ENABLING MULTIMEDIA SERVICES IN UNIFIED ACCESS NETWORK

Drazen Kedmenec [1], Vedran Kedmenec [1], Mislav Grgic [2], Branka Zovko-Cihlar [2]

[1] Croatian Telecom, Draskoviceva 26, Zagreb, CROATIA
[2] University of Zagreb, Faculty of EE & Comp., Unska 3 / XII, Zagreb, CROATIA
drazen.kedmenec@hinet.hr, vedran.kedmenec@hinet.hr

Abstract: *Unified access to VPNs enables considerable flexibility in the way remote locations connect to VPN. Overall design goal of this approach requires support for all services inherent to VPNs including multimedia ones. Classical approach to building VPNs such as ATM or Frame Relay can enable strong support for multimedia traffic because of ability to provide strict QoS guaranties. Architectural requirement of using IP as network protocol can lead to problems in transport of multicast streams for VPNs based on classical networks. New approaches such as MPLS VPNs promise even greater flexibility and scalability through use of native means for IP packet delivery. Methods that can provide multicast traffic transport in those approaches should be investigated. Different access technologies have different characteristics regarding ability to deliver multimedia traffic and are investigated in terms of their usefulness for such purposes.*

Key words: *ATM, Frame Relay, MPLS VPN, IP Multicast, Access Technologies, Multimedia Traffic*

1. INTRODUCTION

Advances in data communications have, from service provider perspective, resulted in three key developments. First, customer intranets are being increasingly transferred to IP protocol. Today, we exclusively see IP used in new intranet developments, and a trend towards migrating legacy platforms to IP in older installations. Secondly, mobility is a very important aspect of the overall intranet architecture. There is high demand for ability to access private network through public infrastructure (ADSL, ISDN, GPRS) regardless of access technology currently available to a mobile location (technology agnostic approach). And finally, newer applications have considerably increased demand for higher bandwidth access to intranets. A service provider can answer those requirements by deploying a high-speed IP based public infrastructure for customer VPNs and by enabling unified access to those networks. MPLS VPN technology is ideally suited for this purpose. This paper presents an overview of issues in enabling such networks for multimedia applications. First part of the paper presents an overview of public networks used to build separate VPNs and a system that will enable universal access to those VPNs. Next, a way to provide access to multimedia applications is described. Finally, strengths and weaknesses regarding each access technology are presented.

2. UNIFIED ACCESS TO VPN CONCEPT

A tendency towards greater mobility and access technology independence can be satisfied with proper core and access network design. Fig. 1. shows three main parts that constitute the unified access network: access part that incorporates all available access technologies, Access

Concentration System that serves as a link between access and core VPN part of the network, and public network that serves as a core platform for VPN deployment.

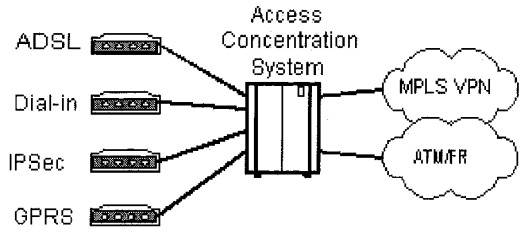

Fig. 1. Unified access network design

The main goal in core network design is enabling VPN flexibility. This flexibility can be either topological (covering diverse geographical locations) or logical (covering diverse networking requirements) and it can also extend into resource domain (providing flexible per site traffic parameter options). A classical approach to building public infrastructure for VPNs is ATM or Frame Relay network, which are more layer 2 centric. Newer approach includes MPLS VPN service, which concentrates on IP only VPNs. Both of those approaches will be detailed later in this section.

On the other hand, access network design concentrates almost exclusively on mobility, i.e. ability to access private VPNs through widely available public access technologies. In order to accommodate requirements of flexibility in the core and mobility in the access part of the VPN, it is necessary to find a common denominator, a technology that will provide for such networking requirements. Of course, the only choice today can be IP. Public network that will enable universal access to VPNs must operate IP as a unifying layer 3 technology. This is required because of Access Concentration system that serves as a mediator between different access technologies and VPNs.

2.1. Core VPN technologies

Using ATM/Frame Relay is a proven approach to building core network for servicing diverse customer VPN requirements. Security, isolation, quality of service, relative simplicity and flexibility are all synonymous with those technologies. Using IP as a layer 3 technology is not a strict requirement in an ATM/Frame Relay based VPN, but becomes necessary when migrating to unified access approach. Some of the perceived shortcomings of ATM/Frame Relay approach are complicated provisioning if full-mash connectivity is a requirement, and relatively poor match between ATM classes of service and TCP flow control mechanism (as is clearly demonstrated in [1]).

