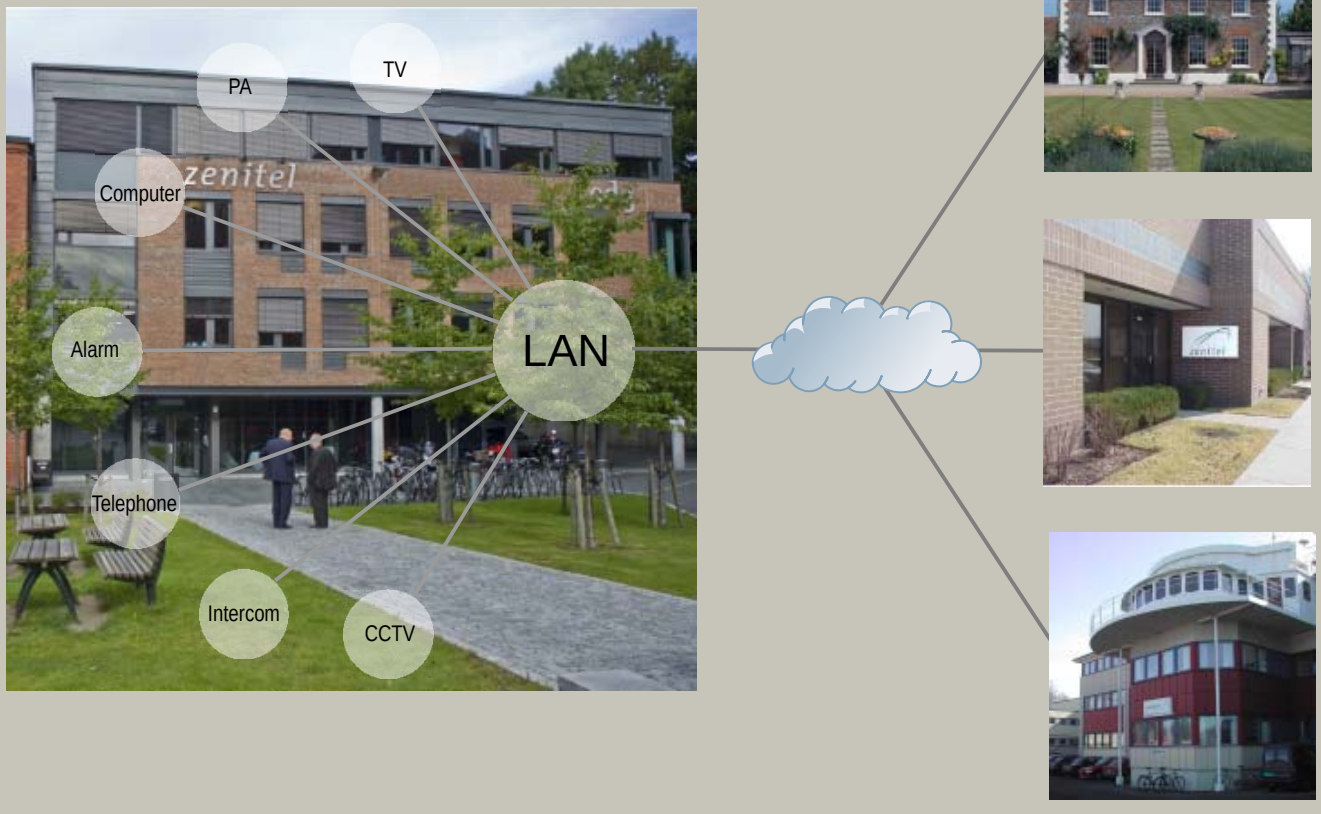
Deploy AlphaCom XE

Analyzing impact on IP infrastructure

STENTOFON



NETWORK DESIGN

A100K10313 v.1.2

06.02.2012

Publication log

Version	Date	Modifications
1.0	2006.05.18	First issue, complete
1.1	2009.04.15	New front and back, no change in text.
1.2	2012.02.06	Updated to AlphaCom XE

Zenitel Norway AS and its country offices assume no responsibilities for any errors that may appear in this publication, or for damages arising from the information in it. No information in this publication should be regarded as a warranty made by Zenitel Norway AS.

The information in this publication may be updated or changed without notice. Product names mentioned in this publication may be trademarks; they are used only for identification.

Zenitel Norway AS, May 2006

Table of Contents

All rights reserved. Note that the content in this document is protected under copyright law. No part of this document may be reproduced or transmitted in any form or by any means, electronic mechanical, photocopying, recording, or otherwise, without the prior written permission of Zenitel Norway AS.

For information contact Zenitel Norway AS marketing dept.

1 Introduction

1.1 AlphaCom and IP

The STENTOFON AlphaCom is recognized for its unique capabilities, meeting all communication and security needs in demanding environments. It has proved to be extremely efficient when used in networks for industrial complexes, health care institutions, prisons and jails, financial institutions, transportation providers, high security buildings, vessels, oil platforms and other areas where communication and security is of vital importance.

The AlphaCom system is developed, produced and marketed by Zenitel, a world leading supplier of critical communication systems worldwide. Our products satisfy customer needs that include security and timecritical communications. We're proud of our reputation of having the most flexible, reliable and superior quality hands-free communication systems today. The AlphaCom XE is the latest version in an evolutionary process where backward compatibility combined with using new IP-technologies has always been the main driving force.
As a result the AlphaCom XE offers completely new ways of improving your internal communication and security solutions.

The AlphaCom XE combines the best of an advanced communications server with the latest IP, Linux and embedded networking technologies. The AlphaCom XE provides a complete set of services, quality, reliability and security characteristics for which AlphaCom has always been recognized. Some of the special features it brings into the IP domain are wideband (7 KHz) audio, a built-in firewall, integrated web server, and low latency switching.
In addition to these important characteristics, a new set of innovative services have been introduced to improve cost efficiency, service capabilities and system operation.
The AlphaCom XE provides full backward compatibility with even the earliest AlphaCom exchanges meaning that if you are already using an AlphaCom, you can continue to use the existing equipment, thereby capitalizing on equipment and competence. It is up to you to decide on the mix of new generation IP stations and services and traditional stations and services.

1.2 Scope of document

This document details the different considerations in implementing and deploying a network of AlphaCom XE exchanges over an IP network. It is divided into three main chapters:

Basics of IP

The chapter *Basics of IP* introduces you to basic concepts of IP networks. Topics such as security and quality of service are given special attention in order to get a better understanding of how to provide Critical Communication over IP.

AlphaCom XE and IP

The chapter *AlphaCom XE and IP* describes the different IP services and capabilities supported by the AlphaCom XE system.

Deployment Guideline

The chapter *Deployment Guideline* walks you through a set of steps for deploying an AlphaCom XE solution.

2 Basics of IP

2.1 Introduction to IP Networks

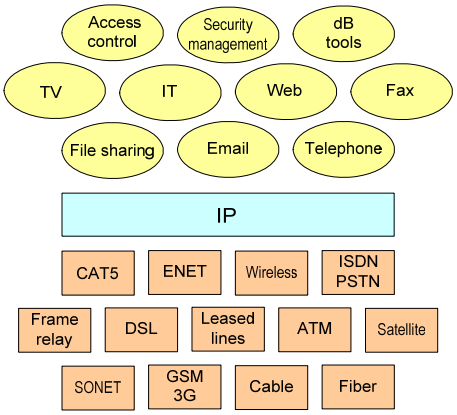


Figure 1 Any service over any infrastructure

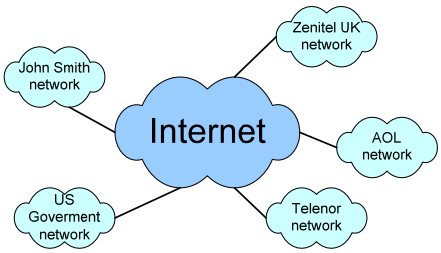


Figure 2 Network of networks

2.1.1 Overview

Any service over any infrastructure

IP is the technology of choice for voice networking, operation and maintenance and integration of 3rd party applications, providing communication for services such as web, email, file sharing, telephony, TV, logging, administration and CCTV.

IP works over many types of network infrastructure such as DSL, Cat5, Ethernet, optical, wireless, ATM, frame relay, satellite, leased lines and ISDN to name a few. We are clearly going towards an all IP world where IP provides support *for any service over any infrastructure*.

Network of networks

The IP (Internet Protocol) provides the capability of linking networks together, having a network of networks. The growth of Internet can in a large degree be attributed to the ability to link networks together to form larger networks. The Internet is in fact a huge number of networks that are inter-linked as shown in Figure 2.

The capabilities of linking networks and providing 'any service over any infrastructure' have made IP available everywhere.

Inter-linked with the Internet there are also a huge number of private IP networks such as home, school and corporate networks. These networks are usually referred to as Intranets.

Definition Intranet

Intranet is the generic term for a collection of private data networks within an organization. Many schools and non-profit groups have deployed intranets, but an intranet is still seen primarily as a corporate productivity tool.

The different networks within an Intranet are categorized as different type of "area networks". The main types of area networks are the Local Area Network (LAN) and the Wide Area Network (WAN).

This chapter will focus on LANs and WANs as these are the networks where Critical Communication over IP is usually deployed.

2.1.2 Wide Area Networks (WAN)

WAN - a definition

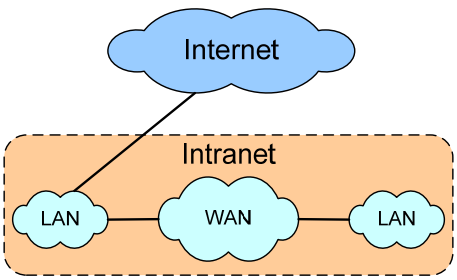


Figure 3 Example Intranet

A wide area network (WAN) spans a large geographic area, such as a state, country or even multiple countries.

WANs normally connect multiple LANs and other smaller-scale area networks. In the example in Figure 3, the WAN joins LANs in two remote locations.

WANs differ from LANs in several important ways.

WANs generally utilize different and much more expensive networking equipment and infrastructures than LANs do. Due to the higher cost of providing data connectivity in the WAN, the WAN usually carries significantly lower data bandwidth than a LAN. Bandwidth is thus a much more scarce resource in the WAN.

