



Integrated IS-IS

Introducción al protocolo y características

Versión 1.0



Introducción

¿Qué es IS-IS?

“Intermediate System to Intermediate System” (IS-IS) es un protocolo de enrutamiento interno (IGP) de alta escalabilidad que nació para el intercambio de rutas del protocolo de capa 3 llamado CLNP (ISO 10589).

La versión posterior que soporta IP se llama Integrated IS-IS (RFC1195), objeto de esta presentación.

Características principales de Integrated IS-IS

- **Protocolo de tipo estado-enlace (link-state) cuyos mensajes usan el formato TLV (Type, Length, Value), lo que lo hace bastante flexible a cambios y nuevas implementaciones.**
- **Forma adyacencias con los routers directamente conectados mediante el intercambio de Hellos, estas adyacencias pueden ser de tipo Level-1 o Level-2.**
- **Las publicaciones de rutas (updates) usan mensajes IS-IS llamados LSPs (Link State PDUs).**
- **Su distancia administrativa es de 115.**
- **El intercambio de tramas IS-IS (hellos, LSPs, etc) se hace a nivel capa 2, sólo las interfaces con IS-IS habilitado son capaces de entender y procesar estos mensajes.**
- **Es ‘classless’, soporta autenticación, sumarización y división en áreas.**
- **La métrica usada para comparar rutas depende del costo de cada enlace (se define manualmente).**



Arquitectura y funcionamiento

Direccionamiento ISO

Mientras en OSPF se usa dirección IPv4 para la identificación de cada router, en IS-IS se usa una dirección de la norma ISO con la siguiente estructura:

----- NET o NSAP -----

IDP (Inter Domain Part)		DSP (Domain Specific Part)		
AFI	IDI	High Order DSP	System ID	NSEL
AREA (1 a 13 bytes)		System ID (6 bytes)		NSEL (1)

Ejm.- 47.0001. 1234.5678. 1234.

◇ Formato completo

◇ Formato simplificado

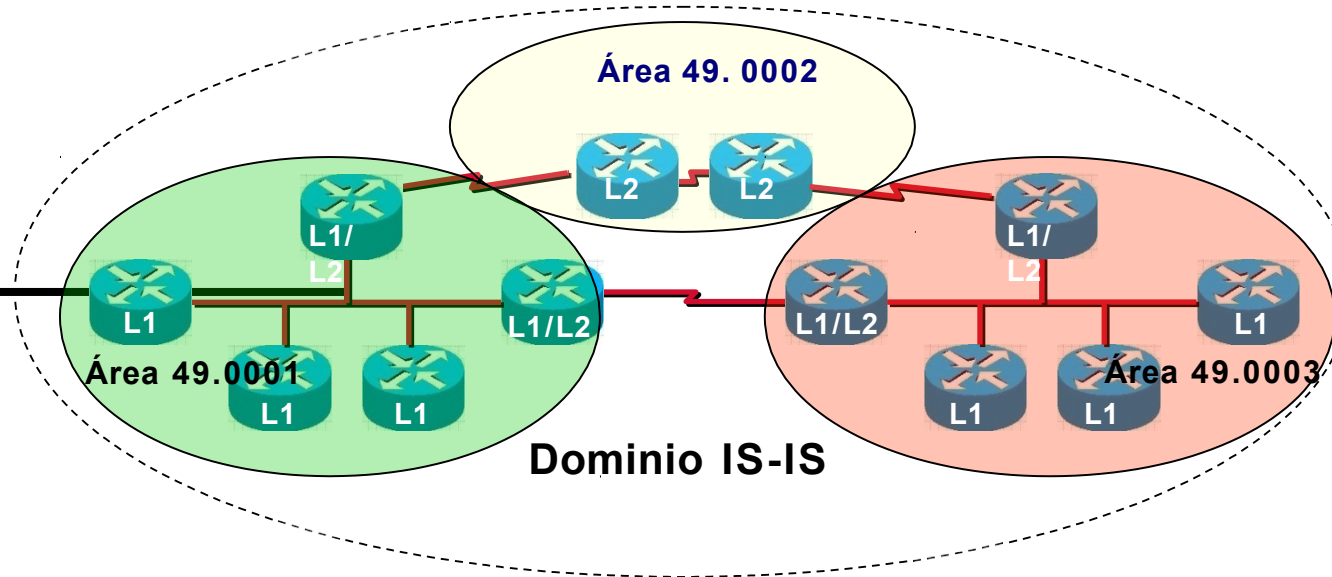
- $\text{Ár}^0 \text{e}^0 \text{a}$ – valores que empiezan normalmente con “49” (valor definido por ISO como “área con direccionamiento privado”)
- System ID – en la implementación de Cisco, es un valor fijo de 6 bytes que identifica al router, debe ser único a nivel área y dominio IS-IS. Normalmente los ISPs forman este identificador a partir de la dirección IPv4 Loopback del router.
- NSEL - La dirección ISO puede ser de dos tipos: NSAP (Network Service Access Point) o NET (Network Entity Title) . La diferencia entre ambas es sólo el NSEL, si es diferente a cero, se trata de un NSAP e identifica al servicio dentro de un host IS-IS tradicional (CLNS). Si el NSEL es igual a cero, se trata de un NET e identifica al propio host (único valor usado en Integrated IS-IS para routers).



Arquitectura y funcionamiento

Concepto de Área en IS-IS

El área en IS-IS está determinada por un conjunto de routers con adyacencias de tipo “Level 1”, mientras que el backbone que une estas áreas es el conjunto de routers unidos por adyacencias “Level 2” que se ubican en el borde de estas áreas.



