Tampereen yliopisto

Esa Karjalainen

AIKOMUSLÄHTÖISET VERKOT TIETO-VERKKOJEN KONFIGUROINNISSA

IBN-sovellukset yritysverkoissa

Informaatioteknologian ja viestinnän tiedekunta
Kandidaatintyö
Toukokuu 2023

TIIVISTELMÄ

Esa Karjalainen: Aikomuslähtöiset verkot tietoverkkojen konfiguroinnissa – IBN-sovellukset yritysverkoissa
Tampereen yliopisto
Tieto- ja sähkötekniikan tutkinto-ohjelma, Tietotekniikka
Kandidaatintyö
Toukokuu 2023

Aikomuslähtöiset verkot ovat tietoverkkoparadigma, jonka tarkoituksena on suoraviivaistaa verkon konfigurointia ja ylläpitoa. Tietoverkkotekniikan viimeaikaisista kehityksistä huolimatta verkkolaitteiden konfigurointi on edelleen hyvin työlästä. Verkkoliikenteen määrän kasvaessa ja tietoverkkojen loogisen rakenteen monimutkaistuessa on uuden abstraktiotason kehittäminen välttämätöntä. Tässä työssä tutkitaan aikomuslähtöisten verkkojen soveltuvuutta yritysverkkojen toteuttamiseen.

Työ toteutettiin kirjallisuustutkielmana ja se on jaettu kolmeen osaan. Ensimmäisessä osassa käsitellään ohjelmisto-ohjattujen verkkojen toimintaperiaatteita, sillä aikomuslähtöiset verkot on kehitetty ohjelmisto-ohjattujen verkkojen pohjalta keskittyen näiden puutteisiin konfiguroinnissa. Toisessa osassa käydään läpi aikomuslähtöisten verkkojen periaatteita ja toteutuksia sekä sitä, miten nämä vaikuttavat tietoverkkojen toteuttamiseen. Kolmannessa osassa esitellään yritykselle tyypillisen verkon rakennetta ja vaatimuksia. Lisäksi osassa tarkastellaan, kuinka aikomuslähtöiset verkot voivat tuoda lisäarvoa yritysverkkoon tukien yrityksen tavoitteita. Työssä ei käsitellä perinteisten tietoverkkojen historiaa tai puutteita, koska aikomuslähtöisten verkkojen parannuskohdat ohjelmisto-ohjattuihin verkkoihin pätevät myös perinteisten tietoverkkojen kohdalla.

Yritysverkkoja täytyy pystyä hallitsemaan tarkasti yritysten erityisiä vaatimuksia mukaillen. Ohjelmisto-ohjatut verkot ovat helpottaneet tätä perinteisten tietoverkkojen ongelmaa keskittämällä verkon loogisen hallinnan erityiselle ohjainlaitteelle. Parannuksista huolimatta ohjelmisto-ohjatuissa verkoissa verkon tilan mukauttamisessa ja ylläpidossa on kehitettävää. Tästä syystä tekniikan kehitys on johtanut aikomuslähtöisten verkkojen kehittämiseen. Aikomuslähtöisten verkkojen tekniikka pyrkii suoraviivaistamaan tietoverkkojen monimutkaiset konfiguraatiotoimenpiteet kehittämällä niille sopivan abstraktiotason. Konfiguraation abstraktiotaso tekee aikomuslähtöisestä verkosta erityisen soveltuvan yritysverkon toteuttamiseen, sillä se myötäilee yrityksen korkean tason toimintamalleja sekä -tavoitteita.

Avainsanat: aikomuslähtöiset verkot, IBN, ohjelmisto-ohjatut verkot, SDN, verkonhallinta, yritysverkot

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

SISÄLLYSLUETTELO

1. JOHDANTO 1
2. TUTKIMUSMENETELMÄ 3
3. OHJELMISTO-OHJATUT VERKOT 4
3.1 Tausta 4
3.2 Tietotaso 5
3.3 Ohjaustaso 6
3.4 Teknologian haasteet 7
4. AIKOMUSLÄHTÖISET VERKOT 8
4.1 Aikomus 8
4.1.1 Aikomuksen tilakone 10
4.1.2 Aikomuspuu 11
4.2 Konfiguraation abstraktiotaso 13
4.3 Tietoturvasovellukset 14
4.4 Teknologian haasteet 15
5. IBN-TOTEUTUKSET YRITYSVERKOISSA 16
5.1 Yritysverkkojen vaatimukset 16
5.2 Yrityksen toimintasuunnitelma 17
5.3 Yritysverkkojen tietoturva 18
5.4 IBN-verkkoon päivittäminen 19
6. YHTEENVETO 20
LÄHTEET 22

LYHENTEET JA MERKINNÄT

API	Application Programming Interface, ohjelmointirajapinta
IBN	Intent-Based Networking, aikomuslähtöiset verkot
IoT	Internet of Things, esineiden internet
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
NBI	Northbound Interface, pohjoinen rajapinta
NFV	Network Functions Virtualization, verkkofunktioiden virtualisointi
NLP	Natural Language Processing, luonnollisen kielen käsittely
ONOS	Open Networking Operating System
SBI	Southbound Interface, eteläinen rajapinta
SDN	Software-Defined Networking, ohjelmisto-ohjatut verkot
WAN	Wide Area Network, laaja alueverkko

1. JOHDANTO

Internetissä välitetyn tiedon määrä jatkaa eksponentiaalista kasvuaan. Tämä johtuu digitalisaation yleistymisestä arkielämässä, uusista Internet-sovelluksista ja käyttäjämäärien kasvusta. Esimerkiksi esineiden Internet (engl. Internet of Things, IoT) on käsite, johon liittyvien teknologioiden kehittyminen on viimeisinä vuosina vaikuttanut merkittävästi tietoverkkotekniikalta vaadittuihin ominaisuuksiin.

Tietoliikenteen määrän kasvu ja uudet teknologiat luovat uusia vaatimuksia yritysverkoille. Verkkoja on kyettävä skaalamaan helposti, toimintavarmasti ja kustannustehokkaasti, sekä käyttämään uusia tekniikoita joustavasti. Yritysverkkojen on oltava myös suorituskykyisiä ja turvallisia, sekä niiden toimintaa on kyettävä ketterästi mukauttamaan yrityksen tavoitteita ja toimintaperiaatteita tukeviksi.

Kasvaneisiin vaatimuksiin on kehitetty ohjelmisto-ohjatut verkot (engl. Software-Defined Networking, SDN), joka laajentaa perinteisen tietoverkkoarkkitehtuurin ohjelmoitavuutta. SDN-arkkitehtuurilla voidaan toteuttaa hyvin skaalautuvia ja vikasietoisia verkkoja, joiden mukauttaminen on arkkitehtuurin ohjelmoitavuuden ansiosta helpompaa, kuin perinteisten tietoverkkojen tapauksessa.

Vaikka SDN-verkkoarkkitehtuuri edesauttaa tietoverkkojen hallintaa, keskittyy arkkitehtuuri pääasiassa verkon tiedonvälityksen kehittämiseen [1]. Ohjelmisto-ohjatut verkot eivät korjaa konfiguraatioiden monimutkaisuutta ja abstraktiotason puutetta. Tämä voi aiheuttaa ongelmia verkon tarkoituksenmukaisen tilan saavuttamisessa ja ylläpidossa. Lisäksi tulevaisuuden kehityksen ja ongelmanratkaisun kannalta on tärkeää kehittää ja laajentaa verkkojen palauteominaisuuksia [1]. Palauteominaisuuksilla tarkoitetaan verkko-operaattoria informoivia menetelmiä, kuten tehtyjen toimenpiteiden dokumentointia. Nykyinen matalatasoinen malli voi aiheuttaa ongelmia korkeamman tason mallien kanssa.

Ratkaisuksi ohjelmisto-ohjattujen verkkojen konfigurointiin on ehdotettu aikomuslähtöistä tietoverkkoa (engl. Intent-Based Networking, IBN), jonka avulla voidaan toteuttaa tietoverkon konfigurointia yksinkertaistava abstraktiotaso. Tässä tutkielmassa tarkastellaan IBN-tekniikan tuomia hyötyjä ohjelmisto-ohjattujen verkkojen käyttöympäristöihin ja konfiguraatioon, erityisesti kasvavien yritysverkkojen näkökulmasta.

