Unified Communications with Lync 2013

ALEXANDRE KOHEN

KTH Information and
Communication Technology

Degree project in
Communication Systems
Second level, 30.0 HEC
Stockholm, Sweden

Unified Communications with Lync 2013

Alexandre Kohen

Master of Science Thesis

Communication Systems
School of Information and Communication Technology
KTH Royal Institute of Technology
Stockholm, Sweden

1 October 2013

Examiner: Prof. G. Q. Maguire Jr.

Abstract

Unified Communications solutions bring together several communication modes, technologies, and applications in order to answer businesses' and individuals' growing need for simpler, faster, and more effective communications means. Although many hardware-based products allow the integration of telephony within a computer network environment, telephony features of software-based unified communications solutions are seldom used, which limits their effectiveness or requires another solution to be used jointly.

This master's thesis project aims to demonstrate that unified communications solutions based on Microsoft Lync Server 2013 can effectively address a wide variety of business scenarios, including a traditional telephony system replacement.

The first part of this master's thesis introduces background knowledge about unified communications and associated technologies, as well as the different components of the selected unified communication solution.

The case study presented in this thesis is the first large-scale Lync 2013 deployment with a complete telephony offering in France. The presentation follows the complete deployment process, starting from the analysis of the client's needs to the solution design, construction, and validation.

This project demonstrated the suitability of Lync 2013 as a telephony system replacement. However, the transition from a classic telephony solution to a unified communications solution can be a technical challenge. An essential step in making this transition successful was to take the users' needs into account. It was also essential to accompany these users throughout the transition.

Sammanfattning

Samordnad kommunikation (engelska: unified communications) lösningar sammanföra flera kommunikationssätt, teknik och tillämpningar för att besvara företags och individers växande behovet av enklare, snabbare och mer effektivt kommunikationsmedel. Även många hårdvara-baserade produkter tillåter integration av telefoni inom ett datornätverk miljö, telefoni funktioner mjukvarubaserad Samordnad kommunikation-lösningar används sällan, vilket begränsar deras effektivitet eller kräver en annan lösning för att användas gemensamt. Detta examensarbete syftar till att visa att samordnad kommunikation lösningar baserade på Microsoft Lync Server 2013 kan effektivt ta itu med en mängd olika scenarier. Den första delen av detta examensarbete introducerar bakgrundskunskap om samordnad kommunikation och tillhörande teknologier liksom de olika komponenterna i den valda samordnad kommunikation lösning.

Fallstudien som presenteras i denna avhandling är den första storskaliga Lync 2013 utplacering med en komplett telefoni erbjuder i Frankrike. Den presentationen följer hela implementeringsprocessen, från analys av kundens kraven till utformning, konstruktion, och validering. Detta projekt visade tillförlitligheten i Lync 2013 som telefoni ersättning men intyga att även övergången från en klassisk telefoni lösning på ett samordnad kommunikation-lösning kan vara en teknisk utmaning, ta användarnas behov i beaktande och medföljande användare genom övergången är kritisk.

Résumé

Les solutions de communications unifiées rassemblent différents modes de communications, technologies, et applications pour répondre aux besoin croissant des entreprises et individus de méthodes de communications plus simples, rapides et efficaces. Bien que de nombreuses solutions matérielles permettent l'intégration de la téléphonie à un réseau informatique, les fonctions de téléphonie des solutions logicielles sont rarement utilisées, ce qui limite leur efficacité ou nécessite l'utilisation conjointe d'autres solutions.

Ce projet a pour but de démontrer l'efficacité des solutions de communications unifiées basées sur Microsoft Lync 2013 à répondre à une grande variété de besoins professionels, dont le remplacement d'un système de téléphonie traditionnel.

La première partie de ce mémoire introduit les notions nécessaires sur les communications unifiées et les technologies associées, ainsi que les différents composants de la solution de communications unifiées choisie.

L'étude de cas présentée décrit le premier déploiement majeur de Lync Server 2013 comportant une offre de téléphonie complète en France, et suit le processus de déploiement complet, de l'analyse des besoins client à la validation du projet, en passant par la conception, la construction et le test.

Ce projet démontre l'aptitude de Lync en temps que système de téléphonie complet. Cependant la transition d'un système traditionnel à une solution de communications unifiées peut présenter des défis techniques, et il est essentiel de prendre en compte les besoins utilisateurs ainsi que de les accompagner durant la transition.

Acknowledgements

First of all, I would like to thank Patrick Nathan, Carine Leschiera-Lombard and Michael Huguenin for granting me the opportunity to collaborate on this project.

I want to thank the whole Microsoft Consulting Services UC team for welcoming me and the time they dedicated to helping me and answering my questions.

I am particularly grateful to Gil, Roland, Quang, Stefan, Thomas, and Sylvain for their valuable contributions to this project.

I also want to thank all the Microsoftees I have had the pleasure of meeting for the great time we shared.

Finally I would like to thank Professor Gerald Q. Maguire Jr. for accepting to supervise this project and his valuable input in the redaction of this report.

Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

AD	Active Directory
CA	certification authorities
OS	operating system
PBX	private branch exchange
PSTN	public switched telephone network
QoS	Quality of Service
RBAC	role-based access control
SPIT	Spam over Internet Telephony
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UM	unified messaging
VoIP	voice over IP
WAN	wide area network
WLAN	wireless local area network

Chapter 1

Introduction

The evolution of technology and business needs allowed previously existing means of communications to converge into unified communications (UC) solutions, which allow companies to be more efficient and productive. UC solutions were originally designed by telephony or routing equipment manufacturers, while consumers used hardware-based telephony features in UC solutions; therefore, the telephony features of software-based UC solutions are rarely used, for example only 11% of Microsoft Lync deployment is used for telephony[1].

The release of Microsoft Lync 2013 was aimed mostly at improving upon the Microsoft Lync Server 2010 features in order to deliver a more robust telephony solution. At the time of the start of this thesis project there were few large scale Lync 2013 telephony enabled deployments.

Therefore, the goal of this thesis project was to demonstrate Lync 2013 telephony features in an actual, large scale deployment. This particular deployment was challenging, as it was the first large scale Lync 2013 complete telephony replacement in France, the project had a tight schedule, and many features depended on other vendors' solutions. This last aspect was particularly unusual for a project conducted through Microsoft Consulting Services.

1.1 Thesis outline

This report is divided into 5 chapters. Chapter 2 presents unified communications, along with relevant protocols and concepts. This chapter should help people new to unified communications or computer networks understand the context of unified communications and the challenges of this project. Chapter 3 describes the different components of the specific Microsoft unified communications solution that was used for this project. This chapter is recommended for readers unfamiliar

with Microsoft server solutions. Chapter 4 documents the deployment design, construction, and test process. The final chapter summarizes the conclusions, suggests future work, and gives some reflections on the social, ethical, and economic aspects of this thesis project.

Chapter 2

Background

This chapter presents the background required for a good understanding of this thesis.

Readers unacquainted with the concepts of unified communications and cloud computing are advised to read the first and second sections, in which these concepts are briefly introduced and contextualized.

Sections 2.3, 2.4, and 2.5 should be relevant for all readers as they present some existing software solutions, the underlying technologies and protocols, as well as the legal background which any solution has to be consistent with.

2.1 Unified Communications

Unified communications solutions can be described as the integration and management of various communications services, both real-time and asynchronous, such as instant messaging, telephony, SMS, presence information, video conferencing, or email; just to name a few. This integrated set of services should be accessible from a variety of devices, with the objective of increasing productivity and ease of use.

Unified communications is not a single technology nor a single software solution, but encompasses all solutions providing suitable functionality, while providing a simplified and unified user experience [2, 3, 4].

2.1.1 History

Unified communications exploits the convergence of information technology and telecommunications as components to create a solution, which requires that these components must inter-operate seamlessly [3]. In order to understand the process

leading to the appearance of unified communications in their current form, we must consider the evolution of telecommunications, IT, and business expectations.

2.1.1.1 Business expectations

Over the last few years, business needs have evolved. Companies now need to operate over wide geographical areas, thus business tools for mobile employees routinely include laptops, mobile phones, and tablets. Similarly when employees are at fixed locations, they increasingly have personal computers and other devices connect to local area networks or wireless local area networks (WLANs).

Business requirements have driven a continuously increasing need for mobility and real-time access to information, to enable employees to remain productive while on the move, to allow teams to remain functional even while their members are at different physical sites, and to provide employees with permanent access to up-to-date information in order to make better decisions[5].

2.1.1.2 Unified Messaging

The combination of the existing email and voice mail into an unified interface was achieved during the 1990s by various partnerships between software and telecommunications companies. The goal of unified messaging (UM) was to provide a single access point for the various asynchronous communications services, such as fax, email, and voice mail[4]. These solutions include "Telephony One Stop" created by Lotus and AT&T in 1995 or "Octel Unified Messaging" created by Microsoft and Octel in 1997[6].

These solutions gradually improved over time with the addition of new functions, such as instant messaging, presence signaling, advanced message management, and cross-media messaging. These functions now form the core of modern unified communications solutions.

2.1.1.3 Integration with business telephony systems

The advances in computing power and device capabilities allowed private branch exchange (PBX) manufacturers to integrate UM solutions and new features into their telephony equipment in order to meet business expectations[6]. These features often included advanced voice mail and call forwarding management, "find me/follow me" features allowing users to reached, desktop notification of incoming calls, and voice management[4].

2.1.1.4 Voice over Internet Protocol

With the constant increase in network capacity, it became very attractive to use a portion of this capacity to carry voice communications, due to its potential to reduce costs by taking advantage of the simplified voice over IP (VoIP) architecture. Although packet speech was first demonstrated in 1974 on the ARPANET[7], the first widespread consumer VoIP application was InternetPhone, developed in 1995 by Vocaltech, Inc. which allowed its users to use their computers, microphones, and speakers to communicate with each other over the Internet[8].

VoIP became widespread in the following years, and is now very popular for both the consumer market, with solutions such as Skype, and the professional market, with solutions such as Microsoft Lync, Google Voice, and Asterisk. Lync will be further studied in this thesis project.

2.1.1.5 Unified Communications

The current state of unified communications solutions is due to the convergence of the increased needs of the companies; the core functionality provided by the existing UM solutions; and the enhanced communications solutions first introduced within PBX systems, but for which pure software counterparts now exist.

These communications systems are complemented by business productivity solutions (word processing, spreadsheets, presentation software, etc.), which were developed to fulfill the needs of various professionals.

The combination of unified communications and business solutions have attracted a lot of attention from companies, and have now established themselves as an essential tool for medium to large-sized business. The adoption of these solutions is seen in the exploding market for unified communications solutions[9]. Additionally, Asterisk and other solutions have been expanding these types of services into small offices and even homes.

2.1.2 Components

As noted earlier, unified communications solutions are not defined by a single piece of software, hence they are always composed of different components which interacting together to provide the desired end user experience. This section lists the main categories of these components. However, not all of these components are included in every solution, nor are all of them available in every device. The actual set of components depends upon the specific implementation and the

specific requirements that an implementation is targeting. Some solutions may also include additional components that do not fit into these categories[10].

2.1.2.1 Call control

Call control components allow the user to have unified control over their telephony communications. For example, information about incoming calls may be displayed on the user's current display (a computer screen for example) and the user can accept or reject calls via their computers. Users can also initiate a call from their computer, but utilize their cellular or desktop phone to participate in the actual call.

2.1.2.2 Multimodal communication

Multimodal communication allows users to reach others via an unified system, while using various means to do so. For example, users can add a new user to their contacts list by name, e-mail address, IM account, etc. then send this user an instant message, before establishing a voice communication session. Subsequently the participants in this session might start a shared screen activity.

2.1.2.3 Voice over IP

Often wrongly confused with unified communications, VoIP can play a crucial role in many unified communications solutions. The term VoIP is used to designate a form of communication which allows voice (and other multimedia) communication sessions to be carried over a computer network instead of using a telephone network.

VoIP services can be interconnected with the public switched telephone network (PSTN), thus allow communications between people connected to a computer network using hardware or software VoIP clients, and people using the telephony network using cellphones or fixed digital /analog phones[11].

2.1.2.4 Presence

Presence information is mainly used to access the availability of users for participation in a communication session. For example, the most common and simple presence application is a contacts list (often called a "buddy list") indicating whether contacts are online, offline, or unavailable for communication. In unified communications systems, presence is often at the center of the solution, hence the systems offers a variety of information, such as availability, localization, skills, or currently supported means of communication for a session[12][13].

2.1.2.5 Mobility

Mobility refers to the ability to maintain a session in spite of any changes in location (terminal mobility), role change (personal mobility), or changes in which devices are used (service mobility)[14].

2.1.2.6 Instant Messaging

The ability to communicate in real-time using text messages can be a very simple, yet powerful way to communicate quickly and effectively. Therefore real time text messaging (often called "instant communication") is a critical component of all unified communications solutions. Although most users are already familiar with consumer instant messaging solutions, enterprise systems have higher security and privacy requirements, so dedicated solutions must be used[4].

2.1.2.7 Unified Messaging

Unified messaging (UM) components are designed to provide users with a single interface for various communications systems, such as email, SMS/MMS, voice mail, and instant messaging[15].

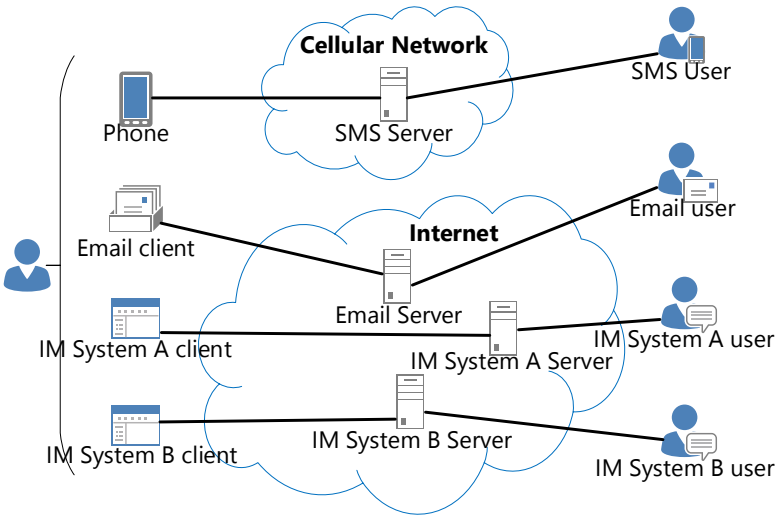

Figure 2.1: Typical communications system

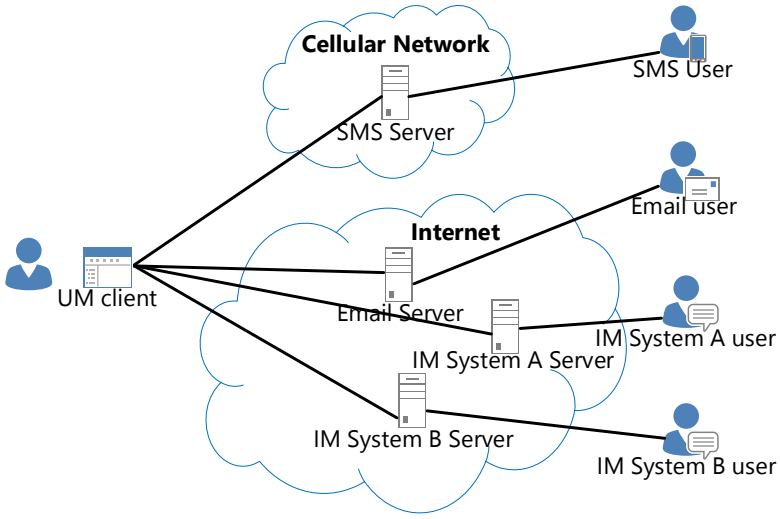

Figure 2.2: Typical communications system

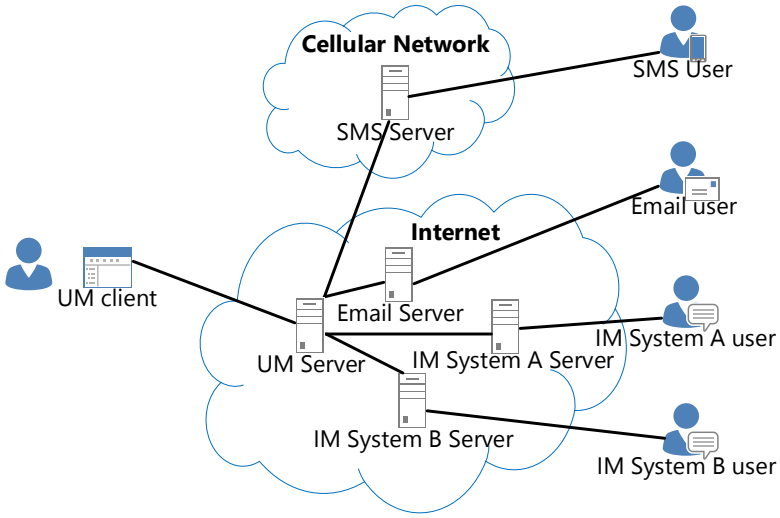

Figure 2.3: Server-based UM

2.1.2.8 Speech access and personal assistant

Personal assistants allow users to access enhanced functionality from low level devices, such as basic phones. Examples of this functionality include using a

speech recognition and synthesis based interface to manage a calendar, meetings, or out of office status[4].

