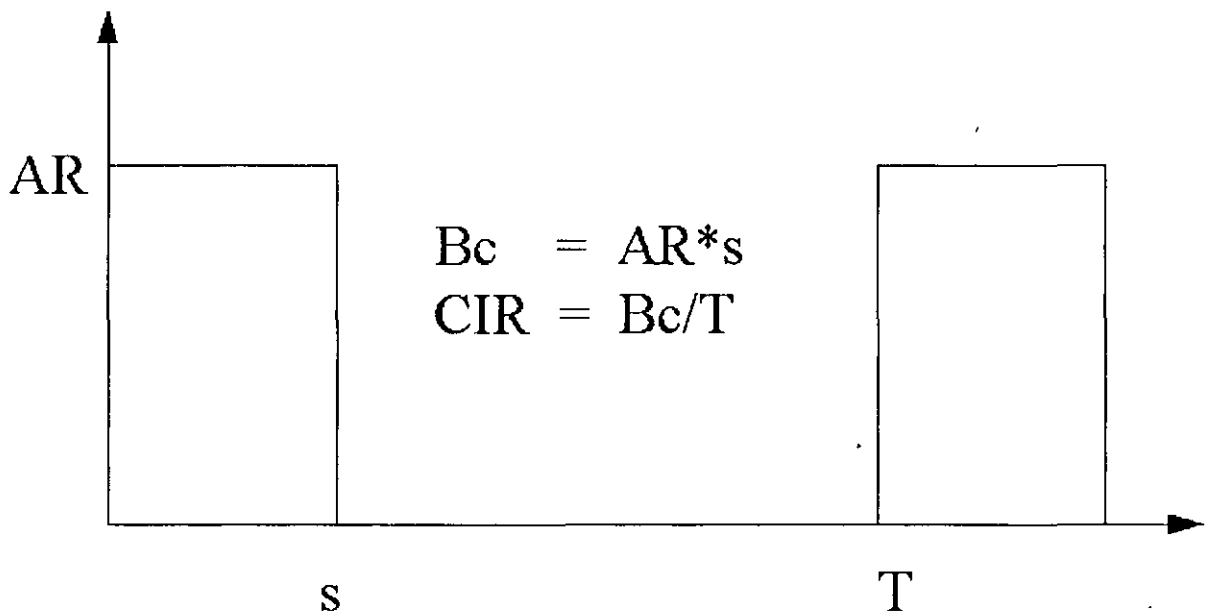
Circuitos Virtuales

- **Permanentes**
- **Conmutados**

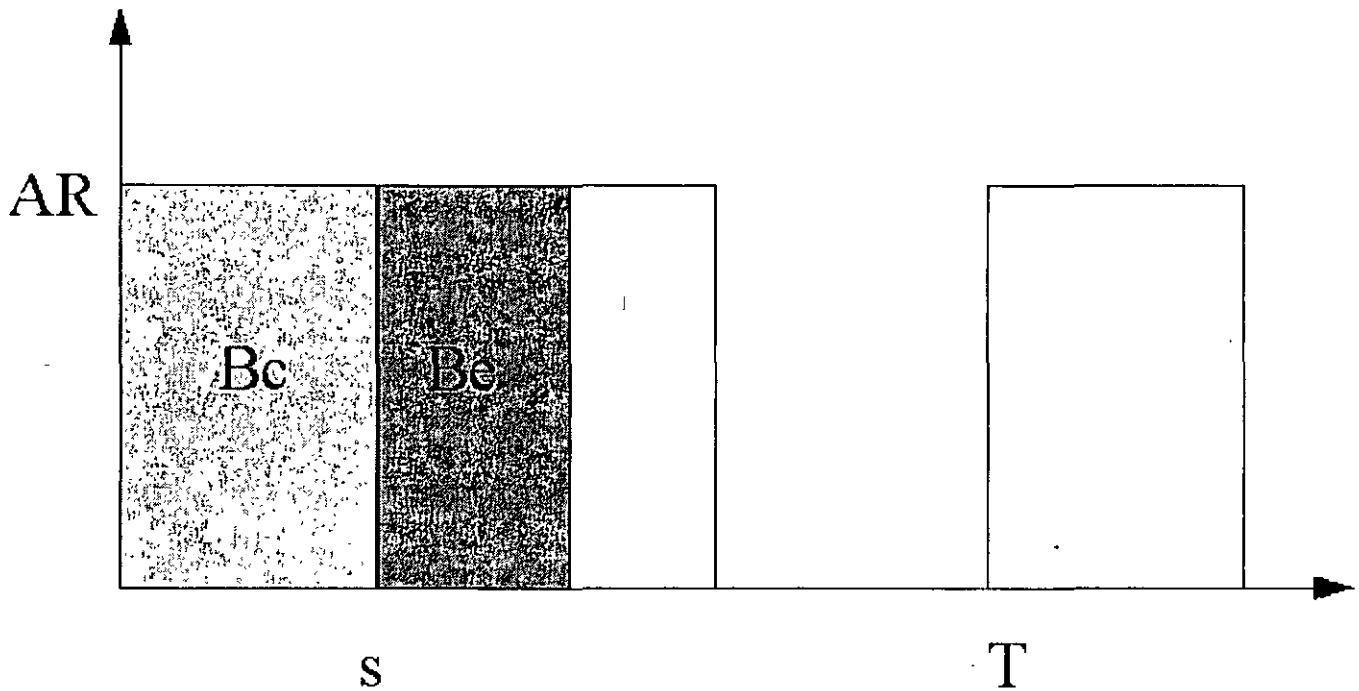


Administración de Tráfico

CIR, Bc, Be



Administración de Tráfico



Control de Congestión

- **Control de congestión explícita**

  Backward explicit congestion notification (BECN)

  Foward explicit congestion notification (FECN)

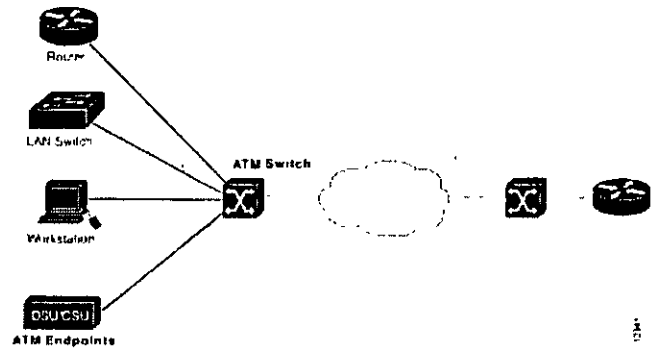
  Consolidated link-layer managment message (CLLM)

- **Control de congestión implícita**

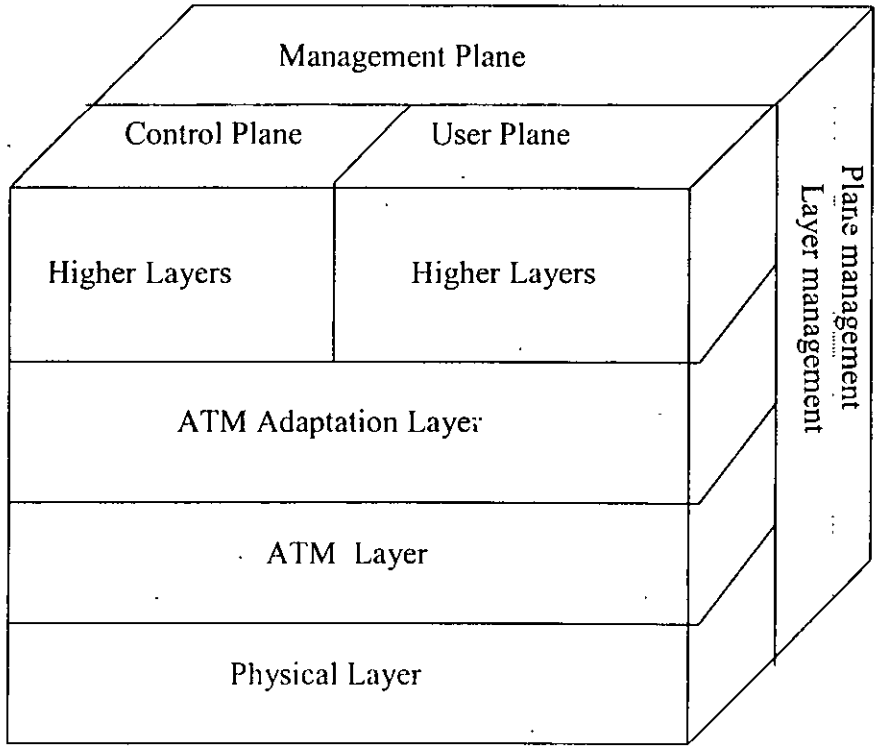
  Q.922

ATM

Integración de servicios.
Escalabilidad.
Independencia de velocidades.
Circuitos virtuales.
Calidad de Servicio (QoS)



Modelo B-ISDN



Planos del B-ISDN RM

Control: Establece, mantiene y termina las conexiones.

Usuario: Transferencia de información. Detección y corrección de errores.

Administración: Coordinación entre los demás planos y administración de los recursos del sistema.

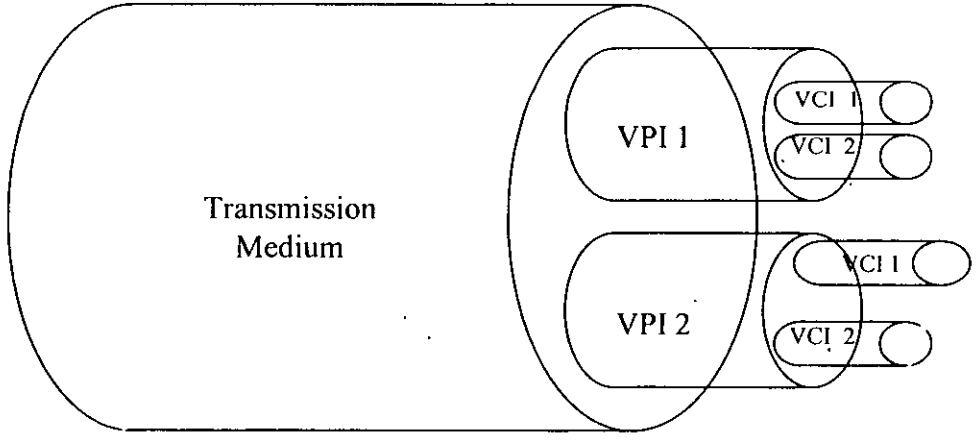
Capa ATM

- Toma ideas de X.25 y Frame Relay.
- Circuitos virtuales (Conexiones virtuales)
  - -Mismo orden de Tx y Rx
  - -Multiplexaje
  - -Handshake
- No hay control de errores.
- Introduce el concepto de celda.

Circuitos Virtuales

VPI: Virtual Path Identifier.
VCI: Virtual Channel Identifier.
VCC: Virtual Channel Connection.
VPC: Virtual Path Connection.

Circuitos Virtuales

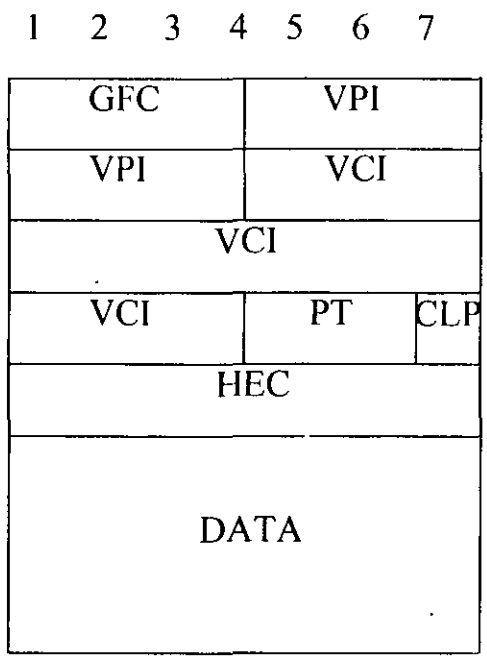


Identificadores de significado local.
Si el VPC está formado solo se realiza el VCC.

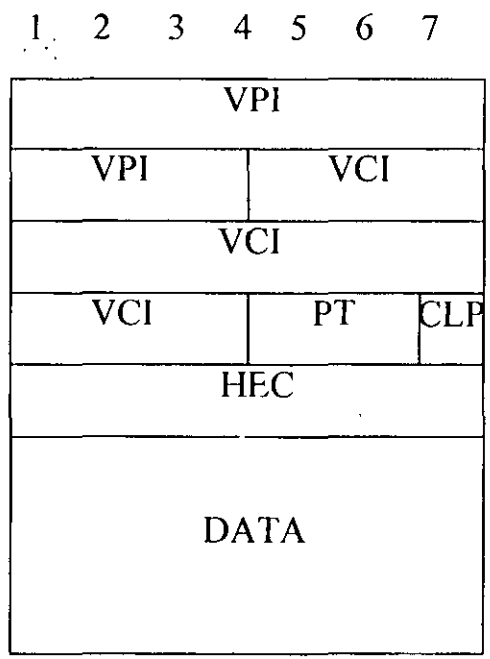
VCC

Calidad de servicio.
PVC o SVC.
Canales meta-signaling.

CELDA



User-to-Network Interface



Network-to-Network Interface

CAPA AAL

ATM Adaptation Layer

Adaptar diferentes tipos de tráfico para ser transportados en ATM.
Se divide en dos subcapas:

- Capa de Convergencia.
- Capa SAR (Segmentation and Reassambly).

Capa de Convergencia

Subcapa superior.
Identifica el tipo de tráfico.
Asigna clase de servicio basándose en tres características.

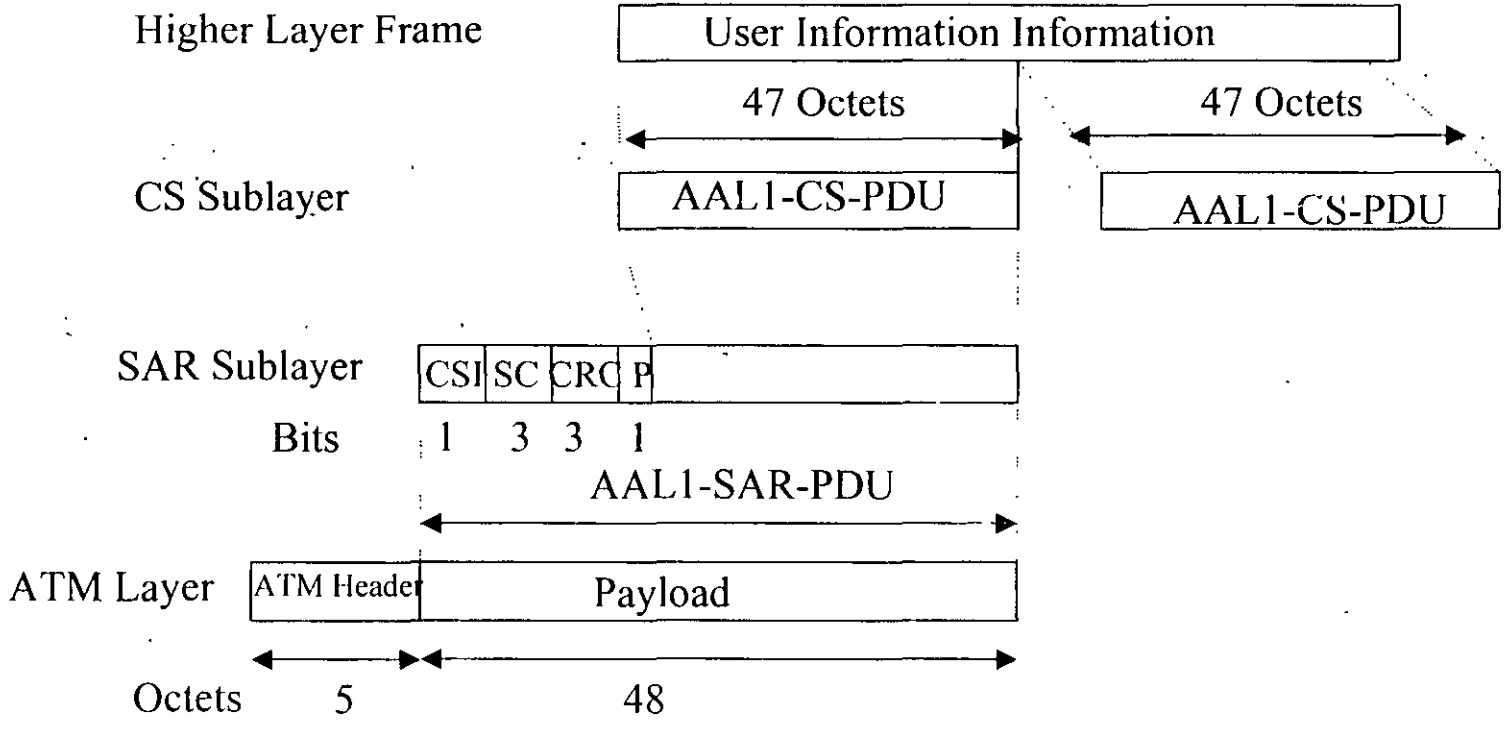
- Sincronía entre fuente y destino.
- Velocidad variable o constante.
- Modo de conexión.

Subcapa SAR

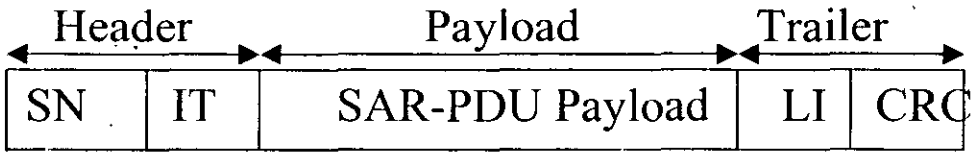
Segmenta y reensambla la información proveniente de la capa de convergencia.

Realiza mecanismos de detección de errores.

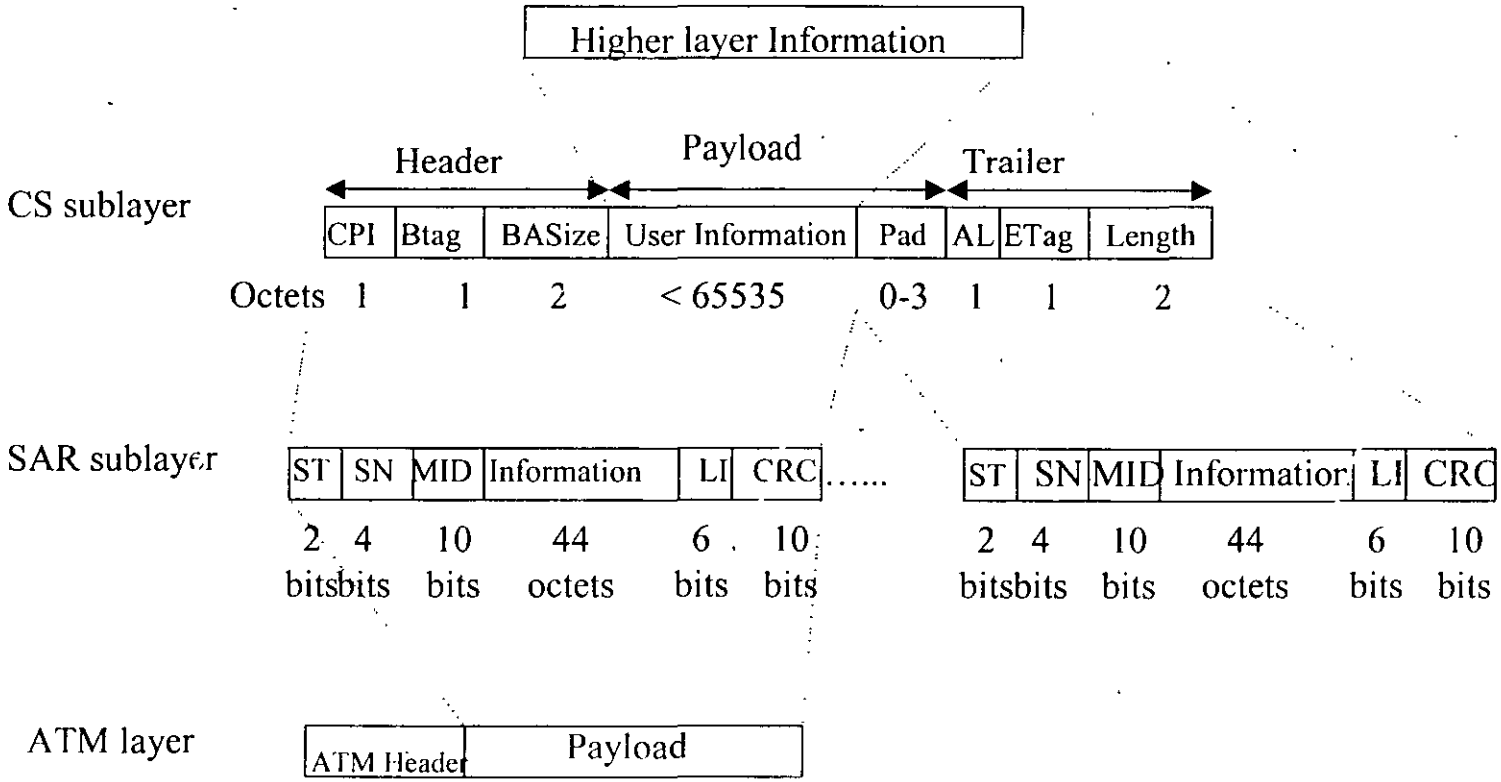
AAL 1


Higher Layer Frame
User Information Information
47 Octets
47 Octets
CS Sublayer
AAL1-CS-PDU
AAL1-CS-PDU
SAR Sublayer
CSI
SC
CRC
P
Bits
1
3
3
1
AAL1-SAR-PDU
ATM Layer
ATM Header
Payload
Octets
5
48

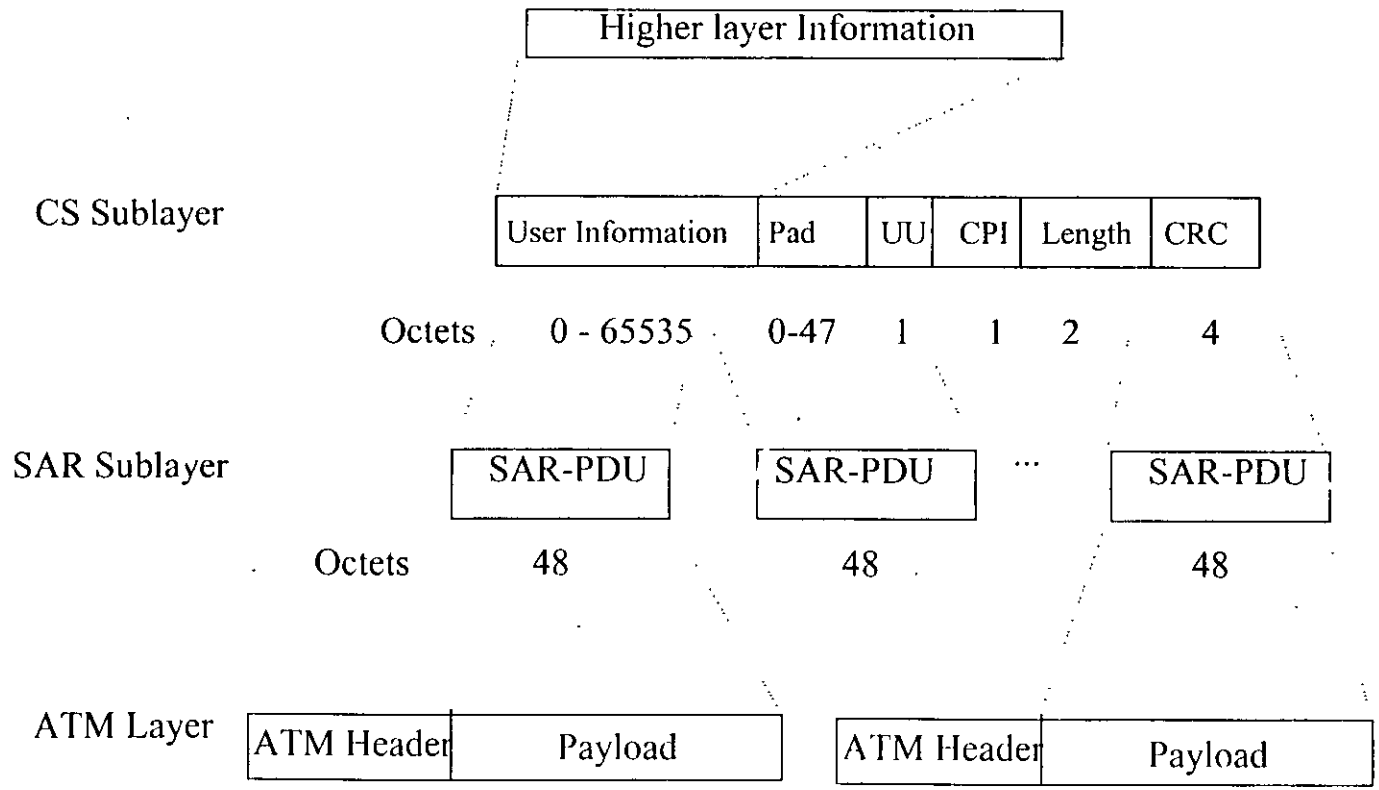
AAL 2



AAL 3/4


Higher layer Information
CS sublayer
Header
Payload
Trailer
CPI
Btag
BASize
User Information
Pad
AL
ETag
Length
Octets 1 1 2 < 65535 0-3 1 1 2
SAR sublayer
ST
SN
MID
Information
LI
CRC
.....
ST
SN
MID
Information
LI
CRC
2 bits
4 bits
10 bits
44 octets
6 bits
10 bits
2 bits
4 bits
10 bits
44 octets
6 bits
10 bits
ATM layer
ATM Header
Payload

AAL 5


Higher layer Information
CS Sublayer
User Information
Pad
UU
CPI
Length
CRC
Octets
0 - 65535
0-47
1
1
2
4
SAR Sublayer
SAR-PDU
SAR-PDU
...
SAR-PDU
Octets
48
48
48
ATM Layer
ATM Header
Payload
ATM Header
Payload

AAL

Type of Traffic	CBR	VBR RT	VBR NRT	ABR	UBR
Timing relationship between source and destination	Required		Not Required		
Bit Rate	Constant	Variable			
Connection Mode	Connection Oriented				Connectionless
AAL recommended	AAL 1	AAL 2		AAL 3/4 AAL 5	AAL 3/4
Class of Service	A	B		C	D

Tipos de Tráficos

CBR: Constant Bit Rate.
VBR: Variable Bit Rate.
ABR: Available Bit Rate.
UBR: Unespicified Bit Rate.

CBR

Aplicaciones de tiempo real basadas en Circuit Switching
Velocidad constante.
Aun si no hay nada que transmitir, el medio está dedicado.
Sensibilidad en la variación de retardo entre trama y trama.
Ejemplo: Telefonía.

Clase tipo A

VBR

VBR-rt y VBR-nrt.
Aplicaciones orientadas a conexión.
Relación de sincronía entre fuente y destino.
Velocidad variable.
Ejemplo de VBR-rt: Compresión de voz.

Clase B

ABR

Aplicaciones orientadas a conexión.
Velocidad variable.
No necesita relación de sincronía.
Aplicaciones generalmente de datos.
Ejemplo: X.25 y Frame Relay.

Clase C

UBR

Trafico no orientado a conexión.
No necesita relación de sincronía.
Velocidad variable.
Usado generalmente en datos.
Ejemplo: Redes LAN.

Clase D

FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA
Tres décadas de orgullosa excelencia 1971 - 2001

CURSOS ABIERTOS

DIPLOMADO INTERNACIONAL EN TELECOMUNICACIONES

MODULO IV: REDES DIGITALES: ACTUALIDAD Y PERSPECTIVAS

TEMA

CONMUTACIÓN DE PAQUETES

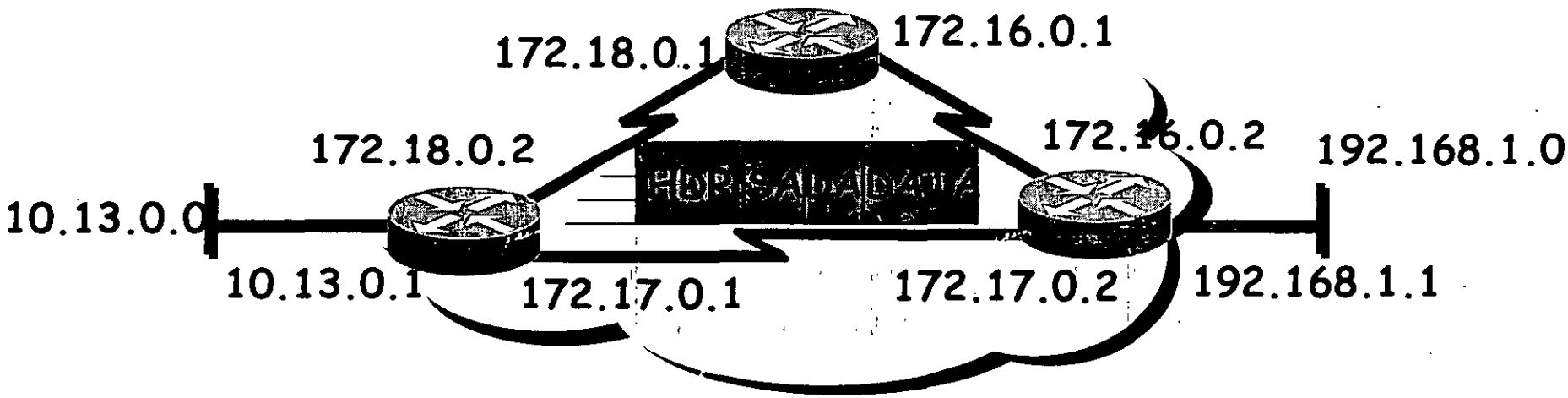
EXPOSITOR: ING. EDUARDO DIAZ GONZALEZ
PALACIO DE MINERIA
JUNIO 2001

5. Conmutación de Paquetes

del 11 al 15 de junio de 2001

Introducción al Direccionamiento IP

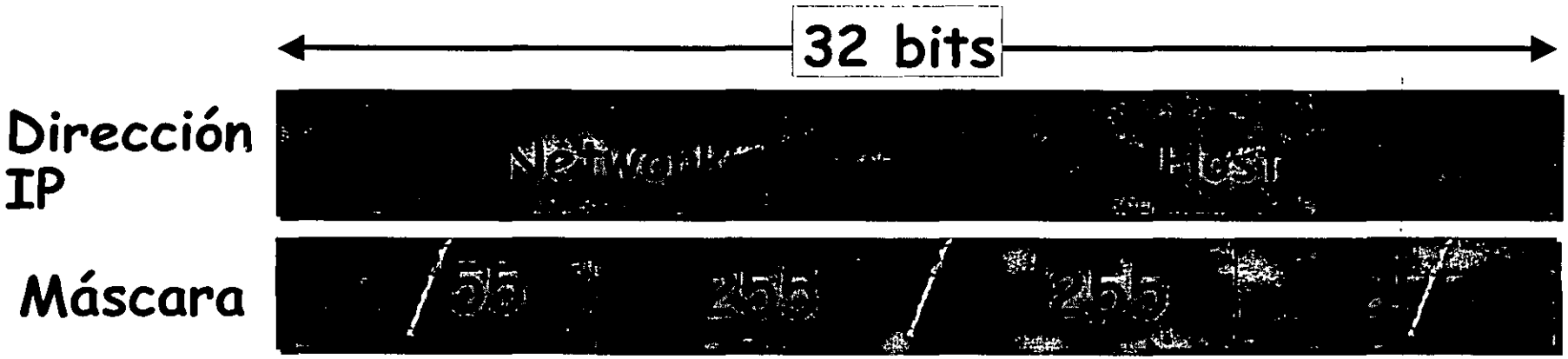
Introducción al direccionamiento IP



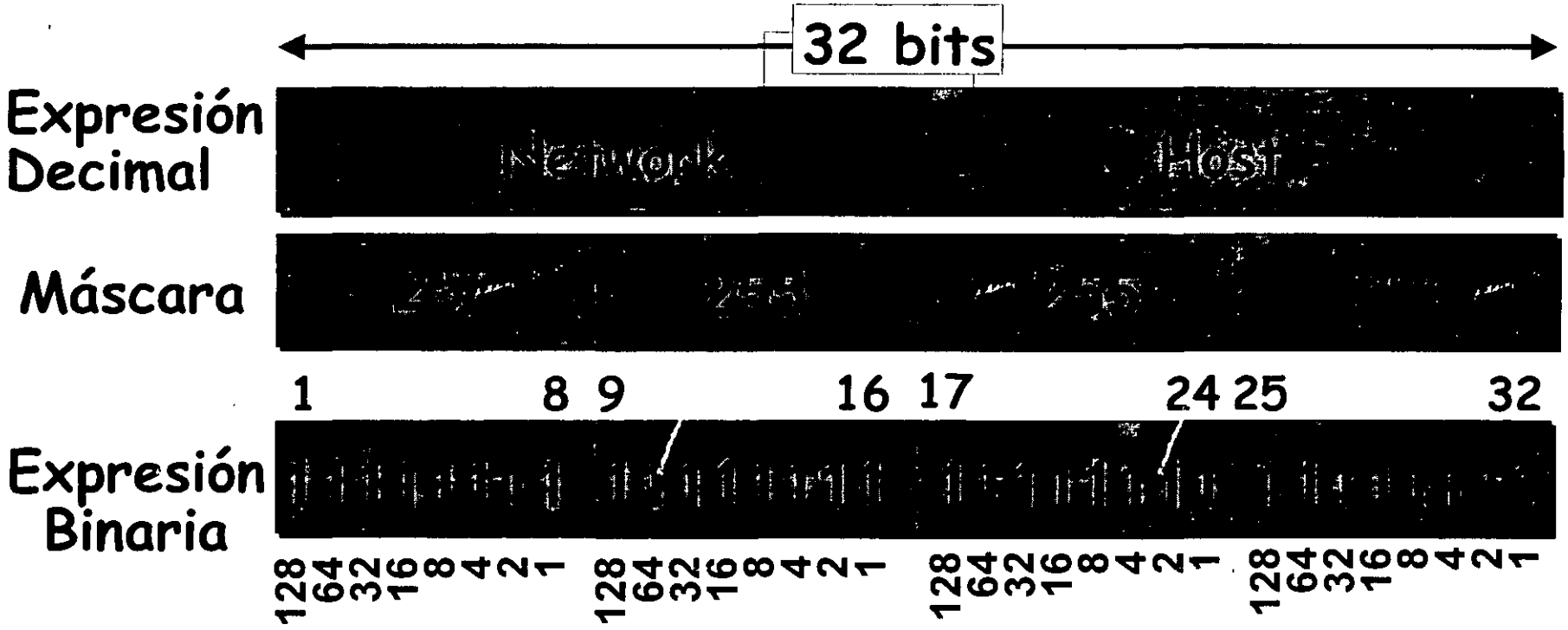
- Direccionamiento único permite la comunicación entre estaciones finales
- Elección de ruta basado en localidad

•Location is represented by an address

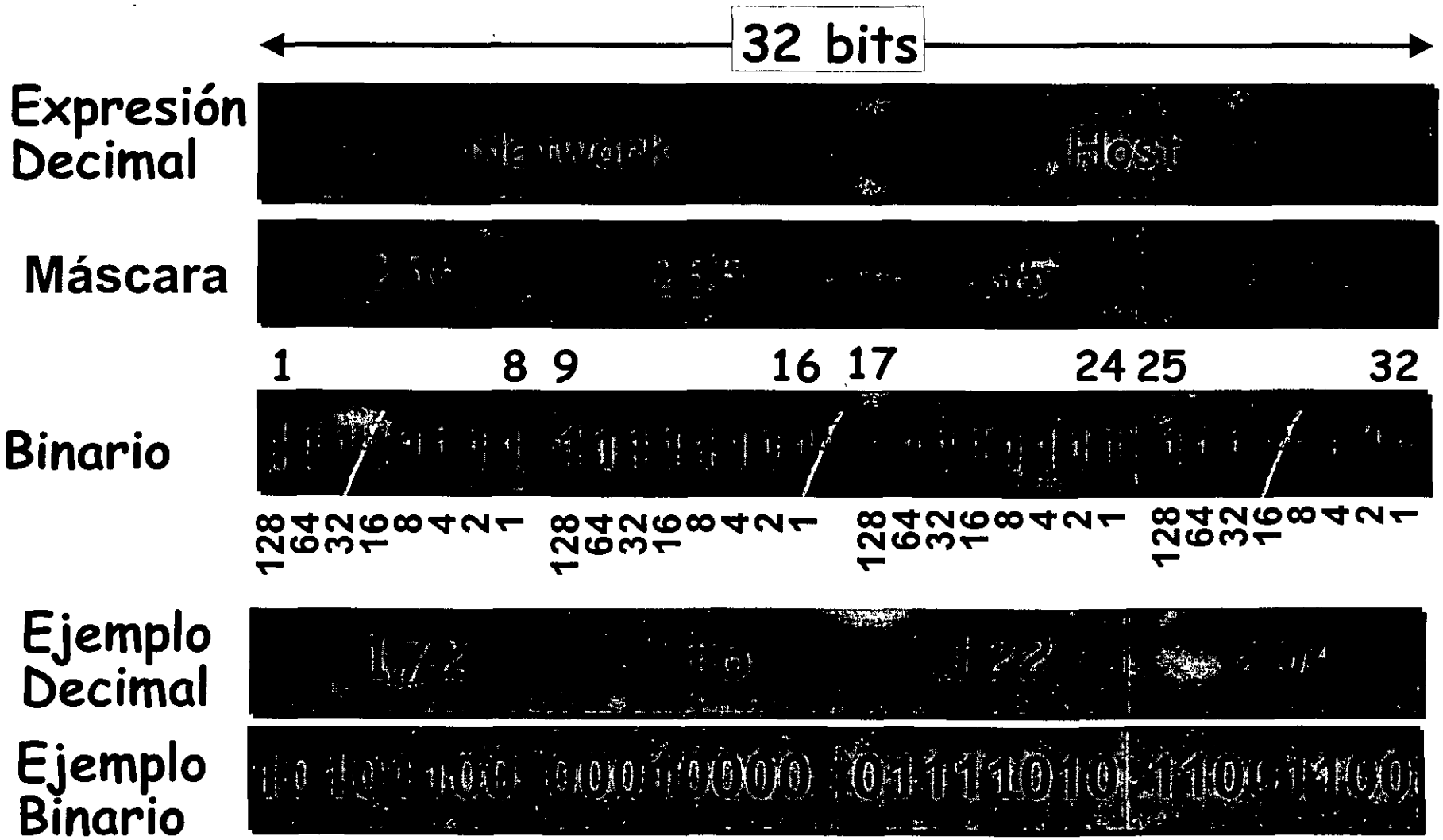
Direccionamiento IP



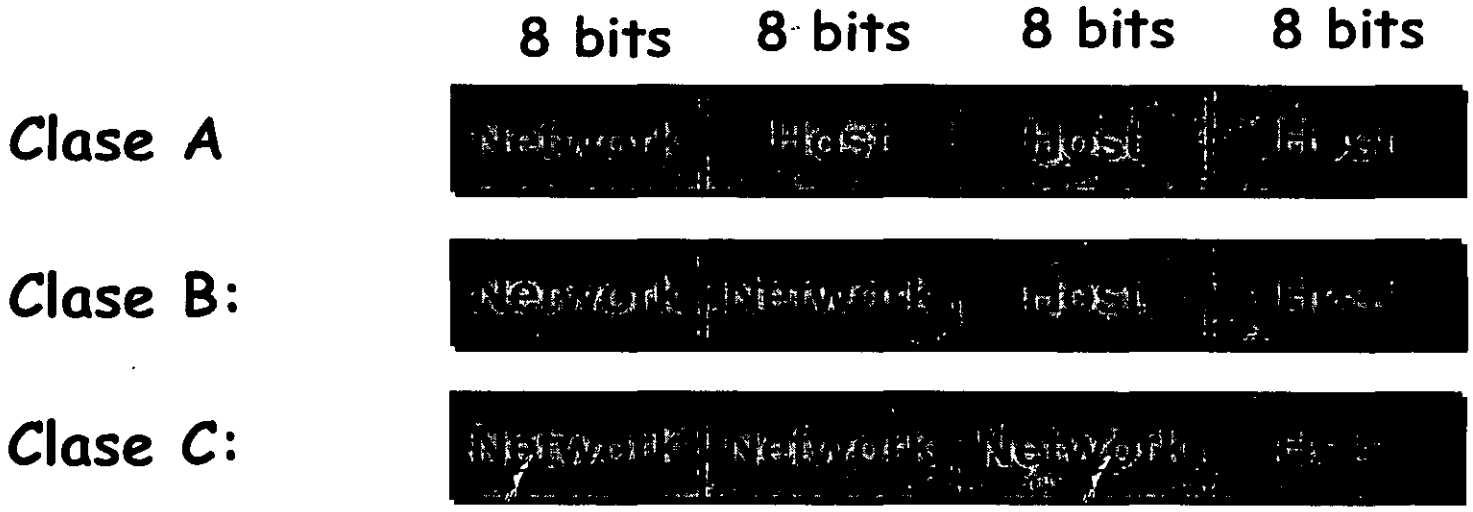
Direccionamiento IP



Direccionamiento IP



Clases de Direcciones IP



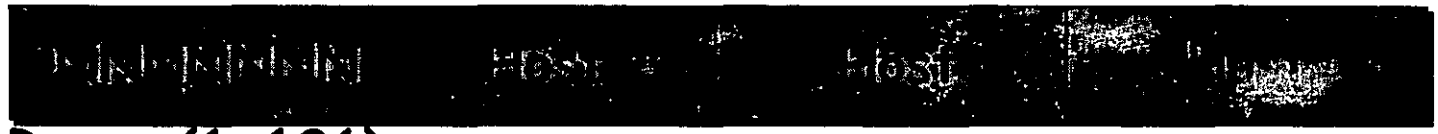
Clase D: Multicast

Clase E: Reservada para Investigación

Clases de Direcciones IP

Bits: 1 8 9 16 17 24 25 32

Clase A:



Rango (1-126)

Bits: 1 8 9 16 17 24 25 32

Clase B:

Rango (128-191)

Bits: 1 8 9 16 17 24 25 32

Clase C:

Rango (192-223)

Bits: 1 8 9 16 17 24 25 32

Clase D:

Rango (224-239)

Determinación del Direccionamiento Disponible en una Dirección de Red

	16 15 14 13 12 11 10 9	8 7 6 5 4 3 2 1	N
10101100 00010000	00000000	00000000	1
	00000000	00000001	2
	00000000	00000011	3
	⋮	⋮	⋮
	11111111	11111101	65534
	11111111	11111110	65535
	11111111	11111111	65536
			- 2
			65534

$2^N-2 = 2^{16}-2 = 65534$

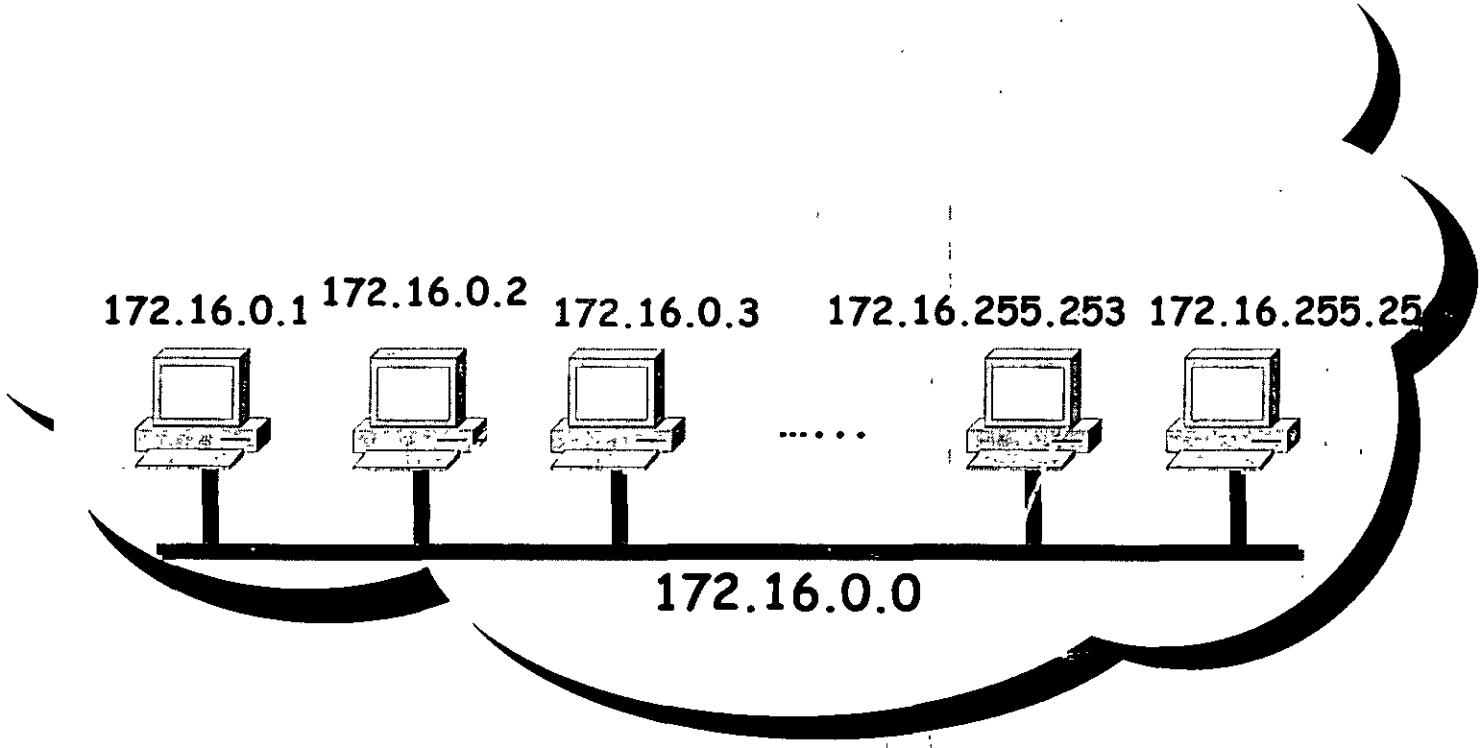
Ejercicio

Dirección	Clase	Network	Host
13.52.100.1			
128.63.2.100			
200.33.137.165			
192.100.183.2			
148.233.64.16			
256.241.201.10			

Respuestas

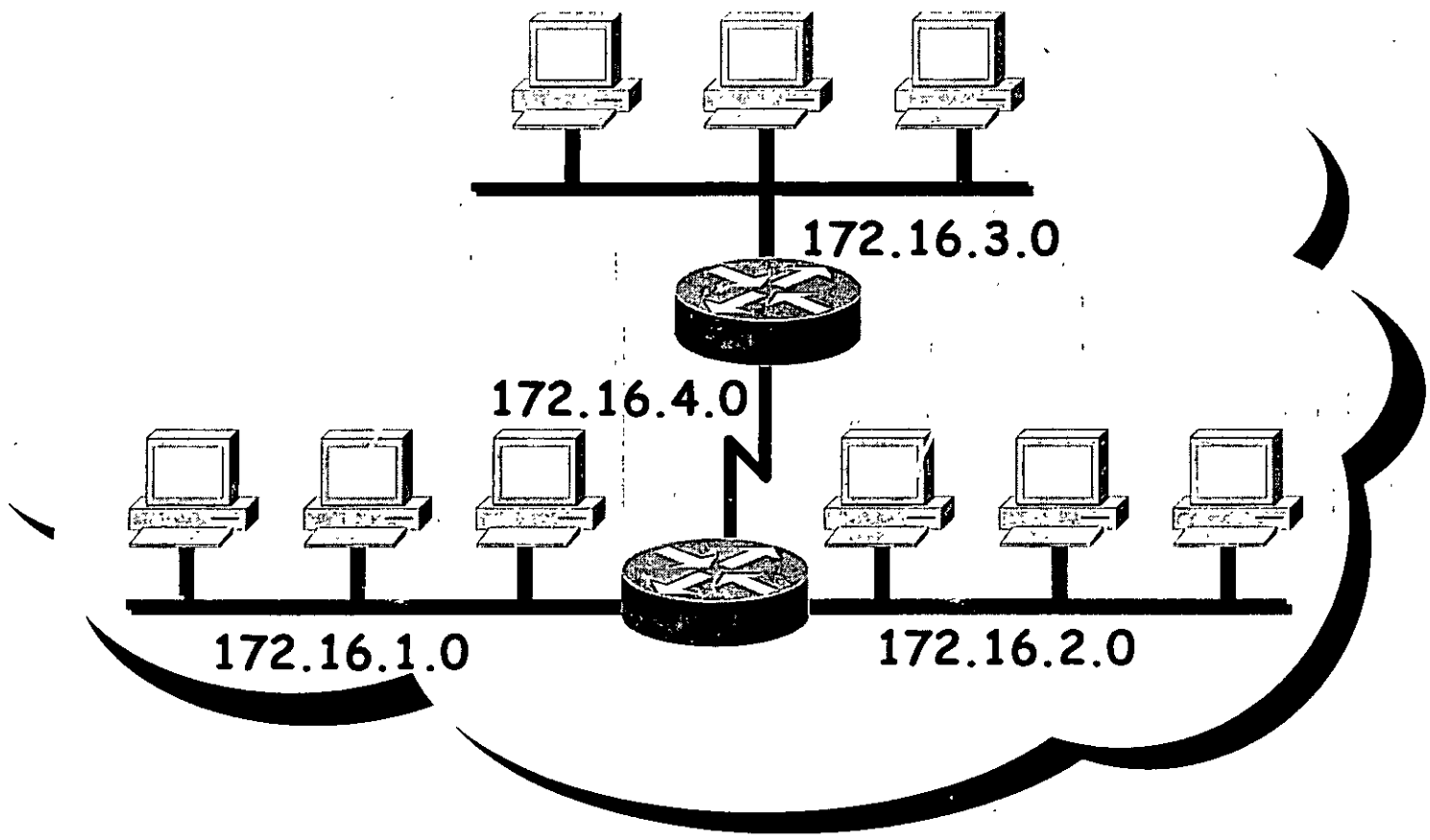
13.52.100.1	A	13.0.0.0	0.52.100.1
128.63.2.100	B	128.63.0.0	0.0.2.100
200.33.137.165	C	200.33.137.0	0.0.0.65
192.100.183.2	C	192.100.183.0	0.0.0.2
148.233.64.16	B	148.233.0.0	0.0.64.16
256.241.201.10	Inválida		

Direccionamiento sin Subredes



- Red 172.16.0.0

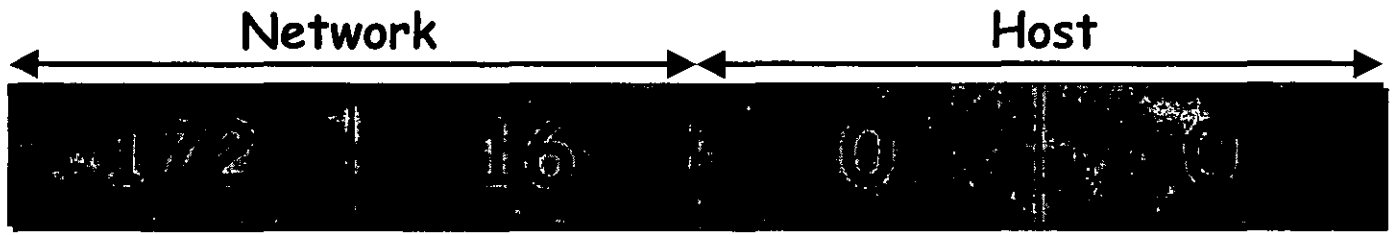
Direccionamiento con Subredes



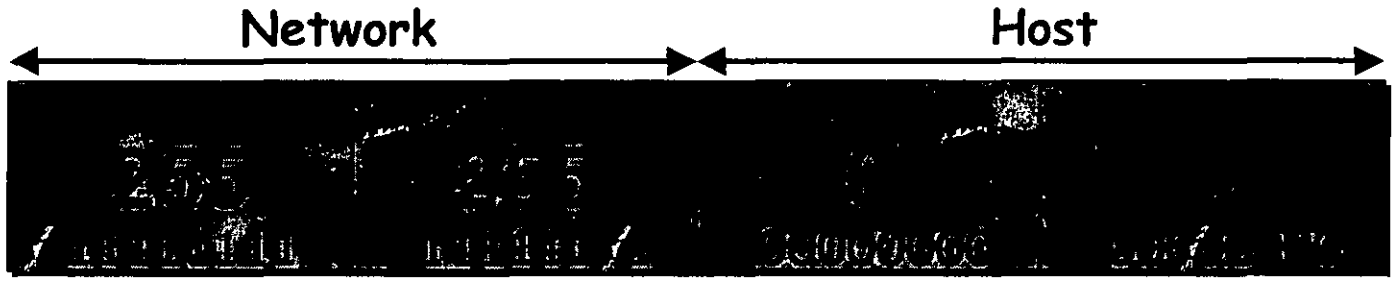
- Red 172.16.0.0

Máscara de Subred

Dirección IP

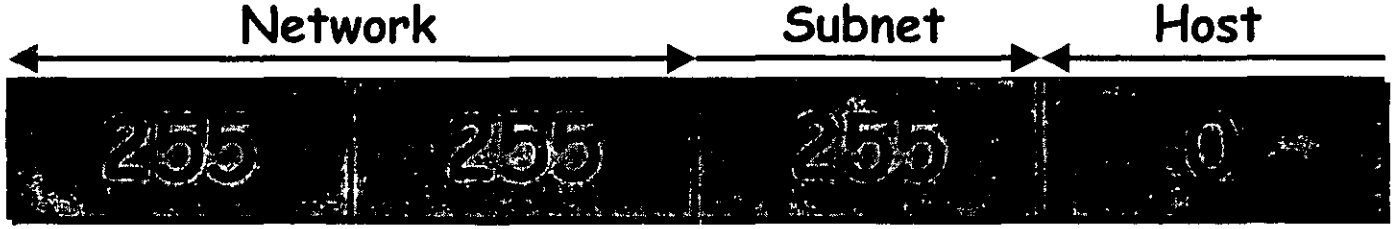


Máscara de Default



También escrita cómo "/16" donde 16 representa el número de 1s en la máscara.

Máscara de 8 bits de Subred



También escrita cómo"/24" donde 24 representa el número de 1s en la máscara.

Expresión Binaria de los Números Decimales

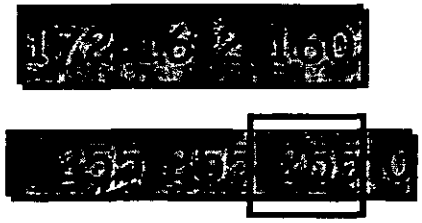
128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Máscara de Red sin Subredes

	Network		Host	
[redacted]	10101100	00010000	00000010	10100000
[redacted]	11111111	11111111	00000000	00000000
	10101100	00010000	00000000	00000000

Número de Red [redacted]

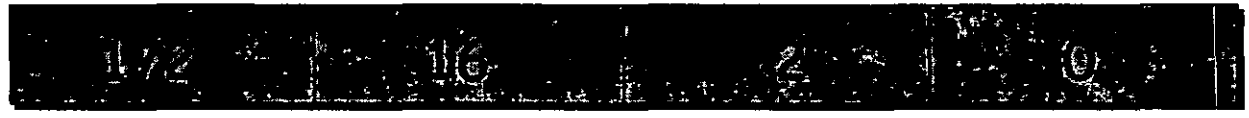
Máscara de Red con Subredes



Network		Subnet	Host
10101100	00010000	00000010	10100000
11111111	11111111	11111111	00000000
10101100	00010000	00000010	00000000

128
192
224
240
248
252
254
255

Número de Red



- Número de red extendido por 8 bits

Máscara de Red con Subredes

	Network		Subnet	Host
[redacted]	10101100	00010000	00000010	10100000
[redacted]	11111111	11111111	11111111	11000000
	10101100	00010000	00000010	10000000
			128 192 224 240 248 252 254 255	128 192 224 240 248 252 254 255

Número De Red [redacted]

- Número de Red extendida por 10 bits

Ejemplo de Subred Clase B

Dirección Ip: 172.16.2.121
Máscara de Red: 255.255.255.0

	Network	Network	Subnet	Host
172.16.2.121:	10101100	00010000	00000010	01111001
255.255.255.0:	11111111	11111111	11111111	00000000
Subred:	10101100	00010000	00000010	00000000
Broadcast:	10101100	00010000	00000010	11111111

- Dirección Subred = 172.16.2.0
- Dirección de Host = 172.16.2.1-172.16.2.254
- Dirección Broadcast = 172.16.2.255
- 8 bits de Subred

Ejemplo de Subred Clase C

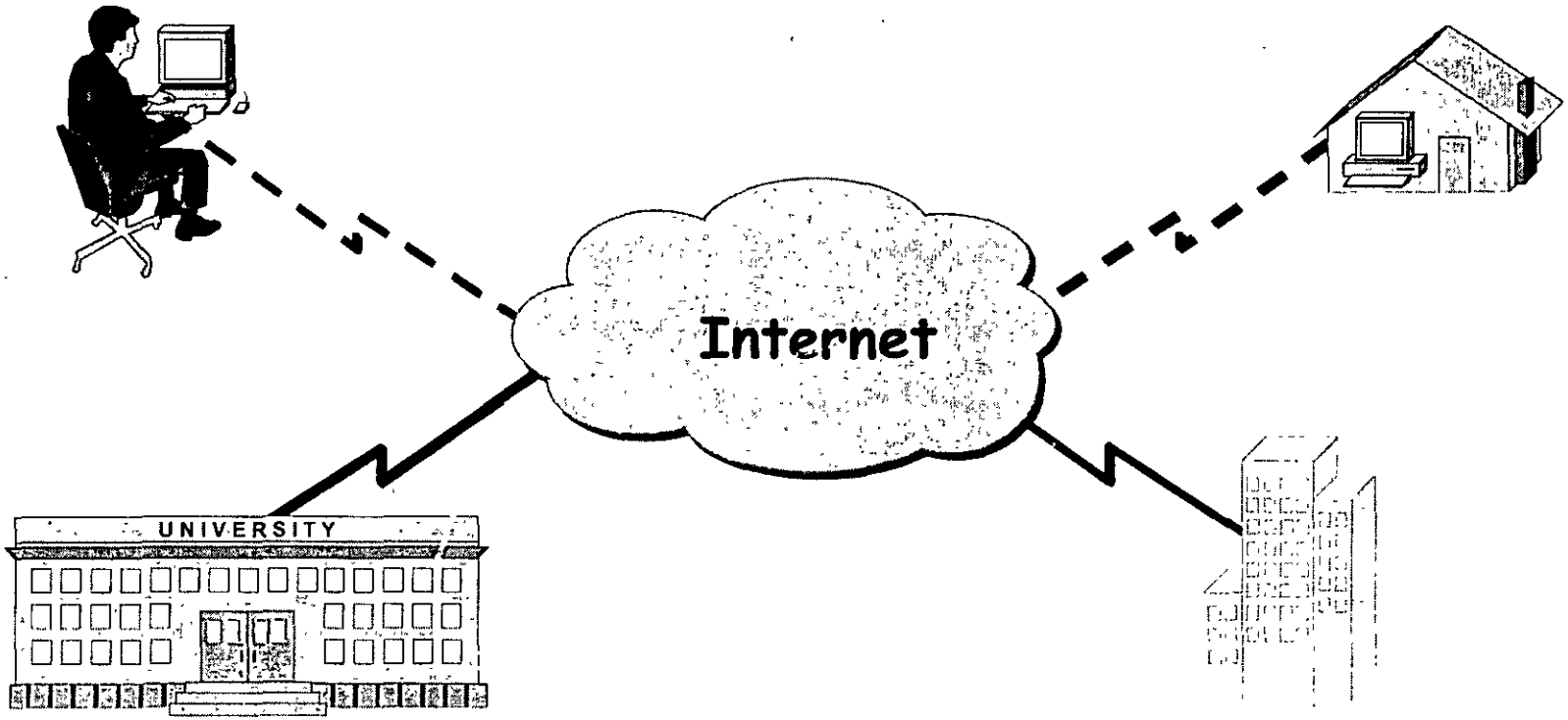
Dirección IP: 192.168.5.121
Máscara de Red: 255.255.255.248

	Network	Network	Network	Subnet	Host
192.168.5.121:	11000000	10101000	00000101	01111	001
255.255.255.248:	11111111	11111111	11111111	11111	000
Subred:	11000000	10101000	00000101	01111	000
Broadcast:	11000000	10101000	00000101	01111	111

- Dirección de Subred = 192.168.5.120
- Dirección de Host = 192.168.5.121–192.168.5.126
- Dirección Broadcast= 192.168.5.127
- 5 bits de Subred

- VLSM
- CIDR
- Sumarización

Problemas con el Direccionamiento IP



- Agotamiento del direccionamiento IP
- Crecimiento de las Tablas de Enrutamiento

Soluciones

- Máscara de Subred; RFCs 950, 1812
- Direccionamiento Jerárquico
- Sumarización de Rutas, RFC 1518
- Máscara de Subred de Longitud Variable, RFC 1812
- Classless Interdomain Routing; RFCs 1518, 1519, 2050
- Asignación de direcciones para Redes Privadas,RFC 1918
- Network Address Translation, RFC 1631

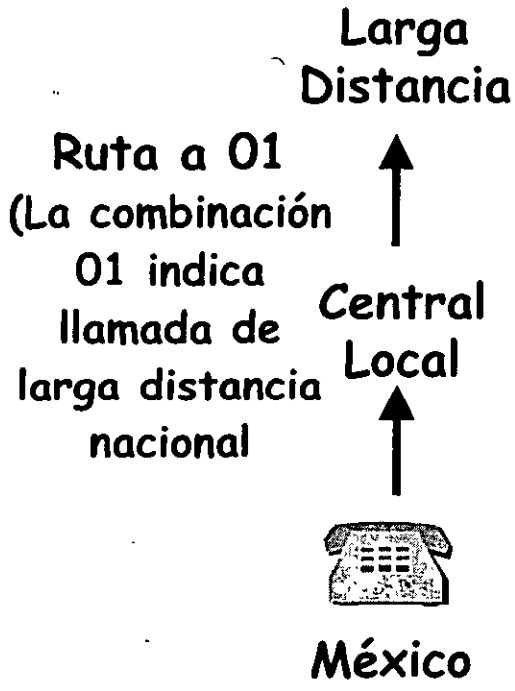
Máscara de Subred

- Moviendo el límite de la máscara de red hacia la derecha, se crean subredes adicionales a expensas de tener un número de hosts reducidos en cada segmento
- La nueva máscara tendrá 1s contiguos adicionales, indicando cuántos bits más ha sido extendida la porción de red
  - La formula 2^n, donde n es igual al número de bits extendidos, indica el máximo número de subredes creadas

Planeación Jerárquica IP

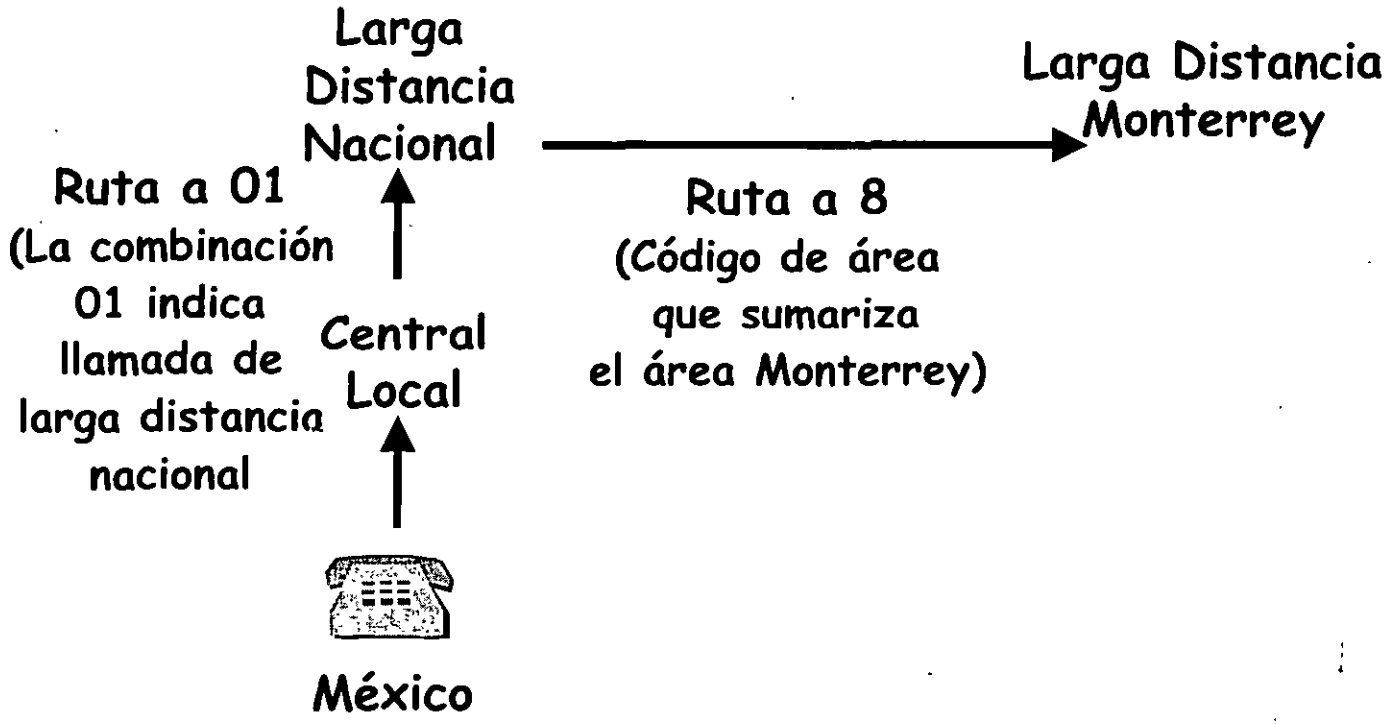
·¿Un conmutador telefónico de México conoce cómo llegar a un teléfono específico en Monterrey?
(01-8-118-8756)

Planeación Jerárquica IP



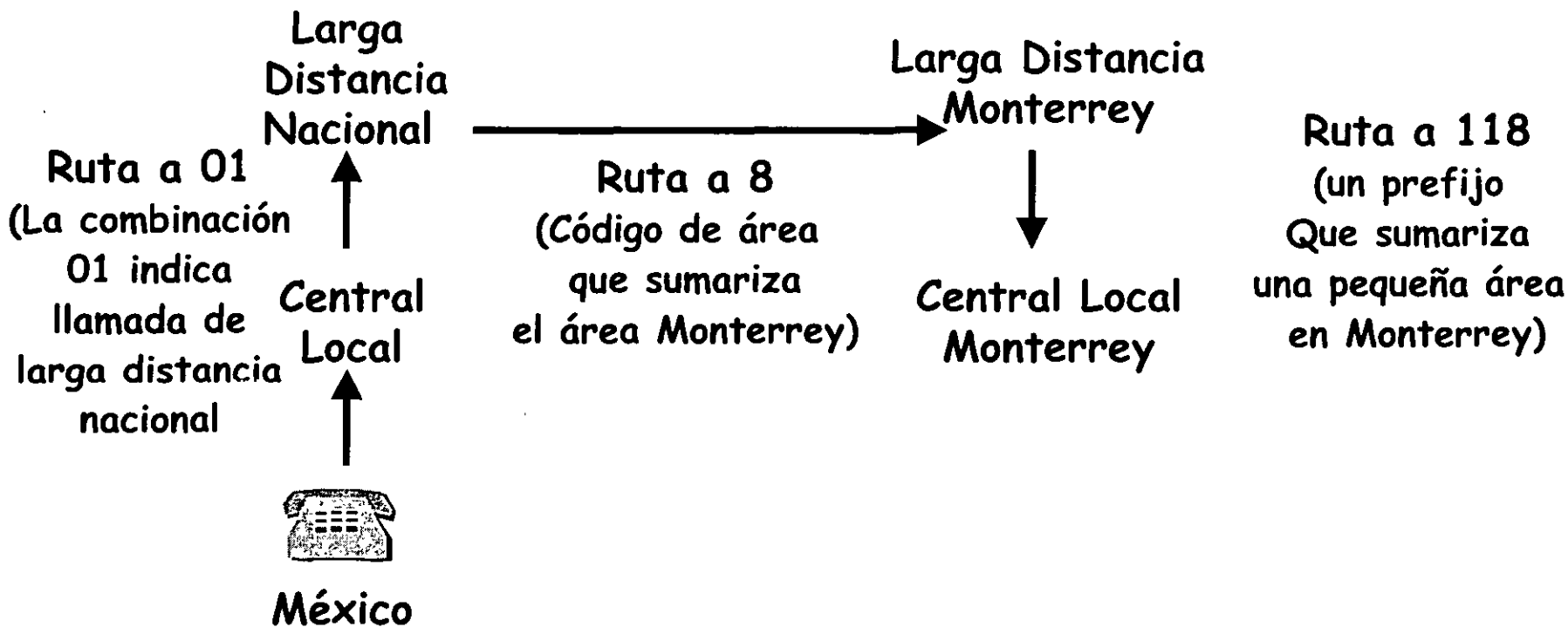
·¿Un conmutador telefónico de México conoce cómo llegar a un teléfono específico en Monterrey?
(01-8-118-8756)

Planeación Jerárquica IP



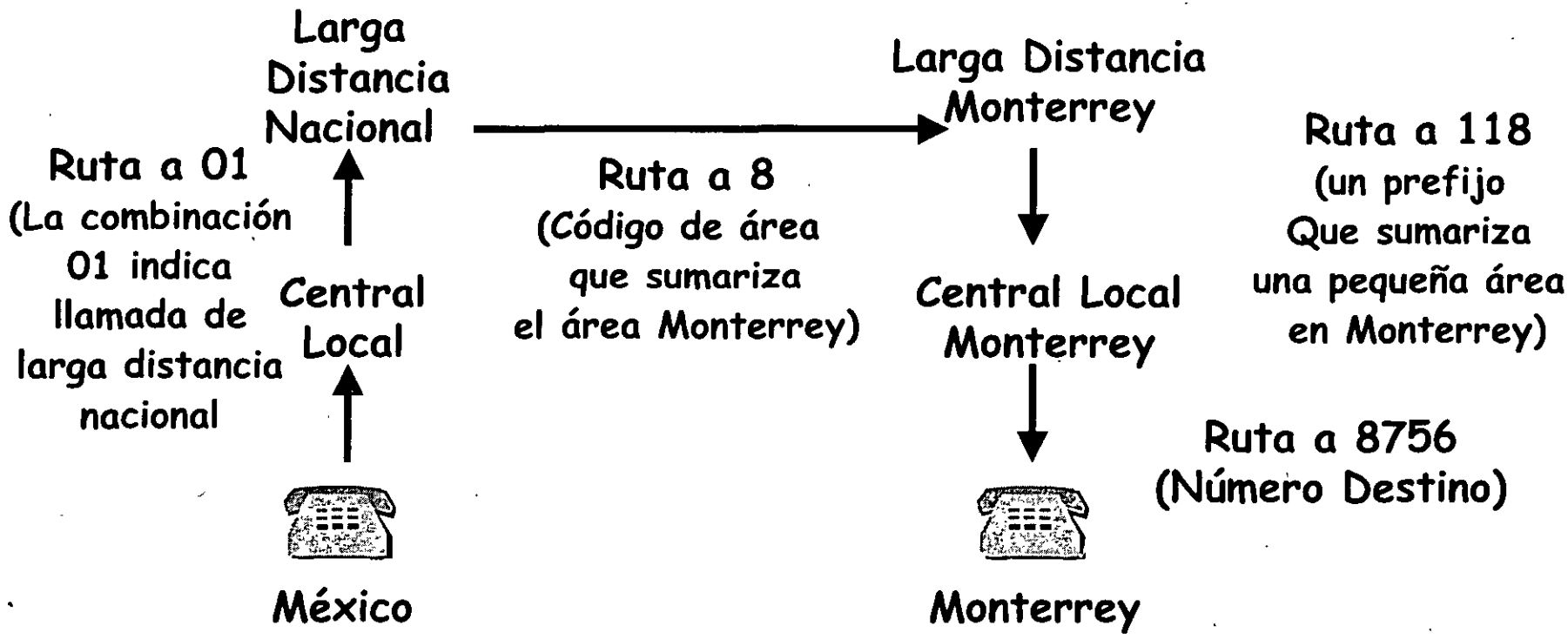
•¿Un conmutador telefónico de México conoce cómo llegar a un teléfono específico en Monterrey?
(01-8-118-8756)

Planeación Jerárquica IP



·¿Un conmutador telefónico de México conoce cómo llegar a un teléfono específico en Monterrey?
(01-8-118-8756)

Planeación Jerárquica IP



·¿Un conmutador telefónico de México conoce cómo llegar a un teléfono específico en Monterrey?
(01-8-118-8756)

Beneficios del Direccionamiento Jerárquico

- Reduce el número de direcciones en la tabla de enrutamiento
  - Sumariza multiples direcciones en rutas sumarizadas
- Eficiente asignación de direcciones
  - Asignación contigua de direcciones permite la utilización de todo el espacio de direccionamiento

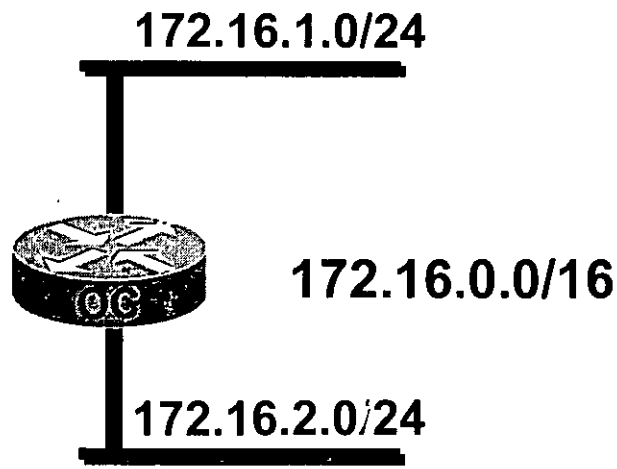
VLSM

Variable Length Subnet Mask
Máscara de Subred Variable

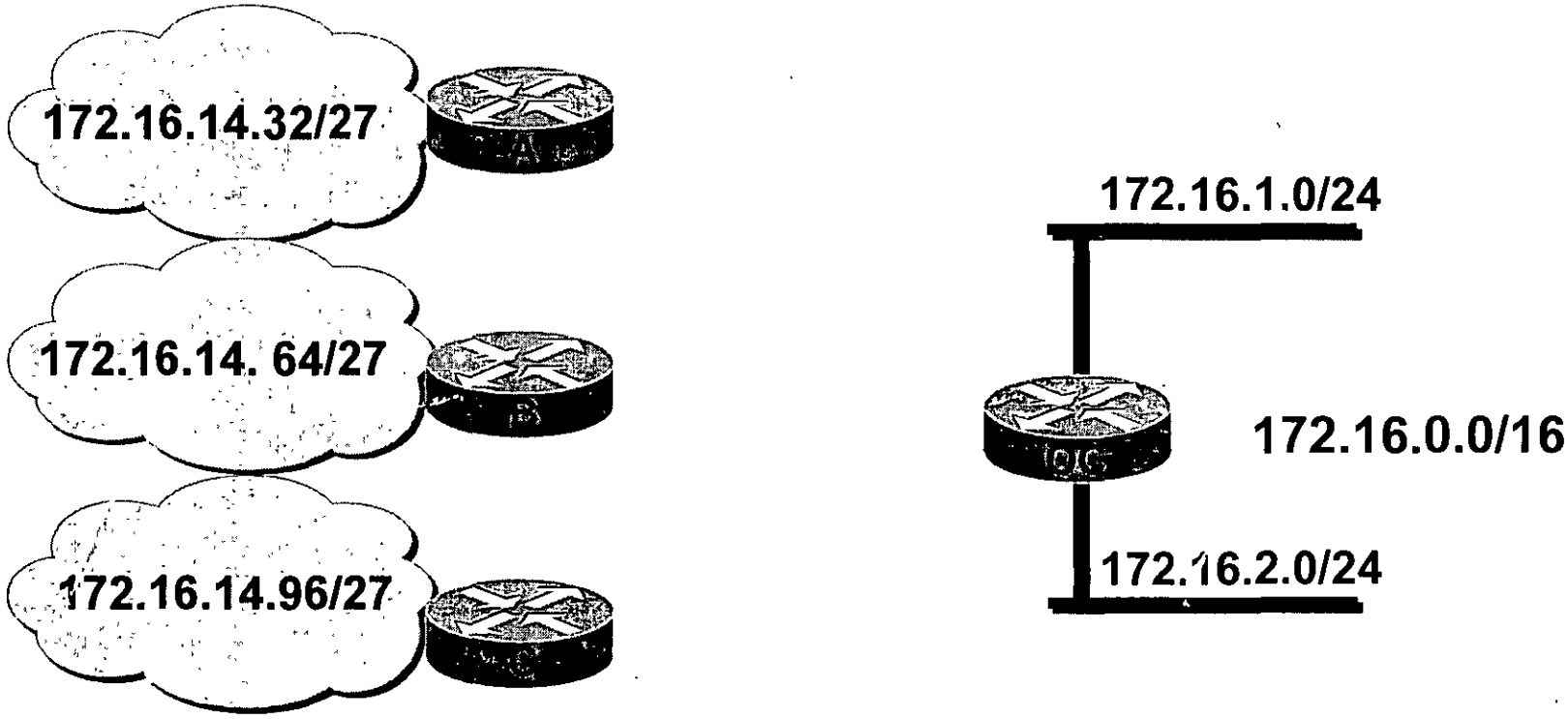
¿Qué es Máscara de Subred Variable?