IBN mahdollistaa ohjelmisto-ohjattujen verkkojen konfiguroinnin korkeamman abstraktiotason avulla [2]. Verkko-operaattori määrittelee verkolle konkreettisia tavoitteita, jotka verkko osaa toteuttaa itsenäisesti jakamalla tavoitteen matalamman tason tehtäviksi ja

suorittaa laitteiden konfiguroinnin. Jos tavoitteena on tietyn verkkoliikenteen priorisointi verkossa, IBN suorittaa vaaditut muutokset automaattisesti ja monitoroi verkon tilaa, jotta tavoite toteutuu myös tulevien muutosten jälkeen. IBN on tärkeä tekniikka, koska verkkolaitteiden määrän kasvaessa ja verkon loogisen rakenteen monimutkaistuessa tulee manuaalisesta konfiguroinnista aina vaikeampaa.

Tässä tutkielmassa sivutetaan perinteisten tietoverkkojen historia, joka on johtanut ohjelmisto-ohjattujen verkkojen kehitykseen. Tämän sijaan tutkielmaa pohjustetaan SDN-verkkojen tekniikalla, koska IBN-tekniikan parannuskohteet SDN-verkoissa pätevät myös perinteisten tietoverkkojen ongelmiin. Tutkielmassa keskitytään SDN-tekniikan puutteisiin konfiguraatiossa ja IBN-tekniikan esittämiin ratkaisuihin.

Tutkielman kolmannessa luvussa esitellään tiiviisti SDN-tekniikan toimintaperiaatetta, sekä sen kehittämiseen johtaneita tekijöitä ja vaatimuksia. Luvun lopussa käydään läpi tekniikan puutteita ja haasteita, jotka ovat johtaneet kysyntään IBN-tekniikalle. Luvussa 4 esitellään IBN-tekniikkaa ja sitä, miten IBN ratkaisee aiemmassa luvussa esiteltyjä konfiguraatio-ongelmia. Luvussa tarkastellaan myös IBN-tekniikan kehityssuuntaa ja pohditaan sen tulevaisuuden asemaa tietoverkkojen konfiguroinnissa. Tutkielman luvussa 5 perehdytään IBN-tekniikan soveltuvuuteen yritysverkoissa.

2. TUTKIMUSMENETELMÄ

Tutkielma toteutettiin kirjallisuuskatsauksena. Lähdeaineistoa etsittiin Tampereen yliopiston Andor hakupalvelusta, sekä ACM Digital Library, IEEE Electronic Library, SpringerLink ja ScienceDirect tietokannoista. Suomenkielistä tutkimusta aikomuslähtöisistä verkoista ei löytynyt, joten tiedonhaku kohdennettiin englanninkielisiin aineistoihin.

Hakusanoina käytettiin pääasiassa termejä ”intent-based networking”, ”software-defined networking” ja ”enterprise networks”. Lisäksi hauissa hyödynnettiin kontekstisanoja, kuten ”security”. Käytettyjä hakusanoja yhdisteltiin myös Boolen operaattoreilla. Aikomuslähtöisten verkkojen osalta aineistoa löytyi vähän, joten suurempaa rajausta ei tarvinnut tehdä. Tutkitummista aiheista tuloksia löytyi huomattavasti enemmän, jolloin näiden osalta jouduttiin suorittamaan tiukempaa rajausta.

Tutkielmassa lähteinä käytettiin tieteellisiä artikkeleita, joita arvioitiin ensisijaisesti artikkelin pituuden, julkaisuvuoden ja tiivistelmän perusteella. Artikkelien julkaisusivustot olivat pääasiassa aikaisemmin mainittuja, hyvämaineisia sivustoja, jolloin sivustojen perusteella karsintaa ei tarvinnut tehdä. Tarkempaa karsintaa artikkeleista suoritettiin johdannon ja lopputuloksien perusteella.

3. OHJELMISTO-OHJATUT VERKOT

SDN-verkkoarkkitehtuuri on tietoverkkoparadigma, joka erottaa tietoverkon hallintalogiikan reititystasosta, eli ohjaustaso erotetaan tietotasosta. Perinteiset tietoverkot ovat toteutukseltaan vertikaalisia, eli niissä ohjaus- ja tietotaso ovat sidottu toisiinsa jokaisessa verkkolaitteessa. Tämä vaikeuttaa verkon hallintaa ja monimutkaistaa reitityslaitteistoa, joka yksinkertaisemmin toteutettuna olisi edullisempaa. SDN-arkkitehtuurissa tieto- ja ohjaustason erottaminen on toteutettu siirtämällä kaikki verkon ohjausmekanismit loogisesti keskitettyyn SDN-ohjaimeen [3]. Tämä parantaa verkon ohjelmoitavuutta ja skaalautuvuutta perinteisiin tietoverkkoihin nähden.

SDN-ohjain hallitsee ja automatisoi laitteiden toimintaa ohjelmistossa toteutetuilla funktioilla. Verkon ohjainkeskeinen hallinta mahdollistaa nopean reagoinnin muuttuviin tietoliikennekuvioihin, sekä liikennevoiden mukauttamisen verkon toiminnan, turvallisuuden ja energiatehokkuuden kehittämiseksi. [3] Lisäksi avoimen lähdekoodin SDN-toteutukset mahdollistavat laitevalmistajariippumattomuuden, mikä on ongelma perinteisissä tietoverkoissa.

Tietoverkkofunktioiden virtualisointi (engl. Network Functions Virtualization, NFV) tukee SDN-arkkitehtuuria. NFV:llä tarkoitetaan tietoverkon toimintojen virtualisointia, jossa verkon toiminnallisuus erotetaan fyysisestä laitteistosta ja toteutetaan verkkotoimintoja virtuaalisessa ympäristössä, kuten pilvilaskentaympäristössä tai loogisesti jaetussa fyysisessä tietoverkkototeutuksessa. Tämä vähentää myös tietoverkkojen riippuvuutta valmistajakohtaisesta laitteistosta ja toteutuksesta. NFV mahdollistaa yksittäisen fyysisen tietoverkkototeutuksen jakamisen loogisesti useammaksi SDN-verkoksi, jolloin eri käyttäjillä voi olla omat SDN-verkkonsa samassa fyysisessä infrastruktuurissa [3].

Seuraavissa luvuissa käsitellään tarkemmin SDN-verkkoarkkitehtuurin ominaisuuksia, sekä sen vaikutuksia tietoverkkotekniikan kehitykseen. Lisäksi luvuissa tarkastellaan SDN-verkkojen ongelmakohtia.

3.1 Tausta

Perinteiset tietoverkot ovat monimutkaisuutensa vuoksi usein kömpelöitä ja epäkäytännöllisiä. Verkon jokainen reitityslaite on konfiguroitava erikseen, usein käyttäen valmistajakohtaisia matalan tason komentoja. Vaihteleva ja suurikapasiteettinen tietoliikenne vaatii tietoverkoilta kykyä mukautua, mutta mekanismit automaattiseen uudelleen konfigurointiin ja tapahtumiin reagointiin ovat perinteisissä tietoverkoissa rajoitetut. [4] Lisäksi

perinteisissä tietoverkoissa toisiinsa sidotut ohjaus- ja tietotasot vaikeuttavat nykyisten tietoliikennevaatimusten täyttymistä.

Ohjelmisto-ohjatut verkot kehitettiin ratkaisuna perinteisten tietoverkkojen ongelmiin, kuten monimutkaiseen konfigurointiin ja rakenteeseen. SDN-verkot korjaavat myös perinteisten tietoverkkojen vertikaalisen toteutuksen ongelman. Verkon vertikaalisuus tarkoittaa sitä, että sen ohjaus- ja tietotaso ovat jokaisessa verkkolaitteessa sidottuina toisiinsa, mikä vähentää joustavuutta, sekä mahdollisuutta uudistaa ja kehittää verkkoinfrastruktuuria. Hyvä esimerkki tästä on siirtymä IPv4-protokollasta IPv6-protokollaan, joka käynnistyi jo 2000-luvun vaihteessa eikä vieläkään ole valmis, vaikka kyseessä on ainoastaan protokollapäivitys. [4] Idea ohjaus- ja tietotason erottamisesta tulee puhelinverkoista, joissa se on todettu turvalliseksi ja kustannustehokkaaksi ratkaisuksi [3].

