Convergence Makes Sense

At the Architecture, Network, and Network Services levels

ALCATEL

ARCHITECTS OF AN INTERNET WORLD

Table of Contents

Abstract

This white paper examines most of the issues surrounding the adoption of a converged voice and data network in a private corporate environment.

The paper begins by comparing and contrasting the background of voice and data, and introduces the three main areas covered later:

- Convergence at the architecture level.
- Convergence at the network level.
- Convergence at the network service level.

Within each of these three topics, several pertinent considerations are reviewed – voice over IP, the H.323 Standard and alternatives, a naming convention and addressing scheme, directory services, and the allocation of bandwidth to time sensitive transmissions (QoS).

Finally, the paper offers a considered view as to how many of the perceived pitfalls of adopting convergence could possibly be avoided.

Setting the scene

Data background

In the last decade, data networking has undergone explosive growth, from a tool used by experts within organizations to an ordinary part of many people's lives, both at work and at home. The most obvious example today is the Internet, and its graphical component, the World Wide Web. Schoolchildren, advertising agents, and political leaders all use the Web on a daily basis.

Underlying the explosion in data network use is a powerful set of infrastructure technologies. It would be impossible for the Internet – and the tens of thousands of other networks in the world – to operate today with the infrastructure of ten years ago.

Voice background

Voice communication systems have been with us for much longer than data networks. Millions of people-years of development and use have produced today's PBXs, resulting in a platinum plated call-processing engine. It delivers 99.999 percent uptime, offers numerous features (on the order of 500) and supports a wide range of value-added applications. User expectations have long been set to expect the PBX to be functional nearly 100 percent of the time, a level of reliability and functionality very few, if any, data networks can offer.

In a modern PBX, the majority of code and functionality is not employed in providing the switching function, but utilized by the applications it contains. Over the last six years, the application content of a PBX has experienced more development than ever before in its history, evolving the PBX into a Private Communications Exchange (the PCX).

Contrasting voice and data communications

Voice and data communications have, to date, evolved as separate entities.

The PBX was developed to provide best-of-class voice, fax, and video communication. Inherent benefits include the ability to handle immediate person-to-person communications, low cost of ownership, superior reliability, availability, and quality of service.

The LAN emerged from the need to share resources and information – driven by an ever-increasing need for more bandwidth and increased throughput. The PC has evolved from a single-user open system to a networked PC supporting numerous applications tailored to individual needs.

Introducing convergence

Today's corporate enterprises use separate voice and data networks. Real-time communications have been the traditional domain of the PBX, while non-real-time communications have been the domain of networked computing and the LAN.

Convergence can be simply defined as the combining of the separate voice and data networks. However, convergence enables much more than this. It allows all the voice applications inherent in a PBX to be accessible from a consolidated communications infrastructure, providing the opportunity for:

- PC / phone convergence.
- Fixed / mobile convergence.
- Voice / packet convergence.
- Office / teleworker convergence.
- Web site / call center convergence.
- Voice / fax / video / email convergence.

Convergence represents the opportunity not only to reduce expenditure on infrastructure and manpower costs, but also to improve the daily productivity of every corporate employee.

New terminals are emerging that will provide multimedia communication using Internet technologies such as JAVA and Web browsers. Wireless terminals with bandwidth-saving data protocols (WAP) are under development that will enable integrated mobile voice and data access.

These WAP enabled wireless terminals (that integrate mobile voice and web browser access to applications), will dominate the cell phone market in the coming years.

The remainder of this white paper is devoted to the considerations supporting convergence at the three main levels of networking:

- Convergence at the architecture level.
- Convergence at the network level.
- Convergence at the service level.

1. Convergence at the architecture level

Corporate information delivered in a timely manner is key to today’s business practices. Convergence at the architecture level provides the network users with the ability to leverage the entire application set and functional capabilities that are accessible through the network, thus ensuring the total corporate information pool is easily accessible.

The primary aim of architecture level convergence is to create a single, logical communication system that is:

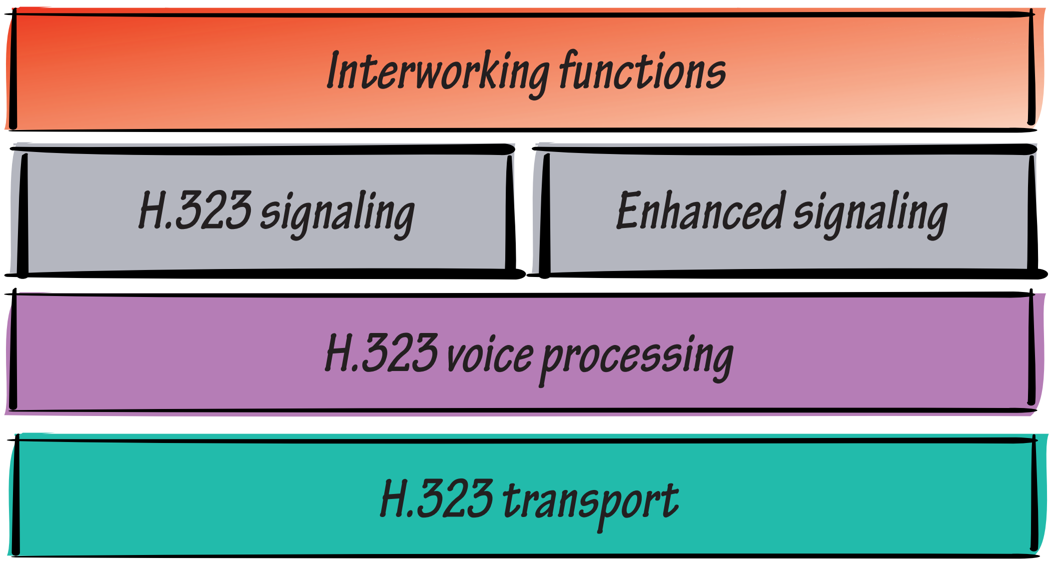
- Easily upgraded and future – proof.
- Scalable and capable of growing in terms of performance and number of users supported.
- Resilient and reliable, producing a service level consistent with its use.
- Ubiquitously accessible.
- Technology transparent.
- User-friendly.

When viewed from an architectural perspective, the separate voice and data networks existing in corporate enterprise communication systems have several points in common.

Existing in both are:

- Applications hosted on servers.
- A range of communication services – for example, name management, security services and directory services.
- Network infrastructures – the cabling and call routing / switching devices.
- Access networks – traditionally circuit switched for voice and fax; packet switched for data and increasing more also for voice.
- User terminals – PCs, telephone handsets, etc.

Architectural convergence integrates functionality at each of these common points.



The delivery of information enabled applications, regardless of network media, in a usable format is the result of such a converged architecture. Such an architecture allows applications to easily make use of both voice and data components. This allows the development and enhancement of multimedia applications, extending their reach and capability set, which will enhance business processes as they exist today.

Architecture level convergence

Converging the enterprise communication system into a single consolidated information system, transparently linking users to communication services and the application set, is the key enabler to sustaining business growth and competitive advantage.

