Pyry Koskinen

Kameravalvontaverkon vaatimusmäärittely

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

10.5.2017

Metropolia

Tekijä Otsikko Sivumäärä Aika	Pyry Koskinen Kameravalvontaverkon vaatimusmäärittely 33 sivua 10.5.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tieto- ja viestintätekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	Teknologiajohtaja Pekka Holopainen Lehtori Erik Pätynen

Insinöörityön tarkoituksena oli valita tuotteistettavaksi turvallisuuspalveluyrityksen käyttöön kytkinmallisto kameravalvontaverkkoihin. Yritys myy asiakkailleen kameravalvontajärjestelmien osana kytkinverkkoja, joiden avulla toteutetaan nykyaikaisen kameravalvonnan kuvansiirto valvontakameratallentimeen ja tehonsiirto kameroille.

Työssä perehdyttiin sellaisiin seikkoihin, jotka osaltaan vaikuttavat kameravalvontaverkon suunnitteluun ja toteutukseen, kuten verkon rakenne, käyttötarkoitus, yleiset päätelaitteet, päätelaitteiden asettamat vaatimukset suorituskyvylle ja tietoturva. Kameravalvonnan erityisvaatimus kytkimille on sen runsaasti tarvitsema teho. Tyypillinen valvontakamera tarvitsee 5–12 watin tehon, jolloin kytkimen tehobudjetin on oltava suuri. Tämä rajaa suuresti valittavien kytkinmallien määrää.

Valvontakameraverkkojen tulee olla luotettavia. Ne voivat sijaita vilkkaasti liikennöidyissä kohteissa, jolloin aktiivisen valvonnan katkeamattomuus on tärkeää, tai vastaavasti hyvinkin eristetyillä alueilla käyttötarkoituksenaan vain tallennus, jolloin verkon ongelmien huomaamiseen voi kulua pitkäkin aika. Tällöin verkossa ei tulisi olla yksittäistä pistettä, joka kaataa koko verkon, ja sitä tulee valvoa. Koska valvontakameraverkkojen tietoturva on huono, työssä perehdytään yleisimpiin hyökkäystyyppeihin kytkimiä vastaan ja tyypillisiin suojautumistapoihin hyökkäyksiä vastaan

Työn tuloksena syntyi vaatimusmäärittely, joka on minimi luotettavuuden ja tietoturvan takaamiseksi. Vaatimusmäärittelyn pohjalta voidaan valita useampikin tuote, sillä vertailtavat ominaisuudet eivät ole yksiselitteisiä, ja edelleen tuotteistettavaksi valittiinkin tuote, joka ei täysin täyttänyt vaatimuksia.

Avainsanat	Kameratallennin, valvontakamera, tietoturva, käytettävyys

Author	Pyry Koskinen
Title	Requirements analysis for video surveillance network
Number of Pages	33 pages
Date	May 10, 2017
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Specialisation option	Computer networks
Instructors	Pekka Holopainen, Chief Technology Officer Erik Pätynen, Senior Lecturer

The goal of this thesis was to choose a family of network switches for productization in a private security company. The company sells network video recorder systems for its customers, and with them, network switches that provide the means for video transmission and power to network cameras.

The themes reviewed in this thesis concerning camera surveillance are network topology, use, common host devices, requirements set by hosts (especially network cameras) and network security. Network cameras demand 5–12 watts of power from power supplying equipment and therefore power budget specification for switches must be high. High PoE budget, on the other hand, greatly limits available options for switch models. Camera surveillance networks should be reliable. They might be used for very active surveillance in congested areas (such as shopping malls), or they might situate in remote sites with no daily or weekly active use so possible failures might go unnoticed for long times. Hence, the network should not have a single point of failure and it must be supervised. Because network security in camera surveillance systems is poor, common attacks and counters to attacks against Layer 2 were also reviewed.

The requirements set by these features were then gathered to a requirement matrix, and a number of switch models of several manufacturers were compared.

According to the requirement matrix, the Juniper EX2200-series switches was the best alternative for further productization. However, Fortinet D–series switches provide many additional possibilities for enhanced network security and was thus chosen for follow-up investigation.

Keywords	network video recorder, network camera, security, availability

Sisällys

Lyhenteet

MAC	Media Access Control, OSI-mallin siirtokerroksen laiteosoite
IEEE	Institute of Electrical and Electronics Engineers, kansainvälinen tekniikan alan standardisointijärjestö
1000BASE-T	1 Gbps RJ45-kytkinportti
100BASE-TX	100 Mbps RJ45-kytkinportti
802.11	WLAN-standardi
802.1Q	Standardi paikallisille ja metropolialueverkoille
802.3	IEEE:n standardi Ethernet-lähiverkkoteniikkaa varten
802.3af	IEEE:n 2003 määrittämä standardi tehonsyöttöön 4-parisessa kaapelissa
802.3at	IEEE:n 2008 määrittämä standardi tehonsyöttöön 4-parisessa kaapelissa
802.1	IEEE:n standardi lähiverkko- ja metropoliverkkoalueita varten
802.1Q	IEEE:n Ethernet-verkon jatkokehitysstandardi
802.1w	IEEE:n Spanning Tree-protokollan standardi
AP	Access Point, tukiasema WLAN-verkossa
APN	Access Point Name, yksityinen mobiiliverkko
ARP	Address Resolution Protocol, osoitteenselvitysprotokolla
BPDU	Bridge Protocol Data Unit, RSTP-protokollan tietokehys
CAM	Content Addressable Memory, kytkimen laiteosoite-tilataulu

CAT5/6	Category 5/6, luokan 5 tai 6 kierretty parikaapeli
CCTV	Closed Circuit Television, valvontakamerajärjestelmä
CDP	Cisco Discovery Protocol, Ciscon laitteissa oleva
DAI	Dynamic ARP Inspection, dynaaminen ARP-viestien suodatus
DHCP	Dynamic Host Configuration Protocol, protokolla verkkolaitteiden dynaamiseen konfigurointiin
DVR	Digital Video Recorder, digitaalinen videotallennin
FIB	Forwarding Information Database, ks. CAM
GBIC	Gigabit Interface Converter, gigabittinopeuksinen mediasovitin
Gbps	Gigabits per second, gigabittiä sekunnissa
H.264	MPEG-4 AVC (Advanced Video Coding), videon ja äänen pakkausmenetelmä
IP	Internet Protocol, internetprotokolla
LAN	Local Area Network, paikallinen lähiverkko
LAN2LAN	Local Area Network to Local Area Network, kahden lähiverkon välinen tunneli
LLDP	Link Layer Discovery Protocol, linkkitason tunnistusprotokolla
MAC	Medium Access Control, laiteosoite
Mbps	Megabits per second, megabittiä sekunnissa
MITM	Man in the middle, “mies keskellä” -hyökkäys

MJPEG	Motion JPEG, häviöllinen videonpakkausformaati
MPLS	Multiprotocol Label Switching, tunnistekytkentäprotokolla
NVR	Network Video Recorder, verkkotallennin
OM1/3	Optical mode 1-3, optinen moodi 1-3, monimuotovalokuitukaapelin standardi
OS1OS2	Optical single, yksimuotokuitukaapeli
OSI	Open Systems Interconnection (Reference Model), tiedonsiirron viitemallihysmalli
PC	Personal Computer, henkilökohtainen tietokone
PoE	Power over Ethernet, Ethernet-teho
RJ45	Registered Jack 45, nimi kaapeliliittimelle
RSTP	Rapid Spanning Tree Protocol, nopea virityspuualgoritmi, siirtokerroksen topologia
SFP	Small Form-factor pluggable, lähetin-vastaanotinmoduuli
SNMP	Simple Network Management Protocol, verkon hallintaprotokolla
VLAN	Virtual Local Area Network, virtuaalinen lähiverkko
WLAN	Wireless Local Area Network, langaton lähiverkko
VPN	Virtual Private Network, virtuaalinen lähiverkko
x86	32-bittinen prosessoriarkkitehtuuri
x64	64-bittinen prosessoriarkkitehtuuri

1 Johdanto

Insinöörityön tarkoituksena oli valita ja tuotteistaa Securitas Oy:n käyttöön kytkinmallisto kameravalvontaa varten. Securitas on vuodesta 1993 Suomessa toiminut turvallisuuspalveluyritys, joka toimittaa asiakkailleen tavallisten hälytys- ja vartiointipalveluiden lisäksi rikosilmoitinlaitteita, kulunvalvontajärjestelmiä ja kameravalvontajärjestelmiä ja niiden suunnittelua ja asennusta.

Kameravalvontajärjestelmät ovat vuosikymmeniä perustuneet koaksiaalikaapeliverkkoihin, joita pitkin kuvasignaali kameralta on siirretty aikaisemmin VHS-nauhuriin, nykyisin digitaalisiin kuvatallentimiin, jotka ovat useimmiten olleet PC-pohjaisia palvelimia. Viimeisen vuosikymmenen aikana on tapahtunut murros, ja useimmat uudet kameravalvontaverkot perustuvat Ethernet-verkkoon, jossa voidaan myös välittää kameroille niiden tarvitsema käyttöjännite. Nopeutuneet operaattoriverkot ja huomattavasti halventuneet tietoliikenneliittymät mahdollistavat nykyään myös kameravalvontajärjestelmien etävalvonnan ja -huollon.

Securitas tarjoaa asiakkailleen suojattujen etäyhteyksien kautta kameravalvontajärjestelmien hälytyskuvavalvonta-, kamera-, kierros-, kuvantallennus- ja etähuoltopalveluita. Esimerkiksi etähuoltopalveluissa vikadiagnostiikkaa pystytään kuitenkin vain toimittamaan kameravalvontapalvelimen kautta – muista verkossa olevista laitteista tai verkkolaitteista ei muodostu minkäänlaista tilannekuvaa, jolloin kameravalvontajärjestelmän vikaantuminen voidaan usein havaita vasta esimerkiksi kamerakuvan tai -kuvien kadotessa.

Kameravalvontajärjestelmien muututtua verkottuneiksi ja etävalvottaviksi on syntynyt tarve ja mahdollisuus toimittaa asiakkaille yhä useammin räätälöityjä laajoja verkkoja, jotka saattavat sijaita useiden eri kiinteistöjen tai rakennusten alueella. Tämän työn tavoitteena on helpottaa kameravalvontaverkkojen suunnittelua, toteutusta, komponenttien valitsemista, myyntiä, elinkaaren hallintaa ja tietoturvaa ja tuottaa Securitakselle sellaista kameravalvontajärjestelmiin liittyvää tietoa, joka ei olisi muuten helposti saatavilla.

Työssä tarkastellaan kameravalvontaa ja -tallennusta suhteessa Ethernet-verkkoihin, kameravalvonnan asettamia vaatimuksia kytkimien suorituskyvyille ja Ethernet-verkkojen rakennetta ja tietoturvaa. Lopuksi pyrin esitettyjen tietojen perusteella rakentamaan vaatimusmäärittelyn kytkimille.

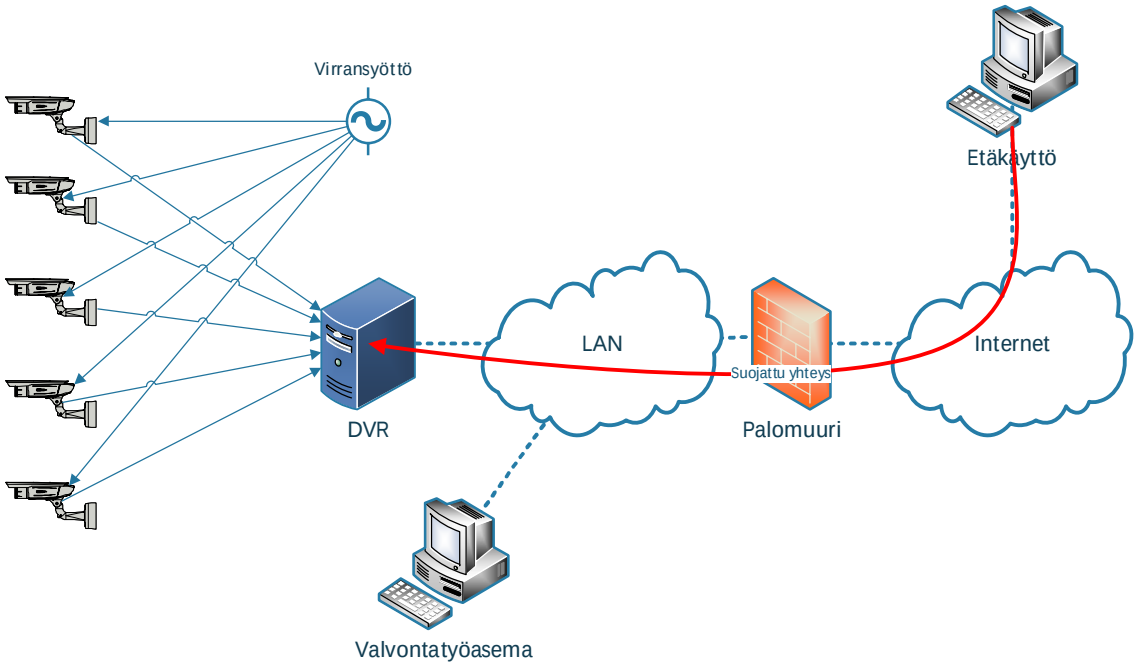
2 Kameravalvonta

2.1 Kameravalvontajärjestelmä

> Videovalvonta (engl. closed circuit television, CCTV) on valvontatekniikka, jossa valvontakameralla kuvataan jotakin kohdetta siten, että näin välittynyttä kuvaa voidaan katsoa jossakin toisessa paikassa monitorista ja/tai kuva tallentuu myöhemmin katsottavaksi [1, s. 4].

Tallentava kameravalvonta mahdollistaa useiden kohteiden samanaikaisen tai lähes samanaikaisen valvonnan etäältä, ja valvonta voidaan suorittaa myös jälkikäteen näin poistaen läsnä olevan tarkkailijan tarpeen. Kameravalvonnan tarkoitus on tallentaa mahdolliset valvottavan alueen tapahtumat ja mahdollistaa henkilöiden tunnistaminen jälkikäteen. [1, s. 5.]

Analoginen kameravalvontajärjestelmä (kuvassa 1) koostuu digitaalisesta videotallentimesta (DVR, Digital Video Recorder), kameroille johtavasta koaksiaalikaapeloinnista, kameroiden jännitesyötöstä ja mahdollisista etäkäyttöyhteyksistä, jotka on toteutettu joko yrityksen lähiverkon (LAN, Local Area Network) kautta tai suojatuin yhteyksin internetin tai muun tietoliikenneyhteyden kautta [2, s. 24].

