Cheat Sheet

OSPF

OSPF är ett link-state routing-protokoll med en administrativ distans av 110. OSPF designades som ett komplement för bristerna i RIP, som inte riktigt höll måttet vid dynamisk routing. RIP var det första protokollet för detta och baserade sina uträkningar på mängden hopp mellan routrar från källa till destination - ju färre desto bättre.

När bandbredd som krävdes av media ökade blev det tydligt att man inte kunde basera den bästa routen på mängden hopp - utan hur snabbt varje hopp kan ske. OSPF använder sig därför av "vikter" mellan point-to-point-anslutningar för att beräkna den bästa routen. Dessa vikter beräknas med hjälp av bandbredd (bandwidth), fördröjning (delay) och belastning (load).

Typer av länkar

- Point-to-point - två routrar kopplade över en länk (vanligtvis serial interface)
- Broadcast multiaccess - flera routrar kopplade över ethernet
- Non-broadcast multiaccess - bland annat frame relay
- Point-to-multipoint - frame relay
- Virtual link network - multiarea ospf

Typer av routrar

En OSPF-initierad router kan vidta fyra olika skepnader:

- Internat Router (IR) - en router med alla interface i samma area
- Backbone Router (BR) - en router i backbone area (area 0)
- Area Border Router (ABR) - en router med interface i två eller fler areor. Sammanfattar routes och skickar ut dessa till Backbone Area
- Autonomous System Border Router (ASBR) - en router med interface mot ett icke-OSPF nätverk, så som routern som kopplas till internet

Areas

I OSPF multiarea finns det två olika typer areor:

- Backbone Area - området vars huvudfunktion är att forsla ut data mellan areor. Kallas även area 0
- Regular Area - ett område som sammankopplar användare och resurser. Tillåter inte andra regular areor att använda dess länkar för att ta sig runt i nätverket. Om en länk går ner i en regular area berör det inte andra regular areor - dock får andra areor en notis om händelsen.

Problemet med Multi Access Network

När man skapar många grannskaper (adjacencies) så kan ethernet-nätverk potentiellt sett sammanlänka många OSPF-routrar på samma länk. Att skapa grannskap mellan varje router är onödigt och inte önskvärt. Detta leder till att en onödigt stor mängd Link State Advertisments (LSAs) skickas mellan routrarna.

I ett multi access network skulle då varje router uppdatera varandra om händelser, vilket slösas på bandbredden.

Detta löses genom att man utser en router till Designatet Router (DR). DR är den central som samlar in och skickar ut alla LSAs inom nätverket så att dessa meddelandena bara skickas *en* gång till varje router.

En Backup Designated Router (BDR) väljs också ut, ifall att DR skulle sluta fungera.

Valet av DR och BDR går efter prioritet:

1. Högst OSPF-prioritet
2. Högst router-ID
3. Högst loopback
4. Högst interface

Link State Advertisments (LSAs)

- Type 1 - genereras av alla routrar och skickas ut inom en area
- Type 2 - genereras av Designated Router på en multiaccess-segment och skickas ut inom en area
- Type 3 - genereras av Area Border Router och skickas ut mellan areor
- Type 4 - genereras av Area Border Router och skickas ut mellan areor för att tillkännage var en Area Border Router befinner sig

Säkerhet

Använd MD5 för autentisering. Interfaces som kopplas mot hosts bör vara i s.k. *passive state*.

PPP

Point-to-point protocol är ett link layer-protokol (alltså lager 2) som lägger data i s.k. *frames* för att skickas över en länk. Protokollet används för att upprätthålla en direkt koppling mellan två noder i ett nätverk. PPP har kapacitet att skicka data över flera medium så som fiber, seriell och telefonlina.

En vidareutveckling av PPP återfinns i PPPoE - PPP over ethernet. PPPoE kombinerar mångsidigheten med PPP och simpliceten av ethernet.

En av fördelarna med PPP är att det är ett öppet protokoll som kan testa länk-kvalitet och stänga ner länkar baserat på testerna.

Komponenter

- En metod för att enkapsulera datagram - PPP tar s.k. *high-level messages* och kapsulerar dessa till *phsyical layer messages*

- En *extensible Link Control Protocol (LCP)* för att upprätta, konfigurera och testa uppkopplingen
- Ett *Network Control Protocol (NCP)* för att upprätta och konfigurera *network layer protocols* som kan köras samtidigt

Etablering av en PPP-länk

1. Establishment - varje PPP skickar ett Link Control Protocol för att konfigurera och testa länken
2. Authentication - använder PAP eller CHAP
3. Network Layer Protocol Phase - varje PPP skickar ut ett Network Control Protocol för att välja och konfigurera ett eller flera protokoll i nätverkslagret som ska enkapsulera och skicka data över länken

VPN

Virtual Private Network (VPN) är en teknik där man skapar en tunnel mellan två noder i ett nätverk. Detta kombineras med andra protokoll för att kryptera och säkra datan.

Fördelar med VPN inkluderar förstärk säkerhet, anonymitet, remote control, delning av filer och möjlighet att kringå filter.

Typer av VPN

- Remote Access VPN - används av t.ex. anställda vid ett företag som kan kålla upp sig mot företagets VPN hemifrån för att jobba
- Point-to-Point VPN - används av stora företag med kontor på olika geografiska platser för att koppla upp sig på samma nätverk

IPSec

IPSec skapar en gräns mellan skyddade och oskyddade delar av nätverket. Protokollet arbetar på nätverkslagret. Det består av protokoll som erbjuder tjänster så som

- Reliability - krypterar data som endast mottagaren kan förstå
- Integrity - garanterar att datan kommer fram oförändrad
- Authenticity - data signeras så att ursprunget kan verifieras
- Replay protection - datagram bearbetas *en enda* gång.

