

6. 114484



CONTENTS

CHAPTER	Page
LIST OF TABLES	i
LIST OF FIGURES	iv
ACKNOWLEDGEMENT	vi
ABSTACT	vii
 CHAPTER	
1 INTRODUCTION	1
1.1 Background	1
1.2 Objective	2
1.3 Output	2
1.4 Scope	3
 2 LITERATURE REVIEW	4
2.1 Overview of GNS3	4
2.2 Attackers and their attacks	5
2.2.1 Developing attack profile	5
2.2.1.1 Hackers	5
2.2.1.2 Crackers	6
2.2.1.3 Script kiddies	6
2.2.1.4 Spies	6
2.2.1.5 Cyberterrorists	6
2.2.2 Understand Basic Attack	6
2.2.2.1 Password guessing	6
2.2.3 Examining identity attacks	9
2.2.3.1 Man-in-the-Middle attacks	9
2.2.3.2 Replay	10
2.2.3.3 TCP/IP hijacking	10
2.2.3.4 Denial of service attacks	11
2.2.3.5 Computer worm	13
2.3 Virtual local area network (VLAN)	14
2.3.1 VLAN Trunking Protocol (VTP)	15
2.3.2 Spanning Tree Protocol (STP)	15
2.4 Client/server protocol 1	16
2.4.1 Remote Authentication Dial In User Service (RADIUS)	16
2.4.2 Terminal Access Controller Access-Control System (TACACS)	18
2.5 TACACS+ and RADIUS Comparison	19
2.5.1 Traffic example	20
2.5.2 RADIUS and TACACS+ advantage	20
2.5.2.1 RADIUS Advantages	20
2.5.2.2 TACACS+ advantages	20
2.6 IP routing protocol	21

2 LITERATURE REVIEW (Continue)	Page
2.6.1 Open Shortest Path First (OSPF)	21
2.6.2 Enhanced interior gateway routing protocol (EIGRP)	21
2.7 Message Digest Authentication (MD)	22
2.8 Network time protocol (NTP)	23
2.8.1 Why should time be synchronized?	23
2.9 PIX firewall	24
2.9.1 Cisco Adaptive Security Device Manager (ASDM)	25
2.10 WAN	26
2.10.1 WAN security	26
2.10.1.1 Virtual private network (VPN)	26
2.10.1.1.1 Remote Access VPN	28
2.10.1.1.2 Site-to-Site VPN	29
2.10.1.1.3 Split Tunnel	30
2.11 Redundancy Protocol	31
2.11.1 Hot standby router protocol (HSRP)	31
2.11.2 Virtual router redundancy protocol (VRRP)	32
2.12 Multilayer Network	33
2.13 EtherChannel	35
2.14 Network Address Translation (NAT)	36
2.15 Cisco Access Control List (ACL)	37
2.16 DHCP Server	39
2.17 DNS Server	40
2.18 Overview of OpenERP	41
2.19 Syslog Server	42
2.20 SNMP Server	43
2.21 Kerberos Server	44
2.22 Intrusion Detection System (IDS)	49
2.22.1 Snort	51
2.23 The Switch Port Analyzer (SPAN)	52
2.24 Remote Switch Prot Analyzer (RSPAN)	58
3. THEORY AND PRICIPLE OF HARDWARE TO BE USED	61
3.1. Router	61
3.2 Layer 2 switch	62
3.3 PIX firewall	62
3.4 Intrusion Detection System (IDS)	63
4. EXPERIMENTAL DESIGN	65
4.1 Network security design	65
4.1.1 First secure topology design	65
4.1.1.1 Show running-configure	66
4.1.2 Final secure topology design	96
4.1.1.2 Show running-configure	100
5. LAB INTERACTION ON VIRTUALIZATION ARCHITECTURE SYSTEM	169

6. CONCLUSION	201
REFERENCE	203
APPENDIX (See inside the CD)	CD
Appendix A – Identification is not authentication	CD
Appendix B – Cisco PIX with ASDM on GNS3	CD
Appendix C – Olive reloaded or how to emulate Juniper routers	CD
Appendix D – vOperations Suite™ Installation Guide	CD
REASERCH TEAM	205
CURRICULUM VITAE	206



LIST OF TABLES

Table

	Page
1.1 Senior project planning and duration	2
1.2 Senior Project 2 Planning and Duration	3
2.1 Protocol that support authentication	23
2.2 HSRP and VRRP comparisons	33
4.1 First secure network shows running configure	66
4.2 Final secure network shows running configure	100

LIST OF FIGURES

Figure

	Page
2.1 GNS3 logo	4
2.2 GNS3 interface	5
2.3 Brute force attacks	8
2.4 One-way enciphered dictionary	8
2.5 Dictionary attack	9
2.6 Man-in-the-Middle attacks	10
2.7 ARP Spoofing	11
2.8 DoS attack	12
2.9 How does worm attack	13
2.10 VLAN conception model	15
2.11 VTP Conception Model	15
2.12 STP Conception Model	16
2.13 Access management in an enterprise using RADIUS	17
2.14 RADIUS Authentications and Authorization Flow	17
2.15 RADIUS Accounting Flow	18
2.16 TACACS+ traffic flow	19
2.17 RADIUS traffic flow	20
2.18 OSPF routing concept	21
2.19 EIGRP routing concept	22
2.20 MD5 Encryption form	22
2.21 NTP interface	24
2.22 Firewall concept	25
2.23 ASDM in different features	26
2.24 VPN conception model	27
2.25 VPN with IPsec	28
2.26 Remote Access VPN Concept	29
2.27 Site-to-Site VPN Concept	30
2.28 Split tunneling concept	31
2.29 Example of HSRP	31
2.30 Example VRRP	32
2.31 Multilayer Network Model	35
2.32 EtherChannel Link Model	36
2.33 NAT Conception Model	37
2.34 How ACL Work	39

LIST OF FIGURES (Continue)	Page
2.35 DHCP server assign IP address	40
2.36 How DNS Server Work	41
2.37 OpenERP Logo	41
2.38 OpenERP Form Page	42
2.39 Syslog data	43
2.40 Network Traffic Graph	44
2.41 How Kerberos Work	49
2.42 IDS Conception Model	50
2.43 IDS Structure	51
2.44 Snort Logo	51
2.45 Snort Conception Model	52
2.46 Hub Forward Traffic	53
2.47 Switch Forward Traffic	53
2.48 Unicast packet send from host A to sniffer	54
2.49 How SPAN Work	55
2.50 Structure of an RSPAN Session	59
3.1 Cisco router	61
3.2 Cisco layer 2 switch	62
3.3 PIX firewall	63
3.4 Cisco IDS	64
4.1 First secure topology design	65
4.2 Final secure topology design	99
5.1 Activity LAB1: Configure NTP, SSH and Syslog	172
5.2 LAB3: Secure topology design	177
5.3 LAB4: Inside Internet: BGP (Version 4) and Internet Service Provider	183

ACKNOWLEDGEMENT

I owe a great and many thanks to people who helped and supported me during this research. Our deepest thanks to the expert in ALCATEL Corporation, Dr. Guy Saidana for guiding and correcting various configurations with attention and carefully. He has taken pain to go through the project and make necessary correction as and when needed. We express our thanks to the University of, Mae Fah Luang University, for financial and material support. I would like to thank my faculty and faculty members without whom this project would have been a distant reality. A special thank to Captain/Dr. Thongchai Yooyativong to his guideline and full support. We also extend my heartfelt thanks to my family and well-wishers.

Khaled KESSALI



ABSTACT

These days' students have no idea how network architecture is in the enterprise and what software applications are used by companies! IC complexity due to Moore's law keeps increasing, which is also associated with different models of virtualization development; now envisage the implementation of a framework for network architecture in a simple computer laboratory. The goal is to make available to students, real industrials system environments and networks that are relatively complete and in which they can interact. In the domain of learning I am interested teaching student for their enjoyment and to enable them to practice with real (but simulated) architecture and systems in enterprise.



CHAPTER 1

INTRODUCTION

1.1 Background

Virtualization technology has become increasingly a hot topic in information technology. Also, successfully managing multiple sites is becoming increasingly difficult as budgets decrease and equipment and facilities age. Use virtualization to help cut costs, increase efficiency, and adapt quickly and automatically to changing requirements. Virtualization technologies provide education with advanced technology tools to create a quality learning environment.

- Hardware virtualization. Run multiple operating systems (for example, Linux and Windows) on a single server.
- Application virtualization. Rapidly deploy applications, even those that conflict with each other, with low administrative overhead.
- Presentation virtualization. Execute an application on one computer and present it with another.
- Desktop virtualization. Run multiple operating systems(OS) on a single desktop. Centrally execute Windows 7 in virtual machines (VMs) running on servers.
- Virtualization management. Manage your entire virtual and physical infrastructures with a unified set of tools.
- Virtualization networking management. Manage your entire virtual and physical network with a unified set of tools.

1.2 Objective

1. Implement Virtualized System Architecture in MFU LAB
2. Setup a Pilot framework in order to understand the concept of industry technology topologies, this framework can be used for signal projects (Operating system, ERP, networking, Service Oriented Architecture, real simulator applications for industry software and networking applications).

1.3 Output

In this Research I will install different operating systems in one physical machine and analyze the interaction between them. Then I will install different Enterprise Resources Planning ERP. Analyze the performance of the physical and virtual hardware. Research about different Network and Application Architectures and answer these questions:

- How to implement Virtualization Software?
- How to optimize virtual software in heterogeneous environment?
- Performance of the Physical Machine?
- Difficulties encounters during the implementation applications and what are the limits of Virtualization Software?
- How to connect Applications and Network devices using Graphical Network Simulator?
- Difficulties to install and Integrating ERP applications in the Enterprise Architecture Network?

Finally, I will use virtualization as an architecture system framework to supplement virtual network laboratories or as accessories network devices.

Teachers or students may use this pilot project to simulate network experiments, Application software, Administration of Operating Systems, interaction between protocols.

1.4 Scope

This research is to implement Virtualized System Architecture using virtualization software. Both, operating system (Windows 2003 & 2008, Open Solaris, Linux) and Network devices (Cisco, Nortel) on only one physical machine will be installed.

Researches could focused on Server virtualization, installation of different applications on different operating systems, shared resources for all the protocols, simulation and visualization of all the protocols, services and applications that run over the top of it.

Finally, Virtualization Technology can be a tool for teaching to learn about management and administration virtualization machine, operating system administration, network topologies (Computer Networks) and hardware performance.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview of Graphical Network Simulator (GNS3)



Figure 2.1 GNS3 logo

GNS3 is a graphical network simulator that allows simulation of complex networks. [4]:

To allow complete simulations, GNS3 is strongly linked with :

- Dynamips, the core program that allows Cisco IOS emulation.
- Dynagen, a text-based front-end for Dynamips.
- Pemu, a Cisco PIX firewall emulator based on Qemu.

GNS3 is an excellent complementary tool to real labs for Cisco network engineers, administrators and people wanting to pass certifications such as CCNA, CCNP, CCIP or CCIE.

It can also be used to experiment features of Cisco IOS or to check configurations that need to be deployed later on real routers.

This project is an open source, free program that may be used on multiple operating systems, including Windows, Linux, and MacOS X.

Features overview

- Design of high quality and complex network topologies.
- Emulation of many Cisco router platforms and PIX firewalls.
- Simulation of simple Ethernet, ATM and Frame Relay switches.
- Connection of the simulated network to the real world!
- Packet capture using Wireshark.

Important notice: users have to provide their own Cisco IOS to use with GNS3.

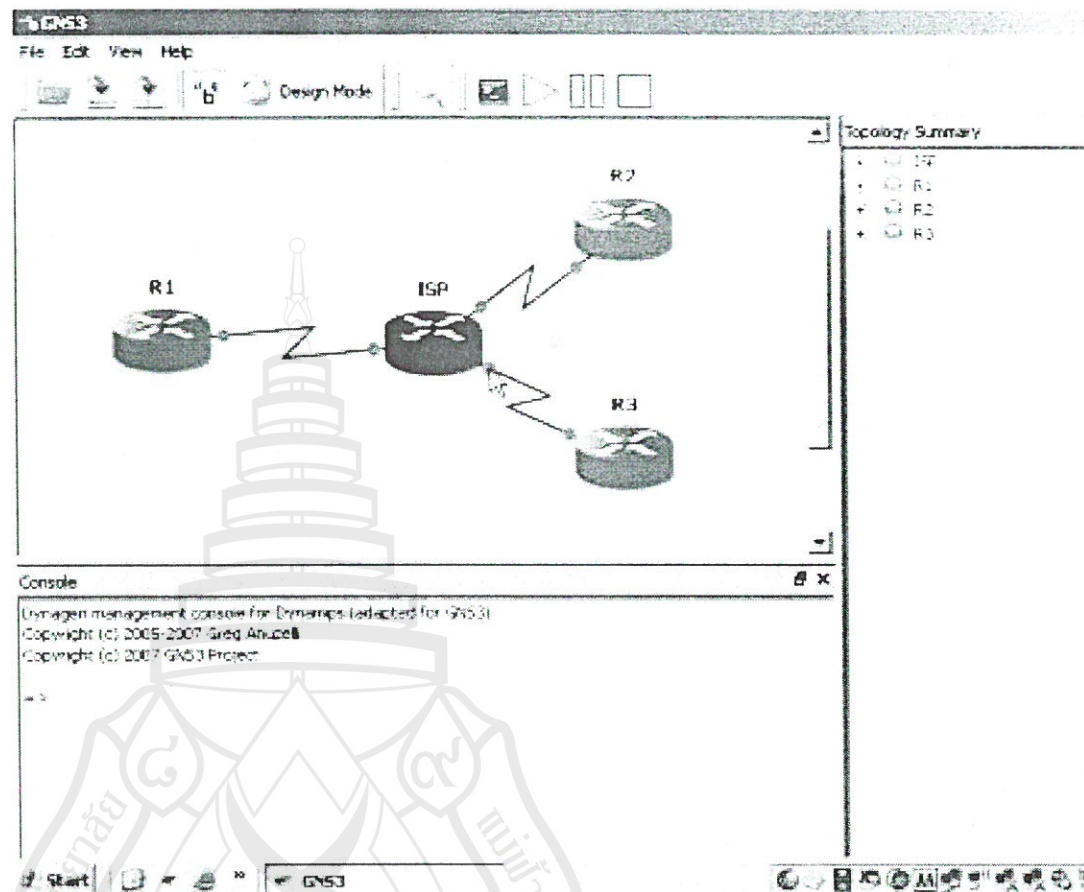


Figure 2.2 GNS3 interface

2.2 Attackers and Their Attacks

2.2.1 Developing attacks profile [1]:

2.2.1.1 Hackers

You can use the common terms “hacker” in two ways. First, “hacker” is used in a generic sense, particularly in the news media, to refer to anyone who illegally breaks into or attempts to break into a computer system. Used in this way, a hacker is synonymous with an attacker.

The term “hacker” also has a narrower definition. A hacker is described as a person who uses his or her advanced computer skills to attack computers, but not with a malicious intent. Instead, hackers use their skills to expose security flaws.

Those who call themselves hackers like to think of themselves as an elite group of people who are adept at exploring computers and networks. Although breaking into another person’s computer system is illegal, hackers believe it’s ethically acceptable as long as they don’t commit theft, vandalism, or breach any confidentiality. This is sometimes called “hacker code of ethics.” Hackers claim that their motive is to improve security. They consider it their responsibility to seek out

security holes so that they can be fixed. These hackers like to think of themselves “ethical hackers.”

2.2.1.2 Cracker

A cracker is a person who violates system security with malicious intent. Like hackers. Crackers have advance knowledge of computer and networks and the skills to exploit them. Unlike ethical hackers who claim to be only searching for security weakness, crackers destroy data, deny legitimate users of service, or otherwise cause serious problems on computers and networks. Crackers can be identified by their malicious actions: they intend to do harm to any computer they can break into.

2.2.1.3 Script kiddies

Much like crackers, script kiddies want to break into computers to create damages. However, whereas crackers have advance knowledge of computers and networks, script kiddies are unskilled users. Script kiddies do their work by downloading automated hacking software from web sites then using it to break into computers.

2.2.1.4 Spies

A computer spy is a person who has been hired to break into a computer and steal information. Spies don't randomly search for unsecured computers to attack as script kiddies, crackers, and hackers do. Rather, spies are hired to attack specific computer that contains sensitive information. Their goal is to break into that computer and take the information without drawing any attention to their action. Spies, like hackers, possess excellent computer skills.

2.2.1.5 Cyberterrorists

Terrorism has become a major security concern around the world as terrorists work to advance their causes. A report distributed by Institute for Security Technology Studies at Dartmouth College lists these three goals of a cyber attack:

- Defect electronics information (such as web sites) to spread disinformation and propaganda.

- Deny service to legitimate computer users.
- Commit unauthorized intrusion into system and networks that result in critical infrastructure outages and corruption of vital data.

2.2.2 Understand basic attacks [1]:

2.2.2.1 Password guessing

Characteristics of weak password include:

- Password that is short. (such as XYZ)

- A common word used as a password. (such as blue)
- Personal information in a password. (such as the name of a pet)
- Using the same password for all accounts.
- Writing the password down and leaving it under the mouse pad or a keyboard.
- Not changing password unless forced to do so.

Attackers attempt to exploit weak password by password guessing. Password-guessing attacks fall into three categories. The first type of attack is **brute force**, in which an attacker attempts to create every possible password combination by systematically changing one character at a time in a hypothetical password, and then using each newly generated password to access system. The second type is a **dictionary attack**. Unlike a brute force attack in which all possible combinations are used, a dictionary attack takes each word from a dictionary and encoded it (call **hashing**) in the same way the computer encodes a user's password. Attackers then compare the encoded dictionary words against those in the encoded password file. The third type is **software exploitation**. This attack takes advantage of any weakness in software to bypass security that requires a password. One of the common exploitation is a **buffer overflow**, which occurs when a computer program attempts to stuff more data into a temporary storage area (a **buffer**) That it can hold. Some computer languages automatically check for buffer overflow and prevent it from occurring.

