Fall 11-2012

IPTV IMPLEMENTATION IN KOSOVO INFRASTRUCTURE

Burim Krasniqi

Universities for Business and Technology
School of Computer Sciences and Engineering

IPTV IMPLEMENTATION IN KOSOVO INFRASTRUCTURE

Bachelor Degree

Burim Krasniqi

November / 2012
Pristine

Universities for Business and Technology
School of Computer Sciences and Engineering

Bachelor Thesis
Academic Year 2011 - 2012

Student: Burim Krasniqi

IPTV IMPLEMENTATION IN KOSOVO INFRASTRUCTURE

Supervisor: Dr.Petrit Shala

November / 2012
Pristine

This thesis is submitted in partial fulfillment of the requirements for a Bachelor Degree

ABSTRACT

Process of Routing information is one of the essential processes ranging from smaller networks communication.

With the growth and development of computer networks in the size and complexity also the issue of IPTV as a network configuration which enables transport of voice and data through DSL (Digital Subscriber Line) technology to the customer premises, today is largely deployed.

These services now days are provided also in Kosovo's network through xDSL technologies, supported by IP/Ethernet optical core network and IP based switching/routing infrastructure.

The readiness of already implemented NGN platform in Kosovo's telecommunication network and steps, which should be taken related to IPTV implementation, are further described in this section.

The readiness of already implemented NGN platform in Kosovo's telecommunication network and steps which should be taken related to IPTV implementation is further described in this section.

Content digitalization and the interactive opportunities offered by IPTV services, enable digital video services to be tailored of individual users, known as *self generated content*.

Since costs of global network distribution are decreasing, and production cost of content generation (records with simple digital camera) are being reduced dramatically, the self content generation feature represents significant added value for users themselves.

ACKNOWLEGMENT

In this case, I would like to thank my mentor Dr. Petrit Shala who helps me a lot doing this thesis offering books, different materials and useful advice about the topic that we have chosen and better preparation of this report.

Respect and special thanks to our colleagues deserve who study together which gave us suggestions and criticism, which positively affected the establishment and enrichment of this project with the elements necessary for a proper academic paper.

Last but certainly not least, I thank them and to be grateful to friends and colleagues with whom we jointly are working in PTK, who also helped me more through information, drawings and examples that we have offered about IPTV implementation in Kosovo infrastructure.

List of figures

List of tables

CONTENT

1.0. Introduction

Every day needs of telecommunication services are related to bandwidth requirements. Despite very large developments in mobile technology, fixed network solutions are providing larger bandwidth and probably will continue to offer in the near future, also.

Internet Protocol TV (IPTV), overall is a system with the help of which all TV channels are closer to customers using IP protocol. Also there are a lot of value added services such as: Time shift TV, Customized Advertising, NPVR (Network Personal Video Recorder),VoD (Video on Demand) and SVoD (Subscription Video on Demand) etc. which are available for all customers using IPTV.

The bandwidth available to the fixed network end-users is limited by the length and quality of the local loop. Problems encountered by DSL (Digital Subscriber Line) technology when using copper cable will be solved by fiber optic NGA (Next Generation Access) topologies and technologies.

Although it is difficult to make predictions about the future applications, it is to believe that the TV content will be on the high-level demands in the next coming years [1]. IPTV as a new product, through either copper or fiber, should open the door to the new revenues for fixed operators attracting more customers. Such efforts on IPTV implementation are going to be taken in Kosovo’s telecommunication network, also.

1.1. Hypotheses

Before started the research I have expected that:

IPTV using WiMAX technology is the most convenient solution for areas with low population density.

2.0. Literature Review

One of the most mentioned concepts for video transport over the high-speed wire line and wireless broadband networks is known as IPTV, what in other words means, the delivering of video content over a converged IP network. Customer's video content accessibility is enabled through the CPE (Customer PremisesEquipment).

CPE has broadband network termination functionality. IPTV via broadband offers potential access to almost very large volume of content compared with traditional distribution capacities for television content. The content itself may be standard or high definition.

IPTV content can be provided through *video on demand library, broadcast terrestrial service* and *satellite access.* IPTV service implementation reflects necessity of network architecture transformation toward IP technology and Ethernet transport platform.

PTK, as telecommunication service provider in Kosovo, has done a large step forward on this transformation by implementation of next generation network IP MPLS (Multiprotocol Label Switching) based, from the edge to the core level. The future steps are oriented on end - to - end Ethernet transmission network transformation.

IPTV has been launched by major service providers worldwide and its popularity with consumers is on the rise. Table 1 represents number of customers of different worldwide operators.

Generally, there are four development stages for IPTV, as further described such as: Video -on -Demand, TV channels delivery, Interactive IPTV, Self generated content.

2.1. Video-on-Demand

Video on demand services are similar with DVD type of video services. The main difference is that the content is stored to service (content) provider to whom the user has access through respective network. The end user decides when to watch, with full control over how content is played: pause, slow motion, fast forward, rewind etc.

For video-on-demand services, the normal DSL bandwidth should be sufficient. But, necessary investments for video-on-demand servers are needed. The problem of in-house networking should be considered, also.

2.2. TV channels Delivery

The next IPTV function is to deliver to customers the existing broadcast TV channels through IPTV platform. Broadcast TV services include the traditional analog channels, digital terrestrial television channels and those offered by coax cable or satellite platform.

This function is a deeper challenge for broadband networks with impacts related to both, the core network and the last mile. Since broadband capacity is limited and falls with distance, last mile bandwidth it is not enough to accommodate all channels to be delivered at the same time.

Thus, quality of services becomes essential, especially at the evening services when most users watch TV and will not tolerate bugs.

For HDTV criterions are even more serious. Commercial offerings may consist of channel packages. Each package is sold individually and usually charged on a monthly fee per package basis.

2.3. Interactive IPTV

IPTV consumers have a new opportunity, from passive television consumption to activate the downloading of the desired content. But, further stage of IPTV service is the opportunity of interactive process of consumers related to the content provided through such a service. As a result of interactive possibilities, this phase offers the potential for a complete turnaround in consumer behavior with the new opportunities related to content and services. Some of these opportunities are: Instant channel change with minimum interruption, Time shifted television, one touch recording, PIP- picture in picture, Time based recording, Customization per category, etc.

2.4. Self Generated Content

Content digitalization and the interactive opportunities offered by IPTV services, enable digital video services to be tailored of individual users, known as *self generated content*. Since costs of global network distribution are decreasing, and production cost of content generation (records with simple digital camera) are being reduced dramatically, the self content generation feature represents significant added value for users themselves.

This feature in one hand will increase the customers' willingness to spend time with such a service and on other hand consequently will impact on higher market revenue. This is a new era on creating TV channels for individual persons, families and companies delivered through telecoms' networks. Interactive advertising could also become a reality.

Based on the above development stages of IPTV, the main advantages of IPTV service, compared with traditional terrestrial, cable and satellite access are listed below.

• On -demand accessibility
• Interactivity (Interoperability)
• Self generated content

3.0. Research Methodology

The research target is to find the most convenient access technology to use for increasing the penetration of fixed services in Kosovo in shortest time?

In order to answer in this question we have used *idiographic approach for a qualitative research*, considering a case study for a small country town.

Short description of how and which research elements are considered:

3.1. Empirical approach

In order to have a conclusion based on real facts and not based on personal preferences. I have considered and compared the technical characteristics for various IPTV technologies considering the same prerequisites.

3.2. Observation

Observation of existing fixed network penetration has resulted that there is a very low penetration. Therefore it has lead to performing a research for finding the best and fastest way for increasing the penetration.

3.3. Questions

During the observation I raised the question:

- Which is the most convenient access network technology for increasing the penetration of fixed services in Kosovo?
- Which is the best way to implement IPTV in Kosovo through IPv4,IPv6 or both?
- What is impact of QoS in IPTV technology?

4.0. Experiment

A rural area was chosen for testing and comparing the parameters of various wireless technologies.

4.1. Quality of Service overview

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Frame Relay, ATM, Ethernet and 802.1 networks, SONET, and IP-routed networks. In particular, QoS features provide improved and more predictable network service by providing the following services:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network [9]

4.2. Quality of Service Architecture

You configure QoS features throughout a network to provide for end-to-end QoS delivery. The following three components are necessary to deliver QoS across a heterogeneous network:

- QoS within a single network element, which includes queuing, scheduling, and traffic shaping features.
- QoS signaling techniques for coordinating QoS for end-to-end delivery between network elements.
- QoS policing and management functions to control and administer end-to-end traffic across a network.

Not all QoS techniques are appropriate for all network routers. Because edge routers and backbone routers in a network do not necessarily perform the same operations, the QoS tasks they perform might differ as well. [9]

To configure an IP network for real-time voice traffic, for example, you would need to consider the functions of both edge and backbone routers in the network, then select the appropriate QoS feature or features.