- Un router normalmente pertenece a una sola área. Todos los routers dentro un área (Level 1) deben tener el mismo “Area ID” en la dirección NET.
- Las áreas dividen el dominio ISIS para limitar la cobertura del intercambio de LSPs, y descargar de procesamiento a los routers. No son necesarias en redes pequeñas.



Arquitectura y funcionamiento

Concepto de Área en IS-IS

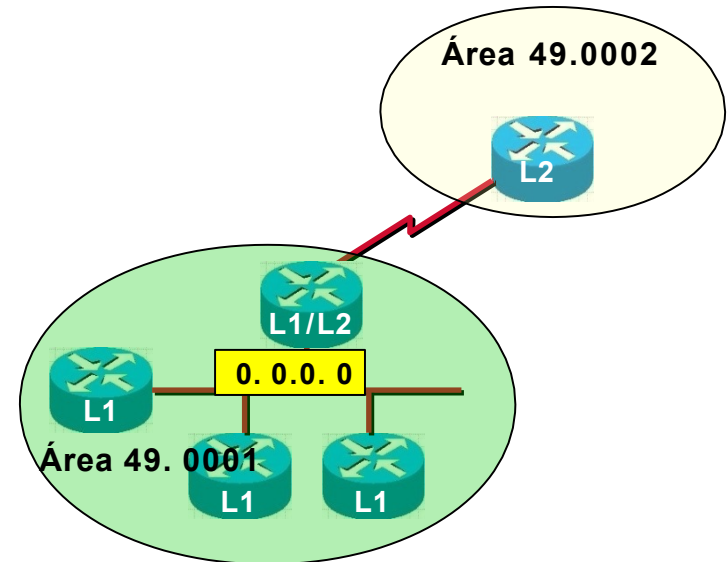
(2)

Routers Level-1 (L1) – Sólo enrutan a destinos dentro del área, en base al “system-id”. Usan una ruta por defecto (0.0.0.0) para enrutar hacia destinos fuera del área a través del router L1/L2 más cercano (siempre y cuando éste se conecte a otras áreas ◇ genere un ATT bit). Mantienen una única base de datos para rutas del área (no contiene información de rutas externas al área*)

Routers Level-2 (L2) – Enrutan a destinos en otras áreas, en base al “area-id”.

Mantienen una única base de datos para rutas del backbone.

Routers Level-1-2 (L1-2) – Actúa como un vínculo para enrutar hacia dentro y fuera del área. Mantiene dos bases de datos separadas, una para rutas del área y otra para rutas externas al área. Si se conecta a otra área, genera un ATT bit hacia L1.



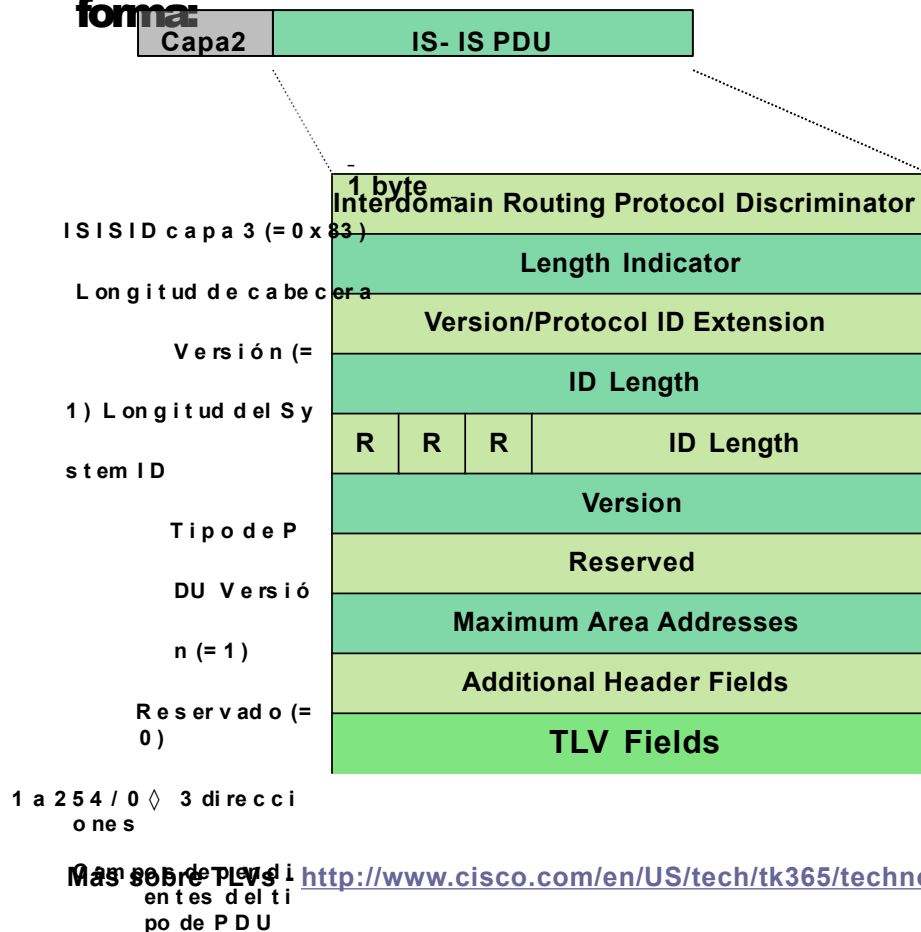
*** Es posible aplicar una técnica conocida como “route leaking” (RFC2966) para permitir que ciertos prefijos externos al área sean redistribuidos dentro de la**