172.16.0.0/16

¿Qué es Máscara de Subred Variable?

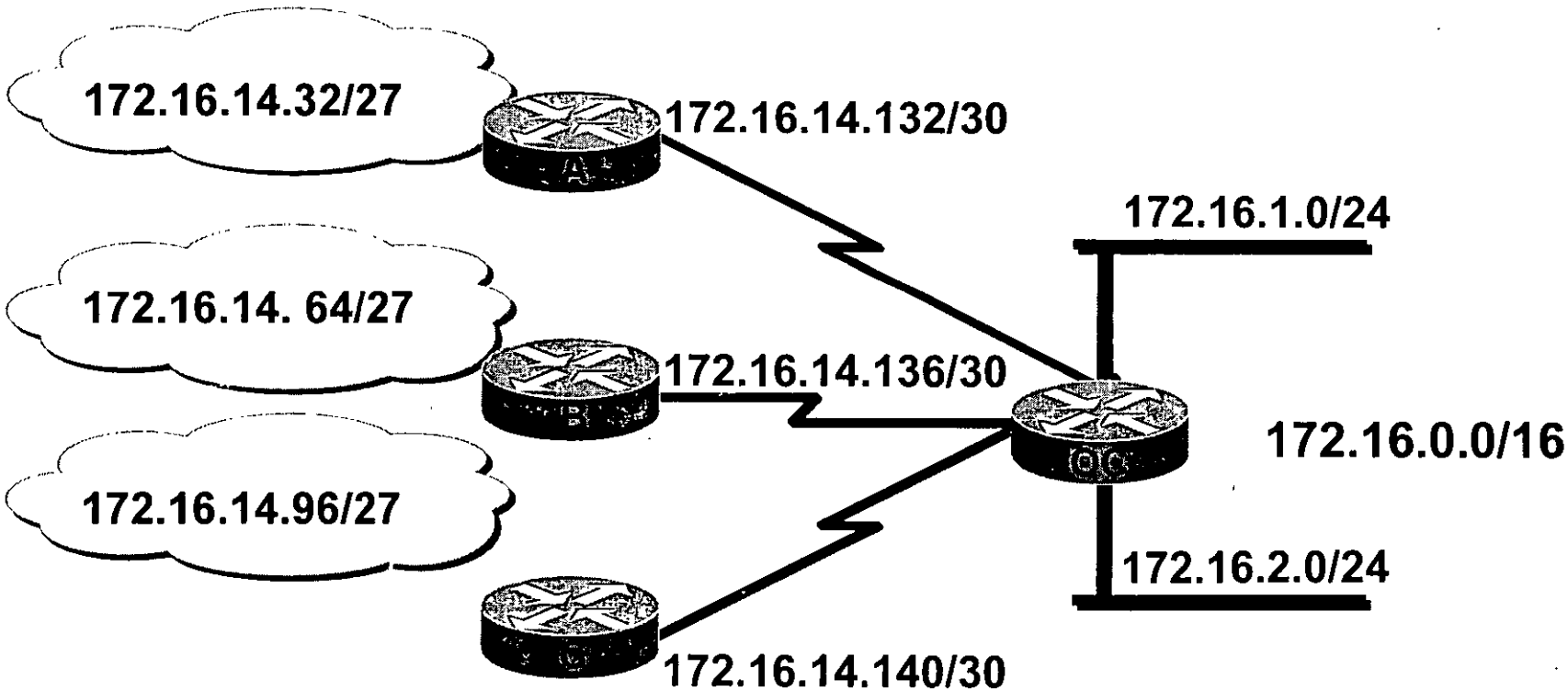


¿Qué es Máscara de Subred Variable?



- La subred 172.16.14.0/24 está dividida en pequeñas subredes:
  - La primera Subred con máscara (/27)

¿Qué es Máscara de Subred Variable?



- La subred 172.16.14.0/24 está dividida en pequeñas subredes:
  - La primera Subred con máscara (/27)
  - Una de estas no es utilizada en otra parte (/30)

Calculando VLSM

Dirección de Subred : 172.16.32.0/20
En Binario 10101100. 00010000.00100000.00000000

Calculando VLSM

Dirección de Subred: 172.16.32.0/20
En Binario 10101100. 00010000.00100000.00000000

Dirección: 172.16.32.0/26
En Binario 10101100. 00010000.00100000.00000000

Calculando VLSM

Subnetted Address: 172.16.32.0/20
In Binary 10101100. 00010000.00100000.00000000

VLSM Address: 172.16.32.0/26
In Binary 10101100. 00010000.0010|0000.00|000000

1st subnet: | 10101100 . 00010000 | .0010 | 0000.00 | **000000=172.16.32.0/26**

Network **Subnet** **VLSM subnet** **Host**

Calculando VLSM

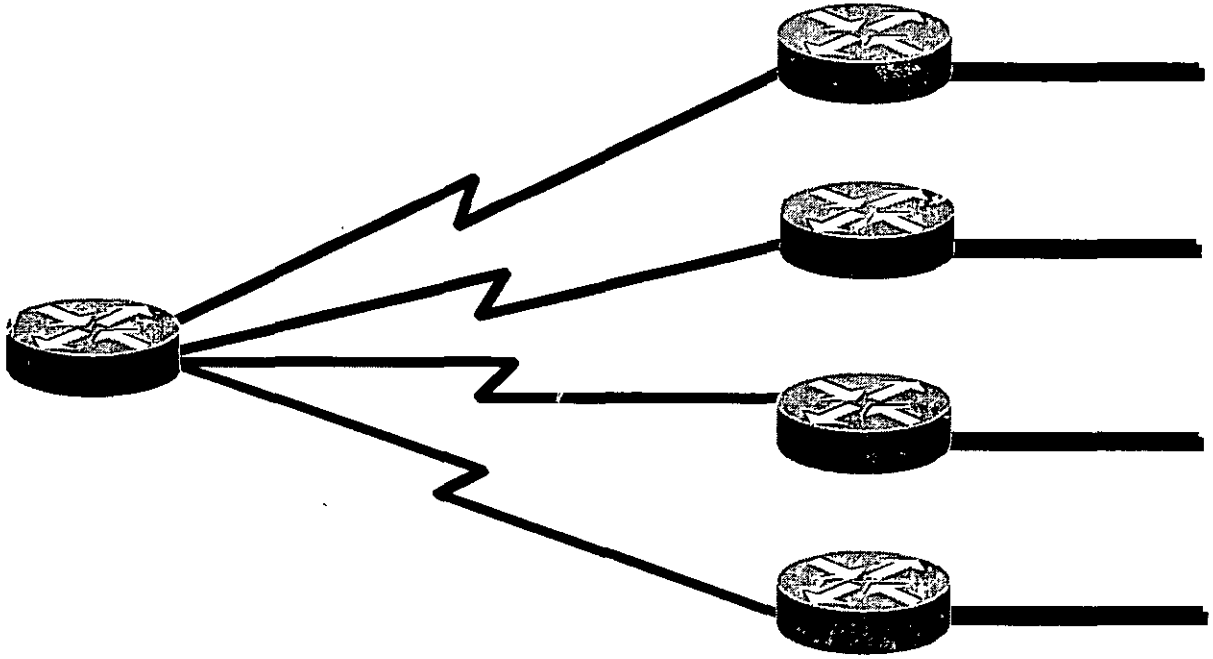
Subnetted Address: 172.16.32.0/20
In Binary 10101100. 00010000.00100000.00000000

VLSM Address: 172.16.32.0/26
In Binary 10101100. 00010000.00100000.00000000

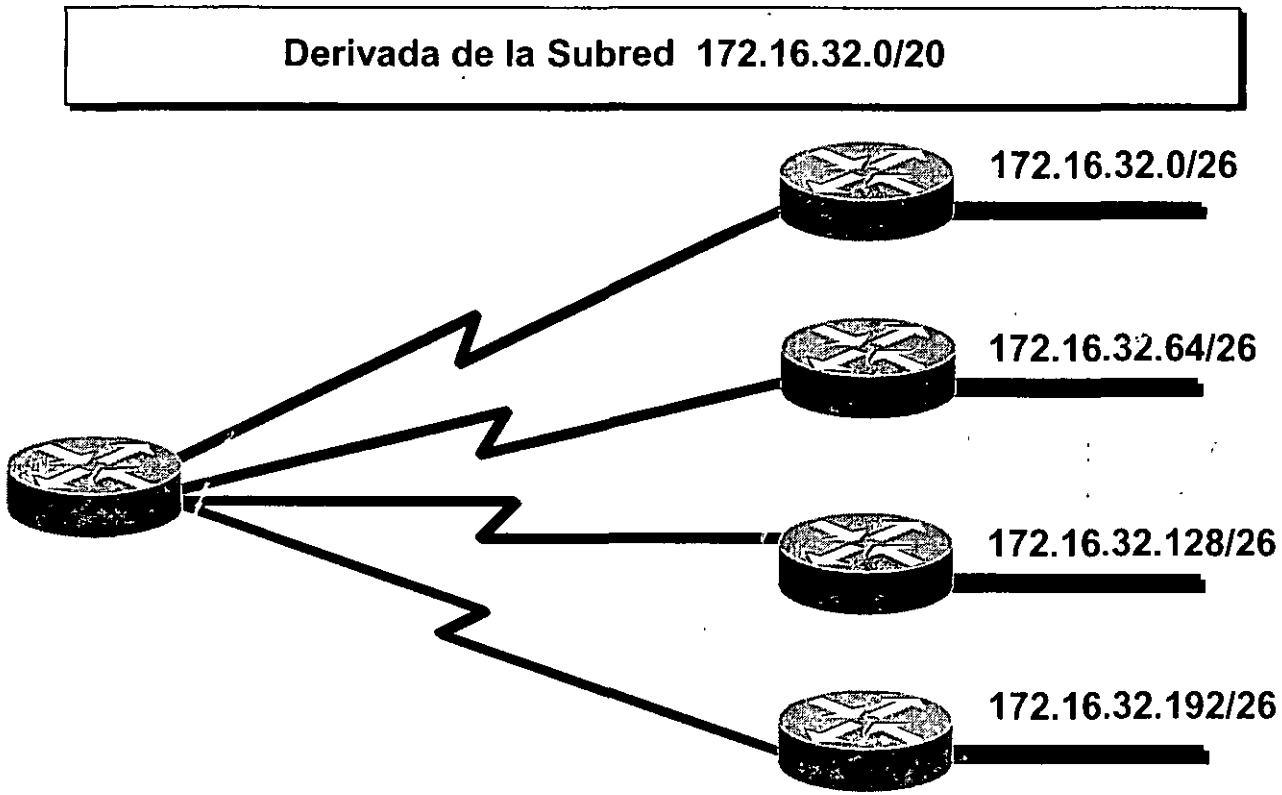
1st subnet:	10101100 . 00010000	.0010	0000.00	000000=172.16.32.0/26
2nd subnet:	172 . 16	.0010	0000.01	000000=172.16.32.64/26
3rd subnet:	172 . 16	.0010	0000.10	000000=172.16.32.128/26
4th subnet:	172 . 16	.0010	0000.11	000000=172.16.32.192/26
5th subnet:	172 . 16	.0010	0001.00	000000=172.16.33.0/26
	Network	Subnet	VLSM Subnet	Host

Ejemplo de VLSM

Derivada de la Subred 172.16.32.0/20

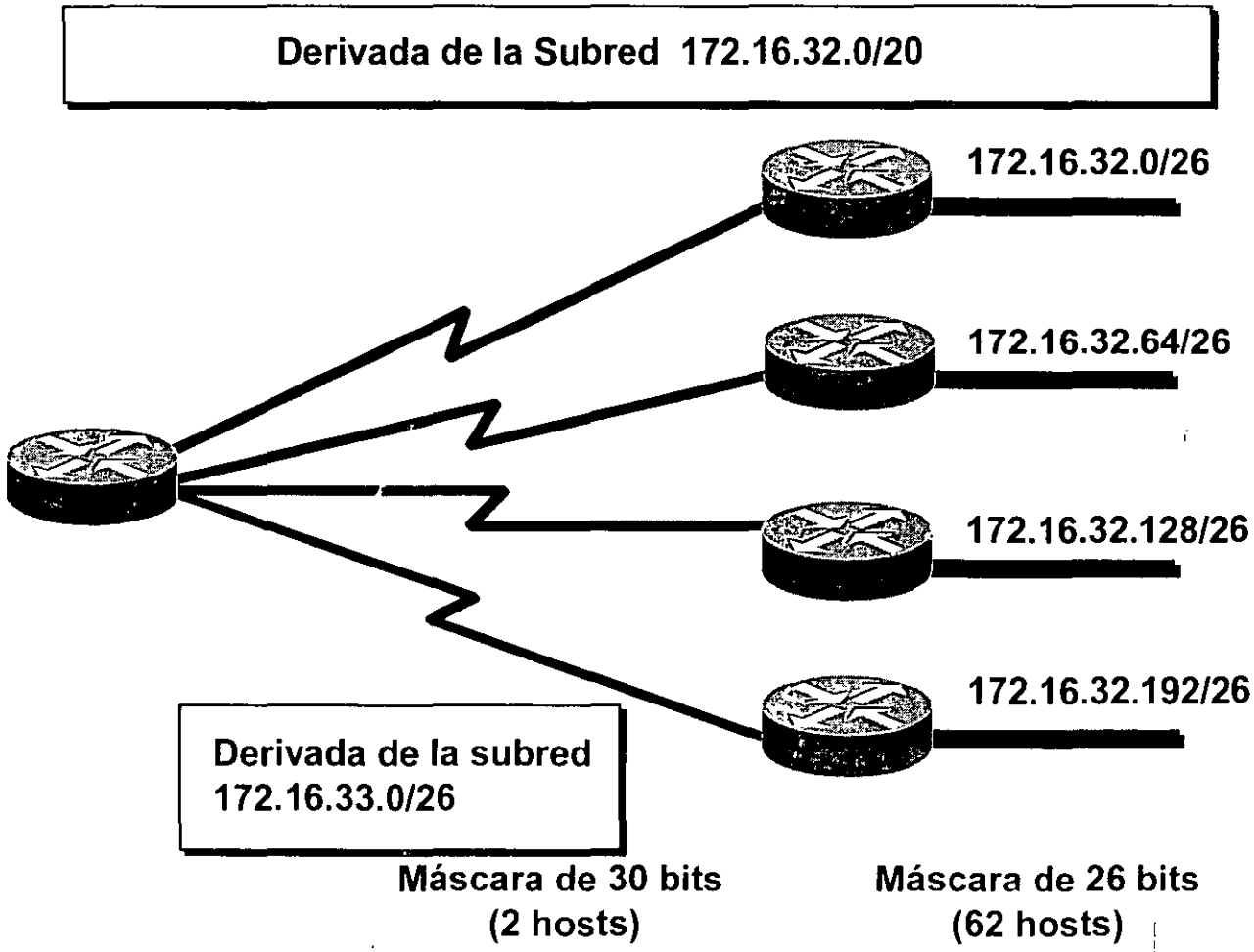


Ejemplo de VLSM

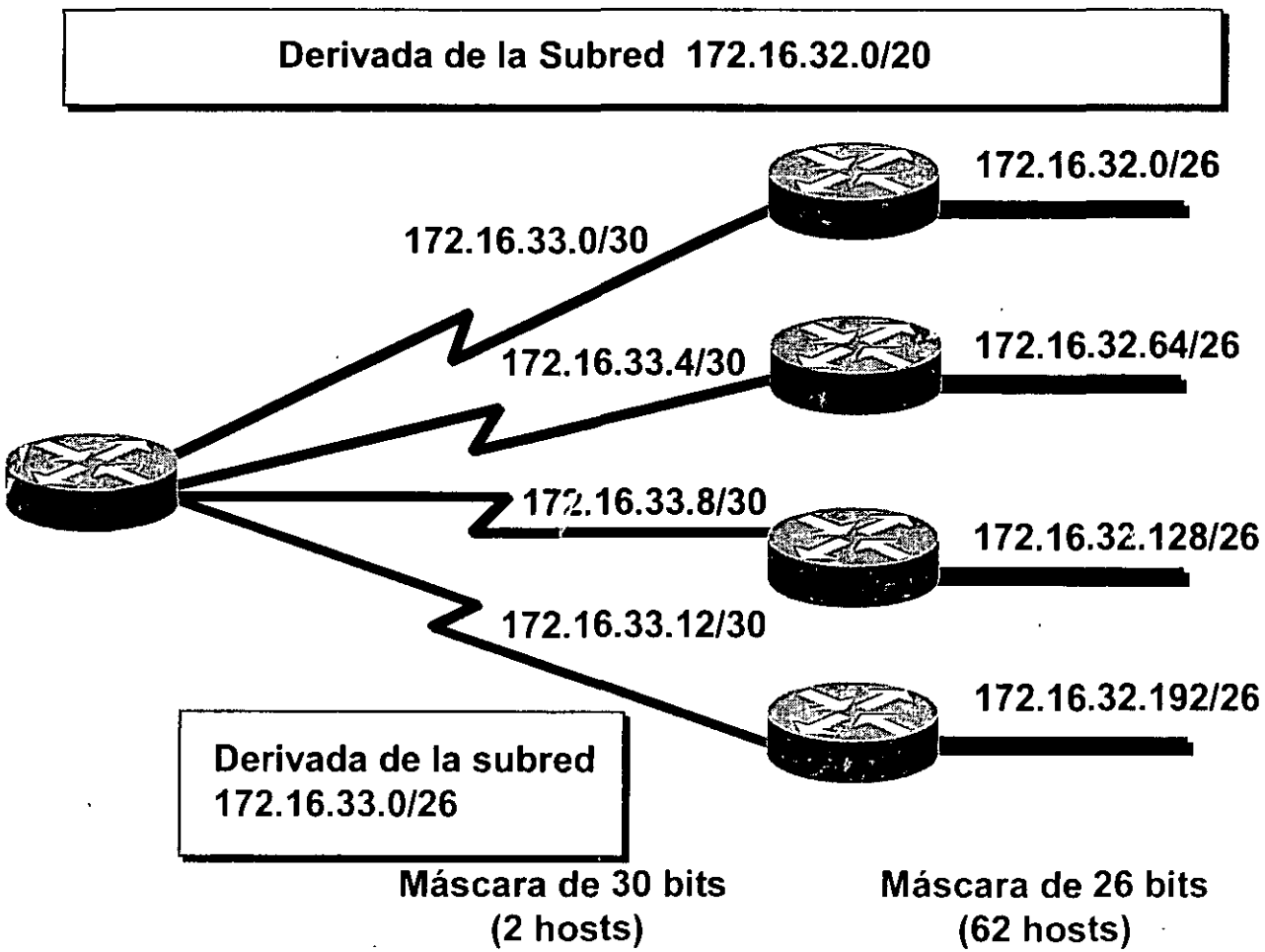


Máscara de 26 bits
(62 hosts)

Ejemplo de VLSM

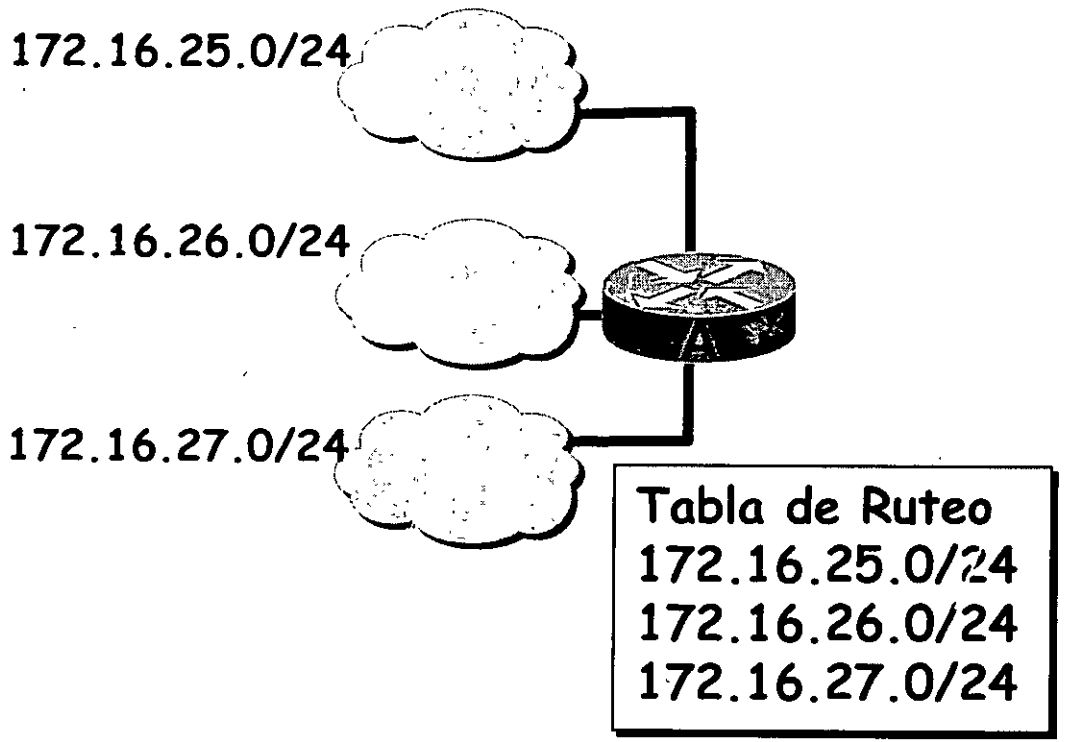


Ejemplo de VLSM

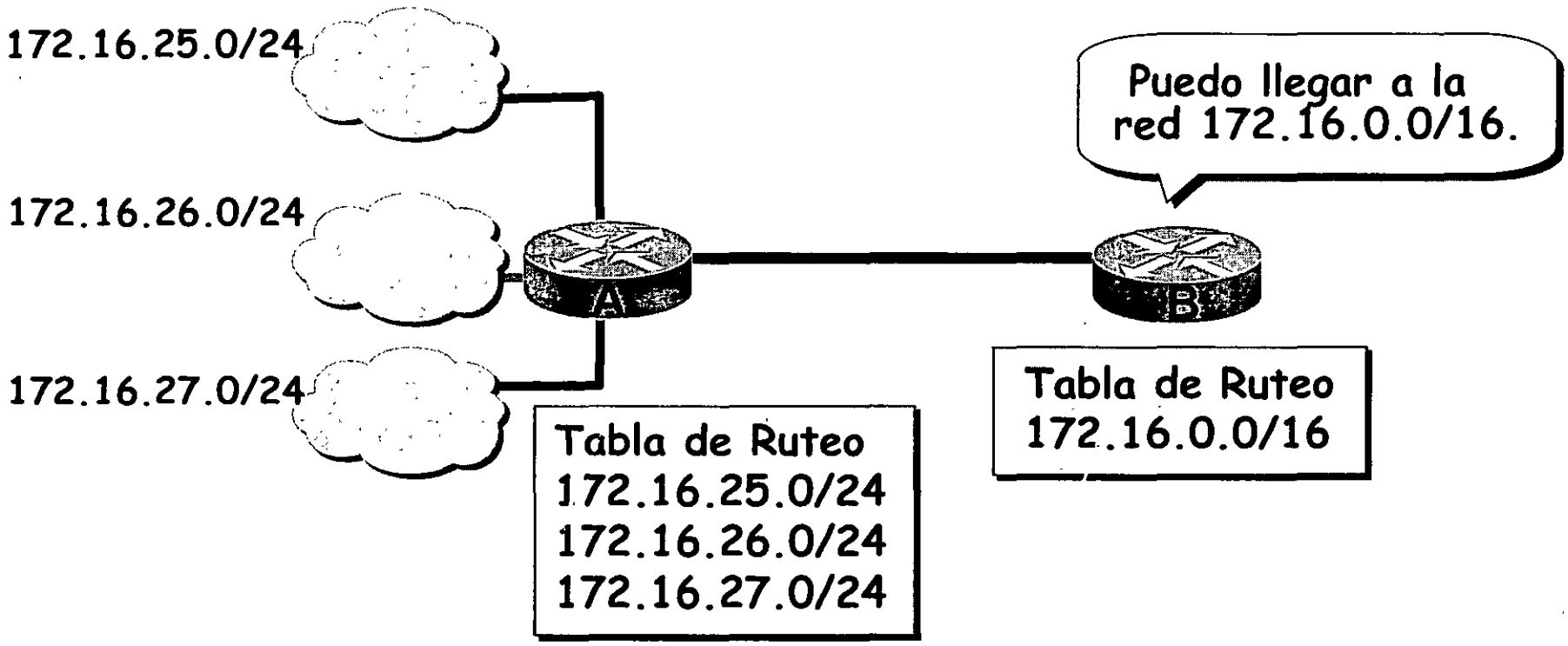


SUMARIZACIÓN

¿Que es la Sumarización?



¿Que es la Sumarización?



- Los protocolos de Enrutamiento pueden sumarizar las direcciones de varias redes en una sola dirección

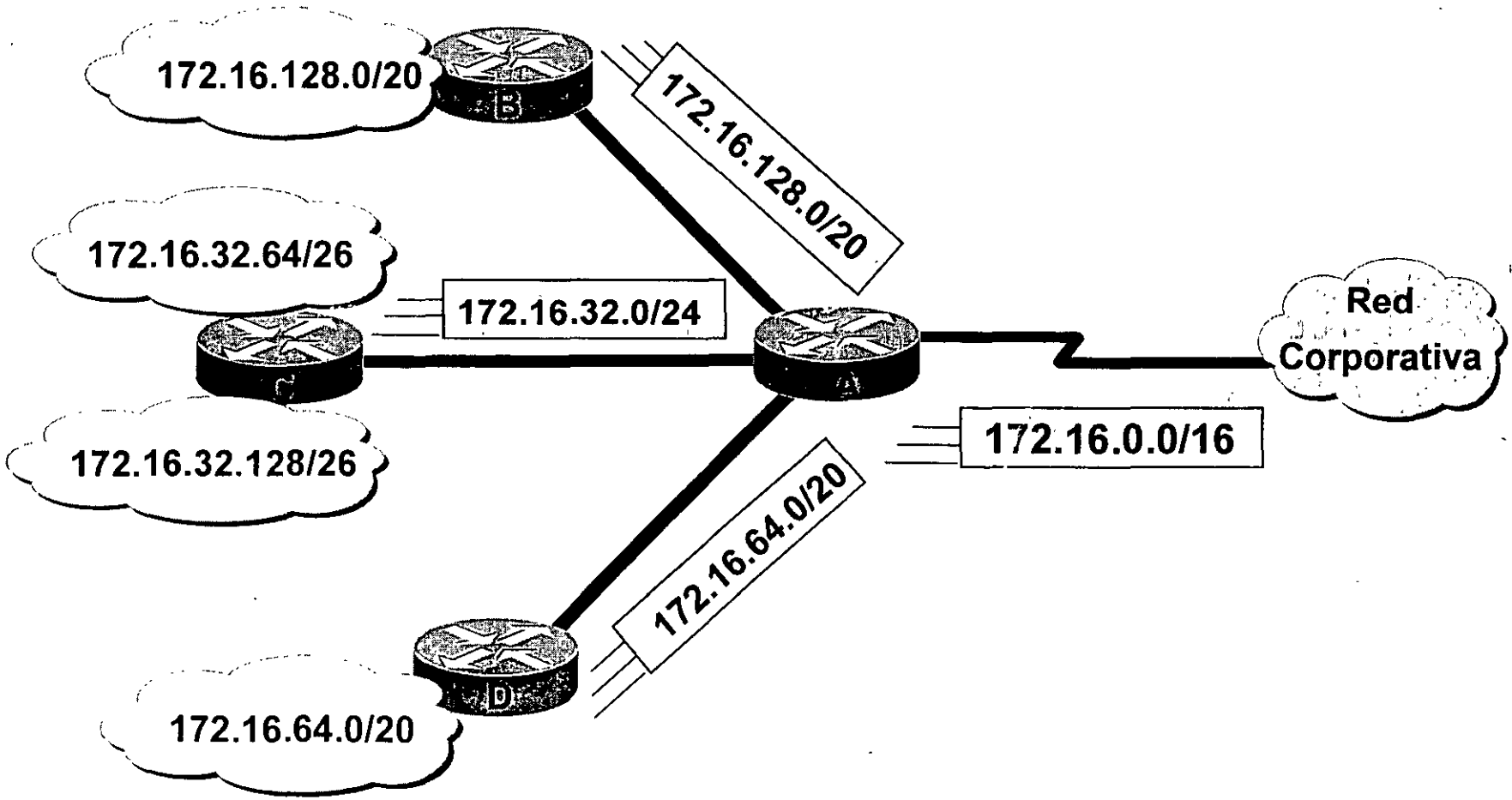
Sumarizando dentro de un Octeto

172.16.168.0/24 =	10101100	.	00010000	.	10101	000	.	00000000
172.16.169.0/24 =	172	.	16	.	10101	001	.	0
172.16.170.0/24 =	172	.	16	.	10101	010	.	0
172.16.171.0/24 =	172	.	16	.	10101	011	.	0
172.16.172.0/24 =	172	.	16	.	10101	100	.	0
172.16.173.0/24 =	172	.	16	.	10101	101	.	0
172.16.174.0/24 =	172	.	16	.	10101	110	.	0
172.16.175.0/24 =	172	.	16	.	10101	111	.	0

Número de bits comunes = 21
Sumarizado: 172.16.168.0/21

Bits no comunes = 11

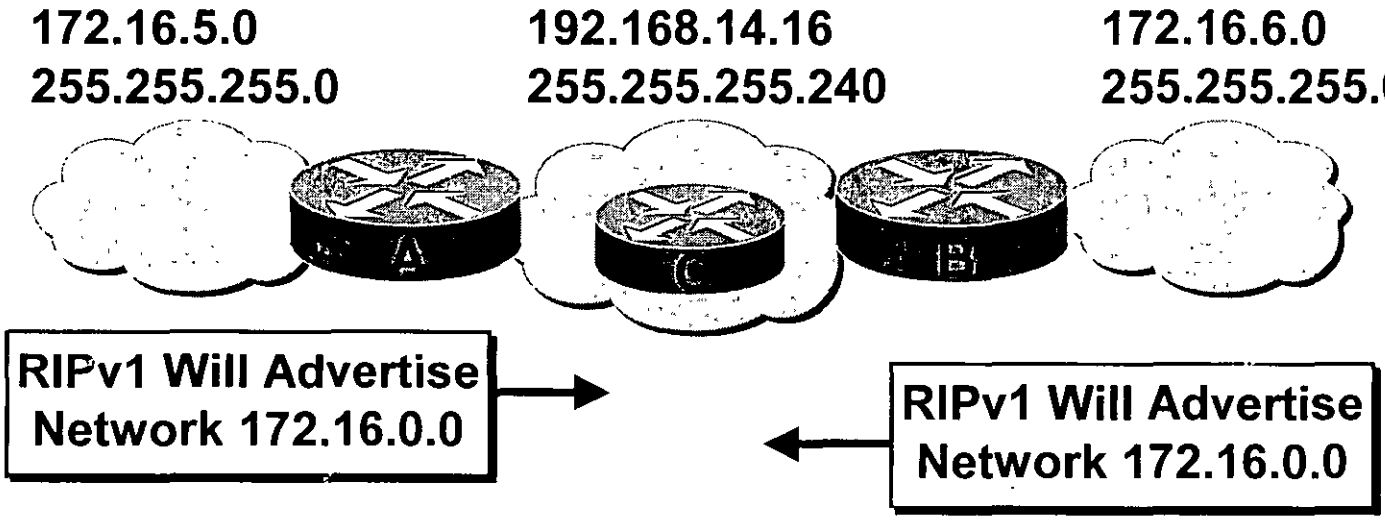
Sumarización de Direcciones en una Red VLSM



Consideraciones de Implementación

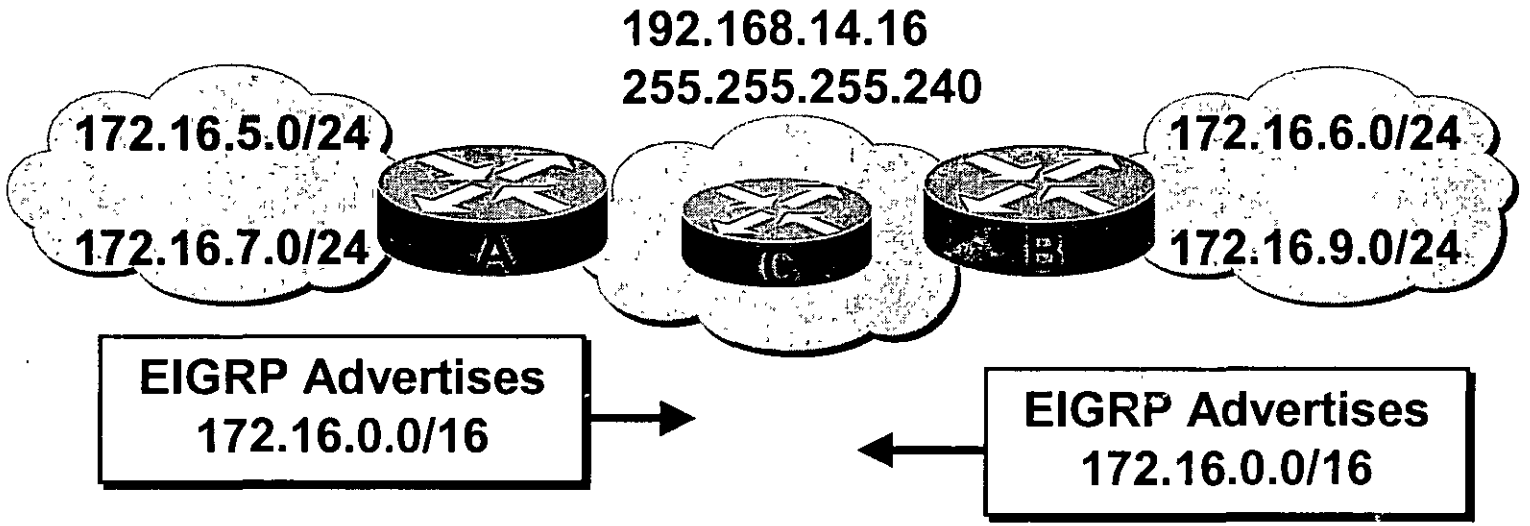
- Multiples direcciones IP deben tener los mismos bits de más alto orden
- Las decisiones de enrutamiento son basadas en la dirección completa
- Los protocolos de enrutamiento deben portar la longitud del prefijo (máscara de subred)

Sumarizando Rutas en Redes Discontiguas



- RIPv1 e IGRP no anuncian las subredes, y por lo tanto no soportan redes discontiguas
- OSPF, EIGRP, y RIPv2 anuncian subredes y por lo tanto soportan redes discontiguas

Be Careful When Summarizing Routes



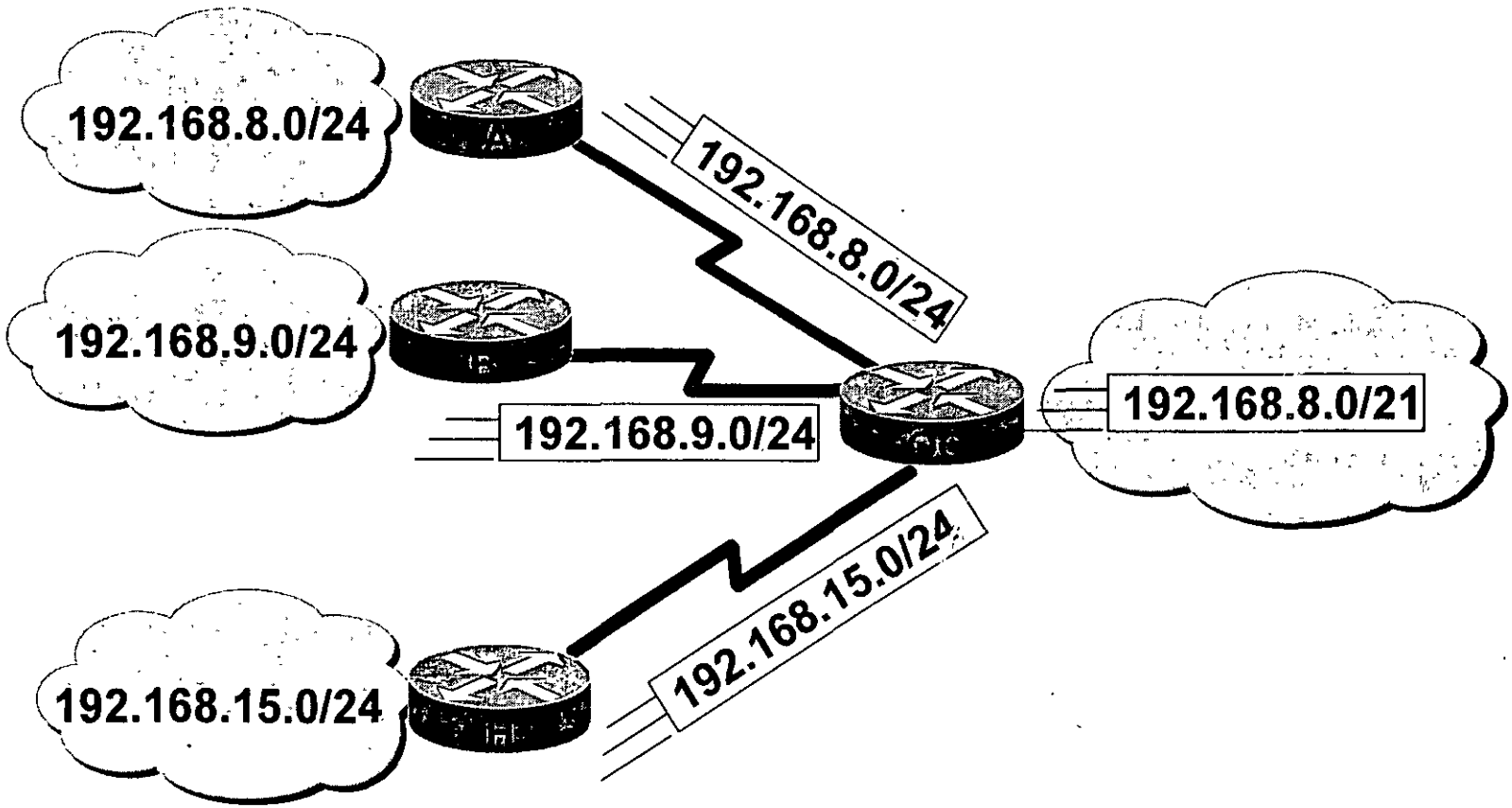
- EIGRP on both Router A and Router B advertise a summarized route to 172.16.0.0/16
- Router C receives two routes to 172.16.0.0/16
- Router A (or B or both) should be configured to not summarize

CIDR
Classless InterDomain Routing

Classless Interdomain Routing

- Mecanismo desarrollado para aliviar el agotamiento de direccionamiento y reducir el tamaño de la tabla de enrutamiento
- Bloques de direcciones clase C asignadas a ISPs. Estos ISPs asignan subconjuntos de estas direcciones a sus clientes
- Los bloques son sumarizados en las tablas de enrutamiento

Ejemplo



- Redes de la 192.168.8.0/24 hasta la 192.168.15.0/24 son sumarizadas por *OC* en un solo anuncio: 192.168.8.0/21

Protocolos de Enrutamiento

What Is Routing?

- Routing is the process of forwarding an item from one location to another
- Routers forward traffic to a logical destination in a computer network
- Routers perform two major functions:
  - Routing
    - Learning the logical topology of the network
  - Switching
    - Forwarding packets from an inbound interface to an outbound interface

Routing Requirements

- Is the protocol suite active on this device?
- Is the destination network known to this device?
  - Is there an entry in the routing table?
  - Is the route currently available?
- Which outbound interface represents the best path?
  - Lowest metric path is preferred
  - Equal lowest metric paths are shared

Routing Information

– Most of the necessary information is contained in the routing table

```
I   172.16.8.0   [100/118654]  via 172.16.7.9,  00:00:23,  Serial0
```

I	-- How the route was learned (IGRP)
172.16.8.0	-- Destination logical network or subnet
[100	-- Administrative distance (trustworthiness factor)
/118654]	-- Metric value (reachability)
via 172.16.7.9	-- Next-hop logical address (next router)
00:00:23	-- Age of entry (in hours:minutes:seconds)
Serial0	-- Interface through which the route was learned and through which the packet will leave

Administrative Distance

- Administrative distance is a selection method for IP routing protocols
- The lower the administrative distance, the more trusted the learning mechanism
  - Manually entered routes are preferred to dynamically learned routes
  - Routing protocols with sophisticated metrics are preferred over protocols with simple metric structures

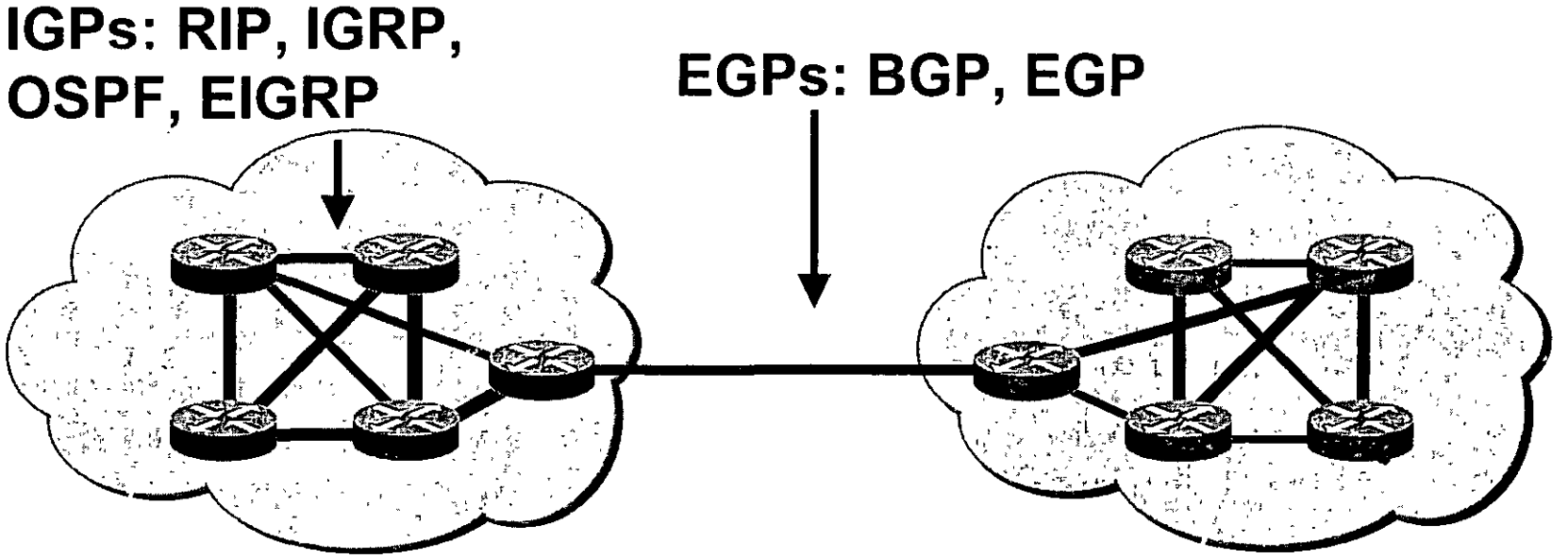
Routing Decisions

- Routing protocols maintain a loop-free, single path to each destination network
- Routes are advertised with a reachability factor referred as a metric
- The path to the destination network is represented by the sum of the metrics associated with all intermediate links
- The routing process uses the metric value to select a preferred path to each destination
  - Multiple paths can be used if metric values are equal

Routers Forward Traffic

- Routing protocols maintain neighbor relationships with adjacent (connected) routers
  - Neighboring routers and routing protocols exchange frames containing either:
    - Hello packets
    - Routing update packets
  - Routing tables contain routes learned from neighboring routers
- Routers forward traffic to the destination network by passing packets to the next-hop logical device (router) in the delivery path

IGP vs EGP



- An autonomous system (AS) is a collection of networks under a a single technical administration
- IGPs operate within an autonomous system
- EGPs connect different autonomous systems

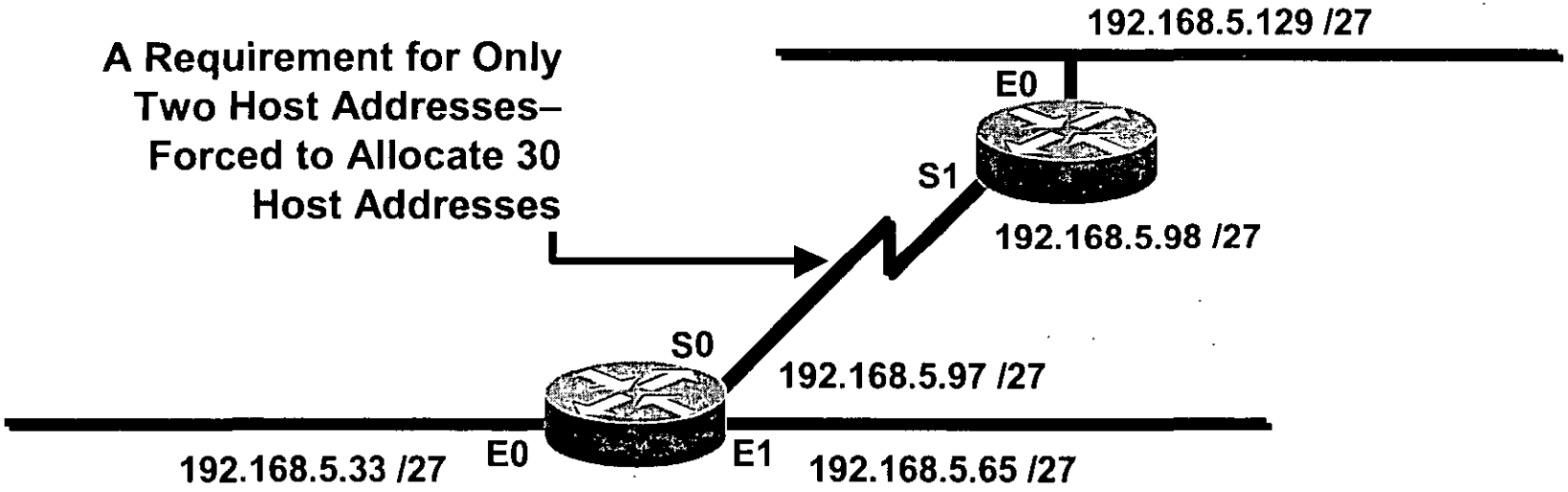
Classfull Routing Overview

- Classfull routing protocols are a consequence of the distance vector method of route calculation
  - RIPv1
  - IGRP
- Routing masks are not carried within the periodic routing updates
  - Within a network, consistency of masks is assumed

Classful Routing Overview

- Classful routing protocols are a consequence of the distance vector method of route calculation
  - RIPv1
  - IGRP
- Routing masks are not carried within the periodic routing updates
  - Within a network, consistency of masks is assumed

Classfull Subnetting Requirements

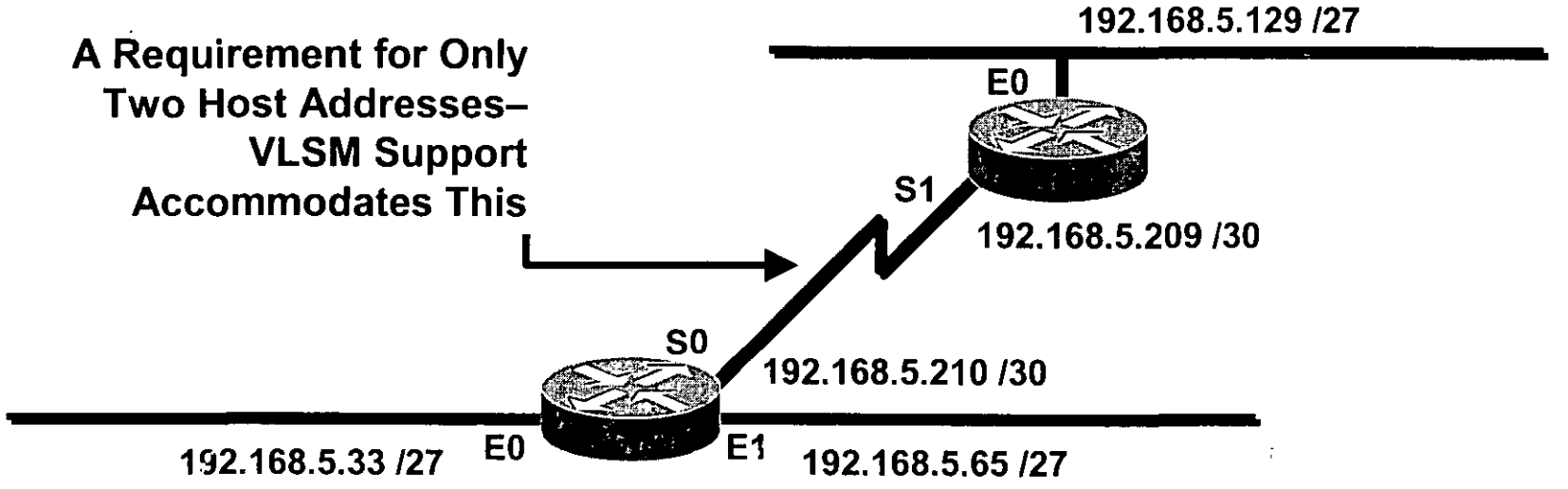


- All router interfaces in the network must have the same subnet mask
- This approach may not fully utilize available allocation of host addresses

Classless Routing Overview

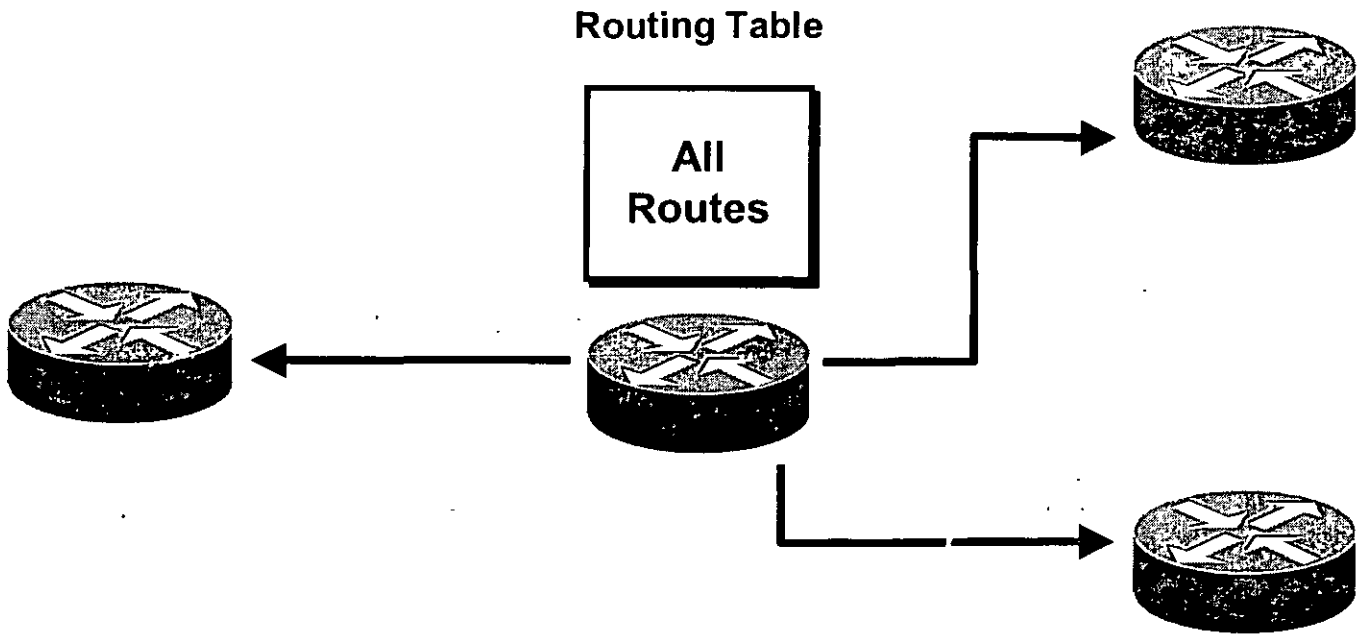
- Classless routing protocols include the routing mask with the route advertisement
  - OSPF
  - EIGRP
  - RIPv2
  - IS-IS
  - BGP
- Summary routes can be manually controlled within the network

Classless Subnetting Requirements



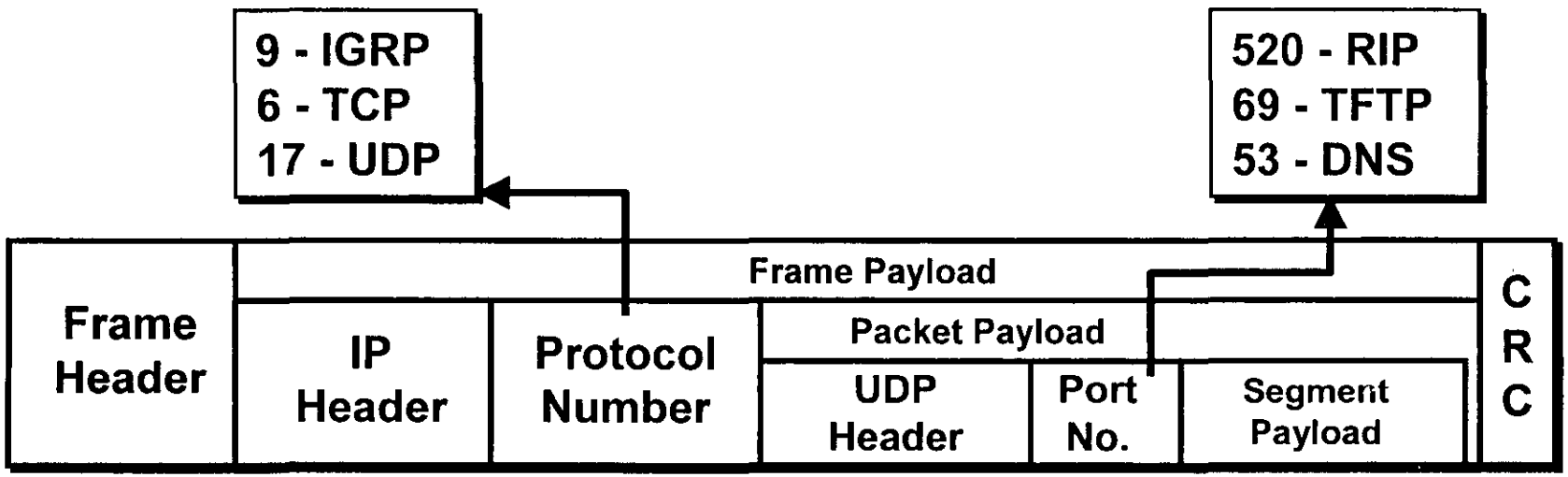
- Router interfaces within the same network can have different subnet masks
  - Variable-length subnet masking (VLSM) is supported
- This approach maximizes allocation of available host addresses

Distance Vector Routing Update Traffic



- In a distance vector environment, routing updates are propagated only to directly connected neighbors

Distance Vector Routing Protocols



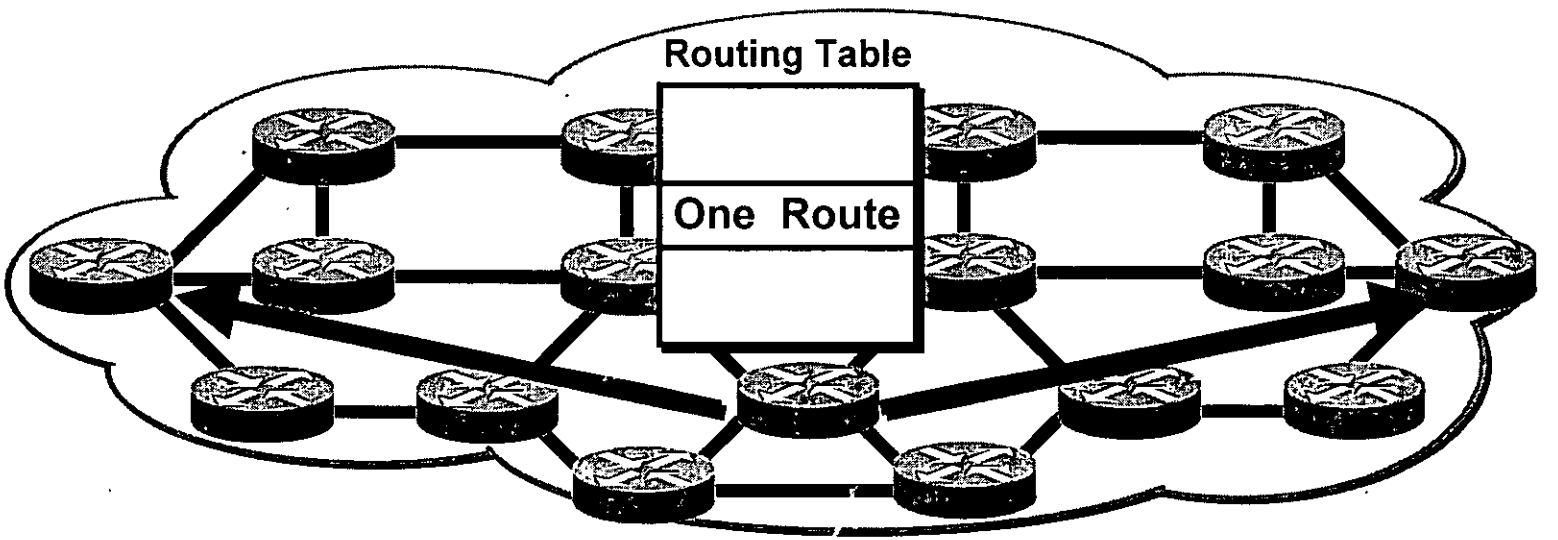
- Cisco routers support several distance vector routing protocols
  - RIP
  - IGRP
- Routing protocols rely on IP packets for delivery of routing information

Distance Vector Protocol Comparison Chart

Characteristic	RIPv1	RIPv2	IGRP	EIGRP**
Count to infinity	X	X	X	
Split horizon	X	X	X	X
Hold-down timer	X	X	X	
Triggered updates with route poisoning	X	X	X	X
Load balancing—Equal paths	X	X	X	X
Load balancing—Unequal paths			X	X
VLSM support		X		X
Routing algorithm	B-F	B-F	B-F	DUAL
Metric	Hops	Hops	Comp	Comp
Hop count limit	16	16	100	100
Scalability	Med	Med	Large	Large

** EIGRP is an advanced distance vector protocol

Link-State Routing Update Traffic



– In a link-state environment, link-state announcements are propagated to all devices in the routing domain
  - Hierarchical design can limit the requirement to notify all devices

Link-State Protocol Comparison Chart

Characteristic	OSPF	IS-IS*	EIGRP**
Hierarchical topology—Required	X	X	
Retains knowledge of all possible routes	X	X	X
Route summarization—Manual	X	X	X
Route summarization—Automatic			X
Event-triggered announcements	X	X	X
Load balancing—Equal paths	X	X	X
Load balancing—Unequal paths			X
VLSM support	X	X	X
Routing algorithm	Dijkstra	IS-IS	DUAL
Metric	Cost	Cost	Comp
Hop count limit	200	1024	100
Scalability	Large	VryLg	Large

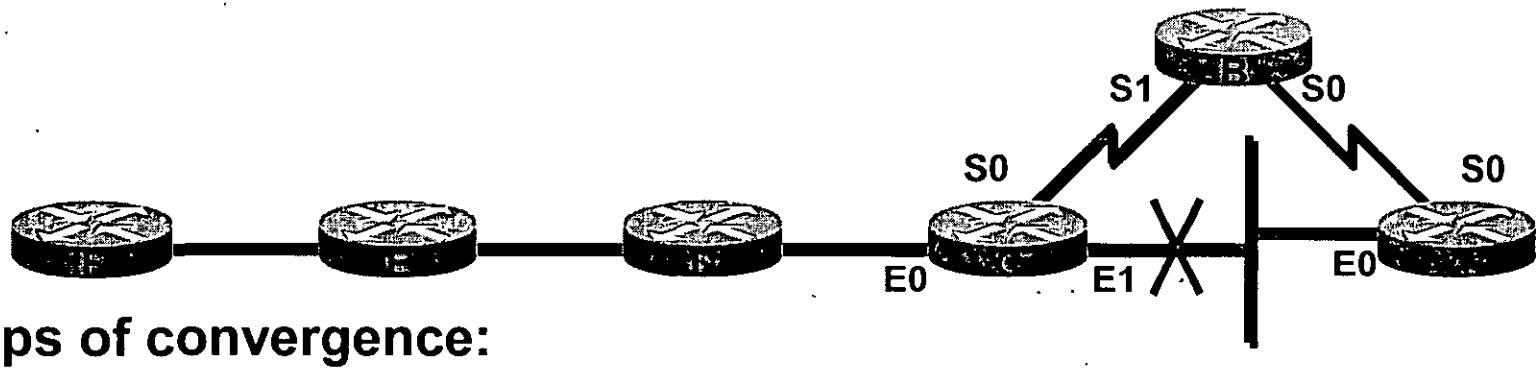
* For comparison purposes only, not a part of this course

** EIGRP has some link-state features

Convergence

- Convergence time is the time it takes for all routers to agree on the network topology after a change such as:
  - New routes being added
  - Existing routes changing state
- Convergence time is affected by:
  - Update mechanism (hold-down timers)
  - Size of the topology table
  - Route calculation algorithm
  - Media type

RIP Convergence

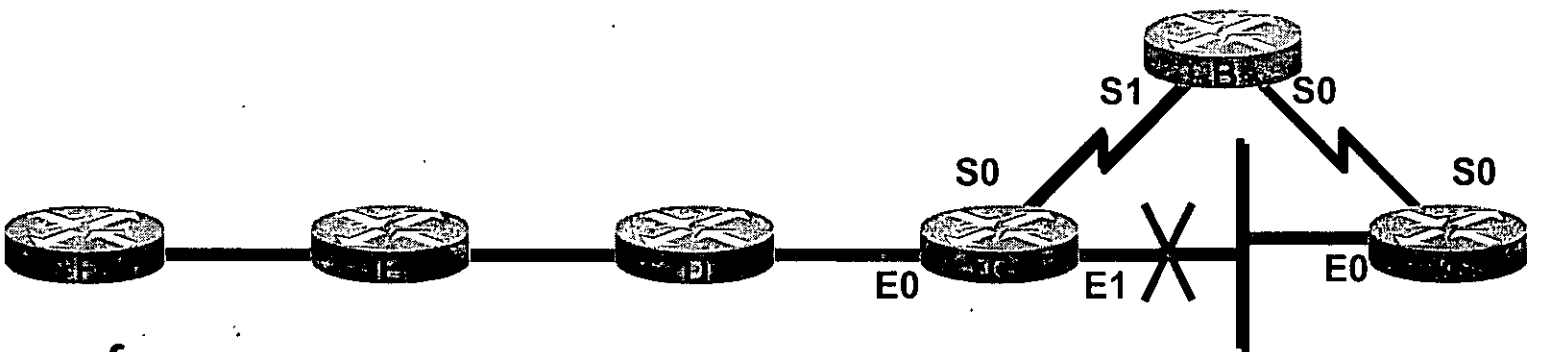


Steps of convergence:

1. C detects link failure; sends Flash update, goes to D and B
   - Route is poisoned to B and D; removed from C's routing table
2. C sends a request to neighbors for alternate path
   - Broadcast for v1, multicast for v2
3. D reports no alternate path; B reports route with weaker metric
   - Route via B immediately placed in routing table
4. C advertises route via B in periodic update to D
   - No change to table because route is in hold-down
5. In D, E, and F, as hold-down timer expires, route is added to table
   - New route propagated in periodic update

Convergence time at F: hold-down time plus two or three update intervals

IGRP Convergence

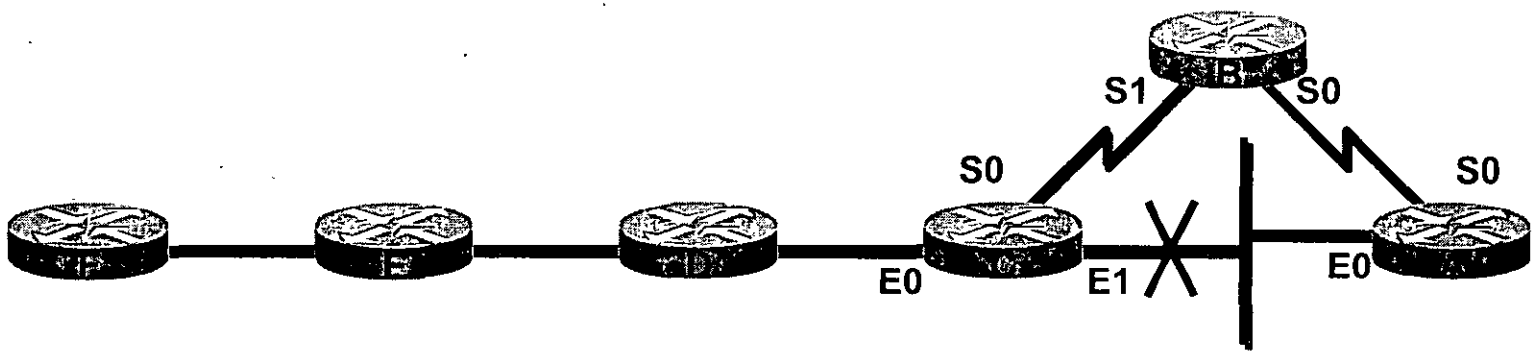


Steps of convergence:

1. C detects link failure; sends Flash update, goes to D and B
   - Route is poisoned to B and D; removed from C's routing table
2. C sends query to neighbors for alternate route
   - Broadcast on all interfaces
3. C receives route with weaker metric from B; poisoned route from D
   - Route via B placed in routing table
4. C advertises route via B in Flash update to D and B
   - No change to table because route is in hold-down
5. In D, E, and F, as hold-down timer expires, route is added to table
   - New route propagated in periodic update

Convergence time at F: hold-down time plus two or three update intervals

EIGRP Convergence

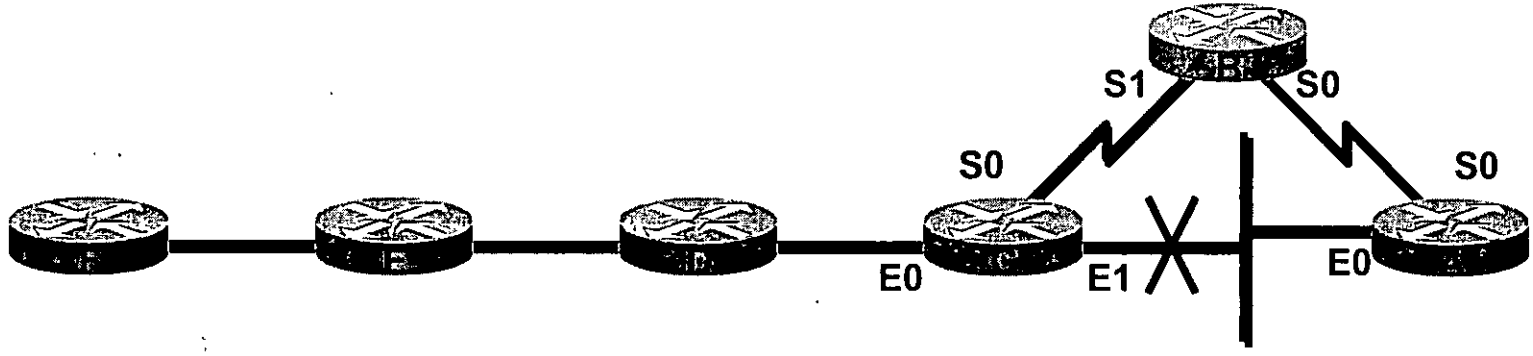


Steps of convergence:

1. C detects link failure; has no FS, goes into active convergence
   - No successor candidates present in topology database
2. C sends query to B and D to get logical successor
   - Because no route with a lower feasible distance available
3. D's response indicates no logical successor
4. B's response indicates FS with higher feasible distance
5. C accepts new path and distance, adds route via B to table
6. Sends Flash update about higher metric, goes to D and B
   - Only higher metric propagated in triggered update

Convergence time to F: approximately 2 seconds

OSPF Convergence



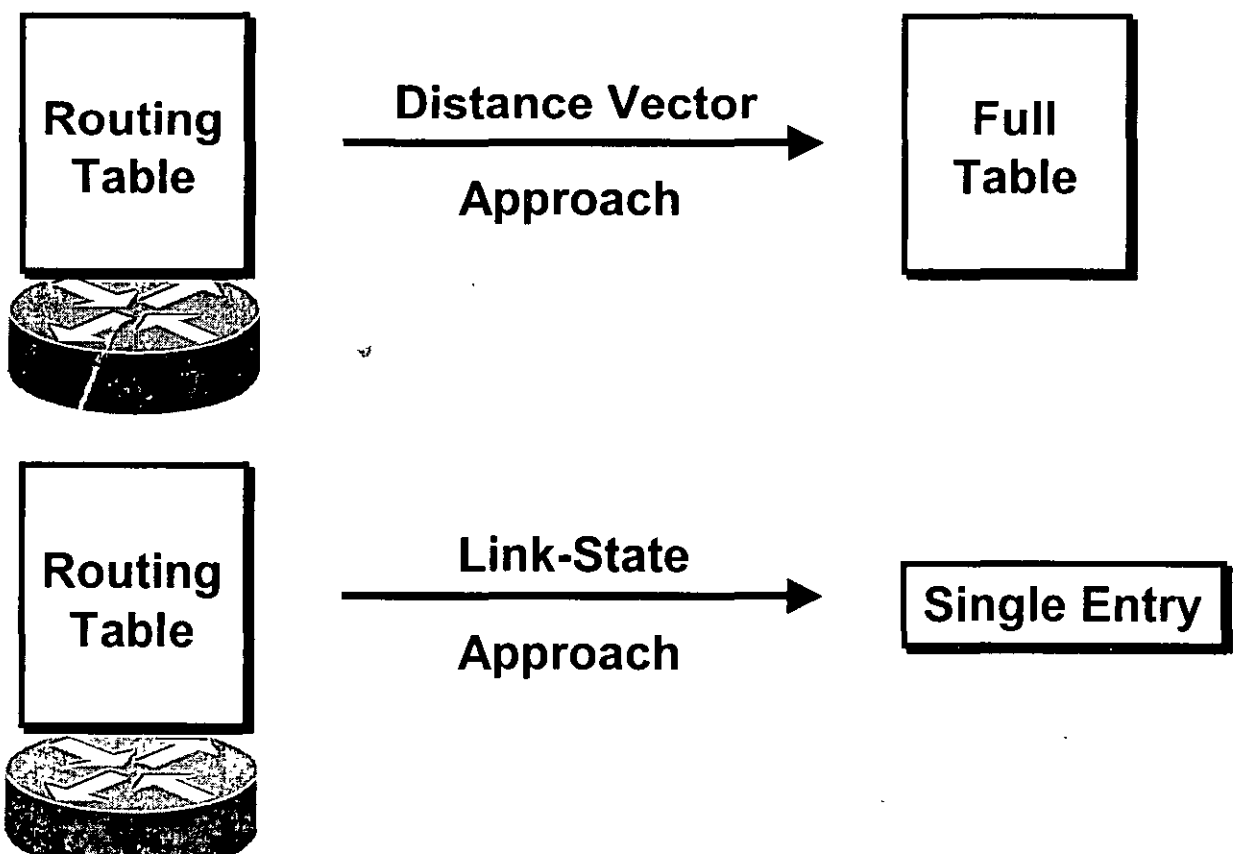
Steps of convergence:

1. C detects link failure; sends link-state advertisement, goes to D and B
   - Topology change is detected, traffic forwarding suspended
2. All routers update topology database; copy LSA and flood to neighbors
   - All devices have topological awareness
3. All routers run Dijkstra algorithm, generate new routing table
   - Route via B in routing tables, traffic forwarding resumed

Convergence time to F: approximately 6 seconds

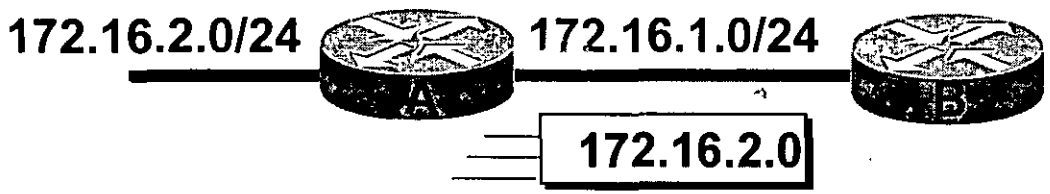
Routing Updates

– Different ways to send route information



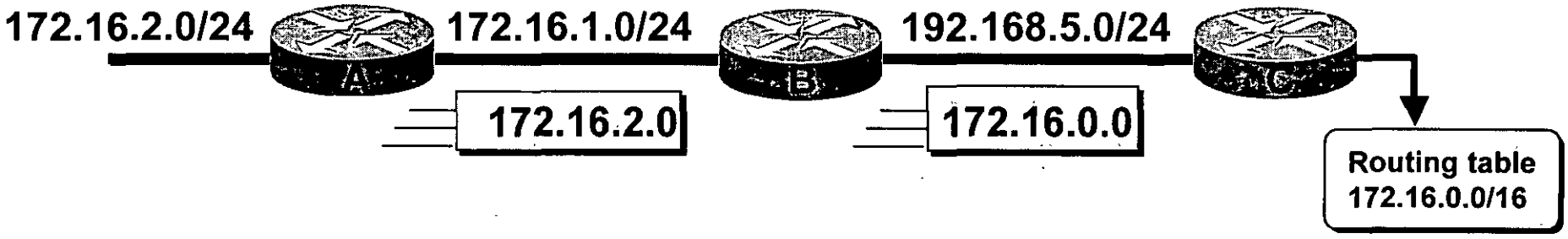
Classfull and Classless Updates

RIPv1 network



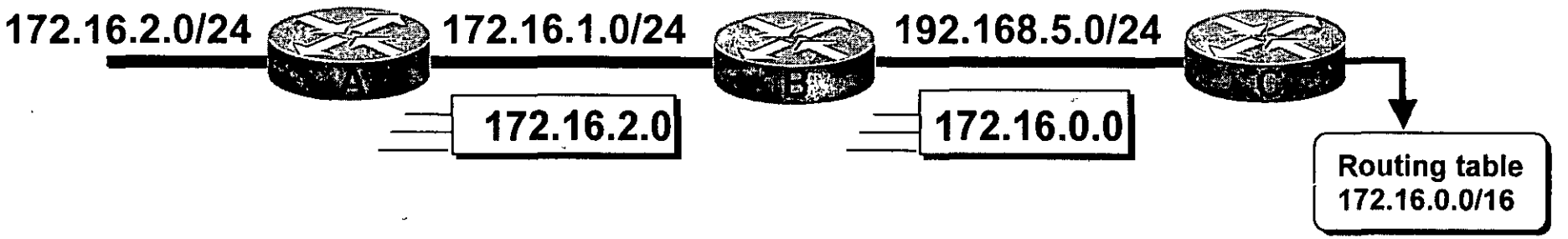
Classfull and Classless Updates

RIPv1 network

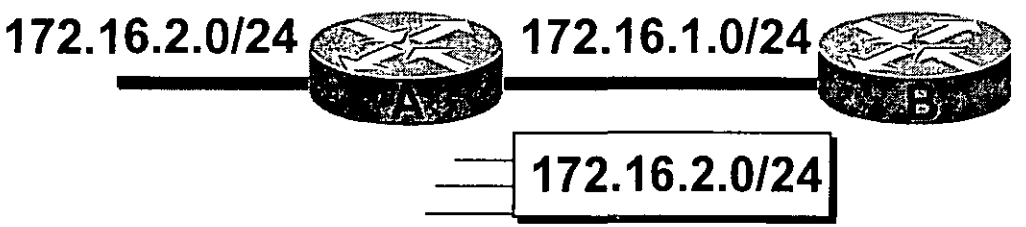


Classfull and Classless Updates

RIPv1 network

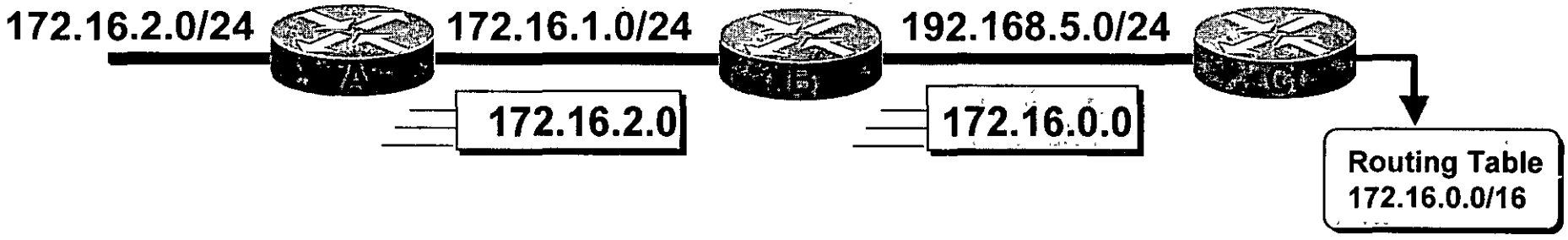


OSPF network

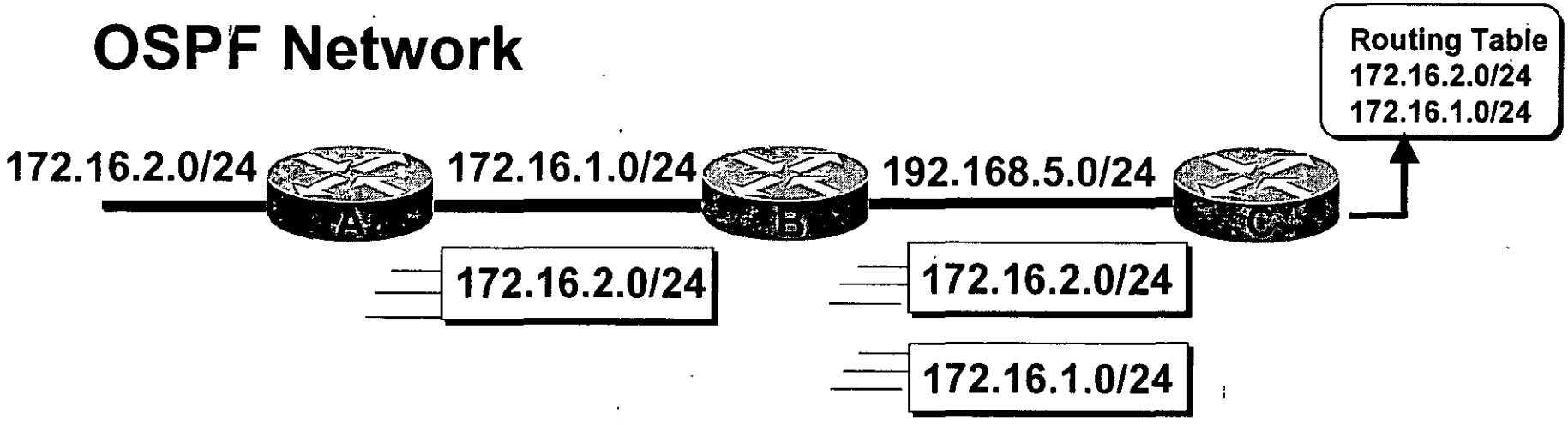


Classfull and Classless Routing Updates

RIPv1 Network



OSPF Network



Routing Tables

- Entries are listed in an efficient search order
  - Simplifies the search mechanism
- Multiple paths to a common destination can be listed
  - Load balancing is enabled by default for IP
- Displayed by the show ip route command
- Entries can be refreshed by the clear ip route command
  - Specify a single entry, use network number
  - Specify all entries, use * as a wildcard character

Poner ej de tabla de enrutamiento

Routing Protocol Comparison Chart

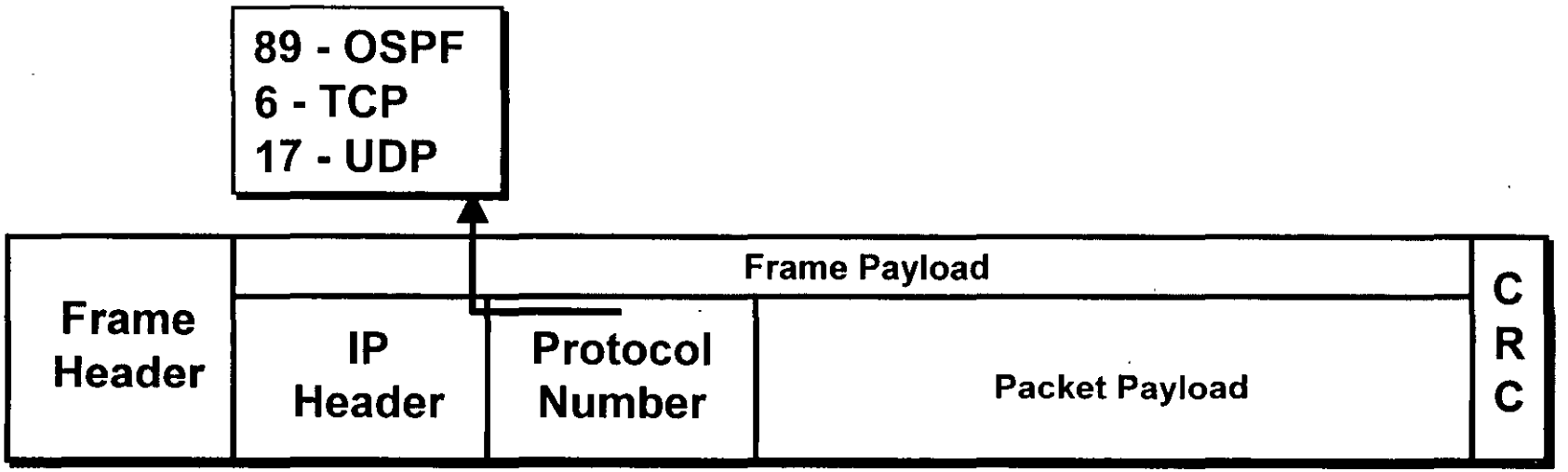
Characteristic	RIPv1	RIPv2	IGRP	EIGRP**	OSPF
Distance vector	X	X	X	X	
Link-state					X
Classful (auto route summ.)	X	X	X	X	
Classless (VLSM support)		X		X	X
Proprietary			X	X	
Scalability	Small	Small	Med.	Large	Large
Convergence time	Slow	Slow	Slow	Fast	Fast

** EIGRP is an advanced distance vector protocol

What Is OSPF?

