

Scalable IPTV Delivery to Home via VPN

Shuai Qu and Jonas Lindqvist

Acreeo, NetLab,
Håstaholmen, 4, 82412 Hudiksvall, Sweden
{shuai.qu, jonas.lindqvist}@acreeo.se

Abstract. The significant interest in IPTV drives the needs for flexible and scalable IPTV delivery way, especially when distributing IPTV service to end-users who are in a separate network or not in an IPTV enabled network. The recent popularity of VPN has made scalable distribution of IPTV possible. VPN can provide global IPTV networking opportunities and extended geographic connectivity. Additionally, the native traits of VPN also provide secure and controllable service features to IPTV. This paper addresses one important area related to IPTV distribution, namely scalability. We present a novel solution to distribute IPTV via VPN to remote end-users over public networks. The solution allows end-users over a wider geographical area to get IPTV service, and it also reduces operating costs. Traffic measurements and evaluation of services performance are also illustrated and discussed in this paper.

Keywords: IPTV, VPN, scalability.

1 Introduction

1.1 Background and Problem Motivations

Internet Protocol Television (IPTV) [1], [2] is a system where a digital TV service is delivered to end-users by using IP over a network infrastructure. IPTV is now gaining popularity very rapidly, Informa Research [3] state that the market will grow by a factor of seven by 2011 based on the 2006 numbers. The significant interest in IPTV services and wholesale business models are driving the need to consider more scalable ways to deliver multicast services[4]. Generally, IPTV platform has been physical platform: leased lines connecting a limited set of locations. The coverage areas of IPTV service are dedicated and depend on network infrastructure built for IPTV distributions. It is therefore difficult to make IPTV service globally available for remote users who are in a separate network or not part of IPTV enabled network. In addition, it is also quite expensive to extend and operate IPTV at very large scale. Therefore, traditional IPTV scheme do not address the challenges that will be faced in the future and that will drive the need of flexible IPTV delivery.

One IPTV platform is in Acreeo's National Testbed (ANT) for broadband [5], which is physically built on the fiber infrastructure of the local municipality network in Hudiksvall in Sweden, Fibstaden. There are around 60 households

comprising end-users living in Hudiksvall, and they are supplied with IPTV via Fiber to the Home (FTTH). As a result of geographic limitation, IPTV service in ANT is only locally accessible. It is also costly to extend and operate ANT a wider geographical area. Thus, IPTV service in ANT is typically of small geographic extent and cannot meet the scalability requirements in future.

To address the problems mentioned above, IPTV VPN is proposed to addresses one area related IPTV distribution, namely scalability. And this solution has been implemented and tested in a small scale field trial. With the help of this novel solution, IPTV is distributed to remote end-users who are not part of ANT network via VPN over public networks, and to therefore provide a path for scalable IPTV service to be globally delivered. 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 [6]. VPN can extend geographic connectivity, provide global networking opportunities, reduce operational costs versus traditional WAN and transit time and transportation costs for remote users. These main VPN benefits can facilitate connections to an IPTV platform, and remote end-users can enjoy IPTV in a scalable way and at a low cost. Therefore, IPTV VPN is an ideal way to tackle the scalability issue of IPTV distribution.

1.2 Related Work

Some standards and specifications about IPTV VPN have been designed and released. "ITU-T IPTV Focus Group Proceedings" [7] 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 Draft "Multicast in MPLS/BGP IP VPNs" [8] was written by engineers at Cisco and describes the MVPN (Multicast in Border Gateway Protocol (BGP)/Multi-Protocol Label Switch (MPLS) IP VPNs) solution of Cisco Systems. The "MPLS and VPN Architectures Volume II" [9], in Chapter 7 Multicast VPN, defines a few multicast VPN concepts and introduces some detailed examples. For these VPN solutions, most standards focus on MPLS VPNs which need in distribution and core networks to support MPLS. However, delivery of IPTV over an MPLS-enabled network cannot be done in an especially scalable way. To ensure interoperability among systems that implement this VPN architecture using MPLS label switched paths as the tunneling technology, all such systems MUST support Label Distribution Protocol (LDP) [MPLS-LDP] [10]. The scheme presented in this paper is built on a variety of networks using IP, which is much easier to implement and distribute IPTV to remote end-users.

