S-38.200 Teletekniikan yksilöllinen opintojakso

Internetreititys

Referaatti Christian Huiteman kirjasta

Routing in the Internet

12.6.1997

Työn ohjaaja Professori Raimo Kantola

Ilkka Peräläinen 47843B

ilkka@luuri.hut.fi

Sisällysluettelo

Lyhenne- ja termiluettelo

AS	Autonomous system, Internetin hallinnollisesti yhtenäinen osa-alue
ARP	Address resolution protocol, muuntaa IP-osoitteen verkko-osoitteeksi
AUP	Acceptable use policy, sallitun käytön politiikka Internetin osa-alueilla
BGP	Border gateway protocol, IP:n alueiden välinen uudempi reititysprotokolla
BOOTP	Bootstrap protocol, käytetään levyttömien tietokoneiden käynnistyksessä
CBQ	Class based queuing, sovellusluokkiin perustuva vuorottelumenetelmä
CBT	Core based trees, ryhmäkohtaisen virityspuun monilähetysreititysmenetelmä
CIDR	Classless inter domain routing, IP:n alueiden välinen uusin reititysprotokolla
CLNP	Connectionless network protocol, OSI:n verkkoprotokolla
DHCP	Dynamic host configuration protocol, dynaaminen autokonfigurointiprotokolla
DNS	Domain name service, Internetin alueosoitteiden tietokanta
DUAL	Diffusing update algorithm, poistaa äkilliset silmukat reititysprotokollista
DVMRP	Distance vector multicast routing protocol, Internetin paljolti RIP:iin perustuva yhdyskäytävien monilähetysprotokolla
EGP	Exterior gateway protocol, IP:n alueiden välinen vanhin reititysprotokolla
EIGRP	Extended Internet gateway routing protocol, Ciscon laajennettu reititysprotokolla
EV	Etäisyysvektori
FIB	Forward information base, reitittimen reitin valinnassa käyttämä tietokanta
GGP	Gateway-to-gateway protocol, Internetin alkuaikojen EV-reititysprotokolla
ICMP	Internet control message protocol, IP:n ohjausviestejä välittävä protokolla
IDPR	Inter domain policy routing, IETF:n alueiden välinen valintareititysprotokolla
IDRP	Inter domain routing protocol, OSI:n alueiden välinen reititysprotokolla, ‘BGP-5’
IETF	Internet engineering task force, Internetin standardisointijärjestö
IGMP	Internet group membership protocol, ryhmäjäsenyyden selvittävä protokolla
IGRP	Internet gateway routing protocol, Ciscon oma sisäinen reititysprotokolla
IHL	Internet header length, Internetotsakkeen pituus

IP	Internet protocol, Internetin verkkokerrosprotokolla
IPMC96	Internet protocol multicast over ATM
IS-IS	Intra-domain intermediate system to intermediate system routing protocol, OSI
L2	OSI-mallin kakkos- eli siirtoyhteyskerros
L3	OSI-mallin kolmos- eli verkkokerros
MBONE	Multicast backbone, IP:n kokeellinen monilähetysprotokolla
MOSPF	Multicast OSPF, OSPF:n monilähetysversio
MPOA	Multiprotocol over ATM, yhdistää virtuaalilähiverkkoja ATM:n yli
MTU	Media transmission unit, siirtotiekohtainen datapaketin pituus
NSSA	Not so stubby area, OSPF:n osittain tynkä reititysalue
NTP	Network time protocol, ICMP:stä kehitetty aikaleimaprotokolla
OSPF	Open shortest path first, TCP/IP:n alueen sisäisen lyhimmän/parhaan reitin valitseva reititysprotokolla
PAR	PNNI Augmented routing
PIM	Protocol independent multicast, protokollasta riippumaton monilähetys
Ping	Yleinen Internetin CMIP:n kaiutusta käyttävä etäyhteyden testausohjelma
Pip	Eräs IP:n parannusehdotus
PNNI	Private network-to-network interface, ATM verkon kytkinten välinen reititysprotokolla
QoS	Quolity of service, televerkon palvelutaso, myös GoS Grade of service
RARP	Reverse address resolution protocol, muuntaa verkko-osoitteen IP-osoitteeksi
RFC	Request for comments, IETF:n numeroitu pysyvä standardiehdotus
RIB	Routing information base, reititystietokanta
RIP	Routing information protocol, TCP/IP:n reititysprotokolla
RPF	Reverse path forwarding, monilähetysreitysprotokolla
RSVP	Resource reservation protocol, Internetin yhteydetön resurssien varausprotokolla
SDPR	Source demand routing protocol, IETF:n ulkoinen erikoisreititysprotokolla
SIP	Simple IP, IP:n vanhentuneista piirteistä riisuttu uusi yksinkertainen versio

SIPP	Simple IP Plus, Pip:stä ja SIP:stä yhdistetty versio, Ipv6:n pohjaversio
SNMP	Simple network management protocol, yksinkertainen verkonhallintaprotokolla
SPF	Shortest path first, Dijkstran kehittämä lyhimmän polun löytävä reititysalgoritmi
STII	Stream protocol version 2, Internetin yhteydellinen resurssien varausprotokolla
TCP	Transport control protocol, Internetin luotettava yhteydellinen siirtoprotokolla
TOS	Type of service, IP:n otsaketieto, reitinvalintaperuste
TTL	Time-to-live, IP:n datapakettien elinkaarilaskuri, jokainen solmu vähentää arvoa
UDP	User datagram protocol, Interntin yksinkertainen siirtoprotokolla
X.25	Virtuaalikanavointia käyttävä etappi-etapilta-protokolla
X.75	X.25 verkkoja yhdistävä protokolla
soft state	verkon tilainformaatio, joka parantaa suorituskykyä, muttei ole välttämätöntä oikean toiminnan kannalta

1. Johdanto

90-luvun suuriin yllätyksiin kuuluu varmasti Internetin käytön huima kasvu. Alkujaan Yhdysvalloissa kehitettynä valtaosa siitä on jo nykyään Yhdysvaltojen ulkopuolella.

Tässä verkkojen verkossa voidaan erottaa kolme hierarkiatasoa: yrityskohtainen, alueellinen ja kauttakulku. Tämän päivän yritysverkotkin koostuvat usein useista aliverkoista: lähiverkot tai lähiverkkosegmentit on liitetty keskittimien, siltojen tai reitittimien avulla toisiinsa joskus yrityskohtaisen runkoverkon esimerkiksi FDDI:n avulla.

Yhteyden ulkomaailmaan yrityskohtaiset verkot saavat alueellisten teleoperaattorien liityntäverkkojen kautta. Vapautuva telekilpailu suo yrityksille mahdollisuuden valita usean operaattorin joukosta sopivin liityntäverkko. Maailmanlaajuisen yhteyden tarjoaa useimmiten kauttakulkuoperaattori, kuten eurooppalaisten teleyhtiöiden yhteisesti hoitama EBONE. Kauttakulkutaso ei ole välttämätön, kun alueelliset operaattorit ovat tarpeeksi isoja.

Internetin jatkaessa maailmalaajuiseksi kasvuaan, sen osaverkkojen liittäminen toisiinsa on tullut yhä tärkeämmäksi. Tämä on korostanut reitityksen merkitystä ja tätä aihepiiriä Christian Huitema valottaa tuoreessa teoksessaan: ‘Inrternetreititys’. Liikenteen yhä lisääntyvä kasvu puolestaan pakottaa tehostamaan verkon liikenteen välityskykyä ja tämäkin korostaa osaltaan reitityksen merkitystä.

2. Arkkitehtuuri ja protokollat

2.1. Internet-arkkitehtuuri

Internetin nykyisen rakenteen ymmärtämiseksi on tärkeää tuntea sen syntyhistoria. Sen kehitystä on osuvasti verrattu kaupungin kasvuun. Kaupunkeja ei yleensä suunnitella etu-käteen. Ne kehittyvät pitkän ajan kuluessa ja niiden kaavoja muutetaan aika ajoin. Tällöinkin vanhan rakenteen peruspiirteet yleensä säilytetään ja uudet lisäykset sovitetaan huolella vanhaan arkkitehtuuriin.

2.1.1. Päästä-päähän-periaate

Kun Internetiä alettiin suunnitella parikymmentä vuotta sitten, lyötiin lukkoon sen tietyt peruslinjat: ‘päästä-päähän-periaate ‘, ‘IP-yli-kaiken’ ja ‘yhdistäminen-on-pääasia’. ‘Päästä-päähän-periaatteen’ mukaan loppukäyttäjille jätetään päätösvalta, joka näin ollen hajautetaan verkon ulkopuolelle. Verkko siis olkoon yksinkertainen: on turha kahdentaa älykkyyttä verkkoon ja sen isäntäkoneisiin. Jokainen datapaketti myös kulkee itsenäisesti verkon läpi ilman sinänsä tehokasta virtuaalikanavaa, joka voisi etappi-etapilta ohjauksellaan joustavasti säädellä liikennevirtoja. Myös uudelleenlähetykset rasittavat vain niitä linkkejä, joissa katkos on sattunut.

Verkon luotettavuus on hyvin keskeinen verkon ominaisuus ja se vaikuttaa myös sen arkkitehtuuriin. Raskaan puoleinen X.25-virtuaalikanavatekniikka hyvine virheenkorjaustoimintoineen oli hyvinkin perusteltu valinta, kun verkot olivat epäluotettavampia kuin nyt. Nykypäivän verkot ovat pääosin jo hyvin luotettavia ja uudelleenlähetykset sen verran harvinaisia, että päästä-päähänkin hoidettuina niiden aiheuttama kuormitus on marginaalinen. Riisutussa Internetissä virheettömän (tai ainakin vähävirheisen) yhteyden takaa TCP, joka varmistus- ja uudelleenlähetystoimintoineen täydentää hyvin Internet-protokollaa.

Pakettipohjainen verkko, kuten Internet, edellyttää parhaan mahdollisen reitin laskemista joka paketille. Koska aktiivien reittien määrä tietyllä aikavälillä on kuitenkin rajattu, voidaan reittitiedot tallettaa nopeaan välimuistiin ja näin nopeuttaa reititystä. Virtuaalikanavapohjaisten X.25-verkkojen ja näitä yhdistävän X.75-protokollan on sen sijaan muistettava suuri joukko kanavaan liittyviä verkon ja solmujen tiloja.

2.1.2. IP kaiken yllä

Internetiä luotaessa päätettiin, että verkko vain reitittää ja käyttäjät vastaavat ohjauksesta.

Erilaisia verkkoja voidaan yhdistää kahdella tavalla, joko muuntamalla protokolla toiseksi tai kapseloimalla. Vaikka muuntamisella voidaan välttää kytkettävien verkkojen ohjelmistojen muutokset, sen haittana on, ettei täyttä vastaavuutta eri protokollille yleensä voida saavuttaa. Siksi Internet-protokolla valittiin kapseloivaksi. Se hoitaa vain tiedon siirron hyvinkin erilaisia palveluja tarjoavien verkkojen välillä. Saatuaan tietopaketin, aliverkko purkaa sen omasta kehyksestään, tutkii IP-osoitteen ja tarvittaessa lähettää sen toiseen verkkoon.

Päästä-päähän periaatteesta seuraava yksinkertaisuus tekee uusien teknologioiden käyttöön oton Internetissä hyvin helpoksi: on vain päätettävä pakettien siirtotapa, osoitemuunnos ja tapa, miten uuden verkon kytkentäominaisuudet hyödynnetään.

Kapseloinnin edellytyksenä on IP-osoitteiden yksikäsitteisyys. Tästä puolestaan seuraa kohtalainen topologiariippumattomuus: kun verkosta poistetaan yhteyksiä tai niitä lisätään, osoitteita ei tarvitse muuttaa, verkko vain sopeutuu muuntamalla reititystä. Kirjan pääteema on, miten se hoidetaan. Yksikäsitteisestä osoiteavaruudesta seuraa myös, että lähettäjä saadaan selville, mikä varsinkin tietoturvamielessä on tärkeää.

Internetiä luotaessa oltiin varsin suvaitsevaisia. Hyväksyttiin moniprotokolla-periaate: IP ei olisi ainoa verkkoprotokolla ja rinnakkaisia protokollia onkin kehitelty esimerkkinä mm. ISO:n CLNP Connection-less network protocol. Rinnakkaisten protokollien hallinta maailmanlaajuisessa verkossa olisi kuitenkin muodostunut työlääksi. Verkkoinsinöörit olisivat joutuneet hallitsemaan useita protokollia kaikkine erityispiirteineen ja reitittimet olisi pitänyt varustaa kunkin protokollan ohjelmistolla. Käytännössä IP onkin jäänyt ainoaksi todelliseksi vaihtoehdoksi. Yrityskohtaisissa aliverkoissa moniprotokollaisuus on tietenkin mahdollista: etuja ja haittoja punnitsemalla itse hallitussa verkossa voidaan hyvin ottaa käyttöön useampiakin protokollia. Olennaista on, että kaikkia yhdistävä Internet on yksinkertainen, eikä pakota verkkopalveluja tarjoavia yrityksiä monen protokollan käyttöön.

2.1.3. Yhteydellisyys palkitsee itsensä

Internetin erittäin nopea kasvu on yllättänyt kaikki asiantuntijat. Verkkoon kytkettyjen aliverkkojen ja tietokoneiden määrä kaksinkertaistuu vuosittain. Yritysten runkoverkkojen protokollatarjonta on nykyään runsas ja paikallisverkkoihin sopivia ohjelmistoja löytyy monen valmistajan myyntilistalta. ‘Verkottumisen’ syyt ovat kuitenkin laaja-alaisempia. Käyttäjien kasvavan kiinnostuksen taustalla on yhtenä merkittävimmistä sovelluksista sähköposti E-mail. Sen avulla maailman eri kolkilla asuvat ihmiset tavoittavat toisensa hyvin helposti. Faksiin verrattuna E-mail on yksilöllinen, viestit saapuvat suoraan käyttäjän näyttöpäätteelle tai jos vastaanottaja ei ole paikalla, viestit ohjautuvat henkilökohtaiseen postilaatikkoon. Sanomat ovat digitaalisuutensa johdosta myös helposti muokattavissa. Muita

tärkeitä Internetin käyttöalueita ovat mm. dokumenttien haut, tietovarastojen selailut ja etäyhteydet.

Yhteydellisyyden nopea kasvu on itseään ruokkiva prosessi. Informaation tarjoajat ovat suuren kysynnän havaittuaan, kehittäneet yhä monipuolisempia hakupalveluja ja tietovarastoja. Ohjelmistotuottajat ovat luoneet World wide web:in ja siihen sopivia selaimia kuten Netscapen. Verkko-operaattorit ovat laajentaneet ja tehostaneet verkkojaan. Voimakkaasti kasvavat markkinat ovat kiihdyke ja mitä paremmat yhteydet operaattori pystyy tarjoamaan, sitä vahvempi sen markkina-asema on.

Internetin alkuaikojen ilmaisliikenne on mennyttä varsinkin kun liike-elämä on ottamassa verkon kaupalliseksi mediakseen. Internetin käyttö muuttuu maksulliseksi, kustannusten jako operaattorien välillä on tuttua jo puhelinliikenteen piiristä.