2.1.2.9 Collaboration tools

Collaboration tools enable enhanced communications between many users, such as audio and video conferencing, screen sharing, whiteboarding, and document sharing tools[3].

2.1.2.10 Business process integration

Integration with business processes and workflow applications is a key to reducing "human latency" , thus increasing efficiency. Unified communications solutions integrated with a business process can, for example, reduce the delay between tasks by facilitating the notification of available and relevant personnel in the case of workflow problems[4].

2.1.3 Devices

To ensure that users can have sufficient mobility while retaining access to the communication system, unified communications solutions must be able to support a very wide range of devices, in many different situations. These devices include:

Computers Desktops and laptops have become one of the main access points to modern communications systems, due to their ability to provide the user with a rich experience. Computers are usually able to access all the functions of the unified communications solution. They can also simulate other devices functions, for example, software used to duplicate a hardware phone's functionality is called a "softphone".

Cellphones Cellphones (or cellular phones) are essential access points for unified communications systems, as almost all business users always carry a cellphone with them, which makes the user reachable as long as they are within a compatible network's coverage area. Today these cellular telephony systems enable users to be always potentially reachable, and these systems can provide various functionality, depending on the phone's features.

Today smartphones with internet access can be used for almost all services.

Tablets and netbooks Tablets and netbooks can be considered either as computers or smartphones, depending on their features. They usually provide the same functionality as computers if they have the appropriate hardware, and they can also be used as a smartphone if they have GSM, 3G, LTE, wireless local area network (WLAN), or similar access.

Phones Although not as mobile as cellular phones, or able to provide the same rich experience as a computer, other types of phones are also very common in unified communications architectures for different reasons. Users are used to using a landline phone, and may prefer to use a phone handset to make calls rather than a computer headset. Some users may also not have a computer at their working location.

While limited, these phones can still provide some advanced features, beside voice calls, due to speech assistants (for example).

Moreover, there are also IP phones, connecting directly to the local area network that can provide advanced features.[11]

Web clients Web clients can allow users to access communications services from any device able to run a compatible browser, without installing software on the device, which enables the use of public computers while on the go. For some examples of softphone functionality provided this way see [16].

Other devices There are also other dedicated devices used in UC solutions, for example, dedicated conferencing devices allow users to hold a meeting in a conference room while streaming the video and audio from the room to remote users participating in the meeting.

2.1.4 Vendors

There are many different UC solutions currently on the market, most of them offering the same core features, but sometimes with very different design philosophies and technical choices. This section describes the Avaya, Cisco, and Microsoft offerings, as they are current leaders in UC solutions.

Avaya is a business collaboration and communications solutions provider and comes from a strong telephony background, as it was originally part of Lucent Technologies and AT&T and has 12% of the world PBX market[1]. Avaya is one of the leading unified communications vendors, with telephony-based products, such as the Avaya Aura, or their IP Deskphones families[17].

Cisco is the leading provider of routers, switches, WLAN, and telepresence equipment, and is a leading UC provider with its Unified Communications Manager[1, 18].

Microsoft is originally a software company, and provides software-based UC solutions. Unlike Avaya and Cisco, Microsoft does not manufacture phones or other telephony devices and instead certifies other vendors' devices for use with Lync, such as Aastra's IP Phones or Polycom's meeting rooms devices [19].

2.1.5 Conclusions

UC can be very interesting for organizations, as it can help reduce communications costs by replacing some (or all) of the PSTN traffic by VoIP traffic over a data network, which is typically a lot cheaper - especially for long distance calls. It can also help companies increase efficiency by enabling employee mobility, and facilitating communications, both within the company, and with partners or clients. UC solutions also reduce the time required to find or contact people relevant to each situation, and can help optimize business processes, which can make employees' lives easier, while enabling the employee to be more efficient and productive. SIP-based communications can also provide increased security against interception due to traffic encryption[20] which makes UC all the more attractive to businesses.

Due to its added value, UC is becoming an essential business requirement and the market for UC solutions is currently rapidly expanding. However, UC poses new challenges, as the transfer of communications from the PSTN to a computer network leads to new issues, such as the need for continuous, high bandwidth, low latency Internet connectivity and the need to supply the electrical power needed by and consumed by the required equipment. A thesis that address this power consumption is [21].

Moreover, unified communications solutions also raise new security, confidentiality, and compliance issues, such as the need for users without PSTN access to be able to contact emergency services, and the risk of Spam over Internet Telephony (SPIT) that can be induced by VoIP communications[11].

2.2 Protocols

Although there is no standard UC protocol, some basic protocols are used in almost all UC solutions.

2.2.1 Internet Protocol (IP)

Function

The Internet Protocol is the main communication protocol used in computer networks and is responsible for routing data packets between hosts. Each packet has two sections, the header which contains information about the packet (such as the source address, destination address, and type), and the payload (which is the actual data to be delivered to the destination)[22].

IP Address

The IP Address is used when forwarding IP packets to their destination. In most cases, an IP address identifies a single computer's interface on a network. There are currently two active versions of the Internet Protocol, IPv4 with 32 bit addresses, such as 172.16.254.1[22], and IPv6 with 128 bit addresses, such as 2001:db8:85a3:0:0:8a2e:370:7334. IPv6 was created to remedy to the current shortage of IPv4 addresses[23].

Each subnet is allocated with a range of IP addresses which can be allocated to devices within this subnet. To indicate a subnet address, the notation $address/mask$ is used, where *mask* is the number of leading bits in the subnet address. For example, the IPv4 block 172.16.254.0/24 represents the addresses from 172.16.254.0 to 172.16.254.255.

Usage

Unlike in circuit-switched networks, IP networks are packet-switched and use dynamic routing: each node along a path makes a local routing decision for each packet. Most of the routing in IP networks is done by dedicated equipments, called routers, which forward incoming packets according to a routing table.

The design of IP networks has several consequences:

- There is no delivery guarantee or error correction. Endpoints must check the message integrity.
- A message can be several packets long and not all of these packets have to take to same path to reach the destination.
- In case of link or node failure occurring only between two packets, the message can still be transmitted.

2.2.2 Domain Name System (DNS)

The major use of the Domain Name System (DNS) is to translate an domain name to an IP address. This IP address can then be used to contact the desired host. While DNS resolution uses IP packets, the process of IP routing and DNS resolution are completely unrelated.

DNS is a hierarchical and distributed system, with each sub-domain belonging to a higher level domain recursively up to a root level. Each DNS server can delegate authority over a sub-domain to another DNS server. A zone is the set of domains and sub-domains over which a name server has authority.

In a domain name, labels are separated by dots and ordered by hierarchy, with the top-level domain being on the right, and the lowest level domain on the left (just after the host's name within this lowest level domain). A Fully Qualified Domain Name (FQDN) is a domain name that includes its full hierarchy, up to the root domain.

When resolving a DNS address to an IP address, clients will usually contact a recursive DNS resolver. This resolver will perform queries as necessary to each level's authoritative server, in order to resolve the name into an IP address.

DNS resolvers usually exploit caching to save previous and intermediate queries' results, which can avoid the need for a complete DNS look-up for each request. Details of the performance of today's DNS system can be found in [24].

2.2.3 Transport Layer Security

The Transport Layer Security (TLS) protocol provides security for transport layers such as TCP. TLS is commonly used to provide security to HTTP[25, 26]. TLS is a successor of the Secure Sockets Layer (SSL) protocol.

TLS uses client and server certificates (asymmetric keys) to generate a common session key which is used to encrypt the data between the client and the server.

STARTTLS is a protocol extension that allows upgrading a plain text connection to an TLS encrypted connection on the same port instead of using a dedicated port for encrypted connections.

2.2.4 Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services. This is a standard protocol that allows

multiple applications to access an LDAP-compliant server to retrieve information such as contacts, but also certificates, printers, services, or any other information that can be stored in a directory [27].

2.2.5 Kerberos

Kerberos is a protocol allowing authentication of users on a network using asymmetric cryptography and the use of tickets. The PKINIT extension for Kerberos adds the use of a smartcard or USB authenticator to the authentication, and is often used in Microsoft Windows environments to provide strong authentication[28, 29].

2.2.6 Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) has been developed and standardized by the Internet Engineering Task Force (IETF) and is used to control real-time multimedia communication sessions over IP networks. This protocol is widely used in VoIP to create, modify or terminate sessions[30].

The H.323 recommendation by the ITU-T also defines the H.225.0 and H.245 protocols, which are also used in some VoIP solutions[31].

2.2.7 Extensible Messaging and Presence Protocol (XMPP)

The Extensible Messaging and Presence Protocol (XMPP) allows the exchange of messages based on XML over IP networks. XMPP is used in many applications, such as Jabber or Google Talk, for instant messaging, presence information, or contact list[32].

2.3 Other useful concepts

The following concepts are not specific to UC solutions, but play a significant role in realizing a modern UC system.

2.3.1 Virtualization

Virtualization refers to the set of techniques used to separate a process from its physical operating environment. There are multiple reasons for virtualization

depending on the type of virtualization, such as hardware efficiency, application availability, or faster development cycles [33].

The most common type of virtualization is operating system virtualization, which allows a host machine to execute several virtual machines. There are multiple advantages to this type of virtualization over physical computers:

- A single computer can host multiple low usage virtual machines, so there is less computing power wasted when one virtual machine is not used;
- More flexibility, as the virtual machine resource usage can be modified in real time;
- Faster deployment;
- Simpler migration or failover; and
- Allows the creation of secure or test environments separated from the host computer environment.

Moreover, virtualization is a necessary component for most cloud computing offerings.

2.3.2 Cloud Computing

Cloud computing is a term describing a variety of computing concepts related to distributed computing and the transfer of part of the computing infrastructure responsibilities to a service provider. Due to the ubiquitous nature of UC solutions, cloud computing is an important component of many UC offerings.

Cloud computing is usually divided into different categories, depending on how responsibilities are separated[34]:

Software as a Service (SaaS) In this service model, a service provider assumes complete responsibility over an application and grants usage rights to clients usually for a monthly or yearly fee. This can cause greatly reduced IT costs for the clients by removing the need for maintaining hardware or software, and simplifies scalability. Microsoft Office 365 or Google Apps are examples of SaaS.

Platform as a Service (PaaS) In this model, the provider offers a computing platform on which the client can run its applications. This allows the client to focus on its applications. Web hosting is an example of PaaS.

Infrastructure as a Service (IaaS) In a IaaS model, the providers offers access to computers. Usually this model relies heavily on virtual machines to provide the required service levels (better availability, scaling, and backup). Unlike in PaaS, the client has full access to the operating system and can use the computers for any use. IaaS offers the client more control, better scalability, and security with a lower upfront investment. Microsoft Windows Azure and Amazon Elastic Compute Cloud (EC2) are examples of IaaS providers.

2.3.3 Quality of Service (QoS)

Quality of Service (QoS) refers to the quality of service which the end user perceives (or an application receives). QoS can also refer to the set of techniques used to enable traffic to cross the network while satisfying certain quality parameters. The relevant quality parameters to guarantee to ensure a good service differ depending on the type of traffic considered, but the most common parameters are: bandwidth, latency, packet loss, and jitter.

The goal of guaranteeing QoS is that users of an application transmitting packets over the network will experience good service. Best-effort handling of packets, which is the default operating mode of the network, simply forwards packets in their order of arrival without offering any QoS guarantees. This delivery method is sufficient when the traffic is low compared to the network capacity and when the service level requirements are low. However, with higher service requirements or insufficient network capacity, this approach leads to degraded service during peaks in the network traffic.

A simple approach would be to over provision resources, so that the network capacity is always greater than the requested usage. However, this would lead to a costly network with most on the resources left unused, except during what many only be brief usage peaks.

PSTN calls use circuit switching to guarantee the service level during a call; hence when a call is to be initiated, resources are allocated for the call, and cannot be used by any other calls until this call has terminated, which guarantees a constant service level. If there are not enough resources available, then the call cannot be established.

The postal service is also a best-effort type network, as letters are transmitted as they are received by the postal service, with additional delays if there is a sudden burst of letters sent. However, there are different rates for different types of letters, with higher rates guaranteeing faster delivery.

IP Networks

There are two main protocols to support Quality of Service in IP Networks, Differentiated Services (DiffServ)[35] and Integrated Services (IntServ)[36].

2.3.4 Public Key Cryptography

A public key algorithm relies on the use of asymmetric keys to encrypt and decrypt messages. Unlike in conventional (or symmetric) cryptography, the keys used to encrypt and decrypt the message are different. This allows the secure exchange of messages, with a decreased risk that the common secret used to encrypt the message is intercepted, and to generate cryptographic signatures. A Public Key Infrastructure (PKI) refers to a set of physical or logical components used to create, store, distribute and verify digital certificates[37].

2.3.5 Erlang

The Erlang is a unit used to telephony to measure the load of telephony circuits. For example, one Erlang can represent that a single resource (such as a telephony circuit, or a server) is used at 100%, or that two resources are used at 50%. Moreover, an user with a phone usage of 0.05 Erlang spends 5% of his time on the phone.

The Erlang-B formula is used to determine the number of circuits required to achieve a determined grade of service, which is the fraction of calls blocked due to all circuits being used.

The Erlang-B formula is defined as:

$$P_b = \frac{\frac{E^m}{m!}}{\sum_{i=0}^{m} \frac{E^i}{i!}}$$

where P_b is the grade of service, E is the load in Erlangs, and m is the number of circuits [38].

2.4 Legal

In France, there are many laws and rules applicable to UC, but no specific legislation and very little case-law. Therefore the resulting legal background for UC is complex, but cannot be ignored as it can affect UC solution deployment and operations.

2.4.1 Privacy

There can be privacy concerns over the content of the communications held through a UC solution. In France, there is no specific law, but different general laws apply, such as the law on the privacy of letters, and on telecommunications exchanges. According to these laws, it's illegal for someone who is not a recipient of a message to prevent or delay its delivery, tamper, read, or diffuse its content[39, 40, 41]. However this applies only to communications identified as personal[42]. Professional communications have different legislation, depending on the company.

2.4.2 Archiving and compliance

UC solutions must also take archiving and compliance with regulation into account. For example, some documents, such as contracts or commercial correspondence must be kept for up to 10 years[43, 44], international companies may have to respect regulation such as the Sarbanes-Oxley[45] or local law[46], which imposes a higher degree of security, and specific scope, duration, and format for archiving.

2.4.3 Safety

Telephony solutions must implement regional standards, such as E911, to allow access to emergency services[47].

2.4.4 Other

Other legislation might have unexpected impact on UC solutions. For example, regulation on the usage of the electromagnetic frequencies limits the strength of signals using the 2.4GHz and 5GHz frequencies, which are used for WiFI. Moreover, the frequencies between 5.25GHz and 5.725GHz are also used for military and meteo radars, which have priority over WiFi emissions[48].

2.5 Related Work

Although there is little available documentation on Lync 2013, a lot of work has already been done on Lync 2010 and other UC solutions.

2.5.1 Lync deployment

There are multiple sources of documentation for planning and deploying Microsoft Lync 2010, such as Microsoft IT's Deploying Lync Server 2010 whitepaper[49], and Microsoft TechNet[50].

2.5.2 Disaster Recovery and Business Continuity Planning in Action: Japan 2011

This article, published by Microsoft IT in July 2011, follows the March 2011 earthquake in Japan and its impact on the Lync 2010 infrastructure, as well as the disaster recovery processes used and the lessons learned[51].

Chapter 3

Microsoft Unified Communication Solution

This chapter presents the Microsoft unified communications solution that is the focus of this master's thesis project. This solution is made up of different closely interconnected software solutions, and each section will present a separate piece of this software. The sections are ordered by integration order, with each piece of software using functions from the previous ones. The complete chapter is essential reading to achieve a good understanding of this master's thesis. The sections on Lync 2013 and Active Directory are particularly relevant.

3.1 Windows Server

Microsoft Windows Server is the operating system (OS) for servers running in a Microsoft Windows environment, hence every server-side software solution used in this project is running on top of Microsoft Windows Server. Relevant details of this OS will be given below.

3.1.1 OS for servers

The OS's task is to manage the computer's resources and to provide resources and services to applications.

The latest version of Microsoft Windows Server is currently Windows Server 2012. For this thesis project, only Windows Server 2008 R2 (Datacenter edition) and Windows Server 2012 (Standard or Datacenter editions) were used.

3.1.2 Features

Windows Server 2008 R2 and Windows Server 2012 are respectively the server version of Windows 7 and Windows 8, therefore they share many of their features with their client counterpart. However, as a server version of the OS, they have some additional features, with the biggest difference being their focus on high availability, scalability, higher security, and ease of administration. Some of the most relevant features of these OSs for this project are:

Virtualization

The integrated virtualization functions of Windows Server 2008 R2 and 2012 allow simple configuration and administration of virtual machines (VMs). This facilitates the creation of lab environments to prototype and test a complete architecture on a single machine or the administration of a production environment where many lightly loaded VMs are run on the same physical server. The integrated VM manager in Windows Server 2008 R2 and 2012 is called Hyper-V.

Active Directory

Windows Server has native support for Active Directory. A given server can be assigned any Active Directory role without requiring any additional software installation. Further details of active directory can be found in section 3.2.

High Availability

Some of the features of Windows Server 2008 R2 and 2012 help to achieve the high availability requirements of UC applications. Among these features are functions to allow administrators to create failover clusters (which allows unreachable servers to be automatically replaced), to use a virtual storage pool to ensure high data availability, and new virtualization tools for quick VM backups or restores without stopping running services.

