Yi Yang

VIRTUAL PRIVATE NETWORK MANAGEMENT

Bachelor's Thesis
Bachelor of Information Technology Program

May 2011

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

Date of the bachelor's thesis

May 19th, 2011

Author(s)
Yi Yang

Degree programme and option
Bachelor of Information Technology
Network Optionion

Name of the bachelor's thesis

Virtual Private Network Management

Abstract

Nowadays Cisco routers are mainly configured with CLI (Command Line Interface). However, Cisco offers some GUI (Graphical User Interface) management tools like SDM (Security Device Manager) and CNA (Cisco Network Assistant). Although these are not widely used at this time, it tends to be familiar by all network managers, especially for the use of SDM, which is introduced in great details on CCNP and CCNA Security courses.

SDM is a Web-based device-management tool for Cisco routers that can improve the productivity of network managers, simplify router deployments, and help troubleshoot complex network and VPN connectivity issues.

A VPN (Virtual Private Network) is a computer network that uses a public telecommunication infrastructure such as the Internet to provide remote offices or individual users with secure access to their organization's network. Its aim is to avoid an expensive system of leased lines that can be used by only one organization.

The aim of my study is to get familiar with the GUI tool SDM and try to use it to establish a Virtual Private Network. Finally, I compared the difference between SDM and the original configuration by command line interface and gave my recommendation.

Subject headings, (keywords)
Wide Area Network, Broad Band Access to the Internet, Virtual Private Network, IPsec, Command Line Interface, Graphical User Interface, TeraTerm Web, Security Device Manager

Pages	Language	URN
71.p + app. 18p	English	

Remarks, notes on appendices

Tutor
Matti Koivisto

Employer of the bachelor's thesis

ACKNOWLEDGEMENT

I would like to pay my sincere thanks to my supervisor Mr. Matti.Koivisto. Thank you so much for giving me the encouragements and instructions during the whole process of my final thesis. Your earnest attitude toward science and technology left deep impression to me.

And thanks all the people I have met in Finland, my lecturers and my friends. You gave me a great memory in my life.

Finally, thanks to my parents for supporting me all the time. You gave me the chance to explore the world and experience happiness and pain, which are all my treasures.

GLOSSARY

3DES	Triple Data Encryption Standard
3G	The Third Generation
ADSL	Asymmetrical Digital Subscriber Loop
AES	Advanced Encryption Standard
AH	Authentication Header
ATM	Asynchronous Transfer Mode
AUX	Auxiliary
BGP	Border Gateway Protocol
CCA	Cisco Configuration Assistant
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CLI	Command Line Interface
CNA	Cisco Network Assistant
DES	Data Encryption Standard
DH	Diffie-Hellman Algorithm
DSL	Digital Subscriber Loop
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FM	Frequency Modulation
GUI	Graphical User Interface
HDLC	High-level Data Link Control
HMAC	Hashed Message Authentication Codes
IKE	Internet Key Exchange
IOS	Internetworking Operating System
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv6	Internet Protocol Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
JRE	Java Runtime Environment

L2F	Layer 2 Forwarding
LAN	Local Area Network
LEO	Low Earth Orbit
MD5	Message Digest 5
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
OS	Operating System
OSI	Open System Interconnect
OSPF	Open Shortest Path First
PC	Personal Computer
PFS	Perfect Forward Secrecy
POP	Point of Presence
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
RIP	Routing Information Protocol
RSA	Rivest-Shamir-Adleman Algorithm
SDM	Security Device Manager
SEAL	Software-optimized Encryption Algorithm
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
VC	Virtual Circuit
VPN	Virtual Private Network
VTY	Virtual Type Terminal
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

FIGURES

Figure 2. 1. Categories of WAN Link Connection 3
Figure 2. 2. Comparision of different Connection Optionion.. 5

Figure 3. 1. Satellite Internet Access in Ghana 8
Figure 3. 2. Connecting Teleworkers to the WAN 8

Figure 4. 1. Category According to Tunnel’s Termination Point 11

Figure 5. 1. IPsec Framework 13
Figure 5. 2. AH Transport Mode.. 15
Figure 5. 3. AH Tunnel Mode Packet 16
Figure 5. 4. ESP Transport Mode Packet 16
Figure 5. 5. ESP Tunnel Mode Packet 16
Figure 5. 6. DES, 3DES and AES 18
Figure 5. 7. Hash Process 19
Figure 5. 8. Implementation of Integrity and Authentication 20

Figure 6. 1. IOS Mode Hierarchical Structure 22
Figure 6. 2. Backboard of Cisco 2811 Router 23
Figure 6. 3. Initial Step of Using Tera Term 24
Figure 6. 4. Terminal Size Changing 25
Figure 6. 5. Font Size Changing 25
Figure 6. 6. Scroll Buffer Changing 25
Figure 6. 7. HyperTerminal 26
Figure 6. 8. Minicom 27
Figure 6. 9. SecureCRT 27
Figure 6. 10. SDM User Interface 28
Figure 6. 11. Change Java Runtime Environment Version 29
Figure 6. 12. Change Internet Explorer Property 30
Figure 6. 13. SDM Launching Interface 31
Figure 6. 14. Results of ‘show running-config’ by SDM 31
Figure 6. 15. Basic Router Configuration by SDM 32

Figure 6. 16. Configure Device Properties-Device 32
Figure 6. 17. Configure Device Properties-Secret Password 33
Figure 6. 18. Edit Username 33
Figure 6. 19. Edit VTY Lines 34
Figure 6. 20. Interfaces and Connections 35
Figure 6. 21. Routing Protocols 35
Figure 6. 22. Network Address Translation.. 36

Figure 7. 1. VPN Topology 37
Figure 7. 2. ISAKMP Parameters 41
Figure 7. 3. Allowed Transform combination 42
Figure 7. 4. Create Site to Site VPN 44
Figure 7. 5. Two GUI Configurating ways.. 44
Figure 7. 6. Defaults Setting of VPN by SDM 45
Figure 7. 7. VPN Quick Setup 46
Figure 7. 8. VPN Quick Setup Summary 46
Figure 7. 9. Step-by-Step Wizard STEP 1... 47
Figure 7. 10. Step-by-Step Wizard STEP 2... 48
Figure 7. 11. Step-by-Step Wizard STEP 2... 48
Figure 7. 12. Step-by-Step Wizard STEP 3... 49
Figure 7. 13. Step-by-Step Wizard STEP 3... 49
Figure 7. 14. Step-by-Step Wizard STEP 4... 50
Figure 7. 15. Step-by-Step Wizard Summary.. 50
Figure 7. 16. Chang Tunnel Parameters 53
Figure 7. 17. VPN Status.. 59
Figure 7. 18. VPN Troubleshooting 59
Figure 7. 19. Generate Mirror... 60
Figure 7. 20. VPN Monitor... 60
Figure 7. 21. Tunnel Test 1... 64
Figure 7. 22. Tunnel Test 2... 65

CONTENTS

1. INTRODUCTION 1

2. WAN LINK CONNECTION OPTIONS 3

  2.1 Leased Line Connection 3

  2.2 Circuit Switched Connection 4

  2.3 Packet Switched Connection 4

  2.4 Internet Connection 4

3. BROADBAND ACCESS TO THE INTERNET 6

  3.1 Digital Subscriber Line 6

  3.2 Cable 6

  3.3 Broadband Wireless 7

4. VIRVUAL PRIVATE NETWORK 9

  4.1 VPN Overview 9

  4.2 Benefits of VPNs 9

  4.3 VPN Categories 11

5. IPSEC PROTOCOL 13

  5.1 IPsec Framework 13

  5.2 IPsec Protocol 14

  5.3 Confidentiality 16

  5.4 Integrity 18

  5.5 Authentication 19

  5.6 Secure Key Exchange 20

6. CONFIGURATION TOOLS 21

  6.1 Two User Interfaces 21

  6.2 Access Methods 22

  6.3 Terminal Emulator Program 23

    6.3.1 TeraTerm Web 24

    6.3.2 Other Terminal Emulator 26

  6.4 Cisco Router and Secure Device Manager 27

    6.4.1 SDM Supporting 28

    6.4.2 Basic Router Configuration by SDM 31

7. CREATING VIRTUAL PRIVATE NETWORKS 37

  7.1 Network Topology 37

7.2 Preparation 38

7.3 Configure Virtual Private Network in Two Ways 41

7.3.1 Internet Key Exchange procedure 41

7.3.2 Quick Setup by SDM 43

7.3.3 Step By Step Wizard 47

7.3.4 VPN Advanced Setting by SDM 52

7.3.5 Command Line Step by Step 54

8. COMPARATION 66

9. CONCLUSION AND EXPECTATION 68

BIBLIOGRAPHY 69

APPENDIXES

1. INTRODUCTION

Nowadays Cisco routers are mainly configured with CLI (Command Line Interface). However, Cisco offers some GUI (Graphical User Interface) management tools like SDM (Security Device Manager) and CNA (Cisco Network Assistant). Although these are not widely used at this time, it tends to be familiar by all network managers, especially for the use of SDM, which is introduced in great detail on new versions of CCNP and CCNA Security courses.

SDM is a Web-based device-management tool for Cisco routers that can improve the productivity of network managers, simplify router deployments, and help troubleshoot complex network and VPN connectivity issues. [1]

A VPN (Virtual Private Network) is a computer network that uses a public telecommunication infrastructure such as the Internet to provide remote offices or individual users with secure access to their organization's network. Its aim is to avoid an expensive system of leased lines that can be used by only one organization.

As mentioned above, the VPN, which is the private network, uses public internet, therefore security is an essential task. Secure VPNs use cryptographic tunneling protocols to provide confidentiality by blocking intercepts and packet sniffing, allowing sender authentication to block identity spoofing, and provide message integrity by preventing message alteration.[2] VPN provides a myriad of security mechanisms, among all these mechanisms, IPsec (Internet Protocol Security) is commonly used. IPsec was originally developed for IPv6. This standards-based security protocol is also widely used with IPv4, and Layer 2 Tunneling Protocol frequently runs over IPsec.

The aim of my study is first to get familiar with the GUI tool SDM, and then try to create an IPsec VPN using both GUI and CLI tools. Finally I compare the benefits and drawbacks of these ways.

In Chapter 2, I first describe methods of WAN (Wide Area Network) link connection. Some of them have lower speed but cost-efficiency, while some provide higher speed but also a higher costs. There is even an option that has perfect performance both in speed and cost, but subjects to security problem, which is based on Internet connection.

In Chapter 3, I illustrate the popular broadband internet access methods, including DSL, cable modem and variety methods of wireless connections such as WiMAX, 3G and satellite. Among all of these methods, DSL and cable modem are widely used by home users. WiMAX is a latest developing technology, while satellite has some special use.

In Chapter 4, I introduce the technology to connect two remote sites by using the public third party network --- Internet. This technology is called Virtual Private Network which is the most preferable way chosen by us.

In Chapter 5, I first demonstrate how to solve the security problem in VPN by using an IPsec protocol. IPsec protocol implements existing algorithms to solve security problem. Then I briefly explain the features of the protocol, such as integrity and confidentiality.

In Chapter 6, I depict the tools that are used in configuring routers and switches in my practical part of creating VPNs. There are two main user interfaces, Command Line Interface (CLI) and Graphical User Interface (GUI). Every user interface has plenty of configuration tools. Among all of these tools, TeraTerm Web and Cisco Router and Security Device Manager are explained in more pages.

In Chapter 7, the complete experimental steps of creating a Virtual Private Networks are introduced. I use three different methods, including two GUI configuration methods, quick setup and step by step wizard, and one CLI configuration.

In Chapter 8, after implementing three different ways of creating VPN tunnel, I compare and analyze the benefits and drawbacks in detail and give my recommendation.

In the last Chapter, I first conclude what I have learned during doing my final thesis. Then I throw my expected future studies that I am interested in. One topic is using Cisco Network Assistant to manage Cisco switches. Another task that I am interested in is how Cisco devices operate VPN tunnel along with network devices from other company. Finally how to create remote access VPN especially SSL VPN by using both CLI and GUI tools seems to be a future study.

2. WAN LINK CONNECTION OPTIONS

There are several options available to implement WAN (Wide Area Network). The differences between them are technology, speed and cost. First, I will shortly describe the differences between them.

WAN connections can be either over a private infrastructure or over a public infrastructure. Private WAN connections include both dedicated and switched communication link options. A public WAN connection option, such as the internet is now a sophisticated technology widely used in our daily communication. Figure 2. 1 simply shows different ways of WAN link connection.

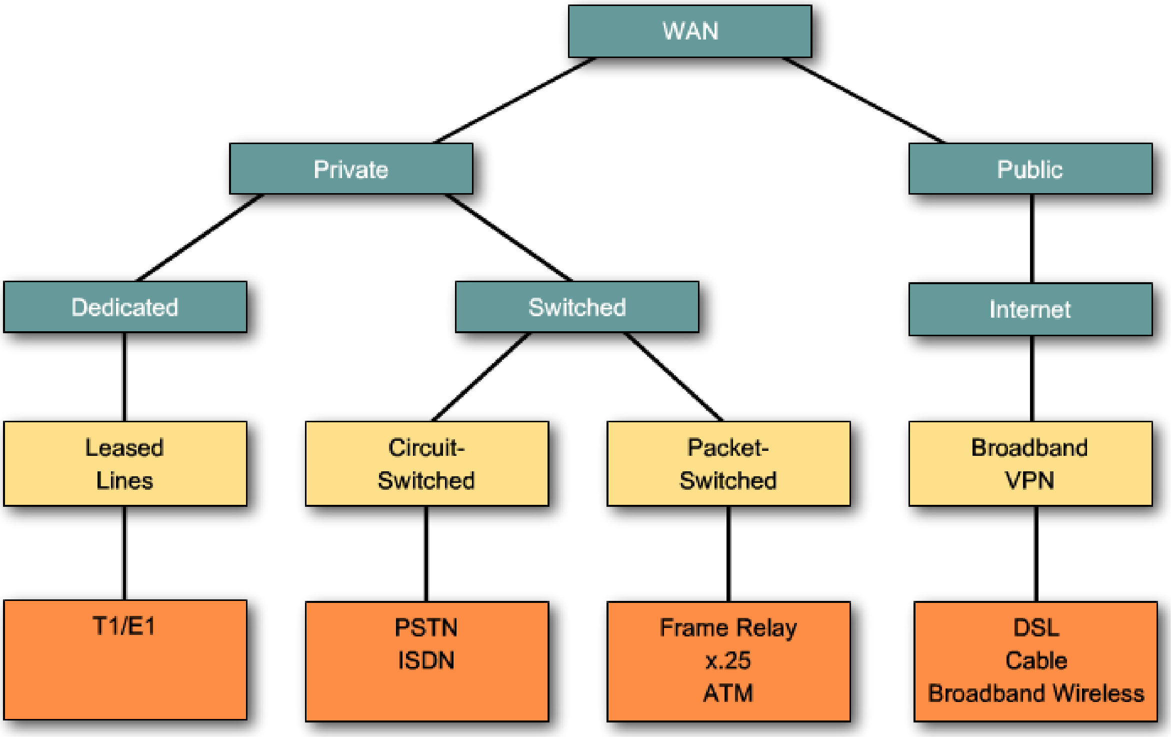


Figure 2. 1. Categories of WAN Link Connection [26]

2.1 Leased Line Connection

Leased lines services (or private line services) became digital in the 1970s with the conversion of the Bell backbone network from analog to digital circuit. [26] Leased line needs a permanent dedicated connection, which for sure costs plenty of money. Therefore it is not very suitable for a long distance connection due to the cost and time of pre-established line before successful transportation. Besides, the bandwidth of the leased line is fixed whereas the traffic is variable, sometimes even empty. A number of drawbacks make it not to be a good choice. However, sometimes the benefits outweigh the cost of the leased line. The dedicated capacity removes latency or jitter between the endpoints. Constant availability is essential for some applications such as VoIP or Video over IP. [26] Two mainly used leased line connection are T1 and E1.

2.2 Circuit Switched Connection

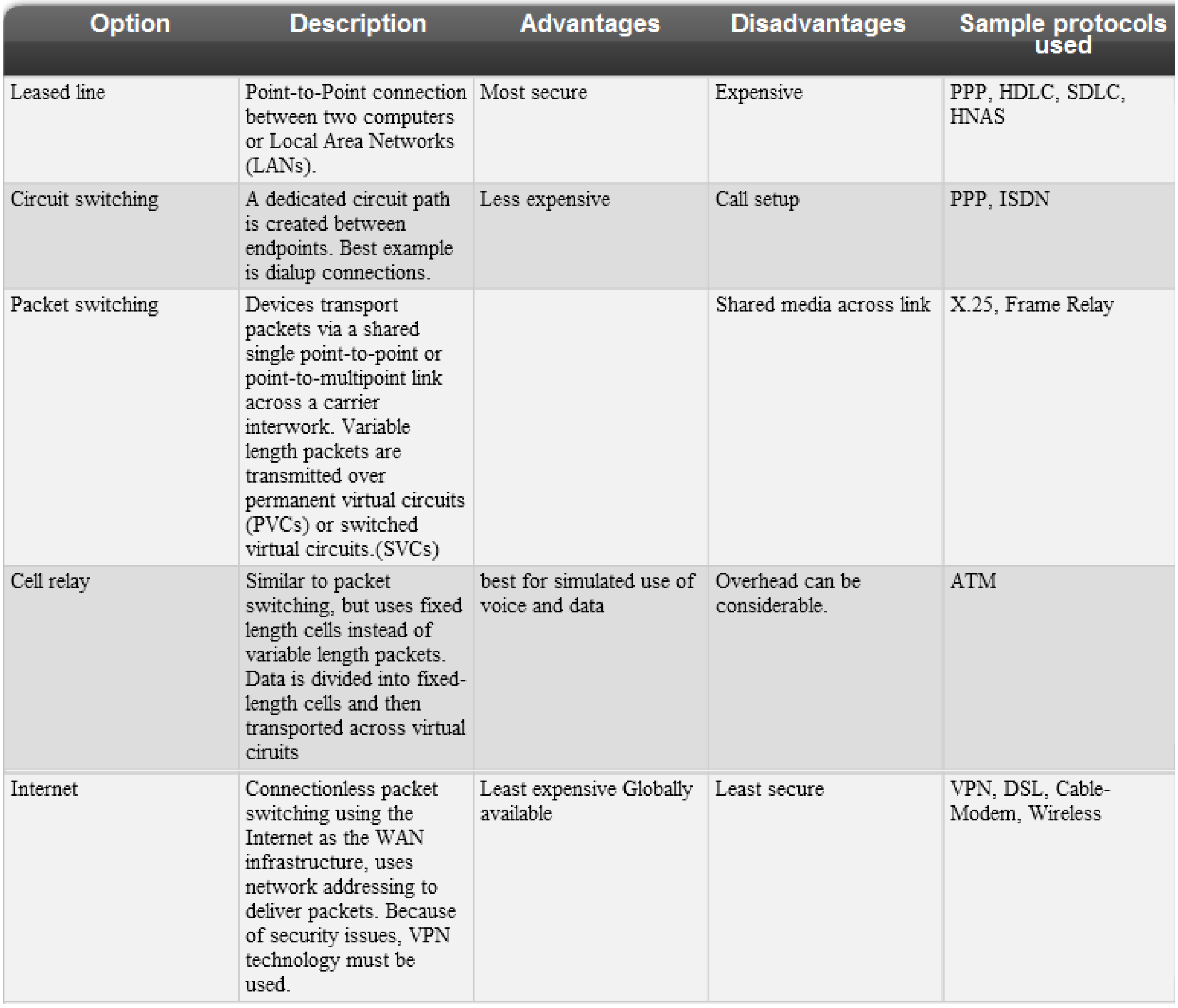
Circuit switching is a telecommunications technology by which two network nodes establish a dedicated communications channel (circuit) connecting them for the duration of the communication session before the nodes may communicate. [4] There are two main technologies using circuit switched technology, Analog Dialup and ISDN (Integrated Services Digital Network). Analog Dialup works just like a normal telephone using PSTN (Public Switched Telephone Network). The line is engaged when transmitting data. Compared to leased line, it has a lower price. On the contrary, user should be subject to the lower speed. In order to address the problem, ISDN is invented to enables the line from home to local telecom operator to carry digital signals. But in today’s network, circuit switched connection has been substituted by new faster and cheaper technology.

2.3 Packet Switched Connection

Unlike in a circuit switched connection, in packet switched there is no need to establish a circuit before communication. Instead, packet switching splits data into packets and allows many pairs of nodes to communicate over the same channel. In order to determine which direction the packet must be sent on next, there are two approaches, connectionless and connection-oriented. Connection-oriented connection relies on DLCIs (Data Link Control Identifiers) working like a VC (Virtual Circuit) used in Frame Relay networks, a widely used packet switched connection nowadays developed from. X.25. Besides, ATM (Asynchronous Transfer Mode) is best for simulated use of data and voice, which is built on a cell-based architecture. ATM cells have always a fixed length of 53 bytes. The ATM cell contains a 5 bytes ATM header followed by 48 bytes of ATM payload. So it seems less efficient than the bigger frames and packets of Frame Relay and X.25.

2.4 Internet Connection

Now, there are mainly three different ways accessing to the internet, DSL (Digital Subscriber Loop), using telephone networks, cable modem, using cable television networks and wireless such as municipal Wi-Fi, WiMAX and Satellite. Besides, with the development of 3G and LTE technology, increasing number of way can be chosen to access the internet. There is even an access method by using electric power line in some places. In Figure 2. 2, there is a comparison of the most popular WAN connections.



Option	Description	Advantages	Disadvantages	Sample protocols used
Leased line	Point-to-Point connection between two computers or Local Area Networks (LANs).	Most secure	Expensive	PPP, HDLC, SDLC, HNAS
Circuit switching	A dedicated circuit path is created between endpoints. Best example is dialup connections.	Less expensive	Call setup	PPP, ISDN
Packet switching	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier interwork. Variable length packets are transmitted over permanent virtual circuits (PVCs) or switched virtual circuits.(SVCs)		Shared media across link	X.25, Frame Relay
Cell relay	Similar to packet switching, but uses fixed length cells instead of variable length packets. Data is divided into fixed-length cells and then transported across virtual ciruits	best for simulated use of voice and data	Overhead can be considerable.	ATM
Internet	Connectionless packet switching using the Internet as the WAN infrastructure, uses network addressing to deliver packets. Because of security issues, VPN technology must be used.	Least expensive Globally available	Least secure	VPN, DSL, Cable-Modem, Wireless

Figure 2. 2. Comparision of different Connection Optionion [26]

3. BROADBAND ACCESS TO THE INTERNET

Nowadays, internet has become to part of our life. On work time, office workers use it to send e-mail and even use online office software to deal with their daily work. Students can learn online courses such as Cisco Online Academy through Internet. After work, a computer with the ability to access the internet is like a entertainment terminal, watching online movies, playing online games, chatting online, etc. If the access speed is high enough, an operating system only with web browser is enough to solve the most of our daily application. This is actually the reason why Google developed an operating system called Chrome OS. The main advantage of Chrome OS compared to other operating systems is that Chrome has a very short user interface launching time. Below, I present the main broadband access methods, DSL, cable and broadband wireless.

3.1 Digital Subscriber Line

Digital Subscriber Line (DSL) is a family of technologies that provides digital data transmission over the wires of a local telephone network. DSL originally stood for digital subscriber loop. In telecommunications marketing, the term Digital Subscriber Line is widely understood to mean Asymmetric Digital Subscriber Line (ADSL), the most commonly installed technical variety of DSL. DSL service is delivered simultaneously with regular telephone on the same telephone line. This is possible because DSL uses a higher frequency. These frequency bands are subsequently separated by filtering. [5] The performance of speed is according to the actual length of the local loop, which is the distance between subscriber and the location of local telephone company.

Several years ago, Bell Labs identified that a typical voice conversation over a local loop only required bandwidth of 300 Hz to 3 kHz. For many years, the telephone networks did not use the bandwidth above 3 kHz. Advances in technology allowed DSL to use the additional bandwidth from 3 kHz up to 1 MHz to deliver high-speed data services over ordinary copper lines. [26]

3.2 Cable

Cable television is a system of providing television to consumers via radio frequency signals transmitted to televisions through coaxial cables or digital light pulses though fixed optical fibers located on the subscriber's property. FM radio programming, high-speed Internet, telephony, and similar non-television services may also be provided. The major difference is the change of radio frequency signals used and optical connections to the subscriber property. [6] In order to access the internet, a cable modem is needed. And the speed depends on the number of people shared the line.

In addition, with the development of fiber optic technology, the convergence among Public Switched Telephone Network, Cable TV and Internet Access has a promising future.

3.3 Broadband Wireless

Wireless routers are now widely used in office and home environment. A computer running Windows7 can act as a wireless router after some additional configuration. But the limitation of current wireless routers is that the cover area is limited. Once a worker left the office or home, wireless access is not available. The service between the laptop and the router is wireless, however the wired connection between the router and the internet is still needed.

Now, we concern about accessing a laptop or mobile phone directly to the internet. Municipal Wi-Fi is such kind of method with overlapping access points. For example, according to my experience, in 2008 Beijing Olympic Games, inside the second ring of Beijing, there was always a free access point, but the signal power was not very high and the speed was also a little bit slow.

WiMAX (Worldwide Interoperability for Microwave Access) is a telecommunications protocol that provides fixed and mobile Internet access. The WiMAX forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL". [7] With the decreasing price of WiMAX, this higher speed technology can be an alternative to municipal Wi-Fi.

3G is also a new wireless way to access the internet. In some area, 3G wireless access is preferred due to its lower price compared to wired access methods. Especially new version of Android OS supports a function that a mobile phone with a 3G connection can act as an access point. This means that the mobile phone change the 3G signal to wireless LAN signal, so that we can access to internet by computer with a Wireless LAN Network Interface Card.

The satellite is a broadband access method in sparsely populated areas, vessels at sea and airplanes in flight. Satellite Internet access is Internet access provided through satellites. The service can be provided to users world-wide through Low Earth Orbit (LEO) satellites. Geostationary satellites can offer higher data speeds, but their signals cannot reach some polar regions of the world. Different types of satellite systems have a wide range of different features and technical limitations, which can greatly affect their usefulness and performance in specific applications. [8] Figure 3. 1 is satellite internet access implementation in Africa.

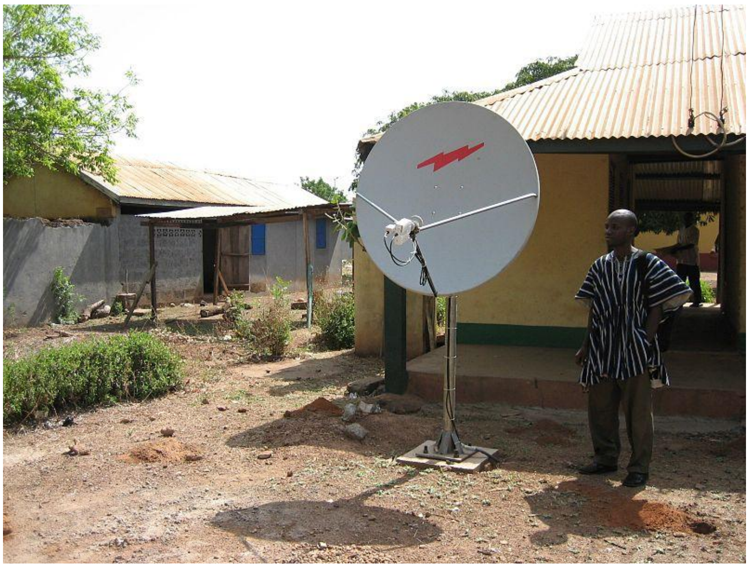


Figure 3. 1. Satellite Internet Access in Ghana [12]

Figure 3. 2 shows diffent ways of accessing to the Internet, including traditional narrowband access method and three new broadband methods, DSL, Cable and Satellite.

