OSPFv2

Open Shortest Path First (v2) är ett routingprotokoll för IPv4. Det är förmodligen världens största interna routingprotokoll (IGP) då det stöds av samtliga stora nätverksleverantörer. OSPFv2 hanterar IPv4, OSPFv3 hanterar IPv6 (och IPv4 hos Cisco), se egen artikel för OSPFv3. OSPFv2 är ett link-state routing protocol, det betyder att en databas för varje länk/nätverk byggs och denna databas delas och ska se likadan ut inom sitt area. Databasen heter link-state database (LSDB). Databasen byts ut mellan OSPFv2 routrar genom link-state advertisements (LSA).

Dijkstras algoritm, uppkallad efter skaparen holländaren Edsger W. Dijkstra, används för att räkna ut kortade vägen till ett nätverk (SPF, shortest path first).

OSPFv2

Database Exchange

OSPFv2 använder sig av 5 olika meddelanden som routrar kan använda för att bygga grannskap och dela med sig av routinginformation.

Router ID

För att en router ska kunna skickas OSPFv2 meddelanden behövs ett router ID (routing identifier, RID). Det är ett 32 bitar långt tecken och ser därmed ut som en IPv4 address. Ett router ID kan vara statiskt konfigurerat med kommandot `router id x.x.x.x` under OSPF processen. Är det inte manuellt konfigurerat tas den högsta IPv4 adressen från Loopback-interface som ej är shutdown. Finns inget loopback interface tas högsta IPv4 adressen från övriga interface.

Finns flera OSPFv2 processer på samma router så kommer de att försöka välja olika router ID:n. Interfacet som router IDt tas från behöver inte vara med i OSPFv2 processen. Interface i Down/down kan väljas som router ID, enbart shutdown som tar bort interface som kandidat. OSPFv2 behöver inte annonsera en rutt till RID. Vilket router ID som används ändras enbart när processen startas om även om ett hårdsätts i konfigurationen. Vid förändring av router ID behöver övriga routrar i samma area räkna om SPF.

OSPF Paket

Paket	Beskrivning

Hello	Används för att hitta grannar, förflytta grannar till 2-Way State och som keepalive
Database Description (DD, DBD)	Används för att dela med sig av LSA Headers under den första topologiutväxlingen så att en router känner till sin grannes LSAer, inklusive versioner
Link-State Request (LSR)	Ett paket som identifierar en eller flera LSAer som en router önskar veta från sin granne
Link-State Update (LSU)	Svar på LSR från granne med full information om begärda LSAer. Skickas även vid topologiförändringar
Link-State Acknowledgement (LSAck)	Skickas som ack efter mottagen LSU

image.png

Kommandot show ip ospf neighbor [details] visar vilket läge nuvarande grannar är i. Se exempeloutput:

```
catalyst#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.2.3.4         1   FULL/BDR        00:00:02    2.3.4.5   Vlan1337

catalyst#show ip ospf neighbor 1.2.3.4 detail
 Neighbor 1.2.3.4, interface address 2.3.4.5, interface-id 145
    In the area 0 via interface Vlan1337
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 1.3.3.7 BDR is  2.3.4.5
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:02
    Neighbor is up for 25w6d
    Index 1/2/6, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 1.2.3.4, interface address 192.168.32.15, interface-id 146
    In the area 0 via interface Vlan1338
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 1.3.3.7 BDR is 3.4.5.6
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
```

LLS Options is 0x1 (LR)

Dead timer due in 00:00:02

Neighbor is up for 4d18h

Index 1/5/10, retransmission queue length 2, number of retransmission 0

First 0x0(0)/0x0(0)/0x7F8D50F91D10(2024369) Next 0x0(0)/0x0(0)/0x7F8D50F91D10(2024369)

Last retransmission scan length is 0, maximum is 0

Last retransmission scan time is 0 msec, maximum is 0 msec

Link State retransmission due in 4588 msec

Neighbor States

OSPF grannar är olika lägen beroende på om ett grannskap har lyckats bildas, är påväg att bildas eller har misslyckats att bildas.

Grannläge	**Förklaring**
Down	Grannskap nere. Syns oftast när ett tidigare bildat grannskap har gått ned.
Attempt	Finns enbart på NBMA och P2MP interface. Grannar placeras direkt i attempt på dessa interface och Hello-paket skickas. Flyttas till Down om granne ej svarar.
Init	Hello paket har tagits emot men Hello-paket innehåller inte mottagande routers RID. Mottagande router kan alltså höra skickande router men är inte säker på tvåvägskommunikation.
2-Way	Hello paket har mottagits från granne och mottagande routers RID finns i Hello-paket. Bekräftar tvåvägskommunikation mellan routrarna. Routrar som inte pratar med varandra, såsom DR/OTHER på multiaccesssegment, kommer att stanna i 2-Way.
ExStart	En granne flyttas från Init eller 2-Way till ExStart när tvåvägskommunkationen är bekräftad. I ExStart vilken router som är Master och vilken som är Slave. Tomma DBD paket bytes ut för att jämföra Router ID, bestämma DR och komma överens om vilket sekvensnummer kommunikationen börjar på för kommande DBD paket i Exchange-läge.
Exchange	Granne flyttas hit från ExStart när Master/Slave har bestämts. DBD paket innehållande alla kända LSAer byts ut mellan routrarna.
Loading	Är i loading efter att LSAer har bytts ut i Exchange men routern behöver tid för att ladda ned LSAer.
Full	Grannskapet flyttas hit från Exchange eller Loading när grannskapet är klart. Databasen är synkad och Hello-paket utbytes för keepalive.

Hello process

Hello-paket fyller flera funktioner i OSPFv2. Hello-paket hittar andra OSPFv2 routrar på gemensamma subnät, de utför checkar på vissa konfigurationsparametrar, de bekräftar tvåvägskommunikation mellan routrarna och de övervakar grannskapet och reagerar när inget svar kommer från granne.

