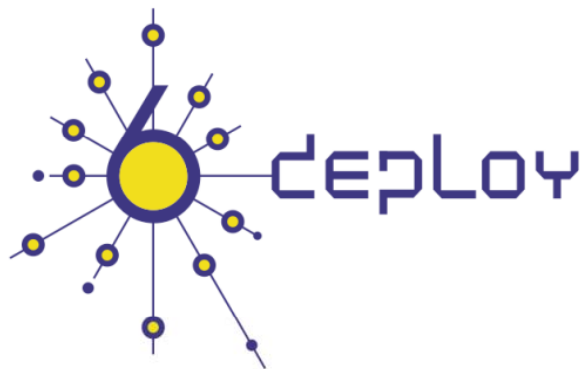


Curso IPv6

WALC 2009

Bogotá – Colombia

21 al 25 Septiembre 2009



César Olvera (cesar.olvera@consulintel.es)

Alvaro Vives (alvaro.vives@consulintel.es)



Contenido del curso (1)

- **Bloque 1. Tutorial IPv6**

1. Introducción a IPv6
2. Formatos de cabeceras y tamaño de paquetes
3. Direccionamiento IPv6
4. ICMPv6, Neighbor Discovery y DHCPv6
5. Seguridad IPv6
6. Encaminamiento con IPv6
7. Mecanismos de Transición
8. Movilidad IPv6



Contenido del curso (2)

- **Bloque 2. Otros Aspectos Avanzados**
 9. Calidad de Servicio (QoS)
 10. Multicast
 11. Multi-homing
 12. Porting de aplicaciones
 13. Gestión SNMP sobre IPv6
 14. IPv6 sobre MPLS
 15. DNS IPv6





Bloque 1

Tutorial IPv6



6. Encaminamiento con IPv6

6.1 Conceptos de Encaminamiento

6.2 RIP

6.3 EIGRP

6.4 OSPF

6.5 IS-IS

6.6 BGP

6.7 Encaminamiento Estático





6.1 Conceptos de Encaminamiento



Visión General Encaminamiento

- Los encaminadores deben saber como llegar al destino final de los paquetes que se le reenvían
- Las rutas estáticas no son adecuadas para redes medianas ni grandes
 - Tampoco para las pequeñas si se producen cambios en la topología de red
- Los protocolos de encaminamiento proporcionan un método automático de generar las tablas de encaminamiento
 - Tienen en cuenta cambio de la topología de red



Tipos de protocolos de encaminamiento

- Atendiendo al ámbito:
 - IGP (Interior Border Gateway)
 - EGP (Exterior Border Gateway)
- En los de tipo IGP
 - Atendiendo a la metodología de propagación
 - Vector Distancia
 - Estado de Link
 - Atendiendo al tipo de rutas que propagan
 - Classful
 - Classless



Criterios de selección IGP

- La selección de uno u otro depende de varios factores:
 - Topología de la intrared
 - Tipos de rutas a propagar
 - Tiempo de convergencia
 - Criterio de cálculo de métricas de la ruta.
 - Escalabilidad
 - Seguridad
- Guía completa en
 - <http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2003.htm>



Protocolos IGP

	VD	LS	Classful	Classless	Seguridad
RIPv1	X		X		
RIPv2	X			X	
IGRP	X		X		
EIGRP	X			X	X
OSPF		X		X	X
IS-IS		X		X	

Protocolos EGP

- No hay muchas alternativas
- BGP
 - El estándar “de facto”



Encaminamiento IPv6

- Mismo mecanismo CIDR “longest-prefix match” que actualmente en IPv4
- Cambios mínimos respecto de los protocolos existentes para encaminado en IPv4 (gestión de direcciones mayores)
 - Unicast: **RIP, OSPF, IS-IS, BGP4+, ...**
 - Multicast: **MOSPF, PIM, ...**
- Se puede utilizar la cabecera de routing con direcciones unicast para encaminar paquetes a través de regiones concretas
 - Por ejemplo, para la selección de proveedores, políticas, prestaciones, etc.