A corporation will therefore put much more consideration in management of the bandwidth in the WAN. The corporations have several options for implementing their Wide Area Network. When implementing the WAN service the company needs to evaluate their

need for bandwidth, security, quality of service as well as what they are willing to pay for the service. We will go through these factors when discussing the main implementation options that are:

- Leased or dedicated line infrastructure
- Outsourced to Internet Service Providers (ISP)
- Virtual Private Networks (VPN)

Leased or dedicated lines

Traditionally an organization that wanted to build a wide-area network needed to procure expensive, dedicated lines to connect their offices together. Only large companies could afford to purchase these lines outright, so most organizations leased their lines and paid a monthly charge, sometimes thousands of dollars, for the privilege of using cables that no one else could tap into.

On top of the dedicated line infrastructure, the companies built their WAN data network using technologies such as frame relay, ATM and X.25. This gives the corporations full control of the management and operation of the complete WAN.

Due to its high costs, many companies are moving away from having the WAN based on dedicated and leased lines. Often they can reduce their networking cost more than 75% by outsourcing their WAN or utilizing VPN.

Note! In the recent years, optical Ethernet has entered the WAN arena. Optical Ethernet is a very good option; corporations that own fiber as Ethernet provide huge bandwidth at relatively low costs.

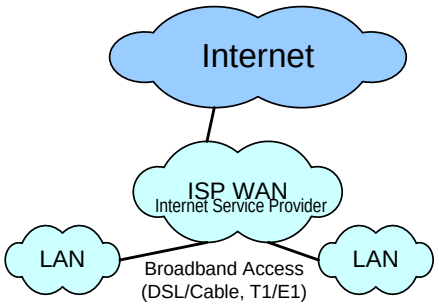


Figure 4 Internet service providers

Outsourced to Internet Service Providers (ISP)

A company can buy an end-to-end WAN service from an Internet Service Provider (ISP). The company then only needs to have a router joining the LAN to the WAN link maintained by the ISP.

Today most ISPs will be able to offer several levels of service on the WAN links. This is defined in the service level agreement (SLA). When going through the SLA with the ISP, the company carefully needs to evaluate their needs for network availability, bandwidth availability, security, IP QoS, response time on failures and what they are willing to pay for the service. Normally an outsourced WAN service will cost 50% less than a leased line infrastructure

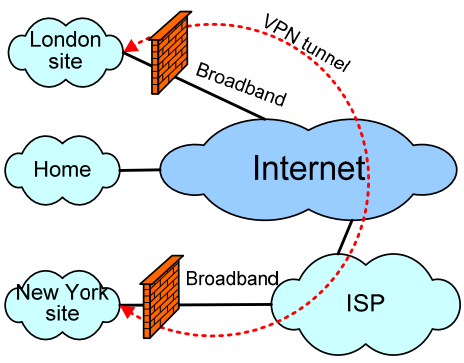


Figure 5 Virtual Private Network

VPN

Virtual Private Network (VPN) provides the most cost efficient way of implementing a WAN. The key feature of a VPN is its ability to use public networks like the Internet rather than rely on private leased lines to carry the data traffic.

VPNs promise two main advantages over competing approaches - cost savings, and scalability

The low cost of a VPN

One way a VPN lowers costs is by eliminating the need for expensive long-distance leased lines. With VPNs, an organization needs only a relatively short dedicated connection to the internet. This connection could be a local leased line (much less expensive than a long-distance one), or it could be a local broadband connection such as a DSL service.

Scalability and VPNs

The cost to an organization of traditional leased lines may be reasonable at first but can increase exponentially as the organization grows. A company with two branch offices, for example, can deploy just one dedicated line to connect the two locations. If a third branch office

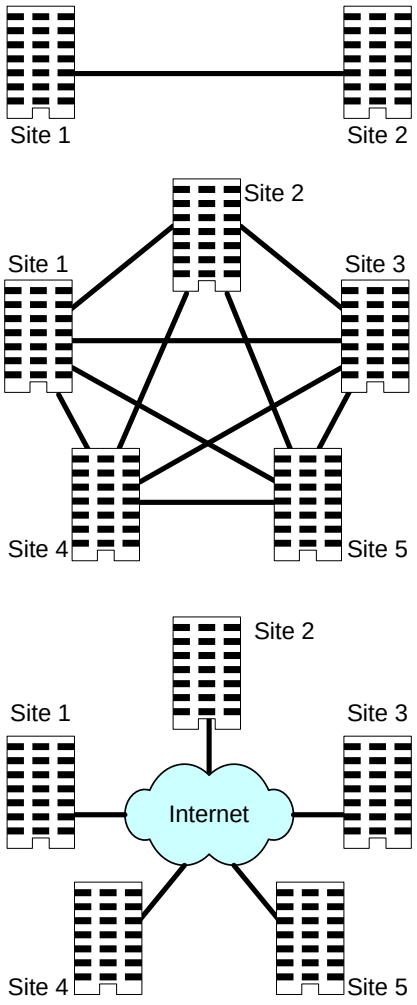


Figure 6 Combinatorial explosion

needs to come online, just two additional lines will be required to directly connect that location to the other two.

However, as an organization grows and more companies must be added to the network, the number of leased lines required increases dramatically. Four branch offices require six lines for full connectivity; five offices require ten lines, and so on. Mathematicians call this phenomenon a "combinatorial explosion," and in a traditional WAN this explosion limits the flexibility for growth. VPNs that utilize the Internet avoid this problem by simply tapping into the geographically-distributed access already available.

Compared to leased lines, Internet-based VPNs offer greater global reach, given that Internet access points are accessible in many places where dedicated lines are not available.

Disadvantages of VPNs

With the hype that has surrounded VPNs historically; the potential pitfalls or "weak spots" in the VPN model can be easy to forget. These two concerns with VPN solutions are often raised.

1. VPNs require an in-depth understanding of public network security issues and taking proper precautions in VPN deployment.

2. The availability and performance of an organization's wide-area VPN depends on Internet. Internet has up till now shown a relative high availability. However, performance factors such as congestion, packet loss, and variable delays are often experienced.

VPN technology

VPN technology is based on the idea of tunneling. Network tunneling involves establishing and maintaining a logical network connection. On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side. VPN protocols also support authentication and encryption to keep the tunnels secure.

Several interesting network protocols have been implemented specifically for use with VPN tunnels. The three most popular VPN tunneling protocols listed below continue to compete with each other for acceptance in the industry. These protocols are generally incompatible with each other.

- IPSec
- L2TP
- Point-to-Point Tunneling Protocol (PPTP)

Note! Only the IPSec protocol provides encryption. This is the only VPN protocol that is recommended to use over Internet.

Critical communication over VPN

VPN provides a very cost efficient way of implementing a WAN service, However, as VPN cannot guarantee a 99.999 % network and bandwidth availability in the Internet, care and consideration should be taken on the criticality on bandwidth availability for the services using the VPN service.

It is possible to build an Intercom over IP service over a VPN WAN link. This will provide a very cost effective solution. As bandwidth availability is not guaranteed and packet loss delay may vary, VPN is not suited for critical communication that must always work. However, if the service can live with 99% availability VPN is a good choice.

2.1.3 Local Area Networks (LAN)

LAN - a definition

A Local Area Network (LAN) supplies connectivity to a group of computers in close proximity to each other such as in an office building, a school or a home.

A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs, and occasionally a LAN will span a group of nearby buildings.

Besides operating in a limited space, LANs include several other distinctive features. LANs are typically owned, controlled, and managed by a single person or organization. They also use certain specific connectivity technologies, primarily Ethernet.

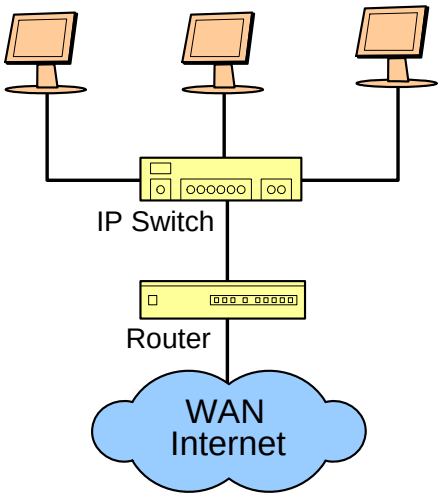


Figure 7 Small LAN

Small LAN

A small LAN is relatively easy to implement. A small LAN (up to 16 data users) consists of the following equipment:

- **IP switch**
  The IP switch provides IP connectivity between the data equipment on the LAN. In a small LAN an unmanaged router can be used. These switched are plug-and-play, meaning that data equipment only need to be plugged to the switch to work, no configuration is needed.
- **Router**
  The router connects the LAN switch to the WAN or Internet. Small routers usually have configuration wizards, guiding you through the needed configuration.

Large LAN

Larger LAN's are more complex to implement. When implementing a larger LAN it is usual to divide the implementation in a physical structure and a logical structure.

LAN physical structure

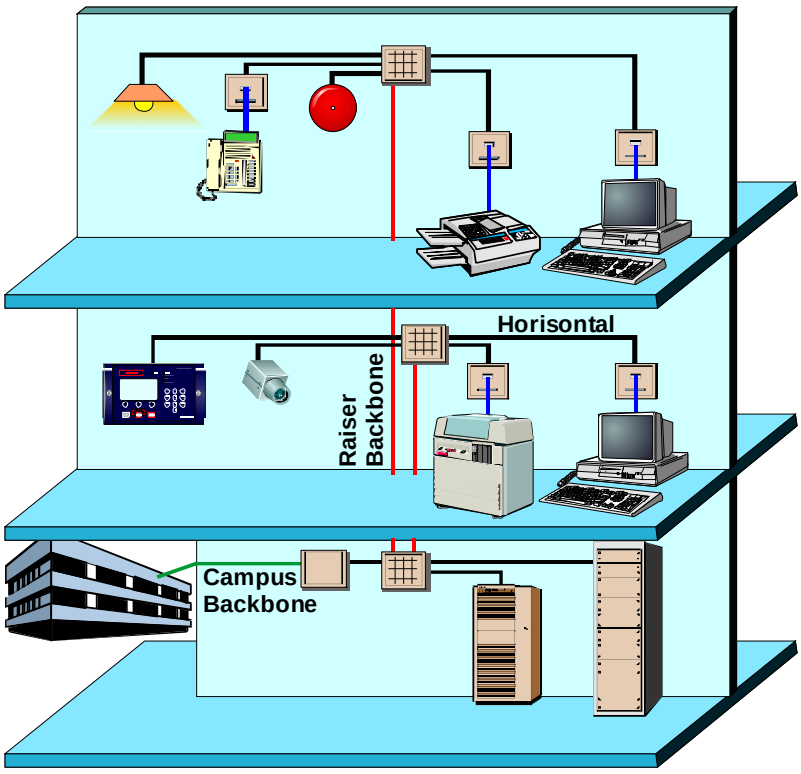


Figure 8 Structured cabling

Today buildings are usually cabled using a structured cabling system (See reference 1). A structured cabling system is a standard for cable design. The main concept of structured cabling is to have a standard cabling infrastructure that can be used for the data network, the telephony network and the building management.

