Jari Korvakangas

Audio/Video Systems and Information Security

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor’s Thesis

15 March 2016

Tiivistelmä

Tekijä(t) Otsikko Sivumäärä Aika	Jari Korvakangas Audio-/Video järjestelmät ja tietoturva 45 sivua 15.3.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Projekti-insinööri, Mission Critical Networks Antonio Ramirez Lehtori Marko Uusitalo

Tämän insinöörityön tarkoitus oli tutkia esitystekniikan järjestelmiä ja niiden potentiaalisia tietoturvauhkia. Tähän valittiin kolme aihepiiriä. Nämä ovat videoneuvottelulaitteet, audio verkon yli- ja IP kuulutusjärjestelmät. Työ kirjoitettiin Pöyry Finland Oy:n MCN teamille.

Insinöörityön ensimmäinen osa kattaa videoneuvottelulaitteet yleisellä tasolla ja potentiaaliset tietoturva-aukkoja kuten myös erilaisia ratkaisuja näihin. Toinen osa on audio verkon yli ja sen muutos analogisista järjestelmistä digitaalisiin. Käsiteltävänä on Dante, AVB/TSN, Ravenna ja muita erilaisia esitystekniikan järjestelmiä. Viimeiseksi, IP kuulutusjärjestelmät ovat kolmas aihepiiri insinöörityössä.

Selvitys antoi joitain ratkaisuja kuinka välttää tietoturva-aukkoja videoneuvottelujärjestelmissä, mutta ei selvää ratkaisua tilanteesta riippumatta, joka olisi myös helppo ottaa käyttöön. Tärkein keino on laittaa laitteet palomuurin taakse ja konfiguroida palomuuri tilanteen mukaan. Tosin tämä ei ole niin helppoa kuin miltä se kuulostaa. Tämä auttaa joihinkin, ehkä useimpiin uhkiin, mutta on olemassa myös muita keinoja parantaa turvallisuutta kuten H.323 välimuistipalvelin ja/tai portinvahti mahdollisesti myös samassa yhteydessä, toimien puhelun välittäjänä.

Yhtään vakavaa tietoturvauhkaa, joka olisi ainoastaan audio verkon yli-järjestelmissä, ei löytynyt. Dante, AVB/TSN ja muut järjestelmät toimivat palomuurin takana välttäen pahimmat uhat. Tästä johtuen aihetta käsiteltiin enemmän yleisellä tasolla ja vähemmän tietoturvan näkökulmasta. Sama voidaan sanoa IP kuulutusjärjestelmistä.

Audio-/video laitteet ovat siirtyneet koko ajan enemmän digitaaliseen muotoon. Tämä vaatii, että tietoverkkosuunnittelijat tuntevat näiden järjestelmien toiminnan suunnitellessaan tietoverkkoja. Tulevaisuudessa tämä kehitys ainoastaan kiihtyy, kun järjestelmät etenevässä määrin käyttävät hyväkseen IP protokollia ja vanhoja analogisia järjestelmiä uusitaan.

Avainsanat	Videoneuvottelu, audio verkon yli, Dante, AVB/TSN, IP kuulutusjärjestelmät

Author(s) Title Number of Pages Date	Jari Korvakangas Audio/Video Systems and Information Security 45 pages 15 March 2016
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Specialisation option	Data Networks
Instructor(s)	Antonio Ramirez, Project Engineer – Mission Critical Networks Marko Uusitalo, Senior Lecturer

The purpose of this thesis was to investigate presentation technology systems and their potential security holes. Three different areas in audio/video were chosen for this. These were Video Conferencing, Audio over Ethernet and IP announcement systems. This study was carried out for Mission Critical Network team of Pöyry Finland Oy.

The first part of this thesis covers Video Conferencing on a general level and potential security breaches it has following different solutions for these problems. The second part deals with Audio over Ethernet and current transformation from analogue to digital systems. Dante AVB/TSN, Ravenna and various other presentation technology systems are covered. Lastly, IP announcement systems are explained.

The analysis offered some solutions for Video Conferencing systems regarding how to avoid security breaches, but no obvious fix for all situations was found that would be easy to implement. The most important thing is to put the devices behind a firewall and configure the firewall according to the situation. This is not as easy as it sounds though. This will prevent some, if not most threats and there are also other ways to improve security like H.323 proxy and/or gatekeeper possibly together acting as middle ground in the call.

Upon analysing Audio over Ethernet, no major security threat unique to it was found. Dante, AVB and others often operate behind firewall avoiding the worst threats. Thus the focus was more on systems on a general level and less on the security perspective. The same can be said for IP announcement systems.

Audio/video devices have been moving to a digitalized form more and more recently. This makes the knowledge of these systems necessary for network engineers when designing networks. In future this progress only increases while systems evolve to take advantage of IP protocols.

Keywords	Video Conferencing, Audio over Ethernet, Dante, AVB/TSN, IP Announcement systems, Public Address systems

Contents

Abbreviations

RTP	Real-time Transport Protocol. Protocol for audio and video over IP networks.
SRTP	Secure Real-time Transport Protocol. Secure version of RTP.
RTCP	RTP Control Protocol. Statistics for RTP protocol.
SIP	Session Initiate Protocol. Used to control multimedia sessions.
QoS	Quality of Service. Prioritized traffic.
DMZ	Demilitarized zone.
LAN	Local Area Network.
VLAN	Virtual LAN.
DHCP	Dynamic Host Configuration Protocol
AES67	Audio-over-IP standard.
VPN	Virtual Private Network.
GPS	Global Positioning System.
AVB	Audio Video Bridging
TSN	Time Sensitive Networking
PTP	Precision Time Protocol

1 Introduction

The purpose of this thesis is to investigate audio and video elements of internet protocol networks like Audio over Ethernet and IP announcement systems. The aim is to describe how to implement these functions securely as a comprehensive solution. This thesis also includes theory related to these subjects and is written for Mission Critical Network team of Pöyry Finland Oy. The chosen method for this is literary research. The purpose is to design networks without weak spots in the information security. This is done by researching current literature for potential issues related to information security and further expand it to show practical examples of how the network could be breached and protected from these threats.

One potential threat was found in video conferencing systems. IP-based video conferencing has spread to everywhere due to its many advantages compared to travelling which is time and money consuming. Some of the possible problems include the abuse of built-in properties and insecure settings, information leaks and even unauthorized access to the rest of the network.

2 General Principles

This section determines general guidelines for designing and maintaining a secure network especially for the subjects chosen for this thesis.

2.1 Definition of needs

The starting point should always be what is required in order to run the wanted operations in the network and based on that define which devices, services, protocols ports and such are necessary. Every installed piece of software offers a potential attack surface to illegitimate access systems. Increased security in systems often adds an extra step to the user which, in turn, affects easy usability or at least increases the cost of maintenance of the network. For this reason proper planning is essential to find cost effective ways for it and make sure security mechanisms are not too laborious which could cause users to circumvent them.

A decision is required to decide which resources need to be protected and on what level. This of course assumes the network is properly documented and all devices are accounted for. Unfortunately this is not always the case. The next step is finding all the pieces how to implement this. Each technology has its limitations and these should be known to cover for any weaknesses.

2.2 Defence in depth

It should always be remembered that a single security mechanism is never enough alone. A proper security design has layers of several fail safes if one is breached. In an optimal situation each layer has a clear function in the system. Different manufacturers might have difficulties with one another when combining products. These can affect the whole picture and cannot be ignored.

2.3 Awareness of potential vulnerabilities

Maintaining sufficient information security is more than just patching software after the system is up and running. Additional systems could offer a way past a well-protected core network.

Video conferencing seems to be a blind spot for some. It may be an unconventional method, but still an effective way to gain information about the target. This also exposes the rest of the network to attacks launched from video conferencing devices.

3 Protocols

This section explains briefly different protocols that are used in Video Conferencing, Audio over Ethernet and IP Announcement systems.

3.1 H.323

H.323 is a common standard in video conferencing and important to configure properly [1]. The management and updating of H.323 devices are sometimes done through an unprotected connection, for example Telnet, HTTP or FTP. In an internal network this is not necessarily a risk, but externally it should never be done.

There are several H.323 related security issues in video conferencing that may not apply in all cases. For example a system used only in an internal network is easier to secure, because it is possible to coordinate systems and settings to work better together. [2]

3.2 H.235

H.235 is a sub protocol of H.323 and it encrypts traffic [3], but implementing it may not be simple. All clients may not support this protocol and performance can be another issue. Sending encrypted packets through a firewall could increase latency. This is one of the points where the maximum amount of security and performance cannot always be combined at the same time. Compatibility with end devices that do not support encryption also suffers. Video conferencing traffic is real time traffic and sensitive to disturbance, latency should not be more than 300 msec [4]. If Multi Control Units exist in the network, they also need to support the H.235 protocol [2].

VPN can be used for encryption, but it does not scale well on bigger environments with many different source networks in the same call. It would have to go through various H.323 devices with encryption support on the way [5] and everything after a basic point-to-point connection with two participants adds more complexity. [6]

3.3 Session Initiation Protocol (SIP)

Session Initiation Protocol is used to control multimedia sessions and use RTP or SRTP. It is utilized in video conferencing, announcement systems, Voice over IP systems as well as possibly with the AES67 protocol. [7] The SIP protocol has many mechanisms to provide more security [8].

3.4 Real-time Transport Protocol (RTP)

The main purpose for the Real-time Transport Protocol is to minimize latency. This is done by monitoring the sent packets and trying to detect lost ones. The RTP header also gives instructions how to compile data at the receiver’s end. Examples of protocols that use RTP are SIP and H.323. [9: p. 5] It is used with real time traffic because TCP and UDP do not manage a high volume of time sensitive data well [10: p. 1].