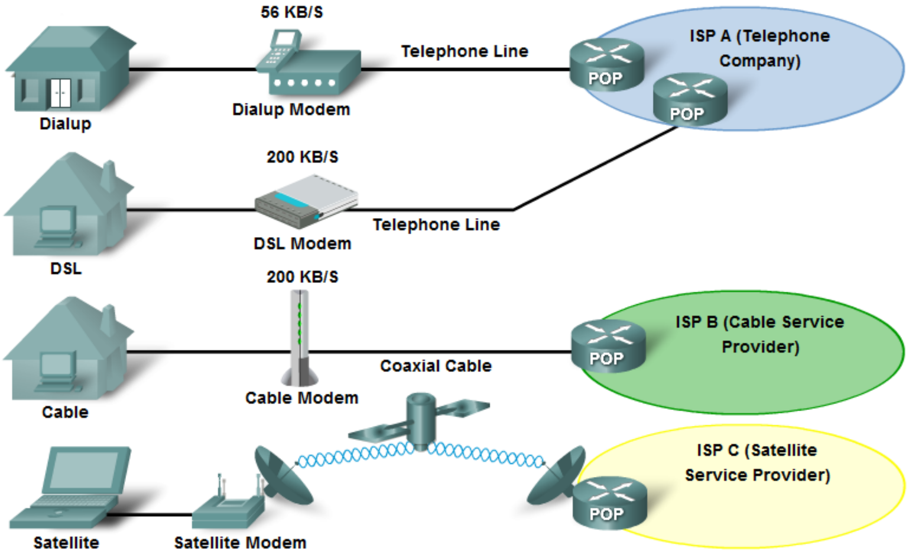


Figure 3. 2. Connecting Teleworkers to the WAN [26]

4. VIRVUAL PRIVATE NETWORK

4.1 VPN Overview

The traditional Layer 2 WAN (Wide Area Network) has developed more than 20 years, based on private connections between two or more locations. However, with the development of technology, companies evolve faster and the traditional ways seem less suitable for modern companies, due to the costs of leasing lines from Telecom Service Provider. In the mean time, people have an easier access to the Internet even in rural area, and the costs of access becomes cheaper and cheaper. The development of wide band technology makes the speed faster and faster.

It is these reasons that make companies more likely to choose a new technology called VPN (Virtual Private Network) to implement WAN access. As can be seen from the name "Virtual Private", this technology uses public Internet service and acts as a private way such as frame relay and ATM by using end-to-end tunnel technology. Organizations use VPNs to provide a virtual WAN infrastructure that connects branch offices, home offices, business partner sites, and remote telecommuters to all or portions of their corporate network. The VPN configuration can be defined on routers, firewalls or even computers. Typically, organizations always create a site-to-site VPN between headquarter and branch companies (Called Intranet) as well as their business partners (Called Extranet). While creating remote access VPN between companies and SOHOs can save commuting time especially in metropolis such as Tokyo and New York City, it always takes office worker more than three hours to drive between home and office. This VPN tunnel configuration is always configured on an enterprise level Firewall while in personal level the computer itself can act as a VPN tunnel end using software called VPN client to access to the main building. In here I take more care of the site-to-site VPNs.

4.2 Benefits of VPNs

Organizations using VPNs benefit from increased flexibility and productivity. Remote sites and teleworkers can connect securely to the corporate network from almost any place. Data on a VPN is encrypted and undecipherable to anyone not entitled to have it. [26]

Here are the main features of VPNs:

Efficiency - In old age, corporations should lease the dedicated expensive WAN links from ISPs which costs them plenty of money and may be the speed is not enough to be qualified the intensive intercompany transport. VPNs enable organizations to use cost-effective, third-party Internet transport to connect remote offices and remote users to the main corporate site. VPNs eliminate the traditional expensive dedicated WAN links. Additionally, with the advent of cost-effective, high-bandwidth technologies, such as DSL (Digital Subscriber Loop), organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth.

Scalability - About 20 years ago, it always takes long time to create a new link between new branch buildings and headquarter. VPNs enable corporations to use the Internet infrastructure that is within Internet Service Providers (ISPs) and devices. This makes it easy to add new users, so that corporations can add significant capacity without adding significant infrastructure.

Productivity – Due to the high leasing price, it is not necessary to create links between companies and individual users using traditional ways. Now this desire is achievable. VPNs allow mobile workers, telecommuters, and people who want to extend their workday to take advantage of high-speed, broadband connectivity to gain access to their corporate networks, providing workers significant flexibility and efficiency.

Security – VPNs provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.

Strictly saying, the last feature is not the advantage of VPN compared to Frame Relay Networks. Traditional WAN access technology is a private way to interconnect different LANs, so there is no need to concern security when transmitting information. The implementing of VPN addresses this most vital problem when using public internet. However, although using our modern technology like encryption, authentication and authorization, it still has theoretical hidden danger. That is why traditional dedicated links still exist today.

Anyway, just like every coin has two sides, more efficient and productive VPN is so complicated that needs network administrator to equip more knowledge to qualify his or her jobs.

4.3 VPN Categories

There are myriad ways to classify VPN:

According to the tunnel's termination point, VPN can be classified into End-to-End, End-to-LAN, End-to-POP, LAN-to-LAN, LAN-to-POP and POP-to-POP. [25]

In the End-to-End tunnel model, the tunnel is from one terminal side to the other side, so it has the highest security. The information transformed from one side to the other side is encrypted and cannot be detected and ruined by others.

In the End-to-LAN model, the tunnel starts from one computer to the gateway of the other LAN. This technology also called remote access VPN is widely used in portable office such as SOHO.

In the LAN-to-LAN model, well known as site-to-site VPN, the tunnel is created between two remote gateways, providing encrypted information transmitting. This technology is always used to create the private connection between headquarter and branch offices.

While in the End-to-POP model, starting from one end computer to the other side of telecom operator, does not have great implementation. Also the same situation exists in the POP-to-POP and the LAN-to-POP. Figure 4. 1 gives you a direct view of categories.

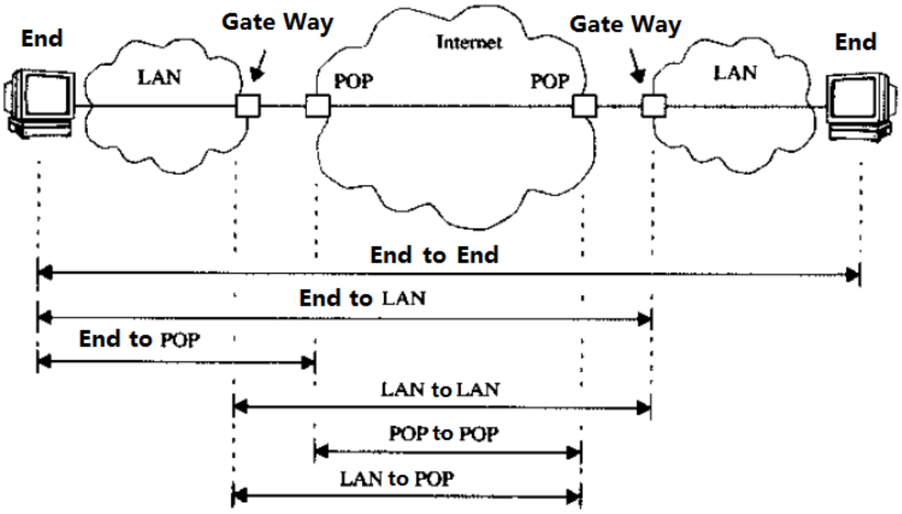


Figure 4. 1. Category According to Tunnel's Termination Point [Modified From 25]

There is also the other way to clasify the tunnel by tunnel protocol. There are some Data Link Layer protocols to provide a tunnel connection, such as Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). Besides, there are some Layer 3 tunneling protocol Generic Routing Encapsulation (GRE) and IPsec protocol suite. There is a tunnel working between Layer2 and Layer3, called Multiprotocol Label Switching (MPLS).

L2F, or Layer 2 Forwarding, is a tunneling protocol developed by Cisco Systems, Inc. to establish virtual private network connections over the Internet. L2F does not provide encryption or confidentiality by itself; It relies on the protocol being tunneled to provide privacy. L2F was specifically designed to tunnel Point-to-Point Protocol (PPP) traffic. [9]

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. A specification for PPTP was published as RFC 2637 and was developed by a vendor consortium formed by Microsoft, Ascend Communications (today part of Alcatel-Lucent), 3Com, and others. [10]

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork. [11] It cannot provide security, and always working together with IPsec to perform secure transmission.

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. [12] In the following chapter, I will briefly explain the working mechanism of IPsec.

MPLS operates at an OSI Model layer that is generally considered to lie between traditional definitions of Layer 2 (Data Link Layer) and Layer 3 (Network Layer), and thus is often referred to as a "Layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model. [13]

5. IPSEC PROTOCOL

5.1 IPsec Framework

As mentioned above, it is the IPsec protocol that makes it possible to transport information safely through public internet. It provides data confidentiality, data integrity, and origin authentication.

IPsec suite works at the Network Layer, protecting and authenticating IP packets between participating IPsec devices (peers). As a result, IPsec can protect virtually all application traffic because the protection can be implemented from Layer 4 through Layer 7 or even the original Layer 3 information. There are some tricky when protecting Layer 3 because all packets should have a plaintext Layer 3 header, so there are no issues with routing.

IPsec provides the framework, and the network administrator just need to choose the algorithms to implement the security services and be sure the same algorithms are used between two sides. By not binding IPsec to specific algorithms, it allows newer and better algorithms to be implemented in the IPsec frame. IPsec can secure a path between a pair of gateways (site-to-site), a pair of hosts, or a gateway and host (remote access). The IPsec framework is shown on Figure 5. 1.

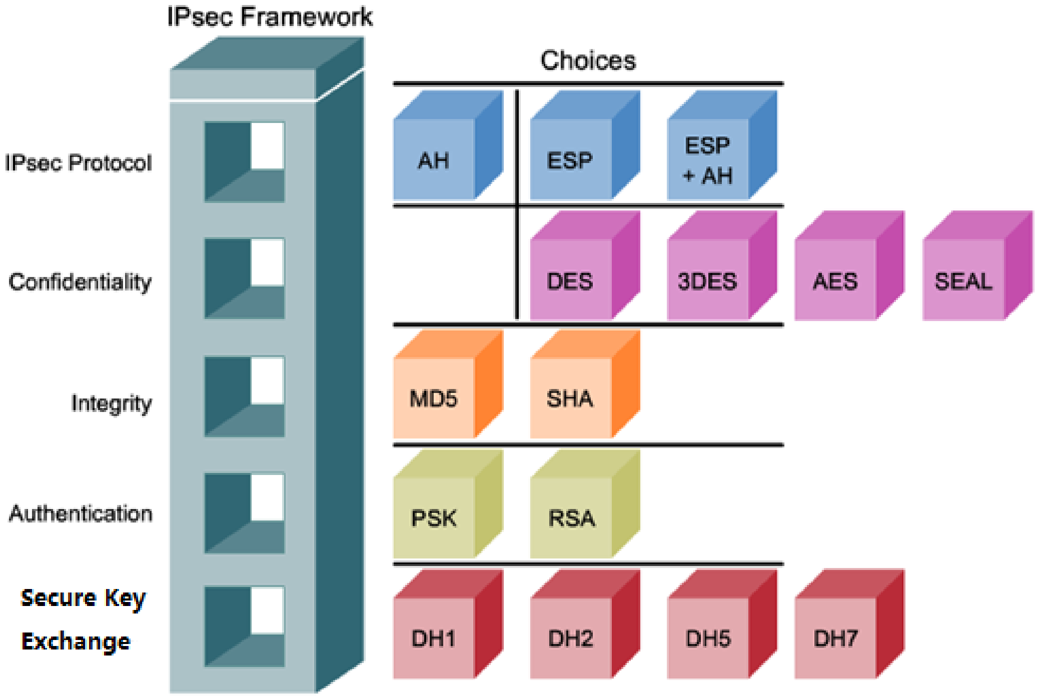


Figure 5. 1. IPsec Framework [21]

IPsec Protocol - The first represents the IPsec protocol. Choices include ESP, AH or both.

Confidentiality - IPsec ensures confidentiality by using encryption. [21] If choosing AH, no confidentiality algorithm can be chosen. While using ESP the administrator need to choose one from DES, 3DES, AES and SEAL. This step is to ensure other none expected hosts are able to understand the information I send.

Integrity - IPsec ensures that data arrives unchanged at the destination using a hash algorithm such as MD5 or SHA. [27] Just ensure non-understandable information is not enough, because hacker can ruin this information by altering it. The unchanged information is what we need. This step is to do this job.

Authentication - IPsec uses Internet Key Exchange (IKE) to authenticate users and devices that can carry out communication independently. IKE uses several types of authentication, including username and password, one-time password, biometrics, pre-shared keys (PSKs), and digital certificates (RSAs). [27] This step is to ensure the information sent from the remote side is what I want and not a forgery. Authentication methods always work with integrity hash algorithm.

Secure key exchange - IPsec uses the DH algorithm to provide a public key exchange method for two remote peers to generate a shared secret key. [27] One of four algorithms can be chosen (DH1, DH2, DH5, DH7). This step is to specify which method the communicating devices get the shared secret key generated by confidentiality algorithm.

According to the IPsec framework, there are 5 important parts available to be chosen in existing algorithms by network administrator when configuring routers. Of course other information such as crypto ACLs and lifetime should be defined during configuration.

5.2 IPsec Protocol

Authentication Header (AH) is IP protocol 51, which can provide data authentication and integrity when IP packets go through two systems. So it is used when confidentiality is not required which means all text is transported unencrypted. [27]

Encapsulating Security Payload (ESP) is IP protocol 50, which can provide not only data authentication and integrity but confidentiality as well. So data payload is encrypted when transporting through two sides. [27]

Besides, both encryption and authentication are optional in ESP, but one of them must be selected at least. I will give you more information later when I discuss the implementation of site-to-site IPsec VPNs.

ESP and AH can be applied to IP packets in two different modes, transport mode and tunnel mode. [27]

In transport mode, security is provided only for the Transport Layer of the OSI model and above. Transport mode protects the payload of the packet but leaves the original IP address in plaintext. The original IP address is used to route the packet through the Internet.

Tunnel mode provides security for the complete original IP packet. The original IP packet is encrypted and then it is encapsulated in another IP packet. This is known as IP-in-IP encryption. The IP address on the outside IP packet is used to route the packet through the Internet.

Figure 5. 2 Figure 5. 5 show different types of IPsec frame encapsulation structure.

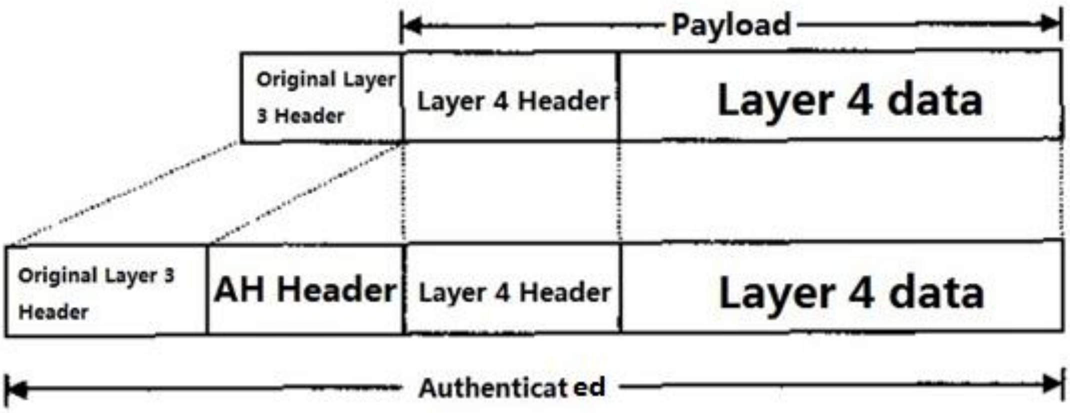


Figure 5. 2. AH Transport Mode [Modified from 25]

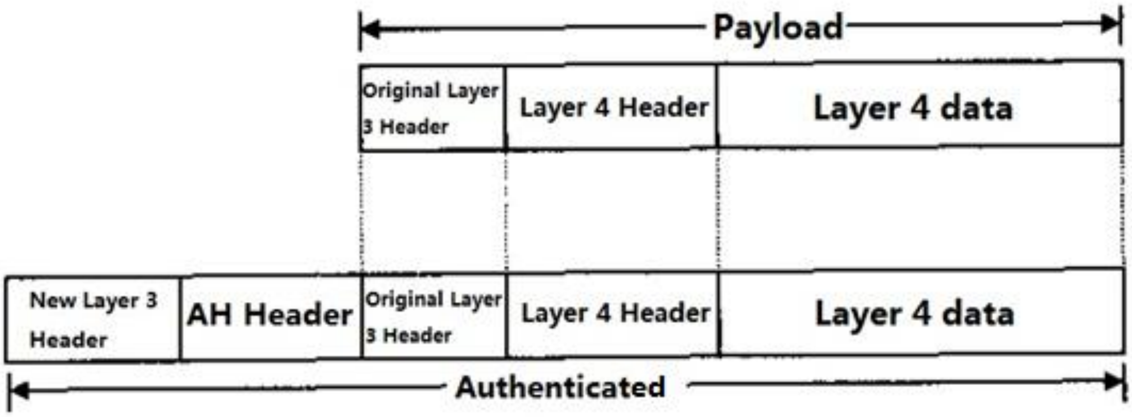


Figure 5. 3. AH Tunnel Mode Packet [Modified from 25]

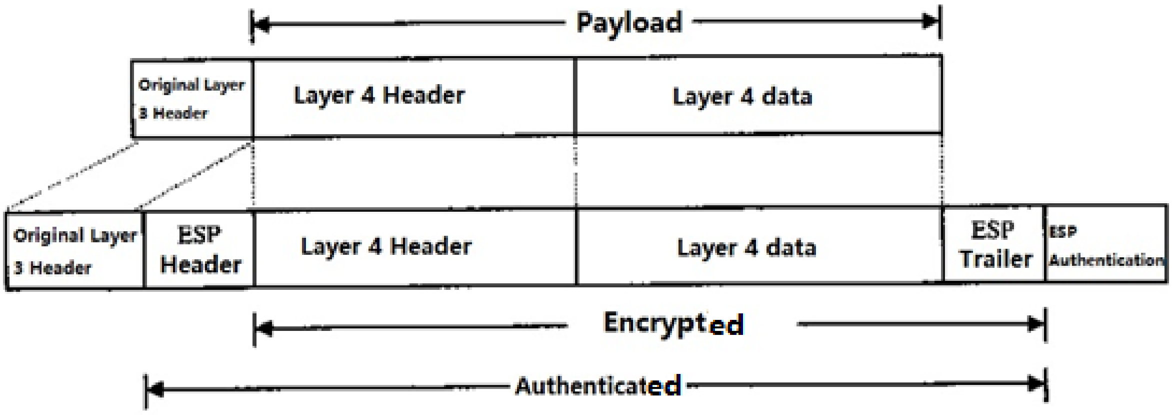


Figure 5. 4. ESP Transport Mode Packet [Modified from 25]

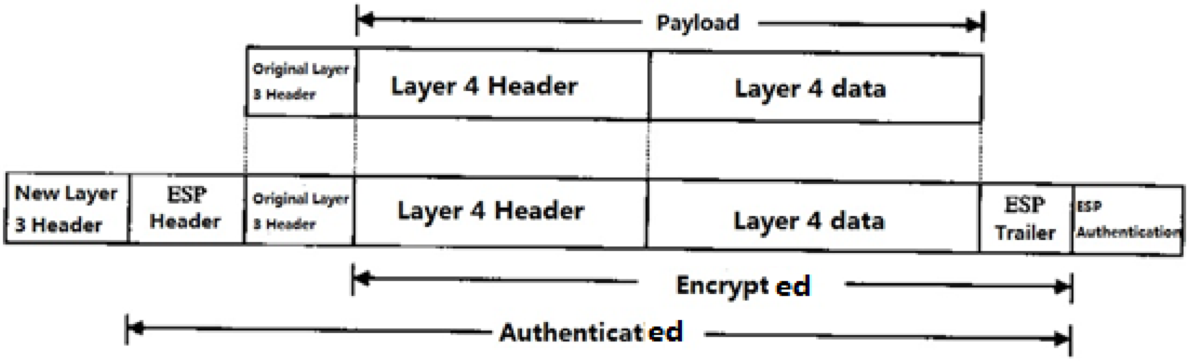


Figure 5. 5. ESP Tunnel Mode Packet [Modified from 25]

5.3 Confidentiality

This part is used only in ESP framework providing encryption methods. AH does not provide data encryption. So, in real world, ESP header is mostly chosen by network administrator when creating VPN tunnel.

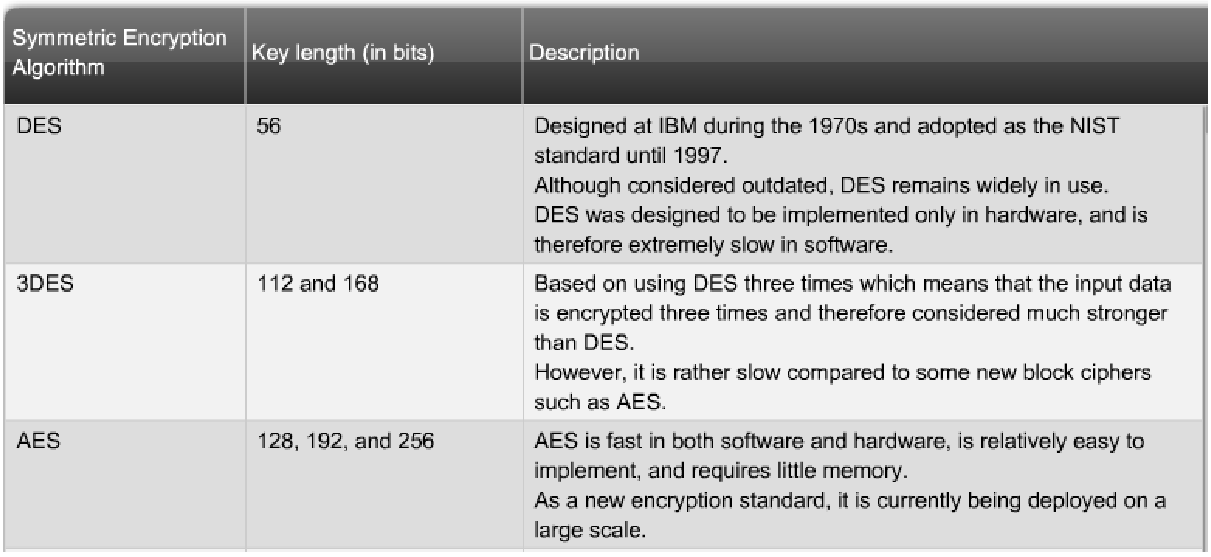
Four encryption algorithms can be chosen in IPsec framework:

DES (Data Encryption Standard) - DES is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally. It is based on a symmetric-key algorithm that uses a 56-bit key. [14]

3DES (Triple DES) - A variant of the 56-bit DES, because of the availability of increasing computational power, the key size of the original DES cipher was becoming subject to brute force attacks. Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a completely new block cipher algorithm. [15]

AES (Advanced Encryption Standard) - The AES is a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor DES. [16]

SEAL (Software Encryption Algorithm) - The Software-optimized Encryption Algorithm (SEAL) is an alternative algorithm to software-based DES, 3DES, and AES. Phillip Rogaway and Don Coppersmith designed SEAL in 1993. It is a stream cipher that uses a 160-bit encryption key. [32] But it is not supported by Cisco IOS until now. Figure 5. 6 compares the first three Cisco supported encryption methods.



Symmetric Encryption Algorithm	Key length (in bits)	Description
DES	56	Designed at IBM during the 1970s and adopted as the NIST standard until 1997. Although considered outdated, DES remains widely in use. DES was designed to be implemented only in hardware, and is therefore extremely slow in software.
3DES	112 and 168	Based on using DES three times which means that the input data is encrypted three times and therefore considered much stronger than DES. However, it is rather slow compared to some new block ciphers such as AES.
AES	128, 192, and 256	AES is fast in both software and hardware, is relatively easy to implement, and requires little memory. As a new encryption standard, it is currently being deployed on a large scale.

Figure 5. 6. DES, 3DES and AES [27]

If for personal use, DES is enough because the longer the key, the harder it is to generate and it is for sure to impact the transform speed and the aftermath is affecting users' mood. It is said that a 64-bit key can take approximately one year to break with a relatively sophisticated computer and a 128-bit key with the same machine can take roughly 10^{19} years to decrypt. [27]

5.4 Integrity

Routers use hash method to provide integrity and get a series of hexadecimal number attached to the packet before sending out. The length of hash value depends on which algorithm has been chosen and this digest is used to authenticate when receiver gets packet.

The hash function hashes arbitrary data into a fixed-length digest known as the hash value, message digest, digest, or fingerprint. [27] There are two common HMAC (Hashed Message Authentication Codes) algorithms:

HMAC-Message Digest 5 (HMAC-MD5) - Uses a 128-bit shared-secret key. The variable-length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash. [27]

HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1) - Uses a 160-bit secret key. Working the same way as MD5 and the output is a 160-bit hash. The algorithm is slightly slower than MD5. [27]

Figure 5. 7 shows a general flow of hash method. Put the arbitrary length text into hash function and get a series of hexadecimal hash value.

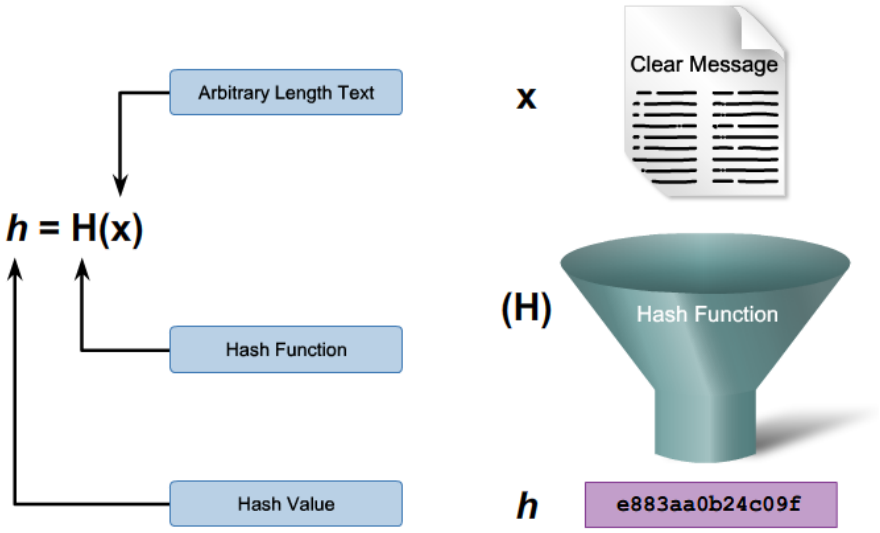


Figure 5. 7. Hash Process [36]

5.5 Authentication

Authentication always works together with a hash method. Put the secret key and variable text into the hash function and get a fixed hash value. This part is to specify what kind of keys are used.

Pre-shared Keys (PSKs): This is a one-way authentication method. Two peers should specify the key manually.

RSA signatures: The exchange of digital certificates authenticates the peers. Each peer must authenticate its opposite peer before the tunnel is considered secure. Unlike PSK, it is a two-way authentication procedure. Local device hash its private key and message and get the hash value. The remote peer should authenticate the received message by recalculating the hash value using the received public key from the original peer.

RSA-encrypted nonces: A nonce is a random number that is generated by the peer. RSA-encrypted nonces use RSA to encrypt the nonce value and other values. This method is the least used of the authentication methods. [27]

Figure 5. 8 shows a picture explainning how integrity and authentication work together.

