



Intel[®] Technology Journal

Converged Communications

Enterprise Converged Network—One Network for Voice, Video, Data, and Wireless

Enterprise Converged Network—One Network for Voice, Video, Data, and Wireless

Sanjay Rungta, Information Technology, Intel Corporation
Omer Ben-Shalom, Information Technology, Intel Corporation

Index words: Voice over IP, local area network, wireless local area network, asynchronous transfer mode, wide area network, access point, Quality of Service, RADIUS, 802.1x

ABSTRACT

The different components of the trio commonly called “triple play” today (Voice, Video, and Data) were originally developed in different domains, and the networks carrying them were designed and engineered specifically for their requirements. The implication was that different network environments had to be supported concurrently to allow all three services to exist. Asynchronous Transfer Mode (ATM) was the first network technology specifically created to allow for the convergence of data, video, and voice over Wide Area Networks (WANs), but it has failed to be accepted in the Local Area Network (LAN) space due to unproven costs and complexity. Ethernet has come out as the clear dominant LAN technology. With the rapid emergence of mobile networking using Ethernet-based wireless LAN (802.11) technologies the market is exhibiting renewed enthusiasm for communication convergence based on LAN technologies. Recent advancements in security and Voice over IP (VoIP) reliability and quality along with the seamless integration of new WLANs and traditional LANs have provided the technical and business impetus to converge data, video, and voice networks into a single cohesive network service infrastructure. However, supporting varying classes of services and capabilities on LAN and WLAN environments has proved to be very challenging due to strict requirements on IP packet loss, packet delay, and delay variation (jitter). To make convergence of services realistic we are looking at recent advancements in Quality of Service (QoS) algorithms particularly in the areas of process and packet prioritization and scheduling as the main enabler for allowing network architects to overlay voice, data, and video on a shared data network. Furthermore, WLANs (802.11) have become a mainstream capability suitable for the enterprise as they provide converged services while being “always connected.” This concept allows the LAN to become an integrated method of connectivity not just

for traditional devices such as desktops but also for a large group of mobile computing devices of varying form factors and mobile telephony users presenting a significant and appealing value to businesses. We propose a campus-level LAN in which the three previously separate networks are “converged” seamlessly into one mobility-enabled enterprise network architecture. We estimate that the simplicity of the converged architecture will contribute significantly to the total cost of ownership (TCO) of managing the capabilities independently in a campus for IT.

In this paper we present the enterprise converged network architecture and its uses. We describe the case studies that will be used by ISTG at Folsom for LAN and voice convergence and the plan for a wireless network to integrate with LAN to make it another access media to support all LAN services.

INTRODUCTION

Most enterprises today support at least three separate networks (LAN, WLAN, and voice) to support static and mobile data and voice (Figure 1). Each network was optimally designed to meet different requirements but with the convergence of services the cost and support burden associated with upholding three separate networks are becoming prohibitive. The unification of voice, video, and data service infrastructures for both stationary and mobile devices is inevitable and already termed “quadruple play” by the industry. Specifically the equipment to provide voice services is going to migrate from today’s vertically oriented PBXs to IP-based telephony servers supporting call, registration, and enhanced calling services. It is anticipated that core telephony services will integrate and blend with video and text-oriented layered services where network service infrastructure convergence is feasible from an operational and cost perspective. Since voice infrastructure will ride over IP, its quality will depend on QoS-enabled IP core network services for delivery of real-

time transport. User and operational advantages are anticipated through a more flexible system based on a PC or server-based model for rapid evolution via voice and data service integration.

The development and integration of rich and integrated applications over a common set of layered services will also enable the unification of electronic mail, voice and

text messaging (e.g., IM) over common users' devices and a converged network infrastructure. Nevertheless, matching the scalability, cost, and reliability advantages which the enterprise maintains with its current environment, will be the single biggest challenge in realizing a voice and data convergent communication vision.

