A

Seminar report

On

VIRTUAL PRIVATE NETWORK

Submitted in partial fulfillment of the requirement for the award of degree of Computer Science

SUBMITTED TO:

www.studymafia.org

SUBMITTED BY:

www.studymafia.org

Preface

I have made this report file on the topic **VIRTUAL PRIVATE NETWORK,**I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to …………..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

ABSTRACT

This seminar report is about “VIRTUAL PRIVATE NETWORK for QUALITY of SERVICE”. In this we review today’s corporate networks and how VPN can be used for corporate networking.

These introduce with VPN Technology, its types, and also describe the various components, its need and functioning with its working in detail.

In this we mainly explain the quality of service for virtual private network, so that they explain why quality of service is needed? And its components are described. They provide an introduction to quality of service architecture for VPNs including rich classification, policing, shaping, queuing, and congestion avoidance.

In quality of service how its parameter are reflected from tunnel packets with their types.

In this we detail study about its advantages, disadvantages, features dedicated and benefit of the VPN. Also see how data kept secure with help of IP protocol.

INTRODUCTION

The wide spread migration towards the Internet Protocol creates a golden age for system integrators, network manager who are creating and implementing IP based Internetworking solution.

Employees on business trips need to stay current with their electronic mail. Sales represents in the field must be able to access corporate databases.
Branch offices must be part of the corporate network.

Virtual private networks (VPNs) offer low-cost, secure, dynamic access to private networks. Such access would otherwise only be possible by using an expensive leased line solution or by dialing directly into the local area network (LAN).

VPNs allow remote users to access private networks securely over the Internet. A remote user in one part of the UK can establish a secure network connection using a VPN to a school LAN in another part of the UK and only incur the call cost for the local Internet connection

Our aims to address the topic of quality of service (QoS) and the tools available for designing a Virtual Private Network (VPN) with appropriate service levels for mission critical applications. This is not meant to be a design guide but more of a glimpse into some of the QoS technologies available to help implement a successful VPN.

The audience is expected to be familiar with VPN related issues such as security, firewalls, and routing/switching.

This also provides an introduction to the end-to-end QoS architecture for VPNs, including rich classification, policing, shaping, queuing and congestion avoidance. And also touches upon the future of QoS policy deployment using Common Open Policy Service (COPS) and Cisco QoS policy servers.

.

CORPORATE NETWORK USING VPN :

Companies whose facilities are spilt between two or more location can connect into a single logical network through the use of VPN.

Using the Internet as the communication backbone, and by authenticating and encrypting data transmissions through secure tunnels ,a new level of integration for physically distinct networks can be created.

This new technology dubbed as VPN , is an exciting new function that enables distant workgroups to communicate efficiently and securely across the Internet.

VPN PHILOSOPHY

What is a VPN?

A virtual private network gives secure access to LAN resources over a shared network infrastructure such as the internet. It can be conceptualised as creating a tunnel from one location to another, with Encrypted data traveling through the tunnel before being decrypted at its destination.

Remote users can connect to their organisation's LAN or any other LAN. They can access resources such as email and documents as if they were connected to the LAN as normal. By using VPN technology it is possible to connect to a school LAN from anywhere in the world via the internet, and to access it securely and privately without incurring the large communication costs associated with other solutions.

One user uses a 56 kilobits per second (Kbps) modem to dial their internet service provider (ISP) and connects to the central LAN with VPN software. A remote site uses ADSL (asymmetric digital subscriber line) to connect to its ISP and a VPN router (a hardware solution) to carry out the VPN connection Few changes are made to the PCs at the remote site and the VPN router carries out the encryption and decryption of data. As both connect to their usual ISP, they only incur their normal ISP call tariffs.