3.5 Secure Real-time Transport Protocol (SRTP)

The Secure Real-time Transport Protocol protects RTP data by taking over data packets on the way. From that point on the packets are considered as SRTPs. Only the payload is encrypted, but message authentication is taken care of for the payload and header. Before packets reach their destination, data is converted again to the original RTP form. There are many variations for different security solutions depending on the application and how secure it needs to be. Compatibility with current systems is an important factor when deciding which one is the most suitable. [11: p. 31] [12]

3.6 RTP Control Protocol (RTCP)

The RTP Control Protocol controls RTP and monitors statistics related to transmission including QoS [9: p. 10]. These include for example jitter and the number of packets sent or lost on the way. This can be useful when quality in the multimedia is adjusted to the available bandwidth and needs to be on a specific level. [9: p. 23]

Scalability with multicast is a potential problem if monitoring is maintained because the number of destinations increase and each one requires their own control traffic. The monitoring traffic should not affect actual multimedia traffic; at that point it does not serve its purpose anymore. [9: p. 24]

3.7 AES67

AES67 is trying to do something the digital audio market needs right now. It was published in September 2013 [13]. Often the problem with new technology in a new, still forming market is a fractured way of different concepts that are competing with each other. Each company has its own standards that may not work well together if put to the same network. Digital audio networking is still a relatively new market and so far poor compatibility between vendors has been an issue. AES67 plans to correct this. The use of the SIP protocol with or without the SIP Server is possible. SIP is required if point-to-point connection is used, but point-to-multicast connection does not need SIP protocol. [14]

AES67 is a layer 3 protocol and is not an independent standard by itself. Instead it is based on standards already established and does not even intend to replace other standards. Rather it works alongside them making sure relevant parts of compatibility are covered and try to make sure technical issues do not prevent adapting new technology to full benefit. [15: p. 14]

3.8 Precision Time Protocol (PTP)

Precision Time Protocol is used for time synchronization in many places and purposes, for example in the Dante networks. It provides a way to send time sensitive packets between devices using one master clock and slave clocks. [16]

3.9 Quality of Service (QoS)

Quality of Service is a complex subject to discuss in detail and for purposes of thesis this subject is not covered. In general it could be said that QoS is an important feature for audio and video networks prioritizing traffic for latency sensitive traffic.

4 Applications

This section covers the main part of the thesis. Three different instances of presentation technology are discussed in detail; these are video conferencing application, Audio over Ethernet method and IP announcement systems. The main focus of video conferencing is on the security perspective while the rest of the two instances are described more on a general level, security included.

4.1 Video Conferencing

Video conferencing as a term can include a huge variety of solutions from dedicated systems to software based solutions like Skype or Hangouts. Software based solutions have improved in quality, having for example more options as to how many persons participate in a call. In future the popularity of these will probably rise at the cost of other options [17]. This thesis does not analyse these further and will, instead, concentrate on dedicated systems.

Interoperability between different vendors can be a problem if the devices use proprietary features and also depending on whether the solution is based on software or hardware. All this depends on how much manufacturers and service providers will co-operate with each other in future. [18]

The conflict between the ease of set up and information security also affects usability. For example the auto-answer function itself is of course a useful feature, but can be problematic in terms of security. In 2012, there was a stir related to about how vulnerable some video conferencing systems are. [19] [20]

A security company called Rapid7 published research about this potential problem and demonstrated in practice how to scan vulnerable systems on the internet. They scanned 3% of the addresses on internet searching devices using the H.323 protocol. A total of 250 000 systems were found. [21]

This triggered a response from Telepresence Options, a publication for video conferencing devices. Their opinion was that this was just being exaggerated out of proportion and not really any serious threat. The main point was how everything can be secured so let’s not worry. While this is technically true, the author at Telepresence Options dodged the actual problem and replied to a different question. [22] Unfortunately the best security practices are not followed everywhere as Rapid7 demonstrated in their research.

4.1.1 Physical security

Physical security is an important part of setting up a secure network. There are several precautions that should be taken. Sensitive documents should not be left on tables at all, but especially not where there are video conferencing cameras in the room which can be activated without the owner being aware. Some models unfortunately do not have a clear indication if it is active, for example in the form of status LED. One way to cover for this is hooding the camera. Not exactly a hi-tech solution, but it gets the job done.

After devices leave the house, they have to be put to the default state. Contact information inside the device is valuable content for people trying to get access to other networks. Also, phone numbers should not be public knowledge.

4.1.2 Insecure default settings

As with most systems, default settings are usually insecure in some way and need to be changed. This can be tough to balance for manufacturers sometimes. There are different network setups and different settings required. More secure settings means more complexity for the set up and companies seem to have trust in customers to apply these settings themselves if applicable, especially Polycom.

Auto-answer is perhaps the most common setting in this case and the one that got attention from a New York Times article. [20] It should not be turned on, but in case it is there are a few things to make it more secure. The camera can be auto-muted to prevent eavesdropping and sound has to be enabled manually. [21] The camera position can be locked in place initially and it cannot be moved without the owner’s action. [21] Also there is a possibility to add password protection to the session to keep any unwanted guests out.

Most manufacturers have auto-answer disabled, but the previously mentioned measures are still useful as a precaution. There might also be a functionality to leave a video message if the receiver does not answer.

4.1.3 Gatekeeper

Gatekeeper is not a mandatory part of the network setup, but still preferred. There are two ways to implement it, pure software or hardware. It makes for example dialling easier, and removes the need to choose different IP addresses as receivers when calling. Instead it translates these to clearly understood names. Gatekeeper can also be used to H.323 endpoint access control with gateway and Multi Control Unit, from endpoint to outside the network. Another function is bandwidth control; it does this in a centralized and scalable way. It is possible to put only one active gatekeeper per zone. Zone is basically a set of H.323 devices crossing the limits of subnets. [23]

There are several levels to choose from depending on how heavy a solution is required. More functions mean of course more complexity to the configurations. It acts as a buffer between recipients adding an additional layer of security.

Some functions are optional and can be used in call management. This includes things like handling status of endpoints, for instance is it free or occupied at the moment. Or bandwidth management, it is important to let the caller through only if there is enough bandwidth available. Otherwise the network will be congested and the video calls may start to take bandwidth from other services. It is also possible to manage security policies through gatekeeper. [23]

To be on the safe side auto discovery of gatekeepers could be turned off and all gatekeepers added manually. [23] This is only a minor issue, but in theory an unauthorized gatekeeper could try to join the network. A balance between slightly less maintenance and more security needs to be decided once again.

4.1.4 Eavesdropping

The most crucial step to prevent eavesdropping is to set up a firewall for the video conferencing devices. In this case it is not a simple task. The reason for that is the wide range of ports the H.323 protocol uses. For starters the Access Control Lists on a router offer limited protection defining allowed source IP address for the endpoints, but this is possible to do mostly when calls are done only internally.

While the call starts with known fixed ports, problems come later. Endpoints negotiate ports dynamically and create problems if no additional component is added to the network topology. This is because the range for ports is 1024-65 535, meaning the firewall would not mean anything after opening all these ports. [24] Table 1 below shows the most important ports for video conferencing. It includes general protocols and products from the different manufacturers.

Table 1. Important ports for video conferencing [24] [25]

System/Service/Device	TCP	UDP
Cisco	5555 - 5574	2326 - 2485
Polycom (fixed ports)	3230 - 3243	3230 - 3290
Lifesize	60 000 - 64 999[26]	60 000 - 64 999
Sony	2253 - 2255	49 152 - 49 239
Remote Management by (HTTP) or HTTPS	(80) & 433 (only for internal use)	
Remote Management by SSH	22 (only for internal use)	
LDAP	389	
Audio Call Control	1731	
H.323	1720	
SIP	5060, 5061[26]	5060
Dynamic H.245	1024 - 65 535	
Dynamic RTP (Video)		1024 - 65 535
Dynamic RTP (Audio)		1024 - 65 535
Dynamic RTCP (Control Information)		1024 - 65 535
Gatekeeper		1718, 1719

It was not possible to include all of the ports; Polycom alone has a much longer list than this depending on what devices are used. [24] The number of ports actually used varies with factors like protocols and the amount of participants in the call [26]. Sometimes it is possible to configure what ports or range of them is used instead of dynamic ports [25].

There are many possible solutions to this problem and what those require are discussed in detail next. There is no clear best way for all cases; it depends on many variables, topology and available resources among other things. Figure 1 shows the H.323 Proxy outside the firewall.

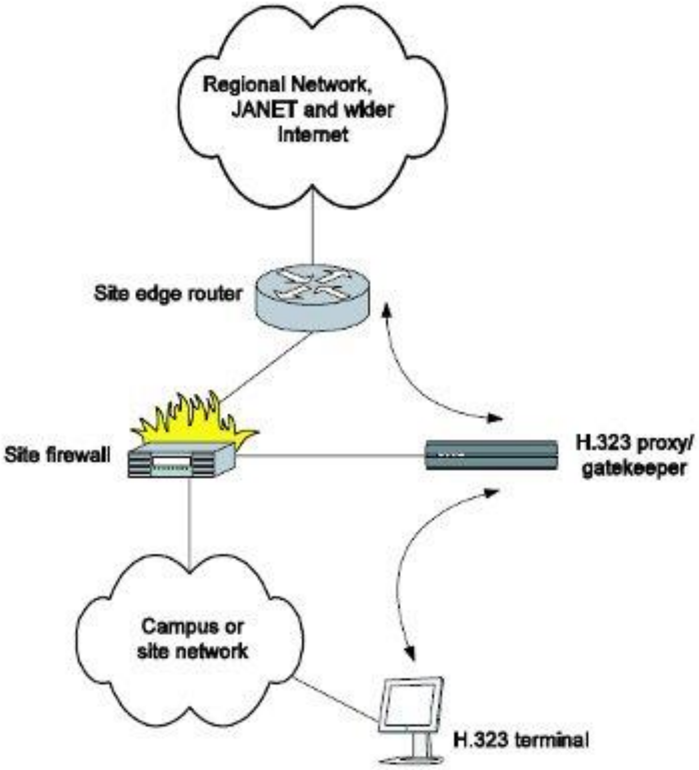

Figure 1. H.323 Proxy outside the firewall. [27]

As shown in Figure 1, the H.323 proxy acts as middle ground for establishing the call and routing between participants after that. It uses own addresses between endpoints and takes care of the table of current calls. This way only limited information about the network is revealed to the participant receiving the packets. [28] The proxy also makes firewall configuration regarding H.323 simple, H.323 traffic passing through the firewall is forwarded to the proxy [29]. The endpoints need to support proxy functionalities as a two way communication and even if only one recipient is using it, all of them need at least partial support of the H.323 proxy [30]. The use of NAT is not recommended when H.323 proxy is outside the firewall. This setup creates unnecessary traffic overhead between the endpoints and the gatekeeper. [28] Only its external address is forwarded to outside and in many ways it works like a web proxy. The H.323 proxy and Gatekeeper functions might be combined to one device [27].