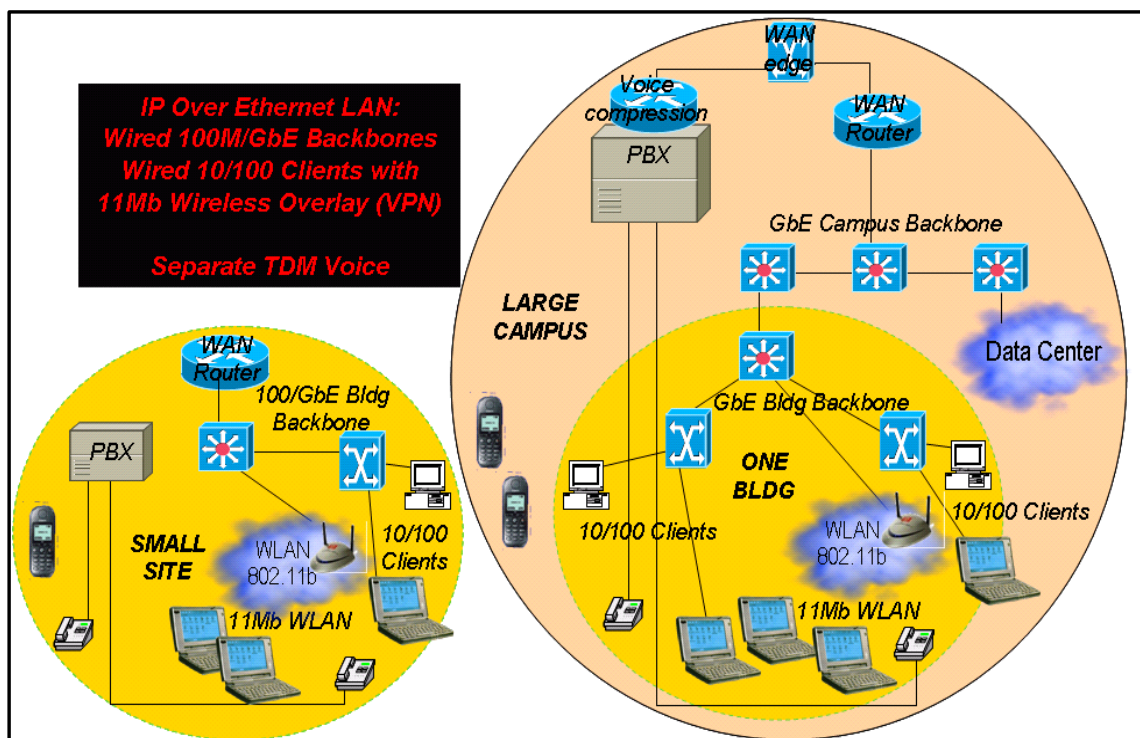


Figure 1: Existing separate LAN, Voice, and WLAN

In order to support voice and video, which are delay sensitive services, data services networks have to address and support basic scheduling capabilities. Since voice is considered by most users and the regulatory domains to be a more critical service than data, securing voice is an important factor. One of the biggest security problems in the enterprise network is the standard “permit all” paradigm of the LAN. While this openness was a catalyst to the growth of computer networks, it also allows devices with security issues to freely connect to the network and potentially compromise other devices. Traditionally LANs have also paid no attention to admission control and cannot separate users with different access rights such as company employees and visitors. As more and more mission-critical services are added to the LAN, steps must be taken to enforce those rights through comprehensive security and QoS mechanisms.

LAN READINESS FOR CONVERGED COMMUNICATION

The LAN infrastructure needs to be robust and redundant in order to support converged services. A typical LAN three-tier architecture is shown in Figure 2. In order to get LAN ready for data, voice, and video convergence over LAN and WLAN, separate changes need to happen at all tiers of the architecture. In the next section we describe required changes in the area of security, power over Ethernet (PoE), QoS, and WLAN integration.

Security

As stated, so far voice and data networks have addressed security by keeping two separate networks with minimum overlap in traffic. However, in converged network environments we are exposing critical services such as VoIP to data network vulnerability. Therefore, during the development of converged networks, all measures should be taken to protect and minimize the impact on data

networks. Figure 2 shows the existing three-tier LAN architecture [1, 2]. The edge of the network (access layer) does not have any security deployed allowing anybody to connect to the Intranet. Most of the LAN infrastructure is not ready for converged communication. During a crisis, access-control lists are deployed at the building distribution level to protect from Malware.