6.2 RIP



RIP IPv6

- RIP para IPv6 o RIPng esta definido en el RFC2080: RIPng for IPv6
- Extiende RIPv1 y RIPv2 para soportar
 - Direcciones de 128 bits
 - Encaminamiento de prefijos IPv6
 - Uso de la dirección FF02::9, del grupo multicast all-RIP-routers, como la dirección destino de los mensajes de update de RIP



6.3 EIGRP



EIGRP IPv6

- Enhanced Interior Gateway Routing Protocol (EIGRP) desarrollado por Cisco es una versión mejorada del IGRP
- EIGRP usa al igual que IGRP el algoritmo de vector de distancias e información de distancia, además de usar algunas características asociadas normalmente con los protocolos del estado de enlace
- Las propiedades de convergencia y la eficiencia operativa son mejores en EIGRP que en IGRP
- EIGRP para IPv4 se ejecuta sobre transporte IPv4, comunica solo peers IPv4 y anuncia solo rutas IPv4, mientras que EIGRP para IPv6 hace lo mismo pero para IPv6
- EIGRP para IPv4 y EIGRP para IPv6 se configuran y gestionan de manera separada, aunque la configuración es similar en ambos casos
- EIGRP para IPv6 esta soportado desde las versiones de IOS 12.4(6)T y 12.2(33)SRB



6.4 OSPF



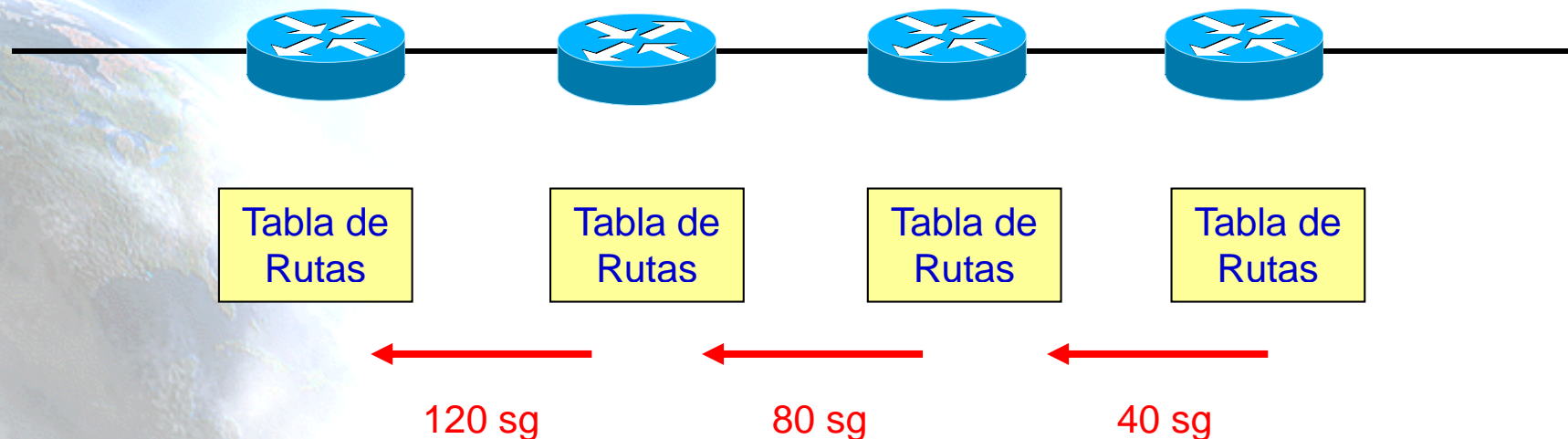
Visión General OSPF (1)

- Protocolo de encaminamiento IGP de tipo “link-state” que intenta dar solución a las necesidades más avanzadas de los Sistemas Autónomos más exigentes:
 - soporte VLSM (Variable Length Subnet Masking)
 - autenticación
 - rápida convergencia cuando se producen cambios en la topología de la red
 - propagación de rutas por medio de multicast
 - marcado de rutas aprendidas de protocolos EGP
 - consideración del ancho de banda en la elección de la mejor ruta
 - etc.
- Los encaminadores conocen la topología de la red por medio del algoritmo SPF



