Virtual Private Networks for Windows

Department of Innovation, Design and Engineering
Mälardalen University
Västerås, Sweden

Mehrdad Saadatmand
msd06002@student.mdh.se

Abstract

Connection between branches of a company or organizations and remotely logging to a private network like an office network have always been an important need for expanding companies and traveling employees. This need can be strongly felt in those companies who intend to grow bigger and bigger and create branches in different locations. Several solutions are available to provide this access, like dial-up. But dial-up connections although secure, have their own limitations in terms of price, bandwidth and stability especially for long distance connections. On the other side, the Internet provides a much cheaper and worldwide connection with so many public networks and computers. So if companies can somehow connect to their branches through this already available worldwide connection, they can not only save lots of money but also get several benefits of local access to the Internet like higher bandwidth and availability. Although this idea looks very great at the beginning, but it opens private networks to a bunch of threats when connections to them are made through a public infrastructure like the Internet. This is exactly where *Virtual Private Networks* come to the rescue; to not only enable companies and people to connect to their private networks remotely through the Internet but also to do it in a secure way.

1. Introduction

Not so long ago, Internet was considered mainly a big source of information which allowed users to easily search and find the information they needed. Today, although this feature of Internet has made lots of improvements, but Internet has got other main roles and in particular it is considered an important means of communication. With technologies like E-mail, Instant messaging, video conferencing and etc., Internet has become a part of people's daily life in terms of communication. The facilities provided by the use of Internet, have their main impact on organizations and companies, and business world has incredibly benefited from Internet. E-business, E-market and terms of this kind are no longer strange words for even ordinary people. Booking travels, shopping and even receiving medical care through Internet today are not considered very complicated and special and one can easily see many people using such services in their daily life.

Along with its fast expansion and improvements, the risks in data transfer and security issues on Internet have also become a hot topic. Handling and storing personal information of users and charging credit cards are some of the security issues which are of great importance for end users. But security issues become more and more complicated and essential when it comes to connections between organizations, branches of companies and governmental institutes. For many of them, loss and disclosure of information could lead to bankruptcy, political problems and issues of this size and importance. So while they need to have interconnections, they also require a trusted and secure infrastructure for their communications especially when it is done through the Internet. One of the elegant technologies devised to solve such problems is *Virtual Private Networks* technology or in short *VPN*.

In this paper, different aspects of Virtual Private Networks from its importance to its usage and implementation are discussed.

2. Virtual Private Networks versus Dial-up

As mentioned earlier, virtual private networks came to solve the problem of communication between branches of companies, organizations and institutes but VPN is not the only solution. While there is just a local network, there are not so many problems of the kind discussed before. But if the company grows and establishes branches in different locations (different cities, states, countries or even continents), and the need for connection between these branches arises, then it has to deal with lots of new issues.

One of the solutions available to provide such a connection between branches is to use a Dial-up connection. Everyone is familiar with the term dial-up as it was once the only way to connect to the Internet (through ISPs). Dial-up connections have some special features. A dial-up connection is a direct connection between two systems. So it does not bear security issues that may be faced in establishing connections across the Internet. But they have a very big problem: cost! While for a connection between two networks located in a city (as an example), this cost may not show its importance, but when these networks are located in farther locations like two countries, this will become a very critical issue. In contract, access to the Internet is very cheap (and it is getting cheaper and cheaper), since it is established locally and also on the other side, many companies however need access to the Internet for their daily

tasks, so using Virtual Private Networks technology will be a better solution for them, since it is established through their already available Internet connection and this way it saves them lots of money.

3. How Virtual Private Networks work

A VPN connection is logical (virtual) in that, there is no real and direct physical connection between the two end points and it does not exist physically. When a VPN connection is established and computers start to communicate through it, packets which are sent will be encrypted and changed. 'Private packets' which are to be sent to the other network are first packed into a new public packet which allows them to transfer over the physical network (routers) which exists between the source and destination. Thus, this intermediate physical connection becomes transparent to the sender and receiver. Packets are decrypted when they reach the destination network and forwarded to the right computer. In general the role of VPN in this scenario is divided into two main parts: Encryption (security) and Tunneling. In VPN it is possible to use different protocols and technologies to secure the connection and encrypt data.

