RC24614 (W0808-005) August 4, 2008
Computer Science

IBM Research Report

Enterprise Architecture for IP Based Voice Systems

William J. Rippon
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

Research Division
Almaden - Austin - Beijing - Cambridge - Haifa - India - T. J. Watson - Tokyo - Zurich

Enterprise Architecture for IP Based Voice Systems

December 9, 2007

William J. Rippon
Department: Research I/S Networking
Organization: IBM Research I/S
Location: Yorktown Heights, NY 10598
E-Mail: bjripp@us.ibm.com

William J. Rippon
Senior Network Engineer
Certified Information Systems Security Professional
CISSP #72768
http://www.isc2.org

***Abstract* — In this paper, we will provide an analysis of enterprise architecture for IP based voice systems. The focus within the enterprise for the past several years has predominantly centered on the requirements for individual services, as opposed to a holistic, cross services approach. Individual service implementations can create islands of IP voice service which are often difficult to integrate with other IP voice services. Enterprises should view the IP voice environment the same way that data application environments are viewed. Enterprise IP voice environments should be built using common building blocks of network and voice infrastructure which can support of variety of voice applications, services and endpoints. This paper will explore the next generation of enterprise architecture for IP based voice system.**

Keywords; IP Voice, VoIP, IP Telephony, SIP, Enterprise, Architecture, Infrastructure

I. INTRODUCTION

Traditional or legacy voice services are rapidly giving way to IP based solutions. Over the last several years there has been an increase in the number of enterprises deploying or migrating to IP based voice services such as; IP Telephony (i.e. IP-PBX), Voice over IP (VoIP) Toll-bypass, audio conferencing, unified messaging and voice enabled applications such as instant messaging, e-mail and the web. In many cases the implementation of these services has been done through point projects that are focused on only one service or perhaps even one instance of a particular service. A variety of reasons may contribute to this approach, such as organizational priorities and funding models. In other words, the architecture and deployments are not done in a holistic, enterprise wide fashion.

As these individual IP based voice services are deployed they create service "islands" which will eventually need to be bridged together over the converged IP network. There are many disadvantages to deploying services on an individual basis, instead of as part of a coordinated enterprise wide offering. These multiple individual implementations will end up duplicating effort and support resources, complicating integration with other services and increasing the enterprises overall cost and complexity. Each instance will need to determine on its own how to peer with all of the other internal and external environments. Since, the integration with other services is not a key requirement of the individual service, significant problems can arise when the time for integration arrives. Management, operation and security of these individual environments will also be more complex and more costly. In fact, the overall security and availability of the environment may be lessened as a result of this approach. The user experience related to the IP voice environment may differ widely between services and different credentials will usually be required for each service. Furthermore, the introduction of new services will be more problematic from the perspective of cost, complexity and delay. The more individual services are deployed in this fashion, the more difficult it will be to migrate to an enterprise wide model in the future.

In this paper we will explore a new generation of architecture for enterprise wide IP voice services. We will begin with a description of the architectural approaches used, followed by a foundation of a common set of enterprise standards, protocols and policies. These standards will apply to a common infrastructure environment and to the extent appropriate, to the individual application and services as well. From this foundation we can design a core infrastructure and a set of common support services that can be leveraged by the various IP based voice applications and services. The end result will be an environment that will provide advantages in many key areas such as; duplication, cost, integration, security, management and operation, flexibility and the user experience.

There is an abundance of documentation available, from a variety of sources, on the subject of IP based voice architecture. Several examples are included in the *References* section of the paper [1]–[6].

II. BACKGROUND

A. IP Based Voice Systems

In general IP based voice systems refers to any application or service that utilizes an IP (Internet Protocol) transport for signaling and media. Here are a few examples of typical IP based voice services and terms.

Voice over IP (VoIP) – Voice over IP is transport focused. It is the digitization and packetization of voice combined with the transport of those packets over a TCP/IP network.

IP Telephony (IPT) - IPT encompasses the use of TCP/IP telephones which are attached to the data network by wired or wireless connections. This includes the network based voice infrastructure and services required to support IP telephones, such as call control servers and voice gateways.

IP Voice Applications and Services – This set of applications and services is geared specifically to the voice

environment. Audio conferencing and unified messaging are two common examples of this type of service.