In general, edge routers perform the following QoS functions:

- Packet classification
- Admission control
- Configuration management

In general, backbone routers perform the following QoS functions:

- Congestion management
- Congestion avoidance

4.3. End-to-End QoS Models

A service model, also called a level of service, describes a set of end-to-end QoS capabilities.

End-to-end QoS is the ability of the network to deliver service required by specific network traffic from one end of the network to another.

Cisco IOS QoS software supports three types of service models: best effort, integrated, and differentiated services. [9]

Consider the following factors when deciding which type of service to deploy in the network:

- The application or problem you are trying to solve. Each of the three types of service best effort,
  Integrated, and differentiated—is appropriate for certain applications.
- The kind of ability you want to allocate to your resources.
- Cost-benefit analysis. For example, the cost of implementing and deploying differentiated service is certain to be more expensive than the cost for a best-effort service.

The following sections describe the service models supported by features in Cisco IOS software:

- Best-Effort Service
- Integrated Service
- Differentiated Service

4.4.. Quality of Service Features

The Cisco IOS QoS software provides the major features such as:

- Classification
- Congestion Management
- Congestion Avoidance
- Policing and Shaping
- Signaling
- Link Efficiency Mechanisms
- QoS Solutions
- Modular QoS Command-Line Interface
- Security Device Manager

The features listed are described more fully in the overview chapters of this book, which is organized into parts, one for each of the major features listed.

Each book part contains an overview chapter and one or more configuration chapters.

4.5. QoS and Video traffic characteristics

QoS can affect a network's bandwidth, delay, jitter, and packet loss properties. Applications have different requirements for bandwidth, delay, jitter, and packet loss. With QoS, a network can better provide the right amounts of QoS resources for each application. [10]

Without QoS, video flows typically degrade. The pictures become unclear. Movement is jerky. Movement appears to be in slow motion. Often, the audio becomes unsynchronized with the video.

The video can be completely gone, but the audio still works. In short, unless the network has significantly more bandwidth than is needed for all traffic, video quality degrades.

Just like the coverage of voice in this chapter, this section breaks down an analysis of video traffic as it relates to the four QoS characteristics: bandwidth, delay, jitter, and loss. First, the basics of packet video are explained, followed by QoS details unique to video in terms of the four QoS characteristics.

4.6. Video Basics

IP packet video can be categorized into two main categories: [10]

• **Interactive video**—Includes H.323-compliant video conferencing systems, such as Cisco's IP/VC 3500 series of products, and Microsoft's NetMeeting desktop videoconferencing product. H.323-compliant video conferencing tools use the familiar RTP protocol for transmission of the voice and audio payload, typically sending the audio in a separate RTP stream than the video.

• **Noninteractive video**—Includes typical e-learning video services and streaming media,and includes products such as Cisco's IP/TV, Microsoft Windows Media Technologies products, and Real Networks products. Some noninteractive video uses H.323 standards for video call setup and teardown, and some do not—for instance, Real Networks most recent servers use Real-Time Streaming Protocol (RTSP) for call setup/teardown, and either the proprietary Real Networks Data Transport (RDT) or RTP for video payload,depending on the video player used.Like voice, video codec's convert the analog audio and video to packetized form. codec delay, packetization delay, and de-jitter initial play out delay are all included in video delay, just like with voice.

Familiar voice codec's, including G.711 and G.729, convert the audio stream, which is typically sent as a separate flow from the video signal. The video signals use a large variety of codec's, including ITU H.261, and the popular Moving Pictures Experts Group (MPEG) codec's. [10]

4.7. Network Topology

The readiness of already implemented NGN platform in Kosovo's telecommunication network and steps which should be taken related to IPTV implementation is further described in this section. PTK network is based on centralized service platform and distributed access. The system is organized in 7 regions, in each region there is a traffic aggregator ESS (Ethernet Service Switch). Further traffic from these 7 ESS is aggregated to the Core Router [3]. Network design is based on 4 main network concepts:

Access Network

Edge/Core Network

Transmission Network

Service Platform

4.8. Access Network

The access network consists of:

Multi-service access nodes - able to deliver different services including: telephony, data, High Speed Internet Access and Video services, where the same copper pair is used for various mix of services. Currently in PTK it is a case of POTS and ADSL services.

DSLAM - (Digital Subscriber Line Access Multiplexer). Within PTK network this type of equipment are used exclusively to offer high speed internet access through ADSL in urban areas [3].

4.9. Edge/Core Network

Edge/Core network build in PTK uses label switching technology MPLS (MultiProtocol Label Switching) which provides the ability to set up connection-oriented paths over a connectionless IP network. There are seven ESS installed, one per region.

All access nodes from the region are connected to regional ESS. ESS is handling intraregional traffic received from end customers through access nodes (Lifespan and DSLAMs) as presented in Fig. 1. Further, all regional ESS is connected to the Service (Core) Router, as presented in system configuration through Fig. 1.

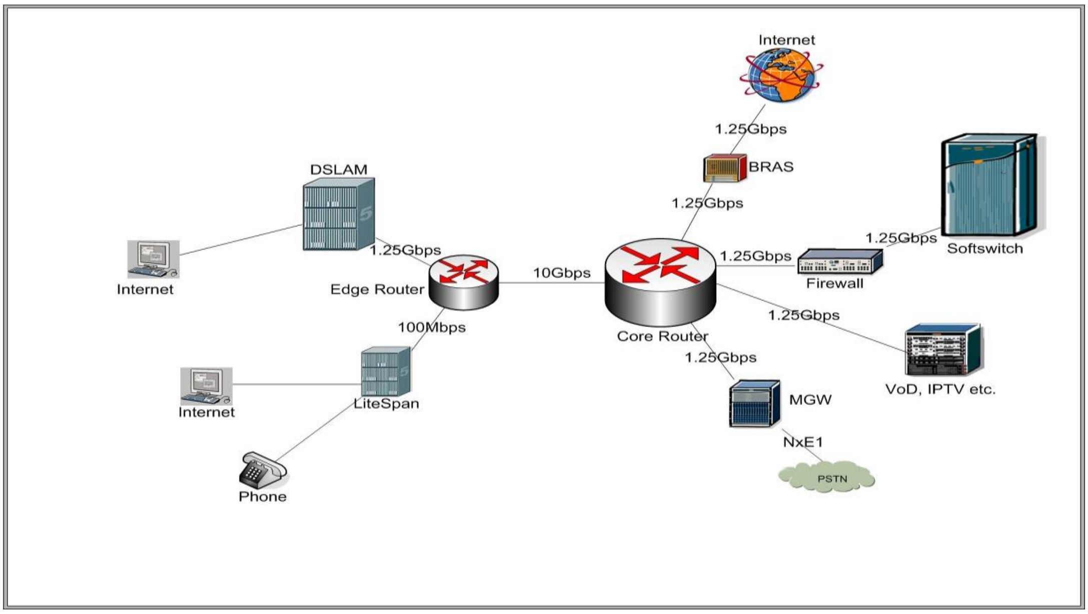

Figure 1.System configuration [PTK group]

Edge/Core network include:

Ethernet Service Switch (ESS) is the edge component of the network able to offer the following types of services: Ethernet pipe (Epipe) Frame-Relay (Fpipe), Virtual Private LAN Service (VPLS), Internet Enhanced Service (IES).

Service Router (SR) – is the core router able to offer the following services: Ethernet pipe (Epipe), ATM VLL (Apipe), Frame-Relay (Fpipe), Virtual Private LAN Service VPLS, Internet Enhanced Service (IES), and Virtual Private Routed Network (VPRN).

Since already implemented NGN structure is VoIP –MPLS, the remote access nodes had to be interconnected on Ethernet platform. This is achieved by three methods. First, through fiber optic equipment using Ethernet interface, second, by dark fiber and media converter, and as a third one where we had no fiber access are used MW equipment with E1/Ethernet converters.

4.10. Transmission Network

The existing transmission network in PTK is build of two systems Micro-Wave (MW) and optical fiber (OF) configured in meshed topology. MW is used where there is no fiber optic access or as a redundancy. For transmission through fiber the SDH-OMSN (Optical Multi–Service Nodes) equipment are used.

By OMSN equipment can be provided capacities like: E1, E3, STM-n, Ethernet, Fast Ethernet, Gigabit Ethernet, VLAN with QoS managed.

This structure enables interconnection of remote access nodes for both, voice and data services. By 2008 the interconnection of all edge routers to the core router will be completely fiber optic based with capacities of 10 GB/s as it is presented in the Fig. 2 [4].

