IS-IS

Intermediate System-to-Intermediate System (IS-IS) är ett populärt routingprotokoll för underlays i större nät, exempelvis Internetleverantörer. IS-IS är ett link-state routing protocol. Protokollet byggdes för OSI (Open System Interconnection) protokollet, alltså ej för IP, men transporterar sedan länge IP bra.

IS-IS

Protokollet definierades först i en ISO/IEC standard som heter 10589:2002.
IS-IS använder sig precis som OSPF sig av Dijkstras Shortest Path First (SPF) algoritm för att räkna ut bästa väg till ett nätverk.
Network Service Access Point (NSAP) adressering används för att identifierar routrar, area-tillhörighet och grannskap. Två hierarkier finns, Level 1 (intra-area) och Level 2 (inter-area). Man kan jämföra Level 2 med area 0 i OSPF och Level 1 med övriga areas.
Meddelanden utbyts i IS-IS via Type-Length-Values (TLV). Dessa skickas som MAC-multicast, protokollet är alltså ej beroende av något annat än datalagret. TLVerna kan innehålla olika typer av adressfamiljer (AFI), stöd finns alltså för både IPv4 och IPv6.

RFC 1195 från år 1990 är första definitionen av hur IS-IS ska fungera i IP-nät och kallas här för Integrated IS-IS.

Adressering

Mycket terminologi i IS-IS kommer från OSI protokollet. Här kallas en host för End System (ES) och en router för Intermediate System (IS). System är en nätverksnod, Circuit är ett interface och Domain är ett Autonomous System (AS). Kommunikation mellan två ES kommer i två former, connectionsless-mode och connection-mode. Connectionless fungerar på samma sätt som IP. I OSI så användes protokollet ConnectionLess-mode Network Protocol (CLNP) på samma sätt som IPv4/6 används idag. Spår av CLNP syns fortfarande i IS-IS. `show clns` används för att verifiera IS-IS relaterade parametrar i IOS-XE. Connection-mode kommunikation använde en version av protokollet X.25.

Kommunikation mellan två ES kräver adressering. Adresseringen, för både connection mode och connectionless, använder sig av Network Service Acces Point (NSAP) adressering. En NSAP-adress tilldelas hela nätverksnoden och ej till specifika interface.
Se adressformat:

image.png

NSAP adressen består av två delar. Initial Domain Part (IDP) och Domain Specific Part (DSP).

IDP består av Authority and Format Identifier (AFI) och Initial Domain identifier (IDI). AFI värdet, en oktett mellan 00 till FF, indikerar formatteringen på resterande adressfält. IDI har en varierande längd beroende på adressformatet indikerat av AFI. Den kan till och med vara tomt. Tillsammans indikerar dem routing-domänen som noden är i.

Hur DSP ser ut beror på formatet indikerat av AFI. Den består av en High-Order Domain Specific Part (HO-DSP), av varierande längd, som identifierar vilken del (area) av domänen noden är i. Fältet kan delas upp i subfält. System ID är en unik identifierare för noden. NSAP tillåter fältet att vara mellan 1 och 8 oktetter lång men samtliga implementationer av NSAP låser fältet i 6 oktetter lång.
SEL fältet, även kallad NSAP Selector eller NSEL, är ett 1 oktett långt fält som identifierar en specifik service i eller ovanför nätverkslagret på destinationsnoden som ska processa datagrammet. Går at jämföra med TCP/UDP.

AFI	**Beskrivning**	**IDI längd och innehåll**	**HO-DSP längd och innehåll**
39	Användning av data landskod (ISO 3166)	2 oktetter, numerisk landskod enligt ISO 3166	10 oktetter, areanummer
45	Användning av internationella telefonnummer (ITU-T E.164)	8 oktetter, internationella telefonnummer enligt E.164	4 oktetter, areanummer
47	Användning av internationell kodväljare (ISO 6523)	2 oktetter, internationell organisationskod enligt ISO 6523	10 oktetter, areanummer
49	Lokalt definierat format (privat adressering)	Formellt sett ej på plats	Mellan 0 och 12 oktetter, areanummer

I dagens integrated IS-IS konfigurationer så används alltid AFI 49. Den minsta storleken på en NSAP adress är 8 oktetter och den största är 20 oktetter. Om SEL-oktettens värde är 0, alltså ingen specifik service hänvisas till, hänvisar man till själva noden. En NSAP adress med SEL oktetten satt till 0 kallas för Network Entity Title (NET) och det är adressen som konfigureras på noden, vilket är ett måste i IS-IS.