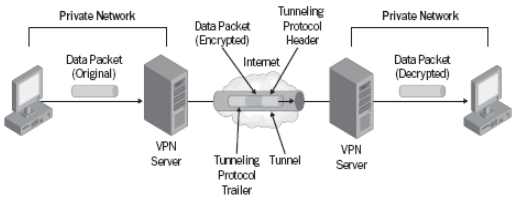

Figure 1: VPN in action [1]

In terms of end points, VPN can have two models: Remote access VPN [1] and Site-to-Site [2] (Router to Router [1]) VPN. The first case is when someone (a user) uses VPN to log into a network and in the latter case the routers in two networks establish a VPN connection between each other. An example for remote access VPN could be an employee who is on a trip and wants to remotely log into the local network of his company, but two branches of a company use site-to-site VPN connection to provide connectivity and unity of the branches. In remote access VPN as soon as the connection is established, to the user it seems that he has logged in locally and he will have access to the resources on the network; of course according to his account's permissions. It is possible to test this transparency by using the *tracert* command as follows:

C:\> tracert <target_computer>

When you run this command you will see interesting results. The output does not contain any intermediate nodes in it, and you feel you are directly connected to your destination network. This is because each of the packets is encapsulated as data section in another packet (with necessary IP addresses for routing) and then is sent out through the Internet. In the destination network, this data is extracted and routed to the target computer according to the information in the header of this original extracted packet. This is why when you perform a trace route to the target computer; you do not see the real physical routers/networks on your way to the target.

4. VPN Protocols

There are several protocols used in implementing Virtual Private Networks. Among the most famous are 'Point to Point Tunneling Protocol' (PPTP), 'Layer 2 Tunneling Protocol' (L2TP), IPSec, MPLS, L2F and etc. In this paper the main focus will be on PPTP and L2TP/IPsec. Each of these protocols provide different sets of features, but in general they may offer features like '*confidentiality (encryption)*', '*data integrity*' and '*data origin authentication*'; some experts also add '*anti replay*' feature to this list. Providing confidentiality means packets are encrypted and you cannot decrypt them without having the necessary keys. Besides confidentiality, VPN protocols which provide data integrity use a mechanism to make sure that packets are not tampered with and modified and data origin authentication feature guarantees that packets come from a recognized and authorized sender. The term 'anti replay' means that if the data which is transferred in a VPN connection is sniffed and captured, it should be impossible to 'play' the recorded packets to fool the target system.

In general, VPN protocols work on the second layer of the OSI model (Data Link Layer) and make use of protocols like Point to Point Protocol (PPP), which is a layer two protocol; the main functionalities of this layer include operations like framing of packets, CRC error checking and physical addressing (MAC).

4.1 Point to Point Tunneling Protocol (PPTP)

PPTP is considered a simple VPN protocol in that it provides only one of the features which a VPN protocol can offer: Confidentiality (encryption). So this protocol is considered less secure in comparison to protocols like L2TP, but on the other hand it is very simple to implement and does not include complexities of L2TP. PPTP makes use of 'Microsoft Point to Point Encryption' (MPPE) to provide encryption between the two ends of the VPN connection.

When a packet is generated to be sent across the Internet through a VPN connection, PPTP takes this packet and encrypts it, then according to a standard named '*Generic Routing Encapsulation*' (GRE: IP protocol 47 [1]), this packet will be encapsulated and an IP header is then added to enable it to be routed correctly through the intermediate networks and routers [1] [2]. You can see an illustration of this process in figure 2.