1.3 Contributions

The contributions in this paper are threefold: 1) One novel solution - IPTV VPN is proposed and implemented to provide a scalable IPTV delivery way. As long as the bandwidth is sufficient, it is possible for people who have broadband

connections to get IPTV service via the Internet all over world. 2) The traffic measurements had been performed, and the results showed that a VPN solution can provide IPTV with acceptable Quality of Service (QoS) to remote end-users. 3) All implementations are built upon different kinds of open source software, which makes the service more scalable and extendable. The rest of this paper is organized as the follows. The proposed scheme is presented in Section 2. Section 3 describes experiments designed to implement proposed scheme. Section 4 presents the performance evaluations and test results. Concluding remarks are made in Section 5.

2 Proposed Scheme

2.1 OpenVPN

In our proposed scheme, OpenVPN [11] is used to provide VPN tunnels from ANT network to remote end-users, and then IPTV is delivered to remote end-users over the VPN tunnels.

OpenVPN is a full-featured open source Secure Socket Layer (SSL) VPN solution that accommodates a wide range of configurations, including remote access, site-to-site VPNs, Wi-Fi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls [11]. It's a real VPN in the sense that IP or Ethernet frames from a virtual network interface are being encrypted, encapsulated in a carrier protocol (TCP or UDP), and tunneled [12]. OpenVPN provides VPN connections via TUN/TAP virtual devices which allow for creating numerous endpoints through scripted interactions that work with "push" or "pull" options. OpenVPN uses the widespread and mature industry standard SSL infrastructure to provide secure communications over the Internet with encryption of data packages and control channels. There are some benefits for using OpenVPN. With OpenVPN, you can [13]:

- tunnel any IP sub-network or virtual Ethernet adapter over a single UDP or TCP port [13],
- 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[13],
- tunnel networks over NAT [13].

2.2 IPTV VPN

Figure 1 illustrates an example of basic IPTV VPN. The main office offers IPTV service to different types of end-users over VPN connections. The IPTV distributions are not constrained by geographic locations, e.g., the main office offers IPTV service to remote office with connected IPTV VPN network, and the remote office could locate anyplace in the world. In addition, IPTV VPN is able

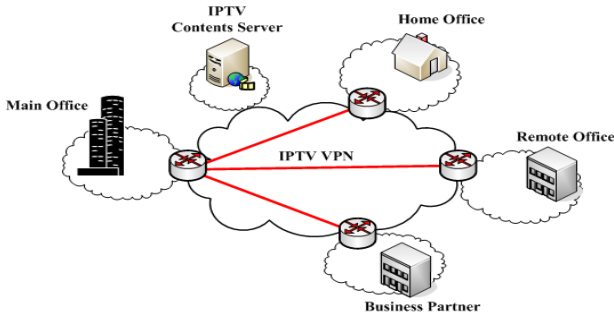


Fig. 1. An example of IPTV service via VPN [7]

to reduce operation costs, transportation costs, provide improved security and better control due to native traits of VPN. IPTV VPN can also provide classified IPTV service features according to geographical groups and customers' demands [7], classified IPTV group services features [7], etc.

3 Experiment Setup

The implementation is based on ANT, which provides different access networks and network applications to support the related research and test activities. The infrastructure of ANT is shown in Figure 2. Based on ANT infrastructure, IPTV VPN network layout was designed as shown in Figure 3.