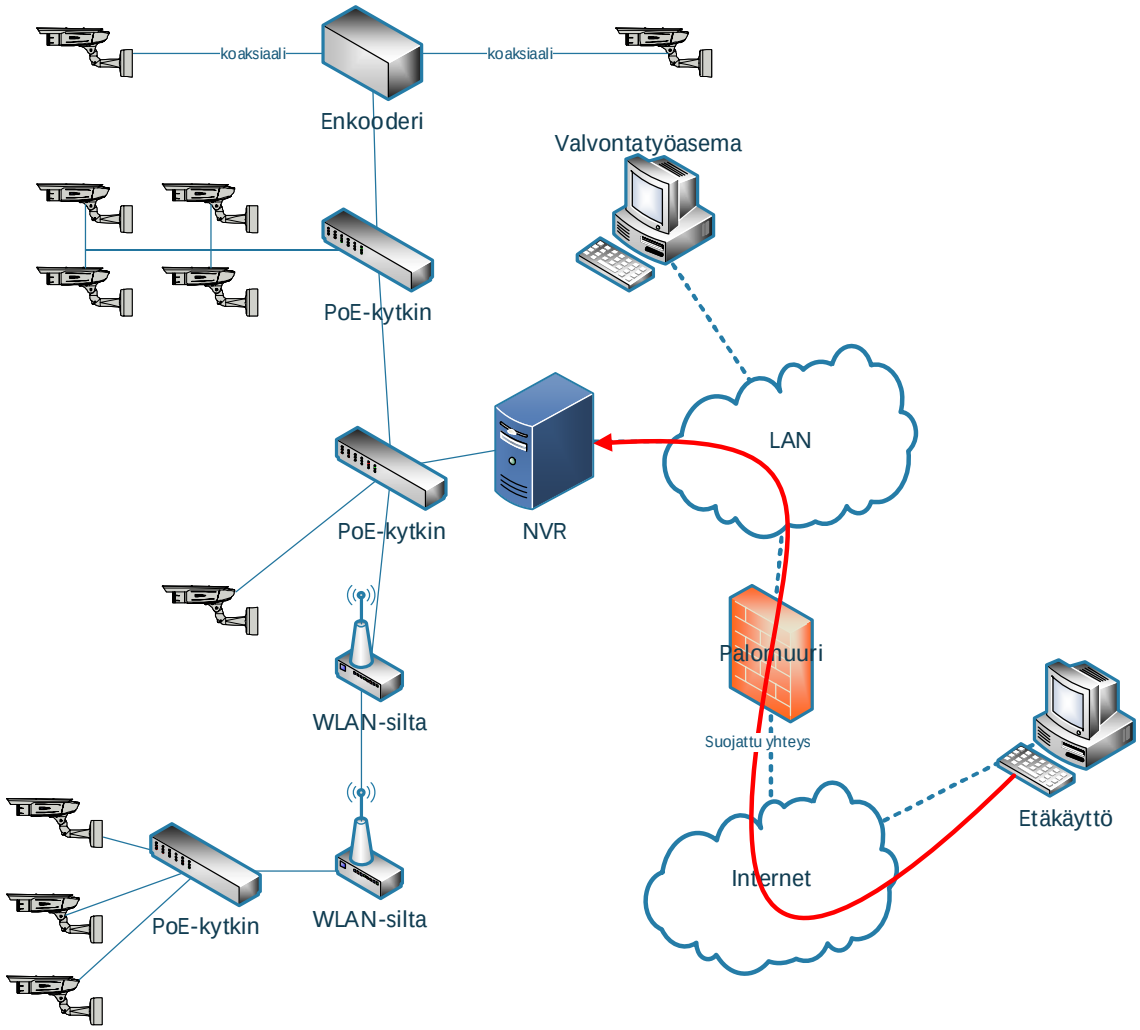


Kuva 1. Tyypillinen analoginen kameravalvontajärjestelmä [2, s. 24].

Verkkopohjainen kameravalvontajärjestelmä koostuu verkkovideotallentimesta (NVR, Network Video Recorder), IP-kameroille (Internet Protocol, verkkokamera) johtavasta CAT5- tai CAT6-kaapeloinnista, PoE-kytkimestä (Power over Ethernet, jännitesyöttö Ethernet-verkon läpi), mahdollisista WLAN-silloista (Wireless Local Area Network, langaton lähiverkko), mahdollisista analogikameroiden videopalvelimista, valvontatyöasemista ja etäkäyttöyhteyksistä.

Videopalvelimet mahdollistavat olemassa olevien koaksiaalikaapelointien ja olemassa olevien analogikameroiden käytön verkkopohjaisessa tallennusjärjestelmässä. Videopalvelin pakkaa analogisen videokuvan H.264- tai MJPEG- pakkauksella ja lähettää sen verkkoa pitkin tallentimelle. WLAN-siltoja käytetään valvottavan kohteen ja videotallentimen välillä, kun ei ole mahdollista käyttää kuitu- tai kuparikaapelointia (kuva 2) [2, s. 25].

Tässä työssä käsitellään verkkopohjaisia kameravalvontajärjestelmiä.



Kuva 2. Verkkopohjainen kameravalvontajärjestelmä [2, s. 25].

2.2 Valvontakameratallennin

Valvontakameratallennin on palvelin, jossa voi olla valmistajan suljetulla käyttöjärjestelmällä varustettu tallenninjärjestelmä (sulautettu tallennin), tai se voi olla Linux- tai Microsoft Windows -yhteensopiva ohjelmisto (ohjelmistopohjainen). Esimerkiksi suomalaisen Valvova Oy:n valmistama Ksenos-valvontakameratallenninohjelmisto on ja Windows- että Linux-yhteensopiva, siinä missä suomalaisen Mirasys Oy:n valmistama Mirasys-valvontakameratallenninohjelmisto on vain Windows-yhteensopiva.

Valvontakameratallentimessa on vaihteleva määrä verkkoliitäntöjä. Kuvassa 3 on tyypillinen toteutus valvontakameratallentimen sisäisestä PoE-kytkimestä. Sisäiset PoE-kytkimet ovat tyypillinen ratkaisu sulautetuissa tallentimissa. Ohjelmistopohjainen tallennin

voidaan asentaa mille tahansa x86- tai x64-pohjaiselle tietokoneelle tai palvelimelle, ja verkkoliitäntöjen määrän määrittää tällöin ostajan tarve tai halu.

Kuva 3. Hikvision DS-7600NI-I2/8P(16P) -tallentimessa on 16-porttinen PoE-kytkin sisäänrakennettuna (vasemmalla) ja erillinen verkkokortti etäyhteyksiä varten (kuvassa oikealla keskellä) [3].

2.3 Kaapelointi

IP-kamerat, enkodeerit, videotallentimet ja WLAN-sillat kaapeloidaan CAT5- tai CAT6-luokan Ethernet-kaapelilla joka on päätetty RJ45-liittimin. CAT5- ja CAT6-standardin maksimikaapelipituus on 100 metriä. On myös mahdollista käyttää OS1/OS2-yksimuotokuitukaapelia (Optical Single, optinen yksimuoto) tai OM2/OM3-monimuotokuitukaapelia (Optical Multimode, optinen monimuoto), joka mahdollistaa yli sadan metrin väliset yhteydet kytkimien tai päätelaitteiden välillä. Vain harvoihin päätelaitteisiin voi kytkeä suoraan kuitukaapeleita, jolloin kuidun ja päätelaitteen välissä tulee käyttää erillistä kuitu-CAT5/CAT6-mediamuunninta.

Mikäli kameravalvontajärjestelmää rakennetaan vanhan analogisen järjestelmän päälle, on myös mahdollista laajentaa Ethernet-verkkoa vanhaa koaksiaalikaapelijärjestelmää pitkin käyttämällä erillistä mediamuunninta.

2.4 Valvontakamerat

Valvontakameroissa tyypillisin verkkoliitäntä on 100BASE-TX, joskin Axis Communications AB julkaisi hiljattain kameramallin Q3708-PVE, joka käyttää 1000BASE-T-liitäntää kolmen korkearesoluutioisen kamerakennon vuoksi. Käytännössä kuitenkin kameroiden tuottama liikennemäärä on huomattavasti pienempi kuin käytetyt verkkoliitäntätyypit. Lopullinen yksittäisen kameran käyttämä kapasiteetti riippuu seuraavista tekijöistä:

- tapahtumaperusteinen tai jatkuva tallennus

- tapahtumien määrä kameran kuva-alueella
- muutosten laajuus kuva-alueella
- käytettävä kuvatahti
- resoluutio
- kuvan pakkaus
- kuva-alueen monimutkaisuus
- valaistusolosuhteet
- sääolosuhteet.

Esimerkiksi FullHD-resoluutiolla 10 kuvaa sekunnissa tallentava H.264-pakattu valvontakameratallenne tuottaa noin 2 Mbps:n liikenteen [23]. Samaan aikaan kuitenkin maailman suurin IP-valvontakameravalmistaja suosittaa käyttämään yli 12 kameran kameraverkoissa vähintään 1 Gbps:n runkolinkkejä [4].

Valvontakameraverkossa kamerat saavat käyttöjännitteensä kytkimeltä käyttäen Power over Ethernet (teho Ethernetin yli) -tekniikkaa. Valvontakameroiden tarvitsema teho vaihtelee välillä 5–25 wattia, joissakin tapauksissa jopa 60 wattiin asti, joten PoE-tehon mitoittaminen on tärkeää [2, s. 28].

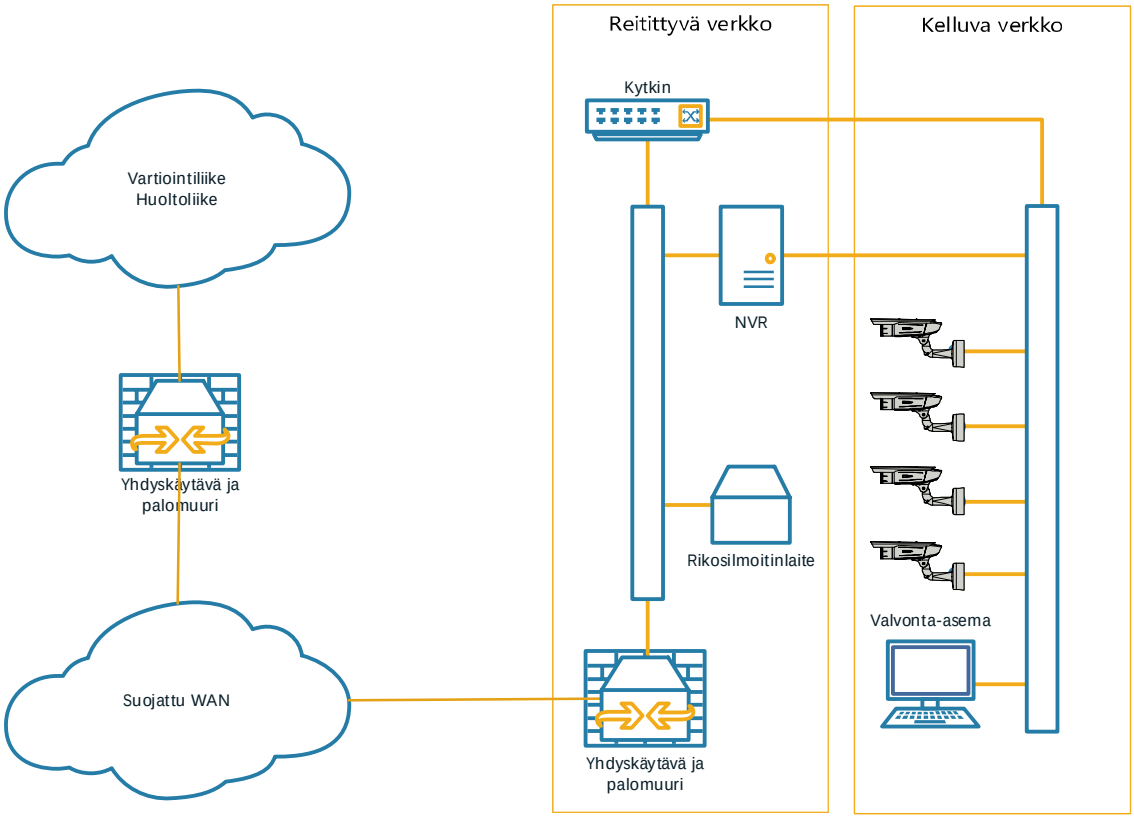
2.5 Muut kameravalvontajärjestelmän päätelaitteet

Muita yleisiä kameravalvontaverkkoon sijoitettavia laitteita voivat olla rikosilmoitinlaitteet ja kulunvalvontajärjestelmät tai -päätteet. Molemmat järjestelmät vaativat usein yhteyden ulkopuolisiin järjestelmiin – esimerkiksi vartiointiliikkeeseen murtohälytysten valvontaa varten tai huoltoliikkeeseen kulunvalvontajärjestelmien pääkäyttöä varten.

2.6 Etäyhteydet

Tapoja tuottaa etäyhteyksiä on monenlaisia, mutta kameravalvontaverkon kannalta tarkasteltuna lopputuloksena on paikallinen lähiverkko, jolla on jonkinlainen yhdyskäytävä muihin verkkoihin.

Etäyhteyksiä käyttävän tahon kannalta merkittävää onkin kytkinverkon rakenne – reititettävien IP-osoitteiden säästämiseksi voidaan valvonta-asemia ja kameroita varten määrittää erillinen, vain paikallinen verkko johon esimerkiksi valvontakameratallennin toimii siltana (kuva 4).



Kuva 4. Kelluva verkko ja reitittyvä verkko etäyhteyksien kontekstissa.