Perinteiset tietoverkot ovat epäoptimaalisia myös verkkostatistiikan keräämisessä. Ohjelmisto-ohjatut verkot tuovat tähän ratkaisun antamalla reitityksprotokollien kehittämiselle joustavan ja kustannustehokkaan ympäristön, jossa uusien ratkaisujen kokeileminen on yksinkertaista. [5] SDN-tekniikka soveltuu tällaiseksi ympäristöksi, sillä sen toteuttama tieto- ja ohjaustason erottelu mahdollistaa verkkologiikan päivittämisen, kun ainoastaan ohjaustasolla toimivia SDN-ohjaimia on konfiguroitava.

3.2 Tietotaso

Verkkologiikan keskittäminen ja reitityslaitteiston yksinkertaistaminen parantaa reititystehokkuutta, koska laitteen ei tarvitse toteuttaa mitään muuta kuin reitityksen vaatimat operaatiot. Logiikan poistaminen laitteistosta mahdollistaa verkon helpomman ja halvemman laajentamisen. Jokaista lisättyä kytkintä tai reititintä ei enää tarvitse konfiguroida erikseen ja laitteiden valmistuskustannukset laskevat, koska niillä ei tarvitse suorittaa raskasta laskentaa.

Ohjelmisto-ohjatuissa verkoissa reitityspäätökset tehdään vuoperusteisesti liikenteen kohdeosoitteiden sijaan. Vuot määritellään tietoliikennekehyksen kenttien arvoina, joita käytetään liikenteen suodattamisessa ja toimintaohjeina, joilla määritetään suodattimiin jääneille kehyksille suoritettavat toimenpiteet. Vuota voidaan käsitellä sarjana kehyksiä, joilla on samat lähde- ja kohdeosoitteet. Reitityssääntöjen pelkistäminen voihin mahdollistaa kaikkien tietotason verkkolaitteiden toiminnallisuuden yhdenmukaistamisen. [4]

Vuot tallennetaan tietotason verkkolaitteessa vuotauluun. Reitityslaitteen vuosääntöjä ei muodosteta itse laitteessa, vaan säännöt muodostetaan ohjaustasolla, eli laite saa ne automaattisesti SDN-ohjaimelta. Vuosääntöjen muodostaminen voidaan toteuttaa oletusvuolla, johon päädytään, mikäli kehys ei vastaa mitään muuta taulukkoon tallennettua

vuota. Tällöin vastaanotettu kehys lähetetään SDN-ohjaimelle tutkittavaksi. SDN-ohjain määrittää kehystä vastaavalle vuolle reitityssäännöt ja välittää nämä reitityslaitteen vuotauluun. Määrittäessä uutta vuosääntöä SDN-ohjain päivittää tarvittaessa myös muiden tietotason verkkolaitteiden vuotaulut.

3.3 Ohjaustaso

SDN-arkkitehtuurissa ohjaustason toiminnoista vastaa SDN-ohjain. Ohjain suorittaa verkon loogisia ja laskennallisesti raskaita toimenpiteitä, jolloin tietotasolla toimivat reitityslaitteet voidaan pitää mahdollisimman yksinkertaisina ja nopeina. Ohjaus- ja tietotason välinen viestintä toteutetaan hyvin määritellyllä ohjelmointirajapinnalla (engl. Application Programming Interface, API) reitityslaitteiden ja SDN-ohjaimen välillä [4]. Verkossa toimivalla ohjaimella on eteläisen rajapinnan (engl. Southbound Interface, SBI) kautta täysi hallinta tietotason reitityslaitteisiin. Esimerkki eteläisestä rajapinnasta on OpenFlow-protokolla. Ohjaimella on myös pohjoinen rajapinta (engl. Northbound Interface, NBI). Pohjoinen rajapinta huolehtii ohjaimen ja verkkoa hyödyntävien sovellusten välisestä viestinnästä, jolloin tekniset ja sovellukselle merkityksettömät yksityiskohdat voidaan piilottaa rajapinnan taakse.

Järjestelmän looginen keskittäminen ei tarkoita sitä, että järjestelmä olisi välttämättä fyysisesti keskitetty [4]. Verkon ohjauslogiikan keskittäminen SDN-ohjaimeen ei itsessään ota kantaa siihen, onko järjestelmä fyysisesti keskitetty. SDN-verkkoja voidaan toteuttaa myös fyysisesti hajautettuina, jolloin järjestelmä voi fyysisten verkkolaitteiden asettelultaan muistuttaa perinteistä tietoverkkoa.

Ohjaustason looginen keskittäminen mahdollistaa järjestelmän tilan automaattisen seurannan ja antaa näin mahdollisuuden varmistaa korkean tason toimintamallien toteutumisen, sillä tietoverkkoa voidaan tarkastella yhtenä kokonaisuutena, eikä ainoastaan joukkona toisiinsa kytkettyjä verkkolaitteita. Lisäksi laaja näkymä kokonaisuudesta helpottaa verkon optimointia sen käyttötarkoituksissa. [4]

Toteutuksia SDN-ohjaimille on nykyään lukuisia. Ohjaimia on sekä suljetun että avoimen lähdekoodin toteutuksina. OpenDaylight ja Open Networking Operating System (ONOS) ovat avoimen lähdekoodin SDN-ohjaintoteutuksia. Tämän tutkielman puitteissa yksittäisiä SDN-toteutuksia ei käsitellä tarkemmin, mutta OpenDaylightista ja ONOS:sta mainitaan niiden toteuttamien IBN-ominaisuuksien vuoksi.

3.4 Teknologian haasteet

SDN-verkot kehittävät tietoverkon hallintamekanismeja. Tästä huolimatta SDN-verkon konfigurointi tehdään matalan tason komennoilla ja määrittelyillä, joista käyttäjällä on oltava syvä ymmärrys. Tämä voi aiheuttaa ongelmia monimutkaisemmissa verkoissa, kun SDN-ohjainta konfiguroidaan. Matalan abstraktiotason konfigurointi johtaa myös siihen, että korkean tason toimintasuunnitelmien ja -mallien toteutumista on vaikeaa mitata.

Toisiinsa kytkettyjen tietoverkkojen välisen tehokkaan reitityksen saavuttamiseksi on verkkojen välillä välitettävä konfiguraatiotietoa. SDN-arkkitehtuurin keskitetyn hallinnan takia SDN-hierarkia-alueiden välillä ei voida välittää tietoa verkkojen toiminnasta. Vierekkäisten SDN-verkkojen välillä ei siis liiku tietoa, jolla tietoliikennettä verkkojen välillä voitaisi optimoida [6]. Tämä muodostuu ongelmaksi SDN-verkon kasvaessa niin suureksi, ettei yhden ohjaimen käyttäminen ole enää realistista. Tämä johtaa tilanteeseen, jossa SDN-verkko on jaettava osiin, joista kutakin hallinnoi yksi SDN-ohjain. Hajautetulle SDN-ohjainjärjestelmälle on kehitetty useita ratkaisuja [6]. Tässä tutkielmassa keskitytään kuitenkin konfiguraatio-ongelmaan, eikä näitä ratkaisuja täten käsitellä.

4. AIKOMUSLÄHTÖISET VERKOT

IBN-verkkoteknologia on uusi tietoverkkoparadigma, joka laajentaa ohjelmisto-ohjattujen verkkojen toimintaa [7]. Se on tietoverkkojen konfigurointiin, hallintaan ja optimointiin keskittyvä tekniikka, jolla voidaan pelkistää tietoverkon ylläpitotoimintoja. IBN perustuu korkeaan abstraktiotasoon, joka mahdollistaa toivotun lopputuloksen suoritettavalle konfiguraatiolle ottamatta kantaa itse toteutustapaan [2]. Tällöin käyttäjällä ei tarvitse olla syvällistä tietoa tai osaamista verkkolaitteiden toiminnasta tai konfiguraatioista.

Verkkoasetusten monimutkaisuuden vuoksi niiden manuaalinen konfigurointi on usein virhealtista ja työlästä. Lisäksi tietoverkkojen konfiguraatiot ovat sidoksissa epäyhtenäiseen ja monimutkaiseen infrastruktuuriin, jolloin manuaaliset asetukset ovat harvoin optimaalisimpia ratkaisuja. [8] Nämä ovat tekijöitä, jotka tietoverkkojen rakenteiden monimutkaistuessa ovat johtaneet uuteen abstraktiotasoon, joka mahdollistaa verkko-operaattoreille helpon verkon hallinnan. Konfiguroinnin virheettömyyden ja optimoinnin merkitys korostuu erityisesti moderneissa tietoverkoissa, joiden on vastattava jatkuvasti kehittyviin vaatimuksiin.