If the proxy gets infected the attacker does not get direct access to inside and has to go through a firewall. The downside to this is higher bandwidth use and possible performance issues because the packets have to go twice through the firewall. [27] Figure 2 illustrates a more performance driven approach. The proxy is put behind the firewall and traffic does not travel the extra distance to reach H.323 terminal. At the same time the inside network is more vulnerable to attacks against proxy.

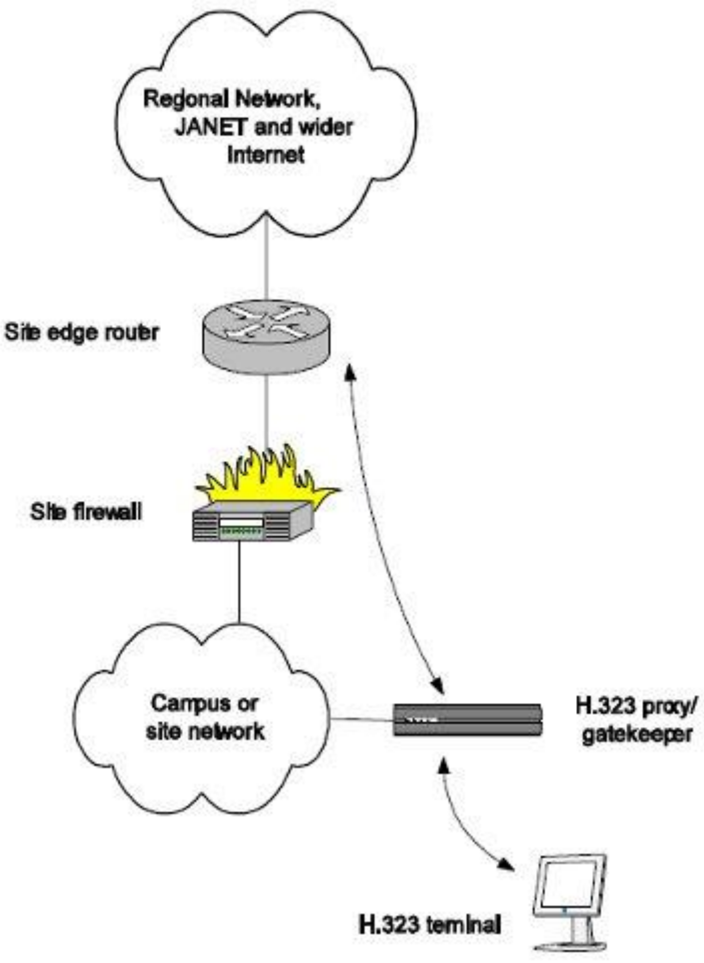

Figure 2. H.323 proxy behind firewall. [27]

The existing cables might make it impractical to implement one or another. Determining the best solution depends on the network topology and what priorities are the most important.

In theory, an H.323 aware firewall is a good way to solve this problem. There is no additional hardware to install, but it can burden the firewall's CPU to the limit where it cannot handle traffic fast enough anymore. Another issue is the different versions of

H.323. A firewall is more expensive and complex to replace than a smaller separate device when the new version comes out.

The principle of DMZ deployment is to place the H.323 endpoint to outside the internal network and keep everything else safe. It does not directly help with the security issues discussed here, but isolates it from the critical part of the network. The topology may make this impractical to implement in bigger networks and the cabling required might be a too big effort. This can make sense as part of the plan in security sense, but alone it is definitely not enough.

Another angle to go through is endpoints and their functionalities. One option is NAT; it translates the internal address to a public one. With a public address the problem of randomly determined ports is outsourced to NAT and it handles the traffic through a firewall. The endpoint knows it has both internal and external address, using external address on data packets. This may not be supported by the endpoint. [31]

Some endpoints make it possible to choose used ports in calls and after that it is easier to configure the firewall with those ports. This forces H.323 to be more firewall friendly.

The first version of H.323 was published in 1996 and since then it has evolved a lot. Version 7 was published in 2009 among other things offering a new possibility that may make the previously mentioned problem easier to solve. It adds functionality where the gatekeeper negotiates with NAT or Firewall to ensure endpoints can communicate directly with each other and keep latency lower. [32] This procedure happens before the call starts and reduces time to establish a connection. Potentially this could make secure H.323 endpoints more feasible to implement without decreasing usability or performance if the gatekeeper, endpoints and other associated devices support it.

When video calls travel to the external network there is a potential threat of man-in-the-middle attack. This makes it possible to intercept traffic and record video and sound without either participant noticing. The possibility of this can be reduced with encryption, but there are some problems with this. [33] These are discussed in Section 3.2.

4.1.5 Administrative interface

An administrative interface comes in many forms depending on the manufacturer as a way to configure the system remotely. These include for example via web, centralized service and console-based interface, automated or manual.

The most important here is to set up a strong password to at least make it harder to access the network. Without a password it is relatively easy to change the settings. An additional precaution is preventing anyone accessing management interfaces externally with a firewall, unless specifically needed.

4.1.6 Device logs

The device logs should be checked regularly for unusual activity. These could include calls from unknown source, unusual time or device activity during the time the meeting room was supposed to be empty and no scheduled meeting there. If the logs need to be accessed from individual devices, there is a danger the logs are never touched in reality due to time consuming process involved. There are ways to make this easier, additional components might pay themselves in longer period of time when maintenance takes less time. These possible components include for example Polycom's RealPresence Resource Manager is available either as hardware or software. [28]

4.1.7 Devices with secure settings

So far the situation discussed has been a case of inadequately configured devices. But when crackers have enough knowledge and tools, devices can be breached even with secure settings on. This has been already done at Black Hat Europe Conference using vulnerabilities in the software so it is past being a theoretical threat. Details of this method are found in Moritz Jodeit's research [34]; in this case it was done with certain Polycom HDX systems. Of course these specific security holes already have patches, but it is safe to assume there are still bugs in the management software or the H.323 protocol. They are either not yet found or discovered by someone, but not revealed publicly. It is more a question of when than if. When these exploits are available, a possibility to call them is enough to take advantage of the exploits. [35: p. 7]

All unnecessary administrative interfaces should be disabled; they can potentially be used as an attack surface for malicious access to a device due to vulnerabilities. It may be possible to keep malicious access in the system even if updates are applied. This is done by booting the device temporarily in the development mode instead of the default production mode and by modifying the settings for outside connections. The command shell via telnet is one way to do it. The first access does not require any credentials, something worth noting. It was an unintended function in the software and later fixed in an update. Then the device is reverted back to the production mode and to the user everything seems normal on the surface. This is a worse situation than an average unpatched system because the issue may seem to be fixed when in fact they are inside with root access. [35: p. 4]

A second variation to the previous scenario is using vulnerability in the interface and through this security hole access is granted following a temporary downgrade to firmware. Then rooting with the same method is done and upgraded back to the latest version. Once again the system appears to be secure.

Another aspect to consider is access to the whole internal network through one H.323 device depending on topology. One weak spot can be enough to go around an otherwise well protected network.

4.1.8 H.323 Multipoint Control Unit (MCU)

Multipoint Control Unit is necessary for calls that have more than two participants. It can be implemented as software or software and hardware handling call forwarding. MCU also offers additional security, because it stays between the callers and removes the point-to-point connection in the call.

It is possible to decentralize MCU with H.323 if the devices support it. [36] Every participant acts as MCU in the call and the quality may be better most of the time. A downside to this is higher bandwidth use because traffic is sent individually to everyone. In a way the same principle applies as with unicast and multicast.

If MCU is taken over by crackers, the H.323 session is possible to capture without anyone noticing. All data goes through MCU and this makes it a potential target. [37]

4.2 Audio over Ethernet

4.2.1 Dante

The transition to digital implementation of audio systems has started to get popularity in recent years. Until now technology was still developing to get to the point where it became a plausible option for the average case. Audinate is an Australian based company who developed Dante in 2006 and they are the current market leader. As technology Dante is on layer 4, using the UDP protocol for audio packets. [38] The general investment level on market has been low in recent years and this has led to out dated competitive products for Dante.

The following figures 3 and 4 are examples of typical Dante networks with some analogue devices still included.

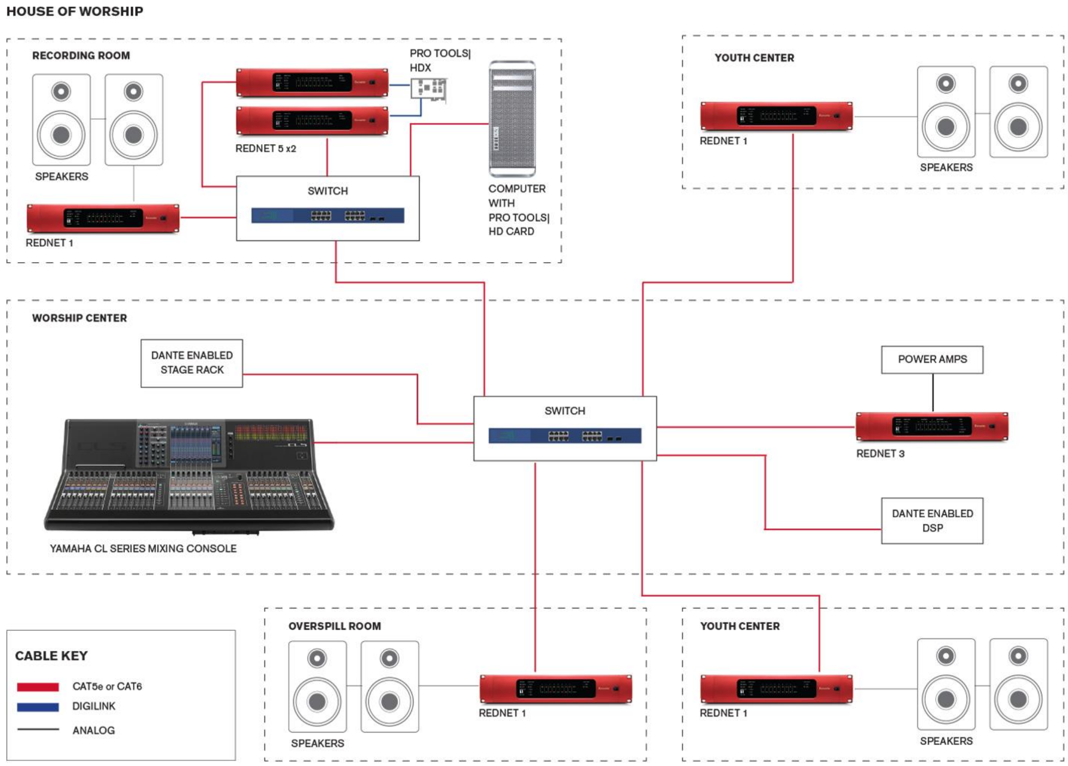

Figure 3. An example of possible Dante audio network topology in church spanning over several rooms. [39]

Figure 3 above shows an Ethernet switch in the middle connected mostly to the red Rednet network audio interfaces, but also with a mixing console, DSP (Digital Signal Processor) for managing and monitoring audio and rack on stage. These audio interfaces translate an analogue signal to digital form from the speakers. Another switch connects the recording room to the network in the same way.

