Experimental IPTV and IPv6 Extended Provisioning in a Virtual Testbed

Shuai Qu, Jonas Lindqvist, and Claus Popp Larsen
Netlab
Acreo AB
Hudiksvall, Sweden.
E-mail: {Shuai.Qu, Jonas.Lindqvist, Claus.Popp.Larsen}@acreo.se

***Abstract*—The increasing interest in Internet Protocol Television (IPTV) and Internet Protocol version 6 (IPv6) has driven the need to find a solution to run IPTV and IPv6 outside of a normal public access network. To find new solutions a virtual testbed based on Virtual Private Network (VPN) was built. VPN is a technology that can provide global networking and extended geographic connectivity, also with native security features and good control of the VPN clients. An experimental solution "Virtual Testbed" based on VPN technology to extend provision of IPTV and IPv6 is presented in this paper. This solution allows remote end users over a wider geographical area to participate in IPTV and IPv6 trial since the public network can be used. This also allows researchers an easier access to the test pilots home network and customer premises equipment (CPE), thus makes user behavior research and traffic measurements possible. Evaluation and performance tests on this solution are also illustrated and discussed.**

Keywords - Virtual Testbed, IPTV, IPv6, VPN.

I. INTRODUCTION

IPTV provides digital television services over IP for residential and business users at a lower cost. IPTV is believed to be a killer application for the next-generation Internet and will provide exciting new revenue opportunities for service providers [1]. However, provisioning the IPTV service brings forth significant new challenges [2]. Many commercial IPTV platforms are conventionally deployed on a certain designated network infrastructure with video servers strategically placed. The coverage area of the IPTV network is dedicated. Therefore, it is difficult to distribute IPTV for remote end users who are not part of an IPTV enabled network or in a separate network. It is also costly to operate and extend IPTV at a very big scale. Therefore, a traditional IPTV delivery scheme does not meet these challenges that will be faced in the future, and this drives the need of a solution to extend IPTV provisioning [3].

The amount of home network, as well as the number of services and hosts in them, is increasing. Often the home users cannot get public IPv4 network allocations from service provider and are forced to use Network Address Translation (NAT) to solve connectivity issues to different home services. The need to reach home services from foreign networks has gradually increased as network attached storage, personal video recorders etc. obtain IP connectivity [4]. Therefore, IPv6 is a possible solution to enhance terminal-to-terminal and terminal-to-services connectivity for CPE. It is also beneficial for deep measurement on user behavior and network traffic inside home network in future. Therefore, extended provisioning of IPTV and IPv6 service solution beyond an IPTV-enabled access network, allows for wider access to a "Virtual Testbed" for various test and demonstration purposes. This is extremely useful for our own testbed activities, and we believe it will be of interest to others as well.

Compared to scalabilities, the traditional platform for live experimentation has been physical testbeds: leased lines connecting a limited set of locations [5]. They are more dedicated and are not suitable to extend IPTV provision and IPv6 connectivity for a live experiment.

The Acreo National Testbed (ANT) is built on the fiber infrastructure of the local municipality network "Fiberstaden" in Hudiksvall in Sweden. Commercial and pre-commercial transmission equipment from different vendors has been used to interconnect sites spaced far apart or with high capacity requirements. The broadband access network itself was designed with commercial Layer 2 and 3 equipment (Ethernet switches and Internet routers), also from different vendors [6]. There are around 60 households comprising end-users living in Hudiksvall, and these households are supplied with Internet access and IPTV via Fiber to the Home (FTTH). As a result of geographic limitation, these test pilots are "static" and can only access to network services in ANT locally. It is difficult to extend IPTV and IPv6 services provision to remote users who are not part of ANT network [3]. To address those issues, a *virtual testbed* solution is proposed and has been implemented in a small scale to provide experimental IPTV and IPv6 extended provisioning. More specifically, this paper narrow down to addressing two services issues below:

- Can a solution extend IPTV services provision to users who are not part of a testbed network?
- Can a solution extend IPv6 connectivity to these users as above?

VPN is a generic term that covers the use of public or private networks to create groups of users that are separated from other network users and that may communicate among them as if they were on a private network [7]. VPN can extend geographic connectivity, provide global networking opportunities and reduce operational costs for remote users versus traditional Wide Area Network (WAN). These benefits can facilitate a flexible and cost-effective way to

 ISBN:978-1-61208-113-7

extend IPTV and IPv6 provision. Therefore, IPTV and IPv6 over VPN is an ideal solution to address the issues.

There is also another overlay network technology Peer-to-Peer (P2P), which also can be used for scalable IPTV distribution. P2P does not rely on dedicated network infrastructures and multicast servers. The P2P clients and their connections form an overlay network to exchange video content cooperatively between peers by leveraging their uploading capacity [8]. While P2P network traffic will not fully go into and pass through a specified network, which results in the difficulties in central management, network traffic measurements and some security issues. Comparing to P2P network, VPN network is more centralized and can be configured to make all VPN clients' traffics go through the VPN server. Additionally, VPN uses a flexible user management based on certification system by simple creating or revoking different certificates for different groups of users to achieve users control and authentication. Therefore, VPN solutions are more suitable for our experimental case in this paper than P2P solutions.

Figure 1 illustrates an example of basic IPTV service over VPN. The central office offers IPTV service to different end-users over VPN connections. The IPTV distributions are not constrained by geographic locations.

