



Swift IP

System Requirements

May 22, 2007

Swift IP

Premises Networks is a supplier of integrated business-class communications solutions, services and support for Enterprise and Public Sector organisations. Consulting, designing and implementing tailor-made solutions to fit individual customer needs blending powerful infrastructure to deliver the benefits of voice, mobile and data convergence to businesses. Premises Networks provides intuitive applications for client mobility, messaging and multimedia collaboration.

At Premises Networks we address customers' needs; our approach is based upon delivering true business benefit and best value for our customers. We know that Technology is a business tool and businesses seek to gain best return on investment, competitive advantage in a simple and clear evolution of their tools that makes sense to them.

About this document

This document is an overview of the Swift IP System Requirements and describes requirement on hardware platform and IP network. This document describes the current release and the current view of Swift IP platforms. The information in this document is subject to change without notice and shall not be interpreted as commitments.

Content

- SYSTEM REQUIREMENTS.....1**
- 1 IP-BASED ENTERPRISE TELEPHONY4**
 - 1.1 Implementation Quality 4
- 2 ARCHITECTURE5**
 - 2.1 System Interfaces 5
- 3 NETWORK REQUIREMENTS.....6**
 - 3.1 General 6
 - 3.2 Network Bandwidth 6
 - 3.3 Voice Quality 7
 - 3.4 Classification, Prioritization (QoS) 8
 - 3.5 Network Devices 9
 - 3.6 Remote Sites 9
 - 3.7 Firewalls and NAT 10
 - 3.8 Network Assessment 10
 - 3.9 Secure VoIP through IPSec 11
- 4 HARDWARE REQUIREMENTS12**
 - 4.1 General 12
 - 4.2 Server Hardware 12
 - 4.2.1 SIP Gateway 12
 - 4.2.2 Call Control Server 12
 - 4.2.3 SIP Signaling Proxy Server 12
 - 4.2.4 Database Server 12
 - 4.2.5 SIP/RTP Proxy Server 13
 - 4.2.6 Voice Mail Server 13
 - 4.2.7 IVR Server 13
 - 4.2.8 Web Portal Server 13
 - 4.2.9 Combined Server 13
 - 4.3 Server Environment 13
 - 4.4 Gateway Connection 14
 - 4.5 Server Software Platform 14
 - 4.6 PC-based Soft-Phones (Software Client) 14
 - 4.6.1 Minimum Requirement Client PC 14
 - 4.6.2 Audio Devices and Head Sets 14
 - 4.7 IP-Telephones, Adaptors and Other SIP Devices 14
 - 4.8 Faxes and Modems 15
- APPENDIX A: NETWORK CHECKLIST16**
- APPENDIX B: NAT TRAVERSAL WITH RTP PROXY18**

1 IP-BASED ENTERPRISE TELEPHONY

Swift IP has a standard based and open platform, Swift IP, for business enterprise telephony. The IP-telephony technique makes the solution more price efficient, more scalable and more efficient especially in geographically distributed installations. We offer solutions for small and large businesses.

For detailed descriptions of the Swift IP product and functionality, refer to Swift IP product documentation.

In this document the general system requirements for a successful implementation of VoIP and Swift IP are outlined.

1.1 Implementation Quality

Swift IP is a complete software solution for business telephony users. Ultimately, the quality of the implementation will be measured in terms of user satisfaction. The total quality and user experience depends on a number of factors. In a Swift IP installation important factors are the hardware platform, such as servers, phone devices and softphone PCs, and the network infrastructure, such as LAN equipment, WAN links and traffic load. In general the user satisfaction is dependent on the following criteria:

- Availability – Can users make calls when they want ?
- Voice quality – Is the voice quality of VoIP calls good enough ?
- Reliability – Are calls dropped or interrupted before they are completed ?
- Accessibility – Can users contact everyone they need to ?
- Feature set – Will features similar or better to those expected by the users be available ?

The latter criterion is fulfilled by the rich feature set of the Swift IP software, but the first four are very dependent on the quality of the overall implementation.

Using VoIP technology and Swift IP have a number of advantages, such as reduced costs and increased efficiency in distributed organizations. The technology offers the company a flexible, coordinated telephony platform with a wide variety of functions and features, but the overall success of an implementation is dependent on effectively planning, implementation, tuning and maintaining of all components in the system.

2 ARCHITECTURE

Swift IP has based Swift IP on standardized components and on established industry standards. The system is based on a soft PBX application platform. The platform is open and flexible to meet the demands from both small and large enterprises as well as Call Centers of all sizes. The Scalability and modularity cater for cost efficient solutions in various applications. The platform has been in heavy use in call center installations since mid 2001 and has a proven record of high availability and reliability. It has lately been deployed as an “IP-Centrex” platform for business telephony service providers and as CPE IP-PBX installations to replace traditional PBX systems. With the current products offered by us, the platform forms a complete base for all kind of business telephony.

The core component in the system is the patented software call control module. Based on this core call control platform there are a number of applications, options and 3rd party interfaces offered.