A converged, high performance application delivery architecture requires: robust application servers, a powerful network infrastructure, and quality of service management, to provide the reliability and resilience for effective communications.

2. Convergence at the network level

At the network level, convergence depends upon the transparent use of normal voice communications, using the underlying higher speed data networking protocol. The transport of real time voice communication using a data oriented networking protocol has been given serious study for many years, producing a variety of options such as:

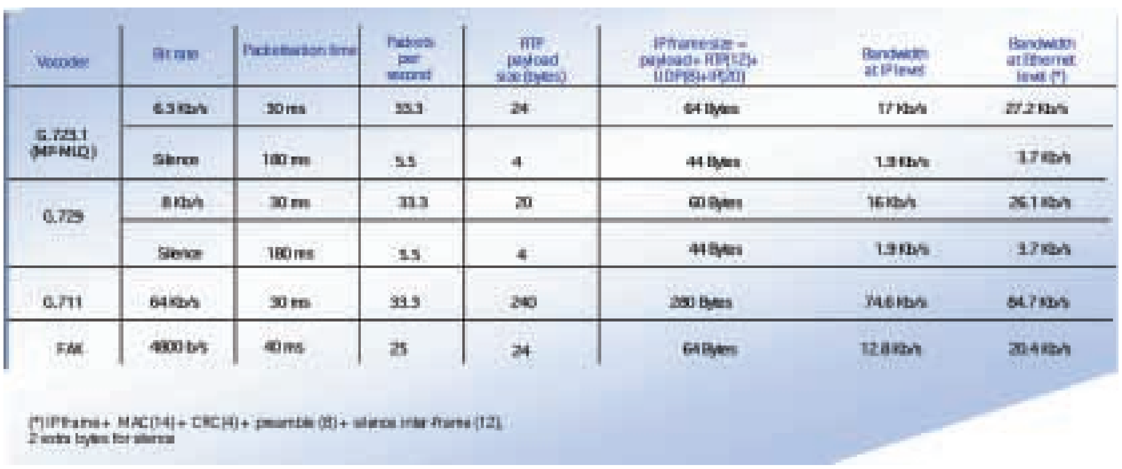
- The voice encoding and compression algorithms for transporting voice in packets over frame relay (VoFR).
- The development with inherent voice support of ATM.

Although several data networking protocols do exist in today's corporate networks, the explosive deployment of the Internet has resulted in the adoption of the Internet Protocol (IP) as the universal network protocol. This has led to the rapid standardization of voice signaling and transport over the IP network, employing voice encoding and compression algorithms.

Voice over IP

Transporting voice over an IP network requires the voice content to be encapsulated in an IP data packet. Adhering to the standard format of an Ethernet frame demands that what is transmitted contains not just the voice information itself but also all the parameters needed by the IP networking protocol and the Ethernet transport. The actual bandwidth required in a data network to transport voice is greatly increased because of this. In addition, the type of voice encoding employed has a significant impact on bandwidth needs.

Bandwidth requirements to transport voice in an IP data network



Vocoder	Bit rate	Packetisation time	Packets per second	RTP payload size (bytes)	IP frame size = payload + RTP(12) + UDP(8) + IP(20)	Bandwidth at IP level	Bandwidth at Ethernet level (*)
G.723.1 (MP-MLQ)	6.3 Kb/s	30 ms	33.3	24	64 Bytes	17 Kb/s	27.2 Kb/s
	Silence	180 ms	5.5	4	44 Bytes	1.9 Kb/s	3.7 Kb/s
G.729	8 Kb/s	30 ms	33.3	20	60 Bytes	16 Kb/s	26.1 Kb/s
	Silence	180 ms	5.5	4	44 Bytes	1.9 Kb/s	3.7 Kb/s
G.711	64 Kb/s	30 ms	33.3	240	280 Bytes	74.6 Kb/s	84.7 Kb/s
FAX	4800 b/s	40 ms	25	24	64 Bytes	12.8 Kb/s	20.4 Kb/s

(*) IP frame + MAC(14) + CRC(4) + preamble (8) + silence inter-frame (12).
2 extra bytes for silence

The rise of data networking

You may recall the outdated concept of partitioned (or party) telephone lines.

A party line is a telephone circuit that's shared by a number of subscribers. Only one person can use it at a time. The others have to wait until the first subscriber is finished to take their turns, and it was very easy to listen to someone else's conversation.

Party lines were once the normal method of connecting telephone subscribers, but have now been almost completely replaced by dedicated connections. As private (switched) connections to the public telephone network became less expensive, this was inevitable.

In the data LAN environment a similar evolution has occurred. The two most widely deployed transmission protocols, Ethernet and token ring, were designed to allow shared user access in the same way as party lines. Today, with the continuing demand for higher and higher bandwidth, these old shared bandwidth networks (hub and router based), are being replaced by switching devices, where every switch provides a dedicated connection for every LAN device.

The bandwidth-sharing capabilities that Ethernet and token ring were initially designed to provide will lie unused, when switching is deployed throughout all networks.

This is why, in the LAN switching business, there is very rarely a situation where LAN equipment isn't already deployed (i.e., a green-field-site).

Currently, LAN and campus networks are in a state of transition. The majority of workstations are still connected to hubs, and the majority of those hubs are still interconnected with routers. However:

- A large minority of workstations are now connected to LAN switches, and many of those are interconnected with backbone switches using Fast Ethernet. LAN switches alone are now a multi-billion dollar business, and they are one of the fastest-growing segments of the networking industry.
- Gigabit Ethernet is about to become a widely accepted tool for campus backbones.
- Layer-3 switching – inside Gigabit Ethernet switches – is on the verge of replacing software-based routers in many networks.

LAN switches have evolved a great deal since they were first developed. LAN switches today have become a fundamental building block of modern networks.

LAN switches have become dramatically less expensive since their introduction.

As a result, it has become possible to connect each device – workstation, printer, server – to its own switch port, completely eliminating hubs. In fact, even Fast Ethernet is now sufficiently inexpensive to allow fully switched 10/100 networks to be installed.

The most obvious advantage of a fully switched network is that each device has its own dedicated bandwidth. Imagine an Ethernet LAN with 50 users. The total theoretical bandwidth in the network is ten Mbps. But a shared Ethernet can't sustain more than a 50% - 70% load, depending on number of machines and cable distances. So the real capacity of the network is five to seven Mbps. Now, imagine this as a switched network, with Fast Ethernet to every desktop. The total network capacity is now 500 Mbps – an increase of two orders of magnitude.

The speeds and potential capacities that can be realistically produced in a modern LAN network are easily able to transport voice traffic in addition to data.

IP telephony

Transporting voice traffic over a high-speed LAN network requires the use of an IP telephony system. Such a system is based on the client / server concept, where the server provides the call handling function (with all the advanced features), and the client is located in the telephony terminal (which may be a PC or telephone handset).