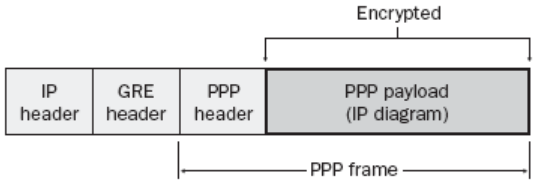

Figure 2: creation of a PPTP packet [2]

As is shown in figure 2, the original packet is treated as data in the new packet and it will be extracted when it reaches its destination and there, routing inside the target network will take place according to the information inside this original extracted packet and it will be finally given to its specified machine.

PPTP uses GRE V2 for encapsulation [3] which is a modification to standard GRE [2] and also to transfer the data it uses TCP port number 1723 [1] so when you want to use it from behind a firewall you should make necessary changes according to these facts in your packet filtering rules. Another interesting and also important fact is that since the original packet is considered as data and necessary IP headers are added to it, so it is possible to use different kinds of protocols in our internal networks while using the Internet; like IPX/SPX, AppleTalk and etc. [3].

In PPTP, for encryption a key is created based on a hash string of the user's password from the authentication phase. This phase (encryption) occurs after the authentication phase of PPP connection, so the encryption system depends on how strong a user's password is (vulnerable to 'dictionary attacks' [2]). From this aspect also PPTP is said to be weaker in security issues. But as mentioned earlier, it is simple to configure and still can be a good choice for many people who want to create a VPN connection [2].

In figure 3 a sample packet capturing done on our test system is shown. GRE and PPP information of packets can be seen in this picture. All the real information are packed and encrypted according to GRE standard, so if you try to capture packets which are sent out from your network, you will see something similar to the following screenshot and the content of the original packets will remain encrypted until they reach their destination network.