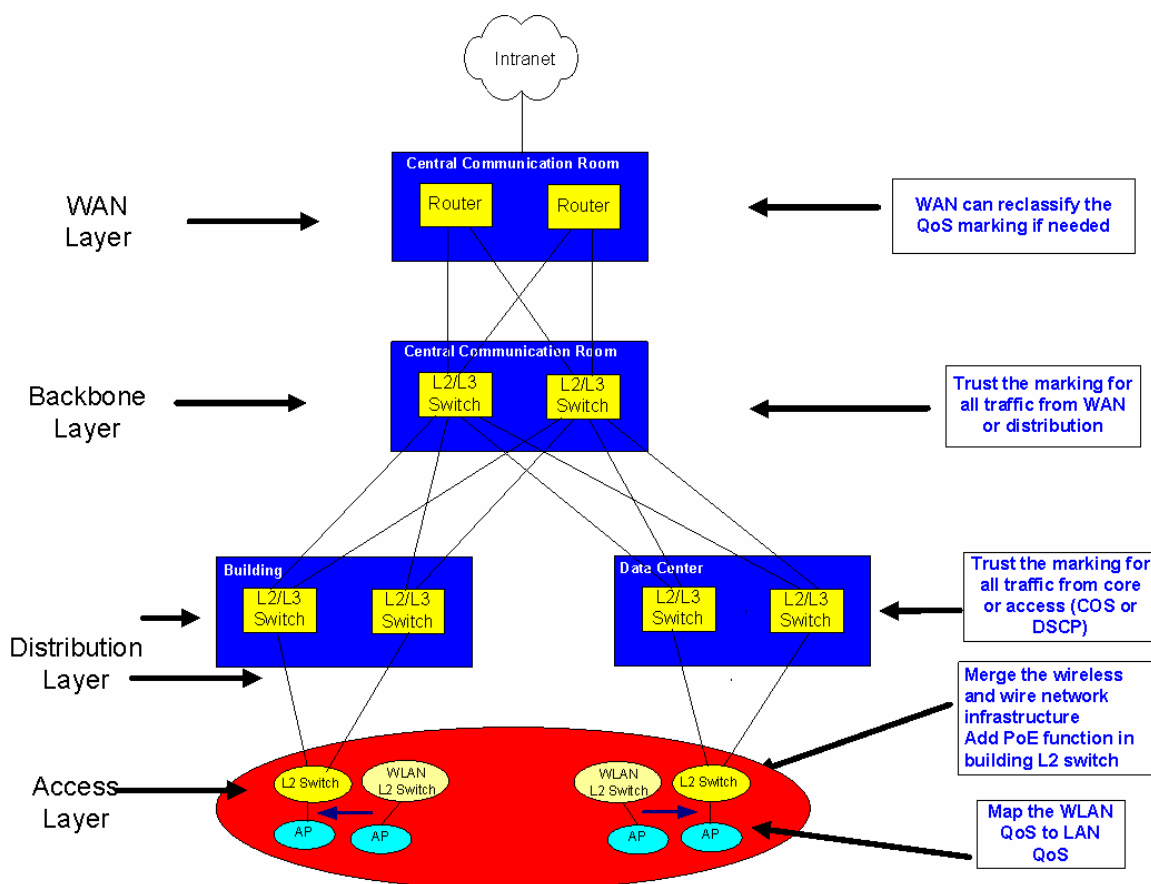


Figure 2: Existing three-tier LAN architecture

Based upon the quantity of building routers, the propagation of ACL can take several hours and during this time sensitive services such as voice may be impacted. In order to avoid this from happening a number of steps should be taken: only authorized machines should be allowed to be connected to the LAN and the ability to detect and remove offending devices at the access location must be developed. In this area, multiple capabilities and technologies need to be leveraged to protect the LAN and reduce the risk of failures due to malicious code. The IEEE 802.1X standard is one example that offers both wired and wireless devices a method to authenticate both the device and the user before allowing access to the network. Based on the Extended Authentication Protocol (EAP), the 802.1X standard allows direct communications

using EAP between the end device and a backend authentication (RADIUS) server prior to allowing network access [3, 4]. Only authenticated users and devices are allowed to connect to the production VLAN. All other devices are either not allowed connection to the enterprise or can be placed on limited access networks. Since EAP is by design extensible, it can be expanded to include checking compliance with corporate policies such as operating system patches and virus signatures. When the device does not have the right credentials, it can be redirected to a different network where it can get patched or be limited to accessing the Internet only. This will guarantee that only trusted machines with the right credentials and posture (domain account, operating system level, patch level, configuration level, etc.) can access the

Intranet, a feature that will enhance the security level for both voice- and data-using devices. In the future, stateful level inspection, network intrusion protection systems, or NBAR can also be performed at the distribution layer. This can provide protection from application-level attacks. The distribution layer should continue to be used as the first multi-layered defense with the access layer used to enforce connection policies and connection termination capabilities. Sub/Super VLAN (also known as private VLAN) technology can also be used to isolate some systems within a broadcast domain.

Special attention should also be given to keep all the critical services (DNS/DHCP/tftp, etc.) in separate protected domains or enclaves.