The system is based on standard Intel-based hardware and the software is based on standard Microsoft Windows operating system. The Standard platform gives a unified and well-known platform for system maintenance, support and security.

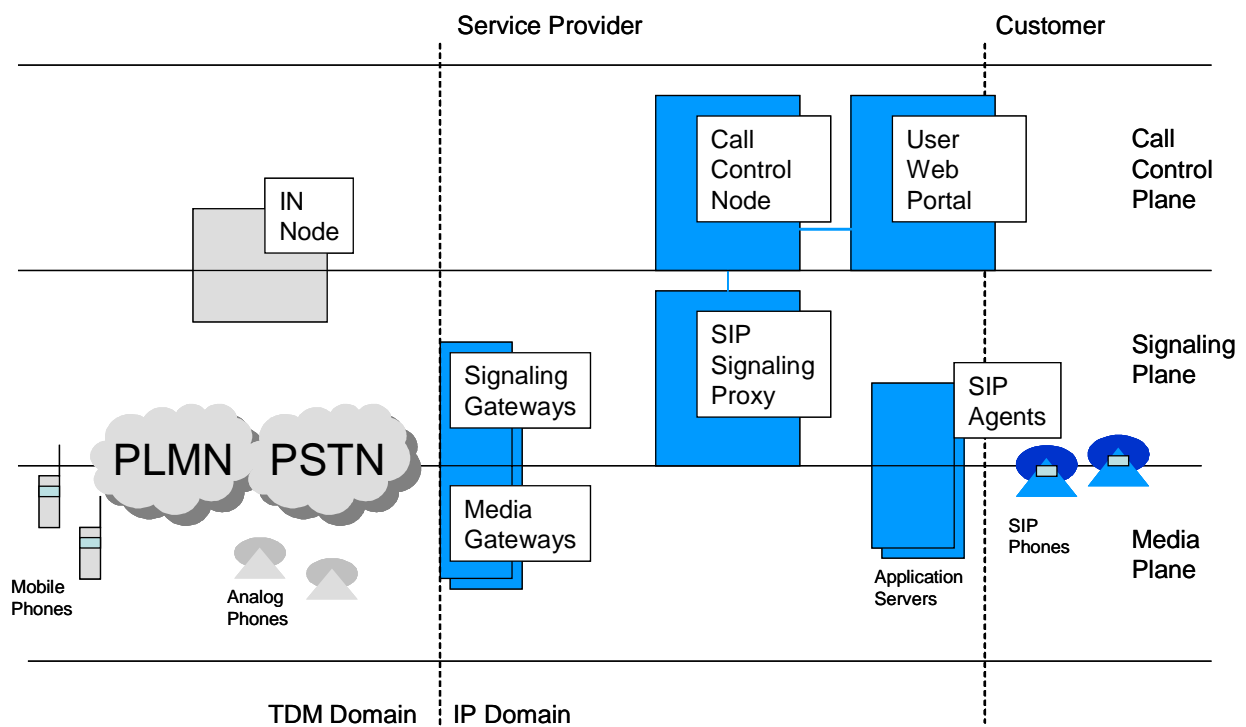


Fig. 1. System components (schematic)

2.1 System Interfaces

All telephony traffic in the IP networks follows the SIP standard (RFC 3261, RFC 2327). The system includes an advanced SIP server and all SIP standard compliant terminals and media servers in the system. The system is connected to the IP network via an IEEE 802.3 (Ethernet), 10/100 Base-T RJ45.

The connection to the PSTN network is generally done via a standard SIP gateway. Typically connected with an ISDN Primary Rate Interface (PRI), ETSI ISDN NET5 (30B+D), Euro ISDN. There is also optional support for connections E1 and SS7 trunks. Digital trunks to PSTN and/or legacy PBX:es are usually connected via RJ45 connectors.

3 NETWORK REQUIREMENTS

3.1 General

IP-based telephony provides lower costs and better flexibility than traditional telecom systems. With modern data communication solutions a complete unified solution including both data and telephony can be provided regardless of location (that is, headquarters, branch office, telecommuter, mobile worker).

Basic quality requirements must be fulfilled to ensure voice quality and reliability.

In general the entire LAN infrastructure must be based on switched technologies (100 Mb/s Ethernet). To ensure a stable level of quality, no shared resources should be used locally. If shared network resources are present, these should have utilization of 30% or less, or equipped with QoS functionality with ability to prioritize IP-telephony traffic.

Voice quality is only as good as the quality of the weakest network link.

Based on the experiences from different VoIP implementations it is clear that the planning of network and infrastructure is one of the most important aspects in a successful deployment. This chapter addresses the many aspects of planning the infrastructure for VoIP and the factors that impact it.

In this chapter we will discuss:

- **Network capacity (bandwidth):** Bandwidth utilization of voice devices.
- **Voice quality:** Factors that can affect voice quality.
- **Quality of Service (QoS):** Software for switches and routers to prioritize voice traffic.
- **Network devices:** Points to consider when examining your network devices.
- **Remote sites:** How remote sites might affect your network.
- **Firewalls and NAT:** How firewalls and NAT devices affect your voice traffic.
- **Network assessment:** Why a detailed network assessment is critical to the success of a voice network deployment.