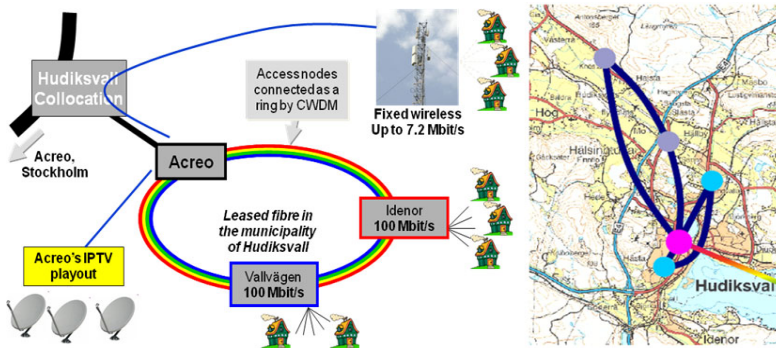


Fig. 2. The ANT network infrastructures

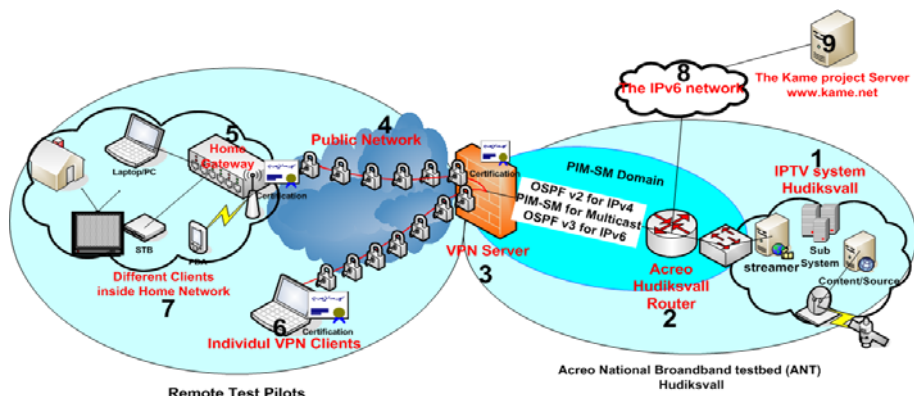


Fig. 3. IPTV VPN network layout. The different components labeled with numbers are described in section 3.1: *IPTV VPN network layout description*.

3.1 IPTV VPN Network Layout Description

The following descriptions all are related to Figure 3.

- Number 1, IPTV system Hudiksvall: The IPTV system is in ANT network and includes the content source, streaming server, sub-systems and the other components.
- Number 2, Acree Hudiksvall Router: the core router in ANT 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 VPN and multicast services to VPN clients.
- Number 4, The Public Network.
- Number 5, Home Gateway: the home gateway is physical placed in-between the link network of the VPN server and home network. The home gateway acts as vpn client for vpn connections, Internet Group Management Protocol (IGMP) proxy[14] for multicast routing besides the roles of normal gateway with the route and DHCP functions. The home gateway is running on an open source routing platform – OpenWRT [15], based an embedded Linux box.
- Number 6, Individual VPN clients: the laptops installed the VPN client program.
- Number 7, Different clients inside home network.

The main implementation is IPTV VPN implementation. In the implementation, 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 embedded Linux box with different open source

software to establish an automatic VPN connection to VPN server and provide home network connectivity for different clients inside home network.

The IPTV VPN starts up as follows. For host-to-gateway connections, an end-user starts up a laptop and a VPN client programme configured with Acreo's own VPN server which will set up a 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 OSPFv2 and PIM-SM routing protocol are running between the VPN server and Acreo Hudiksvall Router. The internet traffic will then be routed over the tunnel via the VPN server to the Acreo Hudiksvall Router. The multicast traffic from the source in the Acreo IPTV system will be 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 difference between the gateway-to-gateway and host-to-gateway VPN connection is the home gateway acts as a VPN client and IGMP proxy, besides playing normal gateway role with the route and DHCP functions for clients inside the home network.