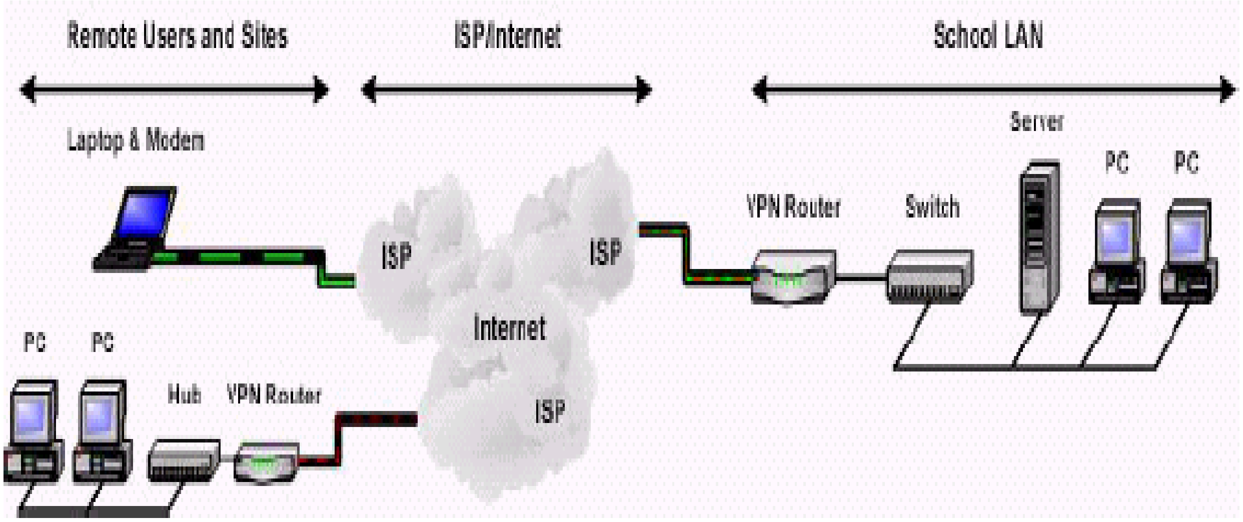


Figure 1: two methods of connecting to a school's LAN using a VPN

In figure 1 two method connected that is one user uses a 56 kilobits per second modem to dial their internet service provider and connects to the central LAN with VPN software.

Second is a remote site uses asymmetric digital subscriber line to connect to its ISP and VPN router to carry out the VPN connection. Few changes are made to the PCs at the VPN router carries out the encryption and decryption of data. As both connect to their usual ISP, they only incur their normal ISP call traffic

What does the term virtual private network really mean? Virtual:

It means that the connection is dynamic. It can change and adapt to different circumstances using the internet's fault tolerant capabilities. When a connection is required it is established and maintained regardless of the network infrastructure between endpoints. When it is no longer required the connection is terminated, reducing costs and the amount of redundant infrastructure.

Private:

It means that the transmitted data is always kept confidential and can only be accessed by authorised users. This is important because the internet's original protocols –TCP/IP (transmission control protocol/internet protocol) – were not designed to provide such levels of privacy. Therefore, privacy must be provided by other means such as additional VPN hardware or software.

Network:

It is the entire infrastructure between the endpoints of users, sites or nodes that carries the data. It is created using the private, public, wired, wireless, internet or any other appropriate network resource available.

What types of VPN are there?

There are many variations of virtual private networks, with the majority based on two main models:

Remote access:

(Virtual private dial-up network (VPDN) or client-to-site)

A remote access VPN is for home or travelling users who need to access their central LAN from a remote location. They dial their ISP and connect over the internet to the LAN. This is made possible by installing a client software program on the remote user's laptop or PC that deals with the encryption and decryption of the VPN traffic between itself and the VPN gateway on the central LAN.

Fixed:

(Intranet and extranet or site-to-site)

A fixed VPN is normally used between two or more sites allowing a central LAN to be accessed by remote LANs over the internet or private communication lines using VPN gateways. VPN gateways (normally a VPN-enabled router) are placed at each remote site and at the central site to allow all encryption and decryption and tunneling to be carried out transparently.

- **Internets:** They are carrying corporate traffic and creating the need for more meshed traffic patterns.
- **Extranets:** They are an integral part of communications with your customers and partners.

What does a VPN consist of ?

As VPN topologies can vary greatly there is no standard for a definitive VPN. However, it is possible to specify what each main component of a VPN does:

VPN gateways: create the virtual tunnels that the data passes through, carrying out the encryption before transmission and decryption at the other end. Gateways can be software, or built into a firewall, or a server or router or a dedicated appliance.

Security servers: maintain the access control list (ACL) and other user-related information that the security gateway uses to determine which traffic has authorised access.

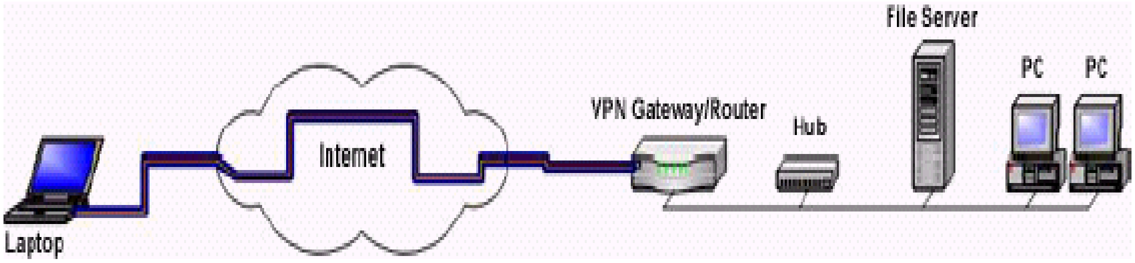
Keys: used for the encryption and decryption of data. Sites can choose to maintain their own database of digital certificates (keys) for users by setting up a certificate server, or they can use an external certificate authority.

Network: there must be an internet infrastructure at both ends to provide the actual transmission medium. Some of these components may be built into a single device or spread over many devices over several sites.

How does a VPN work?