3.2 Network Bandwidth

Considering how the SIP-based Swift IP platform operates it is important to factor in voice over IP bandwidth requirements. VoIP bandwidth is the combination of a variety of factors: the CODEC used (see Voice Compression below), the underlying network path (Ethernet, frame relay, ATM), the number of calls being handled (call volume), and the position of the Swift IP Servers relative to end stations. Each of these factors need to be accounted for when sizing a SIP-based VoIP network.

Most network requirements are based on the maximum traffic load. The planning phase should therefore start with traffic load calculations. It is important to determine what the peak network load is and when it occurs. Traffic load determination is basically the same for IP telephony network as within traditional telephony traffic modeling. In normal business telephony scenarios the maximum number of concurrent calls can be estimated to 10% of the total number of extensions. In small businesses a calculation based on the actual business situation must be done. Many calculators are available to determine call volumes, such as Erlang.com (www.erlang.com). The biggest difference is, instead of acquiring a voice trunk, you will use the trunk amount as a multiple against which you apply the CODEC bandwidth. All audio paths through every network aggregation point must be accounted for. The bandwidth requirements must be fulfilled end to end.

Based on call flows and call volumes the bandwidth requirements can be determined. Various network and phone vendors support a range of voice compression algorithms for assessing VoIP bandwidth. Table 1 shows some characteristics of commonly used VoIP CODECS. Note how delay is affected by the CODEC.

Method	CODEC	Data Rate	Delay (msec)
PCM1	G.711	64 kbps	0,75
CS-ACELP	G.729a	8 kbps	10
MPMLQ	G.723.1	6.3 kbps	30

Table 1: Commonly used VoIP CODECS

We recommend the use of the G.711 CODEC end-to-end, unless lack of capacity requires compression. The G.711 CODEC offers the best voice quality, since it performs no compression, introduces the least delay, and is less sensitive than other CODECs to packet loss. Other CODECs, like G.729 and G.723, consume less bandwidth by performing compression, although doing so introduces delay and makes the voice quality very sensitive to lost packets. This does not mean you can't use G.729 across your wide area network — just make sure your WAN has little or no packet loss and minimal delay before considering a high-compression CODEC.

Note that the CODEC chart in Table 1 specifies only unidirectional (one-way) audio. We strongly recommend to only use full duplex devices and connections. The cost in bandwidth may double if your link is not full-duplex. Make sure you take this into account when sizing your network.

Also, the bandwidth consumed is usually more than the optimal data rate shown in Table 1. In most TCP/IP networks, for example, Ethernet, RTP and TCP/IP headers increase the bandwidth requirements for a G.711 voice call from 64Kbps to 90Kbps. You can verify actual bandwidth usage with a VoIP calculator (www.voipcalculator.com).

Finally, no matter which CODEC you use, it should be used consistently across your network. Moving from G.711 to G.729 across various points, for instance, will increase the total delay, risking echo problems, and also the decompression/compression process will negatively affect voice communications quality.

VoIP impact on the network is estimated by taking the bandwidth per call and extrapolating with the number of concurrent calls expected to be handled during peak hour. The expected concurrent data traffic volume is added, resulting in the overall total bandwidth need. As a general rule, network utilization should not exceed 80% of the available bandwidth during peak load times.

