Nätverksuppbyggnad för kameraövervakning

Tomas Strand

Examensarbete

Informations och medieteknik

2014

Tomas Strand

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informations- och medieteknik
Identifikationsnummer:	4668
Författare:	Tomas Strand
Arbetets namn:	Nätverksuppbyggnad för kameraövervakning
Handledare (Arcada):	Göran Pulkkis
Uppdragsgivare:	Insinööritoimisto Fagertec Oy

Uppdragsgivaren Insinööritoimisto Fagertec Oy fick en förfrågan om de kunde realisera ett kameraövervakningssystem vid ett butiks- och hamnområde. Uppdragsgivaren hade ingen erfarenhet av kameraövervakning eller nätverkstekniker. Examensarbetet är en teknisk beskrivning för hur ett kameraövervakningssystem över ett större område på ett ekonomiskt sätt realiseras genom att använda befintligt kablage och trådlösa tekniker. Examensarbetet består av litteraturforskning och empirisk testning av behövlig utrustning. I examensarbetet framgår vilka kraven är på en nätverkslänk för att videoströmmar skall fungera felfritt, vilken lagstiftning man bör beakta och vilka rättigheter de som blir upptagna i videoinspelningarna har. Vidare har det tagits fram ett system som möjliggör realtidsvisning av specifika videoströmmar på ett säkert sätt över Internet. Tekniker för distansanvänding av kameraövervakningssystem på ett säkert sätt beskrivs. Realiseringen av kameraövervakningssystemet slutfördes i början av sommaren 2014.

Nyckelord:	Kameraövervakning, nätverkstekniker, Ethernet, videoströmmar, Insinööritoimisto Fagertec Oy
Sidantal:	41
Språk:	Svenska
Datum för godkännande:	16.12.2014

DEGREE THESIS	
Arcada	
Degree Programme:	Information and Media Technology
Identification number:	4668
Author:	Tomas Strand
Title:	Network design for camera surveillance systems
Supervisor (Arcada):	Göran Pulkkis
Commissioned by:	Insinööritoimisto Fagertec Oy

Insinööritoimisto Fagertec Oy got a request from a customer that wanted a camera surveillance system installed on its premises that consists of a shop, café, harbor, parking spaces and an outdoor inventory. Fagertec Oy had no experience in network technologies or camera surveillance systems. This thesis will function as a reference for choosing technologies that can be used for implementing a camera surveillance system using existing infrastructure as cabling and wireless technologies for a cost effective implementation. The work in the thesis is based on literature research and empiric testing of network and camera equipment. This report contains requirements for a network that is used for camera surveillance, what effects a poor connection has on the video streams, and the Finnish laws that one has to account for in the design and implementation process. A system for safe distribution of specific video streams from the surveillance system is described as well as techniques for remote operation of a camera surveillance system. The realisation of the video surveillance system was completed in the early summer of 2014.

Keywords:	Video surveillance , network technologies, Ethernet, video streams, Insinööritoimisto Fagertec Oy
Number of pages:	41
Language:	Swedish
Date of acceptance:	16.12.2014

INNEHÅLL

FIGURER

FÖRKORTNINGAR OCH BEGREPP

BNC	Kontakttyp för koaxialkablar
DVR	Digital Video Recorder, Digital video inspelare
EIA	Electronic Industries Alliance
FFMPEG	Multimedia ramverk för
H-264	Grupp av protokoll för att komprimera video
IEEE	Institution of Electrical and Electronic Engineers
IR	InfraRed, Infrarött ljus används för mörkerseende i övervaknings-kameror
LOIIA	Lag om integritetsskydd i arbetslivet 759/2004
MPEG4	Motion Picture Experts Group, en standard för att definiera kom-pression av ljud- och bilddata
NGINX	En webbserver baserad på öppen källkod
NVR	Network Video Recorder, Nätverksinspelare
OnVif	Open Network Video Interface Forum
OSI	Open Systems Interconnection model
P2MP	Point- to Multipoint
P2P	Point- to Point, Punkt- till punkt
PoE	Power over Ethernet

POTS	Plain Old Telephone Service
PUL	Personuppgiftslag 523/1999
RTMP	RealTime Messaging Protocol
RTP	Real-time Transport Protocol
SL	Strafflag 39/1889
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
UDP	User Datagram Protocol
UPS	Uninterruptable Power Supply, Störningsfri strömförsörjning
UTP	Unshielded Twisted Pair, en kabeltyp där två ledningar partvinnats för att motverka utomstående störningar.
WDS	Wireless Distribution System
VLC	Videolan Client, ett öppet källkodsprogram för uppspelning av multimedia
VPN	Virtual Private Network

1 INLEDNING

Examensarbetet har sitt ursprung i att Insinööritoimisto Fagertec Oy fick en förfrågan om att planera och installera ett kameraövervakningssystem för ett butiks- och hamnområde. Företaget i fråga sysslar i första hand med el-. vvs- och alarminstallationer. Erfarenhet av nätverk finns inte och där kommer mitt examensarbete in i bilden. Examensarbetet dokumenterar krav och tekniker som kan användas för att bygga upp ett nätverk för kameraövervakning.

Varför behövs kameraövervakning och vilken nytta har man av den? Under de senaste åren har kameraövervakningen blivit allt vanligare i butiker men även i gatubilden. (Kameravalvontaopas 2010).

Till vad används kameraövervakning? Kameraövervakning kan fungera som en tryggande faktor vid t.ex. kassor där pengar förvaras, eller vid bensinstationer vid pumparna för att motverka att kunden tankar och sedan kör iväg. Man kan anta att sådana stölder minskar ifall det tydligt syns att det finns övervakning på stället. Kameraövervakning kan även fungera bra för att förhindra skadegörelse i och på byggnader.

Övervakningen kan ske aktivt eller passivt. Den aktiva övervakningen kan ske i ett kontrollrum eller på en centralplats som övervakar flera områden. I den aktiva övervakningen finns det en eller flera personer som övervakar videoströmmarna, i sådana fall kan man snabbt reagera och t.o.m. förhindra brott. Sådan övervakning finns oftast i större butiker och varuhus där man från kontrollrummet kan kontakta vakter som patrullerar området. (Kameravalvontaopas 2010)

Vid passiv övervakning sparas videomaterial som kan gås igenom efter att en olycka skett eller ett brott uppdagats på platsen. Passiv övervakning kan i efterskott hjälpa att utreda brott som begåtts på det övervakade området. Då kan man efteråt gå igenom videoupptagningar från händelsen och på så sätt få en bättre bild av händelseförloppet. Passiv övervakning har liksom den aktiva också en avskräckande effekt.

1.1 Målsättning och syfte

Målsättningen är att få en dokumentation som kan användas vid planering av nätverk för kameraövervakning samt för att ge en överblick över vilka tekniker finns för användning av existerande kabeldragningar, exempelvis telefonkablar eller gammal koaxialkabel.

Dokumentationen omfattar även hur man realiserar en webbsida för visning av realtidsströmmar från kameror. Vilka tekniker som kan användas undersöks och testas.

1.2 Metoder

Mycket information finns redan i form av standarder och forskiningsdokument. Litteraturstudier är en stor del av detta arbete. Den praktiska delen består huvudsakligen av empirisk testning av olika kameror och nätverksutrustning för att komma fram till hur en bild-ström beter sig under dåliga nätverksförbindelser och vilka är minimikraven för att få en stabil bildström.

1.3 Avgränsningar

Eftersom examensarbete är gjort med tanke på teknisk realisering tas planering av placering och noggrannare val av kameror inte upp. För planering av kameraplaceringar och övervakningsområden har Finansbranschens Centralförbund publicerat en guide som tar upp hur man planerar uppbyggnaden av och strukturen hos ett kameraövervakningssystem (Finanssialan Keskusliitto, 2006). Examensarbetet fokuserar på den digitala nätverksbaserade kameraövervakningen, de analoga kameraövervakningssystemens detaljer beskrivs inte.

2 LAGSTIFTNING ANGÅENDE KAMERAÖVERVAKNING

Planering och implementering av övervakningssystem regleras av lagstiftning. I huvudsak är det Strafflagen, Lagen om integritetsskydd i arbetslivet och Personuppgiftslagen vilka innehåller bestämmelser som kan tillämpas på kameraövervakning.