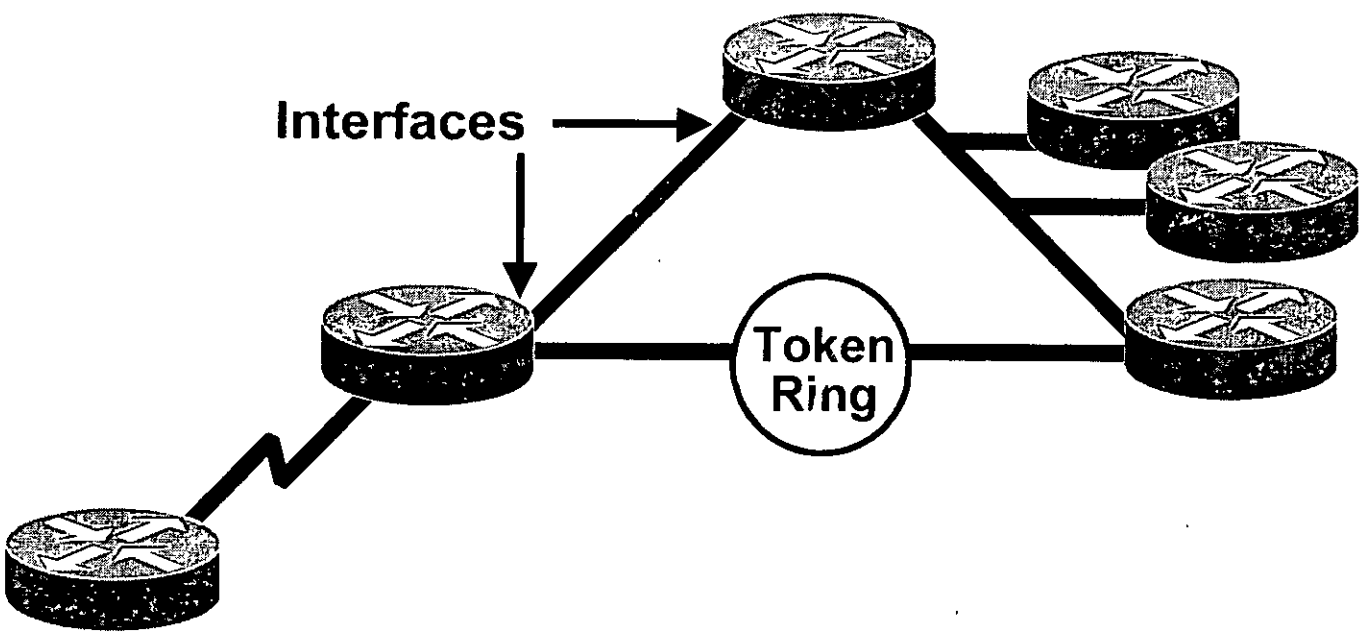
- Has fast convergence
- Supports VLSM
- Processes updates efficiently
- Selects paths based on bandwidth
- Supports equal-cost multipath

OSPF in IP Packets

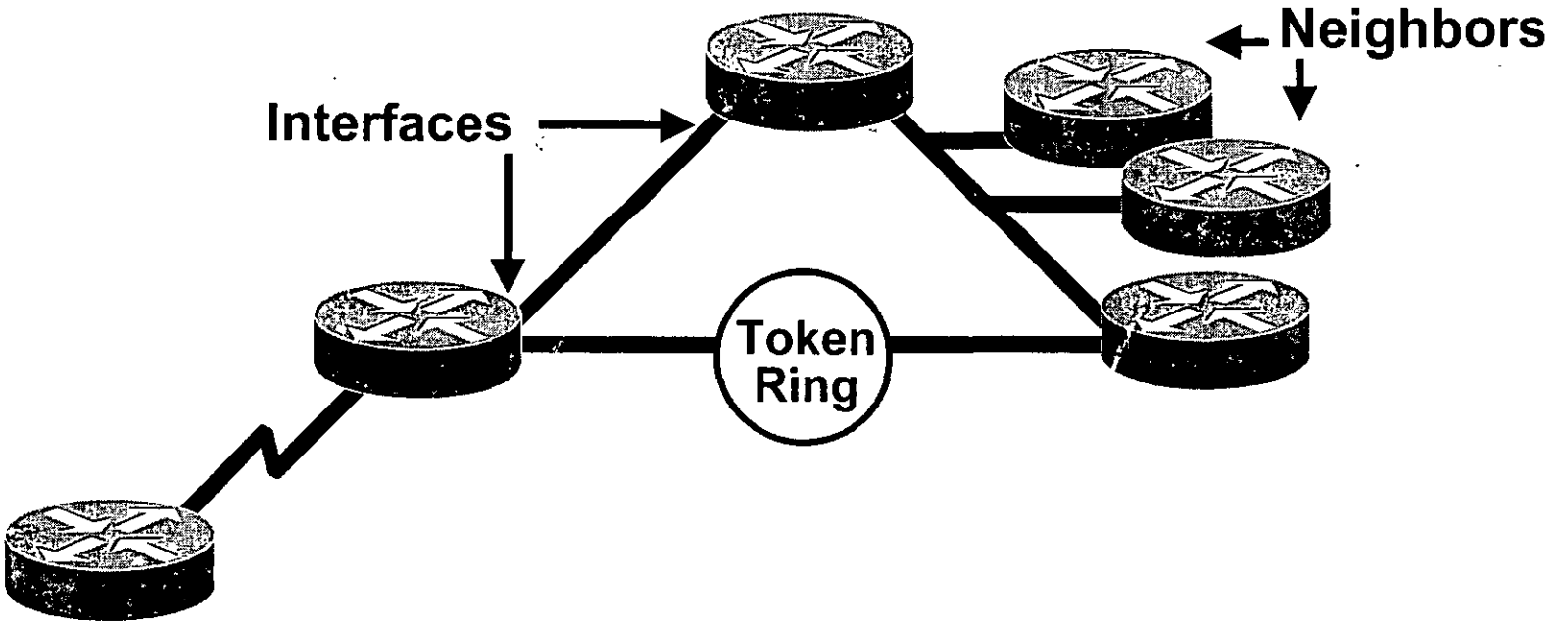


- OSPF is a link-state routing protocol
  - Relies on IP packets for delivery of routing information
  - Uses protocol number 89

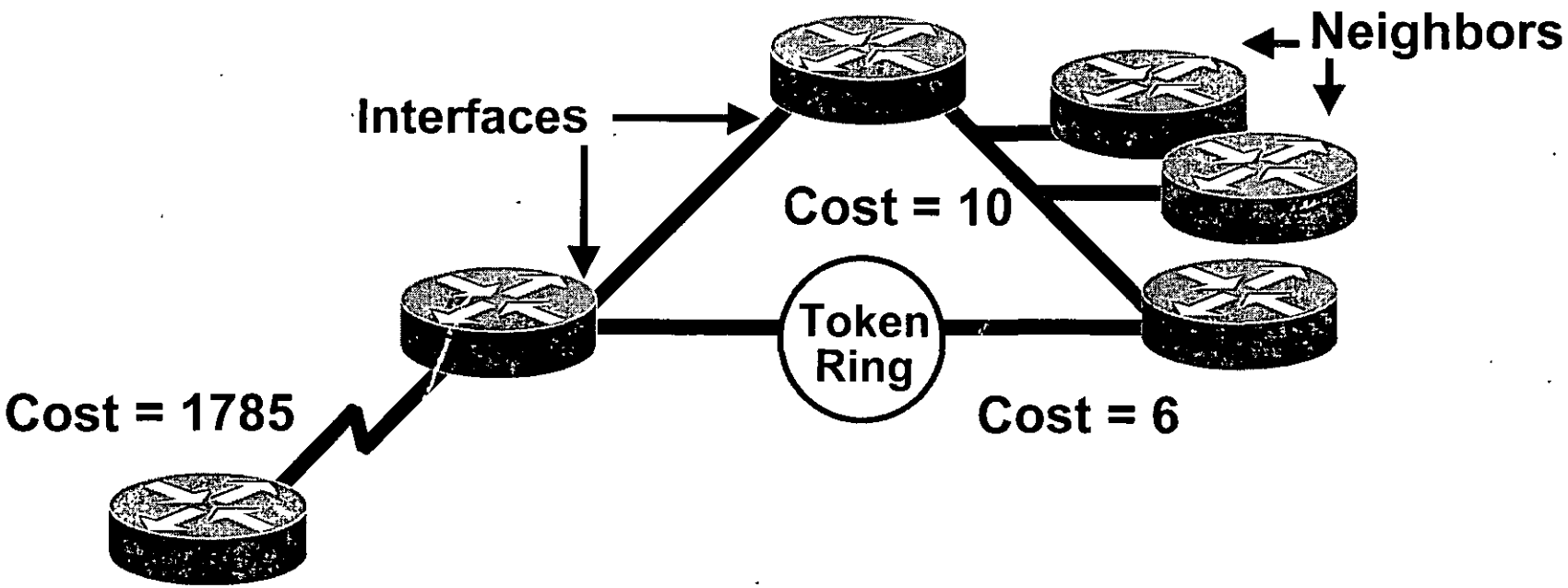
OSPF Terminology



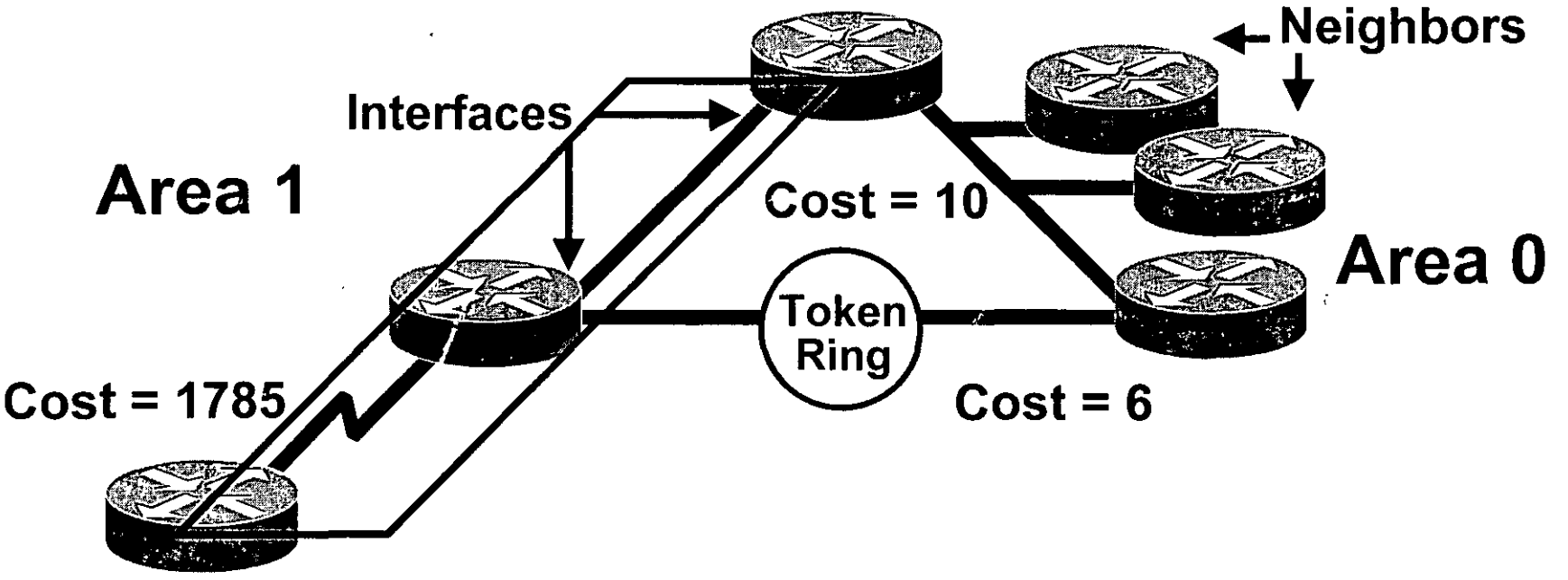
OSPF Terminology



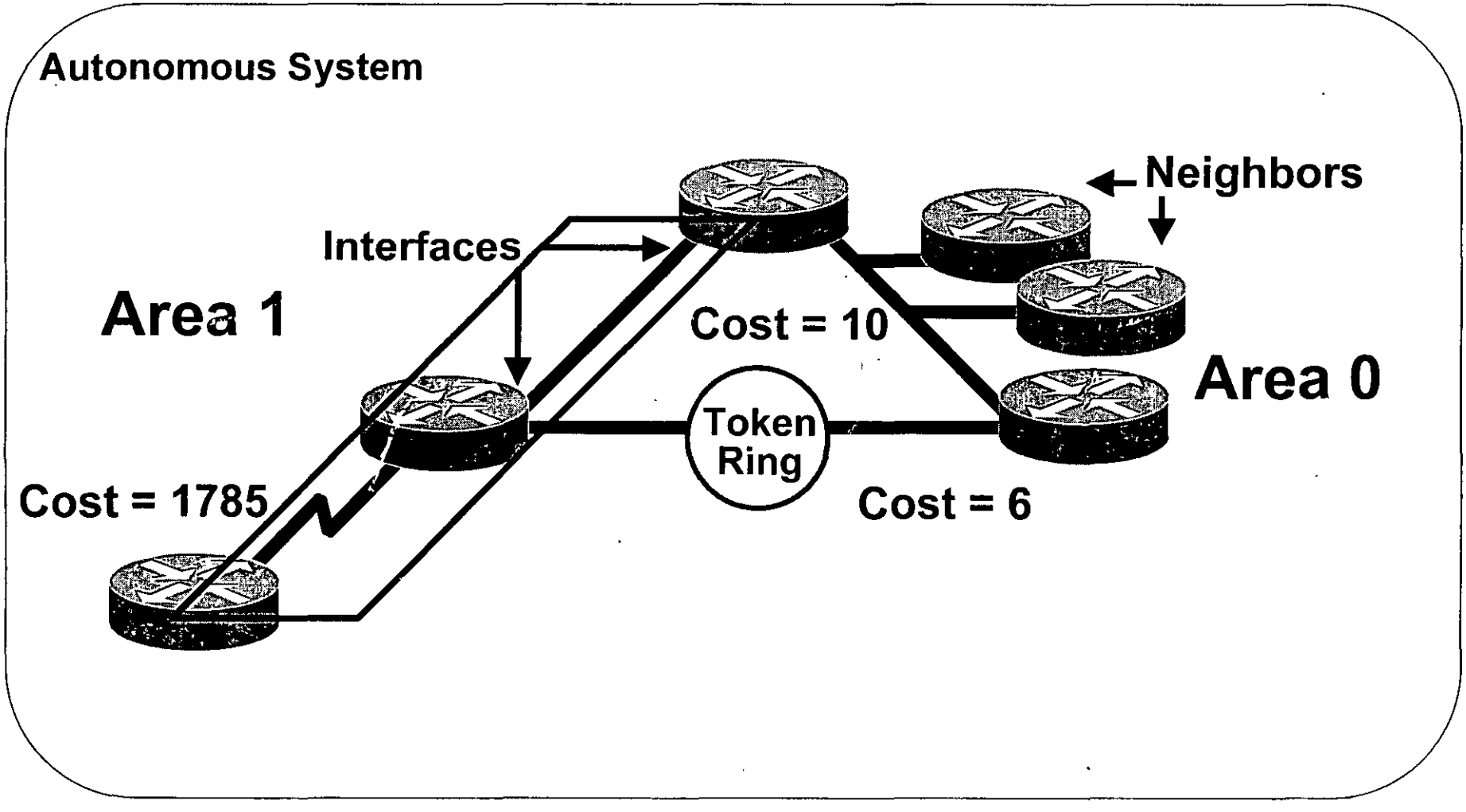
OSPF Terminology



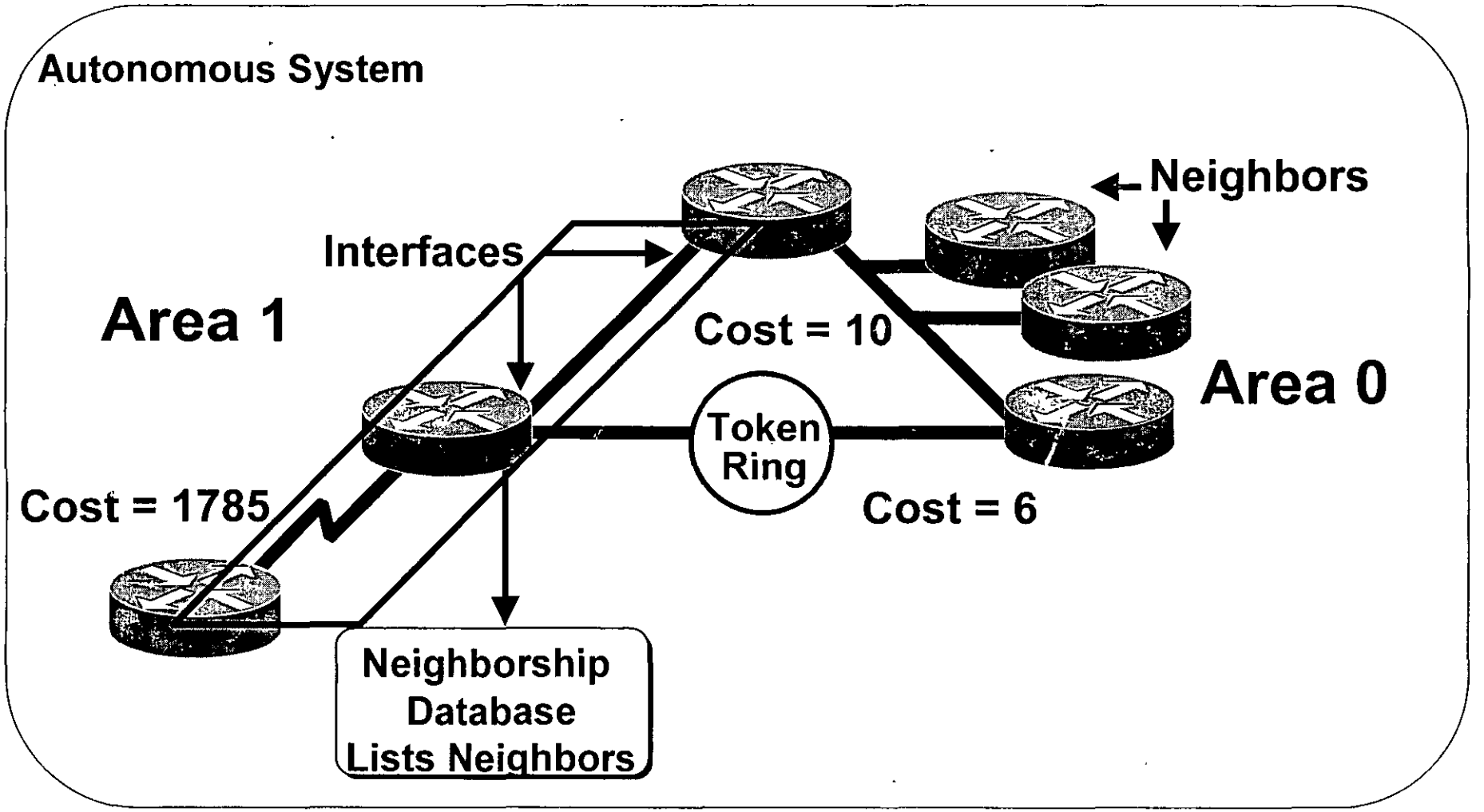
OSPF Terminology



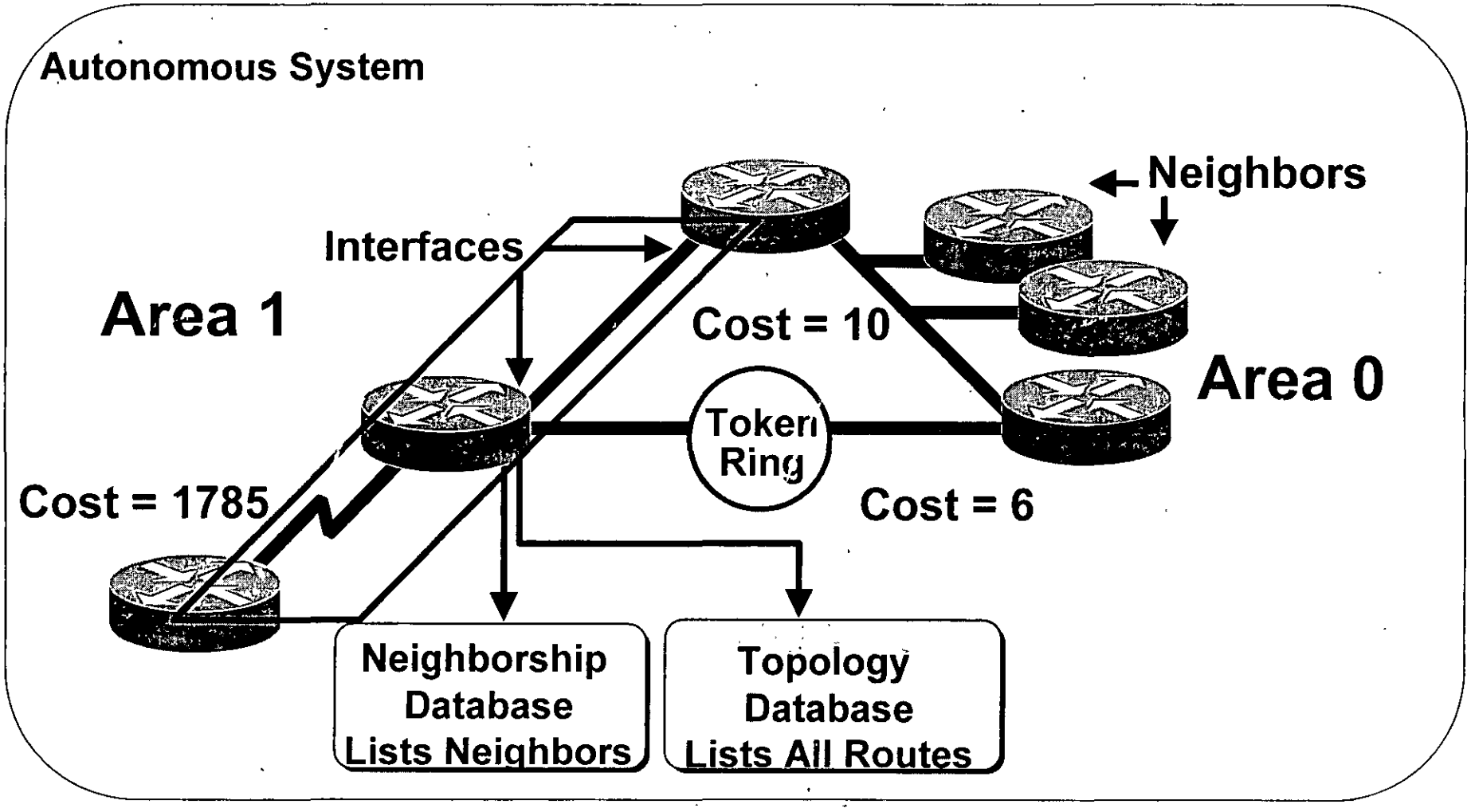
OSPF Terminology



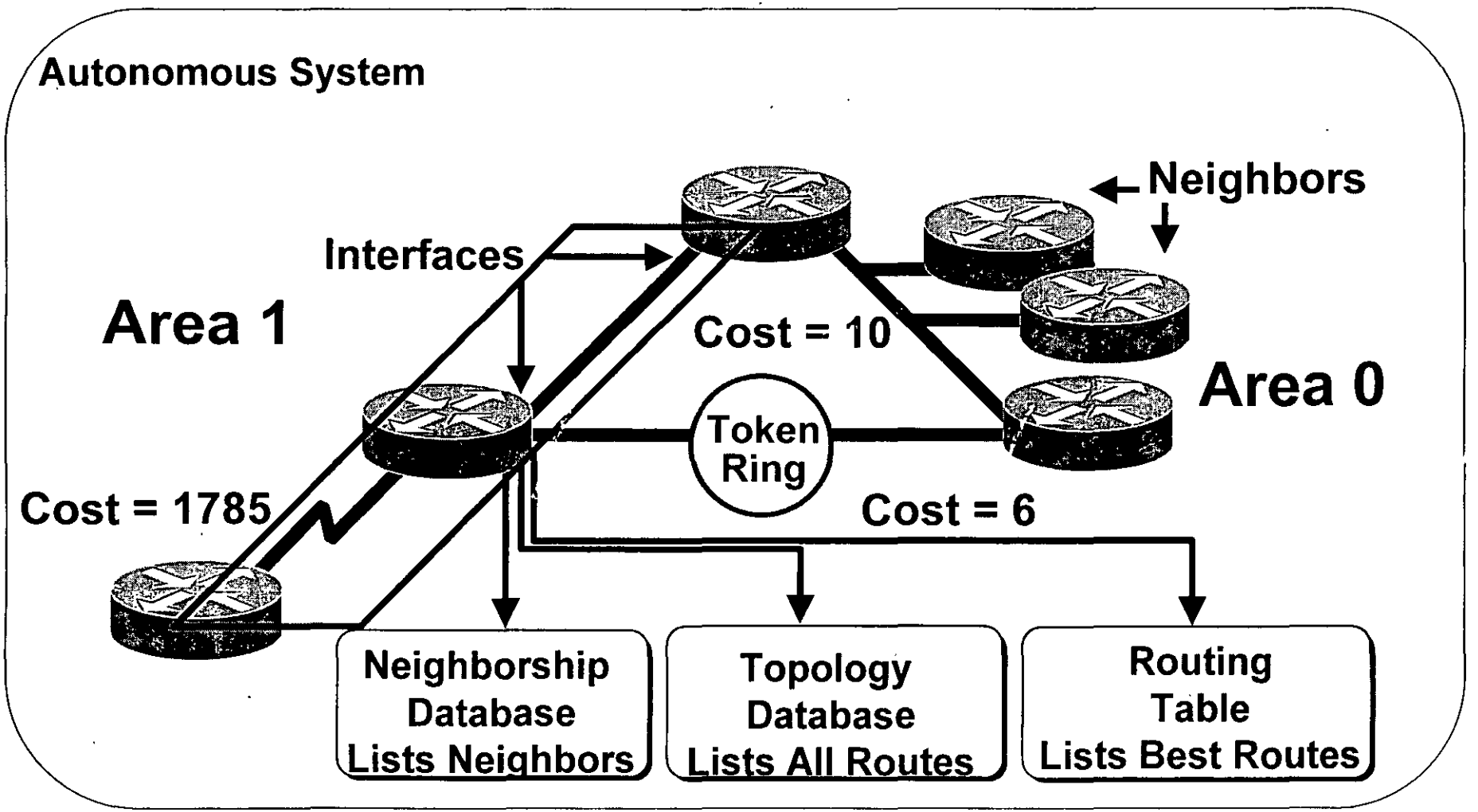
OSPF Terminology



OSPF Terminology

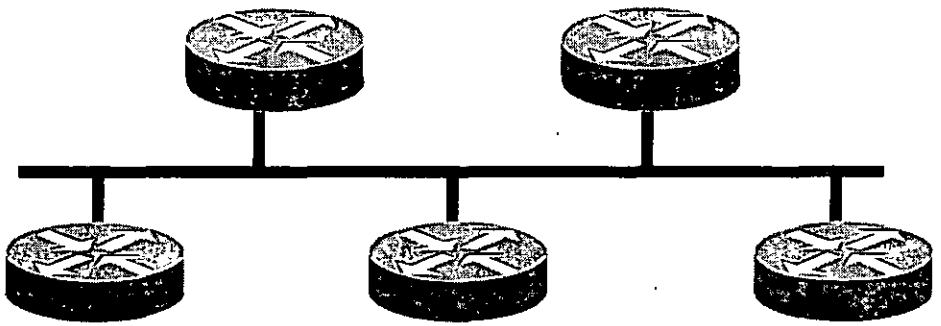


OSPF Terminology



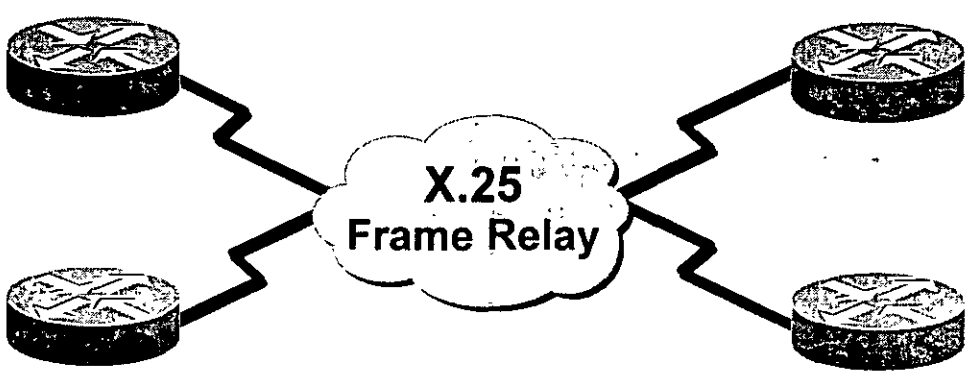
OSPF Topologies

Broadcast Multiaccess

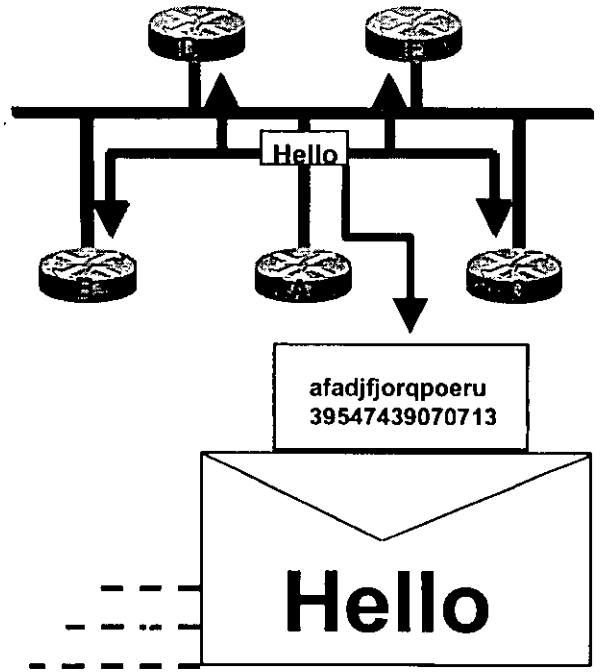


Point-to-Point

NBMA



OSPF Operation in a Broadcast Multiaccess Topology

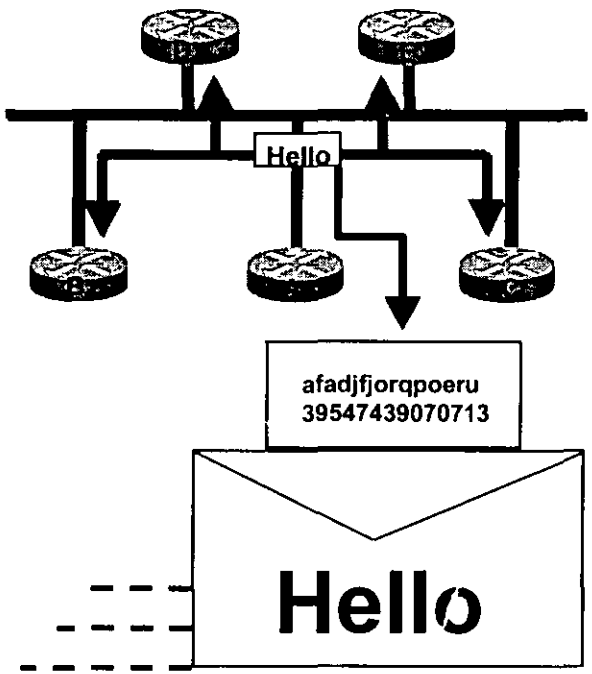


Neighborship

- Router ID
- Hello/dead intervals *
- Neighbors
- Area-ID *
- Router priority
- DR IP address
- BDR IP address
- Authentication password*
- Stub area flag *

* Entry must match on neighboring routers

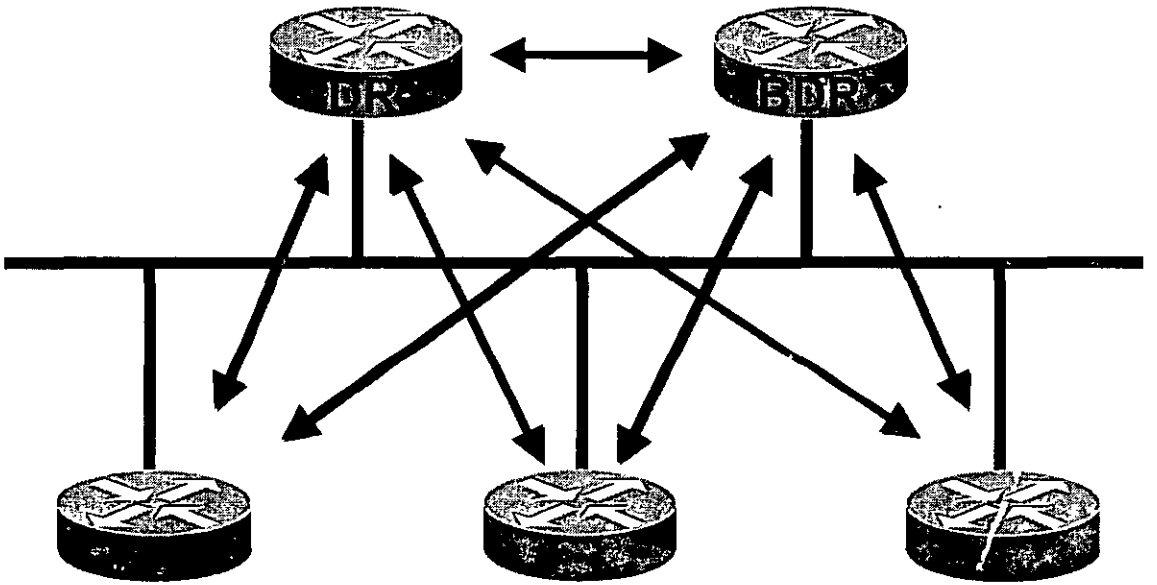
Neighborship (cont.)



- Router ID
- Hello/dead intervals *
- Neighbors
- Area-ID *
- Router priority
- DR IP address
- BDR IP address
- Authentication password*
- Stub area flag *

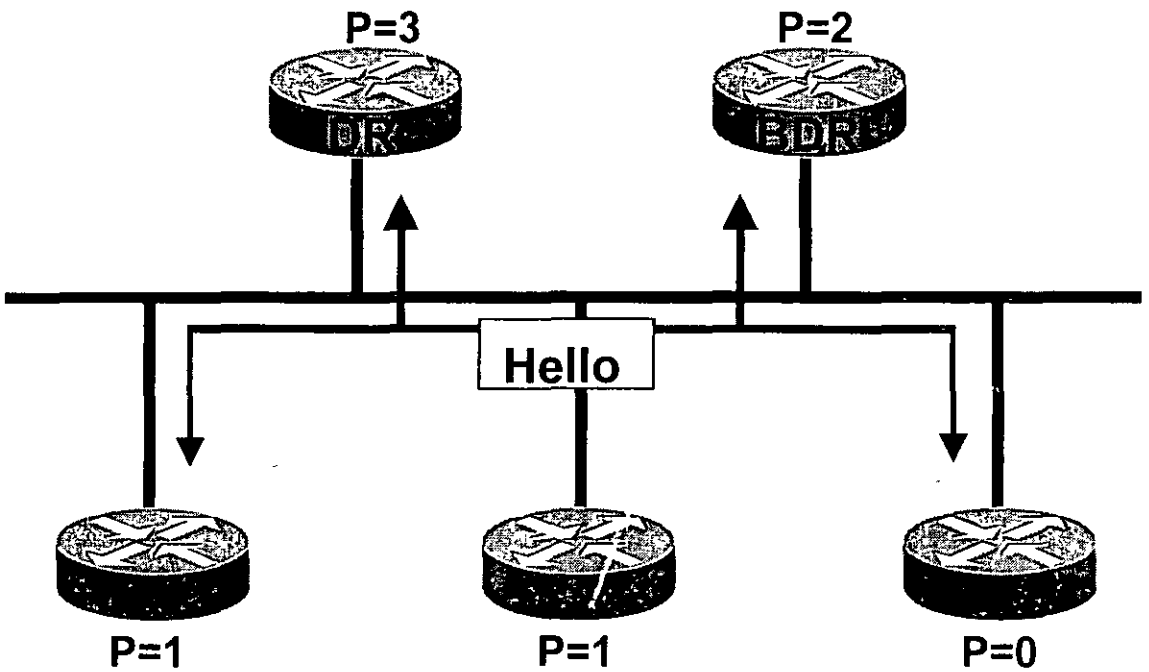
* Entry must match on neighboring routers

DR and BDR



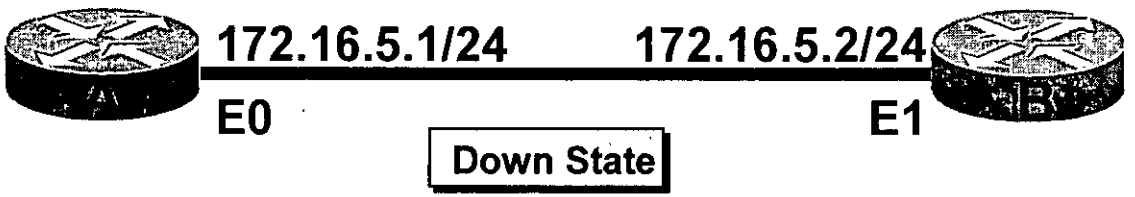
- Hellos elect DR and BDR to represent segment
- Each router then forms adjacency with DR and BDR

Electing the DR and BDR

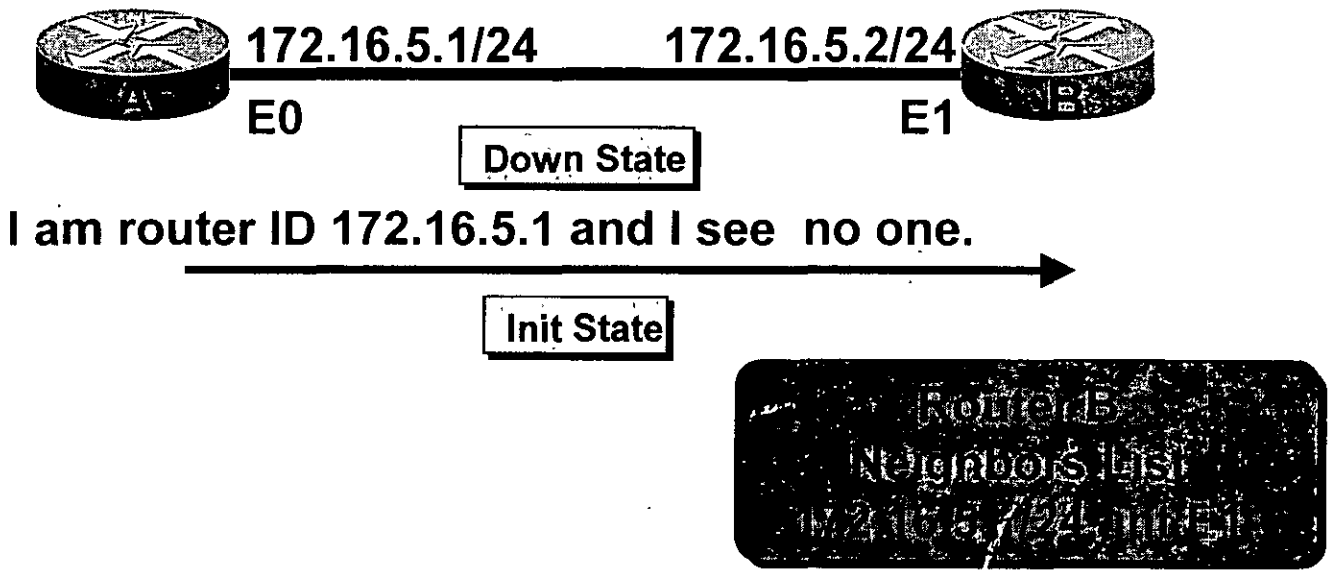


- Hello packets exchanged via IP multicast
- Router with highest OSPF priority elected

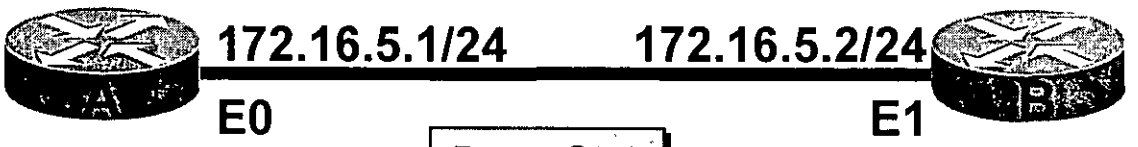
Exchange Process



Exchange Process



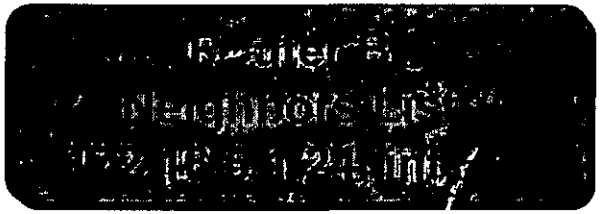
Exchange Process



Down State

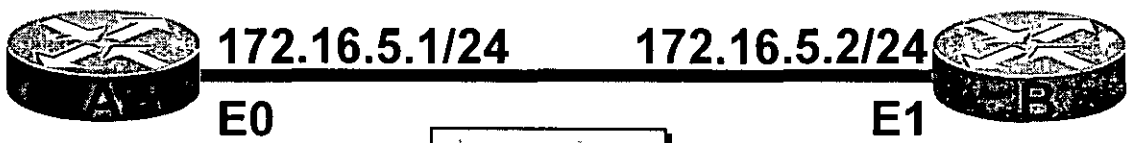
I am router ID 172.16.5.1 and I see no one.

Init State



I am router ID 172.16.5.2, and I see 172.16.5.1.

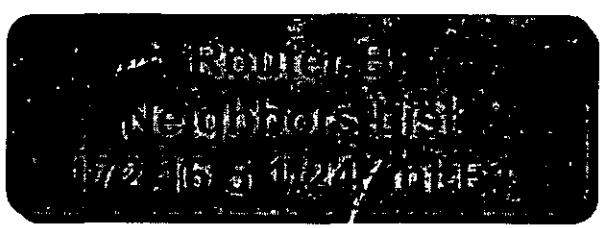
Exchange Process



Down State

I am router ID 172.16.5.1 and I see no one.

Init State

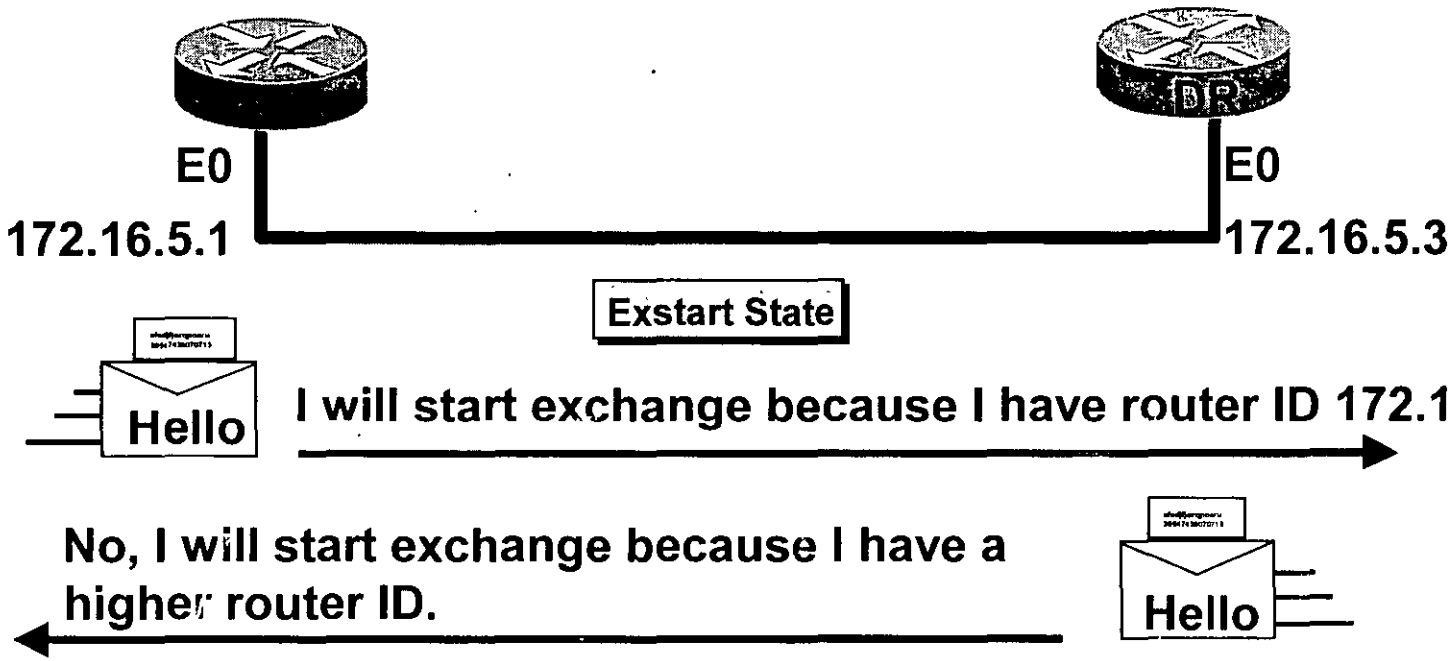


I am router ID 172.16.5.2, and I see 172.16.5.1.

Router A
Neighbors List
172.16.5.2/24, int E0

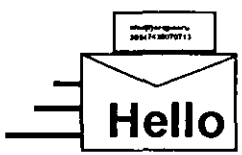
Two-Way State

Discovering Routes



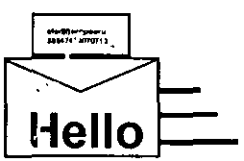
Discovering Routes

Exstart State

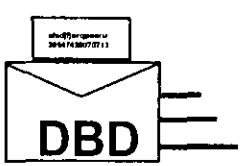


I will start exchange because I have router ID 172.16.5.1.

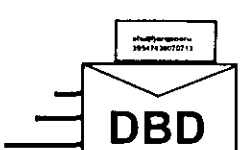
No, I will start exchange because I have a higher router ID.



Exchange State

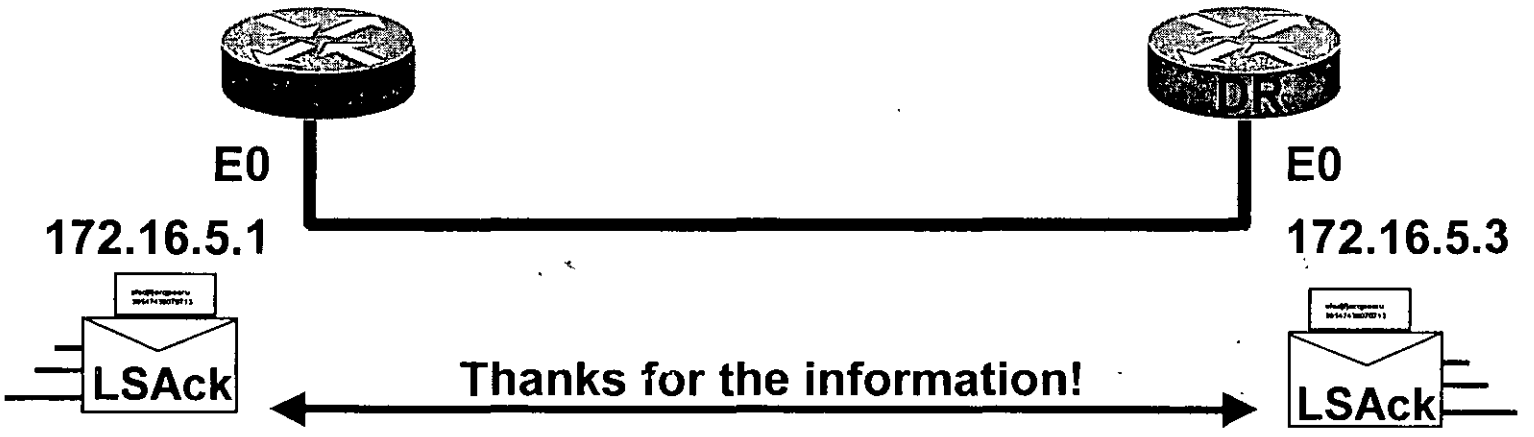


Here is a summary of my link-state database.

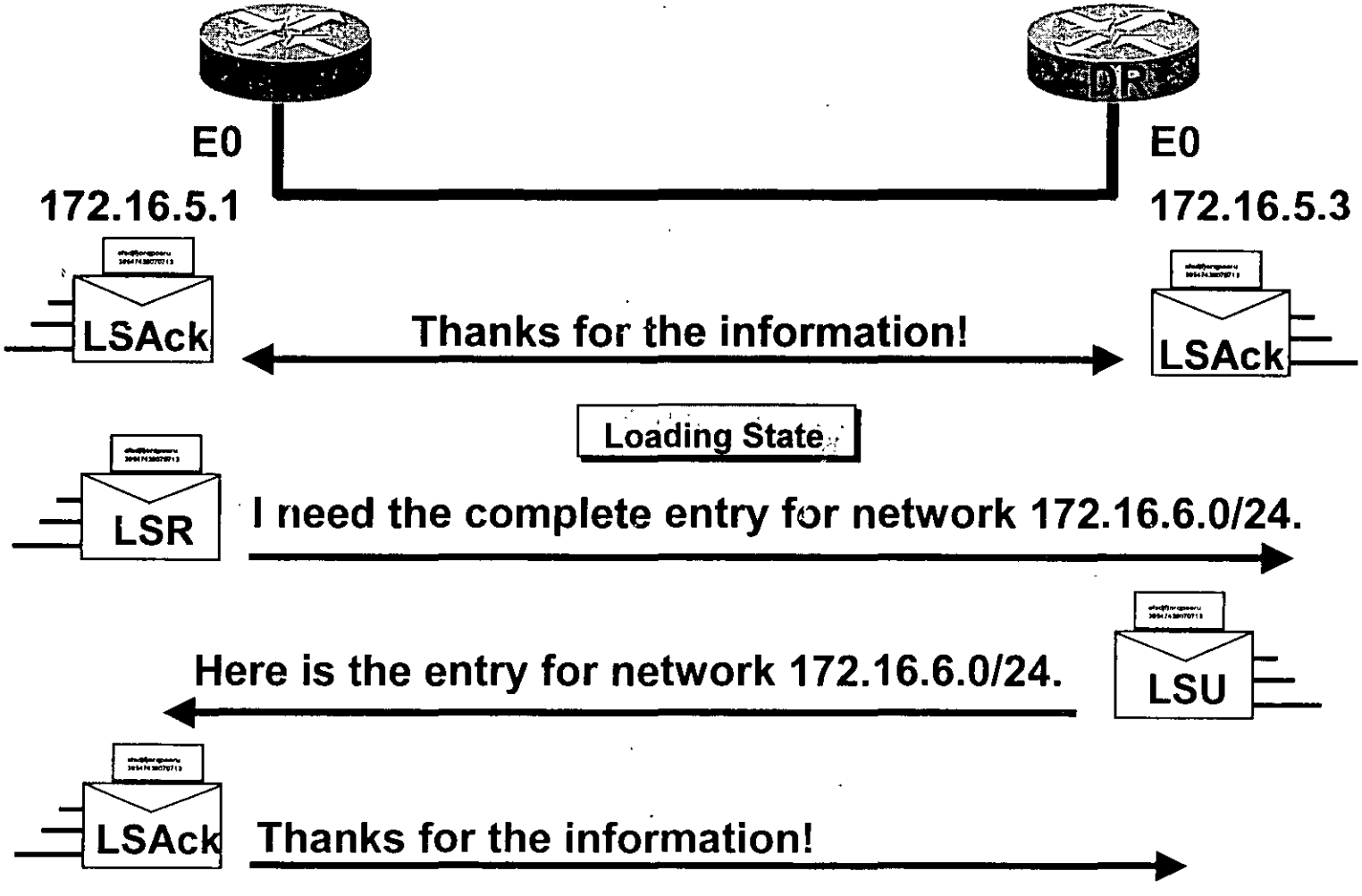


Here is a summary of my link-state database.

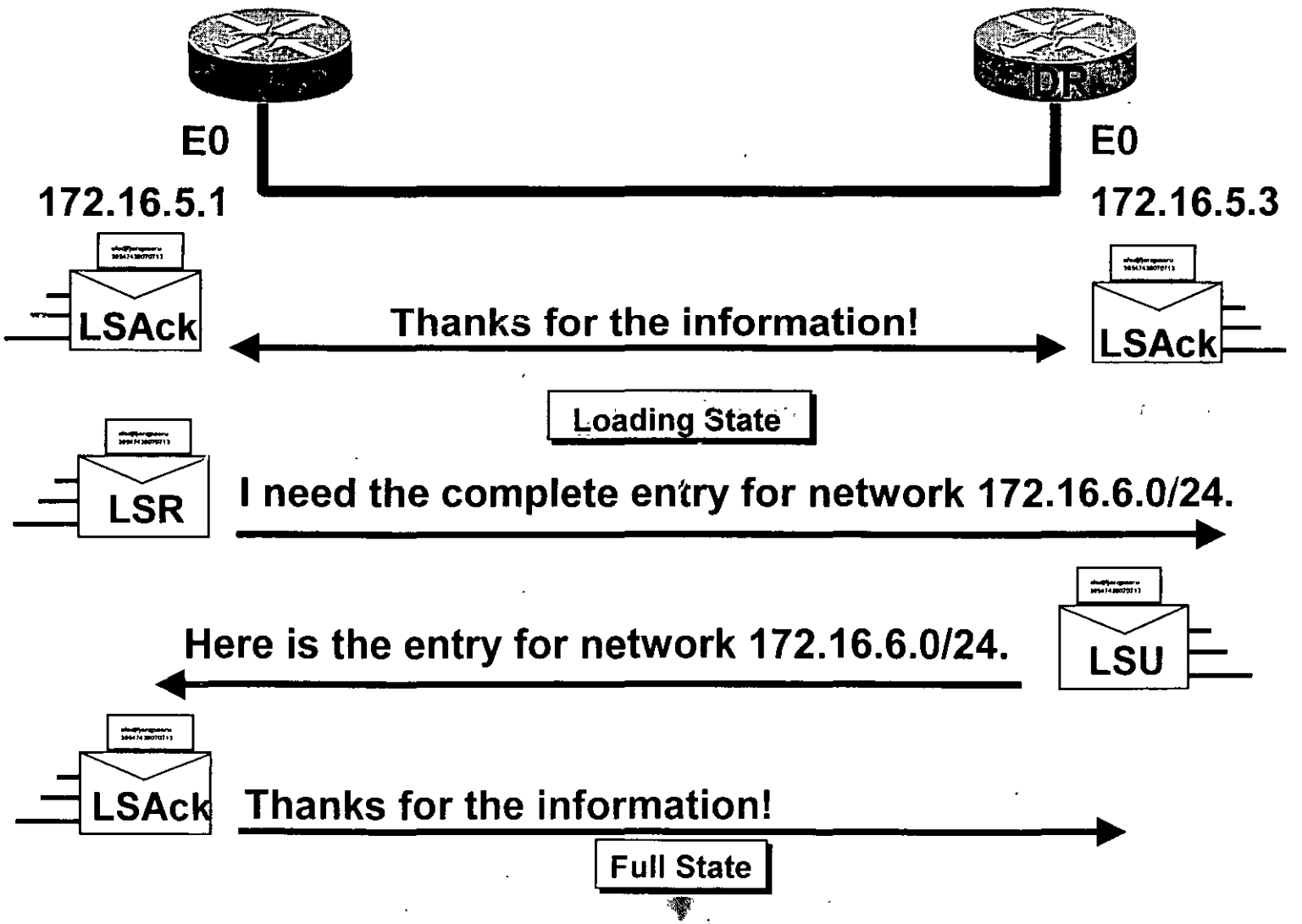
Discovering Routes (cont.)



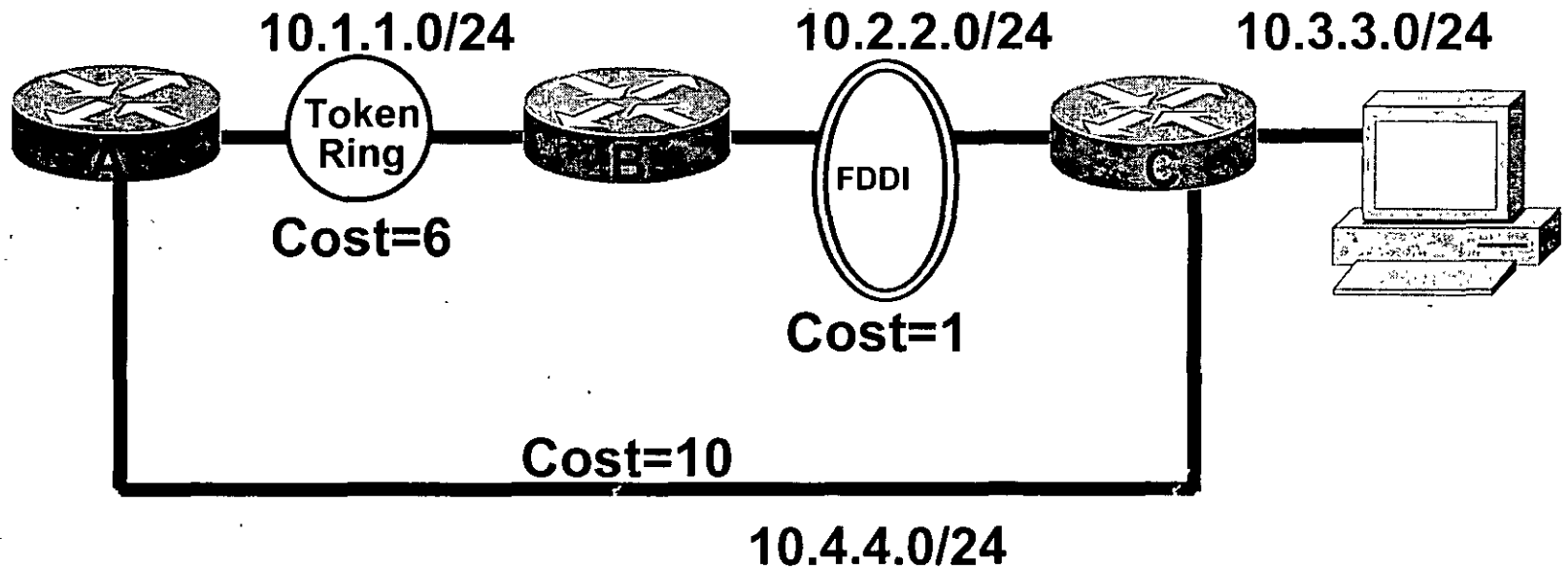
Discovering Routes (cont.)



Discovering Routes (cont.)



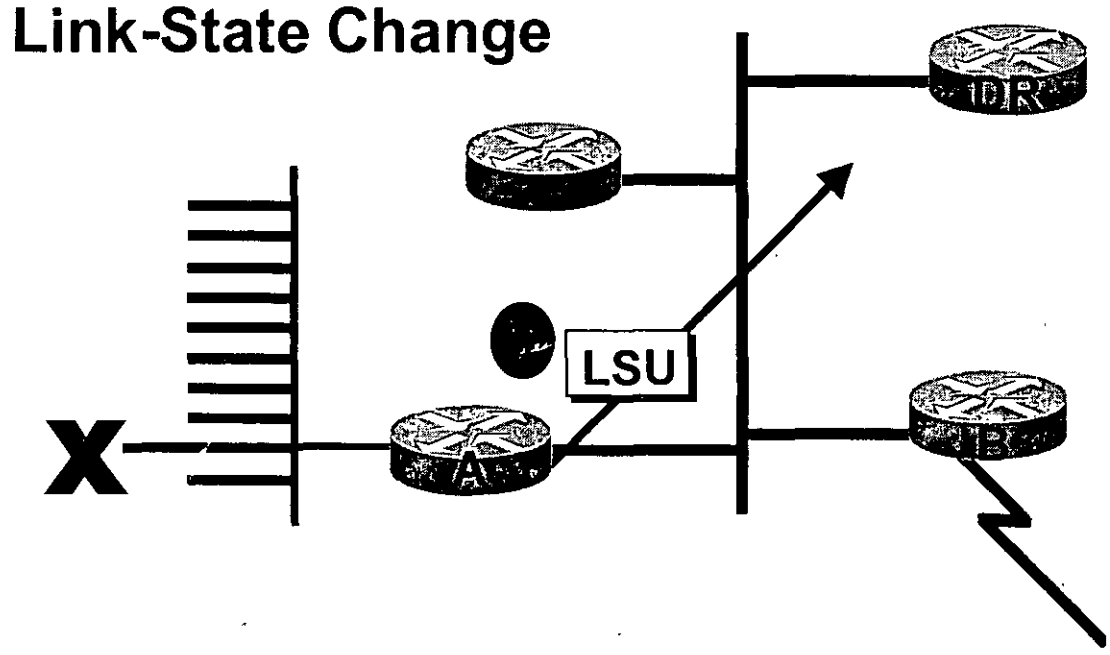
Choosing Routes



Topology Table		
Net	Cost	Out Interface
10.2.2.0	6	To0
10.3.3.0	10	E0

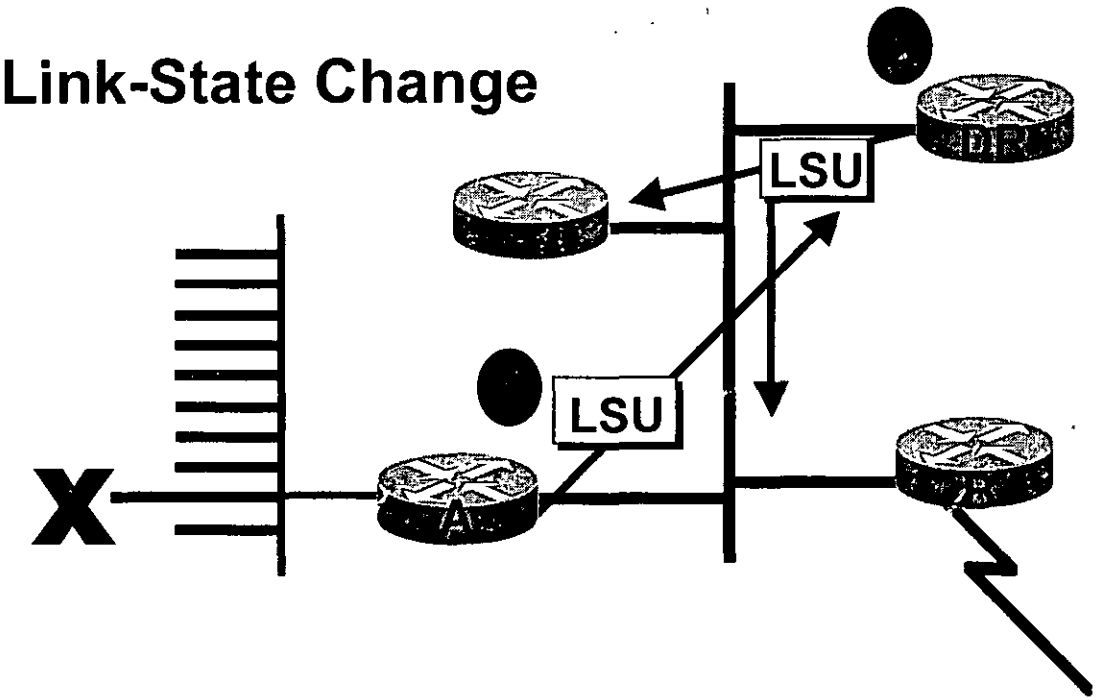
This is the best route to 10.3.3.0.