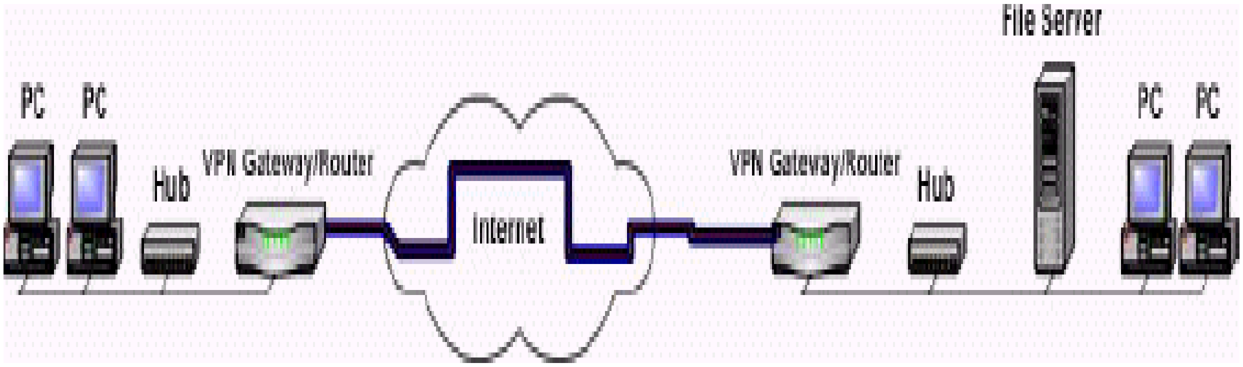
A remote access solution works by the remote user first establishing an internet connection to an ISP in the normal way. The user activates the VPN client software to create a tunnel over the internet and to connect to the central LAN's VPN gateway. The VPN client software then passes its authorization to the VPN gateway. The VPN gateway checks that the user is authorised to connect and then ensures the encryption key from the remote client is valid. All VPN data is encrypted using the key before being transmitted over the internet using a tunneling protocol. It is decrypted at the other end by the VPN gateway, which has an identical set of keys to decrypt the data. Data sent from the central LAN to the remote user is encrypted by the VPN gateway before transmission and decrypted by the remote user's VPN client software.

Fig 2:remote access VPN solution



A fixed solution works by first establishing a VPN gateway at each site. Each VPN gateway has the same key to encrypt/decrypt data and knows the IP addresses of the other sites, so they know where to transmit the data to, and where to expect secure VPN transmissions from. This flow of data is transparent to the users and requires little actual configuration on the PCs.

Figure 3:a fixed VPN solution



The choice of ISP is very important when implementing a VPN solution as it can have a major impact on VPN performance. It may be advisable for all VPN users and sites, including the central LAN, to use the same ISP for their internet connections. This will lessen the amount of data that needs to cross into the networks of other ISPs, which could degrade performance. Most ISPs will offer a service level agreement (SLA) that agrees network uptime, latency, security and other functions. It is important to read the SLAs carefully before deciding which ISP will give the fastest and most reliable service.

The Need for VPNs:

VPNs aim to give the remote corporate user the same level of access to corporate computing and data resources as the user would have if she were physically present at the corporate headquarters. By reducing the costs of transporting data traffic and by enabling network connections in locations where they would not be affordable, VPNs reduce the total cost of ownership of a corporate network.

QUALITY OF SERVICE

The Need for QoS:

Users of a widely scattered VPN do not usually care about the network topology or the high level of security/encryption or firewalls that handle their traffic. They don't care if the network implementers have incorporated IPSec tunnels or GRE tunnels.

What they care about is something more fundamental, such as:

Do I get acceptable response times when I access my mission critical applications from a remote office?

Acceptance levels for delays vary. While a user would be willing to put up with a few additional seconds for a file transfer to complete, the same user would have less tolerance for similar delays when accessing a database or when running voice over an IP data network.

QoS aims to ensure that your mission critical traffic has acceptable performance. In the real world where bandwidth is finite and diverse applications from videoconferencing to ERP database lookups must all vie for scarce resources, QoS becomes a vital tool to ensure that all applications can coexist and function at acceptable levels of performance.

QoS for VPNs:

The primary QoS building blocks of VPNs are:

- Packet classification (using Committed Access Rate [CAR])
- Bandwidth management (policing with CAR, shaping with GTS/FRTS, bandwidth allocation with WFQ)
- Congestion avoidance (with WRED)

Packet Classification:

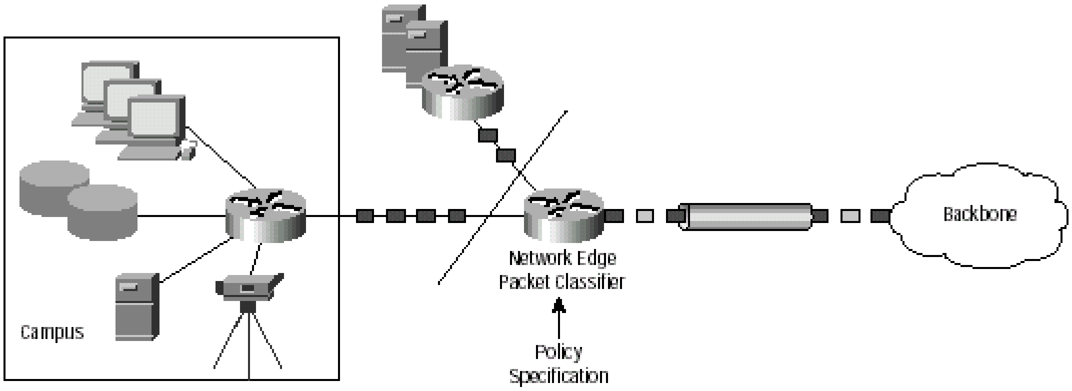
The aim of packet classification is to group packets based on predefined criteria so that the resulting groups of packets can then be subjected to specific packet treatments. The treatments might include faster forwarding by intermediate routers and switches or lesser probability of the packets being dropped due to lack of buffering resources.