IP Voice Enabled Applications – This refers to adding IP voice communications to applications that are primarily data based apps. A variety of common applications, are already enabled for IP voice communications. Examples include; Office Applications (spreadsheets, document editors, presentations), E-mail, IM and the Web.

B. Converged Communications Networks

A converged solution leverages a common network infrastructure for multiple services. Typically this refers to the information systems triad of voice, video and data all running on a common network infrastructure. The desire for converged networks is motivated by the desire for advanced applications and services as well as the demand for continuous cost reductions.

C. Architecture

As one would expect, the architecture of IP based voice services differs from that of traditional telephony. In some cases the differences can be substantial. One of the more significant differences is the amount of centralization, of voice services, that can be achieved with IP based voice solutions. While this can be a major advantage for implementation, management and operation, it creates an even greater dependency on the distributed data network. For example, instead of a traditional central office (CO) switch or private branch exchange (PBX) supporting hundreds or thousands of phones, a centralized IP solution could support "hundreds of thousands" or even millions of phone endpoints.

D. Dependency on Other Parts of the Ecosystem

The reliability and security of IP based voice is heavily dependent on the reliability and security of the related components of the ecosystem such as; people, physical controls, environmental controls, device platforms, networks, servers, etc [7]. This paper does not provide an analysis of all related areas. This observation is merely included for a more complete understanding of the overall environment.

III. CURRENT SITUATION

Large enterprises often approach new technologies in a segmented fashion with no central, enterprise level guidance or coordination. Management backing and funding for enterprise rollouts of new technologies are often difficult to obtain. This was evident in the early stages of the enterprise IP network, where pockets of IP networks began to appear in different groups or sites within the enterprise. Projects and people became dependent on these "grass-roots" type of deployments. As time progressed there was a need to expand the coverage of these individual networks and also to communicate with other similar networks. Ultimately, the enterprise ended up taking over the operation of the service. It was often necessary to significantly rework existing implementations in order to provide enterprise level integration and services. The introduction and growth of IP based voice within the enterprise is demonstrating many similarities to the introduction and growth of IP networks.

In the early stages individuals or project groups began to experiment with IP based voice. Communication was often limited in scope and often did not include access to the general telephony environment of the enterprise or the public switched telephone network (PSTN).

As enterprises began to see the value in migration to IP based voice solutions they started to develop small, usually single service projects, such as the replacement of a single legacy PBX. At this point the enterprise is not yet ready to back an enterprise wide rollout of an IP based voice infrastructure or even an enterprise rollout of a single service (such as the replacement of all legacy PBX systems). Large, worldwide enterprises may see parallel point projects for the same service running in different regions of the company. These separate implementations may focus on different sets of features and often may involve competing vendor solutions.

Parallel projects related to other types of IP based voice systems now begin to appear. These efforts are usually started from "scratch" and need to obtain management backing and funding on the merits of the individual service, not as part of an overall integrated enterprise environment. It is the natural tendency of these projects to optimize functionality and control costs specific to the individual project rather than to focus on the holistic environment within the enterprise. IP softphone deployment to mobile employees is an example of a point solution that might be deployed in parallel with PBX replacements.

Inevitably as the new technology, in this case IP based voice, proves its value in the early deployments there is a strong motivation to quickly expand existing services and to interconnect individual instances and parallel services. There will also be a growing demand for the introduction of new services.

We have now reached a critical point in the life of the enterprise migration to IP voice. The enterprise is now ready to back a fully integrated set of IP based voice services for the enterprise. However, given the nature of how the existing environment has developed, there are a number of potentially significant problems to address.

- Different solutions with incompatible interfaces and protocols. There also may be no consistent protocol to use for communication between services.
- Inconsistent or overlapping name and number schemes.
- Characteristics of existing voice infrastructure components (location, features, capacity) may be insufficient to support enterprise level services.
- Multiple, perhaps conflicting, data repositories.
- Multiple user and administrative security mechanisms.
- Separate management and support organizations.

- Competing requirements and inconsistent implementations related to the underlying data network infrastructure.

IV. Enterprise Architecture Approach

In order to come up with the new enterprise architecture for IP based voice we draw upon experience in both the existing voice and data environments. While some of the approach is new, many of the methodologies and techniques are common and well understood. The combination and packaging of these methodologies and techniques is what brings us to the next generation of the enterprise architecture for IP voice. The following represents a high level summary of the methodologies and techniques utilized.