Maintaining Routing Information



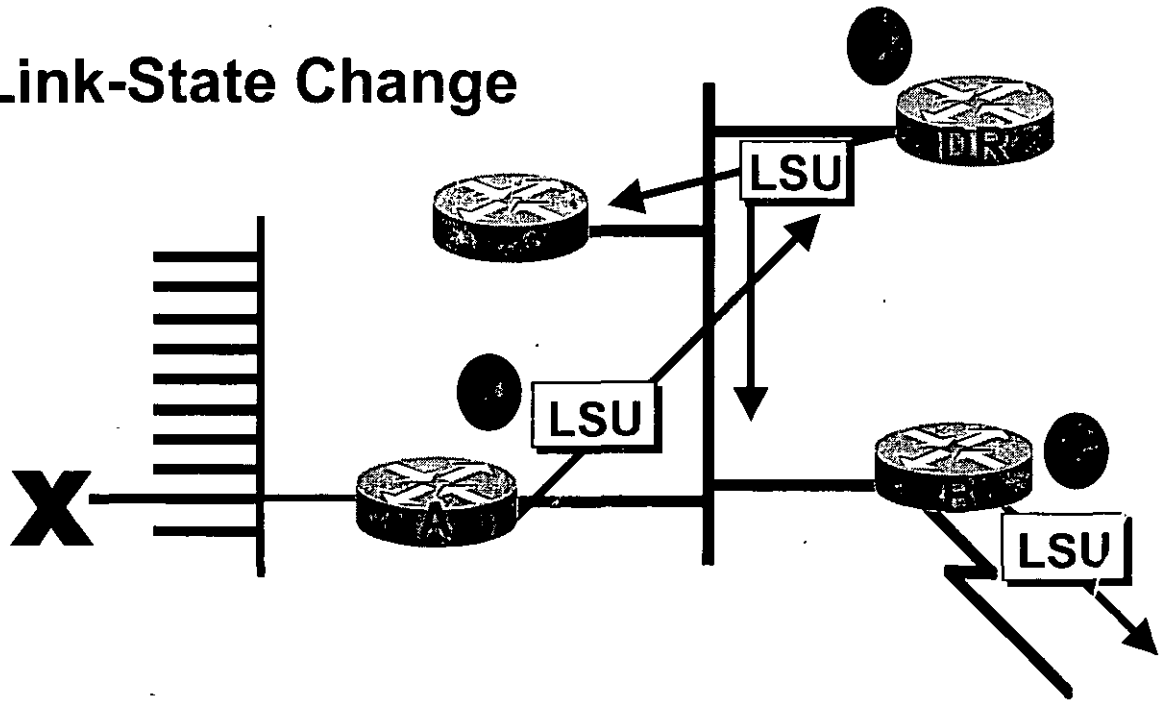
- Router A tells all OSPF DRs on 224.0.0.6

Maintaining Routing Information



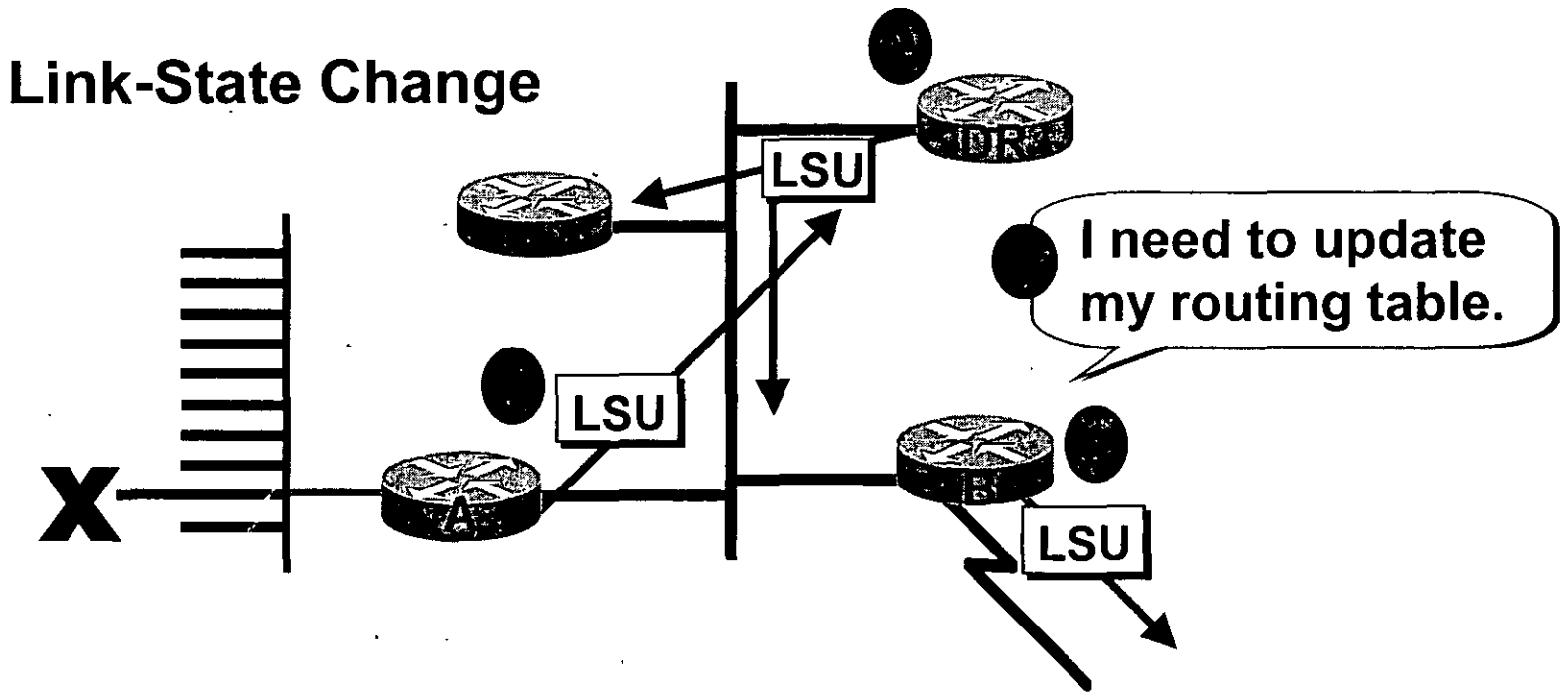
- Router A tells all OSPF DRs on 224.0.0.6
- DR tells others on 224.0.0.5

Maintaining Routing Information



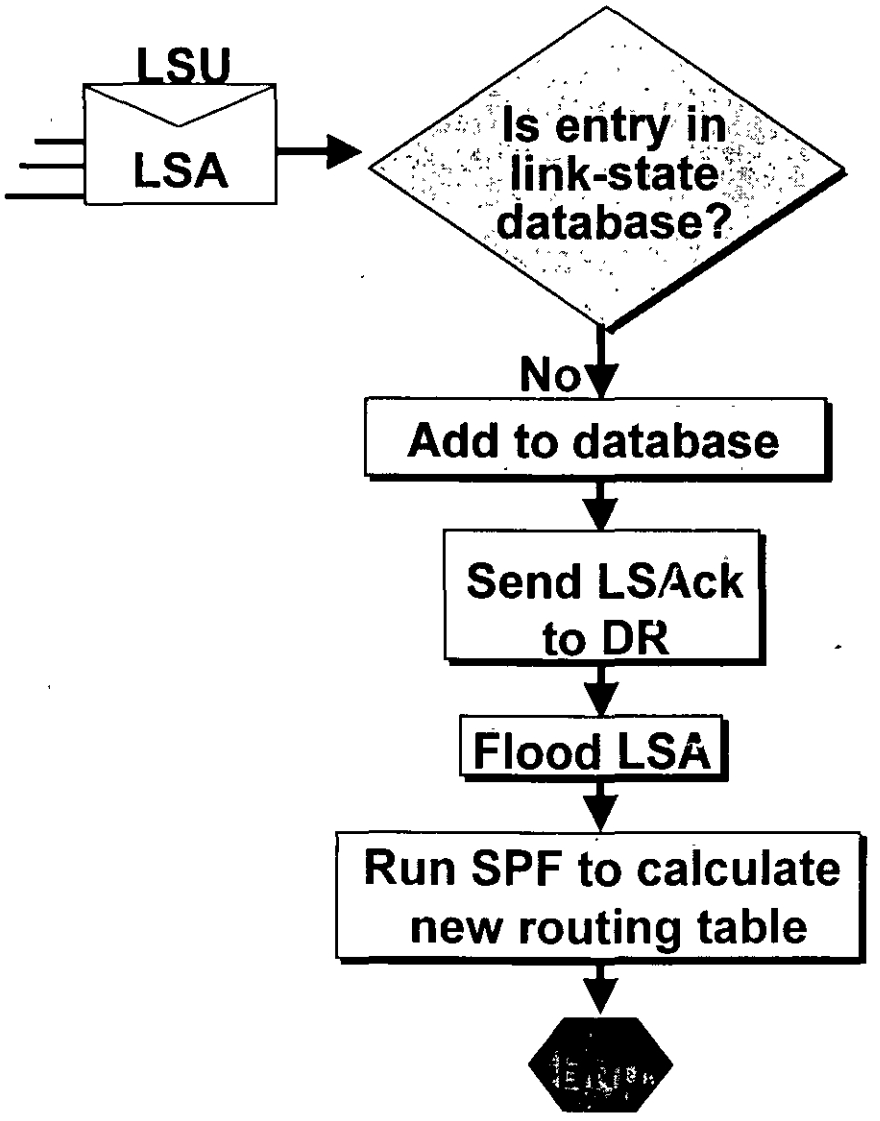
- Router A tells all OSPF DRs on 224.0.0.6
- DR tells others on 224.0.0.5

Maintaining Routing Information

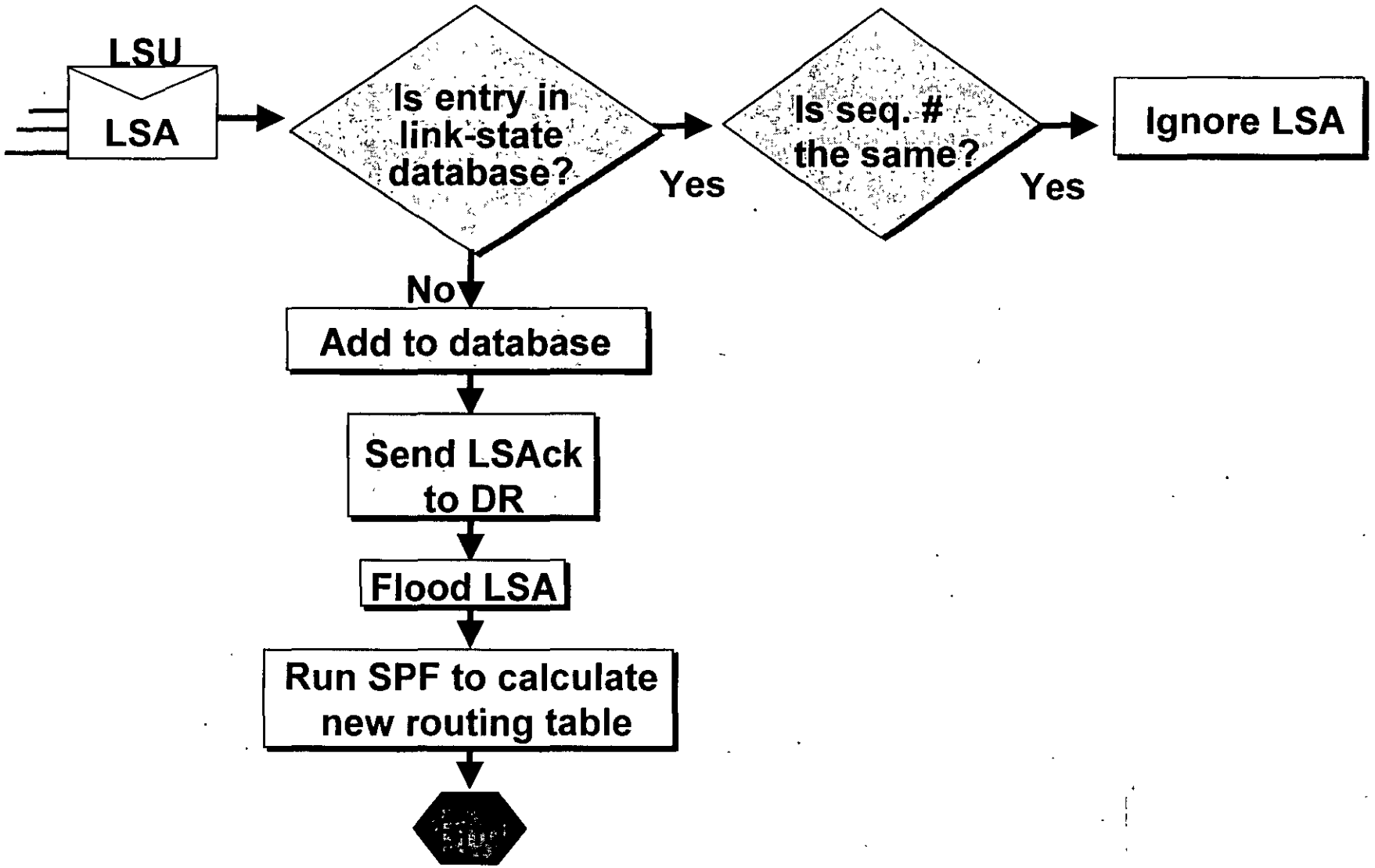


- Router A tells all OSPF DRs on 224.0.0.6
- DR tells others on 224.0.0.5

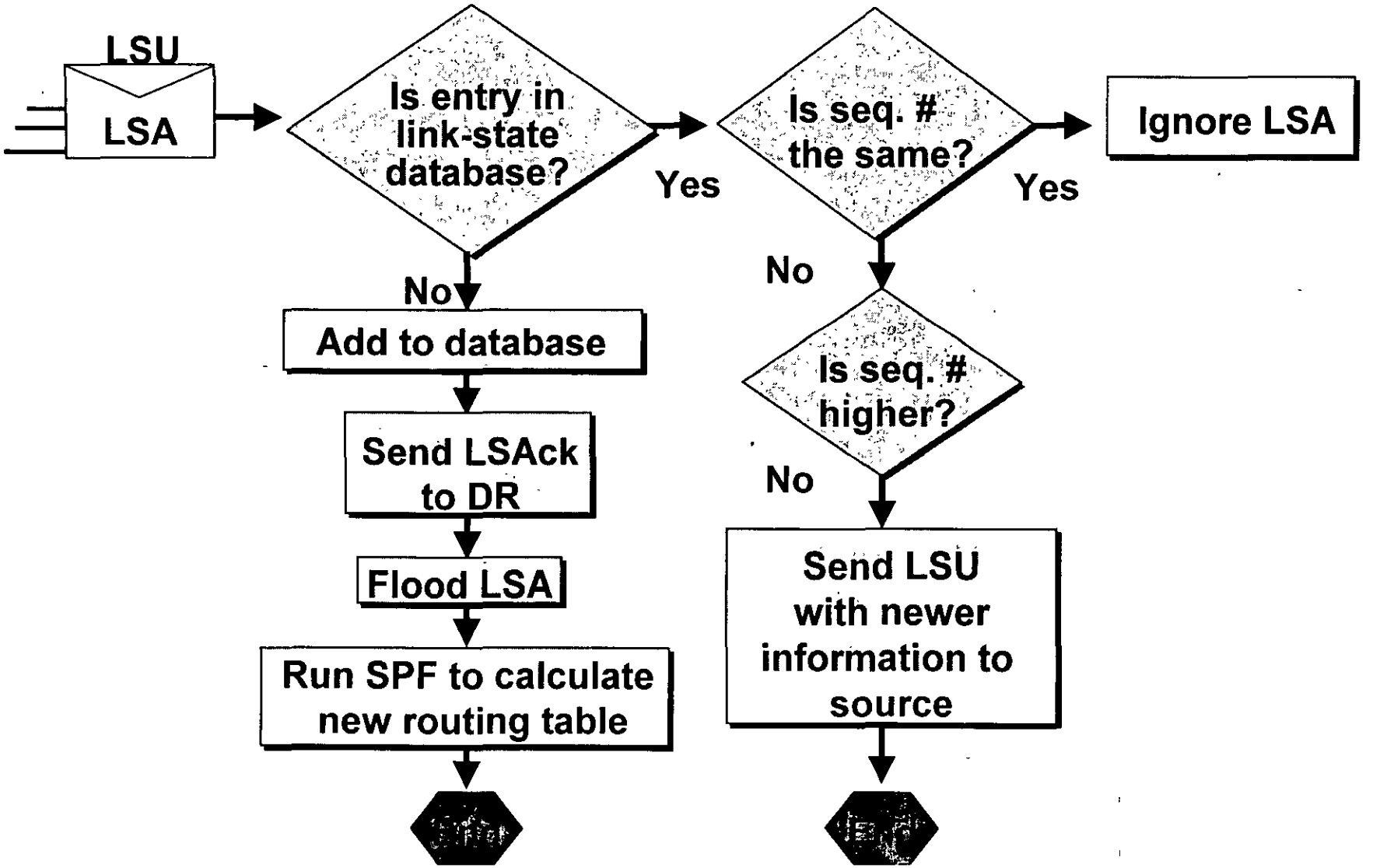
Maintaining Routing Information (cont.)



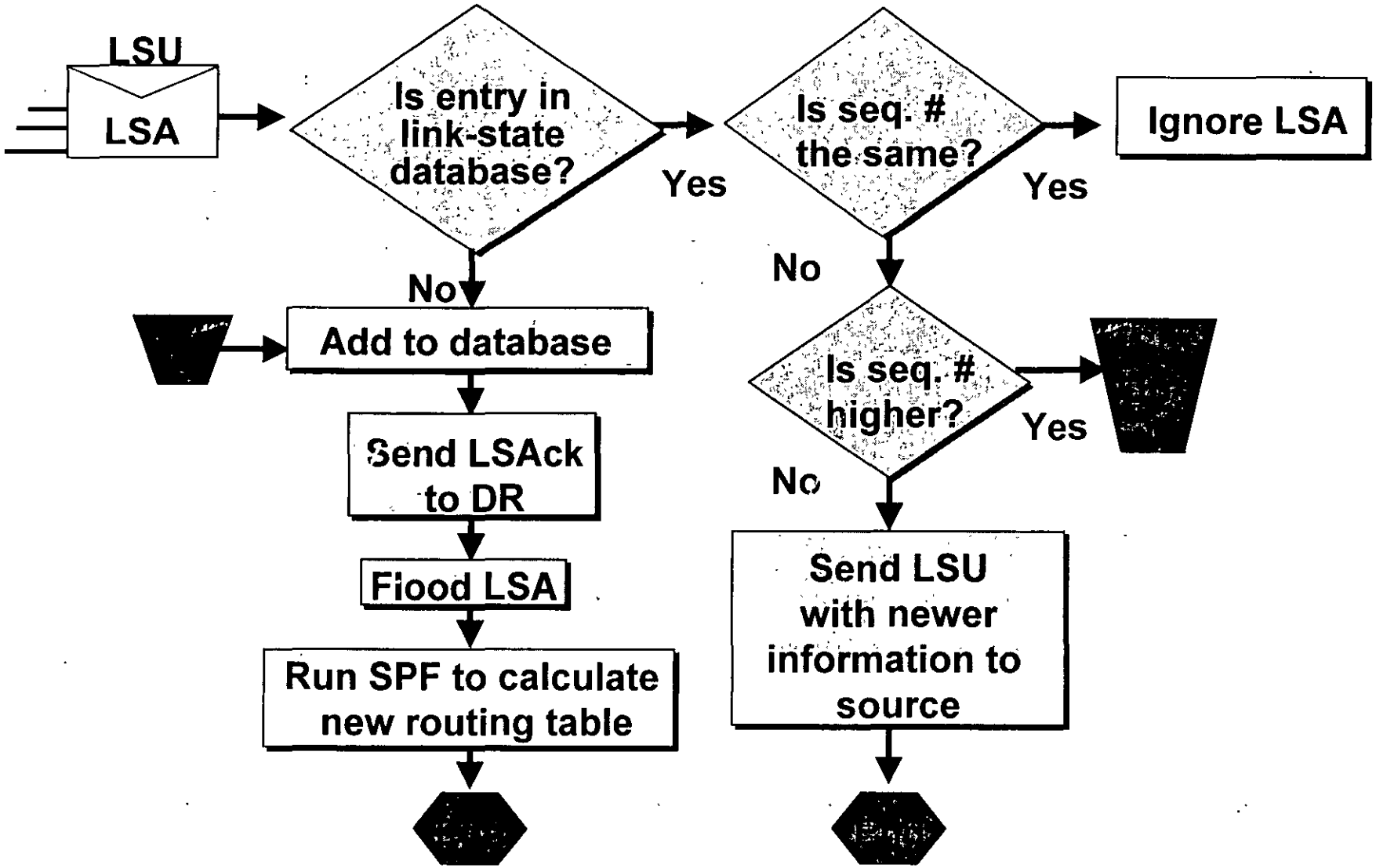
Maintaining Routing Information (cont.)



Maintaining Routing Information (cont.)



Maintaining Routing Information (cont.)

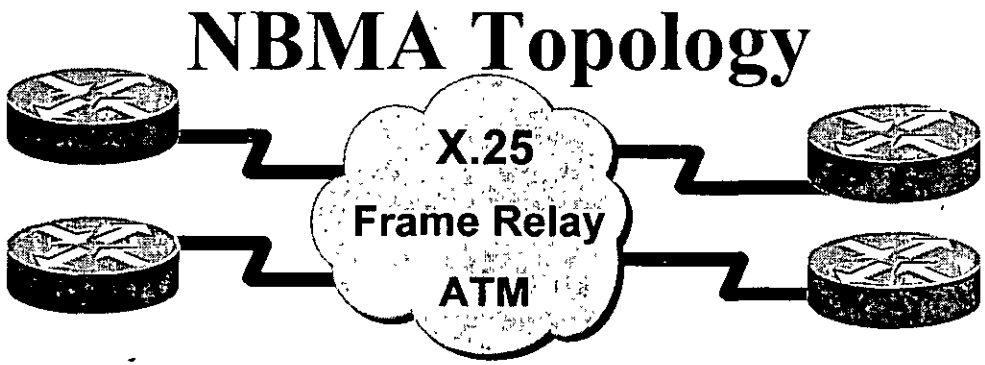


OSPF Operation in a Point-to-Point Topology

Point-to-Point Neighborship

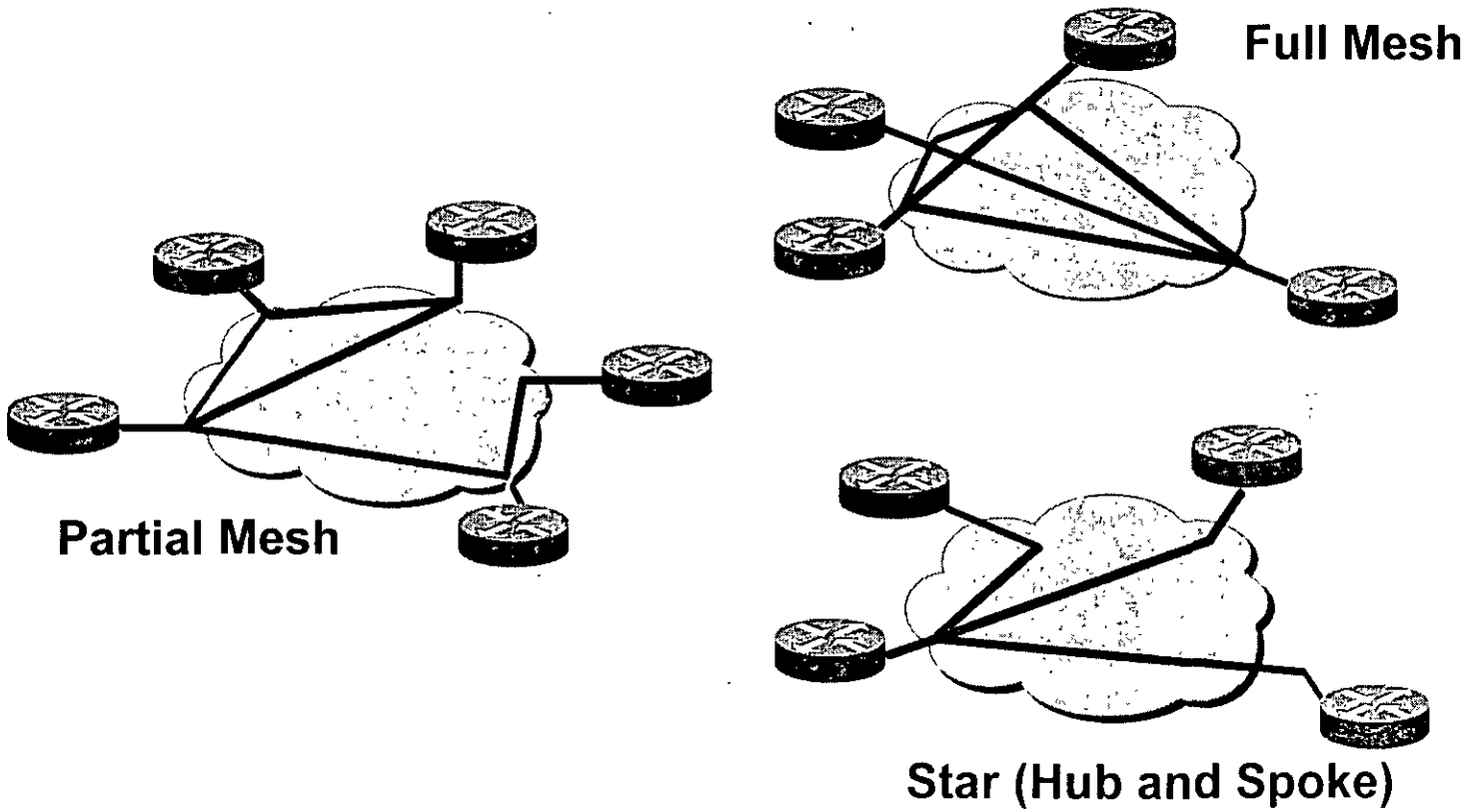
- Router dynamically detects its neighboring router using the Hello protocol
- No election: Adjacency is automatic as soon as the two routers can communicate
- OSPF packets are always sent as multicast 224.0.0.5

OSPF Operation in an NBMA Topology



- Single interface interconnects multiple sites
- NBMA topologies support multiple routers but without broadcasting capabilities

Frame Relay Topologies



DR Selection in NBMA Topology

- OSPF considers NBMA to be like other broadcast media
- DR and BDR need to have full physical connectivity with all other routers
- DR and BDR need a list of neighbors

NBMA Mode Neighborship

- Usually a fully-meshed network
- DR/BDR elected
- Neighbors must be statically configured
- One IP subnet
- Stability of the network may be an issue
- Replicate LSA packets
- RFC 2328 compliant

Point-to-Multipoint Mode Neighborship

- Fully-meshed or partially-meshed topology
- No DR/BDR election
- Neighbors do not need to be statically configured
- One IP subnet
- Replicate LSA packets
- RFC 2328 compliant

Adjacencies Creation

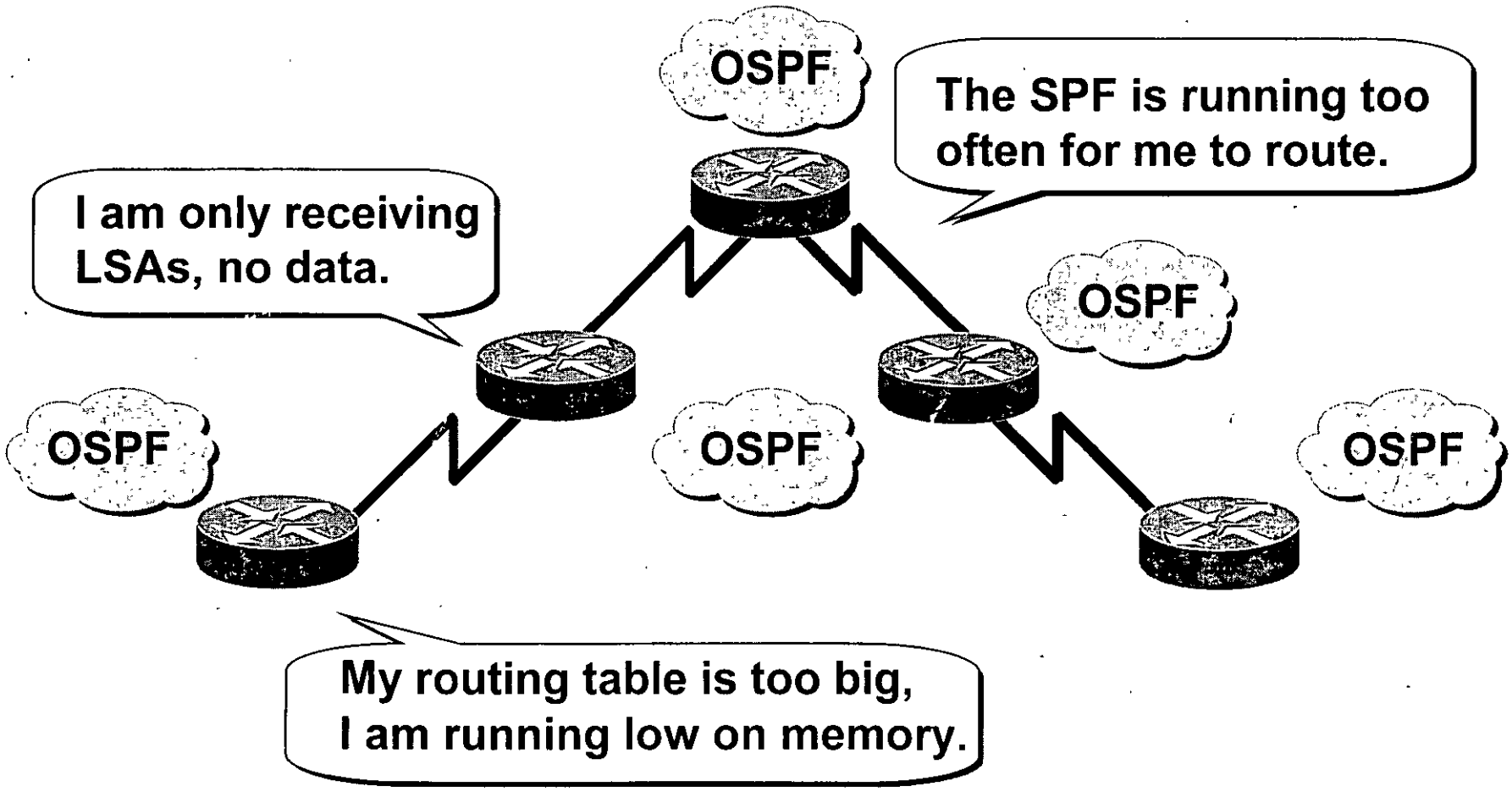
```
Point-to-point interfaces coming up:  No election
%LINK-3-UPDOWN: Interface Serial1, changed state to up
OSPF: Interface Serial1 going Up
OSPF: Rcv hello from 192.168.0.11 area 0 from Serial1 10.1.1.2
OSPF: End of hello processing
OSPF: Build router LSA for area 0, router ID 192.168.0.10
OSPF: Rcv DBD from 192.168.0.11 on Serial1 seq 0x20C4 opt 0x2 flag 0x7 len 32 state INIT
OSPF: 2 Way Communication to 192.168.0.11 on Serial1, state 2WAY
OSPF: Send DBD to 192.168.0.11 on Serial1 seq 0x167F opt 0x2 flag 0x7 len 32
OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: Send DBD to 192.168.0.11 on Serial1 seq 0x20C4 opt 0x2 flag 0x2 len 72
```

```
Ethernet interface coming up: Election
OSPF: 2 Way Communication to 192.168.0.10 on Ethernet0, state 2WAY
OSPF: end of Wait on interface Ethernet0
OSPF: DR/BDR election on Ethernet0
OSPF: Elect BDR 192.168.0.12
OSPF: Elect DR 192.168.0.12
    DR: 192.168.0.12 (Id)   BDR: 192.168.0.12 (Id)
OSPF: Send DBD to 192.168.0.12 on Ethernet0 seq 0x546 opt 0x2 flag 0x7 len 32
<...>
OSPF: DR/BDR election on Ethernet0
OSPF: Elect BDR 192.168.0.11
OSPF: Elect DR 192.168.0.12
    DR: 192.168.0.12 (Id)   BDR: 192.168.0.11 (Id)
```

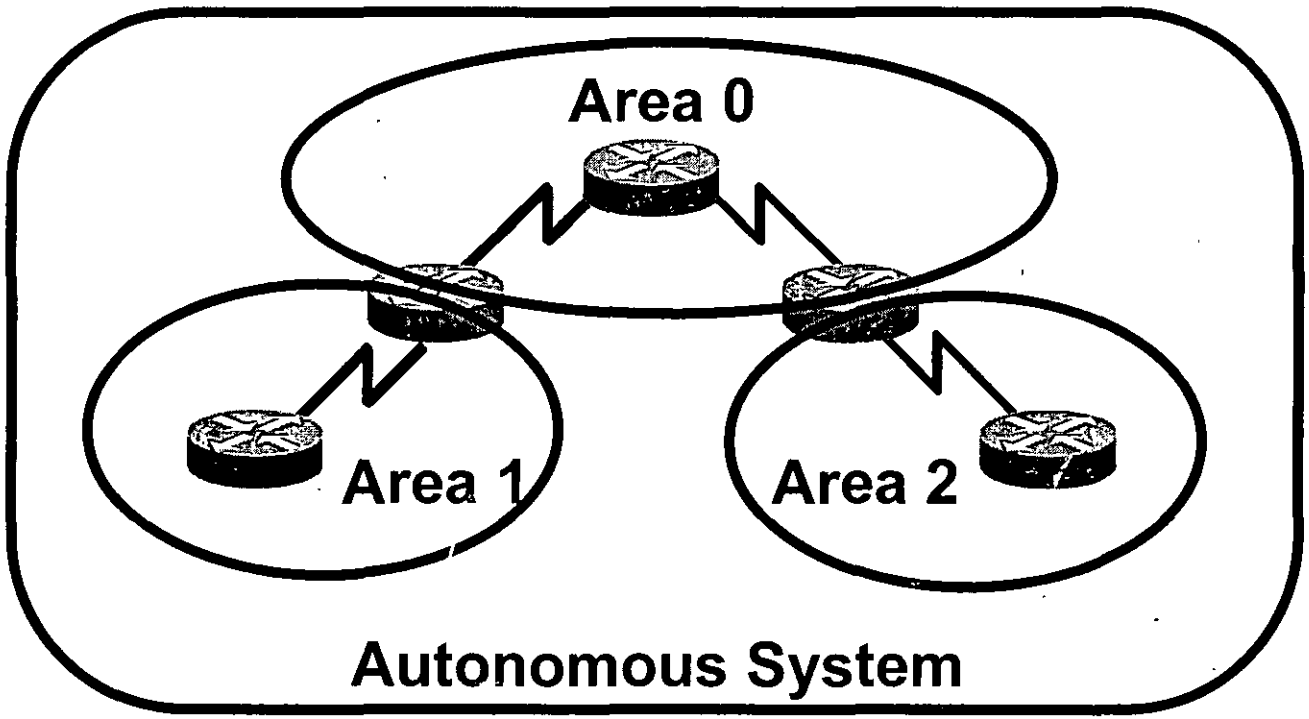
OSPF over NBMA Topology Summary

Mode	Required Neighbor	Subnet Address	Adjacency	RFC or Cisco
NBMA	Fully meshed	Same	Manual configuration DR/BDR elected	RFC
Broadcast	Fully meshed	Same	Automatic DR/BDR elected	Cisco
Point-to-multipoint	Partial mesh or star	Same	Automatic No DR/BDR	RFC
Point-to-multipoint nonbroadcast	Partial mesh or star	Same	Manual configuration No DR/BDR	Cisco
Point-to-point	Partial mesh or star, using subinterface	Different for each subint.	Automatic No DR/BDR	Cisco

Issues with Maintaining a Large OSPF Network



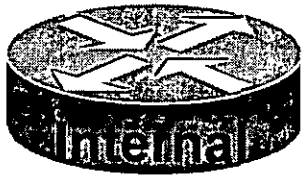
The Solution: OSPF Hierarchical Routing

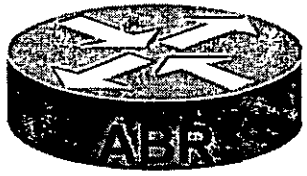


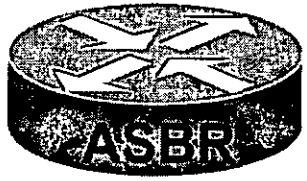
- Consists of areas and autonomous systems
- Minimizes routing update traffic

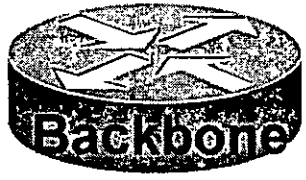
OSPF Multi-Area Components

Routers

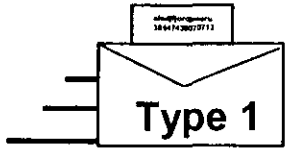


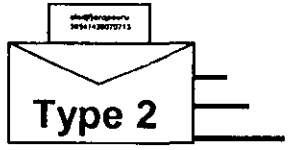


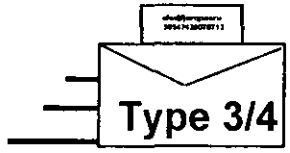


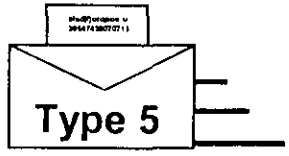


LSAs

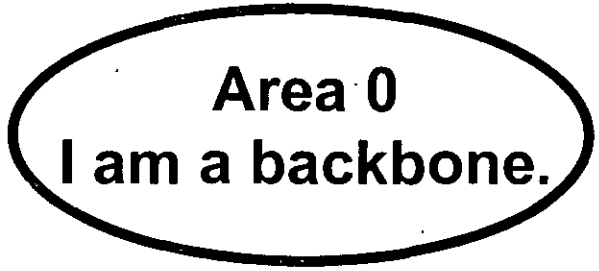


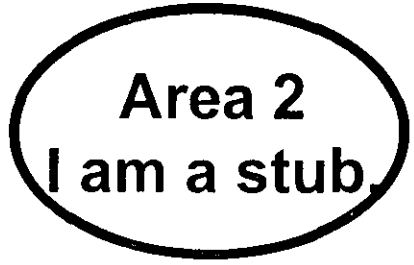




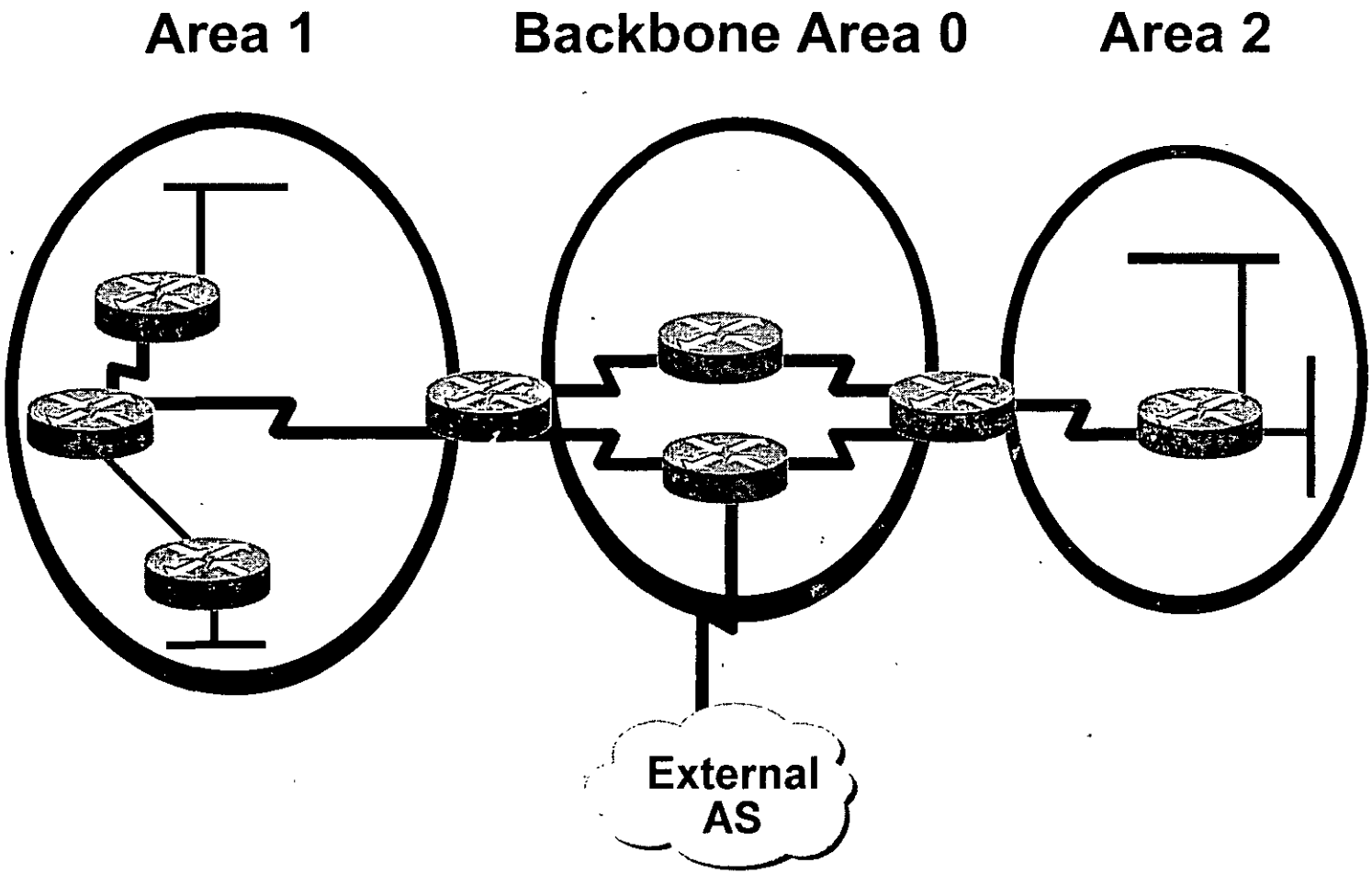


Areas

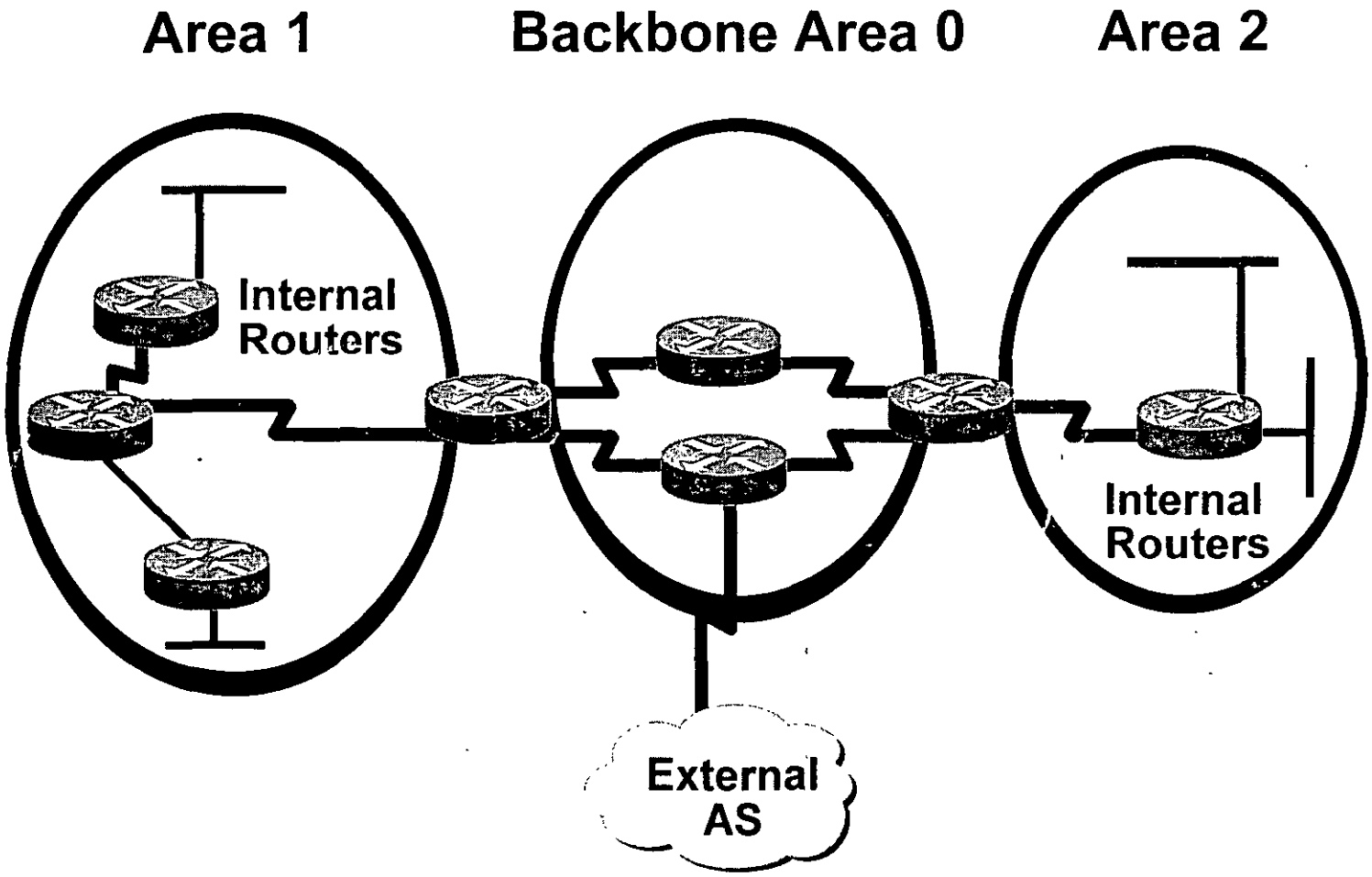




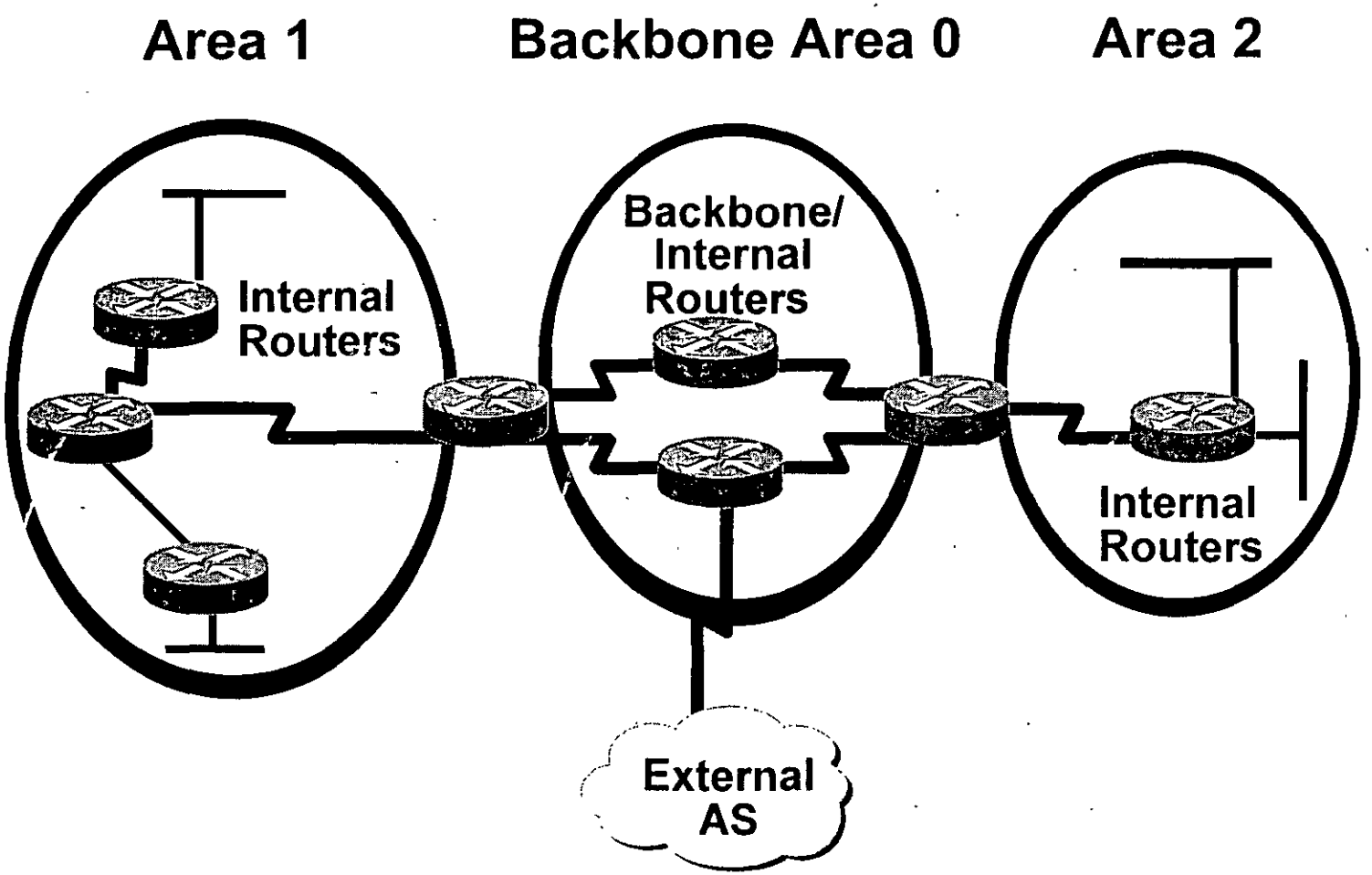
Types of OSPF Routers



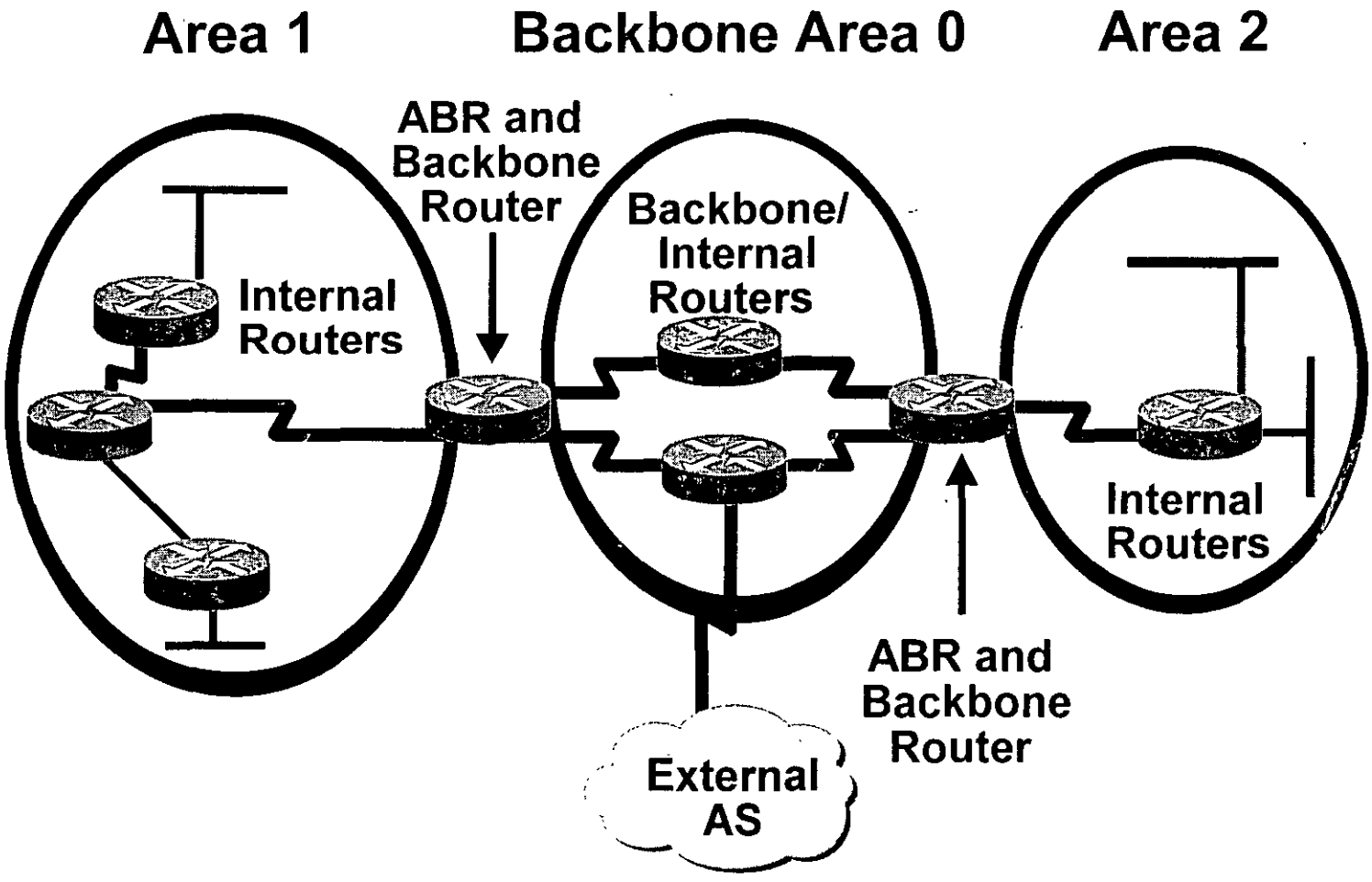
Types of OSPF Routers



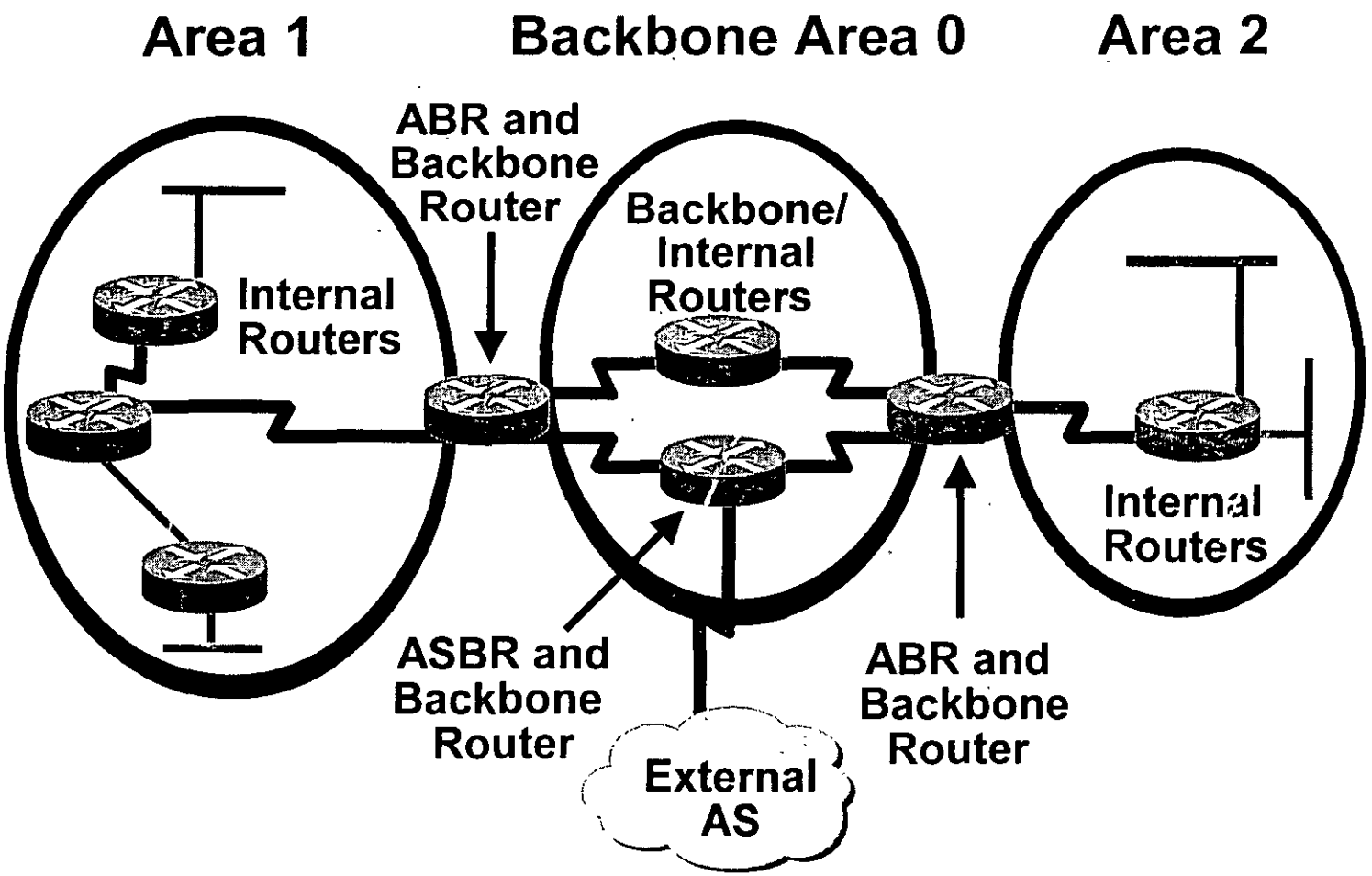
Types of OSPF Routers



Types of OSPF Routers



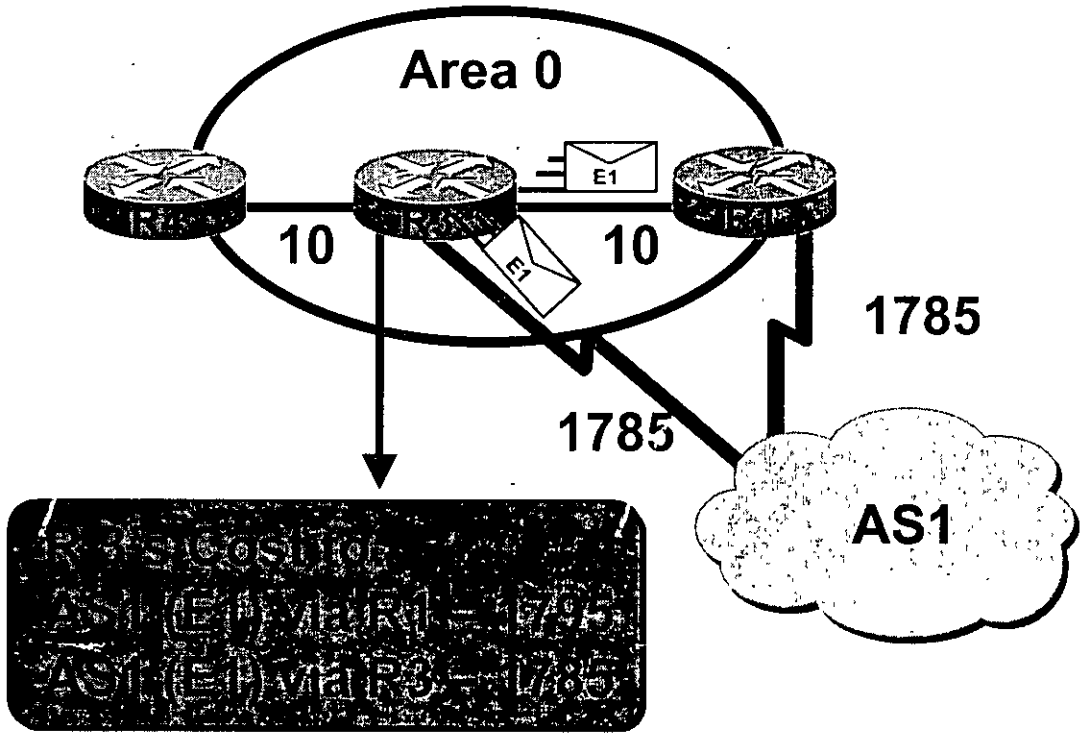
Types of OSPF Routers



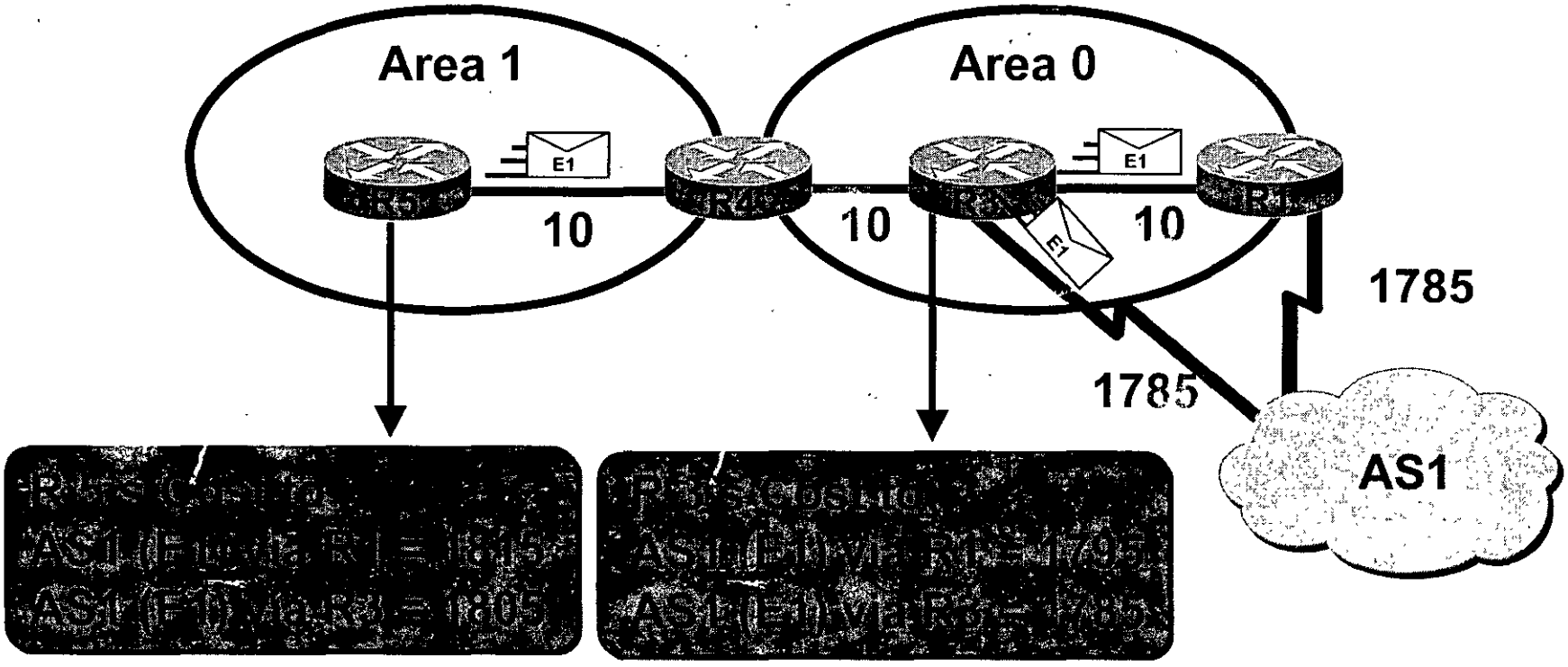
Types of Link-State Advertisements

- Type 1: Router link entry
- Type 2: Network link entry
- Type 3 and 4: Summary link entry
- Type 5: AS external link entry

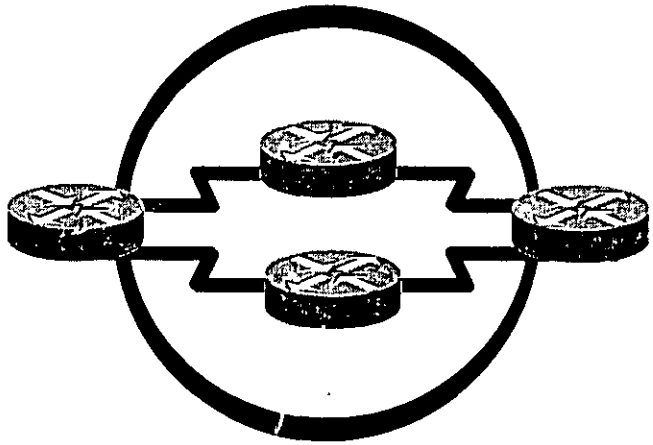
Calculating Costs for Summary and AS External Routes



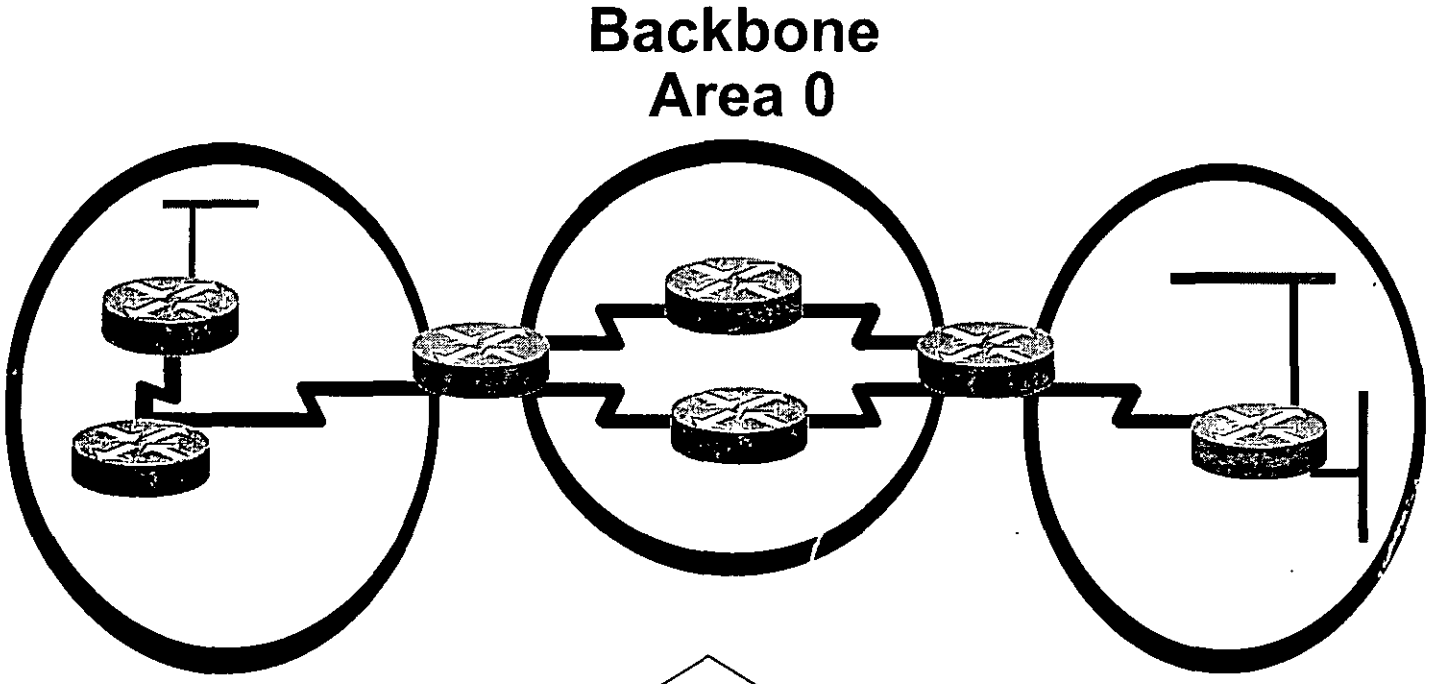
Calculating Costs for Summary and AS External Routes



Types of Areas

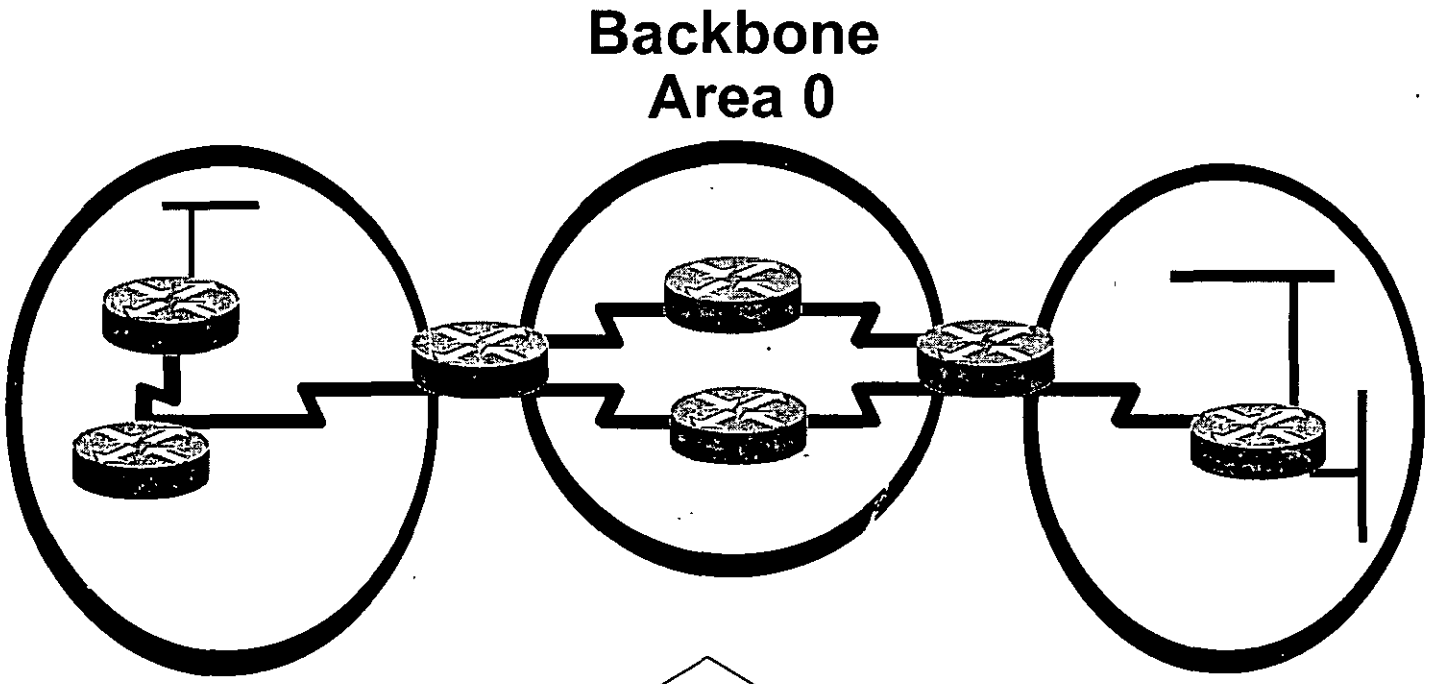


Types of Areas



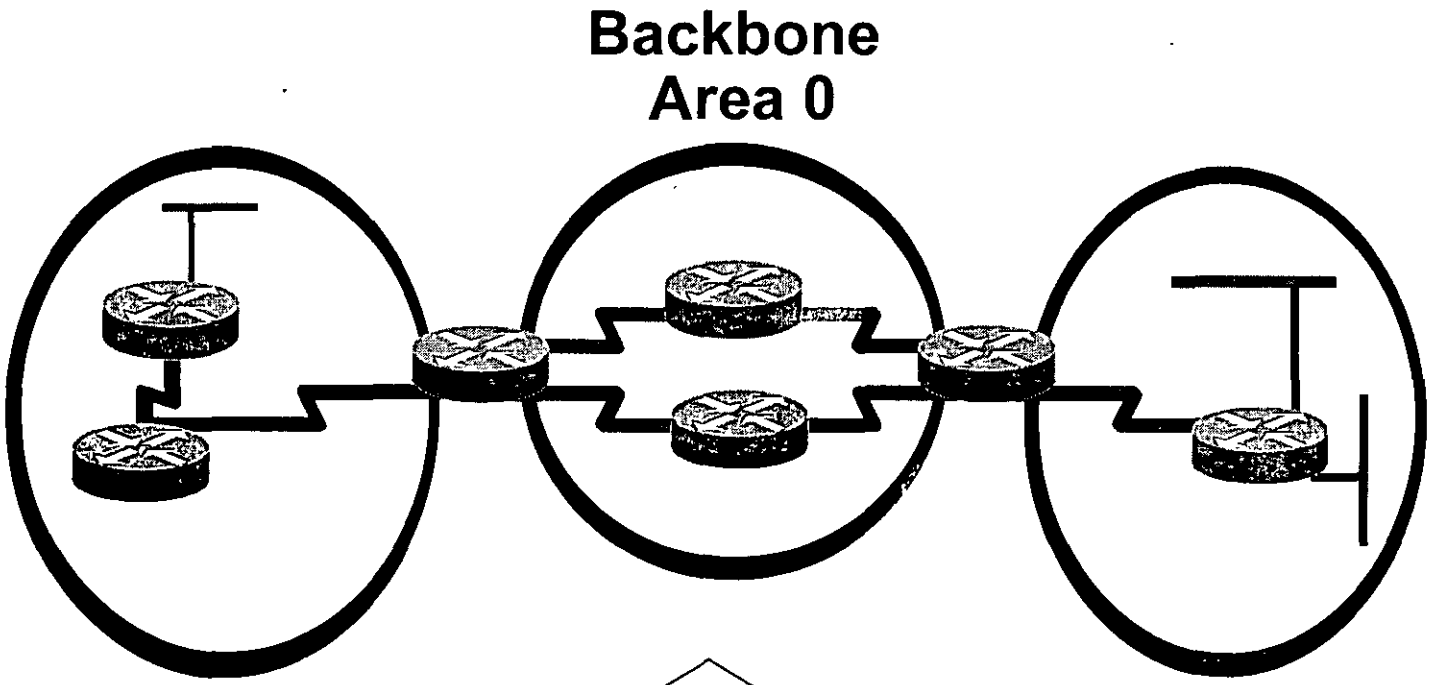
Interconnects areas; accepts all LSAs.

Types of Areas



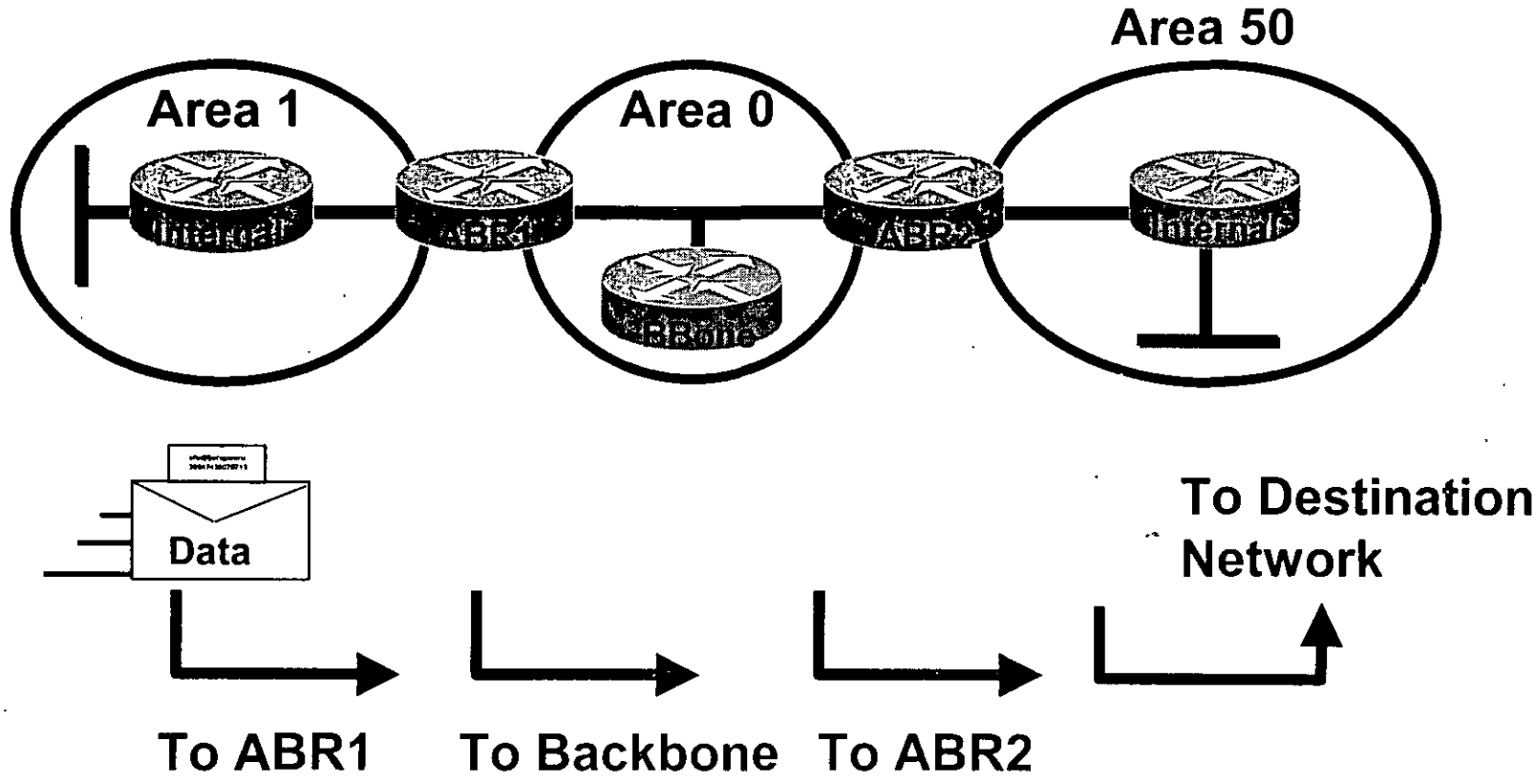
Interconnects areas; accepts all LSAs.

Types of Areas

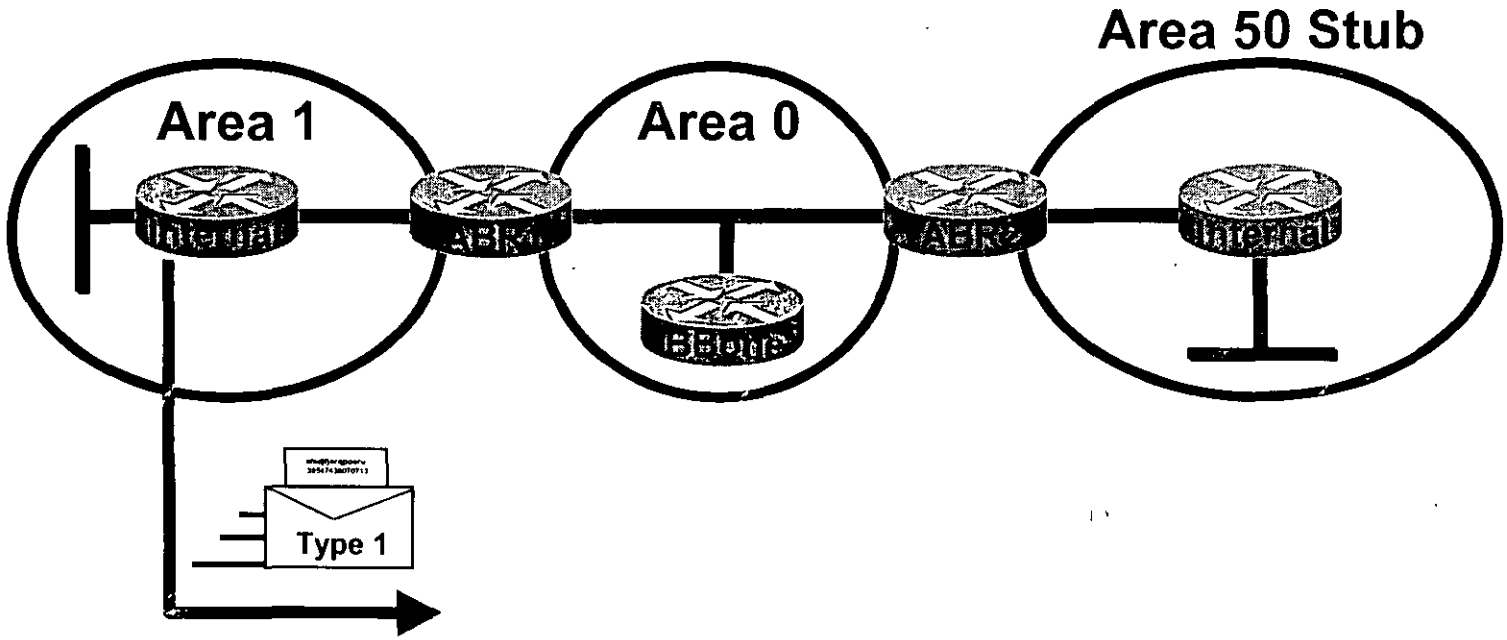


Interconnects areas; accepts all LSAs.

