1.1. Abstract

Traditionally organizations have designed their VPN networks using layer 2 WANs that provide emulated leased lines. In the last years a great variety of VPN technologies has appeared, making more difficult to match the best technology for each organization. In the actual scene service providers are trying that costumers outsource their VPN in order to efficiently manage their networks. In this paper there is a simulation-based analysis of the four main VPN technologies used nowadays: Frame Relay, ATM, IP-Tunneling (GRE, IPSec) across public Internet, and private IP-MPLS network. In this analysis a general scenario has been defined. In this scenario an organization has to interconnect four remote offices with the central building and its servers. The organization has also four remote workers that need access to the corporative intranet. The user profile includes all kind of applications: Web, FTP, E-mail and Database access. A scenario has been created for each technology; then, the network performance has been evaluated from the point of view of efficiency, scalability, QoS and economic cost. The simulations analysis will show the best option for each scenario.

1.2. VPN Overview

The meaning of the VPN term is used in several ways and there are different definitions depending on the technology or the applications used in the VPN. IETF gives the next definition: “VPN is defined as the emulation of a private WAN through public networks”. [1]

We can mainly differentiate between two kinds of VPN models: the Overlay model and the Peer-to-Peer model. In the Overlay model the service provider network provides the costumer a set of emulated leased lines, called virtual circuits, to interconnect the sites. On the other hand, in the Peer-to-Peer model the provider’s edge-routers directly exchange routing information with costumer routers. That fact simplifies costumer routing and bandwidth provisioning links, it is more scalable, and service provider can route packets more efficiently.

In the past, almost all organizations used to design Overlay VPN using layer 2 technologies as Frame Relay or ATM. Later the layer 3 Overlay VPN with GRE and IPSec became more popular, because it has the great advantage of the economical fares of internet connections. With the use of MPLS inside the IP backbones of service providers, the last generation of VPN technologies arrives.
MPLS networks have the advantages of VPN Peer-to-Peer model and also implement QoS for priority traffic. From the service provider’s point of view, MPLS allow several services over a single network, so traffic engineering can be applied to distribute traffic flows efficiently. Many customers decide to outsource their intra or extranet communications due to the great advantages of this service.

1.3. Network Topology

The design of the network model is composed of a central service LAN where we can find all the Intranet servers. There are four remote offices connected to the corporative intranet through the service provider network, and there are also four remote workers that will connect to the intranet using ISDN or xDSL links, depending on the technology of the service provider backbone.
The LAN model design simplifies the reality because the focus of this study is to analyze the WAN that interconnect all corporative LANs. For that reason, all LAN links and hardware are over provisioned to prevent any influence on the study.

The central LAN is composed of four servers supporting standard applications (FTP, Web, E-Mail and database) and several LANs that group 100 users. Everything is interconnected by a single switch.

![Central LAN topology](image3)

**Figure 3: Central LAN topology**

Remote offices are simpler than the central LAN and we can only find a pair of LANs of 50 users.

![Remote LANs topology](image4)

**Figure 4: Remote LANs topology**

For each technology the next scenarios have been defined:

- Frame Relay network
- ATM network
- Public IP network
- Private IP network
1- Frame Relay Network.


b. Hub-and-Spoke topology with double number of remote offices.

Figura 5: Figure 5: Frame Relay basic topology

The Frame Relay WAN network has been modeled with a frame delay represented by an exponential curve centered on 35 ms; that is the typical delay measured on these networks. Also, the 5% of EIR frames will be discarded.

After configuring the WAN node, the PVCs between remote office and central services have been defined with a committed CIR of 512 Kb and an EIR of 2 Mbps.

Figura 6: Figure 6: PVC configuration

The remote workers connectivity is achieved through ISDN links that connect to a RAS device. Frame Relay doesn’t permit integrating VPDN connections.
2- ATM Network.


b. Hub-and-Spoke topology with double number of remote offices.

**Figure 7: ATM topology**

The ATM WAN network has been modeled with a uniform cell delay from 30 to 40 ms; that is the typical delay measured on these networks. Also, the 5-10^-3 of cells will be discarded.

After configuring the WAN node, the SPVCs between remote office and central services have been defined. UBR is the defined contract traffic and AAL5 is used as an adaptation layer.

**Figure 8: SPVC configuration**

As in the Frame Relay scenario, the remote workers connectivity is achieved through ISDN links that are connected to a RAS device. ATM doesn’t permit integrating VPDN connections.
3- **Public IP Network: INTERNET.**


b. Hub-and-Spoke topology with double number of remote offices.