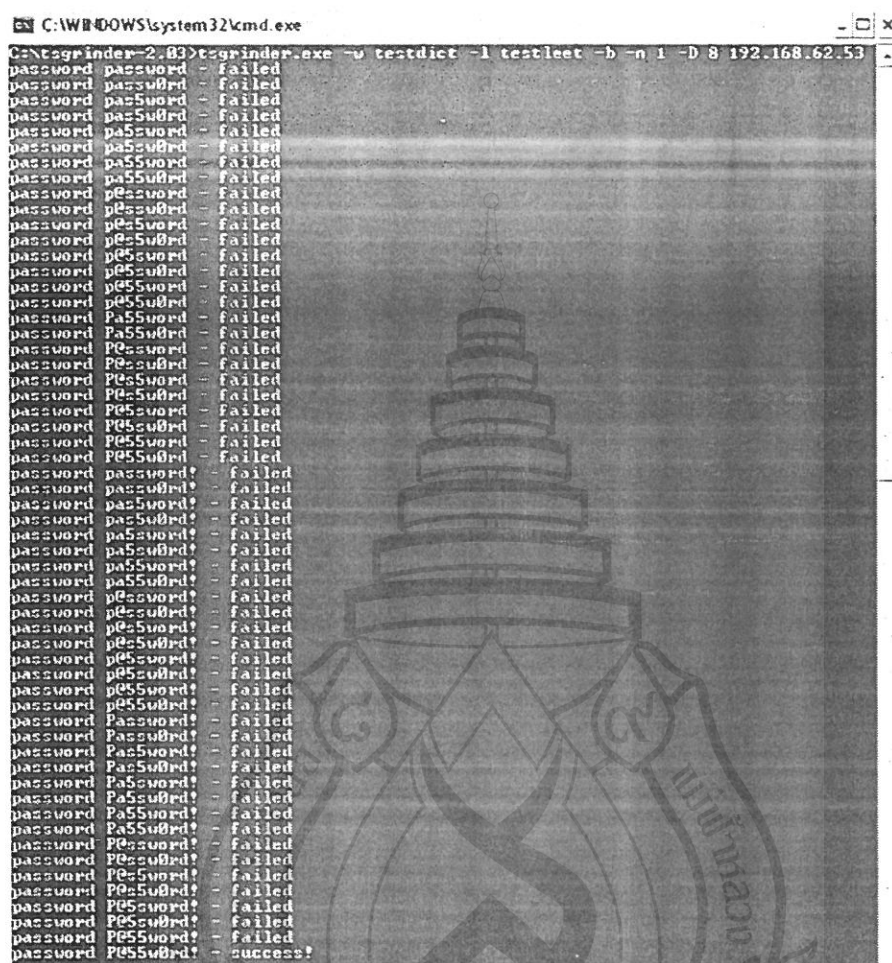


Figure 2.3 brute force attacks

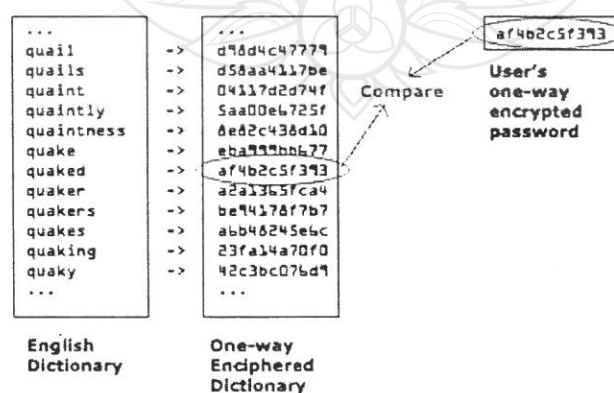


Figure 2.4 one-way enciphered dictionaries

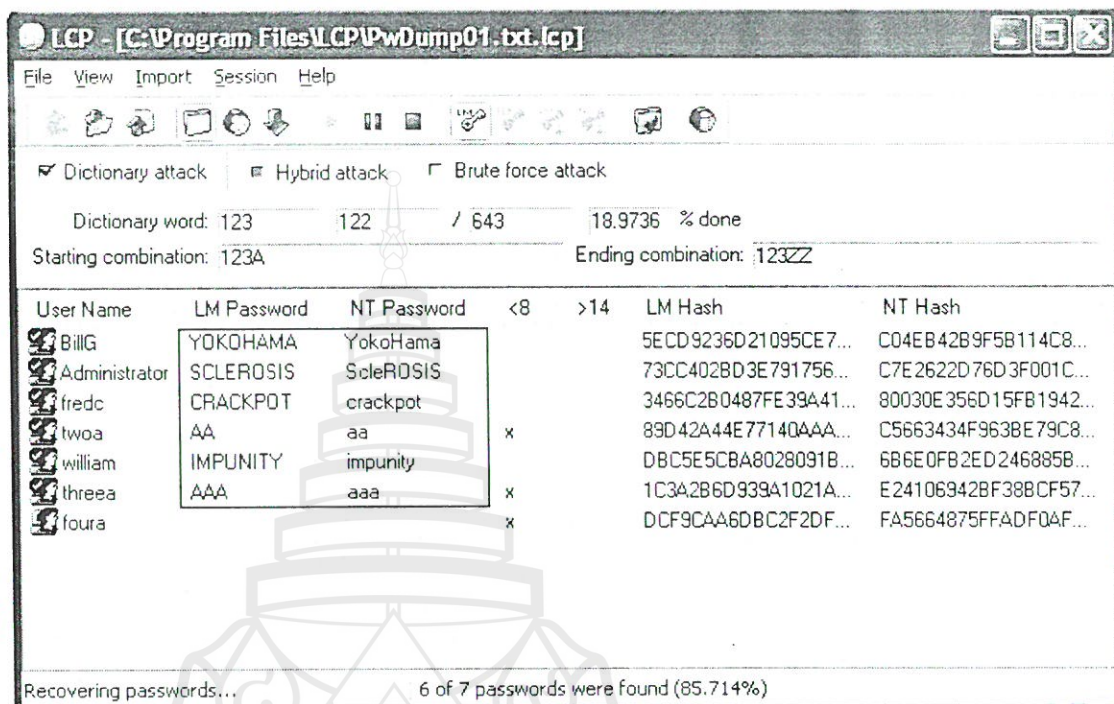


Figure 2.5 Dictionary attack

2.2.3 Examining identity attacks [1]:

2.2.3.1 Man-in-the-Middle attacks

Man-in-the-Middle attacks on computer information are common attacker tools. This type of attack make it seem that two computers are communicating with each other, when actually they're sending and receiving data with a computer between them, or the "Man-in-the-Middle."

Man-in-the-Middle attacks can be active or passive. In a passive attack, the attacker captures the sensitive data that's being transmitted and then send it on to the original recipient without his presence being detected. In an active attack, the contents of the message are intercepted and altered before they're sending on.

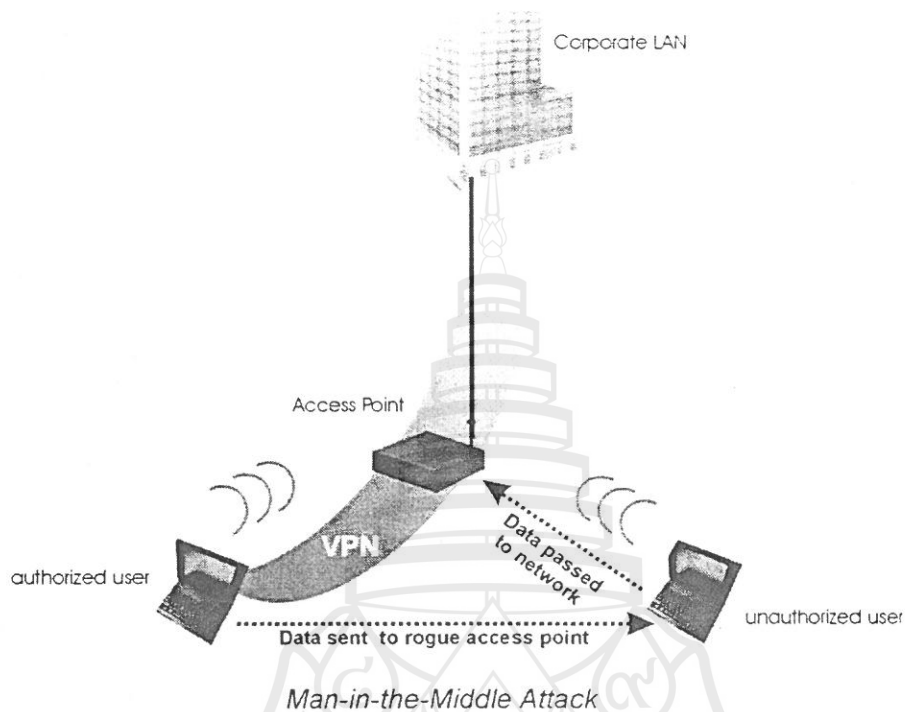


Figure 2.6 Man-in-the-Middle attacks

2.2.3.2 Replay

A replay attack is similar to an active man-in-the-middle attack. However, whereas an active man-in-the-middle attack changes the contents of a message before sending it on, a replay attack only capture the message and the send it again later.

2.2.3.3 TCP/IP hijacking

With wired networks, TCP/IP hijacking used a technique known as spoofing, which is the act of pretending to be the legitimate owner when in reality you are not. One particular type of spoofing is **Address Resolution Protocol (ARP) Spoofing** In an ARP spoofing attack; a hacker changes the table so that packets are redirected to his computer. With TCP/IP hijacking, the attackers use ARP spoofing to send information from the user's computer to the attacker's computer instead of to a valid computer.

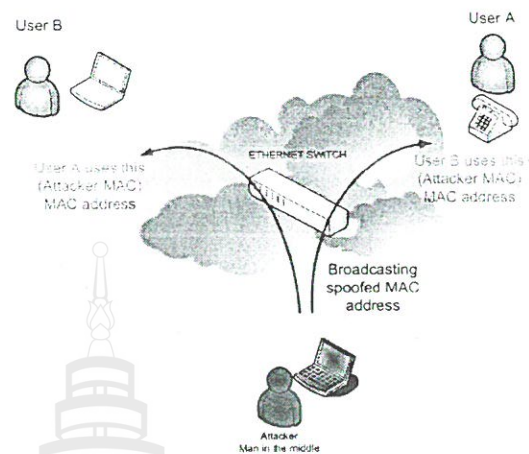


Figure 2.7 ARP Spoofing

2.2.3.4 Denial of service attacks

In contrast to a normal network situation, a denial of service (DoS) attack attempts to make a server or another network device unavailable by flooding it with requests, such as to display a web page or access a stored file. The server responds to each request from the computers that started the process. However, with a DoS attack, the computers that launched the DoS attack are programmed not to reply to the server's response. The servers "hold the line open" and continues to wait for a response. After a short time, the server runs out of resources and can no longer function. This is known as **SYN attack** because it exploits the SYS/ACK "handshake."

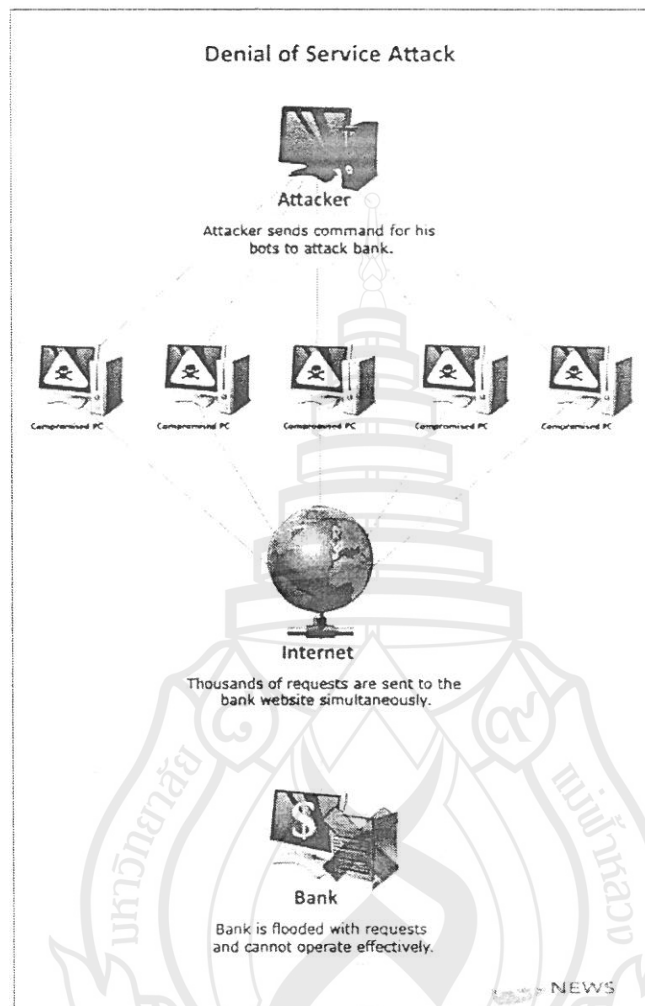


Figure 2.8 DoS attack

A variant of the DoS is the **distributed denial-of-service (DDoS)** attack. Instead of using one computer, a DDoS may use hundreds or thousands of computers. DDoS works in the following stages:

- An attacker breaks into a large computer with plenty of disk space and a fast internet connection. This computer is called the **handler**.
- Special software is loaded onto a handler computer to scan thousands of computers, looking for those that have software vulnerability in the operating system.
- When it locates a computer with a vulnerability, the handler installs software on the computer, known as a **zombie**, and then moves on to the next computer. The user of the zombie has no indication that his or her computer has malicious software installed.

o The handler instructs all of the zombie computers to flood a specific server with requests.

DDoS attacks have been successfully launched against many large organizations. These attacks can be difficult to defend against because it's difficult to restrict hundreds or thousands of computers from accessing a network.

2.2.3.5 Computer worm

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to the poor security the computers infected having. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

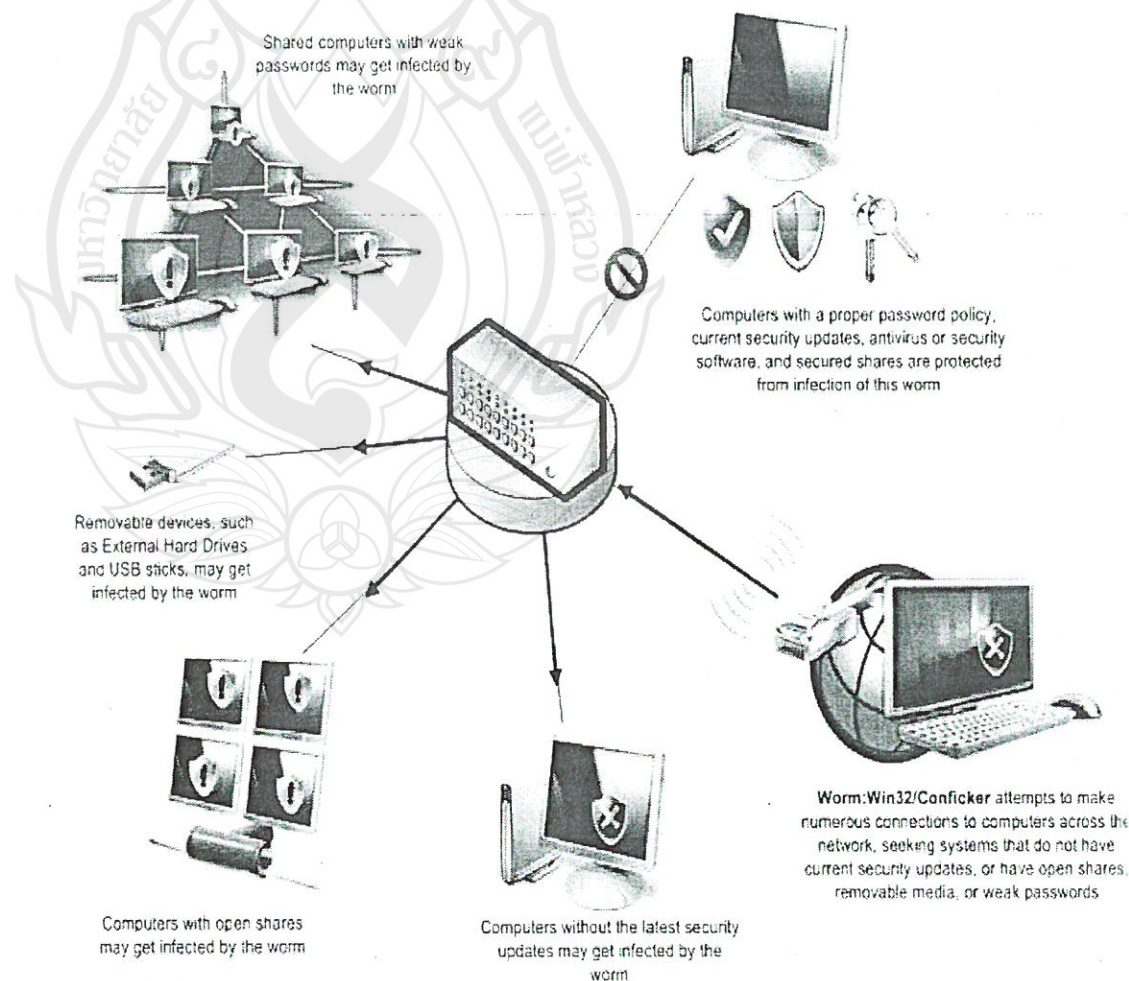


Figure 2.9 How does worm attack

2.3 Virtual Local Area Network (VLAN)

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. By definition, switches may not bridge IP traffic between VLANs as it would violate the integrity of the VLAN broadcast domain.

This is also useful if someone wants to create multiple Layer 3 networks on the same Layer 2 switch. For example, if a DHCP server (which will broadcast its presence) was plugged into a switch it will serve any host on that switch that was configured to get its IP from a DHCP server. By using VLANs you can easily split the network up so some hosts won't use that DHCP server and will obtain Link-local addresses, or obtain an address from a different DHCP server.

Virtual LANs are essentially Layer 2 constructs, compared with IP subnets which are Layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN or have one subnet spread across multiple VLANs. Virtual LANs and IP subnets provide independent Layer 2 and Layer 3 constructs that map to one another and this correspondence is useful during the network design process.

By using VLANs, one can control traffic patterns and react quickly to relocations. VLANs provide the flexibility to adapt to changes in network requirements and allow for simplified administration.

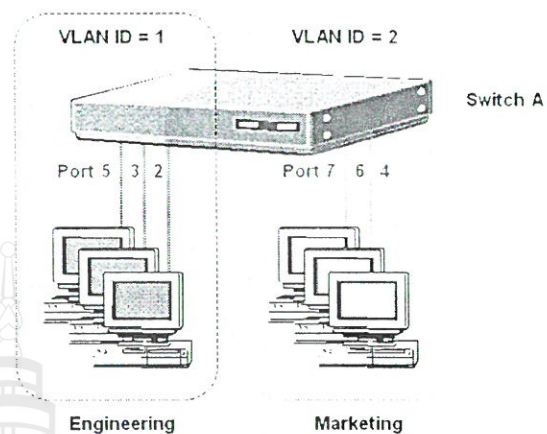


Figure 2.10 VLAN conception model

2.3.1 VLAN Trunking Protocol (VTP)

VLAN Trunking Protocol (VTP) is a Cisco proprietary Layer 2 messaging protocol that manages the addition, deletion, and renaming of Virtual Local Area Networks (VLAN) on a network-wide basis. Cisco's VLAN Trunk Protocol reduces administration in a switched network. When a new VLAN is configured on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. To do this, VTP carries VLAN information to all the switches in a VTP domain. VTP advertisements can be sent over ISL, 802.1q, IEEE 802.10. VTP is available on most of the Cisco Catalyst Family products.

VTP CLIENT AND SERVER CONFIGURATIONS

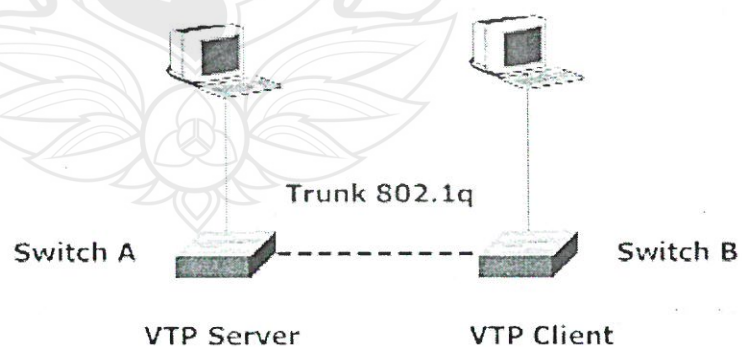


Figure 2.11 VTP Conception Model

2.3.2 Spanning Tree Protocol (STP)

The Spanning tree protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. Thus, the basic function of STP is to prevent bridge loops and ensuing broadcast radiation.

In the OSI model for computer networking, STP falls under the OSI layer-2. It is standardized as 802.1D. As the name suggests, it creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the local network.

