

Methodology, rules and recommendations for VoIP solutions engineering

Summary :

1. Objectives

Implementing VoIP in a data network needs in most cases a complete engineering process as these solutions are integrated on the customers data network and may for example degrade the performances of the network.

One major point of this process is the feasibility analysis of a VoIP solution and the design of the solution.

The aim of this document is to help in this process by defining the methodology together with the main rules and recommendations for building successful VoIP solutions. It gives guidelines, warnings, etc... covering the main aspects of VoIP like QoS, security, IP addressing, etc...

This document intends to be as generic as possible and addresses VoIP solutions built around the OmniPCX 4400 as well as around Office/OmniPCX Office.

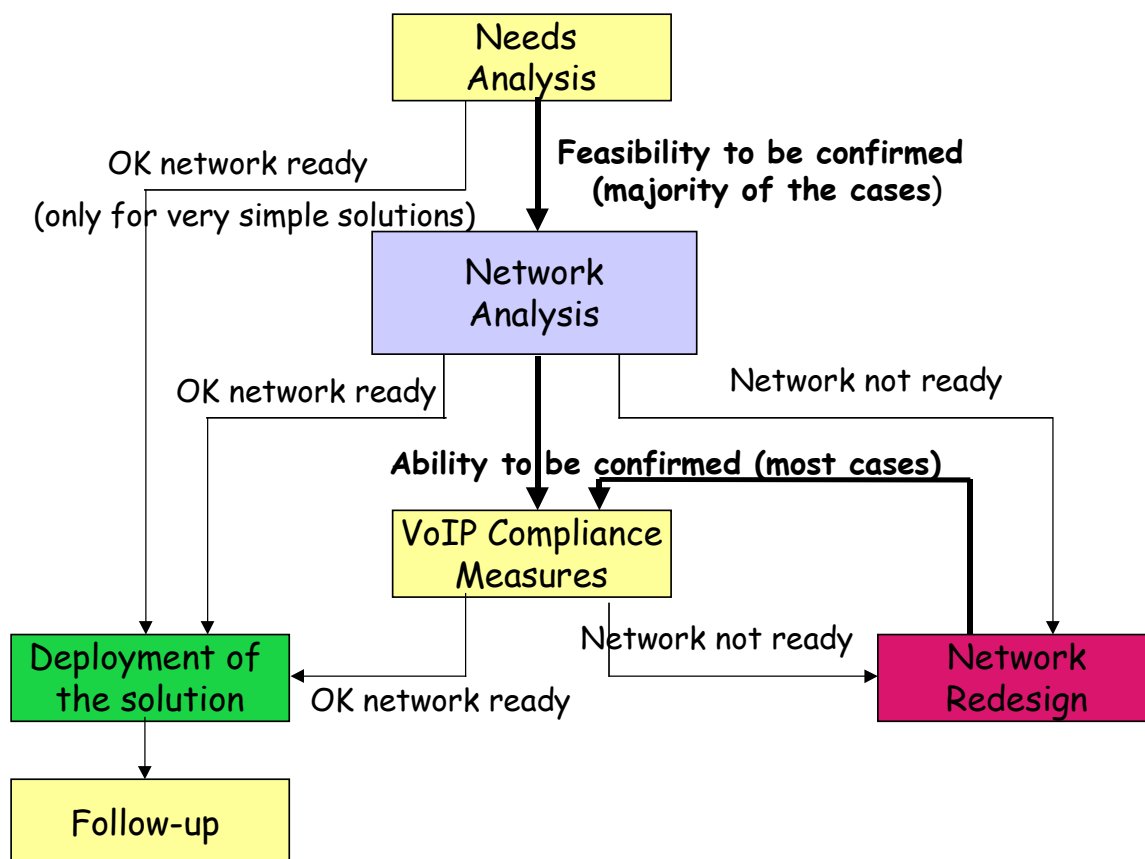
The target public are people in charge of pre-sales, consultants, technical experts of our distributors.

Remark : Installation and configuration rules directly related to our IP products (PBXs, IP Phones, ...) are not in the scope of this document. These informations can be found in the product documentations and their associated technical communications.

CONTENTS

1.	Objectives	1
2.	Reminder of the Global Process for VoIP projects	3
2.1	Phase 1 : Needs Analysis	3
2.2	Phase 2 : Network Analysis	4
2.3	Phase 3 : VoIP Compliance measures	5
2.4	Phase 4 : Deployment of the solution	5
2.5	Phase 5 : Follow-up/Maintenance/Supervision of voice traffic and quality	5
3.	Audit methodology for VoIP solutions and recommendations	6
3.1	Objectives	6
3.2	Reminder about VoIP Quality	6
3.3	VoIP solution involving LAN environments	8
3.3.1	LAN infrastructure analysis	8
3.3.2	Bandwith needs analysis for VoIP	10
3.3.3	Recommendations and warnings	12
3.4	VoIP over the WAN for multi-sites configurations	16
3.4.1	WAN infrastructure analysis	17
3.4.2	Bandwith needs analysis for VoIP	19
3.4.3	Recommendations and warnings	20
3.5	VoIP solution for single Remote worker or Mobile user	25
3.5.1	Infrastructure analysis	26
3.5.2	Number of simultaneous RAS Modem/VPN connections	27
3.5.3	Bandwith needs analysis at the central site	28
3.5.4	Recommendations and warnings	28
4.	General recommendations and warnings	29
5.	VoIP Compliance measures	33
5.1	Principle of VoIP compliance measurements	34
5.1.1	In a LAN environment	34
5.1.2	In a WAN environment	34
5.2	Methodology	35
5.3	Analysis of the measurements and conclusions	36
5.4	Recommendations & warnings	36
6.	Network Performance Audit	37
6.1	Objectives	37
6.2	When should a network performance audit be performed ?	37
7.	Conclusion	38
8.	ANNEX A Bandwith needs	38

2. Reminder of the Global Process for VoIP projects



2.1 Phase 1 : Needs Analysis

- ▼ Understanding of the customer context, activity, needs
- ▼ Identification of the appropriate VoIP solution
- ▼ Understand the **level of quality expected** by the customer (toll-quality, near toll-quality, best effort) and the **network availability required**

Conclusions :

- a) Network ready for VoIP => deployment of the solution

Applicable only in very simple cases : e.g. Local IP Telephony with Office where the network topology follows the recommendations for small configurations (see Network Topology recommendations for VoIP solutions inside the LAN).

- b) Network needs further analysis => Phase 2 : Network analysis (great majority of the cases)**

2.2 Phase 2 : Network Analysis

- ▼ Analysis of the existing data network, identification of network sensitive points
- ▼ Evaluate the level of performance of the network and bandwidth availability

Network Performance audit can be necessary to measure flows, equipments load etc...

(see § Network Performance Audit)

- ▼ Application of the engineering rules and recommendations
- ▼ Appreciate the ability or not of the network to support the VoIP solution (in terms of performance and bandwidth needs)

Conclusions :

- a) Network ready for VoIP => deployment of the solution
- b) Network not ready => Network Redesign
- c) Network probably ready but VoIP compliance measures are needed to confirm it => Phase 3 : VoIP compliance measures (strongly recommended in most cases)**

When the network is not ready to support VoIP, modifications of the infrastructure are required :

- Modification of the network architecture
- Increase of speed of the links
- Upgrade of routers
- Subnetting
- Etc...

Network Redesign will be lead by data specialists.

It will be followed by VoIP compliance measures to validate the new design.

2.3 Phase 3 : VoIP Compliance measures

This phase is not mandatory and depends from the results of Phase 1 and Phase 2 but is strongly recommended in most cases. In case of complex networks it must be the rule.

- ▼ Measurement of the main VoIP parameters (delay, jitter, loss of packets)
- ▼ Measures analysis
- ▼ Ensure bandwidth availability

Conclusions :

- a) Requirements respected (through maybe minor adaptations) => implementation of the solution
- b) Network not ready => Network Redesign

2.4 Phase 4 : Deployment of the solution

- ▼ Definition of the IP addressing plan, setup of QoS policy, etc...
- ▼ Installation
- ▼ Possible VoIP compliance measures to validate the good functioning

2.5 Phase 5 : Follow-up/Maintenance/Supervision of voice traffic and quality

Proactive management of the network is strongly recommended :

- ▼ Data network monitoring (behaviour of the links, use of bandwidth,...)
- ▼ Observation of incidents
- ▼ Recurrent VoIP compliance measurements

3. Audit methodology for VoIP solutions and recommendations

3.1 Objectives

Implementing VoIP solutions may need an evolution of the infrastructure to fulfill the requirements of VoIP which are mainly :

- network performance to ensure the expected quality of the voice (toll-quality, near toll-quality or best effort)
- bandwidth availability
- network availability to ensure the availability of the service
- security of the solution

The objectives of this audit methodology is :

- to help to determine if the data network fundamentally can support VoIP (**Phase 2 of the global process**)
- to ensure through on site tests that the network can support VoIP by providing enough bandwidth and by not imposing unreasonable delay, contributing to packet loss or causing jitter (**Phase 3 of the global process**)

Three typical VoIP solutions have been identified, each addressing specific questions. A global solution can combine all of these three solutions.