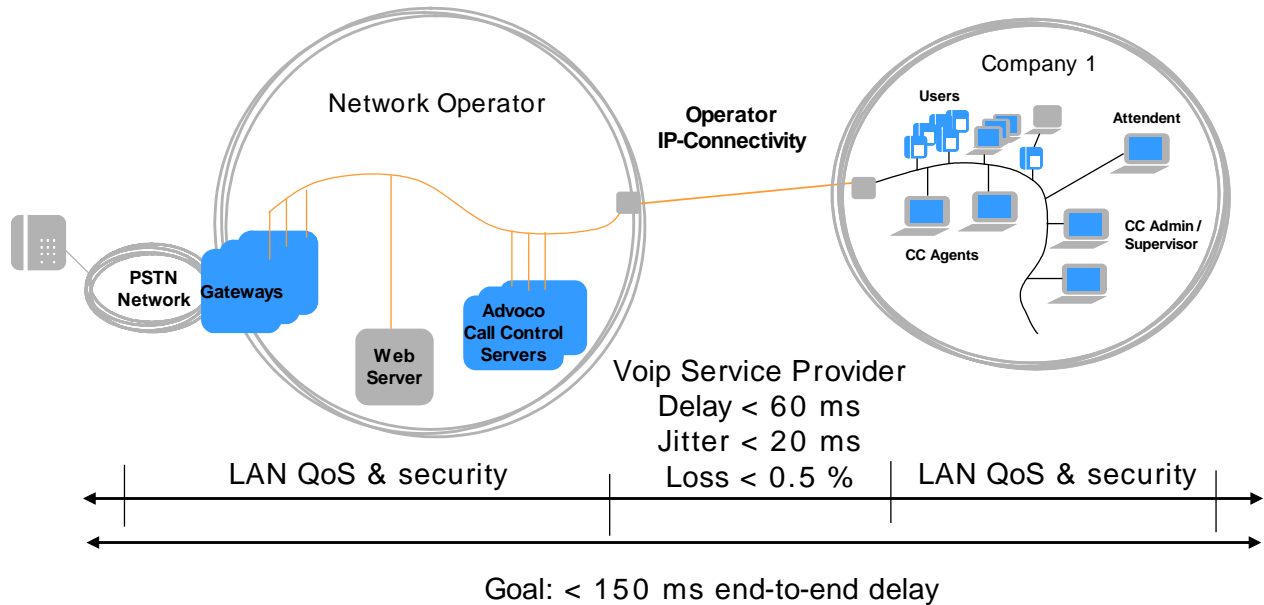
3.3 Voice Quality

End-to-end latency introduced by the networks is a problem that may lower the voice quality and introduce problem with echo. It is therefore imperative to avoid network components that introduce unnecessary latency. In particular the number of routers and firewalls in the voice traffic path should be minimized. To avoid latency problems the total end-to-end latency should be lower than 150 ms. More delay will result in “half duplex” behaviour and call participants will often talk simultaneously or wait at the same time for the other person to speak. Total latency is calculated by adding up the different delays introduced by the components involved in the call. A modern switched layer 2 LAN, connected to the access router, adds very little to this latency. In case of additional routers and firewalls in the customer network the total latency must be estimated or measured to ensure low total latency.

The components adding up to the total delay are:

- Codec delay – end point delay for handling and coding the audio to IP packets. Atypical value is 10 ms in Swift IP.
- End to end transport – transport network delay, time for the IP packets to move from one end point to the other.

- Network equipment – time needed to travel through all network equipment between end points
- Jitter buffer – processing and buffering time needed to compensate for variations and faults in network performance. In most cases totalling to 60 ms.



In general the total delay can only be reduced by minimizing the number of network “hops” needed to traverse the network, and/or upgrading to newer and more efficient network equipment.

Jitter is variation in latency. On low speed WAN connections (in practice 768 kb/s or below) jitter can become a problem that affects voice quality. Jitter should be kept below 20 ms. A technique called LFI (Link Fragmentation Interleaving), is used to reduce jitter by fragment large data frames into regularly sized pieces and to interleave voice frames into the flow. This places bounds on jitter by preventing voice traffic from being delayed behind large data frames. LFI is implemented by the routers handling the WAN-connection. A less sophisticated measure is to reduce the frame/packet size in all routers.

Packet loss, the loss of frames between end points, is a problem that typically can occur in situations where network components are overloaded. In most cases packet loss is below the IP-telephony quality threshold of 1 %. The G.711 codec includes a packet loss concealment technique that can handle 1% of packet loss. When using compression CODECS packet loss should be below 0,1%. Packet loss is reduced by controlling network traffic load and by ensuring proper bandwidth head room both in transport links and routing/switching devices in the path. Note that Fax and modems are very sensitive to packet loss and may have problems with packet loss levels that do not impair voice.

3.4 Classification, Prioritization (QoS)

In most cases there is no need for QoS considerations in a switched LAN. QoS tools should always be considered on shared network links (WAN connections) that has a utilization of more then 30%. In cases where the network link is reserved for IP telephony higher percentages can be accepted.

The routers handling the link perform classification of the traffic. The routers handling the link typically do the classification. The classification should mark RTP based traffic to be handled with high priority. This ensures minimized latency and packet loss for the IP telephony traffic.

There are a number of different techniques for classification and prioritization of packets. The most generic is to use specific end point addresses and different router path for VoIP. This technique can be used both when using VPN connections and on reserved links. Most end points also support a standard known as Differentiated Services (DiffServ) to mark voice packets.

Different vendors also will utilize this information for various queuing algorithms. Check with your network provider for QoS support and use the latest queuing techniques the provider recommends. Refer to the actual router vendor and network provider for detailed discussions and recommendations on prioritization.

3.5 Network Devices

Selecting the network elements that make up your organization's VoIP/SIP infrastructure is a critical task. These devices must provide the capacity, redundancy, interfaces and feature sets required to successfully deploy a SIP-based VoIP solution.

The following items are worthy of noting when selecting network devices for a VoIP deployment. Network devices in the VoIP network should deliver:

- Wire-speed operation while under heavy load with Quality of Service (QoS) services enabled
- Hardware-based QoS mechanism supporting IEEE standard 802.1p/Q
- Provisioning tools for delivery of IntServ and DiffServ QoS methodologies
- Switching fabric capable of sustaining network bandwidth

Even if most data network today are built with modern and capable devices, make sure that all components are designed and configured for VoIP deployment. Refer to the actual device vendor and network provider for detailed discussions on network devices and how to best ensure high quality for VoIP.