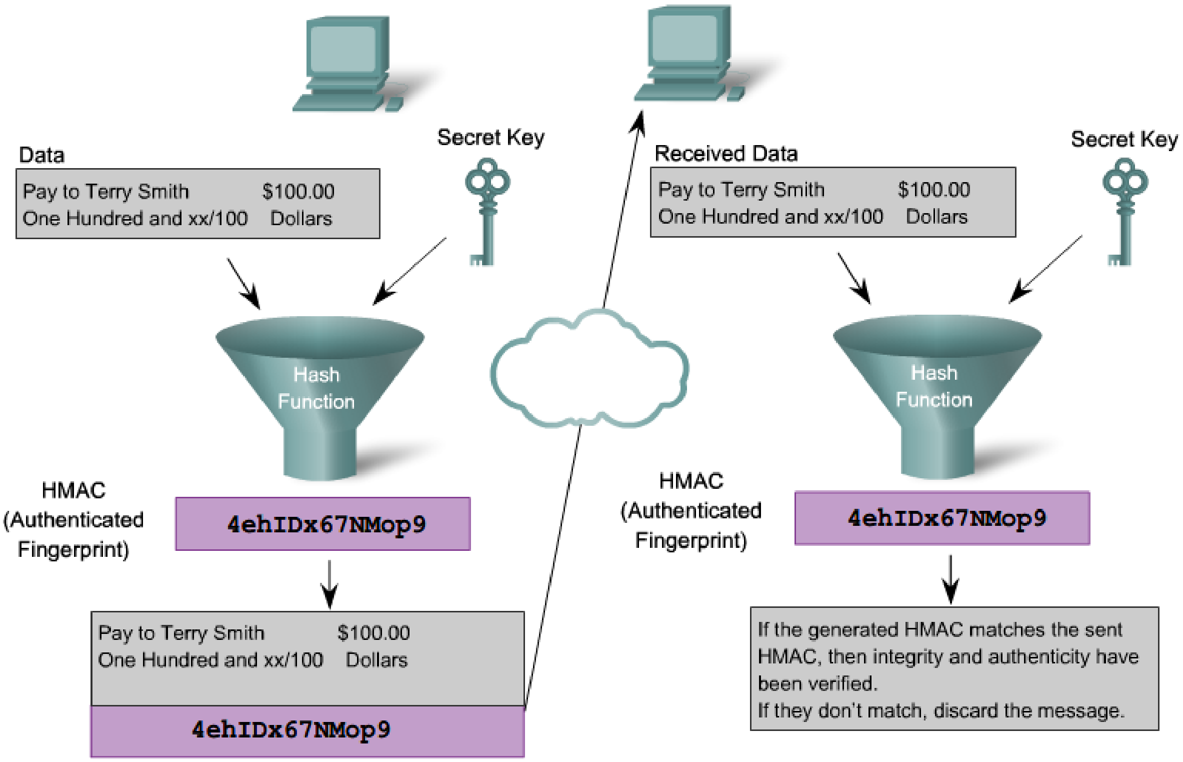

Data
Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars
Secret Key
Hash Function
HMAC (Authenticated Fingerprint)
4ehIDx67NMop9
Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars
4ehIDx67NMop9
Received Data
Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars
Secret Key
Hash Function
HMAC (Authenticated Fingerprint)
4ehIDx67NMop9
If the generated HMAC matches the sent HMAC, then integrity and authenticity have been verified.
If they don't match, discard the message.

Figure 5. 8. Implementation of Integrity and Authentication [27]

5.6 Secure Key Exchange

The DH algorithm is the basis of most modern automatic key exchange methods and is one of the most common protocols used in networking today. Diffie-Hellman is not an encryption mechanism and is not typically used to encrypt data. Instead, it is a method to securely exchange the keys that encrypt data. [27] Encryption algorithms such as DES, 3DES, and AES as well as the MD5 and SHA-1 hashing algorithms require a symmetric, shared public secret key. DH provides a secure key exchange method.

There are four DH groups: 1, 2, 5, and 7. Cisco devices supports group 1 (768-bit key), 2 (1024-bit key) and 5 (1536-bit key). DES and 3DES support groups 1 and 2. AES supports groups 2 and 5. [27]

Until now, I have briefly introduced VPN technology associated protocols and algorithms. In Chapter 7, I will show all the steps of what I have done to create VPN.

6. CONFIGURATION TOOLS

6.1 Two user interfaces

Two main user interfaces used to configure routers and switches are Command Line Interface (CLI) and GUI (Graphical User Interface). CLI looks like using the cmd.exe in Windows or terminal emulator in Linux. GUI instead looks like installing software on computer.

In Cisco device Command Line Interface, the command prompt shows the operating mode. There are three main modes User executive mode, Privileged executive mode, and Global configuration mode. There are also some other specific configuration modes, such as Interface mode, Routing engine mode and Line mode, etc.

Router>	User executive mode
Router#	Privileged executive mode
Router(config)#	Global configuration mode

Router(config-if)#	Interface mode
Router(config-router)#	Routing engine mode
Router(config-line)#	Line mode

In this point, it looks really the same as MS-DOS, while the prompt points out which directory the user is in. Figure 6. 1 shows different types of mode and the hierarchical structure as well as some basic configuration command in command line interface of Cisco devices.

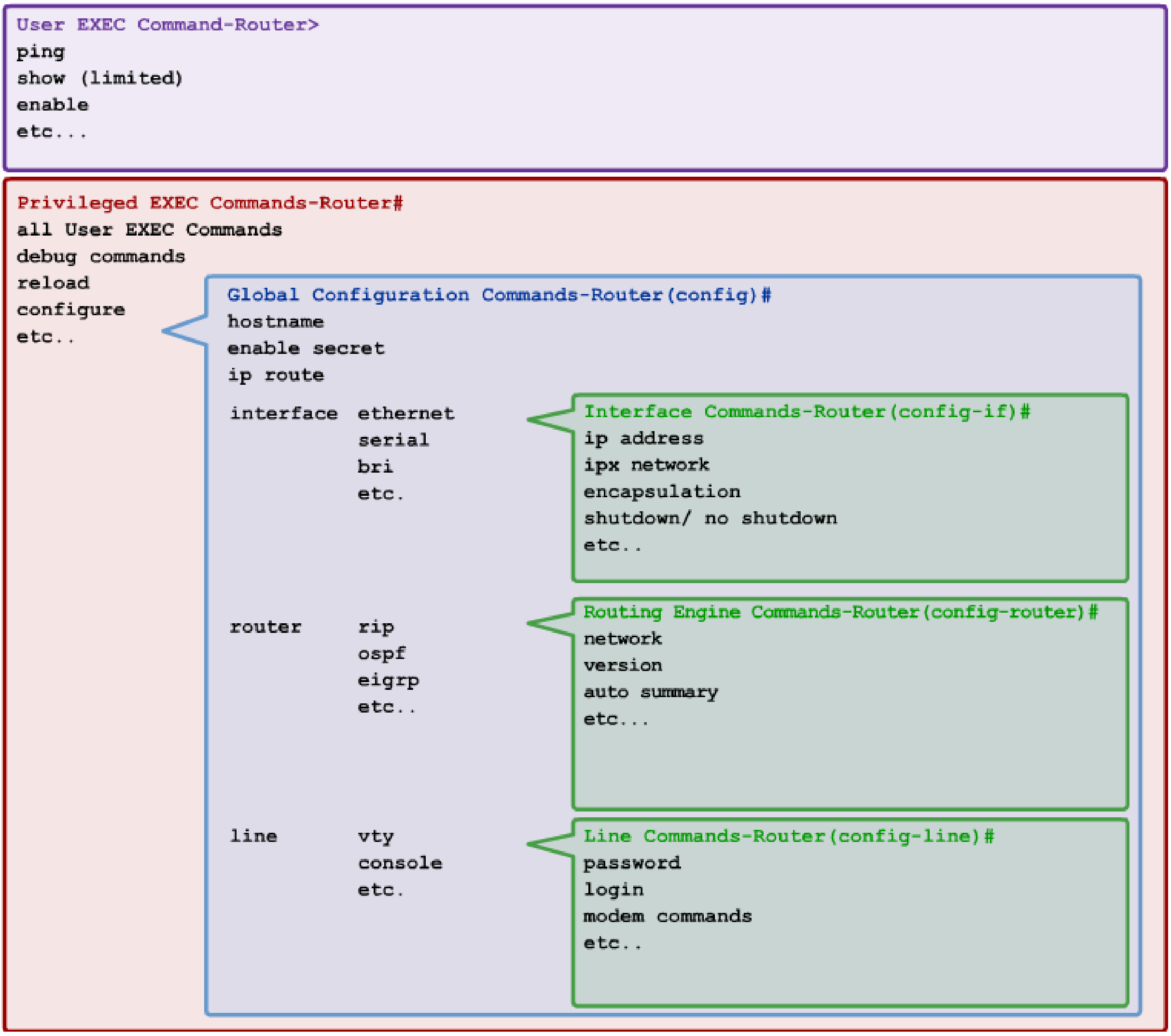


Figure 6. 1. IOS Mode Hierarchical Structure [28]

In the Graphical User Interface, users do not need to remember all the commands to configure router interfaces and routing protocols. The only thing is to click and type some basic information. The hint of how to configure is shown on the screen. It looks really like installation software. So, if network administrators know the basic knowledge, they can qualify the job, because there is always a quick wizard when using the Graphical User Interface.

6.2 Access Methods

There are several ways to access the CLI environment. The most usual methods are Console port, remote access (Telnet or SSH) and Auxiliary port, while Cisco router and Secure Device Manager (SDM) uses remote access connection.

Console port connection uses a low speed roll over cable connected directly between a computer and a router or a switch. This is the most convenient connection option and I have used in my real practical Command Line Interface configuration.

After basic configuration such as username and password of a switch or a router, an available serial port or Fast Ethernet port, which has a remote connection with the computer can be used for telnet and SSH configuration. So, network management assistant can use telnet to fulfill their daily traffic test. In addition, the telnet information are transformed in plaintext, the SSH (Secure Shell) is a more secure method for remote device access. Because SSH provides stronger password authentication than Telnet and uses encryption when transporting session data.

If the remote access connection by Serial ports or Fast Ethernet ports is not available, auxiliary port connection can be used. It is a telephone dialup connection using a modem connected to the router's AUX port. The AUX port can also be used locally, like the console port. However the console port is also preferred over the auxiliary port for troubleshooting because it displays router startup, debugging, and error messages by default. Generally, the only time the AUX port is used locally instead of the console port is when there are problems using the console port, such as when certain console parameters are unknown. [28]

As you can see from Figure 6. 2, console port is used for terminal access, auxiliary port is used for modem access, fast Ethernet ports and serial ports can be used for telnet or SSH access.

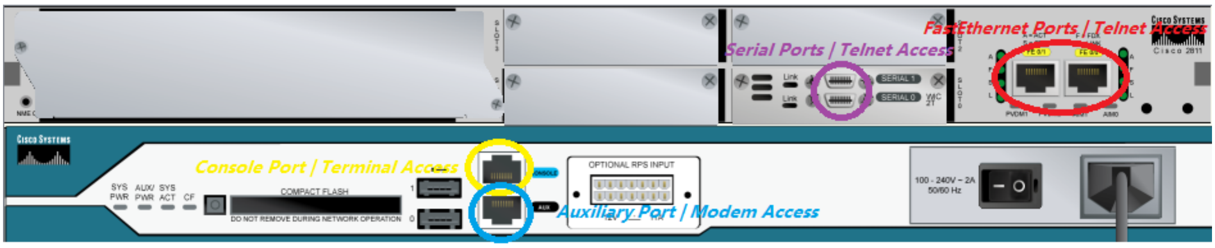


Figure 6. 2. Backboard of Cisco 2811 Router

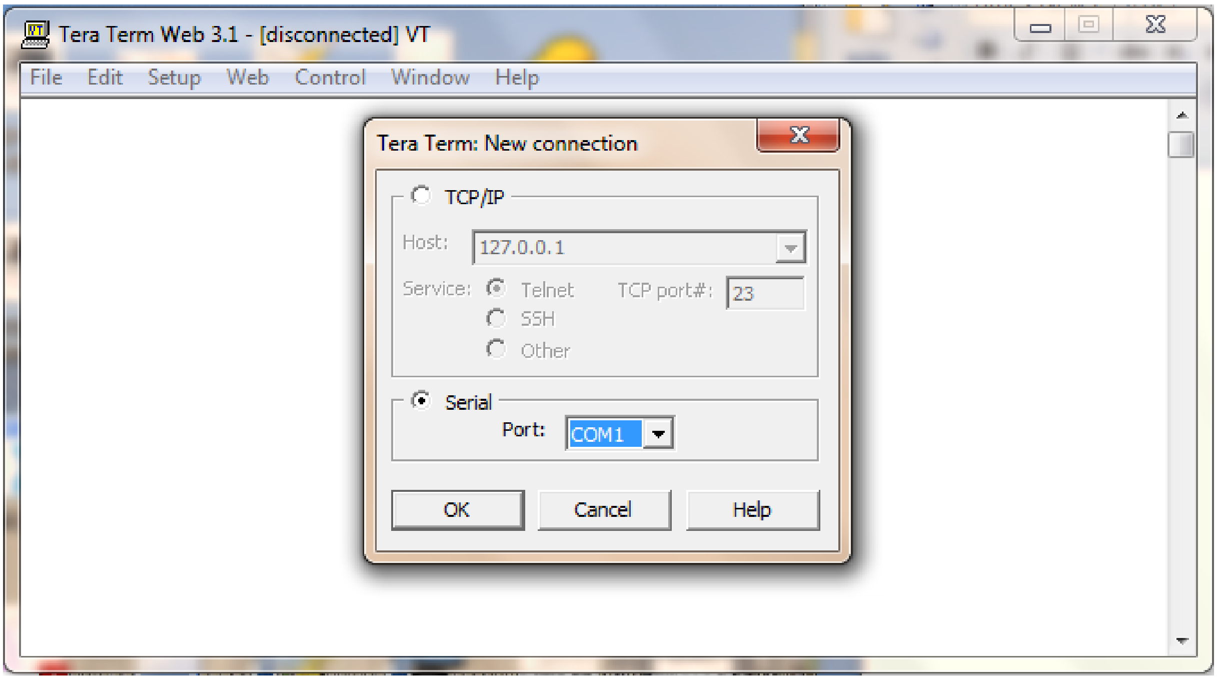
6.3 Terminal Emulator Program

Terminal emulator program is a program that emulates a video terminal within some other display architecture. Though typically synonymous with a command line shell or text terminal, the term terminal covers all remote terminals, including graphical interfaces. A terminal emulator inside a graphical user interface is often called a terminal window. [17]

6.3.1 TeraTerm Web

TeraTerm Web is a simple Windows-based, open-source, free, software implemented terminal emulation program for serial communication that can be used to connect to the console port on Cisco IOS devices. It supports telnet, SSH 1 & 2 and serial port connections. [18] In my practical part, when I create VPN tunnels, I am using this tool to complete Command Line Interface configuration by console port.

Figure 6. 3 shows the initial step of using Tera Term. The first choice is Telnet and the second choice is console.



Tera Term Web 3.1 - [disconnected] VT

Tera Term: New connection

○ TCP/IP

Host: 127.0.0.1

Service: ● Telnet ○ SSH ○ Other

TCP port#: 23

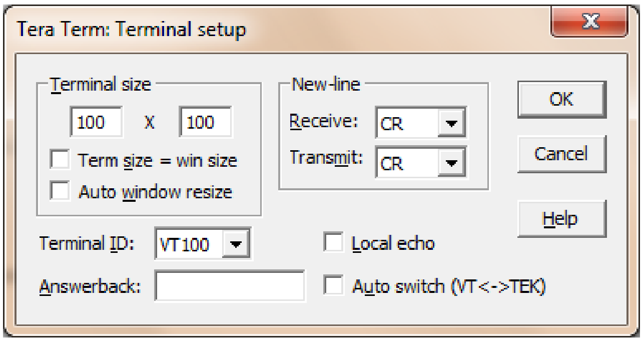
● Serial

Port: COM1

Figure 6. 3. Initial Step of Using Tera Term

Some people who are using it for the very first time may complain that the window and font size are a little bit small also the scroll buffer is too short even after a show command the output can cover the whole scroll buffer and it is not good for the network administrator.

Choose from the MENU, Setup > Terminal, you can change the terminal size. 80*24 is by default (Shown on Figure 6. 4).



Tera Term: Terminal setup

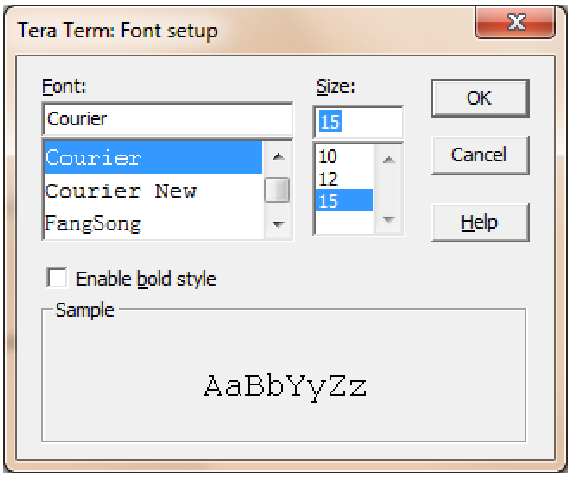
Terminal size: 100 x 100
□ Term size = win size
□ Auto window resize

New-line
Receive: CR
Transmit: CR

Terminal ID: VT100
Answerback:
□ Local echo
□ Auto switch (VT<->TEK)

Figure 6. 4. Terminal Size Changing

Choose from the MENU, *Setup* > *Font*, you can change font size to 15. (Shown on Figure 6. 5)



Tera Term: Font setup

Font: Courier
Courier
Courier New
FangSong

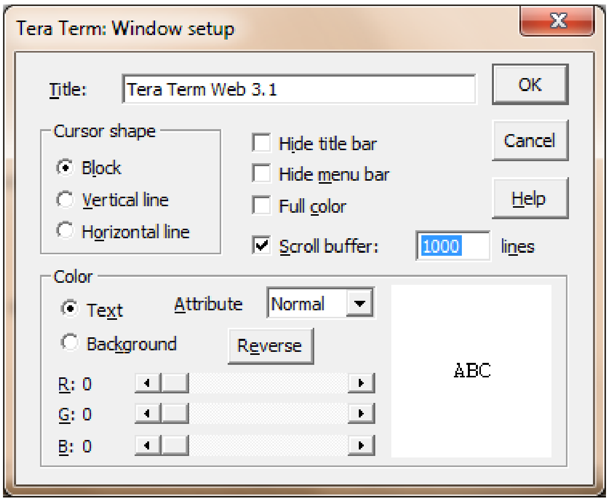
Size: 15
10
12
15

□ Enable bold style

Sample
AaBbYyZz

Figure 6. 5. Font Size Changing

Choose from the MENU, *Setup* > *Window*, you can change the scroll buffer. 100 is by default. (Shown on Figure 6. 6)



Tera Term: Window setup

Title: Tera Term Web 3.1

Cursor shape
● Block
○ Vertical line
○ Horizontal line

□ Hide title bar
□ Hide menu bar
□ Full color
☑ Scroll buffer: 1000 lines

Color
● Text
○ Background
Attribute: Normal
R: 0
G: 0
B: 0
ABC

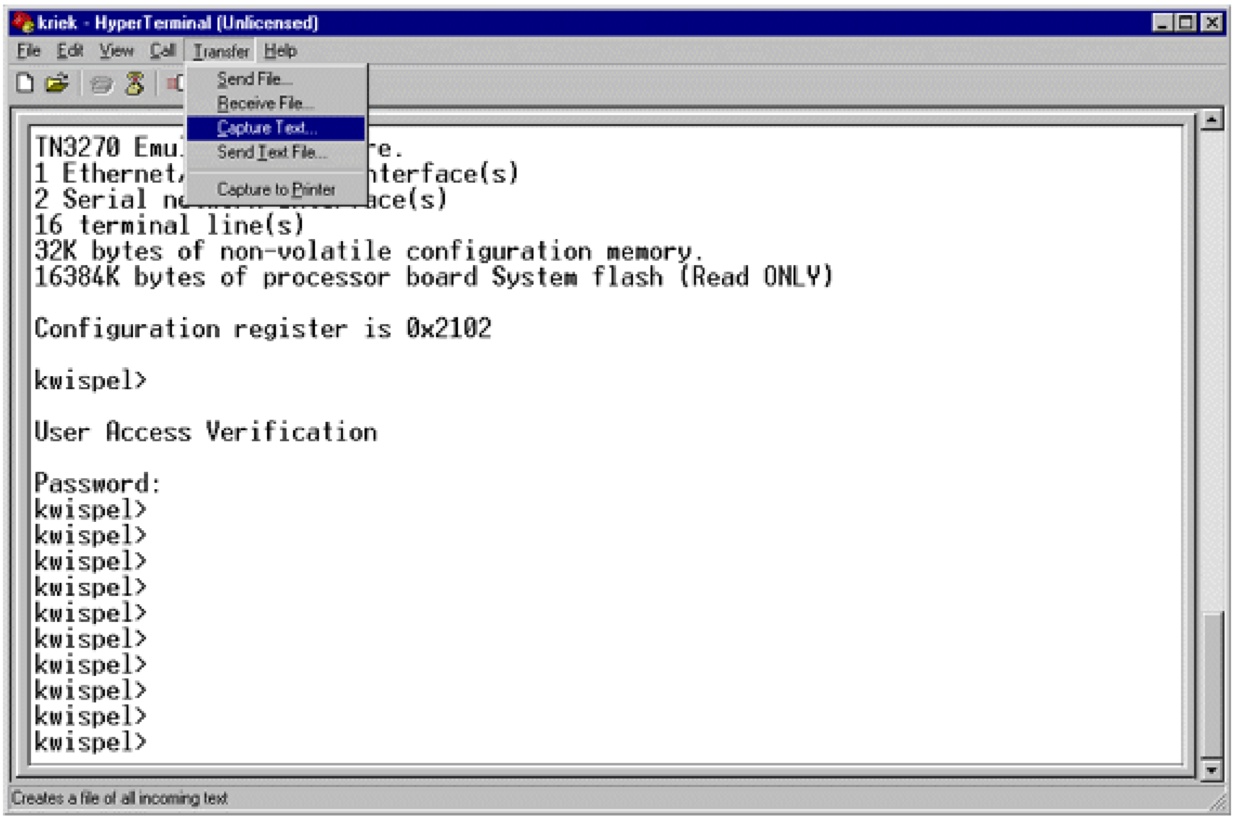
Figure 6. 6. Scroll Buffer Changing

6.3.2 Other Terminal Emulators

Except Tera Term, there are some other terminal emulator software, such as HyperTerminal, Minicom and SecureCRT.

In 1995 Hilgraeve licensed a low-end version of HyperACCESS, known as HyperTerminal (essentially a "Lite" version) to Microsoft for use in their set of communications utilities. It was initially bundled with Windows 95, and subsequently all versions of Windows up to and including Windows XP. Windows Vista and Windows 7 do not include HyperTerminal, though the commercial products HyperTerminal Private Edition and HyperACCESS support all versions of Windows up to and including Windows 7. [19]

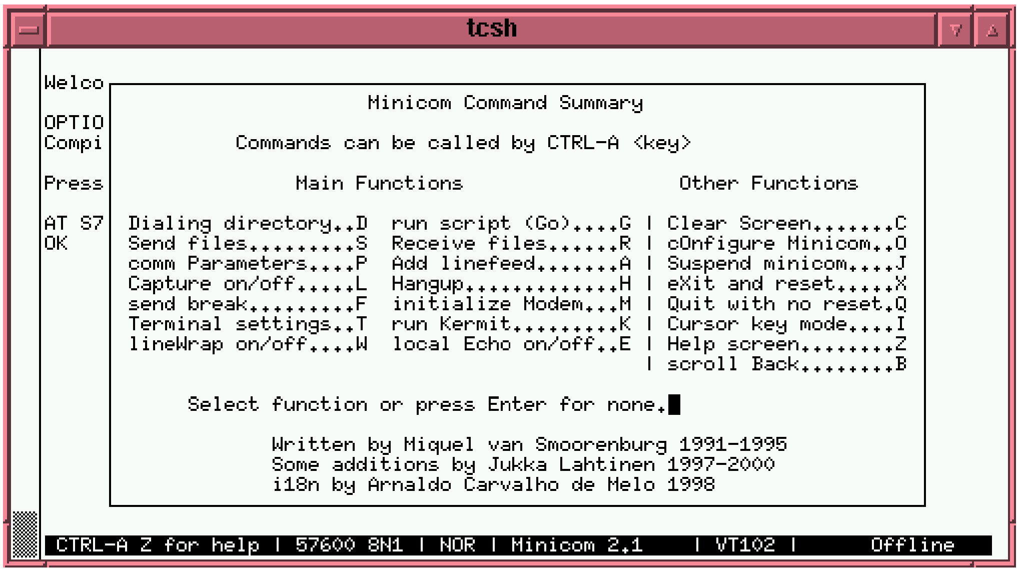
HyperTerminal interface is shown in Figure 6. 7.



```
TN3270 Emu                   e.
1 Ethernet/                  nterface(s)
2 Serial ne                  ace(s)
16 terminal line(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

kwispel>

User Access Verification

Password:
kwispel>
kwispel>
kwispel>
kwispel>
kwispel>
kwispel>
kwispel>
kwispel>
kwispel>
kwispel>
```

Figure 6. 7. HyperTerminal

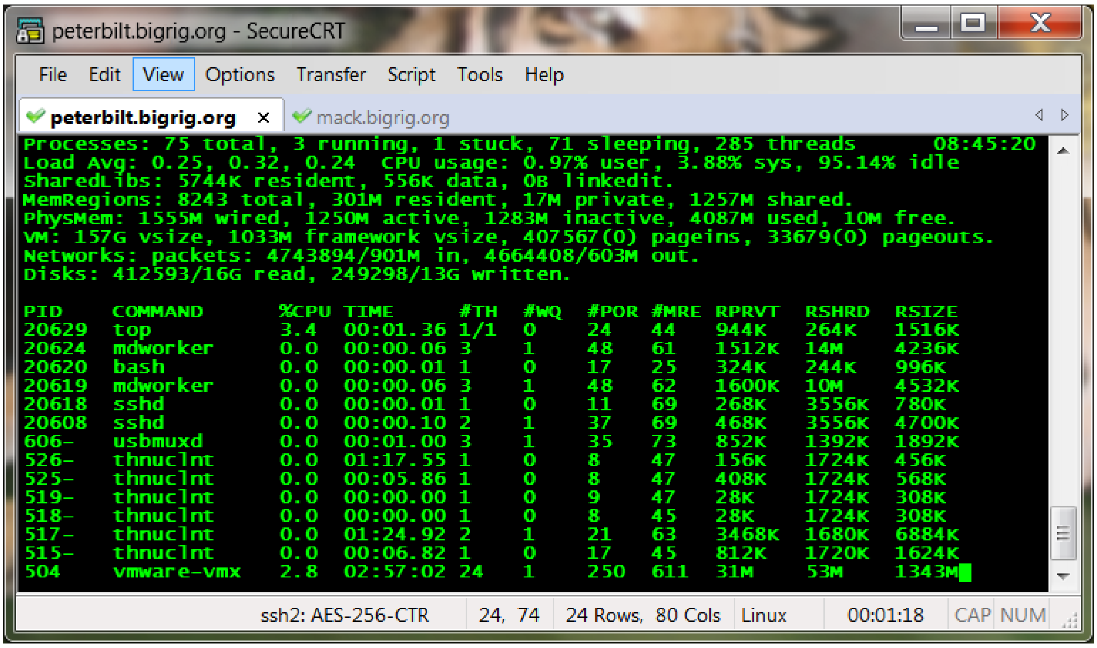
Minicom is a text-based modem control and terminal emulation program for Unix-like operating systems, originally written by Miquel van Smoorenburg, and modeled after the popular MS-DOS program Telix. [20] See Figure 6. 8 for Minicom interface.



```
Welco
                            Minicom Command Summary
OPTIO
Compi              Commands can be called by CTRL-A <key>

Press                 Main Functions                    Other Functions

AT S7 Dialing directory..D  run script (Go)....G | Clear Screen.......C
OK    Send files.........S  Receive files......R | cOnfigure Minicom..O
      comm Parameters....P  Add linefeed.......A | Suspend minicom....J
      Capture on/off.....L  Hangup.............H | eXit and reset.....X
      send break.........F  initialize Modem...M | Quit with no reset.Q
      Terminal settings..T  run Kermit.........K | Cursor key mode....I
      lineWrap on/off....W  local Echo on/off..E | Help screen........Z
                                                 | scroll Back........B

            Select function or press Enter for none.

                    Written by Miquel van Smoorenburg 1991-1995
                    Some additions by Jukka Lahtinen 1997-2000
                    i18n by Arnaldo Carvalho de Melo 1998

 CTRL-A Z for help | 57600 8N1 | NOR | Minicom 2.1    | VT102 |      Offline
```