The methodology will be followed by generic recommendations and warnings as much as possible independent from the system involved (OmniPCX 4400 or Office).

3.2 Reminder about VoIP Quality

The level of performance required by the solution depends on the voice quality expected by the customer. For example, the first criteria can be the economic aspects prior to the voice quality itself.

The different level of quality can be roughly classified into three categories :

- **TOLL-QUALITY** = identical to a conventional system

Network Round Trip delay < 150ms

Jitter < 20 ms

Packet loss ratio < 1%

- **NEAR TOLL-QUALITY** = can imply some disruptions, unwanted signals, inability to recognize tone of voice and crackling (GSM level)

Network Round Trip delay < 400ms

Jitter < 50 ms

Packet loss ratio < 3%

- **BEST-EFFORT QUALITY**= metallic sounding voice, loss of syllables and dropouts (marine radio level)

Network Round Trip delay < 600ms

Jitter < 75 ms

Packet loss ratio < 5%

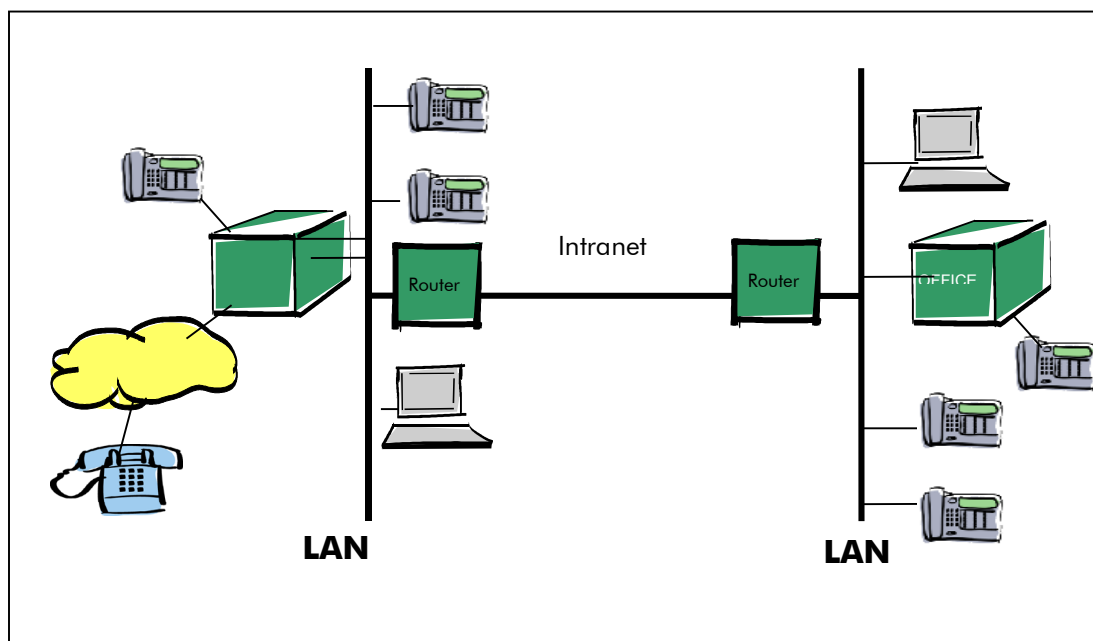
Remark : The Network Round Trip Delay **corresponds strictly to the delay introduced by the network**. The global end to end delay for a user corresponds to the network delay plus the algorithmic delay (compression/decompression) and the delay introduced by the components of the PBX (packetization, dejittering buffer,...) which is approximately between 80ms and 120ms.

This figures will be improved after the voice quality tests which are in progress.

3.3 VoIP solution involving LAN environments

This section deals with IP telephony solutions involving a LAN where we can find IP Phones and/or local 4980/Pimphony applications, external H323 gateways, etc ...

This LAN can be a small remote of a central site as shown in the picture below



3.3.1 LAN infrastructure analysis

The following questions have to be addressed when analyzing the LAN infrastructure:

Network Architecture

Objectives : identify the current topology, the components of the network, the potentialities for QoS e.g of the equipments and anticipate the impact of some equipments like firewall which can slow down the performances.

- network diagram
- cabling infrastructure
- number and distribution of PCXs, IP Phones, softphones, H323 terminals, gateways or gatekeeper over the network

- number and distribution of PC clients, servers, DHCP servers, TFTP servers , etc... over the network
- list of LAN segments involved with VoIP
- type of LAN (ethernet, FDDI ring, WLAN, LANE, extended LAN through optic fiber...)
- list of networks equipments involved with VoIP (switches, routers, firewalls, H323 Gateways/Gatekeeper ...)
- characteristics of these equipments (brand, type, software version, speeds, QoS mechanism supported like IP Tos/Diffserv, SNMP agent,...)
- list of VLAN segments (identification of groups, distribution of users, possibility of grouping on the same VLAN, possibility of allocating priority)
- distribution of the users over these VLAN segments
- reliability of the network (router duplication, etc...)

Applications running on the network

Objectives : identify the critical applications or applications which can generate heavy load on the network in order to understand their possible impact on VoIP and vice versa.

- list of servers with resident applications in particular applications such as Oracle, NetBios, ..., type of Operating System
- geographic distribution of the users for each applications
- synchronization process over the network like Database, directories, etc...

Network operation

Objectives : evaluate whether the performances of the network, the links capacity, the quality of service are compatible with the quality level required by the VoIP flow

- average LAN utilization + type of traffic (broadcast, applications...) and flow matrix
- peak periods on the LAN + % use during these peaks
- utilization of network equipments (switch, routers, firewalls, etc...) in terms of %CPU load, memory utilization, queuing drops etc...
- QoS implemented on the network (RSVP, ToS/Diffserv, 802.1p/Q, WFQ, etc...)
- Security policy (router filtering, proxy, access lists, etc...)
- Routing protocols in use (RIP, OSPF, etc...)

IP addressing plan

Objectives : understand the current IP addressing plan and anticipate potential impacts

- Identify the IP networks or sub-networks
- Check for each IP (sub)network the number of reminding addresses
- Type of addressing scheme (private/public)
- DHCP server plan
- Anticipate future extensions

Network management services

Objectives : identify tools which can help to manage the network, measure the performance of the network, make statistics

- Network management tools (HPoV, Ecoscope, ...)
- Network supervision tools (RMON,...)
- Elements which can be administered

3.3.2 Bandwith needs analysis for VoIP

Objectives : estimate the bandwith required to be compared to the available bandwith and anticipate network and traffic evolution. The network must be capable to support existing data flows + VoIP.

For this exercise the following informations are required :

- number of IP devices (TSC- IP Phones + 4980/Pimphony applications)
- distribution of IP devices and PCX over the LAN
- max number of legacy users in order to calculate the max number of simultaneous calls to legacy users (this traffic will be handled directly by the IP interface board)
- compression type : with (G723.1/G729A) or without compression (G711)

Assuming a traffic per user of 0.16 E (0.08 external traffic and 0.08 internal traffic) and a blocking factor of 1%, but this can change from one case to the other, the bandwith can be estimated as following :

- Global traffic in Erlang : $0.16 E \times \text{number of IP devices}$
- Number of « lines » needed : refer to an Erlang calculator with this global traffic and a blocking factor of 1%. This will give the number of « lines » which are required to support the voice calls of all the IP-devices.

- Global bandwidth estimation : number of « lines » x bandwidth needs for one call (see table in Annex)

The traffic generated for the signalling can be ignored.

- Bandwidth needs at the IP interface board level : will be obtained by considering the external traffic ($0.08 E \times \text{number of IP devices}$) + the traffic to the legacy users ($(0.08E/\text{legacy users} + \text{IP devices}) \times \text{number of IP devices}$)

Remark : these calculations assumes that all the IP devices are on the same LAN segment. If that's not the case, the bandwidth needs can be different from one LAN segment to the other depending on the number of IP devices attached on that segments.

Warning : these calculations assumes that the systems are able to manage direct IP flows between IP devices.

With a PC MS netmeeting or 4980 Nomadic VoIP which need to access the H323 gateway to call another IP device, the traffic on the LAN is doubled.