MPLS VPN [2] is relatively new technology that concentrates on building flexible and scalable IP based VPNs. It is based on a peer-to-peer relationship between VPN sites and the core of the network. This enables the core to actively participate in per VPN IP routing process, essentially emulating a true IP routing core separately to every VPN. Security, isolation and quality of service in this approach are comparable to ATM/Frame Relay concept. They are guaranteed through use of MPLS technology that ensures required

characteristics by utilizing special virtual tunnels (LSPs). MPLS VPN technology is seen as unifying IP and ATM (and other layer 2) worlds. It provides high flexibility and scalability on the IP layer (automatic full-mesh connectivity, automatic distribution of reachable IP network addresses inside VPN) and is ideally aligned with TCP flow control mechanisms. IP-only aspect of the technology can be seen as a deliberate design choice, rather than a significant shortcoming. Since ATM and Frame Relay are still used as an access medium to MPLS VPN core, MPLS VPN can be seen as a complementing, rather than competing technology.

2.2. Access technologies

Access to a VPN must be possible regardless of user's location or access technology used. Basically, any available access technology can be utilized for this purpose. Moreover, it would be preferential if same authentication mechanism is used for VPN access through any of available access technologies. Table I lists some of the more popular publicly available access technologies and their characteristics.

Table I Access technologies and their characteristics

Access Technology	Characteristics
Dial-in (POTS and ISDN)	Universally available, relatively low speeds, not originally intended for data services
xDSL (ADSL, VDSL)	Good solution for access to asymmetric data services, where available
IPSec	Enables secure access to VPN from any remote location connected to Internet
GPRS	Good intermediate solution for mobile data access

2.3. Access Concentration System

A link between different access technologies and core VPN network is realized through Access Concentration System. This system is responsible for access circuit termination (this is where IP requirement surfaces), authentication, accounting and VPN selection. Also, all IP connectivity requirements between VPNs and remote access clients are satisfied here. Main characteristic of the Access Concentration System is that it can be implemented as an add-on to existing network core, without requiring any changes in either core itself or structure of VPNs. It can simply and effectively connect existing access technologies to existing VPNs therefore adding additional value to both.

3. MULTIMEDIA SERVICES IN UNIFIED ACCESS NETWORK

Multimedia services are an essential part of VPNs. It is reasonable to expect demand for their usage across VPN access technologies. Two issues regarding multimedia traffic in unified access network arise: transfer of multimedia data in the core of the VPN and transfer of this data over numerous access technologies. Also, nature of multimedia traffic must be investigated.

3.1. General characteristics of multimedia traffic

Generally speaking, multimedia traffic can be uni- or bidirectional. Of primary interest here is unidirectional traffic like multimedia streaming. Bidirectional traffic, like videoconference or a VoIP call is essentially a special case of unidirectional case, and will be discussed in more detail where appropriate. Main characteristics of multimedia traffic can be summarized as following:

- UDP is chosen as a transport protocol. There is no real value in using TCP for multimedia transport because of its real-time characteristic.
- Important QoS parameters that must be observed and maintained are low packet loss, packet ordering, delay and delay variation.
- Multimedia traffic can range in bit rate, i.e. source can adjust bit rate according to required quality or access line bandwidth.
- IP multicast can be used for more optimal network utilization.

3.2. Handling of multimedia traffic in the VPN network core

Classical VPN realized on ATM/Frame Relay technology can support multimedia IP services in an overlay model. Depending on source and destination locations, appropriate mesh of PVCs must be provisioned, Fig. 2., to satisfy multicast requirements. In unicast mode, requirement on number of PVCs can be eased depending on whether multiple hops for packets are allowed. Required PVC characteristics (traffic parameters, class of service) can easily be provisioned, although exact calculation of PVC sizes may be tricky. Important traffic characteristics like low packet loss, low delay and delay variation and proper packet ordering can all be easily satisfied. It can be observed that in both unicast and multicast case source has to send multiple traffic streams to destinations. This is a result of overlay principle.

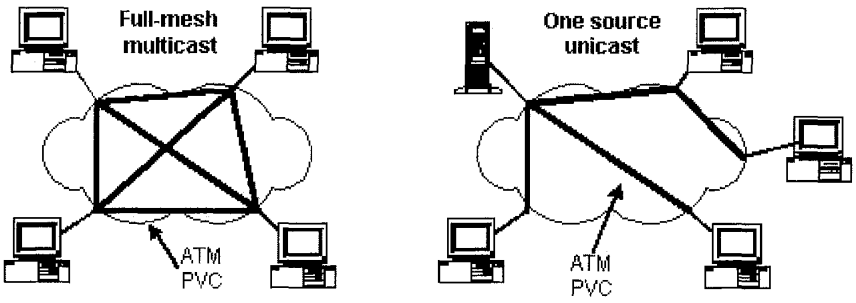

Fig. 2. Handling of multimedia traffic in ATM/Frame Relay core

MPLS VPN standard does not support native multicast transport. Methods that will enable "native" IP multicast support in MPLS VPNs are currently under investigation [3]. This approach will enable true per VPN IP multicast transport in MPLS VPNs (meaning that only one stream of multicast data will be properly distributed to all interested destinations by the core of the network). Currently, multicast can be supported through use of IP-in-IP tunnels. This constitutes an overlay model essentially the same as multicast model in an ATM network, with the same shortcomings, Fig. 3. This approach is not scalable but can be

beneficial if distributing high bandwidth multicast traffic between VPN sites. Delivery of unicast multimedia traffic in MPLS VPN model is straightforward and more efficient than in classical model because of inherent IP characteristics in MPLS VPNs. Although MPLS VPNs distribute traffic through standard IP routing, there are no problems in guaranteeing QoS parameters (packet loss, delay, delay variation, packet ordering) to even very demanding multimedia traffic.