För att hitta grannar skickas multicasttrafik på samtliga OSPFv2 interface som ej är passive till 224.0.0.5. 224.0.0.5 är en reserverad multicastadress till OSPF All Routers. Paketen source IP är interfacets IPv4 adress. Det går att använda unnumbered links, alltså att hänvisa till en IP adress på ex. ett loopback-interface, det går bra.

Vissa kriterier måste matcha för att ett grannskap ska bildas. Dessa är:

1. Autentisering måste matcha
2. Måste vara i samma subnät, inklusive exakt match på subnätsmasken
3. Måste vara i samma OSPFv2 area
4. Måste vara samma areatyp (normal, stub, NSSA)
5. Router ID måste vara unikt
6. OSPFv2 Hello och Dead timers måste matcha

Process ID:t behöver ej matcha då det är lokalt för routern. För att DBD paket ska processas mellan grannar så måste MTU matcha men är tekniskt sett inte en del av Hello-processen. Hello-paket innehåller alla router ID:n från grannar en router har. Hello paketen agerar keepalive. Hellos skickas varje Hello-intervall och om ett Hello-paket ej tas emot inom definierad Dead interval så rivs grannskapet. Default-intervall för Hello paket är 10 sekunder på broadcast interface och 30 sekunder på nonbreadcoast och point-to-multipoint interface. Dead interval är per default 4 gånger så lång som helllo intervallen.

Det går att se timers genom kommandot show ip ospf interface x, se exempeloutput:

```
catalyst#show ip ospf interface vlan 1337
Vlan1337 is up, line protocol is up
  Internet Address 1.2.3.5/31, Interface ID 181, Area 0
  Attached via Interface Enable
  Process ID 1, Router ID 1.3.3.7, Network Type BROADCAST, Cost: 1048
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0          1048      no          no          Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.3.3.7, Interface address 1.2.3.5
  Backup Designated router (ID) 1.2.3.4, Interface address 1.2.3.4
  Timer intervals configured, Hello 1, Dead 3, Wait 3, Retransmit 5
    oob-resync timeout 40
```

```
  Hello due in 00:00:00
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Can be protected by per-prefix Loop-Free FastReroute
Can be used for per-prefix Loop-Free FastReroute repair paths
Not Protected by per-prefix TI-LFA
Index 1/33/37, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 42
Last flood scan time is 0 msec, maximum is 1 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 1.2.3.4  (Backup Designated Router)
Suppress hello for 0 neighbor(s)
Cryptographic authentication enabled
  Youngest key id is 1
```

När två routrar utbyter Hello-paket och parametrarna stämmer kommer inte hela LSA databasen att bytas ut direkt. Först skickas DBD som innehåller rubriker över alla LSAer, en indexerad lista över alla LSAer en router känner till. Därefter så ber routrarna om de LSAer från varandra som de lokalt inte känner till. Varje DBD paket har ett sekvensnummer. Varje DBD paket ackas genom att samma sekvensnummer skickas tillbaka (LSAck). En LSAck behövs för att sändande router ska gå vidare till nästa LSA.

Master/Slave

Dessa roller väljs under ExStart. Rollern dikterar vilket ansvar routern har under utbytet av DBD paket. Enbart master får skicka paket på eget initiatv och öka sekvensnummer. Slave får enbart skicka DBD paket som svar på DBD paket från master. Det blir en polling från master till slave.

DBD paketet innehåller bland annat följande flaggor:

- Master (MS) flag, är flaggad i samtliga paket skickad från master och är ej flaggad i paket från slave
- More (M) flag, flaggas när en router tänker skicka fler DBD paket efter flaggat paket
- Init (I) flag, indikerar att det här är det första DBD paketet från master eller slave, följande paket ska ej ha denna flaggad

Skulle master skicka ett DBD paket och be om fler LSAer fast slave inte har några oskickade så svarar slave med ett tomt DBD paket, detta då slave måste svara på frågor från master. Om en slave har LSAer att dela med sig av som master ej har bett om så kommer slave att sätta M flaggan i sitt DBD-svar till master, då vet master att slave har fler LSAer att dela med sig av. Master slutar att skicka DBD paket till slave när den inte har några fler LSAer att dela med sig av och slaven ej skickade med M-flaggen i sitt senaste DBD paket.

När grannarna placerar varandra i ExStart (efter 2-Way) så anser båda att de är Master och skickar ett tomt DBD paket till varandra med ett slumpat sekvensnumret, MS flaggan, M flaggan och I flaggan. Efter mottagning av varandras DBD paket så ställer den router med lägre RID om sig till slave och svarar med ett DBD paket utan MS och I flaggan och sekvensnumret från routern med högre RID. Master skickar sedan DBD paket med sekvensnumret ökat med 1 och påbörjar utbytet av LSAer.

Requesting, Getting and Acknowledging LSas

Efter utbytet av LSA headers i början av utbytet så känner routrarna till vad sin granne känner till och ber om kompletterande LSAer för det den inte har i sin egen LSDB. För att se vilken router som har mest uppdaterad information jämfört sekvensnumret för en LSA i LSDB mot sekvensnumret för samma LSA i DBD paketet. Varje gång en LSA ändras på så ökar sekvensnumret. Sekvensnumret finns i headern för LSAerna, så om en router ser att en granne har ett högre sekvensnummer för en LSA kommer den att begära att få den LSAn skickad.

Link-State Requests (LSR) används för att begära en eller flera LSAer från en granne. Svar kommer med Link-State Updates. Det här sker i läget Loading. Samtliga LSUer ska ackas med en LSAck eller genom att repetera samma LSU tillbaka.

När LSAerna är synkade och därmed LSDB färdigbyggd kommer routrarna att köra SPF-algoritmen för att hitta snabbaste vägen till nätverket.