Internetiä käyttävien sovellusten määrä on myös voimakkaassa kasvussa. Yhteensopivuuden takaamiseksi mahdollisimman laajalle sovellusjoukolle on päädytty käytännölliseen ratkaisuun: ‘Ole liberaali vastaanottamaasi informaatioon nähden ja konservatiivinen lähettämääsi nähden’ on ohje ohjelmistojen valmistajille. Ehkä yllättävää on, että OSI:n periaate tiukkojen standardien luomisesta tietoliikenteeseen on kääntynyt itseään vastaan. Valmistajat ovat alkaneet kilpailla keskenään oikeaoppisuudessa ja tällöin yhteensopivuus on joutunut vaakalaudalle. Internet-yhteisössä ‘tiukkapipot’ ja häiriköt pidetään ruodussa yleisen mielipiteen avulla. Kerran hankittu huono maine kiirii kauas ja nopeasti.

2.2. Internet-protokolla

2.2.1. Internet-osoite

Joskin Internetin perusperiaatteet valittiin kaukonäköisesti, niin samaa ei voida sanoa osoitteistuksesta. Nykyistä maailman verkon levinneisyyttä ei kukaan villeimmissäkään unelmissa osannut odottaa. Alunperin osoiteavaruus valittiin 32-bittiseksi ja kaksitasoiseksi: verkko ja isäntäkone. Neljän luokan avulla määriteltiin, mikä osa osoitteesta kuvaa verkkoa ja mikä isäntäkonetta. Vuonna -84 oli lisättävä aliverkko välitasoksi. Peitteen avulla aliverkon osoite voitiin määritellä joustavasti yhtenäisenä alueena keskeltä 32-bitin osoiteavaruutta. Kolme tasoakaan ei pitkään riittänyt. Usean C-luokan IP-verkko-osoitenumeron antaminen yhdelle organisaatiolle, kun B-luokan osoitteet loppuivat, oli yritys kiertää osoitteiden loppuminen. Tämä kuitenkin rasitti reititystaulokoita. Myöhemmin esiteltävä Classless-inter-domain-routing CIDR oli lääke tähän ongelmaan.

Itse asiassa IP-osoite ei liity suoraan isäntäkoneeseen vaan liittymään (interface), joka voi kylläkin liittyä vain yhteen laitteeseen. Liittymäosoitteet tekevät esim. täsmäreitityksen mahdolliseksi. Tämä tarjoaa mahdollisuuden saavuttaa isäntäkone tiettyä haluttua reittiä pitkin. Lisäksi alueellisesti hajallaan, mutta organisatorisesti yhteen kuuluvat laitteet voidaan koota saman IP-liittymän alle.

2.2.2. Protokolla

Internet protokollan otsake sisältää lähtö- ja kohdeosoitteen lisäksi lukuisia muita reitityksen kannalta oleellisia parametreja, kuten

- version, nykyinen versio on 4, tulossa ovat versiot 6 - 8
- otsakkeen pituus, IHL
- palvelutyyppi, joka kertoo prioriteetin ja toivotun reititystavan
- elinaika TTL valvoo, ettei paketti jää sotkemaan liikennettä sen jälkeen, kun sen aika on ohi eli sen olisi pitänyt ehtiä perille
- tarkistussumma lasketaan uudelleen ennen jokaista lähetystä

Palvelutyypin reititystapakentällä on viisi eri arvoa, jotka ilmaisevat mitä reitin ominaisuutta reititettäessä on syytä painottaa: ei arvoa eli oletusreitin mukaan, lyhyyttä (D), suurinta läpimenokapasiteettia (T), luotettavuutta (R) tai halpuutta (C). Uusimmat reititysprotokollat kuten OSPF ja BGP pystyvät valitseman reitin minkä tahansa em. ominaisuuden perusteella. Jottei prioriteettia käytettäisi väärin eli asetettaisi liian korkeaksi on ehdotettu, että siihen luotettaisiin vain aliverkossa ja prioriteetin jakelu olisi verkon hoitajan vastuulla.

Internet on hyvin erilaisten verkkojen yhteenliittymä. Osoitteistus, siirto- ja liityntäjärjestelmät vaihtelevat eri aliverkoissa. Datapakettien pituutta joudutaankin usein muuttamaan siirryttäessä verkosta toiseen esimerkiksi FDDI-renkaasta Ethernet-lähiverkkoon. Tällöin 4000 merkin mittainen paketti on pilkottava 1500 mittaisiin osiin. IP:n otsakkeessa on kentät tämän siirron hallintaan. Jos alkuperäiset paketit joudutaan pilkkomaan moneen osaan, niiden kokoamisessa on vaikeutensa. Kehykset, joita ei ole vielä saatu kootuksi täyttävät puskureita kun TCP:n TTL-kentän suositusaika-arvokin on hyvin pitkä. Monelta ongelmalta vältytään, kun TCP selvittää polun paketin pituuden (path MTU) koelähetyksillä ja lopulta valitsee paketin pituudeksi saman kuin polunvarren lyhintä paketin pituutta käyttävä siirtotie.

Aikoinaan IP käytti optioita erialaisiin sovituksiin, mutta nyttemmin niistä on lähes kokonaan luovuttu. Tästä on seurannut Internet-otsakkeen muuttuminen vakiopituiseksi, jolloin sen viisi 32-bitin mittaista sanaa voidaan ladata viiteen rekisteriin ja käsittely nopeutuu sel-

västi. Kun vielä yleisimmät reitit talletetaan nykyään reitittimen välimuistiin aletaan reitityksessä lähestyä hurjaa Gigabitin nopeutta. Aiemmin optioilla hoidettu lähdereititys on korvattu kapseloinnilla. Jos A lähettää paketin B:lle C:n kautta, niin koteloimalla A->B viesti A->C viestin sisään nopeutetaan reititystä huomattavasti, sillä vasta solmu C joutuu tarkemmin käsittelemään ‘kahdesti kädityn’ paketin. Välisolmuille kyseessä on yksinkertainen IP-paketti. Jos reititystä ei ollenkaan optimoida, joudutaan jokaisessa reitittimessä suorittamaan satojakin ohjelmakoodin käskyjä, kun saapunut paketti avataan ja tutkitaan edelleen lähetystä varten.

2.2.3. ICMP

IP on yksinkertainen ja suoraviivainen: käytössä on vain yksi pakettityyppi ja verkko vain koettaa tehdä parhaansa toimittaakseen paketin määränpäähänsä. Ilman virhetilanteiden erittelyä toiminta olisi kuitenkin hyvin vajavaista. Tämän hallintaviestien välityksen hoitaa Internetissä hallintaprotokolla ICMP, joka on IP:n elimellinen osa. Valtaosa viesteistä on perusteluja IP-paketin hylkäämiselle reitittimissä.. ICMP ei suoranaisesti tee IP:n paketin välitystä luotettavammaksi vaan se kertoo verkon ongelmien syyt.

ICMP:hen liittyy myös yhteyden testaamiseen luotu kaiutustoiminto, jota hyvin suosittu ‘ping’ ohjelma käyttää. Ping testaa etäyhteyttä lähettämällä säännöllisin väliajoin halutulle reititti-melle tai isäntäkoneelle kaiutuksia. Lähetyksen ja vastauksen aikaero kertoo väylän laadun.

ICMP:n otsake koostuu virhetyypistä, sen täsmentävästä koodista ja tarkistussummasta. Jotta lähettäjä voisi varmasti tunnistaa paketin, sanomassa on mukana ongelman aiheuttaneen IP-paketin koko otsake ja sisällön kahdeksan ensimmäistä oktettia.

‘Traceroute’ on toinen hyvin yleinen IP:tä ja ICMP:tä käyttävä tarkistusohjelma. Se lähettää kohteelleen tavallisia IP-paketteja, joiden elinaikalaskureita se kasvattaa joka lähetyksen jälkeen yhdellä. Kun esimerkiksi TTL:n arvolla viisi varustettu paketti saavuttaa polun viidennen reitittimen, tämä vähentää TTL:n yhdestä nollaan ja palauttaa lähettäjälle viestin ilmaisten näin olemassaolonsa. Tällä tavoin saadaan koko reitti selville tai löydetään katkokohta. Toiminnon liittämistä varsinaiseen IP:hen on myös ehdotettu.

ICMP:n aikaleimaviestit ovat osoittautuneet varsin tarpeellisiksi. Aikaleimojen avulla verkon kellot pystytään synkronisoimaan. Tämä taas on tarpeellista, jotta eri lähteiden virhelokeja voidaan verrata ja saadaan esimerkiksi tietää, mikä solmu lopetti toimintansa ensimmäisenä. Kellojen synkronisointi on monimutkainen toimitus. Ensinnäkin kelloja voi haitata vaihe-ero tai käyntinopeusero. Satunnaiset erot kuten tilapäiset verkon aiheuttamat viiveet on elimi-

noitava tilastollisella käsittelyllä. Aikaleimakäsittely on johtanut oman protokollan NTP:n syntyyn.

2.2.4. IP-pakettien lähetys

IP tuntee kahdenlaisia olioita: reitittimiä ja isäntäkoneita. Reititinten tehtävänä on valita reitit ja vastata yhteyksistä, mutta isäntäkonekin osallistuu reitittämiseen valitessaan lähettämänsä paketin ensimmäisen etapin. Internetin alkuaikoina isäntäkoneet ylläpitivät omia reititystaulujaan, mutta nykyisen suuruisilla tauluilla tämä olisi hyvin hankalaa. Niinpä isäntäkoneelle riittää ensimmäisen reitittimen löytäminen.

Isäntäkoneen on ensimmäiseksi selvitettävä aliverkkopeitettä käyttämällä kuuluuko vastaanottaja samaan verkkoon. Jos kohde kuuluu samaan aliverkkoon, on seuraavaksi etsittävä ARP-protokollalla IP-osoitetta vastaava verkko- eli mediaosoite. Nämä osoitteet talletetaan välimuistiin, jottei joka paketille tarvitse erikseen selvittää verkko-osoitetta. ARP on nykyään hyvin monipuolinen. Se pystyy vaivatta selvittämään mm. erilaisten LAN:ien osoitteet. Päästä-päähän siirtotapaa käyttävien verkkojen kuten X.25, ISDN ja Frame relay tulkitaan käyttävän kvasipysyviä yhteyksiä. ATM:lle otettaneen käyttöön keskitetty ARP-palvelin. ARP:n vastausviestejä ei aina lähetä kohde itse vaan usein välikäsireititin (proxy), joka tuntee kohteen osoitteen.

Kun kohde ei ole paikallisessa verkossa on ensimmäiseksi löydettävä lähinnä kohdetta oleva reititin. Tämä hoidetaan dynaamisesti siten, että reitittimet lähettävät muutaman minuutin välein ICMP-levitysviestejä, joiden perusteella isäntäkone valitsee aluksi omaan aliverkkoonsa kuuluvan oletusreitittimen. Levitysviesteillä reititin voi myös ilmoittaa, onko se ylipäätään halukas toimimaan oletusreitittimenä. Verkonvalvoja voi etusijakoodit asettamalla jakaa liikennettä reitittimille haluamallaan tavalla. Reitittimellä voi olla useita verkko-osoitteita esimerkiksi jokaiselle liittymälle (interface) oma.

Oletusreititin ei luonnollisesti ole paras etappi kaikkiin suuntiin. Niinpä oletusreititin voi lähettää uudelleensuuntaus ICMP-viestin lähettävälle isäntäkoneelle, jos se havaitsee, että jokin toinen reititin tarjoaisi suoremman polun kohteeseen. Viestin saatuaan isäntäkoneet tallettavat uudelleensuuntaustiedon paikalliseen reititystauluun. ICMP-viestin palvelutyypin perusteella isäntäkoneet voivat valita eri reittejä eri palveluluokille (QoS).

Eräs tärkeä sudenkuoppa, jota reitityksessä on varottava on niin sanotut ‘mustat aukot’. Näitä ovat reitittimet, jotka eivät jostain syystä ole toiminnassa. Isäntäkoneiden onkin syytä tasaisin väliajoin varmistaa lähireitittimen toimivuus jonkinlaisen palautteen avulla. TCP:n jatkuvat

hyväksymisviestit tarjoavat tähän hyvän mahdollisuuden. Osa paketeista voidaan myös hajauttaa toisille reitittimille tai isäntäkone voi varmistaa reitittimen toimivuuden ‘pingillä’.

Jos isäntäkoneella ei ole omaa levyasemaa tai se ei muuten tunne omaa osoitettaan esimerkiksi käynnistyessään, se voi käyttää käänteistä ARP:tä eli RARP:ia, joka selvittää laiteosoitetta vastaan IP-osoitteen. UDP:n päällä toimiva BOOTP pystyy myös tähän ja se tarjoaa tämän lisäksi isäntäkoneelle mahdollisuuden valita verkosta ladattava käynnistystiedosto. Levyttömät työasemat eivät viime aikoina ole olleet muodissa, mutta uudet verkkotietokoneet tekevät tämän tekniikan jälleen ajankohtaiseksi. Autokonfiguroinnin tarvetta RARP ja BOOTP eivät täytä, askel siihen suuntaan on uusi Dynaaminen isäntäkoneen konfigurointiprotokolla DHCP. Tietoturvaan on syytä myös kiinnittää erityistä huomiota verkkokäynnistystä käytettäessä.

2.2.5. IP:n yhteistyöprotokollat

IP:n päällä toimiva TCP paikkaa pari IP:n puutetta. TCP varmistaa pakettien perille tulon luomalla luotettavan päästä-päähän yhteyden kahden eri sovelluksen välille. Lisäksi se varmistaa pakettien oikean tulojärjestyksen. IP:hän voi reitittää paketit eri väyliä pitkin, jolloin ‘ensimmäiset voivat tulla viimeisiksi’. TCP:n uusia piirteitä on hitaan alun-algoritmi, joka aloittaa lähetykset varmuuden vuoksi alhaisella nopeudella, jota mahdollisuuksien mukaan kasvatetaan. Vastaavasti estotilanteissa lähetysnopeutta voidaan nopeasti laskea.

Joillekin sovelluksille, kuten hyvin lyhyitä viestejä lähettävälle DNS:lle, TCP:n varmistukset ovat liian raskaita. Verkonhallintaprotokolla SNMP puolestaan haluaa itse ohjata toimintaansa ja korjata itse siirtovirheensä. Näitä protokollia varten on luotu pelkistetty ja varmistamaton, mutta nopea UDP.

Numerosarjoista koostuvat IP-osoitteet ovat täysin epähavainnollisia ja ne voivat teknisistä syistä muuttua käyttäjän pysyessä samana. Tästä syystä on reitityksessä käytettävien IP-osoitteiden ja symbolisten ja havainnollisten kirjainlyhenteistä koostuvien aluenimien (domain names) muuntamiseksi toisikseen luotu aluenimipalvelu DNS, joka on valtava hajautettu tietokanta. Aluenimi on hierarkinen. Sen ylin taso on maa (kansainvälisillä suuryrityksillä tai organisaatioilla käyttäjäluokka esim. org tai com), seuraavana organisaatio mahdollisine aliorganisaatiotasoineen ja viimeisenä käyttäjän nimi tai sen lyhenne. Aluenimi peittää verkon teknisen ratkaisun käyttäjiltä.

SNMP:n välityksellä verkon hoitajat voivat hallita verkon erilaisia laitteita. Hallintatieto on talletettu MIB-tietokantoihin. SNMP noudattaa asiakas-palvelin arkkitehtuuria. Yksinkertaisuudella pyrittiin siihen, että protokolla voitaisiin toteuttaa halvoissakin järjestelmissä, joilla

on vaatimattomat levytilat ja tiedonkäsittelykapasiteetti. Tästä syystä kaikkien Internet-toteutusten voidaan edellyttää tukevan SNMP:tä. Uudessa versio 2:ssa on huomiota kiinnitetty erityisesti tietoturvaan.