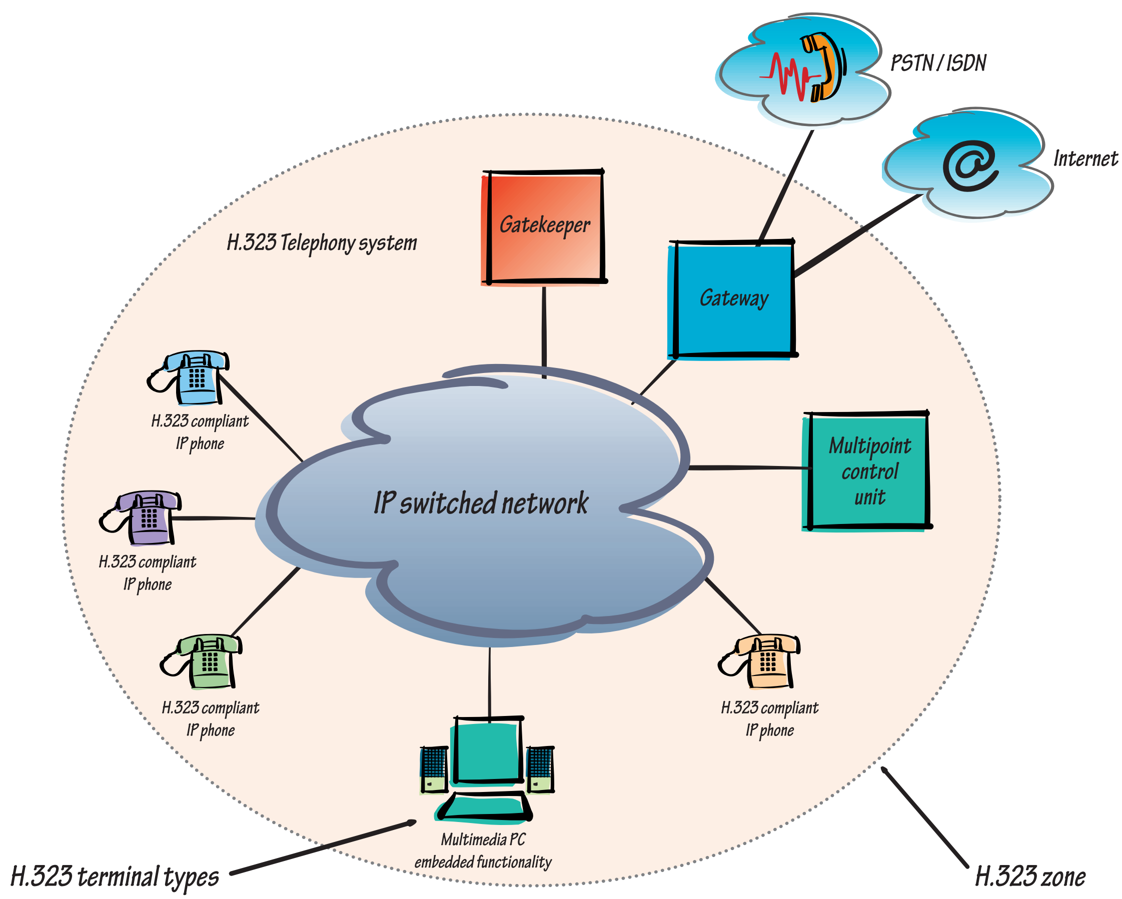
The telephone system in operation today can be used by any single handset to call anywhere in the world. Such a telephone call would probably pass through several different vendors' telephony equipment. The system works because all telephone equipment manufacturers adopt a common set of communications rules.

There are several rules / standards key to the operation of IP telephony. The most readily available today, from a number of equipment manufacturers, is H.323.

The H.323 standard

- H.323 sets multimedia standards for IP based networks, allowing device-to-device and application-to-application interoperability.
- H.323 provides standards for telephony and multimedia communication between IP LANs and other networks.
- H.323 enables the network bandwidth used for conferencing to be restricted.
- H.323 applies to both standalone devices such as IP phones, and the embedded functionality as might be found in a multimedia PC.

The H.323 architecture defines four major components for a network-based communications system as shown below: terminals, gateway, gatekeeper, and multipoint control unit (MCU).



H.323 IP network components

H.323 terminals are the client endpoints on the LAN that provide real-time, full duplex communications. These client endpoint devices may be a stand-alone IP telephone or an H.323 terminal function embedded in a Multimedia PC. The H.323 standard dictates that all client endpoints must support voice communications, both video and data being optional.

The H.323 gateway provides many services. The most significant is the translation function between H.323 conferencing endpoints and other terminal types. This function allows callers using IP phones to communicate outside the H.323 environment with traditional PSTN telephones. Gateways are entrance and exit points into VoIP networks.

A H.323 gatekeeper is an optional entity within the H.323 component group. If a gatekeeper is present, then all H.323 devices must use it. As the name implies, the gatekeeper performs the H.323 zone management functions of:

- Policing the defined conference bandwidth threshold.
- Call re-routing if called endpoint unavailable.
- Translation of LAN aliases for terminals and gateways to IP addresses.

While a gatekeeper is logically separate from H.323 endpoints, the standard allows its functions to be co-located in the gateway or Multiple Control Unit (MCU).

Multipoint Control Units support centralized conferencing capabilities between three or more endpoints. The MCU handles negotiations between all terminals, to determine common capabilities.

Again, while a logically separate function, the standard allows the MCU capability set to be implemented on a stand-alone device, or to be included in any other H.323 component.

Limitations of H.323

In its first release, the H.323 standard did not address several telephony features commonly used in the business environment – call forwarding, call transfer, etc. Approval of H.323 version 2 included these services, in the framework of H.450. H.323 version 3 will support additional supplementary services such as call hold, call park / pickup, call waiting, and caller identification.

However, many commonly used advanced business features still remain to be addressed by the standard for both end user and multi-site installations.

Examples of end user advanced telephony features:

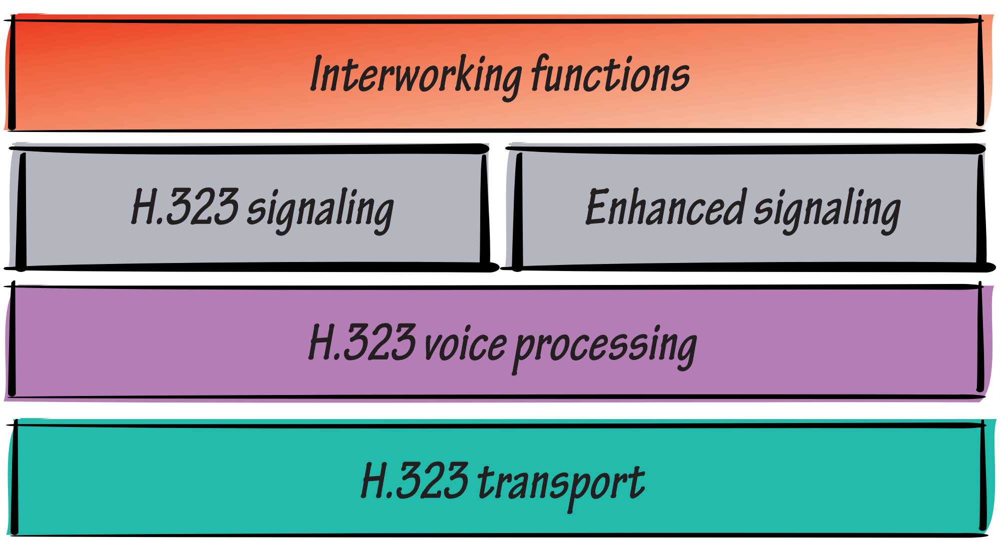
- Multi-line – Ability for one handset to function as if several, with distinct separate telephone numbers. Allows identification of call origin and personal priority of answering.
- Dynamic substitution – Call by call dialing rights, e.g., international calls allowed, dynamically transferred to alternative handset.
- Group telephony – Several telephones logically formed into a group, with incoming call distribution rules.
- Dynamic object supervision of users, trunk lines, and "bundles" of lines – status and supervision of all calls on selected telephones, etc.
- Manager assistant – Dedicated voice communication features tailored to improve the close cooperation between managers and their assistants.