In a structured cabling system each RJ45 outlet on the same floor or building wing is star cabled back to a patch panel using a four pair copper cable (CAT5-7). It is usual to have fiber cable between the different patch panels in the building or to neighboring buildings.

The LAN infrastructure consists of a core network and a workgroup network. These two networks utilize the structured cabling system. The workgroup network provides connectivity in the different floors. The data switching is provides by a Workgroup Ethernet Switch that connects the access points on the patch panel and the core network.

Note! Today the Workgroup Switches can provide power distribution in addition to data connectivity functions. They provide power over Ethernet. Power over Ethernet reduces the need for separate power adaptors for equipment such as IP telephones, WiFi routers, CCTV cameras as well as providing the capability to have UPS backup power for these devices.

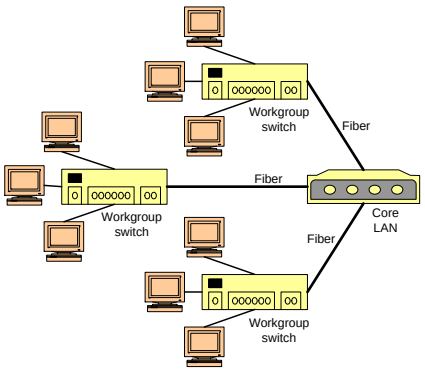


Figure 9 Physical LAN

The core network provides high bandwidth data connection between the different workgroups and it is implemented with core Ethernet switches and fiber links.

Virtual LANs - logical structure

A VLAN is a logical subgroup within a local area network that is created via software rather than manually moving cables in the wiring closet. It combines user stations and network devices into a single unit regardless of the physical LAN segment they are attached to.

There are several benefits to using VLANs. To summarize, VLAN architecture benefits include:

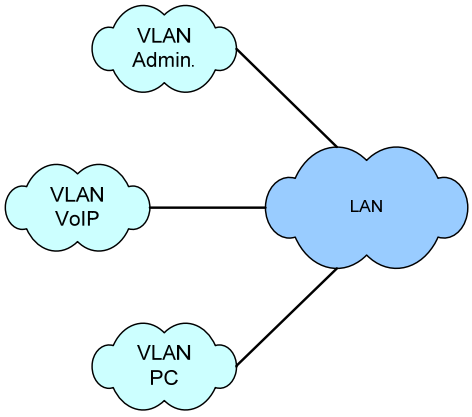


Figure 10 Logical setup

- **Increased performance.**
  Grouping users into logical networks will also increase performance by limiting broadcast traffic to users performing similar functions or within individual workgroups. Additionally, less traffic will need to be routed, and the latency added by routers will be reduced.
- **Improved manageability.**
  VLANs provide an easy, flexible, less costly way to modify logical groups in changing environments. VLANs make large networks more manageable by allowing centralized configuration of devices located in physically diverse locations.
- **Network tuning and simplification of software configurations.**
  VLANs will allow LAN administrators to "fine tune" their networks using priority and bandwidth allocation schemes between VLANs
- **Physical topology independence.**
  VLANs provide independence from the physical topology of the network by allowing physically diverse workgroups to be logically connected within a single broadcast domain. If the physical infrastructure is already in place, it now becomes a simple matter to add ports in new locations to existing VLANs if a department expands or relocates.
- **Increased security options.**
  VLANs have the ability to provide additional security not available in a shared media network environment. By nature, a switched network delivers frames only to the intended recipients, and broadcast frames only to other members of the VLAN. This allows the network administrator to segment users requiring access to sensitive information into separate VLANs

2.2 IP Security

2.2.1 Overview

Security deals with protecting the company's assets from different types of threats – both intentional and unintentional. The security implementation is usually a compromise between level of security, cost and availability of productivity tools. E.g. with a very high security level cost will increase and/or many productivity tools will be restricted.

The company's security policy provides a guideline for how this compromise between security level, cost and productivity tools should be handled. The security policy states how different situations should be handled and what should be allowed and not allowed.

IP has brought in a range of new security threats for the companies. These are:

- Denial of Service
- Eavesdropping
- Manipulation of Data
- Unauthorized Access
- Viruses, Trojan Horses, Spy Ware

To deal with the different security threats, a set of security mechanisms are used. The IP security mechanisms are divided into the following areas:

- Network/Site Perimeter Protection
- Internal and Traffic Protection
- Node Protection

These mechanisms are applied in a defense in depth – a concept similar to how medieval castles were built. Defense in depth principle means - Employment of several security mechanisms and security layers to provide maximum protection.

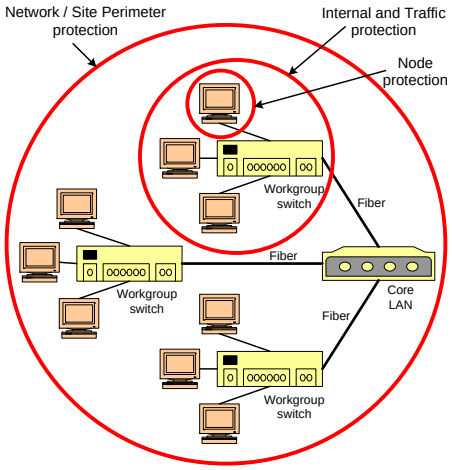


Figure 11 Defense in depth

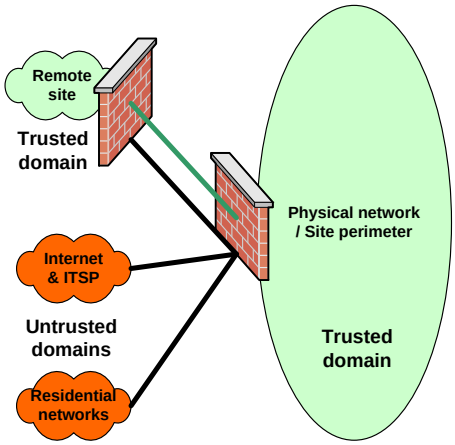


Figure 12 Site protection

2.2.2 Network/Site Perimeter Protection

The network – site protection provides the outer protection for the network site. Both physical and logical structures are taken into account with physical protection of routers, switches, and cabling. Further traffic in and out from untrusted domains like the Internet must go via the firewall for screening, and traffic traveling to other remote sites must be protected from manipulation and eavesdropping.

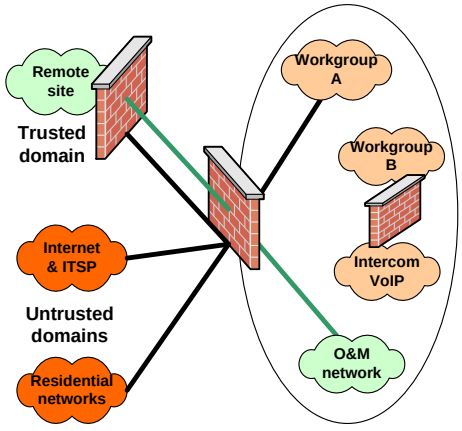


Figure 13 Internal and traffic protection

2.2.3 Internal and Traffic Protection

The next level of protection is the internal protection at the site. This level deals with separating the site into different security and service zones, what traffic should be allowed between networks, monitoring of the site, access to server room, logon privileges

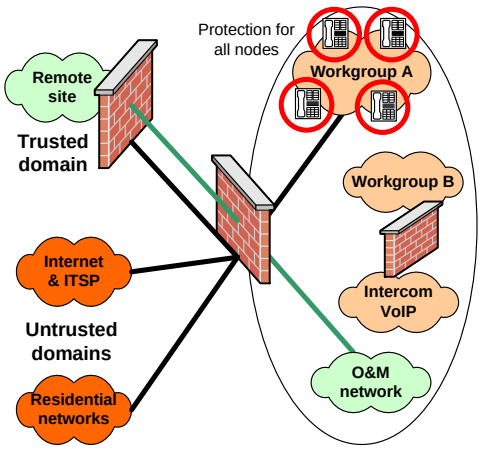


Figure 14 Node protection

2.2.4 Node Protection

The inner level of the security is the node protection. This can be thought about the last level of defense, which the node itself provides. This can be thought about as the nodes armor. These are the nodes robustness to denial of service attacks, unauthorized logons, virus attacks, and so on.

2.3 Quality of Service (QoS) and VoIP

2.3.1 Overview

QoS definition

QoS is the system's ability to service a given application efficiently without affecting its function or performance.

This chapter describes how to preserve voice quality in a VoIP system.

Voice has a set of quality characteristics. At a very high level, basic telephone voice quality is made up of three fundamental components:

- Sound quality (loudness, distortion, frequency, noise)
- Conversation quality (end-to-end delay, talker overlap, echo)
- Service quality (Network availability, busy signals, dropped calls etc)

The sound quality describes audio fidelity, intelligibility, and the characteristics of the analog voice signal itself. The conversation quality describes the interactiveness of the conversation, and the service quality describes the availability of the telephone services.

Voice quality means different things, depending on one's perspective and expectation level. For example, users of cell phones or overseas satellite links tolerate or ignore sound-quality problems because of the usefulness of the call itself. When you listen to your stereo you expect high fidelity 20 kHz bandwidth audio, while on a telephone call 3.4 kHz is sufficient.

For Critical Communication it is also useful to introduce the system robustness as a separate quality factor. Critical Communication is a lot about delivering high sound and conversation quality in critical situations with stressed users, network errors and other external factors such as high background noise. Robustness thus describes how good the audio and conversation quality perform under different network and environment impairments.

