



Key Considerations for Maximizing Your Video Architecture: Moving Beyond Point-to-Point Conferencing

The TANDBERG Solutions Overview

A WHITE PAPER BY

TANDBERG

JULY 2005

I. Executive Summary

Video communications have come of age — corporate networks are becoming more powerful, with sufficient bandwidth to carry video, audio and data signals simultaneously; there is a keen recognition of the cost and productivity advantages of face-to-face video communications; and an increasing number of private and public sector enterprises are adopting this technology as a strategic, mission critical necessity at the core of, and throughout their organizations.

As more businesses consider implementing new video communication solutions or enhancing their existing solution, important decisions must be made. Executives and technical decision makers must choose from an increasing number of alternatives. Knowing what questions to ask, and what features are important in a video architecture will help you make the best decisions for your company.

This white paper gives a basic foundation for approaching the task of selecting the right video solution for your organization's requirements. First, we cover some broad principles to keep in mind:

- the basics (advantages of video communications, understanding user requirements)
- key considerations (migrating from ISDN to IP-based environments, security)
- return on investment issues (legacy accommodation, the importance of selecting a standards-based architecture solution designed for growth).

We then define the components of a typical video architecture and the important features to seek in each. Finally, we provide a summary of the important considerations in selecting a video solution.

Table of Contents

I. Executive Summary1

II. Introduction - Designing Your Video Architecture3

III. Architecture Components6

IV. The TANDBERG Approach to Video Architecture11

V. Summary13

II. Introduction — Designing Your Video Architecture

When designing a video architecture for your organization, there are broad considerations that must be addressed. These include:

- Rationale of video communications
- General selection criteria
- User requirements
- Mixed network environments
- Mobility
- Security considerations
- Multi-vendor/legacy environments
- Standards

Why video communication? Designing an effective video communication system for your organization's needs begins with understanding why video is such an advantage in today's world. In a recent survey, 56% of business professionals estimate they waste more than 30 minutes a day using inefficient communication methods. In the U.S., that equates to an estimated \$297 billion per year.¹

Professionals agree that ideal business communications should be personal, interactive, and accommodate both data and face-to-face (high quality audio/video) information sharing. Video makes important messages easier to understand, enables quicker decisions, builds high trust, makes negotiating easier, reduces confusion and misunderstanding, makes people more accountable, and is better for detailed explanations. Organizations that implement thoughtfully-designed, well-implemented video communication solutions realize significant cost savings and productivity gains throughout their enterprise.

Key criteria for video solutions – Any video communication solution must meet certain general criteria. They should be:

- **Reliable** – The solution must be fault tolerant, compatible with older and newer systems, must support multiple protocols, manufacturers and different speeds and be able to support built in redundancy and fail over in order to deliver maximum reliability.
- **Scalable** – When your needs dictate a move from five to twenty to 500 endpoints, you should not have to redesign your basic architecture. A scalable solution will provide consistency, as well as device and component modularity, in order to scale with your needs. What's more, your video architecture should enable you to take advantage of the latest technology advances easily, primarily with software upgrades. Hardware upgrades should not be required on a regular basis – instead, robust processing capability should be built into your entire system architecture, to future-proof your investment.
- **Usability and Managability** – If your users or administrators find it too difficult to operate or manage your video solution, or the quality of your video calls is average

BENEFITS OF VIDEO COMMUNICATION

- Be two or more places at the same time
- Have more frequent contact with colleagues, partners, suppliers and customers without having to leave the office
- Allow for ad hoc meetings to discuss urgent matters and take immediate action
- Foster highly personal, responsive relationships
- Save time, resources and money
- Improve the effectiveness of your working day and your quality of life

¹ Results of a recent survey conducted by RoperASW and TANDBERG

at best, your use of video communication will dwindle and your ROI will plummet. Administrators must be able to easily dial, schedule, and manage the solution. Users must find it quick, easy and convenient to operate, and have a high quality experience in order to integrate video into their daily business processes.

User requirements – Just as you would have a comprehensive strategy for your email, voice and other communication systems, your video solution should fit into a well-defined and unified communication strategy for your organization. A best-fit video architecture must take into consideration the broad spectrum of user requirements.

- Executives will require multi-point boardroom applications
- Trainers will value interactive, one-to-many capabilities
- Satellite office and telecommuters will need desktop video solutions
- Field and mobile team members will require powerful, ruggedized units

What's more, specialized applications will require more than a "one-size fits all" approach. Video solutions specifically designed to integrate seamlessly into your functional verticals applications (training, medicine, legal/judicial, manufacturing, field operations and more) will be far more successful in meeting your users' needs.

