Technical and management considerations for implementation of VoIP in a Dual-Stack (IPv4/IPv6) compatible environment

Malobe Lottin C.M [1], Austin Amaechi[2], the ICT University, Cameroon, 2020

[1]School of Information and Communication Technology,
Information and Systems Networking (ISN),
ICT University, ICT-U foundation USA, Messasi,526 Yaounde.
PhD Student.— Researcher at ICT Byrd Research Center.
Email: malobecyrille.marcel@ictuniversity.org

[2] School of Information and Communication Technology,
Information and Systems Networking (ISN),
ICT University. PhD.
Author, Writer, Computer technologist and entrepreneur
Email: Austin.amech@ictuniversity.org

Abstract

Voice Over Internet Protocol (VoIP) is a digitalize technology that permits the transfer of analog voice signals converted into data packets in an Internet Protocol (IP) data network. It is a solution that helps in providing telephony and multimedia services that goes beyond the functionalities offered by the traditional Public Switched Telephone Network (PSTN). The Internet Protocol Version 4 (IPv4) has been the main communication protocol through which this technology has been deployed. Today, with the evolvement of Broadband technologies and the tendency to make all communication devices oriented IP, coupled with the problems raised by the limitation of IPv4 to address new requirements in term of availability of IP addresses, security and Quality Of Service (QoS) management, IP next-generation (IPng) also called IPv6 is the new version that definitely addresses these problems in the most effective way. However, the transition from the older to the newer version needs to be done with special considerations. Transition technics such as dual-stack are developed to handle this immediate need. This paper presents a proposal of technical and management parameters that organizations can consider to ensure successful implementation of VoIP telephony service in their network architecture where IPv4 and IPv6 are used as main communication protocols. These considerations concern particularly the physical, logical and security area of the network hierarchy segmented into Access, Distribution, Core and Application levels.

Keywords: IP Telephony, IPv4, IPv6, Dual-stack

1. Introduction and Background

Every organization makes use of communication tools and technologies that provides them with the means to be easily reachable both internally (within the corporate organization) and externally (towards various partners and customers). Most businesses today have come to the consciousness that, to face competition, there is a need to invest in business communication tools that are adapted to their specific environment and that will contribute to ameliorating the way things are done. Motivate the workers by putting in their disposals flexible information technology solutions like VoIP that will minimize stress in the working environment and offer a user-friendly support environment through communication software and applications. Such flexibility cannot be achieved if existing networks are not scalable enough to support the integration of disparate applications for them to work seamlessly. It means considering to reconcile physical and logical connections, perform various reconfigurations that will support the integration of new services and define new policies in term of security and traffic flow management to ensure that the new solution respect the norms of Confidentiality, Availability and Integrity (CIA). It is all about offering to the end-users tools and solutions that optimize their daily productivity. And this cannot be achieved without proper consideration of technical and management procedures.

IP data networks are purposely characterized by their ability to accept the implementation of new services and applications. It is imperative to understand how to properly implement services and protocols, especially if the network has been in existence for some time and some services are no longer needed or have been forgotten[1].

The main communication protocol used to implement these services and applications is the Internet protocol. Connectionless (does not require the establishment of a connection between end parties before the exchange of information takes place) by design, and used in packet-switched networks, this protocol operates in a best-effort mode by not providing mechanisms to guarantee successful delivery of packets, or proper sequencing of packets flows to avoid a situation such as duplicate delivery or error delivery.

The most widely deployed version of this protocol is version 4 (IPv4). It is used in both internal (Private) and external (public) network to route the majority of data generated within the intra-network domain or the inter-network domain. Internet is the most tangible network example, were various services and applications are implemented with IPv4 providing a platform for successful communication and exchange of information between network interconnected around the world for more than 30 decades. IPv4 need to relate with other protocols belonging to the TCP/IP model such as TCP to guaranty integrity of data exchange. Other extended protocols such as the Internet Protocol Security (IPsec) are also used as complementary to IP in the network layer of the Open System Interconnect (OSI) model to offer more security in transmission processes, especially between servers and clients.

However, despite the undeniable role that IPv4 played with various complementary protocols for more efficiency and reliability in data communication, this protocol could no more support the growth of the number of Internet users, satisfy the requirements of services and applications designed for next-generation networks (NGN), the evolvement taking place in digital technology where all devices are IP oriented with the constraint to publicly address these devices for internet access [10]. In consideration of the various challenges ahead of IPv4, the new version, the Internet Protocol Version 6 (IPv6) was developed to provide more functionality and solve the main issue of address space limitation. Also called IP Next-Generation (IPng), IPv6 introduces fundamental features that optimize traffic flow and guarantee a better Quality Of Service [7]. Existing network design over IPv4 can migrate towards this new version of IP by implementing a transition mechanism. IPv4 and IPv6 are not compatible. It means designed program, applications or systems on IPv4 cannot communicate with those on IPv6 and vice-versa. It is therefore fundamental to identify according to network and management goals, the most suitable transition technic that will permit ongoing service to keep running while being open to the integration of new ones.

This article aimed at proposing a certain number of parameters that must be considered during the implementation of a new service in a network environment where IPv4 and IPv6 are configured (dual-stack). It uses VoIP as a practical service that provides IP telephony connectivity to terminals configured either on IPv4, IPv6 or Both. The consideration and respect of these parameters during the implementation of VoIP in a Dual-Stack environment shows how to minimize the risk of poor configuration, excess latency and service interruption or unavailability.