In a VoIP system it is a set of QoS factors that affect the voice quality. These are:

- Network availability
- Bandwidth available
- Delay and delay variation
- Packet loss
- Audio codec

2.3.2 Network Availability

Design of the network availability is based on a number of factors which include equipment reliability and network survivability. With relationship to the network survivability, following are the items to consider; power distribution (UPS's, battery backup), redundant links-multiple options of completing a call, switchover support (external on the network), local intelligence, IP QoS and IP security.

The service provider selection and the QoS Service Level Agreements (SLA's) also need to be considered.

Note! The traditional benchmark for a voice network is an uptime on 99.999% or about 5.25 minutes of downtime per year.

Power over Ethernet

Supplying power to the network connected end-points such as IP-intercoms, IP-telephones and IP-CCTV camera's is an important part of the communication network availability. Where it could be realistic to power each such unit independently from mains, it is not realistic to provide a local power back-up for each unit.

Power over Ethernet (PoE) is a standard for supplying power to end-points across CAT5 cabling. The power is injected into the cable by either an IP-switch (end-span solution) or a special unit near the data switches (mid-span solution). By providing a UPS to the switch and the PoE equipment it is possible to centrally provide power backup to all to the relevant equipment connected end-points.

2.3.3 Bandwidth Availability

Although real-time VoIP has a reasonably low bandwidth requirement, it needs careful attention. When deploying VoIP, the following areas needs to be looked at:

- Bandwidth provisioning
- Bandwidth management
- Ensuring constant bandwidth availability

Bandwidth provisioning

The network should be provisioned to deliver sufficient bandwidth for both the traditional data traffic and the VoIP requirement. In the provisioning process one should calculate the bandwidth needed for the VoIP[1].

In the VoIP bandwidth calculation one should first find out the maximum number of concurrent VoIP calls between the different destinations. Each VoIP call will consume the following type of bandwidth:

- **Audio payload.**
  The audio payload is given by the codec that the audio is coded with. For G.722 this is 64 kbps.
- **IP and VoIP overhead (IP/UDP/RTP).**
  The IP and VoIP overhead is 40 Bytes (320 bits) per VoIP packet.
- **Link layer overhead.**
  The link layer overhead is dependant on the link types the VoIP traffic is carried over.

Link type	Overhead
Ethernet	14 Bytes (112 bits)
Frame relay	4 Bytes (32bits)
IPsec	52 Bytes (416 bits)
GRE	24 Bytes (192 bits)

Figure 15 Link layer overhead

[1] There is no easy way of calculating the bandwidth needs for data. It is therefore recommended to measure the bandwidth consumption that the data service uses in the provisioning.

Example: G.722 VoIP call over a Frame relay WAN link with IPSec and GRE using a voice packet size of 20 ms

Audio payload		= **64 kbps**
VoIP packets per second	= 1/20ms = 50 pps	
IP and VoIP overhead	= 50 pps * 320 bits	= **16 kbps**
Link layer overhead	= 50 pps * (32 + 416 + 192)bits	= **32 kbps**
Total bandwidth	= (64 + 16 + 32)kbps	= **112 kbps**

A method of reducing the overall VoIP bandwidth requirement is by sending less packages as the same overhead is added to each package. Sending less packages means that the payload of each package is larger, but also that the time interval between each package is longer. The downside of this method is that the delay which is introduced at the sending end also increases, see also paragraph 4.3.

Bandwidth management

The VoIP bandwidth management ensures that the system does not use more bandwidth than what it is provisioned for. For instance: If a WAN link is provisioned to carry two VoIP calls. If a third call is setup, this may impact the quality of all three calls as well as it might take needed data capacity for other applications.

Ensuring constant bandwidth availability

Real time VoIP traffic requires a constant availability of bandwidth. As data traffic is quite bursty one needs to put in place a system to be able to deliver this constant bandwidth availability. To ensure constant availability of bandwidth one can use IP QoS and/or over-provisioning.

Over-provisioning means that the system has capacity headroom that caters for the situations with high data bursts. If a high data burst occurs, there would then be still be sufficient bandwidth for the VoIP.

Note! IP-QoS is described in more details in chapter 2.3.7.

2.3.4 Delay & Delay Variation (Jitter/Wander)

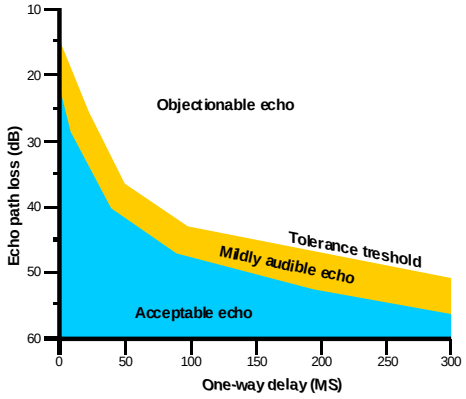


Figure 16 Talker echo tolerance as function of delay

Delay requirements

The typical requirement of telephony equipment with regards to end-to-end (one way) delay is 150 ms. If the delay gets longer than 150 ms, the interactiveness of the conversation goes down and we get crosstalk (people start and stop talking at the same time).

For critical communications, such as loud speaking intercom and PA calls, the expectation level in regards to delay is higher than normal telephones. When we have amplified audio, humans have lower tolerance to echo as the delay and delay variation increases. Our recommendation for Critical Communication is to keep end-to-end delay (Microphone to remote speaker) lower than 35 ms in the LAN and 100 ms in the WAN.

Components of delay

Figure 17 shows the different components that introduce delay in a VoIP system.

The codec and jitter buffer are delay components of the VoIP equipment. In AlphaCom XE, these together add a delay which is 2.5 times the voice frame size. This delay is 25 ms if packets which represent 10 ms of audio are used.

The queuing, serialization and propagation are delay factors that are dependant on the network. These are referred to as the network delay. The network delay can easily be measured using PING type of tests.

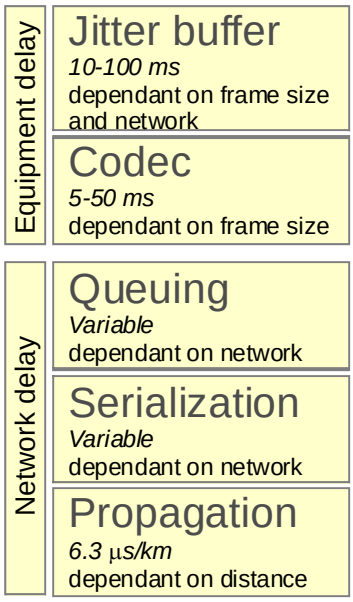


Figure 17 Components of Delay

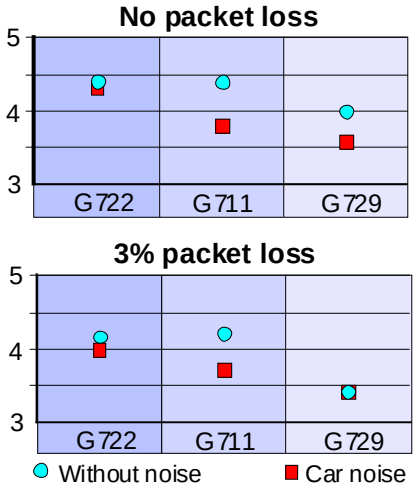


Figure 18 General quality impression

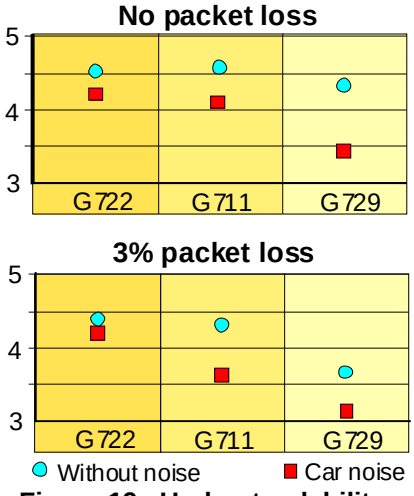


Figure 19 Understandability

2.3.5 Packet Loss

Not all packets make it to their destination. The most typical reasons are corrupted packets caused by collision, or dropped packets in the router due to traffic congestion.

Packet network applications compensate for packet loss by retransmitting lost packets through the use of the Transmission Control Protocol (TCP). Data applications such as file transfers and e-mail are less sensitive to the time it takes for this to occur, but real-time voice traffic cannot tolerate this delay. In addition, VoIP networks use connectionless transfer protocols such as the User Datagram Protocol (UDP) that do not guarantee delivery at all. Lost packets mean lost voice information.

If several packets are dropped, audio quality becomes poor for stations involved in the conversation. The severity depends on the robustness of the audio coding that is applied for the call.

2.3.6 Audio Codec

The robustness of a VoIP network is in a large degree dependant of the audio codec and processing routines that the system provides. Several research studies have been performed to investigate the impact of factors such as packet loss and background noise on a VoIP system.

The graphs (Figure 18 and Figure 19) show the quality impression in conditions with packet loss and background noise. Three different types of codecs are used:

- Wideband codec (G.722, 64 kbps, 7 kHz, stateless)
- Traditional telephone (G.711, 64 kbps, 3.4 kHz audio, stateless)
- Low bit-rate codec (G.729, 8 kbps, 3.4 kHz, stateful)

A stateless codec is a codec where each sample is independent of the previous sample, whereas the meaning of a sample produced by a stateful codec depends on the values of samples in the past. By definition therefore, the loss of a sample of a stateful codec has a worse effect on the audio quality, as it also affects the reproduction into audio of the following samples.

Figure 18 shows the general quality impression using a Mean Opinion Score (MOS). The MOS score uses a rating as follows: (1) bad; (2) poor; (3) fair; (4) good; (5) excellent.

Figure 19 shows the quality on understanding using a Degredation Mean Opinion Score (DMOS). The DMOS score uses a rating as follows: (1) very annoying; (2) annoying; (3) slightly annoying; (4) audible – not annoying; (5) inaudible.

The wideband codec G.722 were superior with regards to quality in difficult environments compared to the other codecs. In critical communication systems we therefore highly recommend to use wideband G.722 codec.