3.6 Remote Sites

Many distributed organizations look to a VoIP network to link regional and local branch offices (and add new ones), to centralize call control between sites, and to avoid toll charges by sending calls over their existing data network. They also see a VoIP network as a vehicle for globally deploying data applications to remote offices — without having to install expensive equipment at each site.

Unfortunately, wide area networks can create new challenges and actually make existing problems worse. In addition to the network challenges they face, multi-site organizations must also consider those services that are critical to daily business functions at each remote location.

In a VoIP deployment, all calls, typically, come in through a single entry point (at a main site or at a service provider central office) and are routed through that point over the data network to the end station.

Remote sites, however, can be connected in different ways to the main office and/or a service provider. One common way to solve data communication requirements between the sites is to use VPN connections over Internet. These links are secured by IPSec between firewalls at each site. When introducing VoIP on this links it must be ensured that the firewalls and the Internet connections have the capacity needed to handle both the data communication and the VoIP traffic. Also note that QoS control will not be possible on these links.

A more controlled way of deploying VoIP to remote sites is to use dedicated WAN links between the sites. In this case the connections are handled by a service provider who can guarantee throughput and QoS on the links.

Finally, ensure that the inter site traffic will add to the overall requirements and be sure to account for all audio path. Enhanced services like accessing voice mail, IVR functionality and conferencing must also be taken into account when dimensioning the infrastructure between sites.

3.7 Firewalls and NAT

Firewalls in general are not capable of handling IP telephony very well. Network Address Translation (NAT) is being used as the general mechanism to protect privacy and unfortunately NAT is a big problem for VoIP communication, mainly because IP addresses are exchanged within the SIP signaling between endpoints. There are four types of NAT used in firewalls and routers today: Full Cone, Restricted Cone, Port Restricted Cone and Symmetric. To be able to support different types of NAT there are several strategies to solve the problem, but none of them is a complete or satisfying solution. At the moment, a combination of SIP and RTP Proxy provides the best solution. However the area is thoroughly covered by standardization bodies and new solutions will emerge.

Some firewalls, Application Layer Gateways (ALG), have explicit support for SIP and can handle SIP traffic efficiently. These are SIP aware and often includes a SIP Proxy and Registrar. Examples are firewalls from Ingate and Cisco. To really benefit from these firewalls a homogenous infrastructure using the same type of firewalls needs to be deployed. Where that is possible the ALG approach has advantages and provides a secure solution.

Most SIP-phones and SIP devices support the STUN-protocol for NAT traversal. Most NAT firewalls can be traversed with STUN, except symmetric NATs. STUN has a disadvantage in enterprise telephony as the protocol does not allow communication between SIP phones behind the same NAT firewall.

Combined SIP and RTP proxies provide a straight forward solution that enable communication through most NAT firewalls. By routing all communication through the proxy all phones will be reachable. Using an RTP proxy has one disadvantage and that is that all RTP communication to/from a device behind a NAT firewall will be routed through the proxy. Hence the bandwidth requirements are increased on the WAN links.

Firewalls on the server side have to be configured to allow traffic to and from the Swift IP server addresses. If the firewall not has support for SIP it must be configured to allow traffic on high port numbers (above 1024), or use VPN tunnels between the server sub net and the end points sub net.

It is recommended to always locate the servers on public IP addresses.

Refer to the Swift IP Configuration Guide for specific configuration examples.

3.8 Network Assessment

A very critical step in deploying voice over IP is to complete a network assessment for every portion of your network carrying VoIP traffic. This assessment should be conducted by a network engineer or technician experienced with both VoIP technology and your particular network vendor. The network assessment should include:

- Hardware and software inventories of every network device
- Detailed traffic analysis during normal and peak hours of network usage
- Review of current cable plant
- Detailed traffic planning based on peak call volumes
- Load testing of existing equipment

It is paramount to ensure that the data network is ready for VoIP, fully upgraded and tuned, before starting a VoIP deployment. The reality is that most data networks today aren't ready to carry good-quality voice conversations. Even if the network is modern and newly installed the configuration must be assessed for carrying VoIP. However, it's easy to assess whether a network is capable of supporting VoIP, since VoIP traffic can be simulated so its characteristics can be measured and analyzed. By simulating VoIP traffic your organization can make any and all changes needed in the network it uses, and can reasonably assure network success before launching a VoIP deployment.

3.9 Secure VoIP through IPSec

Especially in IP Centrex service provider configurations the use of IPSec based tunnels between the service providers back bone network and the customers LAN network is an alternative.

The use of IPSec tunnels ensure security and also makes IP addressing between the service provider and the customer networks possible. The VPN firewalls used to implement the IPSec tunnels must be dimensioned to handle all concurrent calls on each subnet. The central VPN firewall must have throughput enough to handle the total traffic volume from all customers, and it must be ensured that the IPSec handling does not introduce to much delay. Disadvantages in using IPSec are that the load on the central firewall can be high and that, in general, the use of IPSec tunnels requires that each customer site has unique IP subnets. These disadvantages restrict the use of IPSec to special cases where extra security is mandatory.