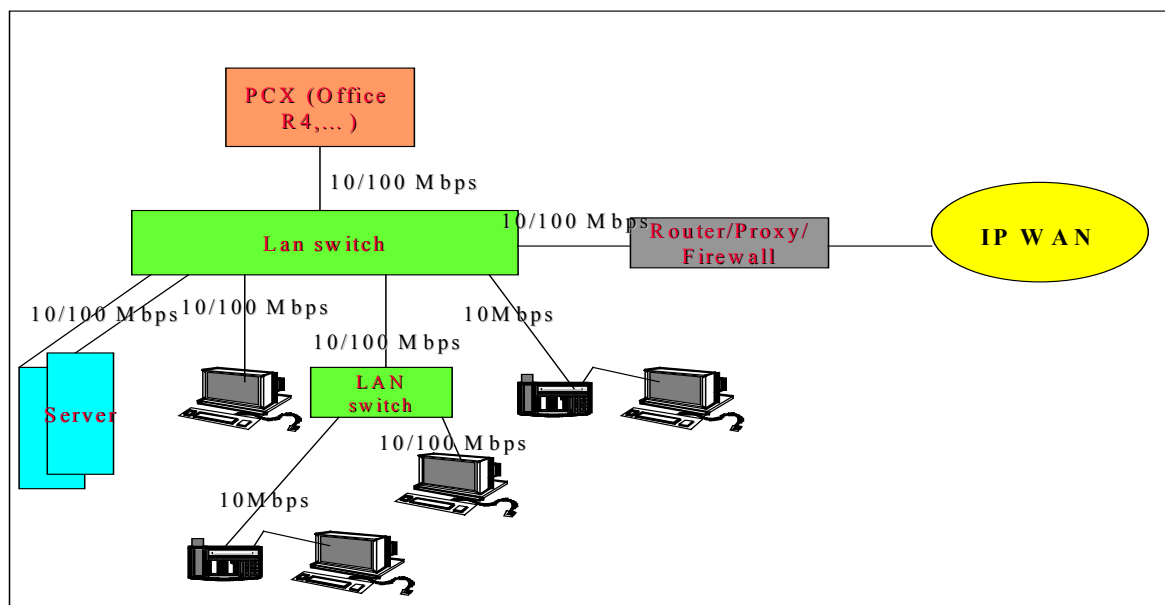
Warning : be careful on the operating mode of the LAN segments. In half-duplex mode (e.g. 10Mb/s half-duplex Ethernet), the real bandwidth needs on the link are the double.

3.3.3 Recommendations and warnings

NETWORK ARCHITECTURE :

Recommendation L1: topology recommendation for small configurations (e.g. Office/OmniPCX Office solution or branch office with OmniPCX 4400)

- The network core is 10 and/or 100Mbps switched. The VLAN (Virtual LAN) option is not necessary
- Servers (NT server, Novell Server, UNIX, LINUX- including external DNS/DHCP Server and H323 Gatekeeper), the WAN IP router, VoIP Interface boards and other LAN switches are directly connected to the main LAN switch (RJ45 cables/optical fiber).
- Other PCs and IP enablers can also be connected to this main LAN switch, or to other cascaded LAN switches (up to 4 cascaded LAN switches).
- number of IP devices (IP-Phones, PIMPHONY/4980) limited to 100



In this configuration, a LAN switch without QoS fits in most cases.

Recommendation L2: Check the conformity of the cabling infrastructure

The quality of the cabling has a great influence on the quality of the transmission (transmission errors, ...).

For example, category 5 cable is required for 100Mb/s links, category 3,4,5 cable is required for 10Mb/s links.

Ensure that the maximum distance for connection of the devices are respected.

Example : 100m maximum for a 10/100Base-TX media, 2000m maximum for a 10/100Base-FX Mono Mode Fiber, etc...

Recommendation L3 : limit the number of router hops within the LAN

Passing a router can add significant delays. VoIP Compliance measures are required if several routers have to be crossed.

Recommendation L4 : use LAN switches for the interconnection of the equipments

It is strongly recommended to connect any equipment (IP-PCX, TSC-IP Phone, IP interface board, 4980, etc...) to the network through a port of a LAN Switch instead of hubs.

Indeed with hubs, collisions can occur with any kind of frame (unicast/multicast/broadcast) and thus reduces the bandwidth per user.

With LAN switches, there are no collisions on full-duplex ports, each port having his dedicated bandwidth.

LAN switches are also recommended for security reasons, the VoIP flows beeing sent only to the concerned ports and not broadcasted to all devices on the network.

Use stackable LAN switches, instead of cascading LAN switches to avoid possible bottlenecks on the uplinks (Example : use a LAN switch of 96 ports instead cascading 4 switches of 24 ports).

Recommendation L5 : connect when possible the systems (OmniPCX 4400, Office R4,..) and the terminals on the same sub-network , on the same LAN switch in order to optimize the VoIP flows

Recommendation L6 : definition of voice VLANs to group IP-Phones and IP interface boards allows to separate voice and data traffic in order to increase the security in the LAN and limit broadcast domains.

It is recommended to define the members of the voice VLAN based on the port numbers (or preferably on the Mac address of the IP devices for mobility reasons) at the LAN switch level. As it is a LAN switch feature, this is independent from the support or not by the PCX of the 802.1p/Q tagging.

NETWORK OPERATION

Recommendation L7 : Optimize the data transfers on the LAN

Examples :

- clients and servers on the same sub-network, on the same LAN switch when possible
- to optimize the bandwidth in case of access to the Internet, introduce a Proxy which caches the most frequent accessed pages
- Implement « Load Balancing » : several physical Web FTP servers are seen as 1 logical server

ED	01	Methodology, rules and recommendations for VoIP solutions engineering		
D. Lienhart		11.21.2002	8AL 01200 1259 QRASA	13/42

- Differ operations which are big consumers of bandwidth when the network is less sollicitated (data base update, ...)
- Use of VLANs in order to reduce the broadcast domain to the ports belonging to the VLAN
- IP multicast in case of applications of type broadcast to group of users (video broadcast, on line informations...)
- Optimize broadcasts of stations (deactivate NetBui if not necessary, deactivate unused applications which generate broadcasts, etc...)
- Etc ...

Rule L8 : the Ethernet traffic in the network core in case of a shared link (with other stations e.g.) mustn't exceed 30 % in average and 50% in peak hours

Above, the number of collisions increases and the number of re-emissions too, leading to link congestion.

This is valid for 10Mb/s links as well as for 100Mb/s links.

On a dedicated 10Mb/s half-duplex Ethernet link (direct connection of the IP interface board to a switch e.g.), it means 30 communications maximum in G711 and 60 communications in G723.1 or G729A (without VAD).

Warning L9 : routers, firewalls within the LAN can increase significantly the transit delay.

Check their routing capacity, CPU power, load, memory utilization etc... VoIP compliance measures are recommended in this cases.

Warning L10: routers can block UDP traffic for security reasons even on a LAN and thus the voice flows

In these conditions, IP Phones or 4980/Pimphony don't work, in particular voice flows don't transit. And opening of UDP ports is not recommended for security reasons.

Check the access lists configured.

QoS

Recommendation L11 : except in well mastered conditions (e.g. the topology recommended above), implement an end-to-end QoS Policy in the LAN in order to be able to maintain a stable quality of service when for example the data flows on the network evolves.

This can mean LAN switches which support QoS, routers supporting IP Tos/Diffserv etc...

Warning L12: LAN switches are not a guarantee of QoS

It depends on the capacity of the switch and on the volume of traffic to be handled by the switch. If QoS is required, use a switch which handles QoS like OmniStack 6024.

IP ADDRESSING

Recommendation L13 : The IP addressing plan should take into account the future extensions :

- Check the compatibility of the addressing class with the addition of new IP addresses for the IP Phones, ...The need of IP addresses for VoIP is important compared to data equipments as each IP Phone will require an IP address.
- If the number of reminding IP addresses is not enough, a new IP class could be proposed or the network can be splitted in new sub-networks through new IP routers, or interfaces inside IP routers can be added

Recommendation L14 : use preferably DHCP dynamic address management in order to facilitate the management of the IP addresses and for maintenance aspects (mobility of IP Phones, rearranging of the network e.g. split into sub-networks,...)

CHOICE OF CODEC

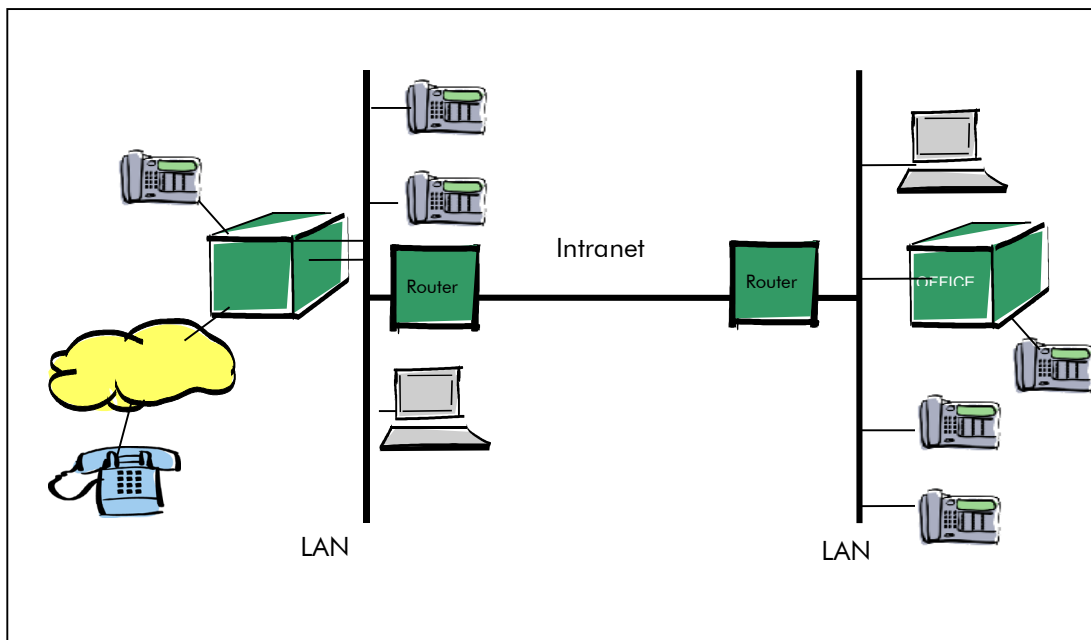
Recommendation L15: in case of a switched LAN, avoid compression and use G711 on the LAN for the IP users for maximum quality and to limit the impact of possible transcoding (successive compression/decompressions) in case of networking through a WAN connection.