2.3.7 Optimizing IP Networks-IP QoS

IP Quality of Service (QoS) is an attempt to provide a service guarantee in the “best effort” world of Internet. The main approach to this problem is to prioritize different data packets according to their delay sensitivity. As an example, it would be ideal to give voice packets higher priority than packets transferring a file between two computers. There are many technologies available to improve this so-called Quality of Service (QoS) of a network:

ToS, and DiffServ

Each IP-packet is given a priority. The switches and routers on the way will look at this part of the package and award priority in transmit queues accordingly, with normal computer data as the lowest priority and voice data as the highest. As the voice related data has the highest priority, all aspects of the quality issues are addressed. The delay and delay jitter are minimized as data is transmitted out as quickly as possible. Packet drop is minimized as voice data enters the queue at the top rather than the bottom. It may cause low priority data which already was in the queue, to drop out.

VLAN, Virtual LAN

The network is divided into logical sub-nets where each subnet is given a fixed part of the total available bandwidth. This means computer data on a certain VLAN cannot interfere and delay traffic on another VLAN, even if the capacity for the computer data VLAN is insufficient. By making certain that the voice VLAN has a higher capacity than the maximum required capacity, it's guaranteed that the voice traffic does not suffer unnecessary delays. For this end, the traffic on the voice VLAN must never be higher than 70 percent of its assigned capacity.

The AlphaCom system supports both of the above priority schemes. It is important that all components in the network support one of the above priority schemes and all components support the same scheme. Older switches may not, and can cause congestion delays.

Note! A network that carries voice packages must never contain hubs as these devices do not allow efficient use of the network.

2.3.8 IP Quality of Service in Practice

A LAN bandwidth is not usually a scarce resource and a VoIP call takes less than one percent of a normal LAN link (if the link is 100 Mbps). Security is an important issue in a LAN as the spreading of viruses, denial of service, etc. are items that must be taken into consideration. Large LANs can be complex and a wrong configuration can cause congestion points and traffic blocks, hindering the performance of the network. Congestion issues can be speed mismatch, aggregation and unexpected traffic pattern.

In a WAN, bandwidth is scarce and is normally an issue. Lack of bandwidth can cause packet loss and congestion/delay issues. Many transmission hops and long distance also add up to the delay possibility. With IP QoS you get a higher predictability when bandwidth availability becomes a problem.

Note! VoIP applications work 99 percent of the time over an ADSL line without using QoS.

3 AlphaCom XE & IP

3.1 VoIP vs. Critical Communication Over IP

When talking about IP in the communication and security business, it is important to distinguish between VoIP and Critical Communication over IP.

Voice over IP (VoIP) simply allows voice communications to be transmitted over a data network, and can deliver cost-savings by eliminating charges associated with long distance calls.

Critical Communication over IP employs VoIP, but goes an important step further by adding new IP services and applications integrating security, quality and reliability capabilities required in critical situations.

The AlphaCom XE solution is the first professional communication and security system providing Critical Communication over IP. The system provides VoIP for external as well as internal communication together with a range of IP services and capabilities such as integrated Web services, IT management tools, IP 3rd party integration, logging and dB tools, PC soft clients, IP security and IP QoS to name a few.

3.2 AlphaNet - Internal Networking

3.2.1 AlphaNet Feature Rich Networking

AlphaNet is STENTOFON's internal networking technology. AlphaNet is made for critical communications. Some of the highlighted features of AlphaNet are:

- Group and conference calls
- VoIP bandwidth management
- Priority handling of events and resources
- Alternative routing
- Backwards compatibility
- All features available over the network
- VoIP, digital and analogue infrastructure support

Group and conference calls

AlphaNet comes with full group and conference call capabilities. Each AlphaCom XE has built in multiparty conferencing units, providing local mixing for group and conference calls. This local mixing allows AlphaCom XE to use a single VoIP channel only when setting up a group or conference call between exchanges.

VoIP bandwidth management

AlphaNet provides bandwidth management limiting the VoIP bandwidth to not take more capacity than provisioned. If a high priority call is set up when all VoIP channels are occupied, AlphaCom XE will immediately release the call with the lowest priority allowing the high priority call to proceed.

Priority handling of events and resources

All calls and events that are sent between nodes are marked with priority. This allows the system to act upon the priority, presenting and handling the events and calls in the correct order.

Alternative routing

Alternate routing of calls allows call completion even when the primary AlphaNet route is down. As a secondary route AlphaCom XE can either

use its secondary IP interface or it can put the call over a traditional interface such as an analogue or digital line.

Backwards compatibility

AlphaCom XE provides 100% backwards compatibility between traditional AlphaNet technologies and new VoIP AlphaNet. The backwards compatibility allows mixing of new AlphaCom XE nodes working over IP with current nodes so configurations can be maintained.

All features available over the network

Consistent features and services across the organization regardless of location providing improved user friendliness

Note! AlphaCom XE provides all current AlphaNet features available today with the enhanced features of connection to LAN/WAN.

VoIP, digital and analogue infrastructure support

AlphaNet works over any infrastructure being IP, digital or analogue.

3.2.2 VoIP AlphaNet Deployment Models

The two most common models for deploying VoIP AlphaNet are:

- Modular AlphaNet architecture
- Wide Area Networking AlphaNet

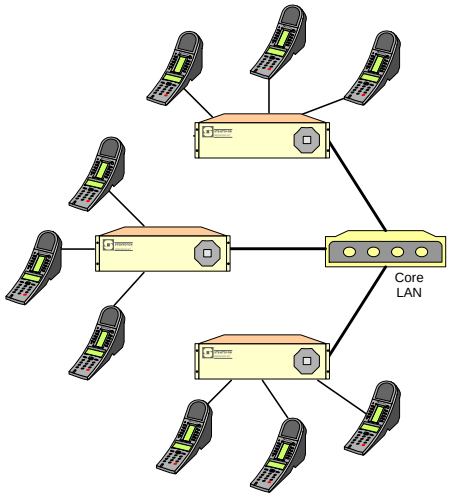


Figure 20 Modular AlphaNet architecture

Modular AlphaNet architecture

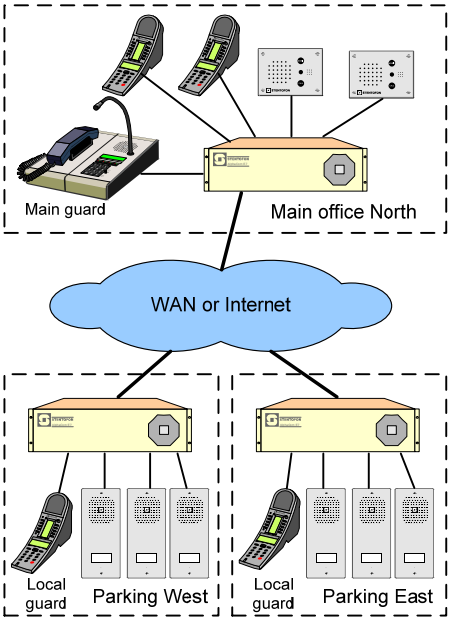
The modular AlphaNet Architecture utilize the LAN and structured cabling infrastructure in the building and campus (See chapter 2.1.3 Local Area Networks (LAN)).

The AlphaCom XE exchanges are placed by the patch panel on different floors, wings or buildings on a campus. The benefits of the modular architecture are:

- Increased security through local intelligence
- Increased security through alternative routing
- Increased security through a dedicated network within each workgroup
- Increased security through AlphaCom XE power distribution to the stations
- Cost efficient with reduced cabling

In a system such as this, no calamity can ever affect the complete communications system in one go, no matter what happens where on the site.

Note! An earlier concern with distributed architecture vs. central server architecture has been increased operation costs of equipment. The AlphaCom XE provides cluster programming of all exchanges from the same GUI as well as centralized remote monitoring services using SNMP, Syslog and web; thus reducing operation cost in a distributed architecture.



Wide Area Networking AlphaNet

VoIP AlphaNet between sites significantly reduces operating costs, allowing two or more AlphaCom systems to be networked seamlessly together over the corporate IP-WAN network.

This allows for the audio traffic to be moved over to the WAN data network, having only a single network to handle. In addition WAN links have experienced large price cuts during the last year due to the introduction of new technologies (DSL, Gigabit Ethernet, LMDS and IP VPN) and increased competition in the market.

Comparison studies show that VoIP AlphaNet provides significant lower operating costs than traditional networking.

3.3 SIP (Session Initiation Protocol)

- AlphaCom XE is the first and only critical communication system supporting SIP. This opens up various new services that were not available before.

SIP (RFC 3261) means interoperability. Over the last couple of years, the Voice over IP community has adopted SIP as its protocol of choice for signaling. For more information on SIP see reference 2 and 3.

AlphaCom XE has an integrated SIP interface. This allows AlphaCom XE to interface directly to SIP compatible devices such iPBX's, Voice Gateways (ISDN, analogue), telephone adapters, VoIP telephones, PC clients and ITSP (Internet Telephone Service Provider).

Note! To use SIP you need an AlphaCom XE SIP trunk license.

3.3.1 SIP External Networking

SIP provides an easy way of connecting your AlphaCom XE Critical Communication system to an external system. This can be done directly if the external system supports SIP. The interfacing can also go via a SIP gateway. There are a variety of SIP gateway products in the market allowing AlphaCom XE to interface to almost any telephony line and protocol such as ISDN (BRI and PRI), CAS and analogue lines.

We see today two main external networking models. These are:

External telephony networking

By using the SIP protocol, it allows the AlphaCom to become an extension of the telephone system or vice versa.

The external telephone networking allows users to get full telephone support between AlphaCom and the external systems. Functions such as direct dialing in, and number presentation are supported.

Critical Communication in a mixed environment

This model provides a tighter integration between the AlphaCom XE system and the external system. Here the external system becomes part of the Critical Communication system supporting functions such as group call, public address and security management.

Note! SIP protocol is a global standard approved for use in all countries. The SIP gateways used to interface to other telephony interface are globally available for any national standard and approval.

3.4 AlphaCom XE IP Security Services

Critical Communication over IP means that security issues related to IP networks are entering the Critical Communication world. The Critical Communication solution can no longer be regarded as a totally independent system isolated from data networks and their associated challenges.