4 Measurement and Analysis

4.1 Test Methodology

Various measurement instruments and methods were used to evaluate the QoS of IPTV VPN service. Most used for the IPTV testing was one professional IPTV measurement system - Agama Analyzer [16]. Other tools were also used to test network delay, network connectivity, network capacities, etc. In addition, end-users' perceived inspections are also a common method and used to measure IPTV visual quality. The main test activities are as follows.

- Evaluate the VPN services qualities.
- Compare IPTV service qualities between the VPN and normal wired line connection.

4.2 VPN Service Qualities Measurements

As carrier tunnels to deliver IPTV service, the QoS of VPN connections will determine IPTV service qualities. Therefore, VPN connections qualities (network delay, network connectivity, capacities loss, etc) were quantified under different VPN server configuration options. These options have some influences on VPN connectivity performance, such as some security options for different encryption algorithms, keyed-Hash Message Authentication Code (HMAC) for integrity check, data compression with "comp-lzo" option, etc. The VPN connectivity was measured with two test cases shown in Figure 4 and Figure 5.

The test case 1 and test case 2 were performed five times in a row with different VPN server configuration options. The measurement values are presented in Table 1. There are six different options in the first row of the table, for example, option 1 is original network bandwidth test without VPN connections; option 5 is VPN bandwidth test with data compression enabled.



Fig. 4. The test case 1, network bandwidth check against www.bredbandskollen.se. skicka=send, ta emot=receive, Svarstid= response time, Mätserver=measurement server.

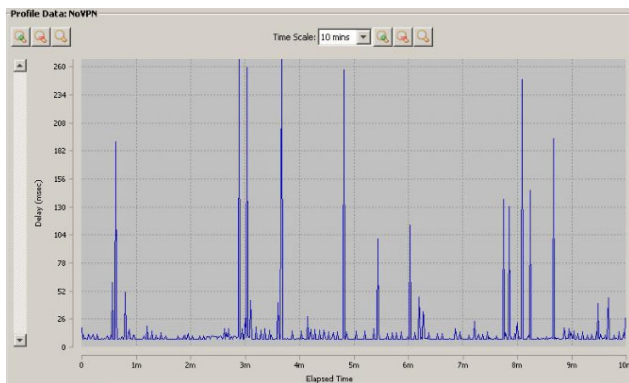


Fig. 5. The test case 2, network delay check against www.bredbandskollen.se with “Anue Network Profiler” [17] test tool in ten minutes

Table 1. Bandwidth connectivity test results for VPN with different VPN server options

	option 1	option 2	option 3	option 4	option 5	option 6
VPN connections		•	•	•	•	•
Encryption		•	•			
Integrity check HMAC		•		•		
Secret Key for HMAC		•		•		
Data compression		•	•	•	•	
Average Sent	32.59Mb/s	22.58Mb/s	22Mb/s	24.77Mb/s	22.40Mb/s	23.37Mb/s
Average Received	50.55Mb/s	36.34Mb/s	36.4Mb/s	37.49Mb/s	36.86Mb/s	37.96Mb/s
Average Network Delay	13.01 ms	36.07 ms	21.27 ms	24.97 ms	14.68 ms	17.30 ms
Maximum Sent	33.17Mb/s	23.55Mb/s	24.3Mb/s	26.03Mb/s	26.96Mb/s	27.12Mb/s
Maximum Received	55.34Mb/s	38.56Mb/s	38.6Mb/s	39.96Mb/s	39.50Mb/s	39.60Mb/s
Shortest Network Delay	7ms	7.95ms	7.94ms	7.94ms	7.91ms	7.76ms

4.3 IPTV VPN Service Qualities

IPTV service qualities comparisons between the VPN and normal wired line connections had been done with an Agama instrument and from user perspectives. Below Figure 6 and Figure 7 are shown that represent test results that one IPTV channel from same streamer was measured by Agama Analyzer during 72 hours (from 2009-05-29 8:00 to 2009-06-01 8:00). In the context of computer networks, the term jitter is often used as a measure of the variability over time of