3. Sisäiset reititysprotokollat

3.1. RIP:n yksinkertaisuus

3.1.1. Etäisyysvektoriprotokollat

Etäisyysvektoriprotokollat, kuten RIP, perustuvat hajautettuun lyhimmän polun algoritmin laskemiseen. Verkkotiedon hallintaa tarkasteltaessa voidaan lähtökohdaksi ottaa niin sanottu ‘kylmä lähtö’, jolloin kaikki solmut käynnistetään saman aikaisesti. Solmut tietävät aluksi vain oman osoitteensa ja linkkinsä ulkomaailmaan, mutteivät esimerkiksi naapuriensa osoitteita. Niiden ainoa etäisyysvektorin komponentti kertoo niiden etäisyyden itseensä, ja sen arvo = 0. Seuraavaksi solmut lähettävät tämän tiedon naapureilleen kaikkia linkkejään pitkin. Naapurit lisäävät saamansa vektorikomponentin arvoa yhdellä ja tallettavat reititystauluunsa tiedon lähettäjästä, päivitetystä etäisyydestä ja tiedon välittäneestä linkistä. Ne lisäävät kaksi ensin mainittua tietoa myös omaan etäisyysvektoriinsa, jonka ne lähettävät edelleen naapureilleen. Vastaanotettua vektoritietoa verrataan aina jo kertyneeseen ja tietyn solmun etäisyys päivitetään vain, jos se on olemassaolevaa lukemaa pienempi eli on löytynyt lyhyempi reitti kyseiseen solmuun. Näin solmujen omien reititystaulujen ja etäisyysvektorien tiedon karttuessa laskenta leviää verkossa ja lopulta solmut ovat oppineet verkon topologian.

Jos joku linkeistä pettää, asiantilan huomanneet solmut päivittävät etäisyydeksi reititystauluihinsa eli kustannukseksi luvun, joka on suurempi kuin suurin mahdollinen todellinen etäisyys mihinkään solmuun. Tätä arvoa kutsutaan myös äärettömäksi. Seuraavaksi solmut päivittävät etäisyysvektorinsa vastaavasti ja lähettävät ne naapureilleen, mikä laukaisee verkossa tarvittavat päivityskierrokset.

Reititystaulujen solmujen välisten linkkien kustannukset vaihtelevat. Syitä voi olla esimerkiksi pitempi etäisyys tai kalliimpi yhteys. Verkon reititystaulujen tietoja välittävien pakettien katoamisen varalta edellytetään reitittimien lähettävän säännöllisin väliajoin tietoja toisilleen. Tässä on se vaara, että kun joku reititin huomaa tietyn linkin pettäneen ja se asettaa etäisyyden linkin toiseen solmuun ‘äärettömäksi’, joku toinen solmu, joka ei tiedä linkin pettäneen, ehtii lähettää etäisyysvektorinsa virhetilanteen huomanneelle solmulle, niin tämä solmu päivittää katkenneen linkin kustannukseksi äsken saamansa ääretöntä pienemmän arvon. Sen jälkeen se tiedottaa asian naapureilleen. Tässä tilanteessa syntyy silmukka linkin katkeamisen huomanneen ja siitä tietämättömän solmun välille. Jos ne saavat välitettäväkseen paketin katkenneen linkin toisessa päässä olevalle solmulle, ne tosiasiassa pallottelevat pakettia toi-silleen, kunnes elinaikalaskuri kasvaa niin suureksi, että paketti tuhotaan. Tämä

virhetilanne poistuu vasta, kun verkko uusien etäisyysvektori-ilmoitusten avulla saavuttaa stabiilin tilan.

Jos katkenneen linkin varayhteys on huomattavan kallis (tai pitkä), kestää useita päivityskierroksia, ennenkuin varareitti noteerataan muissa solmuissa. Koska solmujen päivitysilmoitusten lähettämisajat muodostavat stokastisen prosessin, verkon toipumisaikaa ei voi tarkasti ennustaa. Toipumisaika on myös kaaosmainen: ruuhkaa syntyy pakettien edestakaisista lähetyksistä ja tästä syystä todennäköisesti paketteja myös katoaa. Hankalammaksi tilanteen tekee vielä se, jos nimenomaan päivitysilmoituksia katoaa.

Vastaava ‘äärettömyyteen laskeminen’-tilanne syntyy myös silloin, jos yhteydet verkon tiettyyn osaan kokonaan katkeavat. Ennen pitkää päivityskierrokset kuitenkin johtavat stabiiliin tilanteeseen.

Pakettien edestakaisin pallottelu ja ‘äärettömyyteen laskemisen’ hitaus ovat etäisyysvektoriprotokollien hyvin huonoja puolia. Näitä puutteita on pyritty korjaamaan horisontin jaolla ja laukaistuilla päivityksillä. Horisontin jaossa päivityslevitysviesteistä lähetetään eri solmuille erilaisia versioita. Jos esimerkiksi solmu A käyttää B:tä kauttakulkusolmuna, kun kohteena on C, A pidättäytyy lähettämästä B:lle tietoja etäisyydestään C:hen. Kaikkia silmukoita tämä menetelmä ei kuitenkaan poista.

Oleellinen tekijä vektori-ilmoitusten lähettämisessä on se, koska ilmoitukset lähetetään. Ajankohta on kompromissi päivitystiedon oikea-aikaisuuden, mahdollisimman täydellisen kuvan hankkimiseen ennen omaa päätöstä kuluvan ajan, pakettihävikkien minimoinnin, naapurisolmujen tarkkailun ja monen muun tekijän suhteen.

Virhetilanteiden varalta jokaiseen reititystaulun tietoon liitetään aikaleima. Jos tietoa ei päivitetä uudelleen tietyn ajan sisällä, katsotaan tiedon lähettäneen solmun olevan poissa toiminnasta. RIP:ssä edellytetään, että tämän tiedon virkistysajan takarajan on oltava kuusi kertaa niin pitkä kuin normaali tietojen päivitysväli. Tällöin parin päivityspaketin katoaminen ei vielä aiheuta ongelmia. Toisaalta, jottei päivitystietojen ehkä pitkäkin normaali aikaväli viivyttäisi toipumista virhetilanteista, laukaistulla päivityksellä lähetetään viesti heti, kun reititystiedot ovat muuttuneet.

Kaikkia silmukoita edelliset menetelmätkään eivät poista, mutta ainakin ‘äärettömyyteen laskeminen’ nopeutuu huomattavasti, kun oikean uuden tiedon lähettäjät toimivat nopeammin kuin vanhan väärän tiedon toistajat.

Etäisyysvektoriprotokollat käyttävät joko keskitettyä tai hajautettua lyhimmän polun algoritmia parhaan reitin laskemiseen. Algoritmin askelten määrä on korkeintaan yhtä suuri kuin solmujen lukumäärä.

3.1.2. RIP versio 1

RIP suunniteltiin alunperin BSD UNIX:in verkko-osaksi. Sen ensimmäinen versio oli hyvin yksinkertainen, helppo ymmärtää ja toteuttaa. RIP kuuluu sisäisen yhdyskäytävän protokolliin (IGP), jotka toimivat tietyn autonomisen alueen sisällä. Ulkoisen yhdyskäytävän protokollat vastaavasti yhdistävät kyseisiä alueita toisiinsa.

Etäisyysvektoriprotokollat eroavat toisistaan mm. etäisyysmittansa, osoiterakenteensa ja tukemiensa linkkien määrän suhteen. RIP:n osoite on 32-bittinen Internet-osoite joka liittyy johonkin isäntäkoneeseen, verkkoon tai aliverkkoon. RIP ei tunne osoitetyyppejä, mutta osoitteen rakenteesta se voi erottaa, onko kyseessä verkko vai aliverkko tai isäntäkone. Reititystaulujen tilansäästön vuoksi isäntäkoneiden osoitteet voidaan korvata niiden verkon osoitteella.

Etäisyysmetriikkana on yksinkertainen etappien lukumäärä, niin sanottu ‘hop count’ jonka maksimiarvo on 15. ‘Äärettömyyden’ arvo 16. Tämä ei mahdollista etusijan antamista halutuille linkeille.

Pakettien normaali lähetysväli on 30 sekunttia ja jos reitin tietoja ei ole virkistetty 180 sekunttiin, asetetaan kyseinen etäisyys äärettömäksi ja myöhemmin tieto poistetaan. Peräkkäisten laukaistujen viestien lähetysväli on satunnaisesti jokin aika yhden ja viiden sekunnin välissä. Täten vältetään ‘päivitysmyrskyjä’. RIP:n pakettiin mahtuu 25 taulujäsentä. Päivitysviestin lisäksi RIP tuntee pyynnön. Yleensä pyyntö lähetetään, kun uusi reititin liittyy verkkoon. Tällöin se pyytää naapureiltaan kopion näiden tauluista saadakseen kuvan kaikista reiteistä. Tiettyjen reittien tietojen pyyntöä käytetään lähinnä virheenkorjauksiin.

Kun RIP:n ensimmäinen versio kehitettiin kymmenen vuotta sitten, annettiin myös isäntäkoneille mahdollisuus osallistua reititykseen ja ne pitivät yllä omia reititystaulujaan. RIP:n versio 2:n ja muiden uusien protokollien myötä RIP-1:tä käyttävien isäntäkoneiden taulut jäivät puutteellisiksi. Nyt työn jako on tullut selväksi. Reitittimet hoitavat yksin reitityksen.

3.1.3. RIP versio 2

RIP:n uusittua versiota on perusteltu sillä, että vaikka uudemmat protokollat ovat paljon monipuolisempia, niin RIP:n vaatii vähän kaistanleveyttä, eikä sen konfigurointikaan juuri rasita verkkoa. Lisäksi RIP on hyvin helppo toteuttaa ja hyvin laajalle levinneenä se tulee olemaan pitkään käytössä erityisesti pienissä verkoissa.

RIP-1:n sanomien käyttämättä olleisiin kenttiin oli helppo lisätä uudet ominaisuudet, kuten reititysaluetunnus, salasana, tieto seuraavasta etapista, aliverkkopeite ja lippu ‘tag’. RIP-1 käsittelee luonnollisesti oikein ne RIP-2:n viestit, joissa uusia ominaisuuksia ei hyödynnetä.

RIP-1 tukee aliverkkorakennetta vain omassa verkossaan. Tämä rajoitus on johtanut tiukan hierarkiseen reititykseen oman verkon ulkopuolella: paketit on ollut pakko lähettää lähimälle kohdeverkon reitittimelle, vaikka tällä reitittimellä ei sattuisikaan sillä hetkellä olemaan yhteyttä kohdealiverkkoon. Tämä johtaa pakettien katoamiseen. RIP-2:n aliverkkopeite poistaa tämän puutteen. Lisäksi se mahdollistaa mm. usean C-luokan osoitteen yhdistämisen osoiteryhmän sisällä CIDR:n tapaan.

RIP-1:n tietoturvan puutetta parantava uusi 16-bittinen salasanakenttä käyttää toistaiseksi niin sanottua yksinkertaisen salasanan menetelmää. Ilkeämielisten tunkeutujien on kuitenkin helppo saada salasana selville kuuntelemalla verkon liikennettä. Suojatumpi salasanamenetelmäversio on kuitenkin kehitteillä.

Reititysaluetunnuksen avulla voidaan tunnistaa samaa fyysistä yhteyttä, kuten Ethernet-kaapelia käyttävät aliverkot. Tieto seuraavasta etapista tarkentaa, mille kohdealueen aliverkon reitittimelle paketit on syytä suoraan ohjata.

RIP-2 pystyy luokan D tiettyä IP-osoitetta käyttämällä rajaamaan reititysilmoituslevitysviestit vain reitittimille. RIP-1:n levitysviestit menevät myös isäntäkoneille.

3.1.4. Muita parannuksia

Muutama vuosi sitten huomattiin, että Internetissä esiintyy 30 sekunnin jaksoissa selviä viive- ja pakettihävikkihuippuja. Syynä oli reitittimien yhtäaikainen päivitysviestien lähetys. Tällöin ne joutuvat varsinkin suurissa verkoissa yht’äkkiä ottamaan vastaan hyvin suuren määrän viestejä, jolloin muu liikenne estyy. Vaikka yksityinen reititin alunperin ei toimisi täysin samassa tahdissa muitten kanssa, sekin ennen pitkää synkronisoituu niihin. Tällainen ruuhka voidaan välttää vain valitsemalla päivitysjakso reititinkohtaisesti satunnaisesti riittävän suuresta vaihteluvälistä, 15 ja 45 sekunnin väliltä, jolloin keskimäärinen päivitysväli on edelleen 30 sekunttia.

Päivityslevitysviestien lähettäminen 30 sekunnin välein on hyvin luonnollista esimerkiksi Ethernetissä tai FDDI-renkaassa, mutta kytketyissä verkoissa kuten X.25:ssä ja ISDN:ssä ‘vaikeneminen on kultaa’. Kytketyt verkot luovat aina lähetyksen yhteydessä piirin ja lisäksi X.25:n ja ISDN:n siirtokapasiteetti on varsin pieni. Siksi niiden puskurit voivat vuotaa yli saadessaan useampia päivitysviestejä. Näistä syistä johtuen kytketyissä verkoissa on syytä käyttää vain laukaistuja viestejä ja nekin on hyväksytettävä. Tämä sanomanlähetyksissä säästäminen edellyttää, että reititystauluissa säilytetään parhaan reitin ohella myös ainakin toiseksi paras vaihtoehto, mikä nopeuttaa parhaan reitin katkeamisesta toipumista. Tätä menetelmää on hyödyllistä soveltaa muihinkin verkkotyyppeihin.

Eräs RIP:n puutteista on se, ettei se tee eroa esimerkiksi kalliin ja hitaan X:25:n ja nopean ja vapaan FDDI:n välillä. Siksi RIP soveltuu sellaisenaa huonosti hyvin erilaisista linkeistä koostuviin verkkoihin. Pelkkä etappilaskuri ei kerro reittivaihtoehtojen nopeudesta mitään. Parannuskeinoksi on SIP-työryhmässä ehdotettu uuden tiedon lisäämistä: Väylän nopeus ilmoitetaan 10 * kymmenjärjestelmän logaritmina sen maksiminopeudesta kbps:ssa. Logaritmi tasoittaa hyvin suuria linkkin nopeuseroja. Äärettömyysraja olisi 32 askelta. Ensisijaisesti reitti valittaisiin sen läpäisyn perusteella.

RIP:n heikkoutena on myös silmukoista toipumisen hitaus. Lähteenjäljitystä on ehdotettu parannukseksi. Menetelmä lisää tiedon ensimmäisestä etapista. Sen tehoa epäillään laajalti ja monimutkaisen toteutuksensa vuoksi se sotii RIP:n perusfilosofiaa ‘yksinkertainen on kaunista’ vastaan.

3.2. OSPF:n monimutkaisuus

Kun etäisyysvektoriprotokollat kehitettiin, hajautettu tietojenkäsittely ja sen protokollat olivat kehittymättömiä. Siitä syystä tuohon aikaan suosittiin keskitettyjä ratkaisuja.