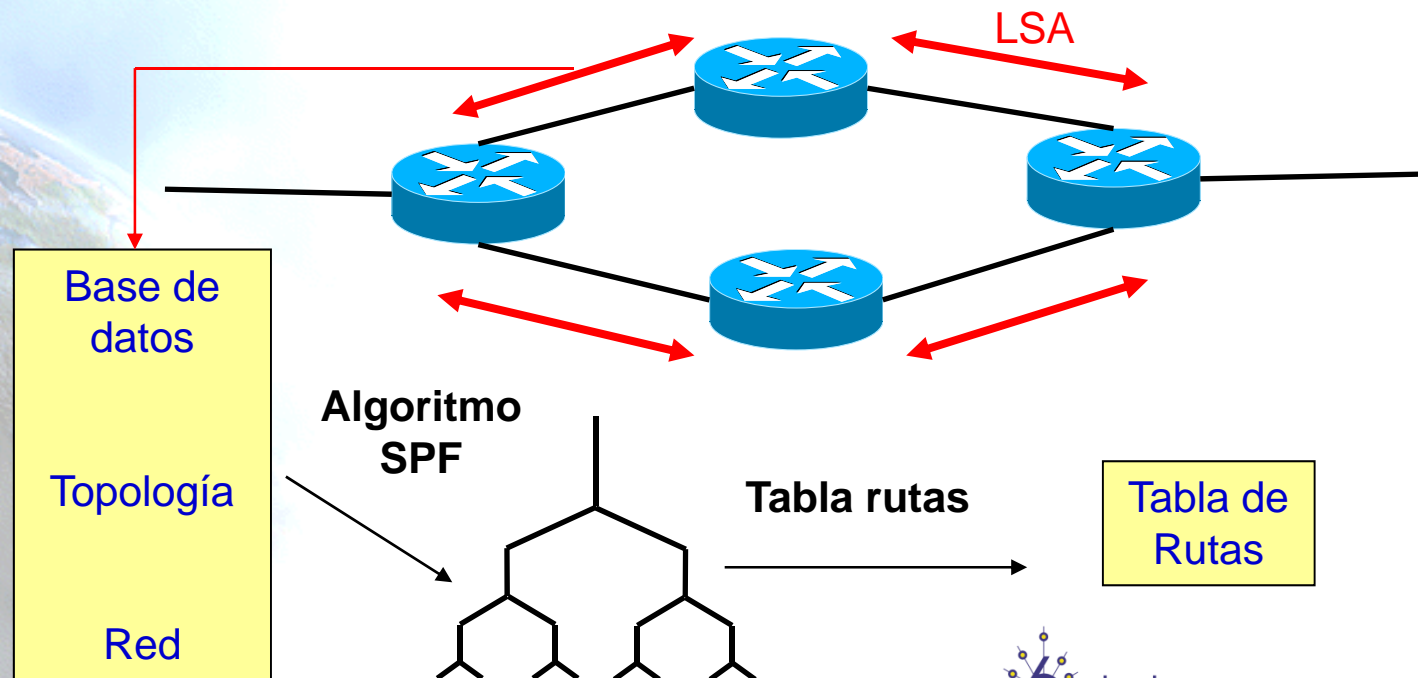
Visión General OSPF (2)

- Los protocolos basados en DV (Distance Vector) envían periódicamente a sus vecinos la tabla de ruta
 - Problemas de ancho de banda
 - Problemas de tiempo de convergencia



Visión General OSPF (3)

- Los protocolos basados en LS (Link-State) solo envían los cambios en los LSA (Link-State Advertisements)
 - Menor ancho de banda
 - Convergencia más rápida
 - Soporta mayores redes



Visión General OSPF (4)

- OSPF utiliza el protocolo Hello para:
 - Determinar qué interfaces recibirán los LSAs
 - Determinar qué otros encaminadores vecinos existen
 - Determinar si los encaminadores vecinos siguen activos (keepalive)
- Los encaminadores envían LSAs (Link-State Advertisements) a todos los encaminadores de la misma unidad jerárquica por medio de una dirección multicast e incluyen entre otros:
 - Prefijo de red
 - Máscara de red
 - Tipo de red
 - Encaminadores conectados
 - Etc.
- Todos construyen la misma base de datos topológica a partir de los LSAs recibidos
 - Se obtiene la nueva tabla de rutas a partir de la nueva topología.