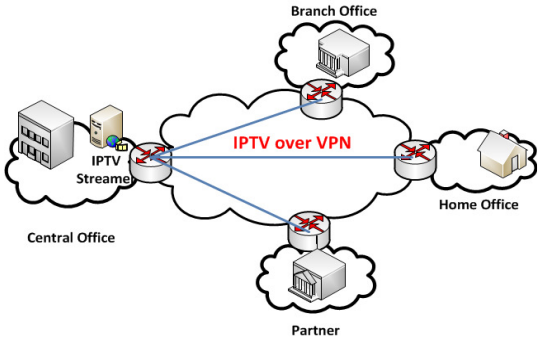

Figure 1. An example of IPTV service over VPN

IPTV over VPN is able to reduce operation costs, transportation costs, provide improved security and better user control [3]. In addition, IPTV over VPN can also provide classified IPTV service features according to geographical groups and customers' demands [9], classified IPTV group services features [9], etc.

One way to provide IPv6 connectivity between end-user sites (when native IPv6 service does not exist) is to use IPv6-over-IPv4 encapsulation (tunneling) between them. The technique encapsulates IPv6 packets within IPv4 so that they can be carried across IPv4 routing infrastructures [10].

Compared to other large virtual testbeds such as PlanetLab [11], our trial is small scale and centralized. The infrastructure is that a VPN network connects one central VPN server, VPN clients and ANT network. Two services, IPTV and IPv6, are running on the same infrastructure. A end user is authenticated with a general client mechanism to be a legal test pilot. Our trial is user-orientated, which provides services directly to end users. This also allows researchers an easier access to the test pilots home network and CPE, thus makes user behavior research and traffic measurements possible.

The contributions in this paper are threefold: 1) One virtual testbed solution is proposed to extend a trial IPTV and IPv6 provision. In principle, people all over world who have broadband connections can access to this virtual testbed and participate in our IPTV and IPv6 services trial over VPN tunnels. 2) The traffic measurements have been performed and the results showed that a VPN solution can provide IPTV and IPv6 with acceptable Quality of Service (QoS) to remote end users. 3) All implementations are built on different kinds of open source software, which makes these services more economical and cost-effective. The rest of this paper is organized as the follows. The proposed scheme is presented in Section 2. Section 3 describes how experiments are designed to implement proposed scheme. Section 4 presents the evaluations and test results. Conclusion is made in Section 5.

II. PROPOSED SCHEME

There are different kinds of VPN technologies, e.g., Point-to-Point Tunnel Protocol (PPTP) VPN, Layer 2 Tunnel Protocol (L2TP) VPN, IPSec VPN and OpenVPN. Those different VPN technologies will be analyzed to find a suitable solution to deliver IPTV and IPv6 over VPN for our case.

A. *State of the Art*

Some standards and specifications about how to deliver IPTV and IPv6 over VPN have been designed. In "MPLS and VPN Architectures Volume II" [12], Chapter 7 "Multicast VPN", defines multicast VPN and introduces some Multicast VPN examples. "Multicast over IPsec VPN Design Guide" [13] was published by Cisco System gives a detailed guide to implement Multicast distribution over IPsec VPN network based on Cisco switches and routers. The Internet Draft "Multicast in MPLS/BGP IP VPNs" [14] was written by engineers at Cisco and describes the MVPN (Multicast in Border Gateway Protocol (BGP)/Multi-Protocol Label Switch (MPLS) IP VPNs) solution with Cisco equipment. "ITU-T IPTV Focus Group Proceedings" [9] promotes the global IPTV standards. In other aspect part of the standards, the Work Group (WG) 3 has identified some requirements on Multicast VPN in IPTV network Control and Multicast VPN Group Management aspect. The Internet Standards Track "Transition Mechanisms for IPv6 Hosts and Routers" [15] describes the "IPv6-over-IPv4 tunneling" technologies and transition mechanism for IPv6. For these IPTV VPN solutions, some standards focus on MPLS VPNs, which needs at least backbone networks to support MPLS. Some solutions use IPSec VPN, which requires specific vendor's hardware or software, for example, Cisco System to deploy. So those solutions are not so flexible and open to set up for our experiment.

B. *Possible VPN solutions for IPTV VPN*

To find out the most suitable VPN solution, comparisons between different VPN technologies are made as shown below.

 ISBN:978-1-61208-113-7

- From security perspectives, 1) PPTP VPN is vulnerable to man-in-the middle attack and weak in authentication. 2) For lack of confidentialities, L2TP is often implemented with IPSec for data confidentiality. 3) OpenVPN offers the same security functions and features as IPSec does. The IPSec protocol is implemented as a modification of the IP stack in the kernel stack. But the kernel interactions add security risks on the Operation System (OS) [16].
- For packet overhead, IPSec adds an extra size byte to the original packet, which needs more overhead compare to OpenVPN [17].
- For easy usage, the kernel-space based IPSec requires independent implementation for every OS. The user-space based OpenVPN is much easier to be ported to other OS
- For NAT traversal compatibility, OpenVPN only uses one single port for communication, which is extremely firewall-friendly. The Authentication Header's (AH) source address checking mechanism makes IPSec incompatible with the NAT traversal.
- From multicast support perspective, OpenVPN can natively support multicast while IPSec needs to combine the Generic Record Encapsulation (GRE) tunnel to support multicast. The IPSec Direct Encapsulation only supports unicast IP. IP multicast (IPmc) is not supported with IPSec Direct Encapsulation. IPSec was created to be a security protocol between two and only two devices, so a service such as multicast is problematic. An IPSec peer encrypts a packet so that only one other IPSec peer can successfully perform the de-encryption. IPmc is not compatible with this mode of operation [13].
- In addition, IPSec services usually require third-party hardware or software while OpenVPN is open source software, which makes it very cost-effective.