2.1 Strafflagen

I strafflagens kapitel 24 finns momenten 5, 6 och 7 som behandlar Olovlig avlyssning, Olovlig observation och Förberedelse till olovlig avlyssning eller Förberedelse till olovlig observation.

Olovlig avlyssning är att någon obehörigt med teknisk anordning avlyssnar på en hemfridsskyddad plats ljud eller prat som inte är avsett för denne eller på en annan plats avlyssnar eller upptar ljudinspelningar utan att de som är på plats har skäl att anta att de avlyssnas. Straffet är då böter eller fängelse i högst ett år för *olovlig avlyssning. (SL kap24§5)*

Olovlig observation är att någon obehörigt med en teknisk utrustning iakttar eller avbildar en person på en hemfridsskyddad plats eller på en toalett, i ett omklädningsrum eller på annan motsvarande plats, eller på ett integritetskränkande iakttar eller avbildar en person som vistas i en sådan byggnad eller lokal eller på ett omgärdat område som avses i § 3 och dit allmänheten inte äger tillträde. Straffet är då böter eller fängelse i högst ett år för *olovlig observation*. (SL kap 24§6)

Om förberedelse till olovlig avlyssning eller förberedelse till olovlig observation stipuleras att den som placerar ut en anordning som avses i § 5 och § 6 skall dömmas till böter eller fängelse i högst sex månader för *förberedelse till olovlig observation/avlyssning*. (SL kap 24 § 7)

I § 3 specificeras platserna som refereras till i § 6 till:
”ämbetsverk, en affärslokal, ett kontor, en produktionsinrättning, en möteslokal eller någon annan motsvarande lokal eller byggnad eller på en sådan byggnads omgärdade gårdsområde, eller på ett kasernområde eller ett annat område som är i försvarsmaktens eller gränsbevakningsväsendets användning”. (SL kap 24 § 3)

2.2 Lagen om integritetsskydd i arbetslivet

Kapitel 5, Kameraövervakning på arbetsplatsen, handlar om hur man skall ordna kameraövervakning och vilka krav som ställs för att få använda den. Lagen ställer också krav

på att man skall överväga användningen av metoder som är mindre inskränkande på arbetstagarnas integritet.

Arbetsgivaren får i sina lokaler genomföra övervakning för att trygga säkerheten för arbetstagaren och andra som vistas i lokalerna samt för att skydda egendom. Man får dock inte övervaka en specifik arbetare eller vissa arbetstagare. Det är inte heller tillåtet att övervaka toaletter, omklädningsrum och andra personalutrymmen. Dock är det tillåtet att övervaka ett arbetsställe där det finns en uppenbar risk för våld samt för att hindra eller utreda brott mot egendom, exempelvis vid en kassa där pengar hanteras. På arbetstagarens begäran får även en specifik arbetstagare övervakas. (LOIIA kap 5 § 16)

I moment § 17 står det att arbetsgivaren vid planering och genomförandet av kameraövervakningen

1) skall utreda möjligheter att använda metoder som inte inskränker arbetstagarens integritet på samma sätt.
2) intrånget i arbetstagarens integritet inte är större än nödvändigt för ändamålet
3) behandling och användning av data som sparas görs i enhet med momenten 5-7, 10 och 32-34 § i personuppgiftslagen
4) upptagningar får endast användas för de ändamål för vilka observationen har utförts
5) arbetstagarna skall enligt 21§ meddelas att kameraövervakning genomförs och i vilka sammanhang upptagningarna får användas och meddelas kamerornas placering i enlighet med moment 2 i 16 §
6) informera om kameraövervakning på ett synligt sätt i de lokaler kameraövervakning sker

Arbetsgivaren får utan hinder av fjärde punkten och 21§ använda upptagningar för att

1) kunna påvisa att ett arbetsförhållande upphävts
2) utreda och bevisa trakasserier som aves i lagen om jämställdhet (609/1986) eller trakasserier och osakligt bemötande som avses i arbetarskyddslagen (738/2002)
3) utreda olycksfall i arbetet eller annan situation som orsakat fara eller risk som avses i arbetarskyddslagen

Arbetstagaren skall se till att upptagningarna genast förstörs när de inte behövs för sitt syfte, senast ett år efter upptagningen slutades. Om en upptagning är nödvändig för att slutföra en behandling av ett ärende som avses i moment 2 som varit aktuellt redan innan en ettårig tidsfrist eller om arbetstagaren behöver påvisa att ett arbetsförhållande upphävts eller om det finns andra särskilda skäl att spara upptagningen.

Ett i moment i sjunde kapitlets 21§, Samarbete vid ordnande av teknisk övervakning och användning av datanät, specificerar att arbetsgivaren skall samarbeta med arbetstagarna och informera dem om ändamålet och metoderna för övervakningen och användningen av datanät.

2.3 Personuppgiftslagen

I Personuppgiftslagen finns generella krav på hur register som innehåller personuppgifter skall hanteras. Lagen tillämpas på alla slag av personregister, dock inte register som är till för en fysisk persons privata bruk.

Personuppgifter definieras som alla slags anteckningar som beskriver en fysisk person eller hans egenskaper eller levnadsförhållanden som kan hänföras till honom själv eller till hans familj eller någon som lever i gemensamt hushåll med honom [PUL kap 1 § 3]

Personregister definieras som en datamängd som innehåller personuppgifter och som består av anteckningar som hör samman på grund av sitt användningsändamål, och som helt eller delvis behandlas med automatisk databehandling eller har ordnats som ett kartotek, en förteckning eller på ett annat motsvarande sätt så att information om en bestämd person kan erhållas med lätthet och utan oskäliga kostnader [PUL kap 1 § 3]

Registeransvarig är den eller de personer, sammanslutningar, inrättningar eller stiftelser för vilkas bruk ett personregister inrättats och vilka har rätt att förfoga över registret eller vilka enligt lag ålagts skyldighet att föra register.

Kapitel 2, Allmänna principer för behandling av personuppgifter ställer krav på hur personregistret behandlas och sparas. Det är den registeransvariges skyldighet att iaktta aktsamhet och god informationshantering för att säkerställa att den personliga integriteten inte begränsas utan grund i en annan lag. Samma skyldigheter har den som handlar för den registeransvarige, exempelvis en företagare som har hand om hela övervakningen. [PUL kap2 § 5]

Det ställs även krav på att användningen av personuppgifter skall vara sakligt motiverad med hänsyn till den registeransvariges verksamhet. [PUL kap 2 § 6]

Utdrag ur Moment § 8 i Personuppgiftslagen, som reglerar i vilka fall man får använda sig av personuppgifterna i personregistret:

1) med den registrerades entydiga samtycke,

2) på uppdrag av den registrerade eller för att fullgöra ett sådant avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås,

3) om behandlingen i ett enskilt fall är nödvändig för att skydda den registrerades vitala intressen,

4) om det bestämts om behandlingen i lag eller om behandlingen föranleds av en uppgift eller förpliktelse som anvisas den registeransvarige i lag eller som påförts honom med stöd av lag,

5) om den registrerade på grund av ett kund-, eller tjänstgöringsförhållande, ett medlemskap eller något annat därmed jämförbart förhållande har en saklig anknytning till den registeransvariges verksamhet (anknytningskrav),

6) om det är fråga om uppgifter om kunder hos eller arbetstagare vid en koncern eller någon annan ekonomisk sammanslutning och dessa uppgifter behandlas inom nämnda sammanslutning,

7) om behandlingen behövs för betalningstjänst, databehandling eller andra därmed jämförbara uppgifter som utförs på uppdrag av den registeransvarige,

8) om det är fråga om en allmänt tillgänglig uppgift som beskriver en persons ställning, uppgifter och skötseln av dessa uppgifter inom ett offentligt samfund eller inom näringslivet och dessa uppgifter behandlas för att trygga rättigheter och intressen hos den registeransvarige eller en sådan tredje man till vilken uppgifterna lämnas ut, eller

9) om datasekretessnämnden för behandlingen beviljat ett tillstånd som avses i 43 § 1 mom.

Personuppgifter kan lämnas ut med stöd av 1 mom. 5 punkten endast om personuppgifter lämnas ut som en sedvanlig del av verksamheten förutsatt att syftet för vilket uppgifterna lämnas ut inte strider mot ändamålet med behandlingen och att den registrerade kan antas känna till att personuppgifter lämnas ut på detta sätt.

PUL kap 2 § 8

I moment § 10 ges regler för en registerbeskrivning som skall finnas för alla register som behandlar personuppgifter.