Questions that need to be addressed include: what does your video communication system need to do, for each set of users? Should it act like a phone, a PC monitor, a stand-alone system? Are data, voice collaboration and instant messaging (IM) or presence required? Is web collaboration important? Ensuring that all forms of communication (video, instant messaging, Web and audio collaboration) are integrated into a single, seamless strategy will ensure maximum adoption and success.

IP migration & mixed environments – Many businesses are moving to voice-over-IP systems, and this will impact the video architecture you design. IP convergence offers many cost and functional consolidation advantages, and video over IP dovetails with this technology. Your organization's migration plans should be considered: is your organization planning a migration to IP-based communications? Does your network have adequate bandwidth for video? Will you still need to accommodate ISDN connections with your offices, contractors, partners or customers? What types of firewalls do those external organizations have? And what about hacking incidents, identity theft and other IP-network concerns? Designing an inclusive, secure video solution will be an important element in your overall strategy.

Mobility – 3G technologies are becoming widely available around the globe, and mobility is critical to productivity. 3G access allows mobile users to connect to any video system on your network. Does your video solution provide access to the 3G network, and what are your plans to increase the productivity of your mobile work force?

Security – Satisfying security requirements while maintaining user access is one of the most important issues in video communications — in communications of all kinds, especially IP-based solutions. Who is listening to your video call? Are callers who they say they are? How can you administer security (quickly, easily and cost-effectively) for each and every caller and protect your network resources? Content security and access control — these are key considerations that must be addressed by the encryption, authentication and call control technologies of your video architecture.

Equipment based on proprietary architectures is obsolete more quickly. However, standards-based equipment from 1995 still can be used today. Standards-based architectures are clearly the better investment.

From AES to Type 1 DoD-level intelligence level security requirements, your video communication architecture must be able to accommodate your needs. Consider what you will need to deploy in order to communicate with all your stakeholder groups. Are external devices required? Will you need to go to a secure facility? How you integrate the answers into your solution are important to ensure that no department is isolated, and you achieve every level of connectivity you require.

Especially, your video architecture should have fully integrated the H.235 authentication standard. This allows you to set call policies, have units self-identify as trusted devices, and provides dramatically easier control over your network by eliminating management redundancies. H.235 authentication provides IT managers with the tools they need to implement video communication security exactly as they would for other applications on the same network.

Multi-vendor/legacy equipment accommodation – Many organizations have existing installations of older equipment that still have value. Looking forward, your organization needs to adopt the newest technologies and capabilities, and will need to manage, schedule and maintain both older and newer equipment in a blended environment. Your video architecture should include a management software that will embrace and maximize your legacy investments, enabling easy administration of both old and newer equipment in a multi-vendor environment from a single, powerful interface.

Standards-based for universal connectivity – The ability to communicate with anyone, using any equipment, should be your goal for your video communications solution. Selecting standards-based solutions is the key – as the move toward universal connectivity proceeds, those solutions developed on standards (not using proprietary mechanisms) will ensure maximum interoperability, and will help you get the longest life from your video equipment.

III. Architecture Components

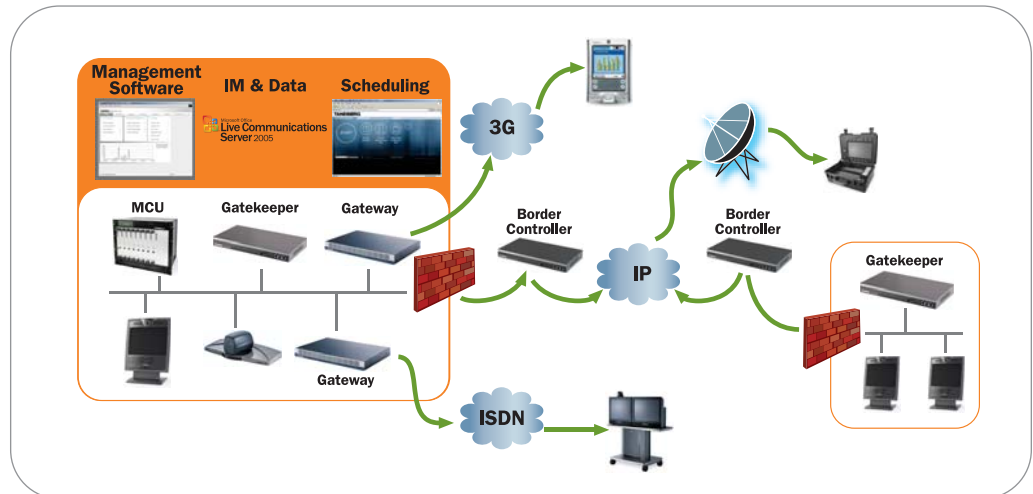
What are the components and required technology involved in a video architecture? Where do these individual components fit in a full solution? Below is an illustration of a typical video architecture, with each group labeled.