It is necessary that traffic be classified before tunneling and encryption since otherwise the tunnel header that is appended to the IP packet would make the QoS markings in the IP header invisible to intermediate routers/switches, which need to read this information and act upon it. Classification brings into question the right match criteria.

There are a number of criteria based upon which we may classify traffic before it enters the VPN:

- IP addresses
- TCP/UDP port numbers
- IP precedence (3 bits in the type of service field of the IP packet header)
- URL and sub-URL
- MAC addresses
- Time of day

Figure 1: Classification at network ingress



Once we classify packets based on the above criteria the next step is to "mark" or "color" packets with a unique identification to ensure that this classification is respected end to end. The simplest way of doing this is via the IP ToS field in the header of an IP datagram. In the near future the Internet Engineering Task Force (IETF)- sponsored Differentiated Service Code Points (DSCP) could become the classification criterion of choice.

The purpose behind this type of marking of packets is to ensure that downstream QoS features such as scheduling and queuing may accord the right treatment for packets thus marked. In some cases the service provider whose backbone is being used for the VPN might provide differentiated services, classification allows you to leverage these services.

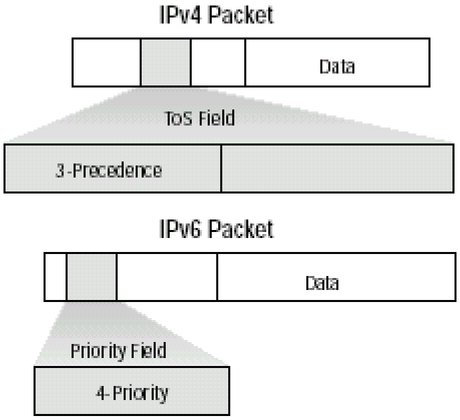


Figure 2 : ToS field in the IP Packet header

Differentiated services allow certain network traffic to receive premium treatment at the expense of other less-critical traffic on the same wide area network (WAN) link. This idea is similar to what we find in airlines where a first-class passenger may receive better treatment or service than an economy-class passenger while they both physically reside on the same airplane.

Bandwidth Management :

Once traffic has been classified the next step is to ensure that it receives special treatment in the routers. This brings into focus scheduling and queuing.

Before we get into the subject of queuing it might be good to step back and consider what we mean by a flow. For this discussion a flow would be a group of packets which share a common criteria whether that criteria is a source/destination IP address or a TCP/UDP port number or a protocol or a type of service (TOS) field.

They provides two implementations of weighted fair queuing (WFQ):

- Flow-based WFQ.
- Class-based WFQ.
- Traffic shaping.

Flow-based WFQ :

In this packets are classified by flow. Each flow corresponds to a separate output queue. When a packet is assigned to a flow, it is placed in the queue for that flow. During periods of congestion, WFQ allocates a portion of the available bandwidth to each active queue.

Class-based WFQ :

Its aims for providing weighted fair queuing functionality among traffic classes defined by the user. A user could create traffic classes using mechanisms like Access Control Lists (ACLs) and then assign a fraction of the output interface bandwidth to each of these traffic classes.

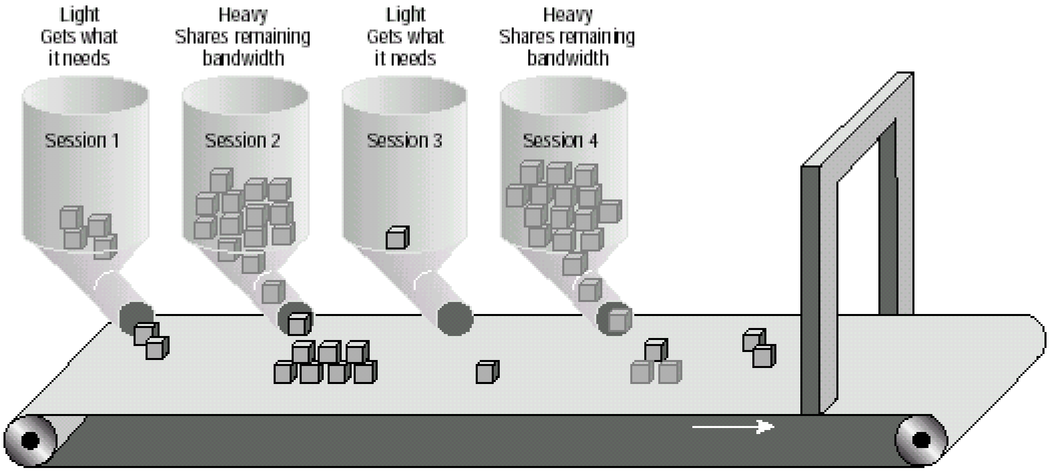
The primary difference between flow-based WFQ and class-based WFQ is the fact that in flow-based WFQ bandwidth allocation is relative to other flows. But in class-based WFQ bandwidth allocation is absolute. Class-based WFQ allows the user to assign bandwidth to a class based upon a percentage of the available bandwidth or a fixed kbps value.