Suojattu WAN (Wide Area Network, laajaverkko) voi tarkoittaa operaattorin toimittamaa MPLS-yhteyttä, APN-yhteyttä, itse rakennettua VPN-yhteyttä tai yritysten välistä LAN2LAN-tunnelia

3 Kytkimet

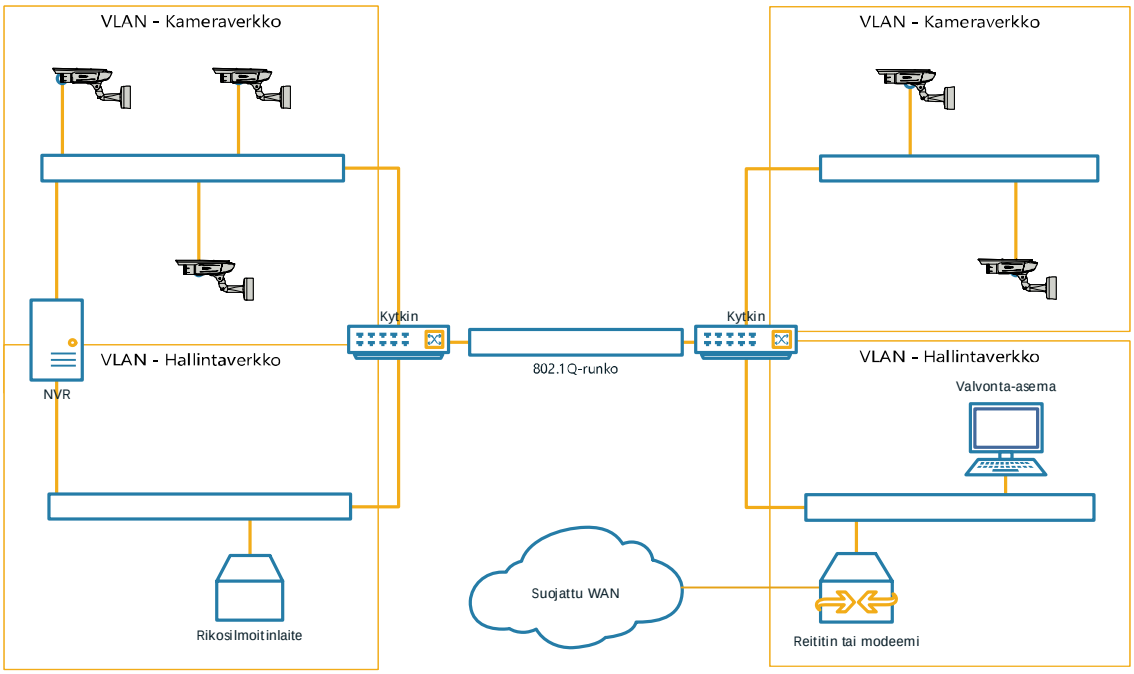
3.1 Kytkinverkko ja kytkimet

Kameravalvontaverkon suunnitteluperiaatteita koskevat samat yleisperiaatteet kuin minkä tahansa Ethernet-verkon suunnittelua. On varmistettava, että verkon suorituskyky riittää kaikissa tilanteissa, pullonkauloja ei synny ja verkon toiminta ei ole riippuvainen yksittäisestä laitteesta tai kytkinportista.

Virtuaalinen lähiverkko

Virtuaalisella lähiverkolla (VLAN, Virtual Local Area Network) tarkoitetaan fyysisen kytkimen tai kytkinverkon alueella olevaa loogista yleislähetysaluetta. Tekniikka mahdollistaa fyysisen verkon jakamisen useaan yleislähetysalueeseen OSI-mallin siirtokerroksella. Kytkimen portti voi olla runkoportti (valmistajsta riippuen tagged tai trunk) tai pääsyportti (access tai untagged) tai se voi olla määrittämätön, jolloin se valmistajasta riippuen joko hylätään tai siirretään oletus-VLANiin. Yhdessä runkoportissa voidaan kuljettaa useita eri virtuaalisia lähiverkkoja. Virtuaalisen lähiverkon pääkäyttötarkoitus on verkkojen segmentointi käyttäjien tai käyttötarkoitusten mukaan. Suurissa sisäverkoissa sitä voidaan myös käyttää yksinkertaisesti yleislähetysalueen pienentämiseen [5.]

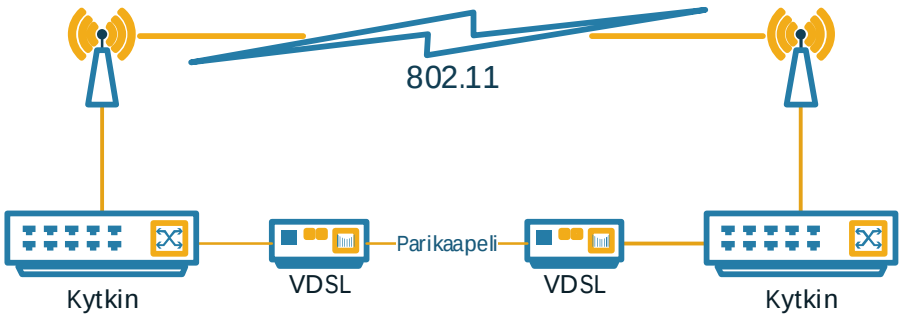
Kuvassa 5 on esitetty verkon segmentointi virtuaalisia lähiverkkoja käyttäen. Kameraverkosta on pääsy vain kameroihin ja kameratallentimeen, hallintaverkosta pääsy ulkoisiin verkkoihin, kuten luvussa 2.6. VLAN-segmentointi ei ole tietoturvaominaisuus.



Kuva 5. Kameravalvontaverkon jako VLANeihin. NVR voidaan liittää kamera- ja hallintaverkkoon joko 802.1Q-runkoporttia tai kahta verkkokorttia ja kahta pääsyporttia käyttäen. Esimerkki.

Rapid Spanning Tree Protocol – Nopea virityspuualgoritmi

Rapid Spanning Tree Protocol (RSTP), nopea virityspuualgoritmi, mahdollistaa silmukattoman topologian rakentamisen OSI-mallin siirtokerroksella. Virityspuualgoritmista on erityisesti hyötyä, mikäli verkossa on epävarmoja tietoliikenneyhteyksiä, joille halutaan rakentaa varmentavia yhteyksiä, kuten kuvassa 6.



Kuva 6. Virityspuualgoritmin käyttö voi olla tarpeellista, mikäli verkossa joudutaan käyttämään epävarmoja linkkejä.

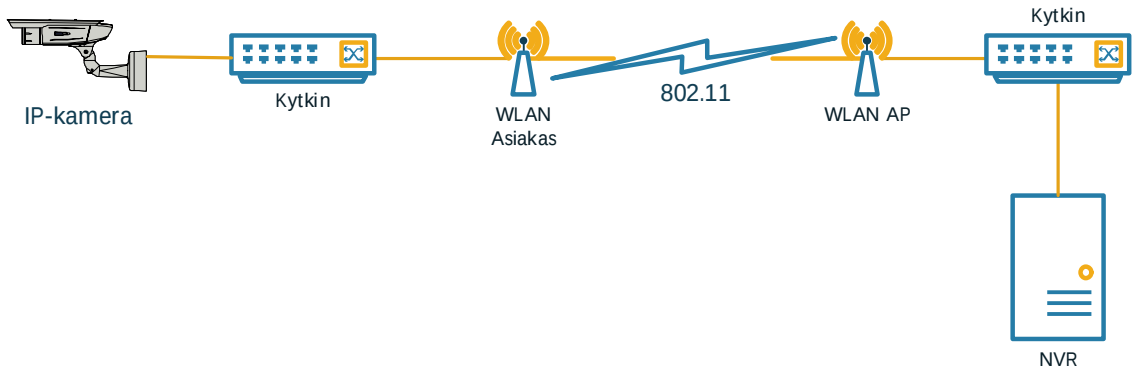
RSTP-topologia rakentuu root bridgen, juurisillan, näkökulmasta rakentuvalle puurakenteelle. Juurikytkimeksi valitaan kytkin, jonne tai jonka kautta suurin osa verkon liikenteestä todennäköisesti kulkee. RSTP-topologiaan kuuluvat jäsenkytkimet vaihtavat keskenään BPDU-paketteja (Bridge Protocol Data Unit), joiden avulla ne voivat laskea parhaimman reitin juurikytkimelle.

Kaikki portit, jotka johtavat juurikytkimelle mutta eivät ole osa parasta reittiä, asetetaan kytkimen toimesta blocked-tilaan (estetty). Juurikytkimelle johtavista porteista käytetään ilmaisua root port, juuriportti. Kun RSTP-topologiaan kytketään uusi jäsen tai jossakin sen juuriporteista tapahtuu tilamuutos, jäsenet laskevat uudestaan parhaan reitin juurikytkimelle.

Kameravalvontaverkossa juurikytkimeksi tulisi yleensä valita kytkin, joka on lähimpänä kameravalvontatallenninta, sillä sinne myös suurin osa liikenteestä ohjautuu. [5; 6]

Langaton lähiverkko

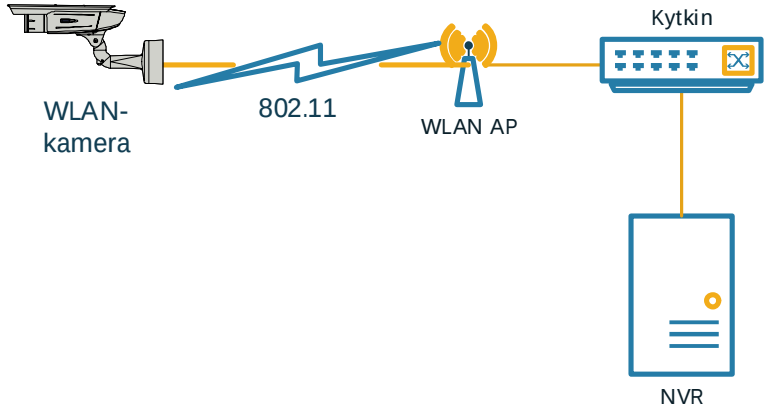
WLAN, Wireless Local Area Network, langaton lähiverkko on tarpeellinen silloin, kun lähiverkko on ulotettava paikkoihin, joihin muuten olisi vaikeaa tai liian kallista asentaa kuitu- tai kuparikaapelointi. WLAN on kuvattu standardissa 802.11. Kameravalvontaverkoissa voidaan käyttää joko WLAN-siltoja (kuva 7) tai WLAN-kameroita (kuva 8).



Kuva 7. Toteutus WLAN-sillalle kameravalvontaverkossa.

WLAN-sillat ovat muun verkon näkökulmasta kuin mikä tahansa OSI-mallin linkkikerroksen yhteys ja vaativat vain WLAN-sillan osapuolien, AP:n (Access Point, tukiasema) ja

WLAN-asiakkaan (Client), konfiguroinnin. WLAN-siltaa voi siis verkon toiminnan kannalta käsitellä langattomana kaapelina.

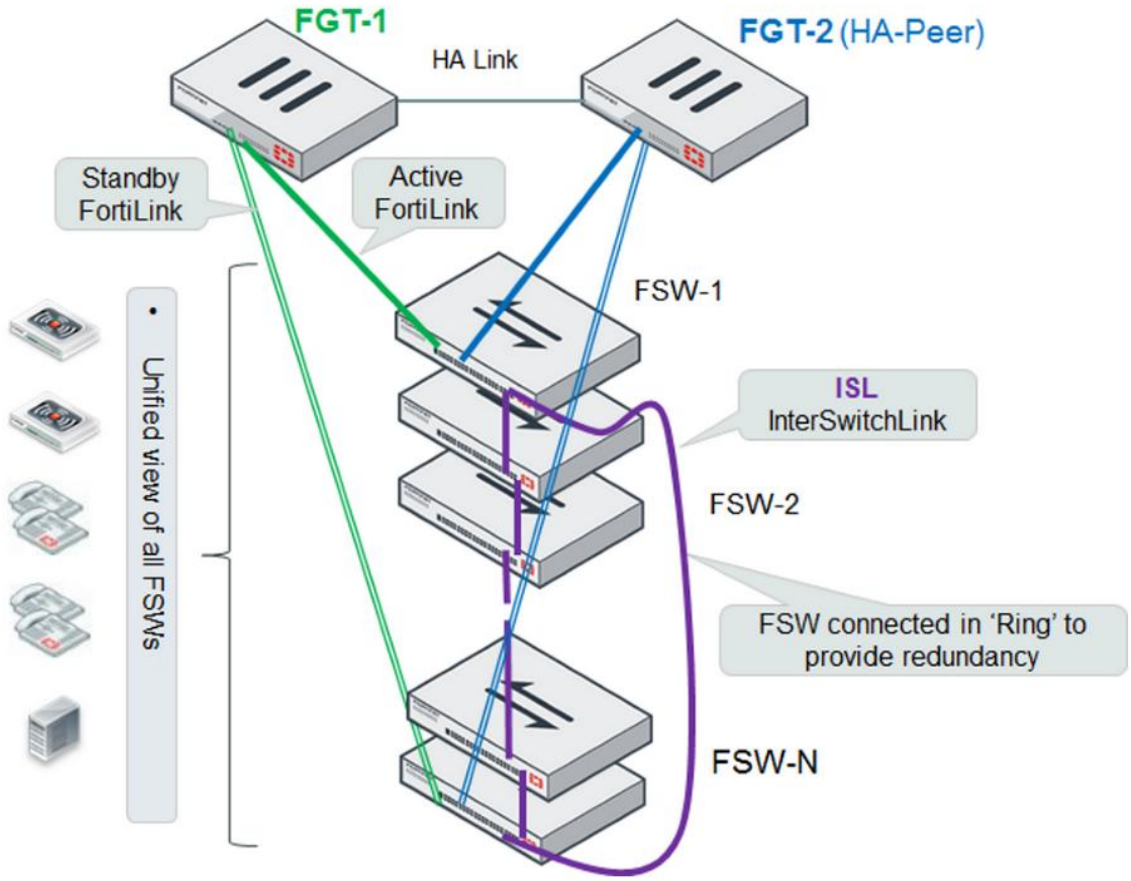


Kuva 8. WLAN-kamera kameravalvontaverkossa. Yhteen tukiasemaan voi liittää useita WLAN-kameroita.

WLAN-kameroiden liittäminen kameravalvontaverkkoon vaatii jokaisen kameran WLAN-ominaisuuksien konfiguroinnin ja jännitesyötön kaapeloinnin. Koska jonkinlaista kaapelointia on joka tapauksessa tehtävä, päädytään usein käyttämään PoE-kameraa WLAN-kameran sijaan [2].