PowerShell

Windows PowerShell 3.0 is integrated with Windows Server 2012 and Windows Server 2008 R2 SP1. PowerShell provides a task automation framework. PowerShell consists of a command-line shell interface and an associated scripting language that allows administrative tasks to be performed on local or remote systems, using ”cmdlets” which are specialized .Net classes. Unlike UNIX’s

shell scripting languages, interactions in PowerShell are object-based, so each command returns a .Net object that can be used by subsequent commands. This allows a programmer to quickly create powerful scripts for task automation.

3.1.3 Administration tools

There are multiple tools available to administer a Windows server. The most common ones are listed here.

Server Manager

The Server Manager is a graphical interface run from the server's desktop. It allows administrators to easily monitor and manage servers in a domain. It provides simple tools for monitoring events and server performance, and managing roles for a whole server group without the need to connect directly to each server.

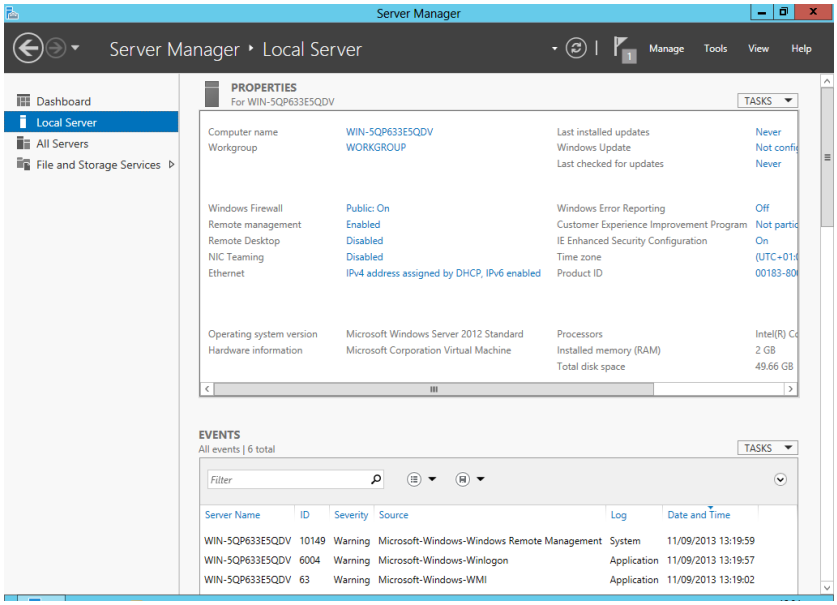

Figure 3.1: Windows Server 2012 Server Manager

Remote Desktop Connection

A Windows Server can also be managed remotely, via a remote Desktop Connection, which allows the administrator to remotely access a server's Desktop

interface.

Microsoft Management Console

The Microsoft Management Console can be used as a graphical interface for configuring and monitoring servers. The console can be customized with various snap-ins, with each snap-in providing some specific functionality.

PowerShell

The PowerShell interface can be used to manage servers without using a graphical interface.

3.2 Active Directory

Active Directory (AD) is the central repository for identities in a Microsoft environment.

3.2.1 Directory Services

AD is Microsoft's LDAP compliant directory service. AD's main function is to provide a central source for identification and authentication for computers running one of Microsoft's OSs when this computer is connected to a network. AD is able to maintain a list resources for a managed network, such as user accounts, computers, printers, shared folders, apply security or administrative policies, distribute software upgrades, and allow controlled access to network resources.

AD plays a central role in almost all of Microsoft software solutions, as it provides a lot of the basic functionality required by other software[52].

3.2.2 Roles

An AD architecture is composed of multiple roles, each role providing a separate functionality. A single server can have one or many roles, and each role can be assigned to multiple servers. Only the AD Domain Services role is required to be assigned to at least one computer in any given AD architecture, all of the other roles are optional.[53, p. 5-7]

3.2.2.1 Active Directory Domain Services (AD DS)

The central role of any AD architecture is to provide a central repository for identity management, as well as the identification and authentication services.

3.2.2.2 Active Directory Lightweight Domain Services (AD LDS)

AD LDS is used to provide a duplicate of the directory store for use by network applications. AD LDS can also be used as a more secure alternative to an AD Domain Services server in low security networks.

3.2.2.3 Active Directory Certificate Services (AD CS)

The AD CS role can be used to create a public key infrastructure by issuing digital certificates binding an identity to a certificate. A private key associated with a certificate can be used for authentication. AD Certificate Services is not always limited to a local network and can be used to provide services to external communities.

3.2.2.4 Active Directory Rights Management Services (AD RMS)

Although AD Domain Services servers can determine whether documents on the network can be accessed, they cannot control how documents are used by the identities that are allowed to access them. The AD Rights Management Services can ensure the integrity of data by enforcing usage policies for documents.

3.2.2.5 Active Directory Federation Services (AD FS)

AD FS allows the AD architecture to span different organizations or platforms, so each organization can maintain its own directory service while allowing some resources to be shared.

3.2.3 Components

Some components are necessary to describe an AD architecture.

3.2.3.1 Domain Controller (DC)

A server responsible for the AD DS role is called a Domain Controller. It provides a Kerberos Key Distribution Center authentication service, as well as other AD services[53, p. 9].

3.2.3.2 Logical divisions of the directory service

The smallest logical division is a domain. Each domain requires at least one domain controller, with each domain controller containing all the information about the domain's identities. A collection of domains in a contiguous DNS namespace is called a tree. Finally, the set of all the domains forms an AD forest, which is the security boundary of the directory service. The first domain in a forest is called the root domain[53, p. 9].

3.2.3.3 Sites

An AD site represents a portion of the enterprise within which there is high data rate and high capacity connectivity. Such a site is a boundary for replication and service usage[53, p. 11].

3.2.3.4 Organizational Unit (OU)

An organizational unit is a container for active directory objects, such as computers, users, or groups. An OU can contain other OUs to create a hierarchical organization. OUs are the main tool for sorting objects and selecting the scope of security or administrative policies[53, p. 11].

3.2.3.5 Single Sign-On (SSO)

Single Sign-On (SSO) allows a user to enter its credential only once when using multiple independent software systems. AD is often used to provide SSO to the various services a company employee might have to access, based on their AD identity, so the user only has to log into Windows to be logged into other services (such as an e-mail client or a web application), even if they are provided by another company (with the use of AD FS).

3.2.3.6 Group Policy

Group Policies are used to administer a large number of domain-joined client computers remotely. A Group Policy Object (GPO) is created by an administrator to define a behavior, linked to users, and synchronized between the AD DCs before being pushed to the client computers. Each client computer applies the different GPOs and resolves potential conflicts before enforcing the resulting configuration.

3.2.4 Conclusion

AD is a basic and critical service of a Windows based IT architecture. Since AD provides identification, authentication, and access control to the computers attached to a network, it needs to meet high availability, security, and functionality requirements. This requires different techniques to be used, such as server redundancy, load balancing, failover systems, security protocols, and data replication techniques.

3.3 Exchange

Exchange is Microsoft's mail server that has been in development for 19 years, and encompasses more than 21 million lines of code. The Microsoft client-side software to access Exchange services is Microsoft Outlook.

3.3.1 Mail Solution

Exchange provides email services and requires an existing AD infrastructure to run, as it extends AD identities to create mailboxes, calendars, and contacts lists[54, Ch. 1]. The latest versions of these software solutions are Microsoft Exchange 2013 and Microsoft Outlook 2013.

3.3.2 Outlook 2013

Outlook 2013 is the client-side software associated with Exchange 2013, but it can also be used as a standalone application. Its most common use is as an email application, but it can also be used for calendar, tasks, and contacts management, RSS reader, and taking notes. Thus Outlook 2013 can be used as a personal information manager.

Outlook is also available as a web application called Outlook Web App (OWA), which is used to provide remote users access to their mailbox, contacts, and calendar.

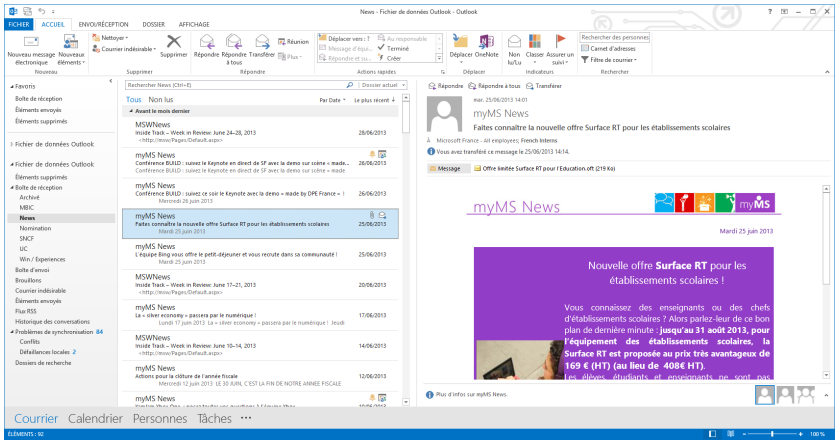

Figure 3.2: Exchange 2013 client

3.3.3 Exchange 2013

Exchange 2013 is the server side software of the mail solution.

3.3.3.1 Active Directory

Of all of Microsoft's applications, Exchange makes the most extensive use of AD. Exchange extends the AD Schema by adding new objects and adding attributes to existing objects, such as email addresses for users. Exchange stores this information in every AD DC in the forest (for schema updates and configuration settings), and in the domain for mail-enabled user identity updates[54, Ch. 1].

3.3.3.2 Server Roles

Exchange 2013 reduced the number of roles from five in Exchange 2010 down to two: the Client Access Server role and the Mailbox role. The Client Access Server is the server used by a client for authentication and redirection to the user's active mailbox server. The mailbox server stores the mailbox data. Each user's mailbox can be replicated on multiple mailbox servers, with one of them being modified directly by the user (called the active mailbox), while the others are passive copies, used in case of failure of the active mailbox server. The active mailbox server can be different for each user[54, Ch. 1].

3.3.3.3 Administration

Exchange 2013 can be administered with graphical user interface (GUI) tools, such as Microsoft Management Console (MMC) snap-ins, but there are also new PowerShell 3.0 cmdlets to create scripts and automate tasks, as well as the web based Exchange Administrator Central that allows an administrator to configure the Exchange 2013 architecture from any browser[54, Ch. 3&5].

3.4 SharePoint

SharePoint 2013 is a collaboration solution, which uses server software to provide users with collaboration tools through a web interface [55, Ch. 1]. SharePoint's most visible aspect is web portals, which can be used to access documents, regroup information, or access SharePoint functionality. SharePoint can be used to create public or private web portals, such as a company's public website, or a department, team, or personal web site. Websites can be created using the desktop application SharePoint Designer 2013. These portals can be used to create a company intranet (which is accessible only from the company's internal network), an extranet (which is available only to company employees or partners even if they are outside the company's offices), or a public website, available to all [55, Ch. 1].

These web portals can be used to store and share any kind of data. Moreover, Microsoft Office integration within SharePoint allows users to quickly open and save documents to or from a SharePoint site, retrieve a previous version of a document, protect documents, co-author a document in real time, synchronize contacts, or integrate Microsoft Access applications in SharePoint.

SharePoint can also be used to search for documents and information on the company's intranet. This enables any employee to use SharePoint's search engine to quickly find data among all the documents he or she has access to.

SharePoint integrates tools for document management according to various compliance standards, such as Sarbanes-Oxley (SOX) and ISO-9000 [55, Ch. 1].

3.5 Lync

Lync is the real-time communications component of Microsoft's UC solution. Lync is composed of two different pieces of software: the Lync Server and the Lync client. This solution provides instant messaging, presence, VoIP, and conferencing functionality to users, as well as providing telephony features with the Enterprise Voice option[56].

3.5.1 Client-side software

To communicate using a Lync infrastructure, users must use one of the Lync client-side software options (i.e., client applications). Some of the characteristics and features of these clients are described in the following paragraphs.

3.5.1.1 Clients

All Lync client functionality is accessible through a client application, which can be either a desktop client (installed on the client computer), a mobile client (installed via the phone's application market), a Lync Phone (a dedicated device on which Lync is running), or a web-based client (which can be accessed from any networked computer with a supported browser[57]). The web based client can be especially useful when inviting external partners to a meeting or to enable employees to use Lync while on the move[56, Ch. 1.1].

3.5.1.2 Contacts

The default main screen of the Lync client is the user's contacts list, that displays this user's list of contacts, sorted by configurable groups. This list displays, for each contact: their name, picture, availability status, location, and a note.

The user can search for contacts by name or skills through the search box. Results will be displayed as contacts in the contact list, along with their role or company (if they are external contacts) and their relevant skills, in the case of a search by skill(s). Contacts can be added to groups and assigned a confidentiality level, to determine what information is available to this contact.

The user can also display the contact card for each contact. This contact card lists messaging options, contact information (such as address or phone number) and their organization information (such as their chain of managers, from their manager to the company's CEO, people with the same manager, or their collaborators). The search and contact card make it easy to find the correct person or persons quickly, enabling users to find available persons with the appropriate skills [56, Ch. 1.1].

3.5.1.3 Presence

The Lync client can be used to access presence information of contacts within the company or within federated organizations. The contact's status is the first form of presence information. This presence information can be set manually or automatically to one of: available, away, busy, do not disturb, be right back, in a conference/call, or offline. This allows people to know how to contact the person, and when they might get an answer. This status also changes how messages

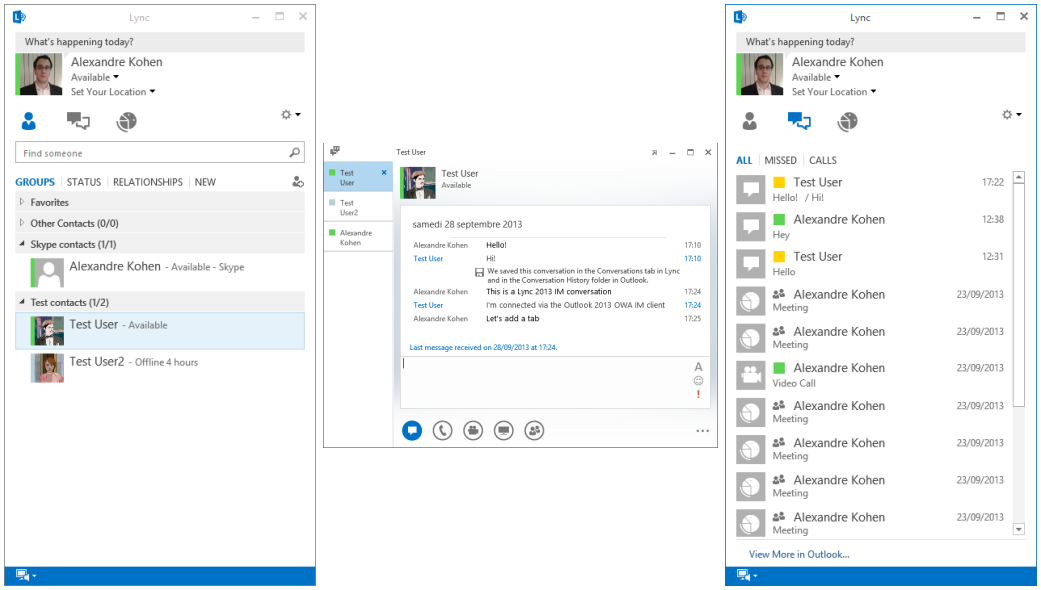

Figure 3.3: Lync 2013 contacts list and conversations

will be delivered, for example, an incoming instant message will play an audio notification if the user's status is set to available, a visual notification if the person is busy, or no notification if the person should not be disturbed.

Users can also leave a note, which will be displayed under their name for all contacts, which allows for more explanation on the reasons for their absence or useful information, such as "I'm in a day-long meeting, please contact XXX if you need help today".

The user's location can also be set. When in a new location, the user can enter a name for the location. This location name will be displayed under the user's name every time they log on in the future from this same location[56, Ch. 1.1].

3.5.1.4 Instant messaging

Instant messaging conversations can be started by double clicking on a contact name in the contacts list. Messages will be sent to the recipient's current device (computer, phone, or browser application), or delivered to them when they next connect to the Lync server. Depending on the user's status, the recipient will get different notifications of the incoming message. The user can reply to or ignore the message. Participants in an instant messaging discussion can invite other people to join the conversation, or add voice, video, whiteboard, presentations, or other activities to the conversation. After leaving the conversation, all of the messages are recorded, and a list of previous conversations is available under the Conversation tab of the main screen.

3.5.1.5 VoIP and Enterprise Voice

The Lync client can be used for voice communications, either by adding voice to a text conversation, or by starting a voice conversation from the contact list or a contact card. If both parties have VoIP support, then the communication is established using VoIP. This is usually the case between Lync Desktop and web clients, or other federated desktop clients, such as Skype.

If the recipient cannot be reached via VoIP, for example because they are not on a computer network, then Lync with Enterprise Voice can establish a communication session over the PSTN. Lync Enterprise Voice users can access various telephony services, such as call forwarding, visual voicemail, device switching, enhanced emergency services, or call delegation [56, Ch. 1.1].