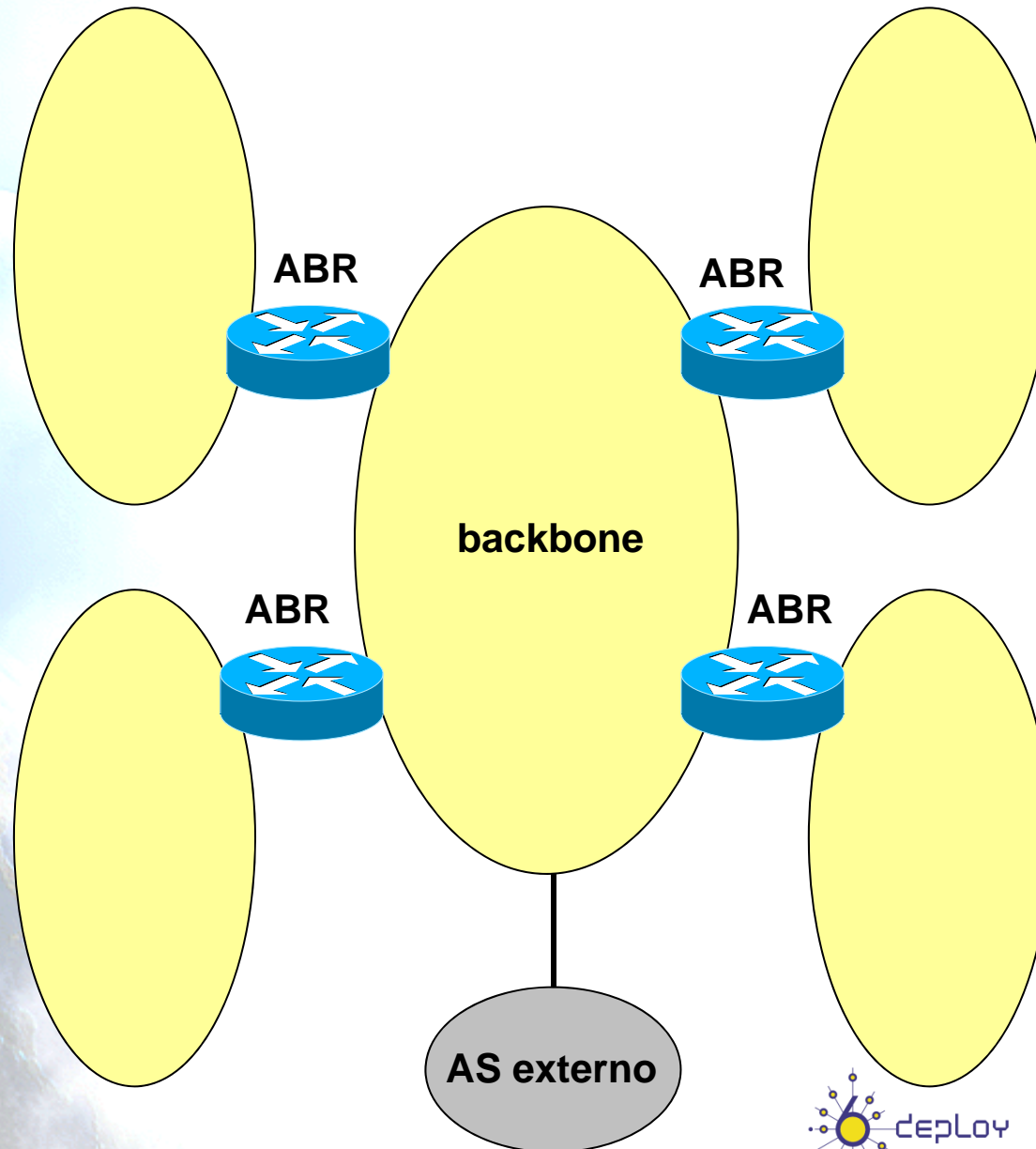


Visión General OSPF (5)

- La métrica de OSPF se calcula como la suma del coste de atravesar diversos nodos hasta el destino final
 - se calcula basándose en el ancho de banda de las interfaces y es configurable por el usuario.
- OSPF divide el AS en pequeñas unidades jerárquicas, cada una de las cuales se conecta al “backbone” por medio de un ABR (Area Border Router)
 - Reduce la carga de procesamiento y memoria



Visión General OSPF (6)



Visión General OSPF (7)

- Los LSAs describen la topología de un área jerárquica
- Existen diversos tipos

Código	LSA	Link-State ID
1	Router LSA	Originating router ID of the router
2	Network LSA	Interface IP address of the DR
3	Network summary LSA	Destination network number
4	ASBR summary LSA	Router ID of AS boundary router
5	AS external LSA	External network number
7	NSSA external LSA	External network number



OSPF IPv6 (1)

- La versión 3 OSPF, para IPv6 (RFC2740), extiende la versión 2 de OSPF (RFC2328) para soportar el encaminamiento de prefijos IPv6 y las direcciones de 128 bits
 - Muchas de las características de OSPF para IPv6 son las mismas que OSPFv2
 - En OSPF para IPv6 no es necesario crear explícitamente un proceso de encaminamiento. Al habilitar OSPF para IPv6 en un interfaz se creará el proceso de encaminamiento, así como su configuración asociada
 - En OSPF para IPv6 cada interfaz debe de habilitarse usando los comandos en el modo de configuración de interfaz. Esto es distinto de OSPFv2, donde cada interfaz se habilita indirectamente usando de modo de configuración del router
 - En IPv6 se pueden configurar muchos prefijos en una interfaz. Así que en OSPF IPv6, todos los prefijos de una interfaz se incluyen por defecto; es decir que no es posible seleccionar algunos de los prefijos para ser importados dentro de OSPF IPv6: se importan o todos o ningún prefijo de la interfaz
 - A diferencia de OSPFv2, se pueden ejecutar múltiples instancias de OSPF para IPv6 en un link
 - En redes NMBA (Non-Broadcast Multi-Access networks) (punto-multipunto) no se detectan automáticamente los encaminadores vecinos sino que hay que especificarlos manualmente



OSPF IPv6 (2)