3.4 VoIP over the WAN for multi-sites configurations

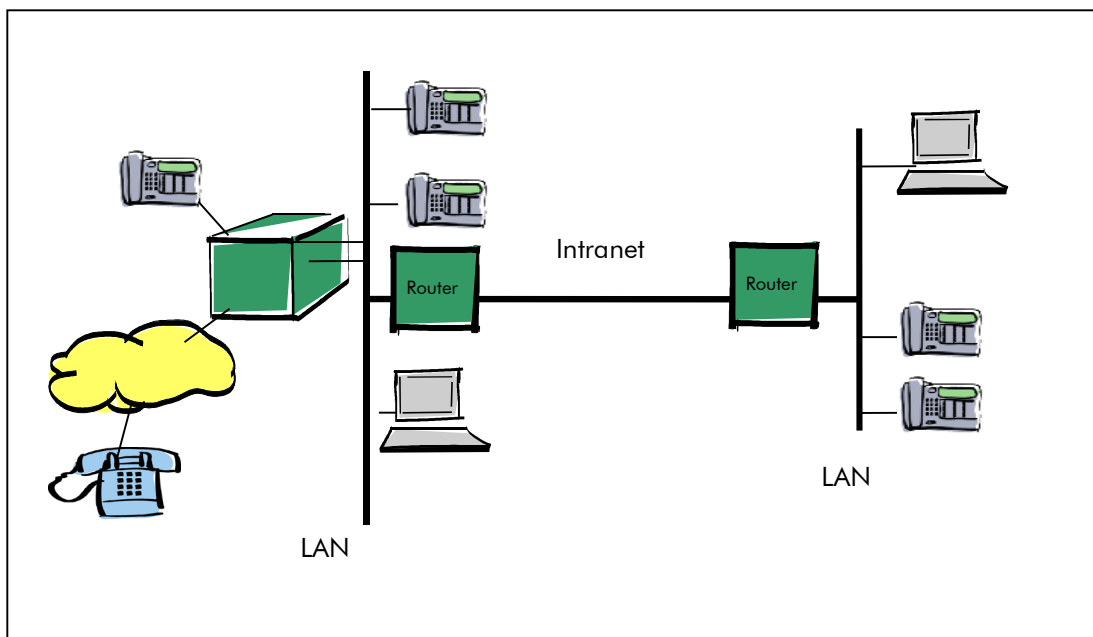
This section deals with multi-sites VoIP solutions involving WAN connections.

It covers :

- networking solutions between sites (through ABC-F VoIP links in case OmniPCX 4400 e.g or H323 trunking)



- small remote sites with several users (IP Phones or PIMPHONY/4980) but not being equipped with a PCX (remote IP telephony)



3.4.1 WAN infrastructure analysis

The following questions have to be addressed when analyzing the WAN infrastructure:

Network Architecture

Objectives : identify the current topology, the type of WAN links and the potentialities for QoS e.g if ATM protocols are in use, capacity for an end-to-end QoS Policy, priorities conflicts when passing over ATM e.g

- network diagram of the different sites
- type of topology : star or meshed
- type of WAN Core network (FR, ATM, etc...)
- list of WAN links involved with VoIP
- characteristics of these links :
 - permanent links (leased line, xDSL, ISDN LL, cable, ATM, Frame Relay...) + bandwidth/CIR
 - dial-up link (PSTN, ISDN BRI, ISDN PRI) + bandwidth
 - type of subscription (carrier, ASP, ISP) and
- VPN connection through intranet/Internet, tunneling protocols supported (PPTP, L2TP, IPSec), encryption method supported (MPPE, DES, 3DES, ...)
- list and location of equipments involved with these links (Layer 3 switch, data router, computer router, VPN server or gateways, VPN clients, Firewalls/proxies, NAT gateway, packet shaper)
- characteristics of these equipments (brand, type, software version, QoS mechanisms supported like IP TOS/Diffserv, packet fragmentation, SNMP agent)
- number and distribution of PCXs, IP Phones, softphones, H323 terminals, gateways or gatekeeper over the network
- number and distribution of PC clients, servers, DHCP servers, TFTP servers , etc... over the network
- reliability of the network :
 - inter-site voice back-up lines + bandwidth
 - inter-site data back-up lines + bandwidth

Applications running on the network

Objectives : identify the critical applications or applications which can generate heavy load over the WAN in order to understand their possible impact on VoIP and vice versa.

- list of applications running over the WAN link in particular applications such as SAP, Oracle, NetBios, NFS, Web Access ...
- synchronization process over the WAN like Database, directories, etc...

Network operation

Objectives : evaluate the available bandwidth, the traffic fluctuations, the capacity of the routers to manage additional flow, the potentialities of QoS in order to ensure that it is possible to add VoIP flows without affecting the existing transactions.

- average bandwidth utilization per WAN link
- peak periods per WAN link + rate during these peaks
- intersite flow matrix and repartition
- utilization of network equipments (switch, routers, firewalls) in terms of %CPU load, memory utilization, etc...
- QoS implemented on the WAN equipments (Tos/Diffserv, WFQ, etc...), end-to-end QoS policy
- QoS guaranteed by the ISP provider
- Security policy
- routing policy in the Core network (RIP, OSPF, ...)

IP addressing :

Objectives : understand the current IP addressing plan and anticipate the potential impacts for networking between sites

- public/private addressing plan in the different sites
- use of Network Address Translation (NAT)

Network management services

Objectives : identify tools which can help to manage the network or collect statistical informations to measure the performance of the WAN links

- Network management tools (HpoV, Ecoscope, ...)
- Network supervision tools (Rmon, ...)
- Elements which can be administered

3.4.2 Bandwidth needs analysis for VoIP

Objectives : estimate the bandwidth required to be compared to the available bandwidth and anticipate traffic growth. The WAN links must be capable to support existing data flows + VoIP.

For this exercise the following informations are required :

- number of simultaneous calls per WAN link/VPN connection including the needs for break-in/ break-out if these services are provided
- compression type : with (G723.1/G729) or without compression (G711)

The bandwidth needs can be obtained through the table in Annex A (the traffic generated for signalling can be ignored).

Warning : in case of H323 trunking, be careful to the fact that H323 path optimization is not available. This means that in case of call transfer or call forwarding between nodes, 2 channels will be maintained. The bandwidth needs must be carefully analyzed. It can be particularly problematic in case of attendant diversion.

Warning : For point to point voice connections (star/hub), mechanisms are there to limit the number of simultaneous calls (dimensionning IP trunk groups for OmniPCX 4400 networks, and IP domains for remote IP phones or IP crystals, etc...)

If the topology of the data network is more complex than that (fully meshed , partially meshed, etc...), it is impossible to avoid bottlenecks, except oversizing the links/change the topology to accommodate the maximum traffic possible, for a case that will almost never happen.

So be careful not to oversubscribe the allocated VoIP bandwidth.

Recommendation : the global bandwidth estimation for data flows and VoIP Flows should not exceed 80% of the bandwidth available on the WAN link. This margin is reserved for additional needs such as routing information, Layer 2 overhead etc...

3.4.3 Recommendations and warnings

NETWORK ARCHITECTURE

Recommendation W1 : use preferably permanent connections instead of demand-dial links for H323 trunking or remote IP telephony

Rule W2 : for ABC-F VoIP links permanent IP connectivity is required

Recommendation W3 : limit the number of router hops

Passing a router can add significant delays. VoIP Compliance measures are required if several routers have to be crossed.

Rule W4: In case of OmniPCX 4400 networks, define « VPN hops » between the nodes of the network in order to optimize the number of compression/decompression and the utilization of compressors.

Remark :

- the maximum number of VPN hops for a call is 2
- a complete meshed network can be defined within the backbone network (maximum 32 nodes in the backbone, 100 nodes in total)

Recommendation W5 : It is not recommended to have a VPN LAN-to-LAN access with demand-dial connections (through ISPs) to offer VoIP services.

This would mean a special ISP subscription (call back option) in order to allow the ISP to ask for the set-up of the dial-up link if the link is not up through a call back.