Following the illustration, we define these components and provide a discussion of the features that are important in each.

SOLUTION COMPONENTS & CONSIDERATIONS:

- Endpoints
- Infrastructure products
 - Gateways
 - Gatekeepers
 - Border controllers
 - MCUs
- Management & scheduling system
- Considerations:
 - Quality of service
 - Firewall traversal
 - Dial plans
 - Call policy
 - Feature sets:
 - H.264
 - Dual stream presentation

Sample Video Architecture



Endpoints

The endpoints of your video architecture are the hardware components through which users send and receive video. Ranging from ruggedized units for mobile field use to full-scale wall-size boardroom systems, your endpoint options should offer form factors for every use, every application, in every work environment.

Endpoint solutions should share a common user interface, and should work on a wide variety of networks and protocols including IP, ISDN, V.35, SIP, SCCP and 3G. In fact, easy use and consistent conventions throughout the entire family of endpoints will maximize more rapid user adoption.

Quality, reliability, and the ability to integrate tightly with other office communication systems (instant messaging, web conferencing, existing video and audio feeds, IP telephony such as Cisco CallManager, Microsoft Exchange or Lotus Notes, for example) are also key features of video endpoints.

Generally, endpoints can be grouped into:

- **Personal Systems** – These units are designed for use by a single users or small groups of no more than three. A premium is therefore placed on quality, ease of use and functionality, and personal systems must maximize the use of office space. Typical requirements for personal systems may include:
 - PC monitor replacement, or large LCD
 - Built-in Multipoint control unit (MCU) for easy, ad hoc conferencing with audio

and video sites

- Dual Stream capability for presentations
- Stereo for multi-media applications

- **Group Systems** – These systems are ideal in conference rooms where large meetings will be held. Typically, display devices are large plasmas or projectors. Requirements include:
 - Built-in MCU for easy, ad hoc conferencing with audio and video sites
 - Dual Stream capability for presentations
 - DVI connections for high resolution presentations
 - Stereo for multi-media applications
 - Large display screens
 - High bandwidth capabilities
- **Industry- or Application-Specific Systems** – These endpoints are specialized units that serve specific vertical requirements, such as mobile, telemedicine, distance education, judicial or manufacturing needs. Each is designed with the unique environment and user requirements of the industry or application they are built to serve.

Infrastructure Products –

Infrastructure products are the components through which video calls are routed, merged, and/or converted to other protocols in order for each endpoint to reach its destination or destinations. The infrastructure products should easily integrate into your existing network and should support the fullest possible video, audio and security feature set. The infrastructure products must provide the highest possible user experience whilst ensuring their own transparency when providing connectivity between a variety of systems across multiple networks and protocols.

- **Gatekeeper** – A gatekeeper provides critical functionality to enable IP video communications, including:
 - **Alias** – for security and ease-of-use issues, dialing by IP address is not recommended. A gatekeeper provides a translation between the actual IP address of a system and an easier-to-use alias, such as a name or number.
 - **Zone management** – A gatekeeper is a central point of registry for all devices in a zone (a virtual video network). This way, aliases can be coordinated and ‘rogue’ video device control is made easier.
 - **Call management** – the gatekeeper is the central point of call management in a zone. A gatekeeper may limit call bandwidth and the total number of calls.
 - **Authentication** – the gatekeeper is the unit through which endpoint authentication is supported via H.235 technology. This adds an additional layer of security, ensuring that each endpoint in your network is authorized for use.
- **Border controller** – A border controller allows H.323 traffic to traverse the firewall without having to “pin hole” or create a specific rule for H.323 video. A border controller seamlessly and securely allows video communications by using default behavior of firewalls. Border controllers should be non-intrusive in regards to existing network design, allowing for easy deployment.
- **MCU** – Multipoint Control Units enable video conferences between three or more

persons. Different network environments require different MCU resources — in distributed network environments where network resources are not centralized, multiple (often smaller) MCUs localize the resource and “no single point of failure” redundancy. In centralized network environments, centralized bridging management is essential and can be achieved with a robust MCU capable of managing large quantities of video traffic and scalable to meet the most demanding needs. Key features of your MCU should include non-blocking design, transcoding, rate matching, continuous presence and highest level encryption technologies.