Designated Routers

För att LSA synkning på multiaccesssegment, ex. Ethernet, inte ska bli superbökig och kräva fulla utbyten mellan samtliga routrar på ett segment finns Designated Routers (DR). DR och Backup DR (BDR) är de enda routrar på ett segment som har fullt grannskap med andra routrar. Istället för att ex. 10 routrar alla skapar grannskap med varandra (det skulle bli totalt 45 grannskap) så sker full synkning enbart till DR & BDR som i sin tur skickar informationen vidare till övriga routrar. En router som inte är DR eller BDR benäms som DROTHER i Cisco outputs.

Grannskapen mot DR och BDR är alltså de enda som tar sig hela vägen till läget Full, sett från en DROTHER. Övriga routrar stannar i 2-Way. Från DR och BDRs synvinkel är samtliga grannskapslägen Full. För att kommunicera mot enbart DR och BDR så finns en broadcastadress, 224.0.0.6 (All OSPF DR Routers), som enbart DR och BDR lyssnar på. DR och BDR skickar sedan vidare mottagen LSA information som LSU till 224.0.0.5 (All OSPF Routers). LSUer som skickas från DROTHER till 224.0.0.6 får ej en LSAck tillbaka från DR/BDR, LSU flooden till 224.0.0.5 räcker som ack. Övriga routrar, inklusive BDR, måste dock Ack:a DR LSU med en unicast LSAck.

Valet av DR och BDR sker vid första grannskap på en länk. Ingen preemption sker, mottages ett Hello-paket med ett populerat DR-värde så accepterar routern denna som sin DR. För att välja om DR, eller BDR, krävs det att grannskap på segmentet bryts på valfritt sätt. Valet av DR/BDR sker när Hello-paket från en granne innehåller en DR med värdet 0.0.0.0, alltså ingen vald, efter en timer som kallas OSPF wait time. OSPF wait time är samma värde som Dead-timern. Detta för att ge eventuella andra routrar på segmentet möjlighet att svara/skicka Hello-paket.

En router kan bli DR/BDR om OSPF prioriteten på interfacet är mellan 1 och 255. Ett värde på 0 innebär att den inte deltar i valet. Varje router väljer sin DR/BDR på egen hand men algoritmen ser till att det blir samma utfall i samtliga routrar. Om en router mottager en Hello-paket med populerat DR/BDR värde under OSPF wait time så kommer routern direkt påbörja DR/BDR valet. Valet sker bara för roller som ej är tillsatta, finns en DR eller en BDR redan så kommer enbart den ena väljas. Skulle två routrar ha samma OSPF priority så vinner högsta RID. Skulle en DR försvinna från segmentet så blir BDR befodrad till DR och ny BDR väljs.

Skulle samma segment innehålla flera routrar som tror sig vara DR/BDR, exempelvis vid länk som har gått ned mellan ett segment av routrar, så kommer regeln om ingen preemnt att skrotas och ett nytt val av DR/BDR sker.

OSPF Network Type

DR/BDR behövs ej på P2P-länkar. På NBMA nät kan DR vara hjälpsamma. Det går att ställa in om DR ska användas genom att ändra OSPF Network Type på interfacet. Beroende på vilken nätverkstyp man väljer så ändras OSPFv2s timers. Hård konfgurerade timers överskrider nätverkstypens default timers.

image.png

Kommandot för att ändra OSPFv2 nätverkstyp i interfacekonfigläge är `ip ospf network TYPE`, där TYPE är något av valen ovan.

Stabil drift

När OSPFv2 har stabiliserat sig och konvergeras, dvs att samtliga routrar inom ett area har exakt samma LSDB och har räknat ut bästa vägarna via SPF, sker följande:

- Routrar skickar Hello-paket baserat på interface timers
- Routrar förväntar sig att ta emot Hello-paket på interface mot grannar och tar ned grannskap om Dead timern räknar slut
- Routrar floodar LSAer genererade lokalt på nytt efter halva sin livslängd (LSA MaxAge). Hela livslängden är default 60 minuter, flooding sker alltså efter 30 minuter
- Routrar förväntar sig att mottagna LSAer ska uppdateras inom LSA MaxAge (default 60 minuter)

OSPF Design, LSAer och Areas

Interface i OSPF gruppas in i areas. Det viktigaste areat är 0. Formatteras enligt industristandard som 0.0.0.0, i IOS-XE kan man skriva det på båda sätt. Area 0 är känt som backbone area. Samtliga övriga areas måste ansluta sig mot area 0. Area 1 kan inte ha en direktlänk till area 2 utan måste traversera area 0 för att nå area 2. En router som ansluter till flera areas kallas för Area Border

Router (ABR). En router blir ABR när den har interface konfigurerade i flera olika areas inklusive area 0, alltså ex. `ip ospf 1 area 0` på GigabitEthernet0/0 och `ip ospf 1 area 1` på GigabitEthernet0/1, och interfacen är uppe. En router som är ansluten till area 1 och area 2, men inte area 0, anser sig inte vara en ABR.

En router som injicerar rötter in i OSPF via redistribuering kallas för Autonomous System Boundary Router (ASBR).

image.png

En OSPFv2 router har en LSDB per area den är ansluten mot. Innehållet i de olika LSDBerna är isolerade, men en ABR kommer att översätta innehållet kontrollerade mellan LSDBerna. SPF-uträkning körs per area.

Det finns flera fördelar av att använda sig av OSPFv2 areas:

- Mindre LSDBer vid styckning av areas. Routrar i mindre areas behöver inte vara lika fläskiga som routrar i större areas
- Snabbare SPF uträkningar då LSDBn är mindre
- Om en länk går ned behöver SPF inbart köras av routrar inom länkens area
- Det är enbart av ABRer (och ASBRer) som summering och filtrering av rötter kan ske i OSPF

Mellan areas skickas inte Typ 1 eller Typ 2 LSAer. Istället skickas Typ 3 LSAer (Summary LSA) som är mindre detaljerade än en typ 1 eller typ 2. Därmed blir även LSDB storleken mindre med användning av areas, även för rötter som läcks mellan areas.