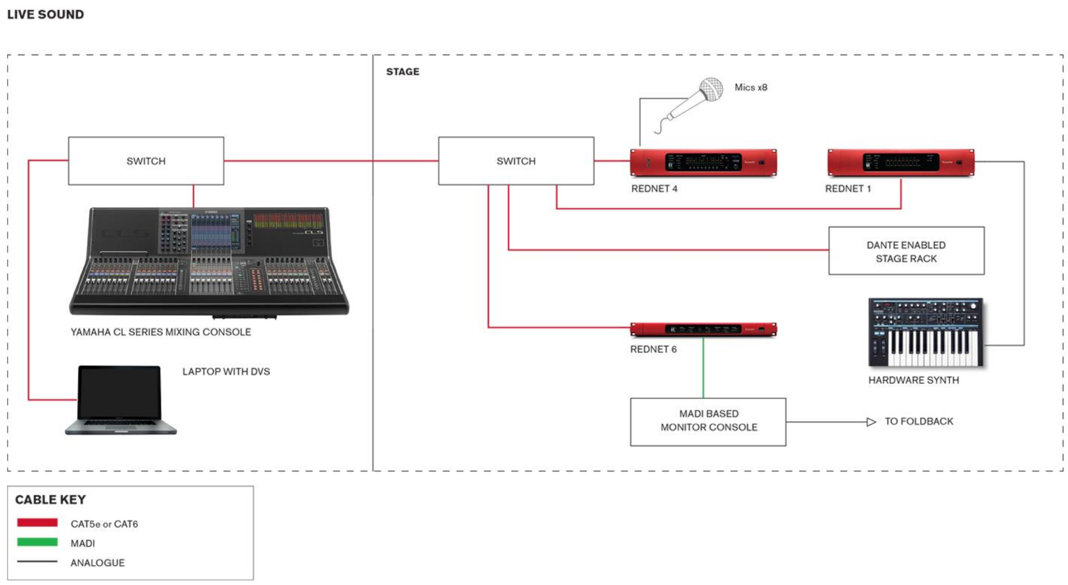

Figure 4. Second scenario with Dante devices. [40]

Figure 4 above shows live sound scenario as well with Dante devices. The mixing console is there the same way as previously, connected to a switch. On stage there is a switch, Rednet audio interfaces and a rack, also microphones and instruments with analogue signals.

One variation to these diagrams is a situation where the signal is digital from the beginning to the end and this setup would make audio interfaces unnecessary. The switches would be enough to connect the devices. PoE is needed on the switch, but a direct connection with the computer is also possible. [41]

The Dante Virtual Soundcard is an option for a small scale, local solution. There is still a requirement for at least one Dante enabled device like mixing consoles or amplifiers. It is licensed software, one license per installed workstation. VMware or other similar solutions are not supported; latency would be a problem with the way virtual machines work. A Gigabit port is recommended on the PC if over 32 channels are active, the maximum for the Virtual Soundcard is 64 channels. The PCI card on the other hand is capable of 128 channels and in heavy use it might be preferable compared to the Virtual Soundcard. [42] Latency is also higher in the latter. Hardware performance is related to it; when latency is smaller a more powerful workstation is needed. This depends on the current case, for example real time monitoring of sound requires low latency [43: p. 59].

Dante Via was published at the end of 2015 offering another software solution. [44] It does not require the Dante hardware to function, a standalone network is also possible. The main idea is to connect the individual devices to the PC and these separate instances of devices are connected to each other. The main difference compared to the Virtual Soundcard is the lack of channel quantity. Via is optimal when a wide range of low end devices are used and connected to the same Dante network.

4.2.2 Major players along Audinate

The Audio Video Bridging (AVB) standard has a different approach to audio over Ethernet, also known as Time Sensitive Networking (TSN) now. It is a layer 2 solution at the moment; layer 3 features may come in future. [45: p. 12] [46] Time Sensitive Networking Task Group is responsible for this new initiate. Their plan is to be the standard for the industry and through that get manufacturers and customers to implement it in devices and networks. There are four IEEE 802.1 AVB standards that switches need to follow. These are 802.1BA [47] for the general AVB system, 802.1AS [48] for timing and synchronization and 802.1Qav [49] & 802.1Qat [50] for the equivalent of QoS for AVB. The main advantage is low latency. This is achieved by reserving a determined portion of bandwidth and no other traffic will not use that reserved bandwidth. [51] Dante has done this the opposite way and it seems to work better, functional solutions become standards eventually just by being dominant in the market. AVB Task Group has a certification program that tests the network equipment is compatible with IEEE standards. After which it can be publicly referred to as AVB compatible. Audinate has promised that Dante will be compatible with AVB when it is mature as a technology. [42]

The German Ravenna is designed for specialized audio networks, broadcast networks. [52] Examples for these include live events and sports stadiums. It is compatible with the AES67 protocol which should make it possible to combine different manufacturers in same network. Among others Ravenna and Dante are already members of that group implementing AES67. [43: p. 66]

4.2.3 Requirements of Dante for Ethernet network

The requirement for switches and Ethernet network varies depending on what solution is selected. Specific details for each one are discussed separately. But on a general notion regardless of solution, be sure to give audio data and management data both separate Virtual Local Area Network (VLAN) and some sort of QoS to prioritize the traffic.

Dante is designed to be easy to use and based on standards as much as possible. As such, no special switches are needed for a Dante compatible network. In theory there are several things needed. These include Gigabit port switches for lower latency than 1 msec with a possibility down to 150 µsec [43: p. 24], Diffserv (DSCP) Quality of Service with strict priority and four queues and energy saving features turned off. While otherwise a potentially good feature, energy efficiency can cause problems with Dante. [53] Dante devices use DHCP addresses by default, but some support static IP addresses. [42]

But all these are standard functions found in switches. If a switch has standard Voice over IP QoS then Dante works also. Dante does not work with a wireless connection, which is one limitation it has. [42] While technically possible, it is not reliable enough. Consistent performance could not be guaranteed causing potential problems with latency.

Dante Controller is software used for routing and monitoring Dante network in various ways. [54] These are for example used bandwidth with unicast or multicast. Also different kind of statistics like performance status, latency statistics and event logs. Other functionalities include among others configurable latency or latencies. By default it is the same, but different values can be configured at the same time to satisfy different needs. For instance live broadcast does not need as good quality as recording for later use. Latency is also consistent and does not fluctuate as long as it is not set up too low causing audio packets unable to achieve that requirement in the network making glitches appear. The threshold for this depends on the size of the network. [43: p. 24]

Dante Controller has one limitation for certain topologies; Dante devices can’t be in different subnets as far as any remotely practical solution goes. There is no real advantage for not putting them in the same subnet, but the network design could be done before the Dante system is even chosen or audio administrator may not always have the power to change IP addresses on the network. Whatever the case is, the easiest course of action is to find a way to use one subnet one way or another. Otherwise device management is more complex because one instance of Controller cannot manage the whole Dante network and Dante devices cannot interact with each other when in different subnets. [79]

Presets are saved configurations that are possible to copy to other devices or just keep as backup to try new settings. [54] It is an xml-file that is possible to edit offline and use compatible settings in each device where loaded. If the device does not support a particular thing, the interface will say so.

Figure 5 below shows an example of the interface and possible options to how to route Dante devices. The inputs and outputs have channels listed under them. The names of devices and channels can be renamed if the given name is difficult to read or remember. [55]

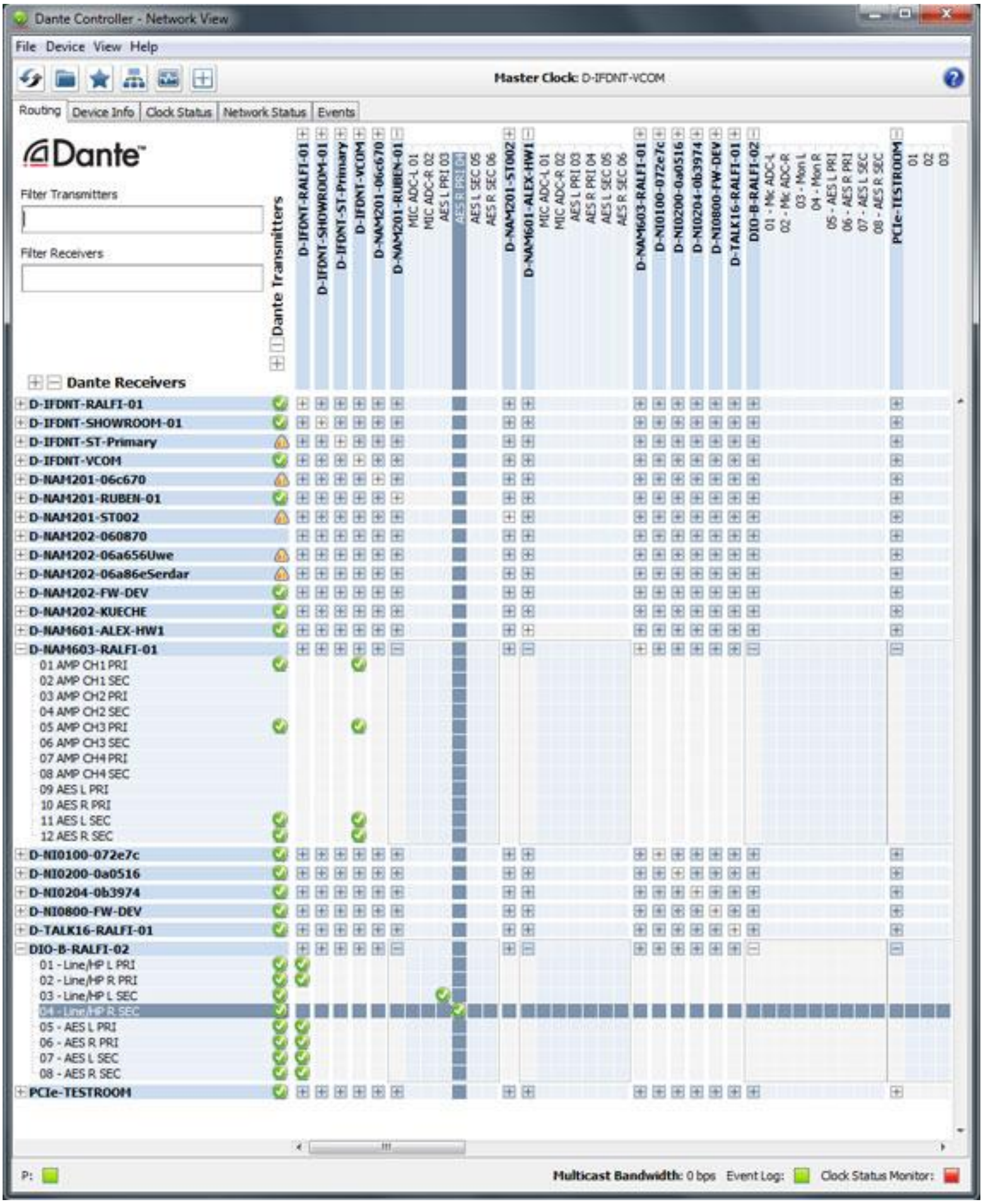

Figure 5. Dante Controller interface [55]