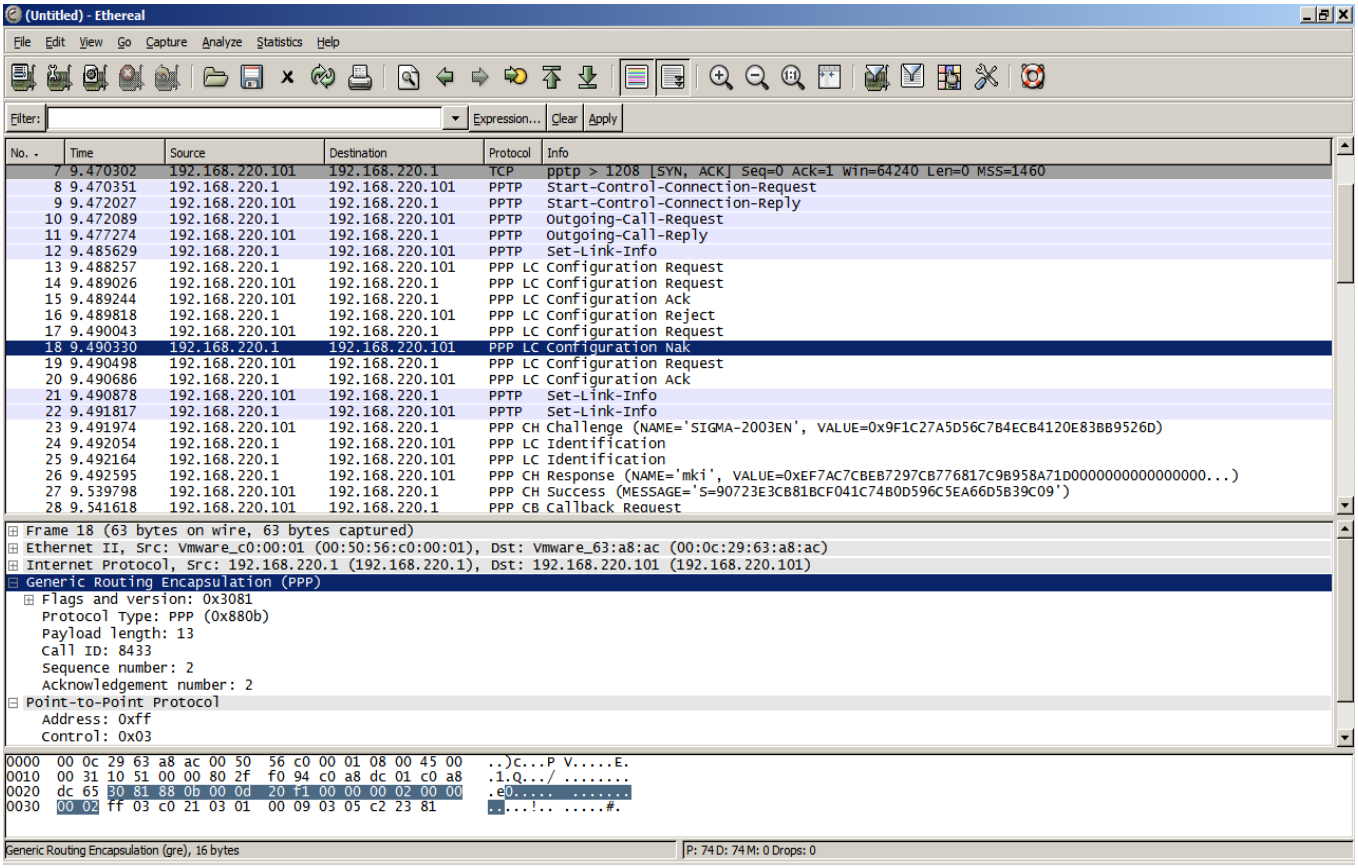

Figure 3: Sample packets captured on a VPN connection (initialization phase)

4.2 Layer 2 Tunneling Protocol (L2TP)/IPSec

First of all, it is important to know that L2TP in itself does not provide any of the listed features of VPN protocols and is just a mere tunneling protocol. But when it is combined with IPSec, it can benefit from the features that IPSec provides. So if you read articles on L2TP, most of the times you see it as L2TP/IPSec. L2TP/IPSec, unlike PPTP, does not use MPPE and GRE for encapsulation and encryption of packets, and uses IPSec encapsulation method instead which is called '*Encapsulation Security Payload*' (ESP) [2]. L2TP/IPSec uses UDP ports for its packet transfer. The port numbers are 500, 1701 and 4500 [1].

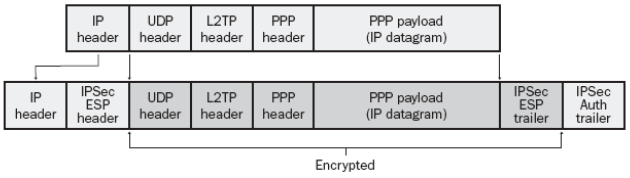

Figure 4: L2TP/IPSec sample packet and its encryption using ESP

One of the important security features of L2TP/IPSec is its ability to authenticate the computers to provide data origin authentication. L2TP/IPSec usually does this by making use of a certificate[1] or a pre-shared key. Since IPSec procedures occur before the PPP connection so, a secure basis is ready for PPP to exchange keys and thus it will be much harder to retrieve any information by capturing and decoding the packets. Although L2TP/IPSec provides more security in establishing a VPN connection in comparison to PPTP, but it needs lots of settings and administration especially in IPSec section. It is worth mentioning that IPSec operates in the third layer (in OSI model) and so it is independent of applications, unlike *proxy* for which one needs to configure his applications to be able to use it; of course only if the applications support the usage of proxy like, Internet Explorer. So by configuring and setting up IPSec on a machine, all applications can benefit from its features transparently and accordingly (in terms of rules: protocols/ports …)

5. VPN Security Protocols and Methods

Each VPN technology uses a combination of protocols to provide security. When a VPN connection is started, first several phases must be completed for the connection to be established. Different protocols have been designed to support security in each phase. In this section some of these protocols are discussed. For better understanding it is good to classify them into three categories: *Authentication*, *Authorization* and *Encryption* protocols. Authentication protocols refer to those protocols which deal with the security of credentials like a username, password or certificate [2]. In authorization the rights of a user/computer are checked, and whether they are 'authorized' at all to make a VPN connection, or during which hours they can connect. Another example could be giving access only to the users of a specific sub-domain/group in our network, like users in university teachers group. Authorization checking occurs after the authentication phase, so a user might provide correct credentials (username and password) but still be not allowed to use the system. Encryption protocols are used to provide confidentiality and make sure that the data transferred cannot be read by others [2].