OpenVPN is an open source and user space tunneling package. OpenVPN uses the OpenSSL library to provide encryption of both the data and control channels [18]. Additional benefits of using OpenVPN are:

- tunnel any IP sub-network or virtual Ethernet adapter over a single User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) port [19],
- multiple load-balanced VPN servers farm, which can handle thousands of dynamic VPN connections,
- use security features of the OpenSSL library to protect network traffic,
- use real-time adaptive link compression and traffic-shaping to manage link bandwidth utilization [19]

One problem of OpenVPN is that OpenVPN is mostly a software-only product until now and it is not found in any hardware applications. Although IPSec is supported by most vendors and can be found in the hardware applications (Routers, Firewalls, etc), incompatibilities between different vendors make IPSec painfully difficult to setup. Another problem of OpenVPN is that it is a user-space program using OpenSSL crypto library. OpenVPN handles data packets based on the TCP/UDP tunnel and TUN/TAP virtual network interface. Therefore, OpenVPN is heavier than IPSec in terms of performance. In summary, OpenVPN is a more suitable VPN solution to deploy multicast service over VPN than the others.

C. *IPv6-over-IPv4 tunnelings*

The tunneling concept is to encapsulate an IPv6 packet as the payload of an IPv4 packet [20]. The IPv4 Protocol field is set to type 41 to indicate an encapsulated IPv6 packet. An IPv4 header with Source and Destination IPv4 addresses is added in front of IPv6 packets. The Source and Destination addresses are set to the tunnel endpoints IPv4 addresses. The tunnel endpoints can be manually configured or automatically derived from the sending tunnel interface and the next-hop address of the matching routing for the destination IPv6 address in tunneled packet, so that IPv6 packets can be sent over the IPv4 infrastructure. Figure 2 illustrates that an example of encapsulating IPv6 in IPv4 packet.

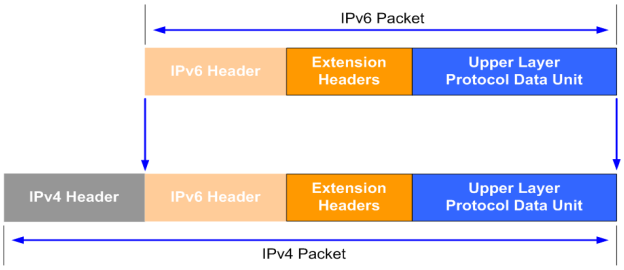

Figure 2. An example of encapsulating IPv6 in IPv4 packet

The IPv6-over-IPv4 tunneling technology also applies to OpenVPN tunnels. Point-to-point IPv6 tunnels are supported on Operating Systems, which have IPv6 TUN driver support (this includes Linux and the BSDs). IPv6 over TAP is always supported as is any other protocol, which can run over Ethernet [21].

III. EXPERIMENTAL SETUP

The experimental implementation is based on ANT infrastructure, which is described in Part I Introduction. The experimental IPTV and IPv6 virtual testbed was built on ANT network infrastructure and designed as shown in Figure 3.

A. *IPTV and IPv6 VPN testbed layout description*

The following descriptions are all related to Figure 3.

- Number 1, IPTV system Hudiksvall.
- Number 2, Acreo Hudiksvall Router: this router is the core router of the ANT project in Hudiksvall.
- Number 3, VPN Server: the VPN Server is linked up together over a VPN tunnel with the VPN individual clients or home gateway. Different open source software was installed on this server. Together with the core router, the VPN server provides IPv4, IPv6, VPN and multicast services to VPN clients.

 ISBN:978-1-61208-113-7

- Number 4, The Public Network.
- Number 5, Home Gateway: the home gateway is physical placed between the VPN server and home network and running on an open source routing platform – OpenWRT [22]. The gateway plays four roles: 1.A VPN client to establish VPN connections. 2. An Internet Group Management Protocol (IGMP) proxy [23] to provide multicast routing. 3. A Router Advertisement Daemon (radvd) [24] to provide IPv6 stateless auto configuration. 4. A home gateway to provide home networking.
- Number 6, Individual VPN clients: the laptops installed the VPN client program.
- Number 7, Different clients inside home network
- Number 8, The IPv6 network
- Number 9, The KAME project (www.kame.net) Server: an IPv6 project named KAME and the server can provide an IPv6 connectivity test.