Vägval

OSPF föredrar alltid en intra-area router, alltså en route som kommer från samma area routern är i, över en inter-area route. Det gäller även om metricen för inter-area routen är bättre än metric för intra-area routen. En ABR kommer ej att processa en typ 3 LSA (summary) om den är mottagen via ett area som ej är backbone. Det är en loopförhindrade mekanism, Split Horizon!

Hackordning är enligt följande (där 1 vinner):

1. Intra-area
2. Inter-area
3. E1/N1
4. E2/N2

Den här hackordningen vinner alltid över cost. Så även om en E2 router är tusen gånger bättre än en Inter-area kommer Inter-area att vinna.

LSA Typer

En LSA kan enbart modifieras av den som skapade LSAn. Övriga routrar har som skyldighet att processa och sprida vidare LSAn enligt sin roll.

LSA Typ	Namn	Beskrivning
1	Router	1 per router i ett area. Innehåller routerns RID och alla dess interface inom det area. Skickas enbart inom ett area.
2	Network	Skapas av DR om sådan finns. Innehåller det subnätet och interface på det subnätet. Skickas enbart inom ett area.
3	Net Summary	Skapas av ABR när typ 1 anländer via ett area och ska annonseras till ett annat area. Definierar subnäten och cost men ingen topologi. Floodas inom ett area.
4	ASBR Summary	Som en typ 3 men annonseras host route för att nå ASBR i ett annat area.
5	AS External	Skapas av ASBR för rötter som injiceras i OSPF. Floodas till alla vanliga areas.
6	Group Membership	Används ej av Cisco IOS
7	NSSA External	Som en typ 5 men från en ASBR i NSSA. Konverteras av typ 5 av ABR.
9-11	Opaque	För framtiden! 9 = link-local flooding, 10 are local flooding, 11 AS flooding som typ 5

Två termer som ska kännas till är Transit network, vilket är ett nätverk som en eller flera OSPFv2 routrar har blivit grannar över, och Stub network, vilket är ett subnät som en OSPFv2 router ej har grannar via.

LSA Typ 1 och 2

Varje router skapar och skickar ut en typ 1 LSA för sig själv i varje area den har interface inom. Typ 1 LSAer beskriver routern, OSPFv2 interfacen inom ett area och en lista över grannar per interface. LSAn identifieras av en link-state ID (LSID) vilket är samma värde som RID.

Typ 2 beskriver ett transit subnet som en DR har blivit vald på. Typ 2 skapas enbart av DR. LSIDn är DRns interface IP address på det subnätet.

Med hjälp av Typ 1 och Typ 2 LSAer kan SPF algortimen räkna ut bästa vägen till ett nätverk inom ett area.

LSAer kan kontrolleras med show ip ospf database. För att se specifikt typ 1 och typ 2 finns show ip ospf database router och show ip ospf database network, se exempel här:

```
catalyst#show ip ospf database router

            OSPF Router with ID (1.3.3.7) (Process ID 1)

□□Router Link States (Area 0)

  LS age: 1583
  Options: (No TOS-capability, No DC)
  LS Type: Router Links
  Link State ID: 1.2.3.4
  Advertising Router: 1.2.3.4
  LS Seq Number: 8000358F
  Checksum: 0x8A41
  Length: 84
  Area Border Router
  AS Boundary Router
  Number of Links: 5

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 2.3.4.5
     (Link Data) Router Interface address: 3.4.5.6
      Number of MTID metrics: 0
       TOS 0 Metrics: 1000

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 10.0.0.0
     (Link Data) Network Mask: 255.255.255.240
      Number of MTID metrics: 0
       TOS 0 Metrics: 10

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 10.0.1.0
     (Link Data) Network Mask: 255.255.255.240
      Number of MTID metrics: 0
       TOS 0 Metrics: 10

    Link connected to: a Stub Network
```

```
    (Link ID) Network/subnet number: 10.0.2.0
    (Link Data) Network Mask: 255.255.255.240
     Number of MTID metrics: 0
      TOS 0 Metrics: 10

   Link connected to: a Transit Network
    (Link ID) Designated Router address: 4.5.6.7
    (Link Data) Router Interface address: 1.2.3.4
     Number of MTID metrics: 0
      TOS 0 Metrics: 10

catalyst#show ip ospf database network

          OSPF Router with ID (1.3.3.7) (Process ID 1)

  Net Link States (Area 0)

  LS age: 1475
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 1.3.3.8 (address of Designated Router)
  Advertising Router: 1.3.3.7
  LS Seq Number: 80000D3F
  Checksum: 0xBC10
  Length: 32
  Network Mask: /28
  Attached Router: 1.3.3.7
  Attached Router: 1.3.3.8
```

För att signalera att ett nätverk har gått ned (ex. interface går ned) så skapar en routar en ny LSA som exkluderar nätverket, alternativt skickas en LSA med där LSA MaxAge har gått ut vilket gör att routrar som mottar den nya LSAn direkt informationen om nätverket.