Figure 6. 8. Minicom

SecureCRT is a commercial SSH and Telnet client and terminal emulator by VanDyke Software. Originally a Windows product, VanDyke has recently added a Mac OS X version and Linux beta. [21] SecureCRT interface is shown in Figure 6. 9.



```
Processes: 75 total, 3 running, 1 stuck, 71 sleeping, 285 threads     08:45:20
Load Avg: 0.25, 0.32, 0.24  CPU usage: 0.97% user, 3.88% sys, 95.14% idle
SharedLibs: 5744K resident, 556K data, 0B linkedit.
MemRegions: 8243 total, 301M resident, 17M private, 1257M shared.
PhysMem: 1555M wired, 1250M active, 1283M inactive, 4087M used, 10M free.
VM: 157G vsize, 1033M framework vsize, 407567(0) pageins, 33679(0) pageouts.
Networks: packets: 4743894/901M in, 4664408/603M out.
Disks: 412593/16G read, 249298/13G written.

PID    COMMAND      %CPU TIME     #TH  #WQ  #POR #MRE RPRVT  RSHRD  RSIZE
20629  top          3.4  00:01.36 1/1  0    24   44   944K   264K   1516K
20624  mdworker     0.0  00:00.06 3    1    48   61   1512K  14M    4236K
20620  bash         0.0  00:00.01 1    0    17   25   324K   244K   996K
20619  mdworker     0.0  00:00.06 3    1    48   62   1600K  10M    4532K
20618  sshd         0.0  00:00.01 1    0    11   69   268K   3556K  780K
20608  sshd         0.0  00:00.10 2    1    37   69   468K   3556K  4700K
606-   usbmuxd      0.0  00:01.00 3    1    35   73   852K   1392K  1892K
526-   thnuclnt     0.0  01:17.55 1    0    8    47   156K   1724K  456K
525-   thnuclnt     0.0  00:05.86 1    0    8    47   408K   1724K  568K
519-   thnuclnt     0.0  00:00.00 1    0    9    47   28K    1724K  308K
518-   thnuclnt     0.0  00:00.00 1    0    8    45   28K    1724K  308K
517-   thnuclnt     0.0  01:24.92 2    1    21   63   3468K  1680K  6884K
515-   thnuclnt     0.0  00:06.82 1    0    17   45   812K   1720K  1624K
504    vmware-vmx   2.8  02:57:02 24   1    250  611  31M    53M    1343M
```

```
ssh2: AES-256-CTR | 24, 74 | 24 Rows, 80 Cols | Linux | 00:01:18 | CAP NUM
```

Figure 6. 9. SecureCRT

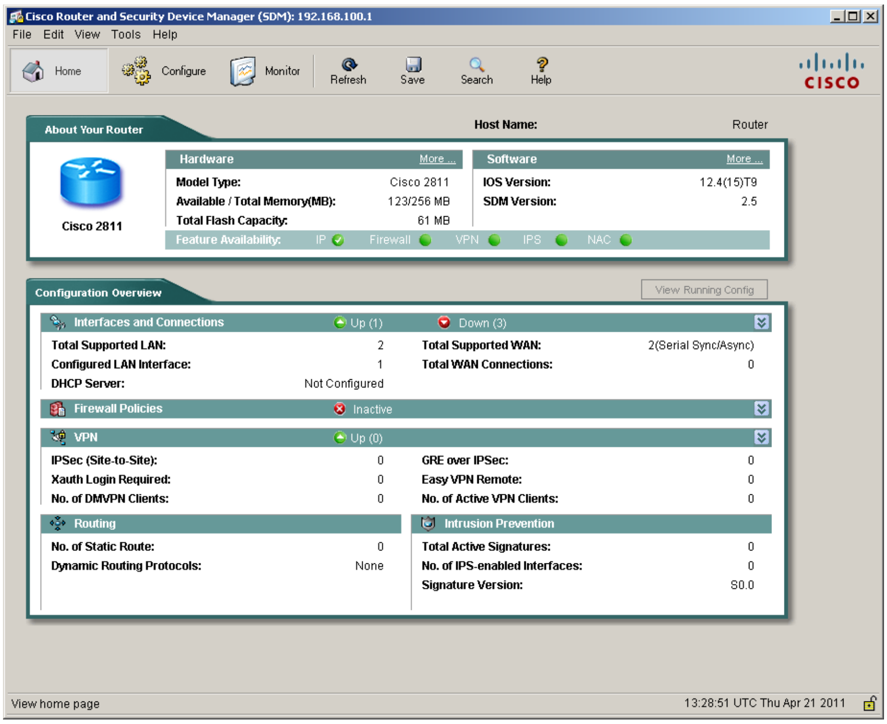
6.4 Cisco Router and Secure Device Manager

SDM is an easy-to-use, Java-based device management tool, designed for configuring LAN, WAN, and security features on a router. SDM is designed for resellers and network administrators of small- to medium-sized businesses who are proficient in basic network design. For fast and efficient configuration of Ethernet networks, WAN connectivity, firewalls and Virtual Private Networks (VPNs), Cisco SDM prompts you through the setup process with wizards. Cisco SDM requires no previous experience with Cisco devices or the Cisco command-line interface (CLI). SDM can reside in router memory or on your PC. [22]

6.4.1 SDM Supporting

Below are the requirements of the SDM. [23]

SDM supports Cisco 2811 router with the IOS version 12.3(8) T4 or later. A minimum of 6 MB of free memory is required to support all SDM files. 2 MB of router memory is required to support SDM Express when SDM is installed on the PC, and the SDM files on the PC require 5.5 MB. SDM is designed to run on a personal computer that has a Pentium III or faster processor. SDM can be run on a PC running Microsoft Windows XP Professional. SDM can be used with the browser Internet Explorer version 5.5 and later. SDM requires Sun Java Runtime Environment (JRE) version 1.4.2_05 or later. Figure 6. 10 shows the home interface of SDM.



Host Name: Router

Model Type: Cisco 2811
Available / Total Memory(MB): 123/256 MB
Total Flash Capacity: 61 MB

IOS Version: 12.4(15)T9
SDM Version: 2.5

Feature Availability: IP ✓ Firewall ● VPN ● IPS ● NAC ●

Interfaces and Connections: Up (1) Down (3)

Total Supported LAN: 2
Configured LAN Interface: 1
DHCP Server: Not Configured
Total Supported WAN: 2(Serial Sync/Async)
Total WAN Connections: 0

Firewall Policies: Inactive

VPN: Up (0)

IPSec (Site-to-Site): 0
Xauth Login Required: 0
No. of DMVPN Clients: 0
GRE over IPSec: 0
Easy VPN Remote: 0
No. of Active VPN Clients: 0

Routing

No. of Static Route: 0
Dynamic Routing Protocols: None

Intrusion Prevention

Total Active Signatures: 0
No. of IPS-enabled Interfaces: 0
Signature Version: S0.0

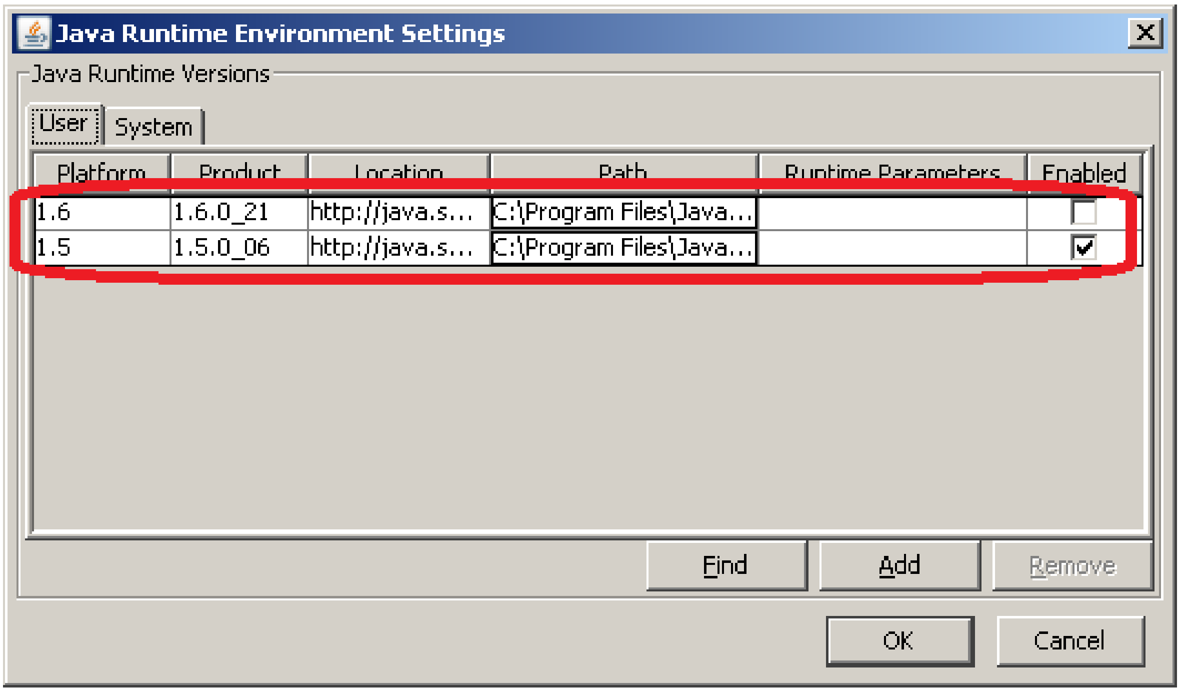
13:28:51 UTC Thu Apr 21 2011

Figure 6. 10. SDM User Interface

In addition to the requirement that Cisco website recommends, there are some other important notes that I have to mention. It seems SDM is no longer supported by Cisco. It means that the latest version of the associated program may not support SDM. In my practical part, I got into some trouble with this Graphical User Interface configuration tool. Such as user can not initiate SDM and even if launching correctly, users are only allowed to handle basic configuration but not some advanced configuration such as Firewall and VPN. These challenges were related to the interoperability problem explained below.

In the first place, the language environment of Operating System should be consistent with SDM, and it is better to use Windows XP, instead of Windows7. My Operating System is Windows7 with Chinese environment, supporting Multilanguage switching. When I change the language into English, my OS is still not compatible with English SDM.

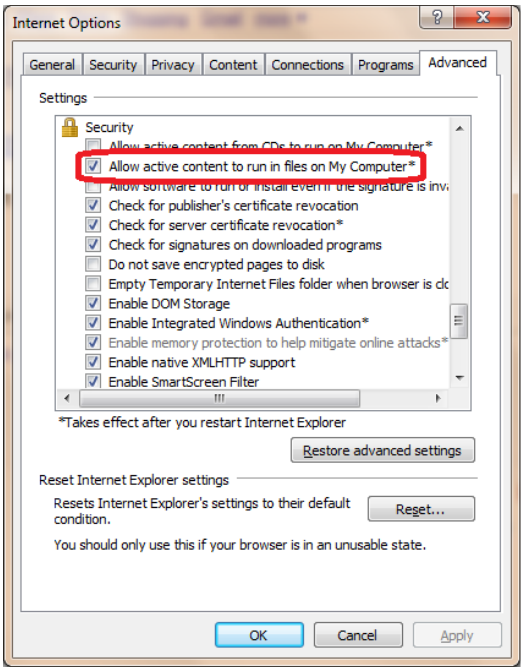
What is more, the latest Java Runtime Environment 1.6.0_21 does not support all the function of SDM. The best way is to downgrade the version to 1.5. After installing Java environment correctly, in bottom right corner task bar, choose Java Control Panel, *Java* > *View* > *User*, disable Java 1.6 and enable Java 1.5. (See Figure 6. 11 for details)



Platform	Product	Location	Path	Runtime Parameters	Enabled
1.6	1.6.0_21	http://java.s...	C:\Program Files\Java...		□
1.5	1.5.0_06	http://java.s...	C:\Program Files\Java...		☑

Figure 6. 11. Change Java Runtime Environment Version

Last but not least, do not forget to change the Internet Explorer property, click *Tools* > *Intnet Options*> *Advanced* and tag the option '*Allow active content to run in files on My Computer*' as shown in Figure 6. 12.



Settings

Security

☐ Allow active content from CDs to run on My Computer*
☑ Allow active content to run in files on My Computer*
☐ Allow software to run or install even if the signature is inv
☑ Check for publisher's certificate revocation
☑ Check for server certificate revocation*
☑ Check for signatures on downloaded programs
☐ Do not save encrypted pages to disk
☐ Empty Temporary Internet Files folder when browser is clc
☑ Enable DOM Storage
☑ Enable Integrated Windows Authentication*
☑ Enable memory protection to help mitigate online attacks*
☑ Enable native XMLHTTP support
☑ Enable SmartScreen Filter

*Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Figure 6. 12. Change Internet Explorer Property

After paying attention to these matters, you can use this easy-to-use software to finish advanced configuration tasks such as VPN. Here is my practical environment:

Cisco 2811 router with IOS version 12.4(15) T9
SDM version is 2.5
Operating System is Windows XP SP3 in English
Java Version 1.5.0_06

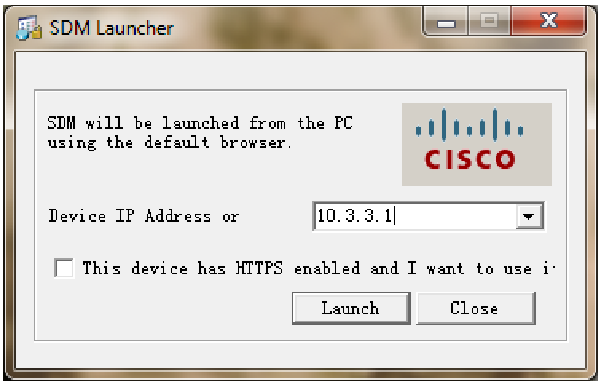
Before using SDM, you should first ensure that the ip address of a computer and one router interface are in the same network. Then after some necessary configuration, the router will support Cisco SDM successfully. In my case, SDM is running on PC2 and PC3. The compulsory configuration is shown below.

```
    R2(config)#ip http server   //   Enable HTTP server
    R2(config)#ip http secure-server   //   Enable HTTPS server
    R2(config)#ip http authentication local   //   Use local authentification
    R2(config)#username Student privilege 15 secret cisco   //   Define username ’Student’,
password ’cisco’and the highest privilege 15
    R2(config)#line vty 0 4
    R2(config-line)#privilege level 15   //   Specify the user who has privilege level 15 can
access virtual terminal port
```

R2(config-line)#login local // Enable local password checking

R2(config-line)#transport input telnet ssh // Configure SSH and Telnet

After necessary configuration, you can launch to the SDM interface. Figure 6. 13 shows the launching interface.



SDM will be launched from the PC using the default browser.

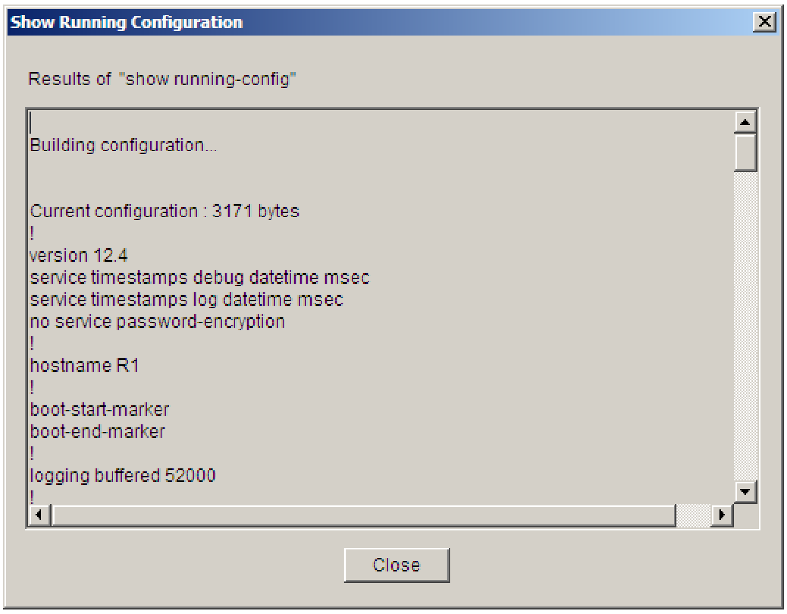
Device IP Address or 10.3.3.1

□ This device has HTTPS enabled and I want to use i·

Figure 6. 13. SDM Launching Interface

6.4.2 Basic Router Configuration by SDM

In home page, there is a button to show running configuration, shown on Figure 6. 14.



Results of "show running-config"

```
Building configuration...

Current configuration : 3171 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging buffered 52000
!
```

Figure 6. 14. Results of ‘show running-config’ by SDM

SDM is a comprehensive graphical interface Cisco router configuration tool that can implement almost all the tasks. Figure 6. 15 displays the basic router configuration tasks we have learned before that I have found from the tool.

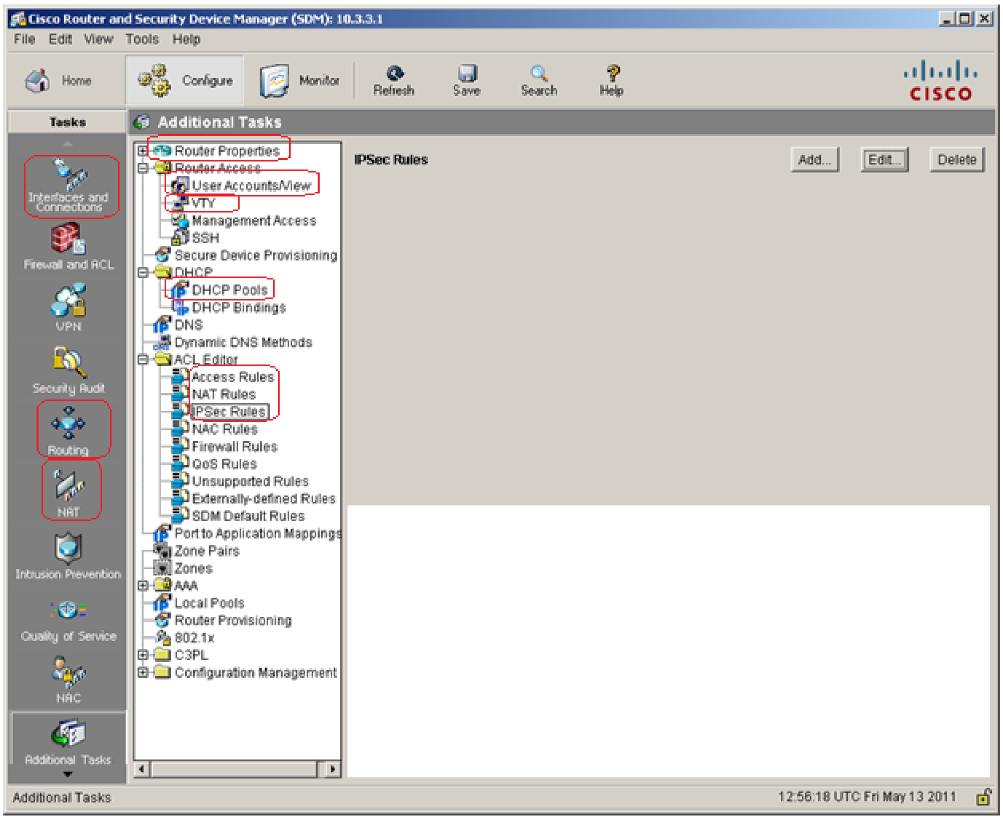
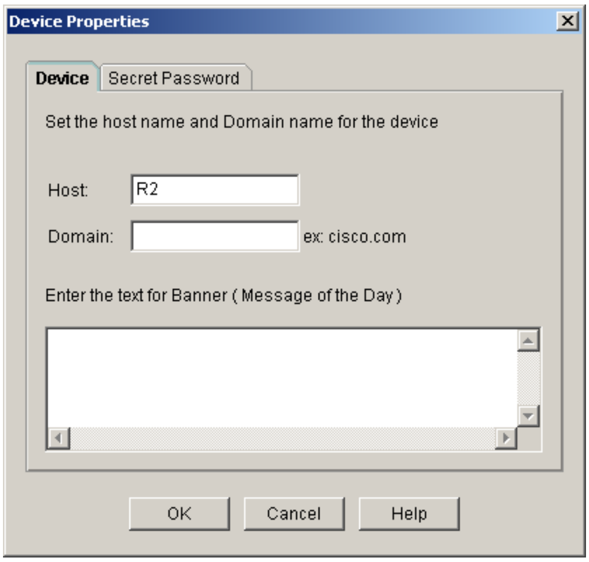


Figure 6. 15. Basic Router Configuration by SDM

To be more specific:

Host name, domain name and daily banner (Shown on Figure 6. 16):

PATH: *Configure* > *Additional Tasks* > *Router Properties* > *Device*



Set the host name and Domain name for the device

Host: R2

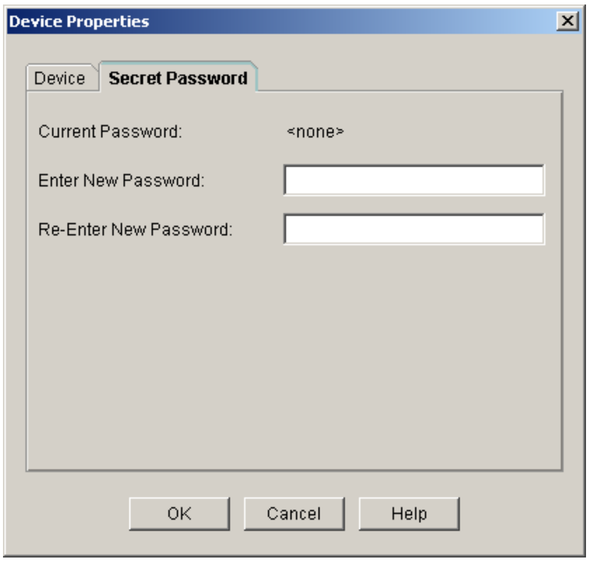
Domain: ex: cisco.com

Enter the text for Banner (Message of the Day)

Figure 6. 16. Configure Device Properties-Device

Enable secret can be configured in the following path (Shown on Figure 6. 17):

PATH: *Configure > Additional Tasks > Router Properties > Secret Password*

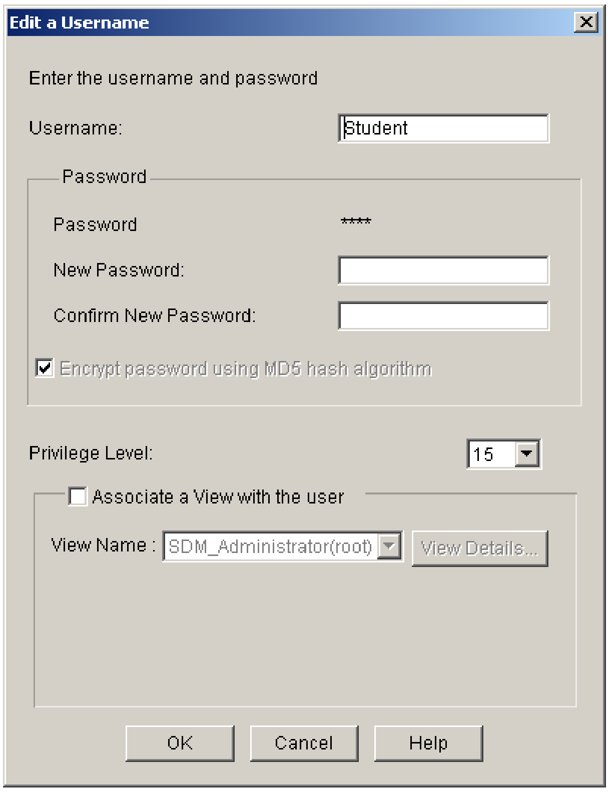


Current Password: <none>

Figure 6. 17. Configure Device Properties-Secret Password

User name, privilege and secret (Shown on Figure 6. 18):

PATH: *Configure > Additional Tasks > Router Access > User Accounts/View*



Username: Student

Password ****

☑ Encrypt password using MD5 hash algorithm

Privilege Level: 15

□ Associate a View with the user

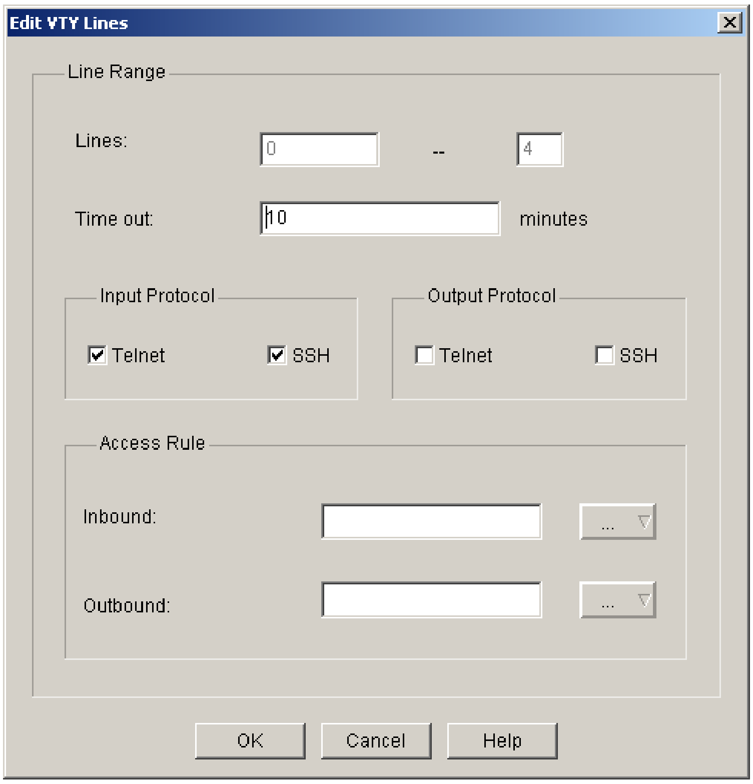
View Name : SDM_Administrator(root)

Figure 6. 18. Edit Username

Line VTY (Shown on Figure 6. 19):

PATH: *Configure > Additional Tasks > Router Access > VTY*

In here I have not found how to create line vty password.