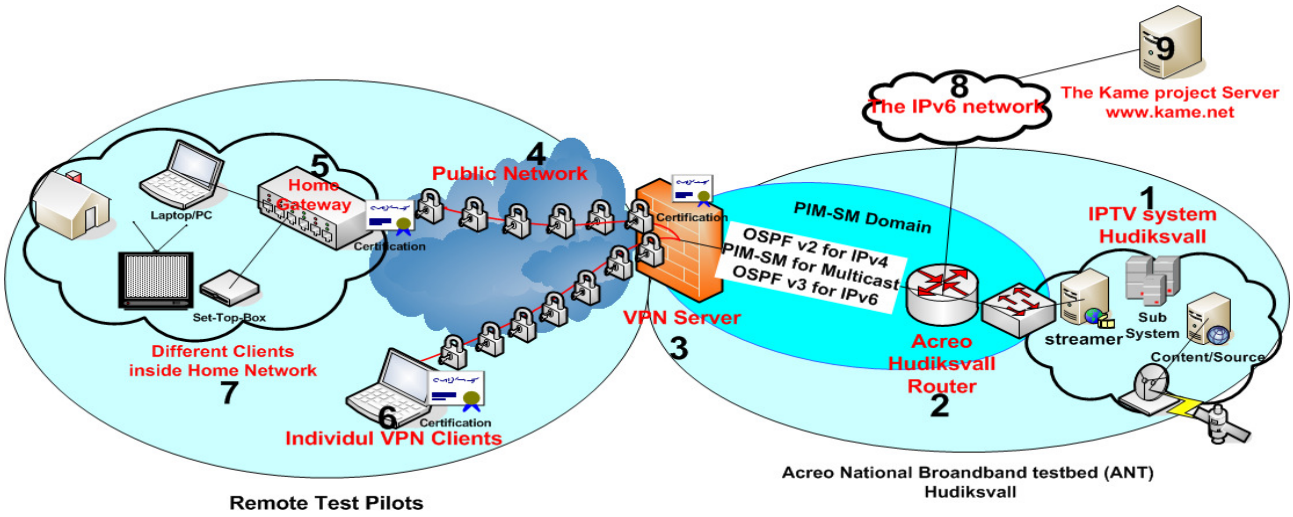

Figure 3. IPTV and IPv6 VPN testbed layout.

There are mainly two implementations: IPTV VPN and IPv6 VPN.

For IPTV VPN, OpenVPN was set up to provide VPN services; Open Shortest Path First version 2 (OSPFv2) was implemented to provide unicast routing; Protocol Independent Multicast - Sparse Mode (PIM-SM) was built up to provide multicast routing; Home gateway was developed to support gateway-to-gateway VPN connections. The home gateway was built on an embedded Linux box with different open source software installed, to establish an automatic VPN connection to the VPN server. In that way IPTV and Internet connections can be provided to the end users in home networks.

The IPTV VPN starts up as follows. For host-to-gateway connections, a laptop with a VPN client program configured connects to Acreo's own VPN server. The server will then set up an IPv4 VPN-tunnel between the server and client. The laptop will then obtain a public VPN IP address via the Dynamic Host Configuration Protocol (DHCP) service, which the VPN server provides. The OSPF v2 and PIM-SM routing protocol are running between the VPN server and Acreo Hudiksvall Router. The internet traffic is routed over the tunnel via the VPN server to the Acreo Hudiksvall Router. The multicast traffic from the source in the IPTV system Hudiksvall is routed via the Acreo Hudiksvall Router (the Rendezvous Point (RP) in the PIM-SM domain) to the VPN server (PIM-SM enabled) over a VPN-tunnel to the client. The differences between the gateway-to-gateway and host-to-gateway VPN connection is the home gateway play three roles of VPN client, IGMP proxy and normal home gateway.

For IPv6 VPN implementations, IPv6-over-IPv4 tunneling and OSPFv3 were implemented to provide IPv6 connectivity and unicast routing. The IPv6 VPN start-up procedure is as follows. For host-to-gateway connections, an end-user's laptop starts up the VPN client program, which automatically establishes an IPv4 based VPN tunnel to the server. The client is manually configured an IPv6 address with the gateway pointed to the VPN server to establish an IPv6-over-IPv4 VPN between the client and server. The IPv6 traffic will then be routed via the OSPFv3 protocol running between VPN server and Acreo Hudiksvall Router to the IPv6 network.

For gateway-to-gateway connection, besides setting up an IPv6 connection from home gateway to the VPN server, the home gateway also provides IPv6 home networking by using radvd. This daemon can listen to router solicitations (RS) and answer with router advertisement (RA). These RAs contains information, which is used for hosts to configure their interfaces and includes IPv6 address prefixes, the link Maximum Transmission Unit (MTU) and default routers information. With the help of radvd, a PC or laptop with IPv6 stack installed is able to automatically configure its interface to appropriate IPv6 address. Any global IPv6 address can be pingable from this home gateway and any IPv6-enabled host in home network. In our trial, only IPv6

 ISBN:978-1-61208-113-7

unicast is deployed. IPv6 multicast is out of scope of this experiment concerns and will not be discussed here.

IV. MEASUREMENTS AND ANALYSIS

Some measurement instruments and methods were used to evaluate the QoS of IPTV and IPv6 over VPN connections. IPTV testing was conducted by one professional IPTV measurement system - Agama Analyzer [25]. VPN connection qualities were measured by two websites, which are world widely-used for broadband speed and quality test. In summary, three test activities shown as below were conducted.

- Evaluate VPN services qualities.
- Compare IPTV over VPN and normal IPTV service qualities.
- A simple test on IPv6 connectivity.

A. *VPN service qualities measurements*

OpenVPN utilizes different cryptographic algorithms to achieve user authentication, authorization, network data confidentiality and integrity. Therefore, as the carrier tunnels for IPTV and IPv6, the QoS impact to the services due to VPN encryption need to be quantified due to its importance to the service quality for distributed users. Fortunately, OpenVPN is flexible to be configured to enable and disable these security options for measurements.