4.2.4 Old layer 2 only solutions for audio networking

Cobranet used to be a major player in networked audio markets, but have gradually lost market share to more advanced products. [15] They operate only on layer 2 and this shows for example with the Quality of Service protocol. Layer 2 QoS has only limited functionality which may affect the performance on the audio network.

Ethersound is another layer 2 solution and a rather old product. [15] While a competent solution years ago, at this day it has already lost its advantages compared to competitors. Compatibility with networking equipment is problematic and the lack of layer 3 protocols does not help either.

With layer 2 solutions daisy chain topology was common and for example layer 3 Dante does not support it most of the times usually using star topology and being connected to a switch. Daisy chain connects network devices in a chain and while easy to implement, the same cannot be said for functionality. The hop count will get too big and traffic will slow down. All devices also become a single point of failure.

4.2.5 Redundancy in Dante

Dante devices have two Ethernet ports for redundancy, primary and secondary. [43: p. 22] These are separated from each other and a secondary port can be used as backup. Configuring settings once is enough, both ports use these automatically. If the primary route loses the connection, the secondary should take the lead without any noticeable disturbance between. The Dante Controller interface shows the status of secondary routes providing a way to check that the backup is working as planned. [56]

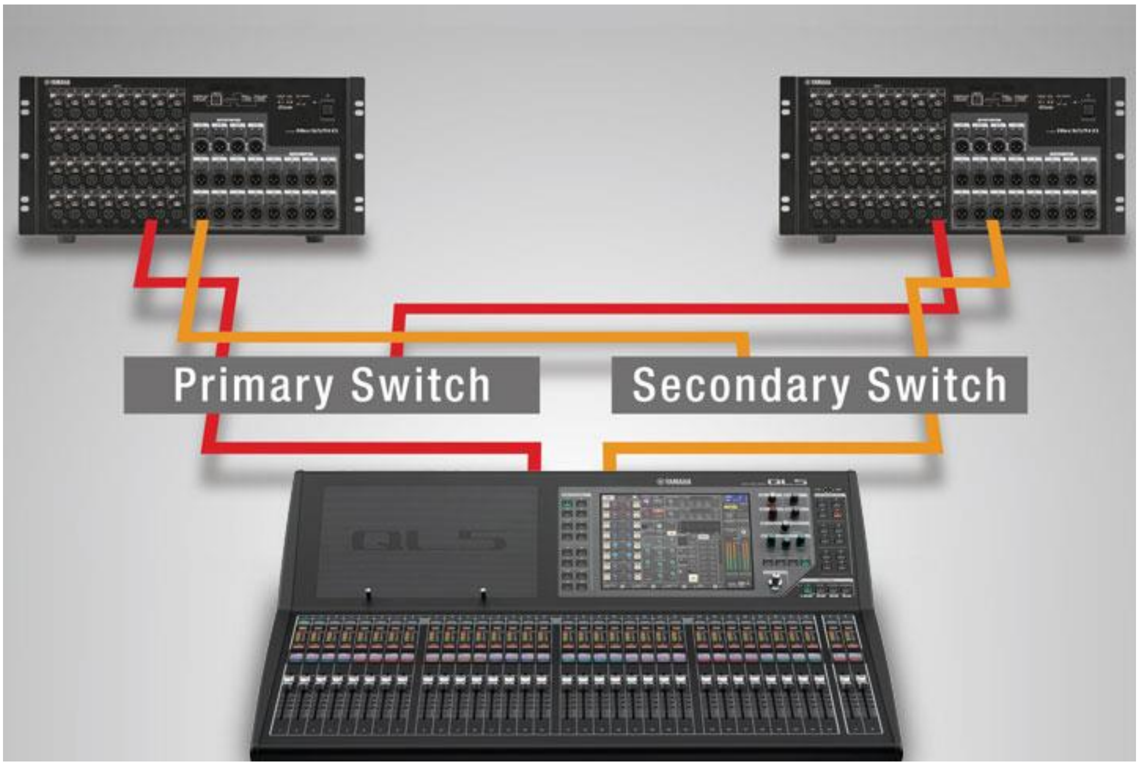

Figure 6. Redundancy setup for Dante network [57]

The situation in Figure 6 above is fully backed up route where the primary and secondary networks are completely separate. This can be done also partially with a VLAN depending on how much redundancy is wanted in the network, for example using the same switch. [58]

There is a recommended order to avoid potential problems when setting up this redundancy. At first Dante devices are configured and then switches. After this the primary network route should be connected. When it works, the secondary network is connected and tested for functionality. [59] While redundancy is useful to have, it is good to at least acknowledge potential complexity in troubleshooting that primary and secondary ports may cause. On a related note, Dante Virtual Soundcard does not support redundancy functions requiring Controller to do it.

4.3 IP announcement systems

4.3.1 Challenging environments

Announcement systems are used in many public places like airports, supermarkets and hospitals. One familiar example is schools where sound quality from speakers could have been better. It is not only a matter of being sensitive to sound quality; communication can also suffer to the point where the message is not understood anymore. At that point something needs to be done; the announcement system is not doing its work anymore. For example train stations present a challenge to announcements. The area to cover is wide, background noise disrupts clear hearing, the smallest details can make the difference if it was helpful at all and finding a suitable volume level may be difficult, too loud hurts those who stand too near while too quiet volume is not good either. [60] In future more clear announcements are possible with software altering speech and making it possible to the lower volume level while still keeping the same level of understanding for listeners. [61]

Public address systems can use wide variety of endpoints, but one specific example is smart phones using a location based service with GPS. When the user is in a certain location, the app gives the information in written form on a smart phone. So far this has been done at least in Australia with an app called OpenAccess Alerts [62]; up-to-date information requires the cooperation of local organizations. This would be a useful service for the deaf and people with impaired hearing. [60: p. 8]

There are many companies that manufacture IP speakers for announcement purposes. These include among others Valcom, CyberData, Atlas IED and Advanced Network Devices. [63] The management side has also many providers for public address systems, for example Singlewire [64], Syn-Apps [65], Honeywell [66] and Zenitel [67].

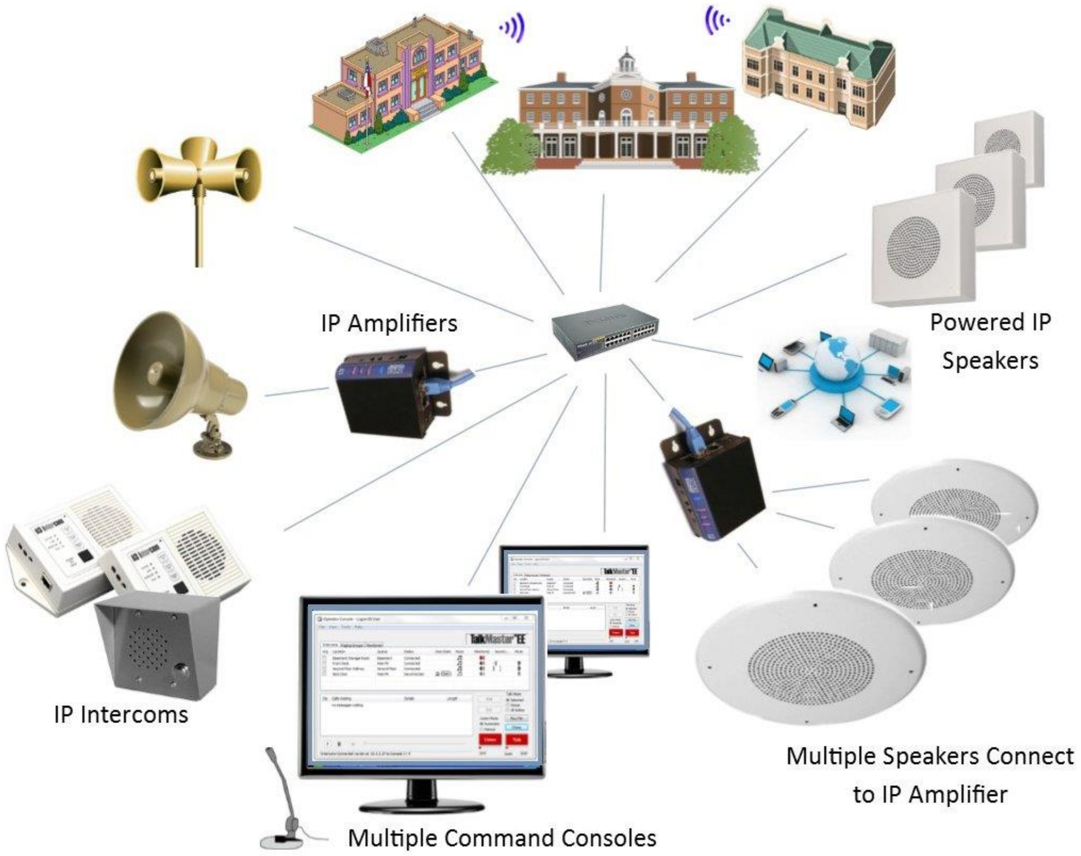
IP Amplifiers
Powered IP Speakers
IP Intercoms
Multiple Speakers Connect to IP Amplifier
Multiple Command Consoles
TalkMaster EE

Figure 7. Various components required for the IP announcement system [68]

Figure 7 above shows speakers with or without IP amplifiers depending on the devices in question. Analogue speakers need IP amplifiers to be connected with a switch while Ethernet compatible speakers are connected straight to the network. Lastly, intercoms offer two way communications to a specific location and if required, also IP access control or IP camera. Management software and a microphone are used to control this network as a whole.