Edit VTY Lines

Line Range

Lines: 0 -- 4

Time out: 10 minutes

Input Protocol

☑ Telnet ☑ SSH

Output Protocol

□ Telnet □ SSH

Access Rule

Inbound:

Outbound:

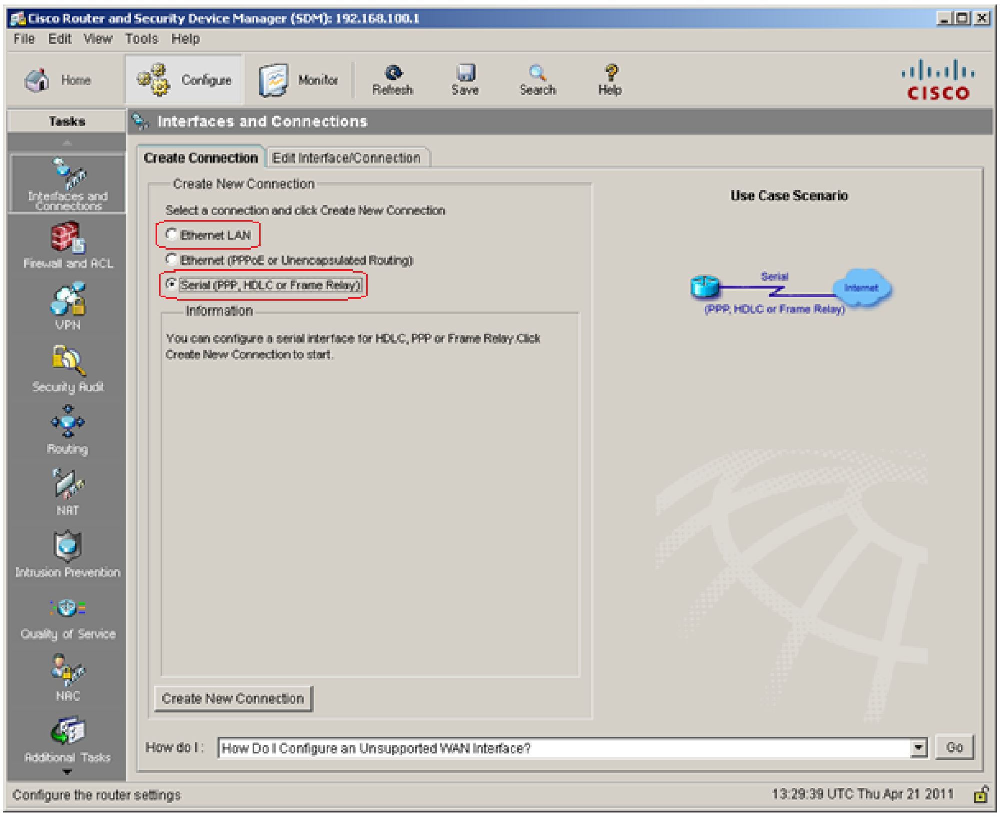
Figure 6. 19. Edit VTY Lines

Access Control List (including Access Rules, NAT Rules and IPSec Rules):

PATH: *Configure > Additional Tasks > ACL Editor > Access Rules (NAT Rules or IPSec Rules)*

Access rules specify which network addresses are allowed to go out or come in, the addresses that are not specified will be denied. Unlike access rules, NAT rules define which network addresses are eligible to be translated, the addresses that are not defined will be sent out directly without address translation. While IPsec rules point out which IP addresses to be protected, the addresses that are not pointed out will be sent in plaintext.

Interfaces (including Ethernet and Serial port): In Ethernet option, administrator can choose either normal port or creating subinterfaces. In Serial option, there are three encapsulation types, PPP, HDLC and Frame Relay. (Shown on Figure 6. 20)



Interfaces and Connections

Create New Connection

Select a connection and click Create New Connection

○ Ethernet LAN

○ Ethernet (PPPoE or Unencapsulated Routing)

● Serial (PPP, HDLC or Frame Relay)

Information

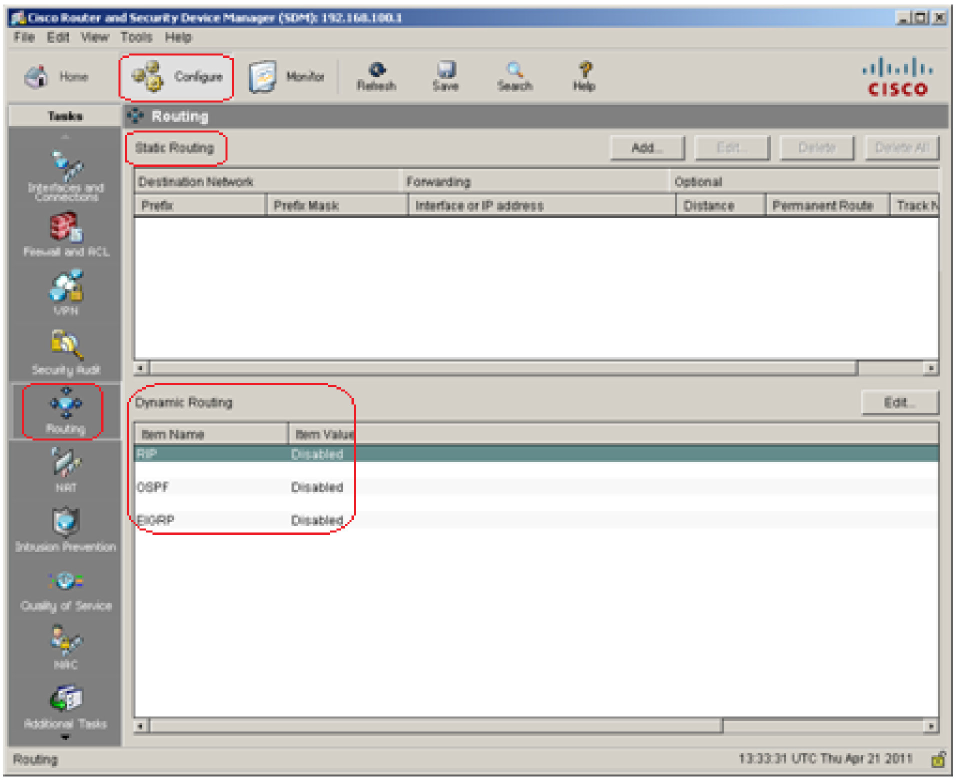
You can configure a serial interface for HDLC, PPP or Frame Relay.Click Create New Connection to start.

How do I : How Do I Configure an Unsupported WAN Interface?

Configure the router settings 13:29:39 UTC Thu Apr 21 2011

Figure 6. 20. Interfaces and Connections

Routing Protocols, including static routing and three dynamic routing protocols, RIP, OSPF and EIGRP, but the BGP protocol is not supported in here. (Shown on Figure 6. 21)



Routing

Static Routing

Destination Network		Forwarding	Optional		
Prefix	Prefix Mask	Interface or IP address	Distance	Permanent Route	Track N

Dynamic Routing

Item Name	Item Value
RIP	Disabled
OSPF	Disabled
EIGRP	Disabled

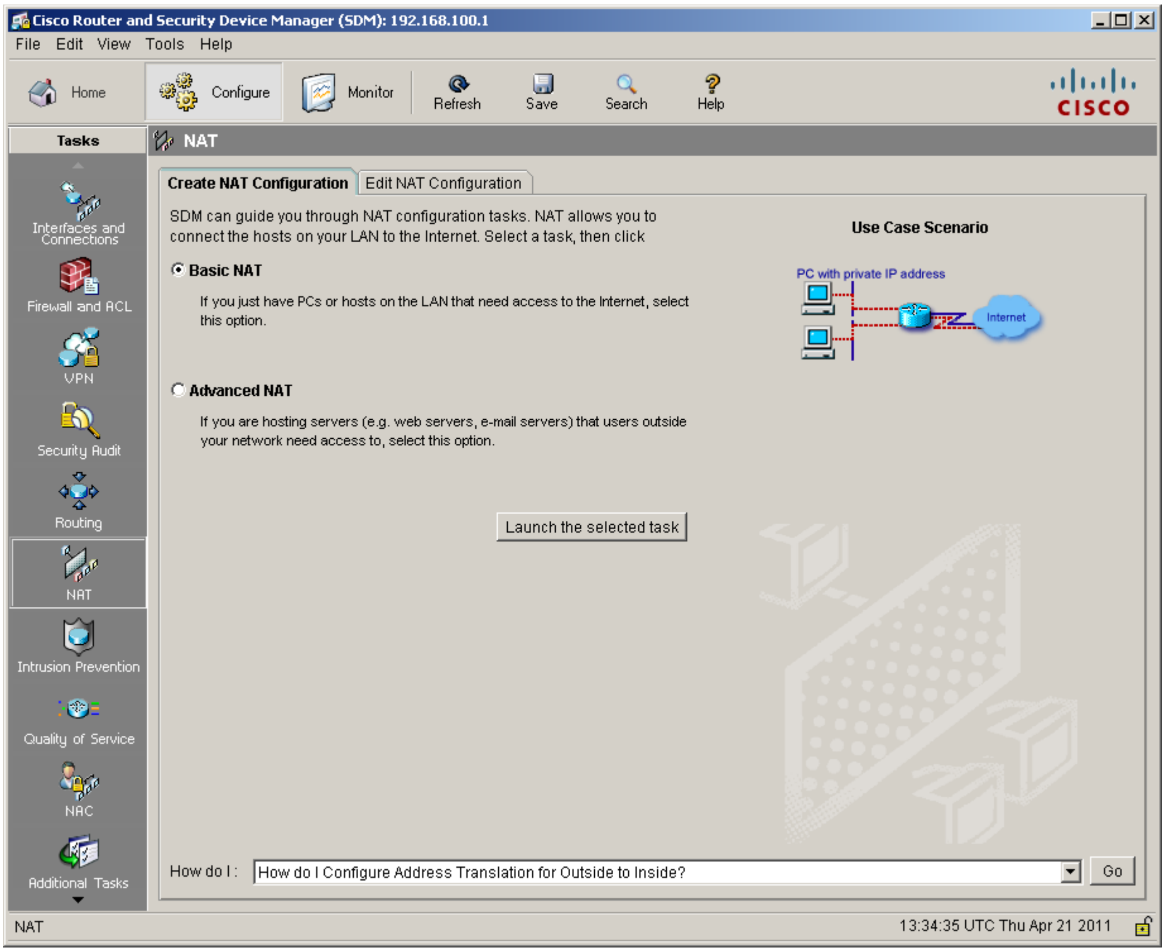
Routing 13:33:31 UTC Thu Apr 21 2011

Figure 6. 21. Routing Protocols

Network Address Translation, including basic NAT and advanced NAT. (Shown on Figure 6. 22)

The basic Network Address Translation provides the normal translation between the LAN hosts' private address and public address.

The advanced Network Address Translation specifies which ip address need to translate and which do not need to, because typically the server ip address should not be translated so that the users outside the local area network can communicate with the server.



SDM can guide you through NAT configuration tasks. NAT allows you to connect the hosts on your LAN to the Internet. Select a task, then click

● Basic NAT

If you just have PCs or hosts on the LAN that need access to the Internet, select this option.

○ Advanced NAT

If you are hosting servers (e.g. web servers, e-mail servers) that users outside your network need access to, select this option.

How do I : How do I Configure Address Translation for Outside to Inside?

NAT

13:34:35 UTC Thu Apr 21 2011

Figure 6. 22. Network Address Translation

7. CREATING VIRTUAL PRIVATE NETWORKS

7.1 Network Topology

Imagine that there is a huge company located in Helsinki (Headquarter) which has a branch office in Mikkeli (Branch Office). Besides, this company cooperates with another company located in Sweden (Collaborate Company). Here is the topology shown in Figure 7. 1.

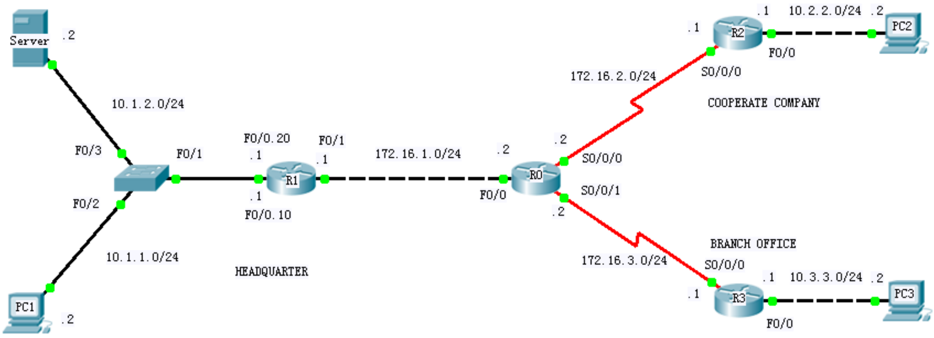


Figure 7. 1. VPN Topology

Supposing that I am a network administrator, and my job is to ensure that the traffic between headquarter and branch office is encrypted so that no other people in the network are not allowed to eavesdrop and distort the information. And the collaborated company can communicate with some part of staff in headquarter to discuss the business collaboration in secret but not allowed to catch the information of the data server.

The central router R0 works like Internet Service Provider being responsible for the connection of all available users. It is better using a network cloud instead of just one router. Internet is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. [24] Besides in the real world, typically serial cable is used to connect to Service Provider. But in our laboratory, one router just has one WAN Interface Card -2T module which provides 2 Serial ports. So I have to use a Fast Ethernet port. But anyway, it is not a big problem, because VPN tunnel is created between 2 routers, regardless of type of interface.

As you can see, there are three different located companies along with three configuration methods, CLI, SDM quick setup and SDM step-by-step setup. In my practical part, I combine these together to one topology. Here is my arrangement:

R1:	*CLI*
R2:	*SDM step-by-step*
R3:	*SDM quick setup*

7.2 Preparation

In my practical environment, my using devices are listed below:

Cisco 2811 Router×4
Cisco 2960 Switch×1
Computer×4
Serial Cable×2
Straight Forward Cable×3
Cross Over Cable×3
Roll Over Cable×n

There is at least one roll over cable. If there is not enough roll over cables, I can configure each router and switch one by one. Besides, there is not any big difference between a computer and a server. Server has special hardware and softwire, but both of these two devices are designed based on the same structure. So in here, I use four computers instead of three computers and one server.

Before the configuration of Virtual Private Network, I should first configure all the routers and switches to make sure all the terminals can communicate between each other. In here I use Command Line Interface. Besides, all the following configuration of routers can also be created by SDM.

Basic Configuration of R0:

```
Router>enable
Router#configure terminal
Router(config)#hostname R0
R0(config)#no ip domain-lookup
R0(config)#line console 0
```

```
R0(config-line)#logging synchronous
R0(config-line)#no exec-timeout
```

The last 2 commands are useful. When you type commands, sometimes there is some weird commands display automatically and affect users normal typing. the first command is used to solve this problem. The second command solves the timeout problem. But in the real world, this causes some secure problems that anyone can access to privileged executive mode without typing username and password. So in the real world, it is highly recommending that not typing this command. After typing this command, user will be still in the current mode and will not exit. It will avoid annoying password retyping after a long time no operating with routers or switches. Same configuration is configured on other routers and switches. It is better to configure console port password, telnet password and enable secret, especially in the real world.

Configuration of the Interfaces of R0:

```
R0(config)#interface fastEthernet 0/0
R0(config-if)#ip address 172.16.1.2 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#interface serial 0/0/0
R0(config-if)#ip address 172.16.2.2 255.255.255.0
R0(config-if)#clock rate 64000
R0(config-if)#no shutdown
R0(config-if)#interface serial 0/0/1
R0(config-if)#ip address 172.16.3.2 255.255.255.0
R0(config-if)#clock rate 64000
R0(config-if)#no shutdown
```

Same configuration is created on R1, R2 and R3. In addition, I use single-arm routing technology to create VLAN. Subinterfaces are configured on fast Ethernet 0/0 of R1 and trunk port is configured on S0/1 of S1. Following are the configuration of R1 and S1:

```
R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 10.1.1.1 255.255.255.0
```

```
R1(config-subif)#interface fastEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 10.1.2.1 255.255.255.0
R1(config-subif)#interface fastEthernet 0/0
R1(config-if)#no shutdown

S1(config)#vlan 10
S1(config-vlan)#name STAFF
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name SERVER
S1(config-vlan)#interface fastEthernet 0/1
S1(config-if)#switchport mode trunk
S1(config-if)#interface fastEthernet 0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#interface fastEthernet 0/3
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
```

After that, it is time to define routing protocols. In here, the topology is not very complicated, static route is enough to fulfill the communication in the network. So I define static route on R0 and default static route on other routers.

```
R0(config)#ip route 10.1.1.0 255.255.255.0 fastEthernet 0/0
R0(config)#ip route 10.1.2.0 255.255.255.0 fastEthernet 0/0
R0(config)#ip route 10.2.2.0 255.255.255.0 serial 0/0/0
R0(config)#ip route 10.3.3.0 255.255.255.0 serial 0/0/1

R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2

R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2

R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.3.2
```

The full configurations of R0 and S1 are listed on appendix A and appendix B. After above configurations, computers can communicate between each other but the information is transferred in plaintext. If ping command is not successful, you can use the following command to check the configuration.

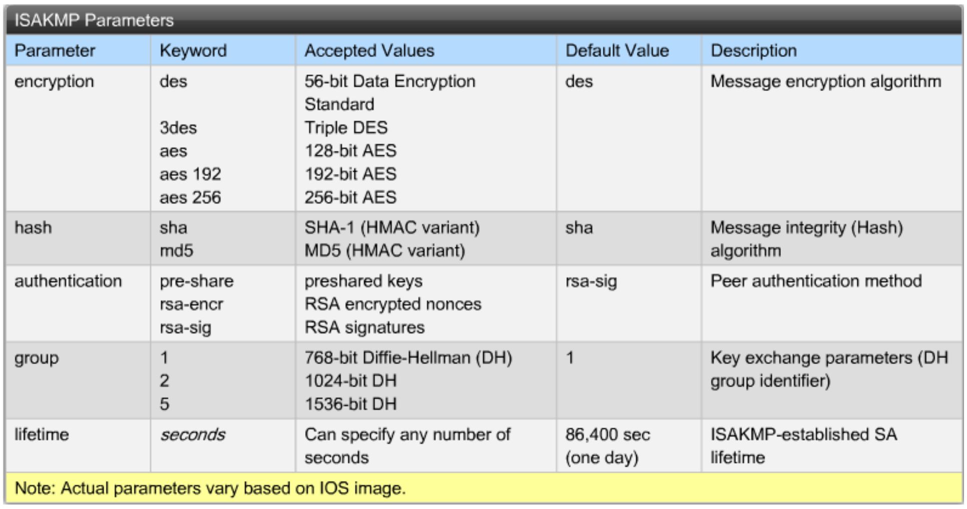
```
R0(config)#show ip interface brief
R0(config)#show ip route
```

7.3 Configuring Virtual Private Network in Three Ways

7.3.1 Internet Key Exchange procedure

Before starting the configuration, I first shortly explain the Internet Key Exchange (IKE) procedure because after knowing it, it will be easier to understand the configuration steps of creating VPN tunnels. There are two main phases during the negotiation procedure.

The first phase is to negotiate ISAKMP (Internet Security Association and Key Management Protocol) policy, including encryption method which ensures confidentiality, hash method which ensures integrity, authentication method, Diffie-Hellman method which ensure secure key exchange method and lifetime. A router can have several policies, if more than one policy can be successfully negotiated, smaller policy will finally be invoked because smaller priority numbers have higher priority. Figure 7. 2 shows the parameters that can be chosen by network administrator.



ISAKMP Parameters

Parameter	Keyword	Accepted Values	Default Value	Description
encryption	des 3des aes aes 192 aes 256	56-bit Data Encryption Standard Triple DES 128-bit AES 192-bit AES 256-bit AES	des	Message encryption algorithm
hash	sha md5	SHA-1 (HMAC variant) MD5 (HMAC variant)	sha	Message integrity (Hash) algorithm
authentication	pre-share rsa-encr rsa-sig	preshared keys RSA encrypted nonces RSA signatures	rsa-sig	Peer authentication method
group	1 2 5	768-bit Diffie-Hellman (DH) 1024-bit DH 1536-bit DH	1	Key exchange parameters (DH group identifier)
lifetime	*seconds*	Can specify any number of seconds	86,400 sec (one day)	ISAKMP-established SA lifetime

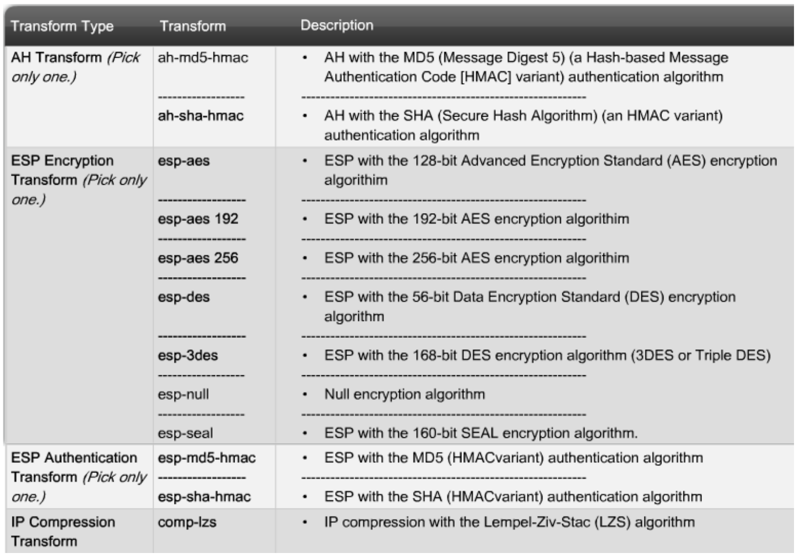
Note: Actual parameters vary based on IOS image.

Figure 7. 2. ISAKMP Parameters [27]

Here are the default values of ISAKMP parameters in my experiment:

```
R1(config)#do show crypto isakmp policy

Global IKE policy
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                86400 seconds, no volume limit
```

The second phase is to negotiate the IPsec transform-set. Transform sets consist of a combination of an AH transform, an ESP transform, and the IPsec mode (either tunnel or transport mode). In a transform, the administrator can specify the AH protocol, the ESP protocol, or both. Each transform represents an IPsec security protocol (AH or ESP) plus the associated algorithm. [27] If an ESP protocol is specified in a transform, an ESP encryption transform is compulsory, and an authentication transform is optional. But you are not allowed to only choose ESP authentication method. All together, you can choose up to four transforms. And the default IPsec mode is tunnel mode. In addition, multiple transform sets can be configured. Not like IKE policy, the transform set is created by using a name instead of a number. If you are a little bit confused, please look at Figure 7. 3, you may be clearer about the procedure.



Transform Type	Transform	Description
AH Transform *(Pick only one.)*	ah-md5-hmac	• AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm
	ah-sha-hmac	• AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm
ESP Encryption Transform *(Pick only one.)*	esp-aes	• ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithim
	esp-aes 192	• ESP with the 192-bit AES encryption algorithim
	esp-aes 256	• ESP with the 256-bit AES encryption algorithim
	esp-des	• ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm
	esp-3des	• ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
	esp-null	• Null encryption algorithm
	esp-seal	• ESP with the 160-bit SEAL encryption algorithm.
ESP Authentication Transform *(Pick only one.)*	esp-md5-hmac	• ESP with the MD5 (HMACvariant) authentication algorithm
	esp-sha-hmac	• ESP with the SHA (HMACvariant) authentication algorithm
IP Compression Transform	comp-lzs	• IP compression with the Lempel-Ziv-Stac (LZS) algorithm

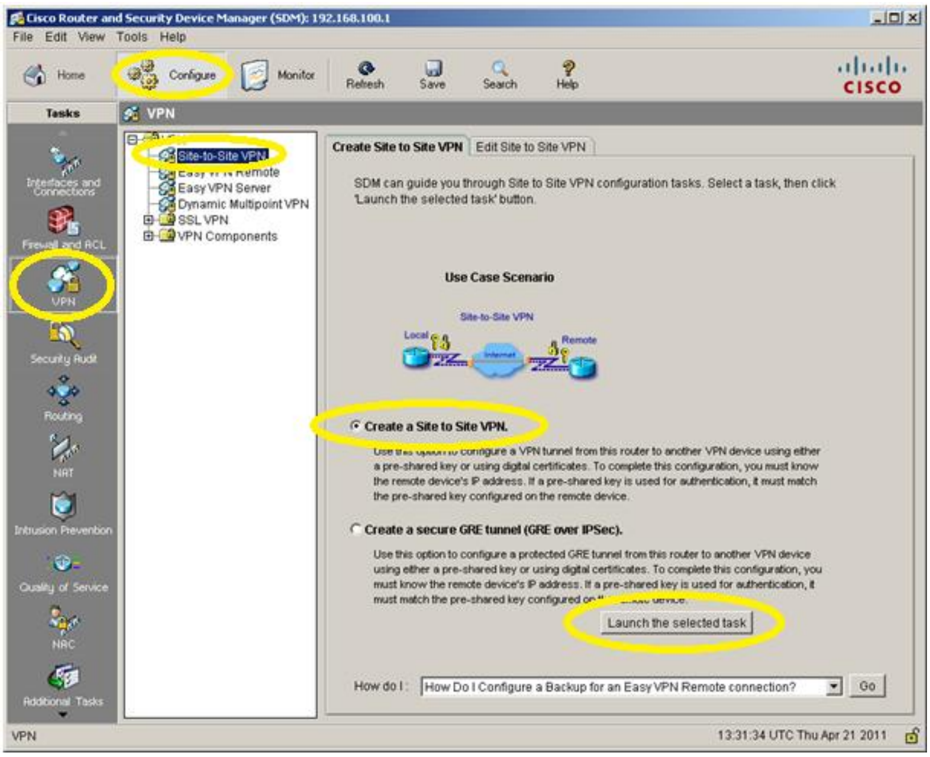
Figure 7. 3. Allowed Transform combination [27]

Here is an example output of debug crypto isakmp command during IKE negotiation.

```
R1# debug crypto isakmp
<output omitted>
*May 16 14:36:36.111: ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy
*May 16 14:36:36.115: ISAKMP:          encryption 3DES-CBC
*May 16 14:36:36.115: ISAKMP:          hash SHA
*May 16 14:36:36.115: ISAKMP:          default group 2
*May 16 14:36:36.115: ISAKMP:          auth pre-share
*May 16 14:36:36.115: ISAKMP:          life type in seconds
*May 16 14:36:36.115: ISAKMP:          life duration (VPI) of    0x0 0x1 0x51 0x80
*May 16 14:36:36.115: ISAKMP:(0):    atts are acceptable.
<output omitted>
*May 16 14:36:36.279: ISAKMP:(4001):Checking IPSec proposal 1
*May 16 14:36:36.279: ISAKMP:           transform 1, ESP_3DES
*May 16 14:36:36.279: ISAKMP:           attributes in transform:
*May 16 14:36:36.279: ISAKMP:          encaps is 1 (Tunnel)
*May 16 14:36:36.279: ISAKMP:          SA life type in seconds
*May 16 14:36:36.279: ISAKMP:          SA life duration (basic) of 3600
*May 16 14:36:36.279: ISAKMP:          SA life type in kilobytes
*May 16 14:36:36.279: ISAKMP:          SA life duration (VPI) of    0x0 0x46 0x50 0x0
*May 16 14:36:36.279: ISAKMP:          authenticator is HMAC-SHA
*May 16 14:36:36.279: ISAKMP:(4001):atts are acceptable.
<output omitted>
```

7.3.2 Quick Setup by SDM

Choose from the menu, *Configure > VPN > Site-to-Site VPN > Create a Site to Site VPN*, and then click '*Launch the selected task*' button. If no response from SDM, please check the Java version and make sure to enable Java 1.5. I have mentioned it before. Figure 7. 4 shows the steps of creating site to site VPN.



SDM can guide you through Site to Site VPN configuration tasks. Select a task, then click 'Launch the selected task' button.

● Create a Site to Site VPN.