Examples of multi-site features:

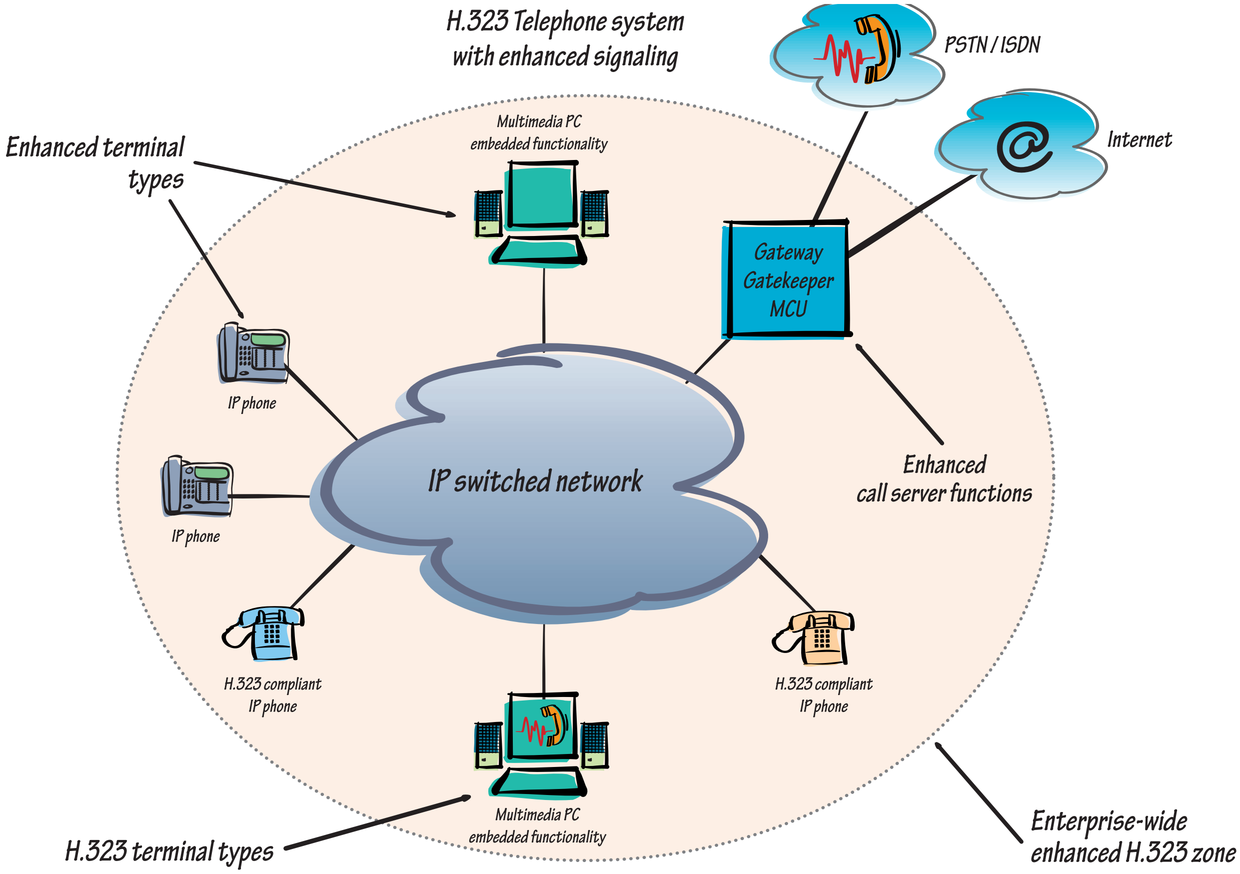
- Multi-site single centralized attendant.
- Multi-site single centralized voice mail system.
- Multi-site distributed call centers.
- Roaming in networked DECT / PWT.

Adherence to standards does provide for openness and interoperability in any sphere of implementation. However, in the case of the current release of H.323, unless users are prepared to sacrifice functionality they are using daily, an alternative to a pure H.323 implementation should be employed. Such an alternative must allow the use of H.323 in communicating outside the enterprise, and be mainly implemented using the H.323 recommendations. To provide the additional telephony feature set, enhanced client / server signaling could be employed, while the interworking functions with H.323 are maintained. Such a system could be easily migrated to standards compliance, as H.323 matures.

Enterprise-wide enhanced H.323



All components of an H.323 system would be maintained with gatekeeper, gateway, MCU, with interworking, and interoperability ensured.



Today, all current enterprise VoIP implementations are using H.323. H.323 is already in its second release and there is a lot of effort and emphasis being employed in developing the H.450 extensions (supplementary services).