Adressen består av fält med hexadecimala tecken separerade med punkter.
Exempelvis: `49.0000.1337.5555.6666.00`. 49 är här adressfamiljen, 0000 är area-numret, 1337.555.666 är system ID:t och 00 är SEL värdet, vilket indikerar att adressen är en NET.

Som tidigare nämnt får inte interface någon NSAP-adress. Interface använder L2-adresser på samma sätt som TCP/IP, forwarding sker till en grannes L2-adress. I OSI-nätverk så kallas L2-adresser för Sub Network Point of Attachment (SNPA). Cisco numrerar sina interface i IS-IS med Local Circuit ID, som ökas med 1 för varje interface som läggs till i IS-IS.

Routingnivåer i OSI nätverk

Routing i OSI nätverk använder sig av nivåer (levels) för att beskriva i vilken omfattning routingen sker.

Nivå	Förklaring
Level 0	Routing mellan två ES noder på samma länk, eller mellan en ES och dess närmaste IS
Level 1	Routing mellan ES noder inom ett area i en domän
Level 2	Routing mellan ES noder i olika areas i en domän
Level 3	Routing mellan ES noder i olika domäner

Level 0 routing berör hur en host (ES) hittar sin närmaste router (IS) och vise versa genom att skicka Hello paket. ES skickar ES Hello (ESH) och IS skickar IS Hello (ISH). Går att jämföra med Router Advertisements/Neighbor Advertisements i IPv6.

Level 1 routing berör intra-area routing, alltså routing mellan ES noder som är medlemmar i samma area. Ett area är en samling routrar som i ett link-state routing protocol har detaljerad och komplett visibiltet till hela areats topologi. IS noder samlar in vilka ES noder de har anslutna till sig och annonserar desssa till sina IS grannar.

Level 2 routing berör inter-area routing inom samma domän. Mellan L2 IS så annonseras inte listan med anslutna ES. Area prefix annonseras mellan L2 IS. Om en L1 IS får ett paket som ska till ett ES i ett annat area kommer L1 IS att skicka paketet till närmaste L2 IS oavsett vilket destinationsarea det gäller. Paketet kommer sedan att skickas mellan L2 IS tills att det kommer till rätt area där det åter hanteras av L1 IS. Man kan säga att L1 routing är routing baserat på system ID och L2 routing är routing baserat på area prefix.

Level 3 routing berör routing mellan domäner. I OSI skulle det hanteras av Inter Domain Routing Protocol (IDRP, ISO 10747). I moderna nätverk så kan BGP transportera information om NSAP-adresser (MP-BGP support for CLNS, address-family nsap (unicast)).

En L1 route kommer att föredras över en L2-route. Sist i hackordningen finns External routes (redistributed).

Metrics, nivåer och grannskap

IS-IS metrics tilldelas till individuella interfaces (links). Den ursprungliga specifikationen för IS-IS definierar fyra typer av metrics:

Metric	Förklaring

Default	Måste stödjas av samtliga IS-IS implementationer. Använder vanligtvis länkens bandwidth. Ett högre metric värde är en långsammare länk.
Delay	Delay-värdet på länken
Expense	Pengakostnaden för att skicka trafik över länken
Error	Bitfel på länk

Idag används främst enbart Default-metricen. Ciscos IS-IS implementation ger alla interface en default-metric, 10, oavsett deras bandbredd. Det är en skillnad från OSPF där OSPF tar interfacets bandbredd till metricen. Istället kan man sätta en metric manuellt på interfacet med kommandot `isis metric x [ level ]`. I den ursprunliga IS-IS specifikationen var metric-värdet 6 bitar stort, vilket tillåter värden menllan 1 och 64, och den kompletta path-metricen var 10 bitar stort, vilket tillåter värden mellan 1 och 1023. Idag behövs större spelrum och därmed finns wide metrics, vilket tillåter 24 bitar för interface metric och 32 bitar för hela path metricen. De ursprunliga metrics:en kallas nu för narrow metrics. IS-IS har en administrative distance (AD) på 115.