The architecture should be heavily based on industry standards to provide open platforms which will enable a high degree of integration and interoperability. The industry standards should be augmented with enterprise documentation that clarifies how the standards should be used in the overall enterprise architecture.

The enterprise should define policies that govern most aspects of the environment. The policies should be specific enough to ensure the appropriate levels of service and integration. However, the policies should also provide the appropriate amount of leeway to permit individual applications and services to meet their objectives. A compliance processes should be in place as well as a governing body that ensures compliance with the enterprise policies. A strongly defined set of policies and compliance processes will ensure that the architectures and implementations will support individual services as well as meet the overall goals of the enterprise.

The architecture will be hierarchical in nature with a logical set of functional building blocks. This will provide a simple, well structured environment that is easy to understand and manage. Separation of function permits selection of components that best match the feature/function requirements.

Centralized services will be exploited wherever possible. This approach applies to the core voice infrastructure services and the requisite common support services, as well as the main components of individual voice services (IP-PBXs, audio conferencing, voice mail, etc.). Based on the reference architecture in this paper (refer below) some examples of core voice infrastructure services include; SIP [8] proxies, media gateways, border elements and Media Infrastructure Services (MIS). MIS refers to a set of services that includes transcoding, audio monitoring and audio repair. Large enterprises may have multiple collections of centralized services to support large geographic regions. However, it is understood that some environments may need some distribution of services to meet specific requirements.

The enterprise voice infrastructure and the underlying data network infrastructure must be highly available and provide the appropriate prioritization, redundancy and resiliency to meet the enterprise goals for the voice services environment. The dependencies on other part of the ecosystem should be taken into consideration (people, device platforms, environmental controls, etc.)

Security and management services should be pervasive throughout the overall enterprise IP voice environment. These services should extend from the core of the architecture all the way to the edge of the managed environment. For security, the internal edge of the enterprise will tend to leverage existing network components for security features. The external edge and the enterprise core of the IP voice environment may utilize more specific security components that are geared toward the protection of the core voice services.

V. Enterprise Standards and Policies

An enterprise should define a set of common standards and policies for the enterprise IP voice environment. These standards and policies will guide the design, development and implementation of the IP voice infrastructure, the individual applications and services and the requisite support services. Individual voice services will need to adhere to the standards and policies in order to properly integrate with the infrastructure services and interoperate with other voice services. While the interconnection point between the voice applications and services and the infrastructure services is the primary focus for adherence to the standards and policies of the enterprise, it is also recommended that the individual applications and services use as many of the enterprise standards and policies as possible, within the confines of the individual application or service.

Many enterprise environments are comprised of solutions from multiple vendors. Therefore, it is recommended that the enterprise leverage standards from industry organizations where possible. Some of these organizations include IEEE, IETF, ITU, 3GPP, and ETSI [9]–[13].

We will define below several examples of standards or policies that might be typical within an enterprise organization. This does not represent all possible standards and policies that may be defined for an enterprise voice environment.

A. Session Protocols

Session protocols are a key part of the communication framework for the enterprise voice environment. These protocols apply to communication within the core voice infrastructure as well as between the core infrastructure and the individual services. The session protocols control the negotiation, establishment, maintenance and termination of connections. We will provide detail on some of the more significant protocols. The selection of a particular protocol does not mean that there are no other protocols of that nature within the environment. It may be necessary to utilize additional protocols of a similar type to provide integration with a specific service or component in the overall architecture.

The Session Initiation Protocol (SIP) is selected as the main session (signaling) protocol due to its widespread support and the fact that it is quickly becoming the “defacto” standard for IP based voice environments.

Closely related to the SIP signaling protocol are the protocols required for real-time media traffic. For negotiating media sessions the Session Description Protocol (SDP) [14] is used. The actual media packets will typically use the Real-

Time Transport Protocol (RTP) [15] or the Secure Real-Time Protocol (SRTP) [16], if encryption is required.

B. Identification and Authentication

The SIP endpoints will typically use Digest Authentication [17]. The authenticator, usually a proxy or B2BUA, will leverage RADIUS [18] to confirm credentials with back-end support services. Other authentication or identification mechanisms that may be used include; simple network access control lists, Transport Layer Security (TLS) [19] and IPSec [20].

C. General Security

There are many facets to security in the enterprise IP voice environment. The following provides a few examples of security related standards and policies.