When to Use Class-Based WFQ Versus Flow-Based WFQ

Flow-based WFQ as it existed in Cisco IOS did not differentiate between traffic

classes. As far as flow-based WFQ was concerned a packet was part of a flow. The flow could be based on source/destination address, TCP/UDP port number or some other criteria. There was no real bandwidth guarantee since the weights were assigned based on IP Precedence. There was no way to ensure that Hyper Text Transport Protocol (HTTP) based web traffic would have a higher guarantee of bandwidth over traffic conforming to FTP (File Transfer Protocol).

Figure 3 : Weighted Fair Queuing



Class-based WFQ gives users the following benefits which were not possible with flow-based WFQ:

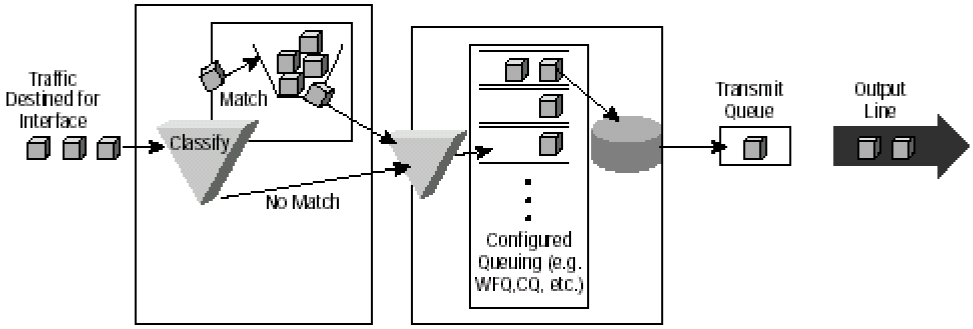
- Bandwidth guarantees for an application
- User defined traffic classes
- In conclusion flow-based WFQ provides QoS guarantees that are relative to other flows whereas class-based WFQ provides for absolute QoS guarantees.

Traffic Shaping :

Traffic shaping becomes necessary when Layer 3 traffic must be shaped to a desired set of rate parameters to enforce a maximum traffic rate. The result will be a smooth traffic stream[1]

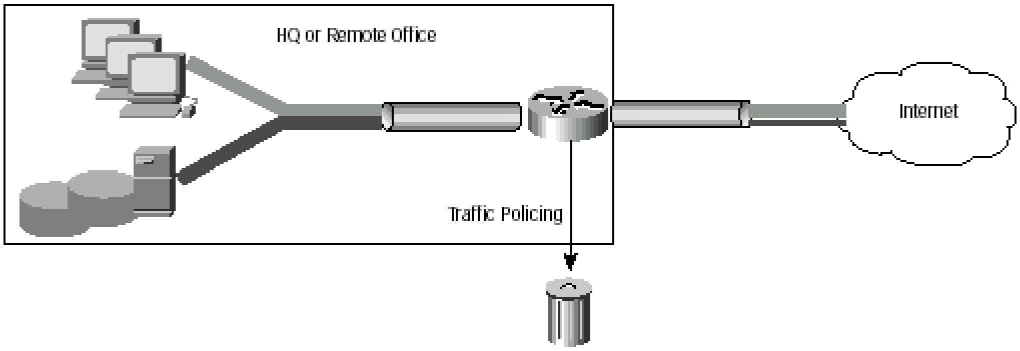
Traffic shaping queues and forwards data streams (as opposed to dropping excess traffic) so as to conform to agreed upon Service Level Agreements (SLAs).

Figure 4 : Generic Traffic Shaping


Traffic Destined for Interface
Match
Classify
No Match
Configured Queuing (e.g. WFQ,CQ, etc.)
Transmit Queue
Output Line

The idea behind traffic shaping is that if bursty traffic (characterized by fits and starts) is queued then the TCP senders will realize this and in turn will back off and ensure that subsequent transmissions conform to a desired rate. This type of traffic is commonly referred to as adaptive traffic. The end result of traffic shaping is a smoothed packet stream.

Figure 5 : Policing traffic



When to Use a Traffic Policer Versus a Traffic Shaper :

Policing literally means to drop excess traffic, shaping on the other hand allows the excess traffic to be queued. To an application shaping is usually a better choice since shaped traffic does not require re-transmission while dropped traffic would require a re-transmission. In such cases Cisco Generic Traffic Shaping (GTS) is the tool of choice.