The experiments were conducted on one OpenVPN server and one OpenVPN client as follows, interconnected with high-speed backbone network with capacity above 1 Gbps spanning about 300km.

OpenVPN Server:

1. SUSE Linux Enterprise Server 10 SP2 (x86_64) (Kernel 2.6.16.60-0.21)
2. 2*Intel Xeon(TM) 3.00GHz 64bit CPU, 1GB RAM
3. 2*NIC 10/100/1000M bps, 100 Mbps Switching
4. OpenVPN 2.1_rc18

OpenVPN Client:

1. Windows 7 Professional, 2*Intel Core(TM)2 Duo CPU P8600 2,4 GHz, 4G RAM.
2. NIC 10/100/1000M bps, 100 Mbps Switching
3. OpenVPN 2.1_rc22 and OpenVPN GUI 1.03
4. The Global Broadband Speed and Quality Test websites: speedtest.net and pingtest.net.

Mission-critical IPTV service quality requires sufficient network bandwidth to assure delivery without loss, low network delay and so on. So the following parameters will be measured: network bandwidth, network delay and network capacity loss. The general testing scenario for a VPN client is as following. A Laptop/PC installed an OpenVPN client remotely connect a VPN Server. After establishing VPN tunnel, the client uses speedtest.net and pingtest.net to measure network quality. The OpenVPN server runs in two modes—either over UDP or TCP. The UDP mode is preferred due to better performance, as the UDP mode is not limited by the TCP congestion control algorithm [26][27]. In particular, UDP based VPN for real-time multicast communication shows minimum impact on traffic and slight CPU requirement increase comparing to TCP based VPN mode [27]. Therefore, UDP based VPN mode, with six different options combing a number of network QoS critical parameters, was chosen to conduct the measurements. Since OpenVPN requires extra management, which could lead to a capacity reduction, so option 1 in Table I is defined as original network connection case to measure and compare network capacity loss. In addition, encryption will increase OpenVPN traffic overhead and compression will influence data transmission efficiency [17]. Therefore, from option 2 to option 5 is different combination of those options to measure and verify which option wins the best QoS.

The test case 1 and test case 2 were performed ten times. Two example results checking against speedtest.net and pingtest.net separately are shown in Figure 4 and Figure 5. The two test cases measurement values are presented in Table I as below.

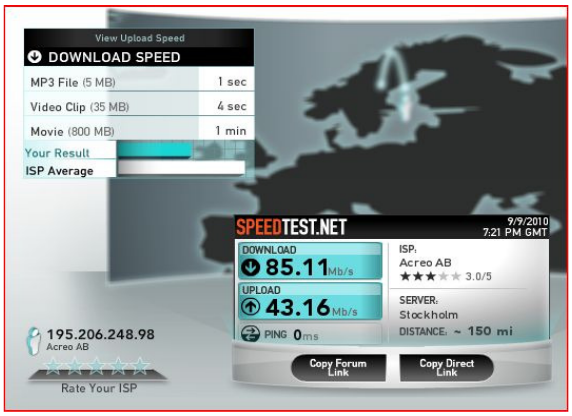

Figure 4. The test case 1, network bandwidth check against speedtestb.net

Figure 5. The test case 2, network delay check against pingtest.net

The VPN service connectivity benchmark results can be summarized as follows. 1) The VPN network requires extra management overhead, which leads to a bandwidth reduction. In Table I, comparing to option 1 results, network bandwidth under other options shows that the VPN network bandwidth loss rate is approximate 26%--32%. 2) For network delay, the data compression "comp-lzo" option can

reduce VPN network delay while the security options worsen the network delay. In Table I, the VPN connection without security options but with data compression enabled is the winner in all tests. The VPN connection with all security options shows rather larger network delay (average 38.35ms). The mission-critical IPTV service requires low network delay and high real-time multicast traffics. However, encryption of multicast streaming will consume system resource and give negative impact on the service QoS. If there is no confidentiality requirement for multicast streaming, then authentication of both communication parties, to some extent, is able to ensure IPTV security. The consumption of system resource is accordingly reduced and the services performance could be improved.

TABLE I: BANDWIDTH CONNECTIVITY TEST RESULTS FOR UDP-BASED VPN MODE WITH DIFFERENT VPN SERVER OPTIONS. HMAC STATNDS FOR "HASH MESSAGE AUTHENTICATION CODE"

	Option 1	Option 2	Option 3	Option 4	Option 5	Option6
VPN connections		x	x	x	x	x
Encryption		x	x			
Integrity check with HMAC		x		x		
Data compression		x	x	x	x	
Average Download Speed	84.15Mb/s	59.48Mb/s	59.72Mb/s	62.09Mb/s	59.78Mb/s	61.45Mb/s
Average Upload Speed	42.56Mb/s	30.83Mb/s	31.94Mb/s	33.04Mb/s	31.98Mb/s	33.45Mb/s
Average Network Delay	13.01ms	38.35ms	20.47ms	24.44ms	16.23ms	17.36ms
Maximum Download Speed	88.75Mb/s	61.84Mb/s	62.32Mb/s	65.38Mb/s	66.82Mb/s	67.18Mb/s
Maximum Upload Speed	47.72 Mb/s	31.45 Mb/s	32.84 Mb/s	35.13Mb/s	35.44 Mb/s	36 Mb/s
Shortest Network Delay	8ms	8.9ms	8.7ms	8.65ms	8.77ms	8.56ms

B. IPTV VPN service qualities

IPTV service qualities comparisons between IPTV VPN and normal IPTV had been done with this Agama instrument – Agama Analyzer. The measurement is based on the network setting up shown in Figure 6. The client is a laptop without OpenVPN client installed. The switch is 10/100M Fast Ethernet Switch. Agama Analyzer is connected to switch with two clients together to measure IPTV QoS. The further descriptions of other components and service scenarios in Figure 6 can be referred to Part III Experiment Setup Section A. During the experiment, the following parameters were used to qualify the QoS provided [28].