IS-IS delar upp sina databaser och routingprocess för de olika nivåerna som finns. Ett IS konfigurerad för enbart L1 kan enbart bilda grannskap med IS som också har L1. För att då kunna transportera trafik mellan areas så finns IS som hanterar både L1 och L2. Två stycken IS som hanterar L1 och L2 kan bilda två grannskap, ett för L1 och ett för L2, så länge area numret för L1 matchar.

För varje level aktiverad på ett IS kommer IS:et att skapa och flooda en Link State PDU (LSP), vilket går att jämföra med en OSPF Link State Update innehållande en eller flera Link State Advertisements. Ett IS använder både L1 och L2 LSPer för att beskriva dess grannskap.

Pakettyper

Det finns fyra definierade IS-IS paket:

- Hello packet
- Link state PDU (LSP)
- Complete Sequence Numbers PDU (CSNP)
- Partial Sequence Number PDU (PSNP)

Hello Packets

IS-IS Hello (IIH) används för att hitta grannar, märka tapp av grannar, verifiera tvåvägskommunikation, skapa och behålla grannskap samt välja en Designated IS (DIS, som en DR i OSPF). På broadcast-interface används olika Hello-paket för L1 och L2 grannskap. På P2p interface används ett enda L1L2 Hello (kallas även P2P Hello). Per default skickas Hello paket var 10 sekund men går att modifiera med interface-kommandot `isis hello-intervall x [ level ]`. Hold-timern är ett värde skapart av Hello multiplier gånger hello-intervallen. Standardvärdet för Hello multiplier är 3 vilket leder till en hold time på 30 sekunder. Multipliervärdet går att ändra med interfacekommandot `isis`

`hello-multiplier x [ level ]`.

Hello-intervall och hello-multiplier behöver **inte** matcha mellan IS för att bilda grannskap.

Värdena på en DIS (Designated IS) är alltid 3 gånger mindre än konfigurerat värde. En DIS skickar alltså Hello-paket var 3.333 sekund enligt defaultvärdet. Det är för att hitta avbrott på en DIS snabbare.

Link State PDUer

En Link State Protocol Data Unit (LSP) använder för att annonsera routinginformation. De går att jämföra med OSPF Link State Update innehållande en eller flera LSAer. Det finns i IS-IS ingen skillnad på olika typer av LSPer. LSPerna innehåller olika Type-Length-Values (TLV) vilket beskriver nätverksinnehållet. IS-IS LSPer kan identifieras av ett ett nummer som består av tre delar:

1. System ID från IS som skapade LSP (6 oktetter från ISets NET adress)
2. Pseudonode ID vilket skiljer ISet i sig från LSPer för multiaccessnät där ISet är DIS (1 oktett)
3. LSP Number vilket betcknar fragmentsnumret för den här LSPn (1 oktett). Kallas även för Fragment eller Fragment Number

Tripletten av information ovan kallas för LSPID. I LSPer som beskriver själva routern är Pseudonode IDt satt till 0. För varje routing-nivå ett IS deltar i så skapas en LSP.

För att skilja mellan olika versioner av samma LSP så används sekvensnummer. Sekvensnumret är ett 32 bitar stort värde vilket ökas med 1 vid varje förändring som börjar vid 0x00000001 och slutar vid 0xFFFFFFFF. Skulle maxvärdet nås så måste ISet som skapade LSPn startas om eller byta System ID, men det tar minst 136 år att nå taket.

Varje LSP har en livstid, Remaining Liftetime. När en LSP skapas är den 1200 sekunder (20 minuter) och minskar konstant. IS-IS routrar förnyar sina självskapade LSPer var 15 minuter. Om en LSPs remaining lifetime når 0 så kommer en router ta bort LSPns innehåll från link-state databasen, behålla headern och annonseras den tomma LSPn med en Remaining Lifetime satt till 0. Att annonsera en LSP med Remaning Lifetime kallas LSP purge. Hela LSPn kommer först rensas efter ZeroAgeLifetime har gått ut efter detta, den är 60 sekunder lång. Cisco routrar kommer dock att behålla den tomma LSP headern i 20 minuter.