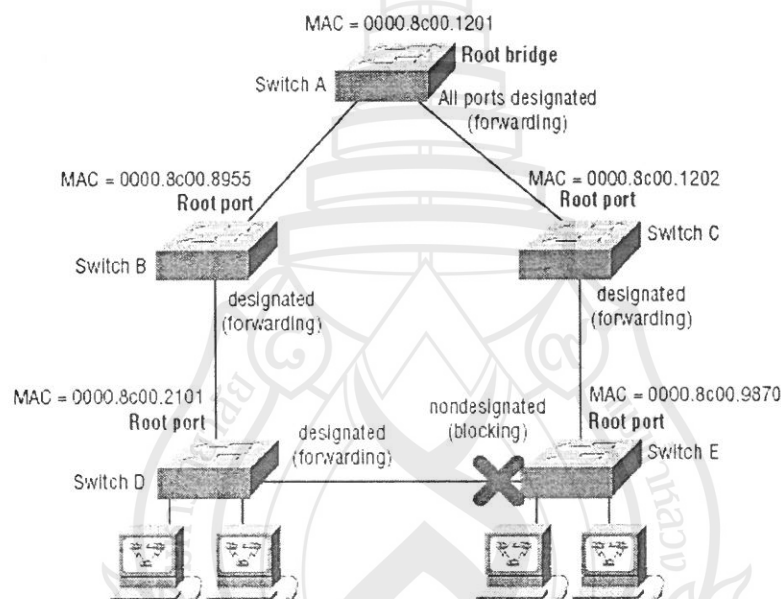


Figure 2.12 STP Conception Model

2.4 Client/server Protocol

2.4.1 Remote Authentication Dial In User Service (RADIUS)

[5]:

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. RADIUS was developed by Livingston Enterprises, Inc., in 1991 as an access server authentication and accounting protocol and later brought into the IETF standards.

Because of the broad support and the ubiquitous nature of the RADIUS protocol it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.

RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote Access Server, the Virtual Private Network server, the Network switch with port-based authentication, and the Network Access Server, are

all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server. The RADIUS server is usually a background process running on a UNIX or Windows NT machine. RADIUS serves three functions:

1. To authenticate users or devices before granting them access to a network,
2. To authorize those users or devices for certain network services and
3. To account for usage of those services.

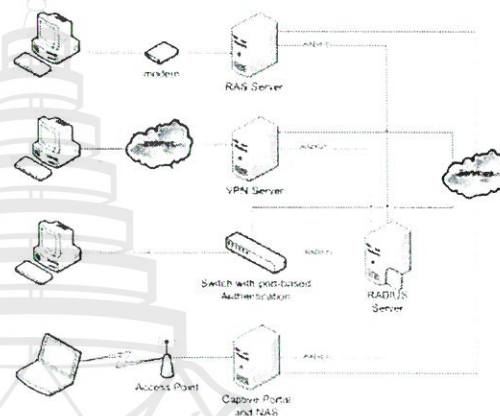


Figure 2.13 Access management in an enterprise using RADIUS

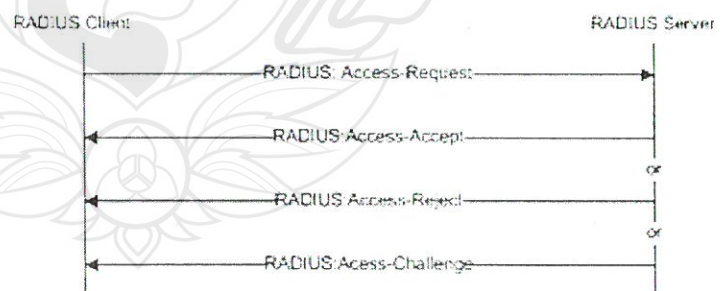


Figure 2.14 RADIUS Authentications and Authorization Flow

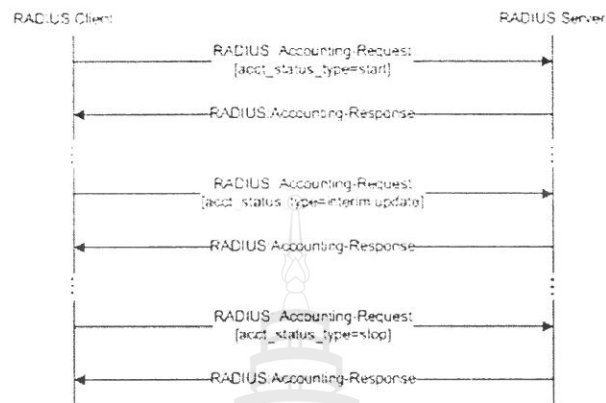


Figure 2.15 RADIUS Accounting Flow

2.4.2 Terminal Access Controller Access-Control System (TACACS)

TACACS is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network. This server was normally a program running on a host. The host would determine whether to accept or deny the request and send a response back.

2.5 TACACS+ and RADIUS Comparison

2.5.1 Traffic example

This example assumes login authentication, exec authorization, command accounting, and command accounting is implemented with TACACS+ when a user Telnets to a router, performs a command, and exits the router: [8]:

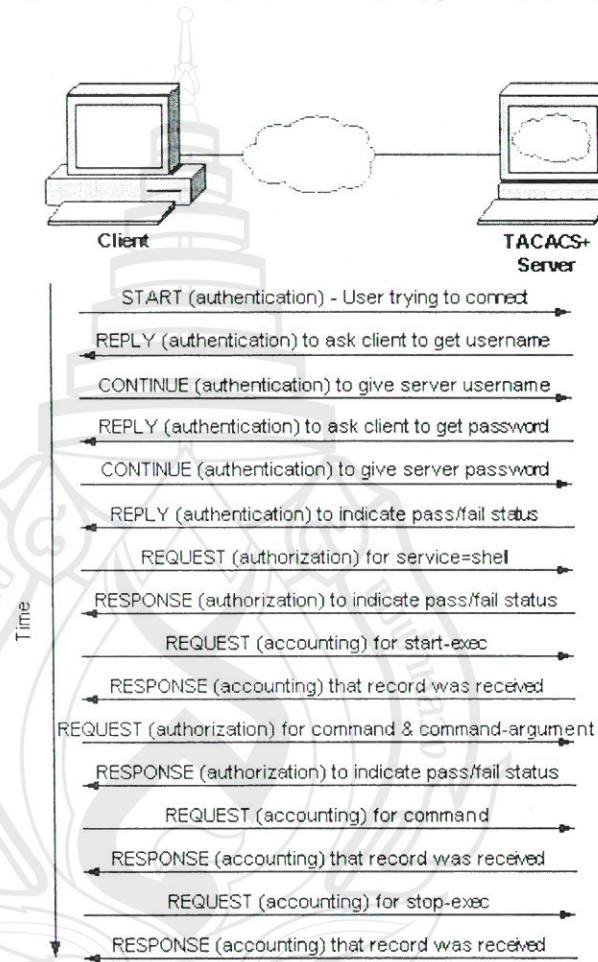


Figure 2.16 TACACS+ traffic flow

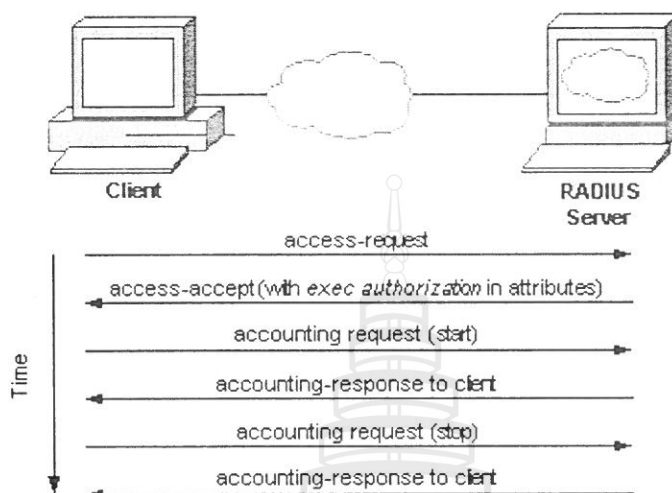


Figure 2.17 RADIUS traffic flow

2.5.2 RADIUS and TACACS+ advantage

2.5.2.1 RADIUS Advantages

The main advantage of RADIUS is availability. Although all modern Cisco devices support TACACS+, support outside the Cisco community is limited. If you work on a mixed vendor network, RADIUS is likely the best option available.

2.5.2.2 TACACS+ Advantages

As an extension of the RADIUS protocol, TACACS+ implements most of the features of RADIUS. The advantages of TACACS+ are in how it changes the implementation of RADIUS, as well as how it extends the protocol to meet the needs of modern networks.

- TACACS+ uses TCP instead of UDP. TCP guarantees communication between the client and server. Unlike UDP, which is connectionless, TCP initiates a connection with the server and is not as susceptible to situations such as network congestion and server crashes.
- TACACS+ encrypts all of the data in the TACACS+ packet. Although RADIUS does encrypt the password in the packet, it doesn't protect against other data interception such as username and accounting information.
- TACACS+ allows for different methods of authentication, authorization, and accounting. RADIUS couples authentication and authorization, making it difficult to use different servers for these purposes.
- TACACS+ allows a network administrator to define what commands a user may run. This fine grain level of control allows more controlled access for a greater number of users on a network.

When choosing a AAA protocol to use on a Cisco-based network, TACACS+ is the obvious choice. RADIUS (or a combination of TACAS+ and RADIUS) may be required if the network uses non-Cisco devices that do not support the TACACS+ protocol.

2.6 IP Routing Protocol

2.6.1 Open Shortest Path First (OSPF) [7]:

OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain (autonomous system). It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP datagram. OSPF was designed to support variable-length subnet masking (VLSM) or Classless Inter-Domain Routing (CIDR) addressing models.

OSPF detects changes in the topology, such as link failures, very quickly and converges on a new loop-free routing structure within seconds. It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a shortest path first algorithm.

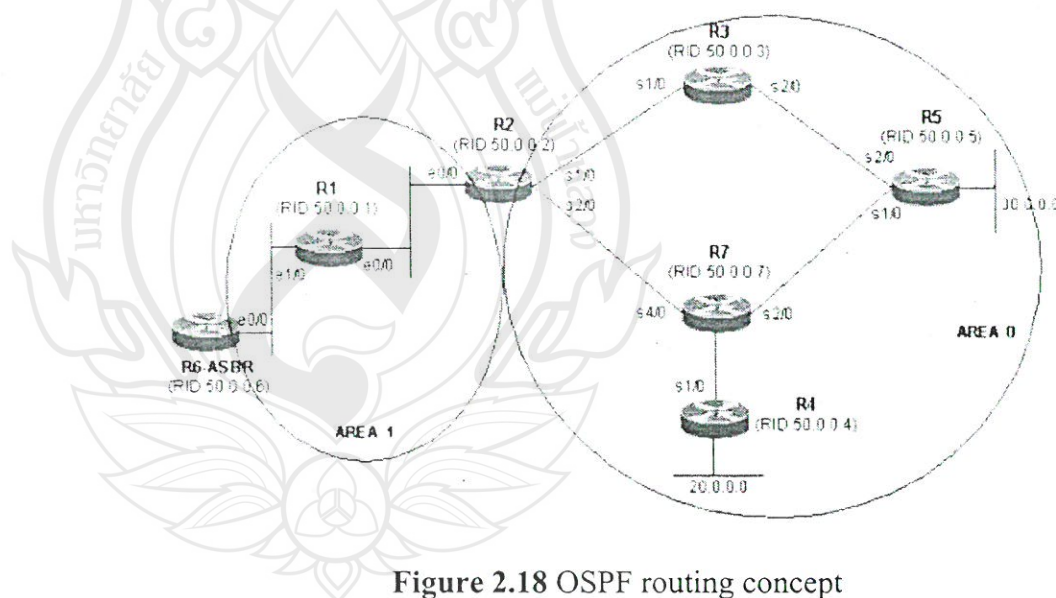


Figure 2.18 OSPF routing concept

2.6.2 Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a Cisco proprietary routing protocol loosely based on their original IGRP. EIGRP is an advanced distance-vector routing protocol, with optimizations to minimize both the routing instability incurred after topology changes, as well as the use of bandwidth and processing power in the router. Routers that support EIGRP will automatically redistribute route information to IGRP neighbors by converting the 32 bit EIGRP metric to the 24 bit IGRP metric. Most of the routing optimizations are based on the Diffusing Update Algorithm (DUAL) work from SRI, which guarantees loop-free operation and provides a mechanism for fast convergence.

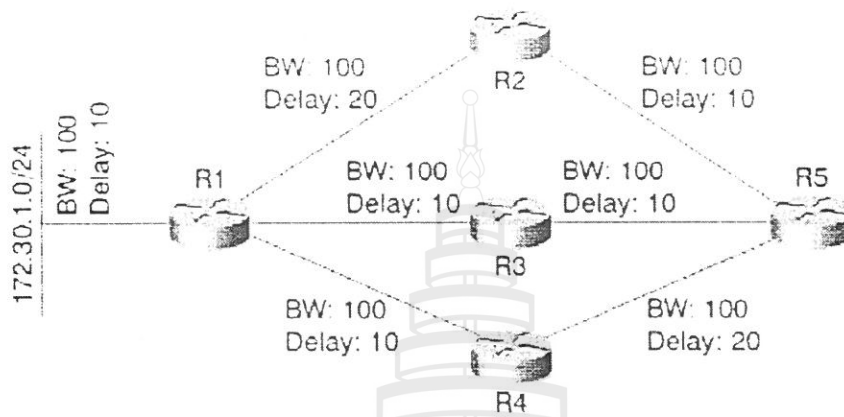


Figure 2.19 EIGRP routing concept

2.7 Message Digest Authentication (MD)

Message Digest authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. It can be configured by both OSPF and EIGRP.

```

1140 918.345356 10.10.10.2      224.0.0.2      HSRP    Hello (state Active)
1143 921.351587 10.10.10.2      224.0.0.2      HSRP    Hello (state Active)
1146 924.355102 10.10.10.2      224.0.0.2      HSRP    Hello (state Active)

• Frame 1129 (62 bytes on wire, 62 bytes captured)
• Ethernet II, Src: All-HSRP-routers_01 (00:00:0c:07:ac:01), Dst: IPv4mcast_00:00:02 (01:00:5e:00:00:02)
• Internet Protocol, Src: 10.10.10.2 (10.10.10.2), Dst: 224.0.0.2 (224.0.0.2)
• User Datagram Protocol, Src Port: hsrp (1985), Dst Port: hsrp (1985)
• Cisco Hot Standby Router Protocol

0000  01 00 5e 00 00 02 00 00 0c 07 ac 01 08 00 45 c0  ..^.....E.
0010  00 30 00 00 00 00 01 11 c4 ef 0a 0a 0a 02 e0 00  .0.....
0020  00 02 07 c1 07 c1 00 1c ae 40 00 00 10 03 0a 96  .....:g.....
0030  01 00 48 53 52 50 40 49 43 54 0a 0a 0a 01      ..HSRP: CT....

```

Figure 2.20 MD5 Encryption form

Protocol Name	Authen- tication	Clear-Text	MD5 Hash	Open Standard
RIP	No	-	-	Yes
IGRP	No	-	-	Proprietary
RIPv2	Yes	Yes	Yes	Yes
EIGRP	Yes	-	Yes	Proprietary
OSPF	Yes	Yes	Yes	Yes

Table 2.1 Protocol that support authentication

2.8 Network Time Protocol (NTP)

NTP stands for Network Time Protocol, and it is an Internet protocol used to synchronize the clocks of computers to some time reference. NTP is an Internet standard protocol [3]:

2.8.1 Why should Time be synchronized?

Time usually just advances. If you have communicating programs running on different computers, time still should even advance if you switch from one computer to another. Obviously if one system is ahead of the others, the others are behind that particular one. From the perspective of an external observer, switching between these systems would cause time to jump forward and back, a non-desirable effect.

As a consequence, isolated networks may run their own wrong time, but as soon as you connect to the Internet, effects will be visible. Just imagine some Email message arrived five minutes before it was sent, and there even was a reply two minutes before the message was sent.


```

Clock is synchronized, stratum 3, reference is 202.12.97.45
nominal freq is 250.0000 Hz, actual freq is 249.9980 Hz, precision is 2**1
8
reference time is C58874BA.4BBA5A64 (09:38:50.295 GMT+7 Fri Jan 7 2005)
clock offset is -7.8664 msec, root delay is 399.54 msec
root dispersion is 80.63 msec, peer dispersion is 1.56 msec
Router-2#show ntp ass
Router-2#show ntp associations

```

disp	address	ref clock	st	when	poll	reach	delay	offset
*~1.6	202.12.97.45	131.188.3.222	2	61	64	377	1.5	-7.87

* master (sync'd), # master (unsync'd), + selected, - candidate, ~ config
ured
Router-2#

Figure 2.21 NTP interface

2.9 PIX Firewall

The PIX is a firewall appliance based on a hardened, specially built operating system, PIX OS, minimizing possible OS-specific security holes. The PIX has received ICSA Firewall and IPsec certification as well as Common Criteria EAL4 evaluation status. PIX firewalls provide a wide range of security and networking services including: [2]:

- Network Address Translation (NAT) or Port Address Translation (PAT)
- content filtering (Java/ActiveX)
- URL filtering
- IPsec VPN
- support for leading X.509 PKI solutions
- DHCP client/server
- PPPoE support
- advanced security services for multimedia applications and protocols including Voice over IP (VoIP), H.323, SIP, Skinny and Microsoft NetMeeting
- AAA (RADIUS/TACACS+) integration

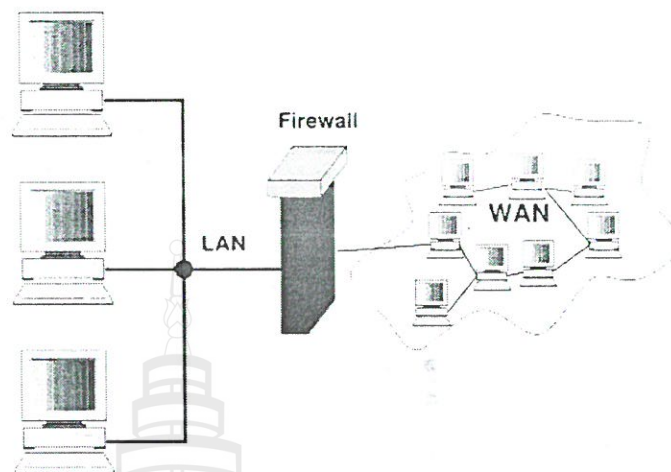


Figure 2.22 Firewall concept

2.9.1 Cisco Adaptive Security Device Manager (ASDM)

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring through an intuitive, easy-to-use Web-based management interface. Bundled with Cisco ASA Series Adaptive Security Appliances and Cisco PIX Security Appliances, Cisco ASDM accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced integrated security and networking features offered by the market-leading suite of Cisco security appliances. Its secure, Web-based design enables anytime, anywhere access to Cisco ASA Adaptive Security Appliances and Cisco PIX Security Appliances.