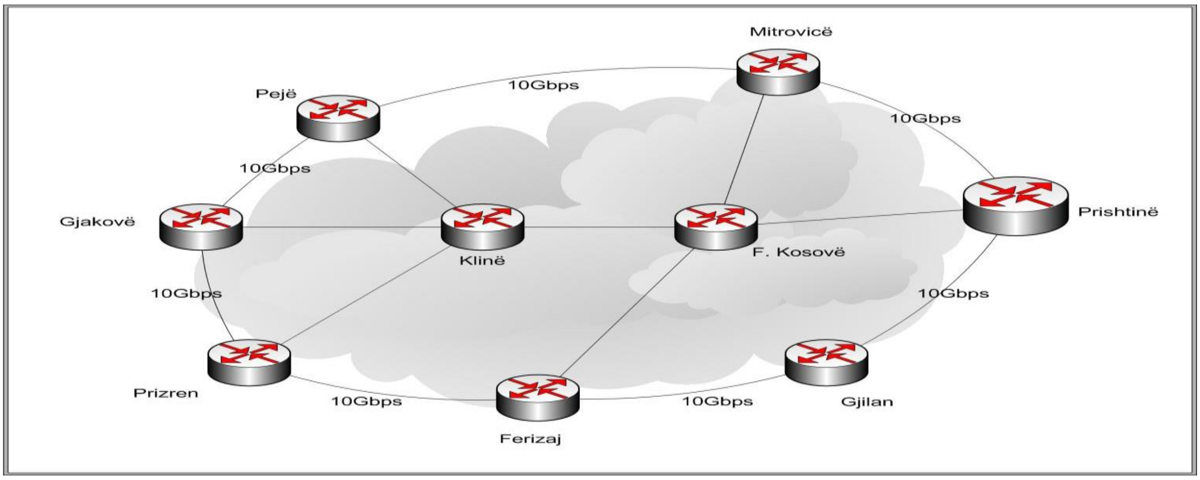

Figure 2. Edge/core transmission network structure [PTK group]

So, regional systems in: Mitrovice, Peje, Gjakove, Prizren, Ferizaj and Gjilan are accumulating traffic from all nodes using MW and OF.

These centers will be interlinked to the main center in Pristine through 10 GB/s. There are two other centers, Kline and F.Kosove established as optical node centers for access of lower level municipalities.

4.11. Service Platform

There are two concepts building service platform:

Narrowband services are phone services offered by Soft Switch and supplementary services offered by IN such as Centrex, Prepaid, Tele voting etc.

Broadband Services are data services offered by broadband platform Routers, BRAS (Broadband Remote Access Server) and Radius server (see fig 2). So far PTK is offering Internet and Virtual Private Networks (VPN). In near future PTK aims to offer IPTV services.

4.12. IPv4 Addresses

IPv4 addresses are 32 bits long; like all network-level addresses, they have a network portion and a host portion. The network portion uniquely identifies a physical or logical link and is common to all devices attached to that link.

The host portion uniquely identifies a particular device attached to the link.

There are several ways to represent the 32 bits of an IP address. For instance, the 32-bit IP address 00001010110101100101011110000011 can be represented in decimal as 181,819,267.

The binary format is cumbersome, and a decimal format of the entire 32-bit number is time consuming to calculate. Figure 3 shows a better format. [1]

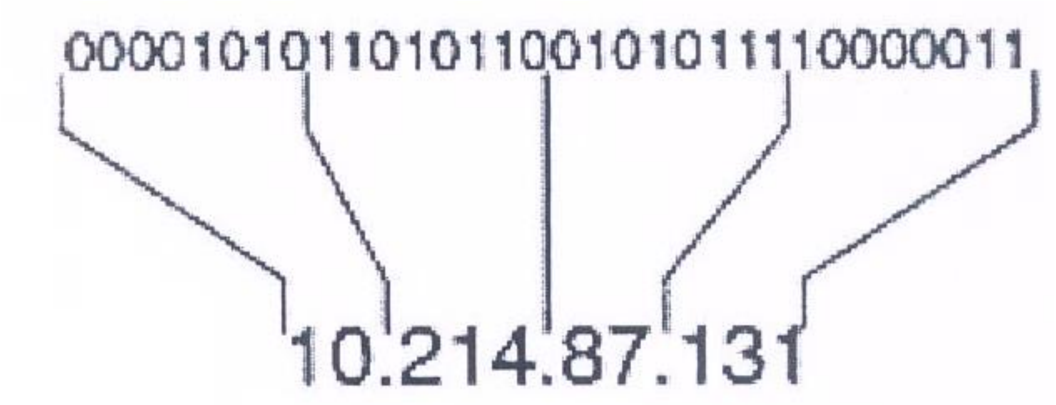

Figure 3. Dotted-decimal format [CCNP Route CISCO]

The 32 bits of the address comprise four octets, each of which can be represented with a decimal number between 0 and 255, with dots between the decimal representations.

In Figure 3, the 32-bit address is mapped into a dotted-decimal representation.

An important distinction to remember when working with IPv4 addresses is that dotted decimal is just an easy way for humans to read and write IP addresses. Always remember that the router is not reading an address in terms of four octets; rather, the router sees a 32-bit binary string. [1]

Probably the most distinctive characteristic of IPv4 addresses is that unlike other network-level addresses, the network and host portions can vary in size within the 32-bit boundaries. That is, the network portion might take up most of the 32 bits, or the host portion might, or they might divide the bits equally. Protocols such as NetWare and AppleTalk were designed for use in relatively small networks, and as a result their network-level addresses have fixed-length network and host portions.

4.13. First Octet Rule

Without putting too fine a point on it, it can be said that there are three sizes of networks admeasured by the number of hosts: big, medium, and small:

Big networks, by definition, have a huge number of hosts. Relatively few big networks exist. Small networks are just the opposite. Each one is small because it has a small number of hosts; a huge number of small networks exist.

Medium networks are just that: a medium number of them (in relation to big and small ones) and a medium number of hosts in each one. [1]

This high level of addressing focus requires three types*classes*of network addresses for the three sizes of networks. Addresses for big networks need to be capable of addressing many hosts, but because so few big networks exist, only a few big-network addresses are required.

Figure 4 shows how the network and host portions of IPv4 addresses are divided up for these three classes.

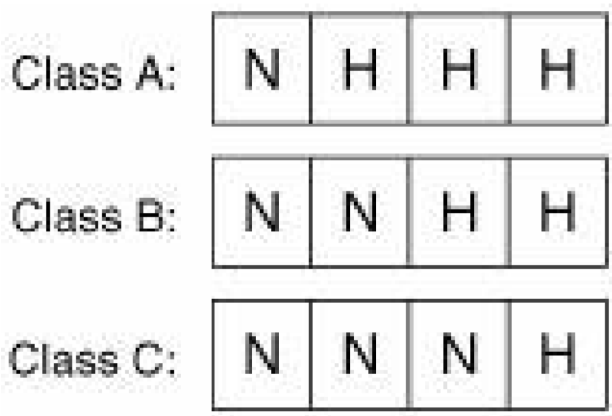

Figure 4. IP packet protocol [CCNP Route CISCO]

The big, medium, and small networks described thus far map to address classes as follows:

Class A IPv4 addresses are for big networks. The first octet is the network portion, and the last three octets are the host portion. Only 256 numbers are available in the eight-bit network part, but 224 or 16,777,216 numbers are available in the host part of each of those network addresses. [1]

Class B addresses are for medium-size networks. The first two octets are the network portion, and the last two octets are the host portion. There are 216 or 65,536 available numbers in the network part and an equal number in the host part.

Class C addresses are just the opposite of Class A. The first three octets are the network portion, and the last octet is the host portion.

Because all IPv4 addresses are 32-bit binary strings, a way of distinguishing the class to which a particular address belongs is necessary.

The *first octet rule*, demonstrated in Tab1. provides the means to make such a distinction

Table 1. First octet rule [Wendell Odom , CCIE]

RULE	MINIMUM AND MAXIMUM	DECIMAL RANGE
CLASS A: First bit is always 0	**0**0000000 = 0 **0**1111111 = 127	1126
CLASS B: Firsst two bits are always 10	**10**000000 = 128 **10**111111 = 191	128191
CLASS C: First three bits are always 110	**110**00000 = 192 **110**11111 = 223	192223

4.14. Address Masks

The address for an entire data link a non-host-specific network addresses represented by the network portion of an IP address, with all host bits set to zero. For instance, an addressing authority might assign to an applicant an address of 172.21.0.0.

This address is a Class B address because 172 is between 128 and 191, so the last two octets make up the host bits. Notice that they are all set to zero.

The first 16 bits (172.21.) are assigned, but address owners are free to do whatever they please with the host bits. [1]

The address mask is a 32-bit string, one bit for each bit of the IPv4 address. As a 32-bit string, the mask can be represented in dotted-decimal format just like an IPv4 address. This representation tends to be a stumbling block for some beginners:

Although the address mask can be written in dotted decimal, it is not an address.

Tab 2. shows the standard address masks for the three classes of IPv4 address.