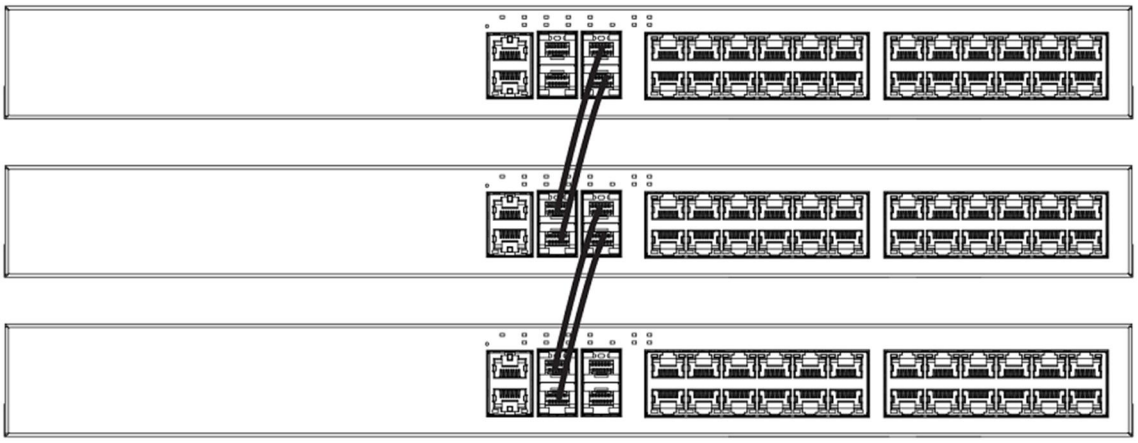
Kytkinpinot

Kytkinpinolla voidaan tarkoittaa hallinnollista pinoa tai liikenteellistä pinoa. Hallinnollisella pinolla tarkoitetaan pinoa, jossa koko kytkinpinon hallinta toteutetaan pinon pääjäsenen kautta. Liikenteellisestä pinoa käytetään myös normaaliin kytkinverkon liikenteeseen, jolloin pinon jäsenten välille ei tarvitse rakentaa RSTP-topologiaa tai muuta vastaavaa siirtokerroksen topologiaa. Hallintapinon jäseniä voi sijaita myös muualla kuin kytkimissä, esimerkiksi palomuurissa (kuva 9).



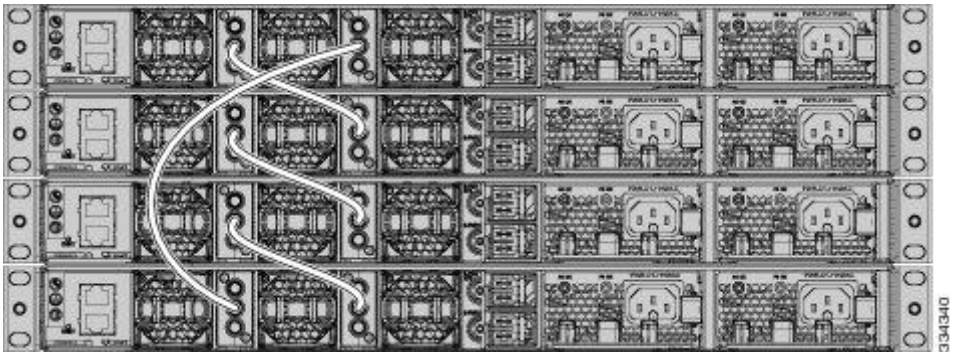
Kuva 9. Fortinetin FortiLink-ominaisuus mahdollistaa koko verkon hallinnan yhdestä pisteestä [7].

Hallintapinon hyöty on siis vähentää hallintarajapintojen määrää ja tätä kautta säästää aikaa asiantuntijatyössä. Liikenteellisen pinon hyöty on yksinkertaisempi topologia, helpompi korkean käytettävyyden konfiguraatio, redundanssin rakentaminen ylävirtaan ja niin edelleen. Kytkinpinoille ei ole kehitetty yhtenäistä standardia, vaan pinoteknologiat ovat valmistajakohtaisia. Esimerkkejä erilaisista pinomenetelmistä ovat Ciscon Stack-Wise ja Fabric Extender, Hewlett-Packardin Intelligent Resilient Framework, Juniperin Virtual Chassis ja Brocaden Stack.



Kuva 10. Brocaden ICX 6450- ja 6430-kytkinmallit voidaan pinota käyttäen etupaneelin SFP-portteja [8].

Kytkinpinoissa valmistajittain eroavana ominaisuutena on mainittava myös pinon fyysinen toteutus eli se voidaanko käyttää kytkimen etupaneelissa olevia kytkinportteja (kuva 10) tai moduulipaikkoja vai joudutaanko käyttämään kytkimen takareunaan asennettavia erillisiä kaapeleita (kuva 11). Etupaneeliin kytkettävä pino helpottaa varsinkin ahtaissa laitekaapeissa tai -hyllyissä toimimista.



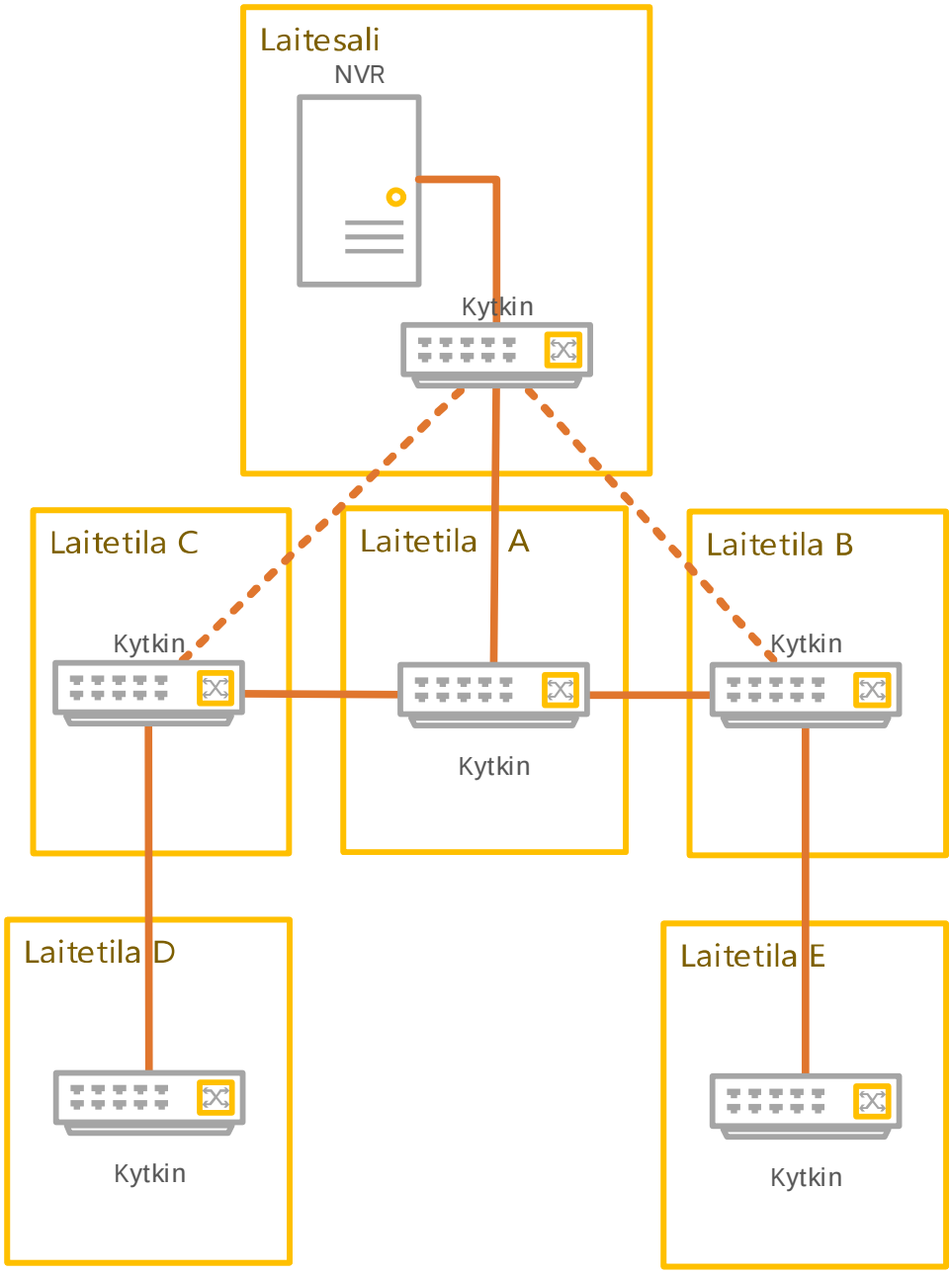
Kuva 11. Vasemmalla keskellä Cisco StackWise -pino rengastopologiaan kytkettynä [9].

Verkon rakenne, koko ja käytettävyys

Kameravalvontaverkon rakenne määräytyy valvottavan kohteen fyysisten kaapelointien ja kytkentöjen ja verkkoon liitettävien laitteiden suorituskyvyn ja niiden konfiguraation perusteella. Verkossa voi olla useita kameravalvontatallentimia, jolloin verkon koko voi vaihdella yhden tallentimen, kahdeksan kameran kokoonpanon ja kymmenen tallentimen, kahdensadan kameran välillä. Käytännössä eri laitteiden määrää verkossa rajoittaa vain verkon rakenne ja sen laitteiden suorituskyky.

Tallennettaessa yli 12 valvontakameran kuvavirtaa on huomioitava verkon rakenteen pullonkaulat. 100 Mbps:n linkkejä kytkimien välillä kannattaa välttää. Yli 120 kameran ja usean tallentimen järjestelmissä on jo huomioitava 1 Gbps:n linkin tuomat pullonkaulat. Vaihtoehtoina on käyttää kahdennettuja 100 Mbps:n tai 1 Gbps:n linkkejä tai 2,5 Gbps – 10 Gbps:n linkkejä tai muuttaa rakennetta niin, ettei yksittäinen kytkin toimi ainoana väylänä runkokytkimelle tai tallentimille.

Verkon käytettävyysvaatimukset riippuvat verkon käyttötarkoituksesta ja valvottavan kohteen riskitasosta. Aktiivisen valvonnan kohteissa, kuten esimerkiksi ostoskeskuksissa, kameravalvontaverkon keskeytyksetön toiminta on huomattavasti tärkeämpää kuin kohteissa, joissa kameravalvontajärjestelmän tarkoitus on ennemminkin auttaa rikoksen jälkiselvityksessä. Käytettävyyttä voidaan korottaa kytkinpinoilla, redundantilla RSTP-topologialla (kuva 12) tai vastaavalla OSI-tason siirtokerroksen protokollalla, kahdennetuilla linkeillä ja kytkinporttien tilamuutosten etävalvonnalla.



Kuva 12. Laitetila A:n kytkimen käytettävyys vaikuttaa merkittävästi koko verkon käytettävyyteen. Laitesalin ja laitetila B:n ja C:n välille kytkettävät varalinkit vähentävät merkittävästi laitetila A:n kytkimen merkitystä verkon toiminnan kannalta.

3.2 Kytkimien tietoturva

Kameraverkkoa koskevat aivan samanlaiset uhat kuin mitä tahansa muutakin verkkoa. Koska kameraverkko sijaitsee siellä, missä sen kamerat sijaitsevat – ja kamerat voivat sijaita alueilla, joihin kenellä tahansa voi olla pääsy – on oletettava, ettei kameraverkkoa

voi täysin suojata perinteisen fyysisen tietoturvan keinoin pääsynhallinnalla, kulunvalvonnalla tai muulla.

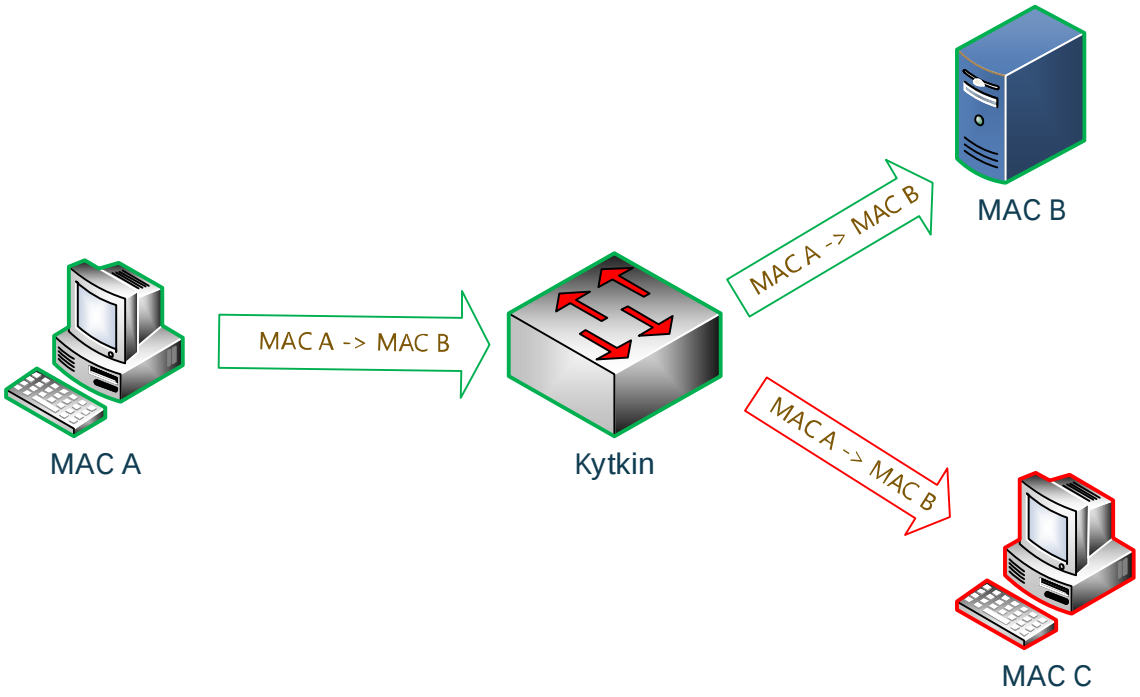
Usein kameravalvontajärjestelmän tietoturva on hoidettu huonosti [10, s. 21–22]. Kameravalvontajärjestelmässä oleva tallenne on henkilörekisteri, jonka tietoturvaa säädellään lain osalta henkilötietolailla. Henkilötietolain puutteeksi jää, ettei se ota kantaa muuta kuin syntyneeseen henkilörekisteriin eikä siihen kiinteästi liittyviin osiin, kuten valvontakameroihin, kytkimiin, etäyhteyksiin tai muihin verkon komponentteihin.