Linkintila-tekniikka kehitettiin Arpanet:iin poistamaan etäisyysvektoriprotokollien ilmeisiä puutteita. Sen sijaan, että solmut vaihtaisivat tietoja solmujen välisistä etäisyyksistä, niistä jokainen ylläpitää koko verkosta karttaa, jonka ne nopeasti päivittävät topologian muuttuessa. Kartan perusteella solmut pystyvät laskemaan tarkemmat reitit kuin mihin ne etäisyysvektoriprotokollia käyttämällä kykenisivät. Laskenta on hajautettua. IETF:n linkintilaprotokolla on OSPF. OSI-mallin vastaava protokolla on IS-IS.

3.2.1. Linkintilaprotokolla

Koko toiminnan pohjana on hajautettu kartta, josta jokaisella solmulla on kopio talletettuna tietokantaan. Verkon linkin tiedot muodostavat yhden tietueen. Tietokantakartan avulla jokainen solmu voi laskea parhaan reitin muihin solmuihin. Koska solmuilla on sama kuva kartasta, reitit ovat yhtenäisiä, eikä silmukoita voi esiintyä.

Verkkotieto päivitetään nopealla ja luotettavalla Tulvaprotokollalla. Jottei vanha tieto peittäisi alleen uutta tietoa sanomiin on liitetty aikaleima tai juokseva numero, joka on modulo 2^{32} - 1. Uutta tietoa vastaanotettaessa verrataan aikaleimaa aina kannassa olevaan (ellei kyse ole uudesta linkistä) ja uudempi otetaan vastaan. Jos tuleva tieto on vanhempi, se hylätään ja muille lähetetään kopio oman kannan uudemmasta tiedosta.

Jos verkon useampi linkki pettää siten, että verkko jakaantuu kahteen erilliseen osaan, kumpikin osaverkko toimii omalla alueellaan oikein. Kun osaverkkojen välille saadaan uudelleen

luotua yhteys on tärkeää, että osaverkkojen solmut saavat jälleen luotua yhtenäiset kartat. Tätä prosessia kutsutaan OSPF:ssä ‘naapurien löytämiseksi’. Erilaiset kannat (eli kartat) pystytään yhdistämään linkkitunnusten ja versionumeroiden avulla. Yhdistämisen alkuvaiheessa kumpikin puoli lähettää täydet kopiot kannoistaan, josta toisen osapuolen solmut poimivat linkkitunnusten ja versionumeroiden avulla vain ‘kiinnostavat tietueet’ eli ne, jotka poikkeavat niiden omista tietueista.

OSPF:ssä on virhetilanteiden varalle lukuisia varmistuksia, joiden avulla taataan kantojen eheys. Näitä varmistuksia ovat mm. tietueiden tarkistussummat, tulvaproseduurin etappikohtaiset hyväksynnät, sanomien tunnussanat ja linkintilatietueiden suojaus aikalaskureilla.

Etäisyysvektoriprotokollien lyhimmän reitin laskemiseen käyttämä algoritmi ei ole kovin tehokas. E.W.Dijkstran ‘lyhin polku ensin’-algoritmi on tehokkaampi ja siitä OSPF onkin saanut nimensä: ‘avaa lyhin polku ensin’. Tarvittavien iteraatioiden määrä on luokkaa O(M.logM). Algoritmi perustuu solmujen jakamiseen käsiteltyihin ja muihin. Laskennan edetessä solmut siirretään joukosta muut käsiteltyihin.

3.2.2. Linkintilaprotokollan paremmuus

Linkintilaprotokolla on etäisyysvektoriprotokollaa parempi monessa suhteessa. Tulvaprotokolla päivittää karttakannat paljon nopeammin kuin laukaistut päivitykset, jotka joutuvat joka askeleella odottamaan muutaman sekunnin. Lisäksi EV-protokollien sanomien määrä on suhteessa kohteiden määrän, mikä isossa verkossa johtaa päivityspakettien jakamiseen. Tärkein ero on kuitenkin linkintilaprotokollien kyky välttää silmukat.

Nykyisessä Internetissä on hyvin suuria kaistanleveyseroja eri linkkien välillä. EV-protokollilla voi äärettömyyteen laskeminen kestää näissä tapauksissa hyvin kauan. Linkitilaprotokollat voivat sen sijaan hyödyntää useita reitinarviointiominaisuuksia, kuten suurinta kaistanleveyttä, pienintä viivettä, alhaisinta hintaa ja suurinta luotettavuutta. OSPF-dokumentit eivät määrittele, miten viive-, luotettavuus- tai hintametriikat asetetaan. Useita perusteita käytettäessä on päätösten johdonmukaisuuteen kiinnitettävä erityistä huomiota. Huolimaton eri perusteiden yhtäaikainen soveltaminen voi johtaa silmukoihin.

Kahdesta yhtäpitkästä reitistä RIP valitsee satunnaisesti toisen. Matemaattisesti on osoitettu, että liikenteen jakaminen useammalle väylälle on tehokkaampaa. Viiveen vaihtelu pienenee myös useammalla väylällä, sillä kunkin väylän pakettien saapumisaikojen korrelaatio pienenee. Liikenteen hajauttaminen pehmentää myös koko liikenneprofiilia, sillä katkosten sattuessa estynyt liikenne jakaantuu varaväylille tasaisemmin, kuin yhden väylän tapauksessa. Haittana on, että pakettien järjestys perillä ei välttämättä säily.

Liikenne on syytä jakaa eri reiteille myös silloin, kun tarjolla olevat reitit ovat pituudeltaan (tai kustannuksiltaan) samaa suuruusluokkaa. Liikennemäärien jako sopivassa suhteessa eri reiteille on kuitenkin monimutkainen laskutehtävä.

Kun verkko on yhdistetty ulkomaailmaan useamman yhdyskäytävän läpi, oletuskäytäväksi voidaan valita lähin. Parhaimman valinta edellyttää ainakin tavallisimpien ulkoisten reittien tietojen tallettamista tauluihin. Kun SPF laskee reittejä O(N.logN)-tehokkuudella, EV-protokollat vaativat $O(N^2)$ laskua. Suuressa verkossa ero on huima.

3.2.3. OSPF:n rakenne

Nykyään suuri osa Internetiin yhteydessä olevista tietokoneista on yhteydessä siihen lähiverkon kautta. OSPF:lle riittää, että reititin tuntee vain ko. lähiverkon IP-aliverkko-osoitteen. OSPF kutsuu tätä tynkäverkkolinkiksi, ‘link to a stub network’.

OSPF optimoi levitysviestien lähettämistä niissä verkoissa, joissa se on mahdollista, määrittelemällä virtuaalisolmun, joka edustaa levitysverkkoa (broadcast network). Edusreitittimen avulla (designated) voidaan rajata naapurien ja linkkien määrä samaksi kuin solmujen määrä. Muilla reitittimillä on naapurina ja taulun linkin kohteena vain edusreititin. Tulvaproseduuri yksinkertaistuu myös, kun päivitysviestit lähetetään vain edusreitittimelle, joka jakaa ne edelleen. OSPF valitsee tälle heti alussa varareitittimen, johon muut luovat myös taulujäsenet, muuten järjestelmä olisi kovin haavoittuva.

Ei-levitysverkoissa (nonbroadcast) luodaan tekopysyvät virtuaaliyhteydet reitittimistä edus- ja varareitittimeen, muille suorille yhteyksille virtuaaliyhteydet luodaan vain tarvittaessa.

Kun verkko kasvaa hyvin suureksi, tietokannat paisuvat liian suuriksi ja päivitysviestien kuorma tukkii verkon. Ratkaisu ongelmaan on hierarkinen verkkorakenne: runkoverkko, joka yhdistää erillisiä reititysalueita, jotka voivat sisältää useita IP-aliverkkoja. Tavalliset reitittimet näkevät vain alueensa. Reuna-aluereitittimet yhdistävät alueet ja runkoverkon pitämällä yllä kaikkien niiden alueverkkojen (tai vain yhden) ja runkoverkon reititiystauluja, johon ne kuuluvat ja välittämällä runko- ja muiden verkkojen verkkokohtaiset tiedot koontitietueissa verkkoihin, joihin ne kuuluvat.

Reititystauluissa valtaosa tietueista kuvaa verkon ulkoisia linkkejä. Jottei OSPF:n käyttö pienissä muutaman reitittimen verkoissa muodostuisi liian raskaaksi, on määritelty tynkäalue (stub), jossa ulkopuoliset reitit yhdistetään yhdelle oletusreitille. Tämä on osoittautunut usein liian rajoittavaksi piirteeksi, joten on luotu myös NSSA-käsite, ei-niin-tynkä-verkko.

3.2.4. Linkintilatietokanta

Linkintilatyyppejä on viisi: reititin, verkko, IP-verkon yhteenveto, rajareitittimen yhteenveto ja ulkopuolinen. Tietuetyyppejä on neljä, sillä yhteenvedot käyttävät samaa formaattia. Linkintilailmoitusotsake on yhteinen kaikille tietuetyypeille. Otsakkeen kenttiä ovat mm. ilmoituksen antanut reititin, linkin tunnus, linkintilatietueen ikä sekunneissa, linkintilan juokseva järjestysnumero, tarkistussumma ja pituus.

Reitittimen linkintilatietue yhdistää kaikkien ilmoituksen antaneesta reitittimestä lähtevien linkkien tiedot. Tässä tietueessa voi olla useita palvelutyyppi- eli TOS-metriikoita. Edusreitittimet lähettävät kauttakulkuverkoille verkkolinkkitietueen, josta käy ilmi kaikki edusreitittimeen naapuruuden luoneet reitittimet. Reuna-aluereitittimet ilmoittavat kohdekohtaiset yhteenvetolinkkitiedot, joissa voi esiintyä useampia TOS-metriikoita, kuten reitittimen linkintilatietueissakin. Raja-reitittimet luovat ulkoisten linkkien tietueet ulkoisten yhdyskäytävien protokollilta kuten BGP:ltä tai EGP:ltä saamistaan tiedoista. Näiden tietueiden metriikat eivät välttämättä ole vertailukelpoiset alueen sisäisten metriikoiden kanssa.

OSPF laskee tietokannan tiedoista SPF-algoritmilla jokaiseen kohteeseen johtavan seuraavan reitittimen ja lyhimmän (parhaan) sekä yhtä hyvän yhteyden siihen.

3.2.5. OSPF:n aliprotokollat

OSPF toimii suoraan IP:n päällä ja se koostuu kolmesta aliprotokollasta.

Hello-protokolla tarkistaa, että linkit toimivat. Se valitsee myös verkon edus- ja varareitittimen. Hello-paketin aikaväli kertoo pakettien lähetysvälin ja kuollut aikaväli vanhenemisajan. Etusijakentän avulla reitittimet voidaan laittaa suosituimmusjärjestykseen valittaessa edus- ja varareitittimiä tai reititin voidaan sulkea pois valittavien joukosta. Linkki on toiminnassa, jos se voi välittää paketteja molempiin suuntiin ja jos linkin molemmat reitittimet voivat lähettää ja vastaanottaa ulkoisia reittejä tai kumpikaan ei voi tätä tehdä.

Kun kaksi reititintä on muodostanut kaksipuolisen yhteyden, ne yhdenmukaistavat tietokantansa vaihtoprotokollan (exchange) avulla. Verkkolinkeillä tämä hoidetaan edus- tai varareitittimien välityksellä. Vaihtoprotokolla on epäsymmetrinen: aluksi valitaan roolit ‘isäntä’ ja ‘orja’, jonka jälkeen reitittimet vaihtavat keskenään tietokantakuvaukset ja kumpikin merkitsee ne tietueet, joissa on uudempaa tietoa kuin heidän omassa kannassaan. Lopuksi ne lähettävät pyyntöpaketit haluamistaan tietueista.

RIP:iin verrattuna OSPF on monimutkainen, sen dokumentaation koodi on viisinkertainen ja hallinta vaatii enemmän tietoa. RIP selviää kahdella eri viestillä, OSPF:llä niitä on viisi ja lisäksi kolme proseduuria. Linkintilapäivitykset on hyväksytettävä, etäisyysvektoreita ei tar-

vitse hyväksyä. Reititintaulujen lisäksi OSPF tarvitsee linkintilatietokannan. Nämä rasitteet OSPF korvaa paremmalla reitityksellä ja vähemmällä signaloinnilla. Kun RIP viestii 30 sekunnin välein, OSPF:lle riittää 30 minuutin päivitysväli.

3.3. Muita reititysprotokollia

OSPF:n ja RIP:n ohella käytetyimmät Internetin reititysprotokollat ovat Ciscon IGRP ja sen laajennettu versio EIGRP ja ISO:n CNLP-protokollalleen standardisoiman IS-IS:n IP-laajennus ‘kaksois IS-IS’.

3.3.1. Reitittimet vai välijärjestelmät

ISO:n OSI-mallista on koetettu luoda virallista tietoliikennestandardia. Yritys on kuitenkin uupunut byrokratian raskaan painon alle. Vaikka OSI-mallia ei olekaan sovellettu runsaasti käytäntöön, sen viitteellinen merkitys on suurempi. Reitittimet ja isäntäkoneet on OSI:ssa korvattu loppu- ja välijärjestelmällä. Reitityksen ja verkon tilalla on ‘reitittely’ ja alueet.

Linkintilaprotokollien tietokannat koostuvat verkon topologiaa kuvaavista ja topologian ja osoitteiden suhteita ilmentävistä tietueista. Topologia on dynaaminen, mutta kaikille protokollille sama. Toisaalta vaikka osoitteiden ja topologian suhde on protokollariippuvainen, niin se on verraten pysyvä. Näistä syistä johtuen OSI:n ‘kaksois IS-IS’ on voitu luoda kuvaamaan sekä CLNP-, että IP-reittejä.

OSI-kehys on hierarkinen ja se jakaa reititysalueet yhdestä tai useammasta lähiverkosta koostuviin alialueisiin, jotka karkeasti vastaavat OSPF:n tynkäalueita. IS-IS:n osaprotokollia ovat Hello ja tulvaprotokolla samoin tehtävin kuin OSPF:llä. IS-IS hoitaa tulvan, vanhenemisen ja linkintilatietueiden vaihdon yhdellä proseduurilla. Etäisyysmetriikat ovat samat neljä kuin OSPF:llä.

Asentamalla reitittimiin CLNP ja IS-IS-paketteja demultipleksoimaan pystyvä koodi, IS-IS:ää voidaan ajaa IP-verkon päällä. Tällöin kuitenkin jäykkyys säilyy, mutta joitakin etuja menetetään. IS-IS:n puutteita ovat myös vain 6-bitin mittainen etäisyyskenttä, joka pahasti rajoittaa reitityksen tarkkuutta sekä 8-bittinen linkintilatietuetunnus, joka sallii reitittimelle vain 256:n tietueen ilmoittamisen. OSPF voi lisäksi toimia rinnan RIP:n kanssa ‘ei-niin-tynkien-alueiden’ välityksellä. Tärkeä etu on myös se, että IETF:n alainen kehitystyö on selvästi nopeampaa ja joustavampaa kuin ISO:n piirissä tehty.

Isoimmissa yritysten runkoverkoissa käytetään usein eri tarkoituksia palvelemaan erilaisia pro-tokollia, jotka myös edellyttävät yksilöllistä reititystä. Yhdistetyn reitityksen ei ole to-

dettu johtavan tehokkaampaan verkon hallintaan kuin ‘laivat yössä’-tyyli, jossa jokainen protokolla reititetään omine välineineen ilman muiden tukea.