The Internet node has been modeled with a packet delay represented by an exponential curve centered on 250 ms; that is the typical delay measured on these networks. Also, the 5% of packets will be discarded.

As in the other Overlay model technologies, the virtual circuits between remote office and central services have been defined. In this case the virtual circuits are configured by the customer using tunneling techniques as IPSEC. The encryption and decryption procedures will add 100 ms to network delay. The tunnels operation mode is compulsory, so security is centralized on the Central LAN.

**Figura 9:** Public IP network topology

The Internet node has been modeled with a packet delay represented by an exponential curve centered on 250 ms; that is the typical delay measured on these networks. Also, the 5% of packets will be discarded.

**Figura 10:** VPN configuration
In this case, remote users can connect to the corporative network through Internet. In this scenario they will use ADSL links to access to Internet.

4- Private IP Network: MPLS


   b. Hub-and-Spoke Topology with double number of remote offices.

![Figure 11: Private IP network topology](image)

One of the advantages of this technology is its ability to integrate all kind of access links. In this model we use Frame Relay, ATM, ADSL, ISDN, and point-to-point leased links.

OPNET does not provide a WAN node with IP-MPLS features, and for that reason we had to model it manually. In the next figure we can observe the backbone design. It is composed of LERs (acting as edge routers), LSRs (in the core of the WAN), and gateways to other networks.
Figura 12: Figure 12: MPLS backbone design

Another limitation of OPNET 8.0 is that it is not possible to configure VPN as it is specified in the standard. It is necessary the implementation of VRF tables on the LER edge routers. We have used an alternative method to implement the VPN, using traffic engineering techniques. It consists on defining some conditions (FECs), that determine which VPN belongs to each packet and its destination. In all LERs that belong to the VPN, each FEC is assigned to a LSP that has been previously defined.

Figura 13: Figure 13: VPN configuration
1.4. Traffic Modeling

The traffic has been modeled in two different ways, with explicit traffic and with background traffic. The reason of this hybrid traffic model is that the explicit traffic makes the simulation very slow; so, in order to get a better simulation performance it is good to combine explicit traffic with conversation pair background traffic.

In the modeled scenarios background traffic represents the 90% percent of the total traffic. This traffic is increased during the simulation, to test the links and devices response to congestion. On the next figure, the background traffic between one remote office and the Central router is shown.

The explicit traffic is generated by users using standard applications, as HTTP, FTP, e-mail, and database access.
1.5. Simulation Results / Analysis

Here are the different results obtained in the simulation of the different scenarios. Also, an analysis of these results is given in order to compare the technologies and scenarios.

1- Frame Relay Network.


Frame Relay Delay

Frame Relay Residual Error Rate

DB Query Response Time

Figura 15: FR delay, residual error rate, and query response time in basic scenario

With a Frame Relay basic scenario the simulation results show a network that provides low frame latency and a low jitter, between 50 and 60 ms. There isn’t any discarded frame until traffic exceeds the committed CIR. The query response time is low at the fist moment of simulation, around 150 ms, but discarded frames cause great delays on application in the last part of the simulation.
b. Hub-and-Spoke topology with double number of remote offices.

**Frame Relay Delay**  
**Frame Relay Residual Error Rate**

![Frame Relay Delay and Residual Error Rate](image)

**DB Query Response Time**  
**Central Router CPU Utilization**

![DB Query Response Time and CPU Utilization](image)

**Figura 16: Figure 16: FR delay, residual error rate, query response time and central router CPU utilization in the double scenario**

In the double scenario the delay and the frame error rate are very similar to the basic scenario. Query response time has increased to the maximum values due to the bigger flow of traffic and the discarded frames.

The last figure is a comparison between the CPU utilization of the central router of each scenario. In the second scenario this parameter is 20 times bigger. In a real system we would probably have to change the actual router to a more powerful one. That fact gives us an idea that it is not a very scalable technology.
2- ATM Network.


**ATM Delay**

**ATM UBR Cell Loss Ratio**

![Graph showing ATM delay and UBR cell loss ratio](image)

**DB Query Response Time**

![Graph showing DB query response time](image)

*Figura 17: Figure 17: ATM delay, UBR CLR and query response time in the basic scenario*

With an ATM VPN the simulation results reflect a very good network performance. The ATM cell delay is very low (around 40 ms) and constant during all the simulation. During the simulation it has not been registered any loss of cell. The query response time is low and considerably constant, between 200 and 400 ms.
b. Hub-and-Spoke topology with double number of remote offices.