Kytkinverkko olisi kuitenkin hyvä suojata helpoimpia ja yleisimpiä hyökkäyksiä vastaan. Helpoiksi ja yleisiksi hyökkäyksiksi voi mieltää sellaiset hyökkäykset, jotka ovat valmiina saatavilla erilaisissa hyökkäyskirjastoissa tai vastaavissa valmiissa työkaluissa tai jotka ovat muuten yleisesti tunnettuja. Tunnettuja hyökkäyskirjastoja tai -työkaluja ovat esimerkiksi metasploit, dsniff ja Nmap. Samalla kuitenkin esimerkiksi pakettianalysaattoria, kuten Wireshark, voidaan käyttää hyökkäyksellisiin tai tiedustelullisiin tarkoituksiin. Hyökkäyskirjastojen ja -työkalujen hallussapito ei kuitenkaan ole laitonta sellaisenaan [11].

CAM-hyökkäys

CAM (Content Addressable Memory)- tai FIB (Forwarding Information Database)-taulu on kytkimessä sijaitseva tietokanta. Tietokannan tietueet koostuvat kytkimen fyysistä porteista ja niihin kytkettyjen laitteiden MAC-osoitteista. Yhteen fyysiseen porttiin voi liittyä useita MAC-osoitteita. CAM- tai FIB-taulua käytetään pakettien kytkemiseen lähiverkossa.

Mikäli kytkimen CAM-taulu täyttyy, se alkaa toimia hubina eli lähettää jokaisen siihen saapuvan paketin jokaisesta siihen kuuluvasta portista (kuva 13). Tyypillinen CAM-taulun koko on 8 000 tietuetta. Hyökkääjä voi siis lähettää kytkimelle tekaistuja Ethernet-kehyksiä satunnaisesti generoiduilla MAC-osoitteilla. Mikäli kytkimeen on kytketty muita kytkimiä, myös niiden CAM-taulut voivat täyttyä. Kytkimen toimiessa hubina hyökkääjä voi kuunnella muuta samassa VLANissa kulkevaa liikennettä. Hyökkäysmetodille on ollut vuodesta 1999 olemassa valmis ohjelma macof, joka on osa Dsniff-hyökkäystyökalua. [12, s. 17—24]

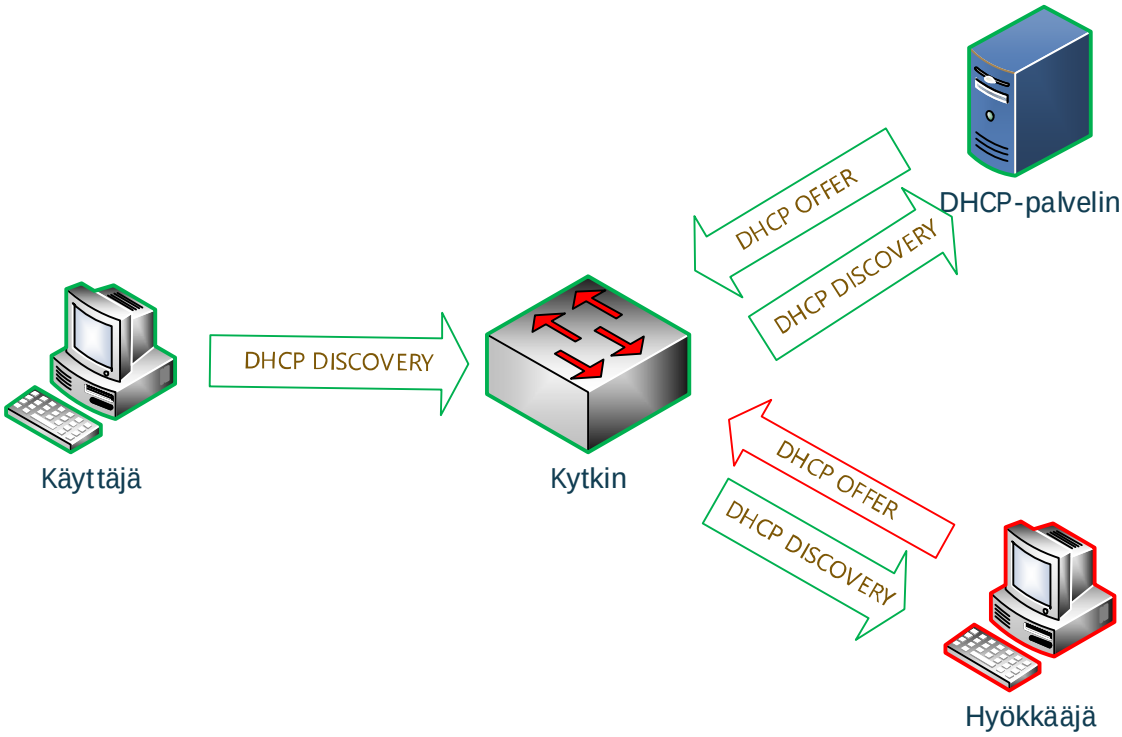


Kuva 13. Kytkin lähettää kaikki vastaanottamansa paketit kaikkiin portteihinsa [12, s. 22].

CAM-hyökkäyksiä voi torjua rajoittamalla kuhunkin porttiin liitettävien MAC-osoitteiden määrää tai lukitsemalla MAC-osoitteen siksi, minkä kytkin ensimmäisellä kerralla laittaa CAM-tauluunsa. Tätä ominaisuusvalikoimaa kutsutaan usein port securityksi.

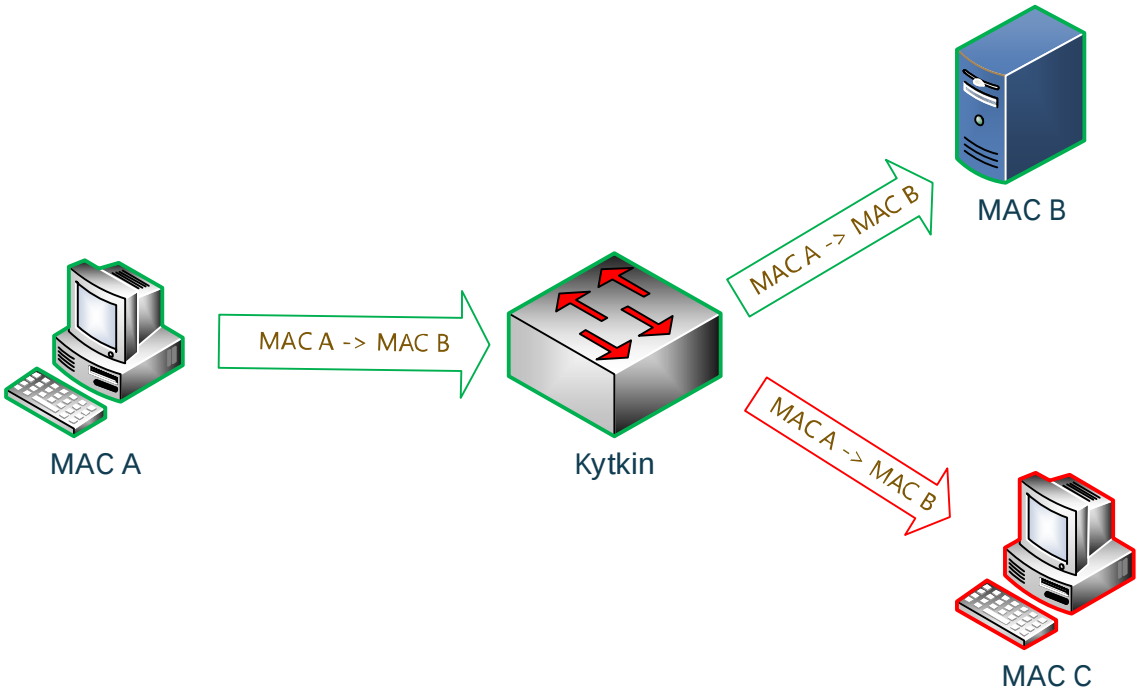
DHCP-hyökkäys

DHCP-asiakas (Dynamic Host Configuration Protocol, verkkolaitteiden dynaamisen konfiguroinnin protokolla) ei oletusarvoisesti varmenna DHCP-palvelimen identiteettiä tai sille saapuvien DHCP-viestien oikeellisuutta. DHCP Discovery (DHCP-pyyntö) -viesti lähetetään lähiverkkoon yleislähetysviestinä, joten se kulkeutuu kaikille samassa VLANissa oleville laitteille. Riippuu laitteista tai niiden käyttäjistä, vastaavatko laitteet DHCP Discoveryyn.



Kuva 14. Hyökkääjä vastaa DHCP-discovery-viestiin luvatta.

Hyökkääjä voi perustaa verkkoon luvattoman DHCP-palvelimen, joka varsinkin samassa lähiverkossa toimiessaan ehtii vastata DHCP-pyyntöihin nopeammin kuin usein yrityksen palvelinsalissa oleva DHCP-palvelin (kuva 14). Hyökkääjä voi tällöin esimerkiksi reitittää kaikkien verkossa olevien DHCP-asiakkaiden liikenteen itsensä kautta, jolloin hyökkääjä voi halutessaan nauhoittaa kaiken liikenteen tai ohjata liikenteen minne haluaa (kuva 15).



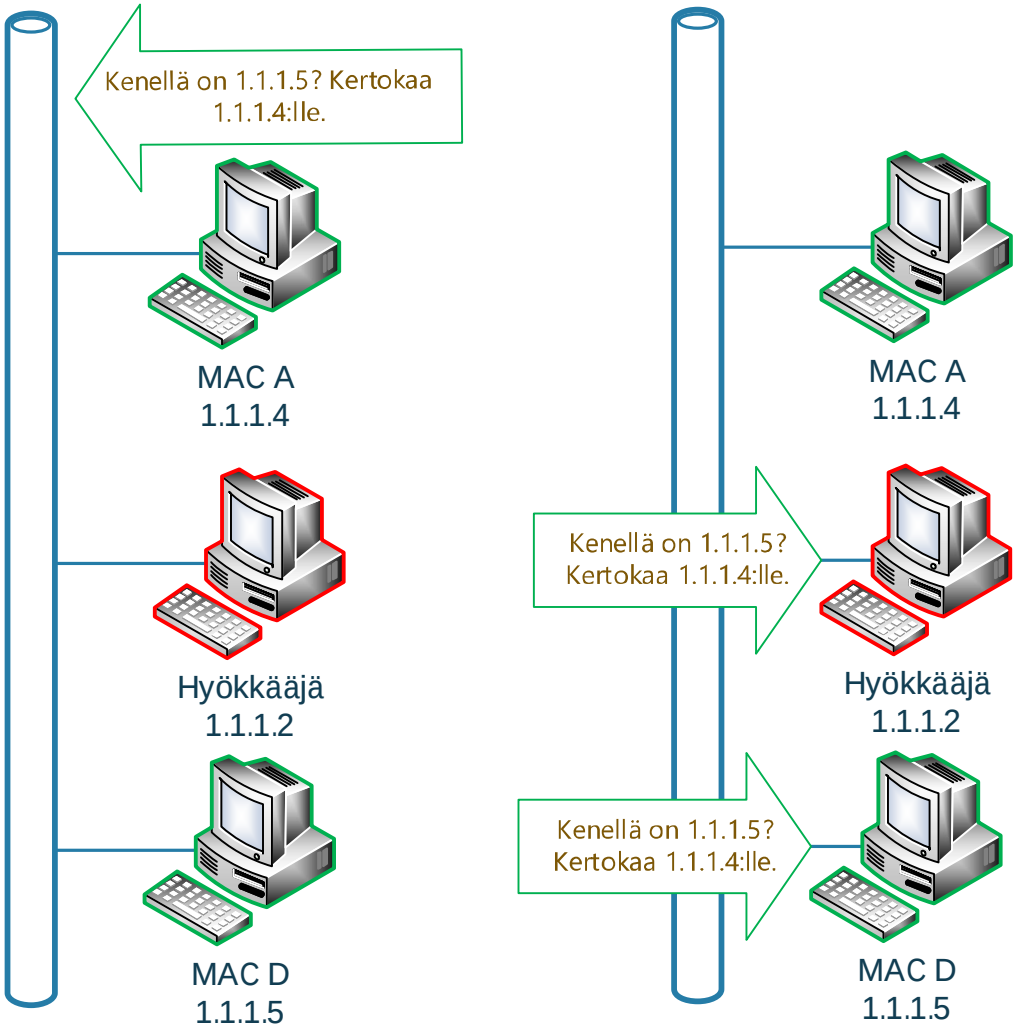
Kuva 15. Käyttäjä luulee liikennöivänsä suoraan yhdyskäytävälle, vaikka liikenne kulkeekin hyökkääjän kautta.

Vaihtoehtoisesti hyökkääjä voi lähettää suuren määrän DHCP-Discovery-viestejä ja varata omaan käyttöönsä koko DHCP-palvelimelle määritetyn IP-osoiteavaruuden. Tällöin hyökkääjä voi estää uusien laitteiden liittymisen verkkoon ja myös estää sinne jo kytkettyjen laitteiden toiminnan niiden DHCP-määritysten vanhetessa, usein noin 8–24 tunnin syklissä. Tämä mahdollistaa palvelunestohyökkäyksen saman yhteislähetysalueen sisällä [12, s. 34–47].

DHCP:n näivettämistä (DHCP Discovery -tulva) vastaan voi suojautua port securitylla, rajoittamalla porttikohtaisia MAC-osoitteita. Luvattomia DHCP-palvelimia vastaan voidaan suojautua määrittelemällä kytkimeen ne portit, joista on sallittua vastata DHCP-pyyntöihin. Tätä kutsutaan DHCP snoopingiksi. DHCP snooping tallentaa kytkimen läpi kulkevat oikeelliset DHCP-neuvottelut ja muodostaa niiden perusteella itselleen tietokannan laitteiden IP-osoitteista, MAC-osoitteista ja porteista, joihin ne on kytketty. Mikäli verkossa on laitteita, jotka eivät toimi DHCP-asiakkaina, niiden tiedot voidaan määrittää manuaalisesti DHCP snooping -tauluun [12].