- Authentication and, or reliable IP network access control are required for any device or service accessing the IP voice infrastructure services.
- Secure protocols are required for user or administrative access to infrastructure components (SSL [19], SSH [21]–[22], etc.).
- Communication between internal enterprise environments and external or quasi-external environments must utilize approved border element components.

D. Management

A common management framework is typically already in place within an enterprise organization. The existing framework will be enhanced to provide functionality that is geared toward the voice environment. The components of the enterprise IP voice infrastructure should contain the necessary feature/function to be managed by the enterprise management framework. This can include items such as; SNMP [23]–[24], syslog [25], SSL and SSH.

E. Standard Conventions for Numbers and Names

Numbering and naming standards related to voice services should be defined for both the internal and external environments of the enterprise. The standards should be enterprise wide and also provide the appropriate hierarchical structure. The standard should be compatible with ither enterprise environments such as the e-mail system. Reserved resources and special prefixes or suffixes should also be defined. These types of standards can also be referred to as dial plans, routing prefixes, directory numbers, extensions, e164, domain, realms, etc. The following list provides some examples for these items:

- Internal phone number – 8 digit number with the first digit representing a worldwide region
- External phone number – Utilize ITU E.164 [26] "As is" from the PSTN
- Internal dialing prefix – 8
- External dialing prefix – 9
- A URI [27] and domain structure that matches the existing data network environment
    - E-mail – blue@sampledomain.com
    - SIP – sip:blue@sampledomain.com

F. List of Supported Features and Functions

A vast array of features and functions exist in the realm of IP and non-IP voice. Since it will not be feasible for the enterprise infrastructure to support every feature and function, it is important to document the ones that are supported. This will provide applications and services with a clear understand of what can be expected from the core infrastructure. The list may be a combination of high level voice features, standards and specific implementation choices. For example, the environment may support the high level feature of "call transfer" but more specifically support the SIP REFER method [28] as the mechanism to accomplish the transfer within the infrastructure.

G. Service Availability

Service availability requirements and expectations should be clearly documented. Service availability requirements will guide design and implementation efforts for the voice infrastructure and provide a level of expectation for the various applications, services and endpoints that will depend upon the infrastructure.

H. Processes for Compliance Verification and Boarding

Part of the overall policy will be a set of processes that will ensure compliance with the enterprise standards and define the rules of engagement for boarding new applications and services onto the enterprise infrastructure.

VI. HIGH LEVEL ARCHITECTURAL VIEW

This section summarizes a view of the high level architectural areas. This is followed up in the subsequent section with a sample reference architecture. Each of the architectural areas is compromised of various components and services.

The converged data network infrastructure is an area that provides an underlying foundation for all the architectural areas and their respective components and services. The data network infrastructure is specifically engineered to support IP voice as an application on the converged network.

The IP voice environment will also need to provide the peering necessary for communication with the public switched telephone network (PSTN) or with other organizations. The implementation of IP voice also opens up new opportunities for peering with providers, partners and the general Internet.

IP voice endpoints, applications or services are the main "clients" of the core IP voice infrastructure (refer below). The core IP voice infrastructure provides support for, and facilitates communication between, the various endpoints, applications and services. Examples of direct IP endpoints include voice

gateways, IP hardphones and IP softphones. Examples of application and services include IP audio conferencing, unified messaging and voice enabled applications such as e-mail, web or Instant Messaging (IM).

The core of the enterprise IP voice infrastructure consists of the main set of services that are required for IP voice. This area is the key focal point of the new enterprise architecture. The majority of services in the core area will be deployed using a hierarchical, centralized model. IP voice endpoints, applications and services will communicate with the core through devices at the edge of the core, such as a border element or an access level component. Some examples of the core services include registration, routing, call admission, translation and media infrastructure services.

There is a set of common support services that will be required by the core IP voice infrastructure. The common support services for the IP Voice infrastructure could also be leveraged by the IP voice endpoints, applications and services deployed within the enterprise. Examples of these services include authentication, authorization, accounting, directories, DNS [29]–[30], DHCP [31], etc.

As with any enterprise environment, security should be an integral part of the architecture, design and implementation. Security mechanisms will be pervasive, touching all of the architectural areas. One aspect of the security area will be security settings that are added to existing components in the enterprise such as access control lists in data network devices. Some security mechanisms will be inherent in the operation of the voice infrastructure such as authentication of endpoints. While still other security services may provide voice or data network infrastructure components that optimized to provide security for the voice environment.