4 HARDWARE REQUIREMENTS

4.1 General

Swift IP is based on standard hardware components and adheres to standard environmental requirements. This chapter describes general requirements servers, gateways, clients and terminals.

Specific requirements and configurations for an installation are always determined in a pre-study before the installation starts.

4.2 Server Hardware

The central part of an Swift IP installation is configured by a number of hardware servers. In smaller installations Swift IP can be configured on one single server, but with additional functionality and increasing number of users, additional servers are needed.

In the following Swift IP general recommendations and requirements on server hardware are described. Always consult the hardware vendors for specific recommendations.

We recommend to use well known, proven server hardware solutions with hot plug RAID disks and redundant power. UPS or other secured power arrangements are recommended. Refer to the Swift IP configuration Guide for specific hardware configuration examples.

4.2.1 SIP Gateway

The gateway act as a signaling and media gateway between the PSTN network and the IP network. In some installation the gateway may also interface a traditional PBX. For full functionality gateways with digital connection to the TDM network are recommended (ISDN BRI/PRI and/or SS7 interfaces). The gateway must comply to the SIP (RFC 3261, RFC 2327) standard.

For small and mid size installations Vegastream gateways are recommended. For larger installations and SS7 installations AudioCodes gateways are recommended.

4.2.2 Call Control Server

The call control server controls the routing of calls in the system. The load on the call control server is usually low.

4.2.3 SIP Signaling Proxy Server

The SIP signaling proxy is a signaling proxy for all SIP signaling in the system. The signaling proxy is a combined SIP Registrar, proxy and B2BUA. All signaling but no media is routed through this server so in most installation the SIP signaling proxy and the call control node can be on the same server.

4.2.4 Database Server

The database server runs Microsoft SQL server and is used to store configuration data, directory and presence/availability information. It is also used for storing of statistics logs. The database server should be dimensioned as a standard MS SQL server hardware. In most installation the database can be installed and executed on the same server as call control and SIP signalling proxy.

4.2.5 SIP/RTP Proxy Server

The SIP/RTP proxy is used to handle far end NAT traversal (SIP end points behind NAT firewalls). The SIP/RTP proxy is a combined SIP proxy and RTP proxy. All SIP signaling is routed through this server and also media (RTP) if any of the end points involved in a call is behind a NAT firewall.

We recommend the Brekeke SIP Server which is a well proven and Swift IP compatible SIP/RTP Proxy for NAT traversal. It can also be collocated together with the voice mail server or installed on separate hardware in larger installations.

4.2.6 Voice Mail Server

The voice mail server hosts the Swift IP voice mail system. For safety this server is recommended to use RAID disks.

4.2.7 IVR Server

The IVR server hosts the Swift IP interactive voice response system. It is used for implementing IVR menus, welcome messages and ACD queue messages. A good general purpose server is recommended.

4.2.8 Web Portal Server

The web portal server runs Microsoft IIS server and is used by the users to control their communication profiles in Swift IP. The web portal server should be dimensioned as a standard MS IIS server hardware.

4.2.9 Combined Server

In installation up to a few hundred users all components can execute on the same server machine. A typical platform for a single combined server is the HP Proliant ML380 server, a mid size database and multipurpose server.

4.3 Server Environment

Swift IP is typically installed in rack configurations.

To allow servicing and adequate airflow, observe the following spatial requirement for the installation.

A standard rack is typically 200 cm high, 60 cm wide and 120 cm deep.

Recommended minimum clearance in front of rack: 64 cm

Recommended minimum clearance behind of rack: 76 cm

Recommended minimum clearance from the back of the rack to another rack: 122 cm

Servers draw in cool air through the front door and expel warm air through the rear door. Therefore the front and rear rack doors must be adequately ventilated.

To ensure continued safe and reliable equipment operation, install or place the system in a well ventilated, climate controlled environment.

Recommended operation temperature range 5 – 35 °C.

Recommended operation relative humidity range 5 – 95 %.

UPS is recommended.

4.4 Gateway Connection

Advoco Software recommends the use of Vegastream SIP gateways in Swift IP. Refer to the chosen SIP gateway for details on how to connect and configure the gateway.

4.5 Server Software Platform

Swift IP servers are implemented on Microsoft Windows. As standard, Microsoft Windows 2003 server is used. Advoco recommends to always install the latest Microsoft security updates.

Swift IP servers also runs on Windows XP Professional. Currently only the Windows 2003 server based configuration is fully tested in production.

The database server uses Microsoft SQL 2000 SP3A. The system also runs on Microsoft Data Engine, MSDE, in smaller installations.

4.6 PC-based Soft-Phones (Software Client)

A modern PC with Windows 2000 or Windows XP has the performance and capacity to be an efficient IP-telephony end point. The Swift IP soft phone application together with a head set makes the PC to a complete and very efficient telephony system. Call Center agents and switchboard attendants always uses the Swift IP PC-based softphone.