- Puesto que en IPv6 una interfaz de red puede tener más de una dirección, los LSAs en OSPFv3 difieren de los de la versión para IPv4

Código	LSA	Link-State ID
1	Router LSA	Originating router ID of the router. En IPv6 no tienen información de la dirección de red y son independientes del protocolo de red.
2	Network LSA	Interface IP address of the DR En IPv6 no tienen información de la dirección de red y son independientes del protocolo de red.
3	Interarea-prefix LSAs for ABRs	Destination network number. En IPv6 se expresa como prefijo, longitud de prefijo.
4	Interarea-router LSAs for ASBRs	Router ID of AS boundary router
5	Autonomous system external LSAs	Redistributing routes from another AS. En IPv6 se expresa como prefijo, longitud de prefijo y la ruta por defecto, de longitud 0.
8	Link LSA	Local-link flooding scope. Informa de las direcciones link-local de todos los encaminadores del segmento de red
9	Intra-Area-Prefix LSA	Describes association to the router LSA.



Diferencias entre OSPFv3 - OSPFv2 (1)

- El funcionamiento es por link, no por subred IP
 - Los términos “red” y “subred” usados en OSPF IPv4 deben en general cambiarse por “link”
- Eliminación de la semántica de direccionamiento
 - Se ha eliminado la semántica de direccionamiento (addressing semantics) de los paquetes OSPF y de los principales tipos de LSA, dejando un núcleo independiente del protocolo de red
- Adición del Flooding scope
 - El Flooding scope para los LSAs se ha generalizado y ahora está codificado explícitamente en el LS type field de los LSAs. Así ahora existen tres flooding scopes para los LSAs: Link-local, Area y AS scope



Diferencias entre OSPFv3 - OSPFv2 (2)

- Soporte explícito de múltiples instancias por link
 - Esto podría usarse en un segmento de un NAP compartido entre varios proveedores – estos podrían ejecutar separadamente varios dominios de ruteo OSPF aun cuando tuvieran uno o mas segmentos de red físicos (o links) en común
 - Se logra mediante un "Instance ID" contenido en las cabeceras de los paquetes OSPF
 - En OSPFv2 esto se hace de manera más complicada con el campo de autenticación en la cabecera de OSPF para IPv4
- Uso de direcciones link-local
 - OSPFv3 asume que cada router tiene asignadas direcciones unicast link-local en cada interfaz física



Diferencias entre OSPFv3 - OSPFv2 (3)

- Autenticación

- En OSPFv3 la autenticación se ha eliminado del paquete OSPF en si

- Los campos "AuType" y "Authentication" se han eliminado de la cabecera del paquete de OSPF, y todos los campos relacionados con autenticación se han eliminado de las estructuras de áreas e interfaces

- OSPFv3 usa las cabeceras de IP Authentication e IP Encapsulating Security Payload para asegurar la integridad, autenticación y confidencialidad en el intercambio de rutas



Diferencias entre OSPFv3 - OSPFv2 (4)

- Cambio del formato del paquete OSPF
 - OSPFv3 se ejecuta directamente sobre IPv6
 - Se ha eliminado la semántica de direccionamiento (addressing semantics) de las cabeceras OSPF y de los LSAs de Router y Network LSA, dejando un núcleo independiente del protocolo de red
 - Toda la información de direccionamiento esta ahora contenida en nuevos LSAs específicos para distribuir la información de las direcciones IPv6 y de los datos necesarios para la resolución del next hop





6.5 IS-IS



Visión General IS-IS (1)

- IS-IS es un protocolo de encaminamiento OSI
- Diseñado para soportar el protocolo CLNP
 - Protocolo de la capa de red similar a IP
- Se ha extendido para soportar también IPv4 y IPv6 (RFC5308)



Visión General IS-IS (2)

- Características
 - Encaminamiento jerárquico
 - Soporte “classless”
 - Uso de direcciones multicast
 - Autenticación mediante password
 - Soporte de múltiples métricas
 - Cálculo SPF local