Eftersom att IS-IS paket enkapsuleras direkt som L2 frames där MTUn kan vara begränsad finns fragmenteringsmetoder för LSPerna. Om placering av samtliga TLVer i en enda LSP skulle överstiga MTUn så kommer routern istället att dela upp TLVerna i flera LSPer. Fragmenteringsnumret ökar för varje LSP med start på 0. Övriga routrar som mottar de fragmenterade LSPerna kommer ej att öka fragmenteringsnumret utan floodar LSPerna som dom är. En konsekvens av denna regel är att **MTU måste vara samma** inom en IS-IS floodingdomän, alltså inom ett area eller mellan samtliga L2-routrar. Om det ej är möjligt måste IS-IS routrar manuellt konfigureras om för att behålla varje LSP som ej är större än den minsta MTUn.

I OSPF skapas olika LSAer beroende på innehåll, area, syfte und so weiter. I IS-IS skapas bara en (möjligtvis fragmenterad) LSP som innehåller all relevant information till routern:

- Grannskap till andra routrar och nätverk (likt typ 1 LSA i OSPF)
- Intra-area och inter-area prefix (likt typ 1, 2 & 3 LSAs)
- Externa prefix (lik typ 5/7 LSAs)

En IS-IS router skapar 1 enda LSA (per level) som beskriver den och dess anslutna nätverk. Är den DIS så kommer den att skapa en Pseudonode ID för varje netvärk den är DIS för.

En LSP har en unik identifierar för hela LSPn och kan enbart floodas, begäras, ackas, förnyas, åldras och flushas i sin helhet. Vid topologiförändringar, ex. ett nätverk som slutas redistribueras in i IS-IS, måste hel LSPn skapas om och flushas på nytt. Det kan anses ineffektivt jämfört med OSPF, där en ny LSA skickas om på nytt, men i IS-IS så behöver en router bara hålla koll på högst ett par-tre stycken LSPer som åldras och förnyas. Det är även lätt att implementera bärande av nytt data/nya funktioner i en LSP då datat är formatterat som TLV information. Skulle en router ta emot LSP innehållande TLVer den ej känner igen kommer den informationen att ignoreras.

Complete och Partial Sequence Number PDUs

CSNP och PSNP är paket som används för att synkronisera link-state databasen. Sekvensnummer används för att beskriva en serie av LSPID värden och ska ej förväxlas med sekvensnummer i individuella LSP paket.

CSNP paket går att jämföra med OSPF Database Description paket. Syftet med CSNP paket är att annonsera en komplett lista över LSPer i sändarens link-state databas. Mottagare av CSNP kan jämföra paketet mot sin egen link-state databas och antingen flooda en nyare eller saknad LSP till sändaren, eller be om en LSP som den själv saknar i sin databas.

Även här fragmenteras paketen till flera CSNP paket om de skulle överskrida MTUn. På P2P länkar byts CSNP paket ut mellan IS under första grannskapsbildandet. På broadcastnätverk skickas CSNP paket periodvis av DIS.

PSNP paket går att jämföra med OSPF Link State Request och Link State Acknowledgement paket. Med hjälp av PSNP kan en router be om en viss LSP eller acka mottagande av LSPn. En PSNP kan begära eller acka flera LSPer. PSNP används på P2P länkar för att både be om LSPer och acka mottagande. På broadcastnätverk används PSNP paket för att be om LSP men ackar sker genom CSNP meddelanden skickade av DIS.

Nätverkstyper

I IS-IS finns bara två nätverkstyper: broadcast och point-to-point (P2P). Det går att köra IS-IS över ex. HDLC, PPP, GRE, Frame Relay och ATM men det finns inga specifika nätverkstyper för dessa interface. I IS-IS finns följande gannskapslägen:

- Down. Första läget efter att IS-IS aktiveras på interface. Inga IIHs har mottagits från granne.
- Initializing. IIHs har mottagits från granne men det är inte säkerställt att tvåvägskommunikation är etablerad, dvs att även grannen mottager IIHs
- Up. IIHs är mottagna och det är säkert att grannen tar emot IIHs

IS-IS över P2P

Över P2P interface förväntar sig IS-IS enbart en granne. I den första implementationen av IS-IS ansågs ett grannskap vara uppe vid första mottagande av IIH från grannen, men då ingen verifiering skedde kunde det leda till problem. Numera frinns ett tre-vägs handskap för IS-IS över P2P-länkar.