ARP-hyökkäykset

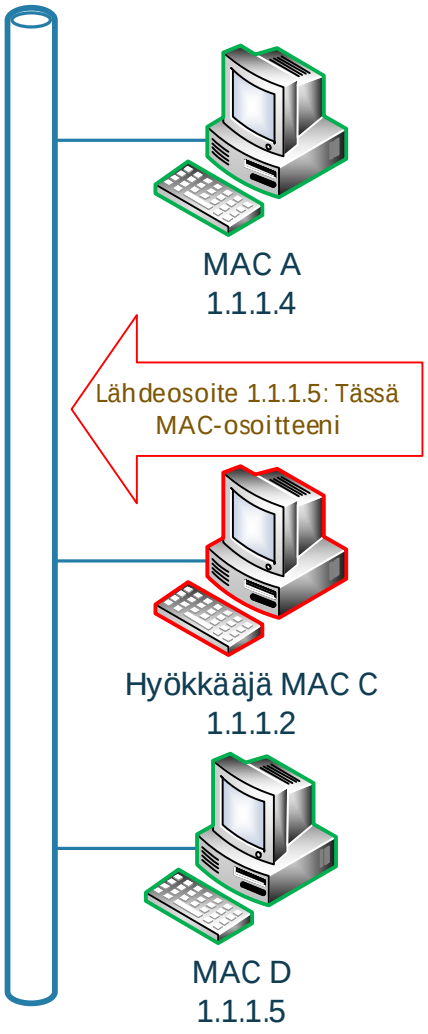
ARP:a (Address Resolution Protocol) käytetään saman yhteislähetysalueen sisällä kohdelaitteiden MAC-osoitteiden selvittämiseen. Kaikki samalla yhteislähetysalueella olevat laitteet saavat kaikki ARP-pyynnöt, eikä ARP-pyynnön lähettäjällä ole mekanismia ARP-vastauksen oikeellisuuden tarkastamiseen tai vastaajan oikeellisuuden tarkastamiseen (kuva 16).



Kuva 16. Kone 1.1.1.4 lähettää ARP-kyselyn verkkoon. Normaalitilanteessa kaikki paitsi kone MAC D hylkäisivät kyselyn.

Hyökkääjä voi vastata kaikkiin tai vain joihinkin verkossa näkemiinsä ARP-kutsuihin (kuva 17). Vastaamalla ARP-kutsuihin väärennetyin tiedoin voidaan ohjata ARP-kutsun

lähettäneen laitteen liikenne hyökkääjän haluamaan suuntaan tai reitittää hyökättävän kohteen liikenne hyökkääjän kautta, jolloin on mahdollista tehdä MITM-hyökkäys. Vaihtoehtoisesti hyökkääjä voi tehdä palvelunestohyökkäyksen vastaamalla kaikkiin ARP-pyyntöihin väärennetyin tiedoin. ARP-hyökkäyksiin ja sen kautta tehtäviin MITM-hyökkäyksiin on valmiit ohjelmistot Dsniff-työkalupaketissa.



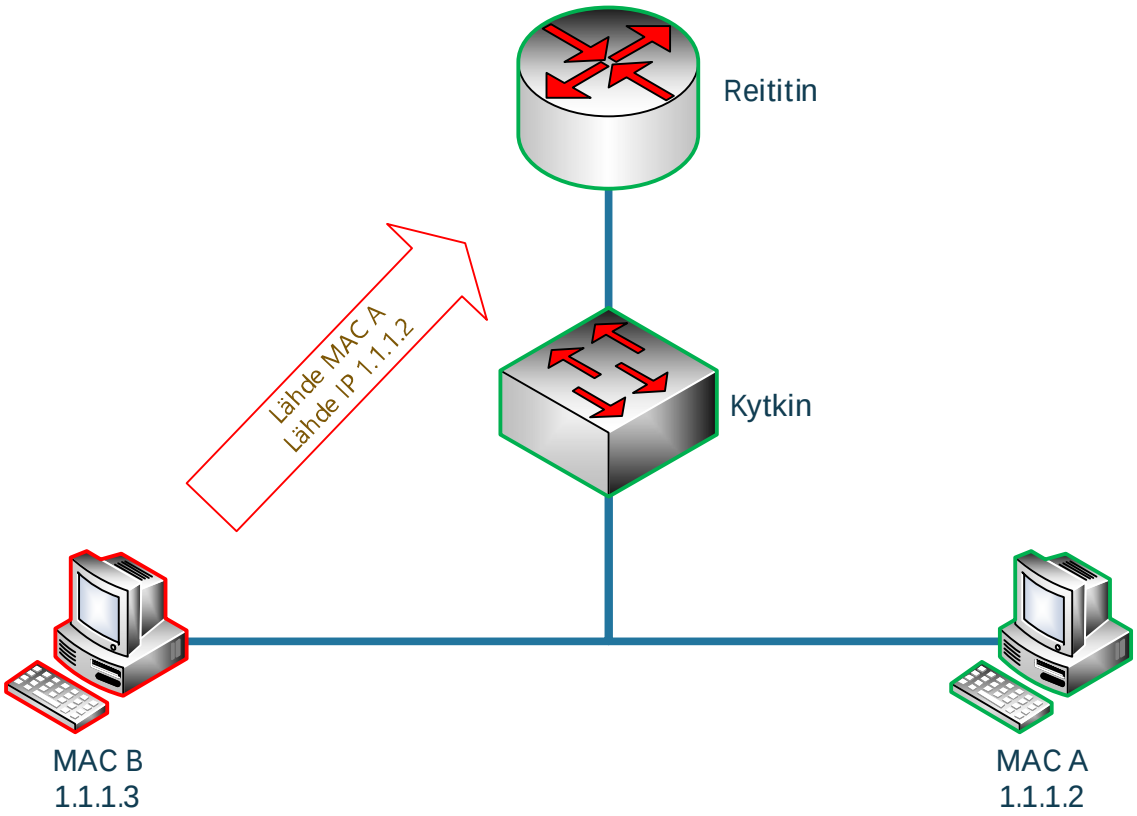
Kuva 17. Hyökkääjä vastaa kyselyyn väärennetyllä lähde-IP-osoitteella ja antaa oman MAC-osoitteensa. Kone 1.1.4. tallentaa ARP-tauluunsa hyökkääjän MAC-osoitteen.

ARP-hyökkäystä vastaan voi suojautua DAI:lla (Dynamic ARP Inspection). Se käyttää apunaan DHCP snooping -tilataulua. Kun jokin verkossa oleva laite vastaa ARP-kyselyyn, kytkin vertaa ARP-vastauksen lähettäjän tietoja (MAC-osoite, IP-osoite, kytkinportti) sen DHCP snooping -tauluun. Mikäli lähettäjän tiedot täsmäävät, paketti sallitaan. Muussa tapauksessa kytkin hylkää ARP-vastauksen. Mikäli verkossa on laitteita, jotka eivät ole DHCP-asiakkaita, niiden tiedot määrittää täytyy manuaalisesti DHCP snooping

-tauluun, jotta DAI toimii oikein. Mikäli verkossa on käytössä port security, määrittämällä kytkinporttiin kytketyn laitteen MAC-osoitteen staattiseksi voidaan myös rajoittaa väärennettyjä ARP-viestejä [12, s. 50–57;13, s. 353].

IP- ja MAC-väärennös

Väärentämällä IP- ja MAC-osoitteensa hyökkääjä voi hyväksikäyttää verkon luottosuhteita, jotka perustuvat MAC- ja IP-osoitteisiin tai tehdä palvelunestohyökkäyksen muita verkon käyttäjiä kohtaan (kuva 18).



Kuva 18. Väärentämällä MAC- ja IP-osoitteensa hyökkääjä saa itsensä näyttämään samalta kuin kone MAC A.

IP/MAC-väärennöstä vastaan voi suojautua IP source guardilla (lähdevahti). Se vaatii toimiakseen DHCP snoopingin ja DAI:n käytön. IP source guardin toiminallisuus on sama kuin DAI:n, sillä erotuksella, että se tutkii jokaisen kytkimelle saapuvan paketin oikeudellisuuden pelkkien ARP-pakettien sijaan. IP source guardilla voi tarkastaa ja IP-osoitteen että MAC-osoitteen oikeellisuuden [12, s. 69–75].

LLDP- ja CDP-vuoto

CDP (Cisco Discovery Protocol) ja LLDP (Link Layer Discovery Protocol) ovat protokollia, joiden on tarkoitus levittää laitetietoja lähiverkossa. CDP on Ciscon laitteissa oletusarvoisesti päällä. CDP ja LLDP lähettävät tasaisin väliajoin kaikista verkkoporteistaan Ethernet-kehyksen, jossa voi olla kuvattuna laitteen IP-osoite, ohjelmistoversio, natiivi VLAN-tunnus ja niin edelleen. Protokolla voi siis tahattomasti antaa tiedustelutietoa verkkoon luvattomasti kytkeytyville henkilöille, ja suosituksena onkin ottaa CDP / LLDP pois käytöstä, mikäli sitä ei tiedä tarvitsevansa [12, s. 85].

3.3 Kytkimien valvonta ja hallinta

> Jos et valvo sitä, et hallitse sitä [14, s. 523].

Järjestelmän tai verkon valvonta on osa sen hallintaa. Valvomalla järjestelmää voi havaita ongelmia, havaita ongelmien aiheuttajia ja välttää syntymässä olevia ongelmia. Verkkoa voi valvoa reaaliaikaisesti tai keräämällä historiallista dataa verkon rasituksesta ja käytettävyydestä

Historiallinen monitorointi

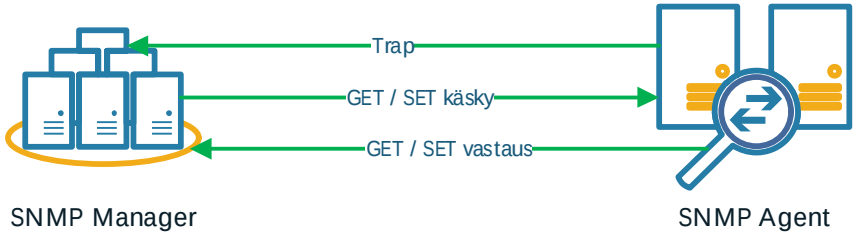
Historiallista monitorointia käytetään järjestelmän pitkäaikaisen käytettävyysajan, käytön ja toiminnan tilastointiin. Historiallinen monitorointi toimii lähettämällä määritetyin väliajoin kohdelaitteille kyselyitä laitteen tilasta. Kytkimen valvottavia arvoja voivat olla esimerkiksi kytkinporttien käyttöaste (syntynyt pullonkaula tiedonsiirrossa) ja kytkimen lämpötila (laite on määritysten mukaisessa lämpötilassa) [14, s. 526].

Reaaliaikainen monitorointi

Reaaliaikaisella monitoroinnilla tarkoitetaan monitorointijärjestelmää, joka kertoo käyttäjälleen valvottavissa laitteissa tapahtuvista tilamuutoksista, jotka vaativat käyttäjän tai jonkun muun toimenpiteitä. Tapahtumia voi olla esimerkiksi jonkin päätelaitteen katoaminen verkosta, jokin palvelu ei vastaa, laitteen ohjeellinen lämpötila on ylittynyt, kytkinportin tila on muuttunut ja niin edelleen. Tapahtumien seurauksena on mahdollista lähettää tekstiviesti, sähköpostiviesti tai jollain muulla tavalla hälyttää käyttäjiä siitä, että verkossa on tapahtunut muutoksia, jotka vaativat reagointia. [14, s. 527].

Yksinkertainen verkonhallintaprotokolla

Yksinkertainen verkonhallintaprotokolla (Simple Network Management Protocol, SNMP) on standardisoitu järjestelmänhallinta- ja monitorointiprotokolla IP-verkoissa oleville laitteille. Järjestelmä koostuu yksinkertaisimmillaan managerista ja yhdestä agentista. Agentilla tarkoitetaan valvottavassa tai hallittavassa laitteessa sijaitsevaa SNMP-ohjelmistoa. SNMP:ssa on standardisoitu, laitekohtainen (reititin, kytkin, PC, modeemi ja niin edelleen) muuttujatietokanta nimeltään MIB (Management Information Base). SNMP manager eli hallintapalvelin pyytää tietoja agentilta esimerkiksi käskyllä GET, vaihtaa agentin asetuksia käskyllä SET ja agentin itse lähettämiä tietoja sanotaan trapeiksi. Managerin ja agentin väliset viestit ovat kuvattu kuvassa 19.



Kuva 19. SNMP-managerin ja SNMP-agentin välittämät viestit.

Reaaliaikaiseen monitorointiin vahvasti liittyvä SNMP:n ominaisuus on trap, joka lähettää agentilta managerille tietoja, kun laitteella tapahtuu muutoksia, joita halutaan valvoa reaaliaikaisesti. SNMP:a ei koeta riittävän turvalliseksi laitteiden konfiguraatiomuutoksiin, ja monitorointiinkin olisi suositeltavaa käyttää SNMP:n versiota 3 [14, s. 528–529; 15]. Kytkimien MIB on määritelty standardissa 802.1Q.

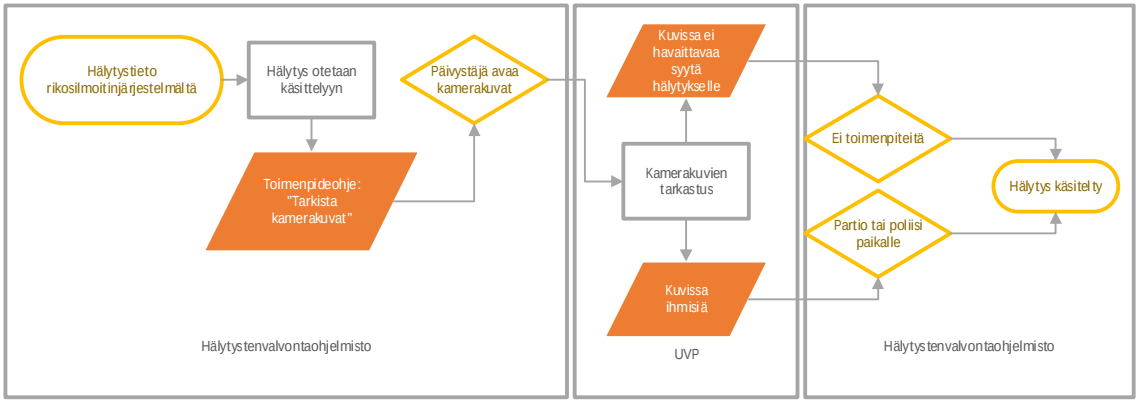
4 Securitaksen palvelut

Kameravalvontaverkon suorituskyvyn ja ominaisuuksien tulee vastata Securitaksen palveluiden asettamia vaatimuksia.