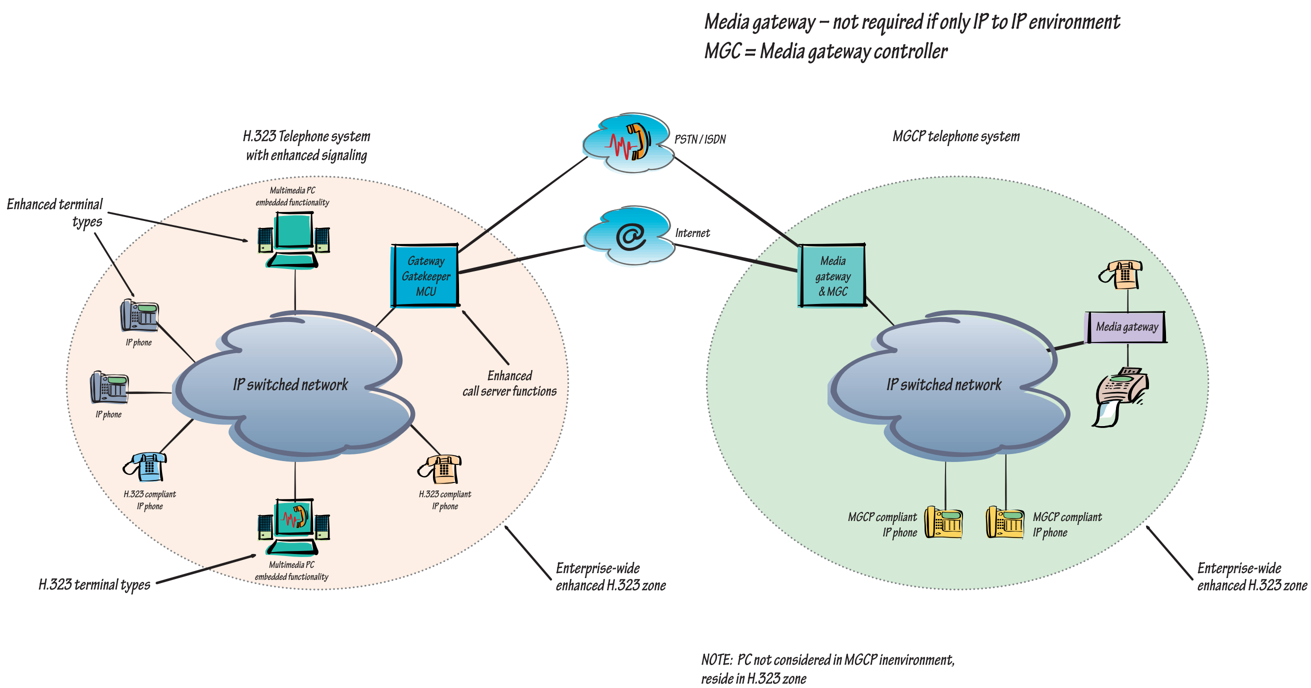
Emerging alternative standards

The reason new standards are being developed is because of the growing popularity of Voice over IP (VoIP).

The Media Gateway Control Protocol (MGCP) is one of a few proposed control and signal standards to compete with H.323 standards for the conversion of audio signals carried on telephone circuits (PSTN), to data packets carried over the Internet or other packet networks.

The MGCP is meant to simplify standards by eliminating the need for complex, processor-intense IP telephony devices. In the MGCP model, the gateways focus on the audio signal translation function, while the call agent (multimedia controllers) handles the signaling and call processing functions. As a consequence, the call agent implements the "signaling" layers of the H.323 standard and presents itself as an "H.323 gatekeeper" or as one or more "H.323 endpoints" to the H.323 systems.

Probable H.323 & MGCP interworking schema



While H.323 is the recognized standard for VoIP terminals, the IETF has also produced specifications for other types of multimedia applications. These other specifications include:

- The Session Announcement Protocol (SAP). Multicast session managers distribute a multicast session description to a large group of recipients on the multicast backbone (MBONE) use SAP.
- The Session Initiation Protocol (SIP). SIP is used to invite an individual user to take part in a point-to-point or unicast session.
- The Real Time Streaming Protocol (RTSP), RFC 2326. RTSP is used to interface a server that provides real time data.

These specifications are alternative signaling standards that allow the transmission of a session description to an interested party. The session description is described according to the Session Description Protocol (SDP), RFC 2237.

Network level convergence

Since Microsoft NetMeeting is H.323 compliant, and delivered with each new PC, H.323 will no doubt become a widely used standard for VoIP.

One of the criticisms of H.323 is that it is a heavy implementation, demanding the use of processor intensive telephones. However, it is possible to use components of H.323 with enhanced signaling between IP Phones and servers, to provide the additional feature set in use in the business community.

For carriers wishing to offer VoIP service to community groups, MGCP/H248 (where signaling processing is done in a server rather than in the handset) will probably gain acceptance by the industry, and rapidly evolve through the standard process.

The Session Initiation Protocol (SIP), which provides a "light" signaling implementation for using VoIP, is in the short term unlikely to be adopted as a preferred implementation. However, as the standard matures, it is probable that SIP may gain some support from the industry and be available in the long term as an alternative to H.323.

3. Convergence at the network service level

Common service requirements of separate, voice and data networks

The provision of network services in an enterprise's communications system, where the voice and data networks remain separate, do have a significant number of common requirements:

- A naming convention that makes usage easier, and an address scheme (in voice systems this is the telephone number, in IP data systems the IP address).
- Directory services that permit information retrieval.
- A security system that prevents unauthorized access.
- Allocation of bandwidth to time sensitive transmissions (QoS).

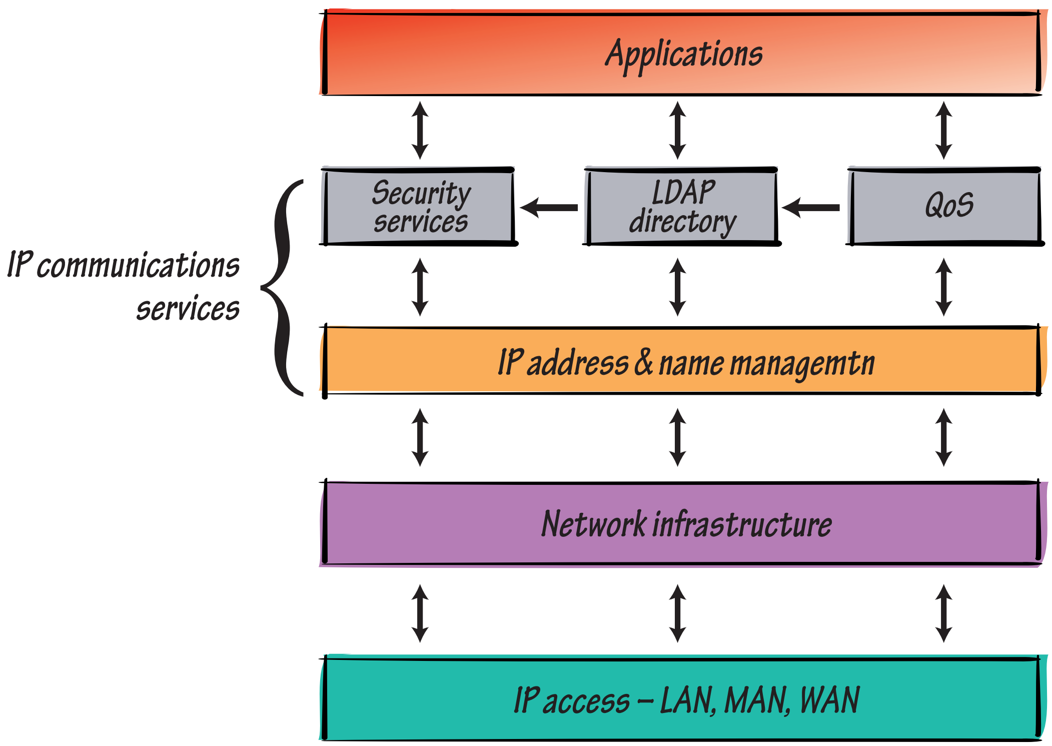
Service in a converged network

In a converged voice and data network using IP, it is both logical and economical to expect one set of services to be provided to the entire network.

Both voice and data terminals will require IP addresses. The IP address allocation is simplified and automated by the use of a DHCP server.

Being able to manage, fault find, configure, and control a converged voice and data IP network from a single station resolves the dilemma of duplication of effort and fault notification. Enabling this to be performed from a Web browser provides the network manager with the flexibility to remotely control the network, regardless of location.