3.5.1.6 Video conferencing and collaboration

Lync also supports video conversations, and conferencing. While conferencing, users can use various media, such as text, voice, video, screen sharing, presentations, or whiteboards. They can also conduct polls and record the conversation. Users can also co-edit documents using Sharepoint during a meeting [56, Ch. 1.1].

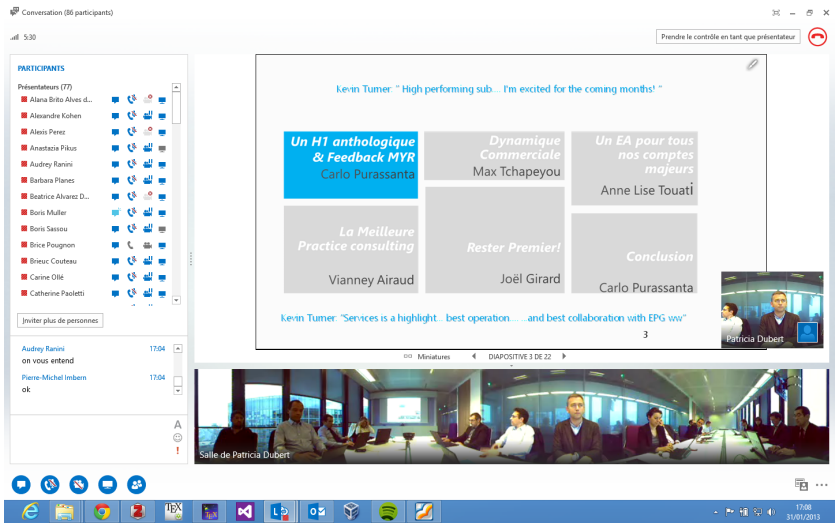

Figure 3.4: Conference with Lync 2013

3.5.1.7 Outlook integration

Lync is closely integrated with Outlook and many features require both to be fully available.

For example, contact information is shared between Outlook and Lync (so users can see presence information while in Outlook) or manage contacts from both applications. Moreover, Lync archives are stored in Outlook and searchable as emails, and voicemails can be accessed from both Lync and Outlook.

Users can schedule meetings from Lync or Outlook, and add to an email a link that can be used to join a Lync meeting. Lync will also use the user's Outlook calendar to automatically update the user's presence information according to their daily schedule [56].

3.5.2 Lync Server 2013

Lync Server 2013 is the main server-side software used to create a Lync infrastructure[58, 56, Ch. 1.2]. .

3.5.2.1 Roles

Each server running Lync Server runs one or more server roles. A server role is a defined set of Lync Server functionalities provided by that server.

Standard Edition Server The Lync Standard Edition Server allows the use of IM, presence, conferencing and Enterprise Voice in one server, and is mostly used by small organizations or pilot projects.

Front End Server The core of any Lync architecture is the Lync Front End Server role, which provides basic Lync Server functions, such as user authentication, registration, presence information, address books, IM, conferencing, web tasks, monitoring, archiving, or application hosting. Front end servers can be grouped in pools to provide scalability and failover capability.

Back End Server The Back End Server role is a database server running Microsoft SQL Server to provide database services to the Front End servers. Both the Front End and Back End server roles are required for a Lync Server Enterprise edition infrastructure to be operational.

Edge Server Edge servers allow users to communicate with others outside of the company's firewalls, and enables connectivity with other IM services, such as Windows Live, Skype, AOL, Yahoo!, or Google Talk.

Mediation Server A Mediation server can act as an interface between the Lync Server architecture and a PSTN gateway, IP-PBX, or SIP trunk, to allow users to reach users connected to other communication networks.

Director Director servers can be used to provide increased security when allowing external user access. The director server can authenticate and redirect Lync users to internal servers without providing any other Lync service to these users. This can protect internal servers from external attacks.

Persistent Chat Finally, a Persistent Chat Server role can be used to enable Lync's persistent chat functionality. In a persistent chat, users can exchange instant messages and see messages that were sent while they are disconnected.

3.5.2.2 Server pools

Most server roles are deployed on a pool of servers in order to provide scalability and high availability. Multiple servers with the same set of roles are placed in a group (i.e. the servers form a pool), and all requests are addressed to the pool instead of to a single server. A load balancing system, either DNS load balancing or hardware load balancing, will redirect each request to a server according to server availability. If one server is unavailable due to maintenance or system failure, the rest of the pool should be able to continue to operate, while continuing to direct new users to an available server. Users connected to an unavailable server are switched to another server to minimize service unavailability.

It is also possible, as a disaster recovery measure, to pair two pools of servers in different locations, so that if one site or pool is unavailable, traffic can be redirected to the other site with minimal interruption of service [56].

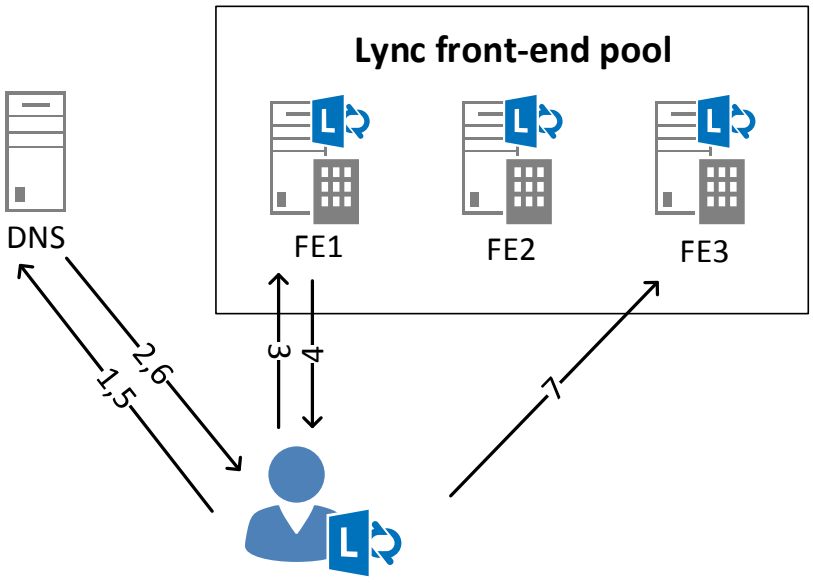

Figure 3.5: Lync client connection (Adapted from figure 1.11 of [56])

The figure 3.5 shows the steps required to connect a client to its home server in a front-end pool:

1. The client queries the DNS server to get the pool's IP
2. The DNS server returns all the IPs of the servers in the pool
3. The client connects to a random server from the pool
4. If this server is not the client's home server, it returns the name of the client's home server
5. The client queries the DNS server to get the home server's IP
6. The DNS server returns the client's home server's IP
7. The client connects to its home server

3.5.2.3 SharePoint Integration

Lync Server can be integrated with SharePoint, which enables the skill search functionality, based on users' skills as specified on a user's SharePoint page. This allows SharePoint sites to display users' presence information based on the data provided by Lync servers, share users' pictures, or directly record and share meetings via SharePoint.

3.5.2.4 Exchange Integration

Lync Server can be integrated with Exchange, which adds unified messaging features, IM and presence to the OWA, and integration of contacts.

3.5.3 Architecture

This section describes some key elements of a Lync architecture.

3.5.3.1 Central Management Store (CMS)

The Lync Central Management Store is a database holding the configuration information for the Lync topology. This database is replicated on all front-end and back-end servers of an enterprise pool. This data can be modified by the Topology Builder, the Lync Server Control Panel, and the Lync Server Management Shell. Access to this database is required for any change to the architecture of the solution. It is recommended to pay particular attention to the availability and backup of this database.

3.5.3.2 Sites

Lync sites define a region of the network containing Lync Server components in which the connectivity is good: the connection between computers of a site has a high speed and low latency. A Lync site can either be a central site, if it contains at least a front-end server (either a Standard edition server, or an enterprise pool), or a branch site, which depends on a central site to provide some Lync services to its users.

A branch site providing telephony services to its users can have a Survivable Branch Appliance (SBA) for sites under 1,000 users or a Survivable Branch Server (SBS) for sites between 1,000 and 5,000 users, which have the Lync Server Registrar and a Mediation server.

Although their definitions are similar, Lync sites and AD sites do not need to correspond [59].

3.5.3.3 Policies

The behavior of the Lync solution is configured by policies which are assigned to users or sites. The management of these policies is an important part of the design and the administration of a Lync solution. Some of these policies are:

Client policy A client policy defines the behavior of the Lync client software, such as which features are available and some client settings. Until Lync server 2010, these settings were controlled via an AD Group Policy. This policy can only be assigned to users.

Client version policy This policy defines which client versions are allowed to log on to Lync Server and which are blocked. This policy can also force silent upgrades of the client, or redirect the user to an URL to download a new version. The Lync server checks the SIP headers to determine the client version, and compares it the client version policies applicable for the user. Client version policies can be applied at the global, site, service or per-user scope.

Conferencing policy Conferencing policies determine which features and capabilities can be used in a conference. Conferencing policies can be applied at the global, site, or per-user scope.

Therefore, to define the permissions and behavior of the solution for an user, multiple policies have to be combined. The precedence of policies (eg. a per-user policy overrides a global policy) has to be taken into account when designing the user profiles.

3.5.3.4 Autodiscover

The autodiscover features allows a client to connect to the Lync infrastructure given only the SIP address of the user. Combined with SSO, this allows the user to connect to Lync without any action.

The autodiscovery method to find the registrar server is based on DNS queries, using the domain name of the SIP address. The queries depend on the client used. For example, for an user with a SIP address of sip:user@domain, the following queries will be made:

Lync 2013
- Host (A) record lyncdiscoverinternal.domain
- Host (A) record lyncdiscover.domain
- Service Locator Record (SRV) record _sipinternaltls._tcp.domain
- Service Locator Record (SRV) record _sip._tls.domain
- Host (A) record sipinternal.domain
- Host (A) record sip.domain
- Host (A) record sipexternal.domain

Lync Mobile
- Host (A) record lyncdiscoverinternal.domain
- Host (A) record lyncdiscover.domain

Lync 2010
- Service Locator Record (SRV) record _sipinternaltls._tcp.domain
- Service Locator Record (SRV) record _sip._tls.domain
- Host (A) record sipinternal.domain
- Host (A) record sip.domain
- Host (A) record sipexternal.domain

3.5.3.5 Media bypass

The media bypass feature allows the audio flux to transit directly to the PSTN gateway, instead of using a mediation server. This can improve the call quality by reducing the latency and reducing the loss (as there is less transcoding), particularly for users of a branch site without a mediation server, as the media flux would go to the datacenter and back to the branch site before reaching the branch site PSTN gateways.

The media bypass can enabled for the whole solution, or for specific sites. If media bypass is enabled, the communication between the Lync client and the gateway is established via the G.711 CODEC.

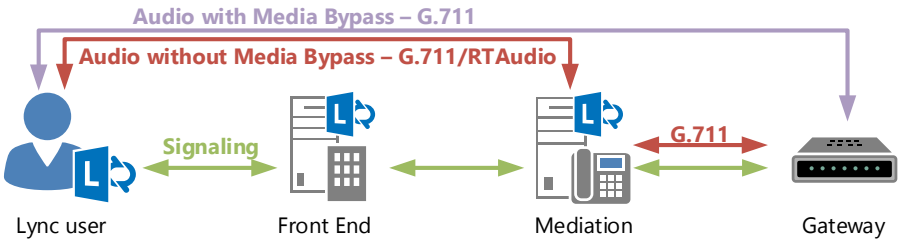

Figure 3.6: Media Bypass

3.5.3.6 Call routing

Lync calls routing uses the following components[60]:

Dialplan A dialplan is made up of different normalization rules, which can manipulate phones numbers. Users dialplan normalizes the phone numbers dialed by the users into the E.164 format. A dialplan can be assigned to each PSTN gateway to manipulate the caller and called number for inbound calls. A normalization rule is composed on a regular expression to detect the number, and the replacement expression.

Voice Policy A voice policy can be assigned to users, site or organizations to determine the Enterprise Voice functionality available.

Route A route allows an outgoing to connect via a mediation server to a gateway. Each route can be associated to multiple trunks.

PSTN Usage A PSTN usage is use to link voice policies and routes. There can be a many-to-many relationship between voice policies and PSTN usage, and between PSTN usage and routes.

Trunk configuration Allows number manipulation on outgoing calls.

The figure 3.7 describes the call routing process used by Lync.

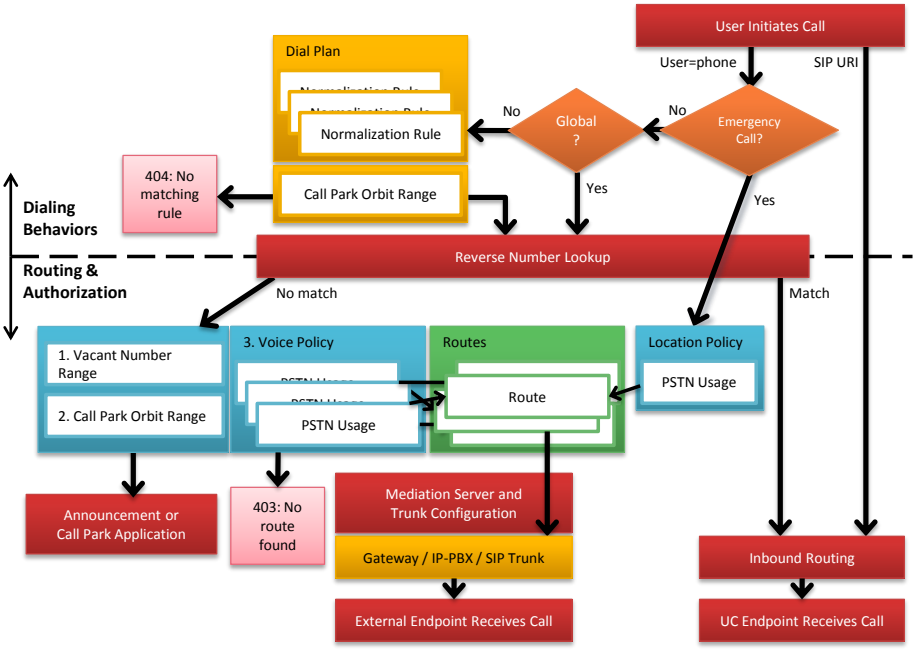

Figure 3.7: Lync 2013 voice routing. From Microsoft TechEd Africa 2013

3.5.4 Security

Security is a major concern for all Lync deployment, as compromising Lync would have great effects on the company and users. The common security threats for Lync are described below[61].

Eavesdropping If an attacker is able to gain access to the data path used, he may be able to read exchanged data. This can be countered by encrypting the transfered data, using TLS and SRTP in the case of Lync.

Compromised-Key Attack If an attacker is able to determine the key used to encrypt the data, an attacker can then use it to recover the encrypted data. To mitigate this risk, Lync Server 2013 uses a PKI to protect key data, and keys are exchanged over TLS connections.

Denial-of-Service Attack An attacker can flood a service with request to prevent legitimate users' request from being processed. The Lync Director role is one of Lync's defense against this type of attack.

Identity Spoofing An attacker can spoof a network component to operate instead of the legitimate component. To counter this risk, all Lync component are identified with secure certificates.

Man-in-the-Middle Attack In a Man-in-the-Middle Attack, an attacker reroutes traffic between two users through a computer he controls in order to read the exchanged traffic. This type of attack in countered in Lync with the use of public-key cryptography.

RTP Replay Attack A replay attack occurs when a valid media transmission between two parties is intercepted and retransmitted for malicious purposes. SRTP used in connection with a secure signaling protocol protects transmissions from replay attacks by enabling the receiver to maintain an index of already received RTP packets and compare each new packet with those already listed in the index.

Viruses and Worms Viruses and worms can be spread through file transfers or URLs sent via IM. This risk can be mitigated with client antivirus software or file transfer restrictions.

Personally Identifiable Information Some personal data can be disclosed over the network when using Lync. This can be controlled using client configuration.

Chapter 4

Case Study

This chapters presents the 30 000 Lync seats and telephony deployment which was the main focus of this thesis. The various stages, technical choices, and difficulties of the project are detailed.

4.1 Project Overview

This section gives an overview of the project.

4.1.1 The Client

The client is a french group with 250,000 employees, which will be called ”Contoso” in this report*.

4.1.2 Context

Contoso planned to move one of their offices to a new site, called in this report ”Campus”, and wanted to take advantage of this move to introduce Lync as a new communications solution, first to the 1,250 Campus users, then to 2,000 nomadic users and 30,000 other users.

By introducing a new UC solution, Contoso IT direction’s goals were:

- Meet the new user needs
- Offer new services

* This company has requested that their name not be made public.

- Assist Contoso in its development and transformation
- Reduce IT and telephony costs and risks

4.1.3 Specifications

Contoso had the following broad specifications for the solution:

- Telephony features allowing the new solution to replace a traditional telephony solution
- Provide videoconferencing features
- Integration with the existing IT, telephony, and videoconferencing environments
- High availability and site survivability
- Available from Contoso's internal network, and from an external network, on computers, smartphones, and tablets

4.1.4 The Constraints

As the project had to be completed in less than six months, time was a major constraint in this implementation. Moreover, Microsoft was responsible for the integration of various vendors' equipment into the solution, which induced additional risks.

4.1.5 Stages

The project was split into 5 stages, according to the V-Model[62, 63] :

Requirements and Architecture During this phase, the client requirements are gathered, and the overall architecture and features of the solution are defined. The deliverables of this phase include a summary of the workshops conducted with the client, and a high level specification of the solution.