Varje IS-IS interface får ett Local Circuit ID. Vilket Local Circuit ID ett interface har fått kan kontrolleras med `show clns interface [ interface ]`. På P2P länkar används Local Circuit ID i IIH paket för att märka identitetsförändringar på andra sidan länken. På broadcastlänkar används Local Circuit ID som Pseudonode IDt om routern är DIS på interfacet. Därför behöver Local Circuit IDt bara vara unikt på riktigt på en broadcastlänk. Samma nummer kan återanvändas på broadcast och P2P-länkar. Local Circuit IDt är 1 oktett stor, begränsningen blir då 256 interface per IS. För att hantera mer än 256 interface finns Extended Local Circuit ID som är 4 oktetter lång.

Trevägshandskakningen baseras på att vardera routers P2P länk annonseras ett adjacency state TLV i sina IIh paket som innehåller följande fält:

- Adjacency Three Way State, status för grannskapet sett från den sändande routern
- Extended Local Circuit ID, IDt för sändande routers interface
- Neighbor System ID, ID på grannskapsroutrar vars IIHs har mottagit
- Neighbor Extended Local Circuit ID, värdet från grannarnas ID i mottagna IIH paket

Tidigare implementationer använde sig enbart av Adjacency Three Way State. Logiken bakom tidiga implementation av trevägshandskakningen är enligt följande när båda routrar anser grannskapet vara Down:

1. Router A mottagar IIH från Router B där Adjacency Three Way State är satt som nere. Router A kan höra Router B, men vet ej om Router B hör Router A. Router A skickar sitt IIH paket med Adjacency Trhee Way State satt till Initializing.
2. Router B mottagare IIH från Router A med Adjacency Three Way State satt till Initializing. Router B vet att tvåvägskommunikation fungerar. Därför skicka den Adjacency Three Way State satt till Up.
3. Router A mottager IIH från Router B med Adjacency Three Way State satt tiill Up. Router A vet att våvägskommunikation fungerar. Router A skickar IIH med Adjacency Three Way State satt till Up och handskakningen är över.

Det här är defaultbeteende som Cisco använder på P2P interface och kan konfigureras i interfacekonfig med `isis three-way-handshake cisco`.

Det finnsf all där ovan kan misslyckas, exempelvis om paket skulle switchas till fel routrar i ATM eller fibernät där RX/TX är separata. För att lösa detta lades Extended Local Circuit ID, Neighbor System ID och Neighbor Extended Local Circuit ID till. Router A skulle här vid första IIH populera Extended Local Circuit ID fältet med sitt sändande interface. Router B skulle svara med sitt eget Extended Local Circuit ID fält populerat med sitt sändande interface, Router A kommer placera Router Bs system ID i Neighbor System ID och kopiera Router Bs Extended Local Circuit ID till Neighbor Extended Local Circuit ID fältet. Därmed kommer Router B att veta vid mottagande av nästa IIH att det är rätt enheter som kommunicerar med varandra. Skulle senare ett IIH paket komma som ej innehåller fälten tas emot kommer det att droppas tyst. Den här metoden konfigureras på interface med `isis three-way-handshake ietf`. Den är även bakåtkompatibel med metoden ovanför.

När grannskapet är uppe kommer routrarna att försöka synkronisera sina link-state databaser. Samtliga LSPer markeras för flooding över P2P interfacet och CSNP paket skickas till varandra. Skulle CSNP paket bytas ut innan första LSP-utbytet kan LSPer som redan är kända avmarkeras för flooding. Ser en granne att en LSP är nyare eller ukänd kommer den även att be om LSPerna via PSNP. Då flooding per default kommer att ske är det här dock inte nödvändigt. Varje LSP som skickas över en P2P länk måste ackas med PSNP eller CSNP paket. IS-IS specifikationerna säger att CSNP paket ej ska bytas ut periodvis över P2P länkar så därmed ackas LSPer med PSNP. Vissa leverantörer implementerar periodvisa CSNPs över P2P länkar men Cisco gör ej det per default, det går dock att aktivera med interfacekommandot `isis csnp-interval x [ level ]`.

IS-IS över Broadcastlänkar

På Ethernetnät enkapsuleras IS-IS paket i IEEE 802.2 Logical Link Control (LLC) formatterade frames. Destination Service Access Points (DSAP) och Source Service Access Point (SSAP) fälten sätts till 0xFE. Samtliga L1 IS-IS paket skickas till multicast MAC-adressen 0180.c200.0014 och alla L2 IS-IS paket skickas till multicast MAC-adressen 0180.c200.0015.