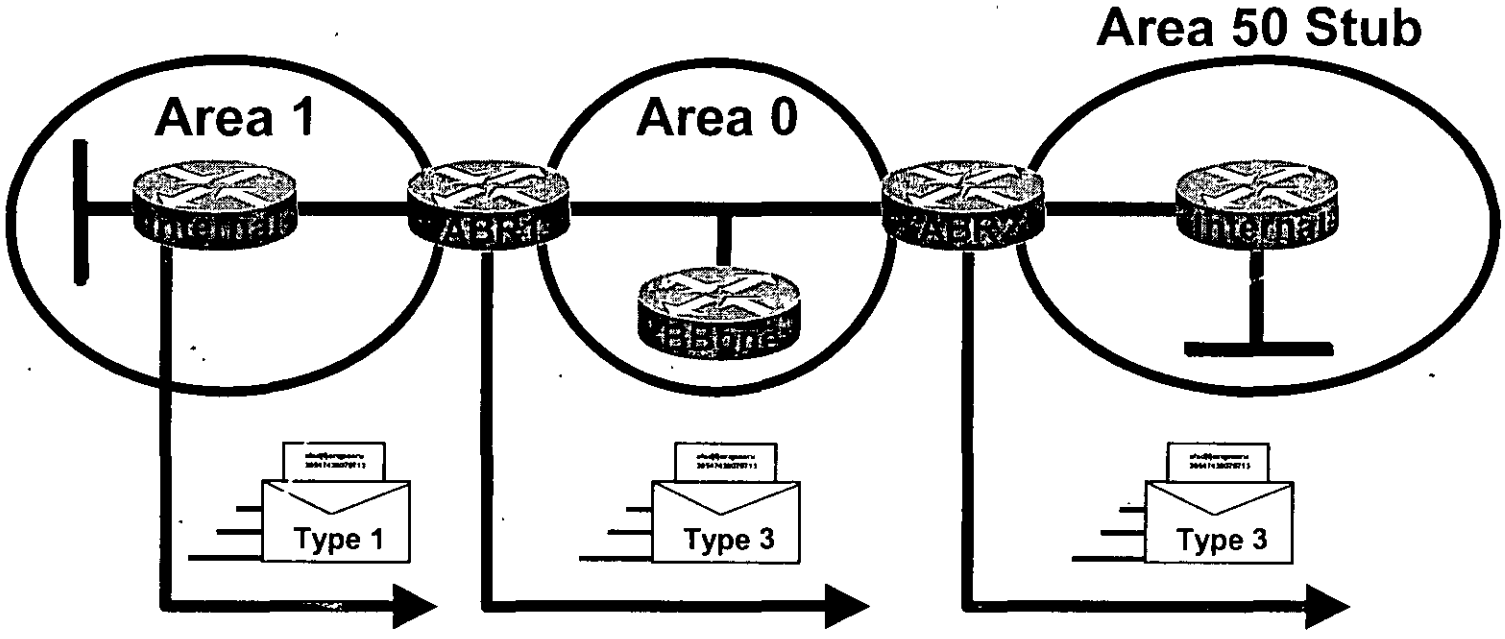
Forwarding Packets in a Multi-Area Network



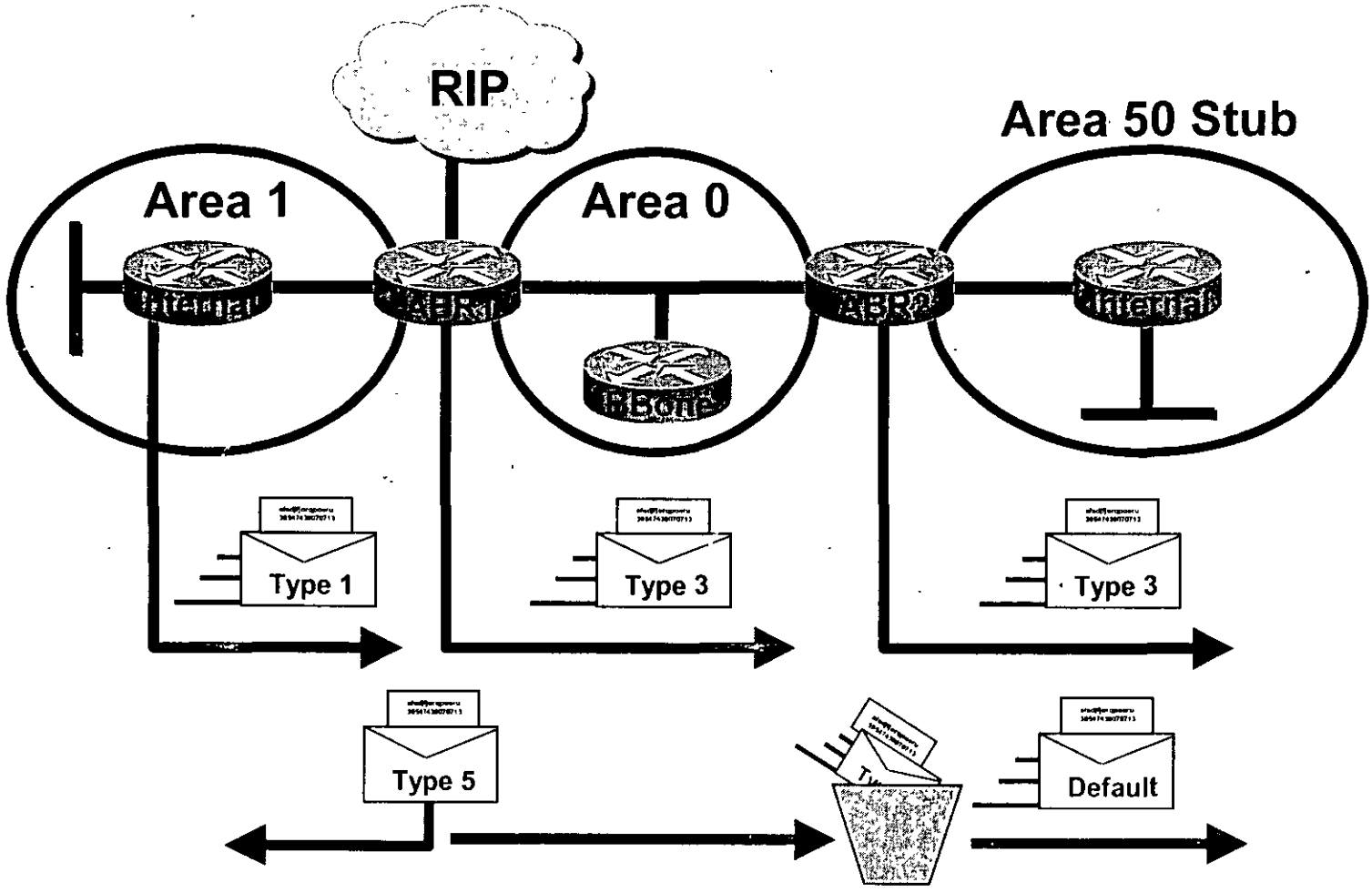
Flooding LSUs to Multiple Areas



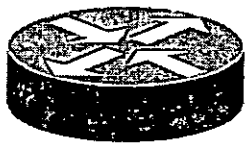
Flooding LSUs to Multiple Areas



Flooding LSUs to Multiple Areas



Flooding LSUs to Multiple Areas (cont.)

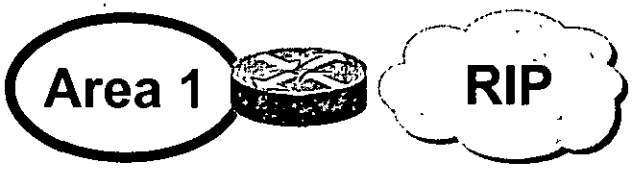


Routing Table

Intra-Area Routes

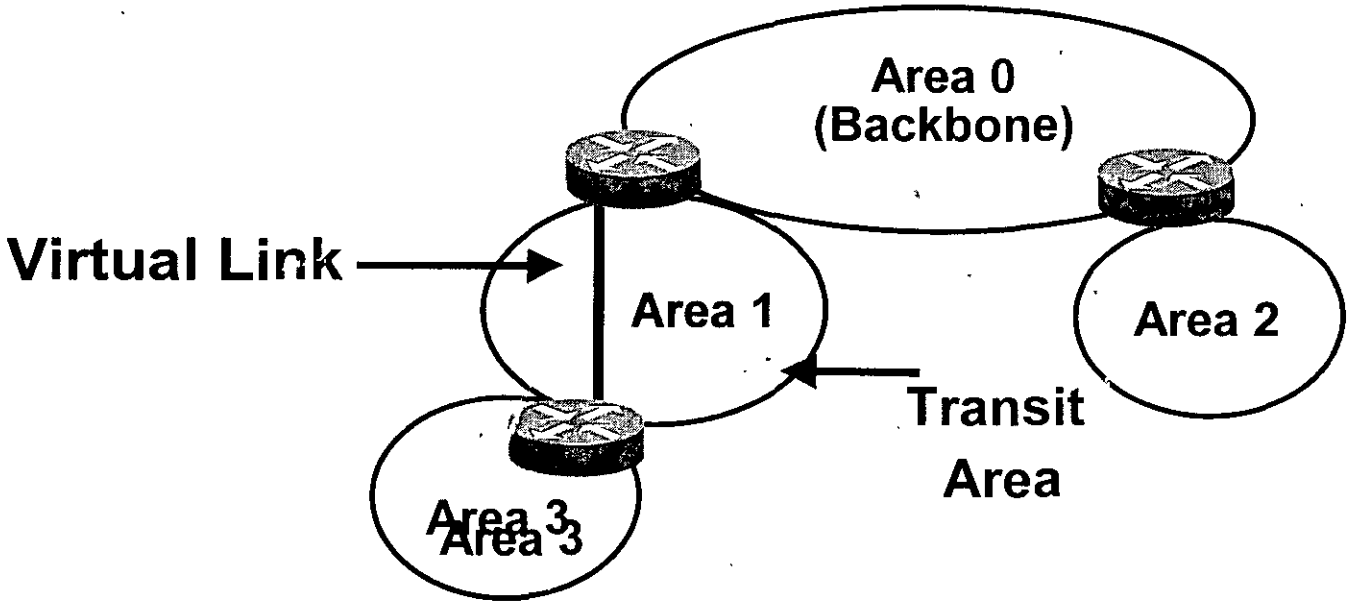
Inter-Area Routes

External (Non-OSPF Routes)



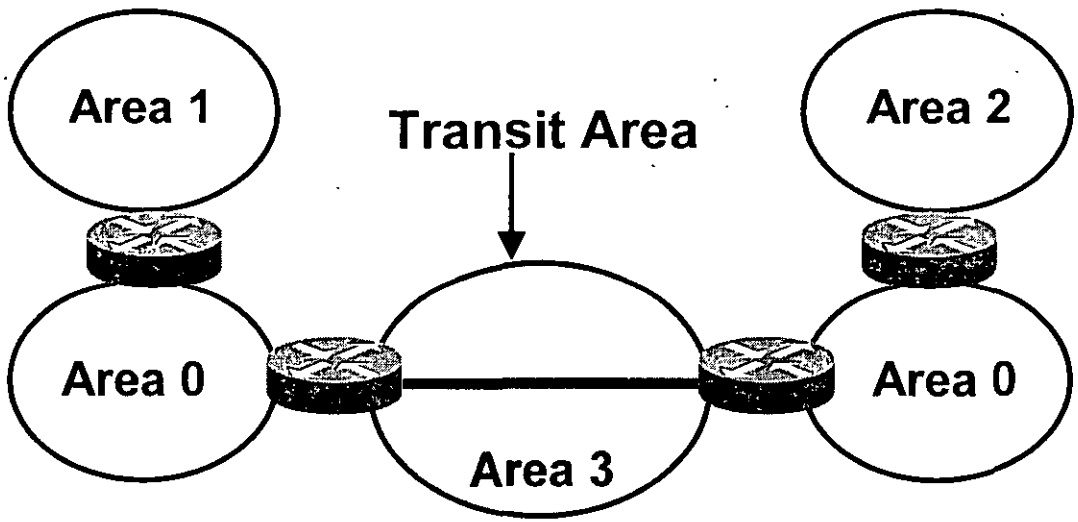
Virtual Links Overview

Meeting the Backbone Area Requirements



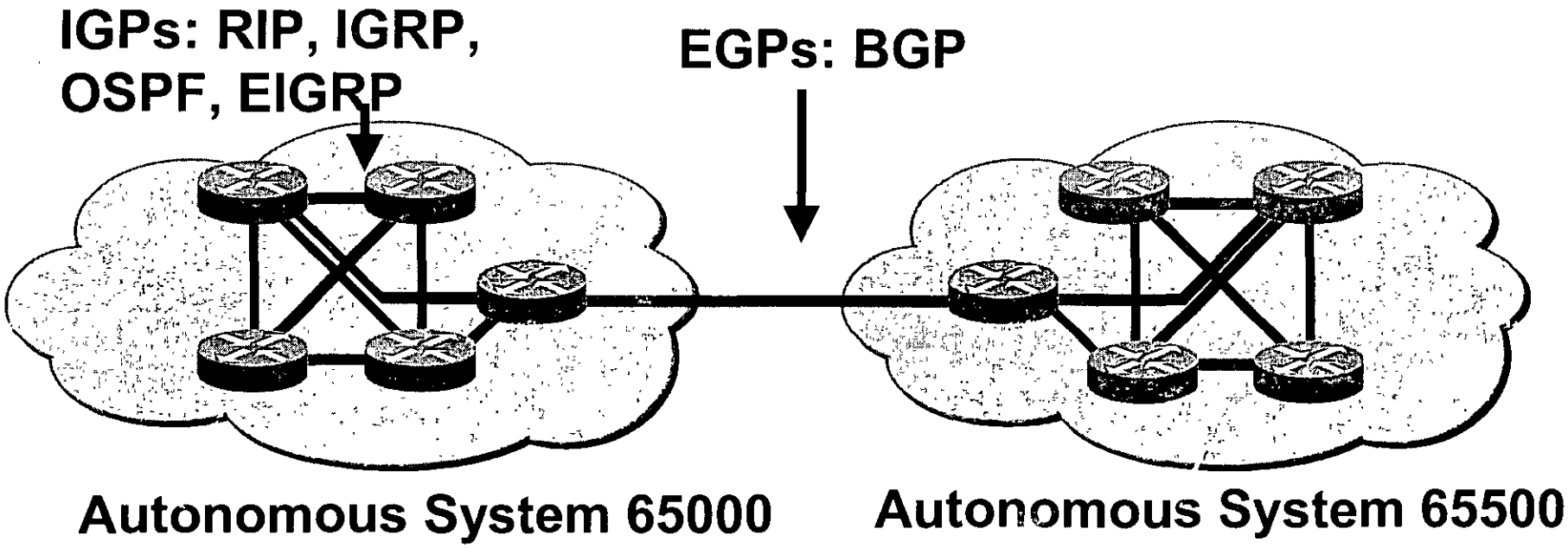
- Backbone center of communication
- Virtual links provide path to backbone
- Avoid configuring virtual links if possible

Meeting the Backbone Area Requirements (cont.)



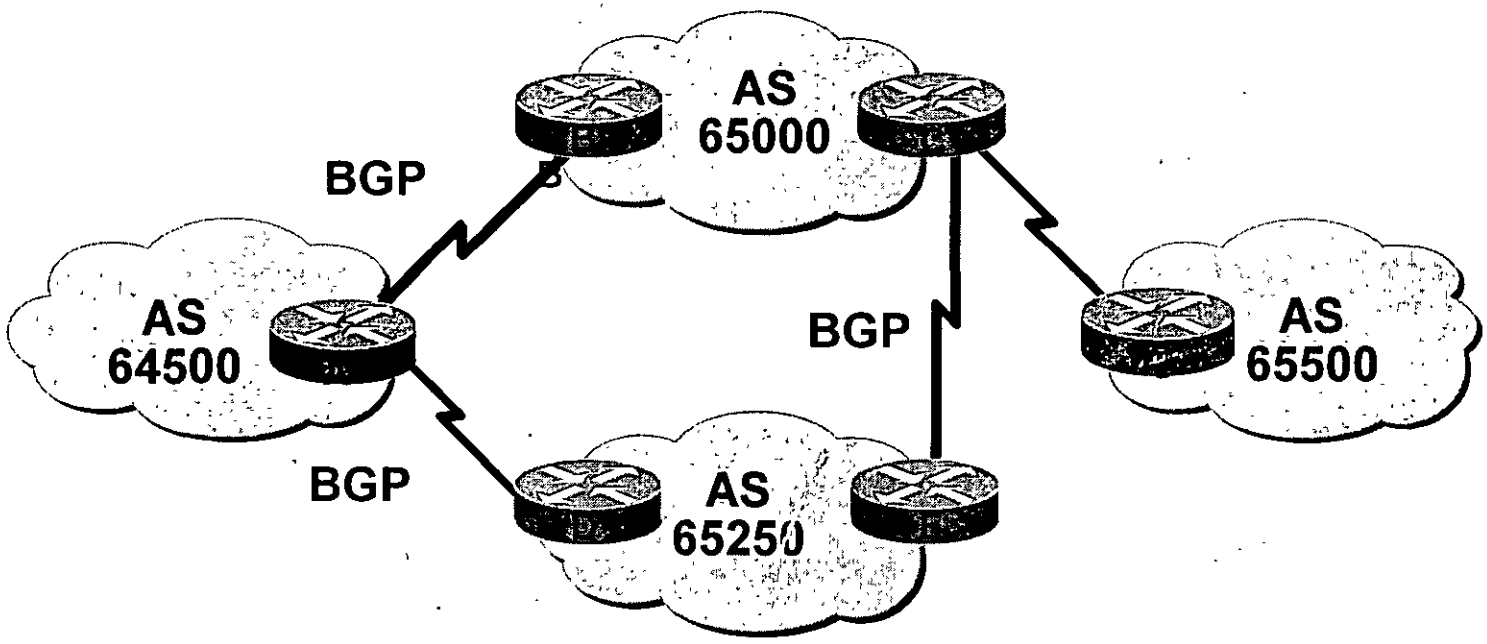
- Link discontiguous backbone
  - Merged networks
  - Redundancy
  - Point-to-point links

BGP Overview



- An autonomous system (AS) is a collection of networks under a a single technical administration
- IGPs operate within an autonomous system
- EGPs connect different autonomous systems

BGP Is Used Between Autonomous Systems



- BGP is used between autonomous systems
- Guarantees exchange of loop-free routing information

Scalable Routing Protocol Comparison

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
OSPF	Interior	LS	Yes	Cost
EIGRP	Interior	Advanced DV	No	Composite
BGP	Exterior	Advanced DV	No	Path vectors or attributes

When to Use BGP

- BGP is most appropriate when at least one of the following conditions exist:
  - An AS allows packets to transit through it to reach other autonomous systems (for example, a service provider)
  - An AS has multiple connections to other autonomous systems
  - The flow of traffic entering and leaving your AS must be manipulated
- And the effects of BGP are well understood

How Big Is the Internet?

- A BGP router in the Internet has:
  - A routing table that uses more than 30 Mb
  - Over 70,000 routes
  - Over 6,500 AS numbers

When Not to Use BGP

- BGP is not always appropriate. Don't use BGP if you have one of the following conditions:
  - A single connection to the Internet or other AS
  - Routing policy and route selection are not a concern for your AS
  - Lack of memory or processor power on BGP routers to handle constant updates
  - Limited understanding of route filtering and BGP path selection process
  - Low bandwidth between autonomous systems
- Use static routes instead

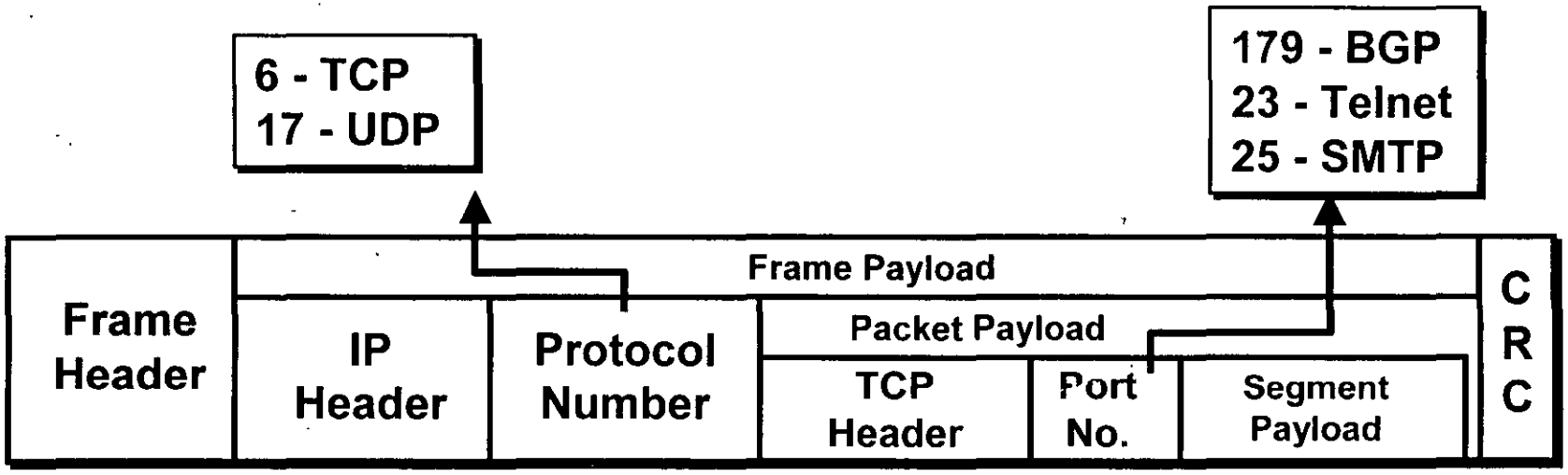
BGP Characteristics

- BGP is a distance vector protocol with enhancements:
  - Reliable updates—BGP runs on top of TCP (port 179)
  - Incremental, triggered updates only
  - Periodic keepalives to verify TCP connectivity
  - Rich metrics (called path vectors or attributes)
  - Designed to scale to huge internetworks

BGP Route Selection Decision Process

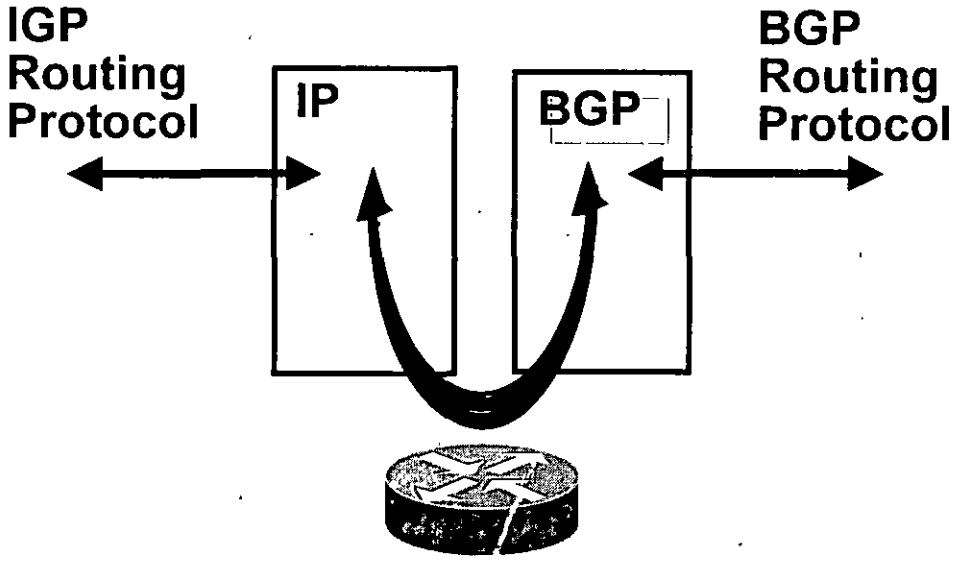
- Consider only (synchronized) routes with no AS loops and a valid next-hop, and then:
  - Prefer highest weight (local to router)
  - Prefer highest local preference (global within AS)
  - Prefer route originated by the local router
  - Prefer shortest AS-path
  - Prefer lowest origin code (IGP < EGP < incomplete)
  - Prefer lowest MED (from other AS)
  - Prefer EBGP path over IBGP path
  - Prefer the path through the closest IGP neighbor
  - Prefer the path with the lowest neighbor BGP router ID

BGP in IP Packets



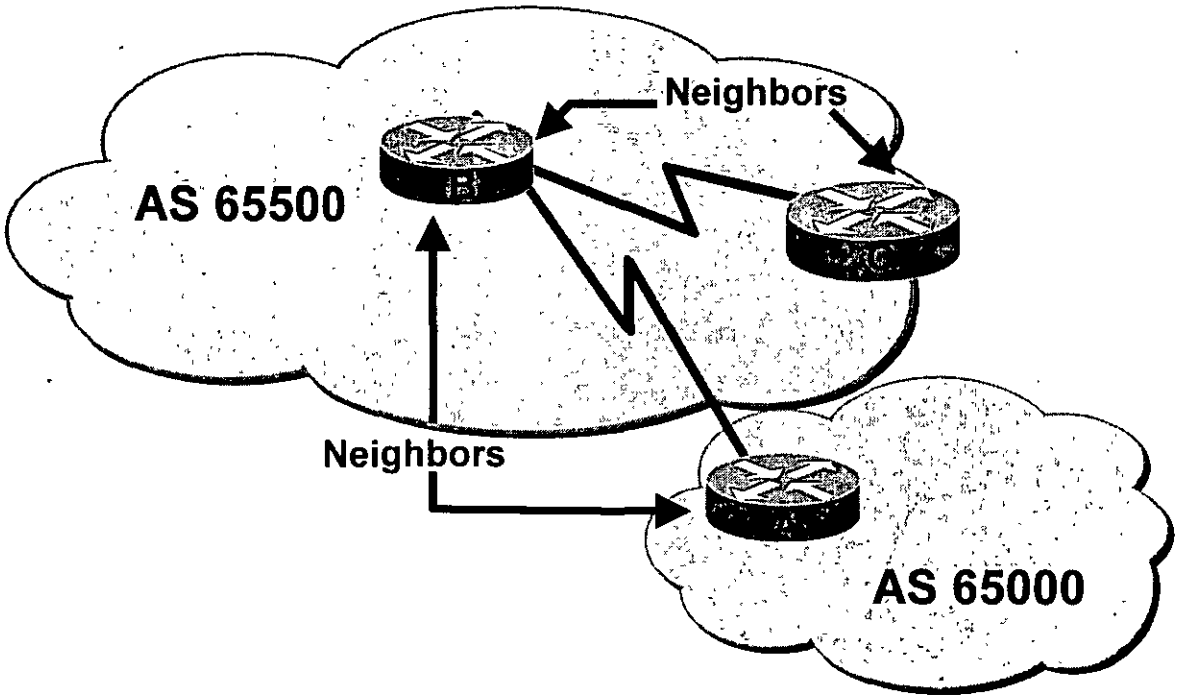
- BGP is an advanced distance vector routing protocol
  - Relies on TCP for reliable session management
  - Uses port number 179

Tables



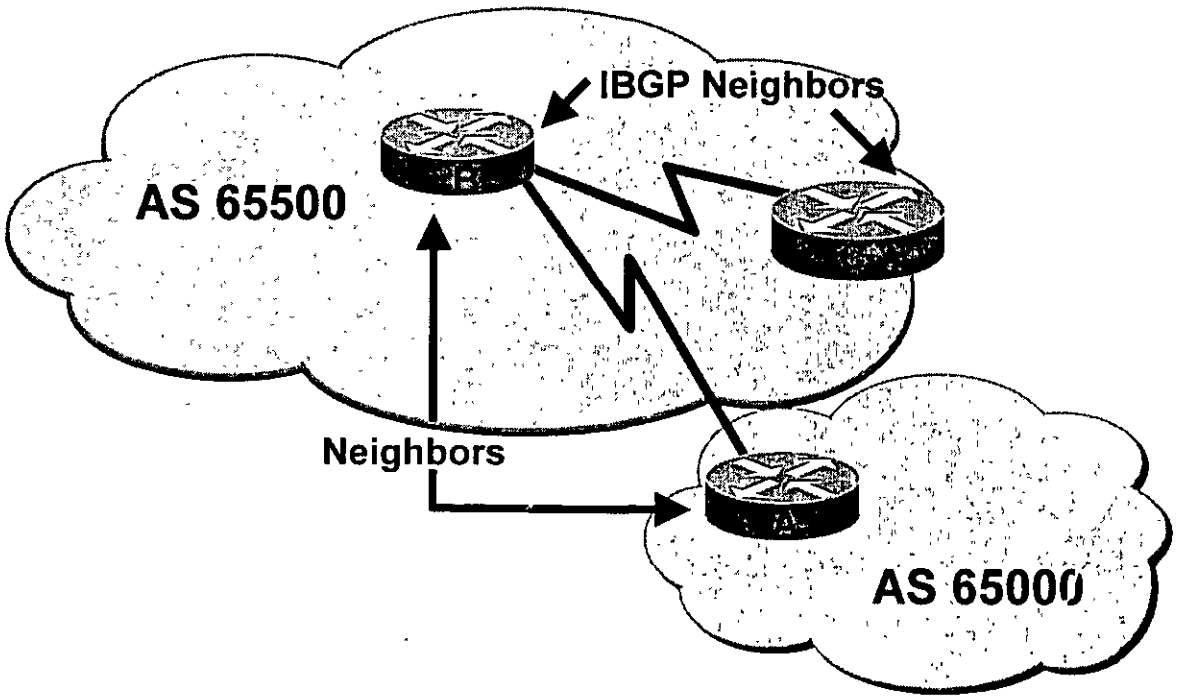
- BGP has its own table, in addition to the IGP routing table
- Information can be exchanged between the two tables

Peers = Neighbors



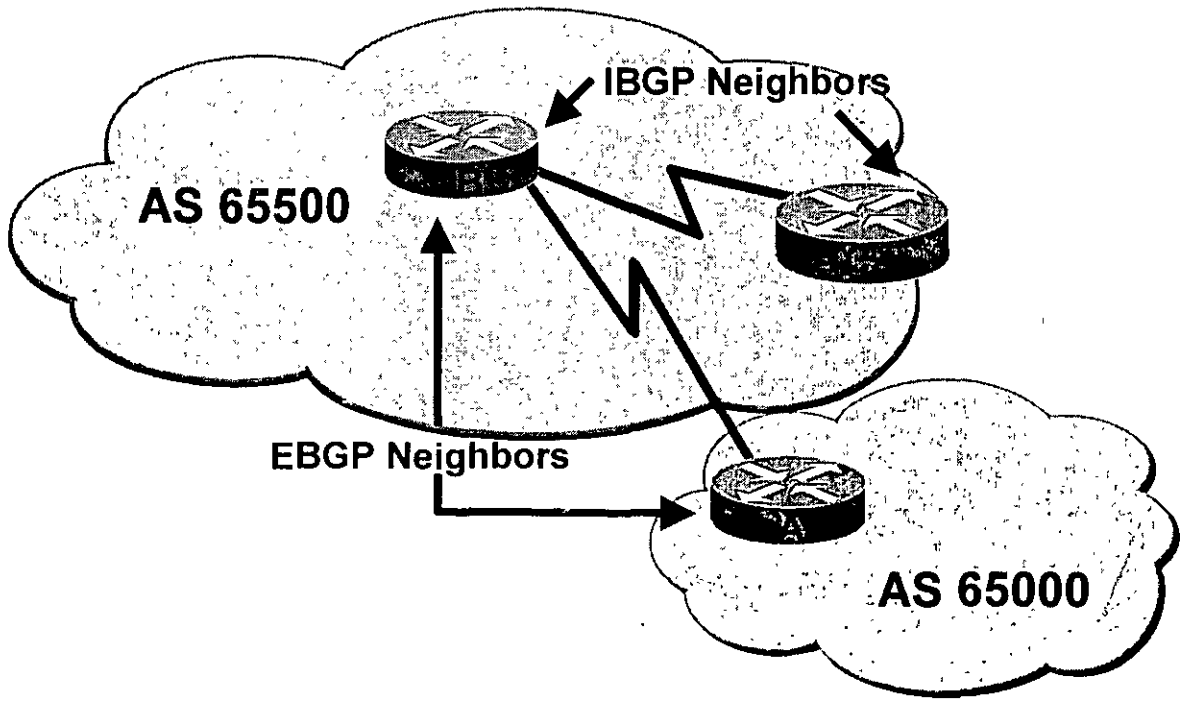
- Any two routers that have formed a TCP connection in order to exchange BGP routing information are called peers or neighbors

Internal BGP



- When BGP neighbors belong to the same AS
- Neighbors do not have to be directly connected

External BGP



- When BGP neighbors belong to different autonomous systems
- Neighbors should be directly connected

Policy-Based Routing

- BGP allows administrators to define policies, or rules, for how data will flow through the autonomous systems
- BGP and associated tools cannot express all routing policies
  - BGP does not enable one AS to send traffic to a neighbor AS, intending that the traffic take a different route from that taken by traffic originating in the neighbor AS
- However, BGP can support any policy conforming to (implementable by) the
  hop-by-hop routing paradigm

BGP Attributes

- BGP metrics are called path attributes
- Characteristics of attributes include:
  - Well-known versus optional
  - Mandatory versus discretionary
  - Transitive versus nontransitive
  - Partial

Well-known Attributes

- Well-known attributes
  - Must be recognized by all compliant BGP implementations
  - Are propagated to other neighbors[HQ]
- Well-known mandatory attributes
  - Must be present in all update messages
- Well-known discretionary attributes
  - Could be present in update messages

Optional Attributes

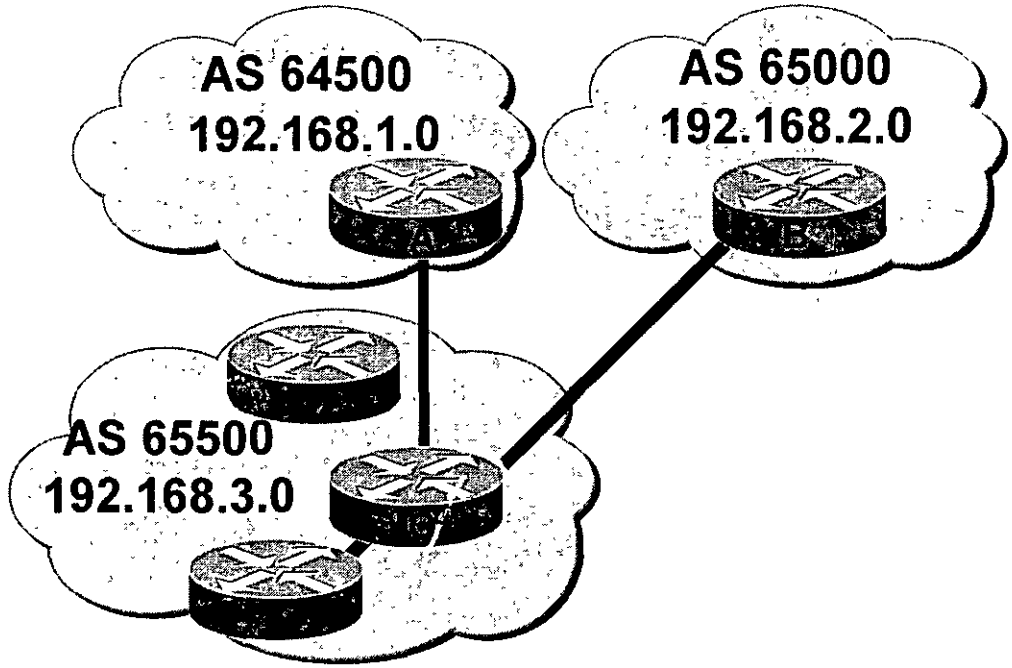
- Optional attributes
  - Recognized by some implementations (could be private), expected not to be recognized by everyone
  - Recognized optional attributes are propagated to other neighbors based on their meaning
- Optional transitive attributes
  - If not recognized, are marked as partial and propagated to other neighbors
- Optional nontransitive attributes
  - Discarded if not recognized

BGP Attributes

- BGP attributes include:
  - AS-path *
  - Next-hop *
  - Local preference
  - Multi-exit-discriminator (MED)
  - Origin *
  - Community

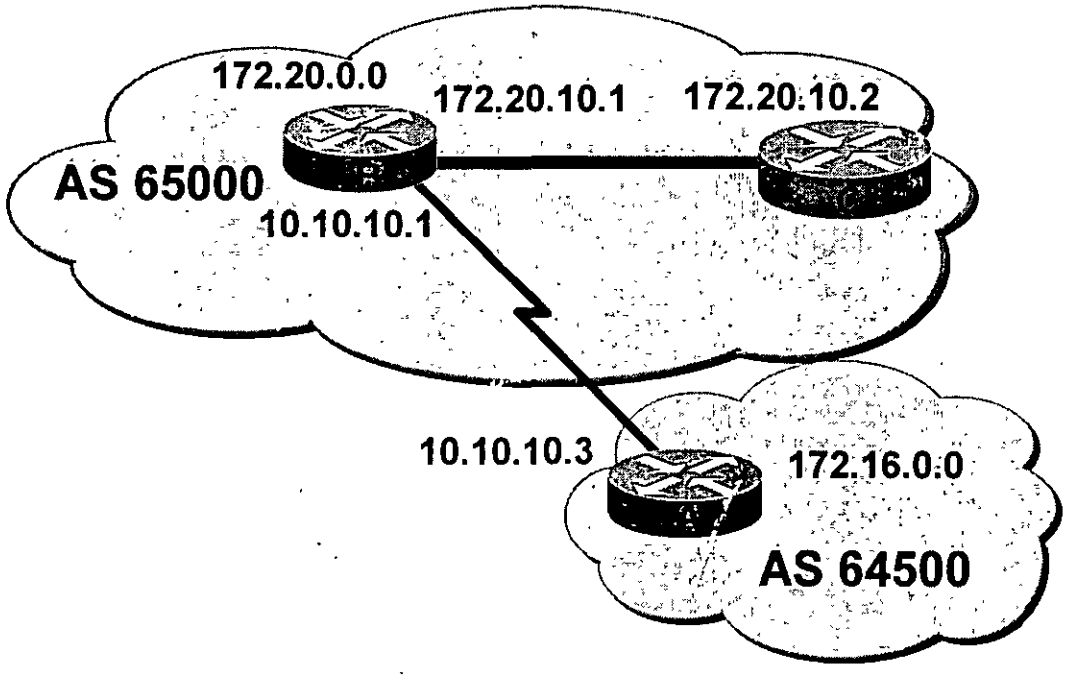
*** = Well-known mandatory attribute**

AS-Path Attribute



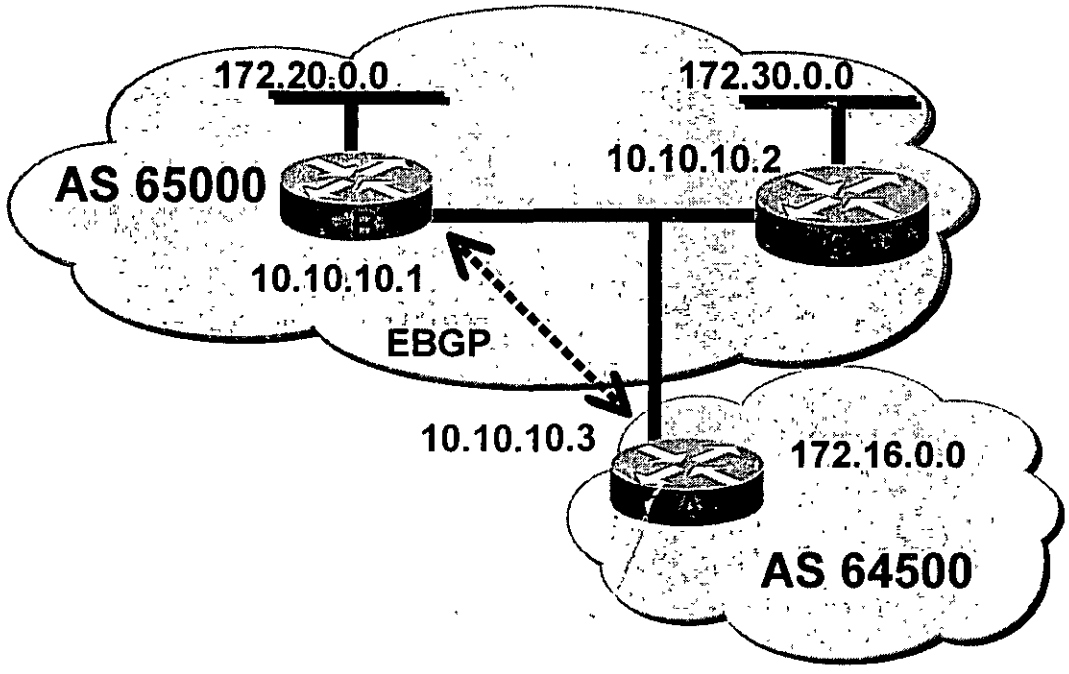
- A list of autonomous systems that a route has traversed
  - For example, on Router B the path to 192.168.1.0 is the AS sequence 65500 64500

Next-Hop Attribute



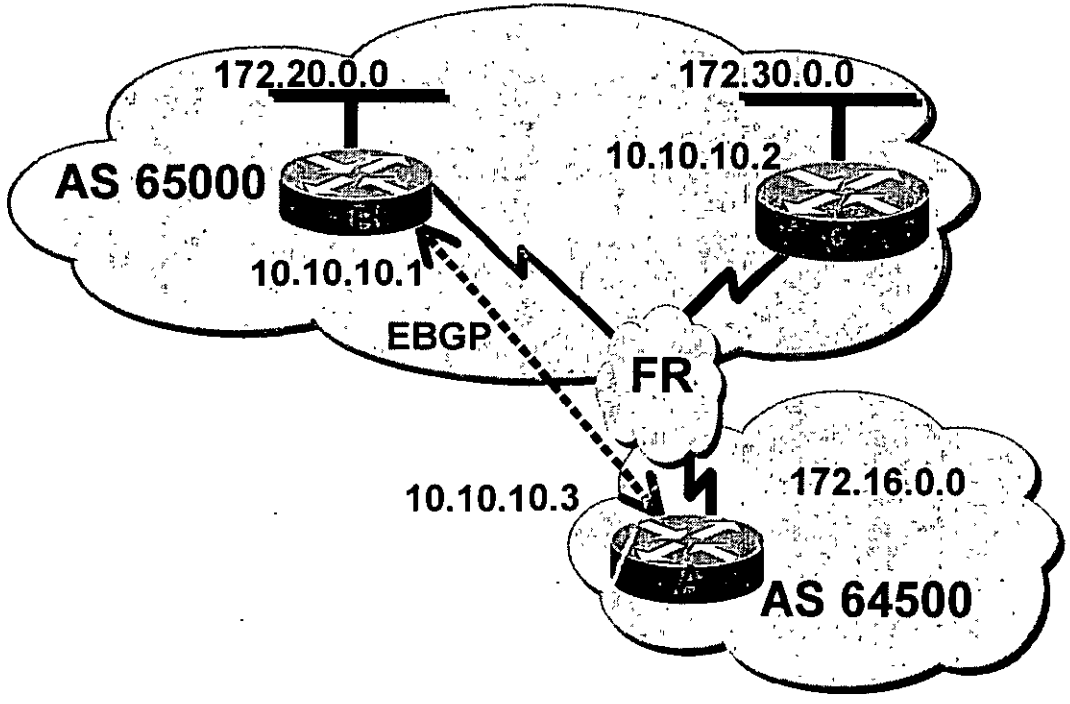
- Next-hop to reach a network
  - Router A advertises network 172.16.0.0 to Router B in EBGP, with a next hop of 10.10.10.3
  - Router B advertises 172.16.0.0 in IBGP to Router C, keeping 10.10.10.3 as the next-hop address

Next-Hop on a Multiaccess Network



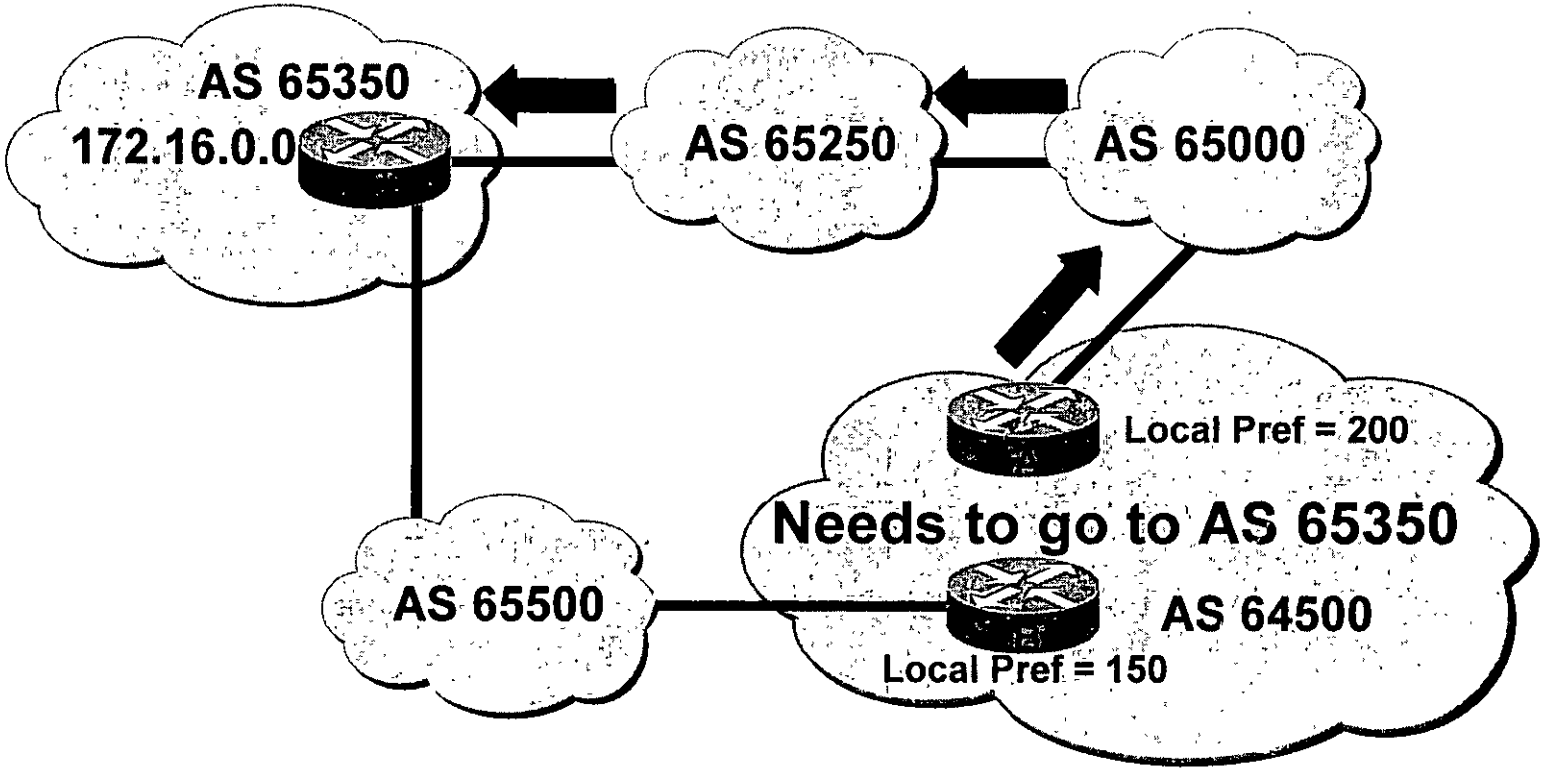
- In a multiaccess network
  - Router B will advertise network 172.30.0.0 to Router A in EBGP, with a next hop of 10.10.10.2, not 10.10.10.1
  - This avoids an unnecessary hop

Next-Hop on an NBMA Network



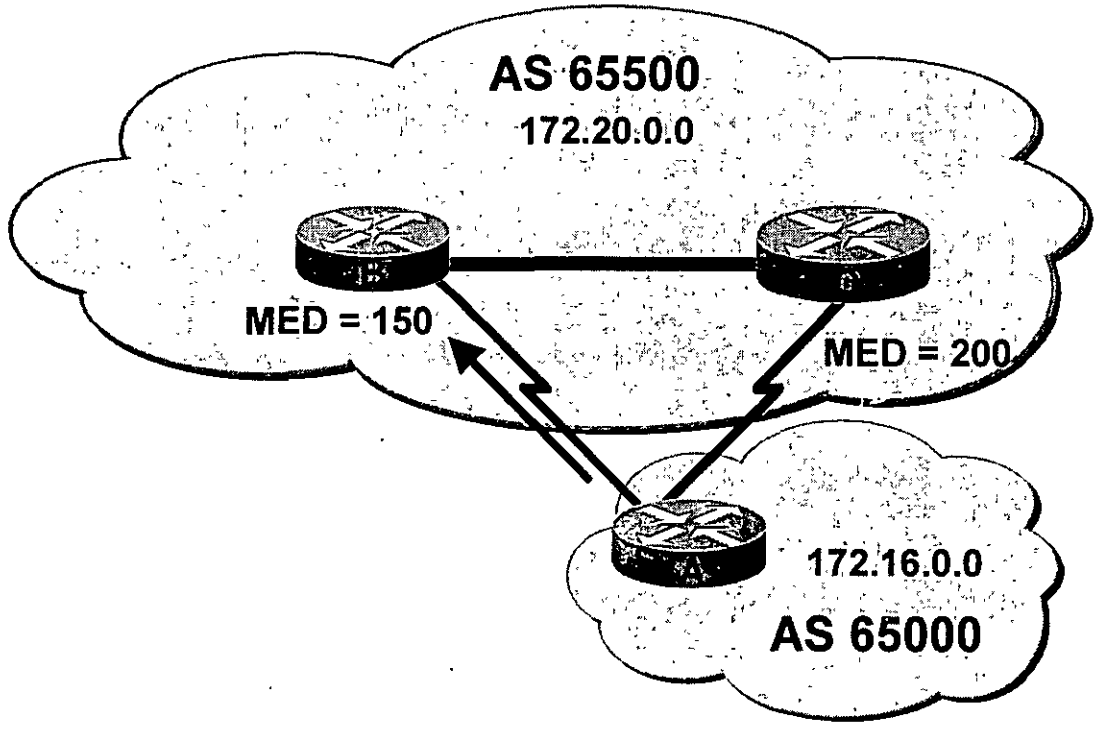
- In an NBMA network
  - By default, Router B will advertise network 172.30.0.0 to Router A in EBGP, with a next hop of 10.10.10.2, not 10.10.10.1
  - Can be overridden

Local Preference Attribute



- Paths with highest preference value are most desirable
  - Preference configured on routers
  - Preference sent to internal BGP neighbors only

MED Attribute



- Paths with lowest MED (also called the metric) value are most desirable
  - MED configured on routers
  - MED sent to external BGP neighbors only

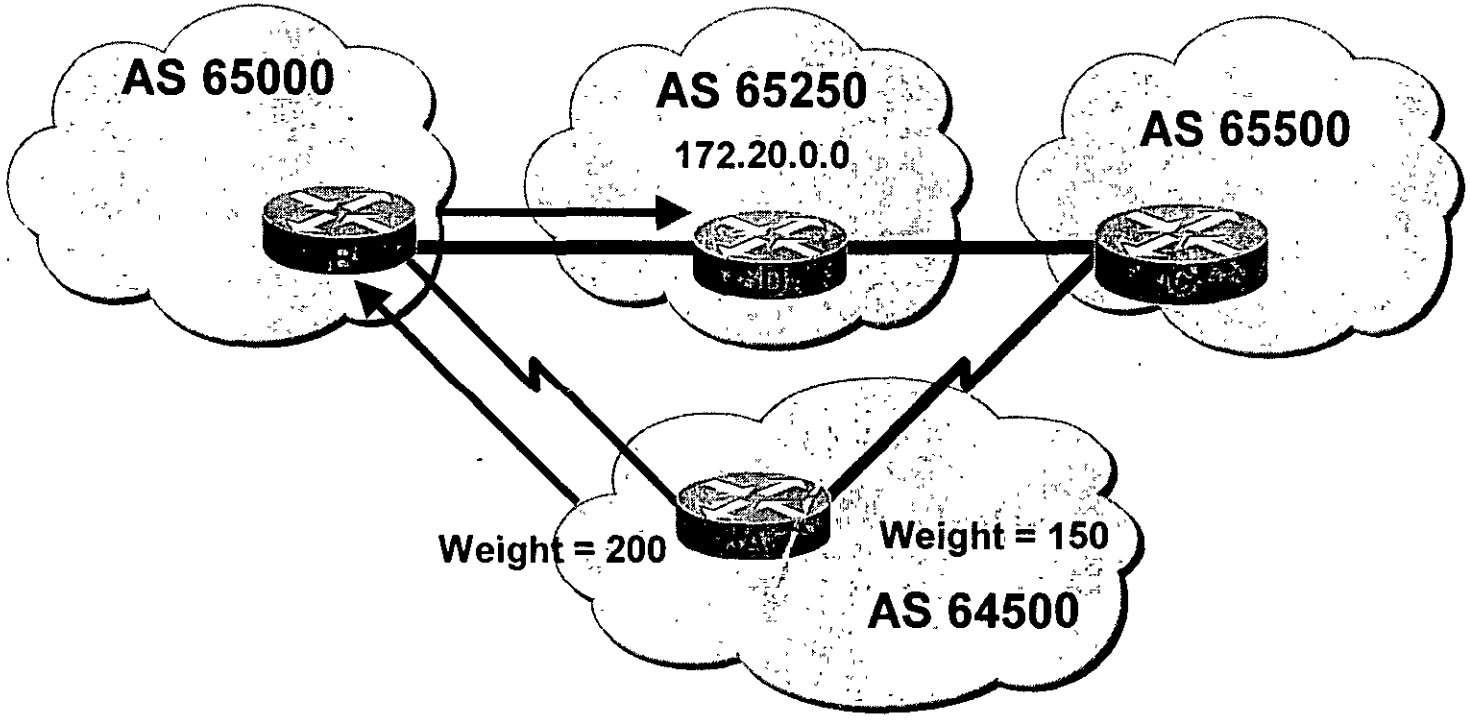
Origin Attribute

- IGP (i)
  - *network* command
- EGP (e)
  - Redistributed from EGP
- Incomplete (?)
  - Redistributed from IGP or static

Community Attribute

- Communities are a means of tagging routes to ensure consistent filtering or route-selection policy
- Any BGP router can tag routes in incoming and outgoing routing updates, or when doing redistribution
- Any BGP router can filter routes in incoming or outgoing updates, or select preferred routes based on communities (the tag)
- By default, communities are stripped in outgoing BGP updates

Weight Attribute (Cisco Only)



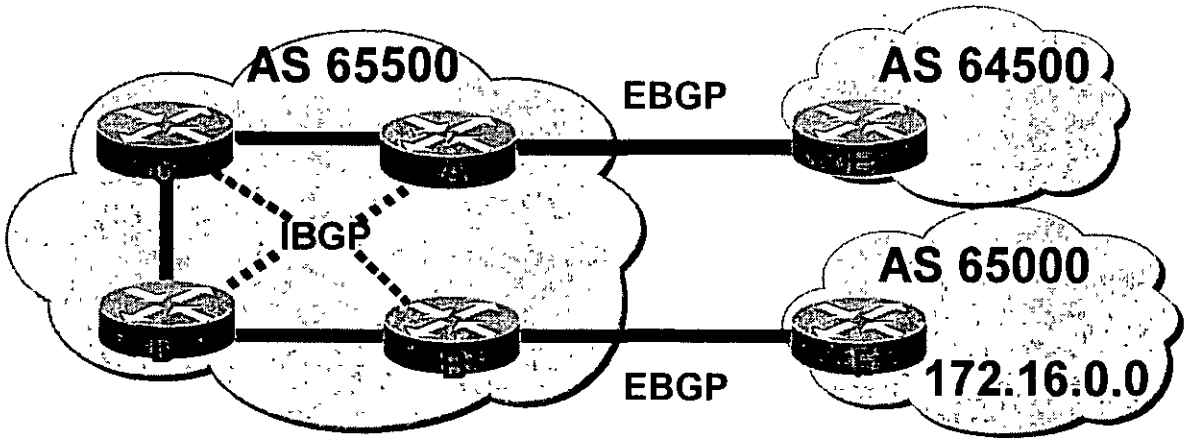
- Paths with highest weight value are most desirable
  - Weight configured on routers, on a per-neighbor basis
  - Weight not sent to any BGP neighbors

BGP Synchronization

- **Synchronization rule:**
  Do not use, or advertise to an external neighbor, a route learned by IBGP, until a matching route has been learned from an IGP

  - Ensures consistency of information throughout the AS
  - Avoids black holes within the AS
  - Safe to turn off when all routers in the AS are running BGP

BGP Synchronization Example



- All routers in AS 65500 are running BGP; no IGP is running

- If synchronization is on (the default) then:
  - Routers A, C, and D would not use or advertise the route to 172.16.0.0 until they receive the matching route via an IGP
  - Router E would not hear about 172.16.0.0
- If synchronization is off then:
  - Routers A, C, and D would use and advertise the route they receive via IBGP; Router E would hear about 172.16.0.0
  - If Router E sends traffic for 172.16.0.0, Routers A, C, and D would route the packets correctly to Router B

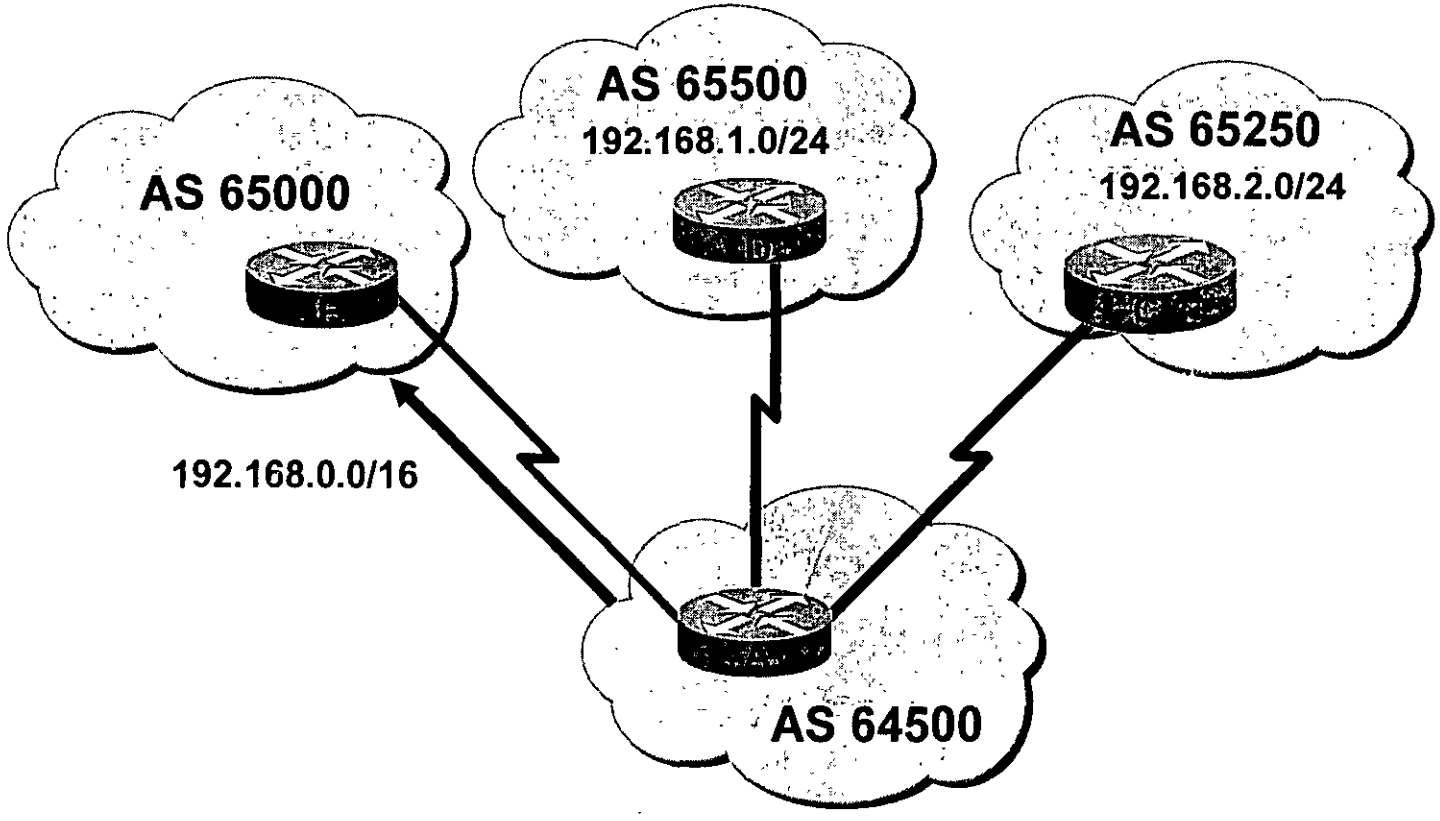
BGP Message Types

- BGP defines the following message types:
  - Open
    - Includes hold time and BGP router ID
  - Keepalive
  - Update
    - Information for one path only (could be to multiple networks)
    - Includes path attributes and networks
  - Notification
    - When error detected
    - BGP connection closed after sent

Route Selection Decision Process

- Consider only (synchronized) routes with no AS loops and a valid next-hop, and then:
  - Prefer highest weight (local to router)
  - Prefer highest local preference (global within AS)
  - Prefer route originated by the local router
  - Prefer shortest AS-path
  - Prefer lowest origin code (IGP < EGP < incomplete)
  - Prefer lowest MED (from other AS)
  - Prefer EBGP path over IBGP path
  - Prefer the path through the closest IGP neighbor
  - Prefer oldest route for EBGP paths
  - Prefer the path with the lowest neighbor BGP router ID

CIDR and Aggregate Addresses



- Routes can be aggregated when passing through an AS

What Is Multihoming?

- Connecting to two or more ISPs to increase:
  - Reliability—If one ISP fails, still connected
  - Performance—Better paths to common Internet destinations

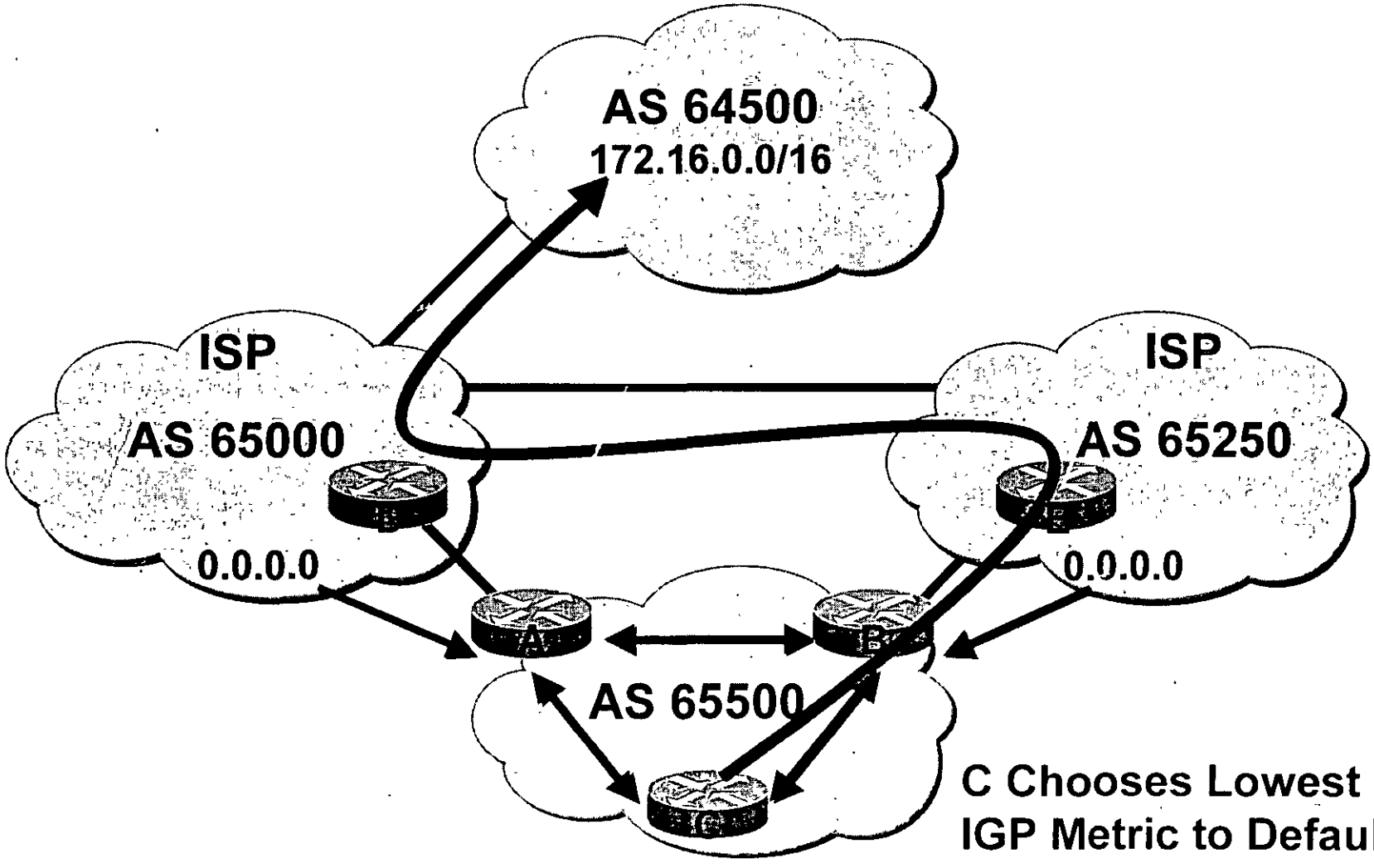
Types of Multihoming

- Three common ways of configuring the connections are:
  - Default routes from all providers
  - Customer routes and default routes from all providers
  - Full routes from all providers

Default Routes from All Providers

- Low memory and CPU usage
- Provider sends BGP default route
  - Choice of provider decided by IGP metrics to reach default route
- AS sends all of its routes to provider
  - Inbound path decided by Internet

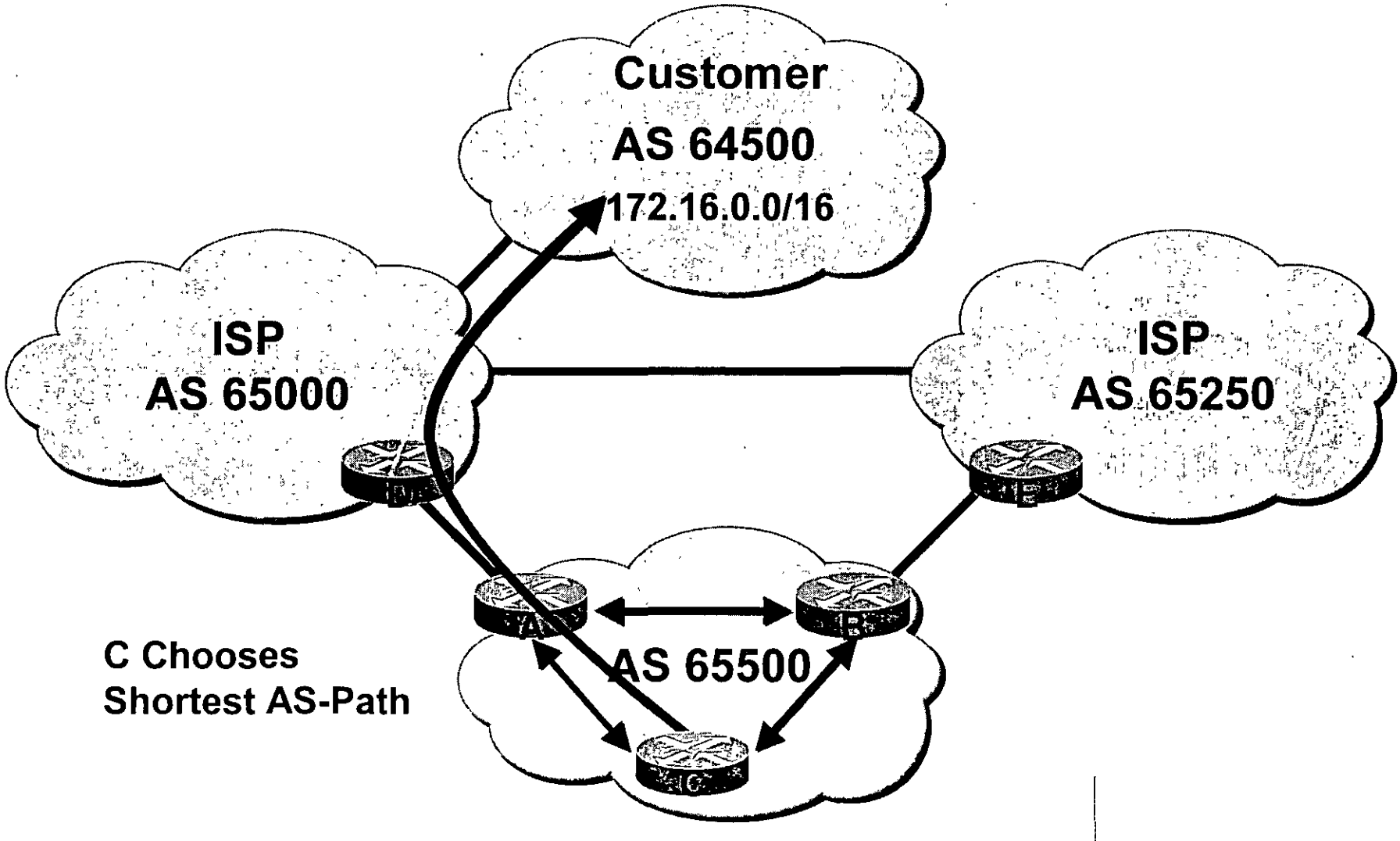
Default Routes from All Providers Example



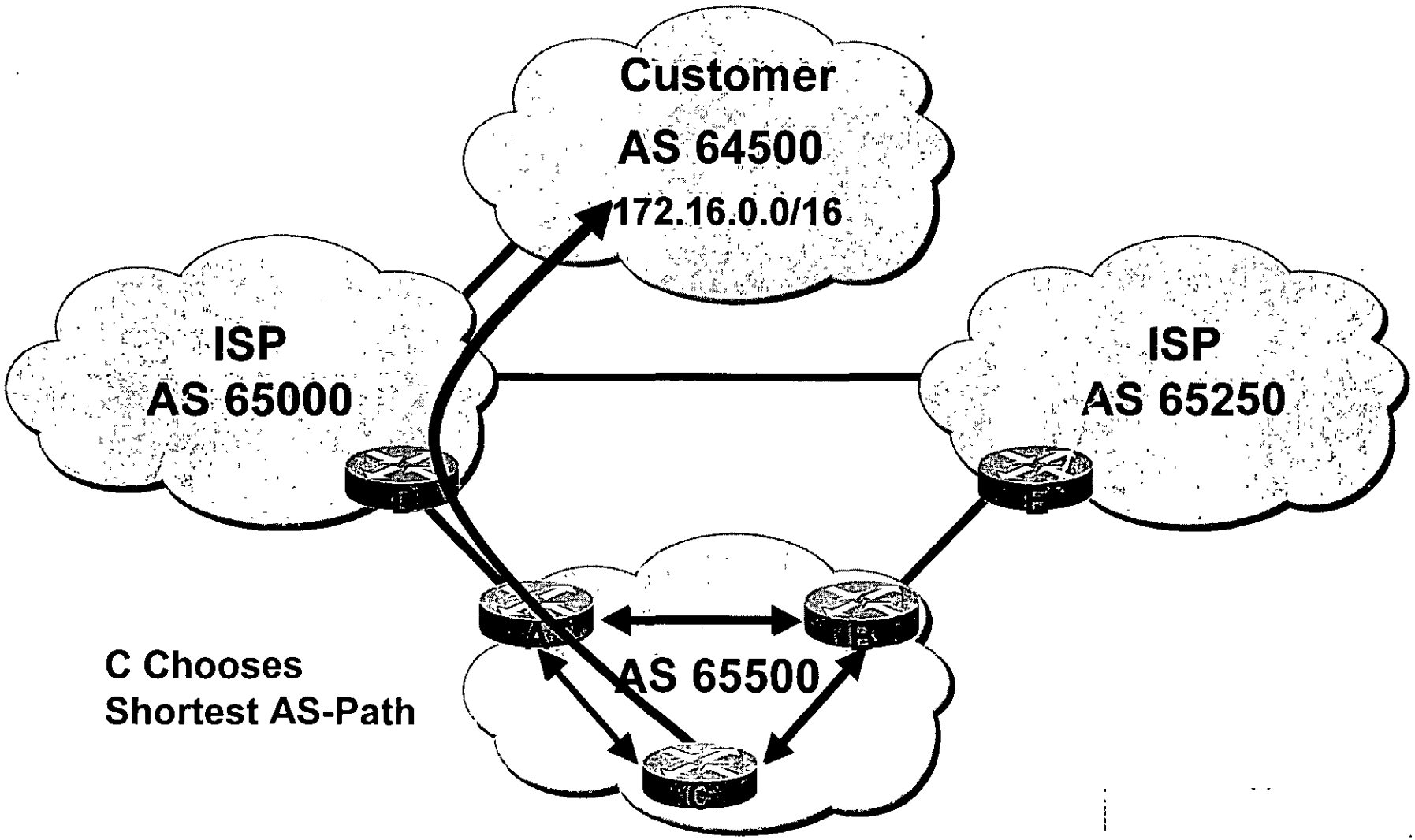
Customer and Default Routes from All Providers

- Medium memory and CPU usage
- Best path is usually shortest AS-path
- Can override path choice
- IGP metric to default route used for all other destinations

Customer and Default Routes from All Providers (cont.)



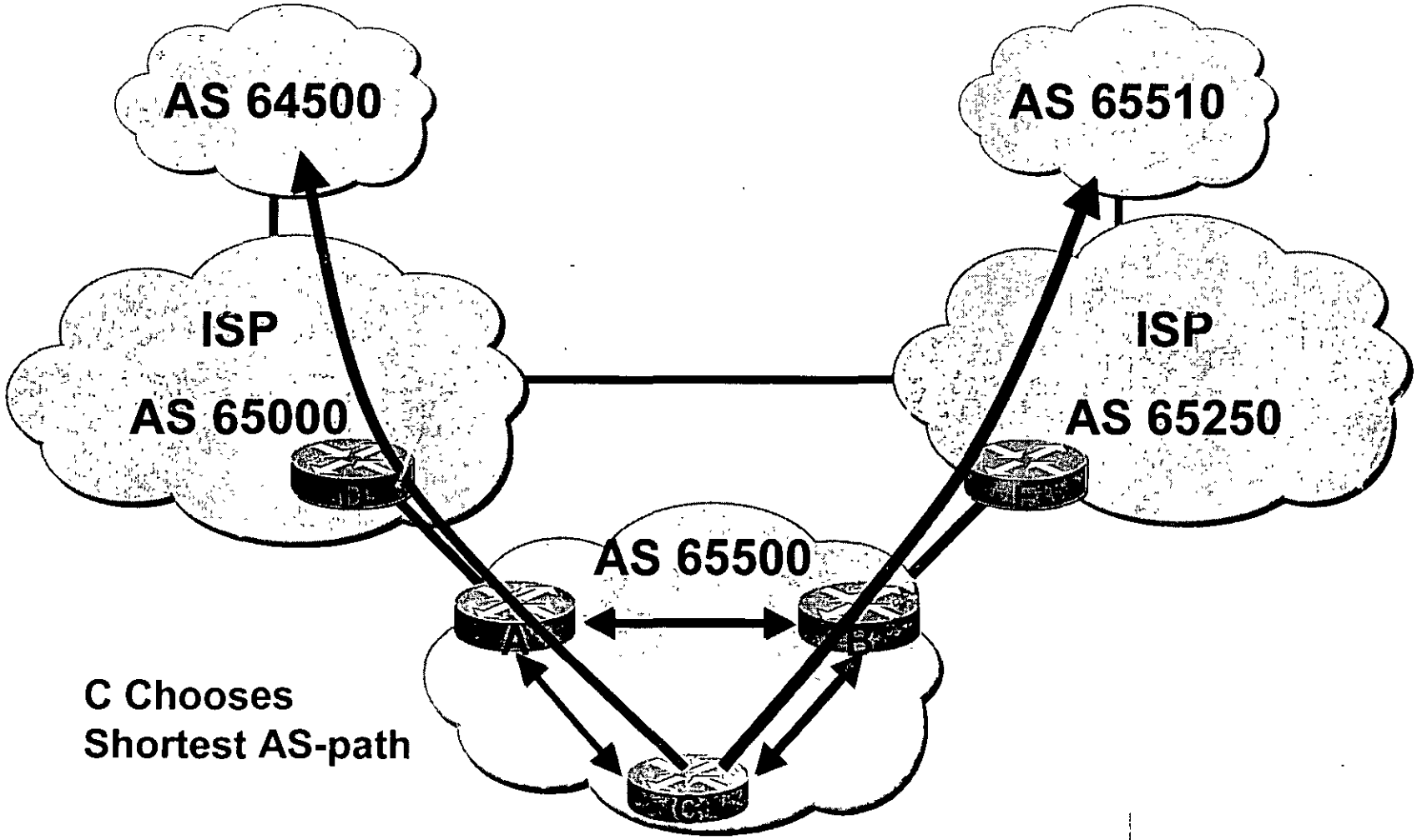
Customer and Default Routes from All Providers (cont.)



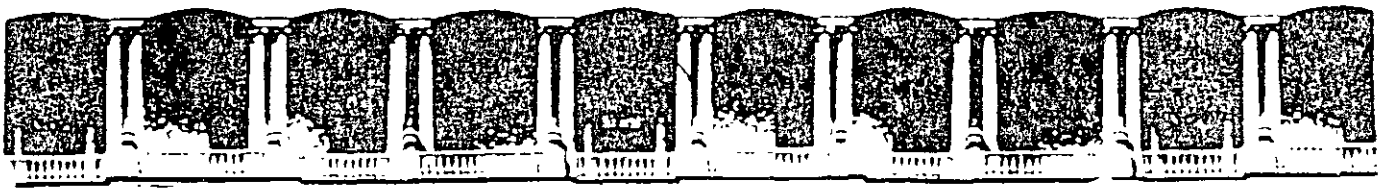
Full Routes from All Providers

- Higher memory and CPU usage
- Reach all destinations by best path
  - Usually shortest AS-path
- Can still manually tune path choice

Full Routes from All Providers (cont.)