Design The goal of this stage is the redaction and validation of the detailed design document, which explains in detail the technical requirements and implementation of the solution.

Implementation This is the main step realizing the concrete goals of the project. Expected deliverables are the installed solution and installation guides.

Test During this phase, the solution is tested to confirm that it is working as specified in the design document.

Validation This stage validates that the solution can be used in the production environment according to the client's needs and the original specification from the first stage.

The stages are successive, but multiple stages can be active at the same time.

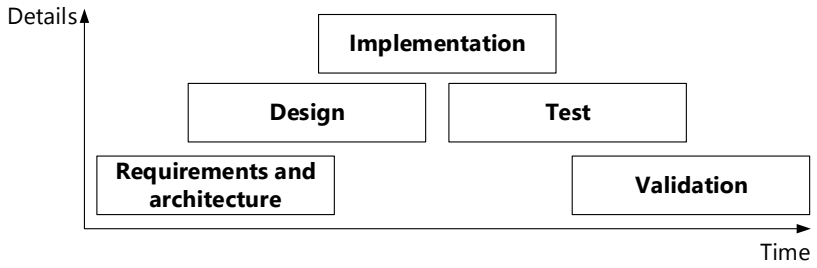

Figure 4.1: The V-model stages

The following subsection describe the various stages of the model.

4.1.6 Personal involvement

During the Requirements and Architecture stage, I gathered the client's requirements in a series of workshops. During the Design stage, I studied the Lync core architecture and dimensioning of the system, as well as the fixed and wireless network requirements and prerequisites for Lync, and was responsible for the associated sections of the design document. During the Implementation stage, I built and documented the core Lync integration infrastructure, and assisted the Contoso team in building the production infrastructure. During the Testing and Validation stage, I designed the test plan, wrote scripts, tested and validated the solution. During all stages, I was responsible of the project documentation and prerequisites checking. Further details of these stages are given in the following sections.

4.2 Requirements and Architecture workshops

Most of the time during the Requirements and Analysis phase was devoted to a series of nine workshops. Each workshop focused on a specific topic and involved

one or two Microsoft consultants, the client project owner, and some relevant technical specialists for half a day to a full day.

The first six workshops were planned from the beginning, while the others were added as the need for more clarification of particular topics arose.

4.2.1 Architecture and Dimensioning workshop

This first workshop's goal was to gather additional information regarding the project scope, the concerned population, usage models, to determine the general infrastructure architecture, and to begin the process of dimensioning the implementation.

In order to dimension the implementation, we used the data found in the Lync Server 2013 User Models[64], unless the client could provide more specific information about their current and expected usage, in which case we would use the client's data.

Contoso had several requirements for the Lync infrastructure:

- A Contoso datacenter should host the main Lync Server 2013 farm, and should provide Lync services to multiple sites.
- The Lync infrastructure had to be highly available, and resistant to a single component failure.
- The interconnection with the company's telephony infrastructure must be secure, but not the interconnection with unified messaging and videoconferencing.
- A disaster recovery plan was not required.
- The campus site should have survivability (i.e., telephony services should operate even if the connection to the datacenter is unavailable).

The unified communications solutions had to be available from:

- A cable-connected computer in any of Contoso's sites,
- A WiFi-connected computer in WiFi enabled sites,
- A WiFi-connected Apple iPhone or Apple iPad,

- A computer outside Contoso's network, connected through a VPN,
- An iPhone or iPad outside Contoso's network, connected through a VPN,
- A Lync or IBM Sametime federated user.

4.2.2 Information Systems Impacts workshop

This second workshop focused on the interactions between the proposed solution and the existing IT infrastructure. Major interactions were expected with AD, DNS, PKI, Exchange, SQL, and support for Lync on a separate disk under the customer's choice of Windows OS.

Active Directory

AD was the first requirement, as AD is the base upon which many of Microsoft's products are based, including Lync Server 2013 or Exchange Server 2013. Contoso's AD has multiple domains and forests and Lync Server 2013 should be installed in the COMMON.CONTOSO.FR and COMMON.INTEGRATION.CONTOSO.FR domains, in which the user accounts to be used for Lync are located.

Due to the critical nature of the AD infrastructure for the organization, any modification to the AD architecture usually requires a long advance notice. The Lync Server 2013 requires a schema extension and a domain/forest preparation, which required a one-month notice at Contoso, so we had to initiate the process early.

If user accounts in another domain need to be activated for Lync, another domain preparation will be required.

DNS

Lync Server 2013 relies on DNS requests to locate service providers, so we needed entries added to the internal and external CONTOSO.FR zones.

Public Key Infrastructure

A public key infrastructure (PKI) is also required by Lync Server 2013, so Contoso had to designate the PKI to be used for Lync. Both the integration and production environments use the same Opentrust[65] PKI, but with different certification authorities (CAs).

Exchange

Each user's SIP address will be the same as their email address, hence they will have the following structure: sip:firstname.lastname@contoso.fr

Contoso uses a Exchange Server 2010 infrastructure, but with a PKI different from the PKI used for Lync Servers, therefore the Exchange infrastructure must be modified to use the same PKI. The Autodiscover and Exchange Web Services were not currently enabled and had to be enabled.

Windows

Contoso asked for Lync servers to be installed on Windows Server 2008 R2, and on a volume not used by the operating system's files. The last point required a supportability check, which turned out to be positive.

SQL

Although Microsoft recommended the use of Microsoft SQL Server 2012, Contoso chose to use Microsoft SQL Server 2008 R2, because:

- Although SQL Server 2012 deployment was on Contoso's roadmap, it was scheduled for a later time.
- The Contoso team's current proficiency with SQL Server 2012 was low, and there was not sufficient time for training.
- The project criticality was too high to increase risks by trying a new solution.

4.2.3 Video interconnection and Internet workshop

The solution had to be interconnected with Contoso's existing videoconferencing solutions and to provide services to some users over the Internet. This workshop allowed Contoso to express their needs on these topics.

Videoconferencing

Contoso had an existing Polycom-based videoconferencing solution which needed to be integrated with the Lync-based solution. Their features requirements were:

- Integrate the Lync address book in the videoconferencing address book

- Show HDX and VSX* equipments as contacts in Lync
- Peer to peer communications with HDX/VSX, with and without RTVideo license
- Conferencing between Lync, HDX and VSX clients in a Lync conference
- Conferencing between Lync, HDX and VSX clients in a RMX† virtual conference room
- Document sharing with HDX and VSX equipments.

Internet Access

The following usage scenarios require Internet access:

- Remote users connecting to Lync from outside Contoso's network
- Federated users
- Mobile users
- Anonymous users

To enable the Internet access features, two components are needed: load-balancing and reverse proxy. Load-balancing can be either DNS-based, or hardware-based. The reverse proxy component is provided by Contoso.

4.2.4 Telephony workshop

Contoso's main requirements for the solution were related to telephony features, as the Lync-based solution had to provide the same features that were provided by the various existing telephony systems in the other offices of the company. Of these requirements, the most critical were:

- Ability to call contacts inside or outside the company
- Single phone number, and the ability to use only the Lync application/phone
- Conferencing
- Auto callback, call forwarding, put a call on hold, response groups
- Caller ID

* Videoconferencing endpoints produced by Polycom † Equipment produced by Polycom to host conferences

- Delegates
- Emergency calls
- 6-digit numbers for internal calls

Initially 1,200 telephony-enabled user accounts will be used at the Campus site, and Campus users must be able to use telephony services even if the Lync datacenter is unavailable. Of all users, a total of 6,500 users will be enabled for Enterprise voice.

The Lync infrastructure must be interconnected with Contoso's other PBX through a G.729 CODEC. The gateways must be highly available.

The phones considered for Campus deployment are:

- An Aastra Lync Phone Edition
- Two SNOM phones for delegates scenarios

The dial plan to follow was provided by Contoso.

4.2.5 Network workshop

Contoso has two wide area networks (WANs) that will be available from the Campus site:

1. ToIP network

- Layer 3 WAN
- 20 Mbps
- Diffserv classes used:
  - Audio
  - Video
  - Data high priority
  - Data critical
  - Data best effort
- Service Level Agreement (SLA) on the quality of service for the audio and video classes
- 30% of the bandwidth can be used by Lync

2. Ethernet based WAN deployed across the company

- Layer 2 WAN
- 2x100 Mbps, upgradable to 1 Gbps
- Before Campus, used only for data
- No SLA

Contoso currently uses QoS on both WANs, based on the DSCP headers of packets. The current values are DSCP46 for Voice and Signaling, and DSCP AF41 for Video – All Lync traffic must be tagged to use QoS.

In all the other offices, Contoso has two distincts VLANs for voice and data traffic. However, all Lync clients (desktop software, phones, or mobile application) generate audio, video, and data traffic.

Campus's WiFi architecture was in the process of being redesigned. The projected WiFi architecture was to use 4 Cisco controllers (providing routing and firewall functionality), and multiple light access points (acting only as relays).

4.2.6 Operation and Supervision workshop

This workshop focused on determining how the solution would be maintained and monitored by Contoso's teams during regular operation.

Supervision

Contoso already uses System Center - Operations Manager (SCOM), and has a dedicated team. The current infrastructure is based on SCOM 2007, and monitors 1000 nodes out of a total of 3000 nodes.

The SCOM team requires personalized rules to filter some of the Lync alerts.

Operation

The main tools for Lync's operation are Powershell and the Lync Server Control Panel.

As Lync's operating model is very close to Exchange's, Contoso wants their Exchange administration team to administer the Lync solution. Contoso's Exchange administration has the following properties:

- The service is administered with Powershell scripts and the Exchange console

- SCOM is used for supervision
- Role-based access control (RBAC) is currently being deployed
- The main support team administers servers while local teams administer users
- Users are classified by OU and delegations to these OU are assigned to regional administrators
- There are 25 regions, each with multiple sites and a single regional administrator
- Dell's (formerly Quest Software) MessageStats solution is used for monitoring

4.2.7 Additional Workshops

These shorter workwhops were not scheduled at the beginning of the phase and were added as more information became available or when new needs emerged from the previous workshops.

4.2.7.1 Lync Mobile workshop

This workshop took place after the public release of the Lync Mobile 2013 client and specifications to review the integration of this Lync client with the implementation and Contoso's needs.

4.2.7.2 Desktop workshop

This workshop provided additional information about the desktop configurations that will be used at the Campus site, as well as desktop issues such as deployment and configuration of the clients, antivirus and firewall properties, and QoS client configuration.

4.2.7.3 Music on Hold workshop

The music on hold feature needs an audio file to play when a call is put on hold. There are two possible locations for this file:

On each client's computer This is Microsoft's recommendation. However, this solution requires that the file is placed and updated on each client computer.

On a central file share This solution removes the need to manage the music on hold file on each of the client computers, but can use more bandwidth and may cause problems for users connected through an Edge server.

4.2.8 Decisions

According to the business and technical needs expressed by Contoso during the series of workshops, the following decisions were taken:

Sizing The solution must be able to support 30,000 users, with 1,250 users at Campus.

Domains The domains names to be used are CONTOSO.FR and ADATUM.COM* with CONTOSO.FR being the default SIP domain.

Client As many of the computers on the Campus site will run Microsoft Windows XP, the client deployed will be the Lync 2010 client.

Deployment in two phases Due to the time constraint and the complexity of the project and of Contoso IT infrastructure and organization, the Edge server portion of the project was removed from the first phase. It will be implemented in a second implementation phase.

Only two environments Contoso's usual deployment process involves three environments, each managed by a different team: Design, Integration, and Production. Due to the limited time available, only the Integration and Production environments will be involved for this project.

Single Datacenter All Lync servers will be hosted in a single Contoso datacenter, and branch sites will connect to the datacenter, with a survivability solution in case the connection to the datacenter is lost.

Redundancy To ensure high availability and resistance to a single failure, all the components in the solution must have an n+1 redundancy, which means that for each component, an extra node should be used, so that there is no service degradation in case of a single node failure. This includes the Lync servers, telephony gateways, reverse proxy and load balancing solutions.

Telephony Lync should be the primary telephony solution for 1200 users at Campus. Users should use their local PSTN access for external calls. Lync should be interconnected with Contoso's telephony environment via the G.729 codec.

* placeholder name for another company

Security To ensure the confidentiality of data and the integrity of the service, all traffic must be encrypted, and Lync Director servers must be used.

WAN usage Due to the limited bandwidth available on the ToIP network, the Ethernet MAN is preferable for Lync data – if the creation of priority classes and an operator SLA can be obtained.

New SCOM 2012 infrastructure A new SCOM 2012 infrastructure is being deployed by Contoso and will be used for Lync.

4.3 Design

The redaction of the Detailed Design Document was the main task of the design stage. This 300-page document explains the design choices and specifications.

This section provides an overview of the design of the final implementation, as specified in the Detailed Design Document.

4.3.1 Prerequisites

This section lists the requirements that had to be met by Contoso's infrastructure *before* the implementation's construction could begin.

4.3.1.1 Active Directory

- The forest functional level of the CONTOSO.FR forest must be Windows Server 2003 native.
- The domain functional level of the COMMON.CONTOSO.FR domain must be Windows Server 2003 native.
- There must be at least one AD DC which is a Global Catalog for the COMMON.CONTOSO.FR domain.
- The forest must be prepared for Lync 2013.
- An account with Domain Admin rights is required for deployment.
- A member of the RTCUniversalServerAdmins group is required for deployment.

4.3.1.2 DNS

- A, SRV and CNAME entries can be added to the DNS zones
- DNS zones CONTOSO.FR and ADATUM.COM must be configured in split-domain.
- The Lync infrastructure and internal clients must be able to resolve the following internal DNS zones: CONTOSO.FR, ADATUM.COM, and COMMON.CONTOSO.FR
- The Lync infrastructure in DMZ must be able to resolve external DNS zones CONTOSO.FR and ADATUM.COM
- External components accessing Lync services must be able to resolve the CONTOSO.FR and ADATUM.COM external zones.

4.3.1.3 PKI and certificates

To allow Lync traffic to use TLS and MTLS connections, the Lync infrastructure requires X.509 certificates. To limit the number of subject alternative name (SAN) by certificate, Contoso wishes that each certificate be deployed on only one server, if possible.

4.3.1.4 File Share

The Lync infrastructure uses a file share for exchanging information, such as topology changes, address book files or conference data. As this component is required, the file share should be highly available. Contoso chose to use their existing Distributed File System (DFS) infrastructure, with the DFS-R replication mechanism, which replicates only the updated part of files.

4.3.1.5 Network

The network quality is crucial to the Lync infrastructure, as it will determine the overall experience quality for the users. The general recommendations for the network are:

- No NAT between Lync internal components.
- QoS components should not process real-time Lync traffic.
- Audio and video bandwidth usage should not exceed 30% of the WAN capacity.

- Packet loss should be less than 1%.
- Jitter should be under 30ms and latency under 150ms.

A preliminary network usage assessment, which results are presented in table 4.1, shows that the bandwidth available for Lync traffic on the ToIP network is insufficient for the Campus site, as there is only 7Mbps available. Therefore, the decision was taken to use the ethernet MAN for transmitting Lync traffic between the datacenter and the branch sites.

Traffic	Bandwidth in Mbps
Signaling, IM, and presence	1,10
Calls to ToIP network via SBC	2,07
PSTN calls for external users	0,63
Audio conference	0,90
Video conference	1,98
Application sharing	2,63
Total	9,31

Table 4.1: Bandwidth requirements for Campus

4.3.2 Architecture

4.3.2.1 Lync

Only one Lync site will be created for this implementation, called ”Datacenter”. A remote site ”Campus” will also be created.

Two SIP domains will be configured in production: CONTOSO.FR and ADATUM.COM, with the CONTOSO.FR domain configured as the default SIP domain.

The dialin, meet, and admin simple URLs will be used in this implementation. To allow the addition of new SIP domains while limiting the number of new certificates needed, the meet and dialin URLs have been chosen as follows: https://lync.contoso.fr/contoso/meet https://lync.contoso.fr/adatum/meet and https://lync.contoso.fr/dialin . The administration URL will be https://lyncadmin.common.contoso.fr

4.3.2.2 DNS

Lync client connection should be automatic, which means that after the user has logged into his Windows session, no configuration or password are required for Lync to connect. As Lync 2010 and 2013 clients will be used, the following DNS records will all have to be created:

Record Type	Value
A	lyncdiscoverinternal.contoso.fr
A	lyncdiscoverinternal.adatum.com
A	lyncdiscover.contoso.fr
A	lyncdiscover.adatum.com
SRV	_sipinternaltls._tcp.contoso.fr
SRV	_sipinternaltls._tcp.adatum.com
SRV	_sip._tls.contoso.fr
SRV	_sip._tls.adatum.com
A	sipinternal.contoso.fr
A	sipinternal.adatum.com
A	sip.contoso.fr
A	sip.adatum.com

Table 4.2: DNS records

4.3.2.3 Strategies

This section lists various configuration choices that have to be implemented in Contoso's Lync infrastructure to enable the desired behavior.

Monitoring

All CDR and QoE records will be kept for 180 days.

QoS

To enable QoS tagging of Lync traffic, two mechanisms are used. On Windows XP clients, the QoS Packet Scheduler was installed, while on servers and other clients, the Lync software was configured to use specific ports, and QoS values were assigned to this ports using GPOs. The DSCP values were chosen to respect the values used by Contoso, or the commonly used values.