LSA Typ 3

En ABR kommer aldrig att skicka vidare en Typ 1 eller Typ 2 LSA från ett area till ett annat. Istället så skapar den en Typ 3 som representerar de Typ 1 eller Typ 2or som ABRen känner till. En ABR kommer enbart att hantera en inkommande Typ 3 som är mottagen via Area 0. När en ABR skapar en typ 3 så kommer enbart intra-area rötter från icke backbone att skickas till backbone som Typ 3. I motsatt riktning, från backbone till annat area, kommer både inter-area och intra-area rötter att skickas vidare som Typ 3.

```
catalyst#show ip ospf database summary

            OSPF Router with ID (1.3.3.7) (Process ID 1)

  Summary Net Link States (Area 0)

  LS age: 1033
  Options: (No TOS-capability, DC, Upward)
  LS Type: Summary Links(Network)
  Link State ID: 10.1.3.0 (summary Network Number)
  Advertising Router: 1.3.3.7
  LS Seq Number: 8000039D
  Checksum: 0x6536
  Length: 28
  Network Mask: /24
  MTID: 0  Metric: 66583

! Cost för att nå en border router kan ses med nedan kommando

catalyst#show ip ospf border-routers

            OSPF Router with ID (1.3.3.7) (Process ID 1)


  Base Topology (MTID 0)

Internal Router Routing Table
Codes: i - Intra-area route, I - Inter-area route

i 9.9.9.9 [3096] via 2.3.4.5, Vlan1337, ABR/ASBR, Area 0, SPF 259

sw-distacc#show ip ospf statistics

            OSPF Router with ID (1.3.3.7) (Process ID 1)

  Area 0: SPF algorithm executed 702 times

  Area 1: SPF algorithm executed 114 times

  Area 3: SPF algorithm executed 15974 times
```

```
  Area 7: SPF algorithm executed 763 times

  Summary OSPF SPF statistic

  SPF calculation time
Delta T   Intra D-Intra Summ D-Summ Ext D-Ext Total Reason
17:30:52   0 1 0 0 0 1 2 R, X
12:46:29   0 0 0 0 0 1 2 R, X
12:45:17   0 0 0 0 1 0 1 R
12:45:16   0 0 1 0 0 1 2 R, X
05:30:33   0 0 0 0 1 0 1 R, X
05:29:29   0 0 0 0 1 0 1 R
05:29:29   0 0 0 0 1 0 1 R, X
00:45:05   0 0 0 0 1 0 1 R, X
00:43:45   1 0 0 0 0 1 2 R
00:43:44   0 0 0 0 1 0 1 R, X
```

En bra nyans att känna till är att trafik mellan areas måste flöda genom en router som är ansluten till backbone. Det betyder dock inte att trafiken behöver flöda via ett interface i backbone. Om en ABR är ansluten till area 0, area 1 och area 2 så kommer trafiken att flöda direkt mellan area 1 och 2 i det fallet.

Typ 4 och 5 SLAer samt External Routes Typ 1 och 2

Redistribuerade rötter in i OSPFv2 märks med External Route Type 1 (E1) eller External Route Type 2 (E2). Metrics för E2 förändras inte hop-per-hop utan är samma konstant enligt vad som specifiseras i redistribueringen. Metrics för E1 ändras per hop, precis som för övriga LSAer. En E1 föredras över en E2 vid routingbeslut.

När en extern route injiceras via redistribuering så skapas en typ 5 LSA för subnätet. LSAn innehåller metricen och metrictypen (E1/E2). LSAn skickas till samtliga OSPFv2-grannar. När en LSA typ 5 traverserar areas så skapar ABR en LSA typ 4 som skickas ut i samband med typ 5. Detta då LSA typ 5 innehåller information om vilken ASBR som nätet finns via vilket det andra areat inte känner till via de typ 3 som har skickats in i areat. LSA typ 4 innehåller information om vilken ABR areat ska använda för att nå nätverket annonserat i LSA Typ 5.

```
! Exempel på typ 5:
catalyst#show ip ospf database summary

        OSPF Router with ID (13.3.7) (Process ID 1)
```

Summary Net Link States (Area 1337)

LS age: 1856

Options: (No TOS-capability, DC, Upward)

LS Type: Summary Links(Network)

Link State ID: 10.0.0.0 (summary Network Number)

Advertising Router: 1.2.3.4

LS Seq Number: 80000D68

Checksum: 0xFDAC

Length: 28

Network Mask: /21

MTID: 0 Metric: 2106

Stubby Areas

Mellan vanliga areas så sker ingen filtrering. Teknikerna beskrivna ovan begränsar hur ofta och omfattande SPF måste räknas om vid topologiförändringar, men visibileten mellan area 0 och övriga "normala" areas är oförändrad. För att ändra vilka rötter som propageras via LSAer mellan areas behöver man använda sig av olika areatyper. Det är enda sättet man kan filtrera och summera rötter i OSPF. Dessa varianter kallas för stubby areas.

Om ett area konfigureras som stub så kommer ABRer ej att annonsera LSA typ 4 eller LSA typ 5 in i areat. Externa rötter kommer alltså inte propageras in i dit. Tanken är att dessa ska täckas av en default-route, som per default kommer annonseras in i areat via ABR. Skulle en typ 5 mottas så kommer en stub-router att strunta i paketet och den kommer aldrig själv att skapa en typ 5.

Beroende på vilken typ av stubby-area man nyttjar kan även Typ 3 ej annonseras in i areat, vilket gör att areat enbart får en default-route injiceras. Det går även att använda sig av Not-so-stubby areas för att tillåta att externa routes injicera från inuti stub-areat. Dessa får en LSA Typ 7 inom areat. Typ 7 översätts till typ 5 av ABR. Se tabell:

Areatyp	**Stoppar typ 4/5?**	**Stoppar typ 3?**	**Tilllåter skapande av typ 7?**	**Konfiguration**
Stubby	Ja	Nej	Nej	area x stub
Totally stubby (S)	Ja	Ja	Nej	area x stub no-summary
Not-so-stubby area (NSSA)	Ja	Nej	Ja	area x nssa
Totally NSSA (NSSA-TS)	Ja	Ja	Ja	area x nssa no-summary

Jag tycker personligen om att använda av NSSA. Möjligheten att summera och filtrera samtidigt som flexibiltet finns för att kunna injicera ex. redistribuerade statiska rötter är väldigt trevlig. Om

en default route ska annonseras i ett NSSA (ej NSSA-TS) så måste det manuellt konfigureras med `area x nssa default-information-originate`.