4.3.2 Possible uses for the announcement systems

Voice over IP phones are a possibility when deciding what end points to connect to the network and be used to make announcements. This gives the added benefit of more digitalized components.

It is possible to use intercom over WAN. This opens possibilities to communicate longer distances without additional systems. Management and monitoring is also possible from a remote location if the topology requires this functionality. [69] [70]

Digital announcement systems may use SIP over TCP protocol instead of UDP to make sure packets reach their destination. There are similarities with VoIP protocol, SIP and RTP protocols are used. Most likely DHCP is also supported.

Intercoms can be combined with access control and surveillance cameras to remotely interact with a person in a building, establishing two way communications with sound and audio. This offers many possibilities. Recording audio and video through the systems is also technically possible, but legal problems may provide obstacles for implementation.

A wired connection is not mandatory for public announcement systems, wireless works as well. This broadens situations where digital systems can be applied; sometimes the wireless option is easier and/or a cheaper way in individual locations. Another additional useful feature is a desktop computer acting as a speaker for IP announcements, for example InformaCast supports this. Depending on topology it may fill the need for a speaker, an example would be a room that always has a powered on computer and user sitting nearby it, therefore the volume level is also enough for its purpose. [71]

Figure 8 below shows a topology for the announcement network and possibility for wireless connection for remote speakers. The management software here is Talkmaster from Kintronics which offers various ways to configure and manage devices.

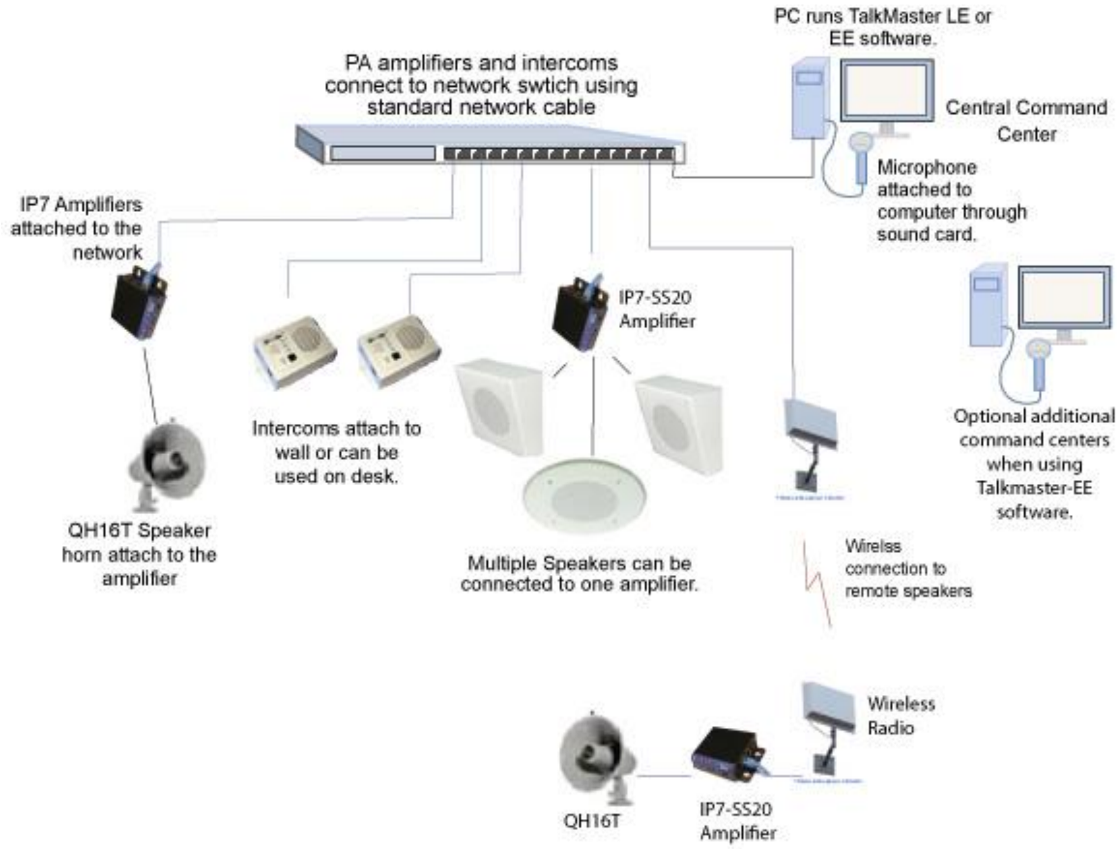
PC runs TalkMaster LE or EE software.
PA amplifiers and intercoms connect to network swtich using standard network cable
Central Command Center
Microphone attached to computer through sound card.
IP7 Amplifiers attached to the network
IP7-SS20 Amplifier
Intercoms attach to wall or can be used on desk.
Optional additional command centers when using Talkmaster-EE software.
QH16T Speaker horn attach to the amplifier
Multiple Speakers can be connected to one amplifier.
Wirelss connection to remote speakers
Wireless Radio
QH16T
IP7-SS20 Amplifier

Figure 8. Topology for announcement network [72]

5 Conclusions

This section discusses what should be done based on theory of previously analysed systems. In addition, it describes what conditions are required from the network and how the different requirements for properties affect the chosen solutions.

5.1 Video conferencing

It is relatively easy to set up a video conferencing system, but another thing to get a secure system. It takes effort to configure the firewall and harden the devices. [73] [74] Dedicated systems vary in size. Some can be small and others big and expensive for bigger offices depending also on the budget available. Depending on the solution a different amount of configuration is required.

Cloud based systems have a different angle; they are easier to scale to different situations. The solution is often offered as one license per user without any need for expensive investments in conference rooms. As such the cost per user is probably less than with dedicated systems. These systems work either with additional hardware or only software on workstation. [75] Updating is easier in this case, often automatic. This is one factor to consider, keeping dedicated devices up to date is one more task for IT infrastructure maintenance which has to be done regularly.

The drawback is of course the reduced amount of control over the system. Using video conferencing on the cloud means that the user considers the service provider trustworthy for the information processed and data stored there. If this is not the case then another solution should be found. Critical data for the organization is probably best to keep off the cloud to be on the safe side.

General best practices for secure network and IT systems also apply here. Default usernames and passwords should be changed from factory settings and all devices put behind firewall. This protection is not only for pure security reasons, it also prevents DOS and DDOS attacks from taking down the service. It is good practice to logically isolate video and audio traffic with VLANs in the network for extra security.

The probability of breaches should affect how strong actions are taken. Unless there is a need for strong security, the costs are probably a decisive factor. The starting point is to keep the times and dates of sessions only between persons who need the information. It may attract unwanted attention when the schedule is known for the public.

If sessions are recorded, access to the recordings should be controlled. For these to fall into wrong hands is the same as letting them to spy on a live session. It is good to check out what the laws say if recordings contain medical or otherwise sensitive information.

Many things that can be done to harden devices from relatively insecure default settings. It depends on the manufacturer how much hardening is needed, but most things apply to all videoconferencing devices. [76: p. 23]

The first thing to disable is auto-answer. It is already discussed in detail in insecure default settings and what should be done if this is required anyway. It is risky for the small comfort it gives. Default usernames and passwords should also be changed like in every device.

There are hardware and software available that allow centralized management and make it possible to maintain devices with less effort. This may improve security indirectly because a more complex setup is possible to keep intact with a larger amount of devices and updating is more organized.

Various issues with video conferencing have been covered in thesis, but these included some form of flawed settings exposing devices. If all points are covered, the situation is under control and most likely secure. There are ways to get through even in this case and this has been done already. There is no need to fear this and let it affect too much, but at the same time also avoid overconfidence that potential threats are not relevant to the system in use. Since new threats could eventually evolve to bypass security, even a secure network needs a fresh overview once in a while.

The question of one or several vendors in a network is a priority between compatibility and security, as is the amount of maintenance. A network including only one vendor for one type of device has a benefit of built compatibility between devices. At the same time it exposes to the same bugs in the code. It is possible to have the same security hole existing in several vendors' systems, but it is not the most probable scenario.

5.2 Audio over Ethernet

Audio over Ethernet as technology is developing all the time, but fully digitalized audio networks as a standard solution are still in future. There are still a lot of existing and fully functional audio equipment with administrators who are cautious to implement new technology. It will reach that point slowly, but eventually.

Technology can be the best on a technical level, but it does not automatically mean it will spread to customers. AVB still requires more support from switches. The current infrastructure of switches most likely needs to be replaced if used with AVB and switch models that support it are limited in number. [77] This makes the transition more difficult. The lack of license fees balances the scale a little bit for the purchase of switches that are more expensive than the same level switch without AVB compatibility. If the support increases in future, the situation may change in favour of AVB. But AVB may have a better future in the automotive and industrial sector even if audio networking does not work for them in the end. They operate also under the name Time Sensitive Networking Task Group now.

5.2.1 Transition from analogue to digital

The transition from analogue to digital is just beginning in audio control systems. Analogue systems have been the way to go for a long time and changes take a while. But it is coming slowly. There are some cases where analogue might still be better than a digital system, especially if lower than normal latency is required. Or maybe the situation is cabling one smaller physical location and it is enough to cover everything. In that case the difference between two systems is smaller in management complexity, monitoring and costs.

A digital system is cheaper and easier to set up, also saving a lot of space from all copper wiring. In past there were serious problems with various aspects that delayed the transition and kept old ways going. Possible obstacles included for example poor support with switches or limited functionality.