5.1 Authentication Protocols:

- 'Password Authentication Protocol' (PAP): In this method, username and passwords are sent in 'clear-text' and not encrypted. Also this protocol does not encrypt the data.
- 'Challenge Handshake Authentication Protocol' (CHAP): This protocol also does not provide any method to encrypt the connection data. This protocol checks the credentials by sending the username in clear text, but instead of the password, it sends an ID and also an arbitrary string as a 'challenge string' [2]. The client will return a hashed (using MD5 hash algorithm) string of the ID, challenge and password [1][2]. The fact that each time it sends a different challenge (even at intervals during the connection) gives this protocol the anti replay ability. If you want to use CHAP, do not forget that you should enable 'store passwords using reversible encryption' in the group policy.
- Microsoft CHAP (MS-CHAP): This protocol is similar to CHAP, but uses MD4 hash algorithm instead of MD5. So the system does not need to store passwords as clear text, and it only keeps a hashed version of them. This protocol also provides encryption of both user credentials and connection data [1].
- Microsoft CHAP V2 (MS-CHAP V2): This is the default selection in Windows 2000, XP, and 2003 Server. In this protocol both ends of the connection send a challenge to each other, first the server and then the client sends a challenge string and this way it provides a two way authentication and thus better security.
- Extensible Authentication Protocol (EAP): This protocol was designed to make use of other authentication methods like smart cards, fingerprints and ID certificates of this kind [2]. The idea behind this protocol is that anyone can gain access to a system by knowing just the username and password, so instead of just working with a username and password, it uses a " two-factor " [2] authentication mechanism, and it means using both username and password plus some additional ID certificate; " Something you have and something you know" [2].

[1] For the definition of Certificates refer to Microsoft windows server documentations.

For L2TP/IPSec connections, since first a secure basis is created (first computers are authenticated and it is only after this phase that user authentication occurs) so any of the above protocols can be used freely for PPP authentication although it is recommended to use the latter two [2].

5.2 Authorization Methods

For the purpose of authorization, you do not need to do anything special as authorization of a user is done according to his account's settings in Windows. For a VPN connection to be authorized, you need to just set some configurations for the user who intends to log in to your network through a VPN connection in the dial-in tab of his user account property page to give him the ability to log in remotely. You can also set hours during which a user can log on in this property page. (Authorization can be stricter and more complicated by using other features of Windows Server 2003, so you may refer to [1] for more information on this issue.)

5.3 Encryption

PPTP, as mentioned before, uses MPPE to encrypt PPP data. MPPE can be set to use a 40, 56 or 128 bit key for encryption [2]. If you have Windows 98 or Millennium system in your network you should use a 40bit key for compatibility issues.

Since in a VPN connection, packets may arrive in any order, so in VPN a slightly modified version of MPPE is used which enables independent (from other packets) encryption and decryption of each packet. So if a packet arrives sooner than its previous one it still can be decrypted and used [2].

In L2TP/IPSec connections, it is IPSec that does the job of encrypting. IPSec uses 'Data Encryption Standard' (DES) and Triple DES (3DES) for its data encryption [2]. With DES you can have a 56-bit key and with 3DES a 168-bit key [1]. Explaining IPSec and its features in detail is beyond the scope of this paper; you can find more information at [4] on how to implement it in Windows and refer to [5] for detailed and precise definitions of IPSec and its architecture.

6. Configuring Your Client and Server For VPN Connections

Necessary theoretical aspects of VPN connections were discussed in previous sections and now it is about time to see how it is implemented in practice. In here a step by step procedure is used to create a remote access VPN server on Windows Server 2003 and finally some important facts about implementing router to router (site to site) VPN connections will be mentioned.