Table 2. Address masks for Class A, B, and C IPv4 addresses [IP routing CISCO]

CLASS	MASK	DOTTED DECIMAL
A	**00000000111111111111111111111111**	**255.0.0.0**
B	**11111111111111110000000000000000**	**255.255.0.0**
C	**11111111111111111111111100000000**	**255.255.255.0**

4.15. Subnets and Subnet Masks

As defined so far, a single Class A, B, or C address can be used only on a single data link. To build a network, separate addresses must be used for each data link so that those networks are uniquely identifiable.

If a separate Class A, B, or C address were assigned to each data link, fewer than 17 million data links could be addressed before all IPv4 addresses were depleted.

The only way to make Class A, B, or C addresses practical is by dividing each major address, such as 172.21.0.0, into sub network addresses. Recall two facts:

- The host portion of an IPv4 address can be used as desired.
- The network portion of an IPv4 address is determined by the address mask assigned to that interface.

Figure 5 shows a network to which the major Class B address 172.21.0.0 has been assigned. Five data links are interconnecting the hosts and routers, each one of which requires a network address.

As it stands, 172.21.0.0 would have to be assigned to a single data link, and then four more addresses would have to be requested for the other four data links

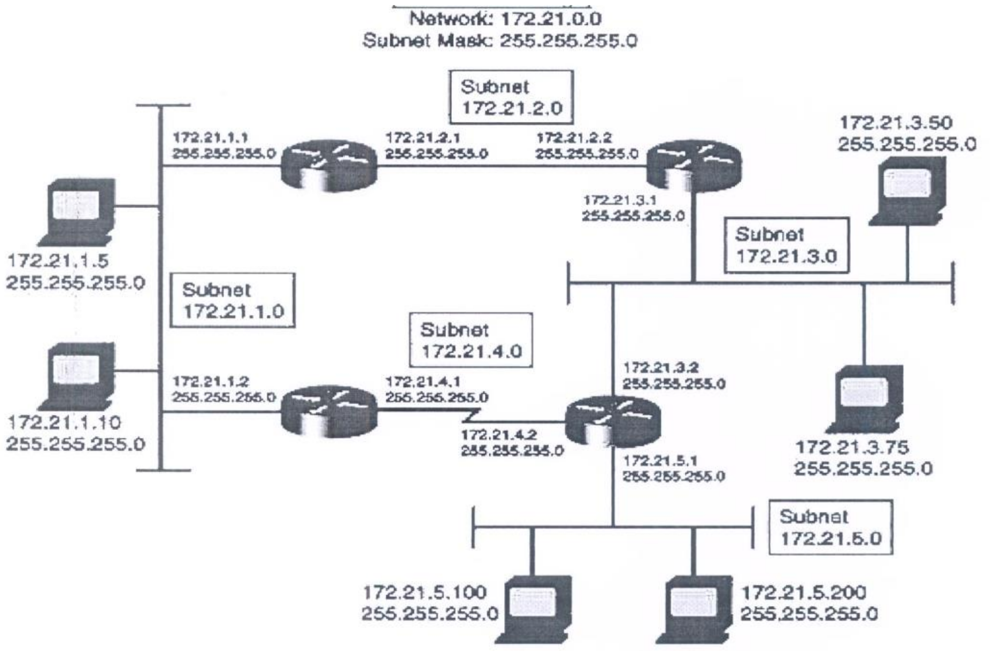

Figure 5. Network to which the major Class B address has been assigned [IP routing CISCO]

The IPv4 address now has three parts: the network part, the subnet part, and the host part. The address mask is now a *subnet mask*, or a mask that is longer than the standard address mask.

The first two octets of the address will always be 172.21, but the third octet whose bits are now subnet bits instead of host bits might range from 0 to 255.

The subnet mask might be represented in any of the following three formats:

Dotted decimal: 255.255.255.0

Bit count: 172.21.0.0/24

Hexadecimal: 0xFFFFFF00

Dotted decimal is commonly used in software that has been around for a while, although the bit count format is becoming increasingly preferred.

Compared to dotted decimal, the bit count format is easier to write.

4.16. Troubleshooting a Subnet Mask

The necessity frequently arises to "dissect" a given host address and mask, usually to identify the subnet to which it belongs. :[1]

For instance, if an address is to be configured on an interface, a good practice is to first verify that the address is valid for the subnet to which the subnet is connected.

Use the following steps to reverse-engineer an IP address:

Step 1. Write the given subnet mask in binary.

Step 2. Write the IPv4 host address in binary.

Step 3. Knowing the class of the host address, the subnet bits of the mask should be apparent. Using the mask bits as a guide, draw a line between the last network bit and the first subnet bit of the address. Draw another line between the last subnet bit and the first host bit.

Step 4. Write the network and subnet bits of the address, setting all host bits to zero. The result is the address of the subnet to which the host address belongs.

Step 5. Again write the network and subnet bits of the address, this time setting all host bits to one. The result is the broadcast address of the subnet.

Step 6. Knowing that the subnet address is the first address in the sequence and that the broadcast address is the last address in the sequence, you also know that all addresses between these two are valid host addresses.

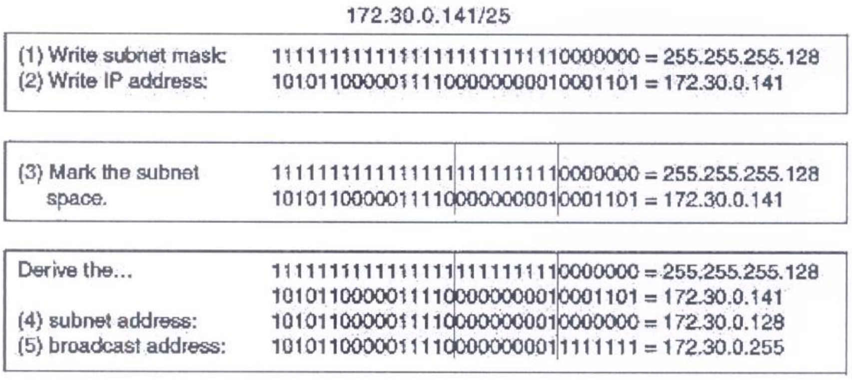

Figure 6. Steps to find the subnet, the broadcast, and the host addresses [CCNP Route CISCO]

In this case valid host addresses for this subnet are 172.30.0.129 – 172.30.0.254

The address is a Class B, so it is known that the first 16 bits are the network bits; therefore, the last nine bits of the 25-bit mask mark the subnet space.

The subnet address is found to be 172.30.0.128, and the broadcast address is 172.30.0.255. Knowing that the valid host addresses for the subnet are bounded by these two addresses, it is determined that the host addresses for subnet 172.30.0.128 are 172.30.0.129 through 172.30.0.254.

4.17. IPv6 Addresses

The ultimate solution to rapidly growing Internet routing tables and IPv4 address depletion was the development of IPv6, which defines 128-bit source and destination addresses.

At the risk of being derided 20 years from now, I'll venture a guess that IPv6 has more addresses than we'll ever need. IPv6 can support over a trillion, trillion IP addresses per person on the planet—with plenty of publicly routable addresses for everyone. Plus, the structure is well established for CIDR-like allocation of address blocks, keeping Internet routing tables small. [2]

4.17. IPv6 Addresses Format

IPv6 addresses have eight *quartets* of hex digits, separated by colons. Each quartet consists of four hex digits, which together represent 16 bits.

The rules for encoding the actual hex values are as follows: [2]

- Each quartet is separated by a colon (:).
- In a quartet, leading hex 0s can optionally be omitted.
- If one or more consecutive quartets are hex 0000, then the set of consecutive all-0 quartets can be represented as a null quartet (::), no matter how many consecutive all-0 quartets are in this range.
- Only one use of :: is allowed in a single IPv6 address.

For example, the following IPv6 address is shown in three different valid formats.

The first one uses no shortcuts; the next removes leading 0s in each quartet; and the last abbreviates multiple, consecutive, all-0 quartets with ::.

0123:0078:0000:0000:9ABC:0000:0000:DEF0

123:78:0:0:9ABC:0:0:DEF0

123:78::9ABC:0:0:DEF0

All three versions are legal and common, but router command output generally shows the briefest form so that command output best fits on the visible screen. Also, notice that there were two places in the address with two consecutive all-0 quartets. The :: shortcut implies one or more consecutive all-0 quartets, so using this abbreviation in more than one place would be ambiguous. [2]

4.18. Simple IPv6 Configuration

Figure 7 shows a small, sample network that is used in this section to show basic IPv6 connectivity using global addresses. [2]

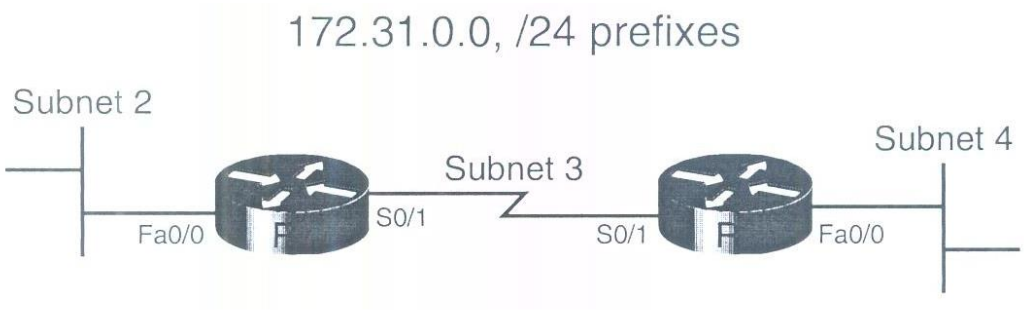

Figure 7. Basic IPv6 connectivity using global addresses [CCNP Route CISCO]

The routers use *dual stacks* (both IPv4 and IPv6 addresses are assigned to the interfaces) for this network. Hosts with dual stacks (running both IPv4 and IPv6) would be able to send IPv4 or IPv6 packets, and the routers could accommodate either.