I registerbeskrivningen skall det finnas information om den registeransvarige samt kontaktinformation, ändamålet med registret, beskrivning av vilka som registreras i registret, till vem innehållet i registret kan lämnas ut till, en beskrivning över hur skyddet av registret har realiserats och om registeruppgifterna lagras utanför Europeiska unionen eller det Europeiska ekonomiska samarbetsområdet. [PUL kap2 § 10]

Se Bilaga 1 för botten på ett registerutdrag.

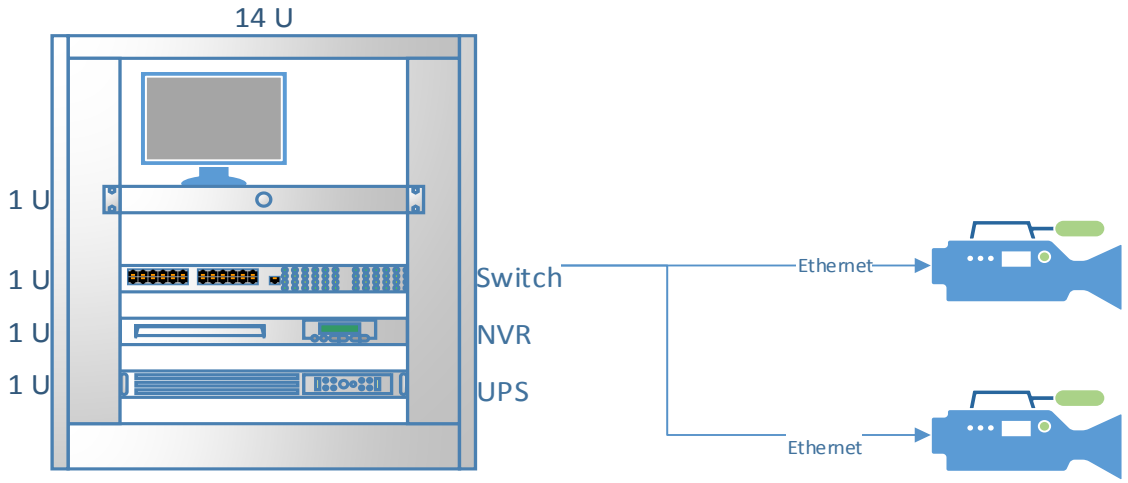
3 KAMERAÖVERVAKNINGSSYSTEMETETS ARKITEKTUR

Det traditionella sättet att bygga upp ett kameraövervakningssystem har varit analog videoöverföring till en central punkt där en DVR (Digital Video Recorder) sköter om lagringen. Överföringen är analog från kameran ändra fram till DVR:en och kräver en egen dedikerad signalväg vanligen koaxial- eller parkabel. (Kameravalvontaopas, 2010, p. 26) I Figur 1 ser vi ett exempel på en digitalinspelare, modellen är Everfocus EDR-16FI/2000 med 16 analoga ingångar med BNC kontakt.

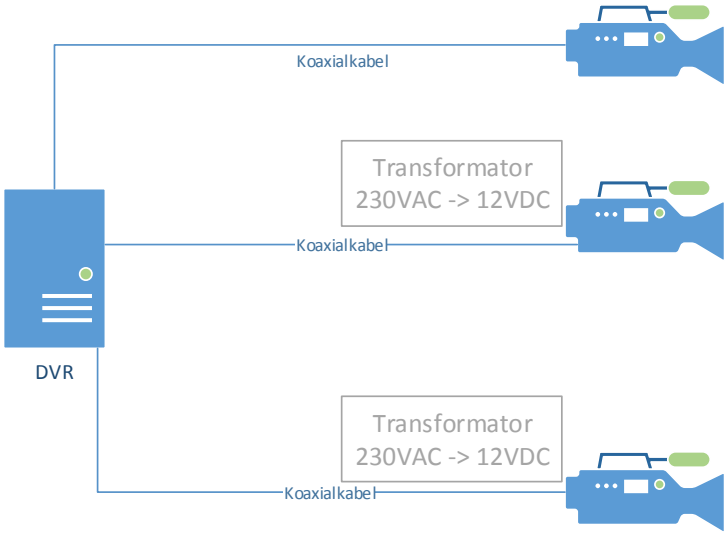
Figur 1 Everfocus EDR-16FI/2000 (FSM Oy)

Ett mera modernt sätt är att använda IP-kameror som ansluts till en nätverksinspelare (NVR Network Video Recorder) över ett TCP/IP nätverk. I ett TCP/IP baserat kameraövervakningssystem används flera aktiva nätverksenheter. I Figur 2 ser vi ett enkelt nät-

verk där vi har inspelaren (NVR) med lokala kontrollmöjligheter, en nätswitch, två kameror, en UPS och en bildskärm. Kamerorna kan med fördel strömförsörjas med ”Power over Ethernet” för att förenkla kabeldragning. Då kan man även använda samma störningsfria kraftförsörjning som för inspelaren. Som motsats i Figur 3 där vi har ett analogt kameraövervakningssystem där alla kameror oberoende hur långt borta från inspelaren är placerade måste ha en egen kabel och strömförsörjning.



Figur 2 Enkelt kameraövervakningsnätverk



Figur 3 Exempel på ett analogt kameraövervakningssystem

3.1 Inspelaren

Inspelaren är den enhet som tar emot videoströmmarna från alla kameror och lagrar dem. Man delar in inspelare i olika kategorier beroende på hur de fungerar. NVR (Network Video Recorder), nätverksinspelare, används tillsammans med IP-baserade kameror. DVR (Digital Video Recorder), digitalinspelare, används med analoga kameror. En Hybrid DVR, kan användas med både analoga och IP-baserade kameror. Inspelaren är ofta en vanlig dator med specialprogram för inspelningen och i DVR- eller hybridbruk med ett eller flera videokapningskort. I större system använder man vanligen PC baserade inspelare med specialmjukvara. I mindre system kan man använda hårdvarubaserade inspelare med inbyggd nätverks- och PoE-switch. De ledande tillverkarna av inspelningsmjukvara i Finland är idag Ksenos Oy och Mirasys Ltd. Som båda erbjuder mjukvara och paket med inspelarhårdvara med förinstallerad mjukvara.

3.2 Kameror

Man indelar kamerorna som används i kupol-, box- och bulletkamera. Boxkameran är den traditionella modellen som kräver en ställning för att monteras eller en ram för utomhusbruk, se Figur 4 för exempel på en boxkamera. Boxkameran har den fördelen att linsen är utbytbar och man kan således använda den för övervakning på längre håll så att människor på bilden ännu är identifierbara enligt K-värdet som är definierat i Finansinspektionens Centralförbunds ”Kameravalvonnan suunniteluohje”. K-värdet anger hur stor del av bilden målet har. Värdet definieras vid identifiering med K120 (målet är minst 120 % av bildhöjden), med K50 vid igenkänning (målet är minst 50 % av bildhöjden) och med K10 vid iakttagelse (målet är 10 % av bildhöjden). (Finanssialan Keskusliitto, 2006)

Figur 4 Sony SNC-EB600 boxkamera (Sony, 2014)

Bulletkameran är färdig att installeras på en vägg eller i taket tack vare sin inbyggda fot. Kameran har en fast lins som kan vara fjärrstyrd eller fixerad, ofta med brännviddsintervall från 2.8 mm till 12 mm. Ofta har bulletkameran också inbyggd IR-belysning för övervakning när den naturliga belysningen är svag eller obefintlig. I Figur 5 ser vi en Dahua IPC-HFW5502C bulletkamera med fjärrstyrd brännvidd mellan 4 och 9 mm.

Figur 5 Dahua IPC-HFW5502C (Dahua, 2014)

Figur 6 Sony SNC-EM600 kupolkamera (Sony, SNC-EM600, 2014)

Kupolkamerorna finns i säkrade varianter som är skyddade mot åverkan och klassificerade enligt Europastandarden EN 62262 (Interelectronix, 2014). Liksom bulletkameran är kupolkameran färdig för direkt montering i taket eller på väggen direkt och kräver ingen monteringsutrustning. En nackdel med kupolkamerorna är det lilla utrymmet som

de har för kameralinsen, på längre avstånd är de inte effektiva. Bulletkameran kan däremot ha en större lins och därmed kan den användas på längre håll. Linsen både i kupol- och i bulletkameran är fastmonterad och går inte att byta ut. En variant av kupolkameran är PTZ-kameran (Pan, Tilt, Zoom), med vilken man kan panera, vinkla och zoom in på distans. Med PTZ-kameror kan man täcka ett större område med färre kameror. En PTZ-kamera kan styras manuellt från ett kontrollrum eller automatiskt enligt rörelse eller fördefinierade mönster.