The client and server ports used by Lync were configured as follows:

Endpoint	Type	Ports	DSCP
Front End servers	Audio	30000 - 36999	46
Front End servers	Video	37000 - 37999	20
Front End servers	Application sharing	38000 - 38999	16
Exchange UM	Audio	30000 - 36999	46
Gateways	Audio	30000 - 33999	46
Clients	Audio	30000 - 30039	46
Clients	Video	37000 - 37039	20
Clients	Application sharing	38000 - 38039	16
Clients	File transfer	39000 - 39039	-
SNOM phones	Audio	30000 - 30039	46

Table 4.3: QoS configuration

4.3.2.4 Lync/Exchange integration

The following Lync 2010 client features depend on the Lync/Exchange integration:

- Contact information
- Calendar information
- Conversation history
- Missed conversations
- Missed calls
- Voice Mail Playback

4.3.2.5 High Availability

This table describes the behavior of the solution when one or more of the components fail or lose connectivity:

Component	# nodes	Impact
Front End	1	No Impact
Front End	2-3	Performance might be reduced
Front End	4-7	All Lync services unavailable, except for local survivability
Edge	1	No impact
Edge	2	Edge features unavailable
OWA	1	No impact
OWA	2	Performance might be reduced
OWA	3	No presentation sharing
Back End	1	No impact if witness is operational Else, see below
Back End	2	User are switched to resiliency mode
Director	1	No impact
Director	2	No external login
DFS	-	No change can be made to the infrastructure
Reverse Proxy	-	No Lync mobile clients support No external web services

Table 4.4: Availability table

4.3.2.6 Load Balancing

High availability requires load balancing for some components. Load balancing allows the distribution of requests among the available nodes.

There are two types of load balancing used for the Lync infrastructure: DNS load balancing, and using a Brocade Hardware Load Balancer (HLB).

The Brocade HLB is used to balance the HTTP/HTTPS traffic to the Front End pool, the Directors, and the Office Web Apps farm, while other traffic uses DNS load balancing.

4.3.2.7 External usage

There are three external usage scenarios possible:

Case 1 Users are directly connected to the Internet.

Case 2 Users are connected through a VPN tunnel, and all traffic goes through the VPN tunnel.

Case 3 Users are connected through a VPN tunnel, but the solution allows split tunneling for Lync traffic.

Case 1 is Microsoft's recommended use case. Case 2 is not supported, as the VPN equipment can degrade the overall call experience. Case 3 is supported, but requires additional work on the VPN infrastructure.

Clients with a mobile device, such as an Apple iPhone or Apple iPad, use the same infrastructure with different access mechanisms, as these clients use the Lync 2013 Unified Communications Web API (UCWA) component which was introduced with Lync 2013 Cumulative Update 1, and installed on the front end server pool.

4.3.3 Infrastructure

The following sections give high level descriptions of the implementation's infrastructure.

4.3.3.1 Internal infrastructure

The internal infrastructure is comprised of all of the servers and equipments connected to Contoso's internal network. Therefore, it is made up of:

Lync clients Desktops, laptops, tablets, phones, or smartphones, the client devices are connected via ethernet or WiFi and allow users to access Lync services.

7-server Lync Front-End pool, with collocated mediation server In this implementation, the Front-End pool has the following tasks:

- SIP server: SIP registrar, SIP session initiation and management, and presence information;
- Audio and video conference room; and
- Mediation server with a PSTN gateway.

According to the company's existing usage data and Microsoft's recommendations, each server can handle 6,660 concurrent users, hence 5 servers are required for 30,000 concurrent users. An extra server is added to handle the additional traffic caused by mobile usage, and another server was added to meet the high availability requirement. Therefore, seven servers are required.

3 SQL Servers Two servers are Back-End servers in a mirroring configuration and host the Lync databases. The third server is a witness server used for automatic failover in case of failure of one of the Back-End servers.

3-server Office Web App pool An Office Web App server is required for displaying shared PowerPoint presentations during conferences. According to the usage data and Microsoft recommendations, each server can handle 20.000 concurrent users, which means that 2 servers are required for 30.000 concurrent users. An extra server has to be added to meet the high availability requirement. Therefore, 3 servers are required.

A highly available DFS share A Contoso file sharing infrastructure, used for Lync data storage. 200GB must be available for Lync Server 2013 on this file share.

A Watcher Node This server monitors the solution's components and reports their status to the SCOM supervision infrastructure. The SQL Server Reporting Services (SSRS) will also be installed on this server.

1 SNOM provisioning server This server is required for automatic provisioning of SNOM phones. This server will be co-located with the SQL Witness

4 SBC Sonus UX2000 gateways 2 in the datacenter, 2 at Campus, they provide interconnection with the ToIP network and the PSTN. Datacenter gateway requirements:

- 1 UX2000-600 (UX2000 with 6 high capacity DSP, allowing 600 concurrent calls)
- 1 UX2000-T1E1-2 (A two-card E1 module)
- 5 UX-SIP-25 (5x25 = 125 SIP licenses)

Campus gateway requirements:

- 1 UX2000-200 (UX2000 with 2 high capacity DSP, allowing 200 concurrent calls)
- 1 UX2000-T1E1-2 (A two-card E1 module)
- 2 UX-SIP-25 (2x25 = 50 SIP lisenses)

A Survivable Branch Server This server allows basic telephony features to remain accessible at the branch site if the Lync infrastructure at the datacenter becomes unreachable.

2-server Lync Director pool This server pool is responsible for authentication and redirection of users to their home front end server.

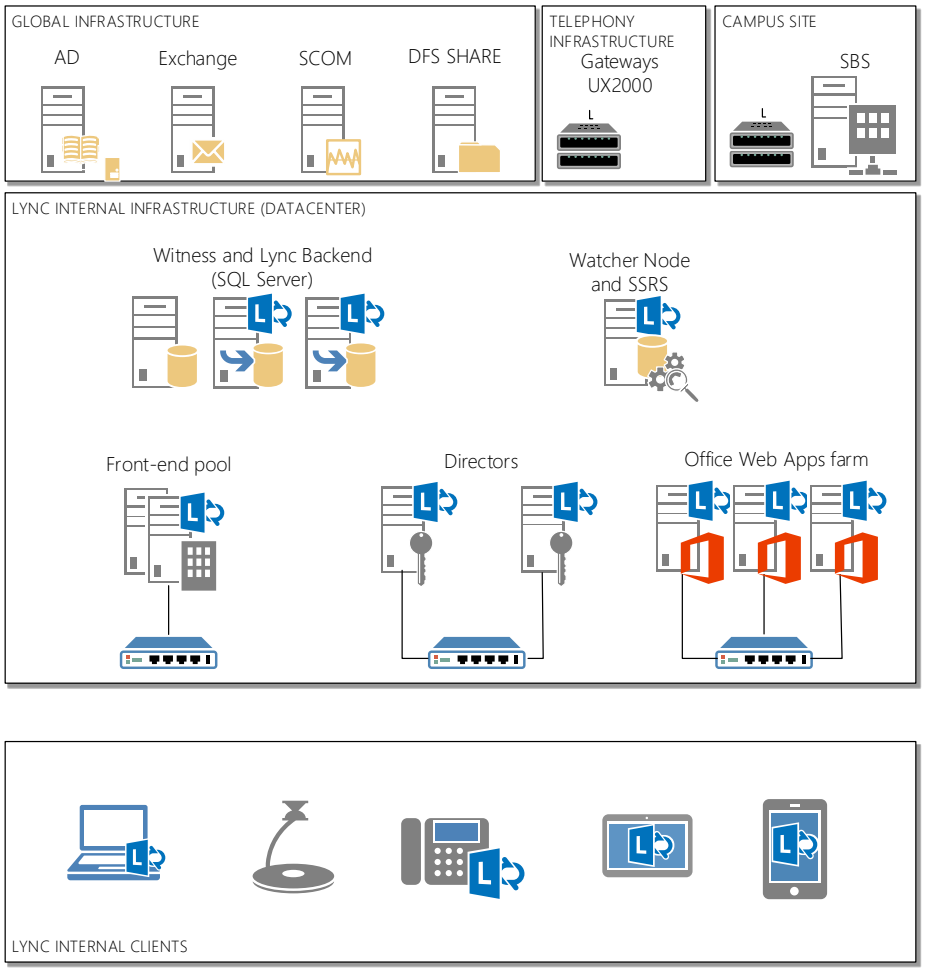

Figure 4.2: Internal infrastructure

4.3.3.2 External infrastructure

The external infrastructure allows communications with networks other than Contoso's, such as the Internet, or the PSTN. The external infrastructure is made up of:

2-server Lync Edge pool This pool handles all non-web traffic, such as voice, video, and sip, from and to external users and federated edge servers. This pool is placed in the DMZ. Each server can handle 12.000 concurrent connections, so only one server and one server for high availability are required.

2 Reverse-proxy servers These servers relay https traffic from mobile and external users. These servers are placed in the DMZ

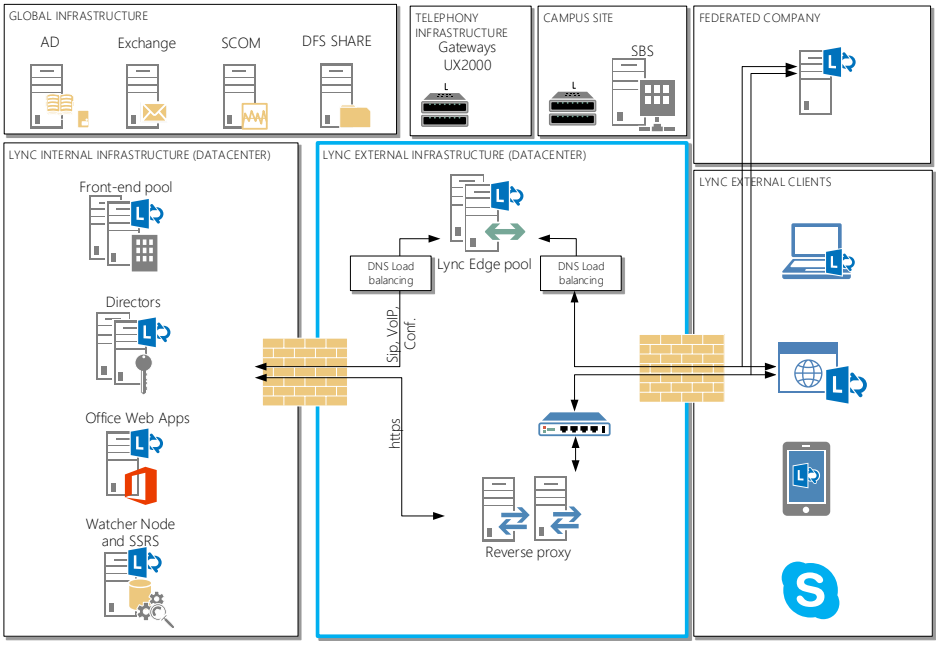

Figure 4.3: External infrastructure

4.3.3.3 System requirements

Type	#	CPU	RAM	Disk	Network
Front End	7	2x6 - 2,33GHz	32GB	2x300GB RAID1 6x300GB RAID10	1Gbps
Back End	2	2x6 - 2,33GHz	32GB	2x300GB RAID1 6x300GB RAID10 6x300GB RAID10	1Gbps
Witness	1	2x4 - 2,33GHz	8GB	2x146GB RAID 1	1Gbps
OWA	3	2x8 - 2,33GHz	16GB	2x300GB RAID1	1Gbps
Watcher node	1	4 2,33GHz	8GB	2x300GB RAID1	1Gbps
SBS	1	2x6 2,33GHz	32GB	2x300GB RAID1 2x300GB RAID1	1Gbps
Director	2	2x4 2,33GHz	16GB	2x300GB RAID1 2x300GB RAID1	1Gbps
Edge	2	2x4 2,33GHz	16GB	2x300GB RAID1 2x300GB RAID1	2x1Gbps

Table 4.5: System requirements

4.3.4 Telephony

This section describes the design of the telephony components of this implementation.

4.3.4.1 Overall Architecture

The telephony architecture is based on the main datacenter, and the campus site.

Datacenter

The datacenter hosts the mediation pool, which is collocated with the front end pool, and interconnects the Lync infrastructure with the ToIP network via the SONUS gateways and a SBC Acme Packet cluster, and with the PSTN via the SONUS gateways.

Contoso's ToIP network has some specificities requiring special consideration, for example only the G.729 ALaw codec is supported, as some equipments are incompatible with the G.729 BLaw codec. Moreover, some Aastra PBX only support the G.711 codec. This influenced the choice of the Sonus gateways, and their configuration.

Campus

Due to the requirements for the Campus site, the Microsoft recommendations and Contoso's preference, it was decided to install an SBS with gateways at the Campus site.

To increase call quality, media bypass should be activated for the Campus site.

4.3.4.2 Interconnection with the ToIP network

Two different scenarios were available for the interconnection with Contoso's ToIP network, differing in the location of the transcoding, the bandwidth used, call quality, ease of configuration and cost.

Interconnection via the local gateways In this scenario, the gateways at the Campus site connect directly to the SBC Acme Packet cluster.

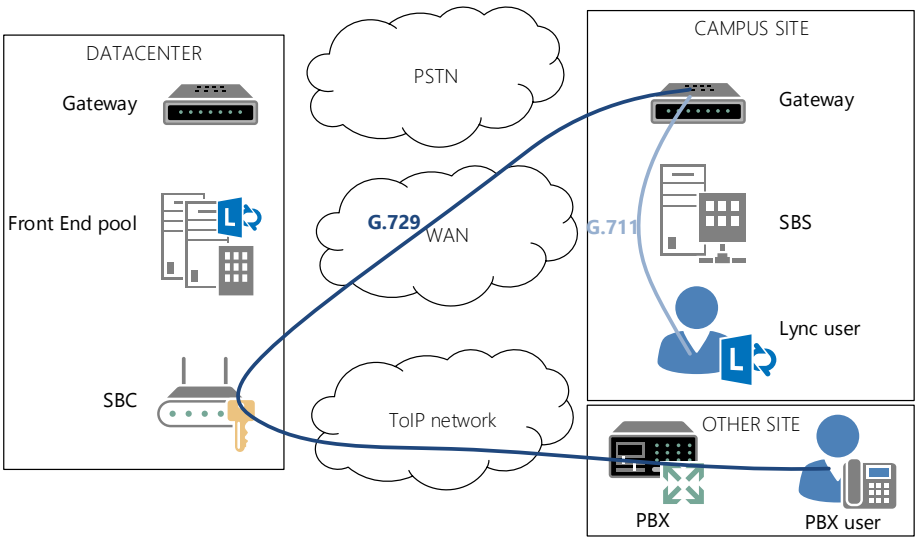

Figure 4.4: ToIP interconnection via the local gateways

Advantages	**Drawback**
The G.729 CODEC is used through the WAN, which requires less bandwidth than G.711	More complex as the SBC will be connected to all gateways, which will be more difficult to configure and maintain
The call quality should be better, as there is one node less and the G.711 CODEC is sure to be used before transcoding	More expensive as each local gateway will require SIP licenses
	No Call Admission Control possible

Table 4.6: Local interconnection advantages and drawbacks

Interconnection via the central gateways In this scenario, the gateways at the datacenter connect to the SBC Acme Packet cluster.

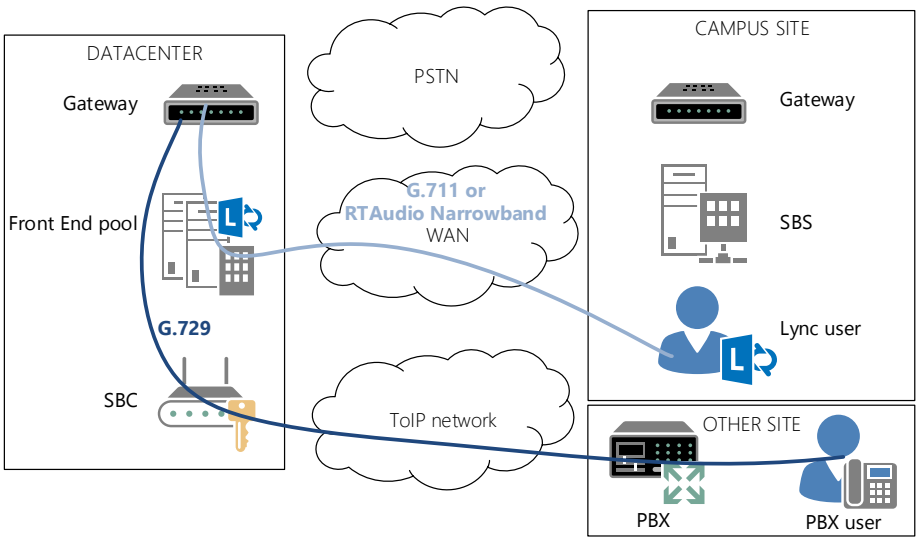

Figure 4.5: ToIP interconnection via the datacenter gateways

Advantages	**Drawback**
Simpler SBC configuration, and less load on the SBC	Using G.711 through the WAN requires more bandwidth
Cheaper as less SIP licenses are required	If the RTT is over 25ms, the RTAudio Narrowband CODEC will be used, which will degrade the call quality
Call Admission Control is possible	One more node is used, which can increase latency and reduce the call quality

Table 4.7: Datacenter interconnection advantages and drawbacks

As voice quality is an essential factor for the Campus site, and the RTT is not guaranteed to be under 25ms, the interconnection via the local gateways was chosen for this implementation.