Configuring Dual-Stack IPv4/IPv6 with OSPF:[2](Refer to Appendix 1)

4.19. IPv6 Addressing Summary

Besides global addresses, other styles of IPv6 addresses exist. Table 4-14 lists and briefly describes the different types of addresses.

Table 3. IPv6 Address Type Summary [IP routing CISCO]

TYPE OF ADDRESS	DEFINITION AND PURPOSE
Aggregately global unicast	Unicast IPv6 address must be globally unique. Registered unique globally routable address
Link-local unicast	Required for each IPv6 interface. Used for processes occurring only on the local link, not routable
Site-local unicast	Intended for use only within a site. Included in the IPv6 definitions in RFC 3513, but deprecated in RFC 3879
Centrally assigned unique local	Similar to IPv4 private addresses, a range of IPv6 addresses that will not be assigned as public globally routable addresses
IPv4 compatible unicast	Used mainly for migration to IPv6 when the core is still IPv4. IPv6 addresses are 96 binary 0s, followed by the interface's assigned IPv4 address.
Anycast	The configuration of the same IPv6 unicast address on multiple hosts, with IPv6 routing packets to the closest host. Used with redundant identical services for load balancing
Multicast	Includes some nonrouted and some routable ranges. Large range (all addresses beginning with FF). Used instead of broadcast addresses.
Broadcast	Nonexistent in IPv6, for instance ARP is replaced by Neighbor Discovery (ND) messages, which use a reserved IPv6 multicast address.

This short section on IPv6 just scratches the surface of IPv6 features in general and Cisco routers in particular. The "Further Reading" section near the end of the chapter lists a couple of good references for additional details about IPv6.

4.20. Implementing IPTV platform with IPv4 and IPv6 devices

For sure IPv6 is arriving for the last 20 years. Mistrust of operators and companies are justified. ICT'2010, one of the most important *Information and Communication Technologies* conferences in Europe organized by the European Commission, presented the current state of implementation of IPv6 in Europe, and the future of IPv6 in Europe does seem overcast;

On the one hand the IPv4 addresses are really finishing: deadline is 2012, on the other hand there are several steps missing for total operation of IPv6 all around Europe, and the countries, which will not work with IPv6 risk incomplete operation within a near future.

Building a network fully IPv6-aware comes up as a difficult task because Internet protocol is related with all the systems and devices (horizontal point of view), and at the same time it is the bottleneck of the layer architecture of the Internet (known as hour-glass model of the Internet). The hour-glass model implies that almost all the layers of the network have to do with the Internet protocol.

In this paper, we analyze the IPv6 start for Internet protocol television (IPTV) centering in the emerged problems when we set in motion IPTV system over devices, some working on IPv4 and some of them working on IPv6.

We propose a solution based on sending to the net-work two parallel multicast streams, each one for one IP protocol (v4 and v6).

To double the IPTV stream, we consider two independent networks and locate a server (IPv4/IPv6 server), which transmits between IPv4 and IPv6 “zones”.

This server is able to receive multicast flows generated by IPv4 devices and resend them in IPv6 multicast transmission to the IPv6 hosts.

It can also perform transmission in opposite direction, when the IPTV signal source is located in IPv6 network and the destination is in
IPv4 domain.

4.21. Overview of the IPTV System

Multimedia communications are crucial for the definitive supremacy of packet networks over other connecting plat-forms.

Practically all the multimedia communications have been or are being placed in the network, one of the most important is the television system carried within the Inter-net.

This system is known as IPTV. IPTV systems have experienced an unexpected success in the network, gaining in popularity compared with other television transmissions.

The reason we may find in the fact that consumers, always more “demand personalized TV experiences that are avail-able anytime, anywhere, on any device”.

The capabilities of IP television to fulfill these requirements as well as the fact that the whole complexity of IPTV systems is actually transparent to the consumers give more and more popular-ity to IPTV systems.

IP television favored changes in business models for the Internet. While before IPTV introduction, users connected more or less occasionally, now with IPTV (classical television or video on demand) the users just do not disconnect the computers from the Internet. The result is that many more consumers are constantly connected and the classical IPv4 addressing is not enough. IPTV demands IPv6 to offer static addressing to all the users. Moreover, another reason for the introduction of IPv6 to carry IPTV streams is the mobility of terminals (UMTS, LTE, etc.). As known, mobility requires enlarged addressing. On the other hand, we may remark another not banal reason for carrying classical television channels by IPv6 network is the enhanced multicast of IPv6 compared to earlier version of Internet protocol. Therefore, IPv6 seems to be crucial for IPTV. Japan was the first country, which implemented a complete IPTV system working on IPv6. This first system is NTT Plala Hikari TV3 and its implementation resulted in-dispensable since Japan developed only-IPv6 network. In any case, Hikari TV resulted very successful and currently has hundreds of thousands of consumers.

Toshiba was the first hardware-specialized company commercializing IPTV devices working on IPv6.The complexity of IPTV systems is due to the high quantity of information carried by television streams. In fact, the IPTV is known as one of the killer applications in the Internet because of the necessity of bandwidth.

The demand of higher quality of the images required by the consumers means in practice that the image resolution is always higher and it implies more bandwidth in the IPTV transmissions.

Figure 8 shows different image resolution codes (most typical in Europe) standardized or commercialized in the in-dictated years. As we may observe, the proposed image resolution generally increased as time went by.

To this increasing image resolution, we should add the higher requirements of television 3D, which in its most popular version, consists of uniting two images in one, doubling, in this way, the necessary bandwidth in the network.

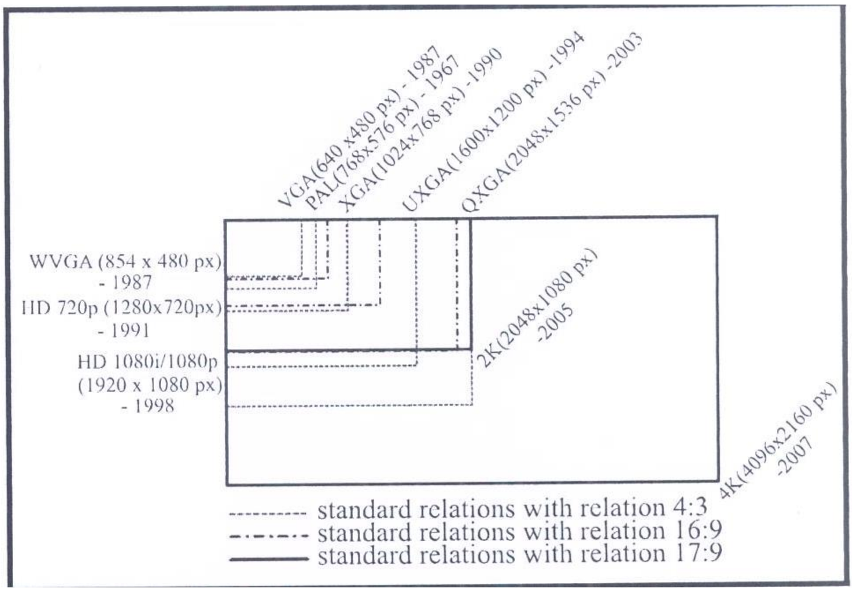

Figure 8. Standards for image resolution[PTK group]

Moreover, new applications related to the IP television as, e.g., interactive television, demand new requirements from the network.

In the case of interactive television, the requirements are more similar to the interactive games than to the classical television.

For the correct management of heavy TV streams served to an increasing demand, the IPTV systems are developing and improving new solutions every day. In this sense, IP television comprises many research areas related to telecommunications.

These areas are, among others, storage technologies, video and audio encoding (for example, MPEG-2 codec or more recent MPEG-4 H.264 codec), data encryption, data distribution, transmission by the network (new control and data planes).

The complexity of IPTV systems as well as their importance is also proved by the increasing number of projects dedicated to improvement of transmission of television streams by the Internet. Between all the projects within the 7th Framework Program funded by the European Union (EU 7FP) we may highlight the following ones: one of the most successful projects, which is currently finishing is the P2P-Next project [4].