För att ett NSSA ska acceptera en default-route från en grannrouter i samband med VRF:er krävs kommandot `capability vrf-lite`. Se ex:

```
router ospf 4 vrf veeerf
 capability vrf-lite
```

Exempelkonfiguration och diverse förklaringar

```
interface Vlan2
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 AABBCCDDEEFF
 ip ospf dead-interval 3
 ip ospf hello-interval 1
 ip ospf 1 area 0
 ip ospf priority 100

router ospf 1
 router-id 1.3.37
 auto-cost reference-bandwidth 1048576
 area 0 filter-list prefix FILTER out
 area 2 nssa
 area 2 range 10.100.0.0 255.255.0.0
 area 2 nssa default-information-originate no-summary
 redistribute static route-map ROUTE_MAP_OSPF
 passive-interface default
 no passive-interface Vlan2
 distribute-list prefix OSPF_IN in
 default-information originate

router ospf 2 vrf ospf-vrf
 router-id 3.4.5.6
 auto-cost reference-bandwidth 1048576
 nsf ietf restart-interval 140
```

```
 capability vrf-lite
 area 10 nssa
 passive-interface default
 no passive-interface Vlan3
!
```

Interface

Det går att aktivera OSPFv2 för ett interface på två sätt. Det ena är som i exemplet ovan, att aktivera det direkt på interfacet. Det andra är att matcha den IP adress som finns på interfacet i OSPFv2 processen. Ex. har Vlan2 IPv4 10.10.10.10 kan interfacet läggas till i OSPFv2 processen genom kommandot network `10.10.10.10 0.0.0.0 area 0`. Nollorna är wildcard, alltså matchar 4 nollor enbart det här interfacet. Aktiveras OSPFv2 via interfacet, som i exemplet ovan, kommer secondary addresses även att annonseras som stubnätverk. Det går att exkludera secondaries genom att lägga till `secondaries none` på slutet av kommandot.

För att aktivera autentisering måste både en autentiseringsmetod och själva nyckeln specifiseras. Den konfiguration som är möjlig att göra i OSPFv2 processen är enbart att sätta default-autentisering för interface i areat. Inga lösenord kan konfigureras där. Kommandona i OSPFV2 processen är `area x authentication` för okrypterad text och `area x authentication message-digest` för MD5 kryptering.

Prioriten är för valet av Designated Router. Hög prioritet är bättre än låg. Default är 1.

OSPFv2 Process

`auto-cost reference bandwidth` ändrar default-kostnaden för interface. Värdet bör matcha på samtliga routrar i OSPFv2-domänen. Cost går även att sätta manuellt på interface.

`area 0 filter-list prefix FILTER out` filtrerar baserat på prefix lista vilka rötter som får lämna area 0 och installeras i övrigt anslutna areas på ABR. Det går även att konfigurera i andra riktningen, in, alltså vilka rötter som får installeras in i ett area.

`distribute-list prefix OSPF_IN in` filtrerar baserat på prefix lista vilka rötter som får installeras från LSDB till RIB. LSDB modifieras ej. Det går även att specifisera distribute-lists per interface.

`area 2 range 10.100.0.0 255.255.0.0` är ett kommando som summerar vilka rötter som finns inom ett area. I det här fallet kommer area 0 enbart känna till /16 masken i area 2 och inte samtliga specifika prefix. Det går även att lägga till `not-advertise` efteråt vilket gör att varken de mindre prefixen eller summeringen annonseras.

Virtual Link

Vid händelse att en OSPFv2 domän är helt trasig eller felbyggd och direktanslutning från area 0 till ett annat area ej är möjligt finns virtual links. De kan ej byggas någon form av stub-area. Det gör

att en router i exempelvis area 5 tror sig vara direktansluten till area 0 även om trafiken går genom area 10. Det är inte ett tunnelprotokoll utan paketen routas som vanligt. Konfigurationen är enkel, i OSPFv2 processen konfigureras `area 10 virtual-link 10.20.30.40`. Det som specifiseras är transit-areat och destinationsroutern router ID.

Det går att nå samma resultat med GRE-tunnlar, även här över stub-areas. Dock så behöver man då tänka på att det är en tunnel och minst 24 bytes måste skyfflas undan åt GRE. Rekommendationen (riktiga rekommendationen är bygg inte OSPFv2 såhär...) är att använda virtual-links om man verkligen måste. GRE om man är utan val.

Autentisering är möjlig för virtual-links. Tillgängliga kommandon är `area x virtual-link 1.2.3.4 authentication null`, `area x virtual-link 1.2.3.4 authentication authentication-key x` och `area x virtual-link 1.2.3.4 authentication message-digest message-digest-key x md5 x`.

Autentisering med SHA-HMAC

Olika autentiseringsmetoder beskrivs ovan. IOS stöd för autentisering med SHA-HMAC med hjälp av key-chains. Det gäller även virtual-links. Send-liftime och accept-life-time går att specifisera för att byta ut nycklar periodvis. Nyckeln med högst key ID används om flera val finns. För skickade paket signerar routern paketen med giltig nyckel med högst key ID. För mottagna paket matchas det key ID som anges i mottagna paketet. Det går att kombinera en key-chian med MD5 kryptering med klassisk OSPFv2 MD5 autentiseringssyntax.

Exempelkonfiguration:

```
key chain OSPF
 key 1
   cryptographic-algorithm hmac-sha-256
    key-string p4ssw0rd1337

interface GigabitEthernet0/1
 ip ospf authentication key-chain OSPF

router ospf 1
 area 10 virtual-link 10.20.30.40 key-chain OSPF
```

TTL Security

OSPFv2 har stöd för TTL-security. Samtliga pakets TTL sätts då till 255 när de skickas. Om ett paket mottags med mindre TTL än 255 så slängs det, då har paketet routats på vägen och är inte direktanslutet. Detta för att skydda mot att någon illasinnat skapar ett OSPFv2 paket som skickas

via unicast. Kan användas som överbelastningsattack mot ens routers CPU. TTL Security kan konfigurerasper interface med kommandot `ip ospf ttl-security` eller i en OSPFv2 process med kommandot `ttl-security all-interfaces`. Om det konfigureras per OSPFv2 process kan det stängas av per interface med `ip ospf ttl-security disable`. Det går att lägga till `hops x` på slutet av kommandot för att tillåta lägre TTL-värde. `ip ospf ttl-security hops 50` skulle ex. tillåta att routern processar ett paket med TTL 205.