Gracias



FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA
Tres décadas de orgullosa excelencia 1971 - 2001

CURSOS ABIERTOS

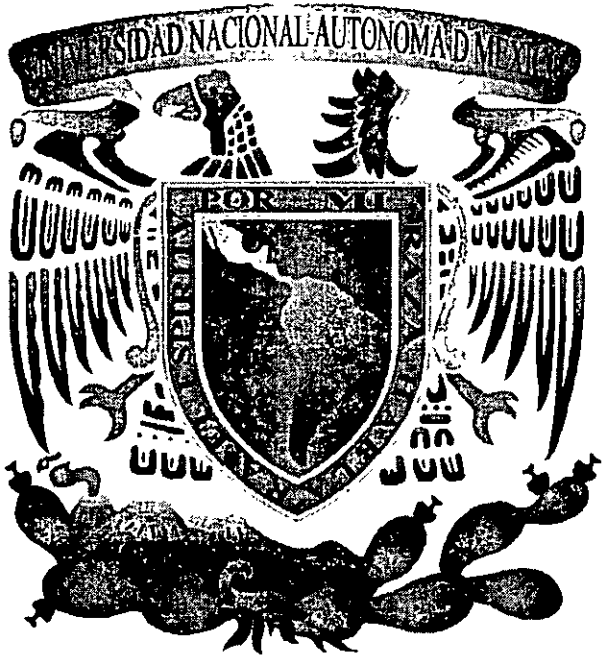
DIPLOMADO INTERNACIONAL EN TELECOMUNICACIONES

MODULO IV: REDES DIGITALES: ACTUALIDAD Y PERSPECTIVAS

TEMA

VLANs Y LAN Emulation

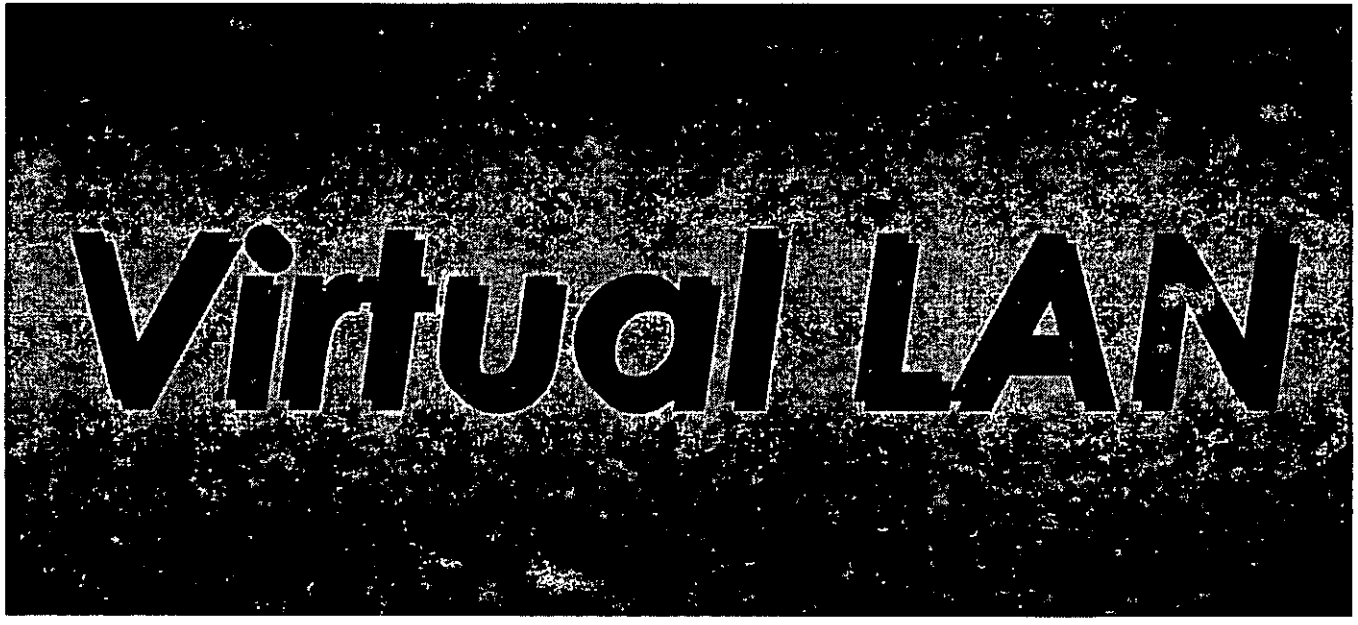
EXPOSITOR: ING. JAVIER LIMON GOMEZ
PALACIO DE MINERIA
JUNIO 2001



6. VLANs y LAN Emulation

del 11 al 15 de junio de 2001

VLANs

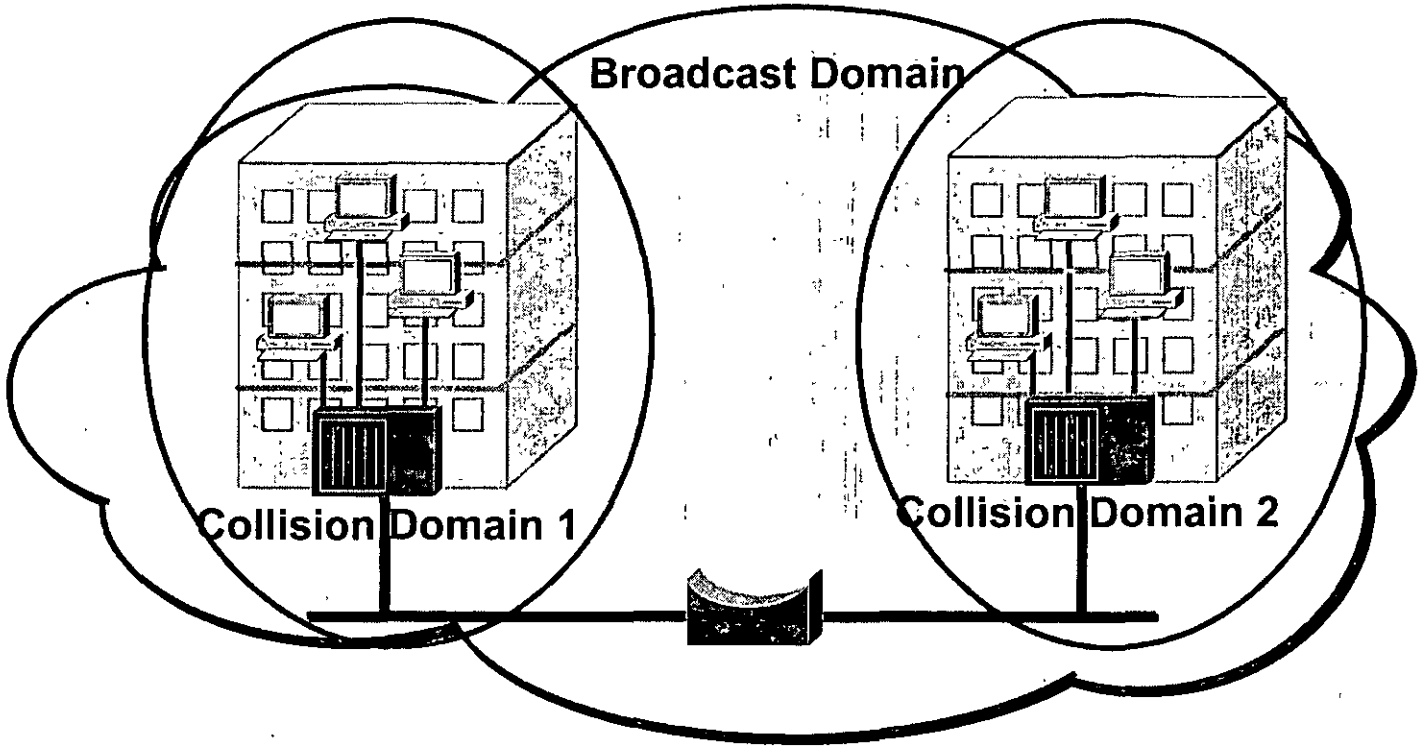


Objetivos

- ✓**Operación**
- ✓**Estándares**
- ✓**Consideraciones de diseño**

Campus de Red Tradicional

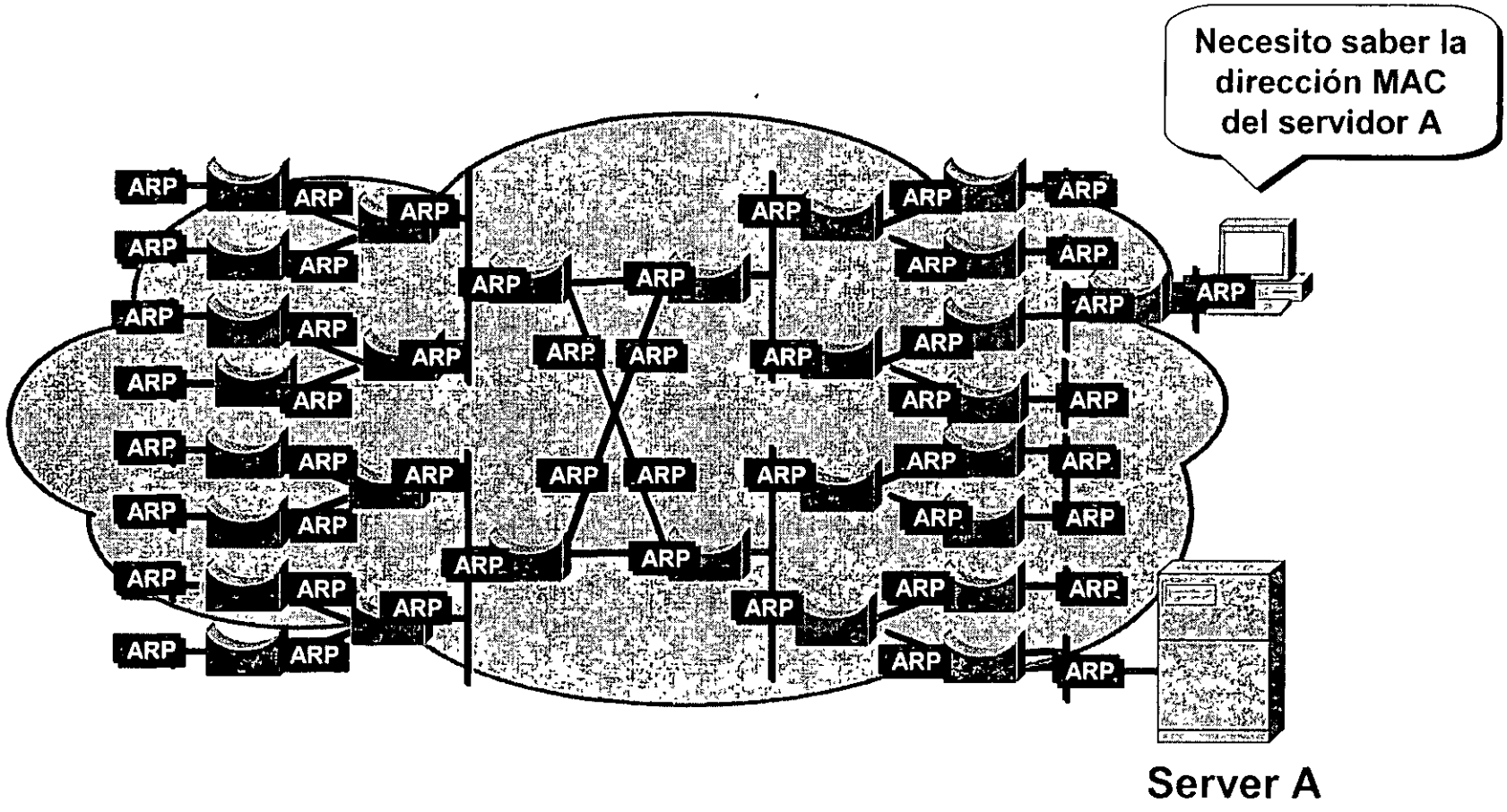
VLANs



- El bridge limita los dominios de colisiones

Interpretación de emisiones

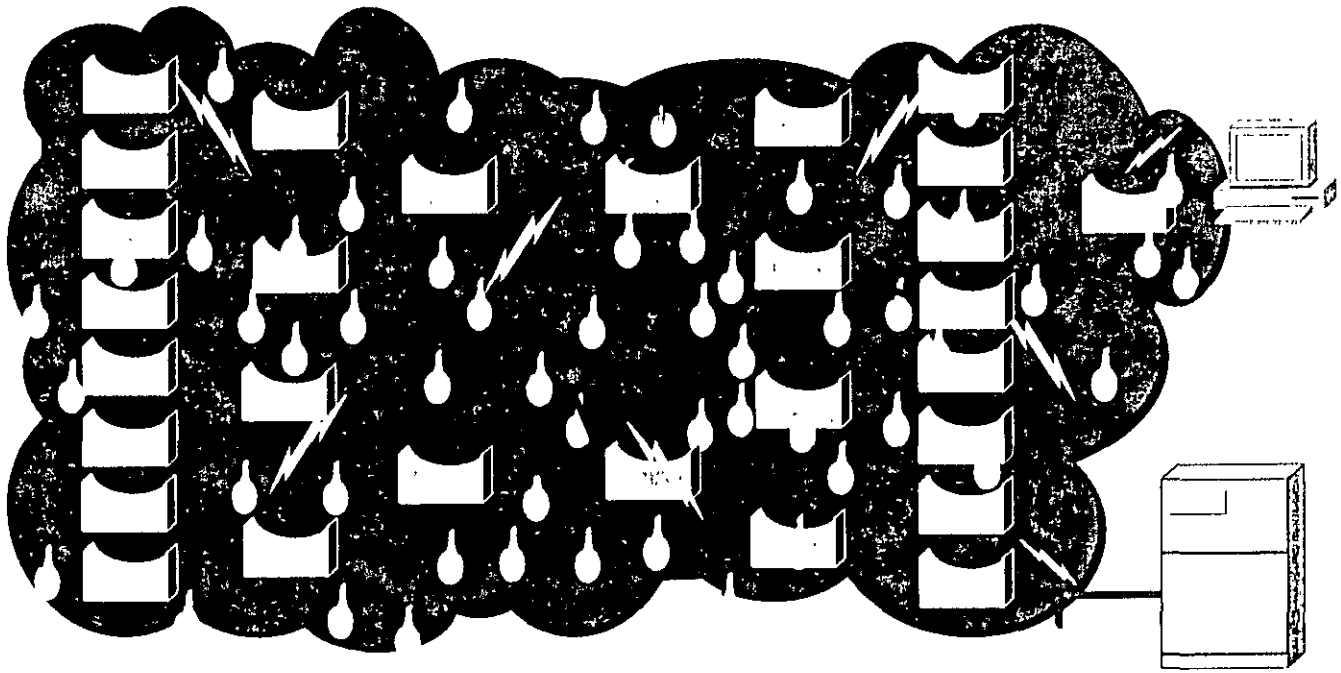
VLANs



- Multicast, broadcast y destinos desconocidos llegan a ser eventos globales.

Emisiones de Broadcast

VLANs

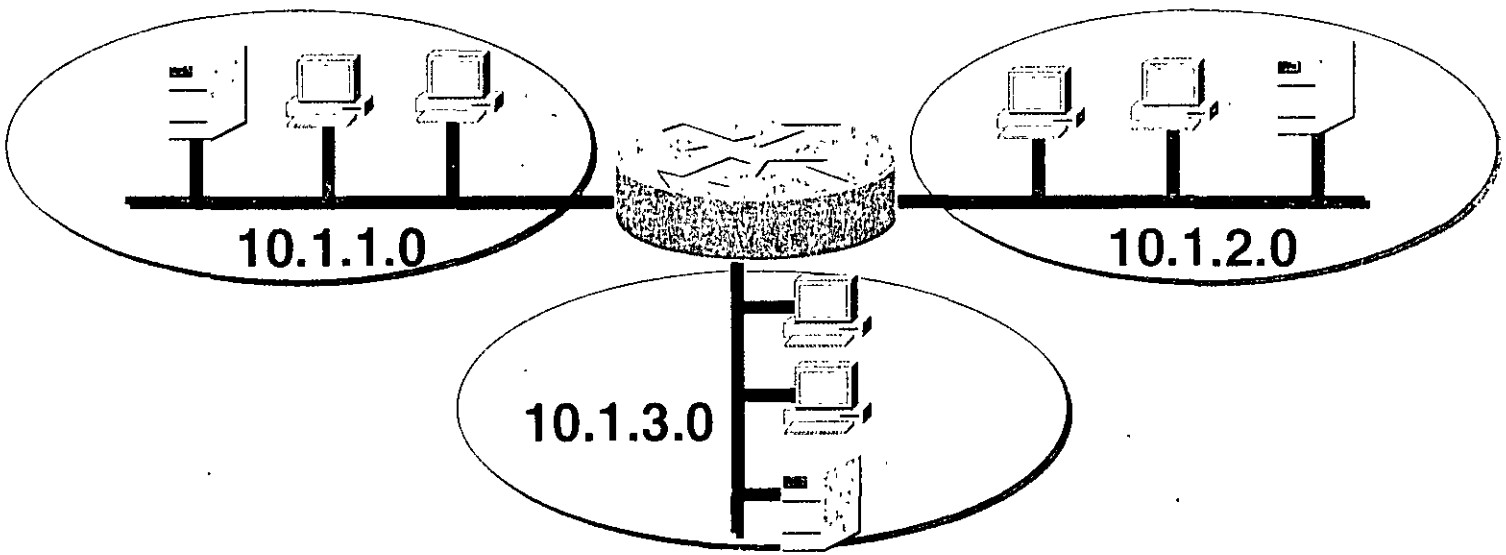


Los broadcasts pueden consumir el ancho de banda disponible

Cada dispositivo debe decodificar el frame de broadcast.

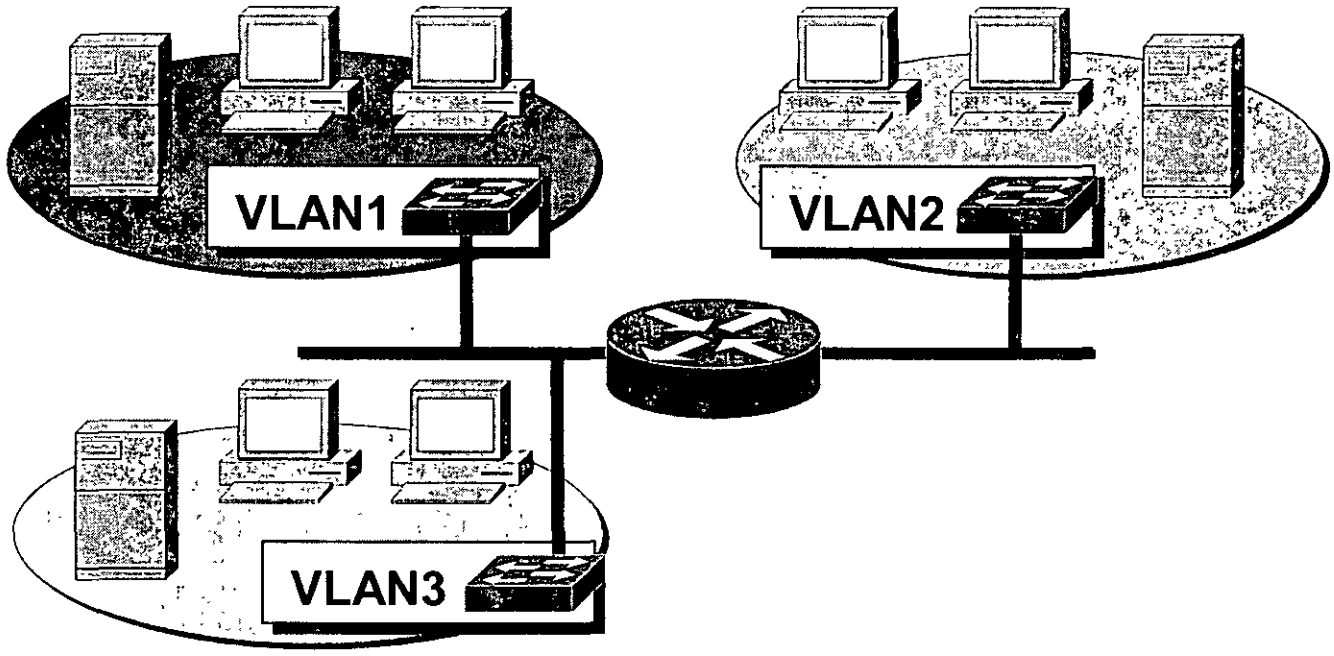
Solución: Regionalizar Tráfico

VLANs



Los broadcasts de LAN terminan en las interfaces del enrutador

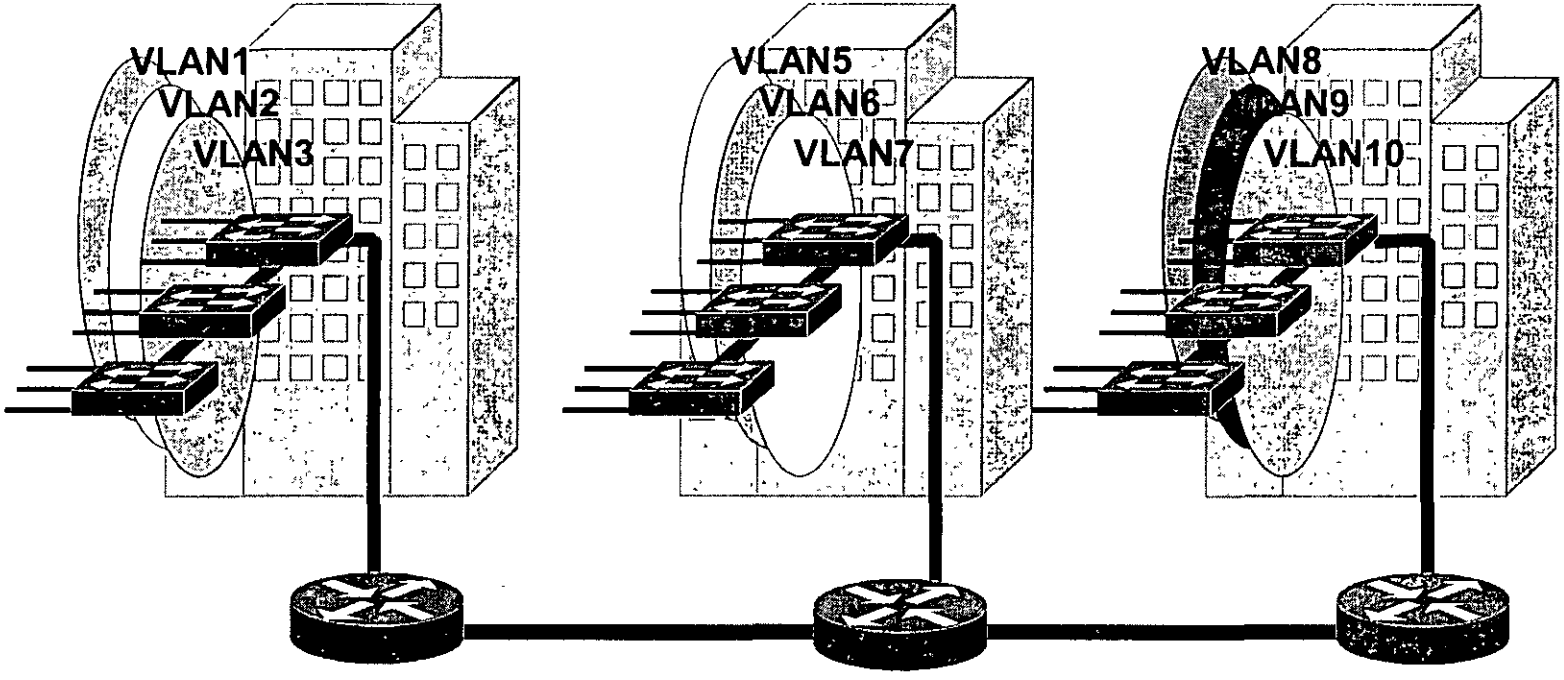
Solución: Regionalizar Tráfico(Cont.) *VLANs*



Las VLANs limitan el tráfico de broadcast y separa el flujo de tráfico.

Campus Actual de Redes

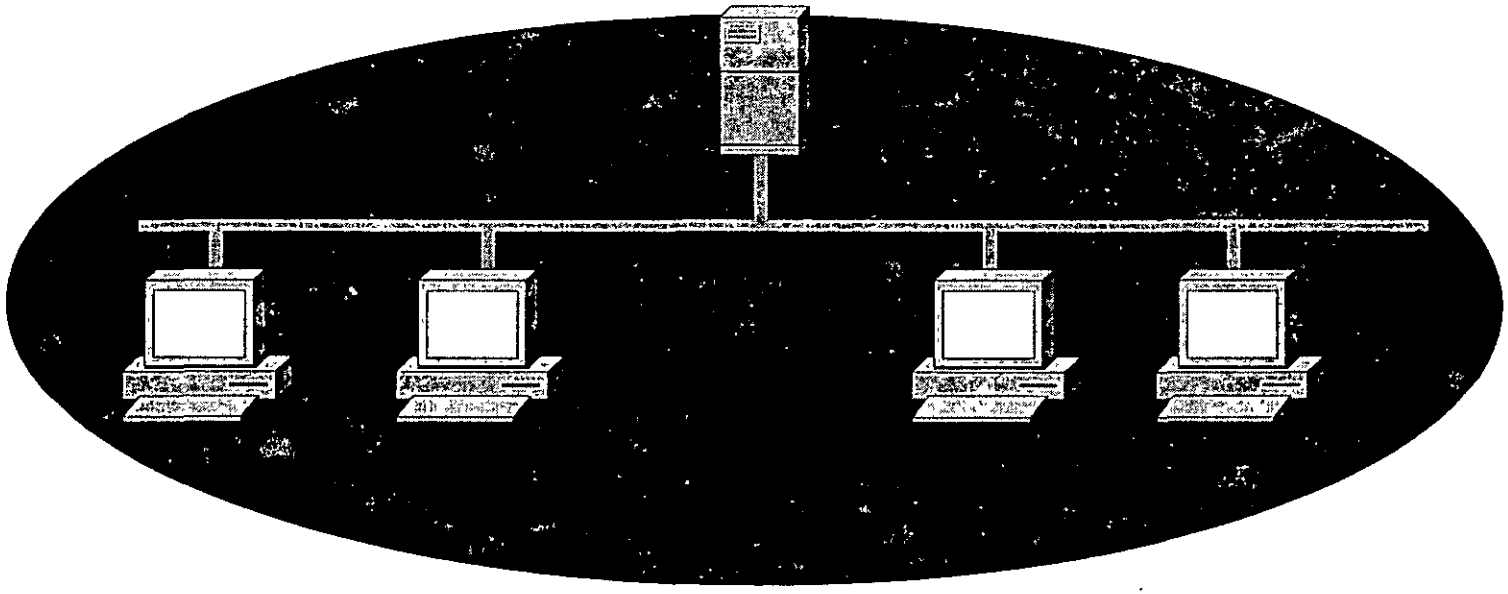
VLANs



- **Los dispositivos de capa 3 interconectan los segmentos LAN, limitando los dominios de broadcast.**

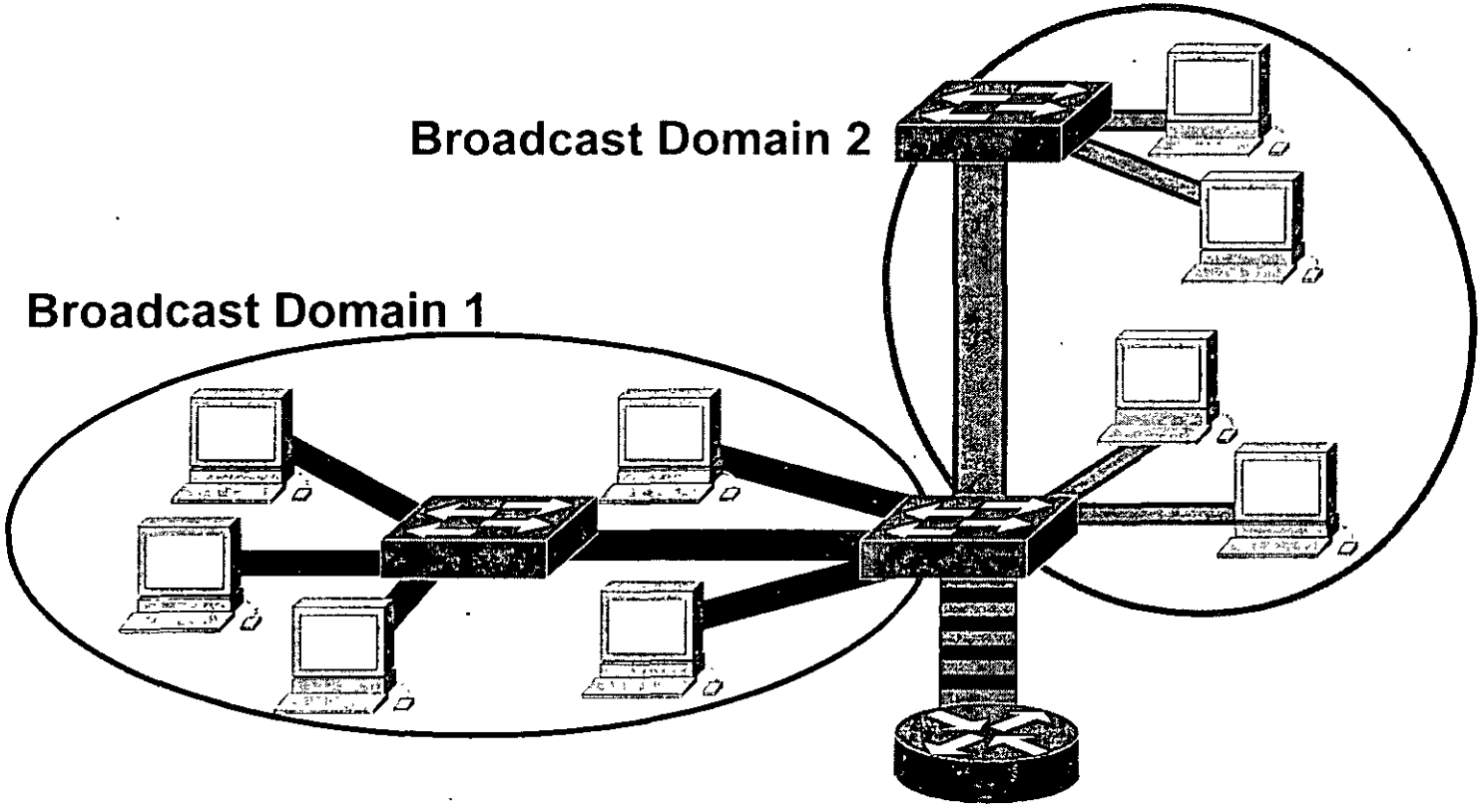
¿Qué es una VLAN ó Virtual LAN?

VLANs



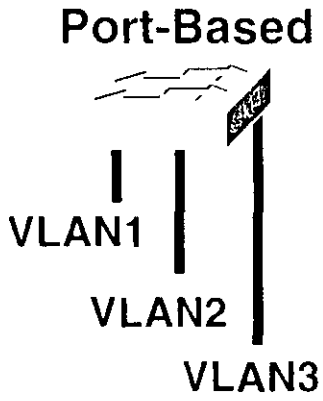
- **Una VLAN es un dominio de broadcast.**
- **Una VLAN es una red conmutada, segmentada lógicamente de acuerdo a funciones, proyectos o aplicaciones independientemente de la localización física de los usuarios.**

Las VLANs establecen los dominios de broadcast

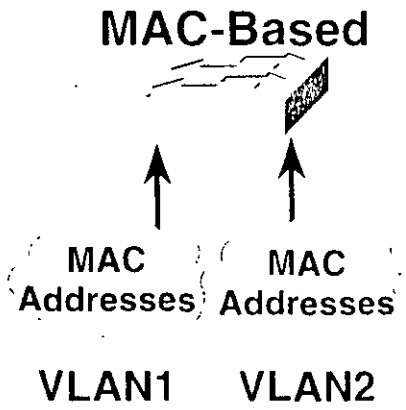


Las VLANs y los routers limitan los broadcast al dominio de origen

Estableciendo la membresía dentro de la VLAN



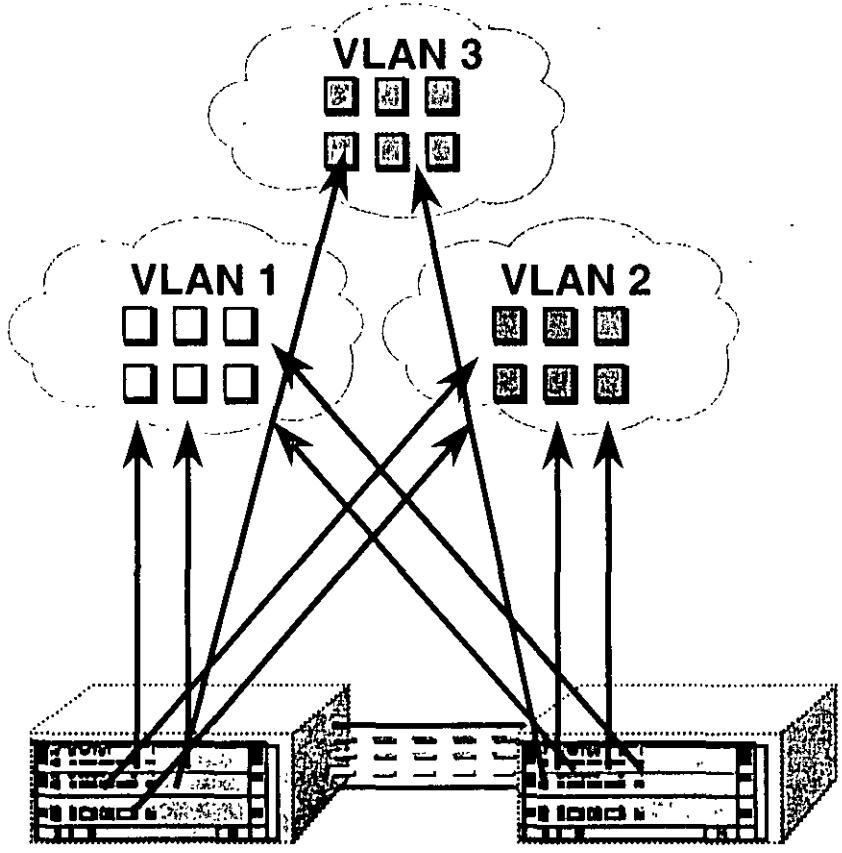
Port-Driven



MAC Address Driven (Layer 2)

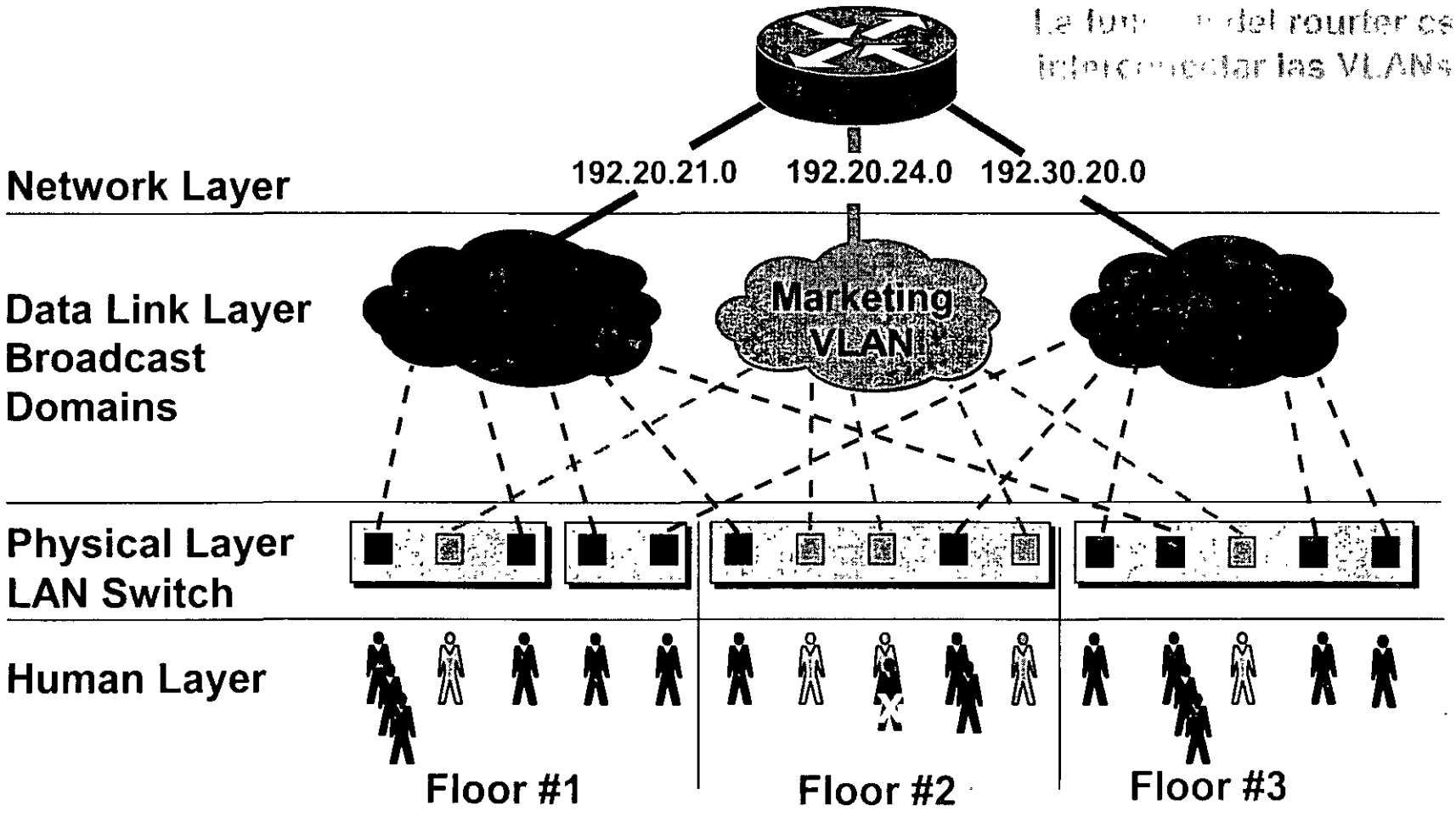
La membresía dentro de la VLAN puede ser estática ó dinámica

Membresía por Puerto



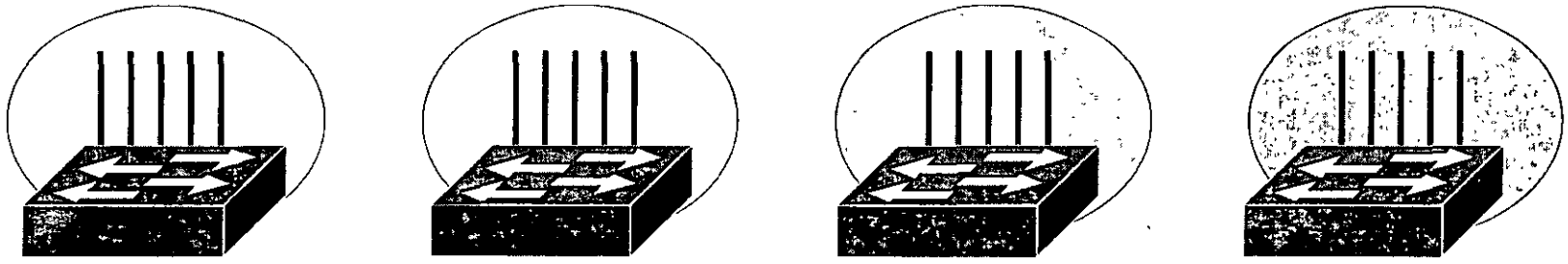
Configurando VLANs Estáticas

La función del router es interconectar las VLANs



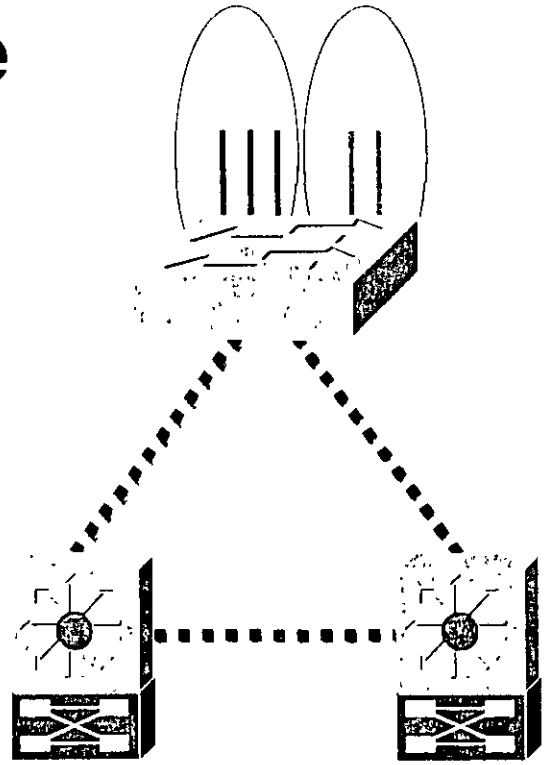
- Todos los usuarios conectados en el mismo puerto del switch, pertenecen a la misma VLAN

Enlace de acceso



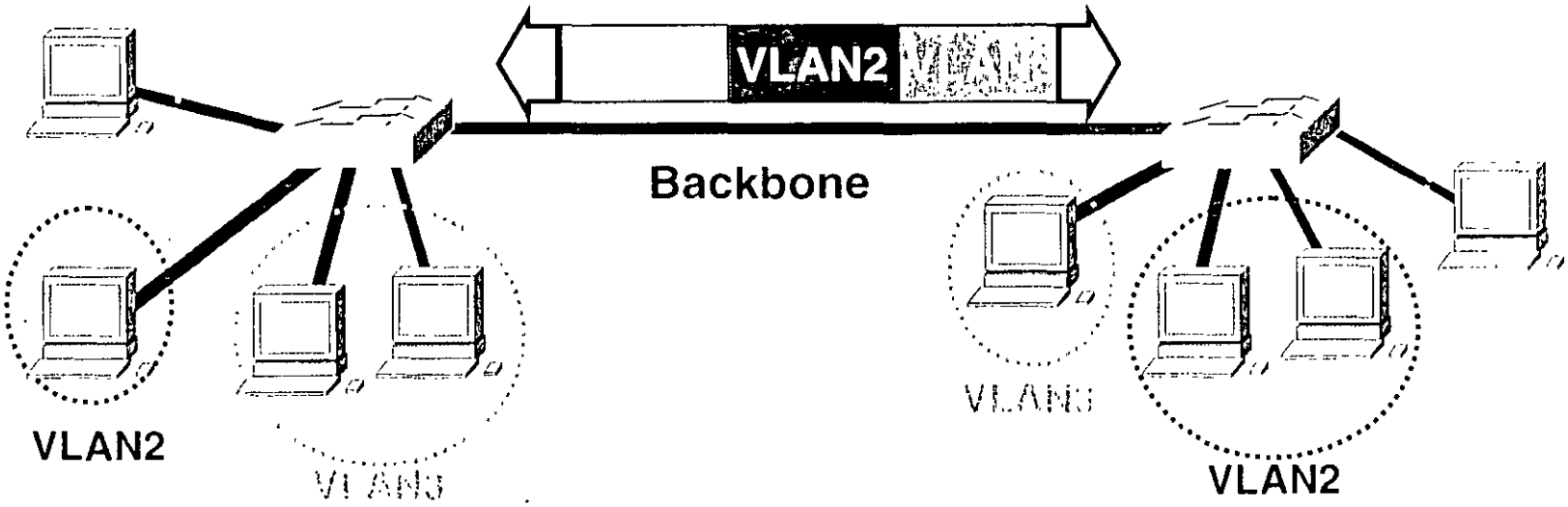
- Un enlace de acceso es un enlace el cual es miembro de una sola VLAN

Enlaces de troncal



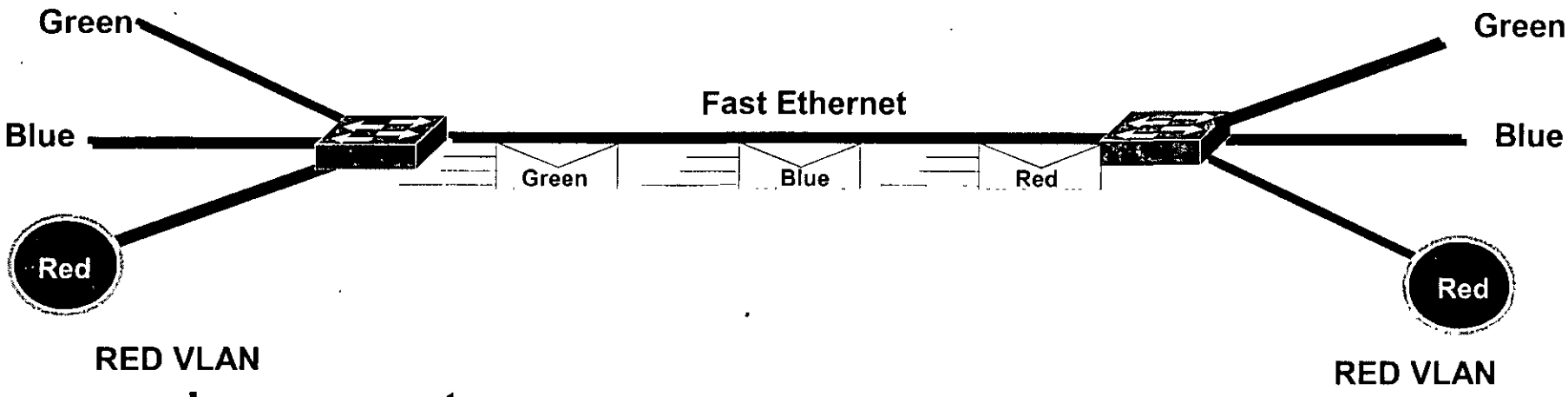
Un enlace de troncal es capaz de transportar múltiples VLANs

Identificación de VLANs



- Especificamente desarollado para multi-VLAN, comunicación interna entre switches
- Dentro del encabezado de cada frame es el único lugar de identificación
- Función de capa 2

Métodos de Identicación de VLANs *VLANs*



- Los paquetes cruzan
- Packets traversing a shared backbone carry VLAN identification within the packet header

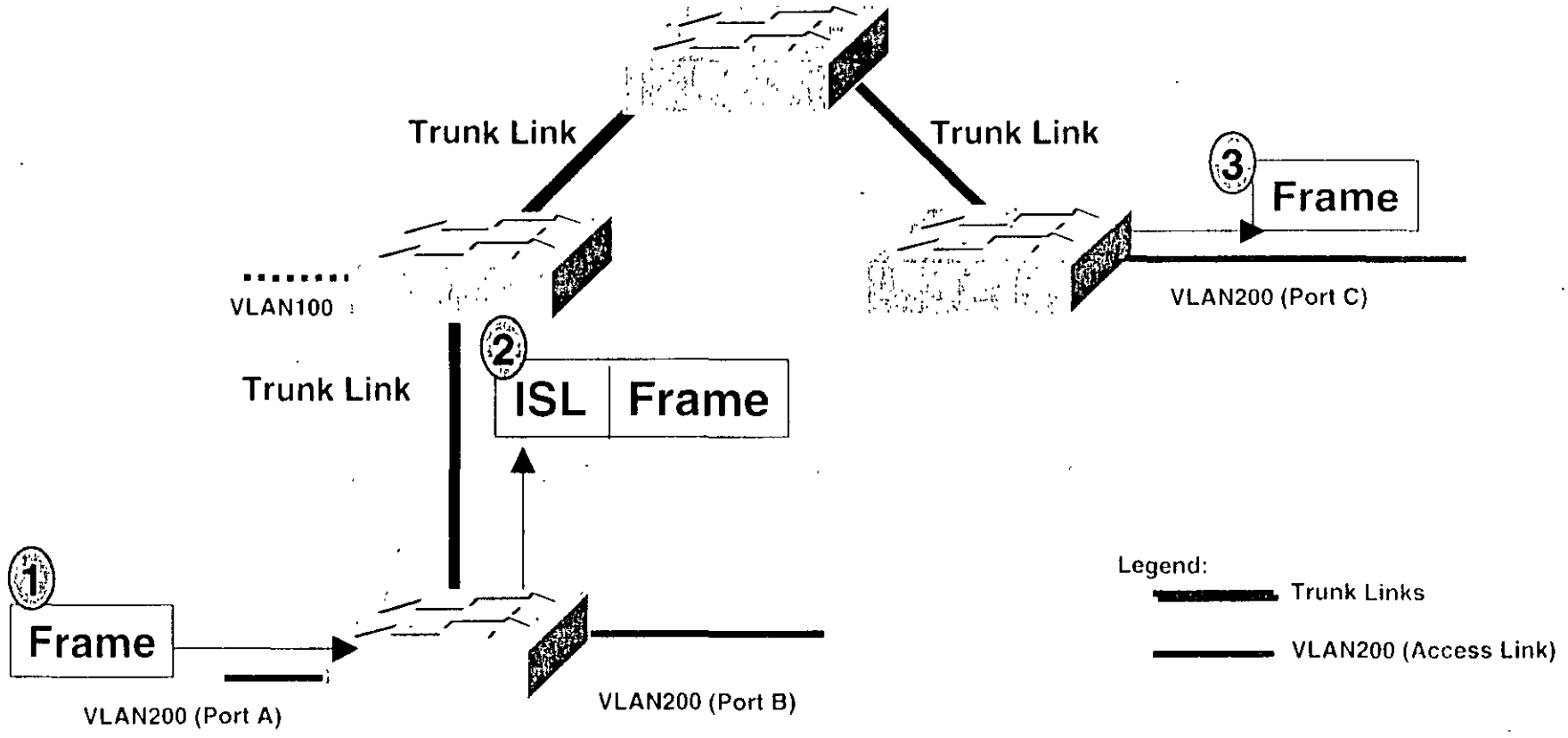
VLAN Identification Options:

IEEE 802.1Q (Frame tagging)

Cisco ISL (Inter-Switch Link)

Cisco 802.10 (FDDI)

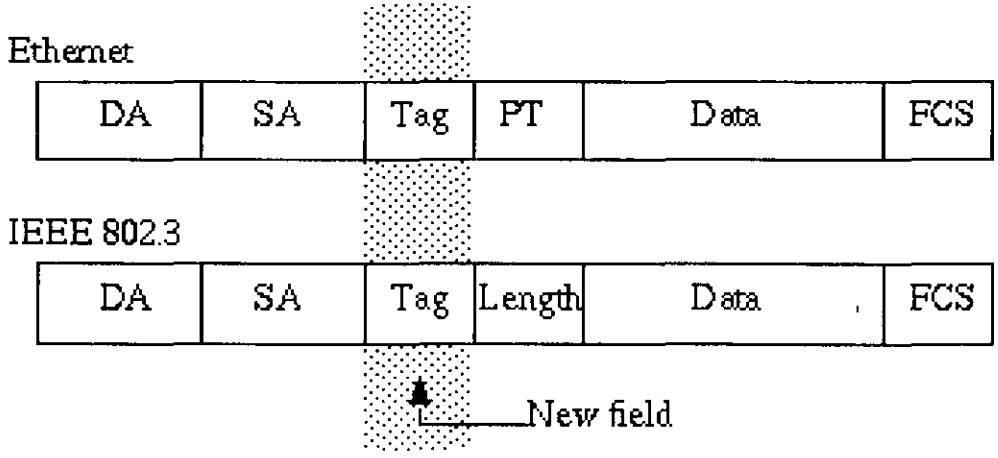
Identificación de VLAN usando ISL



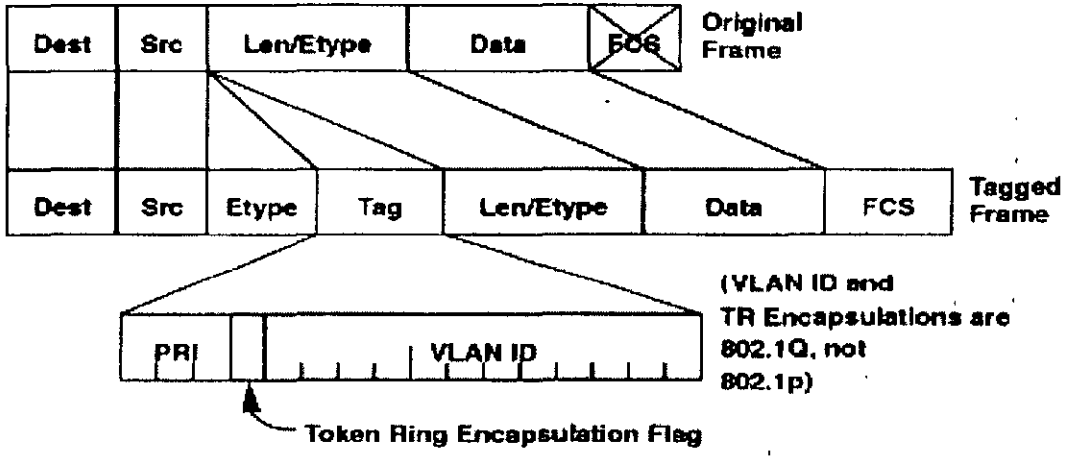
ISL contiene la Información de las VLAN, así como los frames que circulan entre los switches, dentro de los enlaces de troncal

Identificación de VLANs usando IEEE 802.1Q

El nombre oficial de IEEE 802.1Q es *Standard for Virtual Bridged Local Area Networks*



Identificación de VLANs usando IEEE 802.1Q (Con.)



IEEE802.1Q consta de:

2-bytes de etiqueta de indentificación del protocolo (TPID)

Con un valor fijo de 0x8100. Este valor TPID indica que el frame transporta la etiqueta de información 802.1Q/802.1p

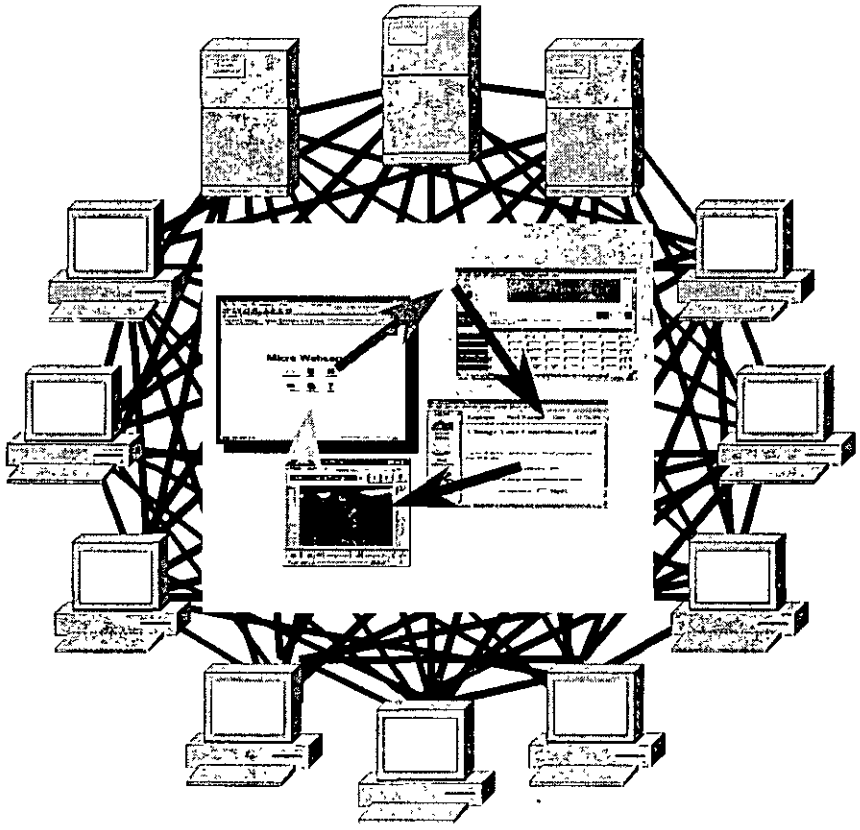
2-bytes de etiqueta de control de información (TCI)

3 bit user priority

1 bit canonical format (CFI Indicator)

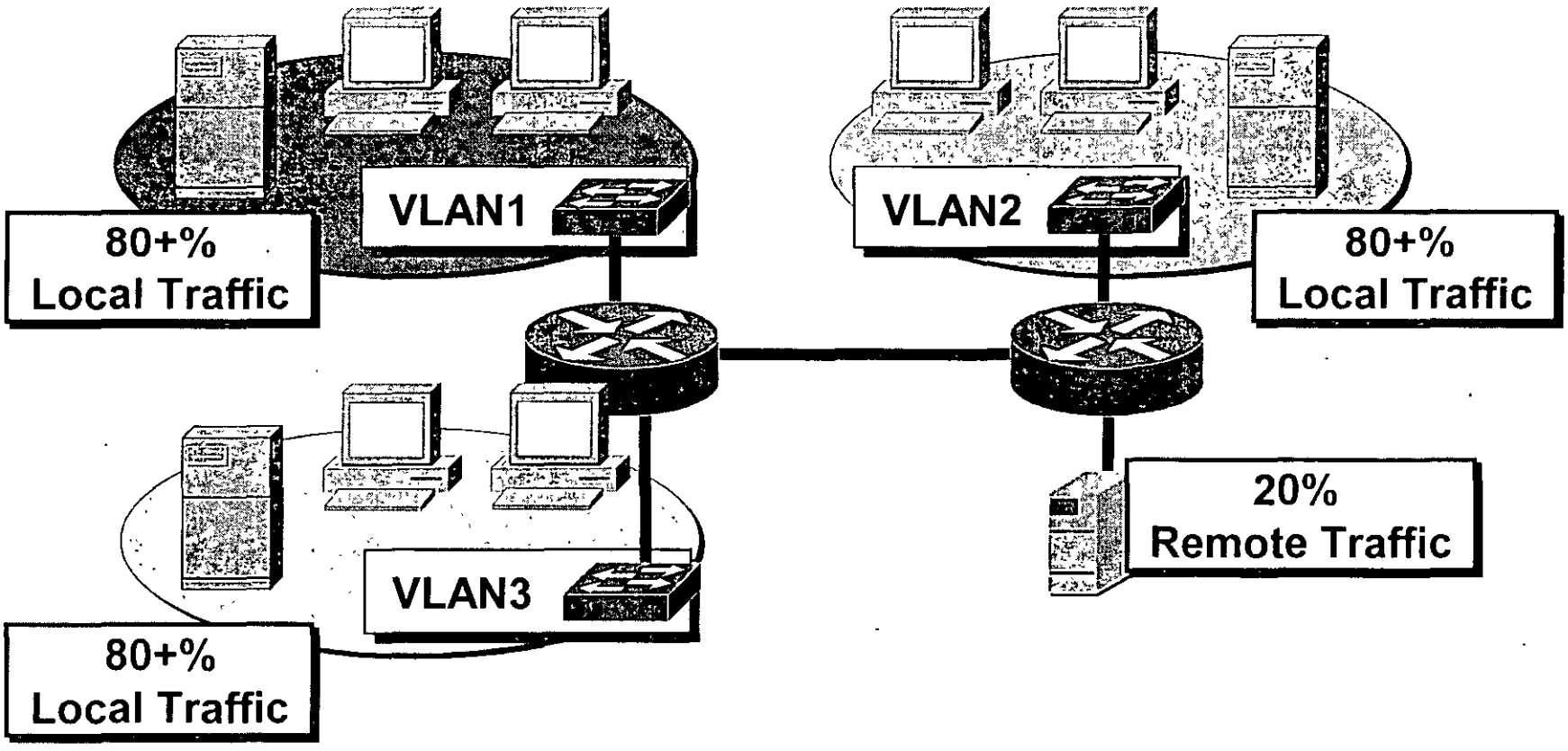
12 bits VLAN Identifier (VID)

Comprendiendo los Patrones de Tráfico



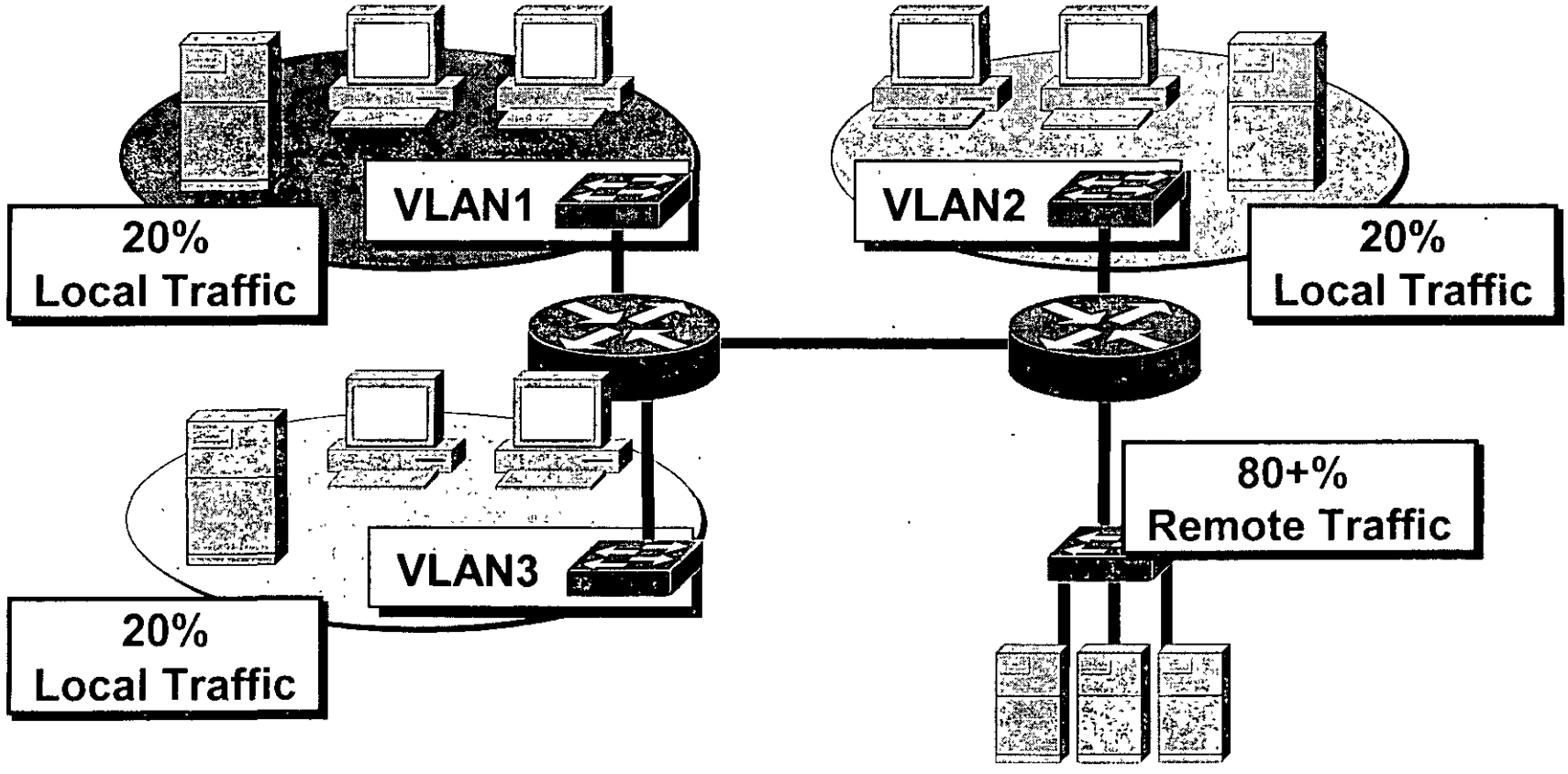
- **La implementación de una red exitosa considera los patrones de tráfico**

La Regla 80/20



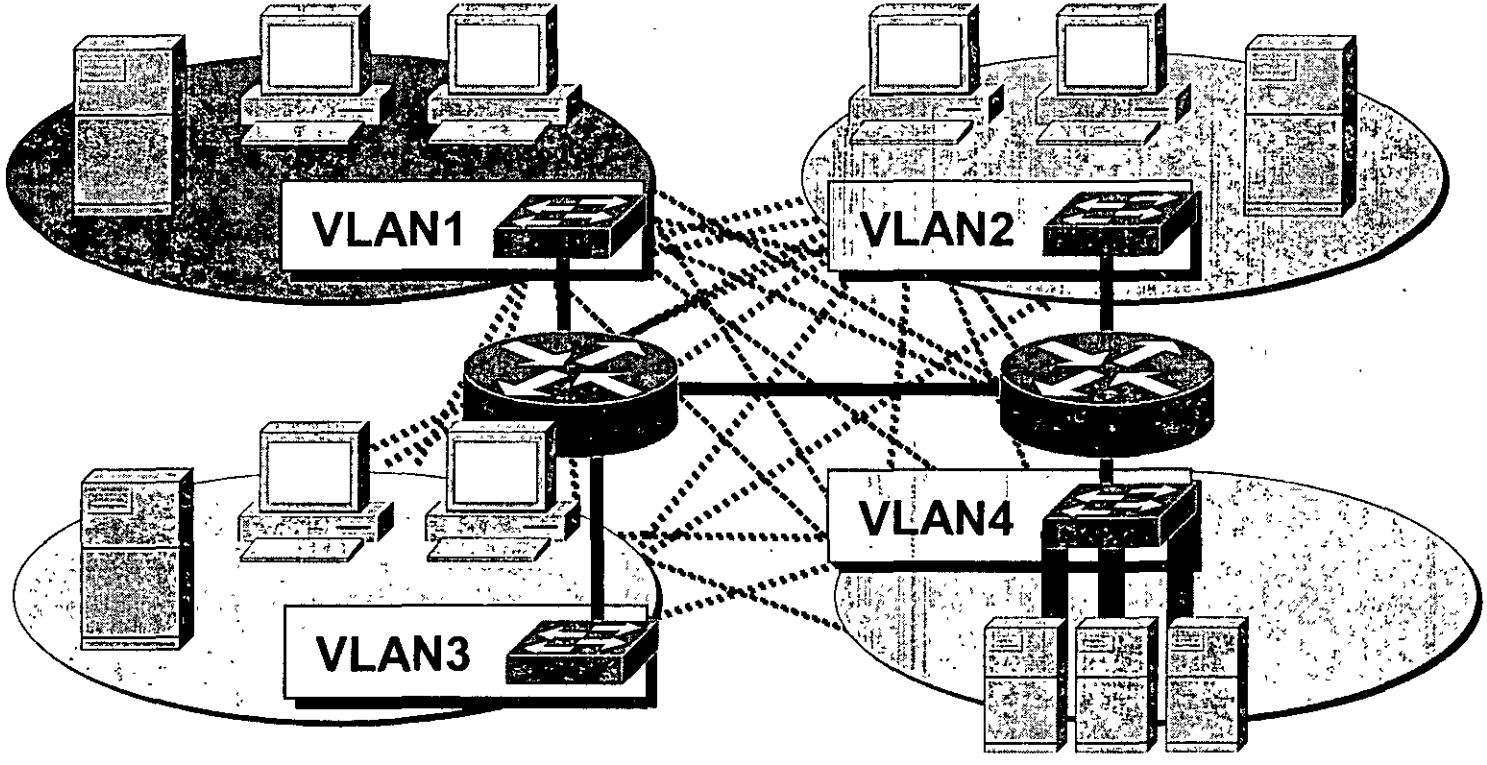
- 80 porciento del tráfico es local y el 20 porciento es remoto

La Nueva Regla 20/80



20 porciento del tráfico es local y el 80 porciento es remoto

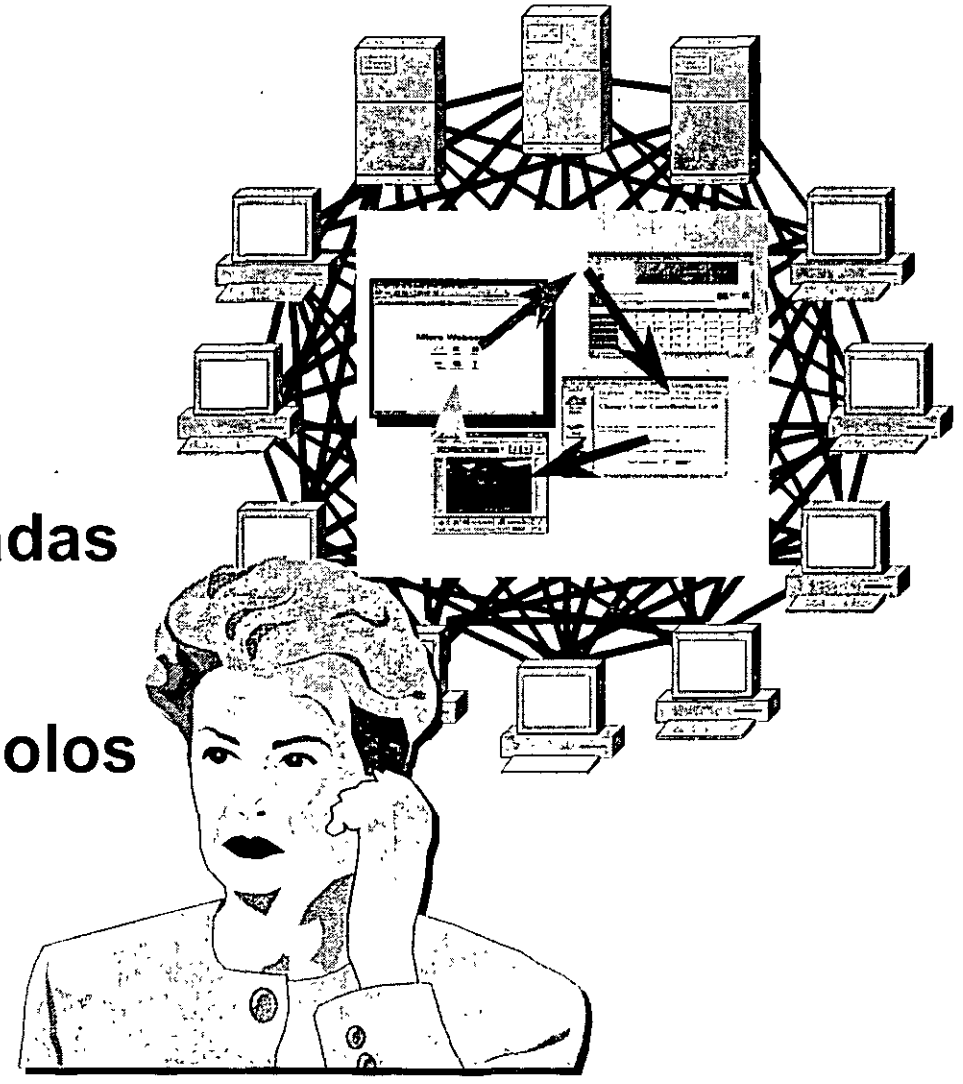
Emergen Patrones de Tráfico



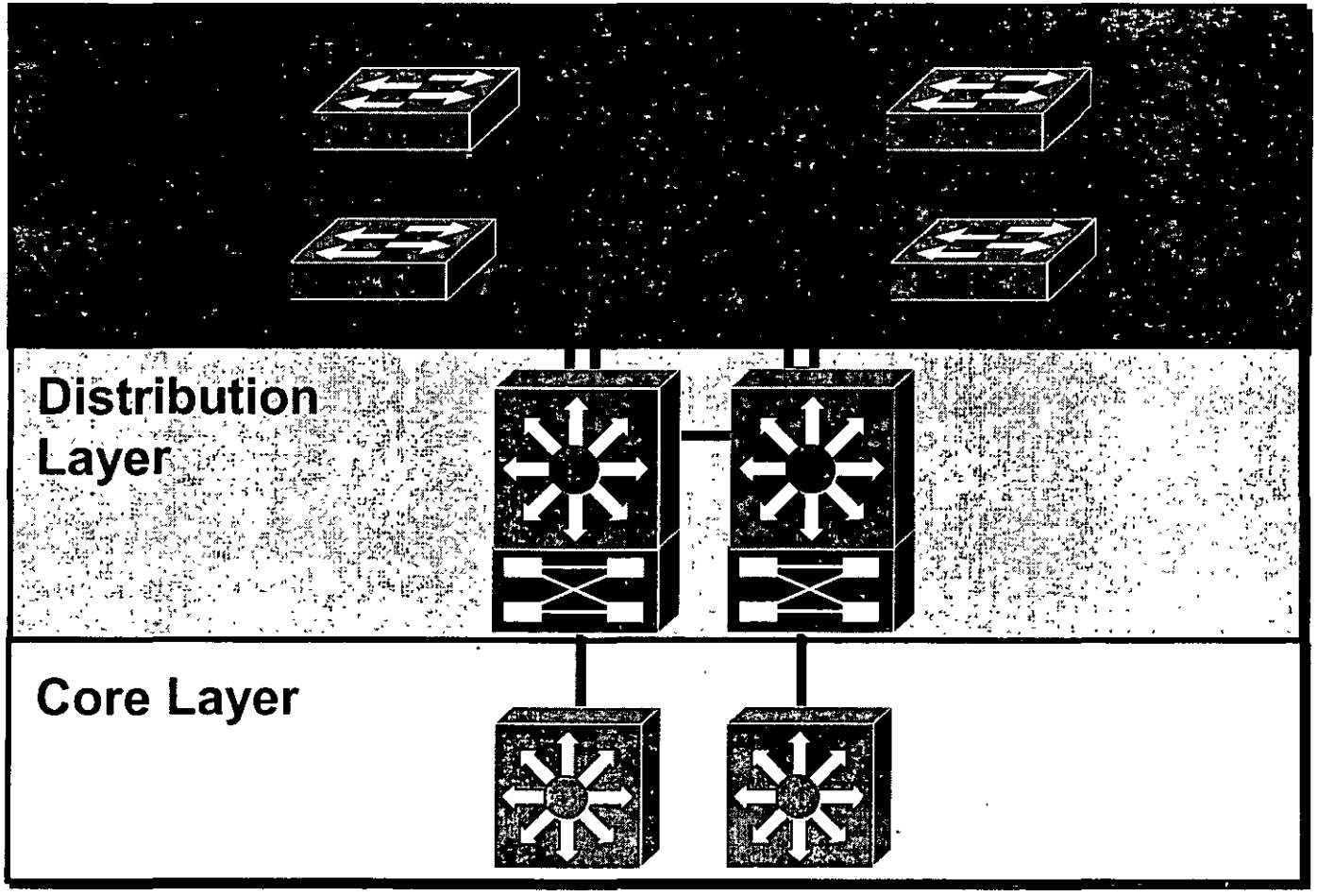
- **La regla 20/80 desafía la implementación de VLANs**

Requerimientos del Cliente

- Rápida convergencia
- Trayectos definidos
- Redundancia
- Escalabilidad
- Aplicaciones centralizadas
- La nueva regla 80/20
- Soporte de multiprotocolos
- Multicasting



El Modelo Jerárquico

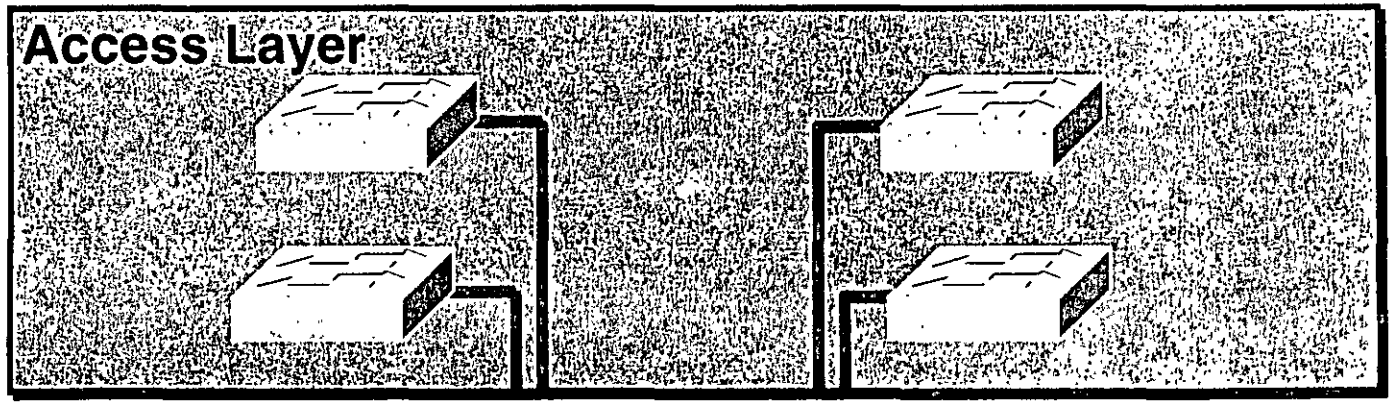


Punto de entrada a la red

Ancho de banda compartido

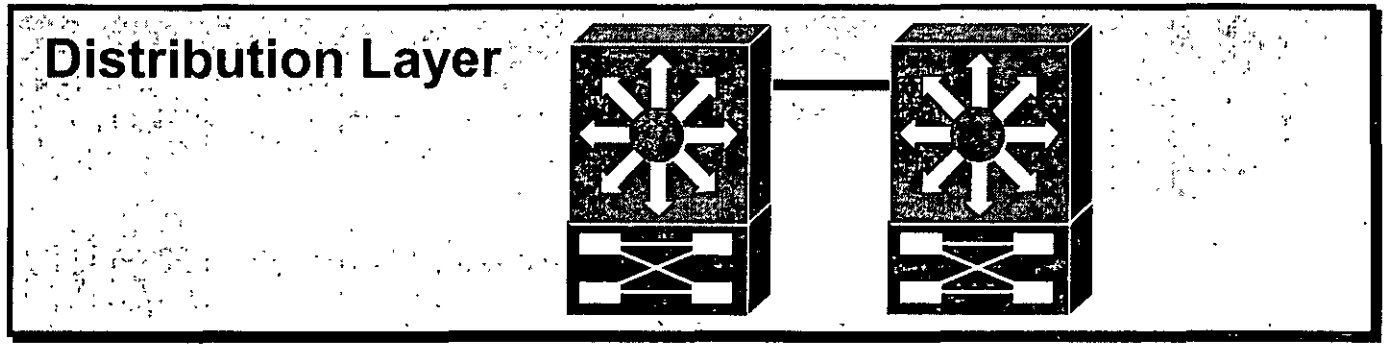
Servicios de capa 2

- **Filtros**
- **Membresía de VLAN**



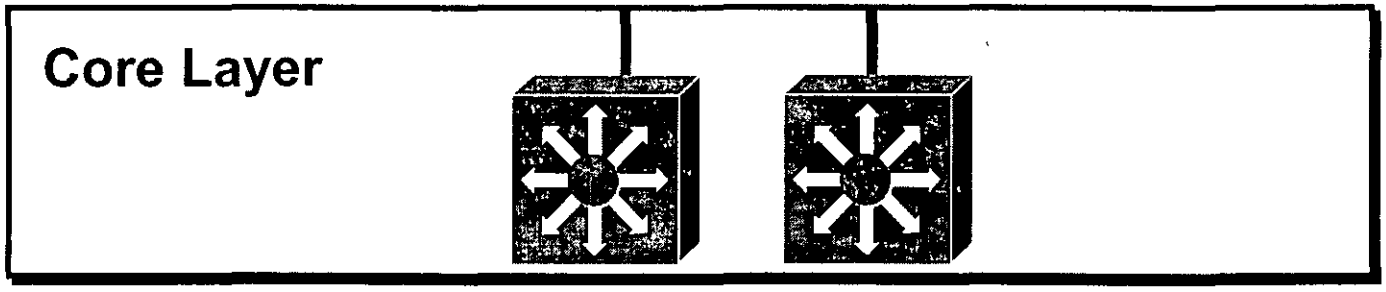
Capa de Distribución

- **Punto de agregación de accesos**
- **Acceso de servicios de Workgroup**
- **Definición de dominios de Broadcast**
- **Ruteo InterVLAN**
- **Traducción de medios**
- **Seguridad**

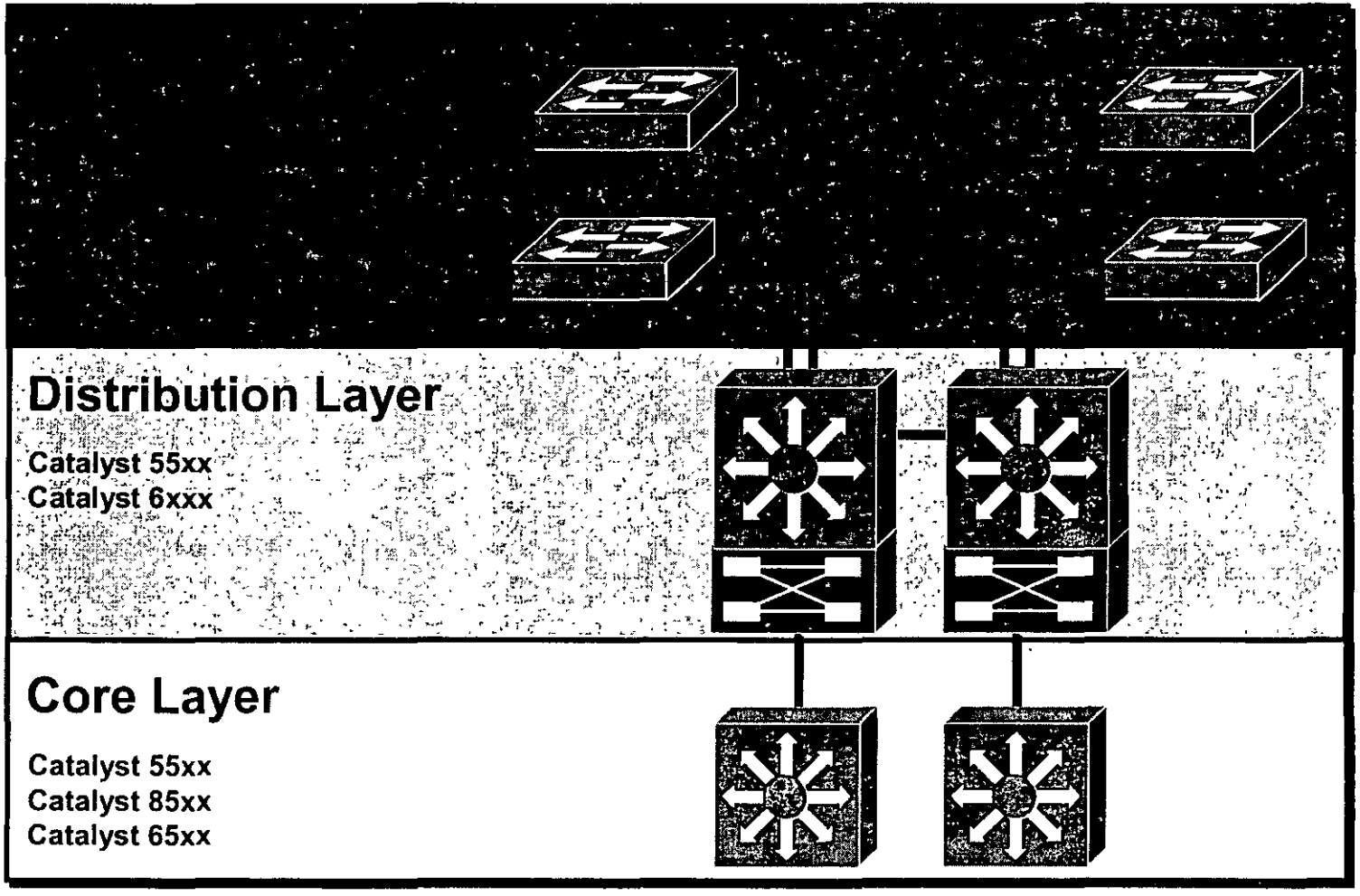


La Capa de Core

- **Transporte rápido**
- **No se procesa capa 3**

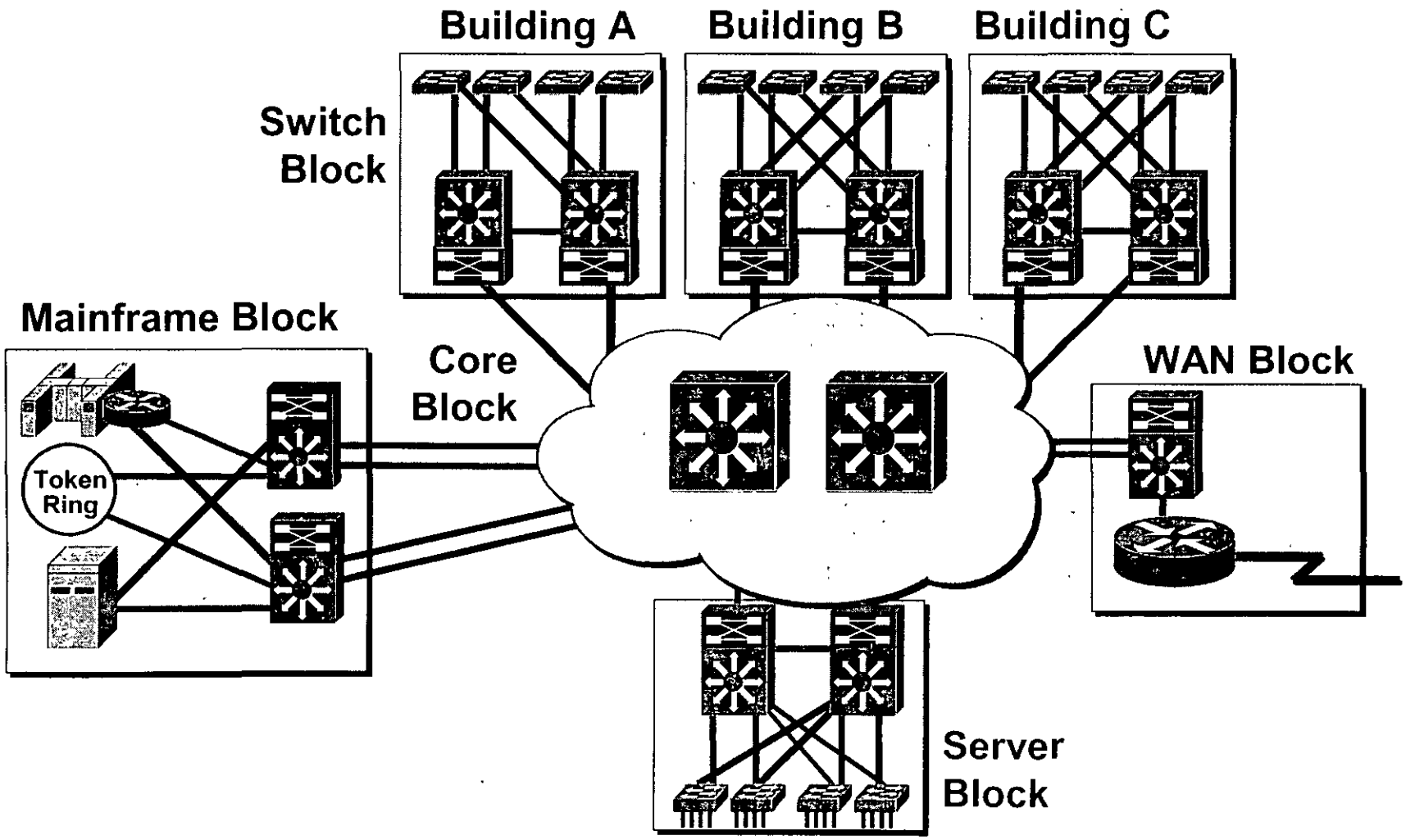


Selección Cisco por Capa



Implementación por Edificio

VLANs



Concentradores Vs. Switches

Diferencias técnicas y económicas

¿Qué es un Concentrador?