Power over Ethernet

With the advent of the 802.3af standard (Power over Ethernet, PoE) the number of cables used is decreased since power is supplied to the end device over the LAN connection. Moreover, if the edge device supports 802.1q trunking, this single connection can support both a dedicated VoIP device (hardphone) and another (data) device such as a desktop computer or a laptop computer connected through it. A single Ethernet port will thereby support both voice and data devices, and the 802.1q protocol will separate voice from data. It will also require that all access switches support PoE function. Enterprises should make the decision on PoE vs. non-PoE at access switches, based upon a return on investment type of analysis. In an existing building with the right switch it is not always necessary to have PoE-based line cards. Most VoIP hardphones can also use an external power supply that can be connected to a regular building power source. Therefore it is good practice to build all new networks with PoE but for existing buildings, using an existing external power supply is still a very cost-effective option.

Quality of Service

The main objective of QoS within LANs and WLANs is the prioritization of traffic during congestion. Since all the LAN traffic is bursty in nature, it can cause buffer (especially transmit buffer) over-runs and under-runs. The first step in a QoS is to identify the traffic and classify it to enable different traffic types to be processed differently. Typically, access control lists are used to identify the traffic using the source/destination IP address and TCP or UDP ports at Layer 4 or the application signature at Layer 7. Policing or shaping of the traffic can happen at the same device, or alternatively the packets may be marked with a specific priority at Class-of-Service (CoS) bits at Layer 2, Type-of-Service (ToS), or Differentiated-Service Code Point (DSCP) at Layer 3, and those markings can be used later on by other devices. To keep the QoS end-to-end, all intermediate routing/switching devices must trust

the marked traffic to minimize the re-marking process. It is also best to identify and mark the traffic closest to the source (normally at the access layer switch in the wiring closet as shown in Figure 2) [5, 6]. Since most of the marking within the Intel LAN environment will be done by the applications running on a system or hardphone, it is essential to allow trust of the endpoint marking within the LAN and WLAN. It is also important to have separate queues for voice (latency sensitive) traffic and for other traffic, and a priority-scheduling scheme should be given to it. In the coming years, new applications/services are being planned to be deployed to improve the productivity of users. VoIP in LAN and WLAN is one of them. Convergence of multiple communication methods will also drive the need for QoS in LANs and WLANs.

WLAN Integration

Many enterprises treat WLAN as unsecure and hence require users to use VPN services before gaining access to corporate resources (Figure 3). This has been the general policy due to the well documented weak security of the Wireless Equivalent Privacy (WEP) security measure. With the latest development in WLAN security standards (802.11i, using WPA2 with authentication based on 802.1X authentication and AES encryption), however, the VPN component can be removed from the wireless network allowing the Access Point (AP) to directly pass traffic to the LAN infrastructure. Recent LAN security-related protocols, mainly MACsec (802.1ae) and MAC key security (802.1af), make the authentication and encryption schemes of WLAN and LAN converge.