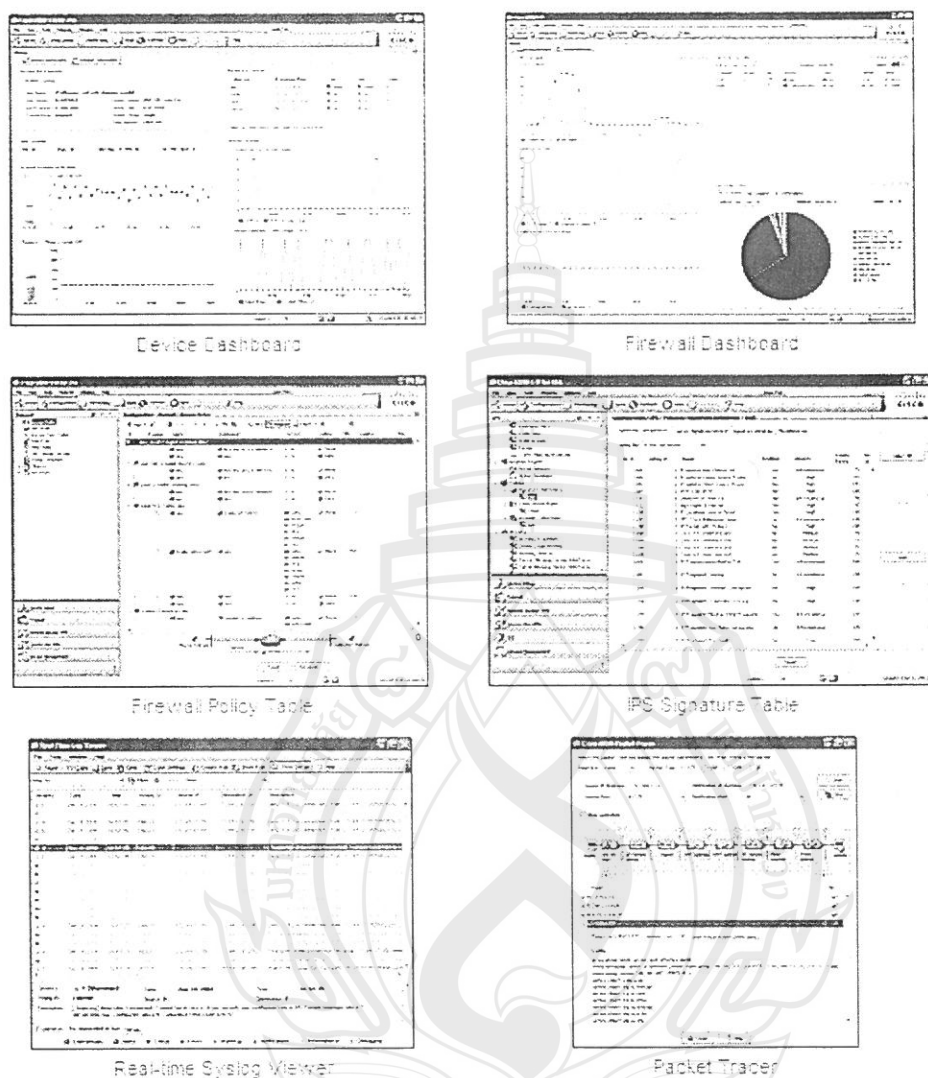


Figure 2.23 ASDM in different features

2.10 Wide Area Network (WAN)

2.10.1 WAN security

2.10.1.1 Virtual private network (VPN)

A **virtual private network (VPN)** is a computer network that is implemented in an additional logical layer (overlay) on top of an existing network. It has the purpose of creating a private scope of computer communications or providing a secure extension of a private network into an insecure network such as the Internet.

The links between nodes of a virtual private network are formed over logical connections or virtual circuits between hosts of the larger network. The Link Layer protocols of the virtual network are said to be tunneled through the underlying transport network.

One common application is to secure communications through the public

Internet, but a VPN does not need to have explicit security features such as authentication or traffic encryption. For example, VPNs can also be used to separate the traffic of different user communities over an underlying network with strong security features, or to provide access to a network via customized or private routing mechanisms.

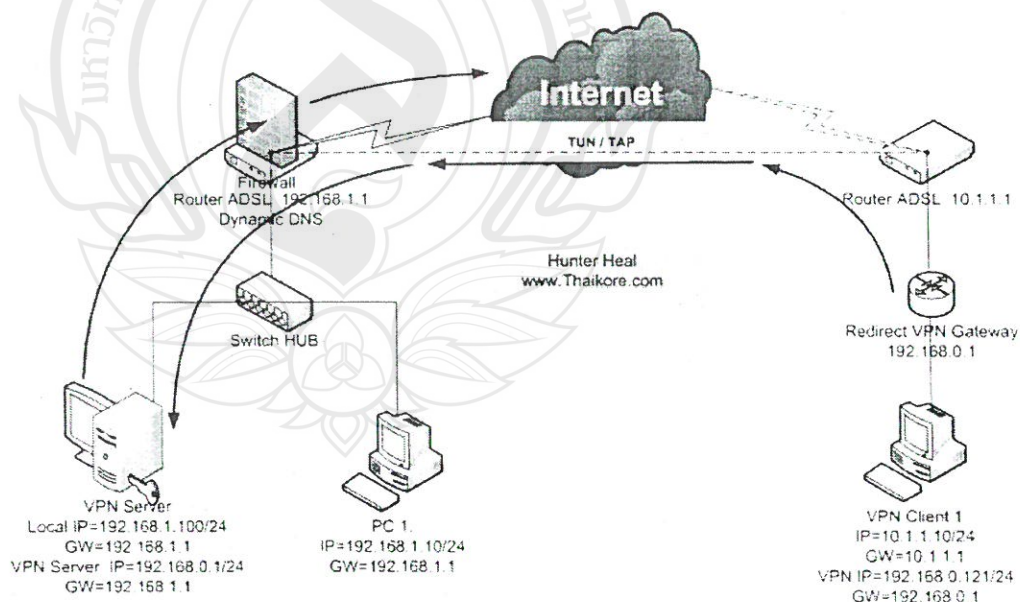
VPNs are often installed by organizations to provide remote access to a secure organizational network. Generally, a VPN has a network topology more complex than a point-to-point connection. VPNs are also used to mask the IP address of individual computers within the Internet in order, for instance, to surf the World Wide Web anonymously or to access location restricted services, such as Internet television.

Most VPN technologies can be separated into two broad categories, secure VPNs and trusted VPNs.

Secure VPNs explicitly provide mechanisms for authentication of the tunnel endpoints during tunnel setup, and encryption of the traffic in transit. Often secure VPNs are used to protect traffic when using the Internet as the underlying backbone, but equally they may be used in any environment when the security level of the underlying network differs from the traffic within the VPN.

VPN Network (Redirect Gateway)

Wednesday, April 02, 2008



Page 1

Figure 2.24 VPN conception model

Secure VPNs may be implemented by organizations wishing to provide remote access facilities to their employees or by organizations wishing to connect

multiple networks together securely using the Internet to carry the traffic. A common use for secure VPNs is in remote access scenarios, where VPN client software on an end user system is used to connect to a remote office network securely. Secure VPN protocols include IPSec, SSL or PPTP (with MPPE).

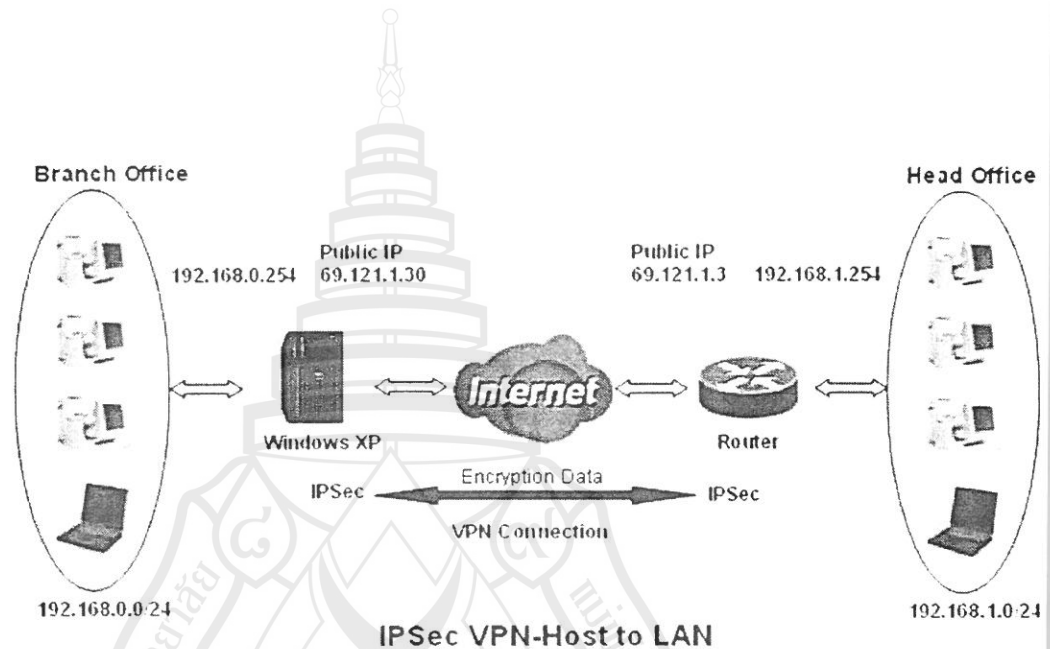


Figure 2.25 VPN with IPSec

Trusted VPNs are commonly created by carriers and large organizations and are used for traffic segmentation on large core networks. They often provide quality of service guarantees and other carrier-grade features. Trusted VPNs may be implemented by network carriers wishing to multiplex multiple customer connections transparently over an existing core network or by large organizations wishing to segregate traffic flows from each other in the network. Trusted VPN protocols include MPLS, ATM or Frame Relay.

From a customer perspective, a trusted VPN may act as a logical wire connecting two networks. The underlying carrier network is not visible to the customer, nor is the customer aware of the presence of other customers traversing the same backbone. Interference between customers, or interference with the backbone itself, is not possible from within a trusted VPN.

2.10.1.1.1 Remote Access VPN

VPN Remote-access, also called a virtual private dial-up network (VPDN), is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations. Typically, a corporation that wishes to set up a large remote-access VPN will outsource to an enterprise

service provider (ESP). The ESP sets up a network access server (NAS) and provides the remote users with desktop client software for their computers. The telecommuters can then dial a toll-free number to reach the NAS and use their VPN client software to access the corporate network.

A good example of a company that needs a remote-access VPN would be a large firm with hundreds of sales people in the field. Remote-access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.

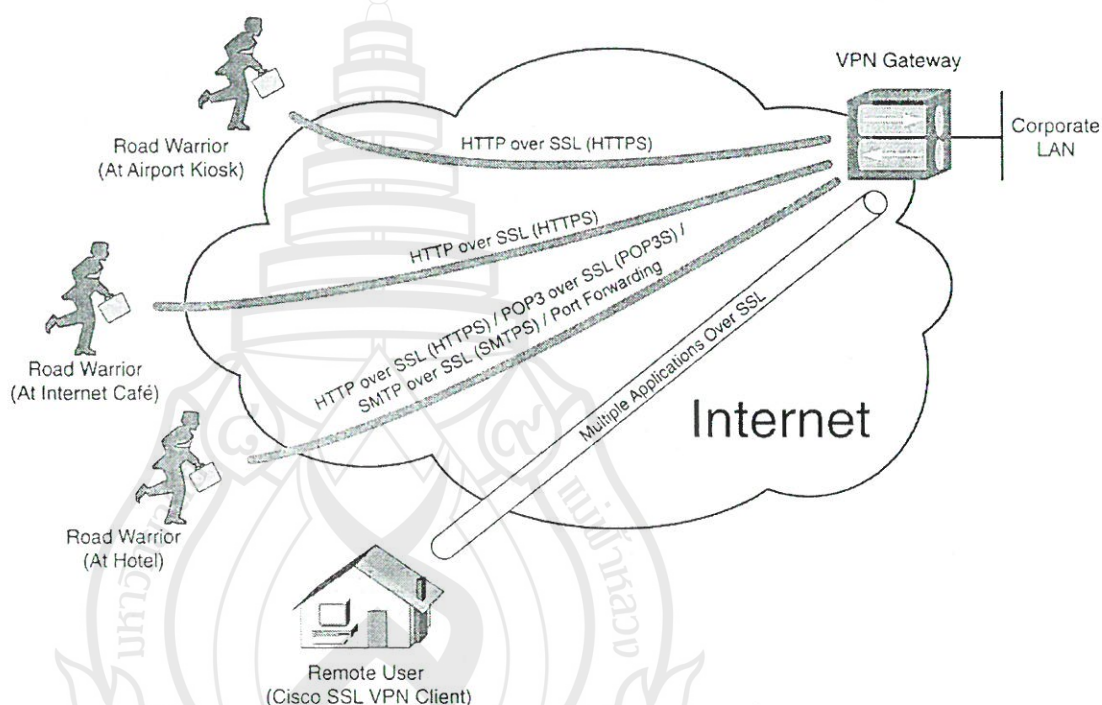


Figure 2.26 Remote Access VPN Concept

2.10.1.1.2 Site-to-Site VPN

Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network such as the Internet. Site-to-site VPNs can be one of two types:

Intranet-based - If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.

Extranet-based - When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

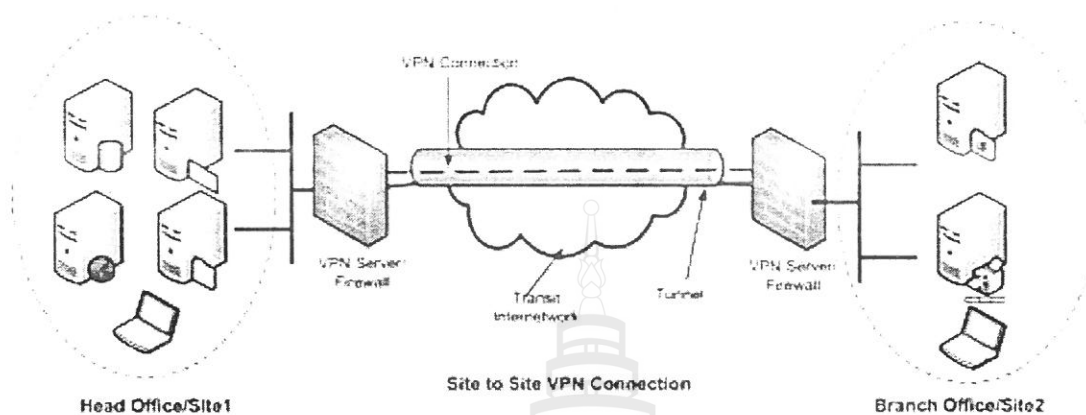


Figure 2.27 Site-to-Site VPN Concept

2.10.1.1.3 Split Tunnel

Split tunneling is a computer networking concept which allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. This connection service is usually facilitated through a program such as a VPN client software application.

For example, suppose a user utilizes a remote access VPN software client connecting to a corporate network using a hotel wireless network. The user with split tunneling enabled is able to connect to file servers, database servers, mail servers and other servers on the corporate network through the VPN connection. When the user connects to Internet resources (Web sites, FTP sites, etc), the connection request goes directly out the gateway provided by the hotel network.

Advantage: One advantage of using split tunneling is that it alleviates bottlenecks and conserves bandwidth as Internet traffic does not have to pass through the VPN server.

Another advantage is in the case where a user works at a supplier or partner site and needs access to network resources on both networks throughout the day. Split-tunneling prevents the user from having to continually connect and disconnect.

Disadvantage: A disadvantage of this method is that it essentially renders the VPN vulnerable to attack as it is accessible through the public, non-secure network. When split tunneling is enabled, users bypass gateway level security that might be in place within the company infrastructure. For example, if web or content filtering is in place, this is something usually controlled at a gateway level, not the client PC.

ISP's that implement DNS hijacking break name resolution of private addresses with a split tunnel.

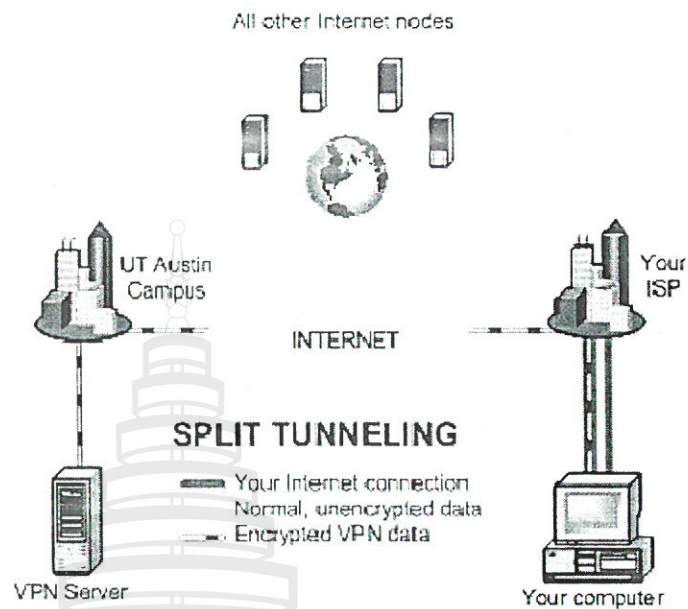


Figure 2.28 Split tunneling concept

2.11 Redundancy Protocol

2.11.1 Hot Standby Router Protocol (HSRP)

The Hot Standby Router Protocol (HSRP) provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

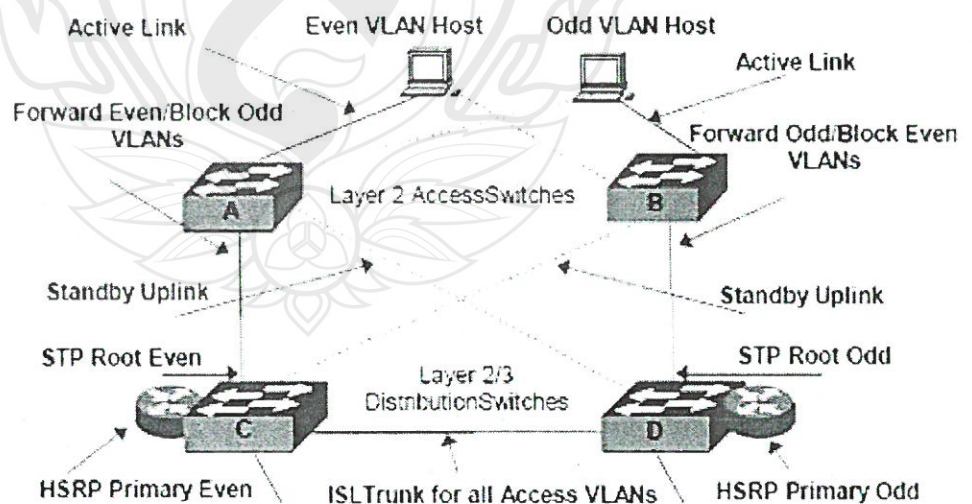


Figure 2.29 Example of HSRP

Parameter	HSRP	VRRP
Protocol and Port	UDP port 1985	IP protocol 112
Virtual MAC	0:0:c:7:ac:[HSRP grp]	0:0:5e:0:1:[VRID]
Virtual IP	User defined	User defined
Hello 'speakers': stable operation	Active and standby routers	Master
Hello 'speakers': during failure	All	All
Hello src IP	Interface IP	Interface IP
Hello src MAC	BIA (non-active rtrs) Virtual MAC (active rtr)	Virtual MAC (active rtr)
Hello dst IP	224.0.0.2 (TTL 1)	224.0.0.18 (TTL 255)
Hello dst MAC	1:0:5e:0:0:2	1:0:5e:0:0:12
Gratuitous ARP: src MAC	Virtual MAC	Virtual MAC
Data to standby group: dst MAC	Virtual MAC	Virtual MAC
Data from standby group: src MAC	BIA	BIA

Table 2.2 HSRP and VRRP comparisons

2.12 Multilayer Network

Most logical architectures for routing and switching are based around a system whereby three sets of functions are abstracted logically from one another. A common one is Core, Distribution and Access. These are often thought of as layers.