SDN-tekniikan tavoin IBN-tekniikkaa toteutetaan keskitetyllä ohjaimella. Verkon keskitetyllä ohjauksella verkkoa voidaan käsitellä kokonaisuutena, eikä joukkona erillisiä komponentteja. Ohjain on suorassa yhteydessä kaikkiin sen alaisuudessa toimiviin verkkolaitteisiin, joihin sillä on täydellinen näkymä ja hallinta. Tämä mahdollistaa SDN-ohjaimen hyödyntämisen aikomuslähtöisessä verkonhallinnassa. [1]

Tässä luvussa esitellään aikomuslähtöisiä verkkoja tarkemmin. Ensin tarkastellaan tekniikan toimintaperiaatteita sekä sen mukanaan tuomia toiminnallisuuksia ja laajennuksia. Tekniikkaa tarkastellaan myös osana tulevaisuuden tietoverkkoja.

4.1 Aikomus

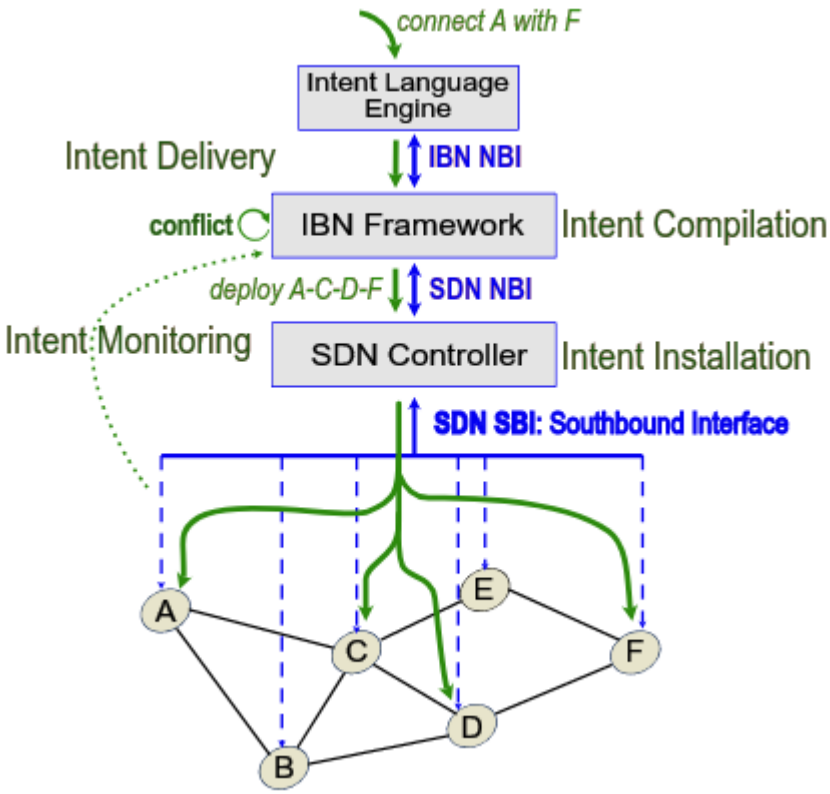
Aikomuslähtöisten verkkojen käsite on esiintynyt tietoverkkotekniikassa jo lähes kaksikymmentä vuotta. Tässä yhteydessä käytetty aikomus-sana viittaa kehittyneeseen käsitteeseen sanoista käytäntö tai menettelytapa, jotka puolestaan ovat peräisin Slomanin “Policy Driven Management System”-käsitteestä jo vuodelta 1994 [9]. Aikomus-käsitteen merkitys voidaan osoittaa tarkastelemalla kokonaisuuksien hallinnan vaikeutta käytännön tietoverkkototeutuksissa, joiden käyttäjät puolestaan haluavat yksinkertaisempia ratkaisuja [10].

IBN-verkon operaattori määrittelee abstraktilla tasolla mitä hän tahtoo tehdä. Tätä tahtoa mallinnetaan IBN-arkkitehtuurissa aikomus–käsitteellä. Keskeinen asia aikomuksen määritelmässä on, ettei se ole riippuvainen käytetyistä protokollista tai laitevalmistajista [2].

Aikomus on konfiguraatiokäsitteistä kaikista korkeimmalla abstraktiotasolla. Aikomus voidaan ilmaista vapaasti ja sitä esittäessä ei ole merkityksellistä, onko aikomus toteutettavissa sellaisenaan. Menettelytapa on keskimmäisen abstraktiotason käsite. Aikomukset voidaan jakaa menettelytavoiksi – säännöiksi, jotka mahdollistavat aikomuksen toteutustavan käytännössä. Alimman abstraktiotason konfiguraatio–käsite huomioi nykyisen verkkoympäristön ja purkaa menettelytavat käytännön komennoiksi, joilla voidaan mukauttaa verkkolaitteiden toimintaa. [2]

Aikomukseen sisältyy kolme osaa: olio, toimenpide ja tulos. Oliolla viitataan verkkoresurssiin ja palveluun verkkoympäristössä. Toimenpiteellä tarkoitetaan toimia, joilla mukautetaan olioita. Tulos viittaa olioiden lopulliseen tilaan toimenpiteen jälkeen. [2]

Kuvassa 1 on esimerkki IBN-järjestelmän toiminnasta. Kuvassa esitetään IBN- ja SDN-rajapintojen sekä reitityslaitteistojen väliset suhteet, kun järjestelmään syötetään aikomus. Kuvaan on merkitty IBN-järjestelmän NBI, sekä SDN-ohjaimen NBI ja SBI. IBN-järjestelmän NBI:tä käytetään verkko-operaattorin kanssa viestimiseen. IBN- ja SDN-komponenttien välinen kommunikaatio tapahtuu SDN-ohjaimen NBI:n välityksellä.



Kuva 1. *IBN-järjestelmä [6].*

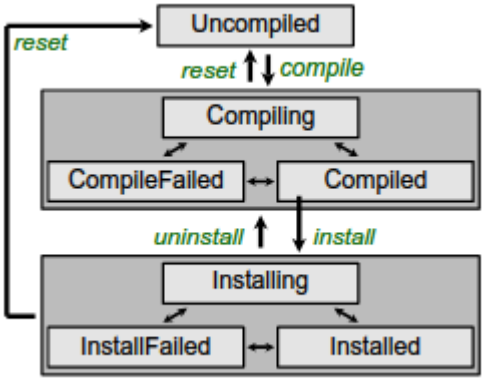
Kuvassa havainnollistetaan, kuinka IBN-ohjelmistokehys toimii SDN-ohjaimen päällä. Aikomus muodostaa yhteys laitteiden A ja F välille syötetään IBN-järjestelmän komponenttiin, jossa se tulkataan koneen ymmärrettäväksi. IBN-ohjelmistokehys suorittaa aikomuksen käännöksen. Käännetty aikomus syötetään lopuksi SDN-ohjaimelle järjestelmään asennettavaksi. Kuvan 1 tapauksessa aikomuksen käyttöönottamiseksi täytyy tehdä konfiguraatiomuutoksia laitteisiin A, C, D ja F. Asennuksen aikana tai jälkeen ilmenevien ristiriitojen ratkaiseminen tapahtuu IBN-ohjelmistokehyksessä.

Aikomuksen toteutumiseksi pitkällä aikavälillä yksi konfigurointikerta ei riitä. Tästä syystä on tarkasteltava aikomukselle suunniteltua tilakonetta, joka kuvaa aikomuksen nykyistä tilaa. Aikomusten käsittelyssä voidaan hyödyntää myös aikomuspuuta. Aikomuspuussa ylimmän tason aikomus on paloiteltu koneellisesti useaksi osa-aikomukseksi. Aikomuspuu on aikomuksen ja sen osa-aikomuksien tiloista koostuva hierarkkinen puurakenne, joka kuvaa aikomuksien välisiä riippuvuuksia [6]. Tilakonetta ja aikomuspuuta käsitellään lisää seuraavissa alaluvuissa.