Alla kameror består i grunden av samma elektronik och samma bildsensor, skillnader är främst linsens storlek och kamerans fysiska form. Vilken typ av kamera man väljer är helt beroende på användningsområdet. En kupolkamera är snyggare, den smälter bättre in i omgivningen och med en färgad kupa ser man inte heller åt vilket håll kameran filmar. Med boxkameran har man den största valmöjligheterna att välja linser enligt behov. Linser finns även med s.k. Fish-Eye teknik med vilken man får en 360 graders bild från ett ställe i taket (se Figur 7).

Figur 7 Överblicksbild med SNC-HM662 (Sony Professional Europe, 2014)

3.1 Paketlösningar

För mindre system kan det löna sig att använda färdiga paket med kameror, nätverksutrustning och inspelare. Sådana paketlösningar tillverkas av flera aktörer och kan bestå av en hårdvaruinspelare med inbyggd nätverksswitch och kameror. Till exempel FSM Oy säljer ett paket med fyra nätverkskameror, inspelare, skärm och alla kablar som behövs (FSM Oy, 2014). Istället för använda en PC-baserad inspelare som kan vara krångligare att konfigurera har flera tillverkare hårdvarubaserade inspelare med plats för några hårddiskar och en inbyggd nätverksswitch med integrerad PSE för PoE. Med en sådan inspelare och kameror från samma tillverkare är konfiguration och installation mycket enkel. Man behöver bara koppla kameran till inspelaren och inspelaren söker alla kameror i nätverket med hjälp av OnVif, och lägger till dem i inspelaren (Planet Networking & Communication, 2014).

4 NÄTVERK FÖR KAMERAÖVERVAKNINGSSYSTEM

I de nätverk som används för kameraövervakning använder man sig av TCP/IP-protokollen över ett Ethernet-nätverk. Eftersom Ethernet-standarden begränsar avståndet på kablarna till 100 m beroende på signaldämpning, används olika Ethernet-förlängare och repeaters för att komma upp i längre avstånd. För att övervaka större områden utomhus kan man också använda sig av trådlösa länkar för att sammanbinda flera nätverk till ett.

4.1 Trådbundna nät

4.1.1 Ethernet

Ethernet implementerar de två lägsta lagren, det fysiska och datalänken, i OSI-modellen. I det fysiska lagret definieras den mekaniska och elektriska signaleringen (Stallings, 2004). Datalänkslagrets uppgift är att se till att kommunikationen i det fysiska lagret sker rätt så att paketen från de övre lagren kommer fram till nästa nod i nätverket. Datalänkslagret ansvarar också för flödes- och felkontroll för paket som sänds i det fysiska nätet.

Ethernet kan använda sig olika fysiska medier såsom fiber, koaxialkabel och partvinnad koppartråd. Kamerorna för kameraövervakning använder sig huvudsakligen av Ethernet-standarderna 10BASE-T eller 100BASE-TX. 10BASE-T och 100BASE-TX använder sig av två par partvinnade oskyddade kopparledningar. 100BASE-TX specificeras att användas med Kategori 5 (Cat5) kabel och ger en hastighet på 100 mbps. 10BASE-T kan användas på sämre Kategori 3 (Cat3) kabel, med hastigheten 10 mbps. I båda fallen är längden på kabeln begränsad i standaren till 100 m pga. signaldämpningen.

Standarden TIA/EIA-568-A specificerar klasserna för partvinnade kablar enligt vilken bandbredd de klarar av och hur stark överhörningen är mellan de olika paren. Cat3 klarar en bandbredd på 16 MHz, Cat5 skall klara av 100 MHz bandbredd. Standarden kräver också att termineringen i båda ändor av kabeln klarar av bandbredden. Senare kom det fram att marginalerna på Cat5 kabeln för 100 Mbit bandbredd var för små. En uppdaterad standard Cat5e ställer högre krav på överhörning (Panduit Corp., 2004). För snabbare Ethernet-förbindelse med 1000BASE-T och 10GBASE-T krävs det bättre kablar och Cat6 standarden som kräver att kabeln certifieras för 250MHz.

Vill man använda Ethernet med partvinnade kablar över längre avstånd behöver man använda en Ethernetförlängare som möjliggör Ethernetförbindelser över något annat fysisk medium, exempelvis fiber eller koaxialkabel. Man kan också använda sig av någon annan teknik för längre länkar, t.ex. xDSL. Vid förhållanden där man kan placera enheter skyddade för vind och väder högst 100 m från varandra klarar man sig med enkla Ethernet-repeaters. Dessa repeaters finns i varianter som strömförsörjes med Power over Ethernet (PoE) och därmed kan utplaceras enklare då man inte behöver skild strömförsörjning på platsen.

PoE, är en standard för att strömförsörja en enhet via en Ethernet länk. Man delar in enheterna som används i ett PoE-system i Powered Device (PD), enheten som använder strömmen, och Power Sourcing Equipment (PSE), enheten som injicerar strömmen i Ethernetlänken. Den nuvarande standarden IEEE 802.3at klarar av att leverera 50 W (MicroSemi, 2010). PoE kan användas för att strömförsörja både nätverkskameror och Ehernet-extenders. Vissa Ethernet-extenders klarar också av att förlänga räckvidden på strömförsörjningen (Vigitron, 2012).

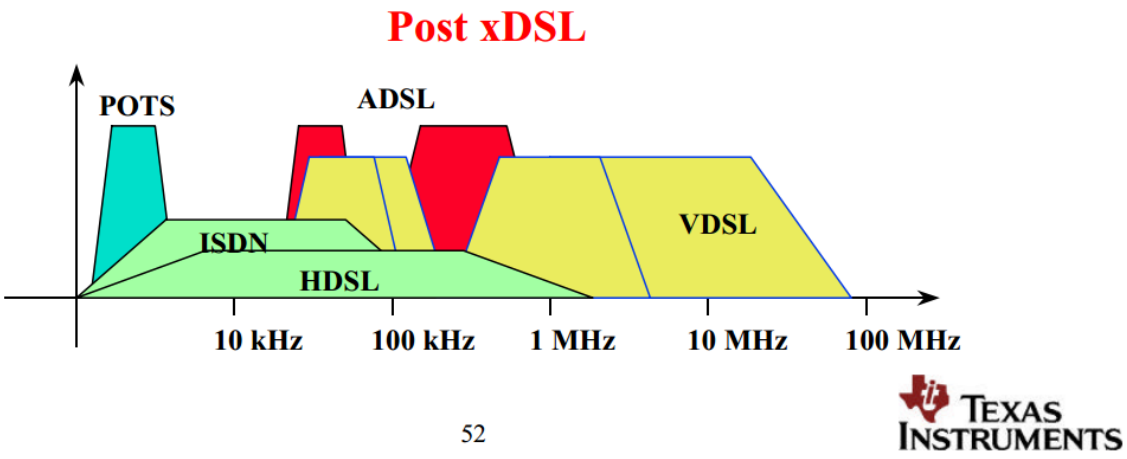
4.1.2 Fiber

Behöver man få förbindelse längre än Ethernet över partvinnad kabel möjliggör är det möjligt att använda sig av fiberoptisk överföring. Med en fiberoptisk länk kommer man upp i avstånd på tiotals kilometer. Det är i huvudsak två olika typer av fiberoptisk kommunikation som används, Multi- och Single-mode. Skillnaden mellan dessa är diametern på själva fibern och vilken våglängds ljus som används. Med Multi-mode används en fiberkabel med en diameter större än våglängden på ljuset, som ljuskälla används lysdioder. Dessa lysdioder ger inte ljus av en specifik våglängd utan ljuset är bredare. Detta betyder att ljuset i fibern tar sig fram med olika hastigheter och begränsar längden på fiberkabeln. Single-mode använder sig av en tunnare fiber och ställer större krav på kontakterna. I en ”Single-mode”-anslutning går ljuset rakt igenom fibern utan att studsa via väggarna och därvid skapa distorsion. Med en ”Single-mode”-länk kan man komma upp i avstånd långt längre än med Multi-mode.