The benefit of adopting the multilayer campus design is clarity of roles performed by each layer. The role of each layer is translated to a set of features required, which in turn translates to which particular type of hardware is to be used.

Access Layer

The access layer within the multilayer campus design model is where users

gain access to the network. Most of the features found within the access layer are geared toward collecting and conditioning the traffic that is coming in from the users' end stations. These features include the following:

- Aggregating all the user endpoints
- Providing traffic conditioning functions such as marking and policing
- Providing intelligent network services such as automatic IP phone discovery
- Providing network security services such as 802.1x and port security
- Providing redundant links toward the distribution layer

In the classic multilayer campus design, the access layer is mainly made up of Layer 2 switches. Therefore, most of the work done here is in optimizing the Layer 2 protocol that governs this layer. This helps to provide a robust Layer 2 environment for the functioning of the IP network.

Distribution Layer

The distribution layer within the multilayer campus design model aggregates the access layer. One of the most important characteristics of the distribution layer is that it is the point where the Layer 2 domain ends and where the Layer 3 domain begins. The features at the distribution layer include the following:

- Aggregating access layer switches
- Terminating virtual LANs (VLANs) that are defined within the Layer 2 domain
- Providing the first-hop gateway service for all the end stations
- Providing traffic conditioning services such as security, quality of service (QoS), and queuing
- Providing redundant links toward the core layer, if required

Because the distribution layer is the meeting place for both the Layer 2 and Layer 3 domains, it runs both Layer 2 and Layer 3 protocols. This is also the place where most of the network intelligence is found and is perhaps one of the most complex parts of the network.

Core Layer

The core layer within the multilayer campus design model has two important tasks:

- Interconnect all the distribution layer blocks
- Forward all the traffic as quickly as it can

As the backbone of the entire network, its function is quite different from that of the access layer and distribution layer. The features that are critical to the functioning of the core layer include the following:

- Aggregating distribution layers to form an interconnected network
- Providing high-speed transfer of traffic among the distribution layers

- Providing a resilient IP routing environment

Because speed is of the essence here, the core layer usually does not provide services that may affect its performance (for example, security, access control, or any activities that require it to process every packet).

In the discussion of multilayer campus design, the inclusion of a core layer is always an interesting question. For a small network, it is common to see a two-tier design, for cost reasons. However, for bigger networks, inclusion of the core layer is always recommended to scale the network in a manageable fashion.

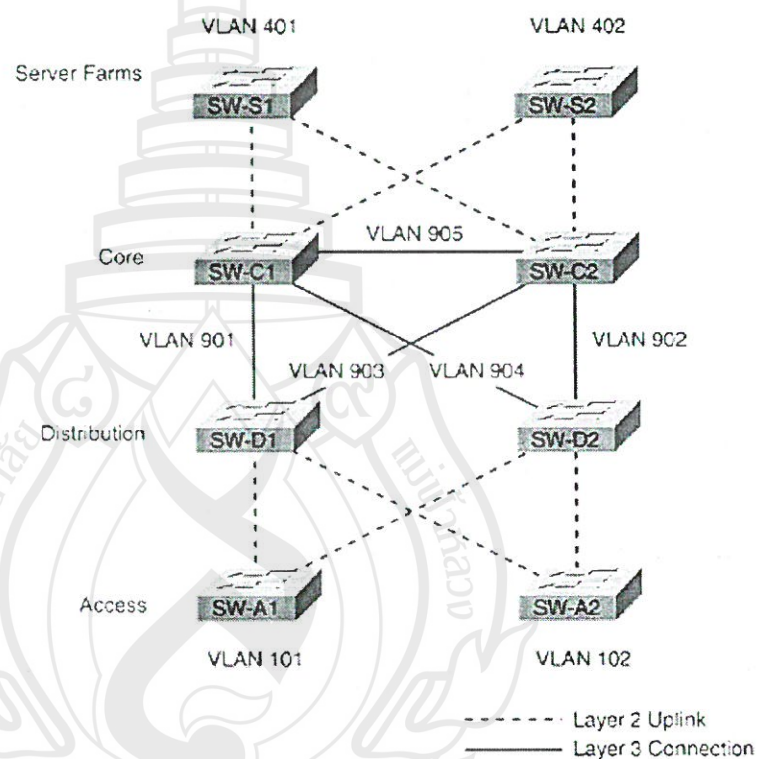


Figure 2.31 Multilayer Network Model

2.13 EtherChannel

EtherChannel is a port trunking (link aggregation being the general term) technology or port-channel architecture used primarily on Cisco switches. It allows grouping several physical Ethernet links to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers. An EtherChannel can be created from between two and eight active Fast Ethernet, Gigabit Ethernet or 10-Gigabit Ethernet ports, with an additional one to eight inactive (failover) ports which become active as the other active ports fail. EtherChannel is primarily used in the backbone network, but can also be used to connect end user machines.

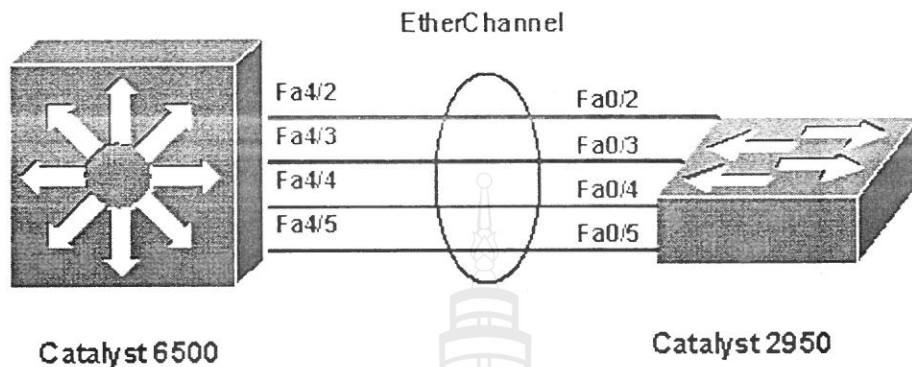


Figure 2.32 EtherChannel Link Model

2.14 Network Address Translation (NAT)

Network Address Translation (NAT) is an IETF standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. All necessary IP address translations occur where the LAN interfaces with the broader Internet. NAT converts the packet headers (and in some cases the port numbers in the headers) for incoming and outgoing traffic and keeps track of each session. This does mean, however, that NAT overrides "Internet transparency", a practice in which packets remain intact throughout their transmission. Routers and Windows Internet Connection Sharing also provide NAT

NAT accomplishes these key purposes:

- * It acts as a firewall by hiding internal IP addresses.
- * It enables an enterprise to use more internal IP addresses, since there is no possibility of conflict between its internal-only IP addresses and those used by other organizations. Essentially, an organization can present itself to the Internet with fewer IP addresses than used on its internal network, which conserves public IP addresses.
- * It allows an enterprise to bundle multiple ISDN connections into one Internet connection.

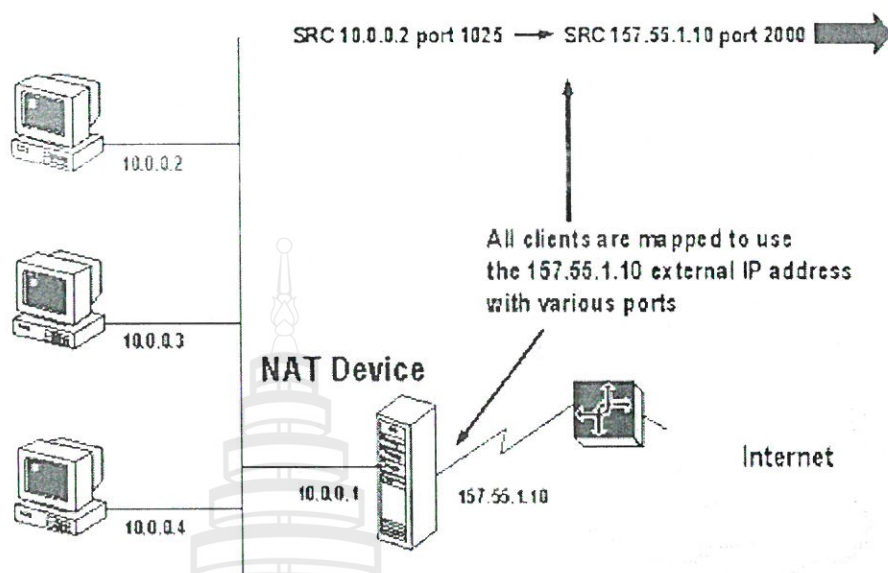


Figure 2.33 NAT Conception Model

2.15 Cisco Access Control List (ACL)

The Cisco Access Control List (ACL) is used for filtering traffic based on a given filtering criteria on a router or switch interface. Based on the conditions supplied by the ACL, a packet is allowed or blocked from further movement.

Cisco ACLs are available for several types of routed protocols including IP, IPX, AppleTalk, XNS, DECnet, and others. However, we will be discussing ACLs pertaining to TCP/IP protocol only.

ACLs for TCP/IP traffic filtering are primarily divided into two types:

- * Standard Access Lists, and
- * Extended Access Lists

Standard Access Control Lists: Standard IP ACLs range from 1 to 99. A Standard Access List allows you to permit or deny traffic FROM specific IP addresses. The destination of the packet and the ports involved can be anything.

This is the command syntax format of a standard ACL.

access-list access-list-number {permit|deny} {host|source source-wildcard|any}
 Standard ACL example:

```
access-list 10 permit 192.168.2.0 0.0.0.255
```

This list allows traffic from all addresses in the range 192.168.2.0 to 192.168.2.255. Note that when configuring access lists on a router, you must identify each access list uniquely by assigning either a name or a number to the protocol's access list.

There is an implicit deny added to every access list. If you entered the command:

```
show access-list 10
```

The output looks like:

```
access-list 10 permit 192.168.2.0 0.0.0.255
```

```
access-list 10 deny any
```

Extended Access Control Lists: Extended IP ACLs allow you to permit or deny traffic from specific IP addresses to a specific destination IP address and port. It also allows you to have granular control by specifying controls for different types of protocols such as ICMP, TCP, UDP, etc within the ACL statements. Extended IP ACLs range from 100 to 199. In Cisco IOS Software Release 12.0.1, extended ACLs began to use additional numbers (2000 to 2699).

The syntax for IP Extended ACL is given below:

```
access-list access-list-number {deny | permit} protocol source source-  
wildcard
```

```
destination destination-wildcard [precedence precedence]
```

Note that the above syntax is simplified, and given for general understanding only.

Extended ACL example:

```
access-list 110 - Applied to traffic leaving the office (outgoing)
```

```
access-list 110 permit tcp 92.128.2.0 0.0.0.255 any eq 80
```

ACL 110 permits traffic originating from any address on the 92.128.2.0 network. The 'any' statement means that the traffic is allowed to have any destination address with the limitation of going to port 80. The value of 0.0.0.0/255.255.255.255 can be specified as 'any'.

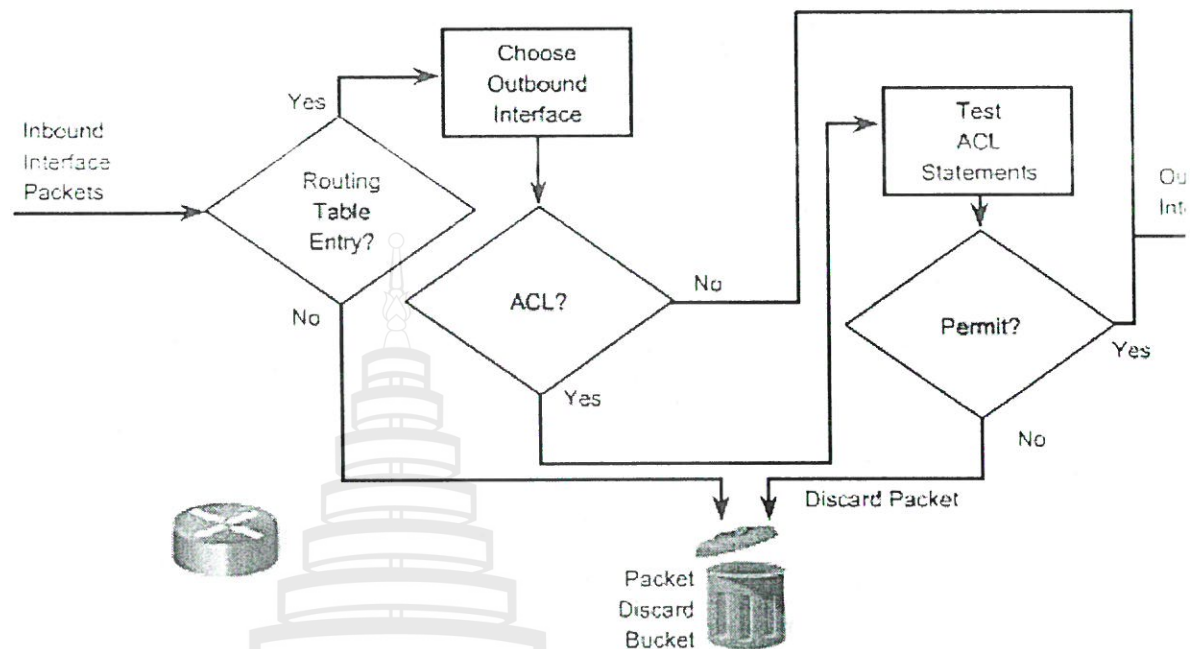


Figure 2.34 How ACL Work

2.16 DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.

DHCP assigns an IP address when a system is started, for example:

1. A user turns on a computer with a DHCP client.
2. The client computer sends a broadcast request (called a DISCOVER or DHCPDISCOVER), looking for a DHCP server to answer.
3. The router directs the DISCOVER packet to the correct DHCP server.
4. The server receives the DISCOVER packet. Based on availability and usage policies set on the server, the server determines an appropriate address (if any) to give to the client. The server then temporarily reserves that address for the client and sends back to the client an OFFER (or DHCPOFFER) packet, with that address information. The server also configures the client's DNS servers, WINS servers, NTP servers, and sometimes other services as well.
5. The client sends a REQUEST (or DHCPREQUEST) packet, letting the server know that it intends to use the address.
6. The server sends an ACK (or DHCPACK) packet, confirming that the client has been given a lease on the address for a server-specified period of time.

When a computer uses a static IP address, it means that the computer is manually configured to use a specific IP address. One problem with static assignment, which can result from user error or inattention to detail, occurs when two computers are

configured with the same IP address. This creates a conflict that results in loss of service. Using DHCP to dynamically assign IP addresses minimizes these conflicts.

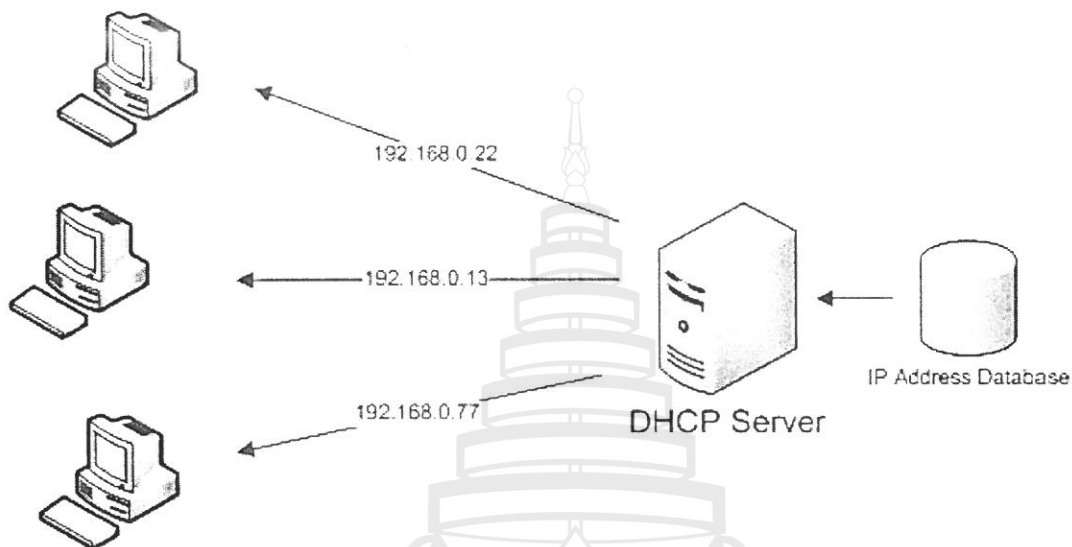


Figure 2.35 DHCP server assign IP address

2.17 DNS Server

The Internet maintains two principal namespaces, the domain name hierarchy and the Internet Protocol (IP) address system. The Domain Name System maintains the domain namespace and provides translation services between these two namespaces. Internet name servers implement the Domain Name System. A DNS name server is a server that stores the DNS records, such as address (A) records, name server (NS) records, and mail exchanger (MX) records for a domain name (see also List of DNS record types) and responds with answers to queries against its database. The top hierarchy of the Internet Domain Name Server is served by the root name servers maintained by delegation by the Internet Corporation for Assigned Names and Numbers (ICANN).

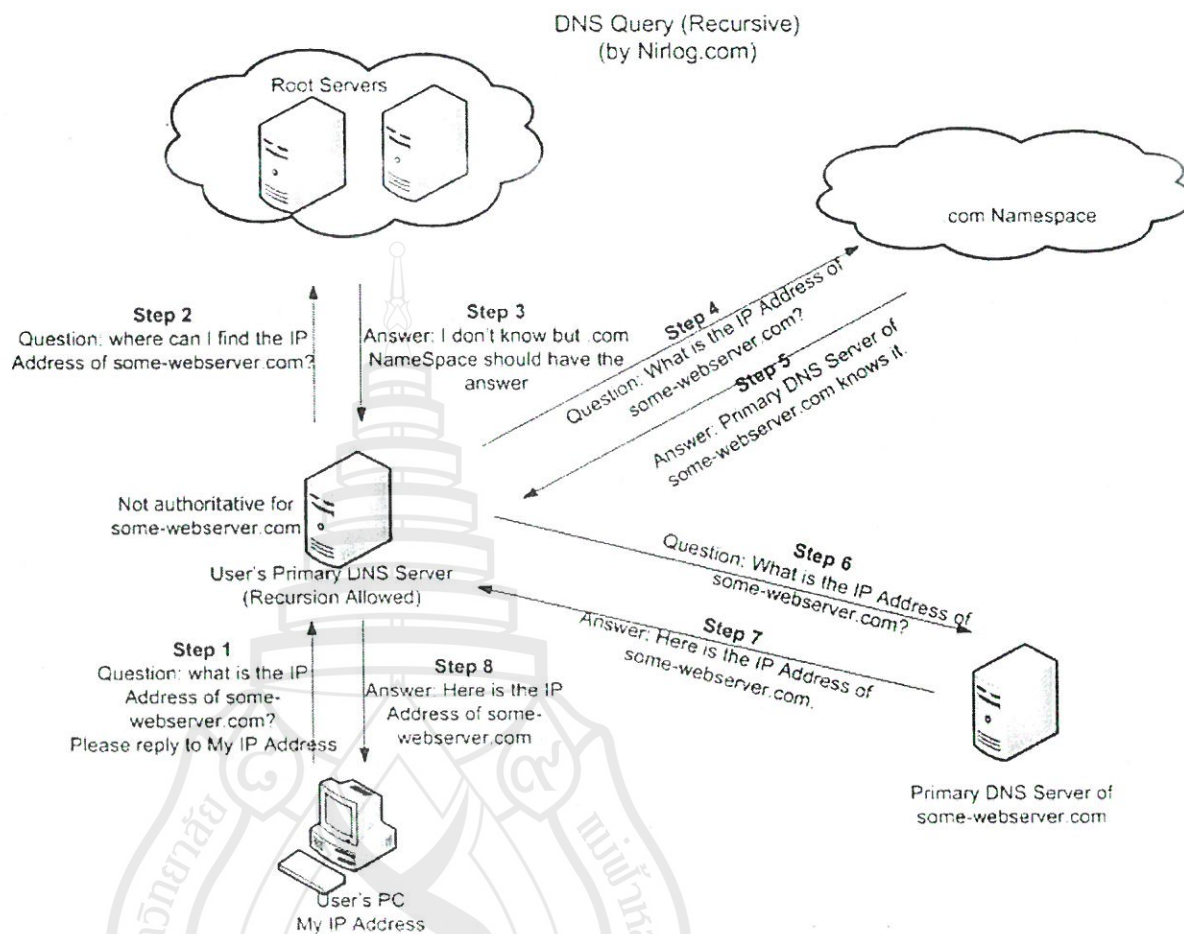


Figure 2.36 How DNS Server Work

2.18 Overview of OpenERP



Figure 2.37 OpenERP Logo

OpenERP is an open source suite of business applications. It has separate client and server components. XML-RPC interfaces are available. Among the features are management accounting, financial accounting, inventory management, sales and purchase management, tasks automation, Human Resource Management, marketing campaigns, help desk, and point of sale. The software is open source and is released under the GNU General Public License. The Linux user interface is GTK+ based. Windows and Mac OS X versions are also available. A web interface (formerly named 'eTiny') is also available using the Turbogears web framework. Since 2008, a KDE user interface is also available. The latest version of Open ERP (5.0) provides dynamic Gantt charts (with drag&drop), shared calendars, an integrated BPM view, a workflow editor and a screen designer. OpenERP offers 500+ available modules and a

Partner Network over 35 countries. It is based on a strong MVC architecture, flexible workflows, a dynamic GUI, an XML-RPC interface, and customizable reporting system with convenient OpenOffice.org integration. Currently the development on the release of OpenERP 6.0 is under process.