- **Un dispositivo con "n" puertos en el que todos los puertos estan interconectados entre sí (en paralelo).**
- **Un concentrador repite en todos sus puertos lo que recibe en uno de ellos.**
- **Funciona con CSMA/CD.**
- **El concentrador es completamente acorde al desarrollo teórico de Ethernet.**

Problemas con los Concentradores Ethernet

- **Los segmentos pueden soportar sólo 1024 estaciones MAC**
- **El protocolo fue diseñado para trabajar con tramas largas.**
- **El protocolo no funciona de forma óptima cuando trabaja con tramas cortas y tráfico elevado generado por las estaciones.**
- **Existen aplicaciones que consumen gran ancho de banda como la manipulación de gráficos, investigación genética, etc.**

- **Puede requerirse la separación no solo para fines técnicos, sino políticos.**
- **Puede haber un ambiente mixto en el que se tenga la necesidad de utilizar más de un protocolo de capa 2.**
- **Casos de TELMEX.**

Soluciones a los Problemas (pre switches)

- **Utilizar enrutadores para dividir el segmento.**
- **Microsegmentar las LANs para disminuir el tráfico.**
- **Utilizar "bridges".**
- **Utilizar Switches (a últimas fechas).**

Breve Historia de los Switches

- **1973 Primera implementación funcional de Ethernet.**
- **1981 10Base5.**
- **1990 10BaseT comercial.**
- **Finales de los 80s, primeros bridges para dividir segmentos.**
- **1991 Lanzamiento de Kalpana de los primeros switches y todas las monerías incluidas.**
- **1995 Cisco adquiere Kalpana y Grand Junction Networks.**

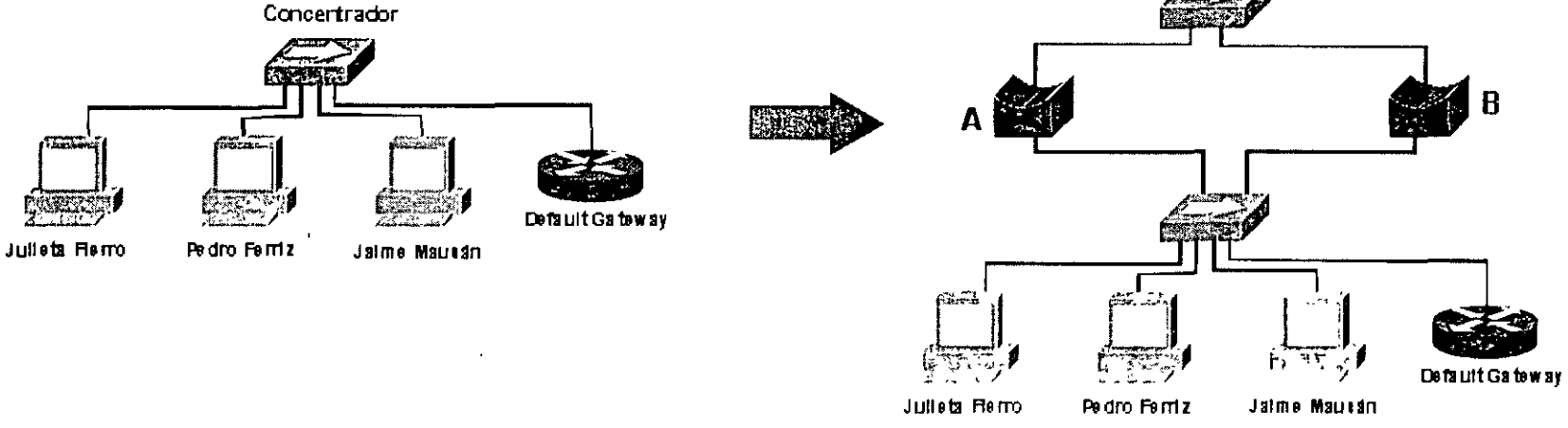
Problemas de los Concentradores

- **Cuando se emplean concentradores el medio es compartido por todos los elementos conectados en el segmento.**
- **No se pueden realizar "loops" (aun cuando fueran deseables).**
- **El número de equipos que se pueden "poner en cascada" está limitado por el mismo protocolo Ethernet.**

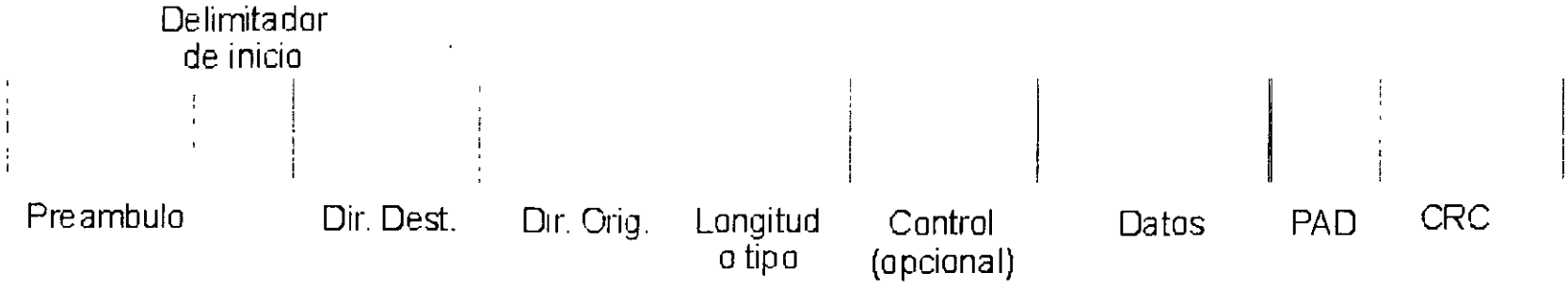
Problemas de los Bridges

- **Las primeras implementaciones comerciales descubrieron el "loop eterno".**
- **No se puede establecer loop de ninguna forma.**
- **Un bridge es siempre más lento que un concentrador.**

Problemáticas de Bridges (detalle)

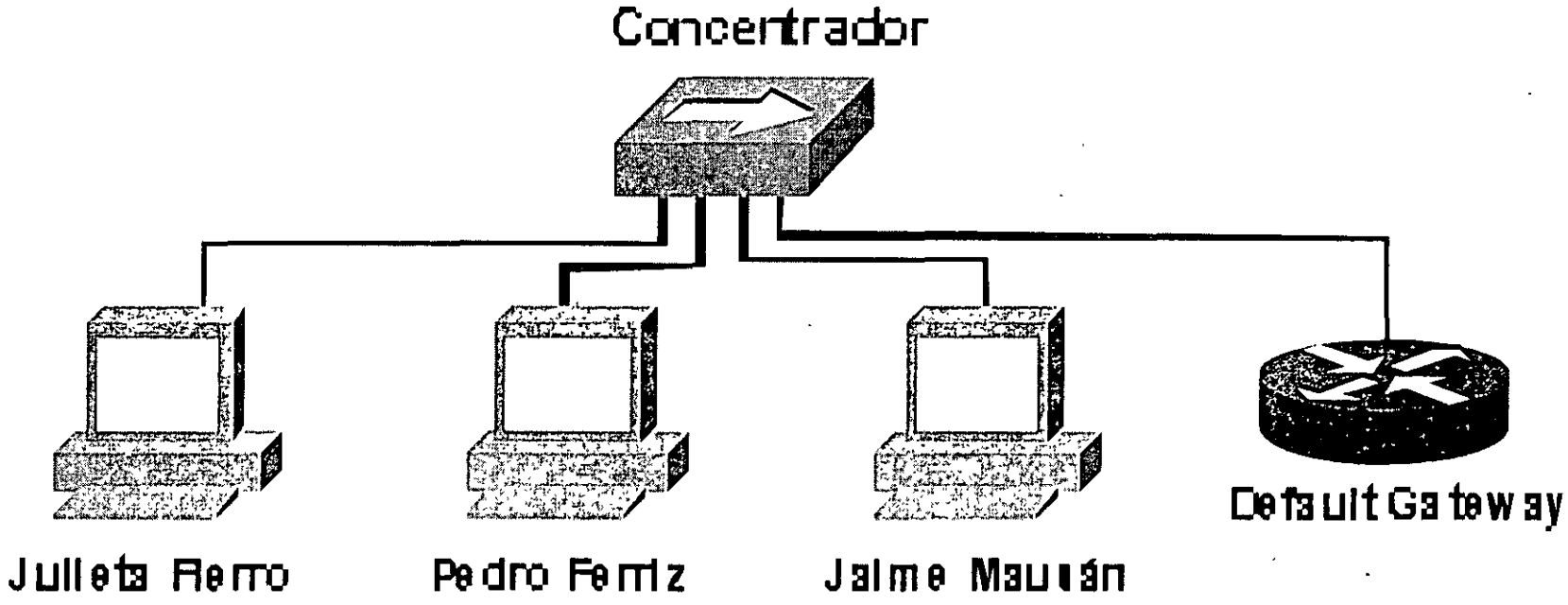


Trama Ethernet



- **Broadcast: Mal necesario.**
- **IP lo usa para la resolución ARP.**
- **En la antigüedad IPX lo empleaba casi para todo.**
- **Un broadcast es una dirección destino 0xFFFF.**
- **También existen direcciones Multicast.**

Como Trabaja ARP en Concentradores



Diferencias a Detalle

- **El concentrador repite el broadcast en todos sus puertos.**
- **Se puede considerar al concentrador como un dispositivo estúpido.**
- **El switch es en realidad un enrutador de capa 2.**
- **El switch es inteligente y tiene la capacidad de discernir en base al origen y destino de los paquetes que recibe.**

La tabla de "ruteo" de un bridge

- **Se considera como una base de datos que almacena registros de tres variables.**
- **Las variables manejadas son:**

  Dirección MAC

  Puerto en el bridge en que se conoce a esa dirección MAC

  Tiempo transcurrido desde que se recibió el último paquete con dicha dirección MAC

Ejemplo de una tabla de bridge/switch

Dirección MAC	Puerto	Aging Time
aa aa aa aa aa aa	1	2
bb bb bb bb bb bb	1	3
cc cc cc cc cc cc	1	10
dd dd dd dd dd dd	2	3
ee ee ee ee ee ee	3	130
11 11 11 11 11 11	4	24
22 22 22 22 22 22	5	15
33 33 33 33 33 33	5	12
44 44 44 44 44 44	6	289

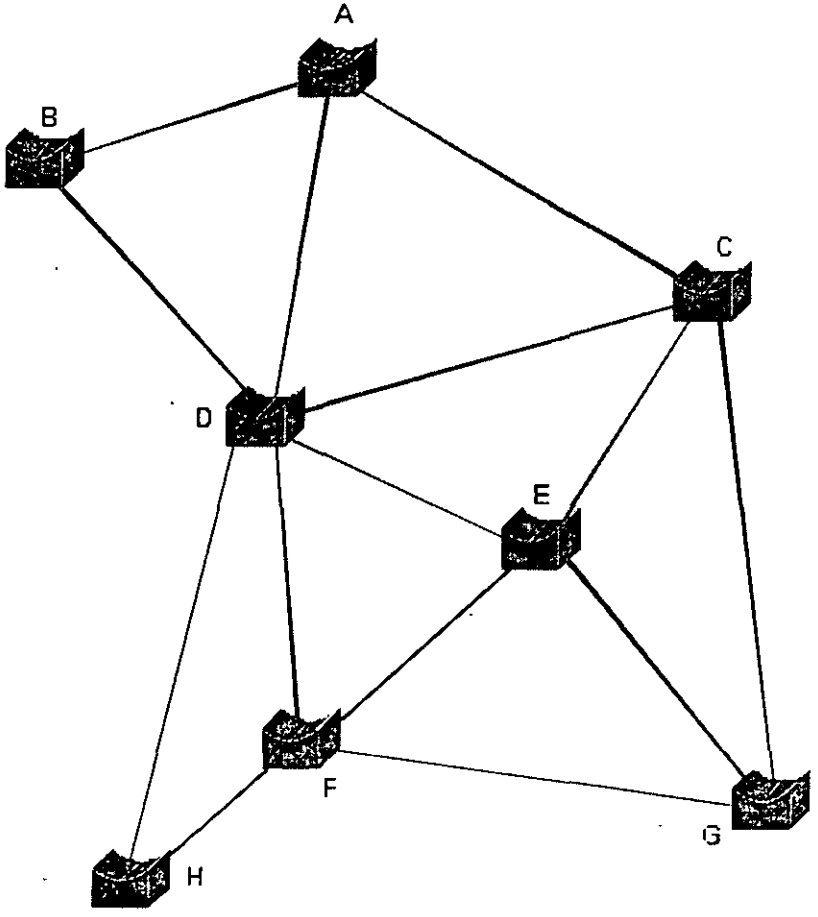
Modos de operación de bridges/switches

- **Store and Forward recibe la totalidad del paquete Ethernet, lo verifica y posteriormente lo reenvía.**
- **Cut trough sólo lee los campos de dirección MAC origen y dirección MAC destino, empieza a transmitir el paquete inmediatamente después de que deduce a donde se dirige.**
- **Existen implementaciones híbridas, para el caso de Cisco es el "Fragment Free", trabaja con Cut Trough pero verifica la validez del paquete, si una estación en particular induce muchos errores, se cambia automáticamente a Store and Forward.**

Objetivos de Spanning Tree

- **Evitar que los equipos hagan loops entre sí.**
- **Permitir establecer esquemas redundantes empleando "ruteo de capa 2".**
- **Que el protocolo sea lo más simple posible y a la vez configurable si el usuario así lo desea.**

Una red que necesita Spanning Tree



La misma red después de Spanning Tree

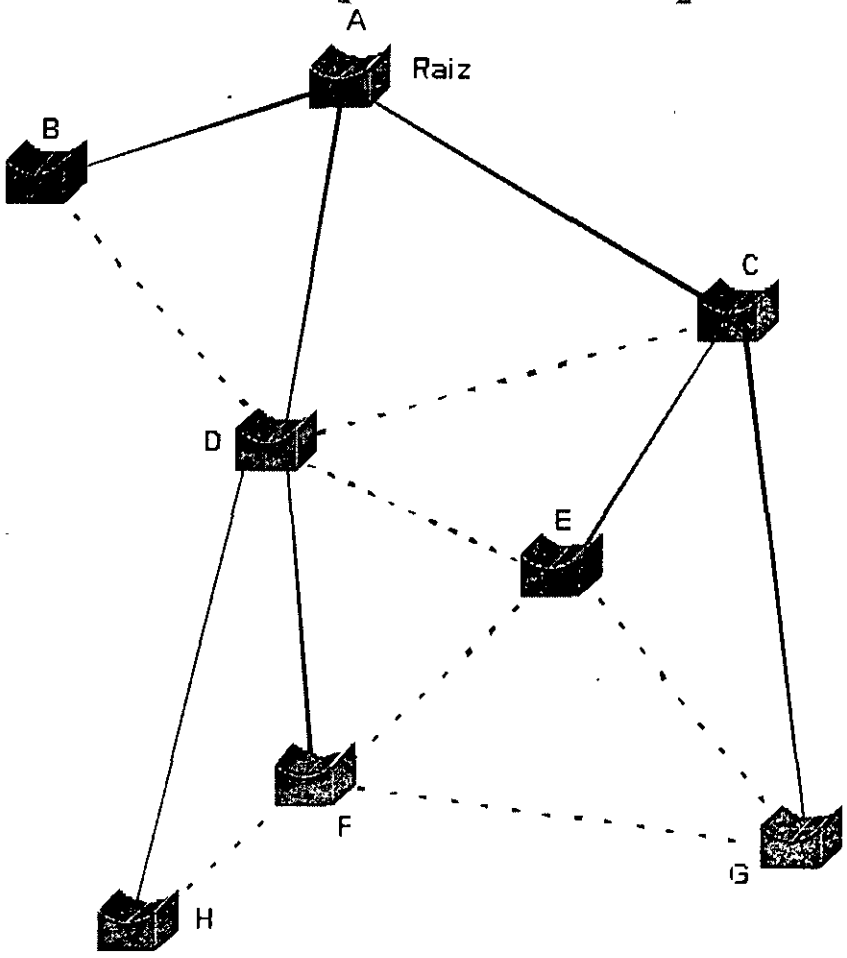
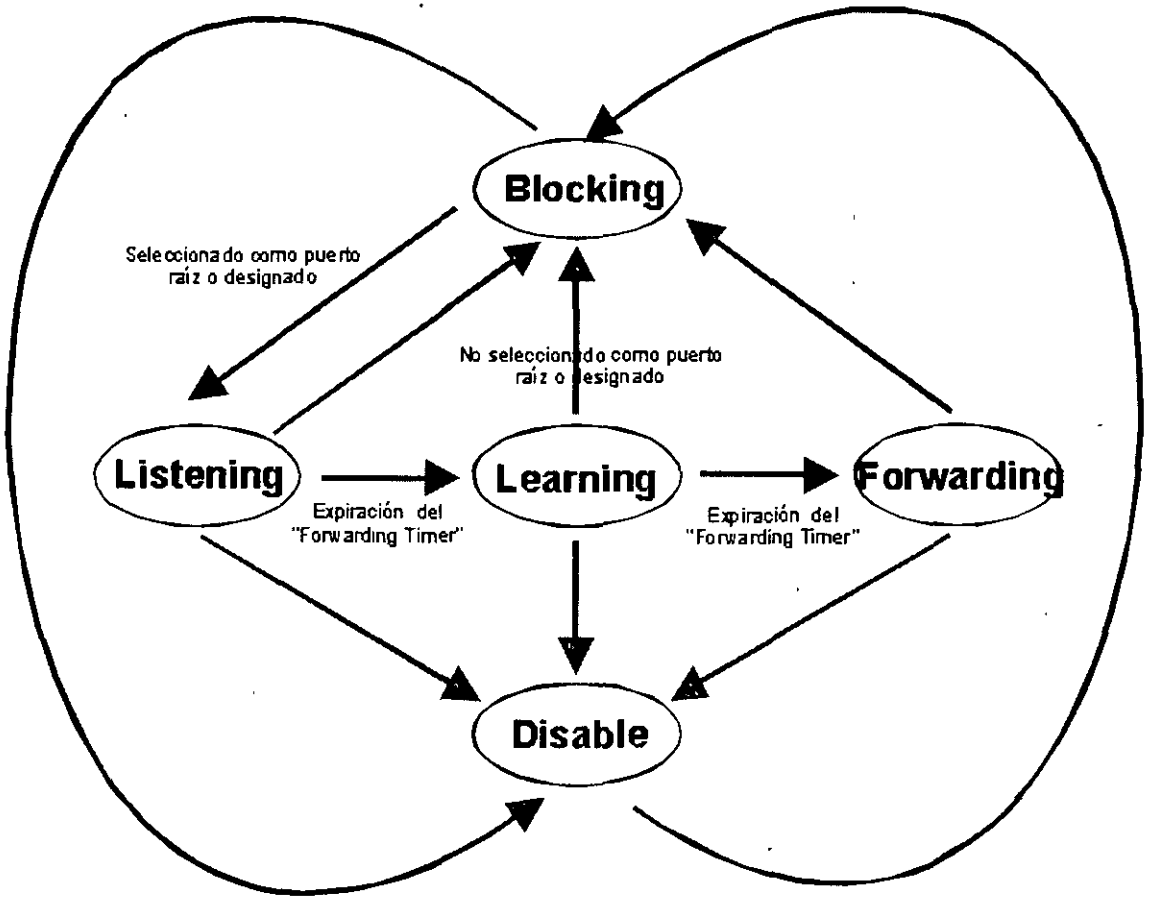


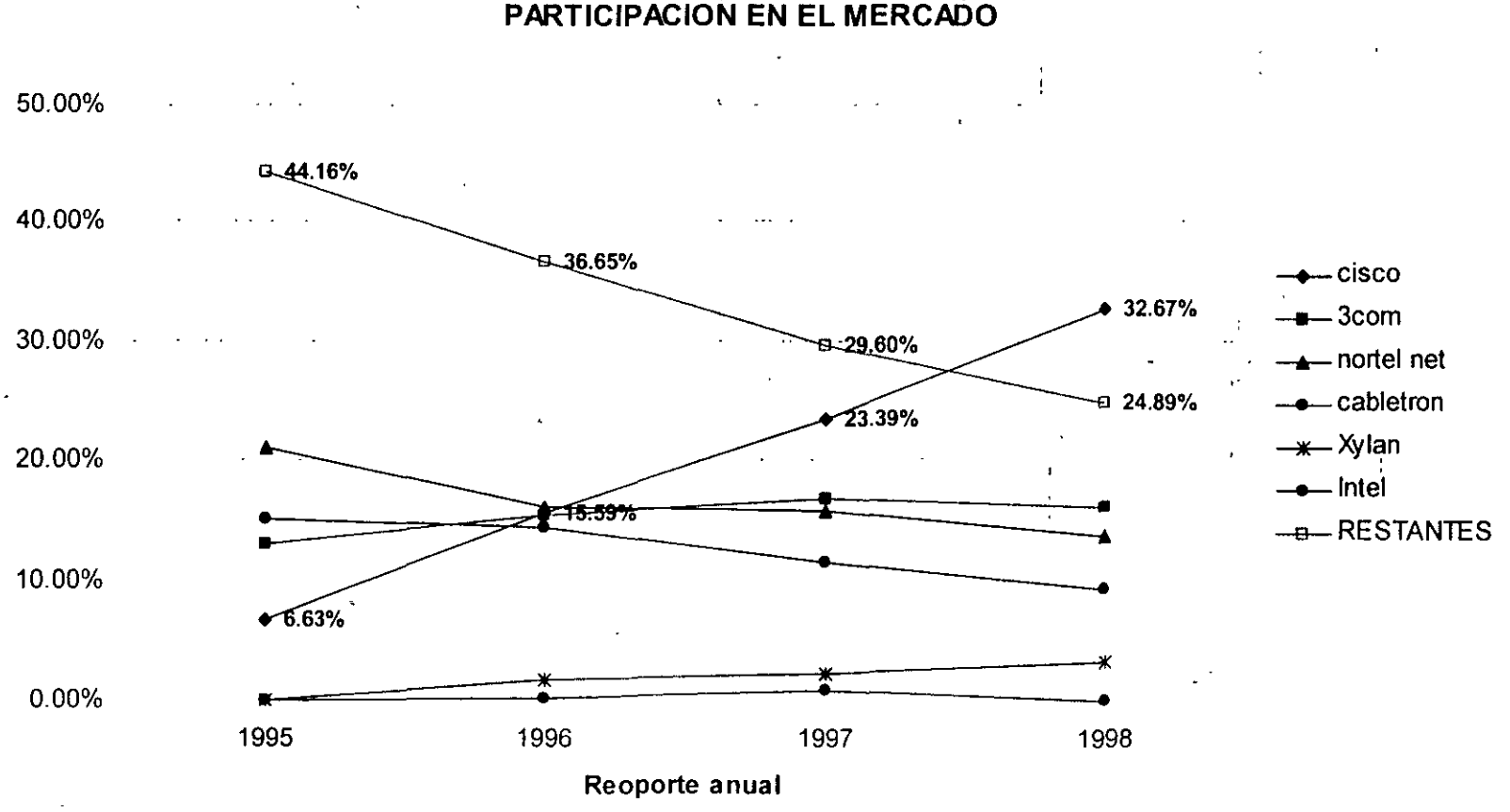
Diagrama de estados de Spanning Tree



Factores que determinan la tecnología

- **Aspectos técnicos.**
- **Aspectos económicos.**
- **Leyes del mercado.**
- **Ley de Moore.**
- **Ley de Metcalfe.**
- **Ley de la economía de escala.**

Distribución del mercado de switches 1998



Precios Hubs Vs. Switches 1998

HUBS

MODELO	3com SuperStack II PS Hub 40 TP	3com Superstack Hub 10	Cabletron SEHI 24	Bay Networks BayStack 106	Bay Networks BayStack 107	Bay Networks Hubstak 102
PRECIO EQUIPO	$1,339.00	$2,099.00	$1,355.00	$1,499.00	$2,099.00	$1,399.00
PRECIO PUERTO	$55.79	$87.46	$56.46	$124.92	$87.46	$58.29

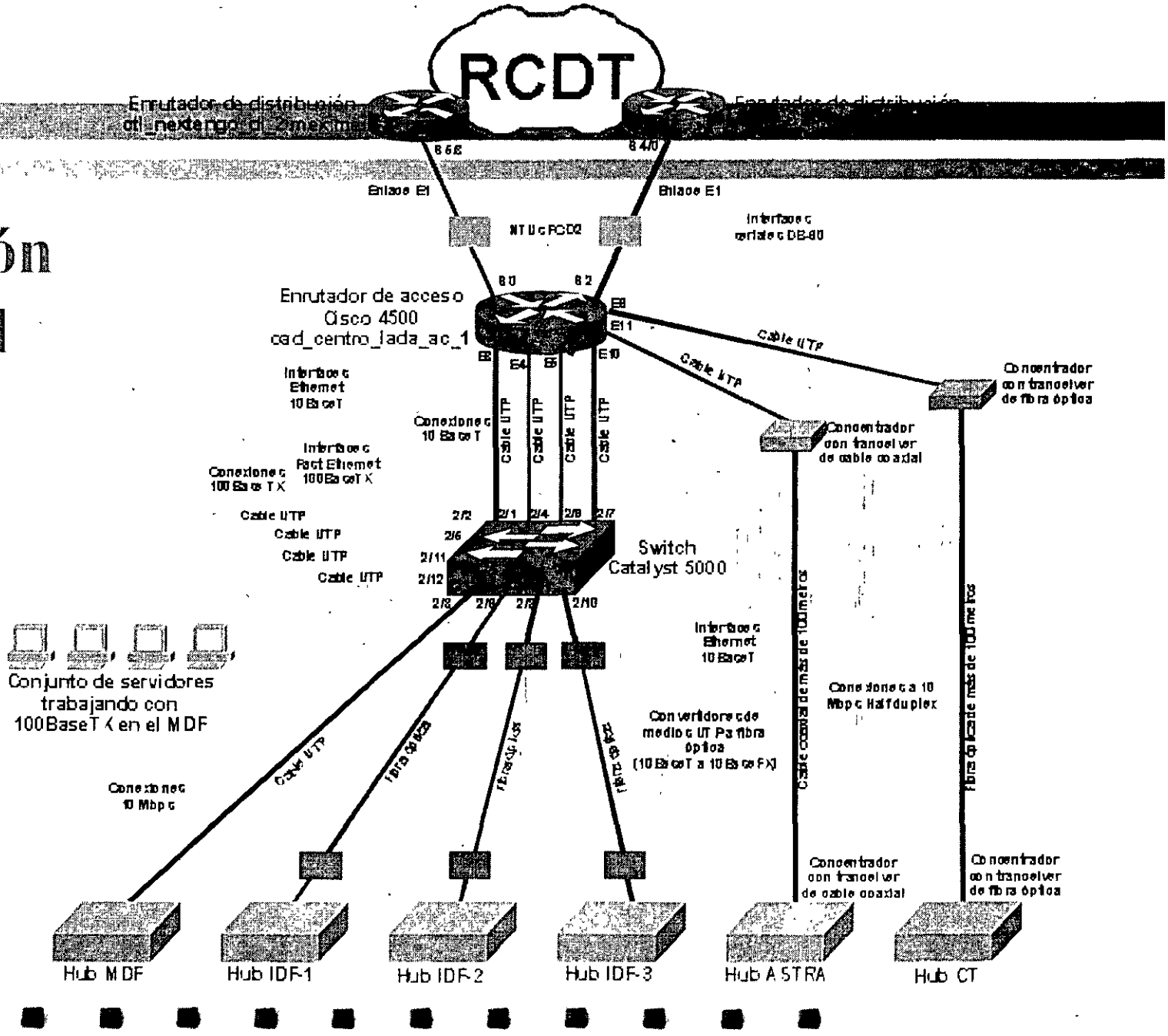
SWITCHES

MODELO	Cabletron ELS100-24TX	Cabletron ELS10-26TX	Bay Networks BayStack 303	3com SuperStack II Switch 1100	Cisco WS-C1924-EN
PRECIO EQUIPO	$2,995.00	$3,895.00	$1,625.00	$1,495.00	$1,525.00
PRECIO PUERTO	$124.79	$144.26	$65.00	$57.50	$56.48

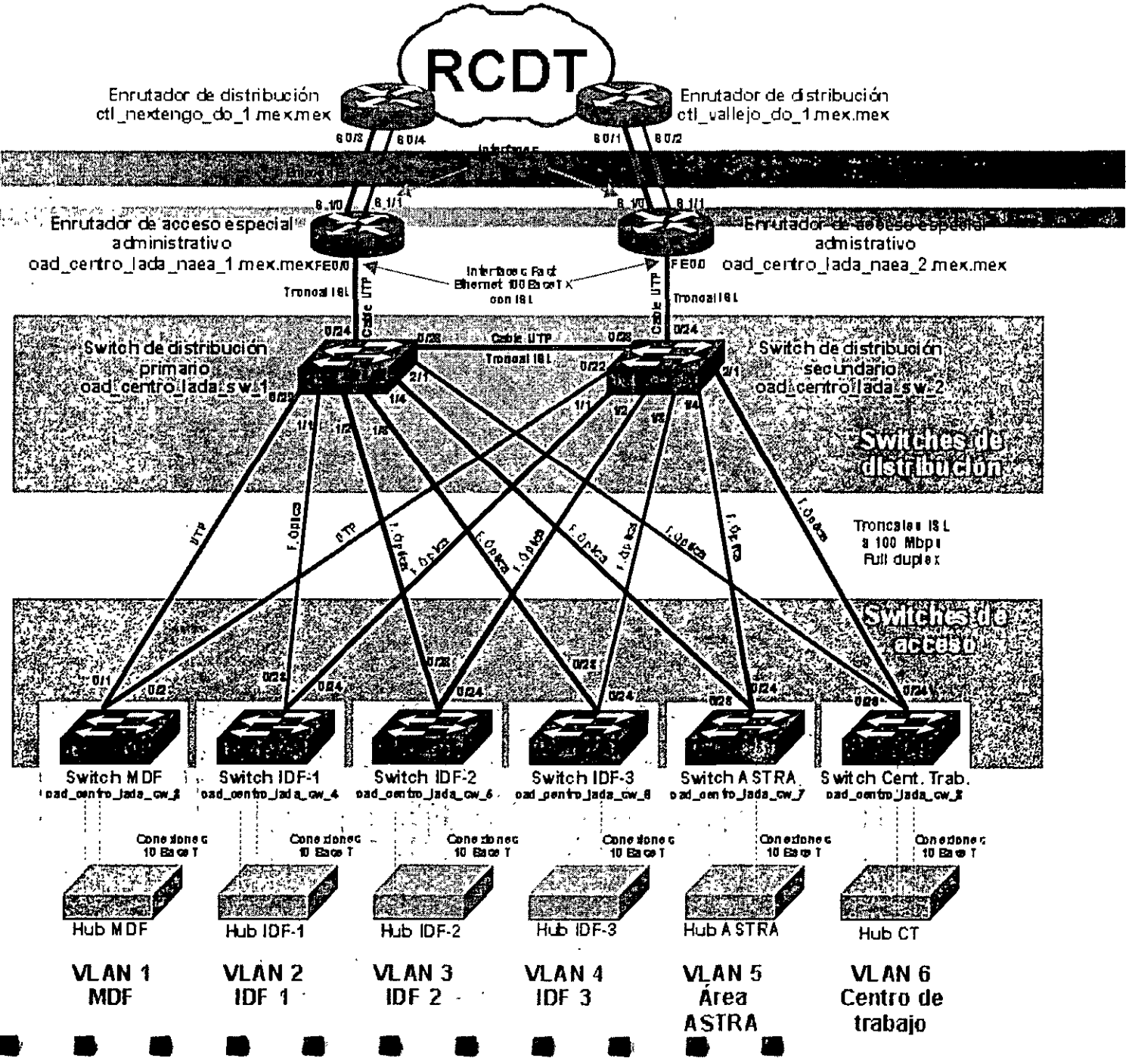
Caso práctico (objetivos)

- **Una red debe aprovechar los recursos disponibles.**
- **Debe ser compatible con los equipos existentes.**
- **Se tienen que cumplir con ciertas limitantes políticas.**
- **Se debe buscar la mejor relación costo/beneficio.**
- **Se debe de apegar a las normas de redes en vigencia.**
- **Debe cumplir con la políticas de la compañía**

Situación inicial



Situación final



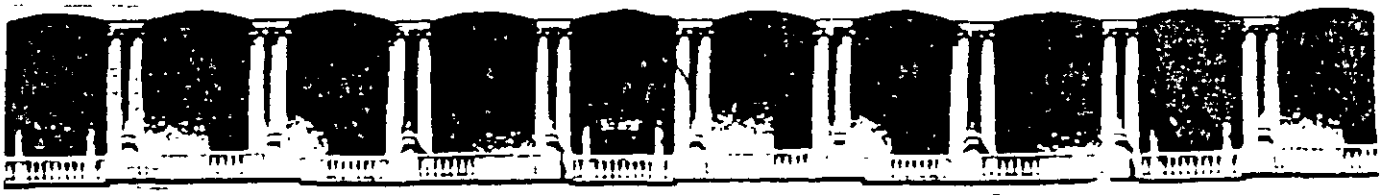
¡ Muchísimas gracias por su atención !

Eduardo Díaz González

Ingeniero de proyectos

edgonzal@telmex.net

edgonzal@hotmail.com



FACULTAD DE INGENIERIA U.N.A.M.
DIVISION DE EDUCACION CONTINUA
Tres décadas de orgullosa excelencia 1971 - 2001

CURSOS ABIERTOS

DIPLOMADO INTERNACIONAL EN TELECOMUNICACIONES

MODULO IV: REDES DIGITALES: ACTUALIDAD Y PERSPECTIVAS

TEMA

VPN's y MPLS

EXPOSITOR: ING. PABLO DOMÍNGUEZ PEREZ
PALACIO DE MINERIA
JUNIO 2001

7. VPN's y MPLS

del 11 al 15 de junio de 2001

Cisco Systems


MPLS
CISCO SYSTEMS

Agenda

- Concepts and goals
- Terminology
- Connection model
- Forwarding
- Mechanisms
- Topologies
- Scaling
- BGP-4 Enhancements
  - Cap. Negotiation, MPLS, Route Refresh, ORF
- Configuration

MPLS-VPN
What is a VPN?

- **An IP network infrastructure delivering *private* network services over a *public* infrastructure**
  - **Use a layer 3 backbone**
  - **Scalability, easy provisioning**
  - **Global as well as non-unique private address space**
  - **QoS**
  - **Controlled access**
  - **Easy configuration for customers**

The Overlay Model

- Private trunks over a TELCO/SP shared infrastructure
  - Leased/Dialup lines
  - FR/ATM circuits
  - IP (GRE) tunnelling
- Transparency between provider and customer networks
- Optimal routing requires full mesh over over backbone

The Peer model

- Both provider and customer network use same network protocol
- CE and PE routers have a routing adjacency at each site
- All provider routers hold the full routing information about all customer networks
- Private addresses are not allowed
- May use the virtual router capabiiity
  - Multiple routing and forwarding tables based on Customer Networks

The True Peer model

- Same as Peer model BUT !!!
- Provider Edge routers receive and hold routing information only about VPNs directly connected
- Reduces the amount of routing information a PE router will store
- Routing information is proportional to the number of VPNs a router is attached to
- MPLS is used within the backbone to switch packets (no need of full routing)

Agenda

- Concepts and goals
- Terminology
- Connection model
- Forwarding
- Mechanisms
- Topologies
- Scaling
- BGP-4 Enhancements
  - Cap. Negotiation, MPLS, Route Refresh, ORF
- Configuration

VPN Terminology

- **Provider Network (P-Network)**

  The backbone under control of a Service Provider

- **Customer Network (C-Network)**

  Network under customer control

- **CE router**

  Customer Edge router. Part of the C-network and interfaces to a PE router

MPLS VPN Terminology

- **Site**

  Set of (sub)networks part of the C-network and co-located

  A site is connected to the VPN backbone through one or more PE/CE links

- **PE router**

  Provider Edge router. Part of the P-Network and interfaces to CE routers

- **P router**

  Provider (core) router, without knowledge of VPN

MPLS VPN Terminology

- **Border router**

  Provider Edge router interfacing to other provider networks

- **Extended Community**

  BGP attribute used to identify a Route-origin, Route-target

- **Site of Origin Identifier (SOO)**

  64 bits identifying routers where the route has been originated

VPN Terminology

- **Route-Target**

  64 bits identifying routers that should receive the route

- **Route Distinguisher**

  Attributes of each route used to uniquely identify prefixes among VPNs (64 bits)

  VRF based (not VPN based)

- **VPN-IPv4 addresses**

  Address including the 64 bits Route Distinguisher and the 32 bits IP address

VPN Terminology

- **VRF**
  - VPN Routing and Forwarding Instance
  - Routing table and FIB table
  - Populated by routing protocol contexts
- **VPN-Aware network**
  - A provider backbone where MPLS-VPN is deployed

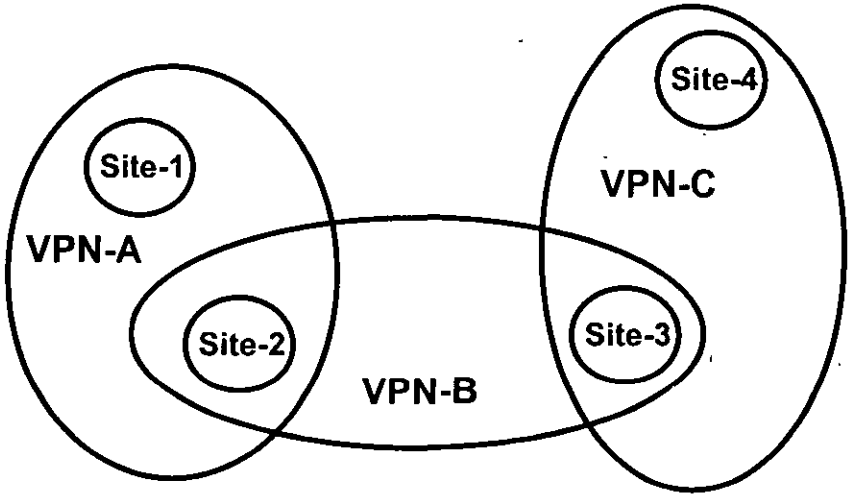
Agenda

- Concepts and goals
- Terminology
- Connection model
- Forwarding
- Mechanisms
- Topologies
- Scaling
- BGP-4 Enhancements
  - Cap. Negotiation, MPLS, Route Refresh, ORF
- Configuration

VPN Connection Model

- A VPN is a collection of sites sharing a common routing information (routing table)
- A site can be part of different VPNs
- A VPN has to be seen as a community of interest (or Closed User Group)
- Multiple Routing/Forwarding instances (VRF) on PE routers

Connection Models

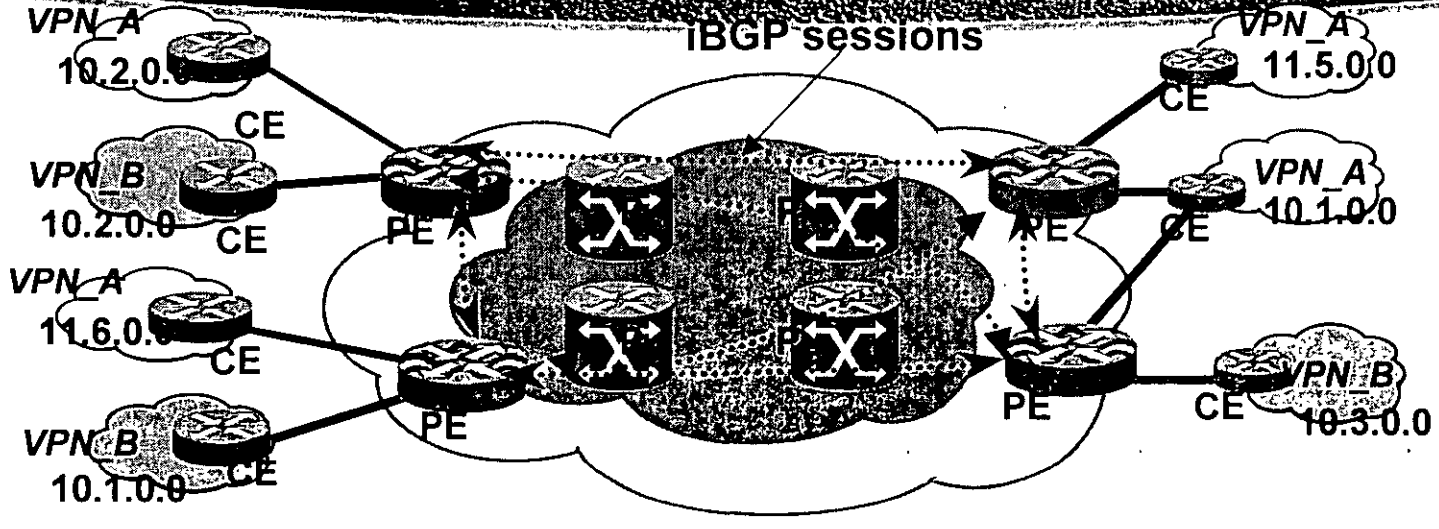


- A site belonging to different VPNs may or MAY NOT be used as a transit point between VPNs
- If two or more VPNs have a common site, address space must be unique among these VPNs

VPN Connection Model

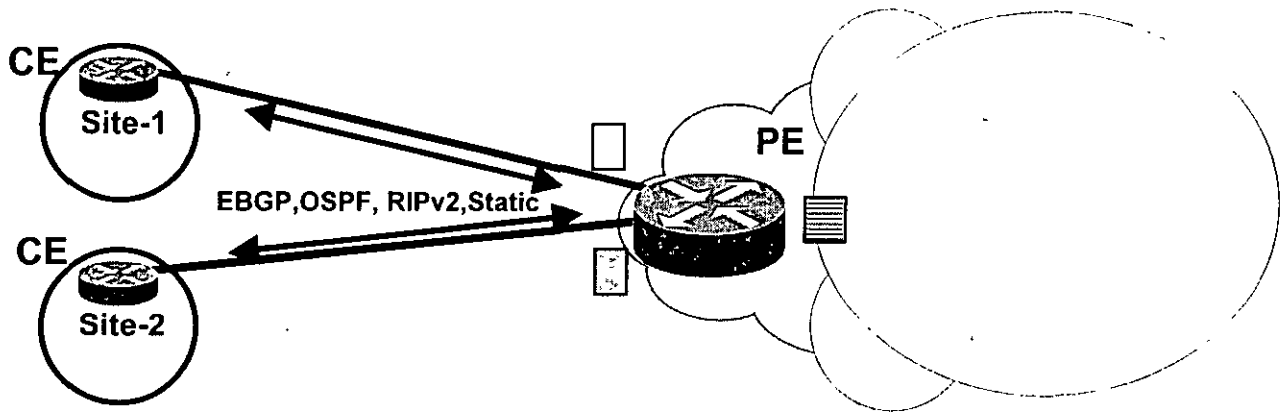
- The VPN backbone is composed by MPLS LSRs
  - PE routers (edge LSRs)
  - P routers (core LSRs)
- PE routers are faced to CE routers and distribute VPN information through MP-BGP to other PE routers

  VPN-IPv4 addresses, Extended Community, Label
- P routers do not run BGP and do not have any VPN knowledge



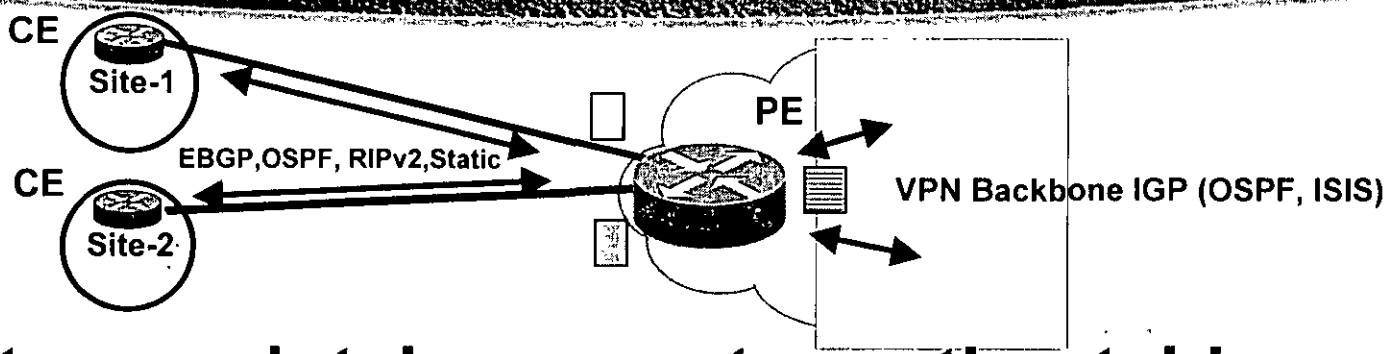
- P routers (LSRs) are in the core of the MPLS cloud
- PE routers use MPLS with the core and plain IP with CE routers
- P and PE routers share a common IGP
- PE router are MP-iBGP fully meshed

PE-CE Connection Models



- PE and CE routers exchange routing information through:
  - EBGP, OSPF, RIPv2, Static routing
- CE router run standard routing software

VPN Connection Model



- **PE routers maintain separate routing tables**
  - **The global routing table**

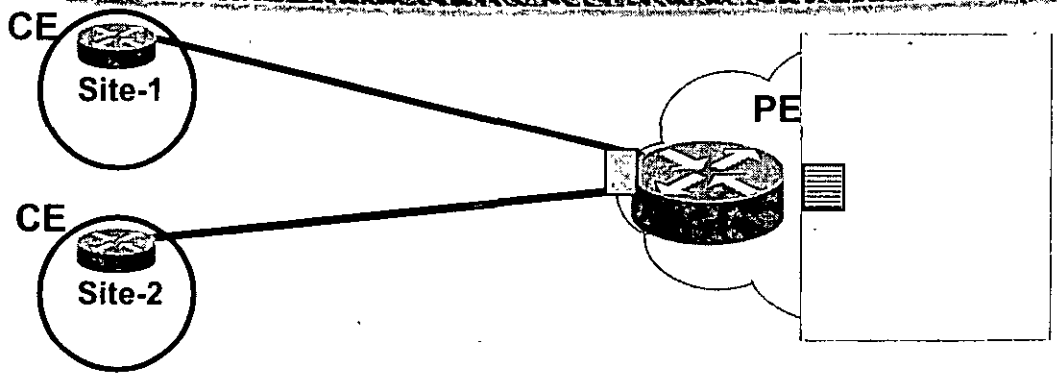
    With all PE and P routes
    Populated by the VPN backbone IGP (ISIS or OSPF)
  - **VRF (VPN Routing and Forwarding)**

    Routing and Forwarding table associated with one or more directly connected sites (CEs)

    VRF are associated to (sub/virtual/tunnel)interfaces

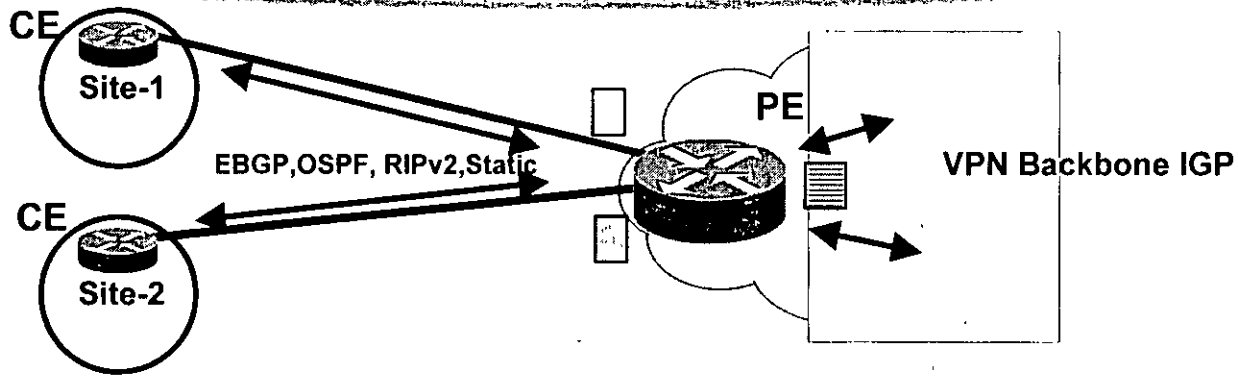
    Interfaces may share the same VRF if the connected sites may share the same routing information

VPN Connection Models



- Different site sharing the same routing information, may share the same VRF
- Interfaces connecting these sites will use the same VRF
- Sites belonging to the same VPN *may* share same VRF

Route Installation: Method

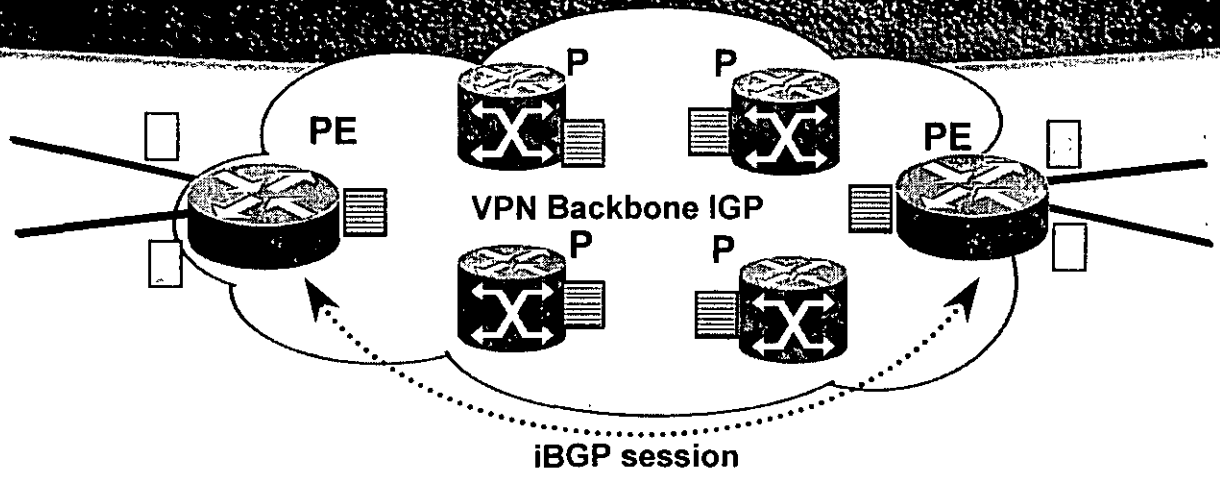


- The routes the PE receives from CE routers are installed in the appropriate VRF
- The routes the PE receives through the backbone IGP are installed in the global routing table
- By using separate VRFs, addresses need NOT to be unique among VPNs

Connection Model

- The Global Routing Table is populated by IGP protocols.
- In PE routers it may contain the BGP Internet routes (standard BGP-4 routes)
- BGP-4 (IPv4) routes go into global routing table
- MP-BGP (VPN-IPv4) routes go into VRFs

Peer Connection Model



- PE and P routers share a common IGP (ISIS or OSPF)
- PEs establish MP-iBGP sessions between them
- PEs use MP-BGP to exchange routing information related to the connected sites and VPNs

  VPN-IPv4 addresses, Extended Community, Label

Cisco Systems

MP-BGP Update

- VPN-IPV4 address
  - Route Distinguisher

    64 bits

    Makes the IPv4 route globally unique

    RD is configured in the PE for each VRF

    RD may or may not be related to a site or a VPN
  - IPv4 address (32bits)
- Extended Community attribute (64 bits)

  Site of Origin (SOO): identifies the originating site

  Route-target (RT): identifies the set of sites the route has to be advertised to

MPLS Application Model: IP BGP Update

- Any other standard BGP attribute
  - Local Preference
  - MED
  - Next-hop
  - AS_PATH
  - Standard Community
  - ...
- A Label identifying:
  - The outgoing interface
  - The VRF where a lookup has to be done (aggregate label)
  - The BGP label will be the second label in the label stack of packets travelling in the core

VPN Connection Model
Example - Extended community

- **BGP extended community attribute**
  - **Structured, to support multiple applications**
  - **64 bits for increased range**
- **General form**
  - **<16bits type>:<ASN>:<32 bit number>**
    - **Registered AS number**
  - **<16bits type>:<IP address>:<16 bit number>**
    - **Registered IP address**

Connection Model - Extended community

- **The Extended Community is used to:**
  - **Identify one or more routers where the route has been originated (site)**

    Site of Origin (SOO)
  - **Selects sites which should receive the route**

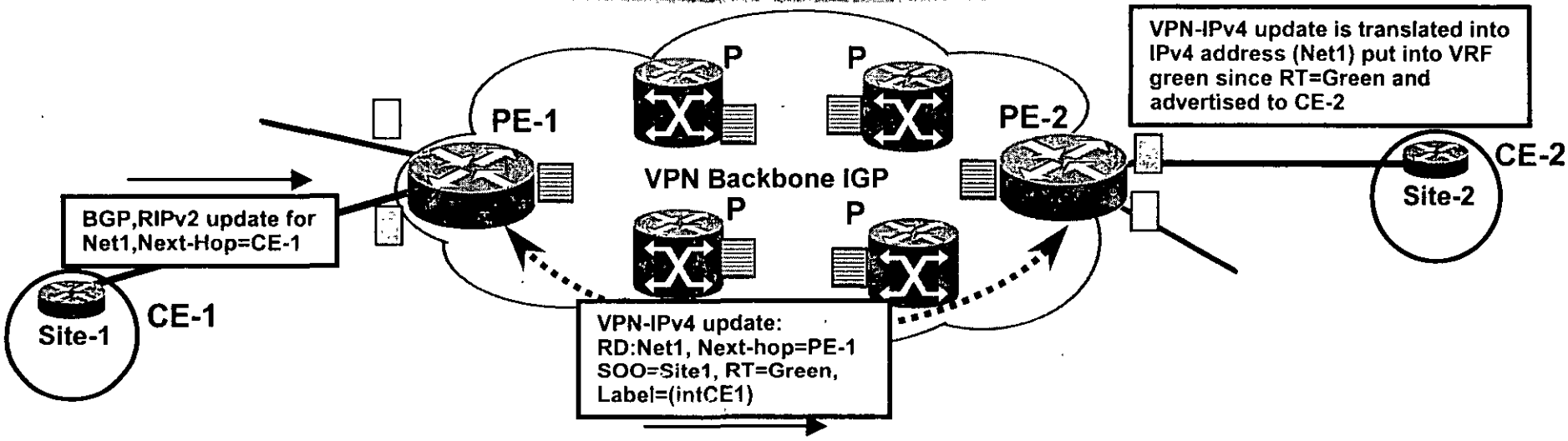
    Route-Target

VPN Connection Model: iBGP Update

- The Label can be assigned only by the router which address is the Next-Hop attribute
  - PE routers re-write the Next-Hop with their own address (loopback interface address)

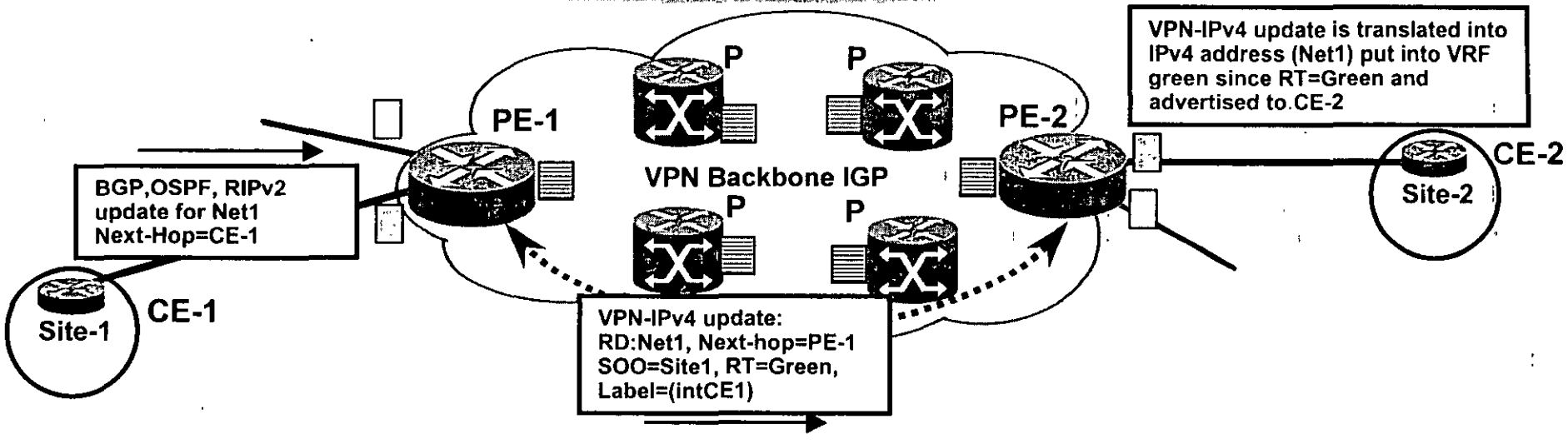
    "Next-Hop-Self" BGP command towards iBGP neighbors
    Loopback addresses are advertised into the backbone IGP
- PE addresses used as BGP Next-Hop must be uniquely known in the backbone IGP
  - No summarisation of loopback addresses in the core

Connection Model



- **PE routers receive IPv4 updates (EBGP, RIPv2, Static)**
- **PE routers translate into VPN-IPv4**
  - **Assign a SOO and RT based on configuration**
  - **Re-write Next-Hop attribute**
  - **Assign a label based on VRF and/or interface**
  - **Send MP-iBGP update to all PE neighbors**

Connection Model



- **Receiving PEs translate to IPv4**

  Insert the route into the VRF identified by the RT attribute (based on PE configuration)

- **The label associated to the VPN-IPv4 address will be set on packet forwarded towards the destination**

Connection Model

- Route distribution to sites is driven by the Site of Origin (SOO) and Route-target attributes
  - BGP Extended Community attribute
- A route is installed in the site VRF corresponding to the Route-target attribute
  - Driven by PE configuration
- A PE which connects sites belonging to multiple VPNs will install the route into the site VRF if the Route-target attribute contains one or more VPNs to which the site is associated

Agenda

- Concepts and goals
- Terminology
- Connection model
- Forwarding
- Mechanisms
- Topologies
- Scaling
- BGP-4 Enhancements
  - Cap. Negotiation, MPLS, Route Refresh, ORF
- Configuration

Forwarding

- PE and P routers have BGP next-hop reachability through the backbone IGP
- Labels are distributed through LDP (hop-by-hop) corresponding to BGP Next-Hops
- Label Stack is used for packet forwarding
  - Top label indicates BGP Next-Hop (interior label)
  - Second level label indicates outgoing interface or VRF (exterior label)

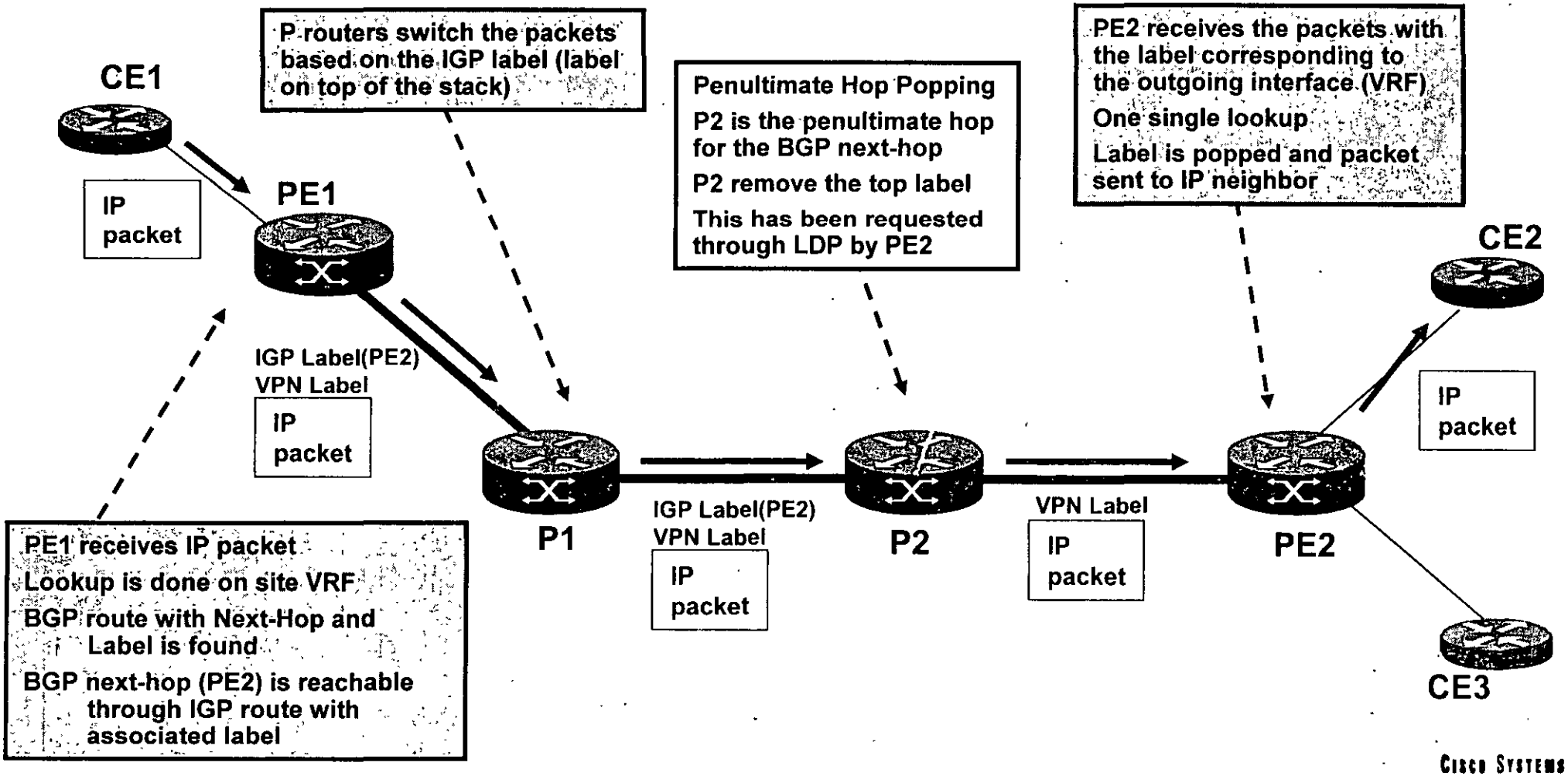
MPLS Forwarding

- MPLS nodes forward packets based on the top label
- P routers do not have BGP (nor VPN) knowledge
  - No VPN routing information
  - No Internet routing information

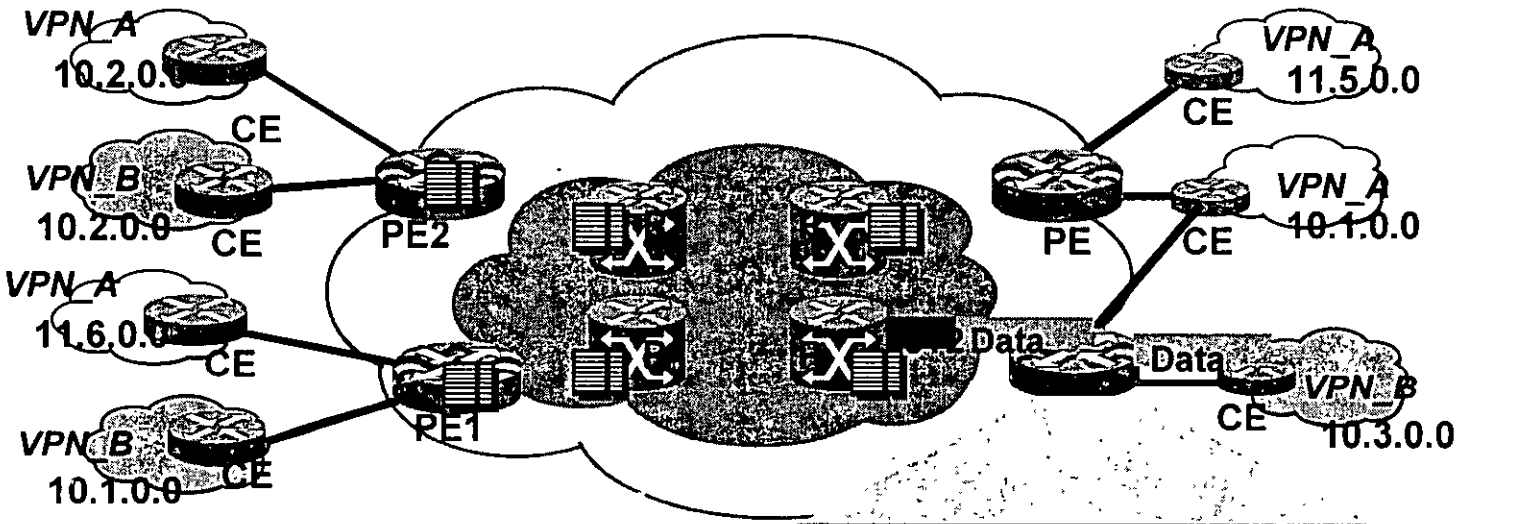
LS Forwarding (Ultimate Hop Popping)

- The upstream LDP peer of the BGP next-hop (PE router) will pop the first level label
  - The penultimate hop will pop the label
- Requested through LDP
- The egress PE router will forward the packet based on the second level label which gives the outgoing interface (and VPN)