Grannar hittas genom att skicka och ta emot IIH paket. I IIH paketen listas en routers samtliga grannar genom dess SNPA (L2-adress, MAC-adress) som har hittats på det interfacet. Om en router mottager ett IIH paket med sin egen SNPA är tvåvägskommunikation verifierad och grannskapet kan flyttas till Up. Om paketet inte innehåller routerns egna SNPA flyttas grannskapet till Initializing.

En DIS väljs per broadcastnätverk. Valet av DIS baseras på följande:

- Högst prioritet på interfacet
- Vid lika prioritet väljs den router med högst SNPA
- Om SNPA ej går att jämföra väljs den router med högst system ID

Prioritet är ett värde mellan 0 och 127. Sätts per interface med kommandot `isis priority x [ level ]`. Samtliga prioriteter deltar i valet och är preemptive, en ny router på samma segment med högre prioritet kommer att ta över DIS-rollen. Samtliga grannar på ett segment har full kommunikation med varandra, ingen motsvarighet till OSPFs DR/OTHER finns i IS-IS. Det DIS är asnvarig för är att hjälpa routers på segmentet att synkronisera och att representera broadcastsegmentet genom

Pseudonode i LSP.

Synkroniseringen sker genom att DIS skapar och skickar ett CSNP paket var tioende sekund (per default). Övriga routrar jämför CSNP paketet med sin egen databas. Innehåller CSNP från DIS en LSP med ett högre sekvensnummer än det en router har lokalt så laddas den ned från DIS genom att skapar en PSNP som begär LSPn. DIS kommer att ta emot PSNPn och flooda LSPn över segmentet. Skulle DIS CCNP indikera ett lägre sekvensnummer på en LSP, eller sakna en LSP som finns i lokala databasen, kommer en router att flooda LSPn på nätverket. DIS blir alltså bara en referenspunkt här och sköter inte all flooding vilket är skillnad från OSPF.

image.png

Genom annonsering av Pseudonode i LSP så minskar antalet länkar som annonseras. I exemplet ovan så skulle det blir 30 annonserade länkar utan pseudonode men bara 12 med pseudonode. Det minskar storleken på LSP som måste propageras som den är inom ett area utan att någon effekt förloras.

Areas

I IS-IS tilldelas areatillhörighet i NSAP adressen. En router kan ha upp till 3 olika NSAP adresser i en IS-IS instans, så länge de bara skiljer sig i area ID:t, men bygger här enbart en link-state database vilket gör att de konfigurerade areas smälter ihop. För att ansluta till andra areas krävs L2 (och L1/L2) routrar, som har möjlighet att skapa grannskap med routrar i andra areas. Kom ihåg att två separata link-state databaser byggs om en router är L1/L2. L2 routrar går alltså att jämföra med Area 0 i OSPF.

image.png

En L1/L2 router annonserar samtliga direktanslutna IP-nätverk samt alla L1 rötter från sitt eget area. Det sker alltså en injicering från L1 databasen till L2 databasen. Ett L1 area går att jämföra med ett OSPF Not So Stubby-Totally Stubb (NSSA-TS) area. De ser rötter inom ett eget area, kan redistribuera in rötter i areat och mottager en default-route från L1/L2-routern. Per default är L1/L2 läget igång i Cisco IOS, går att ändra på såklart.

Anledningen till att använda flera areas idag är för routesummering. I IS-IS sker routesummering vid L1/L2 routrar med kommandot `summary-address x/x` i router isis-processen.

Autentisering

Stöd finns för klartextlösenord och MD5. Välj MD5. Det finns tre sätt att autentisera paket i IS-IS:

1. Area password för L1, autentisering för samtliga routrar i ett area (kom ihåg att LSP floodas oförändrad, här behövs lösenordet!)
2. Domain password för L2, för att autentisera LSPer mellan L2 routrar
3. Autentisering för Hellos (interfacenivå)

Exempelkonfiguration:

```
! Interfaceautentisering, IIH LAN & P2P, L1/L2. Specifisera inte level-1/2 så gäller det för båda
! För P2P ska ej L1/L2 specas
interface GigabitEthernet0/1
 isis auth mode { text | md5 } { level-1 | level-2 }
 isis auth key-chain x { level-1 | level-2 }

! LSP / CSNP / PSNP
! Genom att ändra L1/l2 blir det area-autentisering eller domänautentisering
router isis
 auth mode { text | md5 } { level-1 | level-2 }
 auth key-chain x  level-1 | level-2 }
```

Interfaceautentisering kan slås på gradvis medans area/domänautentisering måste matcha på samtliga routrar.