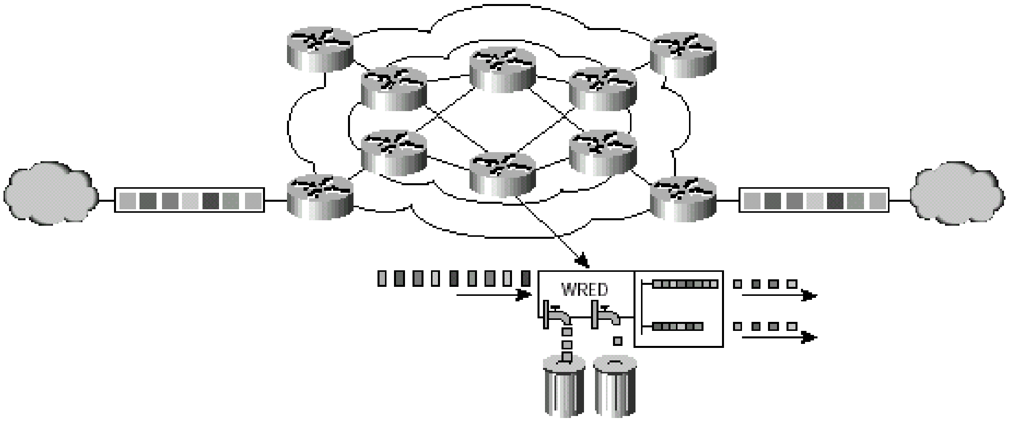
However if you shape in every instance then you might end up with very deep queues in a router which might result in re-transmission by the sender due to perceived delay. Policing/dropping of excess traffic is better suited to IP multicasts or to TCP-based traffic related to non-mission critical applications.

Congestion Avoidance :

Congestion avoidance could be defined as the ability to recognize and act upon congestion on the output direction of an interface so as to reduce or minimize the effects of that congestion.

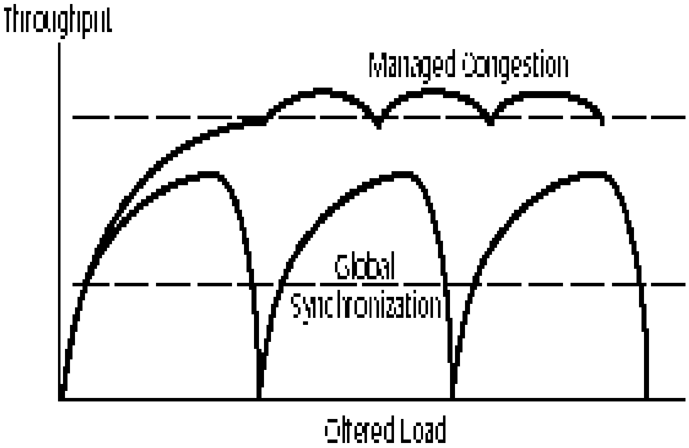
Congestion produces adverse effects in a VPN and should be avoided. With this is mind Cisco Systems provides IOS based tools like Weighted Random Early Detection (WRED) which is a Cisco implementation of the Random Early Detection (RED) algorithm. WRED provides for differential treatment of traffic by adding per-class queue thresholds which determine when packet drops will occur. The thresholds are user-configurable and set using the command line interface (CLI) in Cisco IOS.

Figure 6: Weighted Random Early Detection



Packet dropping is based upon the premise that adaptive flows such as TCP will back off and retransmit if they detect congestion. By monitoring the average output queue depth in the router and by dropping packets from selected flows WRED aims to prevent the ramp up of too many TCP sources at once. Unchecked this ramping up could result in problems such as TCP synchronization.

Figure 7: Global TCP synchronization



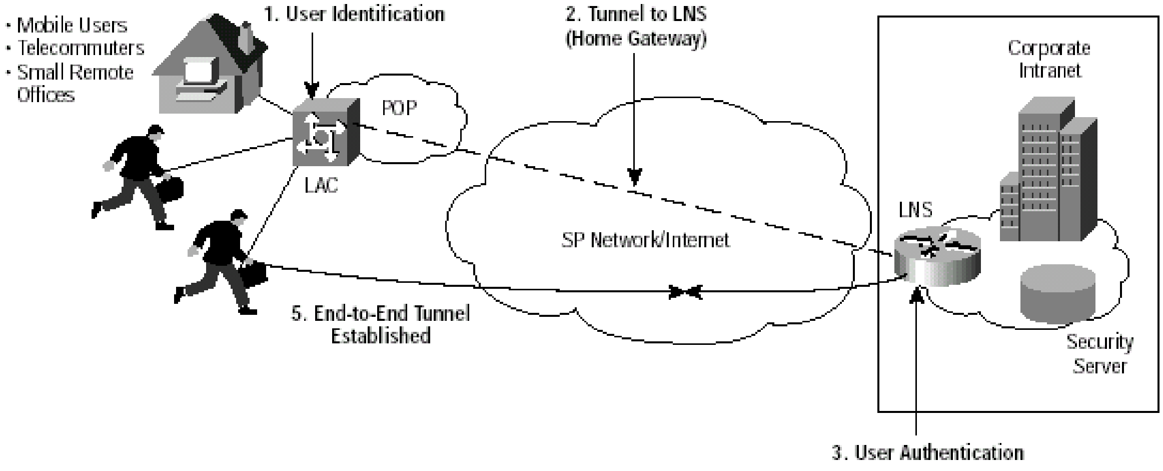
WRED provides for differential treatment by dropping packets from low priority traffic before it begins to drop packets from high priority traffic. WRED allows the user the option to select up to six such traffic classes (standard and premium being just two used for illustrating the point).