The screenshot displays the OpenERP web interface for editing a partner record. The top menu bar includes 'File', 'User', 'Form', 'Options', 'Plugins', 'Shortcuts', and 'Help'. Below this is a toolbar with icons for 'New', 'Save', 'Delete', 'Back', 'Forward', 'List', 'Form', 'Print', 'Action', 'Attachments', 'Menu', 'Reload', and 'Close'. The main form area is titled 'Menu' and contains tabs for 'Invoices', 'Partners', and 'Contacts'. The 'Partners' tab is active, showing the record for 'AGUSTek'. The form fields include 'Name' (AGUSTek), 'Code' (empty), 'Customer' (checked), 'Title' (empty), 'Language' (empty), 'Supplier' (checked), 'General Sales & Purchases History Notes Accounting Categories' (empty), 'Address' (Default), 'Street' (31 Hong Kong street), 'Street2' (empty), 'Zip' (22410), 'City' (Taiwan), 'Country' (Taiwan), 'Fed. State' (empty), 'Phone' (empty), 'Fax' (empty), 'E-Mail' (empty), 'Contacts' (empty), 'Partner Seq.' (0), 'Contact' (Tang), 'Partner Function' (Salesman), 'Phone' (empty), 'Fax' (empty), 'Extension' (empty), 'Other' (empty), 'E-Mail' (empty). The bottom status bar shows 'Record: 1 / 21 of 21 - Editing document (id: 2)', 'socket://localhost:8070 [all]', 'Administrator', 'State: Requests: 1 request(s)'. A large watermark of a Thai temple is visible in the background.

Figure 2.38 OpenERP Form Page

2.19 Syslog Server

Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices, which would otherwise be unable to communicate, a means to notify administrators of problems or performance. Syslog can be used for computer system management and security auditing as well as generalized informational, analysis, and debugging messages. It is supported by a wide variety of devices (like printers and routers) and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository. Messages refer to a facility (auth, authpriv, daemon, cron, ftp, lpr, kern, mail, news, syslog, user, uucp, local0, ..., local7) and are assigned a priority/level (Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug) by the sender of the message.

Configuration allows directing messages to various local devices (console), files (/var/log/) or remote syslog daemons. Care must be taken when updating the

configuration as omitting or misdirecting message facility.level can cause important messages to be ignored by syslog or overlooked by the administrator.

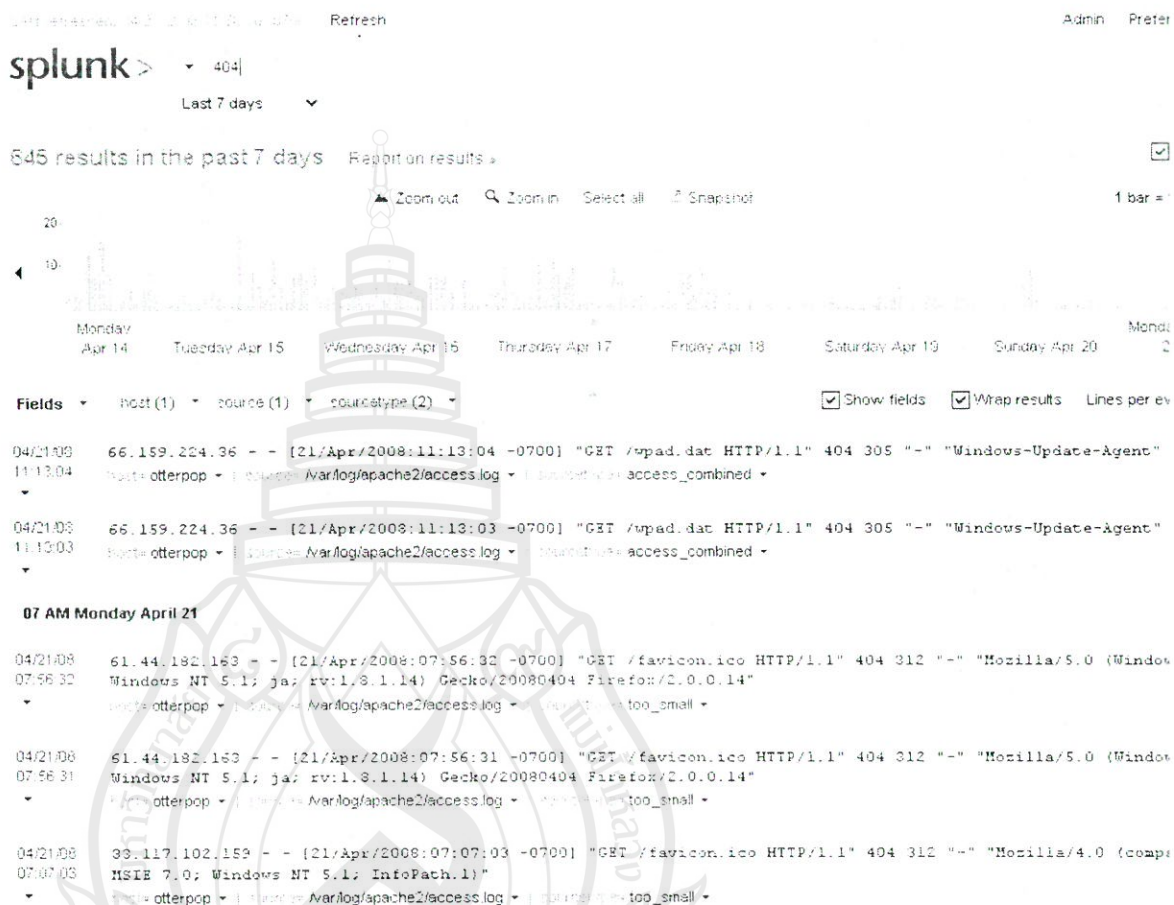


Figure 2.39 Syslog data

2.20 SNMP Server

Simple Network Management Protocol, and is a set of standards for communication with devices in a TCP/IP network. SNMP monitoring is useful for anyone who is responsible for servers and network devices such as hosts, routers, hubs and switches. It lets you keep an eye on network and bandwidth usage, and track important issues such as uptime and traffic levels.

In typical SNMP use, one or more administrative computers called managers have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

Essentially, SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and

other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

An SNMP-managed network consists of three key components:

- Managed device
- Agent — software which runs on managed devices
- Network management system (NMS) — software which runs on the manager

A *managed device* is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An *agent* is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP specific form.

A *network management system* (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

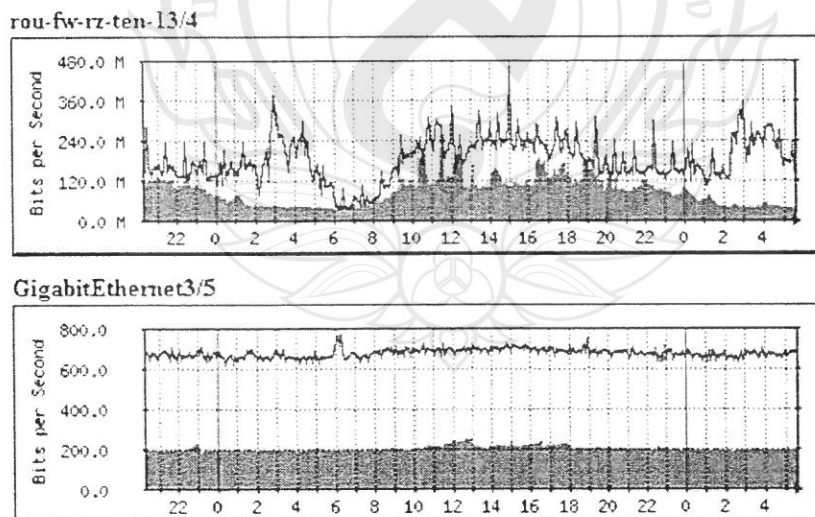


Figure 2.40 Network Traffic Graph

2.21 Kerberos Server

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.

The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by malicious hackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server.

Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure than a computer which is not connected to the network --- and powered off!) In many places, these restrictions are simply unrealistic and unacceptable.

Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

Kerberos is freely available from MIT, under copyright permissions very similar those used for the BSD operating system and the X Window System. MIT provides Kerberos in source form so that anyone who wishes to use it may look over the code for themselves and assure themselves that the code is trustworthy. In addition, for those who prefer to rely on a professionally supported product, Kerberos is available as a product from many different vendors.

In summary, Kerberos is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. We hope you find Kerberos as useful as it has been to us. At MIT, Kerberos has been invaluable to our Information/Technology architecture.

Theory

Kerberos uses as its basis the symmetric Needham-Schroeder protocol. It makes use of a trusted third party, termed a key distribution center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). Kerberos works on the basis of "tickets" which serve to prove the identity of users.

The KDC maintains a database of secret keys; each entity on the network — whether a client or a server — shares a secret key known only to itself and to the KDC. Knowledge of this key serves to prove an entity's identity. For communication between two entities, the KDC generates a session key which they can use to secure their interactions. The security of the protocol relies heavily on participants

maintaining loosely synchronized time and on short-lived assertions of authenticity called Kerberos tickets.

Description

The following is an intuitive description. The client authenticates itself to the Authentication Server and receives a ticket. (All tickets are time-stamped.) It then contacts the Ticket Granting Server, and using the ticket it demonstrates its identity and asks for a service. If the client is eligible for the service, then the Ticket Granting Server sends another ticket to the client. The client then contacts the Service Server, and using this ticket it proves that it has been approved to receive the service.

A simplified and more detailed description of the protocol follows. The following abbreviations are used:

- * AS = Authentication Server
- * SS = Service Server
- * TGS = Ticket-Granting Server
- * TGT = Ticket-Granting Ticket

The client authenticates to the AS once using a long-term shared secret (e.g. a password) and receives a TGT from the AS. Later, when the client wants to contact some SS, it can (re)use this ticket to get additional tickets from TGS, for SS, without resorting to using the shared secret. These tickets can be used to prove authentication to SS. The phases are detailed below.

User Client-based Logon

1. A user enters a username and password on the client machine.
2. The client performs a one-way function (hash usually) on the entered password, and this becomes the secret key of the client/user.

Client Authentication

1. The client sends a cleartext message of the user ID to the AS requesting services on behalf of the user. (Note: Neither the secret key nor the password is sent to the AS.) The AS generates the secret key by hashing the password of the user found at the database (e.g. Active Directory in Windows Server).
2. The AS checks to see if the client is in its database. If it is, the AS sends back the following two messages to the client:

* Message A: Client/TGS Session Key encrypted using the secret key of the client/user.

* Message B: Ticket-Granting Ticket (which includes the client ID, client network address, ticket validity period, and the client/TGS session key) encrypted using the secret key of the TGS.

3. Once the client receives messages A and B, it decrypts message A to obtain the Client/TGS Session Key. This session key is used for further communications with the TGS. (Note: The client cannot decrypt Message B, as it is encrypted using TGS's secret key.) At this point, the client has enough information to authenticate itself to the TGS.

Client Service Authorization

1. When requesting services, the client sends the following two messages to the TGS:

* Message C: Composed of the TGT from message B and the ID of the requested service.

* Message D: Authenticator (which is composed of the client ID and the timestamp), encrypted using the Client/TGS Session Key.

2. Upon receiving messages C and D, the TGS retrieves message B out of message C. It decrypts message B using the TGS secret key. This gives it the "client/TGS session key". Using this key, the TGS decrypts message D (Authenticator) and sends the following two messages to the client:

* Message E: Client-to-server ticket (which includes the client ID, client network address, validity period and Client/Server Session Key) encrypted using the service's secret key.

* Message F: Client/server session key encrypted with the Client/TGS Session Key.

Client Service Request

1. Upon receiving messages E and F from TGS, the client has enough information to authenticate itself to the SS. The client connects to the SS and sends the following two messages:

* Message E from the previous step (the client-to-server ticket, encrypted using service's secret key).

* Message G: a new Authenticator, which includes the client ID, timestamp and is encrypted using client/server session key.

2. The SS decrypts the ticket using its own secret key to retrieve the Client/Server Session Key. Using the sessions key, SS decrypts the Authenticator and sends the

following message to the client to confirm its true identity and willingness to serve the client:

** Message H:* the timestamp found in client's Authenticator plus 1, encrypted using the Client/Server Session Key.

3. The client decrypts the confirmation using the Client/Server Session Key and checks whether the timestamp is correctly updated. If so, then the client can trust the server and can start issuing service requests to the server.

4. The server provides the requested services to the client.

Drawbacks

* Single point of failure: It requires continuous availability of a central server. When the Kerberos server is down, no one can log in. This can be mitigated by using multiple Kerberos servers and fallback authentication mechanisms.

* Kerberos requires the clocks of the involved hosts to be synchronized. The tickets have a time availability period and if the host clock is not synchronized with the Kerberos server clock, the authentication will fail. The default configuration per MIT requires that clock times are no more than five minutes apart. In practice Network Time Protocol daemons are usually used to keep the host clocks synchronized.

* The administration protocol is not standardized and differs between server implementations. Password changes are described in RFC 3244.

* Since all authentication is controlled by a centralized KDC, compromise of this authentication infrastructure will allow an attacker to impersonate any user.

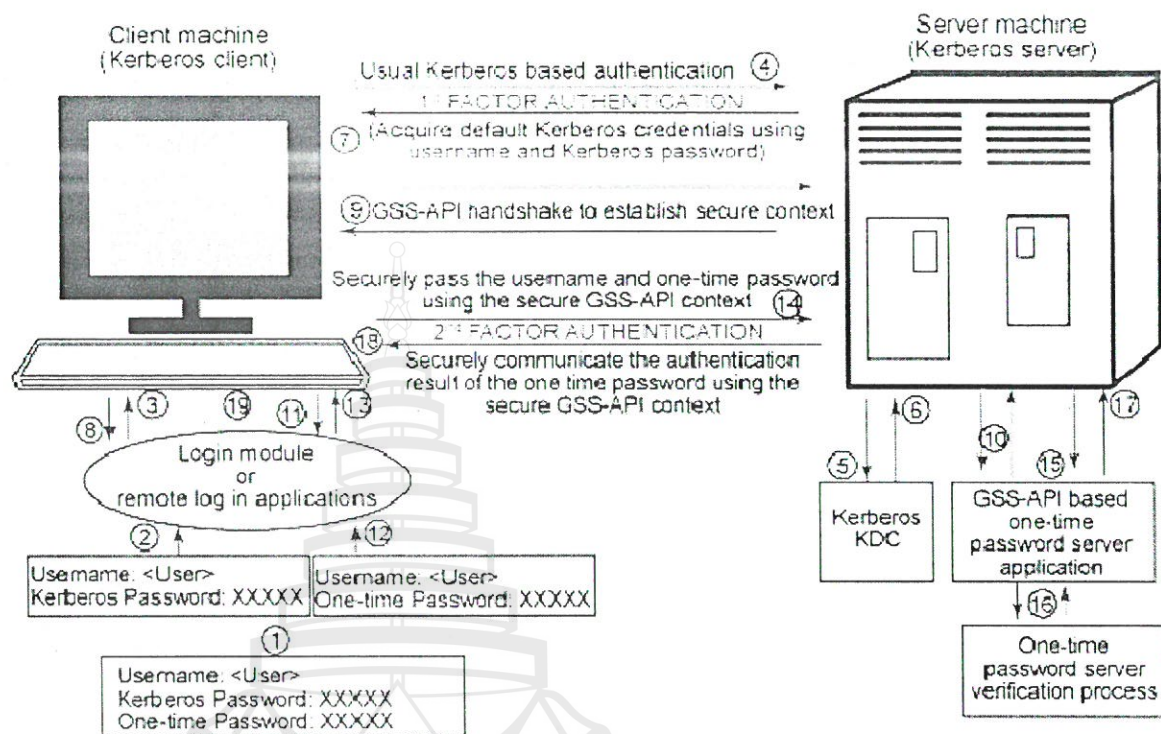


Figure 2.41 How Kerberos Work

2.22 Intrusion Detection System (IDS)

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. There are several ways to categorize an IDS:

- **misuse detection vs. anomaly detection:** in misuse detection, the IDS analyzes the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.
- **network-based vs. host-based systems:** in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.
- **passive system vs. reactive system:** in a passive system, the IDS detects a potential security breach, logs the information and signals an alert. In a reactive system, the IDS responds to the suspicious activity by logging off a

user or by reprogramming the firewall to block network traffic from the suspected malicious source.