SPF Throttiling

Det går att ställa in hur ofta SPF processen ska köras för att räkna ut bästa väg til destinationer. Inledningsvis så ska det här aldrig behöva ändras i miljöer av vanlig storlek. Per default så körs SPF 5 sekunder efter mottagen LSA. Kommer en uppdaterad LSA efter den här SPF-körningen så ökar väntetiden till 10 sekunder. Det är för att undvika att köra SPF medans man fortfarande mottager LSAer konstant.

Praramterarna för en SPF körning är spf-start, spf-hold och spf-max-wait. Start parametern indikerar väntetid innan en SPF uträkning när nätverket har varit stabilt under tid. Hold parametern indikerar väntan mellan efterföljande SPF körningar och dublerar sitt värde efter varje efterföljande SPF körning. max-wait parametern definierar den absoluta maxtiden mellan SPF-körningar, så hold parametern kan aldrig överstiga max-wait. Den definierar också hur länge ett nätverk ska vara stabilt för att flyttas tillbaka till värdet i spf-start.

Se följande för demonstrering:

1. LSA mottages sekund 0. Routern planerar SPF att köras om 10 sekunder.
2. Ny LSA mottages sekund 2. LSA sparas i LSDB och kommer att inkluderas i SPF-körningen.
3. Sekund 10 körs SPF och spf-hold värdet sätts till 15 sekunder. Om en LSA mottages inom dessa 15 sekunder så kommer nästa SPF körning köras sekund 25. Nätverket anses vara stabilt enligt max-wait värdet efter 100 sekunder efter SPF körning, alltså sekund 110.
4. En eller flera LSAer mottags mellan sekund 10 och sekund 25.
5. SPF körning körs sekund 25. spf-hold värdet dubbleras till 30 sekunder, alltså kommer nästa körning för mottagna LSAer ske sekund 55. Nätverket anses vara stabilt enligt max-wait sekund 125.
6. Inga LSAer tas emot kommando 30 sekunder. Väntetiden för SPF körning sätts tillbaka till spf-start värdet, alltså 10 sekunder. Nätverket anses inte stabilt än då sekund 125 ej har nåtts och spf-hold värdet är fortfarande 30 sekunder.
7. Sekund 80 tas en LSA emot. SPF uträkning planeras till sekund 90.
8. Sekund 90 körs SPF. Väntetiden till nästa SPF körning blir dubblerad från tidigare, alltså nu 60 sekunder. Om nya LSAer tas emot de kommande 60 sekunderna kommer SPF körning att ske sekund 150. Nätverket anses stabilt om 100 sekunder, sekund 190.
9. Inga LSAer tas emot de kommande 60 sekunderna. Vänteintervallen sätts tillbaka till spf-start, 10 sekunder, spf-hold är fortsatt 60 sekunder.
10. Inga nya LSAer har mottagits till sekund 190. Nätverket anses vara stabilt och spf-hold är åter 15 sekunder.

SPF throttling ställs in i OSPF-processen med kommandot `timers throttle spf spf-start spf-hold spf-max-wait`, värdena ska såklart bytas ut. Vilka värden som används kan ses med `show ip ospf | inc SPF`.

```
catalyst#show ip ospf | inc SPF
 Initial SPF schedule delay 50 msecs
 Minimum hold time between two consecutive SPFs 200 msecs
 Maximum wait time between two consecutive SPFs 5000 msecs
```

LSA Throttling

Precis som ovan är det här nånting man helst inte skruvar på. Det ska finnas goda skäl för att ändra på de fördefinierade värdena.

Med LSA Throttling kan man ställa in hur ofta en LSA skapas på nytt från en router. LSA Throttling använder sig av ungefära samma värden som SPF Throttling, `start-interval`, `hold-interval` och `max-interval`. När en LSA inte har uppdaterats fler gånger än max-interval värdet säger och den behöver skapas på nytt så återskapas LSAn och skickas till grannar aefter start-interval värdet. Väntetid sätts enligt värdet i hold-interval. Om samma LSA behöver uppdaterats på nytt inom väntetiden så väntar routern med det tills att väntetiden enligt hold-interval har gått ut. Hold-interval dubbleras varje gång LSAn behöver uppdateras inom väntetiden. Väntetiden kommer aldrig att överstiga värdet i max-interval. Om LSAn ej behöver uppdateras när väntetiden har gått ut kommer väntetiden att sättas enligt värdet i start-interval men hold-interval är fortfarande kvar på det högre värdet. Behöver LSAn skickas på nytt under väntetiden, men innan max-interval värdet har nåtts, kommer nästa väntetid att bli enligt det höga hold-interval värdet, fast dubblerat såklart. Verkligen samma beteende som i SPF Throttling.

Defaultbeteende i Cisco IOS är att en uppdaterad LSA skickas direkt och en till uppdatering av denna väntar 5 sekunder. Start-interval blir alltså 0, hold-interval är 5000 millisekunder och max-interval är 5000 millisekunder. Alltså är maxtiden en LSA behöver vänta på att skickas 5 sekunder. LSA throttling konfigureras i OSPFv2 processen med `timers throttle lsa all start-interval hold-interval max-interval`, med utbytta värden såklart. Routerns värden går att se med `show ip ospf | inc LSA`.

```
catalyst#show ip ospf | inc LSA
 Initial LSA throttle delay 50 msecs
 Minimum hold time for LSA throttle 200 msecs
 Maximum wait time for LSA throttle 5000 msecs
 Minimum LSA arrival 100 msecs
 LSA group pacing timer 240 secs
```

Det går även att ställa in så att en router ignorerar LSAer som mottags för tätt intill varandra genom att justera LSA arrival värdet med kommandot `timers lsa arrival milliseconds` i OSPFv2 processen. Om två eller flera likadan LSAer mottags millisekunder mellan varandra så accepteras den första och den andra slängs.