Converged services



IP address & name management service

The most flexible address and name management service, deployed in enterprise IP networks, uses a scheme where the physical (MAC or layer 2) address is not used. Rather a layer 3 or IP address is mapped to a physical or logical device. This mapping is achieved using two address resolution service components:

- Dynamic Host Configuration Protocol (DHCP).
- Domain Name System (DNS).

DHCP provides an automatic dynamic allocation of an IP address. A server assigns IP addresses to devices on an as-needed basis. This removes the need to manually configure IP addresses. In addition, a range or pool of addresses can be shared between a larger number of devices, reducing the total required.

DNS provides a naming convention, allowing the use of easy to remember names in place of the destination IP address. An example of this would be the translation of an Email address, such as john.smith@alcatel.fr, into an IP address.

DHCP and DNS add flexibility and ease of use to the entire enterprise IP network for all LAN devices, both voice and data. In VoIP, the translation from called telephone number to called IP address would use the addresses generated by DHCP.

LDAP directory service

Directories are increasingly being used to store information required by network elements since they are accurate and consistent information pools.

Use of LDIFF (LDAP Directory Interchange File Format) for manual import / export operations (synchronization using file transfer) allows:

- The scheduling of import / export, done for directories sharing the same schema.
- Creation or update of selected imports or exports.

LDUP is the automatic version of LDAP allowing the automatic synchronization and update of all LDAP compliant directories.

The LDAP directory is the depository to set up a directory enabled network.

Replication of all or part of the directory tree of a database enables directory applications access to the same information, while the information itself could be contained on several distributed servers. Each server may only have the administration right for part of the overall directory database. Modifications and updates can be manually or automatically broadcast to all servers to maintain consistency.

Directory services are important to avoid the network manager having to manually configure the network elements, such as nodes or distributed applications. To simplify the management and eliminate the risks of data base inconsistency, the network element can communicate with directory servers to become synchronized.

Security service

Networks need to be designed to protect valuable information and prevent unauthorized use of network resources. The main areas security is concerned with:

- Access control – protecting the access to information (e.g., firewall).
- Authentication – individual authorization, based on a single user or device.
- Confidentiality – encryption of selective sensitive material.

Network security services are designed to control access to the network.

By performing user and device authentication at the edge or entry point to the network, unauthorized entry is prohibited before the allocation of any network resources. A security client embedded in the switching infrastructure could provide the support for standards based authentication servers.

Such a system will provided embedded security services for several types of authentication servers, the CheckPoint authentication server, RADIUS server, etc.

In addition, communication servers in use in the network should provide protection mechanisms such as:

- Device Trusted Host, to control what the management station is allowed to connect to.
- Other mechanisms such as TCP wrapper, that control the type of session authorized between a server and management station (e.g., FTP session only).

QoS service

Quality of Service (QoS) is required to enable different types of information to be transported in an IP network with different priorities. The goal is to prevent congestion from becoming a critical problem for delay-sensitive applications, such as voice.

There are two possible ways of accomplishing this:

- Enter the switching speed and bandwidth race. This implies long-term investment to ensure that network performance keeps up with changing requirements (this approach can quickly become very expensive).
- Manage the available bandwidth "intelligently" by sharing it unequally or by adapting traffic relating to an application at the source. However, the IP networks and protocols are independent of the applications being transported. In other words, they do not distinguish between recreation (e.g., surfing the Internet) and critical applications such as network management, sales inquiry response, and voice. This requires QoS functions to know how to recognize applications and assign them the desired priority.

Quality of Service can be expressed as the ability of a network to deliver a specific service for a particular traffic type. Supporting delay sensitive voice traffic in an IP environment demands some form of prioritization technique to minimize delay and delay variation. Delay would present itself as silence during a telephone conversation and reduce the quality of voice. In the IP environment, the standard 802.1 q / p indicates how a network element may classify level 2 traffic in order to assign a priority to it.

The IETF is working on the specification of OSI layer 3, and specifically IP. Four main QoS categories can be distinguished:

- *Marking*, the oldest technique, consists of inserting network priority information in each frame using the Type of Service (TOS) field. The TOS definition makes it possible to request that the network simultaneously uses the lowest cost, the fastest transit, and the maximum bandwidth. The potential conflicts that this involves have led to the creation of a new Differentiated Services (DiffServ) definition, based on standard behaviors, such as expedited forwarding for delay-sensitive applications, assured forwarding for applications requiring a guaranteed bandwidth, and best effort for the rest.

- *Dynamic resource reservation*, better known by the acronym RSVP (resource reservation protocol), is a signaling protocol. It's a reservation request that uses standard routing tables. It's not possible to provision bandwidth on a given channel when using dynamic routing. The resource is only reserved after the destination party has agreed. This reservation is then maintained by a control dialog.
- *Labeling*, known by the acronym MPLS (Multi-Protocol Label Switching) allows the equipment to send any type of traffic (IP, IPX, Decnet, etc.) with a common label to the same output port. MPLS uses label tables synchronized with the routing tables.
- *Monitoring*, known by the acronym COPS (Common Open Policy Server), uses a rules server (Policy Decision Point) and switches (Policy Enforcement Point) operating in client / server mode. When the switch (Policy Enforcement Point) receives a request, it contacts the server (Policy Decision Point) for validation.

These technical specifications themselves do not provide Quality of Service; they only make it possible to assign relative priority values. This can only be achieved by implementing them in a coordinated way throughout the network, the equipment, network management, workstations, and applications.

Logically the initiator of an IP transmission, the application should be aware of, and request, the quality it requires from the network infrastructure. However, most current applications, such as NetMeeting, ignore quality of service, and although next generation operating systems may support QoS requests, control to prevent every application requesting the highest level of QoS and subsequently flooding the network, will still be required.

Clearly QoS control and monitoring in an IP based enterprise network needs to be performed as a service function to the entire infrastructure.

Network service level convergence

Network services provides the ideal foundation for implementing intelligent converged networks and offers the ability to establish policy-based and directory-enabled networks. Policy based management provides a simplified, yet powerful approach to managing a switched network environment.

Directories enable networks to store policies that can be distributed and accessed as needed throughout the infrastructure in addition to providing a common repository for user profile information, network configurations, and security information.

A modern Enterprise Communication Application Server must automatically synchronize the databases of its different nodes to simplify the broadcast of information and avoid database inconsistencies.

A converged voice and data communication system contains multi-application servers, where applications as different as mobility, ACD, or call handling might share the same database. These databases must be synchronized with other applications such as PC telephony, network management, billing, and many others. LDAP is the way to insure the consistency.

Quality of service, in an IP converged voice and data network, must be implemented wherever it is necessary, at the IP phone connection point, in an IP trunk (or gateway), or included in the interface between workgroup voice switches and the core LAN switches.

Summary

Convergence will occur at all levels of the enterprise communications system, providing business benefits and empowering employees with productivity enhancing communication tools. Convergence is the way to stay competitive and make money. In addition, convergence will:

Save money through:

- A common infrastructure.
- Reducing WAN call charges – with least cost routing and toll bypass.