The AlphaCom system provides carrier class system availability and protects resources in an IP environment by using embedded IP security mechanisms. The main AlphaCom XE security mechanisms are:

- Restricted management access
- Separate management interface
- Internal firewall
- Traffic screening between sub networks
- Firewall Transversal
- Communication grade OS

3.4.1 Restricted Management Access

All users need to authenticate themselves before getting access to the management services. The authentication process uses a MD5 authentication routine, which produces a digital signature for high security.

3.4.2 Separate Management Interface

The AlphaCom XE comes with a separate Ethernet interface, which can be dedicated to management. This allows the administrator to build a separate administration VLAN that can be dedicated to administrators.

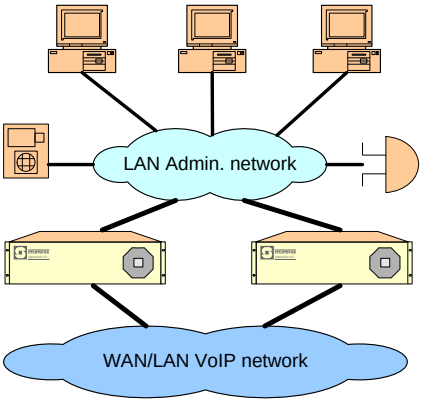


Figure 21 Separate management interface

3.4.3 Internal Firewall

AlphaCom XE has an internal firewall allowing the network administrator to open and close IP services that should be able to access the AlphaCom XE from the different networks. As default the AlphaCom XE come with the most restricted firewall settings.

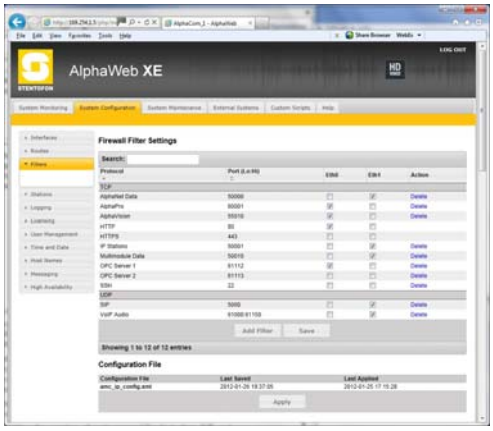


Figure 22 Internal firewall

3.4.4 Traffic Screening Between Networks

Many routers are able to selectively perform their tasks based on a number of facts about an arriving packet such as originating address, destination address, destination service port and so on.

Employing traffic screening is a method for enforcing your security policy with regard to what sorts of access you allow between your network, reducing risk of virus, denial of service attacks and unauthorized access.

AlphaCom XE allows easy ways of screening the traffic between your IP networks by:

- Limiting the number of ports opened for AlphaNet, SIP and RTP/RTCP
- Forcing all AlphaNet, SIP and RTP/RTCP traffic to always go via AlphaCom XE exchanges enables screening on source and destination.

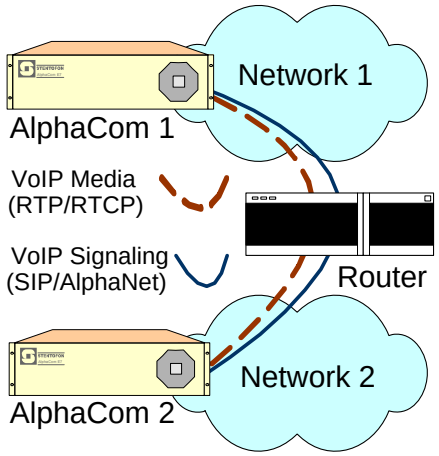


Figure 23 Traffic screening

IP service	Port
HTTP	80 (TCP)
HTTPS	443 (TCP)
AlphaPro	60001 (TCP)
Syslog	514 (UDP)
SNMP (MIB)	161 (UDP)
SNMP (Trap)	162 (UDP)
SIP	5060 (UDP)
AlphaNet	50000 (TCP)
RTP/RTCP	61000:61150 (UDP)
Multi-module data	50100 (TCP)
IP-Stations data	50001 (TCP)
EDO	Configurable (TCP)
EDI	Configurable (TCP)
SSH	22 (TCP)
FTP	21 (TCP)
NTP	123 (UDP)
Serial over IP	Configurable
AlphaCom OPC server port 1	61112 (TCP)
AlphaCom OPC server port 2	61113 (TCP)

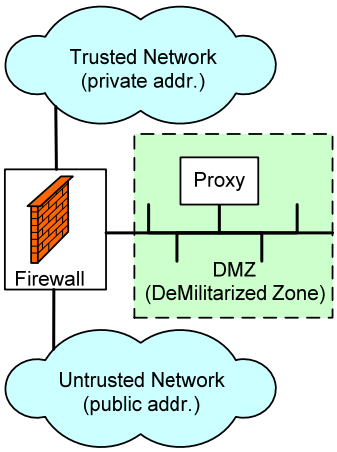


Figure 24 Firewall traversal

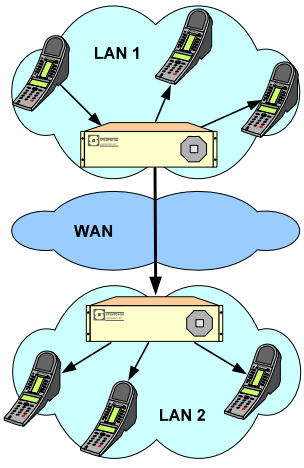


Figure 25 Global group call

3.4.5 Firewall Traversal

The de-militarized zone DMZ is a critical part of a firewall: it is a network that is neither part of the untrusted network, nor part of the trusted network. But, this is a network that connects the untrusted to the trusted. The importance of a DMZ is tremendous, someone who breaks into your network from the Internet have to get through several layers in order to successfully do so. Those layers are provided by various components within the DMZ.

The AlphaCom XE can be set up to work as a proxy (transit exchange) in the DMZ. All VoIP traffic to and from the untrusted network will need to go via the proxy (transit exchange). The AlphaCom XE will:

- Check whether the VoIP traffic belongs to a valid user and call
- Perform IP network address translation
- Forward VoIP traffic to the destination [2]

3.5 AlphaCom XE IP QoS and Media Services

Critical Communication requires robust and high quality audio communication. The AlphaCom XE provides advanced IP QoS and IP media services to provide Critical Communication over IP. These services include:

- **IP priority handling (DiffServ and ToS)**
  All VoIP packets are marked with DiffServ/ToS (EF class/IP precedence) to have priority through the network.
- **Alternative routing**
  In+ case the primary IP route fails, a secondary IP route or traditional network link (E1, analogue) are used to complete the call.
- **Fast transit switching**
  The AlphaCom XE hardware utilizes special network processors, providing fast switching of VoIP traffic. In fact a transit VoIP packet is switched through in less than 1 ms.
- **Wideband audio**
  AlphaCom XE supports wideband codecs (G.722) as well as telephony codecs (G.711) for VoIP calls. Wideband G.722 provides superior quality compared to traditional VoIP codecs (See chapter 2.3.6 Audio Codec)
- **Adaptive jitter buffer**
  A jitter buffer is used to compensate for the jitter in packet arrival and out-of-order packets. The adaptive jitter buffer enables the buffer size to change dynamically in response to network conditions, optimizing audio delay.
- **Bandwidth management**
  The AlphaCom XE provides mechanisms to enforce that not more than a maximum number of calls are set up over the LAN and WAN. If a call with a higher priority is initiated when all resources are occupied, the call with the lowest priority is released and the call with the high priority is completed.
- **Group call bandwidth optimization**
  When setting up a global group or conference call, only a single VoIP channel is needed between the AlphaCom XE exchanges. Each exchange branches out to the intercom stations that are joined in the group and conference call.
- **QoS statistics log**
  Call statistics such as duration, audio delay, codec, time, can be sent a log providing capabilities to log quality for each VoIP call.

[2] General IP forwarding is disabled in all AlphaCom XE exchanges.

3.6 System Management and Operation

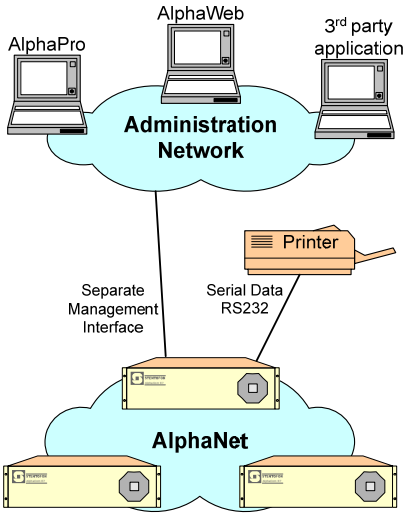


Figure 26 System management and operation architecture

The AlphaCom system provides easy to use, secure and powerful system management capabilities targeted to solve the different customer needs and demands.

The system management architecture is open and flexible to cater for multiple tools, technologies and customer demands.

The management tools and functions come with different level of complexity to match the demand from small standalone systems to large integrated management systems.

The main tools and functions are:

- AlphaPro
- AlphaWeb
- Logging and monitoring
- System upgrade

AlphaPro

AlphaPro is the professional tool for configuration of the AlphaCom system. It is self contained, simple to install and use. When a new exchange shall be configured, the exchange is given a working default factory setting. The operator can then modify the settings. AlphaPro works over IP or a local data port (RS232)

AlphaWeb

The AlphaWeb is an embedded web server running on the AlphaCom XE exchange. It allows the users to logon using a standard web browser such as Internet Explorer or Netscape to operate and manage the AlphaCom system. The server provides functions for:

- System Monitoring
- System Configuration
- System Upgrade

Logging and monitoring

The AlphaCom XE comes with powerful logging and monitoring functions giving the user very good visibility into system status and events.

The customer may choose multiple options for how to retrieve information and events from the system. General system status information can be retrieved from:

- **AlphaWeb**
  AlphaWeb provides system status information such as node states (According to X.733), hardware configuration, software versions, and more.
- **SNMP MIB II (RFC 1905-1907)**
  AlphaCom supports SNMP MIB II according to RFC 1905-1907. The MIB II information is available through a standard SNMP browser or network management tool.

AlphaCom XE has three different types of log events. These are:

- **Technical Log**
  Provides technical log events
- **User Log**
  Provides reporting of custom defined events
- **Statistical Log**
  Provides information regarding call statistics like duration, A-B user,

and average audio delay.