2. Related Literature

VoIP can be implemented in a data network that relies either on IPv4-Only, or IPv6-Only or both. Reference [2] presents a case study of the implementation of a VoIP system in an IPv4-Only compatible network. The solution was as a replacement of an outdated telephone PBX (Private Branch Exchange) platform that was causing the organization to experience miss and delays calls, leading to a considerable number of complaints from customers and causing a serious loss of revenue. The authors made use of the systematic approach of technology retooling to implement a VoIP solution in their existing IPv4 data network. The five steps process-oriented approach used to implement this solution and address this specific problem of ineffectiveness, inefficiency and dysfunction comprises a step to understand the technical problem (open evaluation of the existing environment comprising the software technical support and update, workflow, procedures,

hardware compatibility and availability, identification of limitations for possible review), a step to planning (Brainstorm on possible solutions, determine the optimal option, features and compatibilities, plan for implementation procedures), a step to evaluate alternatives solutions (consider others technologies that may satisfy organization requirements base on technical capacity, features and performance evaluation), a step to implement (implementation of the solution that satisfies most requirements), and, finally, the evaluation step (to see if the problem has been effectively solved). The successful implementation of this solution by the authors was justified by the applications of considerations defined in these five steps process-oriented approach.

The non-compatibility of IPv4 with IPv6 requires that any project of service integration in dual-stack architecture must consider applying a transition mechanism. That is, the deployment of VoIP on IPv6 compatible environment need that a migration process should initially be done. And this migration from IPv4 to IPv6 can only be effective when the various challenges related to such task are successfully overcome. The author of [3] in his article categorizes these roadblocks into four mains issues: interoperability with Software and Hardware, Technology Education, Planning, and Business Return on Investment. It means consideration in implementing an IP telephony solution like VoIP in a network where both IPv4 and IPv6 stacks are used require special consideration in addressing interoperability issues, leftover legacy equipment, management of people that may be resilient to change, management of the uncertainty of the Business Return on Investment once the solution is implemented.

It is also possible to just focus on adding features that add IPv6 capability to existing VoIP features. Here, VoIP will operate both on IPv4 and IPv6. [4] thinks that for such design, it is about considering to add dual-stack support on Voice gateways and Media Termination Points (MTPs), IPv6 support for Session Initiation Protocol (SIP) trunks, and support for Skinny Client Control Protocol (SCCP) with the configuration of a Session Border Controller (SBC) that connect SIP-IPv4 or H.323 IPv4 network to a SIP IPv6 network, to facilitate migration from VoIP4 to VoIP6.

The main consideration for such approach according to [4] is the proper mastering of IPv6 addressing and connectivity procedures, and the proper implementation of Voice configurations in all network entities that participate in VoIP service delivery.

The successful implementation of a VoIP telephony system in a Dual-Stack network depends on two generals and initials conditions:

- the mastering of VoIP technology with network requirements necessary for the delivery of a good Quality Of Service (QoS) and,
- the understanding of how Dual-Stack network architecture is deployed in relation to network transition specifications (IPv4-to-IPv6), network entities (sum of network elements contributing in the Dual-Stack design) and the organization Goal (the type of service to provide according to market demands and infrastructure capability).

These two conditions are fundamental for proper appreciation of the technical and management considerations network designers (Engineering Team) in collaboration with the organization management body, needs for successful implementation of such a solution.

3. VoIP: functions and Network requirements for good service delivery

IP telephony, also called VoIP, Internet Telephony or Broadband phone, is an alternative of the PSTN. In this technology, Analog voice generated during phone calls are converted into digital signals [5] (with the use of Coders-Decoders-CODECs), then forwarded as data packet over a packet-switched network. The main communication protocol responsible in the exchange process of Voice packets is the Internet Protocol (IP). It is an effective communication system compares to the traditional phone systems in term of cost of implementation (Infrastructure require is cheaper than the one of PSTN), cost of operation (calls can be free or are cheaper both locally and remotely depending on the solution put in place), maintenance (service maintenance is dependent of IP data network and equipment performance, not like PSTN where maintenance is associated with human and heavy financial constraints especially at the access level), service and access management (service is a function of the quality of the data, and user

can access service from multiple devices and not dependent on a regular terminal as it the case with Plain Old Telephone Service (POTS) sets).

If organizations have to adopt VoIP as a viable solution in an Only-IPv4 or Dual-Stack network, its components must be able to perform the same functions as the PSTN network and more. Also, the Quality Of Service obtained should not be less than the one on PSTN. It means considering to provide a reliable Signaling system, a database for call registration and translation services (from one type of address to another), a bearer control for connection/ disconnection of calls and, CODECs for the conversion of voice to digital format (vice-versa). Application of these 4 considerations generalizes the essential phase in implementing VoIP service.