6.1 Step 1: Server side configurations

To configure your server to allow VPN connections, you must select 'Routing and Remote Access' (RRAS) from 'Administrative Tools' menu. Then right click on your computer name and select 'Configure and enable routing and remote access'. A window opens up for you where you can select different types of remote access like Dial-up, VPN and also in here you can configure NAT[2] for the computers on your network. In this window we choose the first item which is also selected by default; 'Remote Access (dial-up or VPN)' as is show in the following figure:

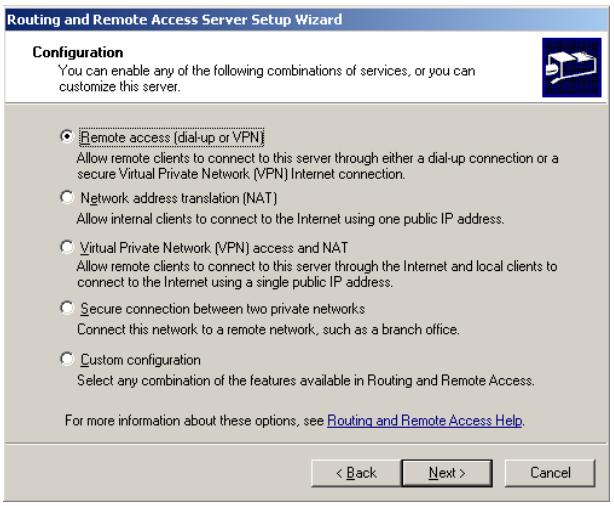

Figure 4: selecting the role of RRAS server

Then in the next window you have two options: VPN or Dial-up, which you should select the former. After that, you should select the interface on which you want to configure VPN access (allow VPN access through that interface). After you have made your selection about the interface, you will be asked to choose the way you want your clients to receive an IP. There are two options available: using a DHCP server or defining a specific address range. If already you have a DHCP server in your network or even if your Windows Server 2003 is also configured to act as a DHCP server, you may want to choose the first option. But here for our test system we select the second one and define our clients' address range in the window which follows, by clicking on 'New' button; you can see a snapshot of it in the following figure:

[2] Network Address Translation

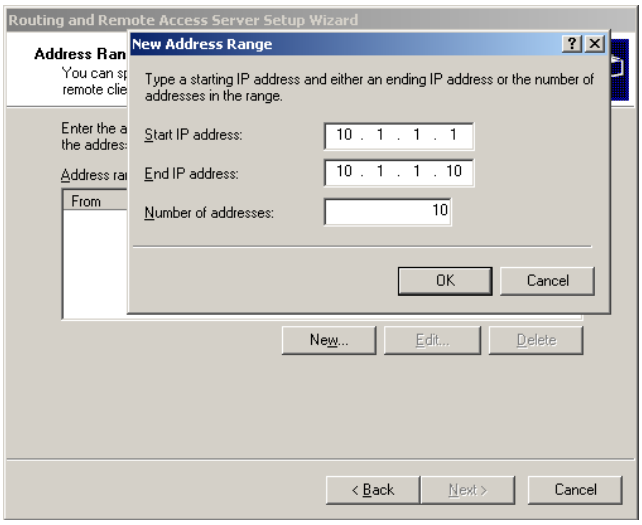

Figure 5: specifying the IP address range

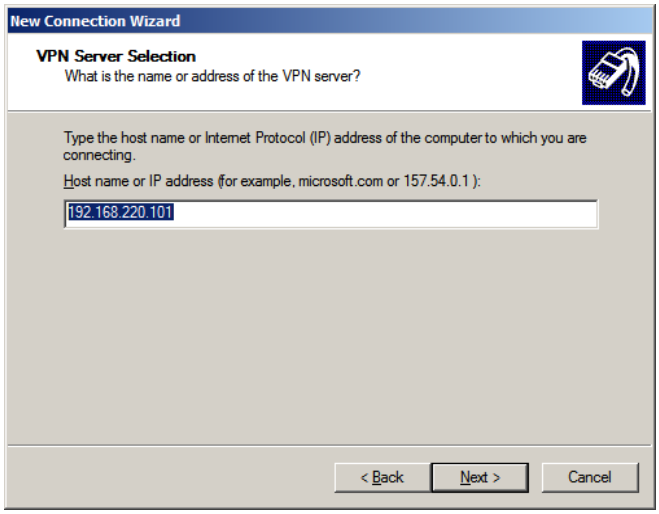

Figure 6: specifying the address of the VPN server

By specifying such an address range, the clients that connect to our server will receive an IP (if still available) from this range. After this step you will be asked about whether you use a *RADIUS* server or not for administrating AAA[3] in your network. For more information about the definition and configuration of a radius server refer to [1]. By clicking on 'Finish' button your server will be configured and ready to accept VPN connections. It is important to know that there are a lot more settings you can make for routing inside your network and between interfaces, available ports, security options and etc. What we mentioned here is just a very simple scenario so that you can test a VPN connection by yourself.

6.2 Step 2: Client side configurations

In this step we will describe how to configure your client to initiate a connection to your VPN server.

Select 'Create a new connection' from 'Network Connections'. Then in the window regarding the connection type select 'Connect to the network at my workplace' and in the window which comes after it select 'Virtual Private Network connection' and after this window just enter a name for this connection, for example VPN_TEST. The next window asks you about whether you want to automatically connect to your ISP, when you choose this connection (VPN_TEST) or not; in this example we select no. After that you should enter the IP address of your VPN server as shown in the following figure:

After this step and pressing the 'Finish' button, just enter your username and password (a valid account on the network in which your VPN server exists). By pressing the CONNECT button your connection will be established and now you have a VPN connection!!!

If you check the information of your VPN connection, you will see something like what is shown in figure 7:

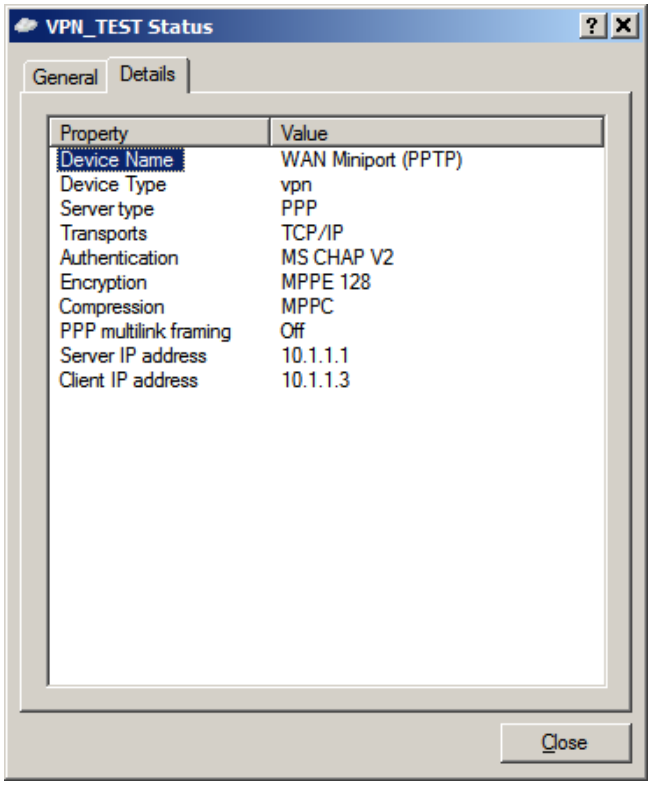

Figure 7: VPN_TEST connection details

[3] AAA: Authentication, Authorization and Accounting; known as Triple A.

As you can see the type of the connection is PPTP, using MS-CHAP V2 for authentication and MPPE with a 128bit key for encryption and the IP address that we have received from the server is from the range that we specified on the server.