Standarden TIA/EIA 492-AAAD specificerar olika klasser på fiberoptisk kabel i ”Multimode”-användning. Den nyaste OM4 klassen klarar av 100 Gigabits Ethernet över 150 m, medan OM3 klarar av 100 m (BlackBox Network Services, 2014). Vid lägre hastigheter kan man använda längre avstånd, upp till 2 km vid 100BASE-FX (100 mbps).
En annan fördel med fiberoptiska länkar är den galvaniska isolationen man får mellan de ihopkopplade punkterna. En överspänning vid ena länken kan inte ta sig över länken till den andra punkten.

4.1.3 xDSL

xDSL är ett samlingsnamn för olika DSL-tekniker (Digital subscriber line). De olika evolutionerna av xDSL är i utvecklingsordning ADSL(Assymetric digital subscriber line), HDSL (High-speed digital subscriber line) och VDSL (Very high-speed digital subscriber line) (Jacobsen, 1999). Kommunikationen i xDSL använder partvinnad kopparkabel som fysiskt medium. xDSL använder frekvenser som inte används i analoga telefoner och utnyttjar samma infrastruktur se Figur 8. Den senaste VDSL2-tekniken använder ett större frekvensområde och klarar därför av högre bandbredd.



Figur 8 Frekvensanvändning i xDSL-tekniker (Jacobsen, 1999, s. 52)

I Figur 9 ser vi en proprietär Ethernet-förlängare, Vigitrons VI2301. Vigitron berättar inte vilket system de använder eller vilken teknik. Databladet för enheten ger dock en anvisning om att det mycket troligt är xDSL och då närmast VDSL2 som används.

Figur 9 Proprietär Ethernet-förlängare, MaxiiCopper High-Speed Ethernet Extender over UTP

Om vi tittar på jämförelsen i Tabell 1 kan vi konstatera att tillverkarna har en ganska bred marginal mot de teoretiska hastigheterna och avstånden som VDSL2 erbjuder. VDSL2 minskar snabbt i hastighet när avståndet ökas, ITU-T's rekommendation G.993.2 specificerar en bandbredd på 30 MHz och hastigheter på upp till 200 Mbit/s tillsammans för upp- och nedströmstrafik. Detta är dock endast möjligt på korta avstånd och hastigheten minskar radikalt genast i början.

Tabell 1. Jämförelse av Ethernet over Twisted pair extenders och VDSL2-standarden.

	Vigitron Vi 2301	Planet VC 231	NetSys NV202	Allied Tele-sis AT-MC605	Teoretiskt max VDSL2
10Mbit/s	914m	900m	1400m	975m	1000m
100Mbit/s	303m	300m	300m	150m	500m

4.2 Trådlösa nät

4.2.1 ”Punkt till punkt”-nät

Med en ”punkt till punkt”-förbindelse kan man förena två eller flera nätverk över relativt långa avstånd. Med Radwin’s RW-2250-0100 utlovas en räckvidd på 20 till 120 km med en bandbredd på 200 mbps och en ”round-trip”-latens på 6 ms (Radwin, 2010). RW-2250-0100 använder frekvenser på 5.3, 5.4 eller 5.8 GHz i enlighet med ETSI standarderna EN 301 893 och EN 302 502. Vid en bryggning med två enheter krävs ingen synkontakt. Vid kortare avstånd är ett betydligt kostnadseffektivare sätt att använda sig av WLAN-länkar. (Prisklassen för ett P2P sändar-mottagar-par av Radwins RW-2250-0100 börjar vid 3000 €).

4.2.2 WLAN

Vid kortare avstånd och vid en P2M-lösning (Point to Multipoint) kan man använda sig av WLAN och dess Wireless Distribution System (WDS). Med WDS kan man brygga två basstationer så att de fungerar som en trådlös Ethernet-förbindelse där även klienternas MAC-adresser hålls intakta över länken.

4.2.3 Mobiltelefoninät

Kan man använda sig av tredje eller fjärde generationens mobiltelefoninätverk för att strömma video från kameror till inspelaren. Eller kan man använda det för distansanvändning av hela övervakningssystemet.

För att inspelaren skall komma åt kameran som har en Internetanslutning via mobiltelefoninätet krävs att operatören tillhandahåller en publik IP för anslutningen, vilket dock är ovanligare. För att då få tillgång till kameran behöver man utrustning som kan länka ihop det externa nätet med kameraövervakningsnätet. Man kan använda sig av en VPN-lösning (Virtual Private Network). Mera om detta i kapitel 5.1.

5 DISTANSANVÄNDING AV KAMERAÖVERVAKNING

Vid distansanvändning rekommenderar Valvora Oy att man har två nätverkskort i inspelaren och håller ena dedikerat för nätverkskamerorna, medan det andra används för distansanvändning (Valvora Oy, 2014). De färdiga paketlösningar som säljs med Valvoras Ksenos mjukvara har två nätverkskort färdigt vid leverans.

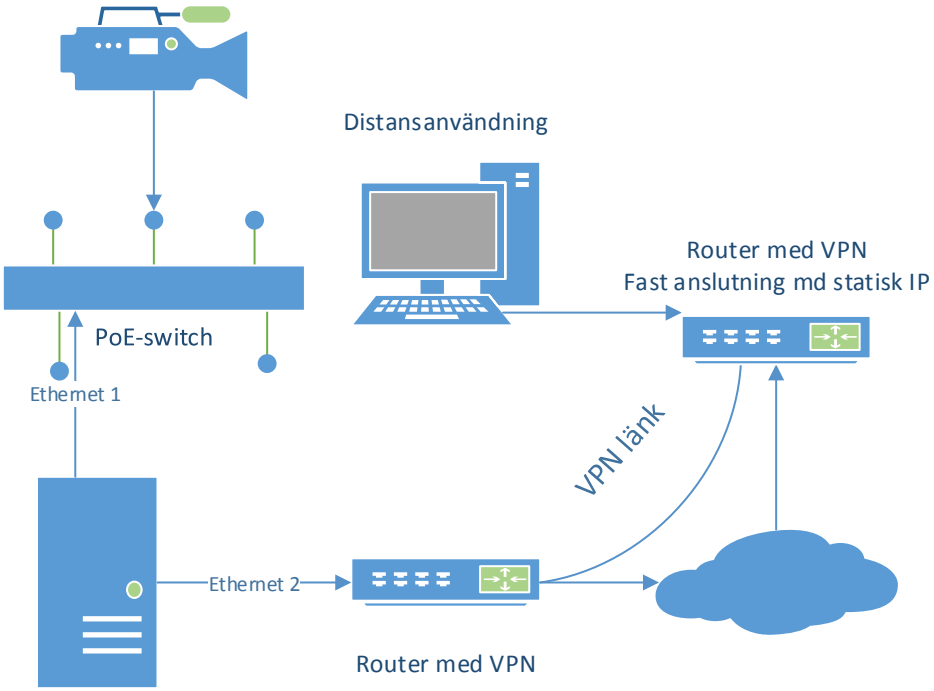
5.1 Tekniker för fjärråtkomst

För att inte behöva ha inspelaren ansluten öppet till Internet kan man använda sig av ett virtuellt privat nätverk (Virtual Private Network, VPN). Det finns färdiga hårdvaruprodukter på marknaden som Tosibox som skapar ett VPN som kräver en hårdvarunyckel för att ansluta sig till (Tosibox Oy, 2014).

Med Tosiboxs VPN-lösning kan man skapa ett virtuellt nätverk även på platser utan fast Internet-förbindelse med en mobil Internet-anslutning. I Tosibox Lock finns nämligen möjligheten att koppla in ett 3G- eller 4G-modem. I detta fall behövs ingen publik IP-adress, eftersom Tosibox Lock skapar ett Virtuellt nät med Tosiboxs server. För att sedan kunna fjärrmanövrera inspelaren krävs att man har en nyckel för att ansluta sig till samma server som Tosibox Lock har förbindelse med. All trafik är krypterad och går via Tosibox-servrar.