IPSec använder AES eller Tripple DES för att kryptera data.

Det finns två lägen av IPSec - transport och tunnelläge. Transportläget används för att skicka IP-paket som vanligt, fast krypterat. Tunnelläget används för att sammanlänka två nätverk över en säker förbindelse. All data som skickas mellan nätverken passerar då "portaler" som sköter kryptering och dekryptering.

Spanning Tree Protocol (STP)

Protokollet använder sig av Dijkstras algoritm. Det blockerar redundanta routes i nätverket för att se till att det enbart finns en logisk väg mellan alla punkter. På så vis kan man ha stöd för flera routes till en punkt, men ändå förebygga loopar i nätverket.

Algoritmen består av följande delar:

- Root bridge - används som referenspunkt i nätverket. Denna punkt används för att hitta de bästa vägarna inom nätverket. Switchen med lägst bridge ID blir utsedd till root bridge
- Root port - portar närmast root bridge
- Designated port - alla portar som vidarebefodrar information, men som inte är root bridges
- Alternate port - konfigurerade för att blockera trafik
- Bridge ID - prioritet + extended system ID + MAC. Längre bridge IDn prioriteras

BPDU - Bridge Protocol Data Unit - är meddelanden som utbyts mellan switchar i ett extended LAN som använder STP. BPDU används för att hitta loopar. Om en loop hittas tas den bort genom att BPDU stänger av berörda interfaces och placerar redundanta portar i backup eller i s.k. *blocked state*

PVST+

Rapid Per VLAN Spanning Tree är en uppdaterad version av STP. Operationer som är nya eller uppdaterade är:

- Blocking - tar mot men skickar inte vidare frames
- Listening - lyssnar efter vägar och skickar ut / tar mot s.k. *BPDU frames*
- Forward - tar mot och skickar vidare data
- Disabled - gör ingenting
- Portfast - går från blocking till forward direkt och är bra för portar med hostar på
- BPDU-guard - en portvakt, tillåter inte BPDU-frames. Om något skickas så stängs porten ned

SMNP

Simple Network Management Protocol (SMNP) är ett applikationslager-protokoll som består av en SMNP Manager och flera SMNP Agents. SMNP Manager ansvarar för att kommunicera med SMNP Agents.

SMNP Agent är enheterna på nätverket som behöver någon form av övervakning / management, så som routrar och switchar. All information sparas i Management Information Bases (MIBs).

I SMNP finns följande meddelandetyper:

- Get Request - manager till agent - hämtar värdet på en eller flera variabler
- Set Request - manager till agent - ändrar värdet på en eller flera variabler
- Trap - agent - manager - en asynkron notifikation. Gör så att agenten kan avisera managern om en förändring som är på väg genom frivilliga SMNP-paket

MAC Databases

Problem inkluderar instabilitet - när en switch får frames med samma MAC-adress från olika portar leder detta till inkonsekventa tabeller. Data störs av att switchen måste hantera och ändra den instabila tabellen.

Broadcast storms - utan någon slags lösning så uppstår loopar i redundanta nätverk och då finns det en risk att frames hamnar i oändliga loopar om de inte har någon TTL.

Multiple frame transmission - hosts får flera identiska meddelanden, något som kan påverka protokoll och leda till fel i data.

EIGRP

EIGRP är ett routingprotokoll som använder Diffusing Update Algorithm (DUAL) och arbetar på lager 3. EIGRP använder fem parametrar för att beräkna kostanden av en väg mellan två noder - *bandwidth*, *delay*, *load*, *reliability* och *MTU*.

Grannskap (adjacencies) skapas genom att routers skickar ut "hello"-paket till de direkt anslutna grannarna för att se om de stöder EIGRP. Grannarna svarar i så fall med *update* och *hello*.

Fördelar med EIGRP inkluderar:

- Ett garanterat loop-fritt nätverk
- Snabb konvergens
- RTP används för att skicka ut pålitliga och opålitliga paket
- Skapar och upprätthåller aktiva grannskap genom partiella uppdateringar - uppdateringar skickas bara när det behövs

DUAL

Använder sig av distansvektorn k1 till k5 (se nedan) för att bestämma den bästa vägen genom ett nätverk. Om algoritmen hittar flera vägar så använder den vägen som har den lägsta *feasible distance* (FS) och använder den som *successor*. Routen med näst bäst väg till destinationen blir feasible successor om den uppfyller vissa krav.

Om en route går ner byts den till FS. Om det inte finns någon väg så fortsätter routern i active state och frågar sina grannar om det finns en annan väg till destinationen.

- k1 - bandwidth
- k2 - load
- k3 - delay
- k4 - reliability
- 5 - reliability

Paket

1. Hello - skickas för att hitta och upprätta grannskap. Skickas som opålitlig uni- eller multicast
2. Update - sprider routing-information pålitligt
3. Acknowledgement-paket - bekräftar mottagandet av ett pålitligt skickat paket
4. Query-paket - söker efter ett nätverk. Skickas pålitligt
5. Reply-paket - svar på en query - skickas pålitligt

Route Summarization

EIGRP Route Summarization tillåter en router att gruppera ihop nätverk och skicka advertisement i en stor grupp. Det innebär att EIGRP automatiskt känner igen subnät etc.

Att summera rutter minskar storleken på routing-uppdateringar. Detta tillåter snabbt växande nätverk. Det reducerar även bandbredden som används och snabbar på queries.