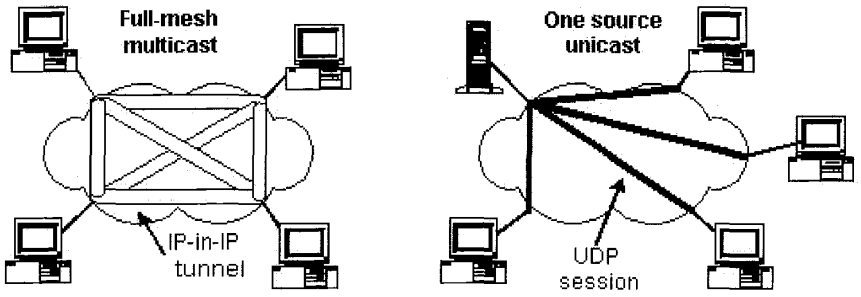

Fig. 3. Handling of multimedia traffic in MPLS VPN core

3.3. Handling of multimedia traffic on different access technologies

Key issue in enabling multimedia services on different access technologies is the characteristic of the Access Concentration System. In order to support multicast traffic distribution to remote access clients, it must be able to separate it across clients connected to different VPNs. Such functionality is possible, and is based on strictly controlled distribution of IGMP messages between remote access clients, Access Concentration System and VPNs. Additionally, Access Concentration System must be able to take part in any multicast protocol active in a VPN (for announcement of active sources and interested destinations). Regarding this functionality, there are three approaches that can be used to support multimedia traffic delivery over different access technologies, Fig. 4.:

- Access Concentration System can support per VPN multicast traffic forwarding – requires rather complicated multicast implementation in Access Concentration System
- Multicast can be supported through IP-in-IP tunneling – can be used if there is a multicast network behind remote access device (xDSL for instance)
- Unicast can be used for remote access sites, and multicast for all other VPN sites

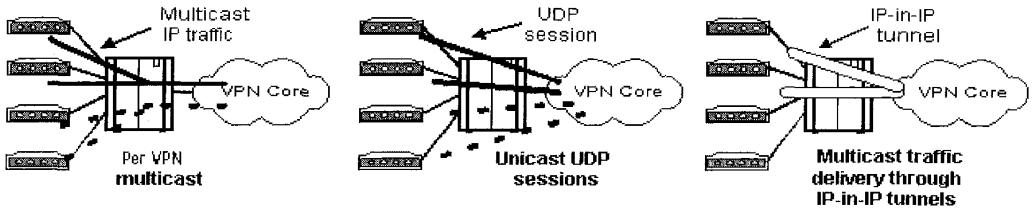

Fig. 4. Handling of multimedia traffic through Access Concentration System

Table II compares different access technologies regarding such key characteristics as support for multicast traffic, available bandwidth and QoS parameters.

Table II Comparison of different access technologies

Access Technology	Multicast Support	Bandwidth	QoS
Dial-in	No	Low bandwidth for low quality unicast multimedia services.	Problematic. Packet fragmentation must be used, if possible.
xDSL	Depends on characteristics of Access Concentration System.	Can support very high bandwidth multimedia services (ADSL one way only).	Can support key QoS requirements.
IPSec	No (Currently under investigation).	Varries. Theoretically, high access bandwidth can be provided.	Problematic. IPSec session traverses public Internet where QoS can not be tightly controlled. Encription process introduces considerable delay that can be reduced with hardware processing.
GPRS	No	Low bandwidth for low quality unicast multimedia services.	Can be very problematic. Delay can be prohibitively high for a real-time multimedia session.

Two-way multimedia delivery (videoconferencing) is possible on all access technologies except GPRS (because of very high, unpredictable delay). xDSL technologies are the most appropriate for such services, having in mind that ADSL will have a low upper bandwidth limit in the upstream direction.

4. CONCLUSION

The concept of unified access to VPNs was presented. Different approaches to building core VPN network and strengths and weaknesses of publicly available access technologies were summarized. The ways of transporting multimedia traffic across core and access technologies were investigated. It was concluded that MPLS VPN technology requires further investigation into per VPN IP multicast transport. Feasibility of using different access technologies for multimedia traffic was demonstrated. Support for VoIP traffic was not studied because of specifics and differences in approach that are required. This topic will be investigated separately.

REFERENCES

[1] M. Behringer, ATM Experiments for Advanced Backbone Services, http://www.iif.hu/rendezvenyek/inet97/F6/F6_3.HTM
[2] E. Rosen, Y. Rekhter, BGP/MPLS VPNs, RFC 2547
[3] E. Rosen, et al., Multicast in MPLS/BGP VPNs, Internet Draft, February 2002