4.1.1 Aikomuksen tilakone

Käytännössä aikomus toteutetaan matalan tason konfiguraatioilla. Koska konfiguraatiot

reagoivat muutoksiin tai lisäyksiin verkon aikomuksissa herkästi, on aikomuksia käsiteltävä aina osana elinkaarta [6]. Tästä syystä konfiguraation pitkäaikaisen toiminnan takaamiseksi voidaan aikomuksen määrittelyssä käyttää tilakonetta. Tilakonetta käytetään aikomuksen kaikkien mahdollisten tilojen ja tilasiirtymien määrittelyyn. Yksinkertainen tilakone aikomukselle on esitetty kuvassa 2.



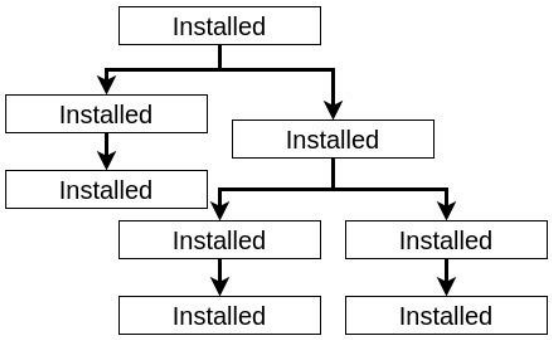
Kuva 2. *Aikomuksen tilakone [6].*

Tilakoneessa kuvataan aikomukselle kaksi välivaihetta: kääntäminen ja asentaminen (engl. compiling ja installing). Nämä välivaiheet ovat riippuvaisia koko järjestelmän laitteiden tilan mukauttamisesta aikomuksen vaatimuksiin sopivaksi. Kääntäminen viittaa siihen, ettei aikomuksen käännöstä ole vielä suoritettu onnistuneesti. Asennus tarkoittaa sitä, ettei jo käännettyä aikomusta ole vielä asennettu kaikille vaadituille laitteille. Kääntäminen tai asentaminen voi epäonnistua, mikäli resursseja ei ole saatavilla tai aikomuksen vaatimukset eivät täyty [6].

4.1.2 Aikomuspuu

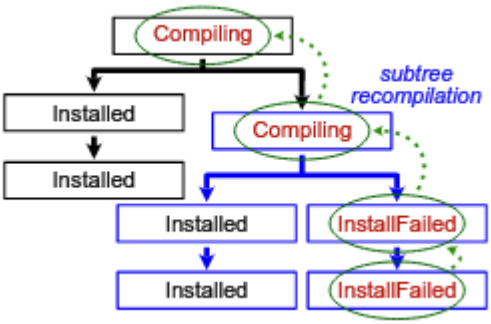
Käyttäjän antama aikomus voidaan suoran toteutuksen sijaan purkaa automaattisesti osa-aikomuksiksi. Tällöin ylimmän tason aikomuksen toteutuminen riippuu sen alaisista osa-aikomuksista. Tässä tapauksessa aikomuksen toteutumisen tarkastelua helpottaa aikomuspuu.

Aikomuksen toteuttavat konfiguraatiot muuttuvat suurella todennäköisyydellä aikomuksen elinkaaren aikana, joten on järkevää tarkastella aikomuksien tilojen riippuvuuksia toisistaan. Aikomuspuussa kunkin aikomuksen toteutumista kuvaa jokin tila tilakoneessa. Yksinkertainen aikomuspuu on esitetty kuvassa 3. Kuvassa esitetään aikomuksia, jotka on onnistuneesti asennettu.



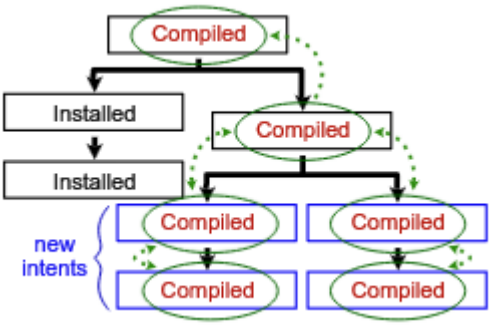
Kuva 3. *Aikomuspuu. Perustuu lähteeseen [6].*

Aikomuksien riippuvuudet kulkevat aikomuspuussa alaspäin. Aikomuksen epäonnistuessa esimerkiksi verkossa tapahtuvan virheen johdosta, epäonnistuvat myös kyseisen aikomuksen yläpuoliset vaiheet. Kuvassa 4 on esitetty tilanne, jossa kahden alimman osa-aikomuksen asennus on epäonnistunut.



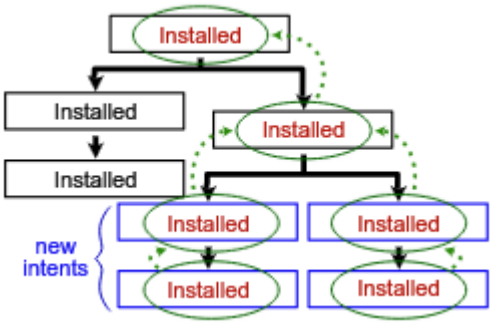
Kuva 4. *Aikomusten riippuvuudet [6].*

Kuvan 4 esittämässä tapauksessa koko puun oksa, joka on riippuvainen epäonnistuneista aikomuksista, käännetään uudelleen (engl. subtree recompilation). Kuvassa 5 on esitetty aiemmassa kuvassa esitetyn epäonnistumisen vuoksi uudelleen käännetyt aikomukset.



Kuva 5. *Uudelleenkäännetyt aikomukset [6].*

Aikomusten uudelleenkäännöstä seuraa näiden asentaminen. Uusien aikomusten onnistunutta asennusta seuraava aikomuspuun tila on esitetty kuvassa 6.



Kuva 6. *Aikomuspuun tila asennuksen jälkeen [6].*

Aikomuspuista on erityistä hyötyä mallintaessa aikomusten välisiä suhteita. Aikomuksien purkaminen osiin helpottaa niiden koneellista käsittelyä, sillä ongelma on helpompaa purkaa osaongelmiksi, jotka voidaan ratkaista rekursiivisesti.

4.2 Konfiguraation abstraktiotaso

Vaikka IBN-käsite on teoriassa jo vanha, on sen toteuttaminen riippuvaista toimivasta koneoppimisteknologiasta, koneellisesta päättelystä ja kontekstipohjaisesta luonnollisen kielen käsittelystä (engl. Natural Language Processing, NLP). Tämä on johtanut siihen, että IBN-sovelluksia on voitu toteuttaa vasta viime vuosina. [1] Koneoppimista IBN:ssä tarvitaan konfiguraation abstraktiotason toteuttamiseen käytännössä.

Aikomuslähtöiset tietoverkot pyrkivät tarjoamaan verkkototeutuksien konfiguroinnille abstraktiotason, joka mahdollistaa toiminnallisten tavoitteiden ja liiketoimintamallien määrityksien esittämisen verkolle sellaisenaan. Tapa, jolla aikomus toteutetaan matalammalla abstraktiotasolla, jätetään kokonaan järjestelmän hoidettavaksi. [10] Tällöin verkon ylläpitäjällä ei tarvitse olla syvää teknistä tuntemusta tietoverkon tarkasta rakenteesta tai toiminnallisuudesta.

Käyttäjä ilmaisee aikomuksensa IBN-järjestelmään toteutetulla käyttöliittymällä. Tämä aikomus on jokin vaatimus tai toiminnallisuus, jonka tietoverkon halutaan toteuttavan. IBN järjestelmä tulkitsee käyttäjän antaman aikomuksen ja muuntaa tämän matalan abstraktiotason konfiguraatiotehtäviksi, jotka järjestelmä voi toteuttaa. Aikomuksen toteuttamisen jälkeen, IBN-järjestelmä monitoroi verkon tilaa ja seuraa aikomuksen toteutumista mahdollisten tietoverkkoon tehtävien muutoksien jälkeen, hyödyntäen esimerkiksi aiemmin käsiteltyä aikomuspuuta.

IBN-järjestelmän abstraktiotason hyödyntämiseen on ehdotettu erilaisia tapoja [11]. Järjestelmän kannalta yksinkertaisin toteutustapa aikomuksen syöttämiselle on graafinen käyttöliittymä, jossa on ennalta määrätyt vaihtoehdot aikomuksen eri avainsanojen ja muuttujien määrittelyyn. Tällaisessa käyttöliittymässä käyttäjä voi valita arvot aikomukseen liittyville muuttujille, kuten verkkolaitteille, laadunvarmistuksen tasoille, tietoturvavaatimuksille ja ajalliselle kestolle. Käyttöliittymää toteuttaessa voidaan ottaa huomioon kohderyhmän taitotaso, jolloin kokeneelle verkko-operaattorille voidaan tarjota tarkempia asetuksia, kuten laitteiden osoitteita, porttinumeroita ja virtuaalisten lähiverkkojen tunnisteita. [11] Tällainen matalan tason asetuksien tarjoaminen on kuitenkin osittain ristiriidassa korkean abstraktiotason periaatteiden kanssa.