MPLS Forwarding
Eg. - Penultimate Hop Pop



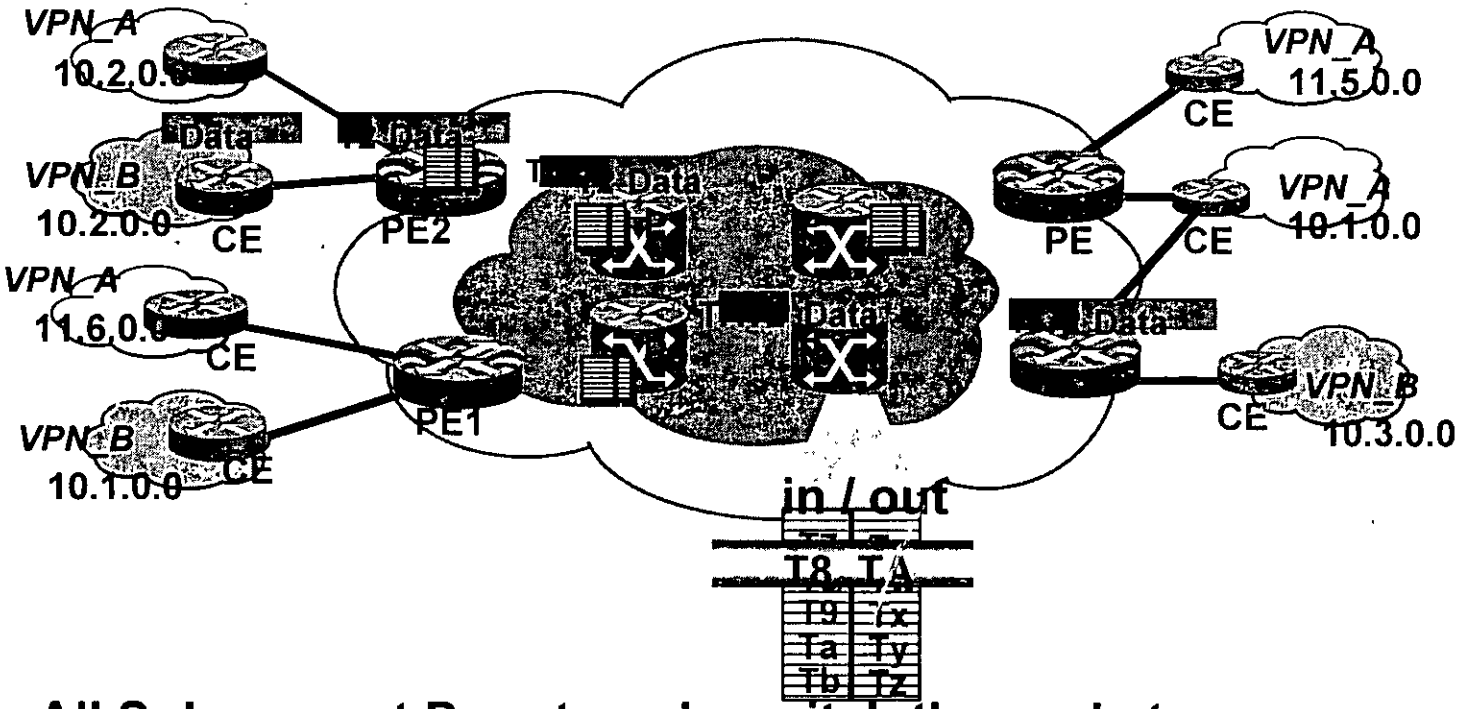
MPLS VPN Forwarding



<RD_B,10.2> , iBGP NH= PE2 , T2	T2	T8
<RD_B,10.2> , iBGP next hop PE2	T2	T8
<RD_B,10.3> , iBGP next hop PE3	T3	T9
<RD_A,11.6> , iBGP next hop PE1	T4	T7
<RD_A,10.1> , iBGP next hop PE4	T5	T8
<RD_A,10.4> , iBGP next hop PE4	T6	T8
<RD_A,10.2> , iBGP next hop PE2	T7	T8

- Ingress PE receives normal IP Packets from CE router
- PE router does "IP Longest Match" from VPN_B FIB , find iBGP next hop PE2 and impose a stack of labels:
  exterior Label T2 + Interior Label T8

MPLS VPN Forwarding



- All Subsequent P routers do switch the packet Solely on Interior Label
- Egress PE router, removes Interior Label
- Egress PE uses Exterior Label to select which VPN/CE to forward the packet to.
- Exterior Label is removed and packet routed to CE router

Agenda

- Concepts and goals
- Terminology
- Connection model
- Forwarding
- Mechanisms
- Topologies
- Scaling
- BGP-4 Enhancements

  Cap. Negotiation, MPLS, Route Refresh, ORF

- Configuration

MPLS VPN Mechanisms
Multiple Routing Instances

- VRF: VPN Routing and Forwarding Instance
  - VRF Routing Protocol Context
  - VRF Routing Tables
  - VRF CEF Forwarding Tables

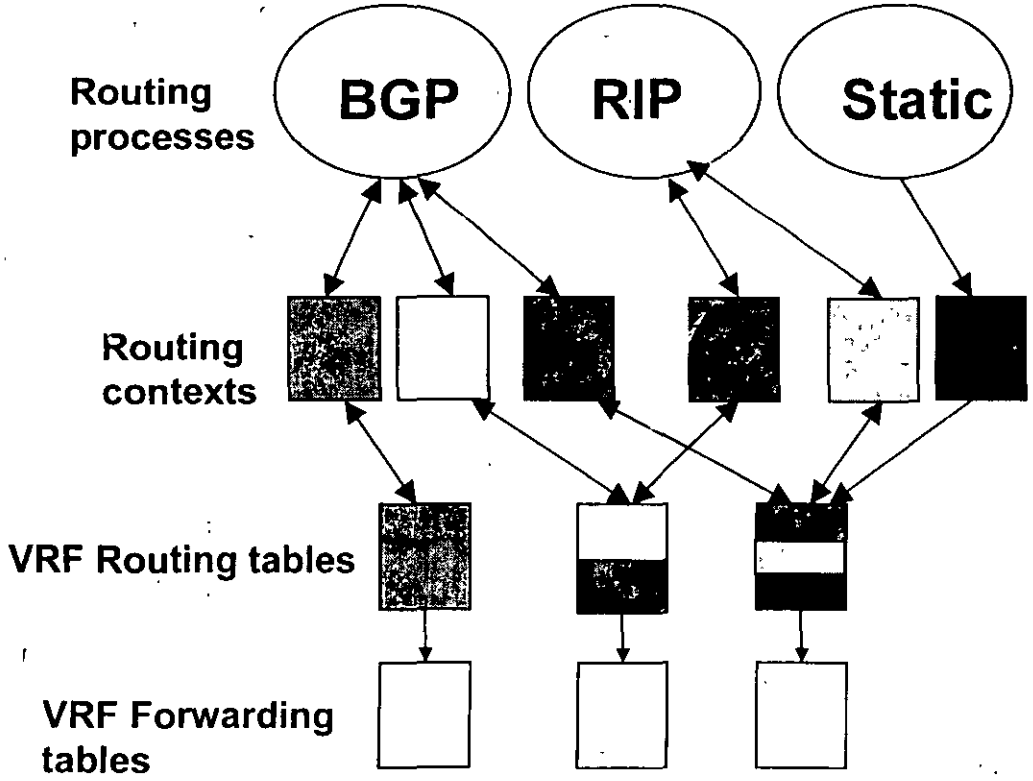
VPN Mechanisms: Multiple Routing Instances

- VPN aware Routing Protocols
- Select/Install routes in appropriate routing table
- Per-instance router variables
- Not necessarily per-instance routing processes
- eBGP, OSPF, RIPv2, Static

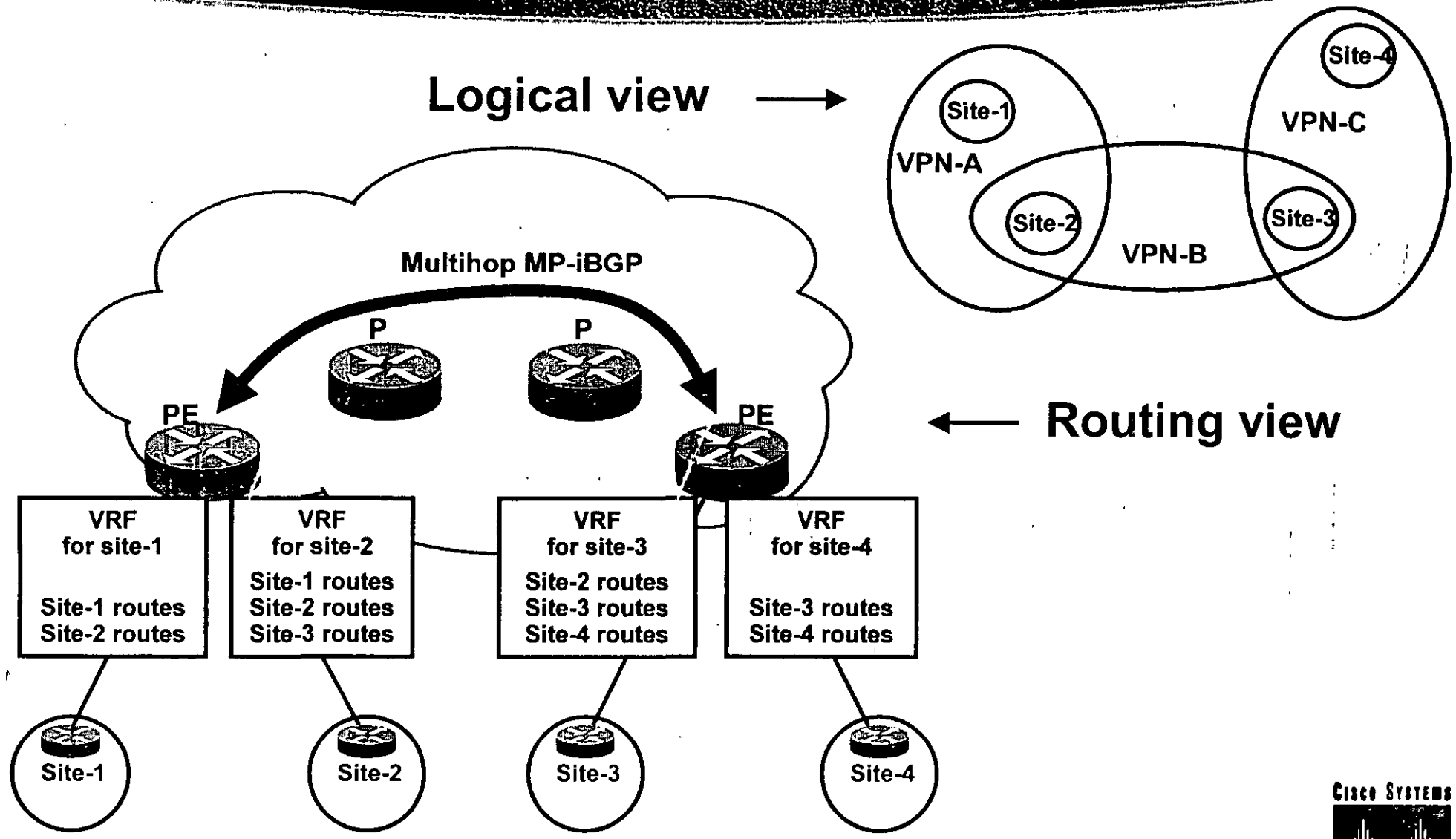
VPN Mechanisms: Multiple Routing Instances

- VRF Routing table contains routes which should be available to a particular set of sites
- Analogous to standard IOS routing table, supports the same set of mechanisms
- Interfaces (sites) are assigned to VRFs
  - One VRF per interface (sub-interface, tunnel or virtual-template)
  - Possible many interfaces per VRF

VPN Mechanisms: Multiple Routing Instances



- Routing processes run within specific routing contexts
- Populate specific VPN routing table and FIBs (VRF)
- Interfaces are assigned to VRFs

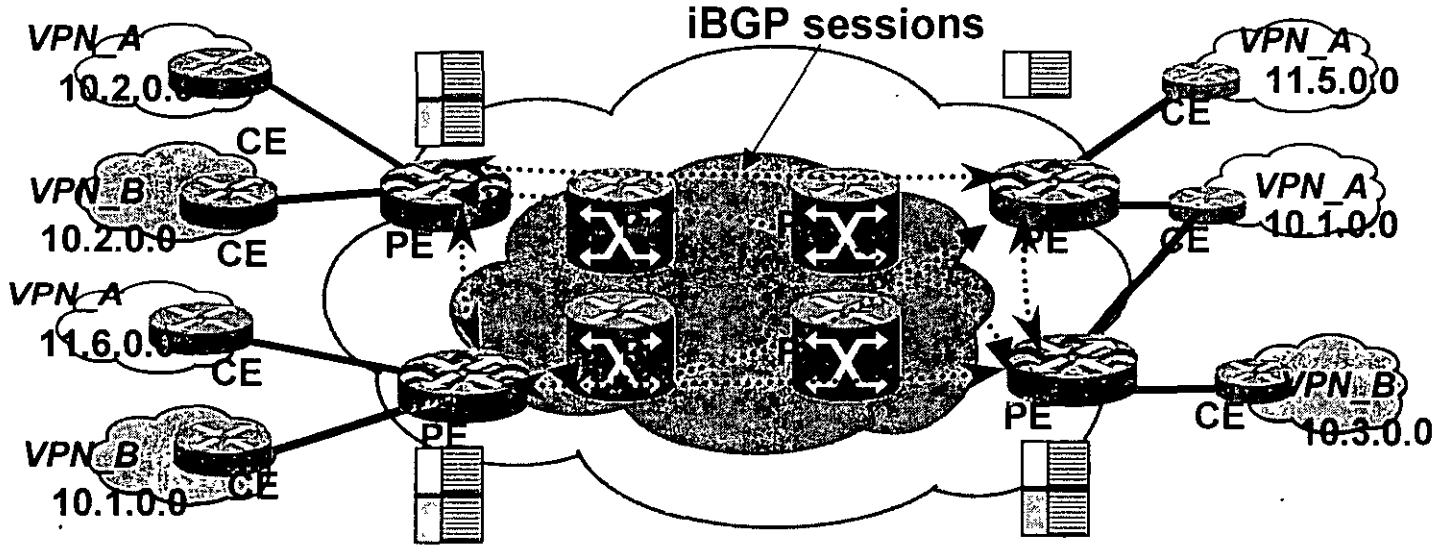

Logical view
Site-1
VPN-A
Site-2
VPN-B
Site-3
VPN-C
Site-4
Routing view
Multihop MP-iBGP
P
P
PE
PE
VRF
for site-1
Site-1 routes
Site-2 routes
VRF
for site-2
Site-1 routes
Site-2 routes
Site-3 routes
VRF
for site-3
Site-2 routes
Site-3 routes
Site-4 routes
VRF
for site-4
Site-3 routes
Site-4 routes
Site-1
Site-2
Site-3
Site-4

Agenda

- Concepts and goals
- Terminology
- Connection model
- Forwarding
- Mechanisms
- Topologies
- Scaling
- BGP-4 Enhancements

  Cap. Negotiation, MPLS, Route Refresh, ORF
- Configuration

VPN Topologies

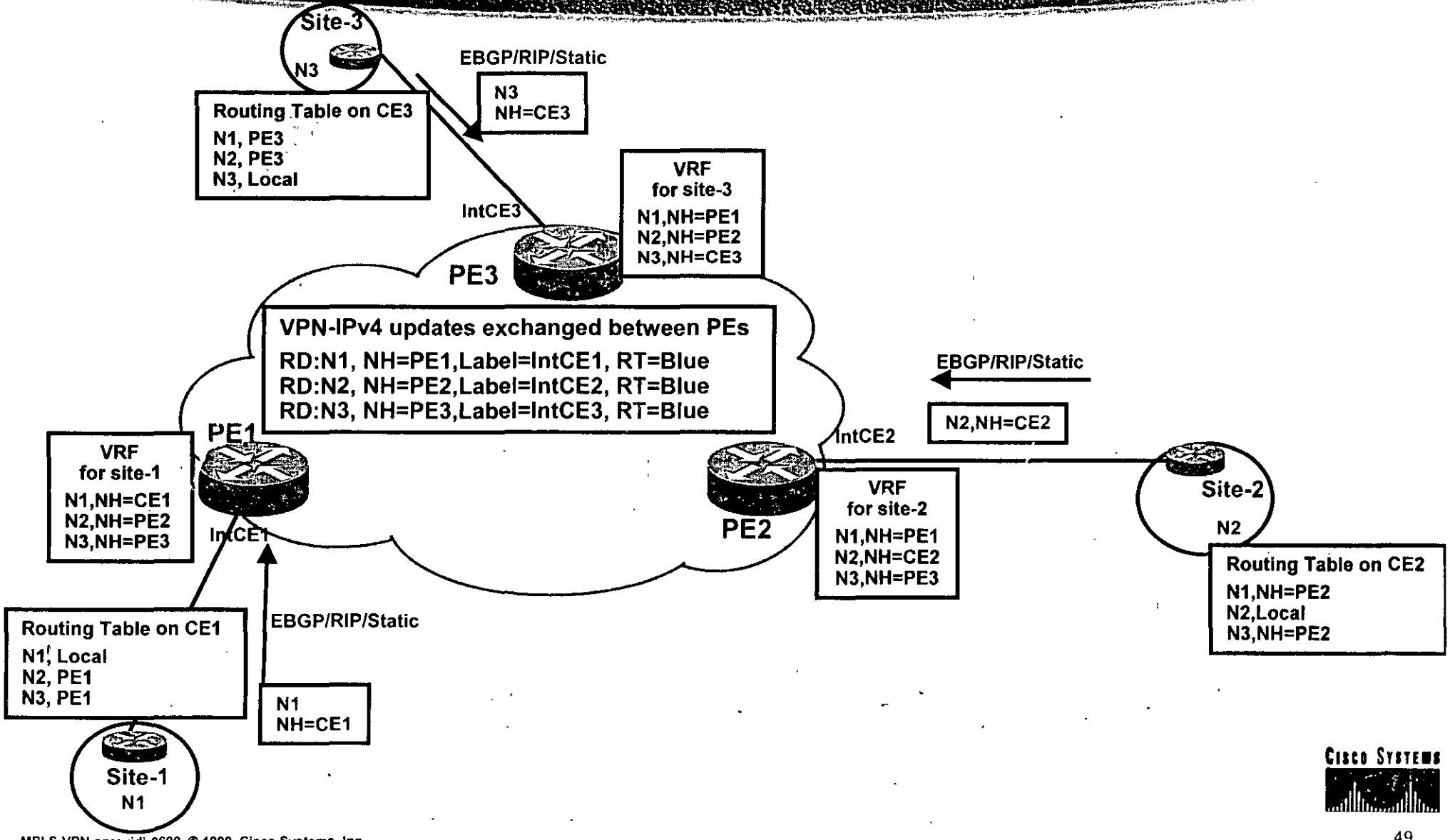


- VPN-IPv4 address are propagated together with the associated label in BGP Multiprotocol extension
- Extended Community attribute (route-target) is associated to each VPN-IPv4 address, to populate the site VRF

VPN Topologies
Optimal Intra-VPN Routing

- Each site has full routing knowledge of all other sites (of same VPN)
- Each CE announces his own address space
- MP-BGP VPN-IPv4 updates are propagated between PEs
- Routing is optimal in the backbone
  - Each route has the BGP Next-Hop closest to the destination
- No site is used as central point for connectivity

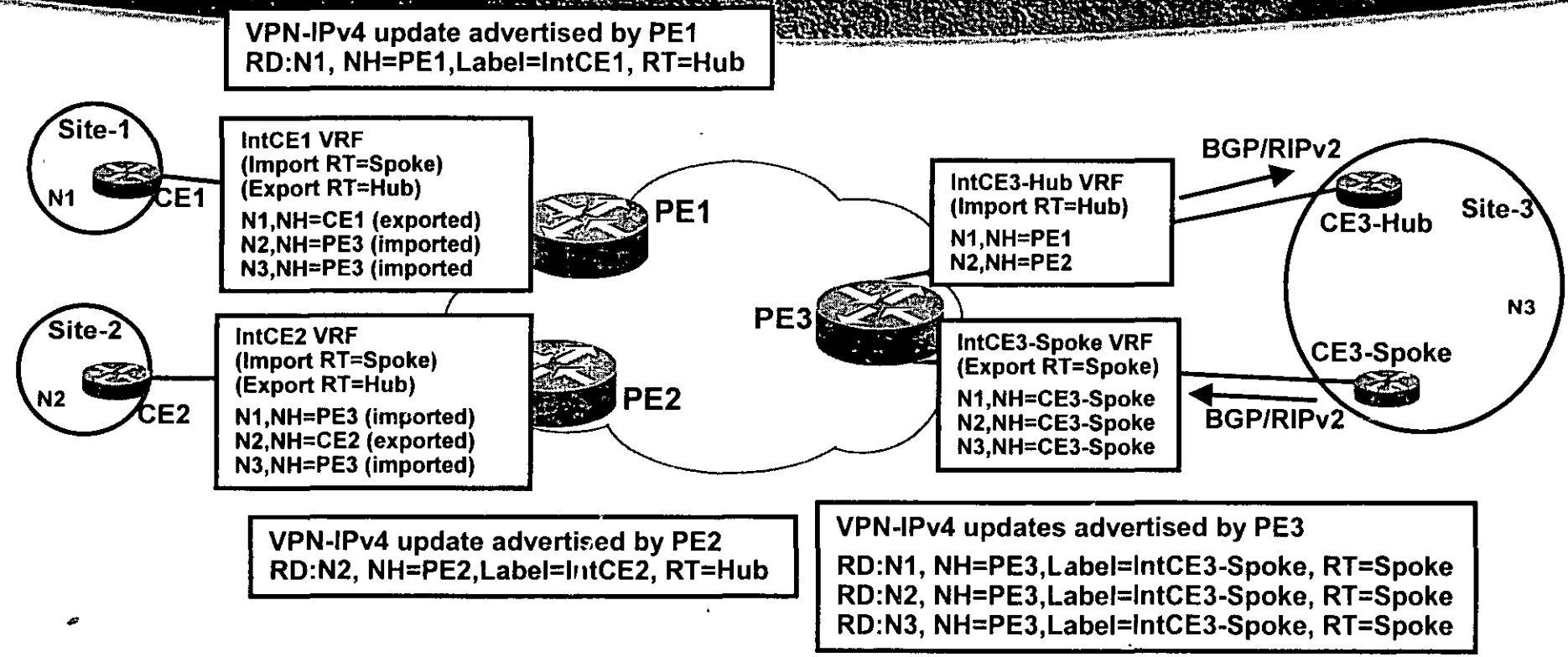
VPN Topologies: Optimal Intra-VPN Routing



VPN Topologies
Hub & Spoke (cont.)

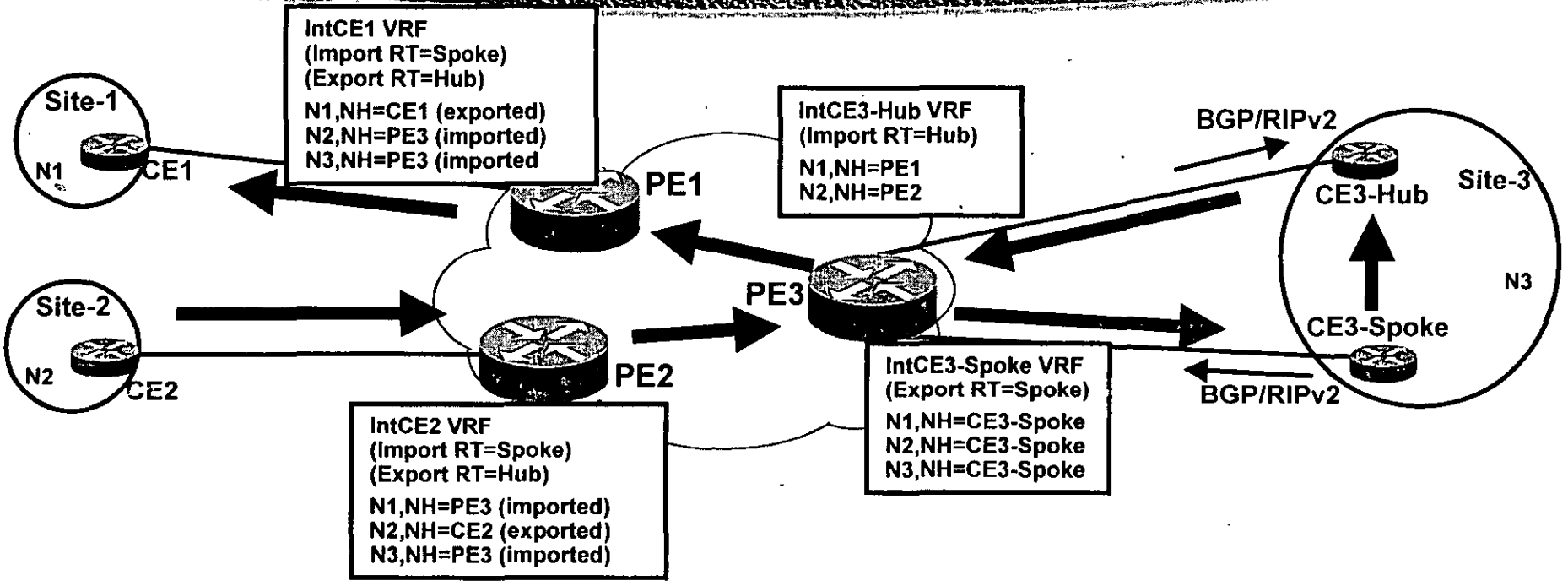
- One central site has full routing knowledge of all other sites (of same VPN)
  - Hub-Site
- Other sites will send traffic to Hub-Site for any destination
  - Spoke-Sites
- Hub-Site is the central transit point between Spoke-Sites
  - Use of central services at Hub-Site

VPN Topologies: Hub & Spoke routing



- **Routes are imported/exported into VRFs based on RT value of the VPN-IPv4 updates**
- **PE3 uses 2 (sub)interfaces with two different VRFs**

VPN Topologies
Hub & Spoke routing



- **Traffic from one spoke to another will travel across the hub site**
- **Hub site may host central services**
  - **Security, NAT, centralised Internet access**

VPN Topologies: With Hub & Spoke routing

- If PE and Hub-site use BGP the PE should not check the received AS_PATH
  - The update the Hub-site advertise contains the VPN backbone AS number
  - By configuration the AS_PATH check is disabled
  - Routing loops are detected through the SOO attribute
- PE and CE routers may use RIPv2 and/or static routing

Internet Routing

- In a VPN, sites may need to have Internet connectivity
- Connectivity to the Internet means:
  - Being able to reach Internet destinations
  - Being able to be reachable from any Internet source
- Security mechanism MUST be used as in ANY other kind of Internet connectivity

Internet Routing

- The Internet routing table is treated separately
- In the VPN backbone the Internet routes are in the Global routing table of PE routers
- Labels are not assigned to external (BGP) routes
- P routers need not (and will not) run BGP

VPN Internet routing - specific default route

- A default route is installed into the site VRF and pointing to a Internet Gateway
- The default route is NOT part of any VPN
  - A single label is used for packets forwarded according to the default route
  - The label is the IGP label corresponding to the IP address of the Internet gateway

    Known in the IGP

Internet routing: default route

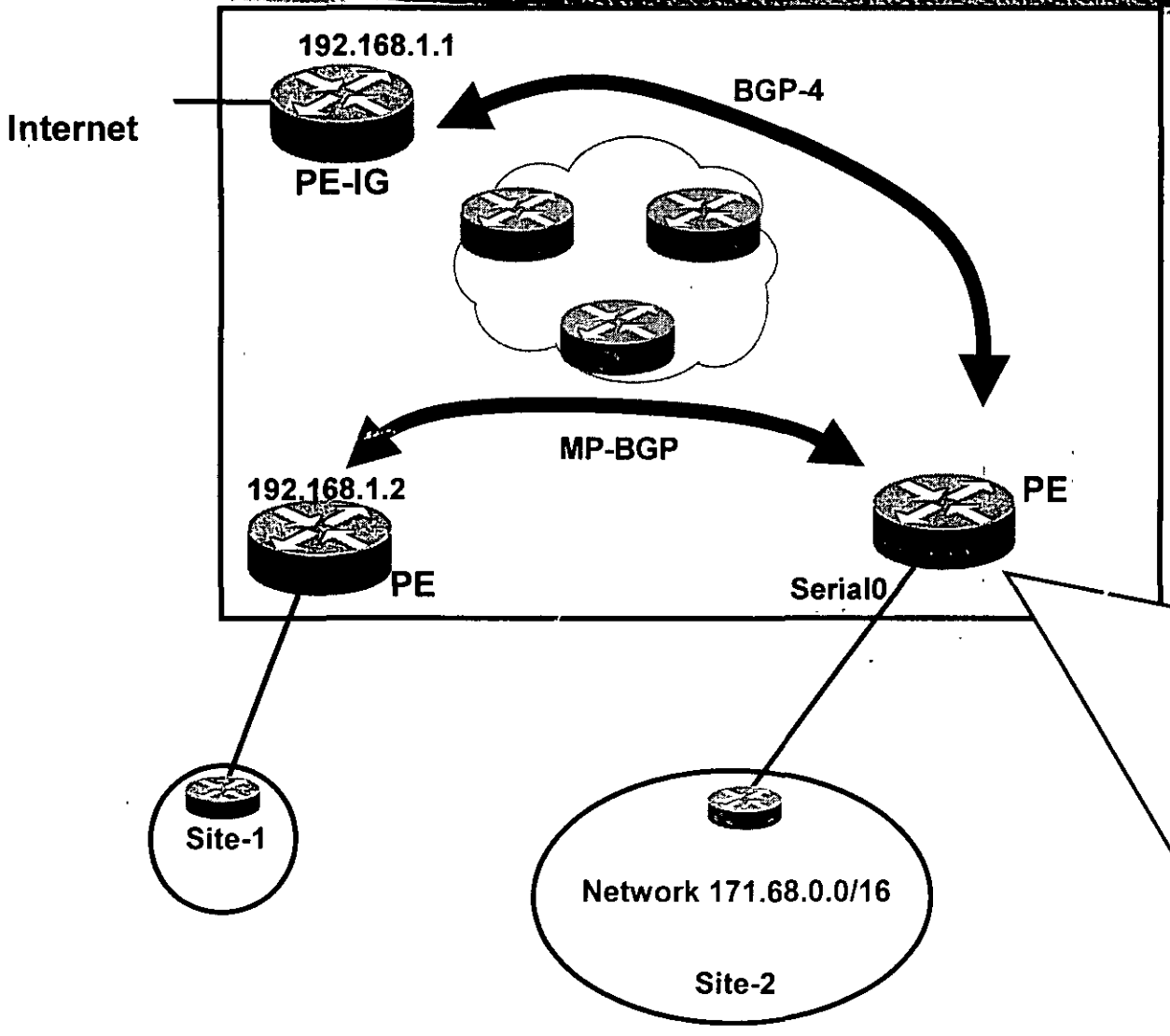
- PE router originates CE routes for the Internet
  - Customer (site) routes are known in the site VRF

    Not in the global table
  - The PE/CE interface is NOT known in the global table. However:

    A static route for customer routes and pointing to the PE/CE interface is installed in the global table
  - This static route is redistributed into BGP-4 global table and advertised to the Internet Gateway
- The Internet gateway knows customer routes and with the PE address as next-hop

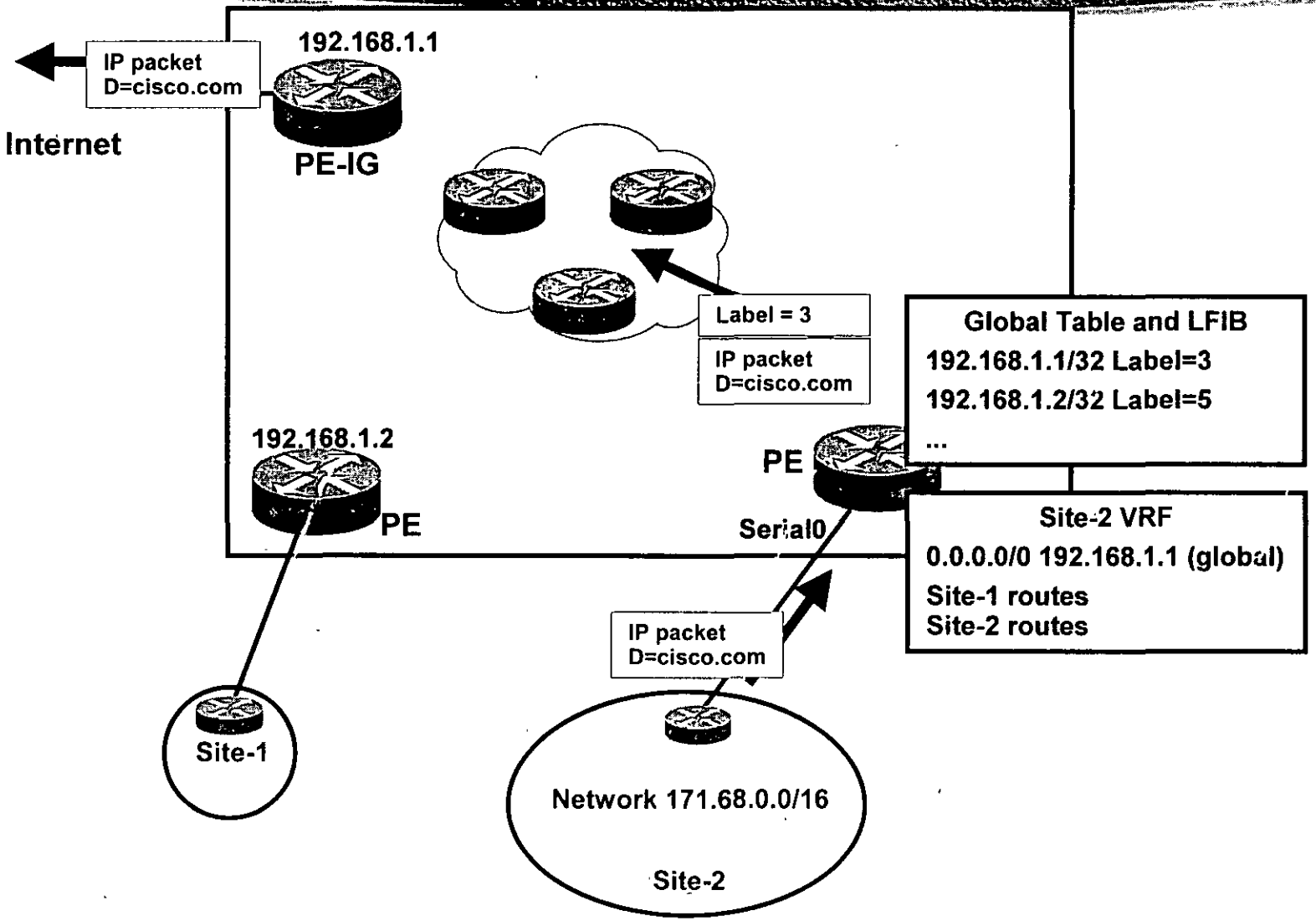
VPN Internet routing: specific default route

- The Internet Gateway specified in the default route (into the VRF) need NOT to be directly connected
- Different Internet gateways can be used for different VRFs
- Using default route for Internet routing does NOT allow any other default route for intra-VPN routing
  - As in any other routing scheme




```
ip vrf VPN-A
rd 100:1
route-target both 100:1
!
Interface Serial0
ip address 192.168.10.1 255.255.255.0
ip vrf forwarding VPN-A
!
Router bgp 100
no bgp default ipv4-unicast
network 171.68.0.0 mask 255.255.0.0
neighbor 192.168.1.1 remote 100
neighbor 192.168.1.1 activate
neighbor 192.168.1.1 next-hop-self
neighbor 192.168.1.1 update-source loopback0
!
address-family ipv4 vrf VPN-A
 neighbor 192.168.10.2 remote-as 65502
 neighbor 192.168.10.2 activate
 exit-address-family
!
address-family vpnv4
 neighbor 192.168.1.2  activate
exit-address-family
!
ip route 171.68.0.0 255.255.0.0 Serial0
ip route vrf VPN-A 0.0.0.0 0.0.0.0 192.168.1.1 global
```

Internet routing: define default route



Internet routing: specific default route

- PE routers need not to hold the Internet table
- PE routers will use BGP-4 sessions to originate customer routes
- Packet forwarding is done with a single label identifying the Internet Gateway IP address
  - More labels if Traffic Engineering is used

Internet Routing
Dedicated (sub)Interfaces

- If CE wishes to receive and announce routes from/to the Internet
  - A dedicated BGP session is used over a separate (sub) interface
  - The PE imports CE routes into the global routing table and advertise them to the Internet

    The interface is not part of any VPN and does not use any VRF
  - Default route or Internet routes are exported to the CE

    PE needs to have Internet routing table

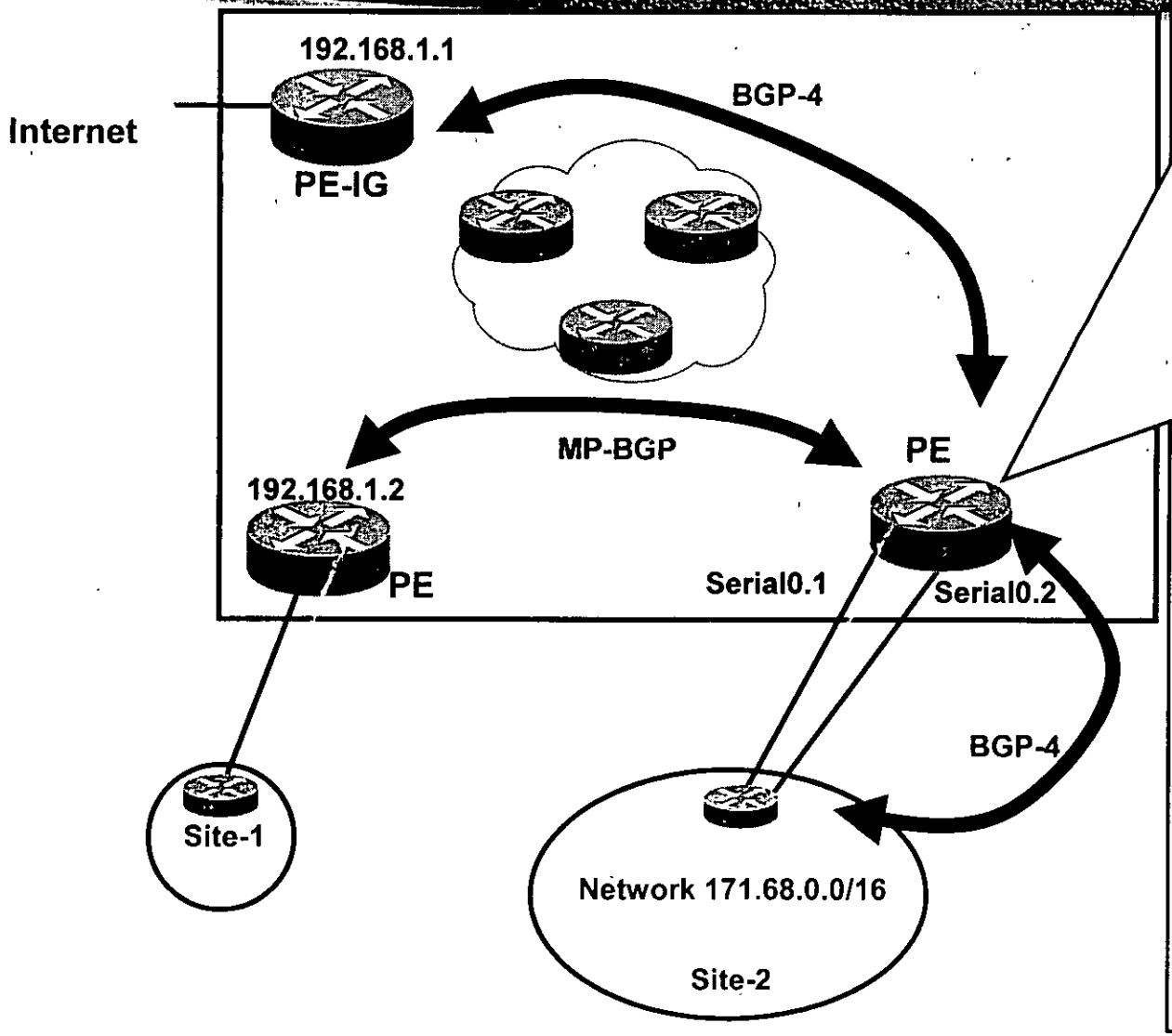
Internet Routing Dedicated (sub)interfaces

- The PE uses separate (sub)interfaces with the CE
  - One (sub)interface for VPN routing

    associated to a VRF
    Can be a tunnel interface
  - One (sub)interface for Internet routing

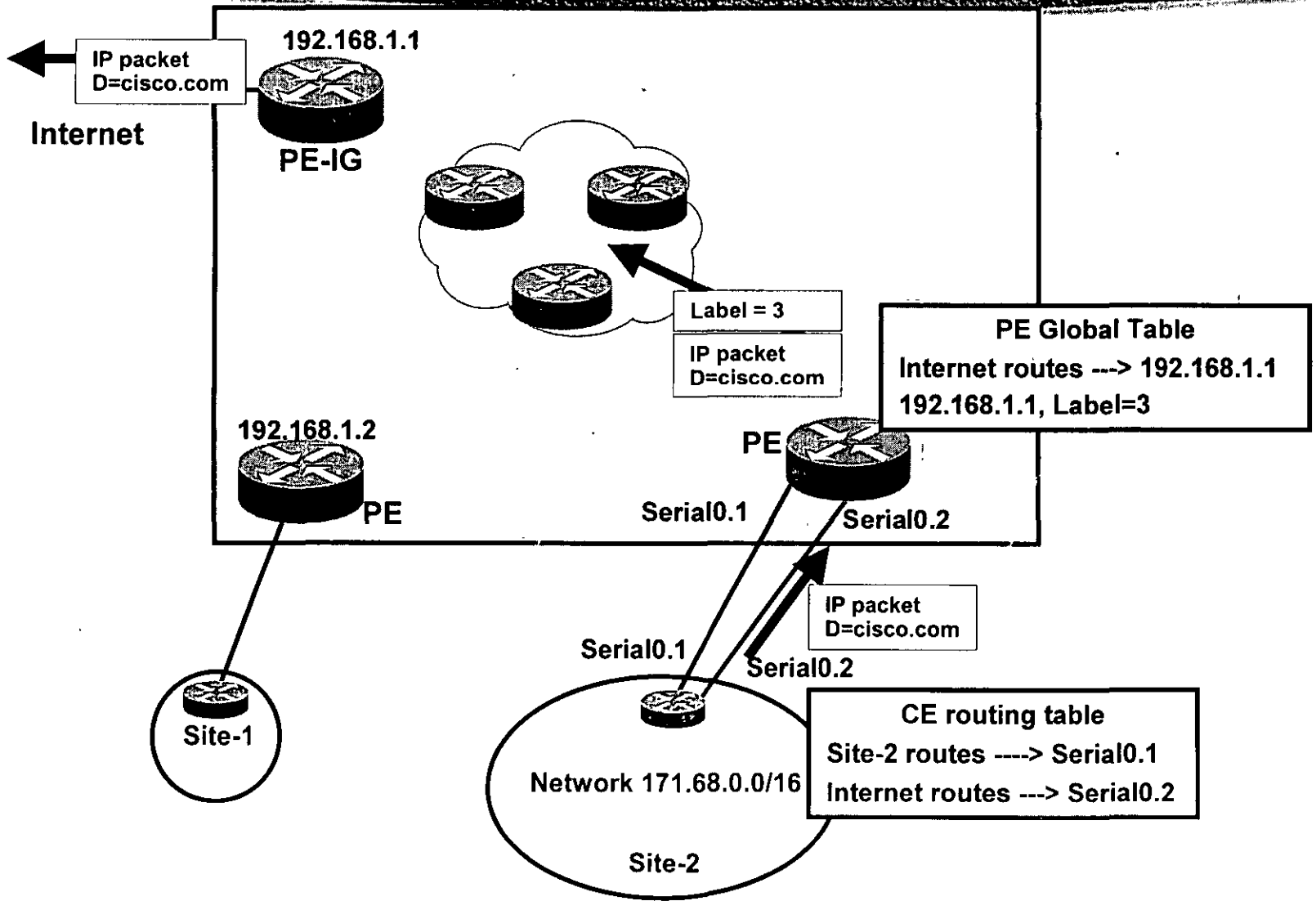
    Associated to the global routing table

Internet Routing (sub)Interfaces




```
ip vrf VPN-A
rd 100:1
route-target both 100:1
!
Interface Serial0
no ip address
!
Interface Serial0.1
ip address 192.168.20.1 255.255.255.0
ip vrf forwarding VPN-A
!
Interface Serial0.2
ip address 171.68.10.1 255.255.255.0
!
Router bgp 100
no bgp default ipv4-unicast
neighbor 192.168.1.1 remote 100
neighbor 192.168.1.1 activate
neighbor 192.168.1.1 next-hop-self
neighbor 192.168.1.1 update-source loopback0
neighbor 171.68.10.2 remote 502
!
address-family ipv4 vrf VPN-A
 neighbor 192.168.20.2 remote-as 502
 neighbor 192.168.20.2 activate
 exit-address-family
!
address-family vpnv4
 neighbor 192.168.1.2  activate
exit-address-family
```

Internet Routing via Static (Custom) Interfaces



Agenda

- Concepts and goals
- Terminology
- Connection model
- Forwarding
- Mechanisms
- Topologies
- Scaling
- BGP-4 Enhancements
  - Cap. Negotiation, MPLS, Route Refresh, ORF
- Configuration

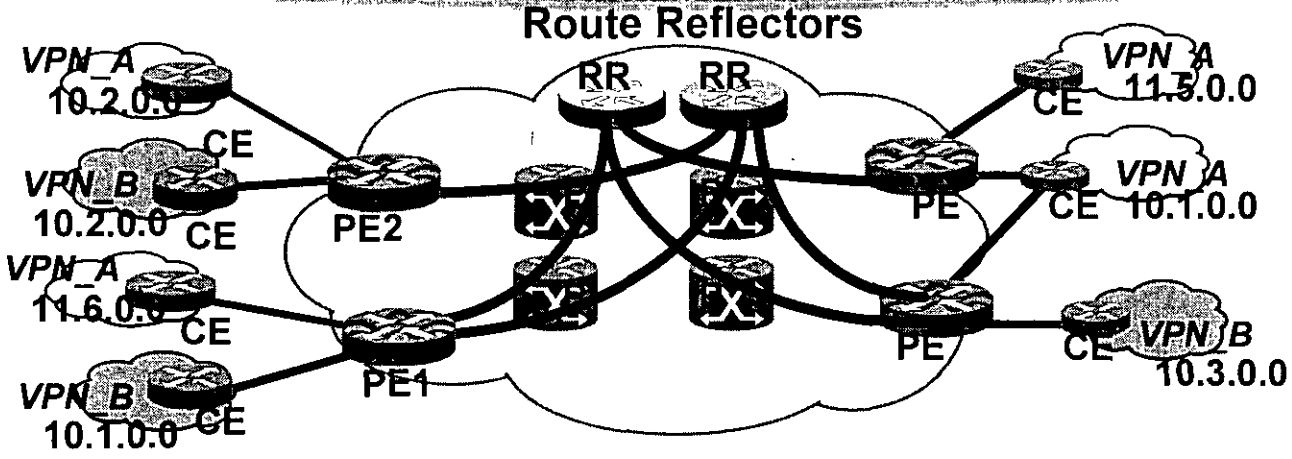
- Existing BGP techniques can be used to scale the route distribution: route reflectors
- Each edge router needs only the information for the VPNs it supports

  Directly connected VPNs
- RRs are used to distribute VPN routing information

Scaling

- **Very highly scalable:**
  - **Initial VPN release: 1000 VPNs x 1000 sites/VPN = 1,000,000 sites**
  - **Architecture supports 100,000+ VPNs, 10,000,000+ sites**
  - **BGP "segmentation" through RRs is essential !!!!**
- **Easy to add new sites**
  - **configure the site on the PE connected to it**
  - **the network automagically does the rest**

MPLS VPN Scaling BGP

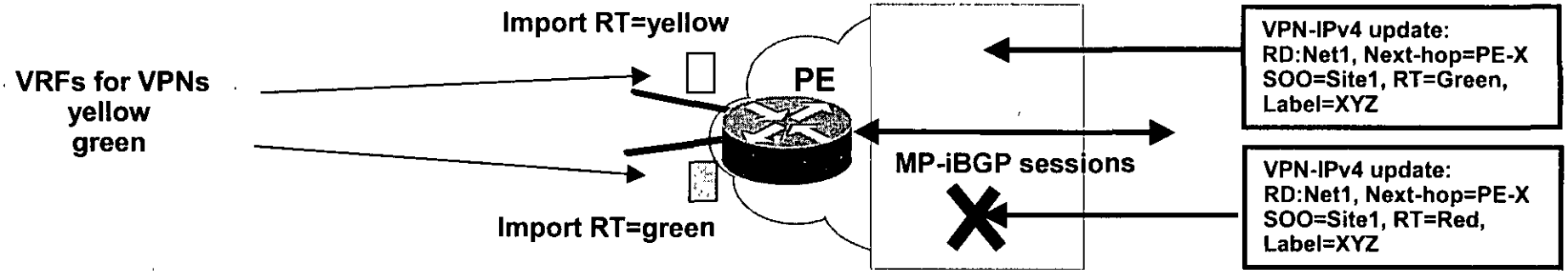


- Route Reflectors may be partitioned
  - Each RR store routes for a set of VPNs
- Thus, no BGP router needs to store ALL VPNs information
- PEs will peer to RRs according to the VPNs they directly connect

Scaling: Updates filtering

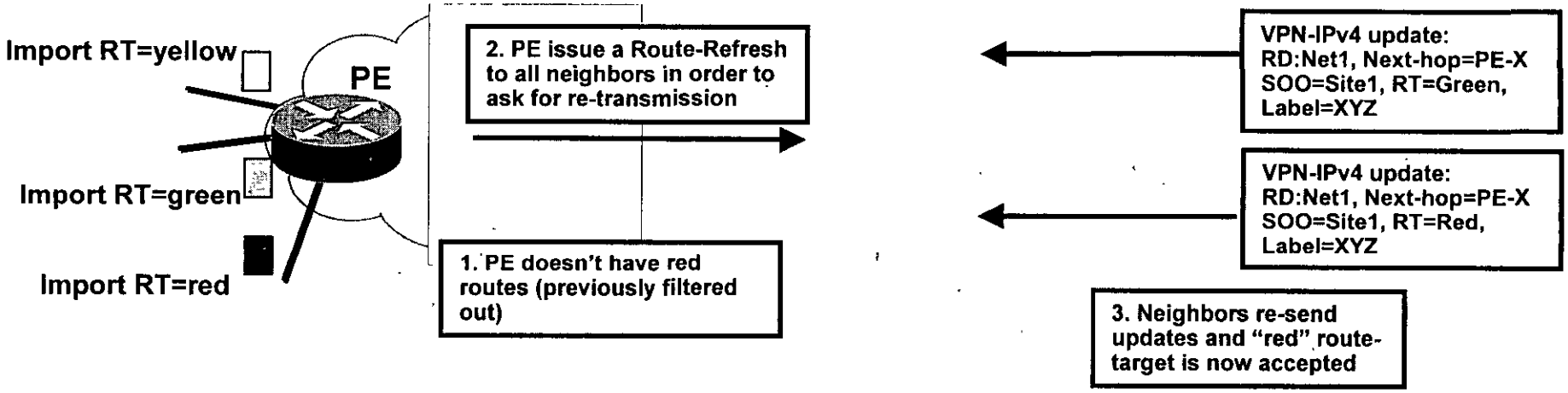
- iBGP full mesh between PEs results in flooding all VPNs routes to all PEs
- Scaling problems when large amount of routes. In addition PEs need only routes for attached VRFs
- Therefore each PE will discard any VPN-IPv4 route that hasn't a route-target configured to be imported in any of the attached VRFs
- This reduces significantly the amount of information each PE has to store
- Volume of BGP table is equivalent of volume of attached VRFs (nothing more)

Installing Updates: Filtering



- Each VRF has an ***import*** and ***export*** policy configured
- Policies use ***route-target*** attribute (extended community)
- PE receives MP-iBGP updates for VPN-IPv4 routes
- If route-target is equal to any of the import values configured in the PE, the update is accepted
- Otherwise it is silently discarded

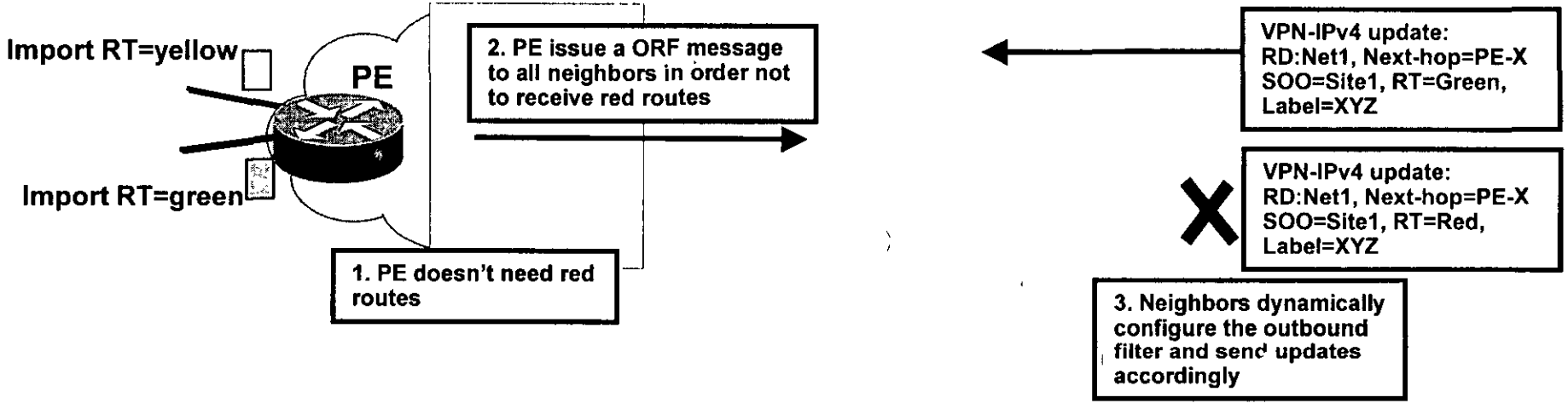
VPN Scaling
Route Refresh



- Policy may change in the PE if VRF modifications are done
  - New VRFs, removal of VRFs
- However, the PE may not have stored routing information which become useful after a change
- PE request a re-transmission of updates to neighbors
  - Route-Refresh

Cisco Systems

Outbound Route Filters



- PE router will discard update with unused route-target
- Optimisation requires these updates NOT to be sent
- Outbound Route Filter (ORF) allows a router to tell its neighbors which filter to use prior to propagate BGP updates

Agenda

- Concepts and goals
- Terminology
- Connection model
- Forwarding
- Mechanisms
- Topologies
- Scaling
- BGP-4 Enhancements
  - Cap. Negotiation, MPLS, Route Refresh, ORF
- Configuration

VPN Extranet

- BGP attribute used to define
  - SOO (Site of Origin Identifier)

    Routers where the route has been originated
  - Route-target

    Set of routers the route has to be exported to
- This enable the Closed User Group functionality
- Set by PE routers in order to define import/export policies in a per site/VRF basis

Extended Community attribute Type code: TBD

Type Field: 2 bytes
Value Field: 6 bytes

Types 0 through 0x7FFF inclusive are assignable by IANA.
Types 0x8000 through 0xFFFF inclusive are vendor-specific.

Extcommunity

- **High order bit of the type field 0x00**
  - **Administrator sub-field: 2 bytes (AS#)**
  - **Assigned Number sub-field: 4 bytes**
- **High order bit of the type field 0x01**
  - **Administrator sub-field: 4 bytes (IP address)**
  - **Assigned Number sub-field: 2 bytes**

Router Origin Community

- Router Origin Community
  - Identifies one or more routers that inject a set of routes (that carry this Community) into BGP
  - The Type field for the Route Origin Community is 0x0001 or 0x0101
  - Similar to the Site of Origin (SOO)

    Site of Origin will use a different code

Route Target Community

- **Route Target Community**
  - **Identifies one or more routers that may receive a set of routes (that carry this Community) carried by BGP**
  - **The Type field for the Route Target Community is 0x0002 or 0x0102.**

Protocol BGP

- Extension to the BGP protocol in order to carry routing information about other protocols
  - Multicast
  - MPLS
  - IPv6
  - IPX
  - ...
- Exchange of Multi-Protocol NLRI must be negotiated at session set up

  BGP Capabilities negotiation

MP-BGP RFCs

- New non-transitive and optional BGP attributes
  - MP_REACH_NLRI

    "Carry the set of reachable destinations together with the next-hop information to be used for forwarding to these destinations" (RFC2283)
  - MP_UNREACH_NLRI

    Carry the set of unreachable destinations
- Attribute contains one or more Triples

  Address Family Information (AFI)

  Next-Hop Information

  NLRI

VPN-IPv4 address in BGP-4

- **Labelled VPN-IPV4 address appears in BGP NLRI**

  AFI = 1 - Sub-AFI = 128

- **NLRI are encoded as one or more triples**

  Length: total length of Label + prefix (RD included)

  Label: 24 bits

  The LABEL field carries one or more labels (stack)

  Prefix: RD (64 bits) + IPv4 prefix (32 bits)

Cisco Systems

IPv4 addresses: BGP-4

- **The label is assigned by the router originating the NLRI**
  - **i.e.: the router identified by the next-hop value**
- **The label is changed by the router that modifies the next-hop value**
  - **Typically the EBGP speaker**
  - **Or iBGP forwarder configured with *next-hop-self***

VPN-IPv4 address in BGP-4

- **Next-hop address must be of the same family of the NLRI**
  - **The next-hop will be a VPN-IPv4 address with RD set to 0**
- **BGP will consider two VPN-IPV4 comparable even with different labels**
  - **A withdrawn of a VPN-IPv4 address will be considered for all NLRI corresponding to the VPN-IPV4 address, whatever are the different assigned labels**

Capabilities Negotiation

- BGP routers establish BGP sessions through the OPEN message
- OPEN message contains optional parameters
- BGP session is terminated if OPEN parameters are not recognised
- A new optional parameter: CAPABILITIES

Capabilities Negotiation

- **A BGP router sends an OPEN message with CAPABILITIES parameter containing its capabilities:**

  Multiprotocol extension

  Route Refresh

  Co-operative Route Filtering

  Multiple routes for same destination

  ...

Capabilities Negotiation

- BGP routers determine capabilities of their neighbors by looking at the capabilities parameters in the open message
- Unknown or unsupported capabilities ***may*** trigger the transmission of a NOTIFICATION message

  "The decision to send the NOTIFICATION message and terminate peering is local to the speaker. Such peering should not be re-established automatically"
  draft-ietf-idr-bgp4-cap-neg-02

- **BGP routers use BGP-4 Multiprotocol Extension to carry label (label) mapping information**
  - **Multiprotocol Extension capability**
  - **Used to negotiate the Address Family Identifier**

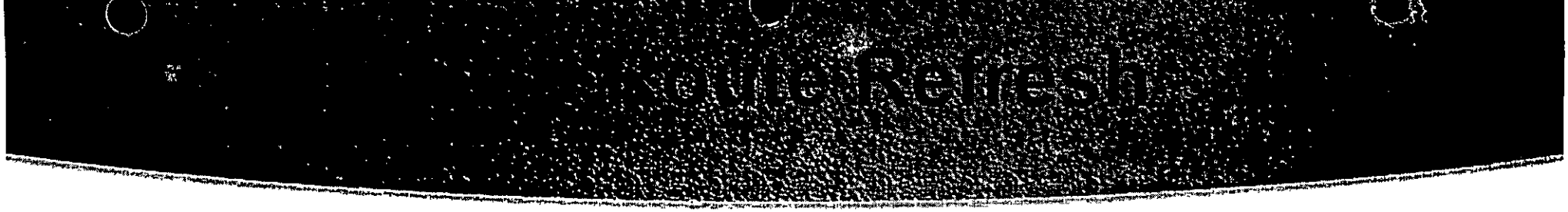
    AFI = 1

    Sub-AFI = 128 for MPLS-VPN

Route Refresh

- New BGP Capability: Route Refresh
- Allows a router to request to any neighbor the re-transmission of BGP updates
  - Useful when inbound policy has been modified
  - Similar to Cisco "soft-reconfiguration"

    without need to store any route
- BGP speakers may send "Route-Refresh" message only to neighbors from which the capability has been exchanged



- When the inbound policy has been modified, the BGP speaker sends a Route-Refresh message to its neighbors
  - With AFI, Sub-AFI attributes
- Neighbors will re-transmit all routes for that particular AFI and Sub-AFI

Outbound Route Filter

- In order to reduce amount of BGP traffic and CPU used to process updates, routers exchange filter configurations
- BGP speakers advertise to downstream neighbors, the outbound filter(s) they have to use
- Filters are described in ORF entries

  Outbound Route Filter

- ORF entries are part of the Route-Refresh message

Outbound Route Filter

- ORF capability must be negotiated during session set-up
  - Capability negotiation
- ORF capable BGP speaker will install ORFs per neighbor
- Each ORF will be defined by the upstream neighbor through route-refresh messages

ORF Entry

- ORF Entry
  - AFI/Sub-AFI

    Filter will apply only to selected address families
  - ORF-Type

    Determine the content of ORF-Value

    NLRI is one ORF-Type

    NLRI is used to match IP addresses (subnets)

ORF Entry

- ORF Entry
  - Action
    - ADD: Add an ORF entry to the current ORF
    - DELETE: Delete a previously received ORF entry
    - DELETE ALL: Delete all existing ORF entries
  - Match
    - PERMIT: Pass routes that match the ORF entry
    - DENY: Do not pass routes that match the ORF entry

ORF Entry

- ORF Entry
  - ORF-Value (for ORF-Type=NLRI) is <Scope,NLRI>

    Scope

    EXACT: Remote peer should consider routes equal to the NLRI specified in the ORF

    REFINE: Remote peer should consider routes that are part of a subset of the NLRI specified in the ORF

    NLRI: <length, prefix>
- Multiple ORF entries will follow longest match

- ORF Entries are carried in BGP Route-Refresh messages
- AFI/Sub-AFI are encoded into the AFI/Sub-AFI field of the route refresh message
- ORF-Type is encoded after AFI/Sub-AFI field
- WHEN-TO-REFRESH field
  - IMMEDIATE: apply the filter immediately
  - DEFER: wait for subsequent route-refresh message

    with same AFI/Sub-AFI and without any ORF entry

    or

    with same AFI/Sub-AFI and with IMMEDIATE when-to-refresh field
- ORF-Type to be extended for Extended Communities

Agenda

- Concepts and goals
- Terminology
- Connection model
- Forwarding
- Mechanisms
- Topologies
- Scaling
- BGP-4 Enhancements
  - Cap. Negotiation, MPLS, Route Refresh, ORF
- Configuration

VPN Configuration

- VPN knowledge is on PE routers
- PE router have to be configured for
  - VRF and Route Distinguisher
  - VRF import/export policies (based on Route-target)
  - Routing protocol used with CEs
  - MP-BGP between PE routers
  - BGP for Internet routers

    With other PE routers

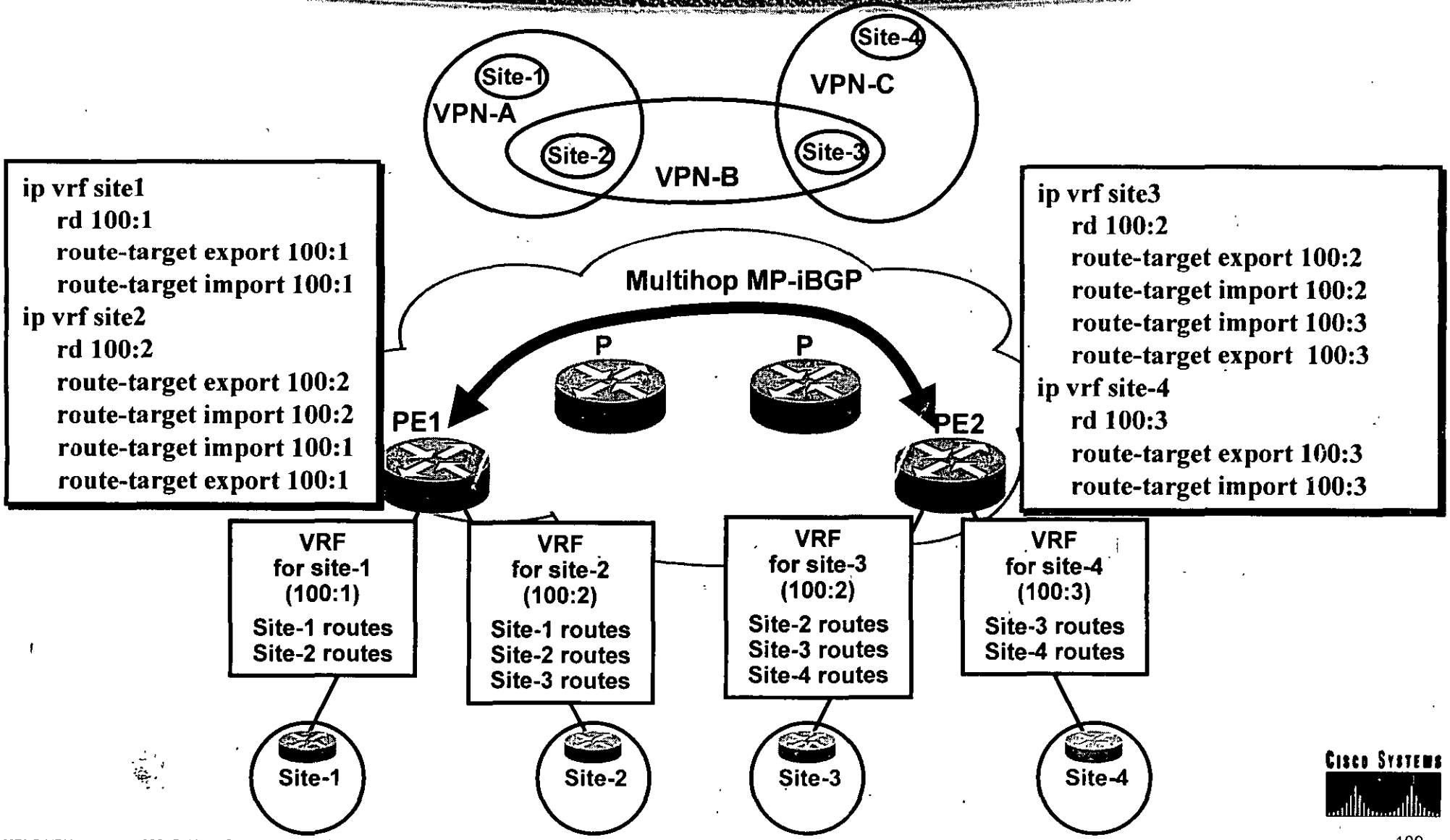
    With CE routers

Configuration: Route Distinguisher

- RD is configured on PE routers (for each VRF)
- VRFs are associated to RDs in each PE
- Common (good) practice is to use the same RD for the same VPN in all PEs
  - But not mandatory
- VRF configuration command

```
ip vrf <vrf-symbolic-name>
  rd <route-distinguisher-value>
  route-target import <Import route-target community>
  route-target export <Import route-target community>
```

VPN Configuration



PE-CE routing protocols

- PE/CE may use BGP, RIPv2 or Static routes
- A routing context is used for each VRF
- Routing contexts are defined within the routing protocol instance

  Address-family router sub-command

```
Router rip
  version 2
  address-family ipv4 vrf <vrf-symbolic-name>
  ...
    any common router sub-command
  ...
```

PE-CE configuration options: routing protocols

- **BGP uses same "address-family" command**

```
Router BGP <asn>
  ...
  address-family ipv4 vrf <vrf-symbolic-name>
  ...
    any common router BGP sub-command
  ...
```

- **Static routes are configured per VRF**

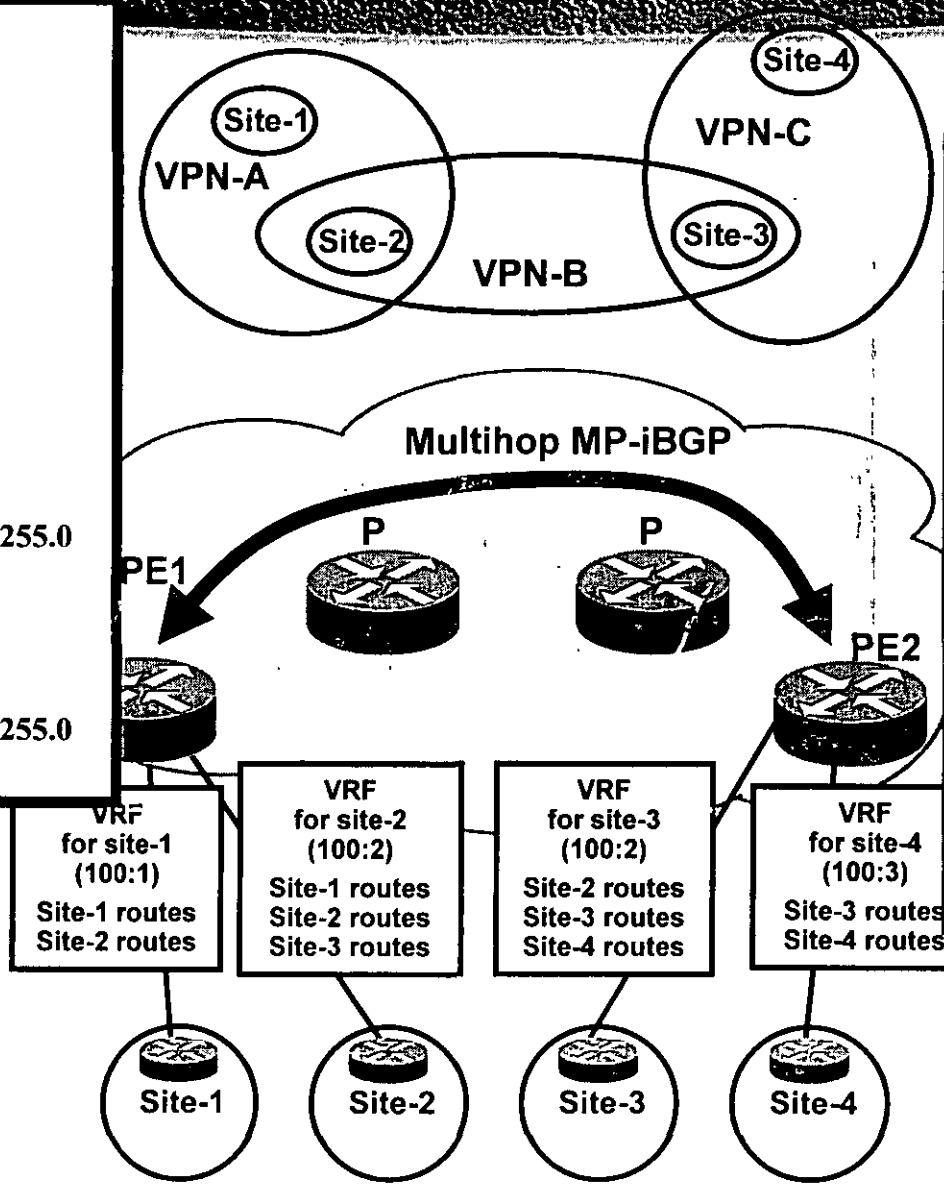
```
ip route vrf <vrf-symbolic-name> ...
```

Configuration Commands

- **All show commands are VRF based**
  - **Show ip route vrf <vrf-symbolic-name> ...**
  - **Show ip protocol vrf <vrf-symbolic-name>**
  - **Show ip cef <vrf-symbolic-name> …**
  - **…**
- **PING and Telnet commands are VRF based**
  - **telnet /vrf <vrf-symbolic-name>**
  - **ping vrf <vrf-symbolic-name>**

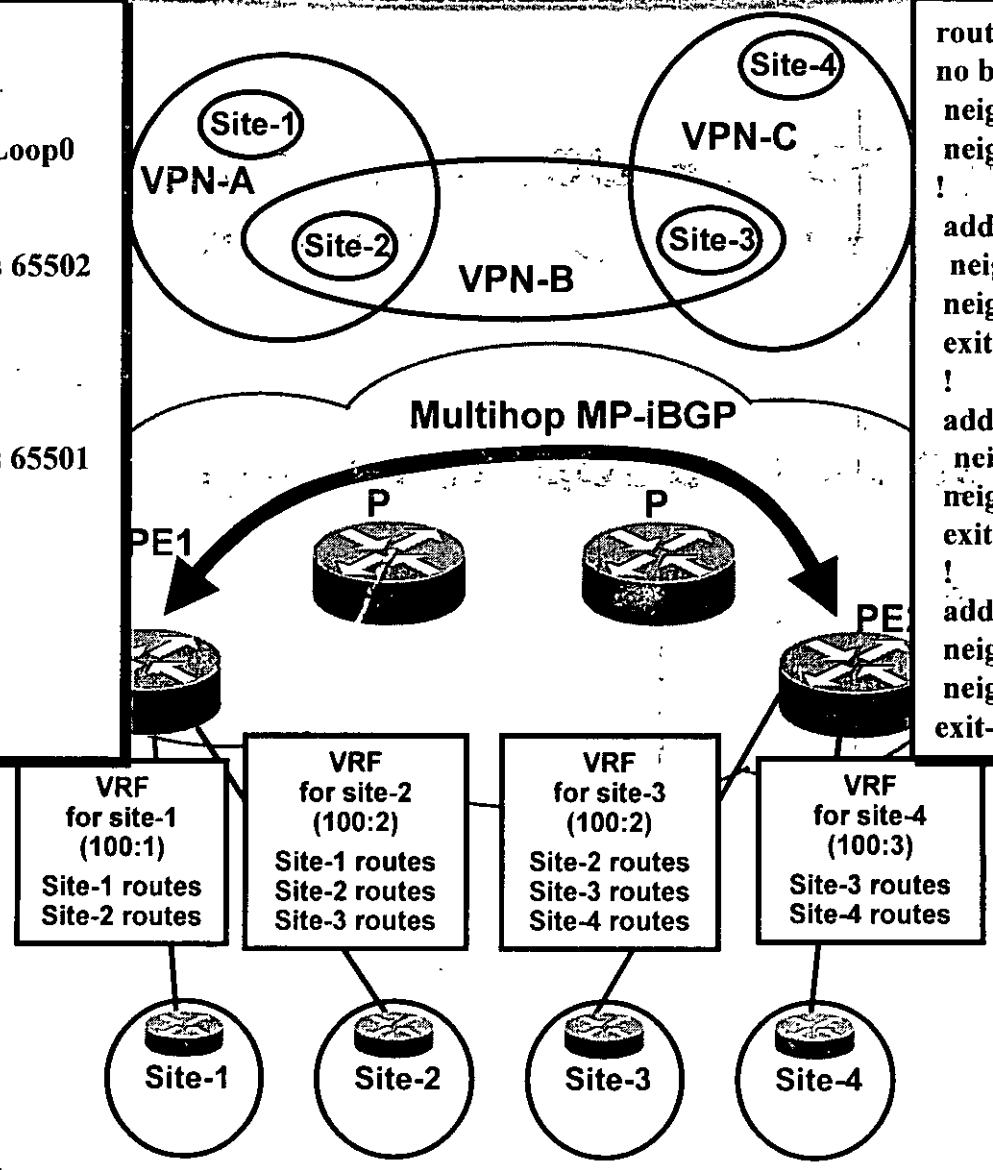
... configuration ... routing protocols ...

```
ip vrf site1
    rd 100:1
    route-target export 100:1
    route-target import 100:1
ip vrf site2
    rd 100:2
    route-target export 100:2
    route-target import 100:2
    route-target import 100:1
    route-target export 100:1
!
interface Serial3/6
 ip vrf forwarding site1
 ip address 192.168.61.6 255.255.255.0
 encapsulation ppp
!
interface Serial3/7
 ip vrf forwarding site2
 ip address 192.168.62.6 255.255.255.0
 encapsulation ppp
```




```
ip vrf site3
    rd 100:2
    route-target export 100:2
    route-target import 100:2
    route-target import 100:3
    route-target export 100:3
ip vrf site-4
    rd 100:3
    route-target export 100:3
    route-target import 100:3
!
interface Serial4/6
 ip vrf forwarding site3
 ip address 192.168.73.7 255.255.255.0
 encapsulation ppp
!
interface Serial4/7
 ip vrf forwarding site4
 ip address 192.168.74.7 255.255.255.0
 encapsulation ppp
```

```
router bgp 100
no bgp default ipv4-unicast
 neighbor 7.7.7.7 remote-as 100
 neighbor 7.7.7.7 update-source Loop0
!
 address-family ipv4 vrf site2
 neighbor 192.168.62.2 remote-as 65502
 neighbor 192.168.62.2 activate
 exit-address-family
 !
 address-family ipv4 vrf site1
 neighbor 192.168.61.1 remote-as 65501
 neighbor 192.168.61.1 activate
 exit-address-family
 !
 address-family vpnv4
 neighbor 7.7.7.7 activate
 neighbor 7.7.7.7 next-hop-self
exit-address-family
```




```
router bgp 100
no bgp default ipv4-unicast
 neighbor 6.6.6.6 remote-as 100
 neighbor 6.6.6.6 update-source Loop0
!
 address-family ipv4 vrf site4
 neighbor 192.168.74.4 remote-as 65504
 neighbor 192.168.74.4 activate
 exit-address-family
 !
 address-family ipv4 vrf site3
 neighbor 192.168.73.3 remote-as 65503
 neighbor 192.168.73.3 activate
 exit-address-family
 !
 address-family vpnv4
 neighbor 6.6.6.6 activate
 neighbor 6.6.6.6 next-hop-self
exit-address-family
```

Summary

- Supports large scale VPN services
- Increases value add by the VPN Service Provider
- Decreases Service Provider's cost of providing VPN services
- Mechanisms are general enough to enable VPN Service Provider to support a wide range of VPN customers
- See RFC2547