Among other objectives, this project specified and implemented a set top box with an interface for connecting to peer to peer networks which offers to the classical television sets the possibility of gaining access to the contents provided by peer to peer networks. Mobile3DTV [5], researches problems of moving 3D television to mobile environment.

As known, mobility has strong limitations of bandwidth availability, which is not according to 3D television bandwidth requirements. Challenges as capture of 3D images, coding, and transmission are investigated in Mobile3DTV.

Otherwise, CANTATA is a project proposed inside the information technology for European advancement (ITEA) and develops a subset of functionalities related with interactive TV systems, which defines the requirements for this kind of television. [6]

Interactive TV enhances IPTV by offering to the consumer the possibility of interacting with the service provider for, e.g., shopping purposes.

Many other 7FP projects aim at introducing content-awareness within the network, which will undeniably open many new business possibilities to the Internet television. In fact, the new proposed architectures interconnect the four actors delineated in IPTV systems: content providers, IPTV service providers, transport and distribution IP network providers and clients. These projects are grouped together in the future media networks cluster. Let us remark that IPTV refers not only to classical broadcast television but also to new video on demand (VoD) services.

The difference between them lies in broadcast (or multicast) transmission of classical television channels and unicast (or any cast for new content aware network architectures) of VoD transmissions. Anyway, the system studied in this paper refers to classical broadcast (multicast) television.

The concept of our IPTV system is presented in Fig. 9. In this system, the high definition television signal, called digital video broadcasting or briefly (DVB) can be delivered either by satellite (DVB-S) or terrestrial (DVB-T) manner.

After receiving by appropriate antenna, television signal is transferred to the dream box device. The dream box [7], is a type of set top box and it is responsible for splitting digital DVB signal into IP packets, buffer them and transmit to the network as an integrated IP packet stream. Because unicast communication is not effective for providing IPTV service, often multicast connections are used for transfer packets between dream box and end devices. Users can watch TV programs directly on their PC computers or laptops, thanks to appropriate IPTV applications.

In case when we want to use a display unit such as a TV set, another set top box (STB) is used to transform again the IP packet stream into high definition television signal.

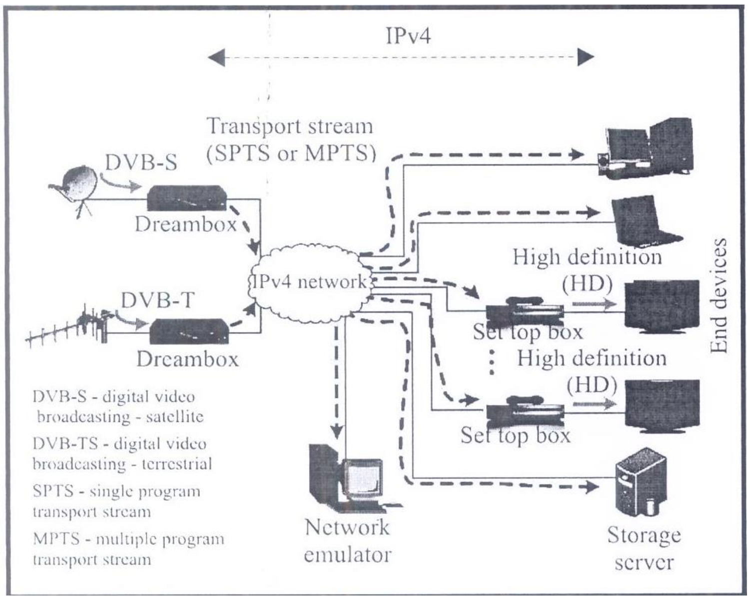

Figure 9. IPTV system over IPv4[PTK group]

The IPTV data are transferred through the network as a transport stream (TS), which is defined in MPEG-2 specification [4]. The TS is a type of container used for multiplexing the audio, video and auxiliary data as, for example, information required for synchronization or error correction.

Transport stream is then packetized and encapsulated into the IP packets. MPEG-2 standard distinguishes between two types of TS: single program transport stream (SPTS) and multiple program transport stream (MPTS).

SPTS correspond to transmission of a single TV channel, whereas MPTS allows transfer of more TV channels together within the same TS. The part of MPTS stream is program associated table (PAT), which contains the list of all transmitted TV channels.

From the network point of view, the most important difference between the SPTS and MPTS is the necessary bandwidth for transmission.

As we will see further below, this difference results crucial for the efficiency of the proposed IPTV solution for IPv4/IPv6 environment.

The stated IPTV system additionally contains a server to storage transmitted video files for further use, as well as a network emulator to perform diverse measurements in the IPTV system, such as measurements of QoS metrics experienced by IPTV flows for different (e.g., high load) network conditions.

The IPTV system described above was originally built to work on IPv4 only. Our aim was to migrate it on IPv6 protocol. The first difficulties that we met during this process were related with used IPTV application, which does not cooperate with IPv6.

Problems with applications may hinder the widespread use of IPv6 protocol. Although many applications nowadays are already IPv6-enabled (especially those associated with Linux system [8], the process of adapting some of them to support IPv6 is still pending.

For example, up to year 2009, the MySQL application, a very popular open source database, makes possible the communication over IPv6 protocol between MySQL main programs (mysqld), called MySQL servers, as well as between the MySQL server and the MySQL cluster management server program (ndb mgmd).

Nonetheless, for now the communication between ndb mgmd program and database repositories (the MySQLcluster data node daemon ndbd program) is still IPv4-only aware [5].

In our IPTV system, we replaced the existing IPv4 commercial application by the open-source Video LAN Client (VLC) media player [6]. VLC can handle most of the media codec's and video formats, as well as various streaming protocols.

It permits also to send and receive data using both IPv4 and IPv6 protocols.

Observe that using IPv6 aware application is obligatory at least in these networks, which are natively IPv6-only. VLC cooperates with video LAN manager (VLMa), which is able to manage broad- casts of TV channels from DVB-S or DVB-T sources and streaming audio and video files. Furthermore, VLMa can be used to stream a received unicast stream in multicast way.

The main problem we found during IPv4/IPv6 migration was that the set top box (STB) devices, used to convert IP packet stream into television signal, could not operate with IPv6 protocol. This issue does not affect dream box devices, which work on Linux-based operating system Enigma2. Enigma2, as a large majority of Linux variants, supports IPv6. Moreover, thanks to open source concept of Linux, dream box software can be easily upgraded by users, if need be. Unfortunately, we were not able to modify software in other STB devices. Taking into account that we had many such STB devices, it was not viable to replace all of them in IPv6-compatible equipment.

To solve this, we proposed to divide the network into two sub domains, isolating the devices, which may work on IPv6 and these ones, which may work on IPv4 only.

4.22. Transmission of IPTV Streams on IPv4/IPv6 Environment

Creating two networks, which separate the IPv4 and IPv6 equipment, effects on the MPEG-2 transport stream transferred through the network between dream boxes and end devices.

Now we should send the transport stream twice:

– in IPv4 sub domain, transport stream is encapsulated into IPv4 packets, what is done by dream boxes,
– in IPv6 sub domain the same transport stream is encapsulated into IPv6 packets.

To perform the latter, we propose to use special tool, called the IPv4/IPv6 server. This server is placed at the border between IPv4 and IPv6 networks and has two network cards.

One of them receives multicast IPv4 stream generated by dream box, while the second one is responsible for resending the same stream after encapsulating it in multicast IPv6 packets. Figure 10 presents the concept of resulting network.

Summarizing, the IPv4/IPv6 server works as a gateway between the networks.

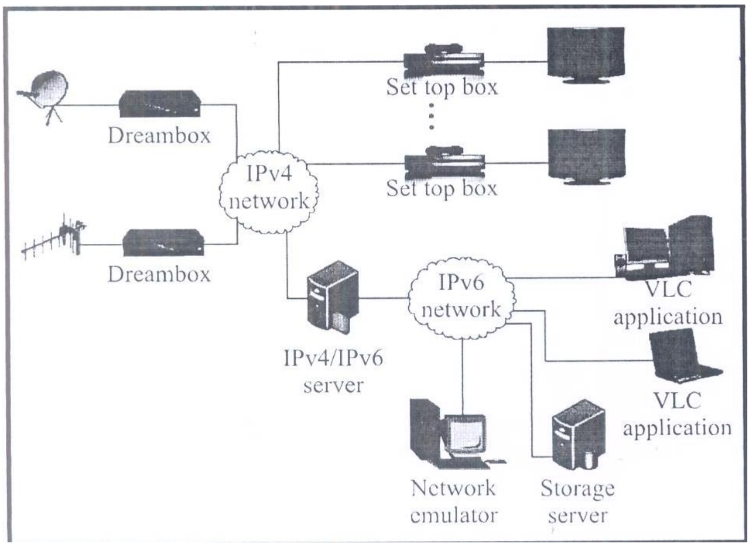

Figure 10. IPTV system in IPv4/IPv6 environment[PTK group]

In the IPv4 domain, the IPv4/IPv6 server acts as an ordinary multicast client, which subscribes to the IPv4 multicast stream in a standard way, using IGMP protocol [7].