4.3.4.3 Interconnection with the PSTN

The solution is interconnected with the PSTN from the datacenter and the Campus site, with each access serving different purposes.

Datacenter interconnection with the PSTN

This access serves 2 main purposes:

- access point for PSTN conference attendees.
- acces to the PSTN for users at a site without PSTN access

Between the PSTN and the front end pool, the G.711 codec is used, while between the front end pool and users from a site without PSTN access, the codec used can be either G.711 or RTAudio Narrowband if the RTT is above 25ms.

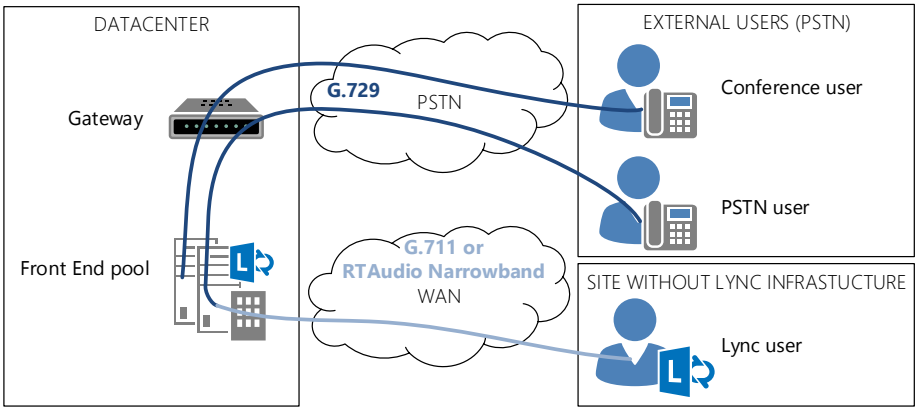

Figure 4.6: Datacenter interconnection with the PSTN

Campus interconnection with the PSTN

This access serves 2 main purposes:

- access point for PSTN conference attendees.
- acces to the PSTN for users at a site without PSTN access

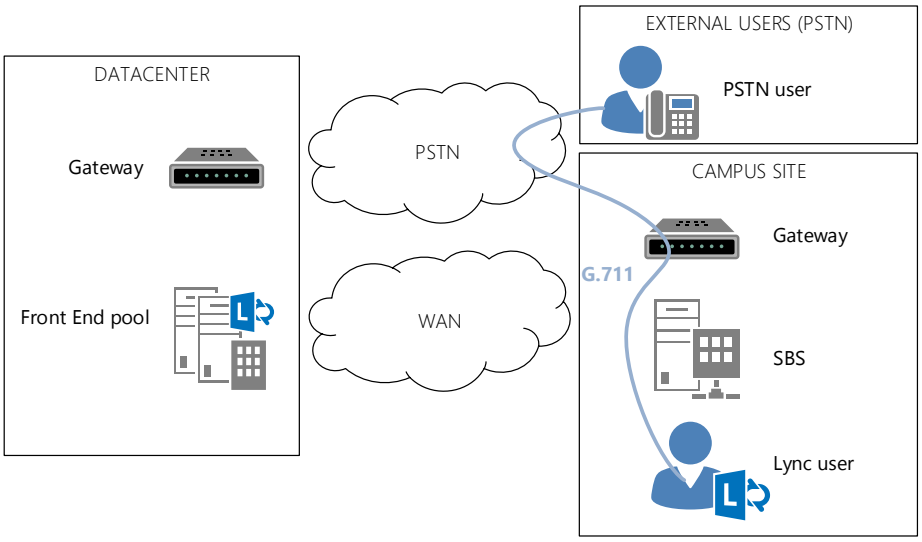

Figure 4.7: Campus interconnection with the PSTN

4.3.4.4 Sizing of the Sonus gateways

To appropriate sizing of the Sonus gateways was determined using usage provided by Contoso. According to this data, the relevant values are:

- 0.014 Erlang/user for PSTN calls
- 0.025 Erlang/user for inter-site calls from the Datacenter
- 0.03 Erlang/user for inter-site calls from branch sites

These values are lower than Microsoft's recommendation, but will be used for the sizing, as they reflect Contoso's usage. However, in case of increased usage, it will be possible to increase the capacity of the gateways easily.

For determining the number of lines required, we used the Erlang-B formula, with a maximum grade of service of 0.01 (When the usage is maximal, less than 1% of incoming calls can be blocked due to insufficient lines)[38].

Datacenter

Only 1,500 users will use the datacenter's gateways, the other 5,000 users will use their local site PSTN infrastructure for PSTN calls. The 1,500 users using the datacenter's gateways will use $1500 * 0.025 = 37.5E$ for calling other sites which requires 50 SIP circuits, as well as $1500 * 0.014 = 21E$ for PSTN calls, which requires 31 PSTN circuits.

The datacenter will be used by 6,500 users enabled for Enterprise Voice. The datacenter's gateways will handle PSTN traffic for audio conferences. Contoso states that conference calls amounts to a third of all regular calls, therefore audio conference will use $6500 * 0.025 * 1/3 = 54E$ which requires 68 SIP circuits, as well as 10 PSTN circuits.

Each gateway will use 118 SIP circuits, which requires 5 SIP modules (25 SIP licenses each), and 41 PSTN circuits, which requires 2 E1 cards (included with the UX2000-600 gateways).

Campus

The 1,250 Campus users enabled for Enterprise Voice will use $1250 * 0.014 = 17.5$ Erlang for PSTN calls and $1250 * 0.03 = 37.5$ Erlang for inter-site calls, which will require 27 PSTN circuits, which requires 2 SIP modules (25 SIP licenses each) and 1 two-E1-card module (included with the UX2000-200 gateways).

4.3.4.5 Mediation server role

If the Mediation server role is co-located on the Front End pool, each server is able to handle 150 concurrent calls. As there are 7 servers in the Front End pool, up to 1050 concurrent calls can be handled, which is a lot more than the number of available circuits on the datacenter gateways.

At the Campus site, the media bypass feature is activated, therefore the SBS will only be used during signalization, and the number of concurrent calls will be limited by the gateways.

The Lync infrastructure will be configured to use Mediation server redundancy so that the datacenter's Mediation servers will be used for Campus users' call signaling if the SBS is disabled.

4.3.4.6 Dialing and number manipulation

Phone numbers format

Microsoft recommends the use of numbers formatted according to the E.164 standard. Therefore, Lync users will have a phone number of the following form: +33ZABPQMCDU;ext=DDSCDU where

- DD is the site identifier (for example 38 for Campus)
- S is a subsite identifier (0 or 1 for Campus)
- CDU is the user line identifier

All contoso users have a 6 digits internal number. However, for users outside campus, there is not always a logical relation between their internal and external number. For example an user with the internal number 393202 can have the external number +33123451234 instead of +33123453202.

Because of this, it is impossible to create generic normalization rules.

Types of traffic

There are three types of telephony traffic possible, each involves a different number manipulation process.

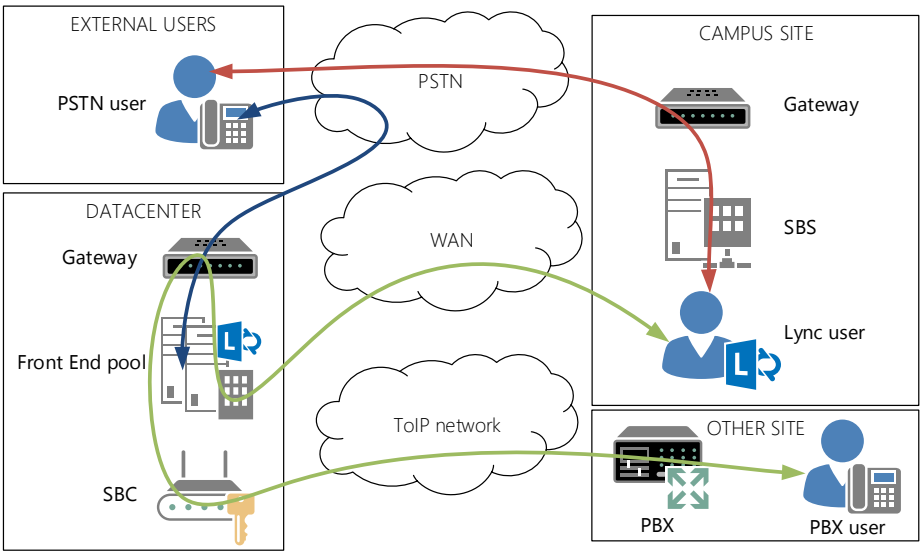

Figure 4.8: The three types of telephony traffic

PSTN to Lync

Called number Usually, the operator provides the last 4 digits of the called number. The Lync front end server translates this number to a E.164 number according to the dialplan corresponding to the gateway.

Caller number Can be either a national number (usually 9 digits), an international number (of variable length) or an anonymous number. If the number is national or international, the gateway translates it into an E.164 number.

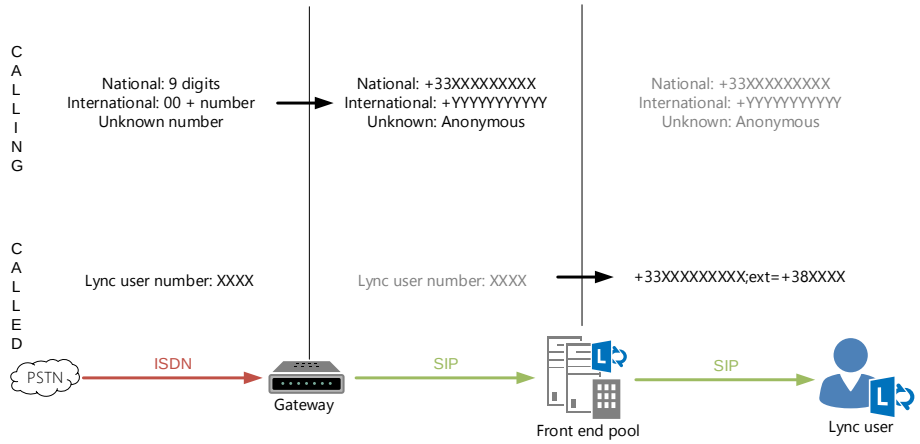

Figure 4.9: PSTN to Lync number manipulations

Lync to PSTN

Called number The Lync server does the translation before sending the number to the gateway.

Caller number The gateway translates the caller number from E.164 to a 9-digit number.

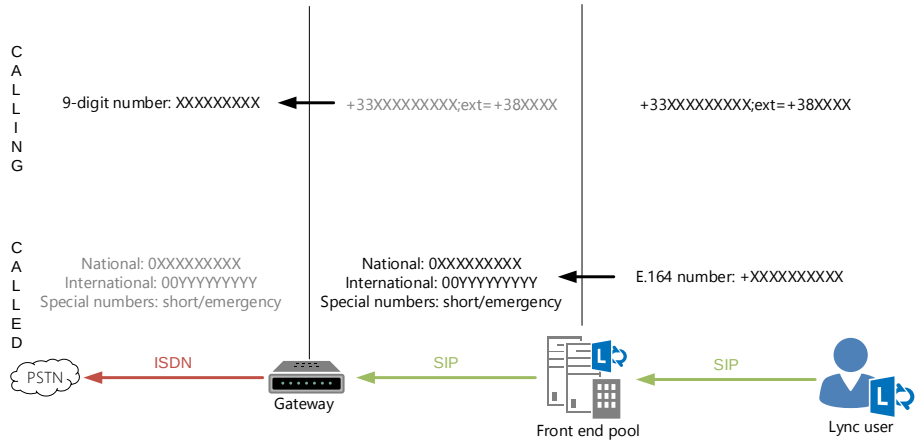

Figure 4.10: Lync to PSTN number manipulations

ToIP to Lync

Called number The SBC returns a 6-digit number. The Lync server translates the number to a E.164 number according to the datacenter's dialplan (as

only the datacenter's gateways are connected to the ToIP network).

Caller number The SBC returns a 6-digit number. There is no manipulation on this number. However this prevents the resolution of the caller id for missed calls.

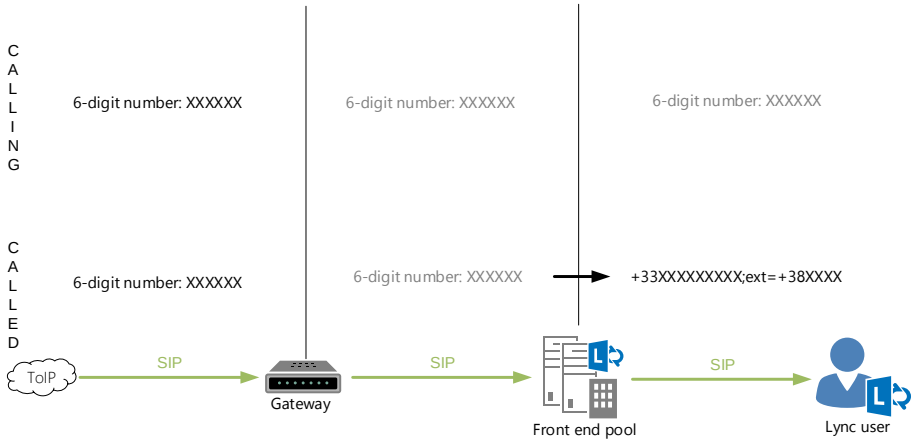

Figure 4.11: ToIP to Lync number manipulations

Lync to ToIP

Called number Most internal numbers are 3 or 6 digits numbers, but some have variable length. Therefore, the +0000 prefix has been chosen to identify internal number. This prefix is added by the Lync client. The Lync server removes and normalizes the number into a E.164 number, and the gateway translates the number into a 6 digit number.

Caller number The Lync client sends a E.164 number, which is translated into a 6 digit number by the gateway.

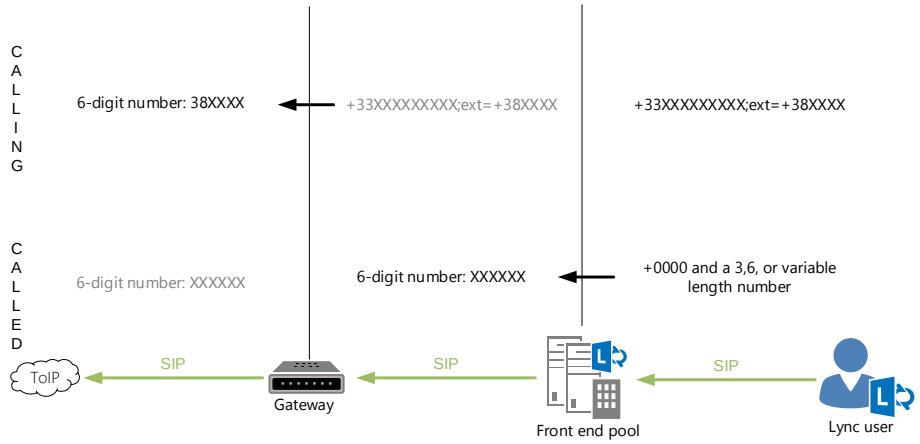

Figure 4.12: Lync to ToIP number manipulations

4.4 Deployment

This section describes the deployment of the implementation, and some of the challenges encountered.

4.4.1 Construction

The previously detailed implementation was deployed on Contoso's architecture in two steps:

Integration First Microsoft consultants setup the solution in the integration environment, and checked that the solution behaved as expected. Based on this implementation, some modifications to the design were made, and construction guides detailing the construction process were redacted. This purpose of this environment is to be able to make sure the solution is designed correctly, that the integration between the solution and others is operational, and that the installation process does not impact other services. Every new solution or update to a solution is applied in the integration environment before going into production.

Production Contoso's teams then deployed the solution in the production environment according to the construction guides. This allowed the Contoso team to familiarized themselves with the solution and ask specific questions about the design.

4.4.2 Testing

To ensure the solution behaved as expected and no mistake was during the design or construction phases, testing was an important part of the project. Different kinds of tests were realized, for different purposes:

Built-in tests Some tests are part of the installation scripts, and are run automatically during construction to validate that the prerequisite for installation are met, or that the previous step was successful. The installation of the Lync Server 2013 binaries includes many of these tests, to check that the AD domain and forest are correctly prepared or that all Lync components are correctly installed.

Unit tests Unit tests are run to validate that a particular component of the solution taken independently functions as intended. These tests include scripts running Lync synthetic tests cmdlets or checking the status or response of a component.

Integration tests These tests are run to validate that the interactions between different components or solutions are correct. Integration testing was crucial to validate the telephony features and identify and fix problems early.

Functional tests A functional test follows a user scenario to validate that the user experience is good. An example of a functional test would be creating a conference between Lync and HDX users, add video, share a document, invite a participant, then view the recording.

These tests were run at varying points and intervals during the construction:

During construction Some tests (automatic or manual) were run during the construction of the solution, between steps, to ensure that the prerequisites were met, prevent human error or identify differences between environments.

Regularly Some tests are run at regular interval (from 1 day to 1 week) to detect problems early, and ensure non regression during construction.

During the test phase For a construction phase (integration or production environment) to be validated, the solution has to pass all required tests at the same time. If some tests fail, corrections are made, and all tests are run again, until the results are acceptable.