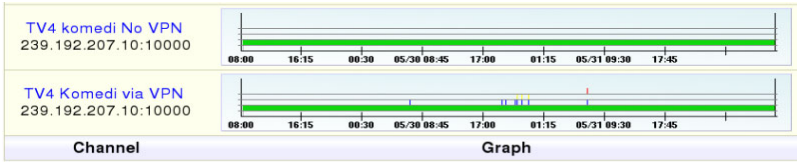


Fig. 6. SVT TV4 Komed channel measuring graph from Agama Analyzer. Green=OK, Blue=minor distortion, Yellow=major distortion, Red=Packet loss.

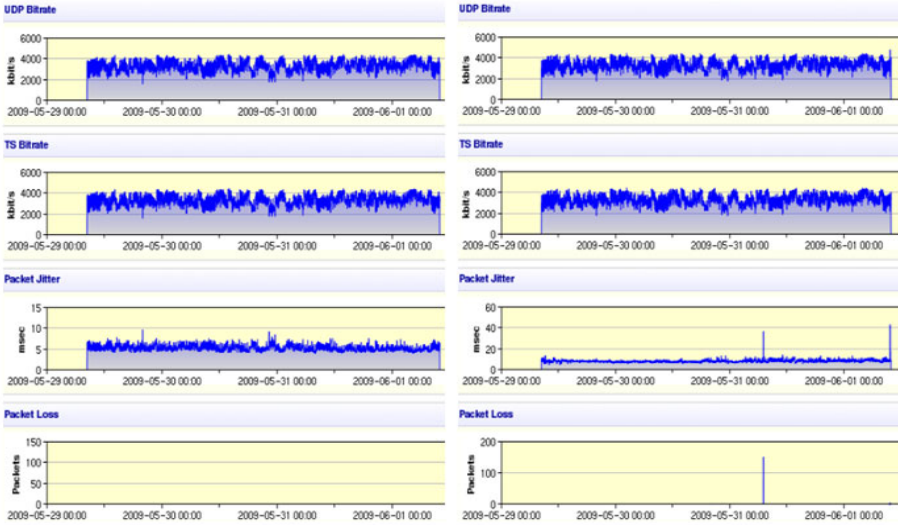


Fig. 7. SVT TV4 Komed channel Real-Time measurement graphs from Agama Analyzer. The left chart is the measurement results with no VPN connections; the right chart is measurement results with VPN connections.

Table 2. The Packet Jitter measurement results from Agama Analyzer

	normal wired lines	VPN
Average Packet Jitter	5.9 ms	9.8ms
Maximum Packet Jitter	9.8ms	41.5ms

the packet latency across a network [18]. A bigger number of packet jitter value means larger packet latency. The Packet Jitter measurements were performed and test results are presented in Table 2. From user perspectives, normal quality TV and High Definition (HD) TV were measured in terms of zapping time in a small scale trial. In the measurement, a normal quality TV’s bitrate is around 4Mb/s and the bitrate for a HD TV is above 7Mb/s. The zapping time for normal quality TV channels between VPN and normal wired line connections are almost same. For HD TV channels, there were comparative long time delay in terms of zapping time.

4.4 Discussion

The VPN service connectivity benchmark results can be summarized as follows. 1) The VPN network bandwidth loss rate is approximate 26%–32% comparing to original network bandwidth. 2) The VPN network bandwidth is nothing with the security options (encryption algorithm, session authentication, HMAC, etc). 3) 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 36.07ms). The mission-critical IPTV service requires low network delay and high real-time multicast traffics. However, securing multicast streaming will consume system resource and give negative impact on the service performance, bandwidth, QoS, etc. If no confidentiality requirement for multicast streaming, to some extent, authentication of both communication parties can ensure IPTV security. In this way, the consumption of system resource is reduced and the services performance is improved.