- Packet loss is measured as the portion of packets transmitted but not received in the destination compared to the total number or packets transmitted.
- Packet Jitter is often used as a measure of the variability over time of the packet latency across a network [29]. A bigger number of packet jitter value means larger packet latency.

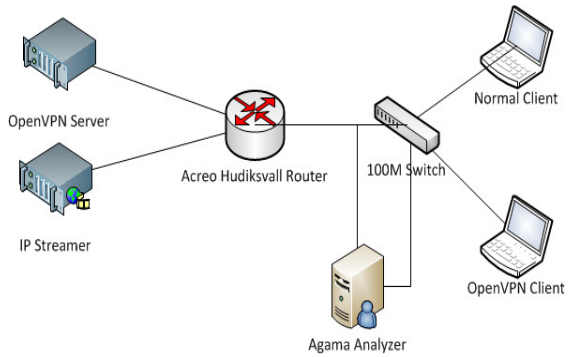

Figure 6. Testbed for IPTV VPN and normal IPTV comparisons

Figure 7, Figure 8 and Figure 9 show that the test results that one IPTV channel with Bitrates around 4Mbit/s from the same streamer was measured by Agama Analyzer during 72 hours (from 2009-05-29 8:00 to 2009-06-01 8:00). The results are summarized as follows: 1.Connection without VPN network bandwidth of 64Mbit/s downstream and 38Mbit/s upstream were achieved. VPN connection network bandwidth of 37Mbit/s downstream and 16Mbit/s upstream were achieved. 2. Over a three days period no noticeable signs of distortion were visually observed by human monitoring.

The Packet Jitter measurement results from Figure 8 and Figure 9 are summarized and presented in Table II as below:

TABLE II: THE PACKET JITTER MEASUREMENT RESULTS FROM AGAMA ANALYZER

	normal wired lines	VPN
Average Packet Jitter	6.1ms	9.6ms
Maximum Packet Jitter	10.1ms	42.3ms

Although there are many suggested video quality metrics with varying degree of performance, most of the more well known e.g., Video Quality Metric (VQM) [30] require access to the original undistorted reference i.e., full reference or reduced reference metrics, which are not in general available. The methods that do not require such access i.e., no-reference metrics have not performed good enough to be standardized. Still we wanted to get on estimate of the performance of the transmission of the IPTV over the VPN connection. The Agama Analyzer analyzes the video stream for consistency and completeness according the codec standard. From this inferences about the likely quality of the transmitted IPTV could be made. They are classified in three levels by the Agama Analyzer. No errors found, which means that the video have the same quality as when it was transmitted. Minor errors found, which will have just minor impact on the quality and then major errors found, which also will have substantial impact on the quality. According to the Agama measurement results, the IPTV has only suffered minor distortions over VPN connections and has only degraded slightly.

 ISBN:978-1-61208-113-7

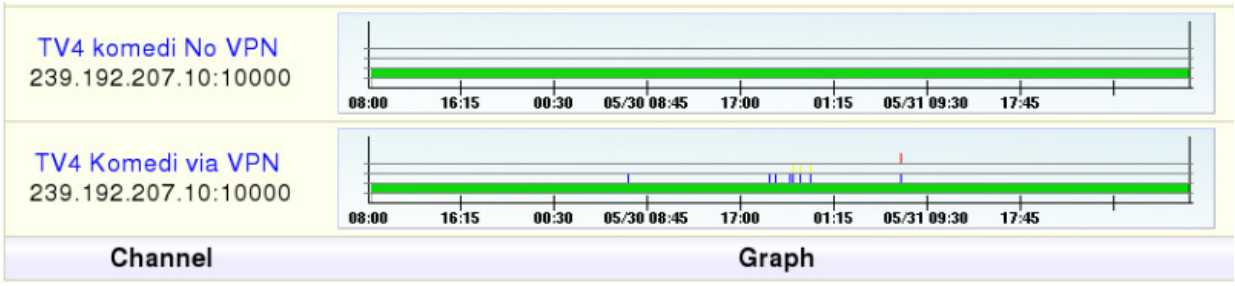

Figure 7. SVT TV4 Komedi channel measuring graph by Agama Analyzer from 2009-05-29 8:00 to 2009-06-01 8:00. Green=OK, Blue=minor distortion, Yellow=major distortion, Red=Packet loss. During the same time, the TV is delivered over the connections without VPN and with VPN connection separately.