3.3.2. IGRP

Kun Cisco aikanaan perustettiin, IP:n tarjolla oleva reititysprotokolla oli RIP. Koska IETF:llä ei ollut vielä silloin valmiina parempaa protokollaa, Cisco päätti luoda oman parannetun painoksen RIP:stä, sisäisen yhdyskäytävän reititysprotokollan IGRP:n. IGRP on etäisyysvektoriprotokolla, joka hoitaa päivitykset monilähetyksellä kuten RIP, mutta lähetysväli on 90 sekunttia, kun se RIP:llä on 30 sekunttia.

IGRP käyttää metriikkaa laskiessaan neljää tekijää, jotka ovat viive, kaistanleveys, luotettavuus ja kuorma. Vertailtaessa kahta reittiä, IGRP laskee em. parametreista ja paketin pituudesta kaavalla kootun metriikan. Ciscon toteutuksessa käytetään viittä eri painokerrointa, joilla reititin voi painottaa tiettyjä osametriikoita paikallisten tarpeitten mukaan. Oletusreittiehdokkaina IGRP käyttää joitakin todellisia verkko-osoitteita (esimerkiksi kauttakulkuverkkojen osoitteita). RIP:in ja OSPF:n oletusreitille käyttämän 0.0.0.0-osoitteen metriikalla on se puute, että se ei suoraan liity etäisyyteen.

IGRP käyttää jaettua horisonttia ja laukaistuja päivityksiä, kuten RIP:kin, muttei myrkyllistä kääntöä (poisonous reverse). Silmukoiden torjuntaan IGRP:n uusimmat versiot käyttävät reitin myrkytystä, joka perustuu siihen huomioon, että silmukan syntyessä etappilaskuri kasvaa. Laskuri voi kasvaa myös muusta syystä, mutta varmuuden vuoksi kyseinen väylä suljetaan kunnes toinen päivitys vahvistaa etappilaskurin kasvun.

Huomattava parannus RIP:hen nähden on myös monipolkureititysmahdollisuus, joka oli myös OSPF:n etu RIP:hen verrattuna. Liikennekuormituksen tasaaminen on tästä saatava etu. Useampi polku takaa myös varajärjestelmän, jonkun linkin pettäessä. Jotta vältettäisiin silmukat, on varareitti on syytä kelpuuttaa vain silloin kun sen seuraava reititin on lähempänä kohdetta kuin lähtösolmu.

3.3.3. EIGRP

Vuonna -88 valmistunut IGRP:n ensimmäinen versio korjasi RIP:n monia puutteita, mutta vaja-vaisuuksia jäi silti jäljelle. Sulkemalla epäilyksen alaiset polut väliaikaisesti IGRP ei pysty takaamaan silmukoiden paljastamista. Jaksottaiset päivitykset aiheuttavat samanlaisia tahdis-tusongelmia kuin RIP:ssä. Cisco ei kuitenkaan päättänyt siirtyä OSPF:ään, sillä useat sen suunnittelijoista uskoivat etäisyysvektoriprotokollien antavan yksinkertaisella tekniikalla suuremman joustavuuden.

Etäisyysvektoriprotokollien ‘hajautettu laskenta’ synnyttää jossain määrin kaaosmaisen välitilan, ennenkuin lukuisten sanomien vaihdon jälkeen verkko vakiintuu. EV-koulukunnan kannattajat vetoavat tekniikkansa yksinkertaisuuteen sekä pienempään muistitarpeeseen ja sanomien määrään.

Yksinkertaisuus on eittämättä etu jo pienemmän virhetodennäköisyyden johdosta. Muistin tarve ei kuitenkaan ole kovin paljon pienempi, kun verrataan kehittyneempää EV-toteutusta esimerkiksi OSPF-toteutukseen. Toteutustapa vaikuttaa muistitarpeeseen yhtä paljon kuin protokolla. Mitä kaistanleveyteen tulee, niin RIP tarvitsee sitä enemmän kuin linkintilaprotokolla OSPF. RIP lähettää verraten tihein välein koko taulunsa verkon kaikille muille solmuille, kun OSPF tiedottaa lähinnä vain sattuneista muutoksista.

EV-tekniikan kannattajat arvostelevat linkintilaprotokollia hetkellisistä silmukoista ja laskentahuipuista. Jonkin linkin pettäessä EV-protokollat laskevat vain kyseistä linkkiä käyttäneet reitit, kun sen sijaan linkintilaprotokollat laskevat koko taulunsa uudelleen. Ero on huomattava varsinkin silloin, kun jokin reititin vikaantuu useiden lyhyiden perättäisten jaksojen ajaksi. Mikään ei kuitenkaan estäisi linkintilaprotokollia käyttämästä osittaista laskentaa. Tällaisia toteutuksia ei vain ole tehty.

EIGRP:n parhaita parannuksia on reititystauluja uudelleen laskettaessa syntyvien äkillisten silmukoiden poisto diffuusipäivitysalgoritmi DUAL:lla (joka sopii myös linkintilaprotokollille). Se jäädyttää reititystaulut päivitysviestien tulviessa, jottei äkillisten välitilojen perusteella tehtäisi virheellisiä reitinvalintoja. DUAL edellytti huomattavia muutoksia IGRP:hen. Sanomien määrä oli lisättävä viiteen: Hello, päivitysviesti, kysely, vastaus ja pyyntö.

Muita muutoksia on reitityksen salliminen mielivaltaisilla aliverkko- tai CIDR-yliverkkopeitteillä. Lisäksi ulkopuoliset reitit merkitään ulkopuolisia yhdyskäytäväprotokollia varten lipulla ‘tag’, kuten RIP-2:ssa tai OSPF:ssä. Toisin kuin OSPF, EIGRP ei tunne aluekäsitettä. Sen sijaan jotkut reitittimet voivat yhdistää aliverkkoja, tai yleisemmin osoite-etuliitteitä. Nämä reitittimet toimivat samaan tapaan kuin OSPF:n reunareitittimet, ehkä vain vielä joustavammin.

3.3.4. Reititinprotokollan valinta

Tulevaisuudessa reitityksessä saattavat kokea ylösnousemuksen jo koetellut tekniikat, kuten ‘tulva- ja lähdereitti’ tai ‘kuumaperunareititys’, missä siirron tehokkuus on uhrattu nopeammalle reitinlaskennalle tai pienemmälle muistintarpeelle. Ajantahdistus voi korostua, jos tau-

lupäivityksiä halutaan nopeuttaa. Optinen kytkentä on esimerkki uusista tekniikoista, jotka nopeuttanevat reitinlaskentaa.

Lähitulevaisuudessa valinta on kuitenkin tehtävä tässä kappaleessa esiteltyjen yhdyskäytäntöjen välillä. IAB ja useat asiantuntijat suosittelevat tänä päivänä OSPF:ää. Sen ja IS-IS:n laatu- tai nopeuserot eivät ole merkittäviä, mutta IETF kehittää OSPF:ää paljon joustavammin kuin OSI IS-IS:äänsä.

Ainoa mielekäs vaihtoehto OSPF:lle lienee nykyään EIGRP. EIGRP on poistanut monia EV-protokollien puutteita, mutta yksinkertaisuuden kustannuksella: naapureiden kaikkien etäisyysvektoreiden tallettaminen vie vähintään saman tilan kuin linkintilatietokannan ylläpito, eikä DUAL-prosessi varmasti vakiinnu nopeammin kuin linkintilalaskenta. Voidaan kyllä perustellusti väittää, että EV-tekniikalla saavutetaan yhtä luotettava reitinlaskenta kuin linkintilatekniikallakin, mutta vain kun ensinmainittu tulee yhtä monimutkaiseksi kuin seuraajansa.

Nykyään tärkeimpinä vertailukriteereinä pidetään toteutuksen laatutasoa, konfiguroinnin helppoutta ja standardoinnin tasoa. Jos esimerkiksi reititin huomaa kovin myöhään linkin katkenneen, paljon sotkua ehditään saada aikaan ennen sitä.

Yleinen protokolla takaa riippumattomuuden laitevalmistajista. Laitevalmistajan oma hyväkin protokolla sen sijaan sitoo käyttäjänsä sen valmistajaan.

4. Ulkoiset reititysprotokollat

4.1. EGP: Ensimmäinen askel kohti maailmanverkkoa

4.1.1. Jako itsenäisiin alueisiin

Kun Internet kasvoi alussa tarpeeksi, sitä ei voitu enään käsitellä yhtenä reititysalueena. Oli luotava käsite itsenäinen alue AS, joka runkoverkon kautta oli yhteydessä muuhun verkkoon. AS määritellään yhden organisaation hallitsemaksi kokoelmaksi reitittimiä ja aliverkkoja, jotka ovat yhteydessä toisiinsa. Jokaisen AS:n reititystauluissa on oltava tieto kaikista mahdollisista Internet-verkoista. Alkuaikojen reititysprotokollana käytettiin GGP:tä. Tuon ajan terminologiassa reitittimet olivat yhdyskäytäviä. Termi on jäänyt uusimpiinkin versioihin.

4.1.2. Tiedon vaihto EGP:n avulla

Ulkoinen yhdyskäytäväprotokolla EGP koostuu kolmesta erillisestä toiminnosta: ‘naapurin hankinnassa’ sovitaan mahdollisesta naapuruudesta, ‘naapurin tavoitettavuus’ tarkkailee naapurien välistä linkkiä ja ‘verkon tavoitettavuus’ hoitaa tavoitettavuustiedon vaihdon. EGP-viestit kuljetetaan IP-datagrammeissa protokollanumerolla 8. Naapurin tavoitettavuutta ei ole syytä päätellä siitä, että verkon kautta on saatu siihen yhteys, naapurin reitityskyvystä se ei kerro mitään. Jos yhteyttä ei saada, asia on selvä, naapuri ei voi olla toiminnassa. Yhteys tarkistetaan lähettämällä esimerkiksi 30 se-kunnin välein ‘hello’-viesti, johon naapuri vastaa ‘I-H-U’:lla (I heard you), jos yhteys toimii. Yhteyden tilan muuttumista ei pidä päätellä vain yhden muutossanoman perusteella. Verkon tavoitettavuus saadaan selville lähettämällä tiedusteluja, yleensä kahden minuutin välein, joi-hin tiedustelun kohteen on vastattava muutaman sekunnin aikana. Kahden itsenäisen alueen välisen tiedonvaihdon hoitavat tehtävään nimetyt reunareitittimet. Jottei niiden tarvitsisi välittää kaikkea alueiden välistä liikennettä, ne kertovat vastausviesteissään myös oman alueensa muiden reitittimien osoitteet.

4.1.3. Reitit, etäisyydet, silmukat

Kun EGP-reititin ilmoittaa jonkun IP-aliverkon olevan tavoitettavissa kauttaan, se tarkoittaa, että kyseisessä itsenäisessä alueessa on toimiva polku tähän kohteeseen ja että itsenäinen alue myöntyy välittämään paketteja tällä polulla. Tämä tarkoittaa myös läpikulkuliikenteen sallimista, joka vie verkon voimavaroja sen omalta liikenteeltä, eikä näin ollen ole itsestään selvä myönnytys.

Itsenäisten alueiden etäisyysmetriikat vaihtelevat, RIP käyttää etappilaskuria ja OSPF tavallisesti viivearviota. EGP:lläkin on metriikka, joka on luku väliltä 0 - 255, missä 255 tarkoittaa, että kohde ei ole tavoitettavissa. EGP:n metriikan päätarkoitus on olla suhteellinen eli antaa joillekin reiteille etusija toisiin reitteihin nähden.

Lyhimmän reitin laskeminen oman verkon ulkopuoliseen kohteeseen on helppoa, jos ulkopuolista liikennettä hoitaa vain yksi reititin, mikä ei aina ole käytännöllistä. Jos sisäinen reititys hoidetaan OSPF:llä, sen E-bitti ilmaisee EGP:ltä saadun reitin olevan ulkopuolinen ja siis todennäköisesti pidempi kuin mikään sisäinen reitinpituus. OSPF käyttää ulkopuolisille kohteille siis EGP:n metriikkaa, lyhin reitti voidaan jälleen yksikäsitteisesti valita.

Jos sisäinen protokolla on RIP, ulkoisen etäisyyden laskeminen on paljon vaikeampaa, mm. RIP-2:n etappilaskurin pienen arvojoukon vuoksi. RIP:tä ei olekaan syytä käyttää, jos ulkoiselle reititykselle asetetaan suurempia vaatimuksia.

Vaikka EGP ensinäkemältä muistuttaa yksinkertaista EV-protokollaa, siitä ei ole yleiseksi reititysprotokollaksi. Vaikka se luotiin alunperin kaksitasoiselle hierarkiselle verkkomallille, se voi toimia myös yleisemmällä topologialla, jos tämä topologia on silmukaton puu. Monimutkaisen ristikkäisiä yhteyksiä käsittävän nykyaikaisen verkon protokollaksi siitä ei kuitenkaan ole. Se suunniteltiin 1983, jolloin Internet oli paljon yksinkertaisempi kuin tänä päivänä.

4.1.4. EGP:n rajoitukset

EGP:n virheellisiä - tahallisia tai tahattomia - reititystietoja on voitu torjua vain käsin konfiguroimalla, EGP ei ole pystynyt automaattisesti estämään erheitä. Kun Internetissä ei ole enään pitkään aikaan ollut vain yhtä runkoverkkoa, EGP:n pelkkään etäisyyteen perustuva reittien valinta ei riitä. Yliopistorunkoverkot ovat ilmaisia käyttäjilleen ja kaupallisten operaattorien hinnat voivat vaihdella paljonkin. Internetin kasvu on johtanut myös tavoitettavista verkoista kertovien pakettien koon kasvuun niin suuriksi, että ne on usein jouduttu pilkkomaan. Pakettien tehokas ja turvallinen jakaminen ei myöskään ole kuulunut EGP:n tehtäviin. Näistä syistä johtuen IETF kehitti EGP:lle seuraajaksi rajayhdyskäytäväprotokollan, BGP:n vuosikymmenen vaihteessa.

4.2. BGP: kohti 90-lukua

Viime vuosikymmenen lopulla runkoverkkopohjainen puutopologiaa noudattava EGP oli todettu aikansa eläneeksi ja vuonna -89 julkaistiin jo seuraaja BGP:n ensimmäinen versio. Vuoden välein tulivat BGP-2 ja BGP-3, joista jälkimmäistä käsitellään tässä luvussa. Uusin versio BGP-4 vuodelta -94 sisältää CIDR-toteutuksen.

4.2.1. Väylävektorit

BGP:n tärkein parannus on polkuvektorit, joiden avulla voidaan estää silmukoiden synty monimutkaisissa verkoissa. Aikanaan lyhin polku oli valintaperuste. Lyhin polku voi kuitenkin käyttää huippukalliin operaattorin yhteyttä tai epävarmaa yliopistoverkkoa. Nykyään reitit pannaankin suosituimmuusjärjestykseen antamalla ‘etäisyyksille’ sopivat arvot. Nämä arvostukset voivat kuitenkin vaihdella eri itsenäisisä alueissa, mikä puolestaan saattaa luoda silmukoita. Tästä syystä ja itsenäisten alueiden kasvavasta määrästä johtuen linkintilatekniikka ei voi tarjota ratkaisua verkkojen yhdistämiseen. EV:t eivät taasen estä silmukoita tehokkaasti.