Andra möjligheter för säker fjärråtkomst är att använda sig av OpenVPN som är en VPN-lösning baserad på öppen källkod. Med OpenVPN måste man själv sätta upp och konfigurera en server som är tillgänglig på Internet. Till denna server ansluter man sedan inspelaren endera direkt med programvara eller med hjälp av en router med inbyggt stöd för OpenVPN. Den alternativa firmwaren DD-WRT (DD-WRT, 2014) och OpenWRT (OpenWrt, 2014) har stöd att både fungera som server och klient. OpenVPN kan konfigureras att skapa det virtuella nätverket genom det tredje nätverkslagret i OSI-modellen och fungerar då som en tunnel för punkt-till-punkt-trafik, eller skapa det som en virtuell nätverksenhet i datalänk-lagret. I båda fallen är all trafik krypterad med SSLv3/TLSv1.

I Figur 10 visas ett exempel på en nätverkslayout med en VPN-länk för distansanvändning. Inspelaren har två nätverkskort där det ena är dedikerat för kamerorna och det andra för distansanvändningen. Länken till Internet från inspelaren kan vara fast eller utnyttja mobilt bredband.



Figur 10 Exempel på VPN-länk

5.2 Distansöverföring av bildströmmar

För att strömma realtidsvideo till många klienter behöver man ett sätt för klienten att ansluta sig till källan. Vill man strömma t.ex. en övervakningskamera är det möjligt att göra det på flera sätt. Det enklaste och osäkraste sättet är att helt enkelt låta hela kameranätverket vara anslutet till Internet, vilket är inte bra med tanke på säkerheten då vem som helst kommer att ha tillgång till det interna nätverket. Ett bättre sätt är att ha en egen server utanför kameranätet endera i samma byggnad eller i en serverhall med snabba Internet-förbindelser. Har man dessutom en PC-baserad inspelare kan man använda sig av fritt tillgängliga program såsom FFMPEG och NGINX för att strömma realtidsvideo över Internet. I Bilaga 4 visas en exempelkonfiguration för NGINX med RTMP-strömning och kommandon för att starta strömning från en nätverkskamera till NGINX. I detta fall kan NGINX med nginx-rtmp-module (Arutyunyan, 2014) användas som server och video-distribuerare. Till servern skickas en komprimerad videoström med ffmpeg (FFmpeg project, 2014).

Real-Time Messaging Protocol (RTMP), är ett protokoll som utvecklades av Macromedia för strömmning av ljud och video över Internet. Adobe som Macromedia är en del av har gjort en version av protokollet fritt tillgängligt (Adobe Systems Incorporated, 2014).

6 SYSTEMTESTNING

6.1 Test av nätverksförbindelser

För testning av vad dåliga nätverksförbindelser har för inverkan på realtidsvideo över nätverket använde jag mig av ett program kallat clumsy som använder sig av biblioteket WinDivert. Clumsy fungerar så att det stoppar alla inkommande och utgående paket på vilka sedan appliceras filter som tappar bort, duplicerar eller ändrar på paketen. Sedan injiceras paketen i nätverksströmmen igen (Tao, 2014). För att granska resultaten användes en klocka på en webbsida som filmades med en nätverkskamera, strömmen från nätverkskameran spelades upp med VLC och skärmbilden spelades in med Windows Media

Encoder, för att man senare skall kunna inspektera svarstider och bedöma hur stabil bildströmmen var med olika kodeks.

6.2 Test av kameror

Vid testning med en Dynacolor W2V1-2 Dome Camera har följande resultat fåtts fram. MJPEG-enkodning av bildströmmen är bättre vid förbindelser där paket tappas bort eller kommer fram korrumperade. Redan vid 1 % tappade paket stannar den H.264-kodade bildströmmen helt, medan den MJPEG-kodade bildströmmen fortsätter att fungera trots att en del pixlar tappas bort. Bildkvaliteten är jämförbar men MJPEG-strömmen tar mera bandbredd (Strand, 2014). Orsaken till bandbreddsskillnaderna och bilströmmens kvalitet vid dåliga förbindelser beror på hur kodningen av bildströmmen sker. I MJPEG kodas alla bildrutor som skilda JPG-bilder, man kan säga att varje bildruta är en keyframe. En keyframe innehåller all data som behövs för att återskapa bilden och är även kallad Intra Frame (I-frame). Den andra sortens bild är en Predictive Frame, (P-frame). En P-frame innehåller bara data om vad som har ändrats sedan föregående bild. Förhållandet mellan dessa kan definieras i kamerans inställningar. Med färre P-frames mellan I-Frames får man en bättre bild som också klarar av mera störningar på förbindelsen. Nackdelen med detta är att bandbredden som krävs stiger eftersom I-Frames innehåller mera data.

Med en 100 mbps Ethernet-länk kan man räkna med att klara av ca 10 videoströmmar med en konstant bitrate på 8 mbps. För att ansluta flera kameror till nätverket bör åtminstone länken mellan switchen och inspelaren vara av Gigabitklass. Då kan man bygga ut ett stomnät med en Gigabit-switch som anslutningspunkt där inspelaren och flera 100 mbps switchar kopplas in. Vid större områden kan man också bygga upp stomnätet med fiberoptiska kablar eller med VDSL2-länkar till kameror som är längre borta.

Ett exempel med en Sanyo VCC-HD2300P har följande inställningar

Kodek	H264 – MPEG-4 AVC (part 10) (h264)
Bildstorlek	1200 x 1600
Bildfrekvens	12.4875 FPS

Bandbredd	4000 bits/s
Protokoll	RTP over UDP

Med VLC visas en genomsnittlig bandbredd på 2718 kb/s med minimal rörelse i bilden. Videon strömmas över ett mobilt nätverk och man märker att uppladdningshastigheten inte hinner ta med alla bildrutor, 3.9% kan inte avkodas och videon är väldigt hackig. Se Bilaga 2.

7 SLUTSATSER

Ett nätverksbaserat kameraövervakningssystem kan göras väldigt flexibelt när man bygger upp nätverket. Alla kommersiellt tillgängliga nätverksprodukter är användbara. Vid planering av nätverket bör man se till att bandbredden är tillräcklig från inspelaren till alla kameror. Användning av existerande infrastruktur som kablage är en möjlighet då man inte vill dra nya kablar eller då det inte är möjligt. I projektet som är grunden till examensarbetet utnyttjades existerande telefonkablar med VDSL2-länkar för en stor del av kamerorna. Inspelarens placering nära huvudcentralen i byggnaden och det allmänna kablaget på området ledde till att inget grävarbete behövde utföras. På ställen där inget kablage fanns användes trådlösa WLAN-länkar. Vid planeringen togs det i beaktande att kameror placerades endast där det fanns nätström tillgängligt eller där de kunde strömförsörjas med PoE. I Bilaga 3 visas uppbyggnaden av det realiserade kameraövervakningssystemet.

KÄLLOR

Adobe Systems Incorporated. (2014). *Real-Time Messaging Protocol (RTMP) specification*. Retrieved 12 10, 2014, from https://www.adobe.com/devnet/rtmp.html

Arutyunyan, R. (2014, 9 23). *nginx-rtmp-module*. Retrieved 12 9, 2014, from https://github.com/arut/nginx-rtmp-module

BlackBox Network Services. (2014, 11 30). Retrieved 11 30, 2014, from Black Box Explains…OM3 and OM4..: http://www.blackbox.com/resources/blackboxexplains.aspx?id=BBE_4979

Dahua. (2014). IPC-HFW5502C. Retrieved from http://www.dahuasecurity.com/upfiles/201406280533228.jpg

Dataombudsmannen byrå. (2011, 04 11). *INTEGRITETSSKYDD OCH BEHANDLING AV PERSONuPPGIFER I SAMBAND MED KAMERAÖVERAKNING*. Retrieved 03 24, 2014, from http://www.tietosuoja.fi/uploads/muzw6devx4h8q3n.pdf

DD-WRT. (2014, 9 1). *OpenVPN*. Retrieved 12 6, 2014, from DD-WRT wiki: http://www.dd-wrt.com/wiki/index.php/OpenVPN

FFmpeg project. (2014, 12 10). *A complete, cross-platform solution to record, convert and stream audio and video.* Retrieved 12 10, 2014, from http://ffmpeg.org/

Finanssialan Keskusliitto. (2006). *Kameravalvonnan suunnitteluohje.* Retrieved 12 12, 2014, from http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Kameravalvonnan_suunnitteluohje_K-menetelma_2006.pdf

FSM Oy. (2014). Retrieved 11 8, 2014, from Dahua tallennin 1Tb, 2+2 kameraa, TFT22: http://www.fsm.fi/nvr8-4-22-1