Warning W6: VoIP is not compatible with bandwidth on demand, because of the delay it introduces

Example : a 128Kb/s ISDN link but not permanent. A first channel at 64 Kb/s is established. When the bandwidth needs are over 64Kb/s, the second channel is established. This would mean for VoIP, variations in the transit delay which are not compatible with the VoIP requirements.

BANDWIDTH NEEDS**Rule W7 : Number of simultaneous calls on WAN links in G723.1/G729A**

The following table gives the maximum number of simultaneous calls supported on a low rate link, VAD not being activated (**a margin of about 20% is kept for additional data traffic, routing protocols for example**). These figures may evolve when VAD is activated.

Bit rate	Maximum Number of simultaneous calls WITHOUT RTP compression	Maximum Number of simultaneous calls WITH RTP headercompression	Codec used
55,6kbps (or lower)	1	2	G723.1/G729A
64kbps	2	4	G723.1/G729A
128kbps	5	9	G723.1/G729A
256kbps	10	18	G723.1/G729A
512kbps	20	36	G723.1/G729A
>= 1024kbps	Only limited to the possible number of VoIP trunks	RTP header compression should not be used	G723.1/G729A

Recommendation W8: Use CRTP header compression over low rate WAN links (< 1Mbits/s)

This technique can be used over a WAN low rate link (~64 kb/s) . The RTP header is reduced from 40 to 2 or 4 bytes.

This feature must be supported by the 2 routers which are connected back to back.

Recommendation W9: Limit the number of simultaneous calls between sites according to the available bandwidth when possible (Call Admission control)

If the number of calls set is greater than the available bandwidth, all communications will be affected.

In case of Office/OmniPCX Office :

- for H323 trunking, limitation is possible through the integrated gatekeeper for each H323 direction
- for remote IP Telephony, the number of sets at the remote site must be carefully defined according to the available bandwidth, because there is no mean to control call admission.

In case of OmniPCX 4400 :

- for ABC-F VoIP links or H323 trunking, limitation is possible by configuring the right number of trunks in the bundles associated to the different directions.
Drawback : before Rel 4.2, an IP Interface board must be dedicated to each direction.

- For remote IP telephony, limitation is possible through the management of IP domains (available from Release 4.1).

CHOICE OF CODEC

Rule W10: Router over Wide Area Network : use G723.1 or G729A because of the limited bandwidth (voice quality compromise)

Warning W11: Transcoding may happen in the network due to the use of different codecs

Be careful of potential transcoding problems with H323 due to the absence of path optimization in case of call transfers or call forwarding.

The transit without compression/decompression which is an optimization implemented for example in Rel 4.1 of OmniPCX 4400 to improve the voice quality doesn't bring any benefit if the codecs are different.

NETWORK OPERATION

Recommendation W12 : if the average percentage of bandwidth exceeds 80, upgrade the bandwidth rate of the link or implement QoS on the WAN router

Recommendation W13: check the capacity of the routers in terms of throughput, CPU performance

The load of the router, and the functions activated on the router (RTP compression, QoS management, etc...) can increase considerably the latency of the router.

Recommendation W14 :In case of an IP server router (like Window NT server, Linux server, ...), ensure that the server router doesn't manage applications like NFS server, Database Server, ... In this case, a dedicated data router is necessary

Recommendation W15: In case of OmniPCX 4400 ABC-F VoIP links, use the possibility of overflowing based on the « Voice Quality » profile to guarantee the level of voice quality.

Warning W16: routers, firewalls connected to the WAN can increase significantly the transit delay.

Check their routing capacity, CPU power, load, memory utilization etc...

VoIP compliance measures are recommended in this cases.

Warning W17: The behaviour of WAN links is often asymeric.

Even if delay, jitter, packet loss requirements are respected in one direction, problems can be present in the other direction. The bandwidth needs may also be quite different in each direction.

QOS

Recommendation W18: QoS is strongly recommended at WAN links especially at access speeds of 56/64kbps-512Kbps to reduce jitter. Even if the average bandwidth occupancy is theoretically adequate to absorb the VoIP flow.

Recommendation W19: implement end-to-end QoS policy in order to be able to manage continuously traffic priorities and not only on some segments.

Rule W20 : IP packet fragmentation on WAN links below 768kbps must be implemented (be careful, because this feature is not systematically available in the routers)

The purpose of IP packet fragmentation is to ensure that a very long data packet does not delay the voice packet from exiting the router in a timely manner.

If appropriate for the link configuration, use one of the fragmentation mechanisms that operate at layer 2 such as FRF12, MLPP or LFI. If using one of these methods is not feasible, then consider the IP MTU size reduction which fragments packets at layer 3. But be careful in this last case if the network supports multi-protocols. Large frames belonging to protocols other than IP are not fragmented.

Layer 2 fragmentation is achieved by programming the router to segment all outbound data packets according to the speed of the WAN access link (see table below).

The counterpart is that it can add 5-10% extra overhead to the data stream, reducing bandwidth efficiency by a similar amount.

Maximum IP Packet Size (for a serial delay of about 32 ms)

WAN Access Speed (kbps)	Maximum IP Packet Size (bytes)
56/64	256
128	512
192	768
256	1024
384	1536
512	2048*
1536	6144*

* Ethernet packets do not exceed 1536 bytes. In an Ethernet LAN environment, packet segmentation is not needed above WAN access speeds of 256 Kbps.

Warning W21: Even if QoS mechanism have been implemented, serial delay is still potentially present.

Voice prioritization can guarantee that the VoIP packets go to the head of the queue in an output buffer. But the serial delay with jitter as a consequence can still happen (if a large packet is currently being sent).

Rule W22: The VPN provider must guarantee the QoS required by VoIP not only in terms of bandwidth but also in terms of delay, jitter, packet loss (check the Service Level

IP ADDRESSING

Rule W23: Private addressing plans can be used in case of interconnection of sites, but the addressing plan must be consistent between the sites (no IP address overlap).

Rule W24 : In case of VPN LAN-to-LAN access, an official static IP address is required on both sites for the establishment of the VPN tunnel (in general at the level of the routers involved in the VPN connection).

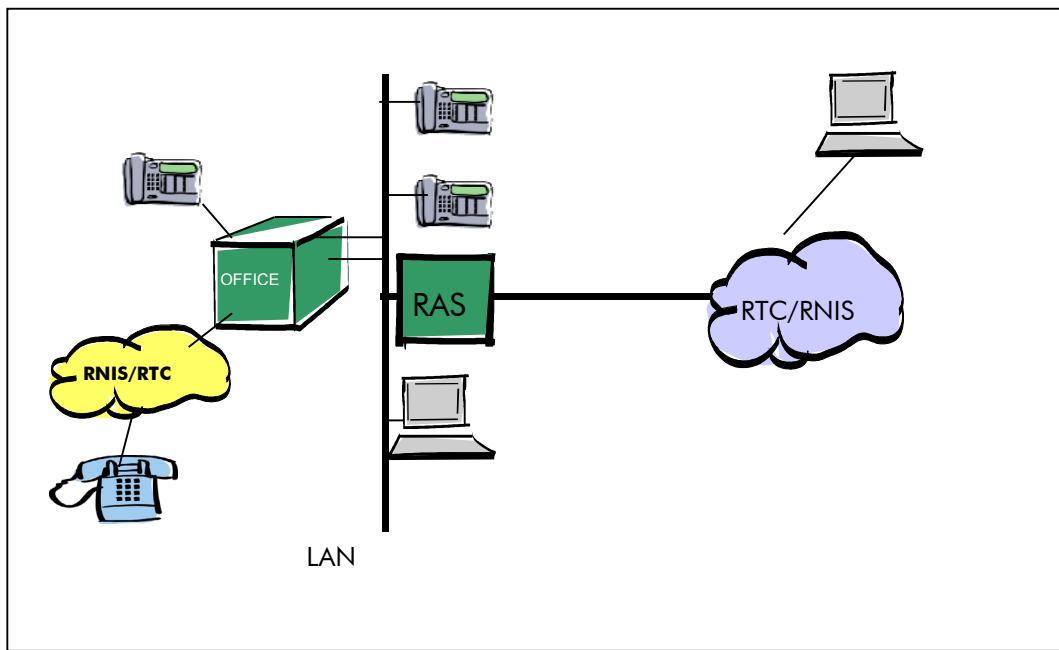
In the other cases, official IP addresses are not mandatory for networking between sites.

Rule W25 : remote IP-Phones must be configured with static IP addressing or can use a local DHCP server in the remote LAN ? ? ?