Provide productivity improvements through:

- The convergence of services and desktop integration in the workplace.
- The integration of communication in IT applications and workflow processes.
- Efficient, effective communication using new intelligent tools.

Improve customer service through:

- New multimedia services and applications.
- Web and call center integration.

Avoiding the pitfalls

Not every company will deploy convergence overnight. The compelling factor to implement convergence, as with all new technologies, will be business benefit driven and not a simple choice of adopting convergence to be trendy in the marketplace. This implies that there will be no reduction in business communication features currently in use in a converged system.

From the voice side of the equation, with a typical PBX offering on the order of 500 features, and a comprehensive applications set (mobility, call center, etc.), companies will have to decide which of this feature set is currently in use, providing business benefit, and select a converged solution that, at minimum, maintains these features.

From the data side, the improved reliability and fault tolerance required when beginning to use the data infrastructure to transport real-time voice communications, will not, in every case, be economically feasible. This arises from the fact that a large number of data infrastructures deployed in the field still contain hub and software intensive routers in their infrastructure which would have to be replaced.

Enterprise companies will begin convergence from different baselines, depending on whether their short-term priorities are to enhance the voice network, the data network, or business applications.

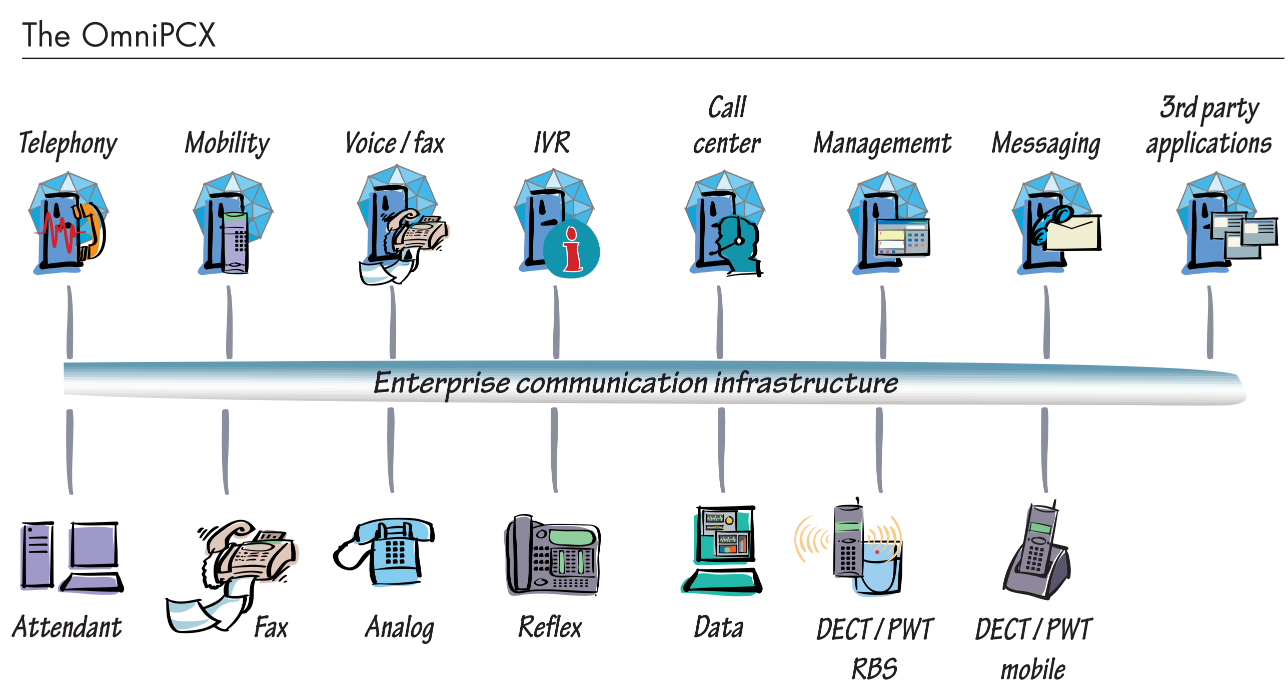
Regardless of this, many companies will have existing desk telephones and fax machines that require analog connections which will have to remain operational alongside IP devices.

At the trunk level of voice communication, the QSIG standard has been used for many years to allow different manufacturer supplied PBXs to interwork. Any converged solution should offer QSIG, allowing the possibility for several different manufacturer's PBXs to coexist in a solution. This may have the side effect of adding life to an existing older PBX system, and enable the interworking of an IP based voice solution.

Although many suppliers are promoting convergence and their IP telephony products, few have the expertise and experience in both voice and data communications to provide a converged solution that will provide the envisioned benefits the first time and every time.

The way forward

The time has come for your PBX – one of the key components of your enterprise information system – to move from its traditionally centralized, proprietary architecture to a client / server model, using open operating systems, public protocols, and industry-standard server platforms. It's a better way to deliver the information integration you need today. This natural successor to the PBX is the private communication exchange (PCX). The Alcatel OmniPCX 4400 is the first system of its kind that's a true PCX as shown below:

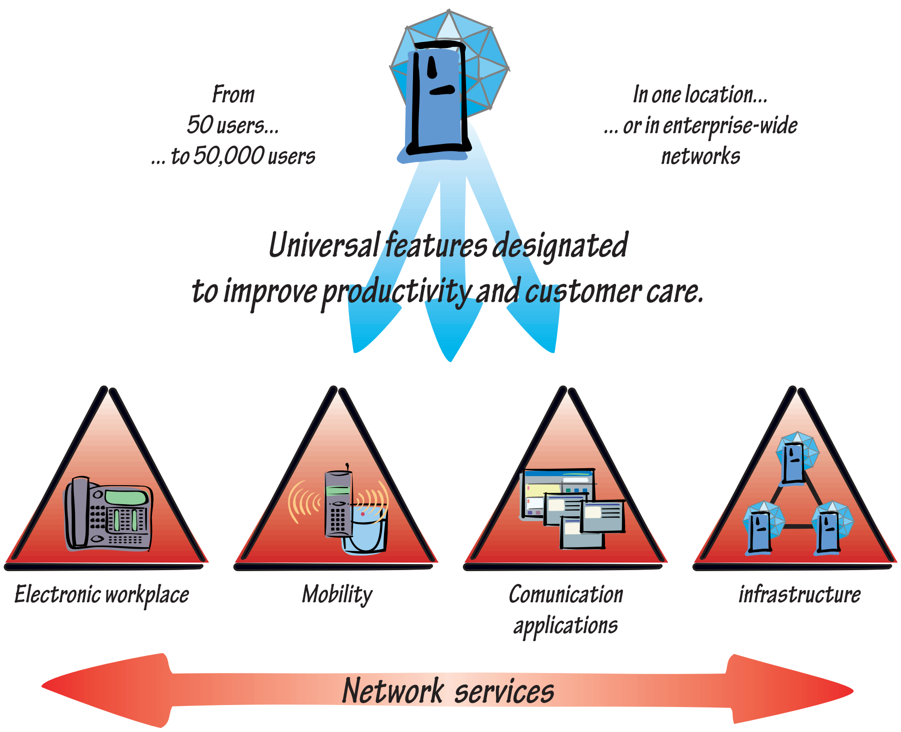


Client / server architecture – UNIX, Universal connectivity – IP, FR, ATM, ISDN, analog, workgroup voice switch, extensive applications – CTI, mobility, messaging, Web call center, advanced telephony – wired, mobile, PC-based, etc.