Though they both relate to network security, an IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

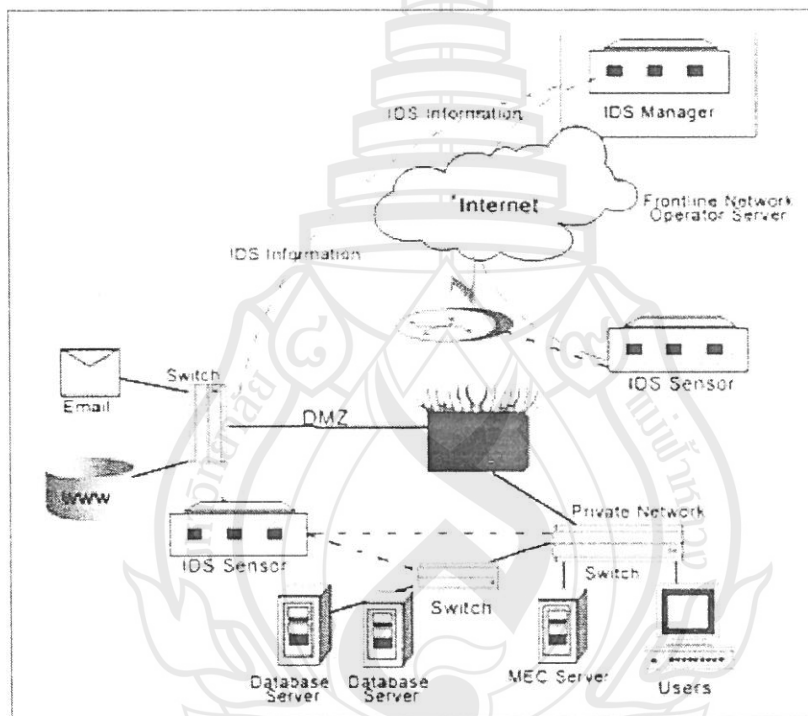


Figure 2.42 IDS Conception Model

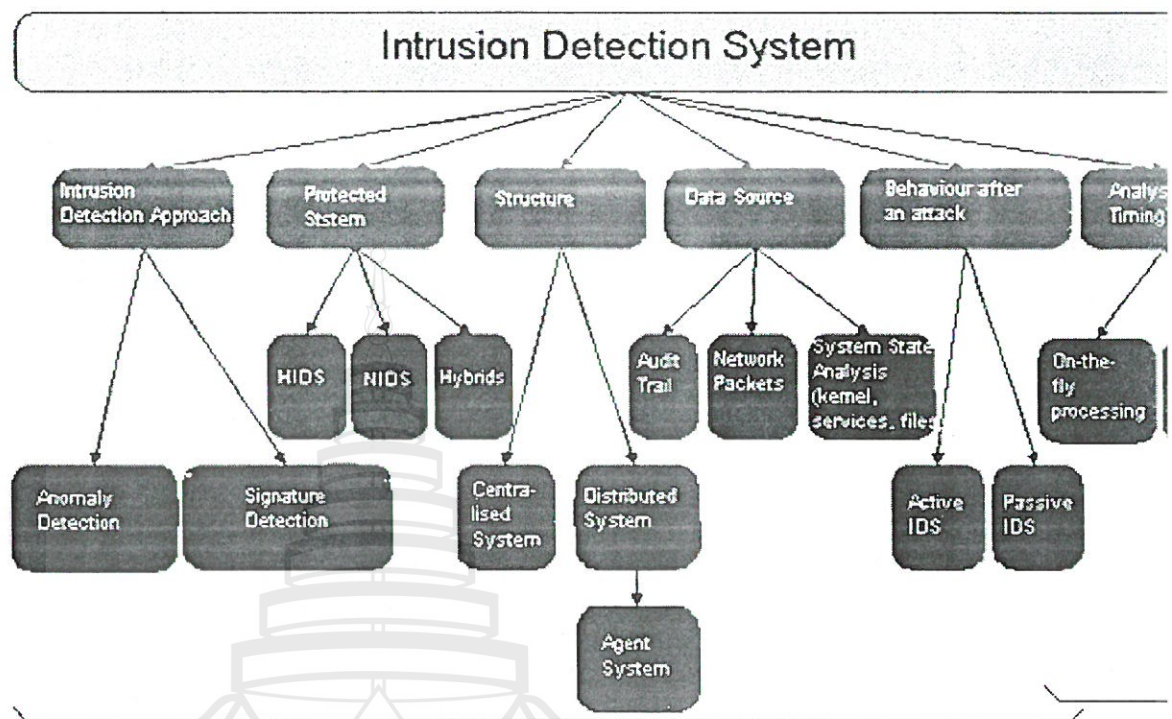


Figure 2.43 IDS Structure

2.22.1 Snort



Figure 2.44 Snort Logo

Snort is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and approximately 300,000 registered users, Snort has become the de facto standard for IPS.

Snort is a free, open source network intrusion detection and prevention system capable of performing real-time traffic analysis and packet logging on IP networks. Initially called a “lightweight” intrusion detection technology, Snort has evolved into a mature, feature-rich IPS technology that has become the de facto standard in intrusion detection and prevention. With nearly 4 million downloads and approximately 300,000 registered users Snort, it is the most widely deployed intrusion prevention technology in the world.

Snort can perform protocol analysis and content searching/matching. It can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port

scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. It uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients. Snort has three primary uses: a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc), or a full-blown network intrusion prevention system.

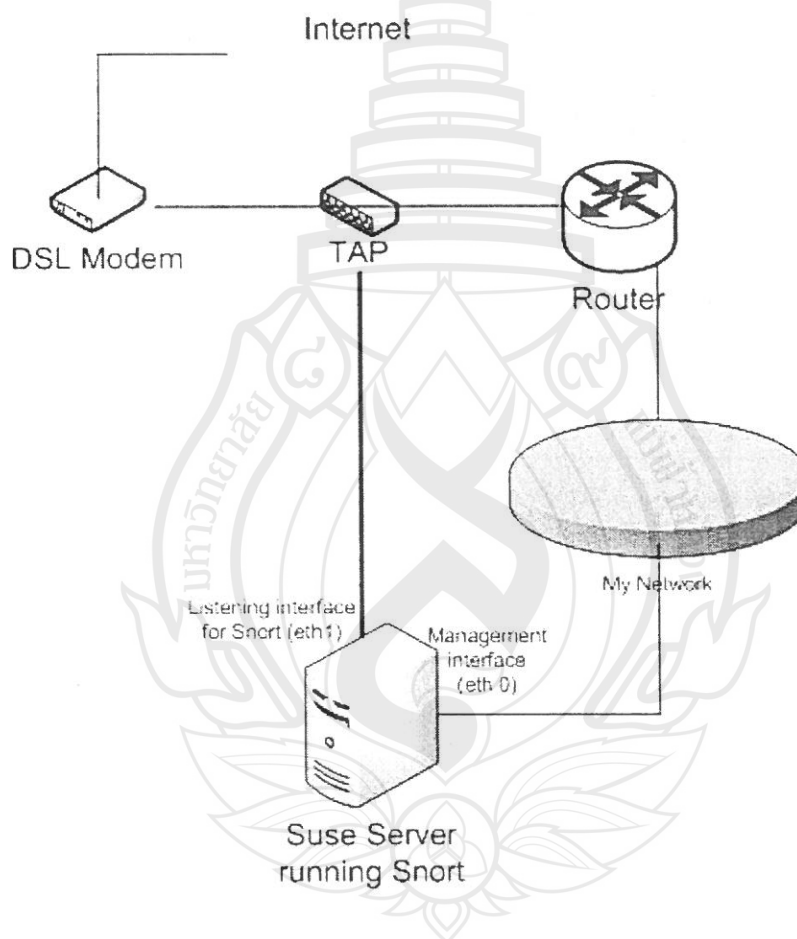


Figure 2.45 Snort Conception Model

2.23 The Switch Port Analyzer (SPAN)

The SPAN feature was introduced on switches because of a fundamental difference that switches have with hubs. When a hub receives a packet on one port, the hub sends out a copy of that packet on all ports except on the one where the hub received the packet. After a switch boots, it starts to build up a Layer 2 forwarding table on the basis of the source MAC address of the different packets that the switch

receives. After this forwarding table is built, the switch forwards traffic that is destined for a MAC address directly to the corresponding port.

For example, if you want to capture Ethernet traffic that is sent by host A to host B, and both are connected to a hub, just attach a sniffer to this hub. All other ports see the traffic between hosts A and B:

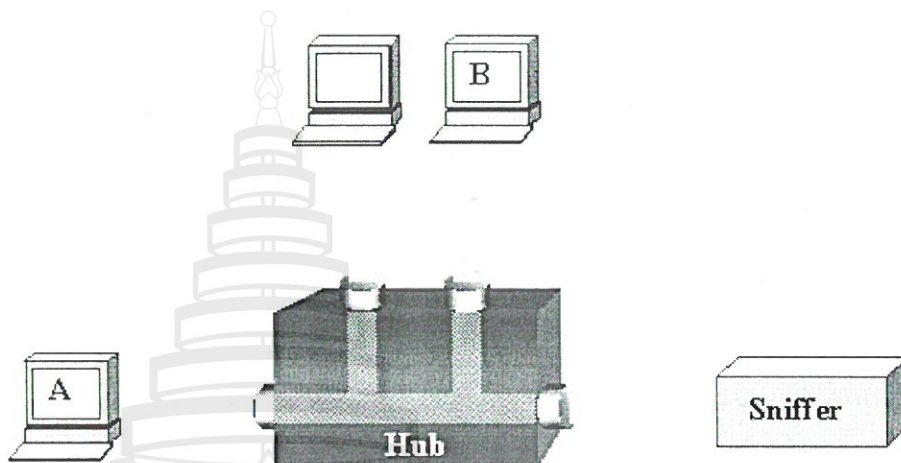


Figure 2.46 Hub Forward Traffic

On a switch, after the host B MAC address is learned, unicast traffic from A to B is only forwarded to the B port. Therefore, the sniffer does not see this traffic:

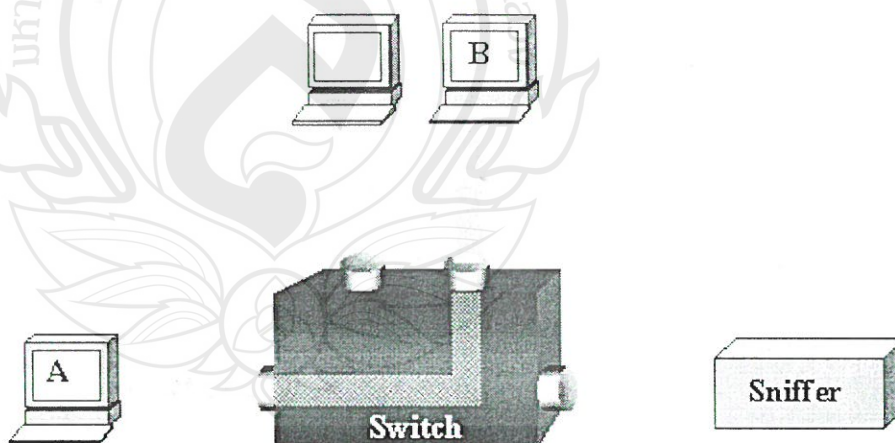


Figure 2.47 Switch Forward Traffic

In this configuration, the sniffer only captures traffic that is flooded to all ports, such as:

- Broadcast traffic
- Multicast traffic with CGMP or Internet Group Management Protocol (IGMP) snooping disabled
- Unknown unicast traffic

Unicast flooding occurs when the switch does not have the destination MAC in its content-addressable memory (CAM) table. The switch does not know where to send the traffic. The switch floods the packets to all the ports in the destination VLAN. An extra feature is necessary that artificially copies unicast packets that host A sends to the sniffer port:

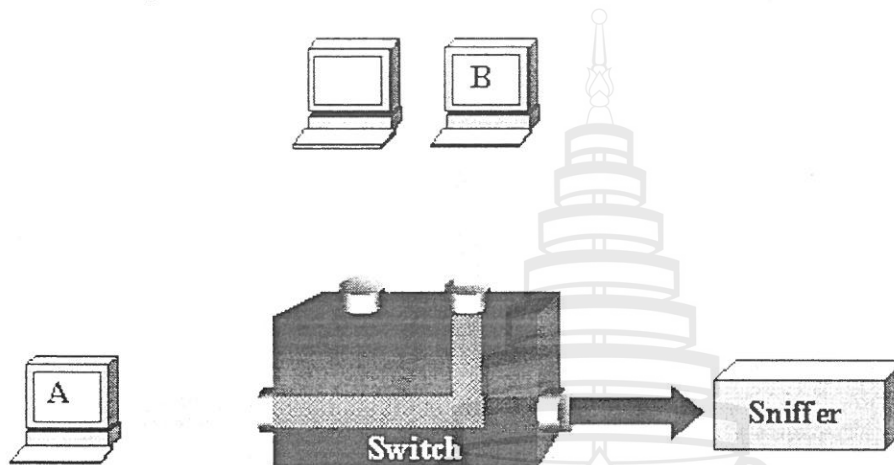


Figure 2.48 Unicast packet send from host A to sniffer

In this diagram, the sniffer is attached to a port that is configured to receive a copy of every packet that host A sends. This port is called a SPAN port. The other sections of this document describe how you can tune this feature very precisely in order to do more than just monitor a port.

SPAN Terminology

- **Ingress traffic**—Traffic that enters the switch.
- **Egress traffic**—Traffic that leaves the switch.
- **Source (SPAN) port** —A port that is monitored with use of the SPAN feature.
- **Source (SPAN) VLAN** —A VLAN whose traffic is monitored with use of the SPAN feature.
- **Destination (SPAN) port** —A port that monitors source ports, usually where a network analyzer is connected.
- **Reflector Port** —A port that copies packets onto an RSPAN VLAN.
- **Monitor port**—A monitor port is also a destination SPAN port in Catalyst 2900XL/3500XL/2950 terminology.

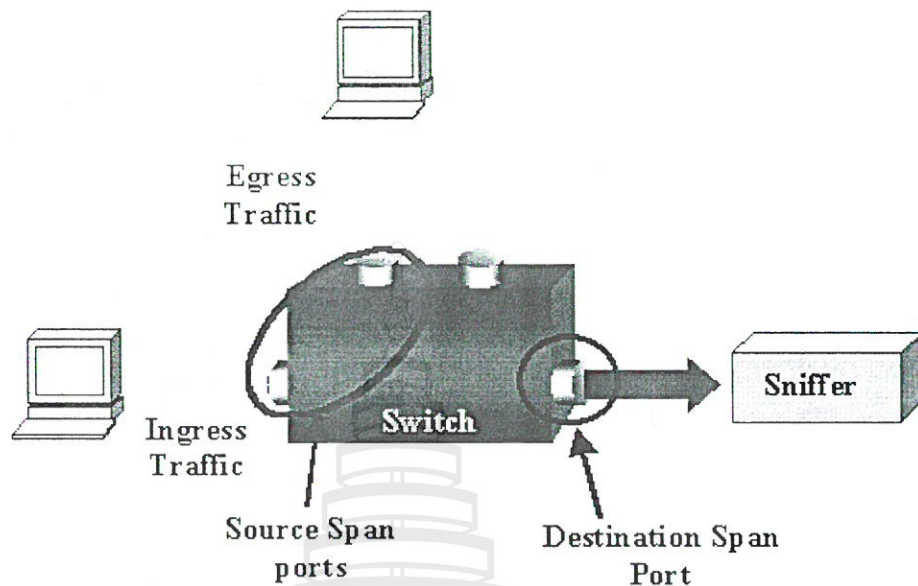


Figure 2.49 How SPAN Work

- **Local SPAN**—The SPAN feature is local when the monitored ports are all located on the same switch as the destination port. This feature is in contrast to Remote SPAN (RSPAN), which this list also defines.
- **Remote SPAN (RSPAN)**—Some source ports are not located on the same switch as the destination port. RSPAN is an advanced feature that requires a special VLAN to carry the traffic that is monitored by SPAN between switches. RSPAN is not supported on all switches. Check the respective release notes or configuration guide to see if you can use RSPAN on the switch that you deploy.
- **Port-based SPAN (PSPAN)**—The user specifies one or several source ports on the switch and one destination port.
- **VLAN-based SPAN (VSPAN)**—On a particular switch, the user can choose to monitor all the ports that belong to a particular VLAN in a single command.
- **ESpan**—This means enhanced SPAN version. This term has been used several times during the evolution of the SPAN in order to name additional features. Therefore, the term is not very clear. Use of this term is avoided in this document.
- **Administrative source**—A list of source ports or VLANs that have been configured to be monitored.
- **Operational source**—A list of ports that are effectively monitored. This list of ports can be different from the administrative source. For example, a port that is in shutdown mode can appear in the administrative source, but is not effectively monitored.

Characteristics of Source Port

A source port, also called a monitored port, is a switched or routed port that you monitor for network traffic analysis. In a single local SPAN session or RSPAN

source session, you can monitor source port traffic, such as received (Rx), transmitted (Tx), or bidirectional (both). The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs.

A source port has these characteristics:

- It can be any port type, such as EtherChannel, Fast Ethernet, Gigabit Ethernet, and so forth.
- It can be monitored in multiple SPAN sessions.
- It cannot be a destination port.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor. For EtherChannel sources, the monitored direction applies to all physical ports in the group.
- Source ports can be in the same or different VLANs.
- For VLAN SPAN sources, all active ports in the source VLAN are included as source ports.

VLAN Filtering

When you monitor a trunk port as a source port, all VLANs active on the trunk are monitored by default. You can use VLAN filtering in order to limit SPAN traffic monitoring on trunk source ports to specific VLANs.

- VLAN filtering applies only to trunk ports or to voice VLAN ports.
- VLAN filtering applies only to port-based sessions and is not allowed in sessions with VLAN sources.
- When a VLAN filter list is specified, only those VLANs in the list are monitored on trunk ports or on voice VLAN access ports.
- SPAN traffic coming from other port types is not affected by VLAN filtering, which means that all VLANs are allowed on other ports.
- VLAN filtering affects only traffic forwarded to the destination SPAN port and does not affect the switching of normal traffic.
- You cannot mix source VLANs and filter VLANs within a session. You can have source VLANs or filter VLANs, but not both at the same time.

Characteristics of Source VLAN

VSPAN is the monitoring of the network traffic in one or more VLANs. The SPAN or RSPAN source interface in VSPAN is a VLAN ID, and traffic is monitored on all the ports for that VLAN.

VSPAN has these characteristics:

- All active ports in the source VLAN are included as source ports and can be monitored in either or both directions.

- On a given port, only traffic on the monitored VLAN is sent to the destination port.
- If a destination port belongs to a source VLAN, it is excluded from the source list and is not monitored.
- If ports are added to or removed from the source VLANs, the traffic on the source VLAN received by those ports is added to or removed from the sources that are monitored.
- You cannot use filter VLANs in the same session with VLAN sources.
- You can monitor only Ethernet VLANs.

Characteristics of Destination Port

Each local SPAN session or RSPAN destination session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports and VLANs.

A destination port has these characteristics:

- A destination port must reside on the same switch as the source port (for a local SPAN session).
- A destination port can be any Ethernet physical port.
- A destination port can participate in only one SPAN session at a time. A destination port in one SPAN session cannot be a destination port for a second SPAN session.
- A destination port cannot be a source port.
- A destination port cannot be an EtherChannel group.

Note: From Cisco IOS Software Release 12.2(33)SXH and later, PortChannel interface can be a destination port. Destination EtherChannels do not support the Port Aggregation Control Protocol (PAgP) or Link Aggregation Control Protocol (LACP) EtherChannel protocols; only the on mode is supported, with all EtherChannel protocol support disabled.

- A destination port can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group has been specified as a SPAN source. The port is removed from the group while it is configured as a SPAN destination port.
- The port does not transmit any traffic except that traffic required for the SPAN session unless learning is enabled. If learning is enabled, the port also transmits traffic directed to hosts that have been learned on the destination port.
- The state of the destination port is up/down by design. The interface shows the port in this state in order to make it evident that the port is currently not usable as a production port.
- If ingress traffic forwarding is enabled for a network security device. The destination port forwards traffic at Layer 2.

- A destination port does not participate in spanning tree while the SPAN session is active.
- When it is a destination port, it does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).
- A destination port that belongs to a source VLAN of any SPAN session is excluded from the source list and is not monitored.
- A destination port receives copies of sent and received traffic for all monitored source ports. If a destination port is oversubscribed, it can become congested. This congestion can affect traffic forwarding on one or more of the source ports.

Characteristics of Reflector Port

The reflector port is the mechanism that copies packets onto an RSPAN VLAN. The reflector port forwards only the traffic from the RSPAN source session with which it is affiliated. Any device connected to a port set as a reflector port loses connectivity until the RSPAN source session is disabled.