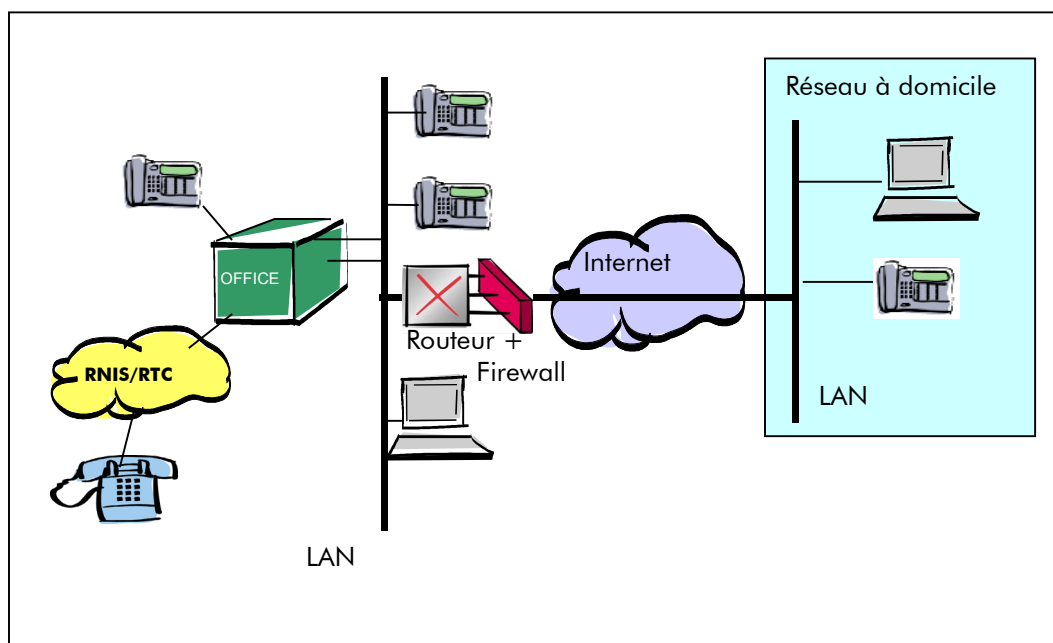
3.5 VoIP solution for single Remote worker or Mobile user

This solution covers the following situations :

- remote worker/ road warrior through Remote Access Service



- remote worker/road warrior through VPN



3.5.1 Infrastructure analysis

The following questions have to be addressed when analyzing the infrastructure :

IP connectivity

Objectives : identify the current topology, the type of connections and the potentialities for QoS of the equipments

- network diagram with the different locations (single or multiple users) and the connection points to the main site
- if connection through Remote Access Service Modem :
 - simple configuration or call back
 - type of access : analog/ISDN
 - bandwidth rate
 - type of RAS server, QoS supported...
- if RAS VPN connection :
 - type of IP router and VPN server or gateway at the main site (QoS supported, protocols supported IPSec, L2TP, PPTP...)
 - ISP provider and QoS guaranteed
 - type of connection at client side among :
 - an analog connection via modem V90
 - a numeric connection
 - xDSL
 - Cable
 - Type of connection at central site among :
 - digital connection
 - ADSL connection
 - Leased line
 - Bandwidth rate
 - type of VPN protocol for the client (Microsoft PPTP, IPSec, AlcatelVPN client...)
 - encryption protocol (MPPE, DES, 3DES, proprietary, etc...)
- other equipments on the main site (Layer 3 switch, data router, computer router, VPN server, Firewall/proxy, packet shaper) involved with these connections
- characteristics of these equipments (brand, type, QoS mechanism, SNMP agent)

LAN infrastructure analysis for the segment between PBX and RAS Modem/VPN server

See VoIP LAN infrastructure analysis

Remote connection operation

Objectives : evaluate the ability of the connections to absorb the traffic of the remote users (between RAS Modem/VPN server and System)

- average utilization per remote connection
- peak periods per remote connection + rate during these peaks
- flow matrix and repartition
- type of applications running (Internet access, e-mail, Client/Server, NFS, ...)
- utilization of network equipments involved in the connection (switch, routers) in terms of %CPU load, memory utilization
- QoS implemented on the equipments involved in the connections (Tos/Diffserv, WFQ, etc...)

IP addressing

Objectives : understand the current IP addressing plan and anticipate the potential impacts for these remote connections

- Dynamic IP addresses at the central site
- public/private addressing plan in the different remote sites

Network services

Objectives : identify tools which can help to manage the network or collect statistical informations to measure the performance of the connections

- Network Management tool
- Network supervision tool

3.5.2 Number of simultaneous RAS Modem/VPN connections

Objectives : estimate the number of simultaneous RAS modem connection or simultaneous VPN connections in order to estimate the number of RAS modems and VPN servers and allow bandwidth needs calculation at the central site.

3.5.3 Bandwidth needs analysis at the central site

Objectives : estimate the bandwidth required to be compared to the available bandwidth .
The connections must be capable to support existing data flows + VoIP.

For this exercise the following informations are required :

- Number of remote IP subscribers
- number of simultaneous calls (RAS modem or RAS VPN)

Warning : In case of VPN connections, the bandwidth needs between the central site and the ISP must take into account the overhead due to VPN tunneling.

3.5.4 Recommendations and warnings

Network architecture

Rule : In case of remote connections using VPN tunneling, a permanent Internet connection is required at the central site.

CHOICE OF CODEC

Rule : use G723.1 or G729A because of the limited bandwidth (voice quality compromise).

QoS

See WAN solutions. In particular, IP packet fragmentation is required on low rate links at the central site as well as on the PC client side.

IP ADDRESSING

Rule : In case of remote connections using VPN tunneling, a static official address is required at the central site for the establishment of the VPN tunnel.

An official IP address is not necessary for the remote worker/road warrior.

4. General recommendations and warnings

Don't forget that VoIP flows are time-critical. If there are intermittent problems as bandwidth problems for example, the voice will be first affected.

VOIP FEATURES

Warning G1:

- ▼ FAX over IP is not supported on Office
- ▼ FAX calls group 3 over VoIP links is supported between OmniPCX 4400 only (max speed 9600b/s)
- ▼ Modem, TA V24 and Minitel are not supported over VoIP links

NETWORK ARCHITECTURE

Warning G2: Compatibility between routers and ADSL modems has to be checked because of ADSL modems supporting only PPTP connection and not PPPoE.

Warning G3: Remote feeding for IP-Phones : tele-alimentation must be limited to the last segment towards the IP-Phone

Warning G4: Remote feeding for IP-Phones : the use of Pins 7&8 of the RJ45 Ethernet connector is not compatible with some boards with Fast Ethernet connection possibility or Token Ring interfaces

Rule G5: For remote IP Phones or remote PIMPHONY/4980, a VPN tunnel between the sites is mandatory to avoid interworking problems related to NAT, by-pass of firewall, TFTP transport.

BANDWIDTH NEEDS

Recommendation G6 : a margin of 20% must be taken when calculating the global bandwidth needs.

Rule G7 : don't take into account the potential gain of VAD when calculating the bandwidth needs

Recommendation G8: In general, don't activate VAD for best quality, but this must be appreciated case by case.

Warning G9 : Voice Activity Detection mustn't be used with G729A in industrial environments.

ED	01	Methodology, rules and recommendations for VoIP solutions engineering		
D. Lienhart		11.21.2002	8AL 01200 1259 QRASA	29/42

Rule G10 : VAD configuration must be consistent in a network : either activated or deactivated on all nodes.

Warning G11: In case of VPN tunneling, the overhead due to VPN (PPTP, IPSEC, ...) must be taken into account.

CHOICE OF CODECS

Recommendation G12 : It is strongly recommended not to apply more than two G723.1/G729 voice compression :

More than 2 compression/decompression (G723.1 or G729A) damages seriously the audio quality.

- - G711 $\Leftrightarrow$ G711 $\Leftrightarrow$ G711 = OK
- - G711 $\Leftrightarrow$ G723.1/G729a $\Leftrightarrow$ G711 = OK
- - G711 $\Leftrightarrow$ G723.1/G729a $\Leftrightarrow$ G723.1/G729a = OK
- - G723.1/G729a $\Leftrightarrow$ G723.1/G729a $\Leftrightarrow$ G711 = OK
- ~~- G723.1/G729a $\Leftrightarrow$ G723.1/G729a $\Leftrightarrow$ G723.1/G729a = KO~~

Be aware that more than likely during VoIP communications involving IP Phones, network gateways , internal compression (VoFR, packet voice over leased linear ISDN) and external compression sources (GSM), several compression and decompression techniques are used which degrade the quality of the voice communication. Examples :

- IP phone calling a GSM phone (GSM FR/EFR) or a voice mail or a DECT set (ADPCM)
- IP Phone on one node calling an IP Phone on another node, the 2 nodes being connected using voice compression (VoIP, VoFR, ...)
- IP Phone on one node going through a VoIP/VoFR/compressed trunk to another node and breaking out to reach a public telephone set

Recommendation G13: use preferably G729A instead of G723.1 mainly because of the delay introduced by G723.1

The choice between G729a and G723.1 often depends on customer appreciation and may require trailing both techniques for suitability. G729A has an intrinsic quality close to G723.1, but behaves differently in case of transcoding and IP network perturbations.

Warning G14: G711 is very sensitive against packet loss.

Over 1% loss of packets, the quality becomes notably inferior to that of G723.1 or G729A.