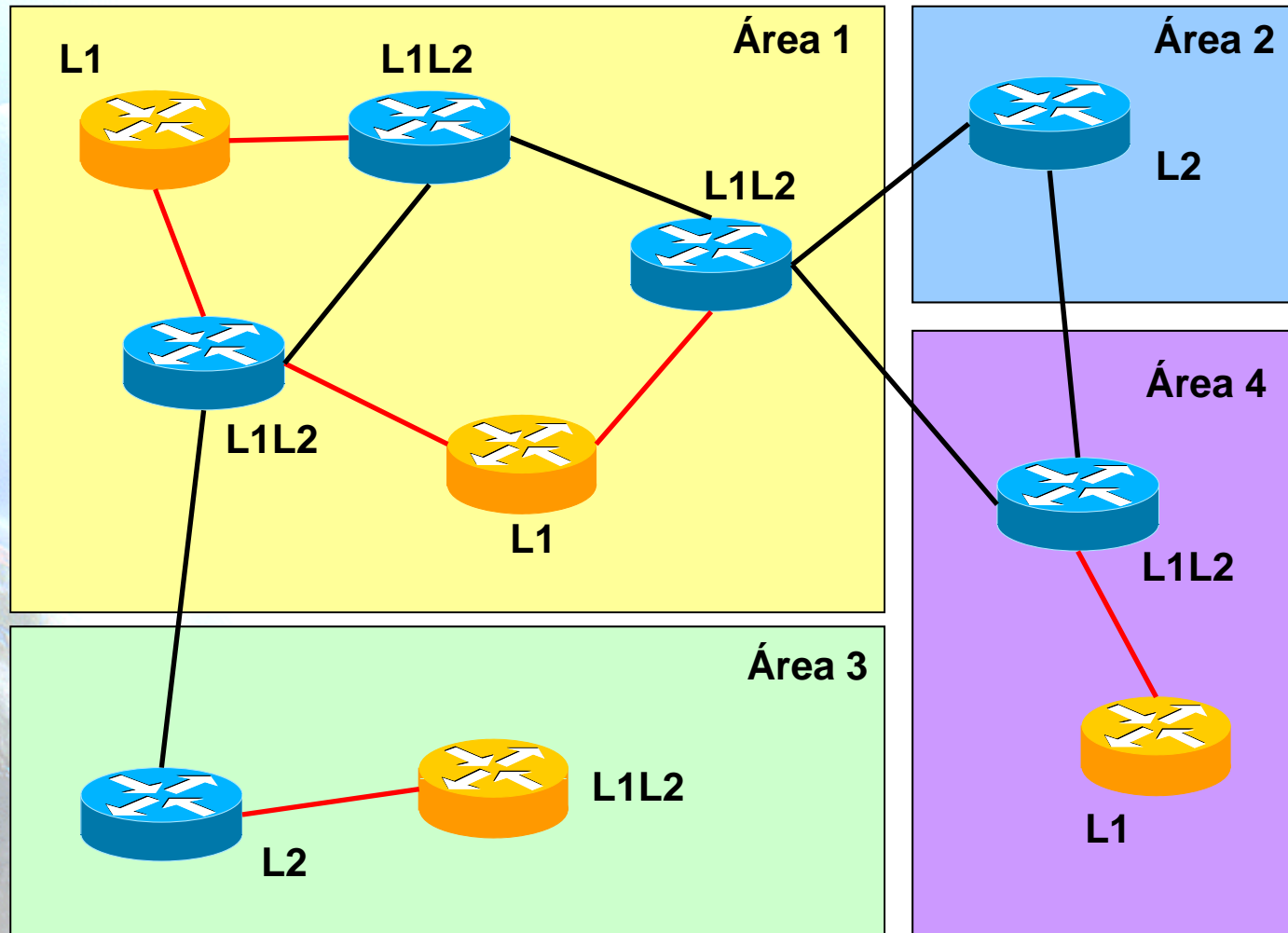


Visión General IS-IS (3)

- Similitudes con OSPF
 - Mantienen una base de datos topológica con los mensajes recibidos (LSAs en OSPF y LSPs en ISIS)
 - Ejecutan el algoritmo SPF
 - Los dos usan áreas para formar una topología de red de dos niveles jerárquicos
 - Ambos soportan rutas “classless” y pueden resumir rutas entre áreas
- Diferencias con OSPF
 - Se define dos niveles jerárquicos
 - Nivel 2: Encaminadores del backbone
 - Nivel 1: Encaminadores de área
 - ISIS no requiere de un “backbone” central
 - En ISIS el “backbone” es realmente un conjunto de encaminadores de nivel 2 contiguos
 - Los bordes que definen las áreas están sobre los enlaces entre los encaminadores, no dentro de ellos como en OSPF



Visión General IS-IS (4)