Toinen, aikomuslähtöisyyttä paremmin tukeva käyttöliittymä on käyttäjän luonnollinen kieli. Tällöin aikomuksen koneelliseen ymmärtämiseen on hyödynnettävä NLP-tekniikkaa, jonka kehittäminen on vielä merkittävä tutkimuskohde. Tekniikka kontekstipohjaisen ja kieliasusta riippuvaisen syötteen erittelemiseksi avainsanoihin ja -määreisiin ei vielä ole täysin virheetöntä [11]. Tästä syystä luonnollisen kielen hyödyntäminen aikomusten määrittelyssä on vielä suhteellisen virhealtista.

4.3 Tietoturvasovellukset

Tietoverkot ovat yksi tietojärjestelmän yleisimmistä hyökkäysvektoreista. Tämä lisää painoarvoa havaita ja poistaa järjestelmistä korkean tason turvallisuuspolitiikan ja sen käytännön toteutuksen väliset ristiriidat. [12] Erityisesti konkreettisten tietoturvariskien poistaminen verkosta on tärkeää. Ilman verkon monitorointia automatisoivaa IBN-järjestelmää on tietoturvapoikkeamien etsiminen kallista ja epävarmaa.

Aikomuslähtöiset verkot ovat ajankohtainen aihe tietoverkkojen turvallisuudessa, sillä IBN-tekniikan toteuttama abstraktiotaso mitätöi tietoverkoille tyypillisiä turvallisuusongelmia. Korkeatasoisia tietoturvapolitiikkoja käyttämällä riski tietoturvapoikkeamien syntymisestä pienenee. Verkkolaitteiden manuaalisessa konfiguroinnissa poikkeamia syntyy herkästi. Tämä korostuu erityisesti laajoissa tietoverkoissa, joissa tietyn tilan saavuttaminen voi vaatia merkittäviä muutoksia lukuisten verkkolaitteiden konfiguraatioihin. Käytännössä IBN-verkossa tekotavan määrittelyn sijaan tarvitsee määritellä ainoastaan se, mitä halutaan tehtävän.

Usein tietoverkkotoimintojen tuottamat lokitiedot ovat matalatasoisia ja määrältään suuria, jolloin niiden analysointi voi olla käyttäjälle vaikeaa [12]. Perinteisten sekä SDN-tekniikkaa käyttävien verkkojen toiminnan analysoinnissa on ymmärrettävä hyvin matalan

tason tietoa. IBN-abstraktio seuraa verkon tilaa automaattisesti, jolloin epäkohtien tunnistaminen konfiguraatiossa tapahtuu myös automaattisesti.

4.4 Teknologian haasteet

IBN-tekniikan tarjoama yksinkertaistettu verkonhallinta ja korkean tason käytäntöjen automaattinen käsittely luo uusia haasteita verkkojen toimintaan. Olemassa olevat SDN-verkkojen diagnostiikkatyökalut toimivat alhaisella abstraktiotasolla, joten IBN:n korkean tason aikomusten käsittely on hankalaa [7,12]. Tämä tarkoittaa sitä, etteivät verkko-operaattorit voi turvautua perinteisiin tietoverkkojen vianetsintätyökaluihin, vaan tilalle on kehitettävä kokonaan uusia sovelluksia. Tämä onkin keskeinen osa IBN-tekniikan kehitystä, koska tekniikka pyrkii juuri automatisoimaan verkon tarkoituksenmukaisen tilan ylläpidon.

Tietotason konfiguroinnin jälkeen on pystyttävä vahvistamaan, että tietotason laitteiden konfiguraatiot vastaavat varmasti aikomuksen vaatimuksia. Lisäksi on tarkkailtava tietotason toteutusta laitteissa, mikä on suurissa verkkototeutuksissa pitkäkestoista ja epäluotettavaa. Tällöin automatisoidusta tiedonkeruujärjestelmästä on hyötyä. Järjestelmällä kyetään automatisoimaan lokitietojen kerääminen verkkolaitteistosta, mistä voidaan automaattisesti tarkistaa konfiguraation vaatimustenmukaisuus. [12]

Havaitsemattomien virheiden tai epätarkkuuksien käsittely IBN-toteutuksen automaatiologiikassa on haastavaa tietojärjestelmän laitteiden ja palveluiden monipuolisuuden takia. Myös aikomuksen subjektiivinen luonne johtaa ongelmiin tilanteissa, joissa järjestelmän toteutus ei tue jonkin toiminnon automatisoimista tai tarvitsee muuten verkko-operaattorin syötettä. [13] Tällaiset ongelmat voidaan ratkaista ulkoisilla tietoverkon toiminnallisuuden vahvistustyökaluilla, jotka tarkastelevat korkean tason aikomusten ja matalan tason konfiguraation vastaavuutta.

IBN-tekniikan mekanismien standardointi on vielä avoin tutkimusongelma [7]. Ensimmäinen standardointihanke IBN-tekniikalle suoritettiin Open Networking Foundationin toimesta vuonna 2016. Tavoitteena oli luoda tekniikalle aikomuskäsittelijä, joka toimii verkko-ohjaimen laitetasolla esimerkiksi SDN-ohjaimessa. [10] IBN on vielä nuori teknologia, mutta ensimmäisiä IBN-verkkoja toteutetaan ja näiden toiminnasta kerätään kehitykselle tärkeää tietoa [1].

5. IBN-TOTEUTUKSET YRITYSVERKOISSA

Modernien yrityksien tietojärjestelmien tulee olla joustavia, skaalautuvia, standardien mukaisia ja tietoturvallisia [1]. Tietoverkot ovat merkittävä osa tietojärjestelmiä, joten niiden on oltava helposti konfiguroitavissa ja tehokkaasti analysoitavissa. Yrityksellä on oltava verkostaan kattava näkyvyys, jotta sen tilaa ja toimintoja voidaan tarkkailla ja tarvittaessa hallita, varmistaen liiketavoitteiden toteutuminen verkossa [1]. Tietoturvapoikkeamat on pystyttävä havaitsemaan ja eliminoimaan tehokkaasti ennen kuin ne ehtivät aiheuttaa yritykselle aineellista tai maineellista haittaa.

Yritysverkot eroavat Internetistä merkittävillä tavoilla. Yrityksen täytyy esimerkiksi pystyä hallitsemaan koko verkkoaan tarkasti. Yritys myös tietää verkkonsa ensisijaiset tavoitteet. Verkonhallinta on toteutettava siten, että tavoitteet eivät häiriinny toissijaisista tekijöistä. IBN-tekniikan korkea abstraktiotaso ja automaattinen seuranta mahdollistavat ongelmien tunnistamisen ja ratkaisemisen, jolloin verkon toiminnallisuus voidaan taata paremmin, kuin pelkässä ohjelmisto-ohjatussa verkossa. [1]

Teknologian kehittyminen luo mahdollisuuksia nopeuttaa yritysten digitalisoitumista tukien uusia sovelluksia, kuten virtuaalitodellisuutta ja 5G- tai IoT-verkkoja. Uusien käyttötarkoitusten tukeminen vaatii yritysverkoilta nopeaa mukautumista [11]. Uudet teknologiat voivat tuoda verkolle perinteisestä poikkeavia ehtoja ja vaatimuksia. Esimerkiksi IoT-laitteiden määrä ja matala teho aiheuttavat tietoverkolle uudenlaisia vaatimuksia.

Seuraavissa kappaleissa käsitellään tarkemmin yritysverkkoja, sekä IBN-tekniikan soveltuvuutta yrityksen toimintasuunnitelman tukemiseen yritysverkoissa. Lisäksi tarkastellaan tekniikan tietoturvavaikutusta yritysten erityisten vaatimuksien kannalta.