FSM Oy. (n.d.). *Digitaalitallennin 16/2000.* Retrieved 12 16, 2014, from Fonel Security Marketing Oy: http://www.fsm.fi/media/catalog/product/cache/1/image/800x600/17f82f742ffe127f42dca9de82fb58b1/e/d/edr-_1.jpg

Interelectronix. (2014, 10 22). *IK TEST EN 62262*. Retrieved 12 7, 2014, from http://www.interelectronix.com/en/kb/ik-test-en-62262.html

Jacobsen, K. S. (1999). *xDSL Technology and Applications.* Retrieved 12 16, 2014, from http://www.ewh.ieee.org/r6/scv/comsoc/9909.pdf

MicroSemi. (2010, 6). *Understanding 802.3at.* Retrieved 11 9, 2014, from http://www.microsemi.com/documents/powerdsine/whitepapers/Understanding_802_3at_PowerDsine.pdf

NV-202. (2014, 3 24). Retrieved from NetSys: http://www.netsys.com.tw/products/vdsl2/nv202.htm

OpenWrt. (2014, 6 10). *OpenVPN Setup Guide*. Retrieved 12 6, 2014, from OpenWrt wiki: http://wiki.openwrt.org/doc/howto/vpn.server.openvpn.tun

Panduit Corp. (2004, 2 27). *The Evolution of Copper Cabling Systems from Cat5 to Cat5e to Cat6.* Retrieved 11 23, 2014, from http://www.gocsc.com/UserFiles/File/Panduit/Panduit098765.pdf

Personuppgiftslagen. (n.d.).

Peterson, L. L., & Davie, B. S. (2012). *Computer Networks a systems approach* (5th ed.). Burlington, USA: Morgan Kaufman.

Planet Networking & Communication. (2014). *8-CH Network Video Recorder*. Retrieved 11 18, 2014, from http://www.planet.com.tw/en/product/product.php?id=42579#dl

Radwin. (2010, 4). *Radwin RW-2250-0100 Datasheet.* Retrieved from http://www.radwin.com/DataSheets/RW2000/RW-2250-0100.pdf

Sony. (2014). SNCEB600. Retrieved from https://pro.sony.com/bbsc/imageController?path=Asset%20Hierarchy$Professional$SEL-yf-generic-153711$SEL-yf-generic-153761SEL-asset-390530.jpg

Sony. (2014). SNC-EM600. Retrieved from https://pro.sony.com/bbsc/imageController?path=Asset%20Hierarchy$Professional$SEL-yf-generic-153711$SEL-yf-generic-153761SEL-asset-360100.jpg

Sony Professional Europe. (2014, 3 6). Sony Professional: SNC-HM662 Mini Dome IP camera. Retrieved 12 13, 2014, from https://www.youtube.com/watch?v=BmqgbfU5P6A

Stallings, W. (2004). *Data and Computer Communications.* Pearson Education, Inc.

Strand, T. (2014, 11). Retrieved 11 29, 2014, from http://fik1.net/thesis/kamera.wmv

Tao, C. (2014). *clumsy, an utility for simulating broken network for Windows*. Retrieved from https://jagt.github.io/clumsy/

Tosibox Oy. (2014, 11 30). *Tosibox tekniska data*. Retrieved 11 25, 2014, from http://www.tosibox.com/sv/teknisk-data/#lock

Turva-alan yrittäjät ry. (2010). *Kameravalvontaopas.* Sähköinfo Oy.

Valvora Oy. (2014, 5 2). Ksenos Installatörshandbok. Retrieved 11 25, 2014, from http://dl.ksenos.fi/doc/InstallersHandbook_sv.pdf

Vigitron. (2012). *MaxiiCopper High-Speed/High Power Ethernet Extender over UTP TM.* Retrieved from http://www.vigitron.com/Admin/Files/Attribute/DSVi2301A.pdf

BILAGOR

Bilaga 1 Registerbeskrivningsmall

REGISTERBESKRIVNING enligt 10 § personuppgiftslagen (523/1999)
Datum: _____

1. Den registeransvarige	Namn
	Kontaktuppgifter (postadress, telefon…)
2. Registerärendenas handläggare och/eller kontaktperson	Namn
	Kontaktuppgifter (postadress, telefon…)
3. Registrets namn (namnet bör beskriva registrets uppgiftsinnehåll)	

Läs ifyllningsanvisningarna före Du fyller i registerbeskrivningen. Använd bilagan om nödvändigt.

4. Syftet med behandlingen av personuppgifter / registrets användningsändamål (Ifall behandlingen av personuppgifter har utkontrakterats, kan en omnämnande av detta göras i denna punkt.)	

Tel. 010 36 66700 (växel)
Tel. 010 36 16670 (rådgivning kl. 9.00 – 15.00) telefax 010 36 66735

www.tietosuoja.fi

5. Registrets datainnehåll (T.ex. den registrerades namn, adress, telefonnummer etc.)	
6. Regelmässiga uppgiftskällor * (Vilka uppgifter fås, av vem och på vilka grunder, t.ex. samtycke eller bestämmelse i lag)	
7. Regelmässigt utlämnande och översändande av uppgifter utanför EU eller EES	

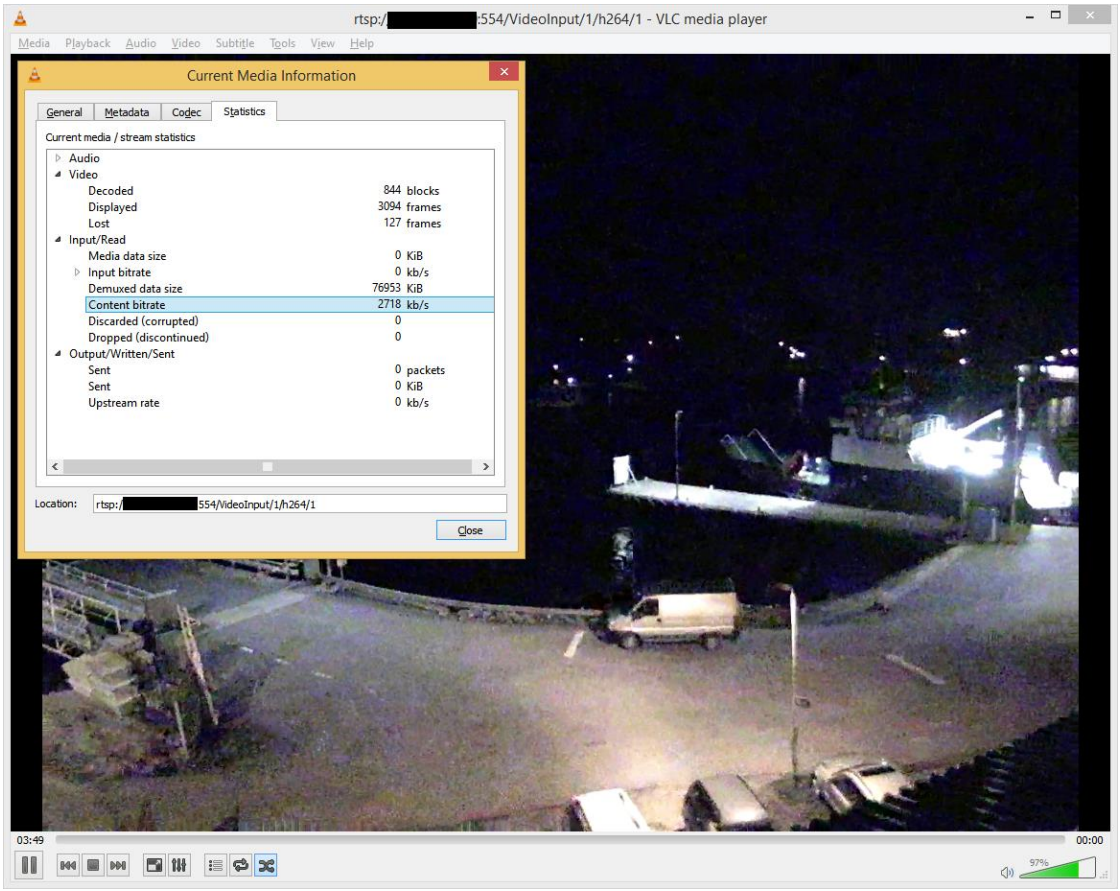
8. Principerna för skyddet av registret	A. Manuellt material (förvaringsplats och skyddande) B. ADB-register (principerna för rätten att använda registret och övervakningen av användningen samt det fysiska skyddet av utrustningarna)

* Personuppgiftslagen 10 § förutsätter inte uttryckligen att källorna anges, men med tanke på de registrerades rätt att få information är det ändamålsenligt ange dem. Denna uppgift ger också en bild av registrets datainnehåll.