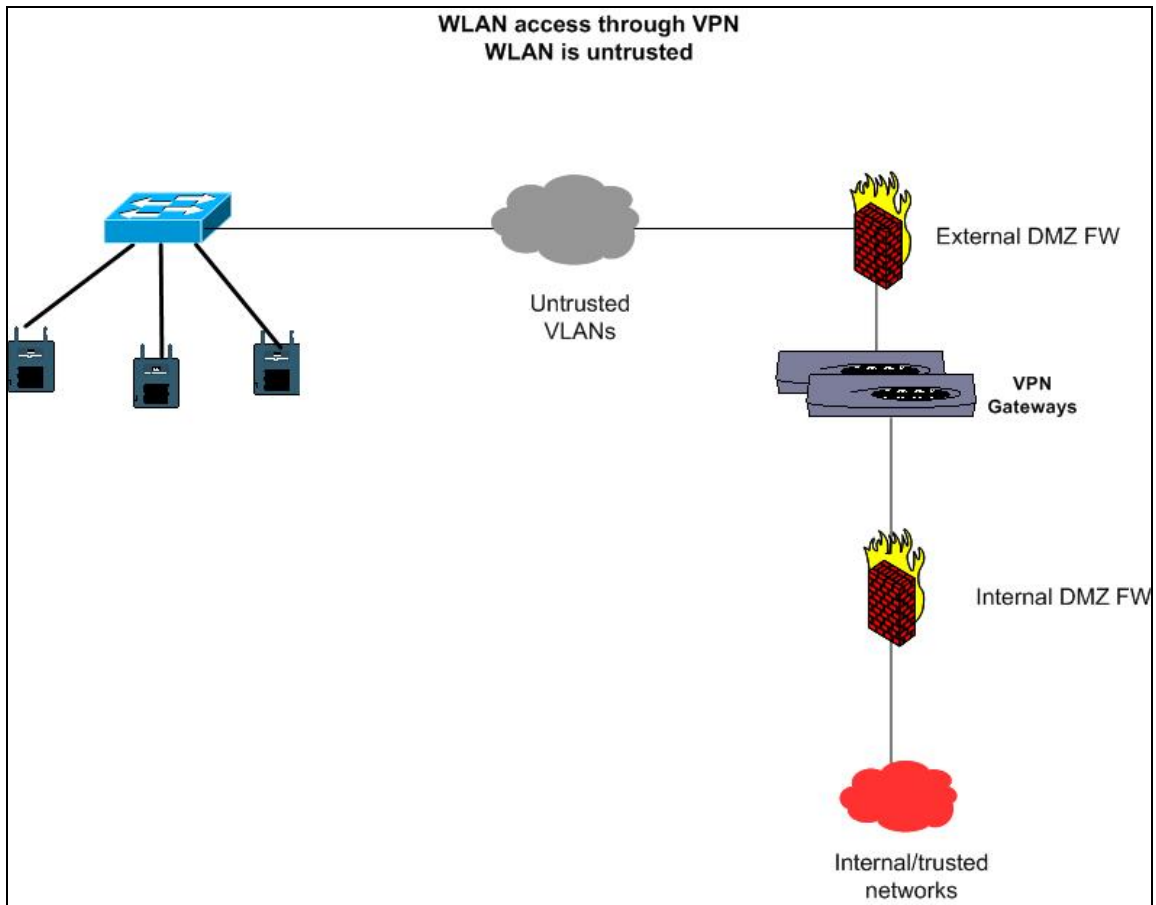


Figure 3: Existing WLAN architecture

New Converged Architecture

Figure 4 shows the integrated converged network where the WLAN is considered as an extension of the LAN, and the endpoint registers with the WLAN controller to provide services. As WLAN access technology changes from 802.11a/b/g to 802.11n, the same architecture can be used to support the new access technology providing enhanced throughput. VoIP becomes the primary voice technology within the building, and it connects to the legacy PBX to provide backward connectivity. However, all VoIP end nodes talk to each other, directly connected by the VoIP server.