5.1 Yritysverkkojen vaatimukset

Yrityksellä on erityisiä vaatimuksia tietoverkkonsa toiminnallisuudelle, hallinnalle ja turvallisuudelle. Digitalisaation myötä monet tiedonkäsittelytehtävät ovat siirtyneet digitalisiin järjestelmiin. Koska tietoverkot ovat järjestelmissä merkittävässä osassa, monet yrityksen työtehtävistä ovat riippuvaisia toimivasta yritysverkosta. Tämä johtaa laajoihin vaatimuksiin tietoverkon palveluille.

Yritysverkko koostuu tyypillisesti:

1. Pienestä määrästä suuria kohteita, eli kampuksia.
2. Suuresta määrästä pieniä hajautettuja kohteita, eli sivukonttoreita.

3. Pienestä määrästä konehuoneita, jotka ylläpitävät yrityksen sovelluksia.
4. Laajasta alueverkosta (engl. Wide Area Network, WAN), joka yhdistää yrityksen kampukset, sivukonttorit ja konehuoneet samaan verkkoon. [1]

Päätelaitteet kuten työasemat, älylaitteet tai valvontakamerat ovat yhteydessä verkkoon kampuksien tai sivukonttorien yhteyspisteiden kautta. Sovelluksia voidaan ylläpitää pilvipalvelutekniikan kehittymisen myötä yrityksen omissa konehuoneissa, kampuksilla, sivukonttoreilla tai ulkoisten palveluntarjoajien verkoissa salatulla yhteydellä. Monipuolisuudesta johtuen ovat myös verkon vaatimukset moninaiset. Pääsynvalvontaa ja tietoturvapoikkeamien havainnointia on suoritettava jatkuvasti.

Yrityksen käyttöönottaessa uusia teknisiä sovelluksia, verkko on saatava mukautettua nopeasti uuden sovelluksen vaatimuksiin. Muutosten automatisointi on parantunut SDN-arkkitehtuurin myötä, mutta palauteominaisuudet verkon uuden tilan toiminnasta eivät ole riittäviä. Perinteiset tavat kerätä tietoa verkkolaitteista ovat riippuvaisia verkko-operaattorin kokemuksesta ja tukeutuvat useisiin työkaluihin, jotka skaalautuvat huonosti nykyajan suuriin ja monimutkaisiin tietoverkkoratkaisuihin. [1]

Yritysverkon suunnittelussa, toteuttamisessa ja ylläpidossa on lukuisia haasteita. Modernissa verkkoympäristössä on huomioitava monimutkainen infrastruktuuri ja arkkitehtuuri. Verkossa voi esimerkiksi olla useiden valmistajien verkkolaitteita, eri ohjelmistoversioita tai rakenteellisia eroja eri toimitilojen toteutuksissa. [1] Verkkoon yhteydessä olevat laitteet monipuolistuvat jatkuvasti, vaatien verkolta joustavuutta ja tukea uusille ominaisuuksille. Lisäksi yrityksen muuttuvan liiketoimintasuunnitelman tukeminen tietoverkossa on vaikeaa, etenkin perinteisissä tietoverkoissa laitekohtaisilla konfiguraatioilla.

Vaikka jatkuvasti kehittyviin vaatimuksiin on vastattava, ovat nykyiset yritysverkkoarkkitehtuurit monimutkaisia, virhe- ja hyökkäysalttiita sekä kalliita ylläpitää [1]. Aikomuslähtöiset verkot tarjoavat ratkaisun näihin ongelmiin mahdollistamalla verkon suoraviivaisen konfiguroinnin ilman, että verkon tilan seuranta ja ylläpitäminen olisi monimutkaista ja kallista.

5.2 Yrityksen toimintasuunnitelma

Yrityksen liiketoimintamallit ja tietoverkkojen toiminnalliset tavoitteet ovat usein abstrakteja, jolloin tietoverkon mukauttaminen vaatimusten mukaiseksi matalan tason konfiguraatiokomennoilla voi olla hankalaa. Yrityksen toimialasta ja luonteesta riippuen se voi tarvita tietoverkoltaan tukea monenlaisille tekniikoille ja monenlaisiin työtehtäviin. Esimerkiksi yrityksen verkko-operaattoreilla ja verkkoa hyödyntävällä myyntihenkilöstöllä on verkolle aivan erilaisia vaatimuksia. Myyntihenkilöllä voi olla esimerkiksi tarve muuttaa

tietyn verkkoliikenteen palvelunlaatua, mikä perinteisesti vaatii verkko-operaattorin ammattitaitoa ja valtuuksia. IBN-verkon suoraviivaistamasta konfiguroinnista johtuen voidaan tällaiset operaatiot mahdollistaa muillekin, kuin vain päteville verkko-operaattoreille.

IBN-tekniikkaa tukeva tietoverkko voidaan konfiguroida ja mukauttaa joustavasti verkko-operaattorin korkean abstraktiotason vaatimuksien kautta. IBN-verkko toteuttaa käyttäjän vaatimukset, piilottaen matalan laitetason yksityiskohtaiset konfiguraatiot. Tästä syystä IBN-verkkojen aikomus–käsite soveltuu yrityksen korkean tason toimintamalleihin ja liikesuunnitelmiin hyvin [11].

5.3 Yritysverkkojen tietoturva

Tietoverkot ovat yksi tietojärjestelmän yleisimpiä hyökkäysvektoreita ja yrityksillä on erityisiä vaatimuksia tietoturvalle. Tämä on johtanut siihen, että yritysverkkojen ajantasaisuuteen on kiinnitettävä erityistä huomiota. Ohjelmisto-ohjatut verkot auttavat osaltaan irrottamalla reitityslaitteistossa ohjaus- ja tietotason toisistaan, jolloin konfiguraatiosta vastaavaan keskitettyyn ohjaustasoon voidaan soveltaa tiukempaa tietoturvapolitiikkaa, eikä pahantahtoinen toimija pääse manipuloimaan tätä tietotason laitteista. Ohjaustason keskittäminen helpottaa haitallisen liikenteen havainnointia, sillä verkosta on näkymä kokonaisuutena, eikä joukkona hajautettuja laitteita. Tästä huolimatta parantamisen varaa on ja tietoturvaa voidaankin edistää IBN-tekniikalla.

Yritysverkon tilaa on kyettävä tarkkailemaan jatkuvasti siten, että tietoturvapoikkeamiin voidaan reagoida mahdollisimman nopeasti. Perinteisesti tietoverkkojen toiminnasta kerättävää analytiikkatietoa on paljon ja matalan tason vuoksi sen tarkastelu on raskasta. IBN-järjestelmän automaattinen verkkotilan seuranta helpottaa tietojen analysointia. [1] Järjestelmä osaa itsenäisesti tarkkailla poikkeamien ja ristiriitojen ilmenemistä, sekä suorittaa näille toimenpiteitä ja ilmoittaa tapahtumista verkko-operaattorille. Lisäksi IBN-järjestelmän toteuttamien konfiguraatioratkaisujen optimaalisuus on tietoturvan kannalta merkittävä tekijä. Kuten aiemmin todettiin, tietoverkon manuaalinen konfiguroiminen on riskialtista ja epävarmaa.

Yritykset adoptoivat joustavasti uusia sovelluksia ja teknologioita, kuten IoT tai pilviympäristöt. Nämä uudet tekniikat luovat verkkoon uusia hyökkäysvektoreita. [14] Pilviympäristöjen ja IoT:n vaatimat uudenlaiset verkkoympäristöt vaativat entistä parempaa tietoturvaa. IBN-tekniikka toimii erinomaisesti myös näissä tapauksissa, koska päätelaitteiden hallinta on automatisoitu, eikä verkko-operaattorilla tarvitse olla täydellistä ymmärrystä uusien teknologioiden yksityiskohdista.

5.4 IBN-verkon käyttöönotto

Päivittäessä yritysverkkoa IBN-tekniikkaan, riippuu käyttöönoton hankaluus verkon alkuperäisestä toteutuksesta. Järjestelmän ohjauslogiikan keskittäminen erilliseen laitteeseen on haastavin työvaihe. Mikäli kyseessä on perinteinen tietoliikenneverkko, eikä SDN-verkko, on siirtyminen IBN-verkkoon työlästä. IBN-tekniikan vaatimuksien lisäksi on huomioitava myös SDN-verkon vaatimukset.