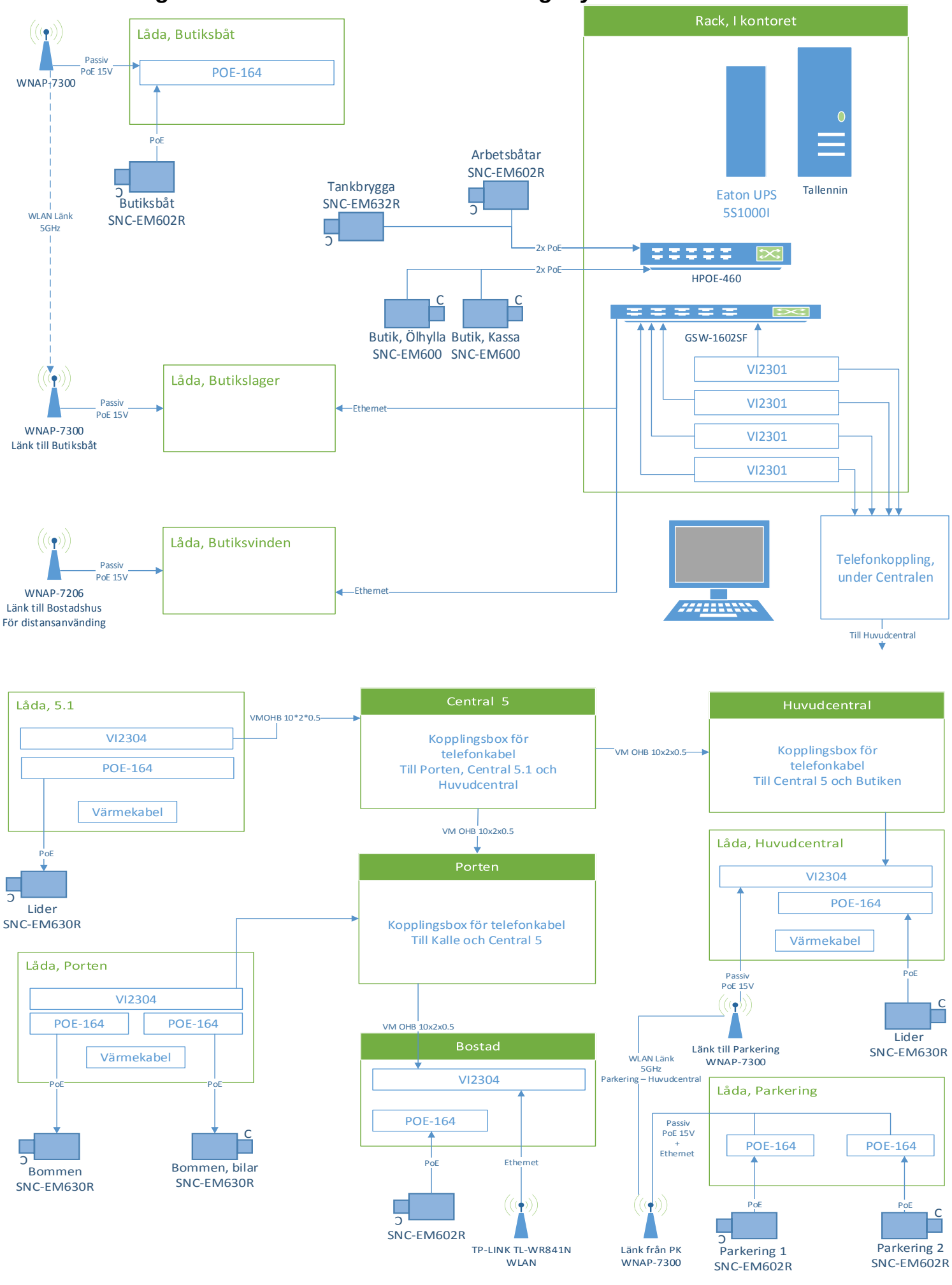
Tel. 010 36 66700 (växel)
Tel. 010 36 16670 (rådgivning kl. 9.00 – 15.00) telefax 010 36 66735

www.tietosuoja.fi

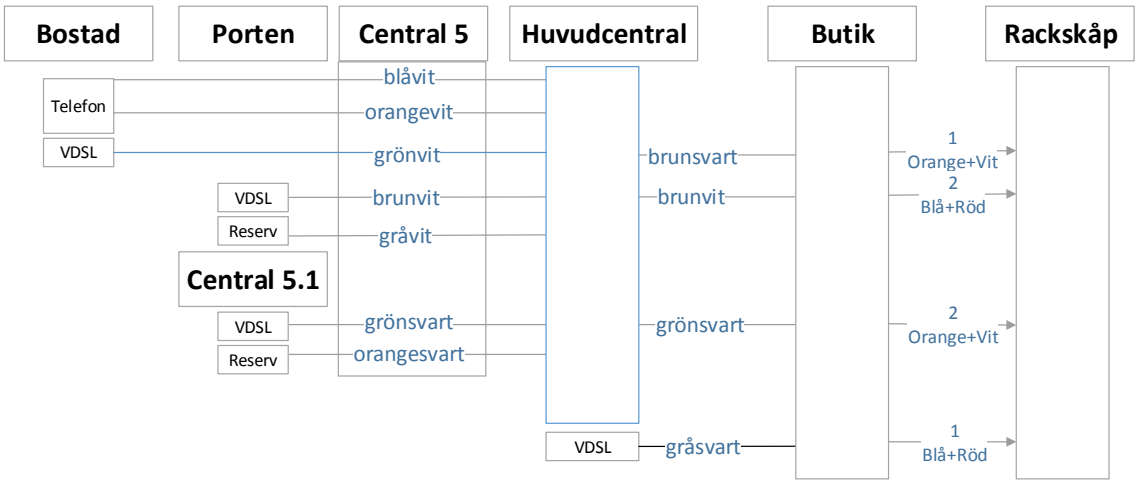
Bilaga 2 Statistik från VLC



Bilaga 3 Realiserat kameraövervakningssystem



Parkabelkopplingar



Bilaga 4 Exempel på strömning via en videodistribuerare

För att använda rtmp-modulen med NGINX måste NGINX kompileras med stöd för modulen. På modulutvecklarens hemsida finns utförliga instruktioner hur man gör. Se https://github.com/arut/nginx-rtmp-module

```
rtmp {
    server {
        listen 1935;
        chunk_size 2048;
        application live {
            live on;
            record off;
        }
    }
}
```

För att strömma videon till NGINX kan ffmpeg användas. Ffmpeg finns tillgängligt för de flesta plattformar i färdiga binärpaket från http://ffmpeg.org/

För att strömma videon med RTMP behöver videon omkodas och multiplexeras till containerformatet FLV (Flash Video). I kommandot nedan hämtas videon från addressen 192.168.1.44 på det lokala nätet, med följande parametrar berättar vi åt ffmpeg vilken kodek som används och vilken bitrate för videon. Med –s bestäms storleken på videon. –acodec copy kopierar ljudströmmen rakt utan omkodning. Sista parametern –f berättar vart vi skickar strömmen och med vilken container. I detta fall används FLV-containern och servern med addressen 192.168.1.100.

ffmpeg.exe -i rtsp://192.168.1.44/h264 -vcodec libx264 -preset veryfast -b:v300k -maxrate 300k -s 640x480 -acodec copy -f flv rtmp:// 192.168.1.100/live/stream

En enkel konfiguration på webbsida för visning av en videostöm skapas med nedanstående html-kod.

För att använda sig av jwplayer behöver man registrera sig på http://www.jwplayer.com/sign-up/ och därifrån kan man välja att ladda ner skriptet eller använda sig av en tillverkarensversion av spelaren.

```
<html>
<head>
<!—Inkludera javascriptet för jwplayer här -->
   <script src=""></script>
</head>
<body>
<div id="player">Loading the player...</div>
<!—I file skriver du in samma address som du stömmar videon till -->
<script type="text/javascript">
   jwplayer("player").setup({
      file: "rtmp://192.168.1.100/live/flv:stream",
      width: 640,
      height: 360,
   });
</script>
</body>
</html>
```