BGP:n ratkaisu on radikaali: jokainen päivitysviesti kertoo kaikki kauttakulkuverkot tai AS:t lähtökohdan ja kohteen välillä. Kun reititin vastaanottaa tällaisen viestin se vain tarkistaa, ettei se jo kuulu AS-listaan. Silmukoiden torjunta on siis yksinkertaista, mutta vastaavasti reititysviesteistä tulee pitkiä ja protokollan muistitarve kasvaa. Etuna on, että metriikat voivat vaihdella.

Väyliä kuvaavista atribuuteista tärkeimmät ovat AS:t, joiden kautta on kuljettu ja lista tavoitettavista verkoista. Muita ovat mm. seuraava etappi, tavoittamaton-merkki ja AS:ien välinen metriikka, joka on täysin paikallinen ja joka antaa etusijan tähän AS:ään johtavalle halutulle väylälle. Reitittimien ei odoteta ymmärtävän kaikkia valinnaisia atribuutteja, mutta niiden on tietysti välitettävä nekin.

Jos jossain AS:ssä on useita ulkoisia reitittimiä, verkon valvojien on luotava niiden välille riittävät yhteydet, jotta ne pystyvät välittämään toisilleen vastaanottamiaan BGP-viestejä.

4.2.2. BGP

Hyvin tärkeä ominaisuus BGP:llä on se, että se ajetaan TCP:n päällä. TCP:n luotettavuudesta johtuen BGP ei tarvitse virheenkorjausta, eikä BGP-viestejä tarvitse sovittaa IP-datagrammien koon mukaisiksi. BGP onkin selvästi yksinkertaisempi ohjelmisto kuin EGP. BGP:n ei tarvitse lähettää myöskään kaikkia reititystietoja tasaisin väliajoin. Riittää, kun vain muutokset ilmoitetaan muille reitittimille. Jopa niinkin alhaisia BGP:n keskimääräisiä liikennevirtoja kuin 5 bps on mitattu. Nykyiset TCP-toteutukset pystyvät sovittamaan lähettämänsä liikenteen verkon kulloisenkin kapasiteetin mukaiseksi. Tällöin on kuitenkin huolehdittava siitä, että estotilojen purkamisen kannalta elintärkeät reitityspäivitykset saavat etusijan muuhun liikenteeseen nähden.

BGP:llä on neljä pakettityyppiä: avausehdotus, päivitys, huomautus ja yhteys voimassa. Yhteyden avausviestissä on autentikointimahdollisuus, mutta vain ei-autentikointia-vaihtoehto on toistaiseksi standardisoitu. Syynä on se, että niin kauan kun TCP on suojaamaton, ei

BGP:täkään kannata turhaan salata. Kun yhteys kahden reitittimen välille on luotu, ne alkavat lähettää toisilleen väyläkohtaisia päivitysviestejä, joista ilmenevät tämän väylän kautta tavoitettavat verkot. Aluksi ne ilmoittavat kaikki väylät, myöhemmin vain näiden muutokset. Uusi vastaanotettu tieto välitetään kaikille naapureille, paitsi saman AS:n reunareitittimille, jos nämä muodostavat ‘yhdistetyn verkon’. Uusi väyläehdotus hyväksytään vain, jos oma AS ei jo kuulu sen verkkolistaan eli kyseessä ei ole silmukka, tai jos verkko on tarpeeksi vakaa eli se ei toistuvasti vaihda tilaansa tavoitettavasta tavoittamattomaksi.

Normaalimuodossa TCP kertoo linkin toimivuuden vain kun linkkiä käytetään. BGP:n on kuitenkin aina tiedettävä linkkien kunto. Niinpä BGP lähettää jatkuvasti paketteja. Jos päivityspaketteja ei ole liikkeellä lähetetään yhteys voimassa-paketteja noin kahden minuutin välein. Jos kyselyn kohde ei vastaa kolmeen viestiin, sen ei katsota olevan toiminnassa, vaikka TCP yhteys siihen olisikin voimassa.

4.2.3. Tahdistus IGP:n kanssa

Ulkoiset BGP-reitittimet joutuvat käyttämään sisäisiä yhteyksiä vaihtaessaan polkuvektoritietoja keskenään. Nämä päivitykset on tahdistettava paikallisten reititystaulumuutosten kanssa. Jos AS käyttää OSPF:ää sisäiseen reititykseen, niin reunareitittimet tuovat AS:ään tiedot ulkoisista väylistä ulkoisten linkintilatietueiden välityksellä, joissa oleva reittilippu (route tag) liitetään paikallisen ja etä-AS:N väliseen reittiin. Normaalisti ulkoisille yhteyksille ei käytetä useita metriikoita ja niinpä BGP ei tue palvelutyyppireititystä.

4.2.4. BGP ja reitityspolitiikka

Internetin muodostavat verkot ovat monien erilaisten intressiryhmien rakentamia. Julkiset verkot on luotu opetus-, tutkimus- ja muuhun yleishyödylliseen käyttöön. Alueverkot tukevat paikallista liike-elämää ja muita paikallisia aktiviteetteja. Sallitun käytön politiikka AUP määrittelee keille annetaan verkon käyttöoikeus. Internetin etappi-etapilta-reitityksessä yhdellä reitittimellä on vain rajatut mahdollisuudet vaikuttaa pakettien koko reittiin. Toisiinsa sopimattomat politiikat voivat pahimmillaan johtaa yksisuuntaisiin yhteyksiin tai yhteyksien estymiseen joittenkin solmujen välillä, kun AS:t valitsevat itsenäisesti AUP:nsä. Jotta reitityspolitiikan ristiriitaisuudet voitaisiin selvittää, reunareitittimet lähettävät jonkun yhteyden katkettua ensin tiedon yhteyden poistumisesta ja sitten ehdotuksen uudesta reitistä.

Paras reitti voidaan valita minimoimalla väylän läpikulkemien AS:ien määrä tai antamalla painot AS:ille omien tarpeitten pohjalta.

4.3. CIDR ja reititysräjähdys

BGP ratkaisi miten Internetissä siirrytään yhden runkoverkon ympäröimästä puutopologiasta yleiseen verkkomaiseen topologiaan. Luokaton alueiden välinen reititys CIDR koittaa selvitä hurjasti kasvaneen Internetin seuraavan polven ongelmien kuten reititystauluräjähdyksen ja B-luokan osoitteiden loppumisen kanssa kunnes IP:n uusi versio valmistuu.

4.3.1. CIDR ja Internetin uhat

Internet-osoitteiden B-luokka tarjoaa yli 16’000 isäntäkoneosoitetta yhtä verkko-osoitetta kohti. Se onkin osoittautunut sopivimmaksi luokaksi useimmille yrityksille ja siksi B-verkko-osoitteet olisivat loppuneet jo alkuvuodesta -94 ilman erikoistoimia.

Reititystaulun vaatima muistitila vaihtelee paljon käytetyn protokollan ja reitittimen arkkitehtuurin mukaan. Reititystaulut on yritetty toteuttaa mm. suoraan reitittimen piirien nopeaan muistiin, johon kaikkien verkkojen seuraavat etapit on talletettu. Ratkaisu oli nopea, mutta kun Internetin verkkojen määrä ylitti piirin muistin määrän, tuli seinä vastaan.

Nykyään reititystaulut muodostetaan prosessorissa, jolla keskusmuistia on runsaammin ja jossa ohjelmointi on helppoa. Kuitenkin reunareitittimet joutuvat pitämään yllä tavoitettavuuslistoja ja vastaavia AS-polkuja kaikkiin sisäisiin ja ulkoisiin naapureihinsa, jolloin muistin tarve on verrannollinen naapureiden ja kohteiden lukumäärien tuloon.

B-osoitteiden ehtymisen uhka on hoidettu siten, että luokkaan pääsemiseksi organisaatiolla pitää nykyään olla ainakin 32 aliverkkoa ja 4096 isäntäkonetta. Tätä pienemmät tarpeet tyydytetään varaamalla tarvittaessa useampia peräkkäisiä C-luokkia. Tämä puolestaan tarjoaa mahdollisuuden pyrkiä reitittämään kootusti alueittain, mikä säästäisi rajallista luonnonvaraa, 32-bittistä Internetin osoiteavaruutta.

4.3.2. Reititystaulujen yhdistäminen

Vuoteen -92 asti Internetin verkko-osoitteilla ei ollut mitään tekemistä topologian kanssa. Etuna oli joustavuus, haittana reititystaulujen nopea täyttyminen. Taulut voidaan yhdistää joko operaattorikohtaisesti tai aluepohjaisesti.

Internet-topologia ei ole suoranaisesti aluepohjainen. Sen alkiot: linkit, reitittimet ja yhteydet ovat operaattoreiden hallinnassa. Jos vierekkäisissä taloissa toimivat isäntäkoneet ovat liittyneet eri operaattoreiden verkkoihin, niiden Internet-etäisyys voi olla hyvinkin pitkä. Kummankin operaattorin reititystaulussa voidaan toisen operaattorin koko verkkoon viitata yhdellä etuliitteellä, joten taulutilan säästö on maksimaalinen. Jottei tätä etua menetettäisi, edellyt-

täisi operaattorin vaihto kuitenkin hankalaa Internet-osoitteen vaihtoa, mikä haittaisi puolestaan kilpailua.

Aluepohjainen verkko-osoitteiden jako vapauttaisi käyttäjät operaattoreiden torppariudesta ja osoitteita voitaisiin silti yhdistää ainakin ylemmillä maanosa-, maa- ja ehkä kaupunkitasoilla. Monien asiantuntijoiden mielestä tämä ei kuitenkaan riittäisi reititystaulujen koko-ongelmaa ratkaisemaan.

Uusimmilla tekniikoilla Internet-numeroiden muutos on periaatteessa tehtävä vain BOOTP- tai DHCP-palvelimeen ja DNS-palvelimen tietokantaan. Hankalammaksi muutoksen tekee se, että kaikkia isäntäkoneita ei sammuteta ja käynnistetä päivittäin. Katkaiseminen keskeyttää myös sähköpostitoiminnon ja TCP-yhteydet. Uudelleen käynnistys on monessa ta-pauksessa ainoa vaihtoehto, mutta se edellyttää tarkkaa vaiheistusta alasajossa, jotta puhtaalta pöydältä aloittaminen onnistuisi hyvin.

DNS-palvelimilla on kopioita reititystiedoista välimuistissa ja muissa palvelimissa. Näiden tietojen kiertoa voi tosin nopeuttaa asettamalla TTL pieneksi. Varsinaisen ongelman muodostavat ne vääräoppiset sovellukset, jotka käyttävät suoraan Internet-osoitteita.

Ehkä tulevaisuus tuo tullessaan sovelluksen, jolla Internet-osoitteet voi muuttaa ‘lennosta’ ja jolla voi säilyttää vanhan ja uuden osoitteen kenties pysyvästikin, mikä takaisi usean operaattorin käyttömahdollisuuden.

4.3.3. CIDR ja reititysprotokollat

Osoitteiden yhdistäminen edellyttää, että myös reititysprotokollat hallitsevat yhdistämisen joko puoliautomaattisesti tai kokonaan ja että ne lisäksi tuntevat yliverkkokäsitteen. BGP-3 ei vielä tuntenut tätä, mutta BGP-4 tuntee ja lisäksi sen päivitysviestissä on CIDR:n kannalta välttämätön tieto Internet-osoite-etuliitteen pituudesta ja sen tarvitsemien oktettien lukumäärästä. BGP-4:ssä on myös jaettu etuliitteitten yhdistämistä varten AS-väylä kahteen osaan: järjestettyyn listaan AS-jono ja järjestämättömään AS-joukkoon. AS-jonoa käytetään väylän valintaan polun pituutta laskettaessa. Molempia osia käytetään silmukoiden torjuntaan. Yhdistäjä- ja atominen-yhdistys-atribuutit sallivat AS:n välittävän rajatun kuvan topologiastaan naapureilleen. Sisääntuloreititin asettaa itseensä liittyvän paikallisen valinta-atribuutin, jota sisäiset reitittimet käyttävät väylän valintaan.

Yhteys-voimassa- ja päivityspakettien välisen sallitun aikaeron määrittelee odotusaika (hold time). Sen avulla voidaan säädellä BGP:n synnyttämää liikennettä. Erityisesti julkisissa kytkentäisissä verkoissa kustannukset pienenevät, kun yhteyden annetaan katketa silloin, kun liikennettä ei ole.

Kun ulkoinen reititysprotokolla päivitetään uudempaan versioon, kaikki AS:n reunareitittimet on päivitettävä kerralla. Jos kauttakulkuverkossa on käytössä BGP-3, niin BGP-4:llä yhdistetyt osoitteet on purettava (de-aggregation). Purku on tehtävä hallitusti ja mielellään vain rajatuille reiteille, muuten purettaessa voi syntyä enemmän osoitteita kuin niitä alunperin yhdistettiin. Saatu väylä ei ole myöskään välttämättä lyhin, mutta silmukattomuus on sittenkin tärkeämpi ominaisuus. Näillä rajoituksilla BGP-3 ja BGP-4 voivat vastaanottaa toisiltaan tavoitettavuustietoja. EGP on nykyään lähinnä käytössä yhden operaattorin hoitamissa tynkä-AS:issä ja silloin riittää vain yhden oletusreitin ilmoitus.

Sisäisistä reititysprotokollista RIP-2, OSPF, IS-IS ja EIGRP osaavat käsitellä aliverkkopeitteitä, jotka eroavat CIDR:n yliverkkopeitteistä vain bittien määrän suhteen. Jos BGP-4:llä on valittavanaan useampia yhdistettyjä reittejä, jotka ovat osin päällekkäisiä, nyrkkisääntönä on pitemmän etuliitteen väylän valinta.

4.4. Reitityspolitiikka

Reitityspolitiikka käsittelee muita kuin lyhintä polkua painottavia reitin valinnan piirteitä, kuten esimerkiksi palvelun laatua ja käyttäjien karsintaa. Käsite on syntynyt Internetin kaupallistumisen myötä.

4.4.1. Operaattorin valinta

BGP kykenee vertailemaan eri operaattoreiden tarjoamia reittejä vain kun operaattoreihin on suora kytkentä. Kun käyttäjät liittyvät Internet-operaattorin verkkoon alueverkon kautta, BGP pystyy jakamaan käyttäjille saapuvan liikenteen näiden itse valitsemien operaattoreiden kautta, mutta käyttäjiltä lähtevä liikenne on ohjattava alueverkosta yhden ‘oletusoperaattorin’ verkon läpi.

Yksinkertainen ratkaisu edellä mainittuun ongelmaan on virtuaalilinkin perustaminen käyttäjän ja operaattorin välille. Kun käyttäjän reunareititin koteloi sisältä vastaanottamansa IP-paketin uuteen IP-pakettiin, se pystyy ohjaamaan sen haluamansa operaattorin reunareitittimelle, joka purkaa ‘ulkokuoren’ ja lähettää alkuperäisen paketin edelleen. Haittana on ylimääräisen otsakkeen tuoma ‘hukkakuorma’ ja reunareitittimien kasvanut työmäärä.