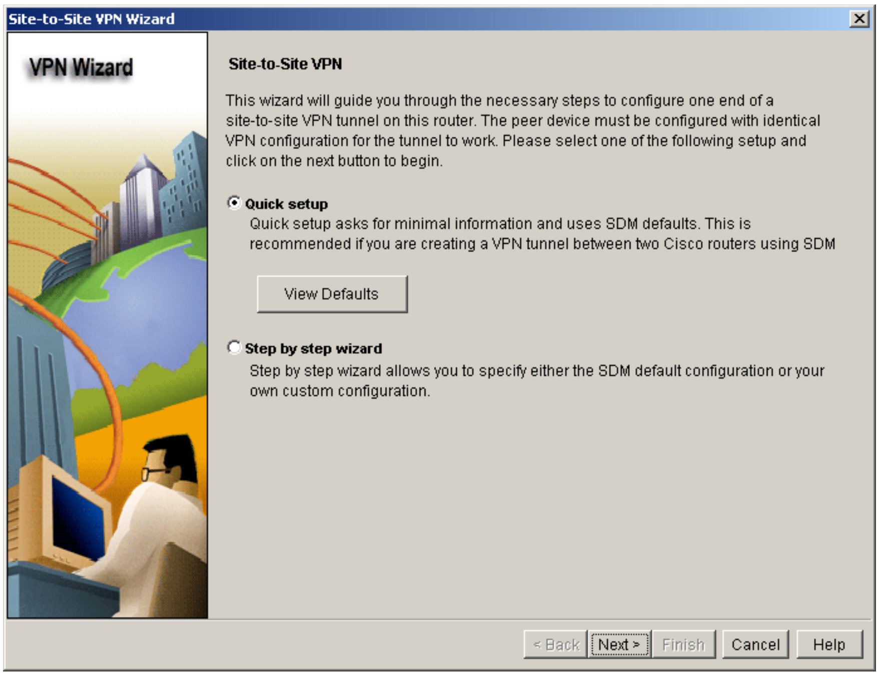
Use this option to configure a VPN tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

○ Create a secure GRE tunnel (GRE over IPSec).

Use this option to configure a protected GRE tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

Figure 7. 4. Create Site to Site VPN

There are two ways in here. I choose the first one, Quick setup, the easiest and the fastest way. I will later explain the other way, Step by step wizard and also the most challenging but the most advanced way, Command Line Interface. Figure 7. 5 displays the two GUI configuration alternatives. Figure 7. 6 shows the default IKE policy and transform set of VPN by SDM.



Site-to-Site VPN

This wizard will guide you through the necessary steps to configure one end of a site-to-site VPN tunnel on this router. The peer device must be configured with identical VPN configuration for the tunnel to work. Please select one of the following setup and click on the next button to begin.

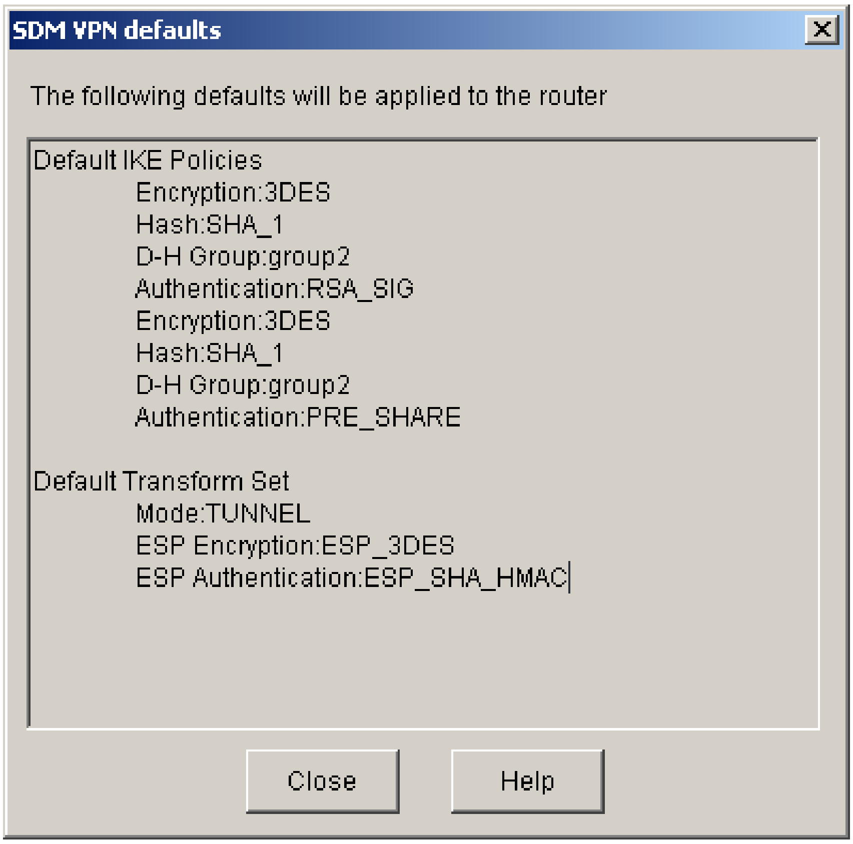
● Quick setup

Quick setup asks for minimal information and uses SDM defaults. This is recommended if you are creating a VPN tunnel between two Cisco routers using SDM

○ Step by step wizard

Step by step wizard allows you to specify either the SDM default configuration or your own custom configuration.

Figure 7. 5. Two GUI Configurating ways



The following defaults will be applied to the router

```
Default IKE Policies
        Encryption:3DES
        Hash:SHA_1
        D-H Group:group2
        Authentication:RSA_SIG
        Encryption:3DES
        Hash:SHA_1
        D-H Group:group2
        Authentication:PRE_SHARE

Default Transform Set
        Mode:TUNNEL
        ESP Encryption:ESP_3DES
        ESP Authentication:ESP_SHA_HMAC
```

Figure 7. 6. Defaults Setting of VPN by SDM

Then, go to the main configuration interface.

STEP 1: Select the local interface for this VPN connection Serial 0/0/0, which is the end point of tunnel.

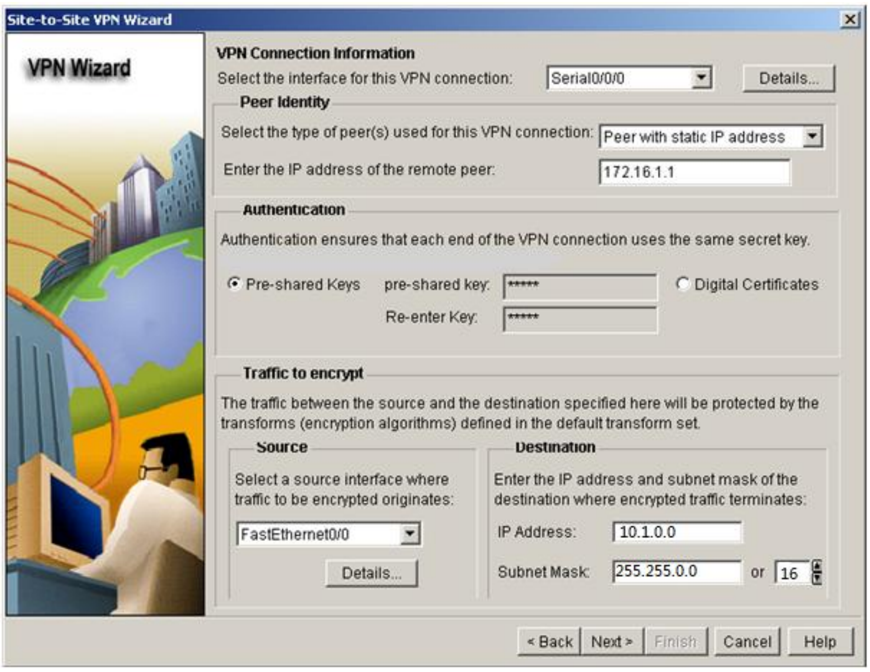
STEP 2: Enter the IP address of remote peer 172.16.1.1 if using static IP address. Besides, dynamic IP address can also be chosen.

STEP 3: Select the authentication method, if pre-shared key is chosen, you have to enter the key, here I type cisco. If choosing, Digital Certificates, it is no need to type the key.

STEP 4: Select the source originating interface FastEthernet 0/0 where the traffic to be encrypted.

STEP 5: Enter the IP address and subnet mask of the destination 10.1.0.0 /16 where encrypted traffic terminates.

Figure 7. 7 shows the real configuration interface.



VPN Connection Information

Select the interface for this VPN connection: Serial0/0/0

Peer Identity

Select the type of peer(s) used for this VPN connection: Peer with static IP address

Enter the IP address of the remote peer: 172.16.1.1

Authentication

Authentication ensures that each end of the VPN connection uses the same secret key.

● Pre-shared Keys pre-shared key: ***** ○ Digital Certificates

Re-enter Key: *****

Traffic to encrypt

The traffic between the source and the destination specified here will be protected by the transforms (encryption algorithms) defined in the default transform set.

Source

Select a source interface where traffic to be encrypted originates: FastEthernet0/0

Destination

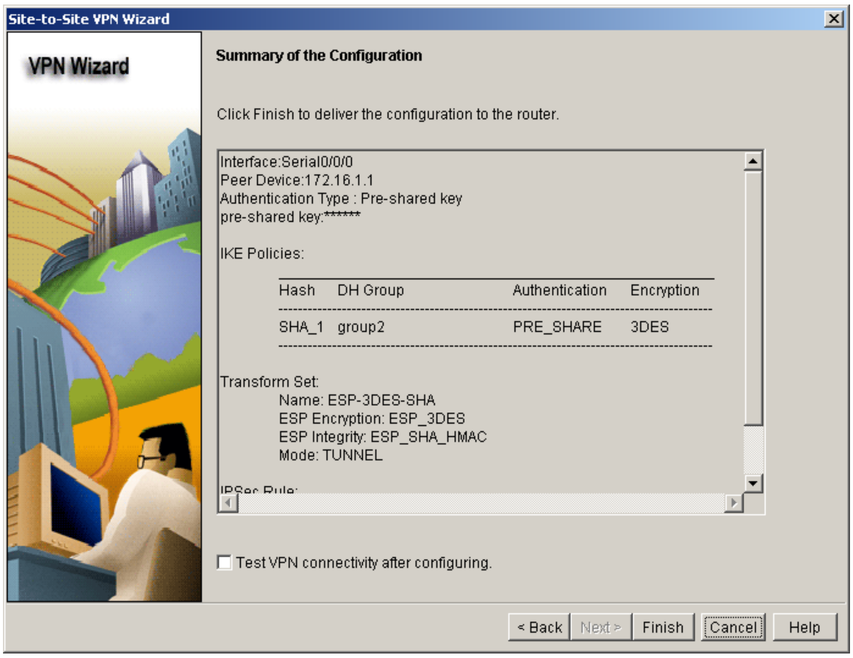
Enter the IP address and subnet mask of the destination where encrypted traffic terminates:

IP Address: 10.1.0.0

Subnet Mask: 255.255.0.0 or 16

Figure 7. 7. VPN Quick Setup

After clicking *Next>* button, the summary of the configuration is displayed, and all the algorithms are configured by default. Please remember these default algorithms because later these will be configured on the remote peer by Command Line Interface. Figure 7. 8 shows the summary.



Summary of the Configuration

Click Finish to deliver the configuration to the router.

```
Interface:Serial0/0/0
Peer Device:172.16.1.1
Authentication Type : Pre-shared key
pre-shared key:******

IKE Policies:

          Hash     DH Group              Authentication    Encryption
          ---------------------------------------------------------------
          SHA_1    group2                PRE_SHARE         3DES
          ---------------------------------------------------------------

Transform Set:
          Name: ESP-3DES-SHA
          ESP Encryption: ESP_3DES
          ESP Integrity: ESP_SHA_HMAC
          Mode: TUNNEL

IPSec Rule:
```

□ Test VPN connectivity after configuring.

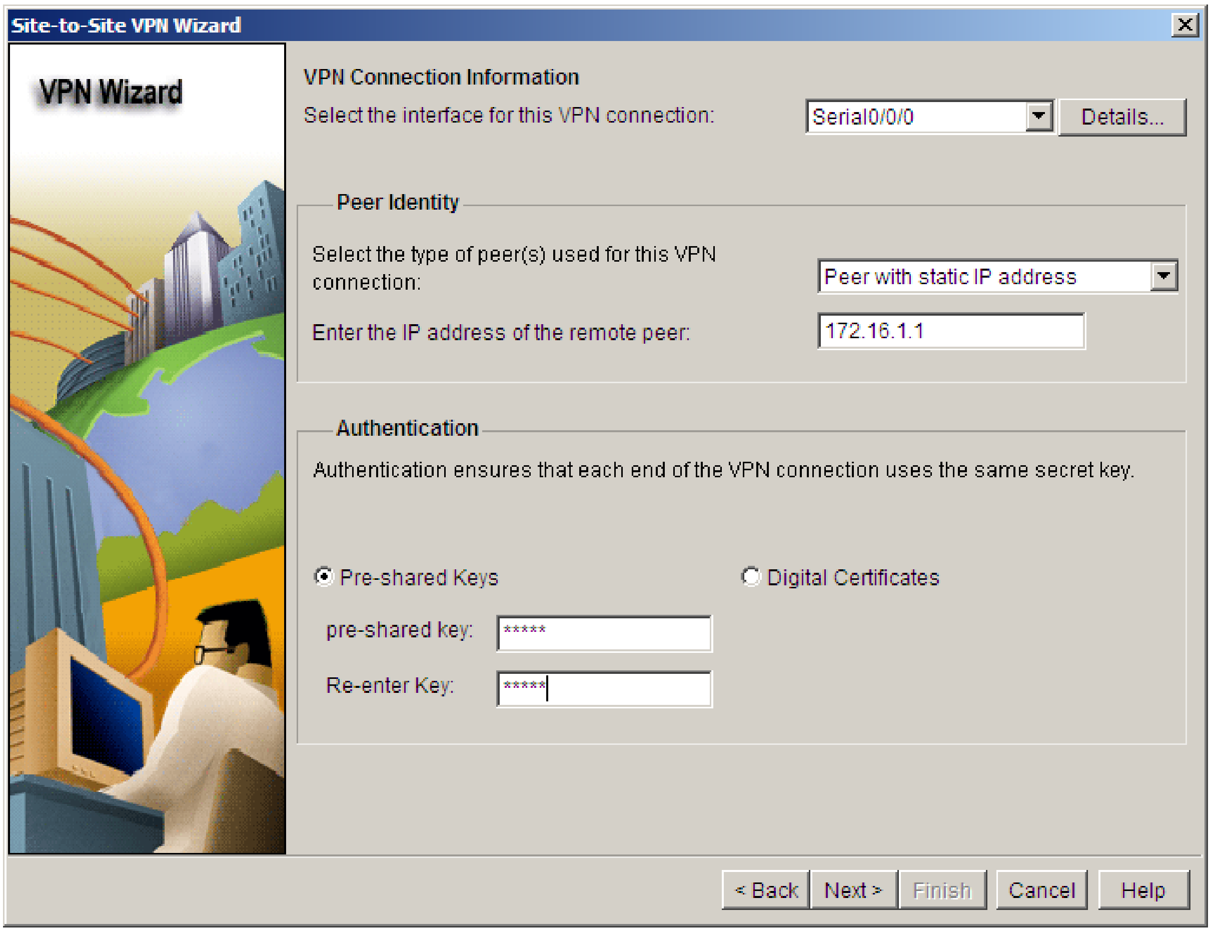
Figure 7. 8. VPN Quick Setup Summary

You may find it is really simple and understandable. But it is not really flexible, because you are not allowed to define IKE policy and Transform Set during the establish process. So, if you create several VPN tunnels on the same router by using the one step finished wizard, the tunnel parameters will be same. Let's look at another GUI configuration flow.

7.3.3 Step by Step Wizard

On the Coordinate Company Side, I specify the VPN parameters by the other SDM method, Step by Step. It can be divided into 4 steps.

STEP 1: Specify two peer to be negotiated. It is similar to the Quick Setup that I have mentioned in section 7.3.2. In authentication option block, I choose Pre-shared Key again and enter *cisco* as key. There is no relationship between the key in here and before when I enter the key in Quick Setup. Figure 7. 9 shows more details.



Site-to-Site VPN Wizard

VPN Wizard

VPN Connection Information

Select the interface for this VPN connection: Serial0/0/0

Peer Identity

Select the type of peer(s) used for this VPN connection: Peer with static IP address

Enter the IP address of the remote peer: 172.16.1.1

Authentication

Authentication ensures that each end of the VPN connection uses the same secret key.

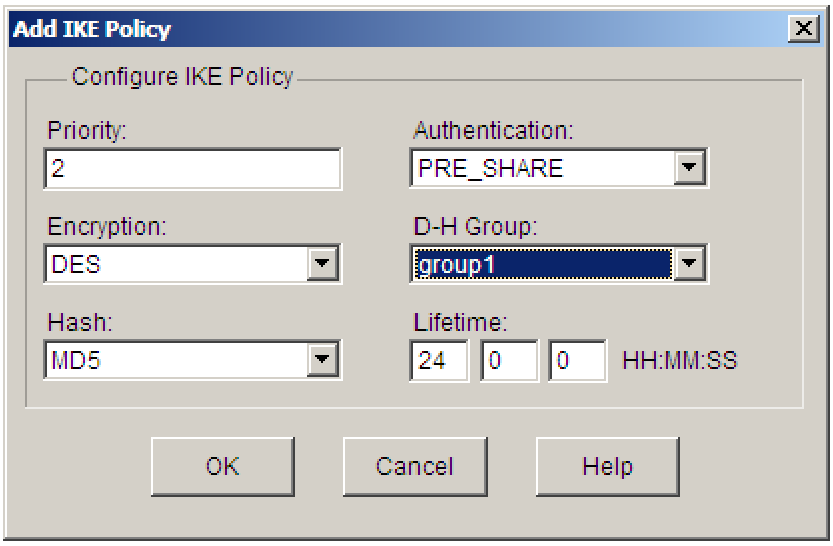
● Pre-shared Keys ○ Digital Certificates

pre-shared key: *****

Re-enter Key: *****

Figure 7. 9. Step-by-Step Wizard STEP 1

STEP 2: Select IKE policy. Unlike the configuration in Quick Setup, network administrator can specify IKE policy, including encryption algorithm, authentication algorithm, hash algorithm, key exchange method and policy lifetime. There is a default policy defined by SDM. Figure 7. 10 and Figure 7. 11 shows more details.



Add IKE Policy

Configure IKE Policy

Priority: 2

Authentication: PRE_SHARE

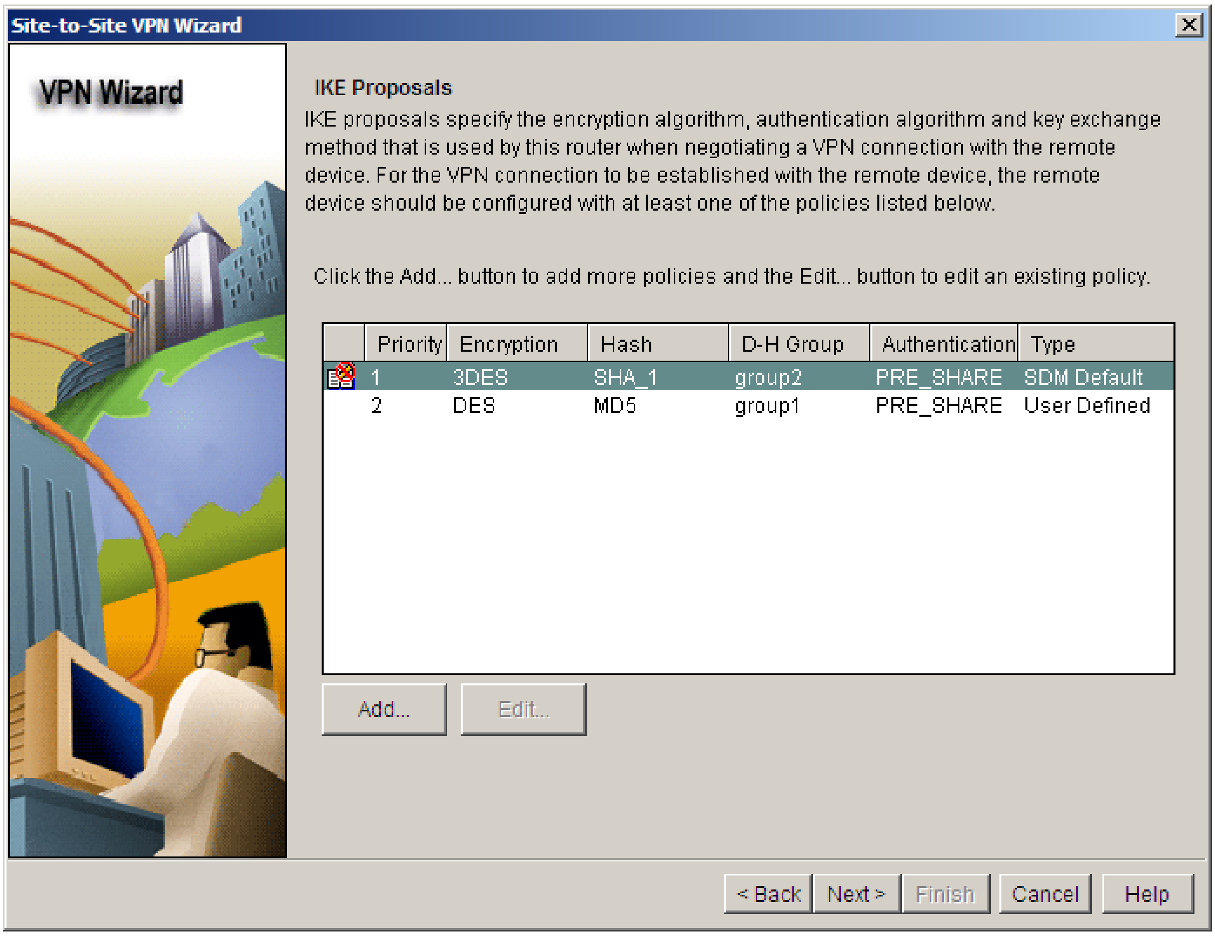
Encryption: DES

D-H Group: group1

Hash: MD5

Lifetime: 24 0 0 HH:MM:SS

Figure 7. 10. Step-by-Step Wizard STEP 2



Site-to-Site VPN Wizard

VPN Wizard

IKE Proposals

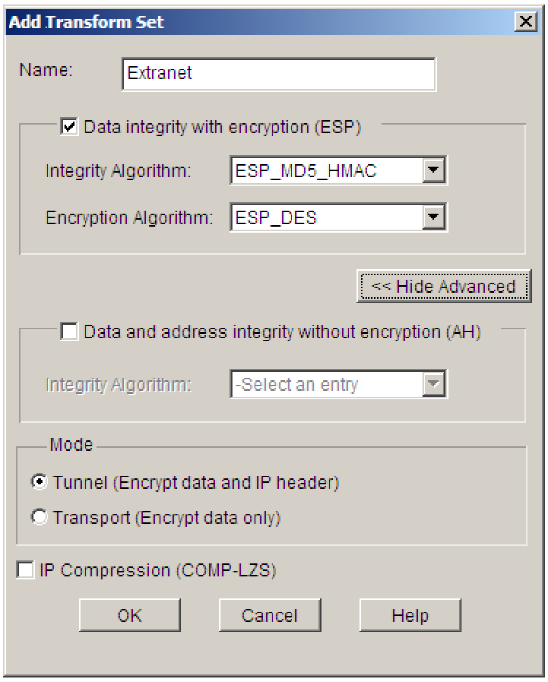
IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

	Priority	Encryption	Hash	D-H Group	Authentication	Type
	1	3DES	SHA_1	group2	PRE_SHARE	SDM Default
	2	DES	MD5	group1	PRE_SHARE	User Defined

Figure 7. 11. Step-by-Step Wizard STEP 2

STEP 3: Define Transform Set. In order to distinguish from the default transform set to the new EXTRANET transform set, ESP_MD5_HMAC and ESP_DES are chosen in here. More details are shown in Figure 7. 12 and Figure 7. 13.



Add Transform Set

Name: Extranet

☑ Data integrity with encryption (ESP)

Integrity Algorithm: ESP_MD5_HMAC

Encryption Algorithm: ESP_DES

☐ Data and address integrity without encryption (AH)

Integrity Algorithm: -Select an entry

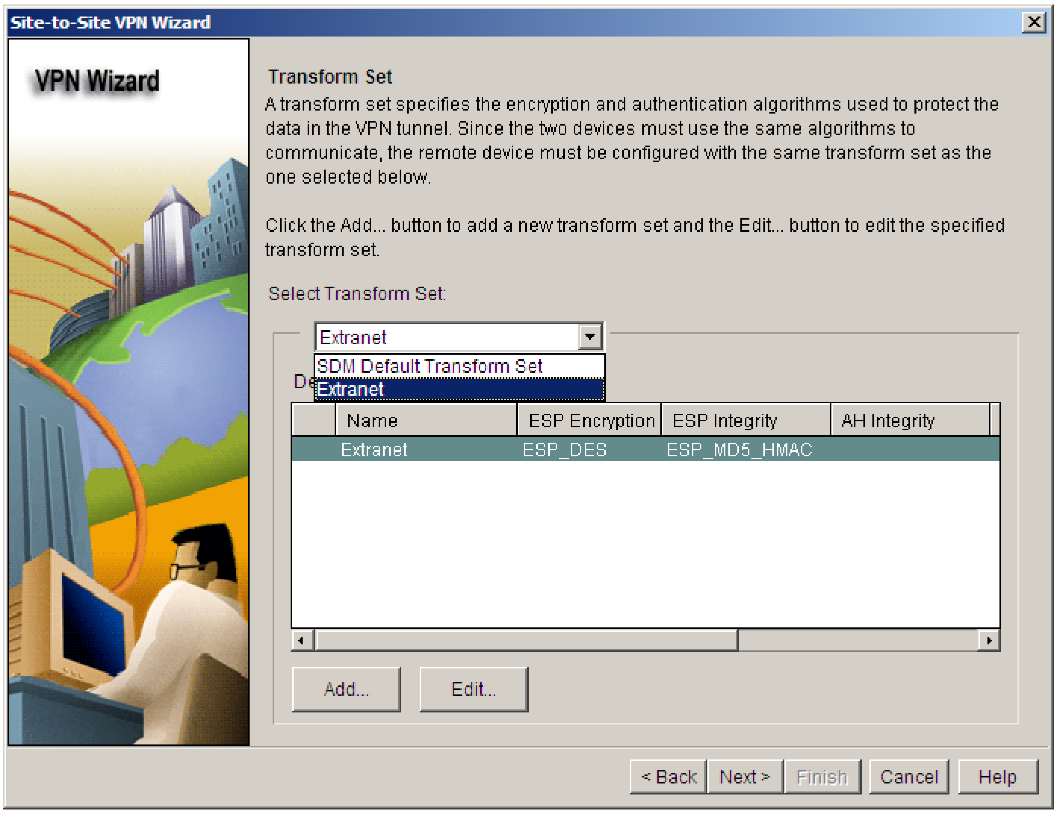
Mode

● Tunnel (Encrypt data and IP header)

○ Transport (Encrypt data only)

☐ IP Compression (COMP-LZS)

Figure 7. 12. Step-by-Step Wizard STEP 3



Site-to-Site VPN Wizard

VPN Wizard

Transform Set

A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel. Since the two devices must use the same algorithms to communicate, the remote device must be configured with the same transform set as the one selected below.

Click the Add... button to add a new transform set and the Edit... button to edit the specified transform set.