— Nivel 2: backbone
— Nivel 1



6.6 BGP

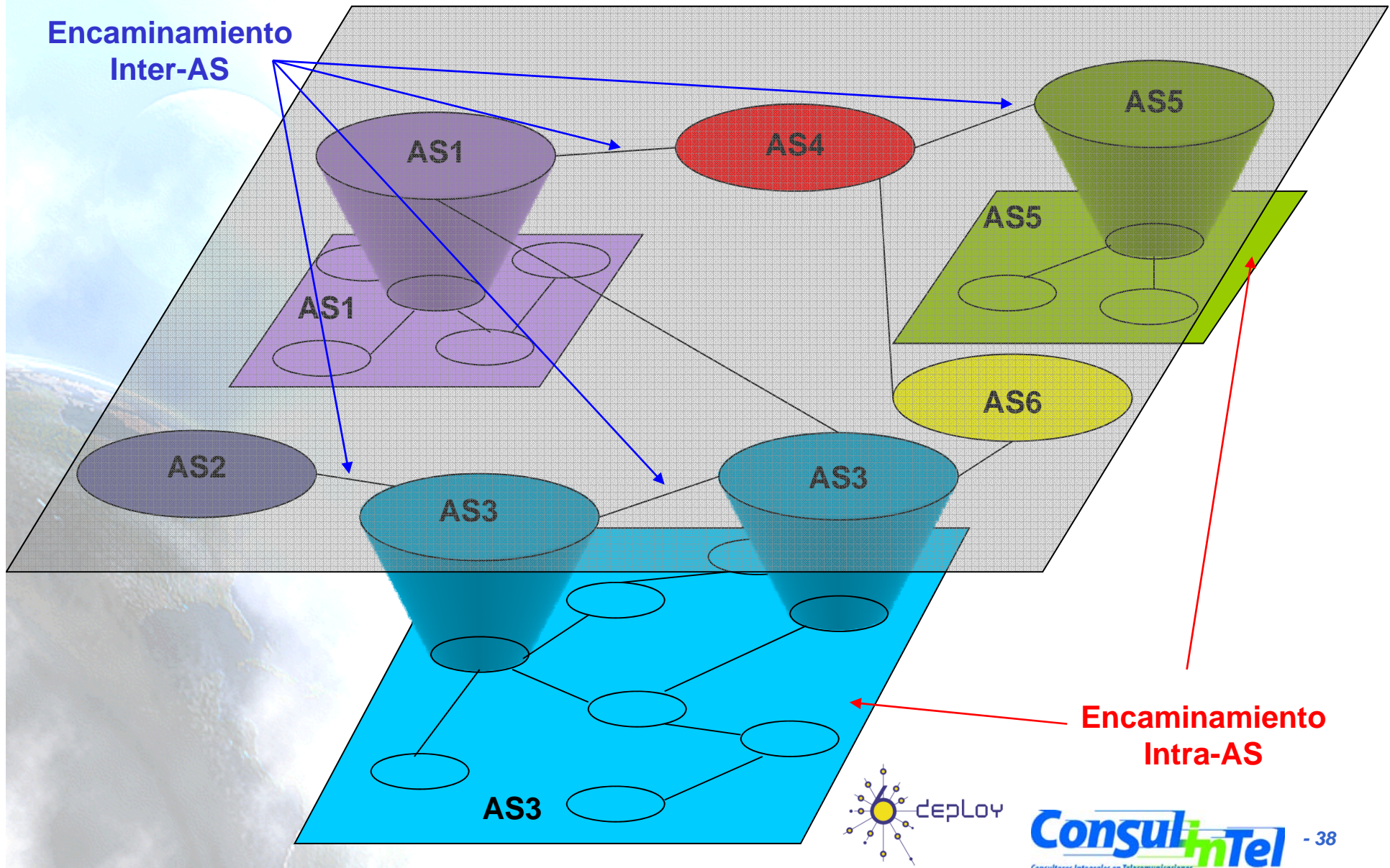


Visión General de BGP (1)

- El encaminamiento en Internet se hace a dos niveles
 - Intra-AS => IGP
 - La gestión de cada AS es local, lo cual incluye el tipo de protocolo de encaminamiento usado
 - Inter-AS => EGP
 - Requiere una estandarización para que todos los ASs sean alcanzados por todos.
 - BGP estándar “de facto”



Visión General de BGP (2)



Visión General de BGP (3)

- BGP “Border Gateway Protocol”
 - estándar “de facto”
- Se basa en el PVP (Path Vector Protocol)
 - Similar al Distance Vector
 - Cada encaminador frontera envía a sus vecinos (“peerings”) la ruta completa a un destino, no solo la distancia
 - El camino (path) es una secuencia de ASs hasta el destino
 - Ejemplo: $\text{Path}(X,Z)=X, Y1, Y2, Y3, Y5, Z$



Visión General de BGP (4)

- Path Vector Protocol
 - El encaminador X envía su ruta a Z a su vecino W
 - Si W la acepta, entonces $P(W,Z)=X$, $\text{Path}(X,Z)$
 - W puede no aceptar dicha ruta
 - Para evitar bucles cerrados
 - Por razones de coste de tráfico
 - Por violación de políticas internas del AS
 - Etc.
- Se puede controlar el tráfico que entra en la red anunciando o no el AS a los vecinos
- Si X no quisiera encaminar tráfico de Z, basta con no anunciar las rutas de Z