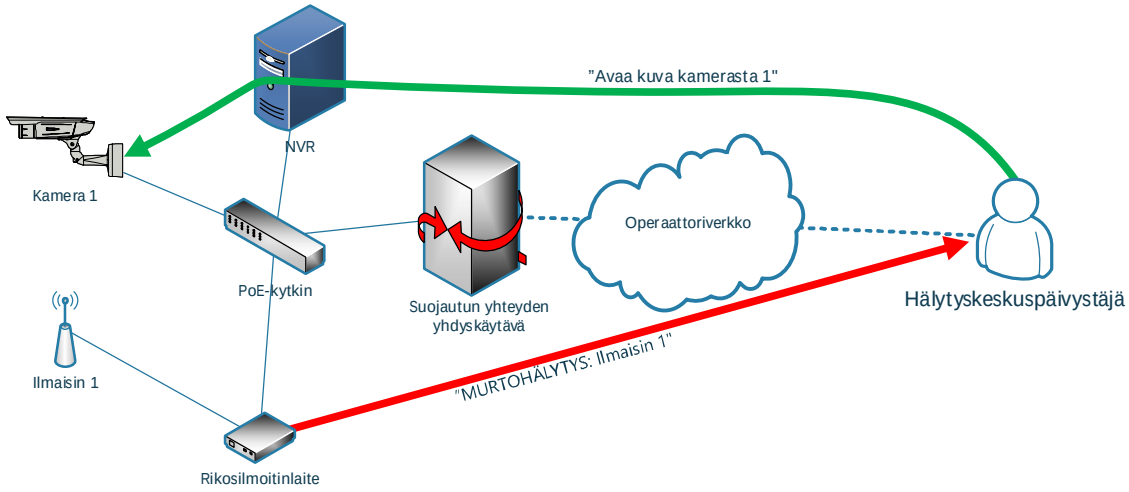
4.1 Hälytyskuvavalvonta

Securitaksen vastaanottaessa asiakkaan rikosilmoitinlaitteelta murtohälytyksen, voi hälytyskeskuspäivystäjä tarkistaa suojatun yhteyden avulla kameravalvontajärjestämän

nauhoitteet ja mitoittaa jatkotoimenpiteet kameratallenteista saadun tiedon perusteella (kuvat 20 ja 21) [16].



Kuva 20. Securitaksen hälytystenkäsittelyprosessi



Kuva 21. Sensoritiedon yhdistäminen rikosilmoitinlaitteelta ja valvontakamerajärjestelmästä.

4.2 Valvontakamerakierrokset ja etäohjaukset

Securitas tuottaa asiakkailleen sopimuksen mukaan kameravalvontakierroksia ja esimerkiksi porttien etäavausta, jossa pääsyoikeus todetaan valvontakameralla ja puhelimitse [17].

4.3 Valvontakamerajärjestelmien etähuollot

Suojatut etätyöpöytä-, terminaali- ja www-yhteydet mahdollistavat valvontakameroiden, valvontapäätteiden ja valvontakameratallentimien etähuollot ja -diagnoosit. Parhaimmillaan huoltomiestä ei tarvitse lähettää ollenkaan paikalle, tai huoltomiehelle saadaan jo ensimmäiselle huoltokäynnille oikeat varaosat mukaan [17].

4.4 Valvontakameratallenteiden nouto

Securitaksen hälytyskeskus suorittaa jo hälytyksen yhteydessä kriittisimpien tietojen hankinnan ja mahdollisen välittämisen poliisille. Esimerkiksi kaupan alalle Securitas tarjoaa palvelua, jossa ilmoitettua rikosaikaa vasten noudetaan valvontakameratallenteet näpistyksestä tai varkaudesta, laaditaan rikosilmoitus asiakkaan valtakirjalla ja lähetetään tallenteet poliisille.

4.5 Verkkoaika

Verkkoaikapalvelulla taataan kameravalvontatallenteiden pysyminen ajassa ja esimerkiksi vikadiagnostiikkalokien pysyminen oikeassa kronologisessa järjestyksessä.

4.6 Combi-järjestelmät

Securitas myy ja toimittaa kameravalvontajärjestelmiä myös itse käyttäen kumppaineinaan alan parhaita toimijoita. Kameravalvontajärjestelmiä myydään erityisesti niin sanottuina combi-palvelutuotteina, jolloin asiakas ei tee investointeja vaan kameravalvontajärjestelmä kaikkine osineen vuokrataan Securitakselta. Combi-sopimuksissa yhden sopimuskauden pituus voi olla jopa 60 kuukautta, jolloin järjestelmien luotettavuus, kestävyys ja elinkaaren hallinta on tärkeää [18].

5 Vaatimusmäärittely ja yhteenveto

Insinöörityössä oli tavoitteena luoda kameravalvontakytkimien vaatimusmäärittely. Valittavan kytkinmalliston tulee täyttää kameravalvontajärjestelmän, kameravalvontajärjestelmän rakenteen, riittävän tietoturvan, hallittavuuden, suorituskyvyn ja Securitaksen palveluiden asettamat vaatimukset. Vaatimusmäärittelyt siis pohjautuvat työssä aikaisemmin esiteltyihin tekniikkoihin. Vaatimusmäärittelyn perustana on keskikokoinen, enintään noin 50 kameran kytkinverkko [4].

Verkon rakenne

Kytkinverkko voi rakentua 1–6 kytkimestä, joiden porttimäärä voi vaihdella 1:n ja 48:n välillä. Osa kytkimistä on oltava mahdollista liittää toisiinsa käyttäen OS1-, OS2-, OM2- tai OM3-kuitukaapelointia. Kytkinverkko tulisi voida määrittää rengastopologiaa käyttäväksi pinoksi. Mikäli kuitenkaan pinoa ei voida käyttää, on huolehdittava, ettei koko verkon toiminta riipu yksittäisestä kytkennästä, jolloin mahdolliset heikot kohdat on varmistettava joko kahdennetulla linkillä tai RSTP-topologian ja varmentavan kytkentäreitin avulla. Kytkinverkon tulee olla jaettavissa eri virtuaalisiin lähiverkkoihin.

Kytkimen suorituskyky

Kytkimen on pystyttävä tuottamaan riittävä teho valvontakameroille. Tehontarvetta voidaan arvioida tapauskohtaisesti. Voidaan kuitenkin todeta, että mitä suurempi tehobudjetti, sitä suuremman liikkumavaran ja helpomman suunniteltavuuden kytkin takaa.

Mikäli kameravalvontajärjestelmässä on yli 12 kameraa, sen kytkimissä on oltava 1 Gbps:n portteja käytettäväksi kytkimien välillä ja kameravalvontatallenninta varten. Kytkimessä tulee olla myös SFP-portteja, mikäli käytössä on kuitukaapelointeja.

Kytkimen hallinta

Kytkimen tulee olla hallittavissa SNMPv3-protokollalla. Kytkimeen tulee olla mahdollista määrittää automaattiset raportointiasetukset järjestelmän historiallista valvontaa varten. Kytkimen tulee olla mahdollista määrittää raja-arvot kytkimen tapahtumille, kuten esimerkiksi kytkinporttien tilamuutoksille tai hallintaliittymän hyväksytyille ja hylätyille kirjautumisyrityksille.

Tietoturva

Kytkimellä tulee pystyä estämään luvaton verkkoon kytkeytyminen MAC-osoitteen sidonnalla, luvattomien DHCP-palvelimien toiminta, hyökkäys kytkimen CAM-taulua vastaan rajoittamalla MAC-osoitteiden määrää kytkinporttia kohden ja estää MAC- ja IP-osoitteen väärentäminen. Kaikista estetyistä yrityksistä on pystyttävä raportoimaan.

5.1 Laitteiston valinta

Vaatimusmäärittelyn perusteella voidaan rakentaa pohjavaatimukset sille, minkälaisia kytkimiä ja minkälaisia kytkinverkkoja Securitas voi rakentaa asiakkailleen. Mikäli pohjavaatimuksista joustetaan, tulee tiedostaa puuttuvien ominaisuuksien aiheuttamat seuraukset ja riskit. Vertailtaviksi vaihtoehdoiksi valittiin sellaisten laitevalmistajien kytkimet joita toimittaa useampi kuin yksi Securitaksen käyttämä tukkuri (taulukko 1). Vertailtavat kytkimet valittiin niin, että käytettävissä olisi 8–12-porttinen ja 24-porttinen kytkin. Kaikkien vertailtavien kytkimien kaikki portit ovat nopeudeltaan vähintään 1 Gbps.

Vertailtavat kytkimet ovat Hewlett-Packard Enterprisen 1920-sarjan kytkimet, Juniper Networksin EX2200- ja EX2200C-sarjan kytkimet, Cisco Systemsin 2960C- ja 2960X-sarja, Fortinetin D-sarja ja D-Linkin DGS-1210-sarja. Pino-ominaisuuksia vertailtaessa on huomioitu, onko pino-ominaisuus hallinnollinen (H) tai liikenteellinen (L).

Taulukko 1. Kytkinominaisuuksien vertailumatriisi 19; 20; 21; 22; 23; 24; 25].

	HPE 1920	**Juniper EX2200 / C**	**Cisco 2960 C / X**	**Fortinet D-Series**	**D-Link DGS-1210**
Pino	32 kpl (H)	4 kpl (L)	X-mallit, 8 kpl, (L)	16 kpl, (L)	Ei
802.1Q	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä

SFP-portit	2 – 4 SFP	2 – 4 SFP	2 – 4 SFP	2– 4 SFP+	2 – 4 SFP
SNMPv3	Kyllä	Kyllä	Kyllä	Kyllä	Ei
PortSecurity	Kyllä	Kyllä	Kyllä	Kyllä	Kyllä
DAI	Kyllä	Kyllä	Kyllä	FortiLink	Kyllä
DHCP Snoo-ping	Ei	Kyllä	Kyllä	FortiLink	Ei
IP Source Guard	Ei	Kyllä	Kyllä	FortiLink	Ei
PoE, wattia	15 / 15	8,3 / 16,9	10,3 /15,5	9,4 / 15	9,8 / 8,0

Vertailutaulukon perusteella voidaan valita lähempään tarkasteluun Juniperin, Ciscon ja Fortinetin kytkimet. Niiden osalta kytkinpino-ominaisuudet eivät ole suoraan vertailukelpoisia. Cisco tarjoaa pino-ominaisuutta pelkästään 2960X-sarjan 24- ja 48-porttisille kytkimille. Juniperin pino-ominaisuus on käytettävissä niin, että vain EX2200-sarjaa (24- ja 48-porttiset) tai EX2200C-sarjaa (12-porttiset) voidaan pinota keskenään. Fortinetin D-Series-kytkimillä on käytettävissä pino-ominaisuus, joka mahdollistaa 16 erikokoisen kytkimen pinoamisen. Fortinetin Dynamic ARP Inspection, DHCP Snooping ja IP Source Guard ovat käytettävissä vain, jos niiden kanssa käytetään Fortinetin FortiGate-palomuuria.

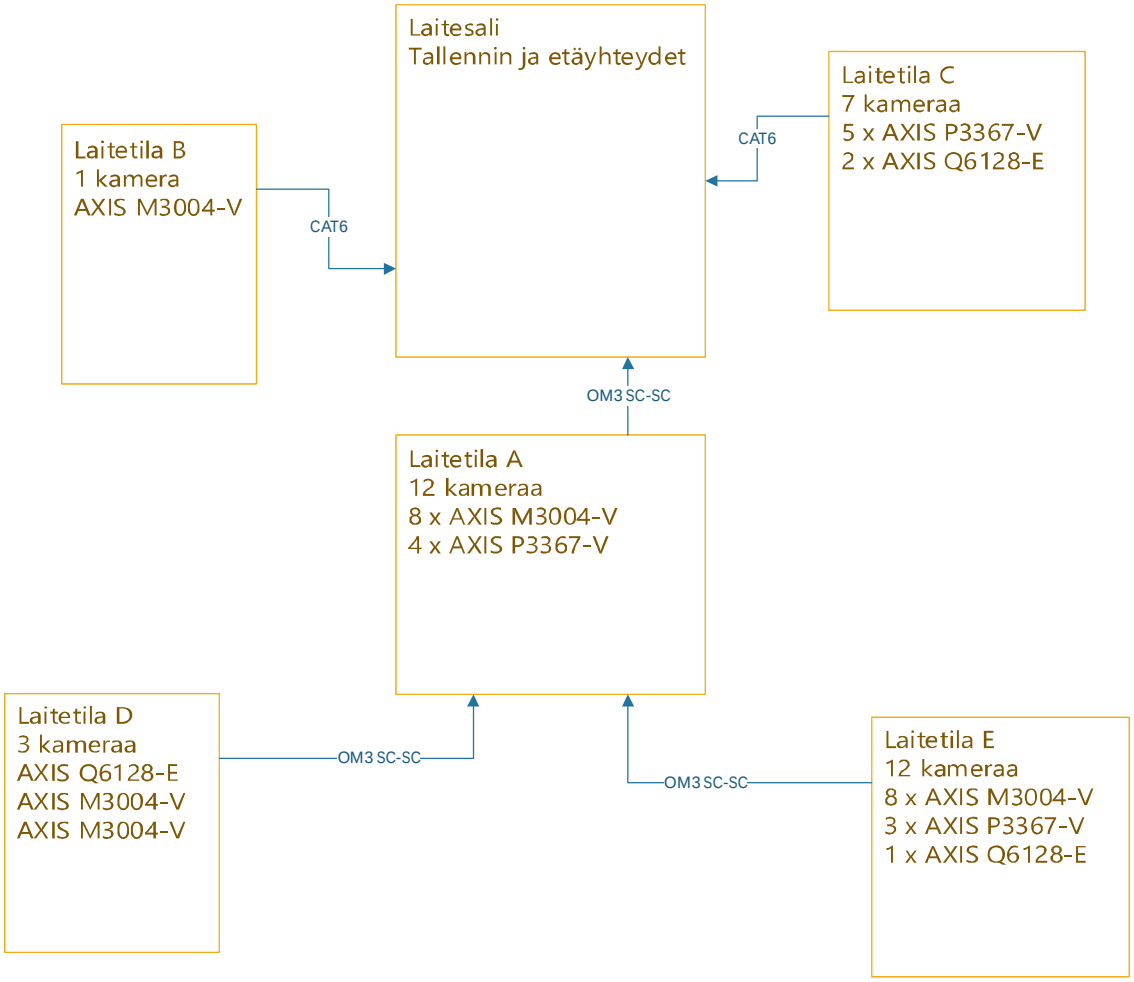
Vertailun perusteella Juniperin EX2200-kytkimet täyttävät vaatimukset parhaiten.