The log events are reported to:

- **Local log port (RS232)**
  The local log port can be used to send log information to a console or printer.
- **Syslog (RFC 3164)**
  Syslog is a standardized way of sending log events to a central log server. Syslog provides the capability to retrieve log information in a multi-vendor environment.
- **AlphaWeb (Local log file)**
  All log information can be sent to a local file on the AlphaCom XE exchange. AlphaWeb provides the capability to search, scroll and download the log files.
- **System clock and time stamps**
  The AlphaCom XE supports the Network Time Protocol (NTP – RFC 1305) for synchronizing the system clock.
  The Network Time Protocol is a widely used protocol, allowing distribution of time information and synchronization of clocks over the IP network.

3.6.1 Other IP Services

All data protocols already available in AlphaCom, such as AlphaNet data protocols, MPC data protocol, EDO/EDI, RIO, Pocket Paging and Fire Alarm are supported over TCP/IP in the AlphaCom XE. This provides a service creation environment with the ultimate toolbox for value added integrators to build a complete security management system, where the interface can be via traditional data links and across IP-networks. The toolbox allows the integrators to design and tailor the behaviors of the AlphaCom XE system as well as the other supplementary systems such that it works as one integrated security management solution.

The 3rd party service creation environment includes the following well recognized tools:

STENTOFON Event Handler

This is the main tool for tailoring AlphaCom system behavior.

On any status change of equipment controlled by the AlphaCom exchange (intercom station, inputs, etc…) the exchange can send an event trigger to the Event Handler.

The Event Handler is programmed by using a scripting language to perform a multitude of functions. These functions can even be conditional as ‘If-Then’ type. Programming of the Event Handler is through the AlphaPro programming tool.

STENTOFON External Data Output

Part of the Event Handler where scripts can be used to send user defined messages and commands to 3rd party equipment.

An example is to send commands to CCTV equipment to switch a camera output to a certain monitor when a voice connection is established between intercom stations.

STENTOFON External Data Input

Part of the Event Handler where scripts can be used to directly interface to data sent from 3rd party equipment.

Prime examples are further integration with CCTV and Fire Alarm equipment. Incoming data strings can trigger the event handler. The string is interpreted in the event handler and the required action can be

performed, such as setting up calls between intercom stations, sending automatic broadcast messages or other appropriate actions.

STENTOFON Link Layer Protocols

The Simple Link Layer, STENTOFON Multidrop and ISO1745 protocols all allow 3rd party applications to control AlphaCom functions such as setup of calls, conferences and group announcements, sending messages, simulating station key inputs and trigger the Event Handler to open doors or provide any other control functionality. In addition, the AlphaCom reports internal statuses on these protocols, which can be used by these applications for display purposes.

All these protocols are equivalent in functionality, but offer different levels of handshaking. The STENTOFON Simple Link Layer protocol is ASCII text based and is therefore easy to debug. The other protocols are binary protocols and offers retransmit capabilities.

4 Deployment Guideline

This chapter describes a process for successful implementation of the AlphaCom XE system into a corporate IP network. The steps in the process are:

1. Sketch network overview
2. Traffic overview
3. VoIP bandwidth provisioning
4. IP security planning
5. Quality of service planning

4.1 Sketch Network Overview

Make a sketch of the network. The sketch should include:

- Location of the AlphaCom XE exchanges
- Interface to external telephone systems
- Overview of the IP network (Internet, WAN, and LANs)

This sketch will provide a visual overview of the solution, and it will be used as basis for further deployment analysis.

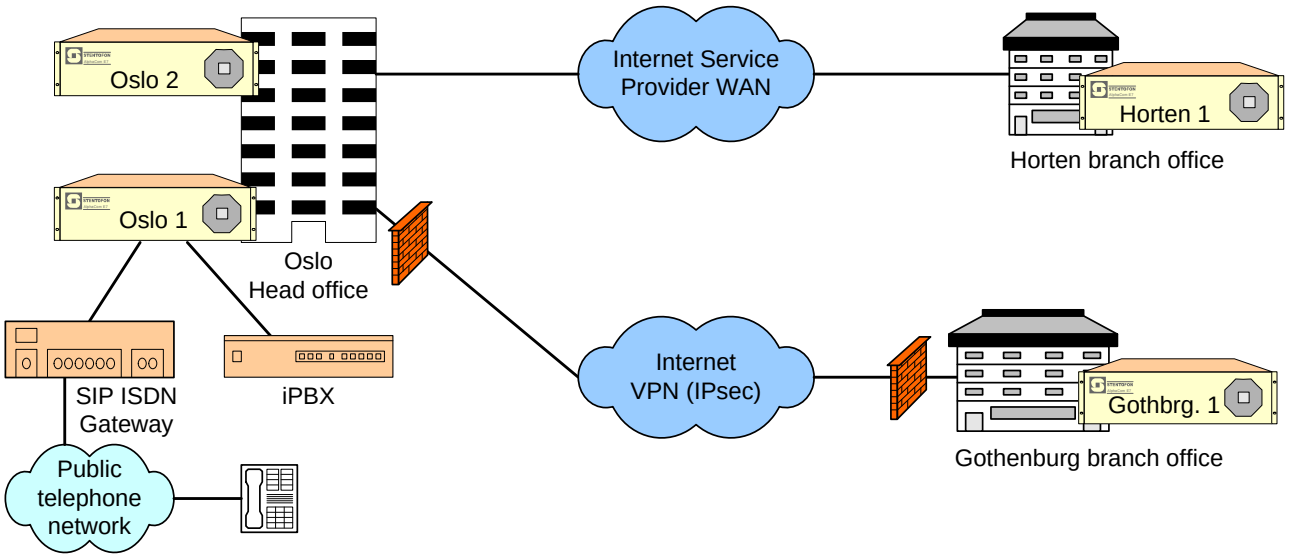


Figure 27 Network example

4.2 Traffic Overview

Make an overview of the VoIP traffic in the system. For each AlphaCom E exchange the following should be listed:

- Number of stations connected to the exchange
- Number of SIP channels to external telephone systems
- Number of VoIP AlphaNet links. See Table 1 as an example

AlphaCom XE exchanges	Stations			External VoIP links	AlphaNet VoIP links
	IP	Traditional	Total		
Oslo 1	5	40	45	4 ch PSTN 6 ch iPBX	4 ch Oslo 2 2 ch Horten 1 2 ch Gothenburg 1
Oslo 2	2	20	22	-	4 ch Oslo 1
Horten 1	2	20	22	-	2 ch Oslo 1
Gothenburg 1	4	20	24	-	2 ch Oslo 1

Table 1 VoIP traffic overview

4.3 VoIP Bandwidth Provisioning

The intention of this task is to calculate the VoIP bandwidth required in the system.

Bandwidth vs. delay

The audio stream is encapsulated in IP packets, where each packet normally consists of 5 to 40 ms of audio. The smaller the portion of audio in each packet, the smaller delay the VoIP system will introduce. Typically the audio delay will be 2.5 times the audio frame size + IP network delay. However, the smaller the audio frame size, the more IP packets are sent, and more overhead bandwidth is introduced in the system.

In VoIP systems there is therefore a tradeoff between VoIP bandwidth and delay. Our recommendation is to set the audio frame size as a factor of WAN/LAN link and network delay.

- If using LAN AlphaNet Links
  Recommend to use 5 ms frame size
- If using WAN and the network delay is less than 20 ms
  Recommend to use 10 ms frame size
- If using WAN and the network delay is more than 20 ms
  Recommend to use 20 ms frame size

VoIP bandwidth

The VoIP bandwidth consists of the **actual audio payload** and the **overhead**. See Table 2 for overhead bandwidth vs. audio frame size.

Overhead Type	Audio frame size		
	5 ms	10 ms	20 ms
VoIP (IP/UDP/RTP)	64.0 kbps	32.0 kbps	16.0 kbps
VPN (IPsec)	83.2 kbps	41.6 kbps	20.8 kbps
Frame relay	1.6 kbps	3.2 kbps	6.4 kbps
Ethernet	5.6 kbps	11.2 kbps	22.4 kbps

Table 2 Overhead bandwidth vs. audio frame size

VoIP bandwidth provisioning

Calculate the VoIP bandwidth for each main network. See example in Table 3.

	Audio frame	OH pr call	Audio payload pr call	Max # of VoIP calls	Total Bandwidth
WAN Oslo Horten	10 ms	32 kbps (VoIP)	64 kbps (G.722)	2	192 kbps
WAN Oslo Gothenburg	20 ms	74 kbps (VoIP + VPN)	64 kbps (G.722)	2	276 kbps
LAN Oslo AlphaNet IP stations SIP iPBX SIP PSTN	5 ms	64 kbps (VoIP)	64 kbps (G.722)	 4 5 6 4	 512 kbps 640 kbps 768 kbps 512 kbps
LAN Horten	5 ms	64 kbps (VoIP)	64 kbps (G.722)	2	256 kbps
LAN Gothenburg	5 ms	64 kbps (VoIP)	64 kbps (G.722)	4	512 kbps

Table 3 VoIP bandwidth provisioning

4.4 IP Security Planning

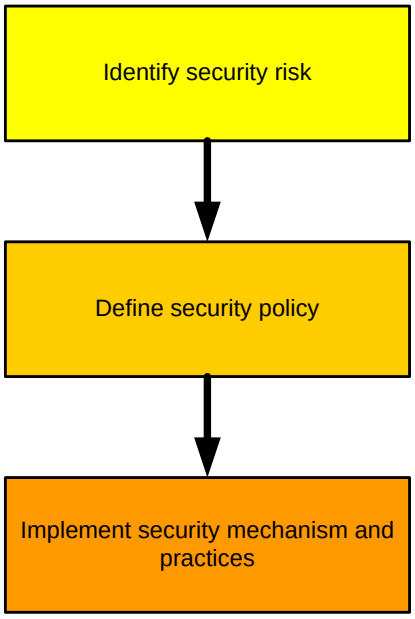


Figure 28 IP security planning

Providing access to your network services gives your staff and company many benefits. However, the more access that is provided, the greater the danger that someone will exploit the increased vulnerability.

In fact, every time a new system, application or network access is added, potential vulnerabilities are added and protection becomes increasingly more difficult and complex. However, if you're willing to realistically confront the serious risks, it is possible to reap the benefits of greater access while minimizing the hazards. To accomplish this, you will need a comprehensive plan as well as the resources to execute it.