5.2.2 Security

There are three main reasons why security in IP audio networks is less of an issue than on average network application. IP audio networks operate by design mostly in internal networks only behind a firewall and as such do not need the same level of security than systems communicating with the outside world. A second factor is the relative lack of confidential information or benefits to crackers. There are more than enough better targets out there. Lastly sabotaging an audio network is hardly worth the effort considering what needs to be done. If the firewall is bypassed on a network, chances are that limited opportunity is used for something else before risking detection with the audio network. After audio data is processed, stored and not managed under Dante, for the purposes of this analysis data is considered more under general data security than in IP audio networking.

Standard security features in network equipment and especially port security apply here the same way as would be expected. Usefulness of adding security features is always relative to the system where it is applied. In this case there is no real advantage what would be gained with it not counting the previously mentioned actions. One possibility is for example restricting management access of the Dante network to only a certain end device with VLAN. Dante audio inputs and outputs need to see each other clearly for the system to work and have as fast route between each other as possible.

Low latency is an important part of performance and relevant to keep in check. In summary it could be said that normal procedures in network security provide sufficient protection from possible threats. Without low latency or good usability Audio over Ethernet would not be a better option over analogue systems even with all its advantages.

When the audio network covers multiple physical locations and traffic going between them, VPN could be turned on. It does not affect the quality of audio data, but additional latency usually comes with it. In most cases it is not a problem since raw audio data is managed in LAN, this is the part where latency matters most. After the audio data is processed and ready to send forward, suitable latency can be selected for each situation.

5.3 IP Announcement systems

The main difference between Dante-like systems and IP announcement systems could be the most critical factor in transmission. Both transmit audio over network, but the former prioritizes latency when on other hand the latter favours getting all packets to the destination at the cost of latency at least in the critical systems. For example music can fit to both cases depending on the case; background music would better fit to announcement systems and live music to Dante. Another way to differentiate the two systems is the usability in an emergency situation.

Compared to an analogue system an IP based system scales easier when new devices are added, they can be connected to existing network without long wires everywhere. It is cheaper and less time consuming to set up. Maintenance is easier when the system gives an indication whether or not all devices are working, i.e. gives out status reports. The relative price for an analogue system increases for every building and location necessary to cover. [72]

Normal network security procedures apply for announcement systems. These include up-to-date management systems protected with passwords, port security, subnets and devices behind firewall. Applying encryption with VPN for connection over WAN is a good precaution.

IP speakers with built-in amplifiers may be suitable to the case at hand if high power levels (W) are not required. A more powerful separate amplifier can power up louder speaker or several speakers with average sound volume, a suitable level can be purchased to get a cost effective solution with the intended sound properties. More powerful models of IP speakers with their own power supply may also fit the purpose. A longer distance and louder sound level need more power; each increase in volume means higher relative increase in power use. This makes louder speakers to consume a lot of power. [78]

Selective use of speakers is possible when needed for example in hospitals [66]. It is not only convenient to target a specific location, but also critical in some cases. Emergency situations may require communication to certain location or locations in order to save lives, broadcasting universally everywhere could create panic and make the situation more difficult to manage.

6 Closure

Regardless of recent years’ increase in service based video conferencing, there is also room for traditional systems in the market. Cloud based systems most likely increase popularity on the low end and partly in the middle. It is easier and cheaper to implement this securely. The service will take care most of it assuming of course that the service provider is trustworthy. But these do not have the same level of quality and usability as more expensive options.

It does not have to mean choosing one or another, the most secure way can be a combination of both. For daily use, a lighter version might be sufficient and at the same time a limited number of dedicated devices exists to cover for cases where it is required. In this scenario, maintenance is easier to manage and through that make a more secure implementation more probable.

There are many things in video conferencing that can be done to mitigate the threats, small and big. What are the correct choices depends entirely on the situation; different networks have different level of needs for security. There is almost always some kind of cost for security. These are financial cost, more laborious maintenance, decrease of usability, compatibility and/or performance.

After a proper analysis of what is an optimal and secure solution there are a few ways to continue. If superior quality of video and audio with features is a priority for video conferencing then dedicated systems are the correct choice. With a properly planned implementation regarding security, there is little risk for breaches. Of course the system won’t be one hundred percent immune to attacks, but most systems rarely are that. When easier targets are available with the same reward, the effort tends to go towards them.

Audio over Ethernet systems are a small and specialized part of the network world and due to this have received little to none attention from big players like Cisco. This has led to a situation where two different approaches merged to market. Dante works with off-the-shelf switches with minimal investment required. Regardless of current network, Dante most likely works there. Features are sufficient and more are in development. The interface also seems easy to use. These factors probably keep Dante on the number one place in the market for a while.

AVB/TSN on the other hand tries to establish a new standard aiming for compatibility on Audio over Ethernet field and is losing the momentum ironically because of that exact reason. It is not compatible with standard switches and if this does not improve soon, recently published AES67 will take over this task instead. It does not try to be ambitious and replace everything, only what is necessary. Practice has shown this pragmatic approach works.

While both previously mentioned Audio over Ethernet and public announcement use sound systems, the priorities are different. For the former audio quality is important. IP Announcement systems on the other hand prioritize reliability.

Compared to analogue systems digital implementation is a more attractive option and advantages increase in relation to the more complex the system gets and the longer the distances between the devices get. In terms of security, there are no serious threats for announcement systems that would need to be addressed. Typical network procedures are sufficient.

7 Summary

The starting point for this thesis was the notion that video conferencing equipment might have security problems.

There were problems to keep the content within a reasonable amount with the current focus, and many topics were discussed less or not at all. To limit the range of topics to a reasonable level, only the minimum depth necessary was analysed. These include VoIP, video walls, various protocols and general topics related to video conferencing, for example the wide range of products that exist. While useful knowledge, it is not in the scope of this thesis. The portion of the video conferencing content was becoming too big and it was limited to make it smaller.

Only a few major manufacturers were mentioned in passing a few times. The same policy was chosen for IP announcement systems, some example products were introduced on a general level. No content for hands on configuration or command line commands were written on purpose as this was not relevant for the scope of this thesis.

There were some problems to find constructive critic about Dante aside from obvious marketing material of its rivals. Sometimes it felt too good to be true because the information found was almost too positive. Some information was found, however, that Dante may not perform with 100% reliability, but it wasn’t possible to confirm whether this is true or not and because of the lack of proper sources it wasn’t mentioned in this thesis. There was no Dante network available for the purposes of the thesis where this hypothesis could be tested.

A similar issue was the scenario with Dante devices spread to more than one subnet under Dante Controller. Audinate announced in 2011 that software called Netspander will be published and after that the knowledge of it almost disappeared without any mention on the official website. Several isolated pieces of information from unofficial sources were found stating that this functionality was integrated to the system later on, but there was no clarification from Audinate that this is the case. An inquiry was sent to their customer support and they responded saying Dante Controller does not support several subnets. [79]

After researching for potential threats, no major security holes were found uniquely from Audio over Ethernet or IP announcement systems. Both systems operate mainly behind a firewall and are therefore protected by normal security procedures. Because of this, the content for these systems was less concentrated on security than on video conferencing and more on a concept level.

References

1 H.323. WWW document. Wikipedia. <https://en.wikipedia.org/wiki/H.323>. Read 15.7.2015

2 Overview of H.323 security issues. WWW document. Jisc Community. <https://community.jisc.ac.uk/library/janet-services-documentation/overview-h323-security-issues>. Read 10.7.2015

3 H.235 protocol. 2005. PDF document. ITU-T. <http://www.itu.int/itu-t/recommendations/rec.aspx?rec=7440&lang=en>. Read 20.7.2015

4 Performance metrics for video conferencing. 2009. WWW document. Techrepublic.<http://www.techrepublic.com/blog/data-center/is-your-network-ready-to-handle-videoconferencing/>. Read 9.11.2015

5 Video Conferencing Security. 2013. WWW document. Wainhouse Research. <http://www.nojitter.com/post/240160666/keeping-video-conferencing-security-in-perspective-8230>. Read 20.12.2015

6 Encryption on video conferencing. WWW document. Jisc Community. <https://community.jisc.ac.uk/library/janet-services-documentation/encryption-ip-security-ipsec-and-vpns>. Read 1.9.2015

7 SIP protocol. 2004. WWW document. Network World. <http://www.networkworld.com/article/2332980/lan-wan/what-is-sip-.html>. Read 12.10.2015

8 Best practices for SIP security. 2011. DOC document. IMTC SIP Parity Group.<https://datatracker.ietf.org/documents/LIAISON/liaison-2013-03-27-imtc-sipcore-imtc-work-on-sip-feature-parity-with-h323-attachment-2.doc>. Read 8.8.2015

9 RTP protocol. 2003. WWW document. IETF. <https://www.ietf.org/rfc/rfc3550.txt>. Read 15.8.2015

10 Protocol overview: RTP and RTCP. PDF document.<https://www.netlab.tkk.fi/opetus/s38130/k99/presentations/4.pdf>. Read 20.8.2015

11 SRTP protocol. 2004. WWW document. IETF. <https://tools.ietf.org/html/rfc3711>. Read 3.9.2015

12 Security for video communications. 2012. WWW document. Cisco. <http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/videodg/vidguide/security.html>. Read 15.1.2016

13 AES67. WWW document. Wikipedia. <https://en.wikipedia.org/wiki/AES67>. Read 11.12.2015

14 AES67 FAQ. WWW document. Media Networking Alliance. <http://medianetworkingalliance.com/faq-aes67/>. Read 4.2.2016

15 Rise of audio networking. 2015. PDF document. Audinate. <http://go.audinate.com/resources/assets/death-of-analog-rise-of-audio-networking-f>. Read 20.10.2015

16 Precision Time Protocol. 2015. WWW document. National Instruments. <http://www.ni.com/newsletter/50130/en/>. Read 20.1.2016

17 Telepresence Options. 2014. WWW document. Video conferencing market predictions. <http://www.telepresenceoptions.com/2014/04/2014_video_conferencing_market/>. Read 20.7.2015

18 Video conferencing interoperability. 2011. WWW document.<http://searchunifiedcommunications.techtarget.com/feature/Video-conferencing-standards-and-interoperability-considerations>. Read 21.7.2015

19 Board Room spying. 2012. WWW document. Rapid7. <https://community.rapid7.com/community/metasploit/blog/2012/01/23/video-conferencing-and-self-selecting-targets>. Read 20.7.2015

20 Coverage for Rapid7 results. 2012. WWW document. NY Times. <http://www.nytimes.com/2012/01/23/technology/flaws-in-videoconferencing-systems-put-boardrooms-at-risk.html?_r=3&pagewanted=all>. Read 20.7.2015