On your VPN server if you check 'Remote Access Clients' subsection in your RRAS window, you can see the clients that are currently connected to your server and the duration of their connections (you need to Refresh the window in order to get the updated list of clients).

In this example, as you may have noticed we did not specify the type of our VPN connection and the default type that windows has selected for us is PPTP. Configuring a L2TP/IPSec involves more configurations and settings. If you check the 'Networking' tab under the property page of your VPN_TEST connection, you can see the type of your VPN connection ('Automatic' by default) and you may change it here for the client part. Also under the 'Security' tab if you select 'Advanced (custom settings)' and then press the 'Settings' button you can see different security protocols that we talked about before. When a connection is being made the most secure protocols selected by both the client and server which are common between them will be selected.

6.3 A Note on Router To Router VPN Connections

For router to router (or site to site) connection, you need to first create a demand-dial interface to allow the other side to login and you need to define user accounts for both of the routers. The point is that the username you specify for dial-out credentials (to connect to the other router/site) is the demand dial interface name created on that router/site and on the other end they should do the same thing and specify the name of your demand dial interface as the username to connect to your server. Also it is possible to use the same name for both of these two demand dial interfaces on each site. You need to create user accounts with the same name as the interfaces and make sure that you give them the correct dial-in permissions too. By using these demand dial interface names as usernames, RRAS can distinguish whether a remote user has tried to make a connection or a router.

7. Summary and Conclusions

In this paper we discussed different aspects of Virtual Private Networks and that in what areas we can or must use them and we saw their advantages over dial up connections especially when it comes to long distance connections between two private networks. We face security risks when we use the Internet as our main means of connection between private networks, so VPN should provide a secure basis for transferring our data. Thus different protocols have been designed to provide security in different phases of a VPN connection.

There are four main features that a VPN connection may offer: 'Confidentiality', 'Data Integrity', 'Data Origin Authentication' and 'Anti Replay'. We discussed L2TP and PPTP in detail, which are two main types of VPN and saw how addition of IPSec to L2TP can make it one of most secure types of VPN technologies available. Also we went through the most important protocols used in VPN connections, like MS-CHAP 2, MPPE and etc. Different methods of packet encapsulation during a VPN connection were also shown and discussed and we realized how a packet can be routed correctly to its final destination via the Internet passing through several public networks and finally reaching its specified machine on the destination private network.

Two forms of VPN connections in terms of client types were introduced: 'Remote Access' and 'Router to Router' (also known as 'site to site') VPN connections. As an example for VPN connections, we implemented a sample PPTP connection with just the very basic settings so that you can see the basic steps in creating a VPN connection. Of course lots of complicated settings and concepts (especially about IPSec) were left out for the sake of simplicity in implementation of our sample VPN and also because most of them needed more detailed knowledge about other aspects of Windows Server 2003 like Active Directory and IPSec, but we mentioned the major pitfalls and issues in configuring a VPN server. So if you are going to study and work on VPN technologies more seriously you can count on this paper as a stepping stone, and then need to study other topics to be able to manage your VPN server better and in a more secure way. As also stated in this paper, some administrative issues, like authorization, authentication and accounting (AAA) are also of great influence in implementing a good VPN system, so you can work on these issues to gain better knowledge of how to build a robust and secure VPN server.

8. References

[1] J. C. Mackin, Ian McLean; "Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure: MCSA/MCSE self-paced training kit (exam 70-291)"; Microsoft Press.

[2] Joe Davies, Elliot Lewis, "Deploying Virtual Private Networks with Microsoft Windows Server 2003", Microsoft Press, October 15, 2003

[3] Charlie Scott, Paul Wolfe, Mike Erwin; "Virtual Private Networks, Second Edition"; O'Reilly, December 1998

[4] Step-by-Step Guide to Internet Protocol Security (IPSec), February 17, 2000, http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/ispstep.mspx

[5] Security Architecture for the Internet Protocol, December 2005, http://www.rfc-archive.org/getrfc.php?rfc=4301