3.1 General consideration 1: Focus on defining the suitable Signaling Protocol

Signalling is the way devices communicate within the network, activating and coordinating the various components needed to complete a call. Signalling traffic constitute one of the three major traffic in a VoIP network, besides the call control and media communication traffic. Just as with the analog PSTN that uses Signaling System 7 (SS7 together with Signal Transfer Point-SCP, Service Switching Point-SSP and Service Control Point-SCP) to provide call connection/disconnection, routing (roaming) and proper billing, VoIP also uses signalling protocols which enable the VoIP network and determine what types of features and functionalities are available, as well as how all the VoIP components interact with one another. In IP data networks, these protocols are: the H.323 and, the Session Initiation Protocol (SIP) for handling the setup and tears down of multimedia sessions between speakers. The effectiveness of this protocol must be associated with a complementary protocol such as: the Real-Time Protocol (RTP) for end-to-end delivery services for data with real-time characteristics (such as interactive audio and video), the Real-Time Transport Protocol (RTCP) to assist RTP in providing feedback on the quality of the data distribution being accomplished by RTP. Also, VoIP needs media control protocols, used by Media gateway for the transportation of media between the IP data network and the PSTN. The Media Gateway Control Protocol (MGCP) or Megago (H.248) provides the switching functionalities between the media gateway, media gateway controller signalling and the gateway functional units.

The wrong implementation of signalling in a VoIP architecture leads to unavailability of service for cases where VoIP terminals need to communicate with external terminals belonging to external networks (PSTN). It is, therefore, capital to consider checking internal and external signalling systems, the VoIP signalling protocol compatibility of the various equipment before their deployment.

3.2 General consideration No 2: Focus on database service registration/translation and bearer control Management for good service delivery

The VoIP Network basically, must provide a call control database to make a way to locate users, register them in a database and translate their addresses in case they belong to different networks. For PSTN, phone numbers are used and translated mean while VoIP will use IP addresses. This will help in generating billing information and providing security functions (Call filtering, etc.).

A network should provide efficient conditions for the call to be able to connect and disconnect on time (with no perceptible delay!). Just as in PSTN where switches connect logical Digital Signal 0 (DS0) channels for completion of a call, VoIP networks need to provide session establishment/disconnection of Real-time multimedia stream proactively.

3.3 General consideration No 3: Focus on providing adequate CODECs with Specifications that satisfy the service to deliver

No matter the quality and the performance of equipment used in providing VoIP in the Network, if the end-user cannot listen to the peer, the overall network is qualified as poor. Technical and Management considerations will be satisfied only if CODECs used are compatible to access devices and network resources. It is the output (codec data stream) of CODECs resulting from the conversion of analog voices into digital information that is packetized and forwarded over the IP data network. Poor conversion, therefore, signifies corrupted packet resulting in poor voice quality, and consequently poor Quality of Service.

3.4 Fundamental Components of a VoIP architecture in a Dual-Stack environment

Figure 1 below shows a proposed architecture of VoIP in a Dual-Stack compatible environment. This architecture summarizes all the fundamental components that comprise a VoIP system with the main particularity that voice packet can be transferred with IPv4 or IPv6, depending on the design to put in place. Four most important components in this architecture contribute to satisfying the three generals considerations discussed in the previous sections (section 3.1, 3.2 and 3.3). These are:

- The (IPv4/IPv6 compatible) **signalling Gateway Controller** also called "called Agent" or Media Gateway Controller: it has multiple roles and performs as the heart of the VoIP platform. Mainly, it connects the PSTN to the IPv4/IPv6 data network with the particularity to support signalling protocols and provide some control mechanism such as bandwidth policing, admission control and media connection provisioning for IPv4 and IPv6 traffic.
- The (IPv4/IPv6 compatible) **Dual-Stack Media Gateways Routers**: this provides IPv4, IPv6 Voice and data packetization and traffic forwarding using RTP/H.323 through Time Division Multiplex (TDM) trunks from one side (PSTN) and IEEE 802.1q trunk at the other side (IPv4/IPv6 network). These gateways also interface with the Internet Router for provisioning of Internet services in the intranet and extending VoIP services to a remote area via the Internet using Ipv4/IPv6 Virtual Private (VPN) Network tunnels.
- The (IPv4/IPv6 compatible) **Dual-Stack Media Servers:** to provide added features such as personalize tone, announcements, video conferencing, voicemail, and voicemail-to-email, to the VoIP dual-Stack platform. Only-IPv4 oriented VoIP network consider this entity as optional, but for Next-generation networks that are Multimedia oriented, a Media server is considered being determinant.
- The (IPv4/IPv6 compatible) **Dual-Stack Application Servers:** this is where the various services are implemented for allocation to end-users. The application server offers supplementary functionality to the Dual-Stack VoIP network so that it can implement functions of the PSTN and more. Some of those functions are for example: basic call services (like call forward always, call forward-busy, call waiting, call transfer, etc.), Call authorization with a PIN, follow-Me options, Call details Records (CDR) and free phone service.

Besides the four main components we just presented on this architecture, there are other components such as the Aggregation Switches that aggregate voice and data traffic from various IPv4/IPv6 core, distribution and access networks elements. These switches are Layer 3 compatible so that they can be able to form dedicated virtual path with keys components of the VoIP System (Media gateway, Media and Application Servers, Access Switches). The access switches are also represented to show how the various VoIP IPv4/IPv6 compatible terminals (IP phones, POTS phones, Softphones, Wi-Fi router gateway and other mobile IPv4/IPv6 compatible gadgets) access the VoIP service in a Dual-Stack network. NGN Softswiches are bringing more intelligence to switching operation of the PSTN (Management dial tone and service activation with the SS7 protocol) while contributing in providing the VoIP network functions such as management of voice, fax, data, video, call routing and connectivity to the IP Multimedia Subsystem (IMS). They are also Dual-Stack compatible and implement SIP/H.323 protocols for IPv6 capability of VoIP processes. Private Branch Exchanges (PBX) connects the traditional POTS phones lines of the PSTN to the VoIP network via the signaling gateway controller and the Soft switch so that analog phones can place call over the IPv4/IPv6 data network through the Dual-Stack Gateway.