Alternatives to the Swift IP Softphone are:

- Eyebeam from Counterpath
- SJPhone from SJLabs

4.6.1 Minimum Requirement Client PC

- Pentium 400 MHz
- 1 GB HDD
- 256 MB RAM
- Windows 2000 SP4 or Windows XP SP2
- Headset (USB-connected headset recommended)

In general portable PCs are less capable of handling real time applications. When using a portable for the soft phone application Advoco recommends 700 MHz processor as a minimum.

4.6.2 Audio Devices and Head Sets

Advoco recommends an extra dedicated audio board to be installed in all PCs used as soft phones. The easiest way to achieve this is to use USB connected headsets. These headsets are connected directly to a USB port and include the audio board device.

Well performing USB headsets are:

- GN Netcom USB adapter GN 8110 & GN Netcom GN 2100 (professional telecom head set)
- Plantronics DSP300 USB (lower price alternative)

4.7 IP-Telephones, Adaptors and Other SIP Devices

The Swift IP system is based on SIP. SIP is an international standard with broad acceptance. A number of vendors support this standard and there is a broad range of SIP compatible equipment on the market.

To ensure functionality and quality, and to minimize configuration and adaptation work, we have tested and recommends certain SIP devices to be used in the Swift IP system. The following devices can be used with Swift IP.

SIP IP Telephones:

- Linksys SPA-901 (1 line SIP phone)
- Linksys SPA-941 (2 or 4 line SIP phone)
- Linksys SPA-942 (2 or 4 line SIP phone, LAN switch)
- Grandstream BT-200 (2 line SIP phone, LAN switch)
- Grandstream GXP-2000 (4 line SIP phone, LAN switch)

SIP analogue adaptors, ATA (FXS ports for connecting analogue standard telephones, DECT or fax equipment):

- Linksys SPA-1001 (1 FXS port, 2 lines)
- Linksys SPA-2002 (2 FXS ports, 2x2 lines)
- Linksys PAP2 (2 FXS ports, 2x2 lines)
- Grandstream HT-386 (2 FXS ports, 2x2 lines, T.38 Fax support)
- Grandstream HT-486 (2 FXS ports, 2x2 lines, T.38 Fax support, LAN switch)

Combined SIP ATA and broad band router:

- Linksys RT31P2-AT (2 FXS ports, 2x2 lines, 4 port LAN switch, WAN port)

All IP-telephony equipment supporting SIP can in principal be used in the Swift IP system. In general the equipment needs to be configured and tested to work with Swift IP components. to the system.

4.8 Faxes and Modems

Special considerations are necessary when using fax machines and data modems over VoIP. In general both fax and modem traffic are difficult to handle over IP. To ensure best throughput G.711 must be used and transfer speeds must be limited to at most 14 400 baud (V.17) for fax and 9 600 baud (V.29) for modems. Both fax and modems requires high quality IP networks to ensure stable transmissions. For fax a special protocol T.38 is used to send fax out of band. Some but not all ATA devices on the market supports T38. Refer to the hardware recommendations for a list of T.38 enabled ATA devices. The use of T38 for fax transmissions is strongly recommended.

Also note that both fax and modems are extremely sensitive to packet loss and packet losses in the network can force the use of even lower transmission rates.

APPENDIX A: NETWORK CHECKLIST

Good quality voice-over-IP (VoIP) conversations depend on maintaining strict constraints for packet loss, delay, and jitter (contrast this with traditional data network traffic, where the focus is on response time or throughput). We've found these design tips successful when deploying VoIP in a data network.