For IPTV VPN, the measurement results show that the qualities of IPTV VPN service is acceptable both from IPTV measurement instrument and user perspectives. By comparison, there was no obvious difference for normal quality TVs between the VPN and normal wired line connections. However, for HD TVs usually with bitrate above 7Mb/s, VPN connections gave a comparatively poor Quality of Experience (QoE) [19].

5 Conclusion

Previously Acreo only had access to end-users in “its own” networks in terms of IPTV. In this paper, a VPN solution is designed and implemented to realize a scalable IPTV delivery way, which can allow remote end-users over a wider geographical area to access IPTV service at a lower operation cost. The evaluations of proposed schema show that the qualities of IPTV service via VPN are acceptable. Although there is a network capacity reduction of VPN due to network management traffic overhead, VPN is still a good way or in some case the only solution of scalable IPTV distributions. Additionally, the VPN solution supports certificate infrastructure and can provide a flexible way for test pilots control simply by creating or revoking different certificates for different groups of users. Besides, this solution is able to reduce operation costs, transportation costs, provide improved security and better control due to native traits of VPN. Finally, almost all implementations are based on open source software, which makes the whole system more scalable and extendable.

References

1. Walko, J.: I love my IPTV. *IEEE Communications Engineer* 3(6), 16–19 (2005)
2. Yarali, A., Cherry, A.: Internet protocol television(IPTV). In: *TENCON 2005 IEEE Region 10*, pp.1–6 (2005)

3. Information Telecom & Media: IPTV: a global analysis (2nd edition). Information Telecom & Media, Tech. Rep. (2006)
4. WHITE PAPER - Emerging Multicast VPN Applications. Juniper Networks, 1–2 (2009)
5. Larsen, C.P., Andersson, L., Berntson, A., Gavler, A., Kauppinen, T., Lindqvist, C., Madsen, T., Mårtensson, J.: Experiences from the Acreo National Broadband Testbed. In: OFC/NFOEC 2006, paper NThF2, Anaheim, CA, USA (2006)
6. Andersson, L., Madsen, T.: Provider Provisioned Virtual Private Network (VPN) Terminology. Internet Request For Comments RFC 4026 (2005)
7. ITU-T: ITU-T IPTV Focus Group Proceedings, pp. 389–390 (2008)
8. Rosen, E., Cai, Y., Wijsnands, J.: Multicast in MPLS/BGP VPNs. Internet Draft (2009)
9. Pepelnjak, I., Guichard, J., Aparcar, J.: MPLS and VPN Architectures, vol. II, pp. 333–387. Cisco Press (2003)
10. Rosen, E., Rekhter, Y.: BGP/MPLS IP Virtual Private Networks (VPNs). Internet Draft RFC4364 (2006)
11. OpenVPN, <http://www.openvpn.net>
12. Yonan, J.: OpenVPN and SSL VPNs (January 26, 2005), <http://www.mail-archive.com/cryptography@metzdowd.com/msg03333.html> (accessed on August 18, 2009)
13. Yonan, J.: Open Source Overview, <http://www.openvpn.net/index.php/open-source.html> (accessed on August 18, 2009)
14. Cho, C., Han, I., Jun, Y., Lee, H.: Improvement of Channel Zapping Time in IPTV Services Using the Adjacent Groups Join-Leave Method. In: 6th International Conference on Advanced Communication Technology, vol. 2, pp. 971–975 (2004)
15. OpenWrt–Wireless Freedom, <http://www.openwrt.org>
16. Agama Analyzer, Agama Technologies AB, Box 602, SE-581 07 Linköping, Sweden (2009)
17. Anue Network Profilerp, Anue Systems Inc., 9737 Great Hills Trail, Suite 200, Austin, TX 78759 (2009)
18. Wolaver, D.H.: Phase-Locked Loop Circuit Design, pp. 211–237. Prentice-Hall, Englewood Cliffs (1991)
19. Siller, M., Woods, J.: Improving quality of experience for multimedia services by QoS arbitration on a QoE Framework. In: Proceedings of the 13th Packed Video Workshop (2003)