The implementation of VoIP in such an architecture require that some specifics considerations should be address both physically and logically so that these network entities should perform as expected.

4. Specific Consideration in the implementation of VoIP in a Dual-Stack environment

During the implementation of VoIP in a Dual-Stack network, specifics considerations need to be focus at four levels: the Network Access Level, the Network Distribution Level, the Network Core level and the Network Service Level [6]. These considerations start by understanding basic operation of a Dual-Stack network then apply it at all levels of the network hierarchy. It means considering deployment factors (metrics) evaluated from technical and management requirement in relation with physical, logical and security parameters [8] that must account during IPv4-IPv6 transition, and, duringthe implementation of a VoIP in that Dual-Stack network.

4.1 Simple view of a Dual –Stack network

Figure 2 above show a simple view of a Dual-stack network with an emphasis on how IPv4 and IPv6 traffic flow is forwarded out from hosts of the

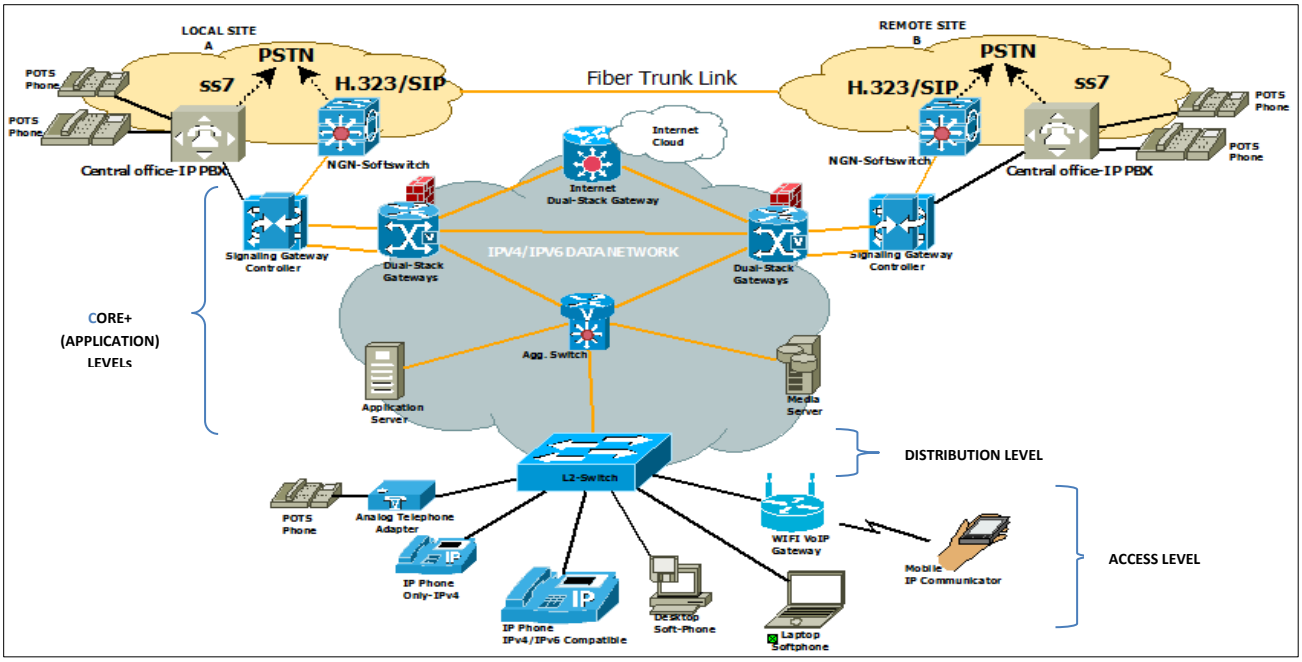

Figure 1: A proposed LAN VoIP architecture- Dual-Stack Oriented

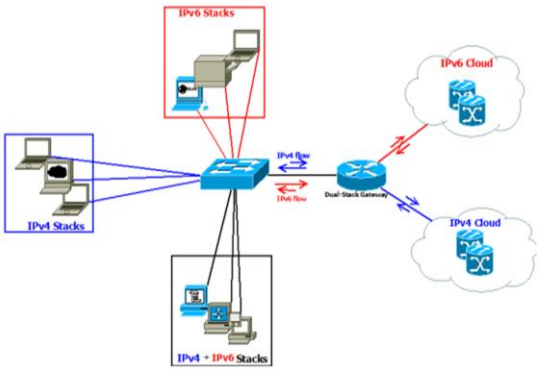

Figure 2: A Basic Dual-Stack Network

Local Area Network (private LAN) to the IPv4/IPv6 public Internet Cloud via default gateway with IPv4 and IPv6 capability. A Dual Stack network is specifically characterized by:

- The existence of Only-IPv4 network entities (IPv4 Stack enable) that process IPv4 traffic only.
- The existence of Only-IPv6 network elements (IPv6 Stack enable): that process IPv4 traffic only.
- The existence of networks element with IPv4 and IPv6 capability (IPv6 and IPv4 Stack enable). Here, node process IPv4 and IPv6 traffic simultaneously. And in this case, the interface is considered Dual-Stacked.
- IPv4 and IPv6 traffic are independent of each other both in term of forwarding and routing.