1. Use the G.711 codec end-to-end, unless lack of capacity requires compression. Codecs are the hardware or software used to convert from analog to digital and back. The G.711 codec gives the best voice quality, since it does no compression, introduces the least delay, and is less sensitive than other codecs to packet loss. Other codecs, like G.729 and G.723, consume less bandwidth by doing compression, but this introduces delay and makes the voice quality very sensitive to lost packets.
2. Keep packet loss well below 1% and avoid bursts of consecutive lost packets. Packet loss occurs because of congestion or electromagnetic noise. It can also occur when jitter is high and the jitter buffer is too small to compensate. Increased bandwidth and good tuning can often reduce network congestion, which, in turn, reduces jitter and packet loss.
3. Use a small speech frame size and reduce the number of speech frames per packet. When voice traffic is a stream of small packets, the effect of one being lost is less severe than losing a big packet with multiple speech frames inside it. A good target is 20ms of speech per frame, with one frame per packet. Of course, using small packets increases the total bandwidth requirement, because each packet requires its own fixed-size header.
4. Always use packet-loss concealment (PLC). Packet-loss concealment masks the loss of a packet or two by using information from the last good packet. Packet loss can occur randomly or in bursts. PLC helps with random packet loss. The cost for doing PLC is minimal, since it's already usually part of the codec processing.
5. Actively minimize one-way delay, keeping it below 150ms. One-way delay = propagation delay + transport delay + CODEC delay + jitter buffer delay. Voice quality degrades quickly when the total one-way delay is greater than 150ms.
6. Propagation delay is the time to travel the physical distance from end to end. For example, it may take a signal about 100ms to go from Dallas to Singapore. When the traffic has to cover long distances like this, make sure the network path is as direct as possible.
7. Transport delay is the total time spent inside each of the devices in the network, like switches, routers, gateways, traffic shapers, and firewalls. Some devices add more latency than others; for example, a software firewall running on a slow PC adds more delay than a dedicated hardware-based firewall. Look at the number of hops traveled by the voice traffic. Reduce the number of hops and find ways to reduce the latency in the devices that are the worst offenders.
8. CODEC delay is the fixed time needed for the codec to do its job. The G.711 codec imposes the smallest delay. In contrast, the codecs that do compression add delay ranging from 25ms to 67ms. Also, avoid converting from one codec to another along the network path.
9. Jitter buffer delay is used to dampen variations in packet arrival rates. If the network delay is low and the jitter is high, you can afford to have a larger jitter buffer than in a network where the delay is already high.
10. Avoid using slow speed links. If you're considering VoIP, don't consider using it extensively on slow serial links. Upgrade the bandwidth on those paths so the VoIP traffic and existing data traffic have plenty of room.
11. Use data packet fragmentation for slow-speed links. Routers use data packet fragmentation to cut large packets into smaller ones, and then reassemble them at the other end. On slow links, this helps assure that small VoIP packets don't get delayed behind large data packets. Enable it for link speeds below 1 Mbps.

12. Use priority scheduling for voice traffic. Voice traffic has stricter packet-loss, delay, and jitter requirements than traditional network traffic, so it makes sense that it should receive an appropriate quality of service (QoS). A preferred QoS method is to mark VoIP packets with the DiffServ setting for Expedited Flow (EF). Also, consider using Weighted Fair Queuing (WFQ), which raises the priority of low volume traffic. Giving VoIP higher priority helps routers decide which traffic to forward first when congestion occurs. Watch for adverse affects on the existing data traffic, though.
13. Get your data network ready for VoIP, fully upgraded and tuned, before starting a VoIP deployment. Most data networks today aren't ready to carry good-quality voice conversations. It's easy to assess whether a network is ready or not, though, because VoIP traffic can be simulated and its characteristics can be measured and analyzed. This means you can make all the changes needed in the network and assure their success before beginning a VoIP deployment.

APPENDIX B: NAT TRAVERSAL WITH RTP PROXY

We recommend the use of an RTP Proxy server to handle NAT traversal. The solution is based on an RTP Proxy in the middle of the RTP flow between endpoints. The RTP Proxy acts as the second endpoint to each of the actual endpoints that are attempting to communicate with each other. A combined SIP/RTP Proxy server in the middle of the SIP flow manipulate the SDP in such a way as to instruct the endpoints to send RTP to the Proxy instead of directly to each other. The Proxy sets up its own internal mapping of a session, noting the source IP:port of each endpoint sending it RTP packets. It then uses that mapping to forward the RTP from endpoint to endpoint.

The following is a typical call flow that might be instantiated between a User Agent behind a symmetric NAT and a voice gateway on the open Internet:

1. UA client sends an INVITE to the SIP/RTP Proxy through the NAT
2. The SIP/RTP Proxy sets up a session internally.
3. The SIP/RTP Proxy assigns an available pair of ports to this Call and then modify the SDP information of the received INVITE request.
4. The SIP/RTP Proxy forwards the SIP INVITE request with modified SDP (reflecting the SIP/RTP Proxy's IP:port) on to the UA Client 2.
5. The second UA client replies (in the 200 OK) with its own SDP information including the port to receive RTP packets.
6. The SIP/RTP Proxy registers the IP:port of UA Client 2 (if the UA client 2 was also behind a NAT, then the SIP/RTP Proxy would wait for packets from the Client 2 before setting the IP:port to forward RTP on to UA).
7. The SIP/RTP Proxy forwards the response upstream back to the UA after modifying the response SDP with the RTP IP:port of the SIP/RTP Proxy.
8. UA begins sending RTP to the IP:port it received in the 200 OK – to the SIP/RTP Proxy.
9. The SIP/RTP Proxy notes the IP:port that it received the packet from (for the first packet), and passes on the packet to the IP:port of the Client 2.
10. RTP packets proceed from the Client 2 to the SIP/RTP Proxy.
11. The SIP/RTP Proxy forwards those packets to the client (according to IP:port that it saved when it received the first RTP packet from the client). When BYE is received by the SIP/RTP Proxy, it tears down the session.

The following considerations should be noted:

1. The client will always need to send and receive RTP on the same port. (Most SIP devices use this scheme.)
2. This solution will work for all types of NATs, but because of the delay associated with the SIP/RTP Proxy (which may be substantial, especially if the SIP/RTP Proxy is not close to at least one of the endpoints), it should not be used unless a NAT is involved.