- **Gateway** – A gateway allows different network protocols to communicate by translating one protocol to another, specifically translating H.323 to H.320 bi-directionally. The gateway negotiates video and audio calls between parties, defines access protocols, and provides operational and security management for your video calls. It should work seamlessly with your video conference call scheduler and management suite software, and should provide highest levels of content and access security. In particular, it should deliver standards-based encryption and authentication (H.235).

Management & scheduling system –

Your system administrators will require an easy, unified way to manage your entire organization’s communication solution. Management software will help you coordinate and troubleshoot resources, understand your usage patterns, and maximize your resources accordingly. Ideally, your management software should work with other manufacturers’ products, so your administrators can manage your entire video system with ease. Graphical reporting and rapid, proactive troubleshooting are important features of a robust video system management software solution.

In addition, software that seamlessly integrates with existing room and appointment scheduling software (such as Lotus Notes or Microsoft Exchange) enables users to quickly and easily schedule all the resources they require for any meeting. For ad hoc calling, integration with presence based applications provides users with a familiar interface by which to launch calls.

- **Considerations:**
 - **Quality of service (QoS)** – QoS refers to the ability of a network to provide consistent and reliable performance that is acceptable for the applications the network carries. For video, jitter and packet loss would ideally be non-existent and delay be minimized. There are several mechanisms used for QoS that prioritize traffic in the network: these include IP Precedence, DiffServ, and RSVP. Separating types of traffic is another way to provide QoS.
 - **Firewall traversal** – Your video architecture must include technology that allows video calls to connect across your firewalls, while still maintaining security, and do so with ease. As a rule, firewalls block video calls. Unsolicited incoming connections are typically not allowed, and although firewalls can be “opened” to allow video calls, often the process is cumbersome, time consuming and unreliable. More importantly, it can make your network vulnerable by reducing security, or cause the loss of important features, such as encryption.

However, there exists technology that allows simple, secure traversal of firewalls

for your video calls. Ideally, this technology should be built into the components of your video solution, rather than be available only with expensive add-ons.

- **Dial plans** – Unlike audio, which has a coherent global dial plan (with standardized country code, region, exchange and terminator numbers), there are no global video numbers dialing plans. Calling from one number to another, outside your own system, can be very difficult.

Technology exists today that enables easy access to other numbers through border controller registration, providing a global dial plan based on URI addresses and DNS, just like email. Enterprises that do not share dialing plans can communicate using a proven, trusted standards-based and scalable method of call routing.

- **Call policy** – Call policy is the ability to define rules for end points, and what network resources are available (gateway, MCU, border controller). The ability to define call policy gives the administrator greater control over the video network. Expensive resources, such as access to ISDN or MCU resources, can be explicitly controlled and managed.

– **Feature sets:**

- **H.264** – The ratification of the H.264 standard was one of the industry's major innovations in 2003, enabling users to achieve the same video quality at half the bandwidth of previous standards, a major cost-savings benefit. Look for a provider that supports H.264 across the entire architecture, including endpoints and infrastructure products, whether you are using ISDN or IP. This ensures that you will receive the best video experience possible.
- **Dual Stream Presentations** – This feature allows for a system to send two video streams simultaneously. This makes communicating easier by allowing a viewer to, at the same time, see the person speaking as well as the presentation, file or object to which the person is referring. H.239 is the ITU standard that defines this feature.
- **Security** – Your video architecture should afford both content and access security. Content security is best ensured by AES/DES encryption, which encrypts all audio, video and data that are sent at the maximum required security levels. Ideally, this is accomplished automatically — complete with automatic secure key exchange, and unique one-time (non-reused) keys. Look for open standards implementation of the ITU approved encryption mechanism.

Access security is also essential to ensure the devices in your architecture are secure. Incorporation of H.235 authentication into your video components requires systems to 'log in' to the video network and receive a customized call policy set up by the video network administrator. Additionally systems should be able to turn off various protocols such as HTTP, FTP and SNMP if they are not being used. Your system should notify administrators of failed log-ins, reporting the source IP address, what protocol was used, and the time of day the failed attempt was made — throughout the management system. Additionally, your video systems should support protocols like HTTPS, MD-5

challenge and others for secure management purposes.