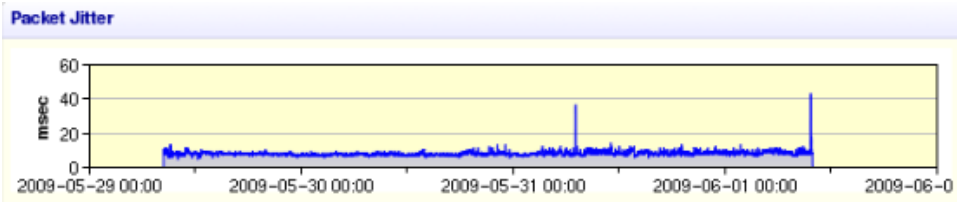

Figure 8. SVT TV4 Komedi channel Packet Jitter measurement results with no VPN connections from Agama Analyzer.

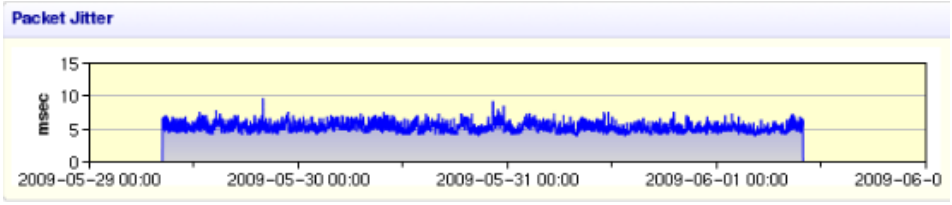

Figure 9. SVT TV4 Komedi channel Packet Jitter measurement results with VPN connection from Agama Analyzer.

C. *IPv6 connectivity measurements*

Based on IPv6 VPN experiment setup described in Part III, with the help of KAME project server with IPv6 enabled, a simple IPv6 trace route test was performed. A VPN client manually configured with an IPv6 address trace route against www.kame.net. In this paper only network connectivity is concerned, and the IPv6 network quality in terms of packet loss, network delay is not considered here. The result is shown in Figure 10.

The result shows that IPv6 packets were successfully routed from a VPN client over an IPv6-over-IPv4 tunnel to the IPv6 network, and the packets traversed the IPv6 network via the IPv6 enabled network nodes hop by hop to the destination.

V. CONCLUSION AND FUTURE RESEARCH

In this paper, a VPN solution is designed and implemented to realize a "Virtual Testbed", which can extend trial provisioning of IPTV and IPv6 spanning a wider geographical area to remote end users at a lower network operation cost. This is very useful for our testbed activities, which have so far been confined to reach test pilots within the municipality of Hudiksvall open city network. The proposed schema uses proven and standardized technologies, with open solutions and open-source software. This solution makes it very cost-effective and commercially applicable, for potential providers who wants to extend their services. The results of the evaluation showed acceptable service QoS. However, it should be aware that this VPN solution is not always the best solution due to an approximate 30% network capacity reduction. But VPN is still a good way or in some case the only solution to extend IPTV service provision with a centralized network infrastructure. Meanwhile, IPv6 connectivity can also be extended over this VPN infrastructure to achieve good terminal-to-terminal and terminal-to-services connectivity. So with the help of this solution, a virtual testbed can have more scalable access from dynamic test pilots and provide an attractive and extendable platform for IPTV and IPv6 services provision and experimentation.

As part of future work, we intend to conduct pressure and load testing to improve and further optimize performance of our system. We plan to more thoroughly investigate the VPN processing performance with multiple streams over many geographically distributed clients. In addition, our future research also includes VPN connection improvement on a

 ISBN:978-1-61208-113-7

high performance. We expect such extended research work will be able to make our solutions even better.

ACKNOWLEDGMENT

The authors acknowledge the EU Regional development Funds for supporting this work through the project "Acreo National Testbed, phase 2" (ANT2)

REFERENCES

[1] Y. Xiao, X. Du, J. Zhang, and F. Hu, "Internet Protocol Television (IPTV):The Killer Application for the Next-Generation Internet," IEEE Communications Magazine, vol. 45, no. 11, pp. 126 - 134, Nov, 2007.

[2] R. Jain, "I want my IPTV," IEEE Multimedia, vol. 12, no. 3, pp. 96, 2005.

[3] S. Qu and J. Lindqvist, "Scalable IPTV Delivery to Home via VPN," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 40, Part 10, pp. 237-246, 2010.

[4] K. Huhtanen, B. Silverajan, and J. Harju, "Utilising IPv6 over VPN to Enhance Home Service Connectivity," Terena 2007 Special Issue of the Journal of Campus-Wide Information Systems Vol 24 No 4 pp. 271-279.

[5] L. Peterson, S. Shenker, and J. Turner In Third Works, "Overcoming the Internet Impasse through Virtualization," in Third Workshop on Hot Topics in Networks (HotNets-III), Nov. 2004.

[6] C. P. Larsen, R. Flodin, C. Lindqvist, R. Lindstrm, H. Pathirana, and A. Gavler, "Experience with IPTV in the Testbed," Acreo Broadband Communication Project report Y2002-Y2006: Dec. letter 2004-01780, Acreo AB, pp. 18 – 27, January 31st 2007.

[7] L. Andersson and T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology," Internet Request for Comments RFC 4026, March 2005.

[8] X. J. Hei, C. Liang, J. Liang, Y. Liu, and K. W. Ross, "A Measurement Study of a Large-Scale P2P IPTV System," IEEE Transactions on Multimedia, vol. 9, no. 8, pp. 1672 – 1687, Dec. 2007

[9] ITU-T, "ITU-T IPTV Focus Group Proceedings," pp. 389 – 390, 2008.