VII. Reference Architecture

This section provides an IP voice, reference architecture, for a large enterprise environment. The size and breadth of some enterprises can even make them appear similar to a carrier environment (a.k.a. "Carrier-prises"). This architecture utilizes SIP as its main communications protocol. A set of logical components and their interconnections are defined. As organizations develop specific architectures for their enterprises it may be desirable to further segment certain logical functions and, or to combine select logical functions. Refer to *Appendix A* for a diagram of the reference architecture.

A. Core IP Voice Infrastructure

1) Internal Access Level Registrar and Call Processing

The internal access level registrar and call processing components are at the edge of the core IP voice infrastructure. They provide services for endpoints, applications and services which are considered "internal" to the enterprise. With the exception of additional security components which may be deployed, these components are the first logical point of entry to the core environment for IP based voice services. In this example these are SIP "proxies" (proxies in this case is meant to include proxies, B2BUAs or soft-switches). These proxies provide registration and authentication functions for endpoints, applications and services (downstream neighbors) and also provide communication paths to the next level of "proxies" (upstream neighbors), the regional/routing components.

A particular instance of an access level component is also expected to be the aggregation point for a common number (i.e. directory numbers) or name space (i.e. domains). For example, a single instance of an access level component might be responsible for the following downstream resources. IP endpoints with the same external PSTN prefix (212-555), the same internal number prefix (8001) and a common domain suffix (*sampledomain.com*).

2) External Access Level Registrar and Call Processing

The external access level registrar and call processing components are also at the edge of the core IP voice infrastructure. However, these access components provide services to applications and services which are contained within external or quasi-external network infrastructures. With the exception of additional security components which may be deployed, these components are the first logical point of entry to the core environment for IP based voice services that enter from external areas. In this example these are SIP "proxies". These proxies provide registration and authentication functions for endpoints, applications and services (downstream neighbors). They also provide communication paths to the next level of the infrastructure, which will typically be a border element (upstream neighbors).

3) Regional Routing Call Processing Services

The regional routing call processing component provides a variety of routing, call admission and translation services for the IP voice environment. These components do not typically provide any direct connection with endpoints, applications or services but rather only communicate with other core IP voice infrastructure components. As with the access level components the regional level components are SIP "proxies" but with a heavier focus on features and functions that are more of a priority at the regional level. These services are provided for; downstream neighbors (access level components and media gateways), peer level neighbors (regional components in other regions) and upstream neighbors such as border elements.

4) Media Gateways

The media gateways provide connectivity between the IP voice network and the circuit switched network environments. On the circuit switch side these gateways will typically connect to the PSTN network. The core media gateway component provides the IP voice environment with centralized access to and from the PSTN. The core media gateways will typically be connected to the regional routing call processing services (upstream neighbor).

5) Media Infrastructure Services

Media Infrastructure Services (MIS) refers to a set of centralized media services which are located in the core cloud of the IP voice infrastructure. The services include, but are not necessarily limited to, media transcoding, media monitoring and media repair. Specific placement of these services will depend on specific calling patterns and their requirements. In some cases the MIS may be placed at the access edge or even in front of endpoints, applications or services. However, in general it is expected that these devices will be connected to

the regional routing call processing services or to border element components.

6) Border Elements

The border element components provide connectivity between two different compartments. These compartments are separated at the network infrastructure layer. The most common reasons for creating different compartments are to separate zones with differing security characteristics or to provide compartments dedicated to a particular service environment. There are many different types of border elements. Some of the most common are Session Border Controllers (SBC), Application Layer Gateways (ALG) and voice aware data firewalls. In this reference architecture example we have chosen the SBC as the main border element. The SBCs are deployed at two main points in the enterprise architecture. The first is on the border between the internal enterprise infrastructure and external or quasi-external infrastructure. In the second, optional deployment scenario, a dedicated voice services compartment is created and the SBC becomes the first contact point for any and all endpoints, applications or services which need IP voice infrastructure services.

B. Security Components and Sevices

1) Voice specific network compartments

Utilize separate logical network compartments when possible to provide logical separation of voice specific environments from the general data network environments. This will provide a focal point for voice specific security and will simplify the deployment of security mechanisms. This can be accomplished through dedicated subnets and virtual LANs as well as Multiprotocol Label Switching (MPLS) [32], VPNs and other virtual network constructs.