Warning G15: Be careful if music on hold signal should be sent through the audio channel. G723.1 and G729A don't support very good audio signals other than human voice

QOS

Recommendation G16 : Implement the right level of QoS considering the needs and the complexity of the management of the network.

Indeed, downsides of QoS is that it adds complexity at network management level, maintenance, evolution of the network.

Recommendation G17 : if Qos is managed, an end-to-end QoS Policy is recommended.

Rule G18 : In a global network, QoS must be applied hop by hop . Condition : all equipments involved in a hop must support the same QoS policy.

For example :

- Layer 2 QoS policy between switch and router
- RSVP mapping to ATM service between Router and backbone ATM

Warning G19: QOS must be consistently processed by the routers, e .g. they must manage the TOS field in the same way.

Warning G20: QoS will not solve the problems of quality if the equipments are overloaded or the links undersized for example.

IP ADDRESSING

Recommendation G21 : Use a centralized external DHCP server when possible instead of the integrated DHCP server .

If the IP-Phones are not located in same sub-network as the DHCP server, **the DHCP relay** feature must be activated in the router between the sub-networks (this DHCP Relay feature is not available in all the routers).

Recommendation G22 : don't mix on the same network integrated DHCP server and DHCP external server. In this case give preference to the external DHCP server.

Warning G23: The need for IP adresses can be very important and can easily be doubled because of the IP Phones.

SECURITY/VPN

Recommendation G24 : For security reasons, don't connect the systems (OmniPCX 4400, Office R4) to a Demilitarized Zone (DMZ).

Recommendation G25 : Protect the access to the OmniPCX 4400 and IP-LAN board for Office R4 to authorized users and against attacks (trusted host features, firewalls, etc...) as for any sensitive data equipment of the network.

Recommendation G26 : Don't open UDP ports in firewalls to allow by-pass of VoIP flows.

Instead :

- use an H323 compliant firewall in case of H323 networking

- use VPN tunneling for remote IP telephony solutions

Recommendation G27 : use VPN tunnels when accessing the ISP network

This will allow to ensure the confidentiality of the voice and solves the problem of by-passing firewalls.

Protocols like L2TP, PPTP or IPSec protocols can be used to create secure tunnels through the Internet.

The renewal of the encryption keys is recommended every 24 hours on permanent VPN links

Recommendation G28 : For a firewall, define the Access Lists (rules) related to VoIP among the first rules in order to limit the delay introduced by the firewall.

Recommendation G29: By-pass of firewalls :

- If the firewall has to allow H323 connections to be made, use a firewall which provides security management of H323 frames. This means, the firewall will dynamically open/close the ports (signaling and RTP/RTCP connections) related to H323. Example : Firewall-1 from Checkpoint.
- If the firewall is concerned with the proprietary VoIP signalling (ex 4980 IP Telephony, IP Phone), use the VPN functionality to tunnel the proprietary signalling. Otherwise the whole range of TCP/UDP ports used has to be opened.

Warning G30: Security equipments like firewall , proxy , VPN encryption add significant delay.

The performance required for these machines depends on the volume of traffic, the managed access lists for firewalls for example.

For VPN encryption by routers (DES, 3DES, ...) hardware processing is recommended to be able to maintain stable performances.

Warning G31: Network Address Translation (NAT) is not compatible with VoIP because of IP addresses exchanged within the messages which are not translated. The solution in that case is to implement a VPN tunnel.

NETWORK MANAGEMENT

Recommendation G32 : A network management tool is strongly recommended in case of complex architectures to monitor links, bandwidth consumption, links congestions, load of the equipments for a pro-active management of the network.

5. VoIP Compliance measures

The objectives of the VoIP compliance measures is to make sure through on site tests that the network is « voice ready » :

- by measuring the key voice indicators (transit delay, jitter and packet loss)
- by ensuring that the required bandwidth is available.
- By verifying the efficiency of QoS settings

These measures are strongly recommended because :

- VoIP has specific requirements (voice is very delay-sensitive) different from classical data applications
- voice quality doesn't support any compromise.

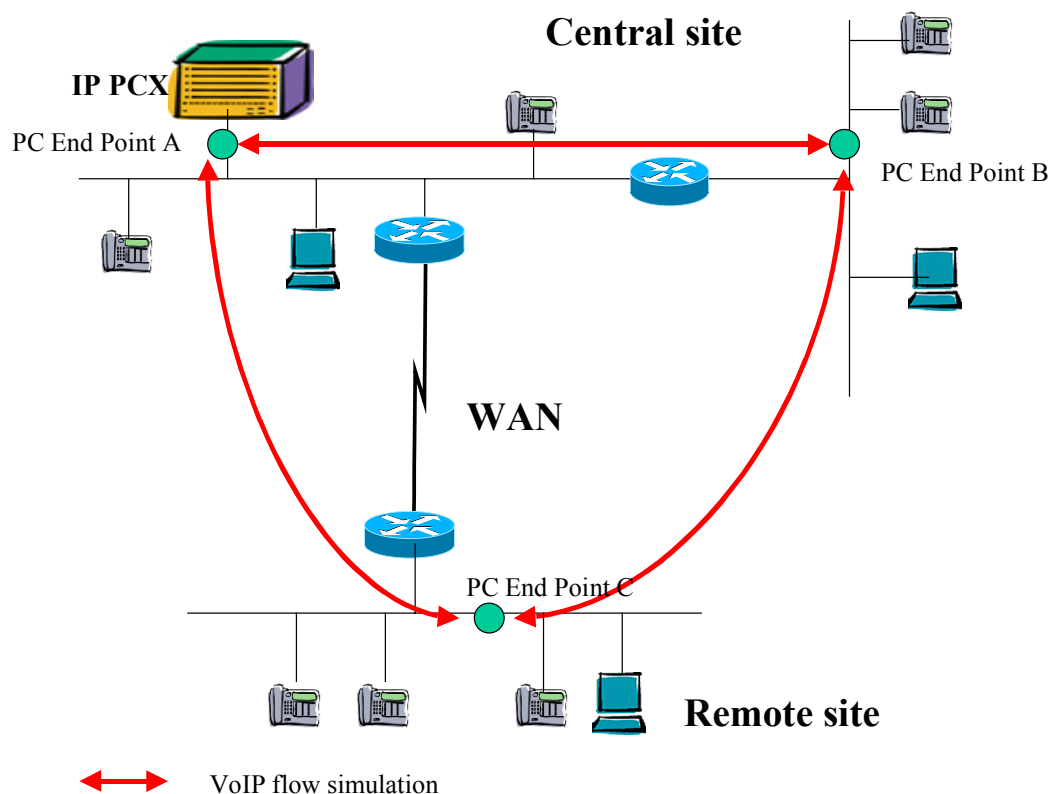
Prior to these measures, It is strongly recommended if a Network Performance Audit hasn't been performed to check briefly main network issues like utilization rate on the LAN, level of broadcasts on the LAN, etc...

5.1 Principle of VoIP compliance measurements

These measures consist in simulating RTP flows between several points within the LAN or over WAN links

The measurement campaign takes place during one day or more during which VoIP flows are simulated.

Example :



5.1.1 In a LAN environment

Make tests between different endpoints and with the IP interface boards.

The maximum number of calls to be simulated for the IP interface boards is given by the number of compressors on that board.

5.1.2 In a WAN environment

Connect the generator PC (or endpoint) and the receiver PC (or endpoint) near the IP interface board of each side, then simulate the number of communications expected on the WAN link.

5.2 Methodology

The process of VoIP compliance measurement can be split into the following steps :

- Understanding of the network infrastructure in order to understand the context and identify the weaknesses of the network
 - LAN/WAN topology
 - Location of PBXs and IP-devices
 - Equipments concerned by the VoIP flows which will be simulated (switches, routers, firewalls, VPN gateways, etc...)
 - VPN connectivity if any (PPTP, IPSec, ...)
 - QoS policy in place (TOS/Diffserv, etc...)
 - IP fragmentation implemented ?
- VoIP Traffic analysis

Prior to any simulation, the VoIP traffic must be analyzed and calculated (see paragraphs « Bandwith needs analysis »)

- Definition of the conditions of the measures
 - Number of endpoints with their location
 - Number of simultaneous calls between endpoints
 - coding alogorithm (G711, G723.1, G729a)
 - use of ToS/DiffServ, 802.1p/Q
 - duration of the simulations (e.g 4mn for each simulation)
 - number of endpoints with their location

This will be based on traffic analysis and calculations (see paragraphs « Bandwith needs analysis »)

- Analysis of the busy, critical hours in order to make pertinent measurements and determine the schedule of the measurement campaign (e.g. during 9-12am and 2-5pm).
- Understanding of the limits and constraints of the test

For example, can not be simulated :

- H323 flows in order to validate the behaviour when crossing a firewall compliant H323
- Etc ...

Constraints :

ED	01	Methodology, rules and recommendations for VoIP solutions engineering		
D. Lienhart		11.21.2002	8AL 01200 1259 QRASA	35/42

- It could be necessary to open some ports number to allow VoIP simulation through a firewall for example
- Etc...