Olemassa olevan SDN-verkon päivittäminen IBN-verkkoon on suoraviivaista, verrattuna perinteisen tietoliikenneverkon päivittämiseen. IBN-tekniikan lisäominaisuudet voidaan toteuttaa SDN-järjestelmän päälle ohjelmallisesti, jolloin ainoa muutos voi olla aikomuksen syöttämiseen vaaditun käyttöliittymän lisääminen. Myös toteutuskohtaisia eroavaisuuksia voi joutua huomioimaan, riippuen käytössä olevasta SDN-ohjaintoteutuksesta. Yksinkertaisimmassa tapauksessa verkossa käytetylle SDN-ratkaisulle on valmiiksi toteutettu IBN-ominaisuuksia, kuten ONOS- tai OpenDaylight-ohjaimissa.

6. YHTEENVETO

Tutkielma alkoi katsauksella ohjelmisto-ohjattujen verkkojen perusteisiin sekä sen puutteisiin verkon konfiguroinnissa. Perusymmärrys SDN-tekniikasta auttaa lukijaa ymmärtämään tarpeen konfiguraation korkealle abstraktiotasolle. Lisäksi SDN-tekniikan perusteet ovat oleelliset IBN-tekniikkaa käsiteltäessä, sillä IBN on kehitetty SDN-arkkitehtuurin periaatteita mukaillen. Taustoituksen jälkeen tutkielmassa esiteltiin IBN-tekniikkaa ja sen ominaisuuksia, joilla ratkaistaan tietoverkkojen matalan tason konfiguraatiosta koituvia ongelmia. Lopuksi tarkasteltiin yritysverkkoja, sekä IBN-tekniikan soveltamisesta koituvia hyötyjä ja haasteita.

Tietotekniikan kehitys on luonut uusia vaatimuksia tietoverkoille. Tämä on johtanut verkkojen virtualisoinnin ja ohjelmisto-ohjattujen verkkojen kehittämiseen. Ohjelmoitavuudesta huolimatta ohjelmisto-ohjatut verkot eivät tarjoa ratkaisua matalan tason konfiguraatiolle. Tämä vaikeuttaa verkkojen skaalautuvuutta ja vaatimuksiin mukautumista. Tietoverkon manuaalisessa konfiguroinnissa verkko-operaattorilla on oltava täydellinen ymmärrys sen tilasta ja ominaisuuksista. Aikomuslähtöiset verkot tarjoavat ratkaisun kyseiseen konfiguraatio-ongelmaan.

Pelkistämällä tietoverkon konfiguraation korkean tason aikomuksiin, IBN-tekniikka poistaa konfigurointiin liittyviä haasteita. Konfiguroinnin suorittaminen korkealla abstraktiotasolla vähentää inhimillisten virheiden todennäköisyyttä, jolloin tietoverkon tavoitteiden toteutuminen voidaan taata paremmin, kuin manuaalisesti matalalla tasolla suorittaen. Lisäksi korkean tason vaatimuksien ja toimintamallien muuttaminen matalan tason konfiguraatioiksi on työlästä, jolloin automatisoinnista on erityistä hyötyä.

Jatkuvasti päivittyvät vaatimukset vaikuttavat merkittävästi tietoverkkojen tarkoituksenmukaiseen toiminnallisuuteen ja tietoturvallisuuteen. Yritysverkoissa on usein erityisiä vaatimuksia verkon suorituskyvylle ja tietoturvallisuudelle. Tietoverkon suorituskyvyn varmistaminen, turvallisuuspoikkeamien kartoittaminen ja poistaminen ovat työläitä toimenpiteitä verkko-operaattorille, eikä täydellistä kattavuutta voida taata. Aikomuslähtöisten verkkojen toteuttama korkean abstraktiotason konfiguraatio on yhteensopiva yrityksen toimintatavoitteiden ja -mallien määritelmiin. Tällöin matalan tason konfiguroinnin automatisoinnista on erityistä hyötyä, koska verkko-operaattori tekee aikomuksen määrittelyn vaivattomasti, jättäen teknisen toteutuksen yksityiskohdat IBN-järjestelmälle.

Tästä syystä aikomuslähtöiset verkot soveltuvat erinomaisesti yritysverkon toteuttamiseen. IBN-tekniikkaa tukevan verkon hyödyt korostuvat erityisesti, jos yritysverkko on laaja, sen tila muuttuu usein tai se on loogisesti monimutkainen.

Kaikista teoreettisista hyödyistään huolimatta IBN-tekniikka on pitkälti riippuvaista koneoppimistekniikoista, jotka ovat viime vuosien edistyksistä huolimatta vielä kehitysvaiheessaan. Tekniikan kehittyessä odotetaan tekoälysovelluksien, kuten aikomuslähtöisten verkkojen yleistyvän, kun järjestelmän tekemien virheiden todennäköisyys laskee ja uusien ominaisuuksien kehitys aloitetaan.

LÄHTEET

[1] Falkner M, Apostolopoulos J. Intent-based networking for the enterprise: a modern network architecture. Communications of the ACM. 2022;65(11):108–17. https://doi.org/10.1145/3538513.

[2] Tsuzaki Y, Okabe Y. Reactive configuration updating for Intent-Based Networking. In: 2017 International Conference on Information Networking (ICOIN). IEEE; 2017. p. 97–102. https://doi.org/10.1109/ICOIN.2017.7899484.

[3] Rawat DB, Reddy SR. Software Defined Networking Architecture, Security and Energy Efficiency: A Survey. IEEE Communications surveys and tutorials. 2017;19(1):325–46. https://doi.org/10.1109/COMST.2016.2618874.

[4] Kreutz D, Ramos FMV, Verissimo PE, Rothenberg CE, Azodolmolky S, Uhlig S. Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE. 2015;103(1):14–76. https://doi.org/10.1109/JPROC.2014.2371999.

[5] Rafiq A, Afaq M, Song WC. Intent-based networking with proactive load distribution in data center using IBN manager and Smart Path manager. Journal of ambient intelligence and humanized computing. 2020;11(11):4855–72. https://doi.org/10.1007/s12652-020-01753-1.

[6] Decentralized Intent-driven Coordination of Multi-Domain IP-Optical Networks. In: The Institute of Electrical and Electronics Engineers, Inc (IEEE) Conference Proceedings. Piscataway: The Institute of Electrical and Electronics Engineers, Inc. (IEEE); 2022. https://doi.org/10.23919/CNSM55787.2022.9964606.

[7] Ujcich BE, Bates A, Sanders WH. Provenance for Intent-Based Networking. In: 2020 6th IEEE Conference on Network Softwarization (NetSoft). IEEE; 2020. p. 195–9. https://doi.org/10.1109/NetSoft48620.2020.9165519.

[8] Khan TA, Muhammad A, Abbas K, Song WC. Intent-based networking platform: An automated approach for policy and configuration of next-generation networks. In: Proceedings of the ACM Symposium on Applied Computing. 2021. p. 1921–30. https://doi.org/10.1145/3412841.3442064.

[9] Sloman M. Policy driven management for distributed systems. Journal of network and systems management. 1994;2(4):333–60. https://doi.org/10.1007/BF02283186.

[10] Zeydan E, Turk Y. Recent Advances in Intent-Based Networking: A Survey. In: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring). IEEE; 2020. p. 1–5. https://doi.org/10.1109/VTC2020-Spring48590.2020.9128422.

[11] Zheng X, Leivadeas A, Falkner M. Intent Based Networking management with conflict detection and policy resolution in an enterprise network. Computer networks (Amsterdam, Netherlands : 1999). 2022;219:109457–. https://doi.org/10.1016/j.comnet.2022.109457.

[12] Herbaut N, Correa C, Robin J, Mazo R. SDN Intent-based conformance checking: application to security policies. In: 2021 IEEE 7th International Conference on Network Softwarization (NetSoft). IEEE; 2021. p. 181–5. https://doi.org/10.1109/NetSoft51509.2021.9492679.

[13] Wang H, Sharma P, Ahmed F, Kang JM, Qian C, Yannakakis M. Epinoia: Intent Checker for Stateful Networks. In: 2021 International Conference on Computer Communications and Networks (ICCCN). IEEE; 2021. p. 1–9. https://doi.org/10.1109/ICCCN52240.2021.9522299.

[14] Chen J, Zhu Q, Başar T. Dynamic Contract Design for Systemic Cyber Risk Management of Interdependent Enterprise Networks. Dynamic games and applications. 2021;11(2):294–325. https://doi.org/10.1007/s13235-020-00363-y.