IPv6 traffic is prioritized by default over IPv4, except if the application, service or device is design to be Only-IPv4.

- The design permits integration of new endpoints, networks services and applications independently of each other.
- Consume more bandwidth from links, more memory and CPU from devices.

From the above characteristics, we can understand that not all equipment or system support IPv6, which justify why a transition or translation mechanism is needed for Only-IPv4 nodes to communicate with Only-IPv6 nodes and, why technical considerations must address each level of the network hierarchy.

4.2 Network Access Level Considerations

The network access level comprises all hardware terminals such as clients/ peer computers, mobile phones, softphones, POTS phones, PBX, Analog Telephone Adapter (ATA), transmission medium and any other access device used to connect to the VOIP network with IPv4 or IPv6. The considerations at this point address access devices according to their type and function and requirements for software, applications and operating systems that are used by these access network elements. It is a very important layer of the network hierarchy because this is where end-users effectively make use of the services and applications provided by the network. The Quality of Service (QoS) and effectiveness in network operation is appreciated here

4.2.1 Physical considerations

Some fundamental technical considerations at the access level, concerning physical elements, focus on addressing issues such as:

- ✓ **The transmission medium**. It needs to provide at least 100 Mbps data Rate peer VoIP link for physical connectivity. Using a Cat5e (e=Enhanced) Ethernet cable for 100MHz bandwidth or Cat6 Ethernet cable for 250 MHz bandwidth is advisable. The bandwidth provided at the access level from this transmission medium must consider that there are two types of flow to handle (IPv4 and IPv6) and each handle service and application independently of each other, using the same transmission medium. The wrong choice of medium with insufficient bandwidth capacity can constitute a major source of delay when cumulated (Propagation delay) and impact on the overall system performance.
- ✓ **Connectors used to terminate Cables:** You need to attach Shielded Ethernet EZ-RJ45 connectors with internal ground properties to the edges of these Ethernet Cables to provide ground connectivity from the equipment RACKS to the Ethernet Network Card Interfaces of the Terminals. These types of connectors are reliable in term of data transmission and flexible for maintenance purpose for sensitive applications such as VoIP.
- ✓ **Network Card Interfaces**: You must ensure that the network Cards interfaces are compatible with the data rate offered by the transmission mediums (100Mbps upwards).
- ✓ **The Type of ATA converters**: should be able to support POTS (FXS, RJ11 ports) phones and Fast / GigaEthernet ports to connect computers, switches or WAN devices by extension of the access network and respond to urgent troubleshooting requirements such as connecting a test terminal to test service availability without necessary going through the network configurations. The ability of these converters to support SIP2.0 and T.38 Fax over IP protocols, with low power consumption is fundamental.
- ✓ **Interference-free environment:** avoid electromagnetic, radiofrequency and electrostatic interference by separating data cables with currents cables or ensuring that radio devices are not interfering with Wi-Fi Data/VoIP Access point. VoIP Performance can be extremely affected by electromagnetic interference (noise) that reduces data transmission speed and affect the Voice and data quality. When power and data cables are enclosed in the same cable concealer or trunking, interference is higher!
- ✓ **Repeaters and Hubs:** should be avoided in the dual-Stack design much as possible because of their inability to separate collision domain and therefore susceptible to impact network performance with broadcast packets causing Broadcast storms and collision, sources of network Congestion.
- ✓ **Stable electrical source**: IP phones should be IEEE 802.3(af or at standard) Power Over Ethernet (PoE) compatible to minimize the risk of Power failure from local electrical sources (power outages from direct lines, Batteries, generators or UPS) and loss of service connectivity. These IP phones should provide at least two Ethernet ports especially for cases where a host will use both the hard phone and the softphone. Power Stability should also be considered for all workstations and access VoIP converters. Remember the intention is to provide service close to or better than the PSTN, that operates even when there is a Power failure at the customer premises.
- ✓ **IPv4-IPv6 Compatible PBX:** Consider to deploy PBX that are IP oriented (IP PBX) with support of IPv4 and IPv6 so that there should be a support of multimedia services (voice, video, data) for both protocols.
- ✓ **Specifications of Workstations:** Computers should have at least 2GB memory (RAM) with CPU processing speed from 1.3 to 3.4 GHz (Dual-Core). This will help in considering that other computer applications and processes may be running and some idling while occupying resources and affecting calls quality from the software phone application during VoIP sessions exchanges.

4.2.2 Logical and security considerations at the access level

At the access level, the logical considerations address the suite of protocols supports, specifications of the Operating Systems and security of Dual-Stack devices accessing the VoIP service. The same security challenges experience with PSTN network such as call diverting, eavesdropping, rerouting also exists with IP telephony. Added to it, they are other security issues related to data transmission in digital communication, best-effort nature of IPv4 and the no-mastery of security around IPv6 deployment in the production environment. Securities considerations, therefore, have to start at the access level that constitutes the first entry point of security vulnerability. Some of the key considerations at this stage are:

- ✓ **Access devices Support of IPv4/IPv4:**

the most capital technical consideration here is that all access devices contributing to data and VoIP communication must be IPv4 and IPv6 compatible to satisfy design goal and scaling purpose. And securing these devices should be done in respect of the protocol capability (IPv4/IPv6) activated on each access device

✓ **Only authorized users access VoIP elements:** Access devices should only be allowed to authorize users. It means ensuring that those using VoIP terminals should be identified both physically (the user is recognized as the genuine user) and logically (access devices are password-protected and authenticate in the network with a profile to access network services and applications). This help in controlling the risk involve by insiders and unwanted users that can be a source of an attack [9]. However, awareness of processing delay introduced by complex encryption technics used for security policies in a delay-sensitive application is important. Compromising VoIP applications constitutes a bridge to bypass security mechanisms and attack internal networks [9]; protecting access to the first layer of network entities is ensuring acceptable secure environment to the operation of IP telephony in the LANs of a corporate IP data network.

✓ **Access Endpoints Firewall Activation:** activation of firewalls on access endpoints such as computers require to allow VoIP traffic on well-defined ports numbers (TCP, UDP, SCCP, RTP, HTTP, etc.) according to the protocol and the device specification. For example, Cisco uses by default TCP port 2000 for Skinny Call Control and UDP 16376-32767, TCP 1720 for RTP and H.323 protocols [6]. This has the benefice to minimize defect on traffic flow due to so many filtering and policies control mechanism by firewalls. It also contributes to ease maintenance especially monitoring task of access devices (availability and the traffic flow). However, it is also important to remember that firewalls are one of the major problems in the exchange of signalling (H.323, SIP) messages in IPv4 VoIP networks. The ideal solution is that the firewall should be stateful Oriented for IPv4/IPv6 traffic flows (focus in detecting association between sessions while allowing communication to go through on voice sessions) or behave as an application layer firewall (that are initially stateful with the ability to authenticate the source of packets transferred on TCP/UDP ports). IPv6 addresses most firewalls related issues (NAT is not accepted, end-to-end authentication and encryption that doesn't require any extra Therefore, activating Firewalls on access devices should be done mostly for only-IPv4 computers and strictly following the level of security the network design intends to provide. Security policies for only-IPv6 devices will be managed at the core and application levels where necessary policies are all defined. The ideal solution is to forward VoIP packet over IPv6 in order to benefit from all advantages provided by this version in term of traffic flow management and security compared to IPv4.

✓ **Apply Updated ANTIVIRUS:** Consider to install Updated antivirus (against Viruses, Trojans and worms) and Antimalware (against Polymorphic malware and zero-day exploits malware) to preserve the operating system files and resources from been corrupt. A viral infection can have a severe impact on the system processing speed, affecting the ability of the operating system software and applications like softphones to effectively place VoIP calls.

Figure 3 below proposes a flow chart that modelled from a practical perspective, the most important Technical Considerations at the access level of the Local Area Network for proper implementation of VoIP in a Dual-Stack environment. The entry point is conditioned by that network goals are clearly identified and that they specifically match the organization business requirements. The flow chart gives in sequential order, the possible outputs that express actions that can be taken to correct a lack in a given area of technical demands at this level of the network hierarchy. The exit point of the chart is the effective implementation of VoIP in a network environment where access network terminals and equipment are configured and declare compatible for forwarding of VoIP and Data packets in IPv4 and IPv6, with all required security features. This exit point initiates the technical considerations at the Distribution, Core and Service level and can only be met if all these sequential steps have been satisfied.

4.3 Considerations at the Distribution Level

The distribution level of the network hierarchy is the point that interfaces the access network equipment with the Core network equipment. It is the layer where services and applications generated at the application levels are effectively delivers to workgroup/end-users via access ports and according to the type of service (policy-based- connectivity) and the interface capacity concerning the required bandwidth. Considerations at this level in a Dual-Stack design addresses physical, logical and security parameters just as it was the case with the access level. Some key considerations are:

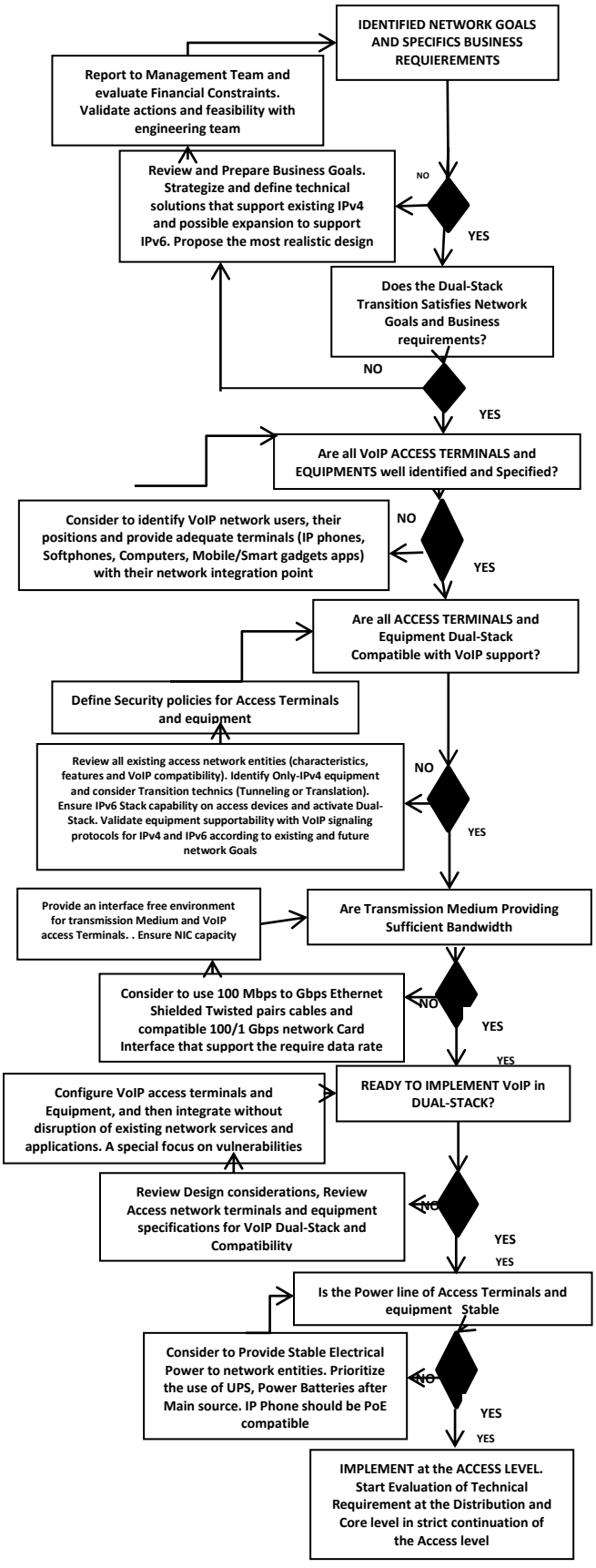

Figure 3: A proposal of a Dual-Stack Implementation flow chart at the Access Level (AL)

✓ **Stable energy supply to all Switches:** The use of Batteries (solar or AC) and Uninterruptible Power Supply (UPS) couple with the main energy source is highly recommended. A power failure on a Distribution device will simply put VoIP service of all access devices that are connected to it down. Energy security is of top priority from this level of the network hierarchy

✓ **Interfaces of Distribution Switches**: physical Layer 2-3 Switches with sufficient interface capacity (100 Mbits/1000 Mbits) Fast Ethernet / Giga Ethernet for proper transfer of Voice, Video and Data traffic over IPv4 and IPv6 and bandwidth compatibility with transmission medium and access devices interfaces. This is very important because if a media provide higher data rate (e.g. 100 Mbps) and the interface is of lower capacity (10 Mbps), the effective transfer takes consideration of the capacity of the interface (max transfer at 10 Mbps). The goal to achieve sufficient bandwidth per user-line is therefore unsatisfied.

✓ **Redundancy of Physical and Logical Links:** providing redundant physicals and logical links that will connect the various distribution equipment (switches, Softswiches) while offering a failover or Backup links to Core (Routers Gateway) devices and critical access network equipment (Signaling Gateway Controller, PBX). This measure contributes to ensuring the reliability of transmission links, availability of Distribution

✓ **Activation of Quality Of Services mechanisms:** Activate QoS functionalities on switches of the Distribution Level and provide L2/L3 QoS mechanisms that differentiate (DiffServ QoS) the type of traffic and allocate resources (bandwidth management and processing-Low Latency Queuing) according to the Class Of Service (CoS) to handle (voice, video or data). Implementation of Traffic Prioritization (to brake priority equality of traffic using best-effort delivery processes and minimize traffic drop because of network condition such as congestion) of IPv4/IPv6 Voice and Multimedia packets over Data is fundamental here! Consider to implement at the layer 2, traffic tagging (802.1q or 802.1p) with appropriate CoS priority value (from 0-low priority-data to 7-higher priority-voice/video). Associate this classification process with Access Control Lists (ACL) that filters based on IPv4/IPv6 traffic, MAC addresses (Non-IP traffic) and users VLANs (mls qos Vlan-based). This way, we ensure that only require Dual-Stack compatible devices access VoIP services with acceptable QoS. Enforce the CoS QoS settings for the trusted packet (Switch ports Configure to Trust IP precedence for incoming voice packets) so that Voice packet should remain prioritized over Data.

✓ **Logical segmentation of users:** use VLANs (Virtual LAN) according to the type of network (IPv4-Only users, IPv6-Only users and IPv4 + IPv6 users) and the type of service to access (Voice + Data, Data only, Voice + Video + Data). Such segmentation

in a complex LAN design architecture such as Dual-Stack with a sensitive service as VoIP (where packet loss, delay or Jitter must be avoided) help in making network management operations easy (Monitoring, Storing by type of users), improve network performance and enhance security configurations according to the type of flow and the device to monitor.

4.4 Considerations at the Core and Application Level

4.4.1 The Core Level

The core level focuses on offering fast transmission and fast processing of information within the intra and internetwork domain. Consideration at this level of the VoIP Dual-Stack network hierarchy also addresses physical, logical and security requirements.

✓ **Enough Memory and Processing Speed capacity:** Physically, all network entities here must have high memory with high processing speed to minimize the delay (processing-packetization, buffering, transmission, Queuing delays) while having enough memory to contain and process routing information of both IPv4 and IPv6 traffic. Aggregation Dual-Stack service Router or VoIP Media Gateway, for example, need about 8-16 GB D-RAM with Quad-Core speed Capability (minimum clock speed at 1.8 GHz). Besides, the capacity of the interface should be in term of Gbps while transmission medium should have high availability with IP redundant links. It is advisable to use Optical Fiber redundant links at this stage to interconnect Core-to-Core devices and Core-to-Distribution devices in other to offer high, reliable transmission speed which minimizes propagation delay and impact on the overall system response time (acceptable at less than 150 ms).

✓ **Minimize or avoid the use of Network Address Translations Technics:** NATing consumes memory and processing speed even if [13] and [14] argues that the impact is negligeable. However, because of the constrain of handling separate routing and forwarding tables (IPv4 and IPv6), it is productive to minimize memory occupation while using benefit of IPv6 capability to satisfy challenges of IPv4[8].

✓ **Provide separate IPv4 and IPv6 addressing plan, subnetting and routing mechanisms (Data and VoIP traffic):** IPv6 addressing (128 bits size) should follow the existing IPv4 (32bits) design logic while making use of the extra bits of IPv6 (48 bits global routing prefix with 16 bits available to create subnets and 64 bits to address IPv6 network entities).

✓ **Provide IPv6 capability to H.323/SIP stacks and RTP/RTCP stacks:** The Dual-Stack Router Gateway must provide IPv6 capability to H.323/SIP stacks and RTP/RTCP stacks for VoIP service [10]. It should be able to create SIP trunk in dual-Stack, Only-IPv4 and Only-IPv6 traffic so that User Agent (UA) should be able to include both IPv4 and IPv6 addresses in their Session Description Protocols (SDP) messages. Apply QoS according to configurations made at the distribution level with a special accent on VoIP flow over IPv4 and IPv6. It is about classifying traffic based on access lists and attributing QoS Policies that will provide bandwidth and queue management with re-marking of packets. These policies must be attached to specific interfaces according to the QoS to achieve in term of resource allocation and Call Quality Metric of Voice on the endpoints (Mean Opinion Score (MOS) ranging from 3.5 to 4.2 depending on the CODEC used [12]).

4.4.2 The Application Level

Considerations at the application level consist of maintaining high service availability of VoIP with IPv4 or IPv6 applications servers. It means ensuring that VoIP functionalities (calls, Voice-mail, call transfer, etc.) do not suffer from any network impairment. VoIP end-users should be able to access these functionalities anytime with the best quality. Consequently, Dual-Stack oriented Media Servers and Applications Servers are strictly dependent on the quality of network elements and configuration deployed at the Core, Distribution and Access level.

5. Conclusion

Implementation of VoIP in a Dual-Stack design topology requires focusing considerations on three major areas: physical, logical and security. Each of this area constitutes a domain where a point of failure of Voice service can be identified. The various levels of IPv4/IPv6 network hierarchy (Access, Distribution, Core and Application levels) must, therefore, be perceived as specific blocs where specifics considerations must be taken in order to minimize network problem that affects the VoIP QoS such as high packet loss, poor system response time, delay-variation and Bandwidth congestion.

REFERENCES

[1] Diane Barret, Kirk Hausman, Martin Weiss (2015), Network implementation of Protocols and Services, Pearson Education, Pearson IT certification.

[2] Roysden, Russell and Shiller, shu (2015) " Retooling for success: A Case Study of VoIP Implementation to Improve Customer Service at a Midwestern Financial Services Office", Journal of the Midwest Association for Information Systems (JMWAIS): Vol. 1: Iss1, Article 5.

[3] Xianhui Che, Dylan Lewis (2010), IPV6: Current Deployment and Migration Status, Faculty of Apply Design and Engineering, Swansea United Kingdom.

[4] Cisco (2011), Implementing VoIP for IPv6, Cisco Systems, How to implement VoIP for IPv6

[5] Robert Valdes & Dave ROOS (2020), How VoIP Works, HowStuffWorks, InfoSpace Holdings, LLC, a Syste1 Company. https://computer.howstuffworks.com

[6] Cisco (2010), Dual-Stack Network, Cisco Systems, AT-A Glance, paper C45625859-00.

[7] Daniel Noworatzky (2019), How IPv6 benefits VoIP, TeleDynamics Thinl Thank, Think Tank Blog. http://info.teledynamics.com/blog/how-ipv6-benefits-voip

[8] Dany McPherson (2011), 8 security considerations for IPv6 deployment so, Special Network World

[9] Mohamed Nassar, Redo State (2009), VoIP Malware : attacks and Tools Scenarios, Olivier Festor Centre de Recherche INRIA Nancy, Conference: Proceedings of IEEE International Conference on Communications, ICC 2009, Dresden, Germany, DOI: 10.1109/ICC.2009.5199570 • Source: DBLP.

[10] Kirstein P, Lambrios L (2007) Integrating Voice over IP services in IPv4 and IPv6 Network. In Proceedings of the International Multi-Conference on Computing in the global Information Technology. IEEE

[11] Amzari J, Waleed, Ali Al, Majid A. (2016) Building IPv6 Based Tunneling Mechanisms for VoIP security, 13th Internationa Multi-Conference on Systems, Signals and Devices, University of Liverpool, UK.

[12] Therdpong Daengsi (2012), VoIP Quality Measurement: Recommendation of MOS and Enhanced Objective Measurement Method for Standard THAI SOKEN LANGUAGE, PhD thesis.

[13 R. Asinovskyy, A. L.WIjesinha, and R. Karne, "VoIP performance with IPsec in IPv4-IPv6 transition networks," Inforcommunication Journal, Special Issue,. vol. LXV, no. 3, 2010, pp. 15–23. [7] R.

[14] Yasinovskyy, A. L. Wijesinha and R. Karne, "Impact of IPsec and 6to4 on VoIP quality over IPv6," Proc. 10th Int. Conf. on Telecommunication, Zegreb, 8-10 June 2009, pp. 235-242.