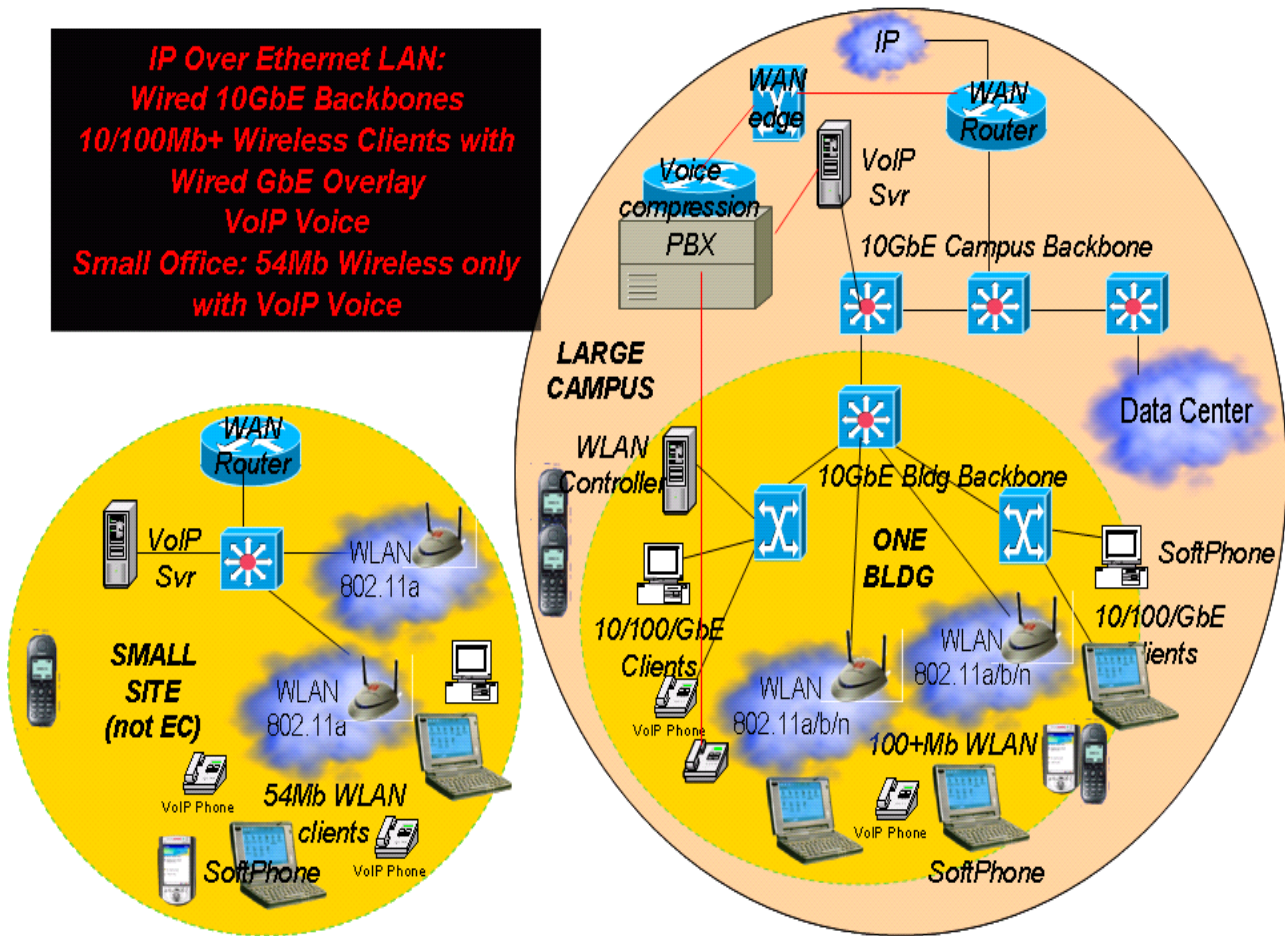


Figure 4: Converged network architecture

FOLSOM LAN AND VOICE CONVERGED NETWORK

Intel is working to build a first converged network at one of its campuses. In this network all 300 users will have only one network connection to their VoIP hardphone and their personal computer will be connected to the VoIP phone. Hardphones will receive power via PoE, and QoS will be used to put the voice traffic on a strict priority queue. All the WLAN APs will be connected to the same LAN switch to eliminate the separate physical infrastructure. Figure 5 shows the high-level topology of the converged network. Before, this site would have had two parallel networks, one for voice and one for data. With this topology, users will only have one connection for all services.