21 Video conferencing hackers. 2012. WWW document. Rapid7. <https://community.rapid7.com/community/metasploit/blog/2012/01/25/mythical-videoconferencing-hackers>. Read 20.7.2015

22 Reply for Rapid7’s revelations. 2012. WWW document. Telepresence Options. <http://www.telepresenceoptions.com/2012/01/how_to_defend_your_boardroom_a/>. Read 20.7.2015

23 H.323 Gatekeepers. 2014. WWW document. Cisco. <http://www.cisco.com/c/en/us/support/docs/voice/h323/5244-understand-gatekeepers.html>. Read 8.9.2015

24 H.323 ports used by Polycom devices. 2015. WWW document. <http://knowledgebaseiframe.polycom.com/kb/viewContent.do;jsessionid=DEA73339132C40F4730AB7E600527E1E?externalId=12174&sliceId=1>. Read 5.10.2015

25 H.323 firewall ports. WWW document. Easymeeting. <http://www.easymeeting.net/firewall/>. Read 10.10.2015

26 Required firewall settings for Lifesize devices. WWW document. <https://www.lifesize.com/~/media/Documents/Product%20Documentation/Video%20Systems/Tech%20Notes/LifeSize%20Tech%20Note%20for%20Firewal%20Transversal.ashx>. Read 8.10.2015

27 H.323 Site deployment. WWW document. Jisc Community. <https://community.jisc.ac.uk/library/janet-services-documentation/h323-site-deployment>. Read 15.8.2015

28 H.323 Gatekeepers. WWW document. Cisco. <http://www.cisco.com/c/en/us/td/docs/ios/12_2/voice/configuration/guide/fvvfax_c/vvf323gk.html>. Read 9.12.2015

29 Davidson, Peters, 2006. Voice over IP Fundamentals, 2nd edition. Cisco Press, page 249. Read 18.2.2016

30 H.323 and firewalls. WWW document. Vtel. <http://www.vtel.com/support/galaxy/h323_proxies_firewalls.htm>. Read 26.1.2016

31 H.323 and SIP ports. 2015. WWW document. 21st Century Video. <http://www.c21video.com/whitepapers/h460_nat_firewall_traversal.html>. Read 12.9.2015

32 H.323 version 7. WWW document. Packetizer. <https://www.packetizer.com/ipmc/h323/whatsnew_v7.html>. Read 8.11.2015

33 H.323 Border Traversals. WWW document. Jisc Community. <https://community.jisc.ac.uk/library/janet-services-documentation/nat-firewalls-and-videoconferencing-h323-border-traversals>. Read 19.8.2015

34 Black Hat Europe research, hacking with secure settings. 2013. WWW document. Computerworld. <http://www.computerworld.com/article/2474852/cybercrime-hacking/black-hat-europe--hacking-to-spy---remotely-control-video-conferencing-systems.html>. Read 20.7.2015

35 Hacking video conferencing systems. 2013. PDF document. Black hat Europe. <https://media.blackhat.com/eu-13/briefings/Jodeit/bh-eu-13-hacking-video-jodeit-wp.pdf>. Read 20.7.2015

36 Ellis, Pursell, Rahman. 2003. Voice, Video and Data network converge: architecture and design, from VoIP to wireless. Academic Press, page 139-142. Read 1.2.2016

37 H.323 session snooping. WWW document. Jisc Community. <https://community.jisc.ac.uk/library/videoconferencing-booking-service/call-snooping-recording-and-unwanted-guests>. Read 27.8.2015

38 Dante FAQ. 2014. WWW document. Audinate. <https://www.audinate.com/resources/faqs>. Read 3.11.2015

39 Church scenario for Dante system. WWW document. Focusrite.<http://us.focusrite.com/rednet-how>. Read 5.11.2015

40 Live sound scenario for Dante system. WWW document. Focusrite.<http://us.focusrite.com/rednet-livesound>. Read 5.11.2015

41 PoE microphones and Dante. WWW document. Audio Technica.<http://www.audio-technica.com/cms/site/90db6b317f40d616/index.html>. Read 15.12.2015

42 Dante FAQ. WWW document. Audinate. <https://www.audinate.com/resources/faqs>. Read 20.11.2015

43 Dante Controller user guide. 2015. PDF document. Audinate. <http://dev.audinate.com/GA/dante-controller/userguide/pdf/latest/AUD-MAN-DanteController-3.6.x-v1.1.pdf>. Read 6.2.2016

44 Dante Via. WWW document. Audinate. <https://www.audinate.com/products/software/dante-via>. Read 20.11.2015

45 AVB/TSN. 2015. PDF document. AVNU. <https://standards.ieee.org/events/automotive/2015/07_AVnu-Ethernet_AVB-TSN_Common_Services.pdf>. Read 6.1.2016

46 AVB and Dante. 2015. WWW document. Tim Shuttleworth. <https://www.linkedin.com/pulse/nominees-avb-dante-winner-tim-shuttleworth>. Read 25.1.2016

47 Standard 802.1BA. 2011. WWW document. IEEE. <http://www.ieee802.org/1/pages/802.1ba.html>. Read 23.2.2016

48 Standard 802.1AS. 2011. WWW document. IEEE. <http://www.ieee802.org/1/pages/802.1as.html>. Read 23.2.2016

49 Standard 802.1Qav. 2009. WWW document. IEEE. <http://www.ieee802.org/1/pages/802.1av.html>. Read 23.2.2016

50 Standard 802.1Qat. 2010. WWW document. IEEE. <http://www.ieee802.org/1/pages/802.1at.html>. Read 23.2.2016

51 Audio Video Bridging. 2014. WWW document. Electronic Design. <http://electronicdesign.com/communications/understanding-audio-video-bridging>. Read 19.11.2015

52 Ravenna. WWW document. ALC NetworX. <http://ravenna.alcnetworx.com/technology/about-ravenna.html>. Read 10.11.2015

53 Energy efficient switches and Dante. 2014. PDF document. Audinate. <https://www.audinate.com/sites/default/files/PDF/dante-network-blacklisted-eee-switches-audinate.pdf>. Read 20.11.2015

54 Dante Controller. WWW document. Audinate. <https://www.audinate.com/products/software/dante-controller>. Read 20.11.2015

55 Dante Controller interface. 2015. WWW document. Delec. <http://www.delec.de/delec/index.php/en/products/unito.html>. Read 2.12.2015

56 Dante Redundancy. WWW document. Audinate. <https://www.audinate.com/resources/videos/gs8-dante-redundancy-getting-started-dante-video-series>. Read 3.12.2016

57 Audio device features. WWW document. Yamaha. <http://www.yamahaproaudio.com/global/en/products/mixers/ql/features.jsp>. Read 10.12.2016

58 Redundant Dante network. 2014. PDF document. Symetrix. <http://www.symetrix.co/wp-content/uploads/2014/10/2014-11-Dante-Redundancy.pdf>. Read on 1.3.2016

59 Dante redundancy. 2014. WWW document. ChurchTechArts. <http://churchtecharts.org/home/2014/10/5/setting-up-a-redundant-dante-network>. Read 3.12.2015

60 Hearing difficulties. PDF document. Hearcom. <http://hearcom.eu/about/DisseminationandExploitation/deliverables/HearCom_D09-11_v2.0.pdf>. Read 29.12.2015

61 More understandable announcements. 2013. WWW document. University of Edinburgh. <http://www.ed.ac.uk/news/2013/speech-090913>. Read 2.1.2016

62 OpenAccess Alerts application. 2016. WWW document. Conexu Foundation. <https://play.google.com/store/apps/details?id=au.com.conexu.silenttweets#details-reviews>. Read 2.1.2016

63 IP Speaker Manufacturers. WWW document. Singlewire. <https://www.singlewire.com/s_endpoints.html>. Read 14.2.2016

64 InformaCast. WWW document. Singlewire. <https://www.singlewire.com/informacast.html>. Read 14.2.2016

65 SA-Announce. WWW document. Syn-Apps. <https://www.syn-apps.com/products/sa-announce>. Read 14.2.2016

66 Emergency Communications Systems. WWW document. Honeywell. <https://www.notifier.com/solutions/bysolution/Pages/emergency-communications-systems.aspx>. Read 27.2.2016

67 Public Address System. WWW document. Zenitel. <https://www.zenitel.com/product?search&system=25>. Read 3.3.2016

68 Paging over IP systems. WWW document. Kintronics. <https://kintronics.com/solutions/paging-over-ip-systems/>. Read 10.1.2016

69 IP based intercoms. WWW document. Barix. <http://wiki.barix.com/index.php5?title=IP_based_Intercom_technology>. Read 9.12.2015

70 Audio over IP. 2008. PDF document. Barix. <http://acutron.net/acutron/pt/barix/broadcast.pdf>. Read 9.12.2015

71 InformaCast Desktop Notifier. WWW document. Singlewire. <https://www.singlewire.com/informacast-desktop-notifier.html>. Read 14.2.2016

72 Analogue vs. digital PA systems. 2011. WWW document. Kintronics. <http://www.imakenews.com/kin2/e_article002292581.cfm?x=b3bFMPj,0,w>. Read 6.8.2015

73 Best practices for video conferencing deployment. 2014. WWW document. Pexip. <https://www.pexip.com/article/whitepaper/best-practices-prevent-your-videoconferencing-deployment-being-compromised>. Read 10.10.2015

74 Best Security practices for United Communications. 2015. PDF document. Polycom.<http://www.polycom.com/content/dam/polycom/common/documents/whitepapers/polycom-uc-security-best-practices-wp-enus.pdf> Read 4.11.2015

75 Cloud based video conferencing. WWW document. IVCi. <http://www.ivci.com/archive/cloud-based-video-conferencing-services-transforming-world-corporate-communication/.>. Read 6.8.2015

76 Analyzing Polycom video conference traffic. 2013. WWW document. SANS Institute. <https://www.sans.org/reading-room/whitepapers/protocols/analyzing-polycom-video-conference-traffic-34167>. Read 13.9.2015

77 Supported switches for AVB. WWW document. AVNU. <http://avnu.org/certified-products/>. Read 13.1.2016

78 Speaker Power and Distance. WWW document. Pui Audio. <https://www.digikey.com/Web%20Export/Supplier%20Content/PUI_668/PDF/PUI_speaker_power_distance.pdf?redirected=1>. Read 15.12.2015

79 Dante support for subnets. 2015. Email. Dante Support. Read 25.1.2015