– Measurement campaign

To be pertinent, it assumes that the simulation takes place in the real conditions, i.e. QoS being configured for example in the network if QoS required, VPN tunnels in place...

– Analysis of the measurements

5.3 Analysis of the measurements and conclusions

The analysis of the measurements will lead to two main conclusions :

- network ready (through maybe minor adaptations as for example QoS configuration, data flows optimization , etc...) => the solution can be deployed.

However, if there are some risks which could hinder the good functioning of the solution, these risks must be exposed to the customer.

– Network Redesign

Warning : For the interpretation of the measures, don't forget that the VoIP compliance measures only measure the delay introduced by the network and not the global end-to-end delay.

To estimate the global end-to-end delay and appreciate the VoIP conformity, **the algorithmic delay and the delay introduced by the components of the system (PBX, IP Phone, ...)** must be taken into account (e.g. about 80ms for the compression/decompression delay in case of G729A).

5.4 Recommendations & warnings

Recommendation: VoIP compliance measures are strongly recommended especially before deploying WAN solutions but not mandatory (except in complex networks, if firewall crossing, crossing of several routers, etc...)

Rule: don't take into account the potential gain of VAD when making simulations

Warning: simulating 802.1p/Q tagging may be problematic (must be supported by the PC's used for the tests)

Warning : simulations in networks with VLAN segmentation, firewalls e.g. may not be immediate as it could mean configuration changes within the network equipments.

6. Network Performance Audit

6.1 Objectives

The objective of network performance audit is to analyze the complete network, to provide a view of the health of the network in order to check its ability to support VoIP.

Such an audit covers in general a period of one day to one week and is lead by data specialists.

Network performance audit must not be confused with VoIP compliance measures.

It will allow to :

- understand the architecture of the network
- Make an inventory of all data equipments of the network (switches, routers, etc...)
- Analyze the active equipments, their load, etc... in order to identify the critical equipments
- Analyze the data flows, flow repartition, top talkers, broadcast rate, etc...
- identify the potential bottlenecks in the network (bandwidth, transit time, packet losses,...), weaknesses in the network

The audit is based on Network management tools which are able through the SNMP protocol to identify the equipments present on the network, provide statistics on router CPU utilization, memory and buffer utilization, bandwidth utilization, etc ...

6.2 When should a network performance audit be performed ?

A network performance audit is recommended during the Network Analysis phase when :

- the network is not managed
- there is no precise knowledge about how the network behaves
- the collected datas are not sufficient
- etc...

7. Conclusion

The methodology described in this document must help to deploy VoIP solutions in the best conditions through the analysis of the current situation of the network and the anticipation of the network evolution.

But one major point is that the voice distributor can not engage alone his responsibility and guarantee the solution. **The success of VoIP solutions relies on the mutual commitment of the different parties involved (customer, data integrator, VoIP supplier, etc...).**

A second major change introduced by VoIP, is the problematic of the perennity of the solutions :

- as the demand for new applications (e-commerce, datawarehouse, etc...) is high and makes a strong pressure on the networks . Networks becomes critical for the enterprises and are in constant evolution.
- as VoIP solutions are time-critical applications and thus potentially very exposed to network evolutions.

Rule : The engineering rules described in this document are applicable not only at the first installation, but during the whole life time of the solution.

Take commitment with the customer in order to ensure that if the network evolves, the VoIP requirements are still taken into account.

8. ANNEX A Bandwith needs

Bandwidth needs versus codec and packetization time (without VAD)

Codec	Bit Rate	Packetisation Time	RTP payload (bytes)	IP Frame Size =RTPpayload +RTP(12)+UDP(8)+IP(20)	Bandwidth at IP level	Bandwidth at Ethernet Level (Full-Duplex Media) (*)	Bandwidth at WAN level without CRTP (**)	Bandwidth at WAN level with CRTP to 2 bytes (**)	PBX implementation (***)
G723.1 (MP-MLQ)	6.4 Kb/s	30 ms	24	64 bytes	17.1 Kb/s	27.2 Kb/s	19.2 Kb/s	9.1 Kb/s	OmniPCX 4400 OfficeR4.2 (by default)
		60 ms	48	88 bytes	11.7 Kb/s	16.8 Kb/s	12.8 Kb/s	7.7 Kb/s	Office R4.2
		90 ms	72	112 bytes	10 Kb/s	13.3 Kb/s	10.7 Kb/s	7.3 Kb/s	Office R4.2
		120 ms	96	136 bytes	9.1 Kb/s	11.6 Kb/s	9.6 Kb/s	7.1 Kb/s	Office R4.2
G 729A	8 Kb/s	30 ms	30	70 bytes	18.7Kb/s	28.8Kb/s	20.8 Kb/s	10.7 Kb/s	OmniPCX 4400 OfficeR4.2(by default)
		60 ms	60	100 bytes	13.3 Kb/s	18.4 Kb/s	14.4 Kb/s	9.3 Kb/s	Office R4.2
		90 ms	90	130 bytes	11.6 Kb/s	14.9 Kb/s	12.3 Kb/s	8.9 Kb/s	Office R4.2
		120 ms	120	160 bytes	10.7 Kb/s	13.2 Kb/s	11.2 Kb/s	8.7 Kb/s	Office R4.2
G 711	64 Kb/s	20 ms	160	200 bytes	80 Kb/s	95.2 Kb/s	83.2 Kb/s	68 Kb/s	Office R4.2
		30 ms	240	280 bytes	74.7Kb/s	84.7Kb/s	76.8 Kb/s	66.7 Kb/s	OmniPCX 4400 Office R4.2(by default)
		60 ms	480	520 bytes	69.3 Kb/s	74.4 Kb/S	70.4 Kb/s	65.3 Kb/s	Office R4.2
		90 ms	720	760 bytes	67.6 Kb/s	70.9 Kb/s	68.3 Kb/s	64.9 Kb/s	Office R4.2

(*) IP Frame + MAC (14) + CRC (4) + preamble (8) + inter-frame silence (12)

(**) 8 bytes Layer 2 overhead (= maximum for PPP, MLPPP, FRF.12, HDLC)

(***) when Office implementation = Office R4.2 and OmniPCX Office R1.0

ED	01	Methodology, rules and recommendations for VoIP solutions engineering
D. Lienhart		11.21.2002
		8AL 01200 1259 QRASA
		39/42

Bandwidth needs in case of Fax transmission

Protocol	Bit Rate	Packettis ation Time	Payload (bytes)	IP Frame Size	Bandwidth at IP level	Bandwidth at Ethernet Level (Full-Duplex Media) (*)	Bandwidth at WAN level without CRTP (**)	PBX implementation (***)
FAX Alcatel	9600b/s	40 ms	48	77 bytes	15.4Kb/s	23 Kb/s	17Kb/s	OmniPCX 4400
Fax T38 Redund 0	9600b/s	40 ms	48	86 bytes	17.2Kb/s	24.8Kb/s ?	18.8Kb/s	OmniPCX 4400
Fax T38 Redund 1	9600b/s	40 ms	96	140 bytes	28Kb/s	35.6Kb/s	29.6Kb/s	OmniPCX 4400
Fax T38 Redund 2	9600b/s	40ms	144	194 bytes	38.8Kb/s	46.4Kb/s	40.4Kb/s	OmniPCX 4400
Fax T38 Redund 3	9600b/s	40ms	192	248 bytes	49.6Kb/s	57.2Kb/s	51.2Kb/s	OmniPCX 4400
FaxT38 Redund 1	9600b/s	80ms	192	236 bytes	23.6Kb/s	27.4Kb/s	24.4Kb/s	?

(*) IP Frame + MAC (14) + CRC (4) + preamble (8) + inter-frame silence (12)

(**) 8 bytes Layer 2 overhead (= maximum for PPP, MLPPP, FRF.12, HDLC)

(***) when Office implementation = Office R4.2 and OmniPCX Office R1.0

ED	01	Methodology, rules and recommendations for VoIP solutions engineering		
D. Lienhart		11.21.2002	8AL 01200 1259 QRASA	40/42

Protocol	Bit Rate	Packeti sation Time	RTP payload (bytes)	IP Frame Size	Bandwith at IP level	Bandwith at Ethernet Level (Full-Duplex Media) (*)	Bandwith at WAN level without CRTP (**)	PBX implementation (***)
FAX T38 Redund 3	14400b/s	40 ms	288	344 bytes	68.8Kb/s	76.4Kb/s	70.4Kb/s	?

(**) 8 bytes Layer 2 overhead (= maximum for PPP, MLPPP, FRF.12, HDLC)

(***) when Office implementation = Office R4.2 and OmniPCX Office R1.0

ED	01	Methodology, rules and recommendations for VoIP solutions engineering		
D. Lienhart		11.21.2002	8AL 01200 1259 QRASA	41/42

END OF DOCUMENT

All rights reserved. Passing on and copying of this document, use and communication of its contents not permitted without written authorization from Alcatel.

ED	01	Methodology, rules and recommendations for VoIP solutions engineering		
D. Lienhart		11.21.2002	8AL 01200 1259 QRASA	42/42