IPv6

Samtliga regler för IPv4 gäller för IPv6. De transporteras i LSPer som TLVer. Samma IS-IS process kan transportera IPv4 TLVer såsom IPv6 TLVer.

Passiva interface

Genom att aktivera `passive-interface` på ett interface som inte är med i IS-IS processen så kommer det nätet att annonseras in i IS-IS. Det är så man kan annonsera ex. klientnät.

Vill man bygga en riktigt liten routingtabell där ingen trafik är ämnad för länknäten kan man kombinera detta med `advertise passive-only`. Blir samma effekt som prefix-suppression i OSPF. Väldigt schysst om man ex. använder IS-IS som underlay i MPLS eller EVPN-nät.

Circuit Type

I sin grundkonfiguration så försöker en Cisco IOS router som kör IS-IS att skapa grannskap över både L1 och L2. En router som är konfigurerad som bara L1 eller L2 kommer naturligtvis inte göra det. Vill man specifisera vilken typ av grannskap som ska bildas över ett visst interface kan man definiera `isis circuit-type { level-1-only | level-2-only }` i interfacekonfen.

Exempelkonfiguration

```
router isis
 net 49.1337.1111.2222.3333.00
 is-type level-1-2
 metric-style wide
 log-adjacency-changes all
 summary-address 10.13.137.0 255.255.255.0
 passive-interface Vlan1337
 advertise passive-only
 !
 address-family ipv6
  summary-prefix 2001:DB8::/32

interface GigabitEthernet0/1
 ip router isis
 isis authentication mode md5
 isis authentication key-chain ISIS-KEY
 isis circuit-type level-2-only
 isis metric 100 level-2
 ipv6 router isis
```

Design

Det finns tre övergripande designmetodier för IS-IS.

Den första är Platt (Flat) IS-IS. Här används enbart L2-routrar. Är att föredra när man börjar bygga ett nät. Det blir enbart en databas. Skulle man behöva lägga till areas så går det att konvertera utvalda routrar till L1/L2. En nackdel är att ingen summering av prefix går att utföra.

Designalternativ två är Three-tie campus/hierarchical design. Core/backbone är L2 routrar. Dist-routrar är L1/l2 och ev. routrar efter dist är enbart L1. Summering sker i distarna.

Designalternativ tre är hybrid IS-IS. Det finns ingen ren backbone (enbart L2) utan en collapsed core används som är L1/L2 routrar. Summering sker då i collapsed core.

NSF & NSR

Är Non Stop Forwarding ej aktiverat så går det att aktivera med `nsf ietf` i IS-IS processen. Verifiering med `show isis nsf`. NSF är en IETF standard och innebär samarbete mellan direktasnslutna routrar.

Flera timers finns associerad med NSF. Dessa värden går att konfigurera. T3 motsvarar restart-time i andra protokoll. Interface specifiserar hur länge den väntar på att interface kommer upp innan

restart/switchover är klar. Interval är för att säkerställa att NSF omstarter inte sker för ofta och är en hold-down timer mellan omstarter.

```
router isis
 nsf interval 7
 nsf interface wait 15
 nsf t3 manual 60
 nsf lifetime 60
 nsf interface-timer 5
 nsf interface-expires 3
```

Non Stop Routing är en lokal funktion som inte signalerar någonting till grannar. Aktiveras genom `nsf cisco` i IS-IS processen. Togs fram före NSF, NSF bör föredras.

Show kommandon

show isis hostname	Se hostname (NSAP adress)
show isis database [detail]	Se LSDB
show isis neighbors [detail]	Se grannar
show clns interface [interface]	Se information om interface
show clns	Global CNS information (ex. NET)
show clns is-neighbors [detail] show clns neighbors [detail]	Grannar, väldigt lika outputs

Revision #1
Created 26 April 2025 12:02:52 by Jehrlander
Updated 26 April 2025 12:02:57 by Jehrlander