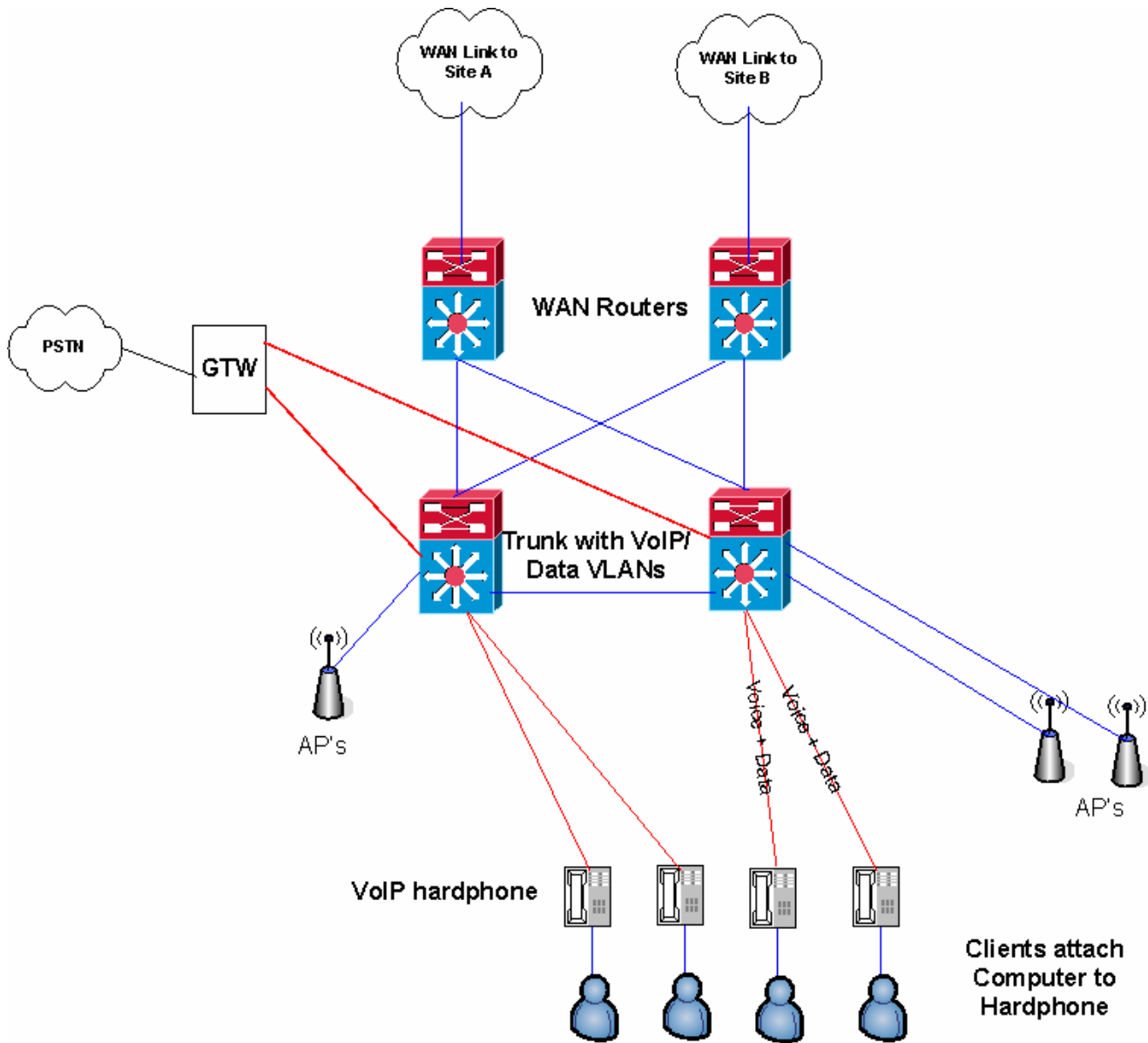


Figure 5: Trial converged network

CHALLENGES

As enterprises strive to converge voice, video, and data over LANs and WLANs, they will face multiple challenges. Some of those challenges are technical, and a significant number of them are business related.

Technical Challenges

The main technical challenges involved in building converged networks are as follows:

1. *New voice backend*—Moving voice from a circuit-based network to a packet-based network involves a radical change in the voice backend. While traditional PBX manufacturers support such a change, a lot of companies can take the opportunity to start fresh with a native VoIP solution. The move should affect user services as little as possible.
2. *Quality-of-Service*—Introducing different services with different network characteristics into the same network requires the ability to prioritize more time-

critical network users such as VoIP over less time-dependent services such as data. Introduction of QoS involves a significant technical challenge and may require a network equipment update and refresh.

3. *Security*—As different networks merge into a single infrastructure, the separation offered by different transports and cabling is lost. In traditional voice networks the only way to access other users' traffic is to physically gain access to their phone cabling or break into distribution frames or PBXs, which are normally locked up. With shared networks, if the network is not protected properly, unauthorized access to other users' data (and therefore VoIP) may ensue without physical attachment with methods such as ARP poisoning.
4. *Training*—Support staff are used to working with the legacy equipment and will have to be trained on the new equipment. Since this is a paradigm shift for most support staff, the required training is extensive. Most organizations have separate support personnel for data and voice; with the integration of voice and video on one data network, support should also merge for better end-to-end service quality.
5. *Troubleshooting*—The resulting converged network is more complex than its component parts. Putting more eggs in the same basket always makes it more difficult to find out the root cause of problems. To make the converged network successful, the right management and troubleshooting tools have to be created for the support staff.

Business Challenges

Besides the above, there are multiple business-oriented challenges that should be addressed before converging networks:

1. *Making the business case (Return on Investment, ROI)*—Probably the single biggest challenge for anyone wanting to make the leap is making the case for this move. In today's business environment changes of this magnitude are unlikely to be approved without a hard dollar calculation showing real savings.
2. *End user expectation reset*—Today, end users are accustomed to very high availability of their voice network and in converged networks that expectation should be level set.

RESULTS

Convergence of services in a common network is inevitable. In order to support high-quality service to the customer, the LAN needs to be redesigned to meet delay,

jitter, and loose characteristics. We have developed a design that can meet voice, video, and data needs in LAN and at the same allow the WLAN to be merged with the wired LAN. We equipped a few small offices with this design and are working to implement it in a 300-user office. We have been successful in replacing end-of-life products with new VoIP and are therefore positioned for worldwide VoIP down the road.

DISCUSSION

Converged networks offer great promise for converged communications by integrating voice, video, and data on LAN and mobile networks. As such, converged networks show great promise for the enterprise. However, the challenges are considerable in the areas of business, finance, and technology.