Arquitectura y funcionamiento

Encapsulamiento IS-IS y TLVs

Todas las tramas que se intercambian en IS-IS van encapsuladas directamente en la **capa 2 (data-link layer)** de la siguiente forma:



TLV principales implementados por Cisco

ISO 10589 TLVs	1	AREA ADDRESS
	2	IS NEIGHBORS
	3	END SYSTEM NEIGHBORS
	4	PARTITION DESIGNATED...
	5	PREFIX NEIGHBORS
	6	IS NEIGHBORS
	7	NOT SPECIFIED
	8	PADDING
	9	LSP ENTRIES
	10	AUTHENTICATION
DRAFT	22	TE IIS NEIGHBORS
RFC 1195	128	IP INT REACHABILITY
	129	PROTOCOLS SUPPORTED
	130	IP EXT ADDRESS
	132	IP INT ADDRESS
	134	TE ROUTER ID
	135	TE IP REACHABILITY



Arquitectura y funcionamiento

Tipos de PDU

Los paquetes de IS-IS se clasifican en tres

1. Hellos – Se usan para establecer y mantener las adyacencias entre nodos IS-IS; tipos:
 - LAN Level-1 Hellos – IIH (PDU tipo 15)
 - LAN Level-2 Hellos – IIH (PDU tipo 16)
 - Hellos punto a punto – IIH (PDU tipo 17)
2. LSPs (Link - State P a c k e t s) – Se usan para distribuir la información de enrutamiento entre nodos IS-IS; tipos:
 - Level-1 LSPs (PDU tipo 18)
 - Level-2 LSPs (PDU tipo 20)
3. SNPs (S e q u e n c e N u m b e r P a c k e t s) – Se usan para controlar y sincronizar la distribución de LSPs; tipos:
 - Level-1 Complete SNP – CSNP (PDU tipo 24)
 - Level-2 Complete SNP – CSNP (PDU tipo 25)
 - Level-1 Partial SNP – PSNP (PDU tipo 26)
 - Level-2 Partial SNP – PSNP (PDU tipo 27)



Arquitectura y funcionamiento

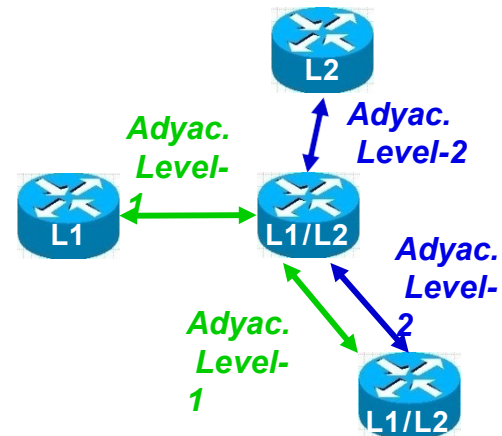
Adyacencias

Las adyacencias se forman con el intercambio de los PDU de tipo “Hello” según:

Level 1	Routers Level 1 y Level 1-2 con la misma área.
Level 2	Routers Level 2 (o Level 1-2), sin importar el área.
Level 1 - 2	Routers Level 1 con la misma área, routers Level 2 sin importar el área.

Adicionalmente:

- El MTU debe coincidir en ambas interfaces.
- Ambos routers deben soportar el mismo nivel (Level 1 y/o 2)
- El System-ID debe ser único.
- La autenticación debe coincidir.
- Los temporizadores de hello y hold-time deben coincidir.





Arquitectura y funcionamiento

Adyacencias (2)

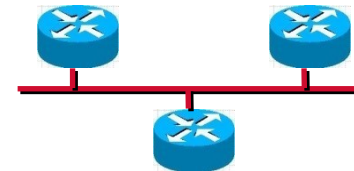
Las características de la adyacencia tendrán que ver con el tipo de red.

Point-to-point



- Se forma la adyacencia apenas se intercambia un Hello.
- Los routers intercambian CSNPs, LSPs y PSNPs para sincronizar sus bases de datos.
- La adyacencia se mantiene periódicamente mediante el intercambio de Hellos cada 10 segundos.
- El Hold-time es de 30 segundos.

Broadcast



- Se forma la adyacencia sólo con el router “DIS” (Designated Intermediate System), el cual se elige en base a la prioridad más alta o a la dirección SNPA (MAC) más alta.
- Los routers intercambian CSNPs, LSPs y PSNPs para sincronizar sus bases de datos.
- La adyacencia se mantiene periódicamente mediante el intercambio de Hellos cada 3.3 segundos, siendo el Hold-time de 10 segundos.

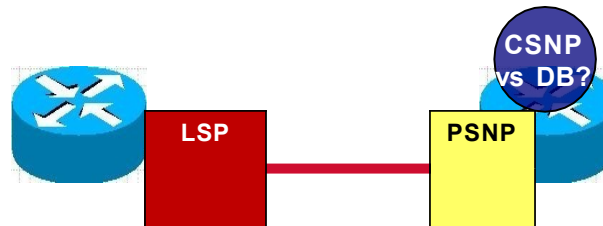
Para el caso de redes NBMA (Non Broadcast Multiaccess), se recomienda migrar a enlaces individuales punto a punto, ya que no hay tipo de red IS-IS que soporte este escenario.



Arquitectura y funcionamiento

Envío de LSPs (rutas)

Al levantarse una adyacencia, se inicia el intercambio de LSPs de la siguiente manera:



1. Intercambio de CSNPs – los routers intercambian paquetes CSNP, los cuales contienen toda la base de datos comprimida.
2. Comparación de CSNPs – los routers comparan su base de datos con el CSNP recibido para verificar si son iguales o si falta algún LSP en la base o en el CSNP recibido.
3. Sincronización mediante PSNPs - en caso hubiera alguna diferencia o ausencia en la comparación, se envía o solicita el LSP faltante mediante paquetes PSNPs. Una vez recibido el LSP, se confirma su recepción con otro PSNP (ACK –
4. Envío de LSPs en demanda – cada vez que ocurre un cambio o por cada 15 minutos (configurable), se envían nuevos LSPs. Los LSPs expiran cada 20 minutos.

* En el caso de redes Broadcast, toda actualización de LSPs se hace a través del DIS (pseudonode)



Arquitectura y funcionamiento

Adyacencias (3)

En caso de broadcast, las direcciones MAC utilizadas son las siguientes:

All1ISs	01-80-C2-00-00-14
All2ISs	01-80-C2-00-00-15
AllIntermediateSystems	09-00-2B-00-00-05
AllEndSystems (ISO)	09-00-2B-00-00-04

Sobre “Hello Padding”

En todo tipo de red, los Hellos se envían con “bits de relleno” (padding) hasta el valor del MTU de la interfaz para facilitar la detección de errores de transmisión.

La desventaja de esto es que se desperdicia ancho de banda, por lo tanto es posible desactivarlo a nivel global o por interfaz. Aún desactivado el “hello padding”, los primeros 5 hellos se enviarán con bits de relleno para mantener la detección de errores al inicio.



Arquitectura y funcionamiento

Adyacencias (4)

Es importante recalcar que para que un LSP sea considerado, éste debe ser válido. Para garantizar la validez de un LSP se usan los siguientes métodos:

LSP Sequence Number

Los LSPs son generados con un número de secuencia que empieza en “1” (hasta un valor de 32 bits). Esto es clave para identificar nuevas versiones de LSPs.

LSP Checksum

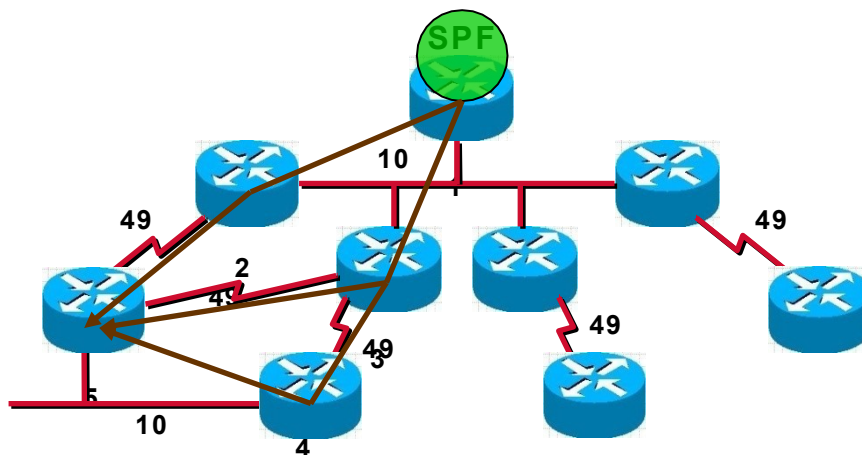
Todos los LSPs tienen un “checksum” adjunto para detección de LSPs corruptos. La recepción de un LSP corrupto provoca una renovación de este LSP en todo el dominio o área.



Arquitectura y funcionamiento

Elección de rutas con SPF

El algoritmo utilizado es el desarrollado por Dijkstra y llamado SPF (igual que en OSPF). Consiste en que cada router arma un 'árbol de rutas' (SPT - Shortest Path Tree) partiendo de sí mismo, colocando a cada ruta una métrica igual a la suma de las métricas de los enlaces a lo largo del camino.



SPF R1 a R5	
Via R2	500
Via R3	100

Balance!
(hasta 16
según la
versión)

- La métrica de cada enlace es fija e igual a 10, pudiendo ésta ser cambiada por configuración. El valor puede ser de hasta 10 bits ('narrow' metric) o de hasta 24 bits ('wide' metric – implementación de Cisco)
- Las rutas con menor métrica son preferidas, así como también las internas o de Level-1 frente a las externas o de Level-2.
- Si no existe un camino dentro del área para el destino, el paquete se envía al router L1/L2 más cercano.



Arquitectura y funcionamiento

Elección de rutas con SPF (2)

Ruta por defecto manual

Es posible generar una ruta por defecto manual, ésta ruta por defecto tendrá preferencia sobre la ruta automática que se genera en cada área hacia el router L1/L2 más cercano.

Overload-bit

Un router que genera LSPs con el 'overload-bit activo', indica al resto de la red que se encuentra bajo en recursos y que no sea considerado para el cálculo de la mejor ruta.

La implementación de Cisco permite activar este bit manualmente.

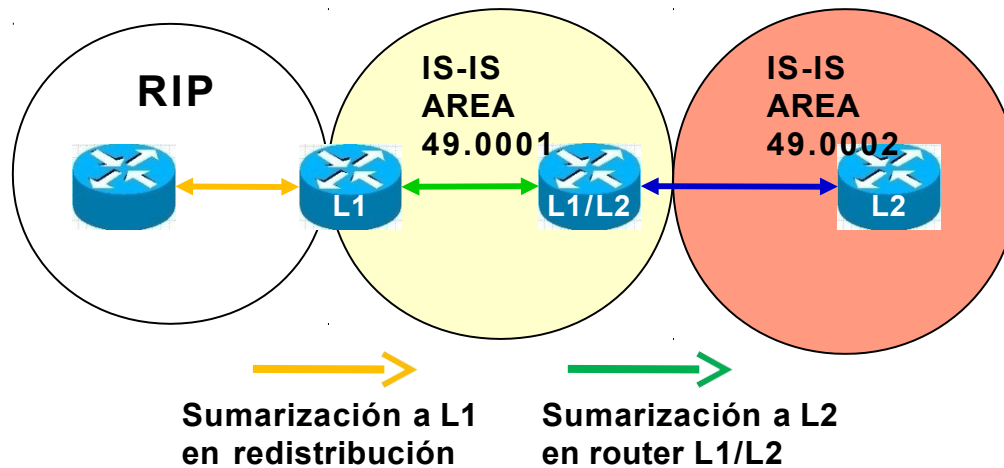


Arquitectura y funcionamiento

Sumarización

IS-IS soporta sumarización en para enviar rutas sumariadas hacia el área (L1) y/o hacia el resto del dominio (L2).

La implementación de Cisco permite configurar sumarización a nivel proceso, para Level-1, Level-2 o para ambos.





Arquitectura y funcionamiento

Autenticación

IS-IS soporta autenticación por norma, pudiendo cada método variar según el fabricante. La implementación de Cisco permite configurar dos tipos de autenticación que pueden configurarse independientes en forma separada o simultánea:

1. Autenticación de Hellos (IIH) – configurable en texto plano o encriptado (MD5). Se configura a nivel interfaz.

2. Autenticación de LSPs/SNPs – configurable en texto plano o encriptado (MD5). Se configura a nivel proceso.

Los LSPs siempre se autentican, mientras que la autenticación de SNPs es opcional.



Consideraciones de diseño

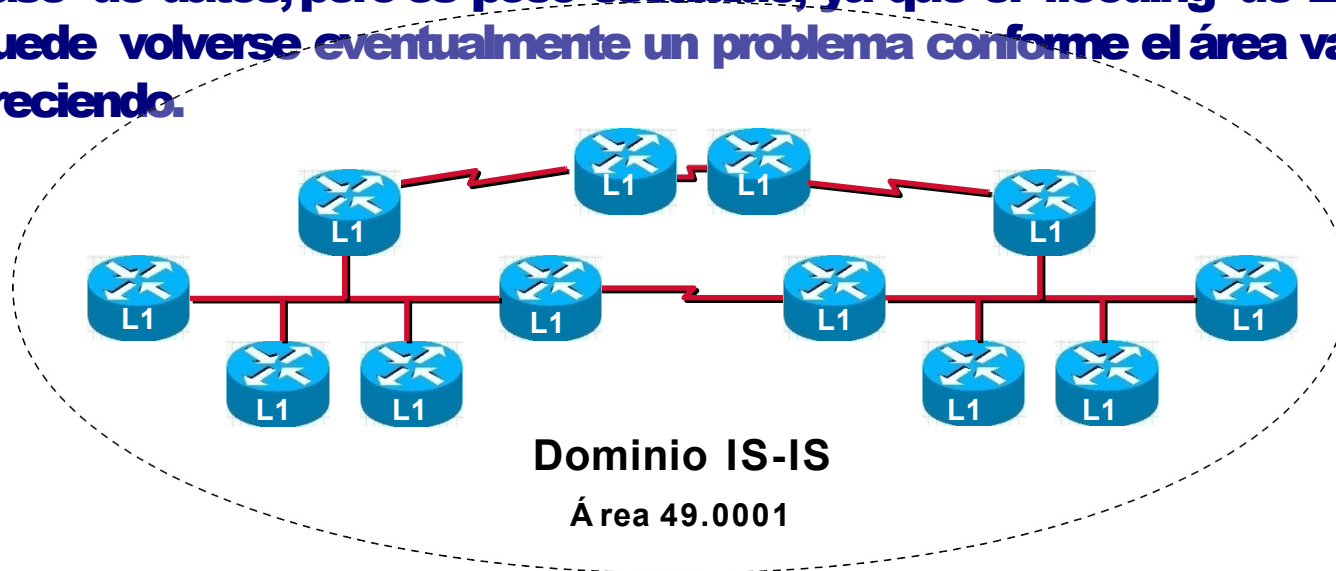
Diseño de áreas

Opción 1 - Área Level-1

Se configura poniendo a todos los routers en level-1 y con la misma

área.

Se trata de un criterio de diseño simple pues se mantiene una única base de datos, pero es poco escalable, ya que el 'flooding' de LSPs puede volverse eventualmente un problema conforme el área vaya creciendo.



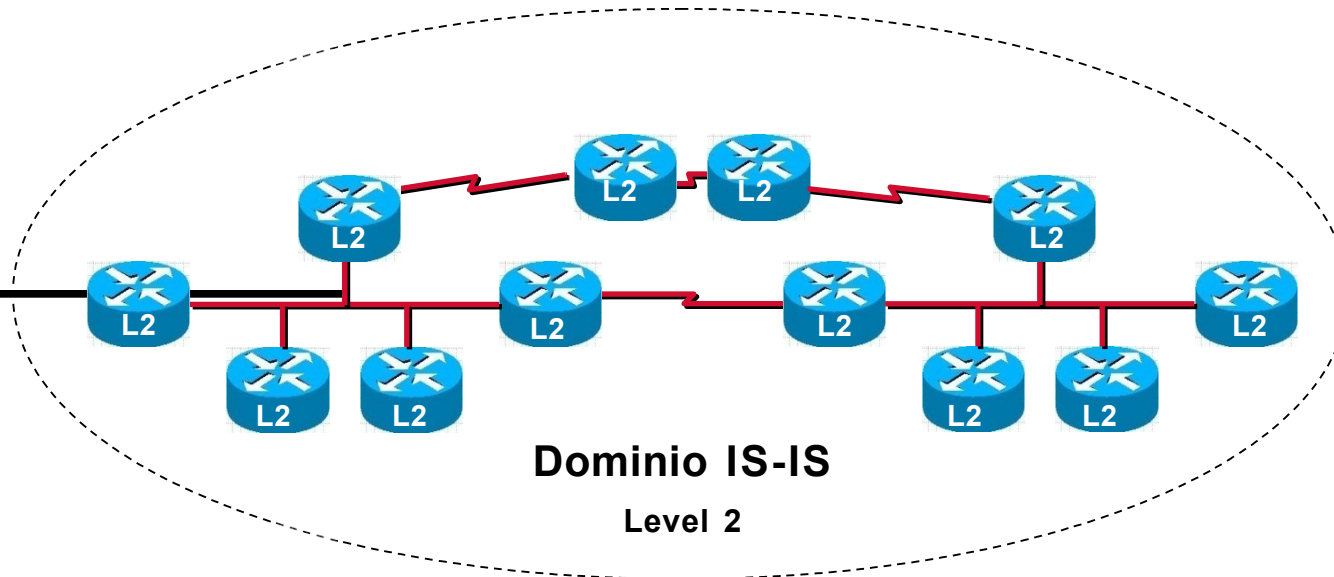


Consideraciones de diseño

Diseño de áreas (2)

Opción 2 - Dominio Level-2

Se configura poniendo a todos los routers el level-2, sin importar el área. Se trata también de un criterio de diseño simple que potencialmente puede tener problemas de 'flooding', pero la diferencia es que permite agregar áreas L1 fácilmente conforme va creciendo.



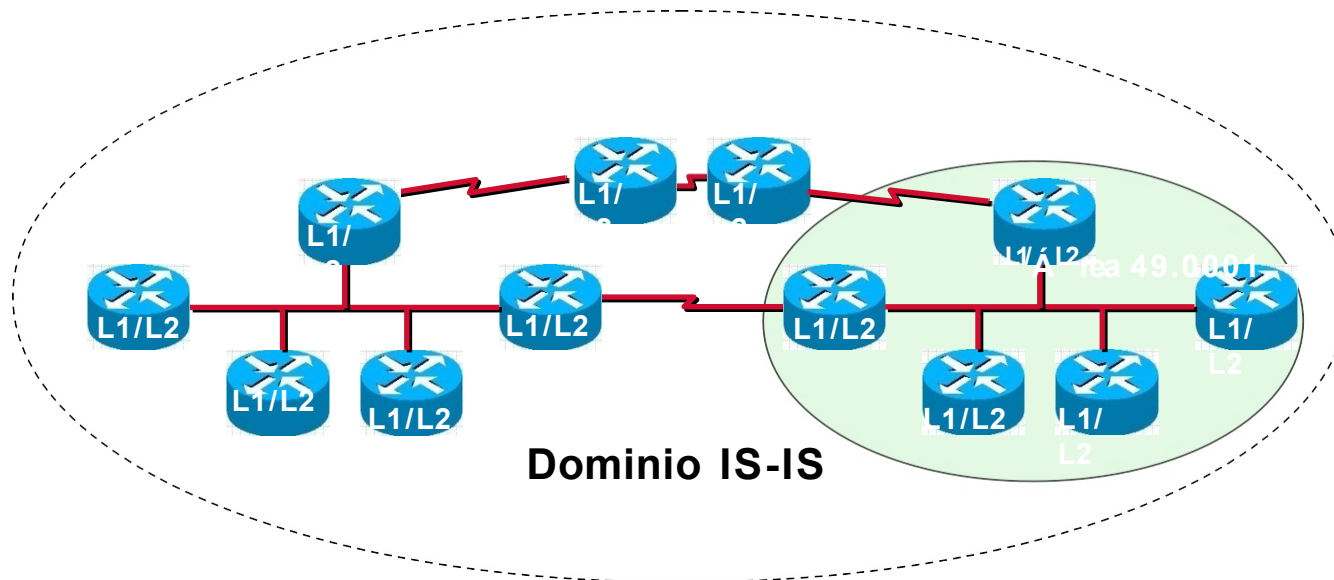


Consideraciones de diseño

Diseño de áreas (3)

Opción 3 - Dominio Level-1-2

Es la configuración por defecto en Cisco, donde todos los routers forman adyacencias L1 y L2 entre sí. Es flexible al permitir una migración rápida hacia un diseño jerárquico. La desventaja es que se mantienen dos bases de datos en cada router.



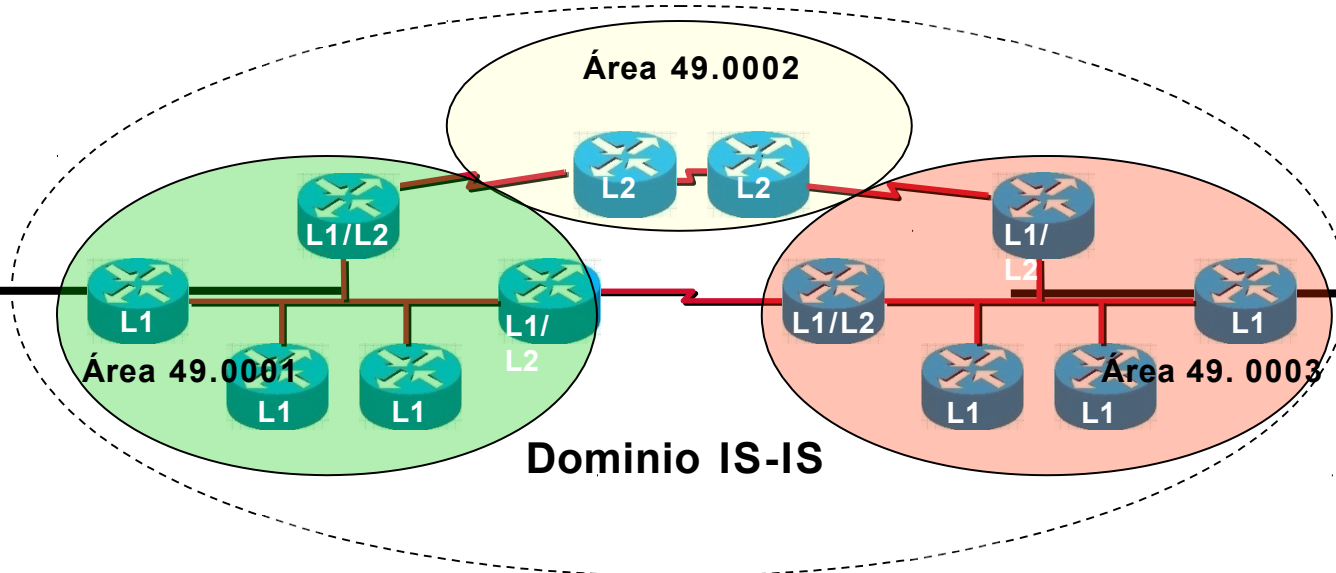


Consideraciones de diseño

Diseño de áreas (4)

Opción 4 - Dominio Level-2 con áreas Level-1

Se configura definiendo áreas de routers que sólo soportan Level-1 unidas por un conjunto de routers de borde L1/L2 (backbone). Es el diseño más escalable, pero podría presentarse algún ruteo sub-óptimo al no existir rutas de otras áreas o backbone en cada área Level-1. En este caso se puede hacer un “route leaking” selectivo.





Consideraciones de diseño


Control de 'LSP flooding'

Existen opciones para minimizar la frecuencia del 'LSP flooding', sobretodo para los casos en los cuales el dominio IS-IS consiste en una sólo área L1 o sólo un backbone L2.

Las medidas a tomar son:

- **Configurar la frecuencia de flooding periódico a un valor alto (lsp-refresh-interval)**
- **Configurar el tiempo de vida útil de los LSPs al valor máximo (max-lsp-lifetime)**

Importante: El 'lsp-refresh-interval' debe ser siempre menor que el 'max-lsp-lifetime', para garantizar que un LSP no expire antes de que sea renovado.

LSP-Refresh-Interval	900 seg		LSP-Refresh-Interval	65000 seg
Max-LSP-Lifetime	1200 seg		Max-LSP-Lifetime	65535 seg



Consideraciones de diseño

Alta convergencia

Los siguientes parámetros influyen directamente sobre el tiempo de convergencia ante un cambio:

- **Intervalo de generación de LSPs (lsp-gen-interval) – cada cuánto se genera un nuevo LSP.**
- **Intervalo de cálculo de SPF (spf-interval) – cada cuánto se hace un nuevo recálculo SPF.**

Los valores por defecto en ambos casos son de 5 segundos. Bajar estos valores puede ser peligroso pues cualquier inestabilidad podría generar LSPs o cálculos SPF innecesarios e impactar en los recursos de los equipos.

La solución es definir valores variables para cada parámetro, por ejemplo:

Parámetro	Primer cambio	Segundo cambio	Cambios sucesivos
lsp-gen-interval	1ms	50ms	5s
spf-interval	1ms	50ms	1s



Glosario de términos

Glosario de IS- IS

Circuit ID	Identifica una interfaz física del router	NET	Network Entity Title – la dirección NSAP de un router, el último byte es siempre 0.
CSNP	Complete Sequence Number PDU – es un resumen de toda la base de datos LSDB	NSAP	Network Service Access Point – Dirección de un equipo CLNS.
CLNP	Connectionless Network Protocol – protocolo ISO no orientado a conexión	NSEL	NSAP Selector – El último byte de una dirección NSAP, que identifica el proceso, por ejemplo “routing”.
CLNS	Connectionless Network Services – Servicio de entrega ‘best-effort’ que corre sobre CNLP	PDU	Protocol Data Unit – unidad de datos
ES	End System – Host o PC que forma parte del ruteo IS-IS tradicional	PRC	Partial Route Calculation – se usa para calcular la alcanzabilidad de una subred o ES
IS	Intermediate System - Término OSI que se refiere a un router	PSNP	Partial Sequence Number PDU – Se usa para pedir más información sobre una red contenida en un CNSP o para confirmar su recepción
ISH	Intermediate System Hello – Hello enviado de un IS a un ES	SNP	Sequence Number PDU – un paquete que permite la sincronización ordenada de las LSDB
IIH	IS to IS Hello – Hello intercambiado entre IS (routers)	SNPA	Subnetwork Point of Attachment – identificador en capa 2 de la interfaz, por ejemplo una MAC o DLCI
LSDB	Link State Database - una base de datos que contiene todas las rutas conocidas	TLV	Type Length Value – campos en un update IS-IS que contienen información de redes
LSP	Link State PDU – ‘Update’ de rutas		



Ejemplos de configuración

Comandos principales de configuración en IOS

router isis *nombre de proceso*

◇ *habilita el proceso IS-IS*

- **net *dirección NSAP***

◇ *configura la dirección NET*

- **passive-interface *interfaz***

◇ *dehabilita en envío de hellos en la interfaz seleccionada*

- **ip router isis *nombre de proceso***

◇ *habilita IS-IS en una interfaz*

- **redistribute {connected | bgp AS | eigrp AS | rip | ospf} {level-1 | level-2 | level-1-2}**

◇ *redistribuye redes desde otros protocolos hacia IS-IS*

- **is-type {level-1 | level-1-2 | level-2-only}**

◇ *define el 'level' de router a nivel global*

- **isis circuit-type {level-1 | level-1-2 | level-2-only}**

◇ *usado en routers L1-L2 para definir el 'level' por interfaz*

- **isis metric *métrica* {level-1 | level-2}**

◇ *cambia la métrica por interfaz*

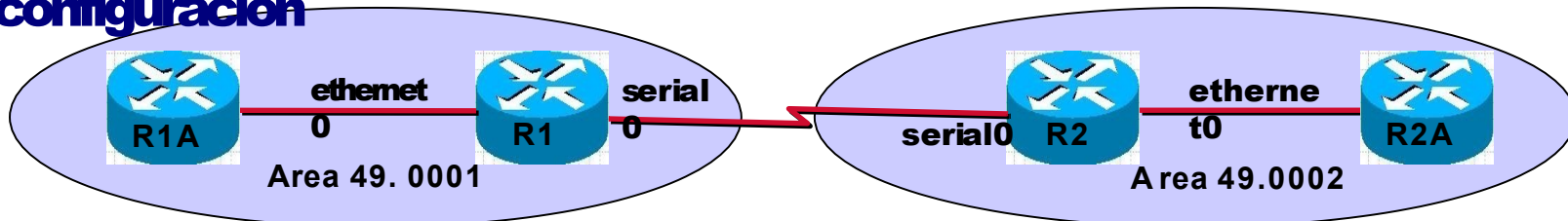
- **summary-address *prefijo máscara* {level-1 | level-2 | level-1-2}**

◇ *configura sumarización de rutas*



Ejemplos de configuración

Ejemplo de configuración



```
R1
interface loopback0
 ip router isis
interface ethernet0
 ip router isis
 isis circuit-type level-1
interface serial0
 ip router isis
 isis metric 10
 isis circuit-type level-2-only

router isis REDALFA
 net
 49.0001.0001.0001.0001.00
```

```
R1A
interface loopback0
 ip router isis
Interface ethernet0
 ip router isis

router isis REDALFA
 is-type level-1
 net
 49.0001.0002.0002.0002.00
```

```
R2
interface loopback0
 ip router isis
interface ethernet0
 ip router isis
 isis circuit-type level-1
interface serial0
 ip router isis
 isis metric
 10
 isis circuit-type level-2-only
 49.0002.0001.0001.0001.00
router isis
REDALFA
```

```
R2A
interface loopback0
 ip router isis
Interface ethernet0
 ip router isis

router isis REDALFA
 is-type level-1
 net
 49.0002.0002.0002.0002.00
```



Troubleshooting

Comandos principales de troubleshooting

- **show clns** – muestra parámetros globales de IS-IS
- **show clns neighbors** – muestra las adyacencias en formato CLNS
- **show clns interface** – muestra parámetros de IS-IS/CLNS por interfaz
- **show clns protocol** – muestra parámetros de área y redistribución
- **show clns traffic** – muestra estadísticas de paquetes intercambiados
- **show isis neighbors** – muestra las adyacencias en formato Integrated IS-IS
- **show isis database** – muestra la base de datos de LSPs
- **show isis spf-log** – muestra los últimos cálculos SPF ejecutados en el nodo
- **debug isis adj-packets** – detalla el intercambio de hellos mientras sucede
- **debug isis spf-events** – detalla los cálculos SPF mientras suceden
- **debug isis snp-packets** – detalla el intercambio de CSNPs/PSNPs mientras suceden
- **debug isis update-packets** – detalla el intercambio de LSPs mientras suceden



Troubleshooting

Problemas comunes

- **System-ID duplicado** – cada router debe tener un identificador único, de otra forma, pensará que está recibiendo sus propios LSPs.

Solución: luego de ver el log, corregir la configuración.

- **Tormenta de LSP Corruptos** – cada LSP corrupto causa una renovación global del LSP, por lo que recibir muchos LSPs corruptos puede causar un problema de recursos.

Solución: Configurar ignore-lsp-errors.

- **MTUs diferentes** – Los MTU deben coincidir en ambos routers para que la adyacencia levante.

Solución: Corregir el MTU físico en un extremo, o usar el comando “`clns mtu`” para que sólo aplique a IS-IS.



Bibliografía y recursos

Libros y otros recursos

- **IS-IS Network Design Solutions – Cisco Press**
- **CCNP BSCI – Official Exam Guide – Cisco Press**
- **CCNP BSCI Quick Reference Sheets – Cisco Press**
- **CCIE Professional Development - Routing TCP-IP, Volume I – Cisco Press**
- **rfc1195 - Use of OSI IS-IS for routing in TCP/IP and dual environments**



Gracias.

Contacto acerca de esta presentación:

Gianpietro Lavado Chiarella

Network Consulting Engineer

Cisco Systems

glch@cisco.com /

glavado@cisco.com