On the other hand, in the IPv6 domain, the IPv4/IPv6 server operates as a shared root of distribution tree for an IPv6 multicast group.

We assume that in the IPv6 network the protocol independent multicast sparse-mode (PIMSM) [8] is implemented, which is the most widely used multicast routing protocol because of its independency from underlying unicast routing protocols and overcoming the scalability problems.

In our case the IPv4/IPv6 server plays role of a so-called PIM-SM rendezvous point (RP) for the entire IPv6 domain. An RP can be considered as the meeting place for sources and receivers of multicast data.Setting up the IPv4/IPv6 server as a RP is crucial if there are more routers in the path between the IPv4/IPv6 server and the end IPv6 multicast clients.RFC 3956 defines an address allocation policy (called embedded-RP) in which the address of the RP is encoded in an IPv6 multicast group address.

The document specifies a sub range of unicast prefix-based IPv6 multicast addresses, which starts with FF70::/12 prefix, by setting one of previously undefined bit from flags field to 1. Furthermore, it prescribes a method for embedding the RP address, which serves given multicast group, to IPv6 multicast address of this group.

Thanks to it, there is no requirement for any multicast pre-configuration of the other routers belonging to multicast tree, if they are not operating as an RP, because routers can automatically obtain information about the RP from IPv6 multicast group address.

According to RFC under consideration, we enforce the multicast group address to be FF77:0xxx: aaaa: aaaa: aaaa: aaaa: gggg: gggg,where all the bits “x” together with “a” bits represent the rendezvous point address, whereas “g” bits represent the identifier of the multicast group. For implementation purpose, we notice that our IPv6 multicast group address should be mapped into Ethernet multicast address on the following form: 33:33: gg: gg: gg: gg.Now we illustrate the procedure of establishing multicast connection by one IPv6 host, which wants to receive the IPTV stream generated by the IPv4 dream box. Let us suppose, for the sake of argument, that:

– dream box has the IPv4 address 210.165.23.7,
– the IPv4/IPv6 server has the IPv6 address

FF77:0130:1111:1111:1111:1111:: which enclose the embedded rendezvous point address 1111:1111:1111:1111::1.

Therefore, the embedded-RP multicast prefix is

FF77:0130:1111:1111:1111:1111::/96.

To start receiving the dream box IPTV stream, the IPv6 host should send a multicast listener report message of multicast listener discovery protocol (MLD) to the destination multicast group address FF77:0130:1111:1111:1111:1111:210.165.23.7.

When the IPv4/IPv6 server receives this message, it joins the new host to given IPv6 multicast group. Next, if there was no transmission of multicast data so far (since there was no any IPv6 multicast listener), the IPv4/IPv6 server starts resending the IPTV stream to the joined IPv6 host. Because the IPv4/IPv6 server operates in IPv6 domain as a source of IPTV streams, the IPTV packets will arrive to the IPv6 host with source address of the IPv4/IPv6 server. It means that IPv6 multicast transmission is performed with destination multicast group address:

FF77:0130:1111:1111:1111:1111:210.165.23.7andsourceaddress

FF77:0130:1111:1111:1111:1111::. In this way, different multicast streams from more than one dream box are allowed if they have different IPv4 addresses.

However, resending more IPTV streams by the IPv4/IPv6 server could cause incorrect work because of hardware limitations.

The effectiveness of the IPv4/IPv6 server we study in the next section.

The second investigated approach is when dream box sends IPv6 stream and the server is the responsible to translate the stream into IPv4 as shown in Fig. 11.

In this case the server uses the MLD protocol to join to IPv6 multicast tree in the IPv6 network. On the other hand, in the IPv4 domain, the IPv4/IPv6 server operates as a shared root of distribution tree for an IPv4 multicast group.

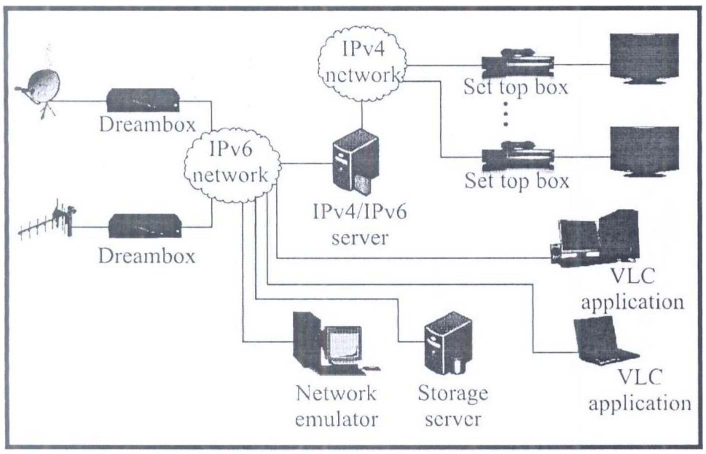

Figure 11. IPTV system in IPv4/IPv6 environment (second approach) [PTK group]

5.0. Effectiveness Study of the Proposed Solutions

In this section we aim at investigating the effectiveness of the IPv4/IPv6 server in both the proposed solutions, i.e., when the server translates IPv4 stream into IPv6 and in the opposite way.In the first approach, we assume that the dream box at the IPv4 domain sends an IPTV packet stream at rate, which increases from one trial to the next. For this purpose the dream box works in MPTS mode.

The MPTS service allows grouping together many TV channels, which may be encoded with standard definition (SD) or high definition (HD) resolution. During the tests, dream box generates one MPTS flow with different number of TV channels, and then the total bandwidth of IPTV stream can be easily obtained as multiplication of bandwidth of the SPTS flow (9.47Mbit/s).

Although we could increase IPTV data rate by simply growing the number of SPTS multicast flows, we believe that the chosen approach imitates better a real IPTV scenario, where one IPTV service provider offers different number of TV channels. Then we monitor whether the IPv4/IPv6 server is able to transfer received IPTV packets to the IPv6 network.

The test run as follows: firstly the multicast tree was created in both IPv4 (using IGMP protocol) and IPv6 domains (using MLD protocol).

5.1. Conclusions and Replication

After gathering all data about technical and demographic parameters I analyzed the case considering research approach mentioned above.

While analyzing the data and facts gathered I concluded which would be the best access technology with regards to population density.

I consider that before massive deployment, short trial period for an area with different geographical relief should be considered with certain equipment vendor.

5.2. Results and Conclusions

To support smooth transition between IPv4 and IPv6 protocols, a set of *good practices* in this direction should be proposed.

In this paper we present a solution for deploying the IPTV system in an scenario which involves presence of two kinds of devices: IPv4-only and IPv6-only.

The proposal exploits special server for transferring IPTV multicast traffic among IPv4 and IPv6 domains.

The proposed solution may be framed as one of these *good practices* because it allows a simple step towards widespread introduction of IPv6.

From the performed experiments we could demonstrate that our IPTV system properly works on IPv4/IPv6 environment. As a consequence, we may conclude that the presented implementation issues are correct.

We implemented two solutions, the first one when the multicast IPv4 stream is translated into multicast IPv6 stream and the second one in the opposite direction. Both the solutions properly worked and showed that they may be valid solutions for the case when IPv4-only and IPv6-only receivers are in the IPTV system.

On the other hand, the obtained results of effectiveness let us to realize that, in case of large bandwidths of IPTV streams, the proposed IPv4/IPv6 server does not properly run and is not capable to transfer the whole incoming IPTV traffic. .

We deliberated that this issue depends on the used hardware but it should be an advice note when one considers using the proposed solution in systems, which demand high bandwidth as classical IPTV does. The effectiveness of the two proposed solutions is similar and it is not possible to conclude which of them behaves better in wide IPTV systems.

Next dream box streamed the DVB-T signal as a unique SPTS in IPv4 multicast mode.

The IPv4/IPv6 server captured the IPTV stream as IPv4 multicast listener, and resent it to the IPv6 end devices in an IPv6 multicast connection. We calculated the rate of packet flow received by the IPv4 network card of the IPv4/IPv6 server (incoming stream) and the rate of packet flow sent by the IPv6 network card (outgoing stream).

The obtained results are presented in Fig.12. After that, we changed SPTS for MPTS flow and repeated the tests for increasing number of TV channels encoded in the stream.

Logically, when MPTS contains more channels, larger bandwidth is necessary to transfer it. In the same way as previously, we calculated the data rate of the incoming stream (to the IPv4/IPv6 server from IPv4 network) and the outgoing stream (from the IPv4/IPv6 server to the IPv6 network).

Figure 12 presents these values.