Should enterprises today take the plunge? We believe there is no simple answer to this question and the important thing to remember is that "one size does not fit all" anymore. In deciding whether converged networks are right for an enterprise, we offer the following advice:

- *Core vs. edge*—Core services are normally centralized and controlled more closely than the edge; therefore, starting the move to convergence at the core is sometimes easier. Moreover, a lot of the immediate financial benefits are more easily seen on the core, since long-distance networks are a major part of the network discretionary spending, and convergence at the core can reduce spending considerably. On the other hand, the core is one of the most sensitive and mission-critical environments, if not *the* most.
- *New/Greenfield vs. legacy sites*—When going into new construction an enterprise has to think ahead at least three years. We believe by this time converged networks are going to be the rule rather than the exception. Therefore, we would recommend considering using converged networks at new sites and campuses. Making the case for retrofitting existing infrastructures is much harder.
- *Risk taking*—Making major changes to an existing environment is risky. In making the decision one has to weigh the risk vs. the gain. Starting convergence in a mission-critical manufacturing plant, design center, or customer support center is quite different from making that move in a standard office environment. Start small and expand as you gain experience and confidence.
- *Standard based vs. proprietary*—Using standards offer a much better chance of interoperability, but some of the standards may still be in the certification track. Using existing proven proprietary protocols may be

required as an interim step. The timetable for implementation will determine this choice ultimately.

- *Network management*—Being successful in converged networks requires new capabilities for managing the converged networks including QoS management, security management, and real-time troubleshooting tools. Having this kind of management is crucial to success in this complex task.
- *Staff and technical expertise*—Moving to converged networks requires a lot of talent and knowledge, radically different talent and knowledge gained from working with legacy networks. Making the change requires paying close attention to skill levels and training for both design and operations personnel.

CONCLUSION

The communication industry has now widely accepted IP as the universal transport protocol for the enterprise. In the last decade all other transport protocols have converged to IP. Now there is rapid adoption and migration by telephone, cable, and media vendors and industry to move to IP to take advantage of converged networks. This has had a snowball affect within the enterprise: vendors are forcing coming enterprises to go to IP transport for all services. Therefore, the enterprise should start planning to make the appropriate changes to their network to position themselves for new IP services. We have started rolling out converged networks for our small offices and are aggressively working to roll out our first big-size office with a converged service network.

ACKNOWLEDGMENTS

We thank Justin Richardson for piloting the converged network architecture and providing input. We also thank our VoIP LAN working group members: Neil Wallace, Tim Verrall, Shelby Siegel, Dave Lizotte, Charles Weaver, John Gresham, Blaine Bauer, Bob Wasserman, Kevin Heine, and Dave Brooks. We also appreciate the contribution of the ITJ editorial staff.

REFERENCES

- [1] "Internetwork Design Guide," Cisco Systems, <http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/>*
- [2] "Open System Interconnection Reference Model," Cisco Systems, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/intoint.htm*

- [3] "Port Based network Access Control," <http://standards.ieee.org/getieee802/download/802.1X-2001.pdf>*
- [4] "RADIUS Protocol Security and Best Practices," Microsoft Corporation, <http://www.microsoft.com/windows2000/techinfo/administration/radius.asp>*
- [5] "IEEE 802.1p: LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization," <http://www.javvin.com/protocol8021P.html>*
- [6] "IEEE 802.11e-2005 wireless network QoS specification," <http://standards.ieee.org/reading/ieee/std/lanman/restricted/802.11e-2005.pdf>*

AUTHORS' BIOGRAPHIES

Sanjay Rungta is a principal engineer with Intel's Information Services and Technology group. He received his B.S.E.E. degree from Western New England College and his M.S. degree from Purdue University in 1991 and 1993, respectively. He is the lead architect and designer for the Local Area Network for Intel. He has over 13 years of network engineering experience with three years of experience in Internet Web hosting. He holds one United States patent and two pending in the area of Network Engineering. His e-mail is sanjay.rungta at intel.com.

Omer Ben-Shalom is a lead engineer for Intel's IT Wireless LAN team. He received his B.Sc. degree in Physics and Computer Science from the Hebrew University in Jerusalem in 1996, and his M.Sc. degree in Computer Science from Tel-Aviv University in 2002. He is a lead engineer in the Information Services and Technology Mobility Services group. His e-mail is omer.ben-shalom at intel.com.

Copyright © Intel Corporation 2006. All rights reserved. This publication was downloaded from <http://developer.intel.com/>.

Legal notices at <http://www.intel.com/sites/corporate/tradmarx.htm>.

THIS PAGE INTENTIONALLY LEFT BLANK

For further information visit:

developer.intel.com/technology/itj/index.htm