**ATM Delay**

**ATM UBR Cell Loss Ratio**

**DB Query Response Time**

**Central Router CPU Utilization**

**Remote Office IP Processing Delay**

**Remote Office Router CPU Utilization**

**Figura 18: Figure 18: ATM delay, UBR CLR, query response time and router utilizations in the double scenario**

In this scenario delay and error rate doesn’t change compared to the ATM basic scenario, but we can see that the response time has an important increase at the third part of simulation. To explain this fact, we can look at the CPU utilization of the
routers. In the central router comparison, the values are on the same order, around 50% (in the double scenario, central router has been modeled with a x5 speed factor) The problem is localized, then on the remote office routers. The CPU utilization is around 80%, causing additional delays of 1.5 s. So like Frame Relay, we also have problems when the network grows in the ATM double scenario.

3- Public IP Network: INTERNET.


![IP Delay vs Dropped Traffic](image)

**Figura 19: Figure 19: IP delay, dropped traffic and query response time in the basic scenario**

With the Internet scenario we have collected the worst network performance results. In this case the delay is 10 times bigger (between 500 and 700 ms) and the jitter increases too. The error rate is also higher, with a mean of 2 dropped packets per second. The response time has been increased in the same proportion as the network delay. The
query application has a latency between 1.5 and 2 seconds, that is a poor performance compared with the 250 ms mean latency of the previous scenarios

b. Hub-and-Spoke topology with double number of remote offices.

**Figure 20: IP delay, dropped traffic, query response time and utilization in the double scenario**

In the double scenario we can see that performance is degraded when the network grows. Network delay grows 100 ms and dropped IP packets are 4 times bigger. The response time is similar to the previous graphic of the basic Internet scenario. The network server comparison shows that in the second scenario the CPU utilization is two times the basic scenario, as it was supposed to be when it had to manage double volume of traffic.
Private IP Network: MPLS


**TCP Delay**

**IP Traffic Dropped**

**DB Query Response Time**

*Figura 21: TCP delay, dropped traffic and query response time in the basic scenario*

In MPLS scenario we achieve a medium performance, between ATM (or FR) and Internet scenario. In this case the simulation results show a variable low delay that goes between 30 and 70 ms. The mean dropped IP packet is around 0.5 packet per second, 4 times less than the Internet scenario with the same traffic. Response time of the query application is low and has a high jitter too, which goes from 50 ms to 150 ms.
b. Hub-and-Spoke topology with double number of remote offices

In the double scenario the results have not changed much respecting the basic scenario. The mean latency and response time has increased in some milliseconds. The dropped IP packets and Central Router CPU utilization has increased a 100%, as it was supposed when the network grows a 100% too. We can see that kind of networks can grow without problems.
1.6. Conclusions

Choosing a VPN technology depends in a high percentage on the applications that run over the network, the geographic situation of LANs and the economic cost. Depending on the organization requirement, we will have to decide which the best technology is.

On the one hand, traditional technologies as Frame Relay have the advantages of being mature, reliable and secure technologies. On the other hand, the link cost is expensive, and usually it is only appropriated for hub-and-spoke topologies, due to Overlay model limitations. For that reason these networks can have problems of scalability. The banks usually implement their networks with this technology, because they need this security and reliability to transport critical traffic.

ATM has similar features to Frame Relay. It is a mature and reliable technology but it has the Overlay model problems too. It can be used to transport big volumes of critical traffic, that need special QoS, or to transport multimedia communications.

New techniques of tunneling and encryption through Internet as GRE or IPSec are the cheapest option, but not very appropriated when a guaranteed SLA is needed. It is usually a good option to interconnect remote workers or SOHOs to corporative Intranet using ISDN, xDSL, or cable links. However, it is not recommendable to use this technology between the important sites of an organization.

Nowadays VPN services over service provider MPLS-IP backbones are the most flexible option. On the one hand, we can implement all kind of topologies without any restriction, it allows the integration of remote users on the same network and it can guarantee a level of service and apply QoS to priority traffic flows. The disadvantages of this service are that: it is not as cheaper as Internet VPN and also, you loose control of VPN network, because it is managed by the service provider.

In the last figure we can see the position of each technology in a cost / quality diagram. As simulation results show, IP-MPLS is the technology that takes more area and is more
flexible with costumer needs, but not always matches all organizations needs.

1.7. References


[8] www.opnet.com