- **AAC** – Your video solution should deliver the industry's highest quality audio. Look for systems that provide excellent fidelity, low signal-to-noise ratio, and that utilize the MPEG4 AAC-LD standard — ratified for use under H.320 and H.323 by the International Telecommunication Union (ITU). This open standard encourages interoperability and systems that support it provide superior digital audio delivering the finest CD-quality stereo sound as an integral part of the visual communication experience.

IV. The TANDBERG Approach to Video Architecture

In creating a comprehensive video architecture, TANDBERG takes these considerations into account, building in the features, functionality and standards-based capability essential in any video communication solution. TANDBERG has designed each software and hardware component with these criteria in mind to ensure our end-to-end video solution meets your individual requirements, and delivers maximum performance and return on your investment.

- TANDBERG Endpoints give you:
 - Broad form factor options for every user, in every kind of work environment
 - Application-specific devices (one size does not fit all), including medical, judicial, mobile and education solutions
 - Superb quality and reliability
 - Consistent user interface throughout entire product family
- The TANDBERG infrastructure components:
 - Are standards-based, future-proofing your video investment and affording maximum ROI
 - Easily integrate and maximize your existing legacy equipment investment
 - Offer single, centralized software management for all components in a multi-vendor environment
 - Come with transcoding and rate matching embedded in the devices, rather than being available only as expensive add-ons
 - Provide universal feature sets throughout your solution, independent of what you are doing at any one point in time: your features work, whether you are on an office system, talking to an auditorium, or talking to a voice-only system
 - Give you the advantage of appliance-based systems (designed specifically for that particular function) — these are less susceptible to problems, more reliable than multi-purpose devices, are easier to deploy and manage
 - Support standards based security mechanisms such as authentication and encryption
- The TANDBERG Management System (TMS) scheduling and management software allows easy, powerful control, administration and management of all your video systems. TMS:
 - Is multi-vendor, managing other manufacturer's devices seamlessly within the system
 - Is multi-device, providing complete system coverage and control
 - Gives graphical views, as well as delivering sophisticated statistical analysis of usage patterns
 - Allows proactive troubleshooting
 - Integrates seamlessly with your organization's scheduling software (Lotus, Microsoft or custom applications)
- Firewalls & dialing plans — TANDBERG's unique Expressway solution creates a secure path through the firewall — for affordable, trusted visual communication without experiencing any feature loss. Expressway is simple to deploy, and even supports IP-video in satellite and home office/telework environments — simply plug a Media Experience (MXP) endpoint into a DSL or cable modem and it works

— and is immediately a part of the enterprise dial plan.

Expressway uses URI-based dialing to provide a global, massively scalable dial-plan for end-to-end IP communications. This proven technology allows enterprises to visually communicate with other enterprises on varying dial-plans, and helps ease IP video network constraints.


- Scalability – To give you maximum flexibility, TANDBERG has designed its entire portfolio to provide video communication solutions that grow with you, painlessly. The ability to scale your solution to meet changing requirements depends largely on how much processing power is built into your equipment, over and above today's requirements. TANDBERG has built remarkable processing power into its MXP platform, allowing new advances to be accommodated primarily by software, not hardware, upgrades. This built-in, robust processing capability helps to keep your costs manageable throughout the lifecycle of your video solution.

V. Summary

As organizations of every size and function adopt video communication solutions, thoughtful consideration must be given to the role video will play in daily processes and productivity, the planned scope of deployment, and the requirements these video solutions must meet in terms of current and anticipated user needs.

Looking at your video architecture from an enterprise-wide view is essential, allowing you to plan for the ongoing needs of your organization as you design video systems that are a best fit for your requirements. By keeping in mind some of the key challenges for the technology (such as handling mixed ISDN and IP environments, firewall/security and dialing scheme issues, etc.) as well as foundation concepts (the importance of standards-based architectures, legacy and multi-vendor environment accommodation), decision makers can make wise purchasing decisions that will ensure long-term performance and maximum ROI.

The TANDBERG approach to developing a comprehensive video architecture is unique — only TANDBERG offers this breadth and depth in complete, end-to-end solution capability. From endpoints to infrastructure, from management software to secure firewall traversal, TANDBERG leads the industry with innovative solutions, and is first to integrate the latest technologies across its entire product line.

Businesses can look to TANDBERG for highest quality, comprehensive video solutions that enable unlimited face-to-face visual communications for maximum productivity. 

For more information on TANDBERG'S Video Architecture Solution, contact:

IVCi, LLC
 180 Adams Avenue
 Hauppauge, NY 11788
 Toll Free: 800 224 7083
 Telephone: +1 631 273 5800
 Fax: +1 631 273 7277
 E-mail: info@ivci.com
 Web: www.ivci.com