2) Voice specific security services (existing components)

Given that the IP based voice services will be deployed within a converged network environment, there are existing infrastructure components and services that can be enhanced to provide improved security for the voice services. Existing data network switches, routers and firewalls are some of the most common components used. These devices can provide specific network based access lists, security controls, quality of service and other such mechanisms that will improve security posture of the IP voice services.

3) Voice specific security infrastructure components

These components can detect, throttle or block unwanted traffic that would otherwise adversely affect the voice services. Examples may include malware, protocol anomalies, SPIT and denial of service. The security features may be integrated with a particular voice infrastructure component and, or may be deployed as a dedicated security component. One example of voice specific security, which was discussed previously, is the use of border element technology between network compartments. Another example would be an Intrusion Prevention System (IPS) that is geared toward the protection of voice services.

C. Peering

A number of peering points may be present in the enterprise architecture. A peering point represents connectivity to a different organization, such as a provider, a partner or the general Internet. The peering connection may utilize circuit switched connectivity or native IP based connectivity.

D. Presence Services

Presence services [33]–[34] represent an interesting component of the voice environment that overlaps several of the architectural building blocks. Presence services track and provide information about entities within the environment. An entity might be a person, group, device or service. Typical information includes the status, context and communication preferences of the entity. It can also include configurations that control the nature and detail of information to provide to other entities. Presence services within the architecture can be viewed from many perspectives. It could be viewed as a core infrastructure service, a voice endpoint application/service, a security related component or a common support service.

E. IP Voice Endpoint

The IP voice endpoints can be thought of as the "clients" and "servers" of the voice environment. These components and the services that they provide are the customers or users of the voice infrastructure. Typical endpoints include applications, services (non-infrastructure) and individual devices. Some examples of applications and services include; audio conferencing unified messaging and "click to call". Examples of individual device endpoints include hardphones, softphones and site gateways.

For the purposes of this reference architecture IP-PBX systems would also be considered an IP voice endpoint. The IP-PBX would represent a set of applications and services that it provides to its clients (downstream). The IP-PBX would then connect as an IP voice endpoint to the enterprise voice infrastructure via the access level component or border element (upstream).

F. Common Support Services for IP Voice

To round out the overall environment for the enterprise voice infrastructure there will be a set of common support services that are required at various points within the infrastructure. Here are some typical examples of support services that would be utilized:

- Authentication, Authorization and Accounting (AAA) – RADIUS, TACACS [35], Etc.
- Directories - LDAP [36], Microsoft Active Directory [37], Etc.
- General Network Services - DNS, DHCP, NTP [38], TFTP [39], Etc.
- Management
- Presence (refer above)
- Device Configuration

VIII. A WORD ABOUT IMS AND THE ENTERPRISE

The IP Multimedia Subsystem (IMS) [5]-[7] was created in the 3rd Generation Partnership Project organization (3GPP), with similar efforts appearing in the ETSI, MSF [40] and PacketCable [41] organizations. These architectures, standards and recommendations are meant to address the need for standard service provider environments that can deliver a range of fixed or mobile multimedia applications and services. While these efforts are not specifically targeted at the enterprise environment, portions of these standards may apply to the enterprise. In particular, the large enterprise, or "carrier-prise", with its own set of fixed/mobile multimedia applications and services, may end up with environments that are very similar to provider deployments. However, given the nature of enterprise environments, some of which is discussed above, it is more likely that the enterprise will take an evolutionary, rather than revolutionary path toward an "IMS-like" environment.

REFERENCES

[1] Various, "Cisco Unified Communications Manager (CallManager) Design Guides", Cisco Systems 2007 - http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html)

[2] Anonymous, "Common VoiP Architecure", AT&T 2003 - http://www.corp.att.com/emea/docs/pb/voip_architecture.pdf

[3] Anonymous, "Nortel Guide for Planning and Deploying Converged VoIP Networks to Enterprises", Nortel 2005 - http://www142.nortelnetworks.com/bvdoc/bestpractice/Nortel_Guide_for_Planning_and_Deploying_Converged_VoIP_Networks_to_Enterprises_1.2.pdf

[4] 3GPP, "TS 23.228: IP Multimedia Subsystem (IMS) (Stage 2) - Release 5", September 2002, <ftp://ftp.3gpp.org/Specs/archive/23_series/23.228/>.

[5] 3GPP, "TS 24.228: Signaling flows for the IP Multimedia call control based on SIP and SDP", September 2002, <ftp://ftp.3gpp.org/Specs/archive/24_series/24.228/>.

[6] 3GPP, "TS 24.229: IP Multimedia Subsystem (IMS) (Stage 3) - Release 5", September 2002, <ftp://ftp.3gpp.org/Specs/archive/24_series/24.229/>.

[7] W. Rippon, "Threat Assessment of IP Based Voice Systems", 1st IEEE Workshop on VoIP Management and Security - VoIP MaSe, 2006 - http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=34342

[8] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, N. Handley, and E. Schooler, "SIP: Session initiation protocol", Internet Engineering Task Force, RFC 3261, 2002.

[9] Institute of Electrical and Electronics Engineers (IEEE) – http://www.ieee.org

[10] Internet Engineering Task Force (IETF) – http://www.ietf.org

[11] International Telecommunications Union (ITU) – http://www.itu.int

[12] 3rd Generation Partnership Project (3GPP) – http://www.3gpp.org

[13] European Telecommunications Standards Institute (ETSI) – http://www.etsi.org

[14] M. Handley, V. Jacobson, and C. Perkins, "Session Description Protocol", IETF, RFC 4566, 2006.

[15] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", Internet Engineering Task Force, RFC 3550, 2003.

[16] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K. Norrman, "The Secure Real-Time Transport Protocol (SRTP)", IETF, RFC 3711, 2004.

[17] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", IETF, RFC 2617, 1999.

[18] C. Rigney, S. Willens, A. Rubens and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", IETF, RFC 2865, 2000.

[19] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", IETF, RFC 4346, 2006.

[20] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", IETF, RFC 2401, 1998.

[21] T. Ylonen and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", IETF, RFC 4251, 2006

[22] T. Ylonen and C. Lonvick, "The Secure Shell (SSH) Authentication Protocol", IETF, RFC 4252, 2006

[23] J. Case, M. Fedor, M. Schoffstall and J. Davin, "A Simple Network Management Protocol (SNMP)", IETF, RFC 1157, 1990.

[24] D. Harrington, R. Presuhn and B. Wijnen, "An architecture for describing SNMP management frameworks", IETF, RFC 2261, January 1998

[25] C. Lonvick, "The BSD Syslog Protocol", IETF, RFC 3164, 2001.

[26] Anonymous, "Series E: Overall Network Operation, Telephone Service, Service Operation and Human Factors, International operation – Numbering plan of the international telephone service", ITU-T E.164, 2005.

[27] T. Berners-Lee, R. Fielding and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", IETF, RFC 2396, 1998.

[28] R. Sparks, "The Session Initiation Protocol (SIP) Refer Method", IETF, RFC 3515, 2003.

[29] P. Mockapetris, "Domain names – concepts and facilities", IETF, STD 13, RFC 1034, 1987

[30] P. Mockapetris, "Domain names – implementation and specification", IETF, STD 13, RFC 1035, 1987

[31] R. Droms, "Dynamic host configuration protocol", IETF, RFC 2131, 1997

[32] E. Rosen, A. Viswanathan and R. Callon, "Multiprotocol Label Switching Architecture", IETF, RFC 3031, 2001

[33] M. Day, J. Rosenburg and H. Sugano, "A Model for Presence and Instant Messaging", IETF, RFC 2778, 2000

[34] Sung Bo Yang, Sung Gon Choi, Se Yun Ban, Yoo-Jung Kim and Jun Kyun Choi, "Presence Service Middleware Architecture for NGN", Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, Volume 2

[35] C. Finseth, "An Access Control Protocol, Sometimes Called TACACS", IETF, RFC 1492, 1993

[36] W. Yeong, T. Howes and S. Kille, "Lightweight Directory Access Protocol", IETF, RFC 1777, 1995
[37] Microsoft Active Directory – http://www.microsoft.com
[38] D. Mills, "Network time protocol (version 3) specifications, implementation and analysis", IETF, RFC 1305, 1992
[39] K. Sollins, "The TFTP Protocol (Revision 2)", IETF, RFC 1350, 1992.
[40] MultiService Forum (MSF) – http://www.msforum.org
[41] CableLabs PacketCable Initiative – http://www.packetcable.com

APPENDIX A.

Conceptual Architecture Diagram