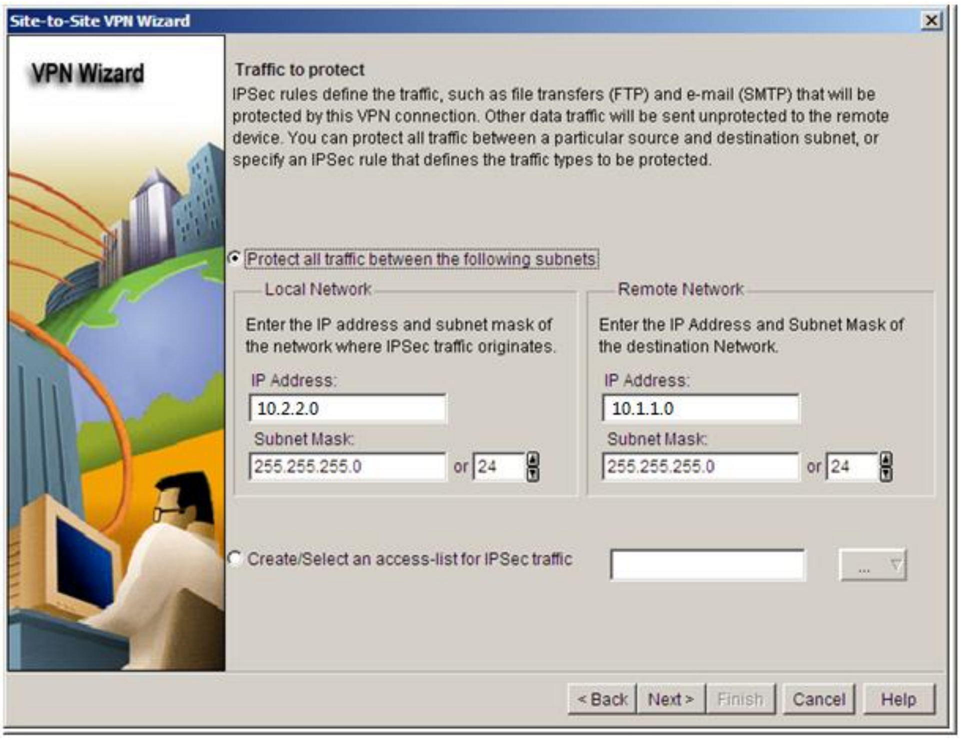
Select Transform Set: Extranet

SDM Default Transform Set
Extranet

Name	ESP Encryption	ESP Integrity	AH Integrity
Extranet	ESP_DES	ESP_MD5_HMAC	

Figure 7. 13. Step-by-Step Wizard STEP 3

STEP 4: Specify source and destination networks that to be protected. It is also similar to the Quick Setup that I have mentioned in section 7.3.2. Figure 7. 14 shows details.



Traffic to protect

IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will be protected by this VPN connection. Other data traffic will be sent unprotected to the remote device. You can protect all traffic between a particular source and destination subnet, or specify an IPSec rule that defines the traffic types to be protected.

● Protect all traffic between the following subnets

Local Network

Enter the IP address and subnet mask of the network where IPSec traffic originates.

IP Address: 10.2.2.0

Subnet Mask: 255.255.255.0 or 24

Remote Network

Enter the IP Address and Subnet Mask of the destination Network.

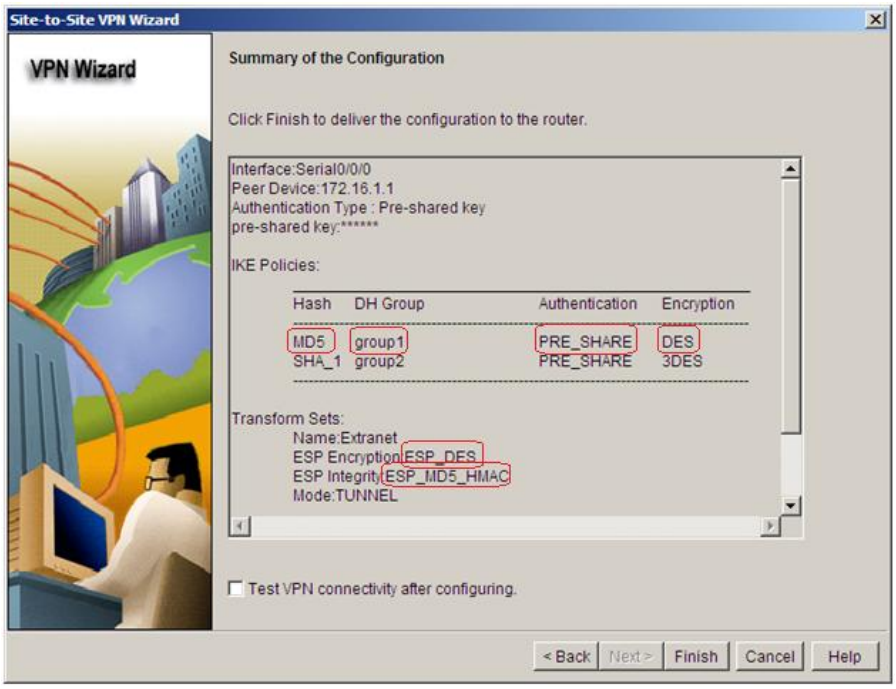
IP Address: 10.1.1.0

Subnet Mask: 255.255.255.0 or 24

○ Create/Select an access-list for IPSec traffic

Figure 7. 14. Step-by-Step Wizard STEP 4

Figure 7. 15 is the summary of configuration.



Summary of the Configuration

Click Finish to deliver the configuration to the router.

```
Interface:Serial0/0/0
Peer Device:172.16.1.1
Authentication Type : Pre-shared key
pre-shared key:******

IKE Policies:

          Hash    DH Group               Authentication    Encryption
          ---------------------------------------------------------
          MD5     group1                 PRE_SHARE         DES
          SHA_1   group2                 PRE_SHARE         3DES
          ---------------------------------------------------------

Transform Sets:
          Name:Extranet
          ESP Encryption:ESP_DES
          ESP Integrity:ESP_MD5_HMAC
          Mode:TUNNEL
```

□ Test VPN connectivity after configuring.

Figure 7. 15. Step-by-Step Wizard Summary

Until now, I have introduced two different GUI methods. The second method has higher flexibility because network administrator has ability to define IKE policies and Transform Sets, but it seems still has some limitation. In *Configure > VPN Site-to-Site VPN > Edit Site to Site VPN,* There are just two buttons, Add... and Delete. It seems that once IKE policies and transform sets are defined by users, they are not able to modify these parameters in here. Fortunately they can delete the tunnels, or create a new tunnel. If you choose the delete button, there are two options, you can choose either delete the map or cancel the relationship between the port and the map. Even if you delete the map, the transform set and IKE policy that you have created still exist in your NVRAM (running configuration). Here is part of the output of my show run command after deleting and creating new maps.

```
R1#show running-config
<output omitted>
!
crypto isakmp policy 1
        encr 3des
authentication pre-share
group 2
crypto isakmp key cisco address 172.16.1.1
!
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA1 esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA2 esp-3des esp-sha-hmac
!
<output omitted>
!
access-list 100 remark SDM_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.3.3.0 0.0.0.255 10.1.0.0 0.0.255.255
access-list 101 remark SDM_ACL Category=4
access-list 101 remark IPSec Rule
access-list 101 permit ip 10.3.3.0 0.0.0.255 10.1.0.0 0.0.255.255
access-list 102 remark SDM_ACL Category=4
```

```
access-list 102 remark IPSec Rule
access-list 102 permit ip 10.3.3.0 0.0.0.255 10.1.0.0 0.0.255.255
access-list 103 remark SDM_ACL Category=4
access-list 103 remark IPSec Rule
access-list 103 permit ip 10.3.3.0 0.0.0.255 10.1.0.0 0.0.255.255
!
<output omitted>
```

There is just one IKE policy and several transform sets and access control lists. I guess because the map, transform sets and access control lists are created separatedly. After deleting the map, the transform sets and access control lists will still exist in the running configuration

It seems not a big deal. Imagine the situation that plenty of IKE policies and transform sets are existed in routers running-configuration. When tunnel negotiation starts, the negotiation will operate several times until matching the parameters. It is a big deal for a huge company because it is not only waste of time but also transport flow during negotiating stage. In this case, it is similar to uninstall software from a computer. PC users usually complain that there are always some remaining folders existing in our hard disk after uninstall software. After long time accumulation, these may influence the performance of computer seriously. Same principle, it will for sure impact the performance of router when too many unnecessary IKE policies and transform sets exist in a router.

7.3.4 VPN Advanced Setting by SDM

VPN quick setup is the easiest and fastest way but least flexible. On one hand, it will guide you through the necessary steps to configure one end of a site-to-site VPN tunnel on the router. On the other hand, users are not allowed to specify IKE policy and transform set, because these parameters are specified by default. So, if the VPN tunnel is created between two Cisco routers, it is fine by using SDM, because the two sides are able to negotiate.

While, step by step setup allows you to specify either the SDM default configuration or your own custom configuration. Every parameter in IKE policy and transform set can be specified and changed by network administrator. But deleting the IKE policy and transform set seems a big problem.

Actually, I finally found how to change the parameters of VPN by not deleting and creating a new tunnel again. According the following path, you can find the answer of how to change the parameters of VPN in SDM. More details are shown on Figure 7. 16.

IKE policy

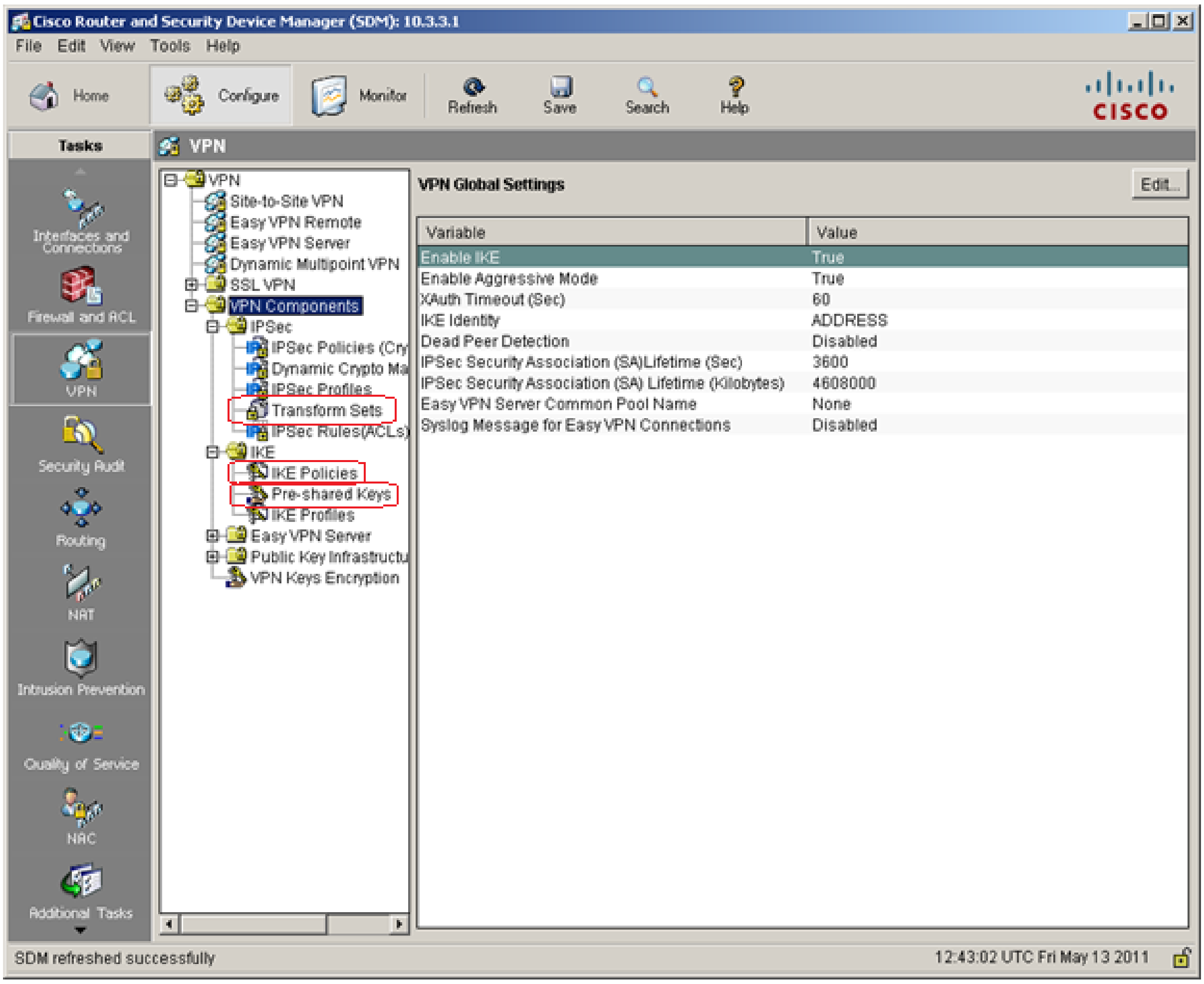
Configure > VPN > VPN > VPN Components > IKE > IKE Policies

Pre-Shared Key

Configure > VPN > VPN > VPN Components > IKE > Pre-shared Keys

Transform Sets

Configure > VPN > VPN > VPN Components > IPSec > Transform Sets



VPN Global Settings

Variable	Value
Enable IKE	True
Enable Aggressive Mode	True
XAuth Timeout (Sec)	60
IKE Identity	ADDRESS
Dead Peer Detection	Disabled
IPSec Security Association (SA)Lifetime (Sec)	3600
IPSec Security Association (SA) Lifetime (Kilobytes)	4608000
Easy VPN Server Common Pool Name	None
Syslog Message for Easy VPN Connections	Disabled

SDM refreshed successfully

12:43:02 UTC Fri May 13 2011

Figure 7. 16. Chang Tunnel Parameters

Then, let’s look at the most comprehensive and the most complicated method - Command Line.

7.3.5 Command Line Configuration

After familiar with SDM Step by Step Setup Wizard, it will be easy to understand Command Line steps. Creating VPN can be divided into 5 steps. Among these steps, creating IKE policies and transform sets are the most significant.

In my real lab work, I found a challenge that some routers do not support the *crypto* command, and finally got the reason according to the show version command. The answer is that the IOS have to contain cryptographic features. The difference between two routers is highlighted below.

```
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.4(15)T9, RELEASE
SOFTWARE (fc5)
<output omitted>
```

```
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version
12.4(15)T9, RELEASE SOFTWARE (fc5)
<output omitted>
This product contains cryptographic features
<output omitted>
```

Fisrt I define the matching parameters of Branch side. Here is the information configured on R3.

Interface:Serial0/0/0
Peer Device:172.16.1.1
Authentication Type : Pre-shared key
*pre-shared key:******

IKE Policies:

Hash	*DH Group*	*Authentication*	*Encryption*

```
SHA_1        group2                    PRE_SHARE3DES
--------------------------------------------------------------------------------------
```

Transform Set:

```
Name: ESP-3DES-SHA
ESP Encryption: ESP_3DES
ESP Integrity: ESP_SHA_HMAC
Mode: TUNNEL
```

IPSec Rule:

```
permit all ip traffic from 10.3.3.1 0.0.0.255 to 10.1.0.0 0.0.255.255
```

STEP 1: Create IKE policy

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#hash sha
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
```

The policy priority number is 1 which is the highest priority. I specified the following things in this step:

Integrity method:	HMAC-SHA-1
Encryption algorithm:	3DES
Authentication method:	pre-shared key,
Secure key exchange algorithm:	GH group 2
Lifetime:	1 day

Before STEP 2, I prefer to check the just created IKE policy, using the following command. Because always check what you have just done before may avoid big challenges.

```
R1(config)#do show crypto isakmp policy
```

```
Global IKE policy
Protection suite of priority 1
        encryption algorithm:    Three key triple DES
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #2 (768 bit)
        lifetime:                 86400 seconds, no volume limit
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:           Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:    #1 (768 bit)
        lifetime:                 86400 seconds, no volume limit
```

You can find that in here there is a default policy. If part of the parameters is same to the default policy, these parameters can be ignored. So the configuration can be simplified to these.

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encryption 3des
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 2
```

Besides, administrator can use 'default' command in *config-isakmp* mode to change the default setting.

```
R1(config-isakmp)#default ?
        authentication   Set authentication method for protection suite
        encryption       Set encryption algorithm for protection suite
        group            Set the Diffie-Hellman group
        hash             Set hash algorithm for protection suite
        lifetime         Set lifetime for ISAKMP security association
```

STEP 1.5: Configure a pre-shared key of peer address

```
R1(config)# crypto isakmp key 6 cisco address 172.16.3.1
```

In step 1, the pre-shared key is chosen to be an authentication method, so I should define the pre-shared key of the peer side. If using RSA, there is no need to do this step. The '6' represents the key is encrypted, '0' is alternative meaning unencrypted.

STEP 2: Define an transform-set

```
R1(config)#crypto ipsec transform-set BRANCH esp-sha-hmac esp-3des
R1(cfg-crypto-trans)#mode tunnel
```

The name of this transform-set is VPN, specifying ESP header, authentication method SHA and encapsulation method 3DES. Then define it in tunnel mode. Tunnel mode is defined by default, so it can be omitted.

Again, before next step, it is better to check this transform-set.

```
R1(cfg-crypto-trans)#do show crypto ipsec transform-set
Transform set BRANCH: { esp-3des esp-sha-hmac    }
      will negotiate = { Tunnel,    },
```

STEP 3: Create access control list, specifying source and destination networks to be protected

```
R1(config)# access-list 101 permit ip 10.1.0.0 0.0.255.255 10.3.3.0 0.0.0.255
```

Remember that networks not specified in access control list communicate with current side in plaintext. Follow the logic, now it is time to check the access control list.

```
R1(config)#do show access-list
Extended IP access list 101
      10 permit ip 10.1.0.0 0.0.255.255 10.3.3.0 0.0.0.255
```

STEP 4: Create tunnel map

```
R1(config)#crypto map VPN 10 ipsec-isakmp
R1(config-crypto-map)#set peer 172.16.3.1
R1(config-crypto-map)#set transform-set BRANCH
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#set security-association lifetime seconds 86400
```

There are at least four things to be specified when creating the tunnel map, the remote peer, the access control list, the transform-set and the SA lifetime. And the key management method is optional, if you want you can choose it again when creating map. Additionally, it is better to set a backup when original peer suffering from some emergency. If the first peer cannot be contacted, the second peer is used. There is no limit to the number of redundant peers that can be configured. But the original peer should be configured adding 'default' command.

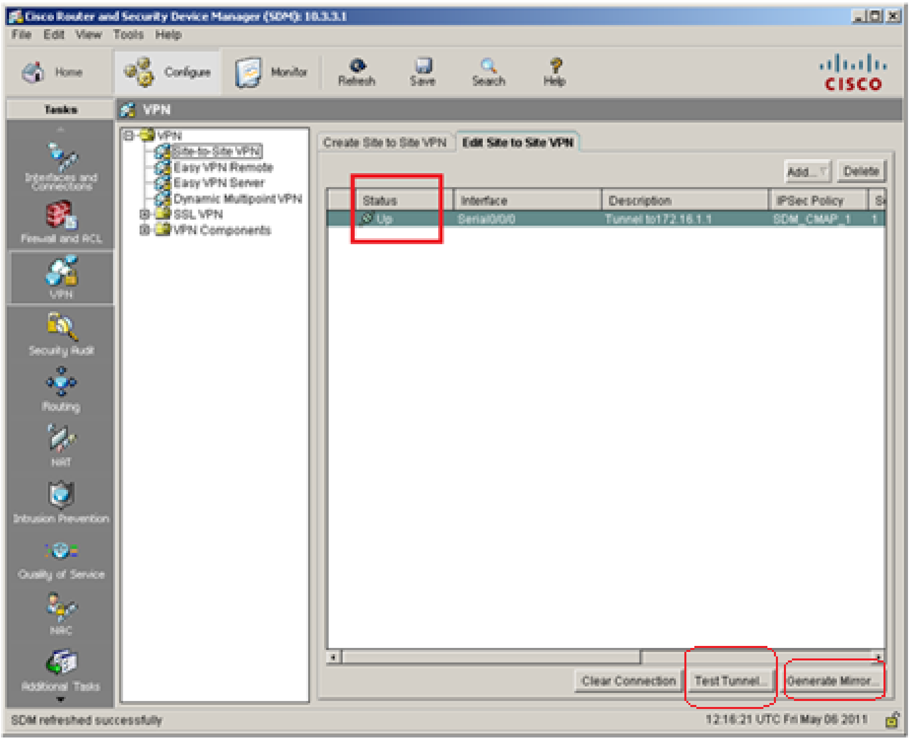
STEP 5: Put this map to a required port

```
R1(config-crypto-map)#interface FastEthernet0/1
R1(config-if)#crypto map VPN
```

Put the map to the port FastEthernet0/1, after that, check the map.

```
R1(config-if)#do show crypto map
Crypto Map "VPN" 1 ipsec-isakmp
      Peer = 172.16.3.1
      Extended IP access list 101
            access-list 101 permit ip 10.1.0.0 0.0.255.255 10.3.3.0 0.0.0.255
      Current peer: 172.16.3.1
      Security association lifetime: 4608000 kilobytes/86400 seconds
      PFS (Y/N): N
      Transform sets={
                  BRANCH,
      }
     Interfaces using crypto map VPN:
                  FastEthernet0/1
```

At this time, ping from 10.3.3.2 to 10.1.1.2 and 10.1.2.2 can be successful and transferred information is protected. VPN status changes to '*Up*', shown on Figure 7. 17.



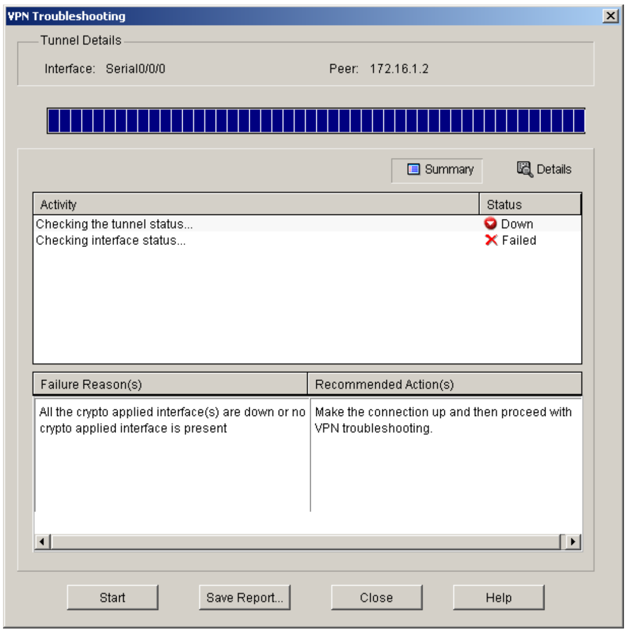
Status	Interface	Description	IPSec Policy	S
Up	Serial0/0/0	Tunnel to172.16.1.1	SDM_CMAP_1	1

SDM refreshed successfully

12:16:21 UTC Fri May 06 2011

Figure 7. 17. VPN Status

If the status is still down, SDM provides a test function to help you find failure reason and also give you some recommended actions to solve the problem, shown on Figure 7. 18.



Interface: Serial0/0/0

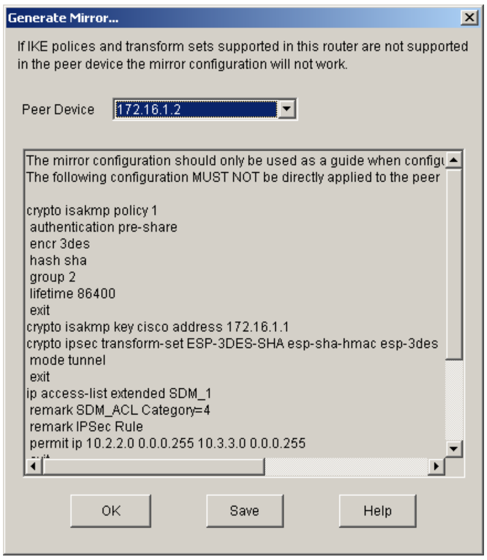
Peer: 172.16.1.2

Activity	Status
Checking the tunnel status...	Down
Checking interface status...	✕ Failed

Failure Reason(s)	Recommended Action(s)
All the crypto applied interface(s) are down or no crypto applied interface is present	Make the connection up and then proceed with VPN troubleshooting.

Figure 7. 18. VPN Troubleshooting

SDM also provides a function called generate mirror. The window shows you the IPSec policy used for the VPN tunnel to the selected peer, and allows you to save the policy in a text file that you can use when configuring the VPN connection on the peer device, shown on Figure 7. 19.



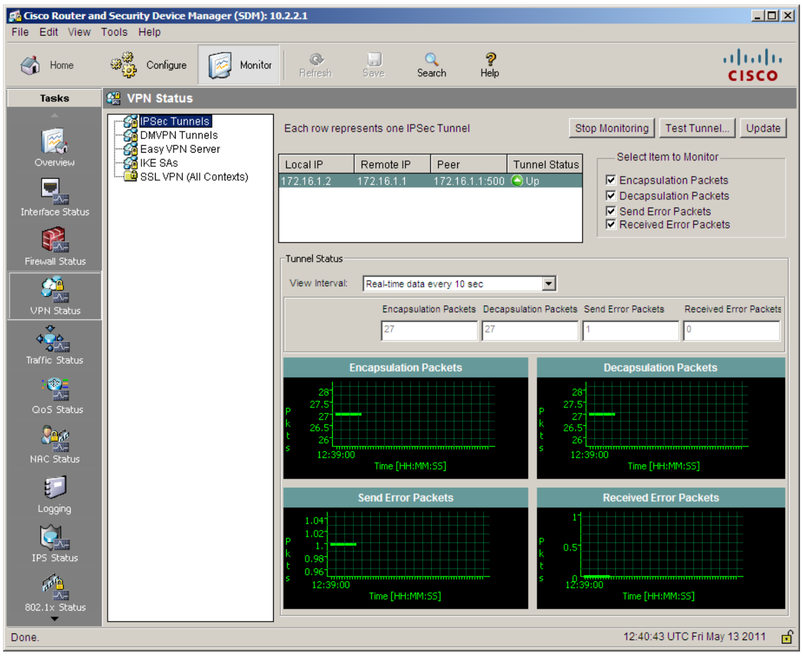
If IKE polices and transform sets supported in this router are not supported in the peer device the mirror configuration will not work.

Peer Device: 172.16.1.2

```
The mirror configuration should only be used as a guide when configu
The following configuration MUST NOT be directly applied to the peer

crypto isakmp policy 1
 authentication pre-share
 encr 3des
 hash sha
 group 2
 lifetime 86400
 exit
crypto isakmp key cisco address 172.16.1.1
crypto ipsec transform-set ESP-3DES-SHA esp-sha-hmac esp-3des
 mode tunnel
 exit
ip access-list extended SDM_1
 remark SDM_ACL Category=4
 remark IPSec Rule
 permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
```

Figure 7. 19. Generate Mirror

Besides, when tunnel status changes to up, administrators can monitor the tunnel state. Click *Monitor > VPN Status > IPSec Tunnels*, you can find four charts displaying the transform status of encapsulation packets, decapsulation packets, send error packets and received error packets. Figure 7. 20 shows details.



Each row represents one IPSec Tunnel

Local IP	Remote IP	Peer	Tunnel Status
172.16.1.2	172.16.1.1	172.16.1.1:500	Up

Select Item to Monitor
- ☑ Encapsulation Packets
- ☑ Decapsulation Packets
- ☑ Send Error Packets
- ☑ Received Error Packets

Tunnel Status

View Interval: Real-time data every 10 sec

Encapsulation Packets	Decapsulation Packets	Send Error Packets	Received Error Packets
27	27	1	0

Done. 12:40:43 UTC Fri May 13 2011

Figure 7. 20. VPN Monitor

Then, define the parameters matching the Coordinate Company by Command Line according to the 5 steps configuration. Here are the parameters configured on R2 by SDM.