QoS for VPN TUNNELS

The QoS issue here is that the QoS parameter normally found in the header of the IP packet should be reflected in the tunnel packet header regardless of the type of tunnel in use. Consider the four primary tunneling protocols relevant to VPNs:

1. Layer 2 Tunneling Protocol (L2TP) Tunnel
2. IP Security (IPSEC) Tunnel
3. Layer 2 Forwarding (L2F) Tunnel
4. Generic Route Encapsulation (GRE) Tunnel

Figure 1 : L2F/L2TP Operation



Layer 2 Tunneling Protocol (L2TP) is commonly used for node-to-node applications where the tunnel terminates at the edge of the user's network. L2TP is an IETF based standard which merges Cisco's Layer 2 Forwarding (L2F) Tunnel protocol with Microsoft's Point-to-Point Tunneling (PPTP) protocol.

L2TP relies on 3rd party security schemes like IPSEC to secure packet level information. L2TP was designed primarily for Point to Point Protocol (PPP) traffic.

Generic Route Encapsulation (GRE) tunnels based on RFC 1702 allows any protocol to be tunneled in an IP packet. Today Cisco offers support for encapsulation of data using either IPSEC or Generic Route Encapsulation (GRE).

In either of these cases Cisco IOS offers the ability to copy the IP ToS values from the packet header into the tunnel header.

This feature which appears in IOS ver 11.3T allows the Type of Service (ToS) bits to be copied to the tunnel header when the router encapsulates the packets using GRE.

It allows routers between GRE-based tunnel endpoints to adhere precedence bits thereby improving the routing of premium service packets.

Advantages and Disadvantages of a VPN

Virtual private networks have a number of advantages and disadvantages over direct dial or leased line solutions.

Advantages:

1. VPNs authenticate all packets of data received, ensuring that they are from a trusted source.

   Encryption ensures that the data remains confidential.

2. Most VPNs connect over the internet so call costs are minimal, even if the remote user is a great distance from the central LAN.

3. Multiple telephone lines and banks of modems at the central site are not required.

4. A reduction in the overall telecommunication infrastructure – as the ISP provides the bulk of the network.

5. Reduced cost of management, maintenance of equipment and technical support.

6. Simplifies network topology by eliminating modem pools and a private network infrastructure.

7. VPN functionality is already present in some IT equipment.

8. VPNs are easily extended by increasing the available bandwidth and by licensing extra client software.

9. If a LAN uses NetBeui or IPX/SPX (both incompatible with the internet) instead of TCP/IP to transmit data to its clients, the VPN gateway can encapsulate these languages into an IP packet and transmit it over the web to another VPN gateway.

Disadvantages:

1. If the ISP or Internet connection is down, so is the VPN.

2. The central site must have a permanent internet connection so that remote clients and other sites can connect at anytime.

3. VPNs may provide each user with less bandwidth than a dedicated line solution.

4. Existing firewalls, proxies, routers and hubs may not support VPN transmissions.

5. The internet connection of the central site must have sufficient bandwidth to cope with VPN traffic, the internet connections originating from the central site and any other traffic such as email and FTP (file transfer protocol).

6. VPN equipment from different manufacturers may comply with different standards.

Any institution that has users who connect to a LAN from a remote location, or which requires its users to connect to a central LAN, should consider implementing a VPN solution. It is considered to be a superior alternative to long-distance dial-in and leased lines; VPNs can be used securely to carry information at a fraction of the cost of other solutions. An institution can reduce its connection and maintenance costs by replacing banks of modems and multiple leased lines with a single link that carries remote access and fixed VPN traffic along with existing internet traffic.

FEATURES of a VPN

It gives reasonable to expect that a fixed hardware VPN, which covers multiple sites, should have more features than a software remote access solution.

Some of the main features are:

1. **AAA** – authentication (who is the user), authorization (what is the user allowed to do) and accounting (recording what the user actually does).

2. **Security –** tunneling support between sites with at least 128bit encryption of the data.

3. **Scalability** – extra users and bandwidth can be added easily to adapt to new requirements.

4. **Services** – quality of service features, including bandwidth, management and traffic shaping, are important to avoid congestion.

5. **Management** – reports on user activity, management of user policies and monitoring of the VPN as a whole.

There are many different VPN manufacturers and it is important to be aware that their products are sometimes incompatible because of the protocols used or the lack of standardized testing.