The key for building a secure network is:

Identify security risks

Typical security risks include, mains power failure, virus attacks, denial of service attacks, eavesdropping, and more.

Articulate security policy

Define what security means to your organization. You need to decide on the risks you are willing to accept and the amount of inconvenience you are willing to take to go through in order to protect it.

Implement security mechanism and practices

Once the security policy has been defined, everything that goes on with the network can be evaluated with respect to that policy. See section 2.2 and 3.4 for description on IP security mechanisms.

Chapter 5, *Appendix*

AlphaCom XE Security Mechanisms, provides an overview of typical IP security risks and policies matching AlphaCom XE's security mechanisms and solutions.

4.5 QoS Planning

4.5.1 QoS in WAN

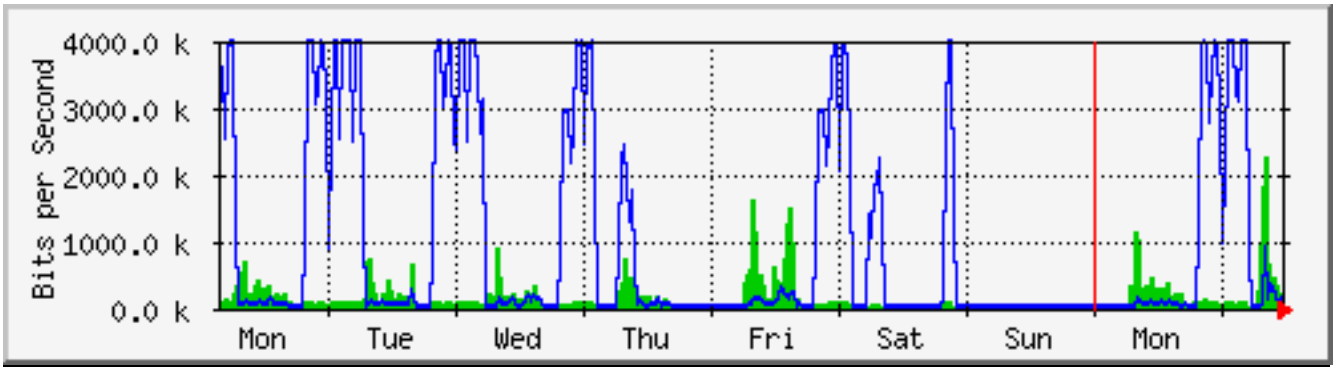
In a WAN, bandwidth is scarce and IP QoS needs careful planning. The steps in the planning process are:

- Assess bandwidth and delay on the WAN links
- Plan mix of VoIP and other data services
- Select IP QoS strategy and implementation

Assess bandwidth and delay on the WAN links

Monitor the traffic in your WAN links to estimate the amount of data traffic and the delay on the links. Tools like MRTG (See reference 6.) provide measurements on your WAN and LAN traffic.

Your ISP should also be able to provide you with measurement on the data traffic in your WAN links.



	Max	Average	Current
In	2771.1 kb/s (69.3%)	242.5 kb/s (6.1%)	156.6 kb/s (3.9%)
Out	3999.9 kb/s (100.0%)	1021.9 kb/s (25.5%)	47.6 kb/s (1.2%)

Figure 29 WAN traffic measurement

Plan mix of VoIP and other data services

Use VoIP bandwidth calculations to setup the mix of IP traffic in your WAN link

Max VoIP bandwidth requirement	0.192 Mbps
Data bandwidth	4.00 Mbps peak 1.02 Mbps average
Routing overhead	1.00 Mbps *
Free headroom	0 Mbps peak 0.92 Mbps average
Total link capacity	4.00 Mbps

* As a standard design principle, 25% of the link capacity shall be reserved for routing and other link overheads. See reference 7 in chapter 5.2 for more details.

Table 4 Example WAN link Oslo - Horten

Select IP QoS strategy and implementation

For critical communication it is recommended to use IP QoS priority services like DiffServ and ToS (See chapter 2.3.7) for the WAN links.

Today most ISPs will be able to offer IP QoS in their WAN. When using an ISP to provide your WAN service it is important to get guarantees on the maximum delay and amount of IP priority traffic they are able to offer on each link.

Note! The AlphaCom XE marks all VoIP packets with DiffServ/ToS priority (EF class/IP precedence) as default.

If you classify the VoIP traffic in your WAN as not critical, you can allow the VoIP service to not use IP QoS. In most cases the VoIP service will function well without IP QoS in the WAN. If this strategy is chosen, keep in mind that the VoIP quality can get degraded with packet loss and long and large variations in delay. It is thus useful to measure delay and packet loss over the links where IP QoS will not be enabled.

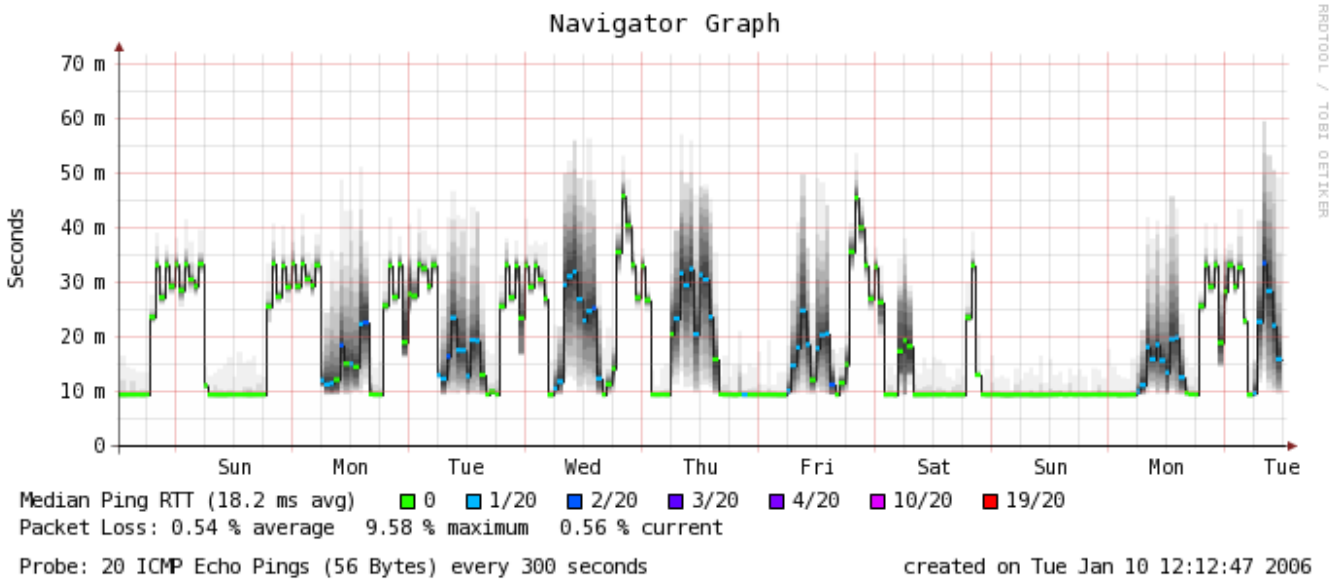


Figure 30 Delay and packet loss measurement

4.5.2 QoS in LAN

In a LAN, bandwidth is not usually a scarce resource[3], and if congestion occurs it is usually not persistent. The need for IP QoS is therefore not as important in the LAN as in the WAN.

However, as large LANs can be complex, wrong configuration can occur causing congestion points and traffic blocks, hindering the performance of the network.

To improve management in large LANs, it is recommended to create a separate VLAN for the VoIP traffic.

[3] VoIP call takes less than one percent of a normal LAN link (if link is 100Mbps).

5 Appendix

5.1 AlphaCom XE Security Mechanisms

Security Risk	Security Policy	AlphaCom security mechanism
Power Blackout	The critical communication system shall survive a power blackout	1. Modular AlphaNet with station powered from AlphaCom and UPS on critical network infrastructure (See chapter 3.2.2) 2. Station are powered over Ethernet and UPS on critical network infrastructure
Damaged network infrastructure	The critical communication system shall survive and be able to complete calls when part of the network infrastructure is damaged	1. Alternative routing (See chapter 3.2) 2. Modular AlphaNet (See chapter 3.2.2)
Virus and other node attacks	Traffic screening between network segments Something about node security	1. Internal firewall (See chapter 3.4.3) 2. Easy traffic screening (See chapter 3.4.4)
Unauthorised administration access	Access to network resources shall be restricted. It is often useful to have different level of access restriction for the types of systems e.g. dB, router, firewall, PC etc.	1. Logon authentication 2. Separate management interface 3. See chapter 3.4 for more information
Visibility on system status	All systems shall be monitored and logged via central network monitoring applications	1. Syslog event reporting 2. SNMP MIB II system status 3. Local log files 4. Test calls and reporting See chapter 3.6 for more information
Internet attacks	Stateful firewall towards Internet	1. DMZ proxy solution (See chapter 3.4.5)

5.2 References

1. *Structured Cabling Tutorial, http://www.iec.org/online/tutorials/scs/*
2. *Gonzalo Camarillo SIP Demystified, McGraw-Hill TELECOM*
3. *Henning Schulzrinne, Colombia University, http://www.cs.columbia.edu/sip/*
4. *Peter Morrissey, Network desing – security, http://www.windowsecurity.com/whitepaper/misc/*
5. *Matt Curtin, Introduction to Network Security, http://www.interhack.net/pubs/network-security/*
6. *Multi Router Traffic Grapher, http://mrtg.hdl.com/mrtg.html*
7. *Ramesh Kaza, Salman Asadulla, Cisco IP Telephony: Planning, Design, Implementation, Operation, and Optimization*
8. *Other related STENTOFON AlphaCom documentation on http://www.zenitel.biz*

www.stentofon.com

Zenitel Norway AS
P.O.Box 4498 Nydalen
NO-0403 OSLO
Norway

support@stentofon.com

STENTOFON and VINGTOR products are developed and marketed by Zenitel Norway AS. The company's Quality Assurance System is certified to meet the requirements in NS-EN ISO 9001:2002. ZENITEL NORWAY AS reserves the right to modify designs and alter specifications without prior notice, in pursuance of a policy of continuous improvement. © 2009 Zenitel Norway AS