Alcatel OmniPCX 4400 is a voice communication system with an innovative architecture for medium and large enterprises using universal solutions for companies with between 50 and 50,000 employees. Besides the system itself, the offering integrates five additional building blocks designed to improve productivity and enhance customer care:

- User / GroupWare – Integrates terminals and PC clients to easily access time saving features and develop advanced teamwork throughout your organization.
- Mobility solutions – Solutions for on-site, company-wide, and external mobile employees including mobile terminals, mobile infrastructure, and mobility applications.
- Networking – A complete offering of voice data integration, VPN, and compression solutions to cut communication costs, as well as cost of ownership and to develop synergy between your distributed workforce.
- Network services – A complete set services designed to manage converged networks.
- Communication applications – Call center, voice mail and greeting solutions, and other applications to speed up internal communication and improve quality and quantity of customer welcome.

OmniPCX and additional building blocks



Alcatel's intelligent infrastructure solutions

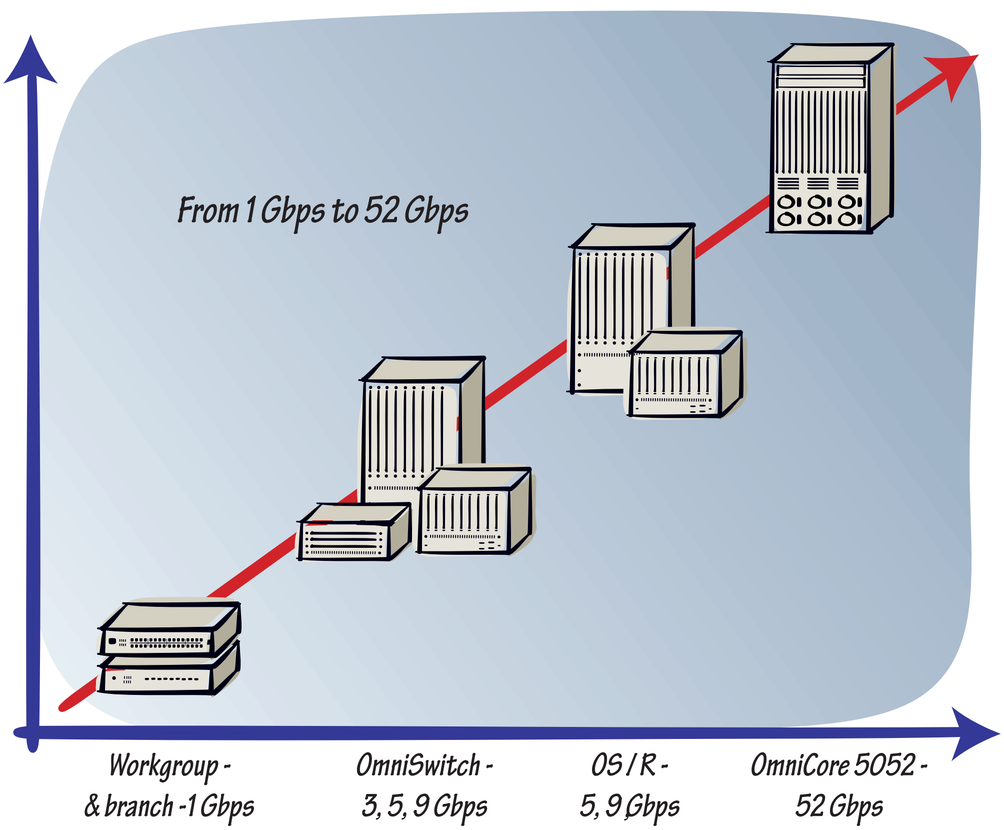
Intelligent switching equipment within the network infrastructure provides the foundation on which to build converged communications solutions.

Infrastructure needs vary in terms of both switch scalability and necessary performance. Alcatel's Omni line of intelligent switching equipment covers the needs of all:

- OmniAccess line, for deployment in branch or SOHO environments.
- OmniStack line, for deployment in departmental or workgroup environments.
- OmniSwitch and OmniSwitch / Router product lines for deployment in the wiring closet and backbone environments.
- OmniCore line for deployment at the very core of the network.

The Omni lines support multi-layer switching and concurrent use of high-speed packet and cell technologies.

Omni line of intelligent and scalable switching platforms



Embedded intelligence within the switches provides the value-added features and functions that allow the construction of reliable converged communications infrastructures. These are standard, and include:

- Comprehensive, standards based Quality of Service (QoS) and prioritization techniques. Negotiating QoS and prioritization parameters with network attached devices and mapping these parameters across the entire network

- Integration of diverse campus switching media from a single device, including token ring, Ethernet (all speeds), FDDI, and ATM, as well as wide area access via frame relay, ISDN, PPP, and ATM.
- Address management services, automatically and dynamically assigning IP addresses (DHCP).
- Intelligently distributing multicast information, thereby systematically directing information only to those individuals who actually need it.
- Direct integration from the switch with organizational directories, enabling applications to authenticate users, optimize available bandwidth, and dynamically access network resources (LDAP).
- Policy-based routing and VPNs. Providing complete user mobility while maintaining security and QoS policies.
- Firewall security. Policy-based firewalls integrated within the switches protecting the organization from illicit and harmful intrusion from the Internet as well as safeguarding the use of internal servers.
- Authentication security. Organizational users can be authenticated via the switches allowing them to access only those network resources for which they have been authorized.

Converged communications solutions from Alcatel

Converged communications solutions offered by Alcatel feature:

- No reduction in business communication features guaranteed.
- Transparent use of complete PBX feature set.
- A converged solution tailored to individual network infrastructures, allowing a "graceful" convergence in a time span that allows existing infrastructure equipment to be replaced only at the end of its lifecycle.
- A product set that allows the transparent connection and use of existing analog telephone handsets and fax machines in a converged environment.
- QSIG interworking with older PBXs.
- The most complete application suite (workplace, mobility, call center, voice processing, network services).

Alcatel is one of very few companies that has extensive expertise and experience in both voice and data communications. Integration and interworking testing with most mainstream manufactures of voice and data products allows Alcatel to guarantee interoperability of a converged solution.

As more and more enterprise corporations adopt a converged network solution, keeping the network operational increases in importance. Timely service and support will play a key role in maintaining the operational state of the converged network, allowing daily business to continue uninterrupted.

Alcatel's world-wide service organization is not only available for fault finding and resolution, but provides a network audit and planning service at the commencement of any convergence project. In this way, implementation is right the first time - without any surprises - and performed in the expected timeframe.

NOTES