Visión General de BGP (5)

- Se utiliza TCP para el intercambio de mensajes BGP
 - OPEN – abre una conexión TCP
 - UPDATE – anuncia o confirma un nuevo camino
 - KEEPALIVE – en ausencia de UPDATES sirve para mantener abierta la conexión TCP y como ACK de un mensaje OPEN
 - NOTIFICATION – informa de errores en mensajes precedentes y para cerrar conexiones



Visión General de BGP (6)

- Atributos del “path”
 - “bien conocidos” – son reconocidos por todos los encaminadores y se pasan a los vecinos
 - Obligatorios y se incluyen en los mensajes UPDATE
 - opcionales – no hay obligación de que los conozcan todas las implementaciones BGP



BGP para IPv6 (BGP4+) (1)

- La versión actual de BGP es la versión 4, i.e. BGP4
 - BGP4 (BGP para IPv4) se describe en RFC4271
- Las Extensiones Multiprotocolo para BGP, i.e. BGP4+, permiten usar BGP4 con diferentes familias de direcciones (address family), tales como IPv6 y Multicast
 - Extensiones multiprotocolo para BGP (BGP para IPv6) se describen en RFC4760
 - Define la extensiones para BGP necesarias para manejar informacion de ruteo sobre distintos protocolos de nivel de red (e.g., IPv6, IPX, L3VPN, etc.)



BGP para IPv6 (BGP4+) (2)

- Las extensiones multiprotocolo para BGP para IPv6 soportan las mismas funcionalidades y características que BGP para IPv4
 - Las extensiones para IPv6 incluyen el soporte para
 - La familia de direcciones IPv6 (IPv6 address family) y la network layer reachability information (NLRI)
 - El atributo de next hop (el router siguiente en el camino hacia el destino), que ahora usa direcciones IPv6
- Las extensiones multiprotocolo para BGP para IPv6 Multicast soportan las mismas funcionalidades y características que BGP para IPv4 Multicast
 - Las extensiones para IPv6 Multicast incluyen el soporte para
 - La familia de direcciones IPv6 Multicast (IPv6 Multicast address family) y la network layer reachability information (NLRI)
 - El atributo de next hop (el router siguiente en el camino hacia el destino), que ahora usa direcciones IPv6 Multicast



Características de BGP4+ (1)

- Los únicos componentes de información de BGP que son específicos para IPv4 son los atributos
 1. NEXT_HOP (expresado como una dirección IPv4)
 2. AGGREGATOR (contiene una dirección IPv4)
 3. NLRI (expresado como prefijos de direcciones IPv4)
- RFC4760 asume que cualquier router BGP (incluyendo los que soportan el mismo RFC4760) tiene una dirección IPv4 (la cual se usará, entre otras cosas en el atributo de AGGREGATOR)
- Así para habilitar en BGP4 el soporte de ruteo para múltiples protocolos de nivel de red, los dos únicos componentes que hay que agregar a BGP son
 1. La habilidad para asociar un protocolo de red particular con la información del next hop
 2. La habilidad para asociar un protocolo de red particular con la network layer reachability information (NLRI)
- Para identificar un protocolo de red particular asociado con la información del next hop y la semántica del NLRI, el RFC4760 usa una combinación de
 - Una Address Family, como esta definida en “IANA's Address Family Numbers registry” (<http://www.iana.org/numbers.html>), y
 - Una Subsequent Address Family, como esta descrita en el mismo RFC4760



Características de BGP4+ (2)

- Para proveer compatibilidad con versiones anteriores, así como para simplificar la introducción de las capacidades multiprotocolo en BGP4, el RFC4760 define dos nuevos atributos
 - Multiprotocol Reachable NLRI (MP_REACH_NLRI), contiene la información de los destinos alcanzables, así como la información de next hop usada para hacer el reenvío (forwarding) hacia esos destinos
 - Multiprotocol Unreachable NLRI (MP_UNREACH_NLRI), contiene la información de los destinos inalcanzables
- Ambos atributos son opcionales y no-transitivos
 - Es decir, un router BGP que no soporta las extensiones multiprotocolo ignorará la información llevada en estos atributos y no la pasará a otros routers BGP



6.7 Encaminamiento Estático



Configuración Rutas Estáticas

- La forma de configurar rutas estáticas es similar a IPv4
 - Default gateway
 - Delegación de prefijos



Gracias !!

Contacto:

- Cesar Olvera (Consulintel): cesar.olvera@consulintel.es
- Alvaro Vives (Consulintel): alvaro.vives@consulintel.es

6DEPLOY Project: <http://www.6deploy.org>

The IPv6 Portal: <http://www.ipv6tf.org>