5.2 Verkon suunnittelu, toteutus ja ylläpito

Verkon suunnitteluun tarvitaan tiedot verkkoon liitettävien laitteiden määrästä, niiden vaatimasta PoE-tehosta, niiden fyysisistä kytkennöistä, kaapeloinnista, kaapelointityypistä ja kytkentärimojen tyypistä. Kuvassa 22 olevilla tiedoilla voidaan laskea tarvittava kytkimien määrä jakunkin kytkimen tarvitsema vähimmäisporttimäärä ja valita oikeat SFP GBIC -liittimet kuituliitäntöjä varten. Kytkinkohtaisen PoE-tehon vaatimukset voi laskea laskentataulukolla (esimerkki taulukossa 2) tai Axiksen suunnittelutyökalulla [26].

Taulukko 2. Kuvan 22 mukaisen laitetila E:n kameroiden yhteenlaskettu PoE-teho [27; 28; 29].

Laitetila E	Kameran maksimi PoE-teho	Kameroiden lukumäärä	Kokonaisteho
Axis M3004-V	4 W	8	32 W
Axis P3367-V	7 W	3	21 W
Axis Q6128-E	30 W	1	30 W
Yhteensä			83 W



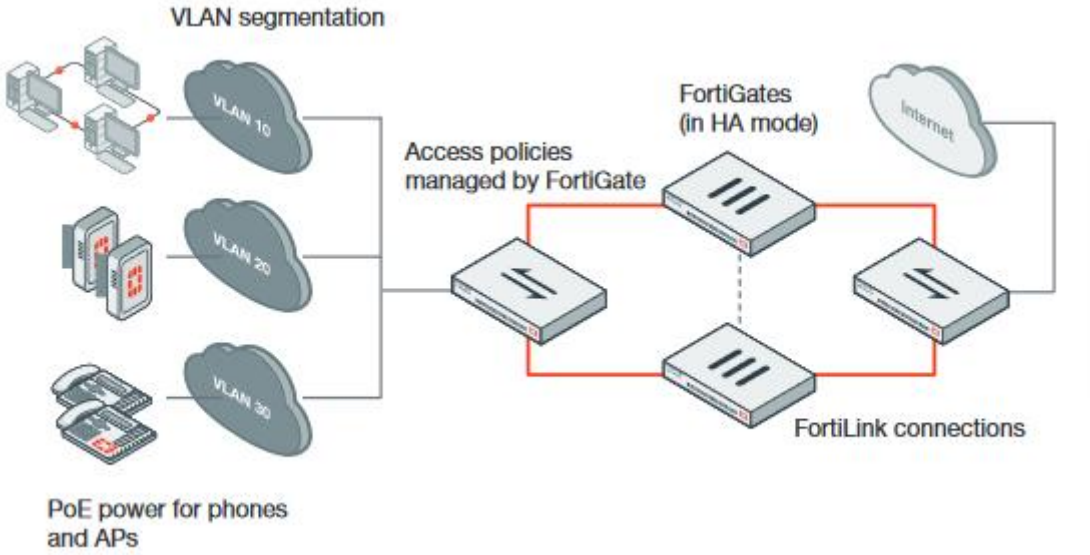
Kuva 22. Eri laitetiloihin kaapeloitavien laitteiden määrät ja laadut kuvattuna ja laitetilojen sijainnit suhteessa toisiinsa. Esimerkki.

5.3 Yhteenveto ja pohdinta

Insinöörityön tavoitteena oli luoda pohja Securitas Oy:n kameravalvontaverkkojen suunnittelulle ja hallittavuuden ja tietoturvan parantamiselle. Aikaisemmin kameravalvontaverkon suunnittelu on lähtenyt aina puhtaalta pöydältä. Käytössä on ollut vakioituja kytkimiä, mutta niiden ominaisuuksien valinnalle ei ole ollut syvällistä pohjaa. Työn tuloksena pystyn määrittämään teknisen alarajan Securitaksen käyttämille kytkimille.

Vaatimusmäärittelyn perusteella Juniperin kytkimet olisivat soveliain valinta kameravalvontaverkon kytkimiksi, mutta tuotteiden spesifikaatioita tutkiessa kävi ilmi, että Fortinetin palomuurit, kytkimet ja WLAN-tukiasemat pystytään yhdistämään yhdeksi hallittavaksi loogiseksi kokonaisuudeksi, esitettynä kuvassa 23. Yhdeltä FortiGate-palomuurilta

pystytään hallitsemaan yhdestä käyttäjänäkymästä kaikkien samassa verkossa olevien Fortinet-kytkimien asetukset ja tapahtumat [21].



Kuva 23. FortiLink-järjestelmä [21].

Fortinetin tarjoamien mahdollisuuksien vuoksi jatkan tuotteistusta Fortinetin tuotteilla.

Mikäli ei tehdä selviä rajauksia ja vaatimuksia kameravalvontaverkon laitteiden ominaisuuksille, voi kameravalvontaverkon muoto olla melkein mitä tahansa ja erilaiset laitekonfiguraatiovariaatiot ovat loputtomia. Laitteita, laitteiden suorituskykyjä, asennustapoja, laitteiden käyttötapoja ja muita seikkoja normittamalla voidaan myös normittaa verkon rakennetta. Verkon rakenteen standardisoituessa asiantuntijaresursseja ei tarvitse käyttää hieman erilaisiin, mutta silti toistuviin tehtäviin. Asiantuntijatyötä voidaan alkaa monistaa. Kuitenkin äärimmilleen räätälöityjen verkkojen suunnittelu on jatkossa helpompaa, kun on tiedossa seikat, jotka olennaisesti vaikuttavat kameravalvontaverkon toimintaan.

On kuitenkin huomioitava, että koko kameravalvontajärjestelmän suojaaminen on paljon muutakin kuin pelkästään kytkimen tietoturvaominaisuuksien säätely. Jokaisen verkossa olevan komponentin tekniset tietoturvaseikat on huomioitava erikseen, ja teknisen tietoturvan lisäksi on huomioitava fyysinen turvallisuus ja henkilöstöturvallisuus. Kameravalvontajärjestelmän tärkein suojattava osa on kameravalvontatallennin, sillä valvontakameratallenne muodostaa automaattisesti henkilötietolain mukaisen henkilörekisterin,

jonka käsittelyä ja suojausta määrittää henkilötietolaki. Asiakkaalle kameravalvontajärjestelmän tuottamat funktiot ovat hälytyskuvavalvonnan lisäksi rikosten tai muiden tapahtumien jälkiselvitys. Ilman tallenteita ei voida selvittää rikoksia, ja ilman toimivia kamerayhteyksiä ei voida toimittaa Securitaksen palveluita.

Kytkintopologioiden määrittämisestä, tietoturvakysymysten avaamisesta, valvonnan ja hallinnan helpottamisesta ja lopullisesta laitevalinnasta on vielä pitkä matka turvallisten kameravalvontaverkkojen toteutukseen. Kun käytettävät laitteet on valittu, on neuvoteltava tukkureiden kanssa tilaus- ja toimitusprosessista ja neuvoteltava hinnat, koulutettava myyjille myyntiargumentit, koulutettava projektipäälliköt dokumentoimaan riittävällä tarkkuudella, perustettava dokumenttivarastot sekä perustettava ja määritettävä valvonta- ja hallintajärjestelmät.

Insinöörityön tekeminen avarsi silmiäni varsinkin kytkinverkkojen tietoturvaan liittyen. Hyökkäysohjelmistoja on helposti saatavilla ja hyökkäyksillä voidaan tehdä merkittäviäkin tietomurtoja. Havaitsin myös, että kameravalvontaan ja turvallisuusjärjestelmiin liittyvää julkista tietoa on vaikeasti saatavilla tai sitä ei ole edes olemassa. Tulen käyttämään kytkinverkon suojauksesta oppimiani asioita työssäni ja aion myös syventää osaamistani samalla osa-alueella.

Lähteet

1 Takala, Hannu. 1998. Videovalvonta ja rikollisuuden ehkäisy. Verkkodokumentti. <http://www.rikoksentorjunta.fi/material/attachments/rtn/rtn/julkaisut/julkaisutoptula/6CexHGV1S/Videovalvonta_ja_rikollisuuden_ehkaisy.pdf>. Luettu 16.2.2017.

2 Sallinen, Pekka. 2010. Kameravalvontaopas. Verkkodokumentti. <http://www.turva-alanyrittajat.fi/doc/kameravalvonta/KAMERAVALVONTA-OPAS_2010.pdf>. Luettu 17.2.2017.

3 DS-7600NI-I2/8P(16P) Embedded Plug & Play NVR. 2017. Verkkodokumentti. Hikvision Hangzhou. <http://www.hikvision.com/europe/Products_accessries_212_i8840.html>. Luettu 30.3.2017.

4 Bandwidth and storage considerations. 2017. Verkkodokumentti. Axis Communications AB. <https://www.axis.com/ng/en/learning/web-articles/technical-guide-to-network-video/bandwidth-considerations>. Luettu 2.4.2017.

5 802.1Q-2014 IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks. 2017. Verkkodokumentti. Institute of Electrical and Electronics Engineers. <http://standards.ieee.org/getieee802/download/802-1Q-2014.pdf>. Luettu 22.2.2017.

6 IEEE 802.11™: Wireless Lans. 2017. Verkkodokumentti. Institute of Electrical and Electronics Engineers. <https://standards.ieee.org/getieee802/download/802.11-2012.pdf>. Luettu 4.3.2017.

7 Managing a FortiSwitch unit with a FortiGate. 2017. Verkkodokumentti. Fortinet. <http://docs.fortinet.com/uploaded/files/2439/manageFSWfromFGT52.pdf>. Luettu 1.4.2017.

8 ICX 6430 and ICX 6450 stack topologies. 2017. Verkkodokumentti. Brocade. <http://www.brocade.com/content/html/en/configuration-guide/fastiron-08030b-switchstackingguide/GUID-778EF90A-B65D-467F-8AFB-14C893020F2F.html>. Luettu 2.4.2017.

9 Catalyst 3850 Switch Hardware Installation Guide. 2017. Verkkodokumentti. Cisco Systems Inc. <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/hardware/installation/guide/b_c3850_hig/b_c3850_hig_chapter_010.html>. Luettu 2.4.2017.

10 Halkosaari, Antti. 2014. Kameravalvonnan nykytila. Verkkodokumentti. <http://urn.fi/URN:NBN:fi:amk-2014112016160>. Luettu 1.4.2017.

11 Rikoslaki. 540/11.2.2007.

12 Bhaiji, Yusuf. 2009. Understanding, Preventing, and Defending Against Layer 2 Attacks. Verkkodokumentti. <http://www.cisco.com/c/dam/global/en_ae/assets/exposaudi2009/assets/docs/layer2-attacks-and-mitigation-t.pdf>. Luettu 18.2.2017.

13 Fortiswitch administration guide. 2012. Verkkodokumentti. Fortinet. <http://docs.fortinet.com/uploaded/files/1415/fortiswitch-548b-admin-v5202.pdf>. Luettu 2.4.2017.

14 Limoncelli, Thomas A. 2007. The Practice of System and Network Administration. Crawfordsville, Indiana: RR Donnelley.

15 Harrington, D. 2002. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. Verkkodokumentti. < https://www.ietf.org/rfc/rfc3411.txt>. Luettu 3.4.2017.

16 Hälytyskeskuspalvelut. 2017. Verkkodokumentti. Securitas Oy.<http://www.securitas.fi/fi/turvallisuuspalvelut/halytyskeskuspalvelut/>. Luettu 18.2.2017.

17 Etäpalvelut. 2017. Verkkodokumentti. Securitas Oy. <http://www.securitas.fi/globalassets/finland/files/esitteet/etapalvelut_suojattu.pdf> Luettu 18.2.2017.

18 Combi-palvelut. 2017. Verkkodokumentti. Securitas Oy. <http://www.securitas.fi/fi/turvallisuuspalvelut/turvallisuustekniikka/Combi-kokonaisratkaisu/>. Luettu 18.2.2017.

19 Cisco Catalyst 2960-X Series Switches Data Sheet. 2017. Verkkodokumentti. Cisco Systems Inc. <http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html>. Luettu 9.4.2017.

20 Cisco Catalyst 2960-C and 3560-C Series Compact Switches. 2017. Verkkodokumentti. Cisco Systems Inc. <http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-c-series-switches/data_sheet_c78-639705.pdf>. Luettu 9.4.2017.

21 FortiSwitch™ Secure Access Series. 2017. Verkkodokumentti. Fortinet. <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSwitch_D_Series.pdf>. Luettu 9.4.2017.

22 EX2200 Ethernet Switch. 2017. Verkkodokumentti. Juniper Networks. <https://www.juniper.net/us/en/local/pdf/datasheets/1000307-en.pdf>. Luettu 9.4.2017.

23 Compact EX2200-C Ethernet Switch. 2017. Verkkodokumentti. Juniper Networks. <https://www.juniper.net/us/en/local/pdf/datasheets/1000388-en.pdf>. Luettu 9.4.2017.

24 HPE OfficeConnect 1920 Switch Series. 2017. Verkkodokumentti. Hewlett-Packard Enterprise. <https://www.hpe.com/h20195/v2/GetPDF.aspx/c04394247.pdf>. Luettu 9.4.2017.

25 DGS-1210 Series Gigabit Web Smart Switches. 2015. Verkkodokumentti. D-Link Corporation. <http://content.us.dlink.com/wp-content/uploads/2015/01/DGS-1210_REVC_DATASHEET_1.00_EN_US.pdf>. Luettu 9.4.2017.

26 Axis Design Tool. 2017. Verkkodokumentti. Axis Communications AB. <https://www.axis.com/au/en/tools/axis-design-tool>. Luettu 11.4.2017

27 AXIS P3367-V Network Camera. 2017. Verkkodokumentti. Axis Communications AB. <https://www.axis.com/files/datasheet/ds_p3367v_1471716_en_1702.pdf>. Luettu 11.4.2017.

28 Axis M3004-V Network Camera. 2017. Verkkodokumentti. Axis Communications AB. <https://www.axis.com/files/datasheet/ds_m3004v_1485629_en_1605.pdf>. Luettu 11.4.2017.

29 Axis Q6128-E Network Camera. 2017. Verkkodokumentti. Axis Communications AB. <https://www.axis.com/files/datasheet/ds_q6128e_1499380_en_1610.pdf>. Luettu 11.4.2017.