4.4.3 Usage

The introduction of Lync to the new users was done in multiple steps. First, the solution was presented to users in internal events, showcasing some of the features and benefits of Lync, so that users can be more familiar with the solution in order to accept the change better.

In a second phase, some users were given access to Lync, first on a proof-of-concept infrastructure, then on the real infrastructure. Users were added in three successive groups, for a total of more than 500 users. The goal of this phase was to begin to test how Lync would be used and received by the users, as well as to train some users (the first users selected were in IT teams, and will have to provide support or administer the production solution) and increase adoption. This phase showed that Lync was well received by users, and more than 80% of users used Lync regularly during the test. However, some obstacles to Lync adoption were reported:

- A regular telephony solution was maintained during the test (for the first 2 waves)
- Not all users were using Lync (the best Lync usage was obtained when full teams were involved in the test)
- Some technical problems and missing features were reported on the proof-of-concept environment
- The training for test users was minimal and users were frustrated not to be able to perform some actions.

In the third phase, all future Campus users were given detailed FAQ sheets and procedures for the most common tasks, such as changing the profile picture, forwarding a call, or organizing and joining a conference. Users and administrators were also given specific training depending on their role, to ensure that users will know how to use the solution and avoid getting stuck on simple tasks when they move to Campus.

4.4.4 Difficulties

Almost all the problems encountered during this project has one of the following root causes:

Multiple teams involved As unified communications spans many domains, multiple teams had to work together on this project, belonging to different departments, such as IT, telephony or videoconferencing. At Contoso, these teams are not

used to working together, are located 400km apart and do not all have the same priorities and schedules. This caused a lot of planning problems, as all teams depended on others to advance, so a lot of time was spent waiting or coordinating teams.

It is worth remarking that a common problem with Lync deployments, which was not encountered at Contoso as the solution did not replace any existing service, is the reluctance of one or more of the involved teams, as Lync can move some of their responsibilities to other teams (usually telephony responsibilities going to IT).

Different design philosophy A recurrent problem was the difference between Lync's design philosophy and choices and the habits of users used to using classic telephony systems for years. Unlike telephony systems, Lync is design is "user-centric", so Lync is designed around the idea that users try to reach an user, and not a number. Therefore, some telephony features are less relevant in Lync, and were not included. Some of these features were introduced in the Lync Cumulative update 1 (such as call pickup) due to feedback from the early adoption program, but others features needed third party software (such as advanced delegation support).

Moreover, some situations encountered by Contoso were not included in Lync's design, such as their sites and regions layout, which might cause performance problems due to the complexity of the resulting dialplans and routing tables.

Some of these problems can be solved through user training, and the creation of new habits, but others will require modifications to the Lync client and server software.

Integration with components from other vendors The implementation had to interact with different systems, many of those from other vendors. Therefore there were some problems during construction, either because we depended on the vendor's support teams to install or configure equipment, or because of incompatibilities between Lync and the other vendor's equipment. For example, we had to wait for Polycom's updates to connect their products to the implementation, and the direct connection between Lync and a VSX still requires a update that has not yet been released.

Chapter 5

Conclusions and Future Work

5.1 Telephony with Lync 2013

This master's thesis project demonstrated that Lync 2013 can be en effective solution for multiple purposes, including a complete telephony replacement.

This project also helped providing data and feedback about Lync server 2013. This led to two upgrade requests to the product development team (improvements to the call delegates features and to the call routing) and some of the data was used to redact the reference documents for deploying Lync Server 2013.

The project also showed that although technical problems can arise during the construction of an unified communications solutions based on Lync, most problems, and the most critical problems are organizational problems, or problems that can be resolved through the analysis of the users' needs and user training.

5.2 Future Work

5.2.1 Contoso's implementation

This implementation can still be improved, by adding the edge features that were cut due to the time constraint, which will allow external connections and federations scenarios. It's also possible to consider the addition of the other remote sites, and their particular needs. Another aspect that was left out of this project is a complete backup/restore, disaster recovery and PSTN access redudancy plan.

5.2.2 Lync and Unified Communications

Some aspects of Lync were not studied in this project, and might be of interest, such as the integration of the Lync 2013 client, or the use of Lync as a platform for more complex applications, such as a call-center, with the use of the Lync APIs.

A more in-depth study of Lync's network usage, including QoS and CAC impact would be helpful in determining precisely the right network sizing for future implementations.

5.3 Reflections

This master's thesis project is the design and construction of an unified communication solution, used for instant messaging, conferencing and telephony. Unified communications solutions can have a variety of positive consequences for companies, but other effects may require further reflection or attention when planning an unified communications solution.

One the most common cause of concern for employees when an unified communications solution is introduced in the workplace is due to the presence indicator, which is a central part of all UC solutions. Employees fear that this feature can be used to track their worktime, their activity, or their communications. Moreover, if UC solutions can help remote workers, it can also lead to the employees being asked to stay connected and available for work all the time, even outside the workplace. These practices are usually controlled by legislation.

UC solutions can also pose a threat to the safety of people if not planned correctly, as UC solutions can be used for calling emergency number, but do not automatically provide the same services, such as location information. There are a variety of solutions to this problem, from configuring the UC solution to include location information to disabling emergency calling on UC phones and instructing users to call from an emergency phone, or cell phone.

Bibliography

[1] Elizabeth Harrin, "Unified communications 101: Intro to UC," Apr. 2013, retrieved 2013-06-18. [Online]. Available: http://www.enterprisenetworkingplanet.com/unified_communications/unified-communications-101-intro-to-uc.html

[2] A. Fikry and Z. A. Ghani@Mukhtar, "Unified communication: it's all between you and me," *Business Strategy Series*, vol. 13, no. 4, pp. 168–172, 2012. doi: 10.1108/17515631211246230. [Online]. Available: http://www.emeraldinsight.com.focus.lib.kth.se/journals.htm?articleid=17042088&show=abstract

[3] K. Riemer and S. Taing, "Unified communications," *Business & Information Systems Engineering*, vol. 1, no. 4, pp. 326–330, Jun. 2009. doi: 10.1007/s12599-009-0062-3. [Online]. Available: http://rd.springer.com/article/10.1007%2Fs12599-009-0062-3

[4] B. Pleasant, "What UC is and isn't," Jul. 2008, retrieved 2013-01-24. [Online]. Available: http://searchunifiedcommunications.techtarget.com/feature/What-UC-is-and-isnt

[5] W. McKnight, "Mobile business intelligence: When mobility matters," MicroStrategy, Tech. Rep., 2011.

[6] M. Parker, "A short history of UC - unified communications strategies," Jul. 2009, retrieved 2013-01-24. [Online]. Available: http://www.ucstrategies.com/unified-communications-strategies-views/a-short-history-of-uc.aspx

[7] R. Gray, "The 1974 origins of VoIP," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 87–90, 2005. doi: 10.1109/MSP.2005.1458295

[8] J. Hallock, "A brief history of VoIP," University of Washington, Washington, Tech. Rep., Nov. 2004.

[9] Infonetics Research, "Infonetics: $377 billion to be spent on VoIP and UC services over next 5 years," Oct. 2012. [Online]. Available: http://www.infonetics.com/pr/2012/VoIP-UC-Services-Market-Highlights.asp

[10] S. S. R. Ahamed, *Comprehensive Performance Analysis of Unified Communications Technology*, ser. Journal of Theoretical and Applied Information Technology, 2008. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.208.5250

[11] M. Desantis, "Understanding voice over internet protocol," US-CERT, Tech. Rep., 2008. [Online]. Available: http://www.us-cert.gov/cas/tips/ST05-018.html

[12] K. Peternel, L. Zebec, and A. Kos, "Using presence information for an effective collaboration," in *6th International Symposium on Communication Systems, Networks and Digital Signal Processing, 2008. CNSDSP 2008*, Jul. 2008. doi: 10.1109/CSNDSP.2008.4610766 pp. 119 –123.

[13] H. Schulzrinne, "The SIMPLE presence and event architecture," in *First International Conference on Communication System Software and Middleware, 2006. Comsware 2006*, 2006. doi: 10.1109/COMSWA.2006.1665181 pp. 1 –9.

[14] H. J. Wang and R. H. Katz, "Mobility support in unified communication networks," in *Proceedings of the 4th ACM international workshop on Wireless mobile multimedia*, ser. WOWMOM '01. New York, NY, USA: ACM, 2001. doi: 10.1145/605991.606004. ISBN 1-58113-384-7 pp. 95–102. [Online]. Available: http://doi.acm.org/10.1145/605991.606004

[15] C. Banner, "Understanding unified messaging," *IT Professional*, vol. 12, no. 1, pp. 40 –45, Feb. 2010. doi: 10.1109/MITP.2010.38

[16] A. Arumugam Mathivanan, "MiniSIP as a plug-in," Master's thesis, KTH, Communication Systems, CoS, Stockholm, Sweden, Nov. 2012, TRITA-ICT-EX 2012:247. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-104646

[17] "Avaya company overview," Nov. 2012, retrieved 2013-06-17. [Online]. Available: http://www.avaya.com/usa/about-avaya/our-company/company_overview/company-overview

[18] "Cisco corporate overview and resources - the network: Cisco's technology news site," retrieved 2013-06-17. [Online]. Available: http://newsroom.cisco.com/overview

[19] Microsoft TechNet, "Phones and devices qualified for microsoft lync," 2013, retrieved 2013-06-17. [Online]. Available: http://technet.microsoft.com/en-us/lync/gg278164.aspx

[20] E. Carrara, *Security for IP multimedia applications over heterogeneous networks*, ser. Trita-IMIT-LCN. AVH. KTH, Microelectronics and Information Technology, IMIT, 2005, no. 05:01, QC 20101125.

[21] G. Talaganov, "Green VoIP : A SIP based approach," Master's thesis, KTH, Communication Systems, CoS, Stockholm, Sweden, Jul. 2012, TRITA-ICT-EX 2012:162. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-98795

[22] J. Postel, "Internet Protocol," RFC 791 (INTERNET STANDARD), Internet Engineering Task Force, Sep. 1981, updated by RFCs 1349, 2474. [Online]. Available: http://www.ietf.org/rfc/rfc791.txt

[23] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460 (Draft Standard), Internet Engineering Task Force, Dec. 1998, updated by RFCs 5095, 5722, 5871, 6437, 6564. [Online]. Available: http://www.ietf.org/rfc/rfc2460.txt

[24] Y. Bentahar, *DNS performance*, ser. Trita-ICT-EX. KTH, School of Information and Communication Technology (ICT), 2013, no. 2013:2.

[25] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246 (Proposed Standard), Internet Engineering Task Force, Aug. 2008, updated by RFCs 5746, 5878, 6176. [Online]. Available: http://www.ietf.org/rfc/rfc5246.txt

[26] E. Rescorla, *SSL and TLS: Designing and Building Secure Systems*, 1st ed. Addison-Wesley Professional, Oct. 2000. ISBN 0201615983

[27] K. Zeilenga, "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," RFC 4510 (Proposed Standard), Internet Engineering Task Force, Jun. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4510.txt

[28] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service (V5)," RFC 4120 (Proposed Standard), Internet Engineering Task Force, Jul. 2005, updated by RFCs 4537, 5021, 5896, 6111, 6112, 6113, 6649, 6806. [Online]. Available: http://www.ietf.org/rfc/rfc4120.txt

[29] L. Zhu and B. Tung, "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)," RFC 4556 (Proposed Standard), Internet Engineering Task Force, Jun. 2006, updated by RFC 6112. [Online]. Available: http://www.ietf.org/rfc/rfc4556.txt

[30] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261 (Proposed Standard), Internet Engineering Task Force, Jun. 2002, updated by RFCs 3265, 3853, 4320, 4916, 5393, 5621, 5626, 5630, 5922, 5954, 6026, 6141, 6665. [Online]. Available: http://www.ietf.org/rfc/rfc3261.txt

[31] I. Dalgic and H. Fang, "Comparison of h.323 and SIP for IP telephony signaling," in *Multimedia Systems and Applications*, vol. 3845, 1999, p. 106–122.

[32] P. Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Core," RFC 6120 (Proposed Standard), Internet Engineering Task Force, Mar. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6120.txt

[33] Alan Murphy, "Virtualization defined - eight different ways," F5, Tech. Rep., Feb. 2008. [Online]. Available: http://www.f5.com/pdf/white-papers/virtualization-defined-wp.pdf

[34] Peter Mell and Timothy Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, Gaithersburg, Tech. Rep. Special Publication 800-145, Sep. 2011.

[35] K. Nichols, S. Blake, F. Baker, and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," RFC 2474 (Proposed Standard), Internet Engineering Task Force, Dec. 1998, updated by RFCs 3168, 3260. [Online]. Available: http://www.ietf.org/rfc/rfc2474.txt

[36] R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: an Overview," RFC 1633 (Informational), Internet Engineering Task Force, Jun. 1994. [Online]. Available: http://www.ietf.org/rfc/rfc1633.txt

[37] W. Stallings, *Cryptography and network security: principles and practice*, 2014. ISBN 9780133354690 0133354695

[38] S. Qiao and L. Qiao, "A robust and efficient algorithm for evaluating erlang's formula," Ph.D. dissertation, McMaster University, Oct. 1998.

[39] "Code pénal - article 226-15: De l'atteinte au secret des correspondances."

[40] "Loi n° 91-646 du 10 juillet 1991 - article 1."

[41] "Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique."

[42] "Cour de cassation chambre sociale arrêt du 15 décembre 2010." [Online]. Available: http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3061

[43] "Code de commerce - article l110-4."

[44] "Code de la consommation - article l134-2." [Online]. Available: http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=73D83D8C410F4714C03C1965BDA9EBEA.tpdjo04v_1?cidTexte=LEGITEXT000006069565&idArticle=LEGIARTI000006292189&dateTexte=20130905&categorieLien=id#LEGIARTI000006292189

[45] "The sarbanes-oxley act 2002." [Online]. Available: http://www.soxlaw.com/

[46] "LOI n° 2005-842 du 26 juillet 2005 pour la confiance et la modernisation de l'économie," 2005.

[47] "VoIP and 911 service | FCC.gov." [Online]. Available: http://www.fcc.gov/guides/voip-and-911-service

[48] ARCEP, "Réseaux locaux radioélectriques ou RLAN (wi-fi) : les puissances d'émissions autorisées." [Online]. Available: http://www.arcep.fr/index.php?id=9272#c12931

[49] M. I. Showcase, "Deploying lync server 2010," Microsoft Corporation, Technical White Paper, Dec. 2011.

[50] Microsoft TechNet, "Microsoft lync server 2013," Jan. 2013, retrieved 2013-02-05. [Online]. Available: http://technet.microsoft.com/en-us/library/gg398616.aspx

[51] M. I. Showcase, "Disaster recovery and business continuity planning in action: Japan 2011," Microsoft Corporation, Technical White Paper, Jul. 2011. [Online]. Available: http://www.microsoft.com/en-us/download/details.aspx?id=26680

[52] B. Desmond, J. Richards, R. Allen, and A. G. Lowe-Norris, *Active Directory: Designing, Deploying, and Running Active Directory, Fourth Edition*, fourth edition ed. O'Reilly Media, Dec. 2008. ISBN 059652059X

[53] D. Holme, N. Ruest, D. Ruest, and J. Kellington, *Self-Paced Training Kit (Exam 70-640): Configuring Windows Server 2008 Active Directory*, second edition ed. Microsoft Press, Jul. 2011. ISBN 0735651930

[54] T. Redmond, *Microsoft® Exchange Server 2010 Inside Out*. Microsoft Press, Nov. 2010. ISBN 978-0-7356-4061-0. [Online]. Available: http://shop.oreilly.com/product/0790145300898.do

[55] G. Husman and C. Ståhl, *Beginning SharePoint 2010 Administration: Windows SharePoint Foundation 2010 and Microsoft SharePoint Server 2010*, 1st ed. Wrox, Jun. 2010. ISBN 0470597127

[56] N. Winters and K. Hanna, *Mastering Microsoft Lync Server 2010*, 1st ed. Sybex, Feb. 2012. ISBN 1118089537

[57] Microsoft TechNet, "Lync web app supported platforms," Apr. 2013. [Online]. Available: http://technet.microsoft.com/en-us/library/gg425820.aspx

[58] ——, "Lync 2013: Server roles," Jan. 2013, retrieved 2013-02-05. [Online]. Available: http://technet.microsoft.com/en-US/library/gg398536(v=ocs.15)

[59] ——, "Sites," Oct. 2012. [Online]. Available: http://technet.microsoft.com/en-us/library/gg398076.aspx

[60] ——, "Dial plans and normalization rules," Sep. 2012. [Online]. Available: http://technet.microsoft.com/en-us/library/gg413082.aspx

[61] ——, "Common security threats in modern day computing," Sep. 2013. [Online]. Available: http://technet.microsoft.com/en-us/library/dn433220.aspx

[62] V. Schuppan and W. Russwurm, *A CMM-Based Evaluation of the V-Model 97*, 2000.

[63] J. Sheffield, "Systemic knowledge and the v-model," *Int. J. Business Information Systems*, vol. 1, no. 1/2, 2005.

[64] Microsoft TechNet, "Lync server 2013 user models," 2013, retrieved 2013-05-27. [Online]. Available: http://technet.microsoft.com/en-us/library/gg398811.aspx

[65] “OpenTrust.” [Online]. Available: http://www.keynectis.com/

TRITA-ICT-EX-2013:230

www.kth.se