IETF:n lähdereititysprotokolla SDRP suo lähettävälle solmulle erikoistapauksissa mahdollisuuden valita reitti välittämättä kauttakulkualueiden yleisistä reitityspäätöksistä. Reititinkohtaisen väylän valinnan hoitavat AS:t. Lähdereititys on itse asiassa ylemmän tason aluereititystä (domain routing). Lähdereititysotsake on verraten monimutkainen, sillä SDRP:ssä on panostettu mm. virheenkorjaukseen ja väylätukeen. Tulevaisuudessa protokollaan lisättäneen

proseduuri, jolla etappireitittimet pystyvät muistamaan lähdereitin. Kotelointia on käytettävä varoen, sillä sitä käytettäessä ohitetaan tavallinen reititys ja hallinta.

4.4.2. IDPR-lähestymistapa

Internetin huikean koon johdosta on solutason reititystä alettu korvata aluereitityksellä. Eräs esimerkki on IETF:n Alueiden välinen valintareititysprotokolla IDPR, joka on nykyään vähän käytetty. Se perustuu linkintilatekniikkaan ja on monimutkainen. IDPR:ssä solmujen reititystiedot yhdistetään AS-tasolla ja reititys käsittelee vain AS:ien välisiä linkkejä. Protokollalla on objekteina alue eli AS ja virtuaaliyhdyskäytävä, joka koostuu AS:iä yhdistävistä valinta-yhdyskäytävistä (policy-) eli reunareitittimistä. Tietokannassa on tiedot virtuaalikäytävien toimintakunnosta ja alueiden kauttakulkukonfiguroinnista eli käyttörajoituksista, laadusta ja hinnasta. OSPF:ää vastaava tulvaprotokolla on voitu tehdä yksinkertaiseksi, sillä elinaikaparametri on IDPR:llä paljon pidempi. Koska IDPR:n reitittimet sijaitsevat hyvin hajallaan eri organisaatioden alaisuudessa, on tulvaprotokollassa digitaaliseen nimikirjoitukseen pohjautuva autentikointi.

IDPR laskee reitit pyynnöstä. Lyhimmän polun algoritmi on helppo muuntaa sellaiseksi, että se ottaa huomioon linkin valintaperusteet. On hyvä huomata, että valintareitin laskenta vaihtelee eri osissa verkkoa. Valintayhdyskäytävät välittävät julkiset rajoitukset kaikille reittipalvelimille, mutta paikalliset verkon hoitajat pitävät omat valintaperusteensa usein salaisina. Näin ollen eri reittipalvelimilla on erilainen kuva verkosta. Hyvä puoli tässä on tietokannan tilan säästö, rajoituksena se, että reittejä ei voida laskea etappikohtaisesti vaan lähettäjäpohjaisesti.

4.4.3. Valintareitityksen tulevaisuus

Valintareititys ei kirjan ilmestymisen aikoihin ollut levinnyt koekäyttöä laajemmaksi. IDPR on yhtä monimutkainen kuin OSPF ja BGP yhteensä. Sen väylät poikkeavat Internetin päästäpäähän periaatteesta, tosin oikeastaan perustellusti, sillä koko väylätiedon lähetys joka paketissa olisi raskasta. Reitin laskennan ja paketin lähetyksen erottaminen eri laitteisiin on mielenkiintoinen piirre. Kun tietokoneet hoitavat laskennan, sitä on helppo muuttaa ja tehoa lisätä. Valintareititys toteutettaneen tulevaisuudessa IDPR:n ja SDRP:n sekamuotona.

5. Uusia kehityssuuntia

5.1. Monilähetys

5.1.1. IP-monilähetyksen hyödyt

IP-monilähetystä on ensimmäiseksi käytetty laitteiden löytämiseen paikallisverkoista. Kun OSPF reititin haluaa saada selville muut paikallisreitittimet, se lähettää vain yhden hello-viestin ‘yleis-OSPF-reititin’-osoitteeseen. ‘Yleis-RIP’-osoite toimii samoin. Monilähetys voidaan laajentaa paikallisverkkojen ulkopuolellekin. Se on kuitenkin hoidettava huolella, jottei syntyisi silmukoita tai suoranaisia monilähetysviestien lumivyöryjä, jotka voivat hyvinkin tukkia koko verkon. TTL-parametrilla rajaamalla voidaan monilähetysviesteillä etsiä mm. lähin nimipalvelin.

Monilähetys on yksinkertainen ja vähentää liikenteen määrää, sillä pisteestä pisteeseen-lähetykseen verrattuna jokaiselle linkille lähetetään vain yksi paketti. Tiedostojen monilähetys odottaa kuitenkin vielä tänä päivänä tiedostojen monilähetysprotokollan kehittämistä.

Kolmas tärkeä sovellusalue on multimediakokoukset, joita esimerkiksi IETF on käyttänyt. Tehokkaat työasemat digitoivat ja pakkaavat ääni- ja videosignaalit ja lähettävät ne UDP-paketteina konferenssin IP-osoitteeseen. Kuuntelijat pyytävät itselleen tähän ryhmäosoitteeseen lähetetyt paketit. Monelta-monelle-kokoussovelluksissa on lisäksi käytössä yhteinen kirjoitustaulu. Tällöin on monessa mielessä kyse monilähetyksestä: monimedia, monta vastaanottajaa ja lähettäjää. Varsinkin suuressa osallistujajoukossa on eriaikaisia liittyjiä ja poistujia. Monilähetyksellä ja ryhmäosoitteilla tietoliikenne on selvästi kevyempää kuin, että jokaisen osallistujan sisääntulo ja poistuminen olisi signaloitava erikseen.

5.1.2. Monilähetysreititys

Tulviminen on yksikertaisin monilähetysreititystapa. Vastaanottaessaan paketin reititin tarkistaa äskettäin saapuneitten listaaltaan, onko kyseessä ensilähetys vai uusinta. Jos kyseessä on ensilähetys, niin reititin lähettää paketin edelleen kaikille naapureilleen paketin lähettäjää lukuunottamatta. Tämä menetelmä on yksinkertainen ja toimiva. Se ei tarvitse reititystaulua, mutta lähetettyjen lista vaatii muistia ja kaikkien väylien käyttö kuluttaa siirtokapasiteettia.

Virittäjäpuu-tekniikka muodostaa silmukattoman verkon valituista linkeistä, jotka yhdistävät jokaisen solmun muihin vain yhtä yhteyttä pitkin. Kun virittäjäpuu on luotu, pakettien monilähetys on yksinkertaista. Tämäkin menetelmä on toimintavarma, eikä se kuluta paljoa muis-

tia. Se ei kuitenkaan sisällä ryhmäjäsenyyttä ja keskittää liikenteen vain valituille väylille, mikä voi synnyttää estoa.

Vastaväylälähetys RPF käyttää reititystaulua ja luo lähettäjäkohtaiset virittäjäpuut. Jos paketti on saapunut lähettäjälle johtavaa lyhintä polkua pitkin, se lähetetään edelleen kaikkia muita käytössä olevia väyliä pitkin. Pienellä reititystaulun lisäyksellä saadaan selville onko oma solmu lähettäjän ja naapurin lyhimmän polun etappi. Jos ei ole, niin pakettia ei kannata välittää naapurille. Pelkkään virittäjäpuureititykseen nähden verkon liikenne jakautuu tasaisemmin, mutta ryhmäjäsenyys puuttuu ja paketit yksinkertaisesti tulvivat koko verkkoon. MBONE:ssa on käytetty tulvi ja karsi-versiota, jossa ensimmäinen paketti tulvii läpi verkon. Ne solmut, jotka eivät ryhmään kuulu palauttavat tästä tiedon ja karsivat itsensä lähetyslistalta. Samoin reitittimet pitävät kirjaa siitä karsivatko niiden kohdesolmut itsensä listalta. Tämä on hyvin työlästä, sillä ryhmäjäsenyydet vaihtelevat nopeasti.

Ydinpuureitityksessä CBT valitaan monilähetysryhmän ydinjäsen, jolle muut ilmoittautuvat. Ryhmän liikennettä välittävät reitittimet pitävät kirjaa kyseisen ryhmän yhteyksistä. Näin syntyy yksi ryhmäkohtainen virittäjäpuu, RPF:n lähettäjä- ja ryhmäkohtaisia puita ei tarvita. Tällöin kaikki polut eivät ole kuitenkaan välttämättä optimaalisia. Suuri etu on lähetysten rajaaminen vain ryhmän jäsenille. Virittäjäpuun käyttöön perustuvana ydinpuumenetelmä ei tarvitse minkäänlaisia reititystaulukoita.

5.1.3. Kokeellinen monilähetysrunkoverkko

Kokeellisella monilähetysrunkoverkko MBONE:lla on testattu Internetin monilähetyskelpoisuutta varsinaisia standardeja odoteltaessa. Tämä edellytti tunneloinnin ja oman reititysprotokollan käyttöä. Tunnelointia tarvitaan, jos väylän varrella on reitittimiä, jotka eivät tunne monilähetystä. MOBNE-reitittimet selvittävät yksinkertaisella DVMRP:llä vastaväylälähetyksen käyttämät vastaväylät. Elinaikalaskurilla rajataan monilähetys organisaatioon, alueeseen tai maanosaan. MBONE:n ensimmäisessä versiossa ryhmänjäsenyys tutkittiin vain virittäjäpuun lehtitasolla, mikä aiheutti paljon turhaa liikennettä.

MBONE on osoittautunut varsin arvokkaaksi monilähetyssovellusten testi- ja arviointivälineeksi. Audio- ja videokonferenssikokeilut ovat paljastaneet aivan ilmeisen tarpeen tällaiselle protokollalle. DVMRP:n epätarkkuus mm. tunnelien hinnoittelussa ja elinaikaparametrin asettamisessa on ollut haitta. Tunnelointi onkin vaihdettu kotelointiin. Videoliikenteen vaatima suuri kaistanleveys on osoittanut kaistanleveysrajoitusten ja resurssien varauksen tarpeellisuuden.

5.1.4. Internetin monilähetysstandardeja

IGMP oli pitkään Internetin ainoa monilähetysstandardi. Sittemmin OSPF:stä on kehitetty reitityksen tehokkuutta painottava AS:ään rajoittuva monilähetysversio MOSPF ja koko Internetille protokollariippumaton monilähetys PIM.

MOSPF täydentää OSPF:n linkintilatietokantaa ryhmäjäsenyystietueella, mistä seuraa se, että OSPF-reitittimet voivat laskea RPF ja karsinta-algoritmin ‘muistissa’ ilman, että niiden tarvitsisi turvautua tulvimiseen ensimmäistä pakettia lähettäessään. MOSPF on hyvin voimakas protokolla. Se edellyttää lyhimmän polun selvittämistä jokaiselle lähettäjä-ryhmä-parille jokaisen reitityspäivityksen jälkeen, mikä tekee laskennan raskaaksi. Vain pyynnöstä tehty laskenta saattaa olla ratkaisu tähän ongelmaan.

PIM:stä on kaksi versiota: tiheä ja harva. Ryhmä on tiheä, jos todennäköisyys sille, että jollain alueella on kyseiseen ryhmään kuuluva jäsen, on suuri. PIM käyttää RPF ja karsintamenetelmää, sillä tiheydestä johtuen karsintapakettien aiheuttama liikennemäärä verkossa jää pieneksi. PIM on DVMRP:tä yksinkertaisempi, koska se ei tarvitse reititystauluja. Se edellyttää vain, että reitittimet pystyvät muistamaan lähettäjä-ryhmäparin karsintaviestit. PIM olettaa, että käytössä on toimiva solmusta solmuun protokolla.

Harva PIM lähettää paketteja vain ryhmän jäsenille. Pienryhmien tulvalevitys tukkisi Internetin. Toiminta muistaa paljon ydinpuualgoritmia. CBT:n ‘kovatila’-päivitysten sijaan harva PIM luottaa liittymisilmoituksissa ‘pehmeätila’-päivityksiin: jos tiloja ei virkistetä tasaisin välein, ne hävitetään.

IGMP-tuki löytyy jo monesta TCP/IP-toteutuksesta ja useat reititinvalmistajat ovat lisänneet yksinkertaisen, mutta paljon laskentatehoa vaativan MOSPF-ominaisuuden reitittimiensä OSPF-osaan. Vaikka tiheä PIM:kin alkaa esiintyä uusissa verkkosovelluksissa, selvitettäviä asioita on useita, ennen kaikkea PIM:n MOSPF:n ja DVMRP:n yhteistoiminta. Ryhmien ja lähettäjien yhdistäminen CIDR:n tapaan voisi keventää harvaa PIM:iä.

5.2. Liikkuvuus

5.2.1. IP-liikkuvuuden tavoitteet

Kun tietokoneet pystyttiin rakentamaan tarpeeksi kevyiksi, syntyi kannettava tietokone, joka voidaan kytkeä siirron jälkeen tilapäisosoitteella verkkoon tai modeemin kautta matkapuhelimeen. Liikkuva tietokone pysyy kytkettynä myös siirrettäessä. Tekniikkana on käytetty pakettiradiota, jossa useat solmut jakavat rajatulla alueella eli solussa yhden radiokanavan, jonka pääasemalla on yhteys Internetiin. Liikkuessaan tietokone kuuntelee pääasemien ilmoituksia

ja valitsee niistä parhaiten kuuluvan. Pakettiradion ohella on käytetty myös hajaspektritekniikkaa ja varsinkin sisätiloissa radioaaltoja häiriösietoisempaa infrapunasiirtoa.

Kolmas liikkuvuuteen liittyvä käsite on liikkuva verkko. Autojen suuria kaapelimääriä yritetään korvata mini-LAN:eilla. Tietokoneverkkoja on jo käytössä lentokoneissa, laivoissa ja junissa. Kun sekä isäntälaite, että verkko voivat liikkua, on solmun paikan lisäksi jatkuvasti kyettävä muuttamaan reittiä sen luo.

IP-liikkuvuudelle on asetettu seuraavia vaatimuksia. Jotta TCP yhteys säilyisi, on IP-osoitteen oltava koko ajan sama. Liikkuvan isäntäkoneen tulee kyetä olemaan yhteydessä olemassaoleviin muihin isäntäkoneisiin, reitittimiin ja palveluihin. IP:n turvallisuus ei saa heiketä ja lisäksi tarvitaan vielä sijainnin suojaus ja monilähetyskelpoisuus.

5.2.2. Arkkitehtuuri ja sanasto

Liikkuvaan isäntäkoneeseen otetaan yhteys lähettämällä IP-paketit ensin erikoisreitittimeen, jota kutsutaan kotiosoitevälittäjäksi. Tämä tietää aina liikkuvan isäntäkoneen sijainnin ja lähettää seuraavaksi paketit tunneloimalla sen solun kanta-asemalle, jossa liikkuva isäntä parhaillaan on. Erityisesti on hoidettava niiden pakettien uudelleenreititys, jotka ovat matkalla soluun, josta liikkuva isäntä juuri poistui.

Koiranjalkareititykseksi kutsutaan sitä, että liikkuvaan isäntäkoneeseen on pitempi yhteys kuin päinvastoin, sillä ensimmäinen suunta kulkee aina kotiosoitevälittäjän kautta, mikä voi aiheuttaa pitkän ylimääräisen lenkin.

Jos isäntä liikkuu nopeasti ja leikkaa pian liikeratansa, voivat uudelleenreititysviestit aiheuttaa silmukan. Jos edellä mainituista viesteistä yksikin katoaa, liikkuva isäntä katoaa ns. mustaan aukkoon. Elinaikalaskurilla voidaan estää tällaiset virhetilanteet.