Incrimental SPF

ISPF är att sätt att låta SPF enbart räkna om de delar av topologin som förändras vid LSDB-uppdateirng. Det kan minska CPU-lasten och snabba på konvergenstiden. Kan vara bra att använda sig av i större topologier. Aktiveras med kommandot `ispf` i OSPFv2 processen.

```
catalyst#show ip ospf | inc Incremental
 Incremental-SPF disabled
```

OSPFv2 Prefix Suppression

I stora nät kan en stor del av innehållet i LSDB vara länknät (transit networks). Det kan vara helt ointressant för en router i Kiruna att känna till ett länknät i Kapstaden när det egentligen är är stub network som är intressant, alltså subnätet som hostar siter anslutna mot. RFC 6860 definierar en metod för att dölja eller bli väck med dessa prefix från LSDB. I en typ 1 LSA så definieras en routers anslutna nätverk. Dessa kan vara P2P, transit networks, stub networks eller virtual links. Prefix Suppression gör då att en router ej annonserar de som är definierade som transit network. Typ 2 LSAer är lite meckigare. Routern som skapar typ LSAn kommer här att sätta nätmasken till 255.255.255.255, som då är helt ogiltig för en Typ 2 LSA. Routrar som förstår RFC 6860 kommer ej att installera den här LSAn. Routrar som inte förstår RFC 6860 kommer att installera en host route.

OSPFv2 Prefix Suppression kan aktiveras per process eller per interface. I OSPFv2 processen är kommandot `prefix-suppression`, vid aktivering kommer routern att suppressa allt förutom loopbacks, sekundära adresser och prefix på passiva interface. Vill man stänga av prefix-suppression för ett visst interface är kommandot `ip ospf prefix-suppression disable`. Vill man aktivera prefix-suppression per interface är kommandot `ip ospf prefix-suppression`.

Ett bra användningsområde av prefix suppression är nät där man använder sig av GRE-tunnlar. Då riskerar man inte att det blir recursive routing, dvs att man lär sig tunnelns endpoint-adresser via tunneln.

Stub Router

Det är skillnad på stub router och ett stub area. En stub router är en router som under viss tid, eller permanent, ej kan bli en transit router. Det vill säga att den inte används för att skicka paket vidare till en annan router. Det kan vara bra vid underhåll, ex. om en ASBR kör både OSPF och BGP, alltid annonserar en default route via OSPF, men vid omboot tar BGPn längre tid på sig att konvergeras vill man ej att trafik går via denna router. ASBRn kommer när den är en stub router att annonsera sina egna LSAer med en infinite metric cost (16,777,215) för samtliga transit-adjacencies. Dess direktanslutna stubnät annonseras som vanligt.

Det här går att ställa in i OSPFv2 processen. Det går att göra med `max-metric router-lsa on-startup announce-time`, då kommer routenr att annonsera transit LSAer med infinite metric tills att announce-time värdet har nåtts. För just BGP finns kommandot `max-metric router-lsa on-startup wait-for-bgp` vilket gör att annonsering blir med infinite metric tills att BGP har signalerat att den är klar eller 10 minuter har passerats.

Graceful Restart

Graceful restart (GR) tillåter en router att fortfarande skyffla trafik medans OSPFv2 processen är nere. Konfigureras i routingprocessen med kommandot `nsf`. Detta då Cisco utvecklade en egen variant, Non Stop Forwarding, innan GR implementerades. Cisco IOS stöder båda varianter.

När GR används så signalerar en router att den äri restart mode. Direktanslutna granar är i helper mode. Grannarna struntar under GR tiden att dfe inte mottar några Hellos och justerar varken LSDB eller routingtabell därefter. Om en DR signalerar att den är i restart mode så förlorar den ej rollen som DR.

```
catalyst#show ip ospf | inc NSF
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
```

Graceful Shutdown

Graceful shutdown används när man stänger av OSPFv2 genom att konfigurera `shutdown` i OSPFv2 processen eller `ip ospf shutdown` på interfacenivå. Routern tar då ned OSPFv2 grannskap (samtliga eller för specifiserat interface), skickar ut egenskapade LSAer med LS Age satt till LSA MaxAge (default 3600 sekunder) för att tömma domänen, skickar Hello-paket till grannar med DR/BDR fälten satta till 0.0.0.0 och en tom grannlista och til sist slutar skicka och ta emot OSPFv2 paket.

Återaktivering sker genom att ta bort konfigurationen ovan.

Default route

En default route kan injiceras i OSPFv2 processen genom kommando `default-information originate [ always ]`. Utan nyckelordet always på slutet så krävs det att en defaultroute redan finns i routingtabellen.

Om en default route ska annonseras i ett NSSA (ej NSSA-TS) så måste det manuellt konfigureras med `area x nssa default-information-originate`.

För att ett NSSA ska acceptera en default-route från en grannrouter i samband med VRF:er krävs kommandot `capability vrf-lite`. Se ex:

```
router ospf 4 vrf veeerf
 capability vrf-lite
```

NSF & NSR

NSF aktiveras i OSPFv2 processen med `nsf ietf`, om inte redan aktiverat. Verifiering med `show ip ospf x nsf`, där x är process ID.
Timers kan sättas i OSPFv2 processen med `nsf ietf restart-interval x`. Det går att stänga av en routers möjlighet att vara NSF helper med `nsf ietf helper disable`.

NSR aktiveras via kommandot `nsr` i OSPFv2 processen.

Max LSA & redistribute maximum-prefix

Sedan IOS-XE 17.11.1 (källa här) är funktionerna Max LSA och Redistribute maximum-prefix aktiverade per default. I tidigare releaser är de avstängda. Max LSA är aktiverat med värdet 50 000 per default och redistribute maximum-prefix är aktiverat med värdet 10 240 per default. max-lsa begränsar hur många LSAer en OSPF process kan ta emot. redistribute maximum-prefix begränsar hur många prefix en process kan redistribuera.

Syns enbart i konfigen om man har manuellt ändrat värdena:

```
router ospf 1
 max-lsa 50001
 redistribute maximum-prefix 10241
```

Revision #1
Created 26 April 2025 12:02:26 by Jehrlander
Updated 26 April 2025 12:02:31 by Jehrlander