Interface:Serial0/0/0
Peer Device:172.16.1.1
Authentication Type : Pre-shared key
*pre-shared key:*******

IKE Policies:

Hash	*DH Group*	*Authentication*	*Encryption*
MD5	*group1*	*PRE_SHAREDES*	
SHA_1	*group2*	*PRE_SHARE3DES*	

Transform Sets:

Name:Extranet
ESP Encryption:ESP_DES
ESP Integrity:ESP_MD5_HMAC
Mode:TUNNEL

IPSec Rule:

permit all ip traffic from 10.2.2.0 0.0.0.255 to 10.1.1.0 0.0.0.255

R1 configuration by Command Line:

STEP 1:

```
R1(config)#crypto isakmp policy 2
R1(config-isakmp)#group 1
R1(config-isakmp)#hash md5
R1(config-isakmp)#encryption des
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#lifetime 86400
```

```
R1(config-isakmp)#exit
```

STEP 1.5:

```
R1(config)# crypto isakmp key 6 cisco address 172.16.2.1
```

SHOW IKE POLICY

```
R1(config)#do show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:    Three key triple DES
        hash algorithm:            Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:     #2 (1024 bit)
        lifetime:                  86400 seconds, no volume limit
Protection suite of priority 2
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:            Message Digest 5
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:     #1 (768 bit)
        lifetime:                  86400 seconds, no volume limit
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys).
        hash algorithm:            Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:     #1 (768 bit)
        lifetime:                  86400 seconds, no volume limit
```

STEP 2:

```
R1(config)#crypto ipsec transform-set EXTRANET esp-des esp-md5-hmac
R1(cfg-crypto-trans)#mode tunnel
R1(cfg-crypto-trans)#exit
```

SHOW TRANSFORM SET:

```
R1(cfg-crypto-trans)#do show crypto ipsec transform-set
```

```
Transform set BRANCH: { esp-3des esp-sha-hmac    }
        will negotiate = { Tunnel,    },
Transform set EXTRANET: { esp-des esp-md5-hmac    }
        will negotiate = { Tunnel,    },
```

STEP 3:

```
R1(config)#access-list 102 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
```

STEP 4:

```
R1(config)#crypto map VPN 20 ipsec-isakmp
R1(config-crypto-map)#set peer 172.16.2.1
R1(config-crypto-map)#set transform-set EXTRANET
R1(config-crypto-map)#match address 102
```

SHOW MAP:

```
R1#show crypto map

Crypto Map "VPN" 10 ipsec-isakmp
          Peer = 172.16.3.1
          Extended IP access list 101
                   access-list 101 permit ip 10.1.0.0 0.0.255.255 10.3.3.0 0.0.0.255
          Current peer: 172.16.3.1
          Security association lifetime: 4608000 kilobytes/86400 seconds
          PFS (Y/N): N
          Transform sets={
                            BRANCH,
          }

Crypto Map "VPN" 20 ipsec-isakmp
          Peer = 172.16.2.1
          Extended IP access list 102
                   access-list 102 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
          Current peer: 172.16.2.1
          Security association lifetime: 4608000 kilobytes/3600 seconds
```

PFS (Y/N): N

Transform sets={

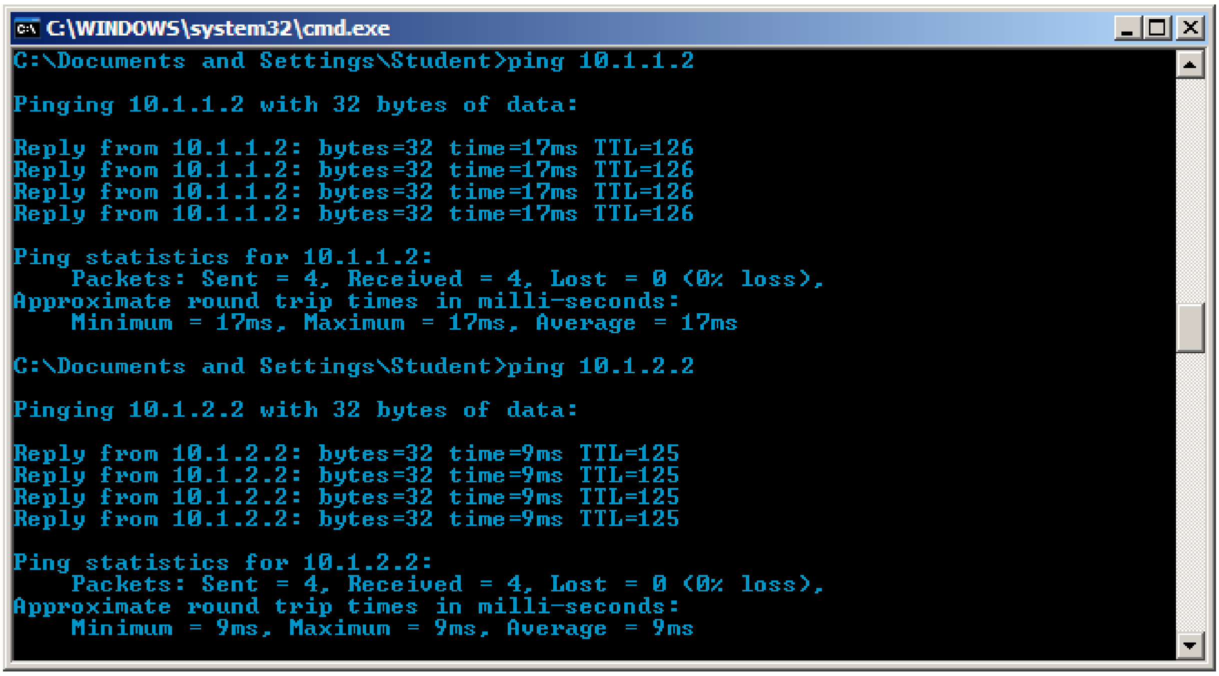
EXTRANET,

}

Interfaces using crypto map VPN:

FastEthernet0/1

The crypto map VPN has been mapped to Fast Ethernet 0/1, so step 5 can be omitted. Every VPN map is allowed to have plenty of priority number. In this case, I use two different numbers to distinguish two remote sides. Until now, the two tunnels are accomplished. However, PC2 can still ping Server, shown on Figure 7. 21.



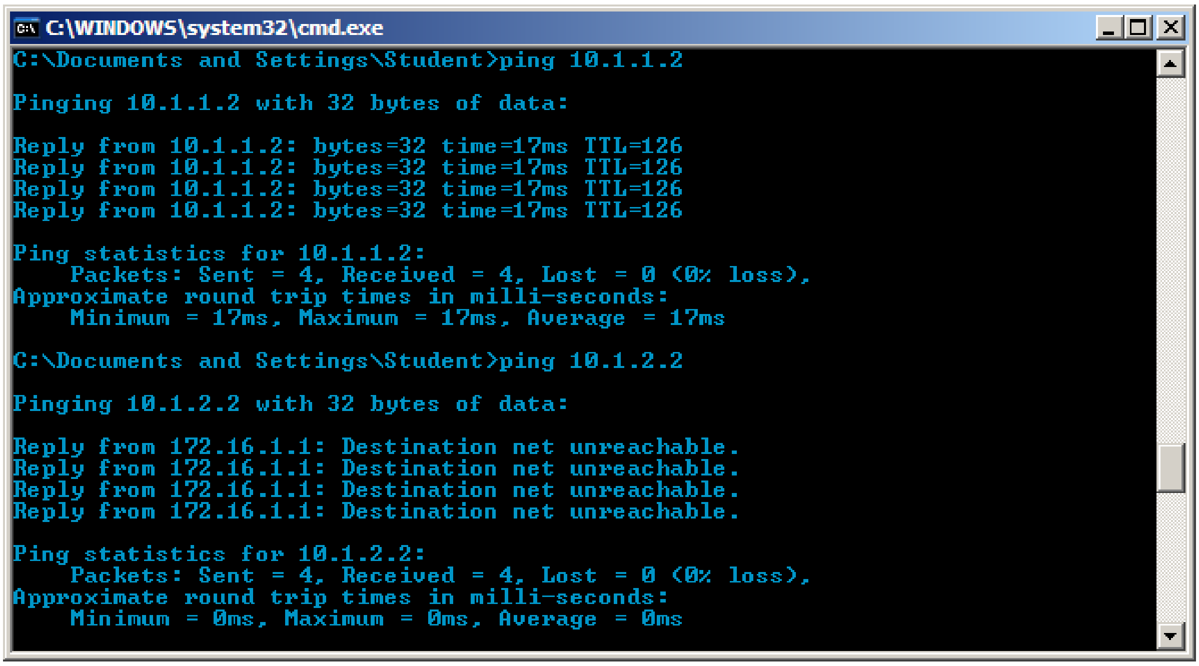
```
C:\Documents and Settings\Student>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=17ms TTL=126
Reply from 10.1.1.2: bytes=32 time=17ms TTL=126
Reply from 10.1.1.2: bytes=32 time=17ms TTL=126
Reply from 10.1.1.2: bytes=32 time=17ms TTL=126

Ping statistics for 10.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 17ms, Average = 17ms

C:\Documents and Settings\Student>ping 10.1.2.2

Pinging 10.1.2.2 with 32 bytes of data:

Reply from 10.1.2.2: bytes=32 time=9ms TTL=125
Reply from 10.1.2.2: bytes=32 time=9ms TTL=125
Reply from 10.1.2.2: bytes=32 time=9ms TTL=125
Reply from 10.1.2.2: bytes=32 time=9ms TTL=125

Ping statistics for 10.1.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 9ms, Average = 9ms
```

Figure 7. 21. Tunnel Test 1

Because I have not created access control list to deny traffics from PC2 to Server, PC2 can transfer information to server in plaintext. Here is the configuration.

```
R1(config)#access-list 103 deny ip 10.2.2.0 0.0.0.255 10.1.2.0 0.0.0.255
R1(config)#access-list 103 permit ip any any
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip access-group 103 in
```

After the above configuration, check it again, shown on Figure 7. 22



```
C:\Documents and Settings\Student>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=17ms TTL=126
Reply from 10.1.1.2: bytes=32 time=17ms TTL=126
Reply from 10.1.1.2: bytes=32 time=17ms TTL=126
Reply from 10.1.1.2: bytes=32 time=17ms TTL=126

Ping statistics for 10.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 17ms, Average = 17ms

C:\Documents and Settings\Student>ping 10.1.2.2

Pinging 10.1.2.2 with 32 bytes of data:

Reply from 172.16.1.1: Destination net unreachable.
Reply from 172.16.1.1: Destination net unreachable.
Reply from 172.16.1.1: Destination net unreachable.
Reply from 172.16.1.1: Destination net unreachable.

Ping statistics for 10.1.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 7. 22. Tunnel Test 2

The whole configuration of VPN is finished. I have introduced three ways from the easiest method to the most complicated method. I will analyze the benefits and drawbacks in Chapter 8. Before that, I first shortly describe some advanced setting of VPN by using SDM.

8. COMPARATION

From what I have been discussed above, you may find that both Command Line Interface and Graphical User Interface have their own benefits and drawbacks.

GUI is a kind of user friendly interface. Having a complete and elaborate user wizard, SDM explain the general idea of every step. So an experienced network administrator who has not operated with Cisco Devices in his former career may benefit from this remarkable feature, because he can solve the problem without learning the specific commands. Different network device supplier has its own Internetworking Operating System based on international standard. Although the configuration command can be different, the meaning is the same. Just like the command in Windows cmd.exe and Linux shell script can be different but have same function. The same situation exists for example between Cisco Corporation and HUAWEI. Besides, some advanced tasks accomplished by SDM have a great feature of saving time during the configuration. But it seems Cisco does not support SDM anymore. In the same time, Cisco release a brand new GUI configuration tools Cisco Configuration Assistant (CCA).

However, CLI seems suitable for professional technicians. People who want to use terminal emulator to solve problems must first learn these codes. Although it is not necessary to learn all the command by heart, at least you can find the answer with help of Google or question mark in the terminal emulator. After learning specific knowledge, the network technician can qualify this challenging job. In addition, it is highly flexible, so every specific detail can be specified and modified by administrator. However, it is for sure the most complicated configuration tool. Typically, every release of IOS may be a little bit different in configuration procedure. So, please not always believe the material from the internet or books.

For example, when I use Packet Tracer 5.3, which is an remarkable Cisco devices simulation tool, to familiar with the flow of configuring VPN by Command Line Interface, the pre-shared key can not be specified in encrypted. While in laboratory, our routers support the encrypted pre-shared key. I found that the IOS version of 2811 routers in Packet Tracer is 12.4(15) T1. But the IOS version of 2811 routers in laboratory is 12.4(15) T9. The part of output of *show version* and *crypto isakmp key* command in Packet Tracer 2811 router and laboratory 2811 router are highlighted below.

Packet Tracer:

```
R1#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M),
Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
<output omitted>

R1(config)#crypto isakmp key ?
        WORD    The UNENCRYPTED (cleartext) user password
```

Laboratory:

```
R1#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M),
Version 12.4(15)T9, RELEASE SOFTWARE (fc5)
<output omitted>

R1(config)#crypto isakmp key ?
        0   Specifies an UNENCRYPTED password will follow
        6   Specifies an ENCRYPTED password will follow
```

So, my recommendation is that at this time when configuring some basic tasks, SDM is not an advisable choice, because there should be some configurations by using Command Line in advance before enable a router to support SDM, but this basic configuration can be fulfilled in just a couple of commands. However, when it comes to some advanced tasks, combining SDM and CLI together can be a good choice. Because the configuration speed of SDM is considerably faster than Command Line. While Command Line supports complete function of modification and definition of VPN. But any way, I believe GUI has a promising field in the future and finally becomes a substitute of CLI, like Windows Operating System replaced MS-DOS.

9. CONCLUSION AND FUTURE STUDIES

Before doing this task, I had just heard the term VPN, knowing it is a private and secure network structure. However, I did not know how it works, let alone how to configure it. Besides, I just knew there are some graphical configuration tools, but I did not know how to use them. After finishing the study of VPN management, I get familiar to the operation mechanism of this Virtual Private Networks. In addition, I am now more familiar with Cisco Internetworking Operating System and get to know a really easy-to-use graphical interface configuration tool Cisco Router and Security Device Manager (SDM). In addition, three related future tasks come to my mind.

First of all, as you know SDM only supports router configuration. While another graphical interface configuration tool Cisco Network Assistant (CNA) supports switch configuration tasks. Even, Cisco Configuration Assistant (CCA) supports more comprehensive devices, including routers, switches and even wireless access points. What is more, there are a lot of graphical management tools. The features of those tools could be analyzed in more details in the future.

Moreover, another task that I am interested in is how Cisco devices operate VPN tunnel along with network devices from other company. Cisco is just one of various network equipment suppliers. It would be interesting to analyze the interoperability of VPN between different manufacturers.

Last but not least, how to create remote access VPN especially SSL VPN by using both CLI and GUI tools seems to be my future study. Cisco IOS SSL VPN is an emerging technology that provides remote-access connectivity from almost any Internet-enabled location using a web browser and its native SSL encryption. Originally developed by Netscape, SSL has been universally accepted on the Web. [27]

BIBLIOGRAPHY

Electronic Sources

[1] Cisco 2011. Cisco Router and Security Device Manager. Referred 2.4.2011.
URL: http://www.cisco.com/en/US/products/sw/secursw/ps5318/index.html

[2] Wikipedia 2011. Virtual Private Network. Updated 28.3.2011. Referred 2.4.2011.
URL: http://en.wikipedia.org/wiki/Virtual_private_network

[3] Wikipedia 2011. Leased line. Updated 28.3.2011. Referred 4.4.2011.
URL http://en.wikipedia.org/wiki/Leased_line

[4] Wikipedia 2011. Circuit Switching. Updated 28.3.2011. Referred 6.4.2011.
URL http://en.wikipedia.org/wiki/Circuit_switching

[5] Wikipedia 2011. DSL. Updated 2.4.2011. Referred 8.4.2011.
URL http://en.wikipedia.org/wiki/DSL

[6] Wikipedia 2011. Cable television. Updated 2.4.2011. Referred 8.4.2011.
URL http://en.wikipedia.org/wiki/Cable_television

[7] Wikipedia 2011. WiMAX. Updated 2.4.2011. Referred 8.4.2011.
URL http://en.wikipedia.org/wiki/WiMAX

[8] Wikipedia 2011.Satellite internet access . Updated 2.4.2011. Referred 8.4.2011.
URL http://en.wikipedia.org/wiki/Satellite_internet_access

[9] Wikipedia 2011. L2F. Updated 10.4.2011. Referred 12.4.2011.
URL http://en.wikipedia.org/wiki/L2F

[10] Wikipedia 2011. Point-to-Point Tunneling Protocol. Updated 10.4.2011. Referred 12.4.2011.
URL http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol

[11] Wikipedia 2011. Generic Routing Encapsulation. Updated 10.4.2011. Referred 12.4.2011.

URL http://en.wikipedia.org/wiki/Generic_Routing_Encapsulation

[12] Wikipedia 2011. IPsec. Updated 10.4.2011. Referred 12.4.2011.

URL http://en.wikipedia.org/wiki/IPsec

[13] Wikipedia 2011. Multiprotocol Label Switching. Updated 10.4.2011. Referred 12.4.2011.

URL http://en.wikipedia.org/wiki/Multiprotocol_Label_Switching

[14] Wikipedia 2011. Data Encryption Standard. Updated 10.4.2011. Referred 15.4.2011.

URL http://en.wikipedia.org/wiki/Data_Encryption_Standard

[15] Wikipedia 2011. Triple DES. Updated 10.4.2011. Referred 15.4.2011.

URL http://en.wikipedia.org/wiki/Triple_DES

[16] Wikipedia 2011. Advanced Encryption Standard. Updated 10.4.2011. Referred 15.4.2011.

URL http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[17] Wikipedia 2011. Terminal emulator. Updated 11.4.2011. Referred 17.4.2011.

URL http://en.wikipedia.org/wiki/Terminal_emulator

[18] Wikipedia 2011. Tera Term. Updated 11.4.2011. Referred 17.4.2011.

URL http://en.wikipedia.org/wiki/Tera_Term

[19] Wikipedia 2011. HyperTerminal. Updated 11.4.2011. Referred 17.4.2011.

URL http://en.wikipedia.org/wiki/HyperTerminal

[20] Wikipedia 2011. Minicom. Updated 11.4.2011. Referred 17.4.2011.

URL http://en.wikipedia.org/wiki/Minicom

[21] Wikipedia 2011. SecureCRT. Updated 11.4.2011. Referred 17.4.2011.

URL http://en.wikipedia.org/wiki/SecureCRT

[22] Cisco 2011. Downloading and Installing Cisco Router and Security Device Manager. Referred 18.4.2011.
URL:http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_installation_guide09186a00803e4727.html#wp70999

[23] Cisco 2011. SDM 2.5 Release Note. Referred 18.4.2011.
URL:http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr25.html

[24] Wikipedia 2011. Internet. Updated 11.4.2011. Referred 18.4.2011.
URL http://en.wikipedia.org/wiki/Internet

Books

[25] Ruixi Yuan and W. Timothy Strayer 2003. Virtual Private Networks: Technologies and Solutions. Beijing. China Electric Power Press. 32,55-58.

[26] CCNA Exploration Access the WAN 4.0. Cisco Network Academy. Available in online books. Require user account. Updated 20.1.2009. Referred 11.4.2011.
URL: http://www.cisco.com/web/learning/netacad/index.html
Page 1.3.1.1, 1.3.2.1, 1.3.5.4, 6.2.1.1, 6.2.3.1, 6.3.1.2.

[27]. CCNA Security 1.0. Cisco Network Academy. Available in online books. Require user account. Updated 21.7.2010. Referred 15.5.2011.
URL: http://www.cisco.com/web/learning/netacad/index.html
Page 7.2.1.1, 7.2.1.2, 7.2.3.2, 7.3.1.3, 7.3.6.1, 8.3.1.1, 8.3.1.4, 8.3.2.2, 8.3.2.3, 8.3.2.5, 8.4.3.1, 8.6.3.1.

[28]. CCNA Exploration Network Fundamentals 4.0. Cisco Network Academy. Available in online books. Require user account. Updated 21.4.2009. Referred 20.4.2011.
URL: http://www.cisco.com/web/learning/netacad/index.html
Page 11.1.1.2, 11.1.3.1.

APPENDIX A

R0 Show Run Output

```
Current configuration : 1120 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R0
!
!
!
!
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
dot11 syslog
!
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
voice-card 0
  no dspfarm
!
```

```
archive
  log config
    hidekeys
!
interface FastEthernet0/0
  ip address 172.16.1.2 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial0/0/0
  ip address 172.16.2.2 255.255.255.0
  no fair-queue
!
interface Serial0/0/1
  ip address 172.16.3.2 255.255.255.0
!
ip forward-protocol nd
ip route 10.1.1.0 255.255.255.0 FastEthernet0/0
ip route 10.1.2.0 255.255.255.0 FastEthernet0/0
ip route 10.2.2.0 255.255.255.0 Serial0/0/0
ip route 10.3.3.0 255.255.255.0 Serial0/0/1
!
!
!
!

ip http server
```

```
no ip http secure-server
!
control-plane
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
  login
!
scheduler allocate 20000 1000
!
end
```

APPENDIX B

S1 Show Run Output

```
Current configuration : 1415 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S1
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
!
```

```
interface FastEthernet0/3
  switchport access vlan 20
  switchport mode access
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  no ip route-cache
  shutdown
!
ip http server
!
control-plane
!
line con 0
  exec-timeout 0 0
  logging synchronous
line vty 0 4
  login
line vty 5 15
  login
end
```

APPENDIX C

R1 Show Run Output

```
Current configuration : 2039 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
dot11 syslog
!
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
voice-card 0
 no dspfarm
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
```

```
!
crypto isakmp policy 2
 hash md5
 authentication pre-share
crypto isakmp key 6 cisco address 172.16.2.1
crypto isakmp key 6 cisco address 172.16.3.1
!
crypto ipsec transform-set BRANCH esp-3des esp-sha-hmac
crypto ipsec transform-set EXTRANET esp-des esp-md5-hmac
!
crypto map VPN 1 ipsec-isakmp
 set peer 172.16.3.1
 set security-association lifetime seconds 86400
 set transform-set BRANCH
 match address 101
crypto map VPN 20 ipsec-isakmp
 set peer 172.16.2.1
 set transform-set EXTRANET
 match address 102
!
archive
 log config
  hidekeys
!
interface FastEthernet0/0
 no ip address
 ip access-group 103 in
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.1.1.1 255.255.255.0
```

```
!
interface FastEthernet0/0.20
  encapsulation dot1Q 20
  ip address 10.1.2.1 255.255.255.0
!
interface FastEthernet0/1
  ip address 172.16.1.1 255.255.255.0
  ip access-group 103 in
  duplex auto
  speed auto
  crypto map VPN
!
interface Serial0/0/0
  no ip address
  shutdown
  no fair-queue
  clock rate 125000
!
interface Serial0/0/1
  no ip address
  shutdown
  clock rate 125000
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.16.1.2
!
ip http server
no ip http secure-server
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.3.3.0 0.0.0.255
access-list 102 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 103 deny     ip 10.2.2.0 0.0.0.255 10.1.2.0 0.0.0.255
access-list 103 permit ip any any
```

```
!
control-plane
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
  login
!
scheduler allocate 20000 1000
!
end
```

APPENDIX D

R2 Show Run Output

```
Current configuration : 3314 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
dot11 syslog
!
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
voice-card 0
  no dspfarm
!
crypto pki trustpoint TP-self-signed-2697678929
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2697678929
  revocation-check none
  rsakeypair TP-self-signed-2697678929
```

```
!
crypto pki certificate chain TP-self-signed-2697678929
 certificate self-signed 01
  3082023A 308201A3 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32363937 36373839 3239301E 170D3131 30353036 31303233
  33395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 36393736
  37383932 3930819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100D959 D99C00DB 180F4324 AAC98AB6 140AFF80 045C936D 6E60668C E6076073
  D04648A6 5C15E313 91FACC49 4F103B3C 22B58D30 1C377665 C2754D91 A2F0B8B7
  4E397DEA 3CE5E6BE 6B434DF5 3F6AC69F 7DB1C947 52C3B587 650ADF40 73E6E306
  8C810409 83D02E5F 71ECA9B5 EB0E2355 C6240567 2B1232A3 844D4B37 86136530
  FD130203 010001A3 62306030 0F060355 1D130101 FF040530 030101FF 300D0603
  551D1104 06300482 02523230 1F060355 1D230418 30168014 5B621470 EC4E7FE7
  67184573 D71A4032 F0D3CB29 301D0603 551D0E04 1604145B 621470EC 4E7FE767
  184573D7 1A4032F0 D3CB2930 0D06092A 864886F7 0D010104 05000381 81000BC7
  D3146BDE F34711DA BD7DAA9A 2D186507 E7A65408 628579AC DE5B4F6A 8EB1CF7D
  D1CFE3AC 5BECB478 FAE19377 69F97C83 185AD3E3 1D3FC592 B3EEBA8C D29E2443
  04E3E287 E2A5B4FA 948626B2 30E71F1E 92FED0B9 93598529 562EDE54 E2FDCDD3
  5A3EC6D7 43065CC8 658BB380 B0BCF5EA 54AA762F 53B085D3 54F3580B 82E0
        quit
!
username Student privilege 15 secret 5 $1$JGGf$.wBEAwWRRbdT7LPwIrmc6/
archive
 log config
  hidekeys
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
```

```
crypto isakmp policy 2
 hash md5
 authentication pre-share
crypto isakmp key cisco address 172.16.1.1
!
crypto ipsec transform-set Extranet esp-des esp-md5-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1
 set peer 172.16.1.1
 set transform-set Extranet
 match address 100
!
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.16.2.1 255.255.255.0
 no fair-queue
 clock rate 125000
 crypto map SDM_CMAP_1
!
interface Serial0/0/1
 no ip address
 shutdown
```

```
  clock rate 125000
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.16.2.2
!
ip http server
ip http authentication local
ip http secure-server
!
access-list 100 remark SDM_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
!
control-plane
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
  privilege level 15
  login local
  transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

APPENDIX E

R3 Show Run Output

```
Current configuration : 4084 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
logging buffered 52000
!
no aaa new-model
dot11 syslog
!
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
!
voice-card 0
 no dspfarm
!
crypto pki trustpoint TP-self-signed-976373574
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-976373574
 revocation-check none
 rsakeypair TP-self-signed-976373574
!
!
crypto pki certificate chain TP-self-signed-976373574
 certificate self-signed 01
  30820238 308201A1 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 39373633 37333537 34301E17 0D313130 35303631 30313735
  385A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3937 36333733
  35373430 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  C0FE8683 A72F0F85 ABE7B63A B83211D8 CC3BCE35 660EA109 09CA2053 C552D931
  D9EB29AB 66FC6C33 2C03BA9E 4F7B0271 12B84C14 5F42A8B5 0C7ACAC2 B84E468F
  777982CB DA725328 9EC7AFA9 145245E2 6C997377 BE1D2F53 FB9B6D2C C7D43EB0
  F69BD80C 8704A6F7 049C1E12 2E8E0660 0F00F10A A3A0EBB4 57B6A6BD 9A7ACE6F
  02030100 01A36230 60300F06 03551D13 0101FF04 05300301 01FF300D 0603551D
  11040630 04820252 33301F06 03551D23 04183016 80146F19 8BC8F384 B55376A7
  83226264 45E914FD D8A4301D 0603551D 0E041604 146F198B C8F384B5 5376A783
  22626445 E914FDD8 A4300D06 092A8648 86F70D01 01040500 03818100 9DE6638C
  EFA638A9 9D2A45A0 60951C94 284C5F0F 4AD3EEC6 DD93D2DE 1D8AAE0B 931C67E6
  2A5A5D8E 524720EF 9256ECB1 480E94A0 57BEEBBF D7150FB8 D905F9C1 1698B5F8
  2828107F 23AE00D3 C98E6545 2E0F3B03 540DCE2F 468C4F76 F25B0EE7 8224FCE5
  5051FB50 85B21ABC 543C6628 9C7E0F41 16521744 92A6422A BDA6CFCD
        quit
!
username Student privilege 15 secret 5 $1$YvfP$b0rhZpoi3XWFAKnqhfxtd0
archive
 log config
  hidekeys
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco address 172.16.1.1
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA1 esp-3des esp-sha-hmac
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1
 set peer 172.16.1.1
 set transform-set ESP-3DES-SHA4
 match address 104
!
interface FastEthernet0/0
 ip address 10.3.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.16.3.1 255.255.255.0
 clock rate 125000
 crypto map SDM_CMAP_1
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 125000
```

```
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.16.3.2
!
ip http server
ip http authentication local
ip http secure-server
!
access-list 100 remark SDM_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.3.3.0 0.0.0.255 10.1.0.0 0.0.255.255
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```