VPN use dedicated hardware or software:

HARDWARE:

Some VPN solutions use dedicated hardware appliances that are specifically designed for the tasks of tunneling, encryption, and user authentication. These devices usually operate as encrypting bridges and they are often placed between the routers on the networks. Although most of these hardware tunnels are designed for fixed configurations, some products also support remote access tunneling. Many of these products perform very well on throughput and when handling large numbers of simultaneous tunnels, which is crucial for supporting a large number of users. Hardware solutions are generally considered to be more secure and provide good logging and reporting options.

SOFTWARE:

One user between a remote client and a security gateway can install VPN client software on laptops and individual PCs for use. VPN software may be used on a server that will act as a VPN gateway for an entire site to create and manage tunnels between a pair of security gateways.

These VPN software systems are often good low-cost choices for networks that are relatively small and which do not have to process a lot of traffic. Such solutions can run on existing servers, share resources with existing applications and serve as a good starting point for getting familiar with VPN Many of these systems are well suited for remote access connections. Software-based VPN solutions allow great flexibility in terms of implementation and usage, but flexibility brings extra management and support costs.

The impact and benefits of VPNs

VPNs allow institutions to take advantage of the Internet's infrastructure for secure, private communications between schools, remote sites, and home-based workers. Access to a school's

LAN is entirely possible from home before, during or after school hours. A user can access all of resources on the LAN as if they were actually on site.

A VPN solution can reduce the need for dedicated equipment by using existing Internet equipment. VPNs are scalable solutions, which allow new users to be added without major restructuring. . An SSL-based VPN does away with the need for VPN software to be installed on the users' PCs, although the applications that can use are limited to those available in a web-enabled format.

Implementing a VPN solution for school links would be extremely beneficial, allowing a large number of users to access a school's network from home while requiring very few changes to be made to the existing LAN infrastructure.

SECURITY

VPN keep the data secure

TCP/IP is not designed for security, so VPNs use a mix of IP protocols and systems to provide the best security solution for each type of connection. Some protocols encrypt the packets of data while other protocols protect the packet whilst it is being transmitted. Some of the more popular protocols and systems that a VPN uses to keep the data secure are:

1. **PPTP (point-to-point tunneling protocol**)

Creates a virtual tunnel for connections which, along with L2TP (layer two tunneling protocol) and L2F (layer two forwarding), is used mainly for remote access VPNs.

2. **IPSec (internet protocol security)**

Is becoming the most commonly used security option for fixed VPN solutions. Each packet of data is encrypted and has an authenticating stamp verifying its origin. This makes IPSec a very secure option. IPSec works in one of two ways:

3. **TRANSPORT MODE**

In this mode only the payload portion of the packet is encrypted. (The payload consists of the actual data that is being transmitted.)

4. **TUNNEL MODE**

The entire packet, including the header is encrypted. (The header contains the source and destination IP addresses.)

5. **ENCRYPTION STANDARDS**

DES (data encryption standard) and 3DES (triple DES) secure the data to different levels ranging from 56- to 168-bit encryption

6. **AUHENTICATION SYSTEMS**

Prove that the sender of the packets is genuine and not a hacker attempting to deceive the receiver by intercepting and altering the packets before they arrive at their destination.

7. **PKE (public key encryption)**

PKE can be used with VPNs. Instead of manually entering encryption codes, internet key exchange (IKE) allows keys to be automatically exchanged – which is useful on larger networks.

There are many ways to protect the data during transmission. Most VPN solutions use either encryption or authentication for data security. As the security level increases so does the time required to process and assemble each packet. The typical overhead for VPN encryption during web browsing is 20 per cent; other user applications that run over VPNs may increase the overhead significantly more. To alleviate this problem some VPN systems compress data before sending to improve network performance.

VPN be used to secure a wireless network

As a VPN encrypts data from one point to another it is ideal for use over a wireless local area network (WLAN). However, it is worth noting that the biggest cause of WLAN security problems is the network not being made secure at time of installation, either by bad installation practices or lack of knowledge of the product. Further information about installing and configuring WLANs can be found in Becta's WLAN technical document

CONCLUSION

As we have gone through all possible details we conclude that VPN is the best option for the corporate networking.

As many companies need to have access to Internet and hence security is also the main concern. VPN provides best possible combination of security and private network capabilities with adequate cost –saving to the companies who are presently working with leased lines.

Many tools are available today to help you manage WAN links. These range from Quality of Service tools for traffic classification, Policing/Shaping, Bandwidth Allocation, and Congestion Avoidance.

The IETF diffserv efforts provide the basis to extend enterprise QoS policy into the SP network Cisco intend to participate and monitor these effort to ensure that our QoS meets this new model's criteria for end to end QoS.

BIBLIOGRAPHY

[1] http://www.ictadivice.org.uk, June 2003.
Technical paper "Virtual Private Network"

[2] http://www.cisco.com/offices, 2002.
White Paper "Quality of Service for Virtual Private Network".

[3] L. Keng Lim and Prastant Chandra "Customization Virtual Private Network Service with Quality of Service" Carnegie Mellon University Pittsburgh, August 2000