[10] B. Carpenter, B. Fink, and K. Moore, "Connecting IPv6 Routing Domains Over the IPv4 Internet," The Internet Protocol Journal, vol. 3, no. 1, pp.2-10, March 2000.

[11] PlannetLab, http://www.planet-lab.org/, 10.11.2010.

[12] I. Pepelnjak, J. Guichard, and J. Apcar, "MPLS and VPN Architectures Volume II," *Cisco Press*, pp. 333 – 387, 2003.

[13] "Multicast over IPsec VPN Design Guide," www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PNIPmc.html , 11.11.2010.

[14] E. Rosen, Y. Cai, and J. Wijsnands, "Multicast in MPLS/BGP VPNs," Internet Draft, August 18, 2009.

[15] R. Gilligan and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers (RFC 2893)," IETF, August, 2000.

[16] C. Hosner, "OpenVPN and the SSL VPN Revolution," SANS Institute, pp.10, Aug 2004.

[17] A. Alshamsi and T. Saito, "A Technical Comparison of IPSec and SSL," 19th Intl. Conf. on Advanced Information Networking and Applications (AINA'05), vol. 2, pp. 392–395, Mar. 2005.

[18] D. H. Ryu and S. H. Nam, "Implementation of wireless VoIP system based on VPN," Proc. The 7th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications, Cambrige, UK, Feb. 2008.

[19] "What is OpenVPN," http://www.openvpn.net/index.php/open-source/333-what-is-openvpn.html, 11.11.2010.

[20] D. C. Lee, D. L. Lough, S. F. Midkiff, N. J. Davis and P. E. Benchoff, "The Next Generation of the Internet: Aspects of the Internet Protocol Version 6," IEEE Network, January/February 1998, pp. 28 - 33.

[21] "Is IPv6 support planned/in the works?" http://openvpn.net/index.php/open-source/faq/77-server/287-is-ipv6-support-plannedin-the-works.html, 10.11.2010.

[22] OpenWrt – Wireless Freedom, http://www.openwrt.org, 11.11.2010.

[23] C. Cho, I. Han, Y. Jun and H. Lee, "Improvement of Channel Zapping Time in IPTV Services Using the Adjacent Groups Join-Leave Method," Advanced Communication Technology, the 6th International Conference on, Vol. 2, pp. 971 – 975, 2004.

[24] P. Vidales, G. Mapp, F. Stajano, J. Crowcroft, C.J. Bernardos, "A Practical Approach for 4G Systems: Deployment of Overlay Networks," *TRIDENTCOM'05*, pp. 172 – 181, 2005.

[25] Agama Analyzer, Agama Technologies AB, Box 602, SE-581 07 Linkoping, Sweden, 2010.

[26] V. Jacobso, "Congestion avoidance and control," ACM SIGCOMM '88, Stanford, CA (1988) 314–329

[27] P. Holub, E. Hladka, M. Prochazka, M. Liska, "Secure and Pervasive Collaborative Platform for Medical Applications," IOS PRESS, Studies In Health Technology and Informatics, 2007, VOL 126, pp. 229-238.

[28] IP Performance Metrics (IPPM) Working Group, IETF, http://www.ietf.org/html.charters/ippm-charter.html, 11.11.2010.

[29] D. H. Wolaver, "Phase-Locked Loop Circuit Design," Prentice-Hall, ISBN 0-13-662743-9, pp. 211-237.

[30] M. Pinson and S. Wolf, "A New Standardized Method for Objectively Measuring Video Quality", IEEE Transactions on Broadcasting , vol. 50, Issue. 3, pp. 312-322 , Sept. 2004.

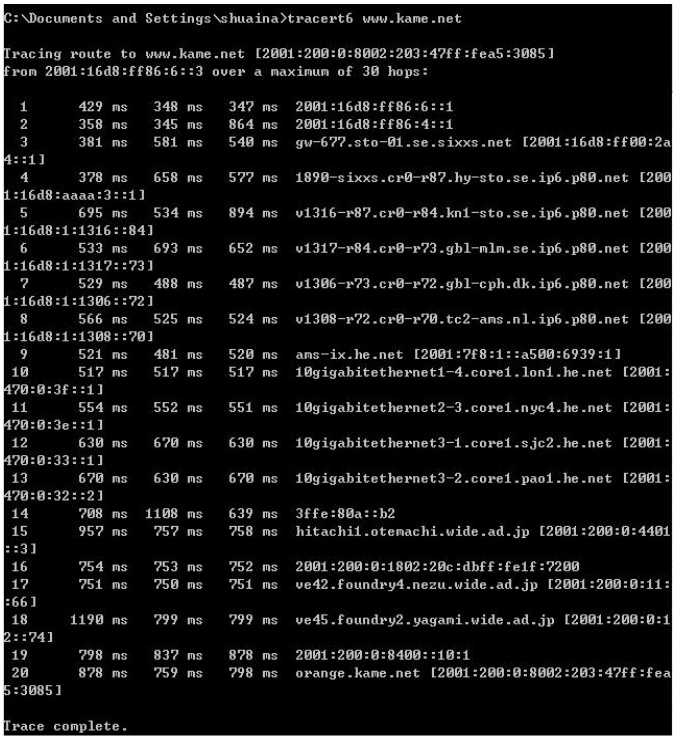

Figure 10. The IPv6 trace route check against www.kame.net