5.2.3. Protokollat ja sopimukset

Liikkuvia protokollia kehittäessään IETF:n työryhmä pyrki aina valitsemaan yksinkertaisimman ratkaisun. Vilkkuprotokollalla (Beaconing protocol) kanta-asemat kertovat olemassaolostaan säännöllisin väliajoin. Radiotaajuuksien rajallisuuden takia, tätä merkinantoa kannattaa minimoida. Monessa toteutuksessa liikkuvat isännät huomaavat vaihtaneensa solua tarkkaillessaan eri taajuuksien energiasignaalien eroja. Tällöin ne voivat pyytää kanta-asemailmoituksia yleisestä kanta-asemaosoitteesta ja saavat konekohtaisen vastauksen. Huomattuaan vaihtaneensa kanta-asemaa, liikkuva isäntä rekisteröityy uudelle asemalle, hankkii soluosoitteen ja ilmoittaa sen kotiosoitevälittäjälleen.

5.2.4. Muita hienouksia ja tulevaisuus

Kotiosoitevälittäjän hajauttaminen usealle reitittimelle toisi toimintavarmuutta liikkuvaan tiedonvälitykseen. Tavoitteena on, että liikkuvalla ja kiinteällä isäntäkoneella ei olisi mitään eroa ja toisaalta etteivät liikkuvan ja kiinteän verkon reitittimetkään eroaisi toisistaan.

Jos kanta-asemien niputetaan ryppäiksi, vain ryppäästä toiseen siirtymiset pitäisi ilmoittaa kotiosoitevälittäjälle. Solusta toiseen siirtymistä helpottaisi myös solujen ryhmittäminen aliverkoksi, jonka ulkopuolelle siirtyminen vasta aiheuttaisi olinpaikkailmoituksen ‘kotiin’. Toinen ratkaisu olisi paikallisen kotiosoitevälittäjän asettaminen alkuperäisen välittäjän ja kanta-asemien väliin. Solun vaihdot voitaisiin hoitaa paikallisesti.

Koiranjalkareitityksestä päästään varmalla tavalla eroon vasta autentikointimekanismien avulla. Hintana on kuitenkin liikkuvan isännän olinpaikan paljastuminen, joka ei ehkä aina jostain syystä ole suotavaa.

Liikkuvuus on hyvin lupaavaa. Ensimmäiset protokollat on varmuuden vuoksi tehty konservatiivisiksi. Seuraavan polven protokollat sisältänevät jo edellä esitettyjä parannuksia. Liikkuvuus asettaa myös aivan uusia vaatimuksia TCP:lle, esimerkiksi silloin, kun se yrittää mukauttaa tarjottua liikennettä havaitsemaansa estoon. Liikkuvien isäntäkoneiden aiheuttamia kuormituksen muutoksia on hyvin vaikeaa ennustaa lähimenneisyydestä.

5.3. Resurssien varaus

Internet-protokolla toimii datagrammi pohjalta. Paketit lähetetään ilman yhteyden muodostusta toisistaan riippumattomina. Verkko ‘tekee parhaansa’ takaamatta palvelunlaatua, mikä ei monen mielestä sovellu uusille multimediasovelluksille.

5.3.1. Jonot ja viiveet

Useimmat Internet-reitittimet palvelevat ensin saapuneet paketit ensin. Viiveen on osoitettu riippuvan verkon kuormasta ja tätä viivettä voidaan vähentää tehostamalla reititintä tai vähentämällä kuormaa. Kun IGRP:llä on tieto linkin kuormituksesta, voitaisiin OSPF:llä harkita linkin käytössä olevan kaistanleveyden huomioon ottamista linkkimetriikkaa arvioitaessa. Linkin kuormitus kuitenkin vaihtelee paljon nopeammin kuin mitä reititystaulujen uudelleen laskemiseen kuluu aikaa. Jotta verkon vakaus säilyisi, kuormituksen muutokset voidaan ottaa huomioon vain pitemmän aikavälin keskiarvoina.

Reitityksen muutos ‘kaikki-tai-mitään’-periaatteella aiheuttaisi kuormituksen jyrkkiä heilahteluja. Ainoa järkevä vaihtoehto onkin turvautua yhtä pitkiä väyliä tukeviin protokolliin, jotka

sallivat kuormituksen asteittaisen siirron vapaammalle väylälle. Vapaampaa reittiä etsittäessä on lisäksi huomattava varoa pakettien ohjaamista vapaammalle väylälle, joka on pitkä kiertotie. Tällöin verkon kokonaiskuormitus vain kasvaisi.

Internetissä tukkeutumista vähennetään TCP:n ‘tukkeutumisikkunalla’ ja hitaalla lähdöllä. Paketteja lähetetään aluksi harvakseltaan ja nopeutta lisätään vähitellen, kunnes mahdollisessa estotilanteessa lähetysnopeutta jälleen vähennetään. Tämän menetelmän reiluutta vähentää se, että päästä-päähän-algoritmi on hyvin riippuvainen verkon vastausajasta. Toiminta perustuu myös kaikkien käyttäjien oletettuun yhteistoimintaan: luotetaan siihen, ettei kukaan ‘syö kuormasta’. Alussa todettiin, etteivät käyttäjät saisi liikaa luottaa verkkoon. Nyt havaitaan, ettei verkkokaan saa mielin määrin luottaa käyttäjiinsä.

5.3.2. Jonotus ja vuoron jako

Reilu jonotus perustuu reitittimeen tulevan liikenteen voihin jakoon ja siirtokapasiteetin tasaiseen jakoon voiden kesken. Jokaiselle vuolle varataan oma jono ja vuorotus hoidetaan round robin-periaatteella. Vuojako ei kuitenkaan ole aivan helppoa IP-verkossa. Pelkkä lähettäjäperusteinen jako antaa yhdelle työasemalle saman osuuden kuin monia päätteitä palvelevalle keskustietokoneelle. TCP-yhteyksiin perustuvassa jaossa on tutkittava paketin sisältö. IP-otsakkeessa ei ole tätä tietoa. Lähettäjä/kohde-jako poistaa useita yhteyksiä hoitavien keskustietokoneiden aliedustuksen, mutta moniyhteyksiset yksittäiset tietokoneet saavat liian suuren osuuden siirtokapasiteetista. Lisäksi lähettäjä/kohdepareja voi olla erittäin paljon. Jakamalla saapuva liikenne satunnaisesti rajatulle määrälle jonoja tämän ongelma poistuu.

Painotettu reilu jako on oikeudenmukaisempi menetelmä. Se perustuu virtuaalikellon käyttöön. Jokaiselle vuolle määritellään virtuaalikello, jonka arvoa jokainen kyseisen vuon saapuva paketti kasvattaa arvolla, joka saadaan, kun paketin pituus jaetaan virtuaalilinkin nopeudella. Kun paketit lähetetään virtuaalikelloaikojen mukaan nousevassa järjestyksessä alinopeutta käyttäneet yhteydet voivat myöhemmin käyttää keskimääräistä nopeuttaan suurempaa siirtokapasiteettia ja päin vastoin. Sopivan tarkkailuaikavälin valinta on tärkeää. Ylimääräisellä virtuaalikellolla voidaan vielä estää yhteyksiä keräämästä itselleen liikakapasi-teettia olemalla pitkään hiljaa. Muutoin nämä yhteydet voisivat purskeillaan tukkia koko yhteyden.

Runkoverkkoliittymissä vuorottelu voidaan hoitaa liityntälinkkien mukaan. Tarvittaessa liityntäliikenne voidaan edelleen jakaa protokollan, tietokoneluokan tai sovelluksen mukaan. Protokollat käyttäytyvät kuitenkin hyvin eri tavoin. Kohtelias TCP antaa ystävällisesti muille tilaa. Kiinteiden osuuksien jako on tässä tarpeen. Sovellusprofiilipohjainen jako tosiaikaisiin, eräajo- ja keskusteleviin sovelluksiin on oikeudenmukainen. Luokkapohjainen jako CBQ

jakaa sovellukset hierarkisesti: ylimmällä tasolla ovat verkkoprotokollat ja niiden alla muut sovellukset. Vuorot jaetaan virtuaalikellojen tapaan.

Äskettäin on osoitettu, että kun rajoitettu pakettivuo saa kohtuullisen palvelun, sen viive on hyvin rajattu. Viive ei perustu topologiaan, eikä lähteen käyttäymiseen vaan välittävien reitittimien aiheuttamaan värinään. Vuotavan ämpärin-menetelmä ei riitä vuon hallintaan. Palvelulaadun tarvitsema kapasiteetin varaus edellyttää pääsynhallintaa. Tarvittava kapasiteetti voidaan varata takuuvarmaa palvelua varten, jolloin muiden lähteiden käyttäyminen ei vaikuta omaan palveluun, tai ennustavalle palvelulle, joka arvioi todennäkoisen resurssitarpeen äsken koetun liikenteen pohjalta.

5.3.3. Resurssien varausprotokolla

Toisin kuin aikaisemmat resurssien varausprotokollat, kuten ST-2, RSVP ei luo virtuaalikanavaa. RSVP-viestit lähetetään rinnakkain IP-pakettien kanssa. RSVP:n perusoletus on, että resurssien varausta tarvitsevat lähinnä monilähetyssovellukset kuten videosiirrot. RSVP:tä ei ole myöskään sidottu mihinkään reititysprotokollaan, sillä ne kehittyvät koko ajan. Tämä pitää paikkansa varsinkin monilähetysprotokolliin nähden. RSVP selvittää automaattisesti sen vuon reitin, jolle varausviestit voi lähettää. Kolmas periaate on pehmeän tilan käyttö: varaukset uusitaan varmuuden vuoksi säännöllisin välein. Resursseja varataan mm. päästä-päähän-viivettä ja keskimääräistä bittinopeutta varten. Pääsynhallintaa tarvitaan siltä varalta, ettei verkko pysty täyttämään käyttäjän palvelunlaatuvaatimuksia.

RSVP joutuu mukautumaan verkon muuttuviin reitteihin. Istuntojen lähettävät osapuolet lähettävät säännöllisin väliajoin polkuviestejä kohteeseen. Kun reititystaulua muutetaan, uusitaan polkuviestit. Kun polku on luotu, voivat vastaanottajat lähettää varausviestit. Polkuviestien aikaväli on selvästi pienempi kuin varausviestien, jottei joidenkin polkuviestien katoaminen katkaisisi luotua polkua. Jonkinlainen valinta- tai erikoisreititys on ilmeisesti tarpeen, jottei esimerkiksi hieman parempien reittien avautumisen johdosta tarvitsisi aina varata uutta RSVP-polkua. Liikkuvuus luo tietysti vielä aivan omat haasteensa resurssien varaamiselle.

5.3.4. Tarvitaanko kapasiteetin varausta?

Datagrammiverkossa lähetettyjen pakettien vasteajat vaihtelevat. Paketit voivat kulkea eri reittejä pitkin ja samaa reittiä etenevät paketit voivat joutua reitittimissä eri jonoihin. Tätä verkon aiheuttamaa värinää voidaan kompensoida jälleensynkronoinnilla, eräänlaisella vastaanoton viiveellä, joka perustuu joko maksimiviiveeseen tai tilastolliseen arvioon verkon viiveestä. Äänen siirto-ohjelma ‘vat’ pohjautuu äänen epäjatkuvuuteen. Taukojen aikana voidaan laskea uusi maksimiviive ja näin voidaan mukautua vaihteluihin.

Aiemmin uskottiin, että video- ja äänilähetykset vaatisivat kiinteän kaistanleveyden, mutta digitaalista materiaalia voidaan muokata esimerkiksi vaihtelemalla tiivistämistä. Kun tavallinen puhelinlinja varaa 64 kbps PCM kaistan, GSM:llä päästään jo 13 kbps tiivistykseen ja sotilaspuhelimilla jopa 2,4 kbps kaistan leveyteen.

Jotta lähetykset voitaisiin mukauttaa verkon kulloiseenkin kapasiteettiin, on vastaanottajien ilmoitettava kokemansa siirron laatu ja mahdolliset virheet. Monilähetyksissä voidaan satunnaisotannalla saavuttaa luotettava kuva verkon tilasta ilman liian suurta ilmoitusten määrää. Matemaattisella analyysillä voidaan arvioida pakettihäviöiden korvaamiseen tarvittava reservikapasiteetti. Matemaattisesti voidaan myös osoittaa, että jos niin sanottu tyytyväisyysfunktio on ‘konveksi’, niin mitä useampi käyttäjä jakaa käytettävän kapasiteetin, sitä suurempi on kokonaistyytyväisyys - tiettyyn rajaan asti.

Tarvittavaan kaistanleveyteen perustuva laskutus on vastoin tämän päivän Internetin periaatteita. Se vaatisi käyttäjien tunnistamisen digitaalisilla allekirjoituksella ja myös käyttäjän ja välittävien operaattorien väliset sopimukset.

5.4. Kohti uutta IP:tä

Internetin suurimmat muutokset tähän asti ovat olleet jako aliverkkoihin, Internetin organisointi autonomisiin alueisiin ja reitityksen erottelu sisäiseen ja ulkoiseen. Suurimmat uhat viime aikoina ovat olleet B-luokan osoitteiden ehtyminen, reititystaulujen räjähdysmäinen kasvu ja osoiteavaruuden loppuun kuluminen. Pääsyy on ollut tavattoman nopea kasvu, Internet on uhannut joutua menestyksensä uhriksi.

Internet on kuitenkin osoittautunut hyvin elinkelpoiseksi. CIDR ratkaisi B-luokan osoiteongelman. BGP-4:n reititystaulujen yhdistäminen poisti toisen uhan. Kolme vuotta sitten Internetiin oli kytketty 2’500’000 tietokonetta. Osoiteavaruutta on hyödynnetty tehottomasti. On arvioitu, että vain 5 % varatusta avaruudesta on todella käytössä. Vaikka käyttäjämäärä kaksinkertaistuisi vuosittain, osoitteita riittäisi vielä vuonna 1999. CIDR tehostaa jo osoiteavaruuden käyttöä, mikä antaa lisäaikaa. Selvää kuitenkin on, että uusi IP tarvitaan. Sen kehittämiseen on silti kohtuullisesti aikaa jäljellä.

IP:n korvaajaksi on ehdotettu OSI:n CLNP:tä, jolla on tarpeeksi laaja osoiteavaruus. Kehitys on kuitenkin auttamatta ajanut sen ohi. Internetin piirissä on kehitetty IP:lle useita seuraajaehdokkaita. Pip sisältää hyvin tehokkaan ‘reititysdirektiivi’-listoihin perustuvan reititysstrategian, joka mahdollistaa valintareitityksen ja helpottaa monilähetystä. Yksinkertaisessa IP:ssä SIP:ssä on 64-bitin soitteen pituus ja se poistaisi useita IP:n vanhentuneita piirteitä. Se käyttää kotelointia valintojen sijasta ja tekee pakettien jaosta valinnaisen.

Syksyllä -93 Pip:n ja SIP:n parhaat ominaisuudet yhdistettiin SIPP:ksi, joka puolestaan otettiin seuraavana vuonna uuden IP:n Ipv6:n pohjaksi. Samalla osoitteen pituus kasvatettiin 128 bittiin, joka helpottaa autokonfiguraatiota. Uusi IP aiheuttaa luonnollisesti muutoksia myös mm. OSPF:ään, BGP:hen ja SNMP:hen.