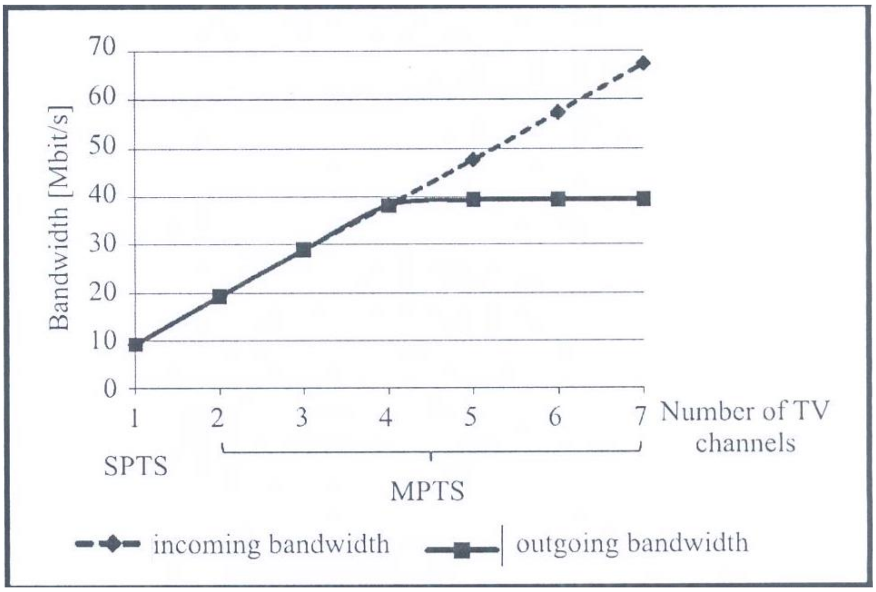

Figure 12 Results of IPv4/IPv6 server's effectiveness [PTK group]

As one can observe, for low rates the IPv4/IPv6 server does not affect resent IPTV stream.

The limit value corresponds to four SPTS flows' bandwidth. Higher rates of IPTV traffic results in packet losses within the IPv4/IPv6 server.

We may indicate that the hardware limitations of the server cause this effect.

The IPv4/IPv6 server was implemented on PC with processor Intel CoreTM2 duo desktop processor E8500 3.16 GHz and Linux operating system with kernel version 2.2.17. Anyway, presented studies show that the proposed solution has limitations.

Certainly, the IPv4/IPv6 server may be used for providing to user a single TV channel (SPTS) as, e.g., a football match in a pay-per-view video service, but the hardware limitations cause that it is not suitable for serving, e.g., the public television, which transmits many TV channels.

In the second approach, we assume that IPTV packet stream is sending by the dream box, which is in this case located in the IPv6 domain.

As in the previous test, the dream box generated IPv6 packets with increasing rate by working in MPTS mode and emitting the same number of channels as described above.
The hardware used to implement the IPv4/IPv6 server was the same one.
The test run similarly to the preceding one, i.e.: firstly, the multicast tree was created in both IPv6 (using MLD protocol) and IPv4 domains (using IGMP protocol).
Next dream box streamed the DVB-T signal as SPTS or MPTS (in consecutive trials) in IPv6 multicast mode. The IPv4/IPv6 server captured the IPTV stream as IPv6 multicast listener, and resent it to the IPv4 set top boxes in an IPv4 multicast connection.
We calculated the rate of packet flow received by the IPv6 network card of the IPv4/IPv6 server (incoming stream) and the rate of packet flow sent by the IPv4 network card (outgoing stream).
The obtained results are presented in Fig. 13.

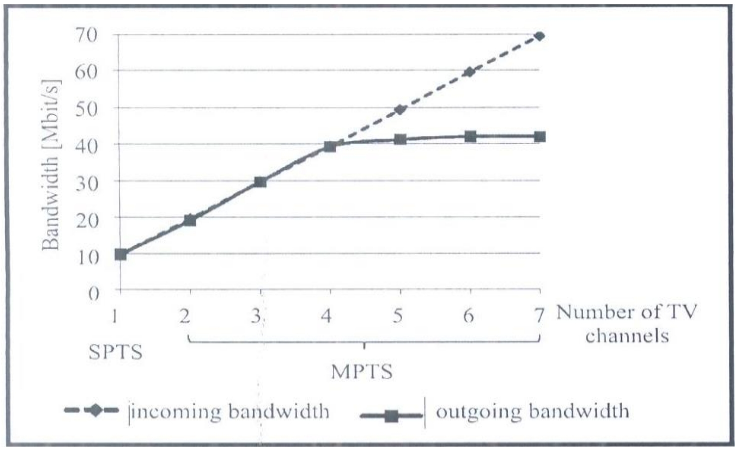

Figure 13. Results of IPv4/IPv6 server's effectiveness (SPTS and MPTS) Second approach [PTK group]

As we may observe in Fig. 12 and Fig. 13, the effectiveness is very similar in both of the approaches. The minimal differences (rather imperceptible in the figures) in favor of the second option could be provoked by the more complexity in sending multicast IPv6 packets than multicast IPv4 packets.

6.0. Reference:

[1] Cisco@2005 - Routing TCPIP, Volume I 2nd Edition By Jeff Doyle CCIE 1919

[2]CCIE Routing and Switching, CISCO Press 2007, 3rd edition By Wendell Odom,

[3]CCIE No.1624,Rus Healy CCIE No. 15025 and contributing author: Naren Mehta CCIE No.9797

[4] Cisco Quality of Service Solutions Configuration guide, release 12.2, 170West Tasman Drive San JOSE, CA 95134-1706

[5] Cisco DQoS – Exam certification guide by Wendell Odom , CCIE No. 1624 and Michael J. Cavanaugh, CCIE No.4516

[6] Batalla, J. M., & Krawiec, P. (2011). On Implementing IPTV Platform with IPv4 and IPv6 Devices. National Institute of Telecommunications,, 31-36.

[7] Watkins, Michael (2008), CCNA Security, *CISCO*

[8] Wallance, Kevin (2011), CCNP TSHOOT 642-832

[9] Teare, Diane (2010). Implementig IP routing *CISCO*

[10] Odom, Wendell (2010) CCNP Route *CISCO*

[11] Bruno, A and Jordan, S (2011) CCDA, *CISCO*

[12] Bieringer, P., Baraldi, F., Piunno, S., Tortonesi, M., Toselli, E., & Tumiati, D. (2013, 06 23*). Current Status of IPv6 Support for Networking Applications. Retrieved February 10, 2014, from http://deepspace6.net/docs/ipv6_status_page_apps.html*

[13] Dream Property GmbH. (2013, 07 17*). Dream. Retrieved February 2, 2014, from dream-multimedia: http://www.dream-multimedia-tv.de/en*

7.0. Appendixes

7.1. Appendix 1

```
! The ipv6 unicast-routing command enables IPv6 forwarding on this router.
! The ipv6 cef command is optional, but it does cause CEF switching of IPv6.
Router1# show run
!lines omitted for brevity
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
! The ipv6 address command lists the global routing prefix and IPV6 subnet 2.
! The /64 means that only the first 64 bits defines the prefix, and the
! eui-64 parameter means that the router should dynamically create the rest of the
! address for the interface. Note that the :: at the end of the address implies
! 3 quartets of 0s, which will be replaced with the EUI-64 interface id.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
interface FastEthernet0/0
mac-address 0200.1111.1111
ip address 172.31.2.1 255.255.255.0
ipv6 address 2001:0:0:2::/64 eui-64
ipv6 ospf 1 area 0
!
! Above, the ipv6 address command does the same thing it did for fa0/0, but this
! time with a subnet value of 3.
!
interface Serial0/1
ip address 172.31.3.1 255.255.255.0
ipv6 address 2001:0:0:3::/64 eui-64
ipv6 ospf 1 area 0
!
! The ipv6 router ospf 1 command creates an IPv6 OSPF process; the command
! was automatically created when the ipv6 ospf 1 area 0 commands were added
! under the fa0/0 and s0/1 interfaces. These two commands enable OSPF on the
! respective interfaces, and identify the OSPF process id and area number.
!
ipv6 router ospf 1
log-adjacency-changes
! Next, the full IPv6 addresses are shown. Note that the interfaces have 2
! addresses; one is the automatically generated link-local address, beginning with
! FE80, used for some protocols on the local link. Note the subnets can be seen
! in the third quartet.
Router1# sh ipv6 int brief
FastEthernet0/0 [up/up]
```

FE80::11FF:FE11:1111
2001::2:0:11FF:FE11:1111
Serial0/1 [up/up]
FE80::11FF:FE11:1111
2001::3:0:11FF:FE11:1111
Virtual-Access1 [up/up]
Unassigned
!
! Below, the ping from R1 to R2's fa0/0 works.
!
Router1# ping 2001::4:0:22FF:FE22:2222
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001::3:0:22FF:FE22:2222, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms