Building Virtual Private Networks to Support Mobile VPN users in a Group with Quality of Service Guarantees

Chittaranjan Hota
Lecturer, Computer Science & Engineering
Birla Institute of Technology & Science
Pilani, Rajasthan, 333031, INDIA
c_hota@bits-pilani.ac.in

G. Raghurama
Professor, Electrical & Electronics Engineering
Birla Institute of Technology & Science
Pilani, Rajasthan, 333031, INDIA
graghu@bits-pilani.ac.in

Abstract

Flexible, secure and cost effective in comparison to traditional solutions, IP-VPNs exhibit many of the traits enterprises are seeking today. Mobile VPN users have special requirements relating to resource adoption and customization. In this paper we have discussed how mobile agent technology can be applied to IP-VPN in finding a route for a tunnel with QoS features and also how can it provide service capabilities to mobile users. In our approach, we have considered the requirement from a group of VPN users. We have developed a framework to use active packets that can help us in discovering an optimal QoS route based on the available bandwidth and link cost. Also we have described an alternative approach for resource management between two agents. Taking into account, the structuring mechanisms enabled by standard mobile agent platforms, like regions, agencies grouped within regions, and places belonging to agencies, we have applied these structural principles to our target mobile communications environment. We have assumed that service providers have access to node's control environment, algorithms and states. A possible framework for supporting mobile user groups after the deployment of the VPN is suggested in this paper. We have considered the concept of Place Oriented VPNs that are based on agent technology and can be built on top of existing VPN infrastructure.

1. Introduction

The Internet revolution has dramatically altered the networking requirements & opportunities of the enterprise. The deployment of new IP applications and the availability of tremendous capacity i.e. high connectivity has promised to facilitate the exchange of critical information both within the enterprise and throughout its sphere of influence. However, this way of expanding the value of a network as a business asset does present challenges. There are many ways of handling this. IP-VPN is one of the better solutions. In this sluggish corporate spending environment, Internet Virtual Private Networks continue to attract attention as a way to reduce remote access costs for enterprise networks. But while the number of implementations is clearly on the rise and VPN technology has become well understood, it also continues to be in many respects, a work in progress. *A VPN is a communications network, built for the private use of the enterprise, over a shared public infrastructure [8].* There are two primary applications covered by this definition: remote access connectivity and site-to-site connectivity (see Figure 1). VPNs can be categorized into three types as Remote Access, Intranet, and Extranet. Remote access connects remote users to corporate LAN, Intranet connects branch offices to corporate LAN, and the Extranet VPN gives access to business partners.

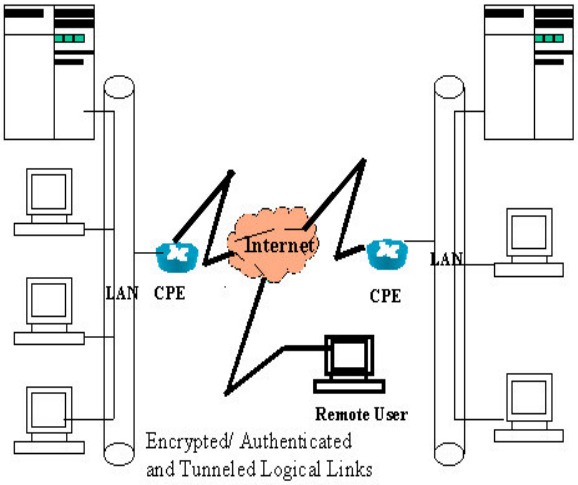

Fig.1. An Example of IPVPN

The motivation for building VPNs is numerous. However, a common thread in each is the requirement to make some portion of the public network 'invisible' to outside people, while taking advantage of the efficiency of a common communication infrastructure. The two basic motivations are (a) cheap cost and (b) need for communication privacy. The general conclusion [1] is that a collection of virtual networks implemented on a single common physical communications plant is cheaper to operate than the equivalent collection of smaller physically discrete communications plants, each serving a single network client.

The majority of theoretical work being done recently on the performance enhancement of the VPNs concerns security [2]. Researchers have focused on devising different architectures for different deployment scenarios. Little has been done to provide QoS support in a VPN

environment and also to support roaming users (users who often move from one network to another). The main problem we face in supporting mobile users is the technology integration. These traveling VPN users must be supported in small groups or separately. We discuss here, how can we use agent technology and active networking concept to support our roaming users to get the VPN services from the corporate network. Also the tunnel that is to be formed between source and destination should guarantee maximum quality of service requirements. VPNs are designed mostly with static users in mind and little has been done to integrate mobile users or to provide mobile user support after their deployment. The problem here is that the availability of information and communication services varies from place to place and from time to time. The major requirement here is that for dynamic reconfiguration of the new environment and customization.

The advent of high-speed networking technology has enabled many multimedia applications like video conferencing, medical imaging and VOIP. These applications have different performance requirements of bandwidth, delay, jitter and loss rate, which leads to an important issue of how to support QoS on the modern high-speed virtual private networks.

It is known that the original Internet is a "best-effort" network, which has no QoS support for different classes of services. However, there may not exist one solution to all the problems of **QoS** support, because the application-specific state of QoS should be frequently changeable or easily deployable when needed, while the conventional network is simple and stateless. Now, recent research has shown that the programmable **"Active *Networks*"** may be a better solution to guarantee QoS in the VPNs.

2. Related Work

2.1 Place Oriented VPNs

A PO-VPN is an alternative virtual private network [4]. It differs from a legacy VPN where the legacy VPN has its own resources which are managed by its own users in a policy related way. But current VPNs are not sufficiently flexible, have long set up and deployment times, are not dynamic enough to accommodate rapid changes, and can't be controlled by the users. It is again more difficult to manage if the VPN spawns different networks with different policies. PO-VPNs are a right solution for this problem. These are built on top of existing physical networks and are controlled by agents.

2.2 Active Networks

Active networks are a novel approach to network architecture in which the switches of the network perform customized computations on the message flowing through them. The first piece of this architecture is a protocol that would replace original "passive" IP packet with the "active" object code. The motivation of active networks is to permit applications to inject programs into the nodes of networks and then to support faster service innovation by making it easier to deploy new network services. Active networks are highly programmable networks that perform computations on the user data that is passing through them. In contrast, nodes of the traditional networks, such as ATM switches or IP routers, are closed, integrated systems, whose functions and interfaces are determined through standardized processes. These nodes transport packets (or cells) between end-systems and the processing of these packets is limited to operation on the header, primarily for the routing purposes. Specially, the network nodes neither interpret nor modify the packet payloads. Active networks, in the other hand, break this tradition by letting the network perform customized computation on the packets, including their payloads. There can be mainly two approaches to active networks: discrete and integrated, depending on whether programs and data are carried discretely.

Programmable switches – a discrete Approach: In this approach, the existing packet formats are remained and it provides a discrete mechanism that supports the downloading of programs, which separates the injection of programs from the processing of messages.

Capsules – An Integrated Approach: In this approach, the existing "passive" packet will be replaced with the "active" miniature programs, called "capsules", which are encapsulated in the transmission frames and executed at each node along their path. User data, the payload, will be computed and embedded in the capsules.

2.3 Agent System

Mobile agents [3] are software components that act alone or in communities on behalf of an entity and are delegated to perform tasks under some constraints or action plans. The essential characteristics of these agents are mobility that allows them to move from one node to another and continue their execution. An agent is a process that enables users to control their system, and at the same time, to allow sharing of resources, that is it controls the access to resources of a remote computer, and also provides protection. An agent system consists mainly of places. A place is a context in which an agent is executed [4]. This context can provide services like access to local resources. A place consists of place name and address of agent system within which the place resides. A place can contain other places. All places follow parent child relationship. The assignment of places to agent system is done by ways like dynamically as they enter into different nodes based on some criteria like originating from same user or statically assigned per entity i.e. per user or per enterprise.

2.4 Active Node

The active node consists of a programmable router at the lowest layer, above which a node OS lies, which again supports Execution Environments. At the top, we have the application programs running [4].

3. Our Approach

VPNs are designed with static users in mind and almost all the recent VPN technologies do not support mobile users, i.e. once the VPN is deployed if the user is moving into another network (a third party) then again the same VPN has to be reestablished with the new network as the source. To do this, we must also have the required client software available at the new node and also it should support VPN connections. If everything is right, we then have to reestablish the whole VPN connection starting from the scratch. This scenario of VPN deployment can also be called as Flexible VPN. This requires resource adaptation and customization. To make this feasible, we have applied the concept of Agent technology & Active networks. The Mobile agents used are active, mobile, and can travel. They may reside in a host or client computer, and roam other computers, networks, or the Internet to execute their tasks. They are frequently used to collect data, information, or changes. The use of these agents have several advantages like reducing the network load, overcoming network latency, encapsulating protocols, executing asynchronously and autonomously, dynamic and heterogeneous. These mobile agents can migrate along with mobile users, adopt local and remote resources dynamically and generally manage and mediate all requirements of mobile users.

3.1 Mobile User Support

To support mobile users, we have allowed each user to act within his own place. This place hosts one or more cooperating agents that keep track of user's requirements and current status. Agents here take the role of customer, the service provider and the network provider. These agents reconfigure the services that user wants in the new environment. They also see that the adoption is optimal in the new environment. The reconfiguration is fully transparent to the users.

A VPN with mobile users comprises of a graph with changing nodes. As the user moves, we face the challenge of re-assigning the connections between the nodes in order to provide the same services. This whole process does take place without the notice of the user. To support mobility, we have to dynamically and flexibly provision VPNs. The deployment should take minimal time. There are multiple network and service providers in the underground infrastructure on top of which we want to build our VPN. Here, we consider three agents **UA** (user agent), VPN **SPA** (service provider agent), and **NPA** (network provider agent). The process for supporting mobile users is two fold:

3.1.1 Initial VPN provisioning

1. UAs negotiate and decide upon a common set of requirements and services desired by the users.

2. All UAs elect a leader using the Bully leader election algorithm (using the priority number, election and coordinator messages), and the leader is called as GA, the group agent.

3. Then GA tries to find out an optimal tunnel path for the VPN topology on the basis of bandwidth and link cost covering all the UAs. Here, GA issues self-routable packets, which travel in the network and get happiness levels from NPAs. The self-routable packet contains a time stamp according to which it has to follow back to GA. GA also negotiates with VPN NPAs to find out different resource supports.

4. Now GA interacts with the SPA in order to find out which topology supports the desired services. At the end of this phase, GA has a network topology that supports the services desired fulfilling the SLAs demanded by the user or customer or the UA.

5. GA then, integrates all the information received and uses a rule-based system to process the information. The happiness levels are averaged and the deviation is measured. The rule based system acts as a control element using this deviation as input.

6. It then issues active packets based on the rule-based system, which tries to restore the happiness levels. The happiness is here nothing but the bandwidth consumption and link cost. Thus routes are added and deleted from the routers dynamically to redirect the load so that the VPN is happy or well behaved. The GA does this thing. It can also consider other parameters like error statistics, reputation of nodes, cost security etc in deciding an optimal path for the VPN.

7. Finally GA requests service and network providers to set up the services and the connections. As, a last step, GA informs all UA that the VPN is ready to use, after which it may die or remain alive as a central authority to monitor future requests and topologies.

3.1.2 Dynamic VPN adoption

When a user moves from one network to another, his services must be maintained in the new environment. The steps below are needed to achieve this:

1. When a user moves from the home network, all the User Agents stop after getting a "operation stop" signal from the system. All the UAs then inform the GA, the central agent that the user is no more active in his home network.

2. When the user logs into another network after migrating, this new location address is sent back to the User Agents

those were available in the previous domain but were stopped.

3. With this information, all the user agents migrate themselves to the new environment after authenticating themselves in the new domain.

4. The UA after establishing itself over the new domain examines the services needed by the user and whether these are supported & provided by the new domain. If yes, it configures those in the new environment. If not, UA may ask the old node to get the active code that implements the missing services in the new domain. This is where, active networks concept comes into play. The other possibility is having an agent based resource management system as depicted below:

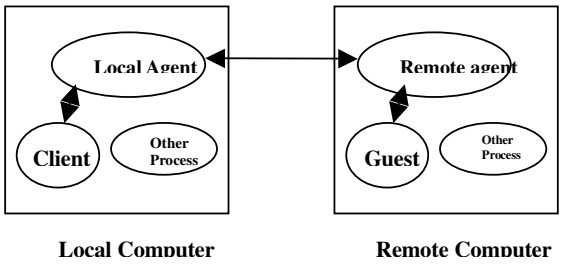

Fig. 2. Relationship Between Different Processes

Local agent must perform the following actions:

a. Locate a remote computer with the required resources

b. Negotiate with that Computer to borrow the resources

c. Invoke the service requested by the client

d. Handle the Exception Conditions (resource revocation, and location of a new host and deportation of the guest process) in a way that is transparent to the client and guest

The remote agent process has to lend the resources and protect the interests of the computer owner. In particular it should perform the following actions:

a. Receive the borrowing request from an agent

b. Analyze the request to determine whether the resource can be granted

c. Create an appropriate execution environment for the guest process (Creating a new process and supplying the guest with capabilities to access other components of the system, according to the request specification, e.g. network connections to the client so that the guest and client can communicate directly).

d. Exception handling, for example attempts to access resources, which the guest was not allowed to utilize, revocation of rights.

Providing remote resources or services in the above type of agent based resource management system can be categorized into three phases as Negotiation, Resource Utilization, and Resource Release with different messages being labeled as shown in Figure 3.

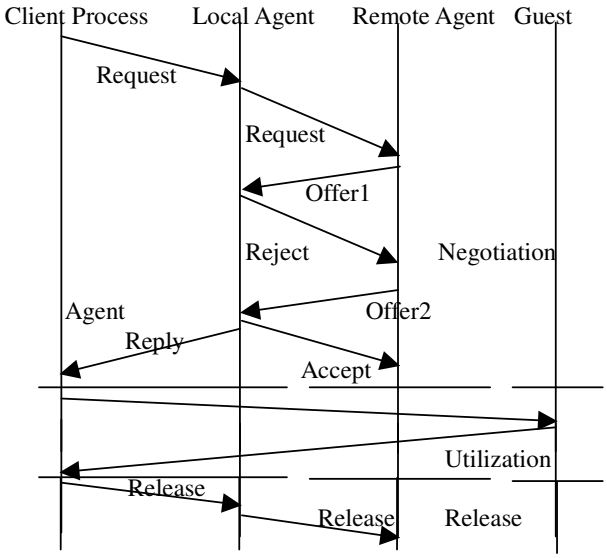

Fig.3. Negotiation and Utilization Messages

5. Finally, after establishing the new environment either with the help of active codes getting transferred or with the help of a distributed message communication model as described in the above step, UA informs GA, which in turn multicasts this new VPN node to rest all affected UAs. This is done to enable all UA to configure their local services to comply wit h the new topology of the VPN.

3.2 Active Quality Of Service Routing

Steps 3 to 6 of section 3.1.1 (Initial VPN provisioning) has been considered as Active QoS routing, which is based on the concepts of active networks, where the behaviors of network elements, such as routers and switches, can be modified and manipulated dynamically by injecting customized codes into the network elements. The basic functionality of active QoS routing is to find a network path to satisfy the given constraints that are required by the QoS requirements of a specific connection. In traditional routing, packets are delivered by using routing tables that are located on routers along the chosen route and the routing tables are formed only by the route information that is based on hops, source and destination address. But here selecting a path that provides QoS requires additional information, which are the traffic quality requirements such as bandwidth, delay, jitter and cost etc. In addition to the routing table, in AQR, the network elements also keep the state representation of the whole network or their sub-network and also with the

routing algorithms the best feasible route from a given source to a destination that satisfies the QoS constraints is chosen. In addition, most active QoS routing algorithms consider the optimization of resource utilization. Here we would like to introduce two of the AQR technologies.

One of the technologies is using Active Packet that is packet with a piece of executable code in its header. Basically, the idea of this technology is to find the best path according to QoS specifications by sending Active Packets from the source to destination, each time the first packet reaches the destination it sends a reply packet carrying the updated QoS and path information back to the source address. Thereafter, the subsequent packets will follow this path. With a certain interval, the Active Packets are sent again to detect the network state, then, the source may change the path according to the reply packet information.

The other one is using agent code at chosen routers through the network. Basically the agent is an independent executing code that can autonomously perform in response to events. With AQR, for the router to select the best path, the QoS parameters and traffic specifications are the most important factors, so these parameters are going to be kept in the agent routers' routing table. For example, the QoS parameters are residual bandwidth, loss probability, delay, Jitter, security status and cost etc. The traffic specifications can be categorized as video conferencing, FTP, email, audio stream and video stream or voice etc. As a result, the routing tables become multiplex and complex, which are called as search matrix as shown in the figures below.

Table 1. Search Matrix

	R0	R1	R2	R3
R0		R01	R02	R03
R1	R10		R12	R13
R2	R20	R21		R23
R3	R30	R31	R32	

In the above table, the entry R01 to R32 refer to the costs incurred by traffic delivering between two routers in the sub- networks, for example R01 is the cost of traffic from R0 to R1. The following table illustrates every kind of the cost. As shown below, the cost depends on the QoS requirements and the types of traffic. With all these information the router will decide which path is the optimal and effective route, but probably not the shortest path, for the specific traffic. Off-course, every connection will not include every cost, it depends on the grade of QoS service that this connection requests. Like the routing table in OSPF (Open Shortest Path First) algorithm, the matrices are going to be updated with a certain interval. Otherwise the rapid changing link parameters will cause incorrect routing decisions.

Table 2. Different Kinds of Cost for Different Traffic

	Bandwidth	Cost	Delay	Hops
Video-Conf	M00	M01	M02	M03
FTP	M10	M11	M12	M13
Email	M20	M21	M22	M23

3.2.1 Active Packet Format

An active packet is the basic entity on which the whole Active Network Infrastructure is built. The structure of this packet is as follows:

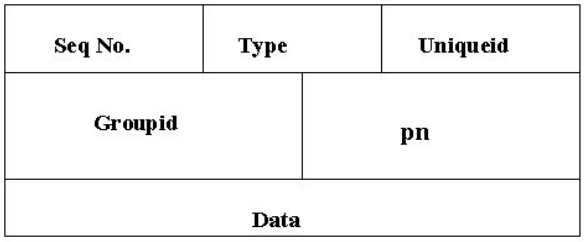

Fig. 4. Active Packet Format

SEQ NO is an integer field that denotes the sequence number of the packet. The protocol used for their transmission is UDP hence proper assembling requires some ordering as datagrams arrive out of order. **TYPE** field can carry binary values of 0 and 1, where Zero denotes that payload is some code while one denotes that it is either normal user data or data used by some code previously sent. **UNIQUEID** field is used to authenticate the packet as having a valid ID. The field is also helpful in constructing the filenames for various protocols sent by multiple users. **GROUPID** field assists the above field of uniqueid in verification and differentiating among protocols sent by multiple users over the network. **PN** is the priority number over of the packet. **DATA** is the normal user data. Only here it is wrapped around with another layer of headers for active identification of this packet.

These packets are wrapped in a UDP packet and sent for transmission. UDP is chosen to wrap it because the packet can itself control the reliability by the code in it. Also if the code is written in perspicacious manner the packets can also self-route itself based on the conditions imposed by the code & data placed in it. Here, the idea is to place intelligence in the packet, and not on the devices controlling the packet.

3.2.2 Server & Client Implementation

Server and client programs are used to send and receive active packets at various machines. Both the server and the client implementation are required at both the ends if they want to communicate. This is so because the nature of packet object is recursive, in the sense it can go to destination and try to contact back the master.

These two programs can be together called as the **execution environment**. The server process listens to connections from various hosts and receives packets from them. If they contain code then the packets are not only saved on the machine but also compiled and executed to change the behavior of the machine.

These daemons receive the active packets wrapped under the UDP cover. They open the UDP layer and read the active layer headers. Validate the packet. Set an environment with access restrictions as laid by the system administrator for these packets at that end host.

As shown in figure below, the execution environment consists of three processes namely daemon process, server process and client process, which are running together and using IPC (inter process communication) between them. First the daemon listens at UDP layer and picks up all active packets and delivers them to EE of the machine. The EE SERVER process of the machine understands the code in the packet. If valid the code is sent for further processing else the active packet is dropped. The EE manipulator segregates the packet into code and data and forks a copy of it. The child process exec's to load on the executor and executes the code inside the packet. If this packet has code, which demands for new packet formation and delivery, then the EE CLIENT side is used to frame such packets and deliver them to UDP via DEAMON process for delivery. The acknowledgements of the active packets are in turn active packets again and use the same EE CLIENT side process.

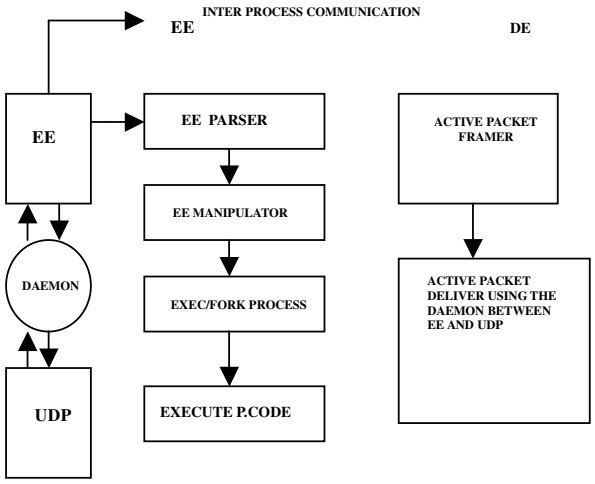

Fig. 5. Structure of Execution Environment

3.2.3 Route Optimization & Routing Agent

Route optimization is implemented using two QoS parameters i.e. bandwidth & cost of the link. Their tables are maintained as explained in one of the sections above on Active QoS routing. Routing Agent is a simple C code that is transferred using the client to server where it is assembled and installed. The routing agent queries the route optimization algorithm, giving it the destination and asking it for next best possible router to move at. The Route Optimization code can be transferred prior to Routing agent on the routers on the path and installed over there using the active network scheme. The Routing agent just queries this to find the next possible position. The routing algorithm returns a structure called ***"routeLink"*** which has the information regarding the next IP to go to and bandwidth available along with the cost of the link. The routing agent also connects back to the home address to tell the current router specification where it is. As this initial packet follows the whole route it keeps sending the ***"communicator Packets"*** regarding the information of links it is traversing. The failure or loss of this initial packet shall not lead to catastrophic failure of the whole system as the information about the whole route is being queued at the end point.

As the information is built up at the end node the rest of the data packets can follow the route that is built up. After some time another routing agent can be sent to get the route, as changes are possible over the path because of ascertain behavior of the parameters on which the system is working.

4. Results and Conclusion

The Internet as of today does not support secure communication between a group of mobile users with minimal effort. We have considered the notion of PO-VPNs suggested in [4], an alternative form of VPNs whose aim is to provide an infrastructure for groups with special characteristics like short time to live, low population etc.. These PO-VPNs can be deployed on top of existing VPNs and offer customized services in a flexible, interoperable and cost effective way. We have implemented the active QoS routing (section 3.2) using Unix socket API. As a result of this implementation, we found a path for a VPN tunnel (between a mobile user and corporate office) satisfying the QoS requirements as demanded by the user's SLA. To fulfill the requirement of mobile user group, a virtual environment with the help of active networks and intelligent agents can be a better option as described in our approach. Also in our approach, an alternative to active networks is suggested, where for resource management in the new environment the agents can communicate with each other as described in step 4 of section 3.1.2. But this option is a slower one because of message communication overhead. This can only be preferred when we have access restrictions or security problems in supporting active networks concept. It can be seen that active networks have many advantages over the traditional networks to support QoS. Firstly, it is an adaptive scheme that can support many classes of services. Secondly, it is more scalable than RSVP and possible to develop a simpler architecture to enable QoS than using IntServ and Diffserv together. Thirdly, active networks support user-driven computation and provide more powerful way for user to shape the traffic for particular QoS requirements. As a future work, we plan to implement

a simulated environment for supporting mobile VPN users group under a legacy VPN set up which will include tunneling, and encryption algorithms as well. This will also embed our QoS routing part presented in section 3.2 (VPN path selection). Also we would like to analyze the performance of the VPN supporting mobile users when the number of mobile users is large.

References

[1] Paul Ferguson, Geoff Huston, "What is a VPN?", Cisco White Paper, April 1998.

[2] S. Kent, R. Atkinson, "Security Architecture for Internet Protocol", RFC 2401, November 1998

[3] R. Murch, T. Johnson, " Intelligent Software Agents", Prentice Hall PTR, 1998.

[4] S. Karnouskos, I. Busse, S. Covaci " Place Oriented Virtual Private Networks", International Conference on System Sciences, Hawaii, 2000

[5] D. Mitra, J.A.Morrison, and K. G. Ramakrishnan, " Virtual Private Networks: Joint Resource Allocation and Routing Design", IEEE Transactions on Networking, 1999

[6] N. G. Duffield, P. Goyal, and A. Greenberg, " A Flexible Model for Resource Management in Virtual Private Networks, IEEE Transactions on Networking.

[7] S. Karnouskos, " Supporting Nomadic Users within Virtual Private Networks", Proceedings of GLOBECOM workshop on service portability, 1st Dec, 2000, San Fran, USA

[8] Bruce Perlmutter, "Virtual Private Networks: A View from Trenches", PH PTR