The reflector port has these characteristics:

- It is a port set to loopback.
- It cannot be an EtherChannel group, it does not trunk, and it cannot do protocol filtering.
- It can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group is specified as a SPAN source. The port is removed from the group while it is configured as a reflector port.
- A port used as a reflector port cannot be a SPAN source or destination port, nor can a port be a reflector port for more than one session at a time.
- It is invisible to all VLANs.
- The native VLAN for looped-back traffic on a reflector port is the RSPAN VLAN.
- The reflector port loops back untagged traffic to the switch. The traffic is then placed on the RSPAN VLAN and flooded to any trunk ports that carry the RSPAN VLAN.
- Spanning tree is automatically disabled on a reflector port.
- A reflector port receives copies of sent and received traffic for all monitored source ports.

2.24 Remote Switch Prot Analyzer (RSPAN)

RSPAN allows you to monitor source ports that are spread all over a switched network, not only locally on a switch with SPAN. This feature appears in CatOS 5.3 in the Catalyst 6500/6000 Series Switches and is added in the Catalyst 4500/4000 Series Switches in CatOS 6.3 and later. The functionality works exactly as a regular SPAN session. The traffic that is monitored by SPAN is not directly copied to the destination port, but flooded into a special RSPAN VLAN. The destination port can

then be located anywhere in this RSPAN VLAN. There can even be several destination ports. This diagram illustrates the structure of an RSPAN session:

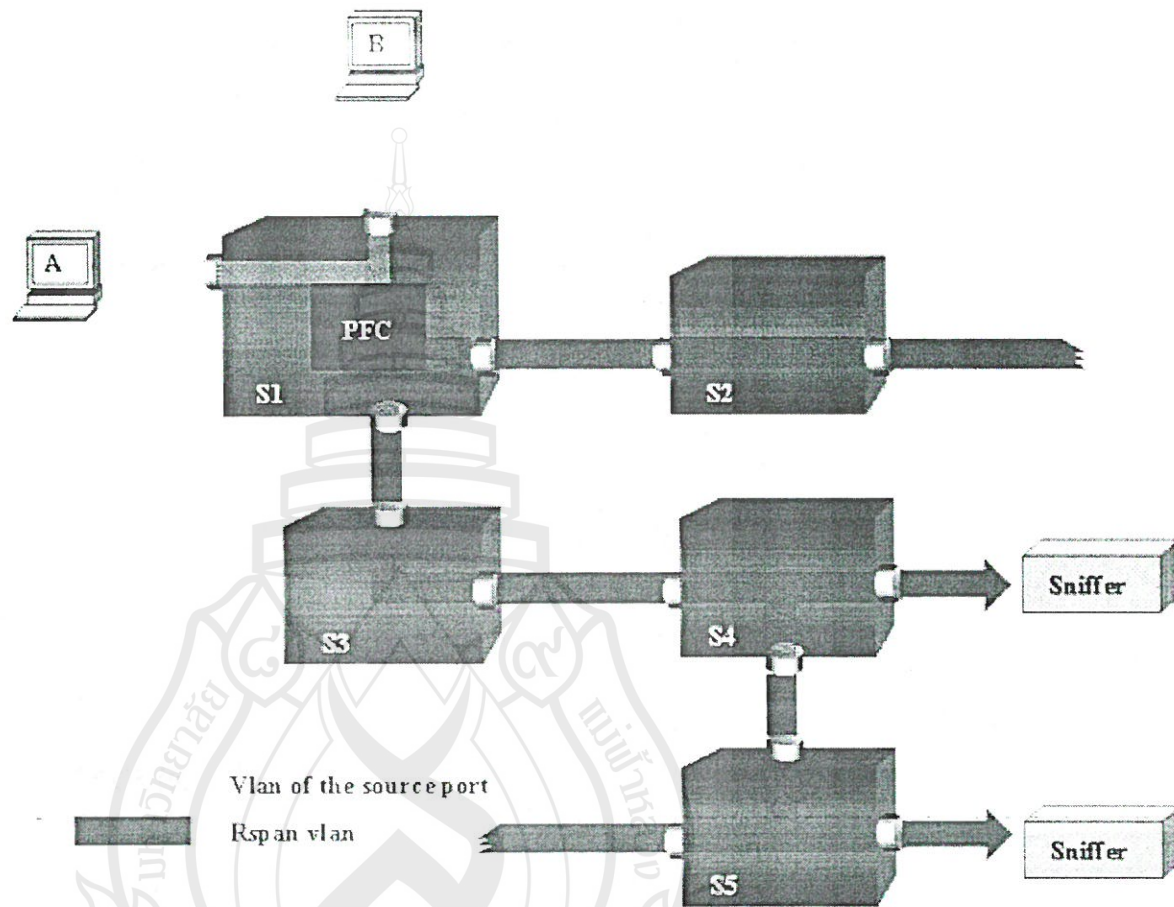


Figure 2.50 Structure of an RSPAN Session

In this example, you configure RSPAN to monitor traffic that host A sends. When A generates a frame that is destined for B, the packet is copied by an application-specific integrated circuit (ASIC) of the Catalyst 6500/6000 Policy Feature Card (PFC) into a predefined RSPAN VLAN. From there, the packet is flooded to all other ports that belong to the RSPAN VLAN. All the interswitch links that are drawn here are trunks, which is a requirement for RSPAN. The only access ports are destination ports, where the sniffers are connected (here, on S4 and S5).

These are a few remarks on this design:

- S1 is called a source switch. Packets only enter the RSPAN VLAN in switches that are configured as RSPAN source. Currently, a switch can only be the source for one RSPAN session, which means that a source switch can only feed one RSPAN VLAN at a time.
- S2 and S3 are intermediate switches. They are not RSPAN sources and do not have destination ports. A switch can be intermediate for any number of RSPAN sessions.

- S4 and S5 are destination switches. Some of their ports are configured to be destination for an RSPAN session. Currently, a Catalyst 6500/6000 can have up to 24 RSPAN destination ports, for one or several different sessions. You can also notice that S4 is both a destination and an intermediate switch.
- You can see that RSPAN packets are flooded into the RSPAN VLAN. Even switches that are not on the path to a destination port, such as S2, receive the traffic for the RSPAN VLAN. You can find it useful to prune this VLAN on such S1-S2 links.
- In order to achieve the flooding, learning is disabled on the RSPAN VLAN.
- In order to prevent loops, the STP has been maintained on the RSPAN VLAN. Therefore, RSPAN cannot monitor Bridge Protocol Data Units (BPDUs).



CHAPTER 3

THEORY AND PRINCIPLE OF HARDWARE TO BE USED

3.1 Router

A router is an electronic device used to forward data between computer networks. More technically, a router is a networking device whose software and hardware are usually tailored to the tasks of routing and forwarding information. Routers connect two or more logical subnets, which do not necessarily map one-to-one to the physical interfaces of the router.^[1] The term "layer 3 switching" is often used interchangeably with routing, but switch is a general term without a rigorous technical definition. In marketing usage, a switch is generally optimized for Ethernet LAN interfaces and may not have other physical interface types. In comparison, the network hub (predecessor of the "switch" or "switching hub") does not do any routing instead every packet it receives on one network line gets forwarded to all the other network lines.

Routers operate in two different planes:

- Control plane, in which the router learns the outgoing interface that is most appropriate for forwarding specific packets to specific destinations,
- Forwarding plane, which is responsible for the actual process of sending a packet received on a logical interface to an outbound logical interface.

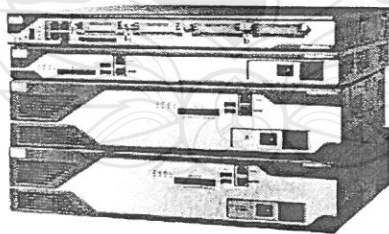


Figure 3.1 Cisco router

3.2 Layer 2 switch

The network switch, packet switch (or just switch) plays an integral part in most Ethernet local area networks or LANs. Mid-to-large sized LANs contain a number of linked managed switches. Small office/home office (SOHO) applications typically use a single switch, or an all-purpose converged device such as gateway access to small office/home broadband services such as DSL router or cable Wi-Fi router. In most of these cases, the end user device contains a router and components that interface to the particular physical broadband technology. User devices may also include a telephone interface to VoIP.

In the context of a standard 10/100 Ethernet switch, a switch operates at the data-link layer of the OSI model to create a different collision domain per switch port. If you have 4 computers A/B/C/D on 4 switch ports, then A and B can transfer data between them as well as C and D at the same time, and they will never interfere with each others' conversations. In the case of a "hub" then they would all have to share the bandwidth and run in Half duplex. The result is that there would be collisions and retransmissions. Using a switch is called micro-segmentation. It allows you to have dedicated bandwidth on point to point connections with every computer and to therefore run in Full duplex with no collisions.

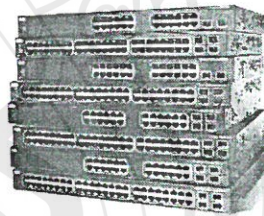


Figure 3.2 Cisco layer 2 switch

3.3 PIX firewall

The PIX runs a custom-written proprietary operating system originally called Finesse (Fast InterNEt Server Executive), but now the software is known simply as PIX OS. It is classified as a network layer firewall with stateful inspection, although technically the PIX would more precisely be called a Layer 4, or Transport Layer Firewall, as its access is not restricted to Network Layer routing, but socket based connections (a port and an IP Address - Port communications occur at Layer 4). By default it allows internal connections out (outbound traffic), and only allows inbound traffic that is a response to a valid request or is allowed by an Access Control List (ACL) or a *conduit*. The PIX can be configured to perform many functions including network address translation (NAT) and port address translation (PAT), as well as being a virtual private network (VPN) endpoint appliance.

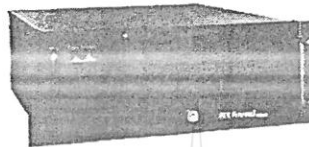


Figure 3.3 Cisco PIX firewall

3.4 Intrusion Detection System (IDS)

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

There are several ways to categorize an IDS:

- **Misuse detection vs. anomaly detection:** in misuse detection, the IDS analyze the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.
- **Network-based vs. host-based systems:** in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. In a host-based system, the IDS examines the activity on each individual computer or host.
- **Passive system vs. reactive system:** in a passive system, the IDS detects a potential security breach, logs the information and signals an alert. In a reactive system, the IDS respond to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

Though they both relate to network security, an IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.



Figure 3.4 Cisco IDS



CHAPTER 4

EXPERIMENTAL DESIGN

4.1 Network security design

4.1.1 First secure topology design

This topology use PIX firewall to protect inside network from outside network. DMZ is allowed outside network .to access HTTP server. VPN tunneling and IPSec tunnel mode involve establishing and maintaining a logical network connection, support authentication and encryption to keep the tunnels secure between Brach office and GW router. EIGRP routing protocol has used on R1 and R2 router. Network Time Protocol (NTP) has used to synchronize timekeeping among a set of distributed time servers and clients. Inside Server is installed AAA Radius server to manage user profiles for authentication (verifying user name and password) for secure R1 and R2 router when enter username and password.

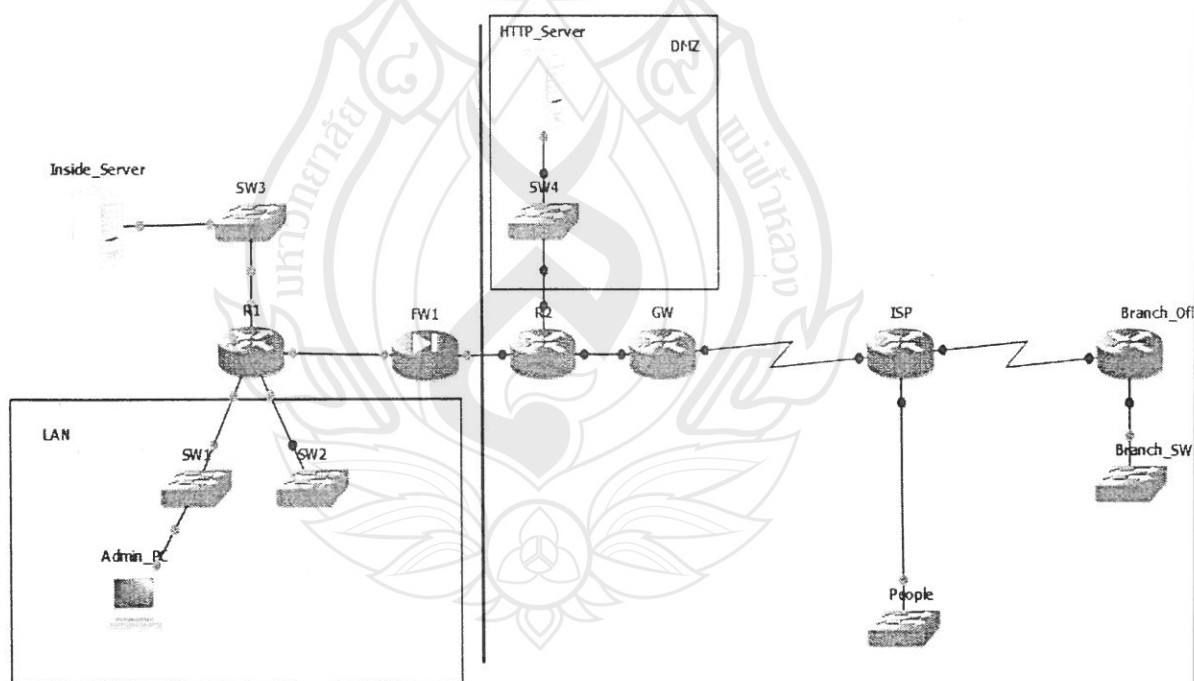


Figure 4.1 First secure topology design

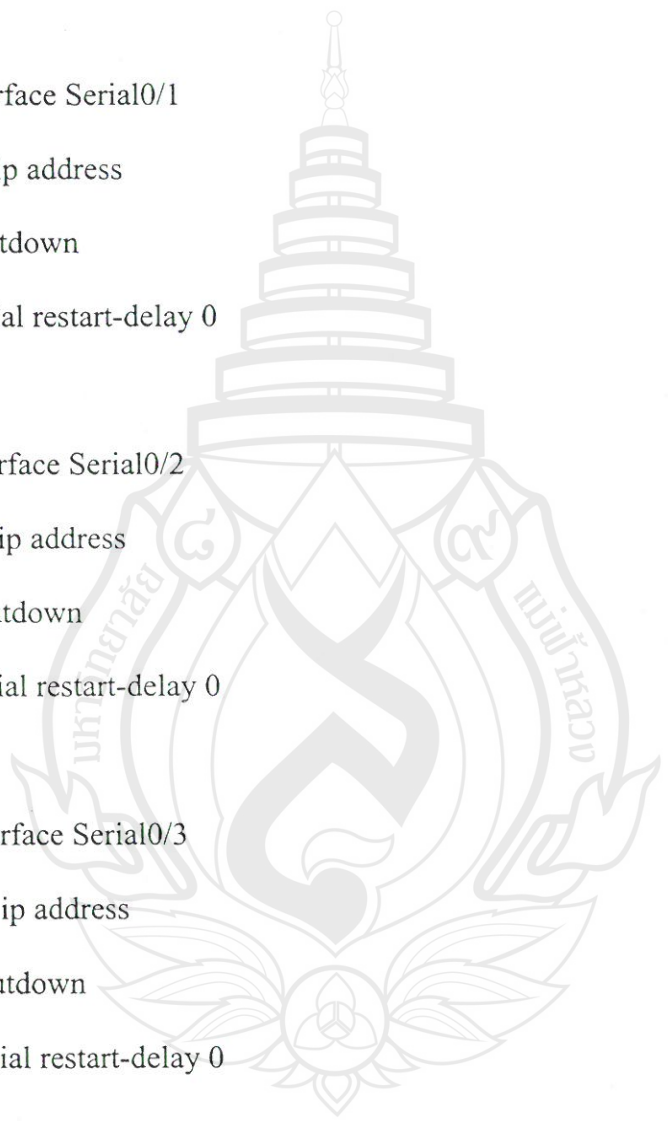
4.1.1.1 Show running-configure.

Table 4.1 First secure network shows running configure.

<u>Brach Office</u>
!
version 12.4
service timestamps debug datetime msec
<i>// Indicates that the timestamp should be applied to debugging messages include milliseconds</i>
service timestamps log datetime msec
<i>// Indicates that the timestamp should be applied to system logging messages include milliseconds</i>
no service password-encryption
!
hostname Branch_Office
<i>// Router named Brach_Office.</i>
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef

```
crypto isakmp policy 10.  
  
encr aes  
  
// Define Internet Key Exchange (IKE) policy  
  
authentication pre-share  
  
group 2  
  
// pre-share authentication  
  
crypto isakmp key IPSEC address 192.168.100.1  
  
// Specify the shared secret.  
  
!  
  
!  
  
crypto ipsec transform-set TUNNEL esp-aes esp-sha-hmac  
  
// Define the IPSec transform set.  
  
!  
  
crypto ipsec profile TUNNEL  
  
set transform-set TUNNEL  
  
// Create an IPSec profile to be applied dynamically to the GRE over IPSec tunnels.  
  
interface Tunnel0  
  
ip address 192.168.200.2 255.255.255.0  
  
tunnel source Serial0/0  
  
tunnel destination 192.168.100.1  
  
tunnel mode ipsec ipv4  
  
tunnel protection ipsec profile TUNNEL  
  
// This is the configure of mGRE interface for dynamic GRE tunnels.  
  
!
```

```
interface Serial0/0
ip address 10.1.1.1 255.255.255.0
serial restart-delay 0
!
interface Serial0/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial0/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial0/3
no ip address
shutdown
serial restart-delay 0
!
interface FastEthernet1/0
ip address 10.1.2.1 255.255.255.0
duplex auto
speed auto
!
```




```
router eigrp 10

network 10.1.2.0 0.0.0.255

network 192.168.200.0

auto-summary

// This is configure of EIGRP routing protocol number 10.

!

ip http server

no ip http secure-server

ip route 192.168.100.1 255.255.255.255 10.1.1.2

// This is static routing.

!

!

control-plane

!

!

line con 0

exec-timeout 0 0

logging synchronous

// log the messages to the console without interfering with your work in the console in Cisco IOS

line aux 0

line vty 0 4

login

end
```



ISP

```
!  
version 12.4  
service timestamps debug datetime msec  
  
// Indicates that the timestamp should be applied to debugging messages include  
milliseconds  
  
service timestamps log datetime msec  
  
// Indicates that the timestamp should be applied to logging messages include  
milliseconds  
  
no service password-encryption  
!  
hostname ISP  
  
// Router named ISP.  
  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
memory-size iomem 5  
!  
!  
ip cef  
!  
!  
interface Serial0/0  
ip address 192.168.100.2 255.255.255.0  
serial restart-delay 0  
!  
interface Serial0/1  
ip address 10.1.1.2 255.255.255.0  
serial restart-delay 0  
!  
interface Serial0/2  
no ip address  
shutdown  
serial restart-delay 0  
!  
interface Serial0/3
```

```

no ip address
shutdown
serial restart-delay 0
!
interface FastEthernet1/0
ip address 10.10.10.1 255.255.255.0
duplex auto
speed auto
!
router ospf 10
log-adjacency-changes

// send a syslog message when an OSPF neighbor goes up or down.

network 10.10.10.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0

// Configure of OSPF routing protocol in area 10.

!
ip http server
no ip http secure-server
!

!
control-plane
!

!
line con 0
exec-timeout 0 0
logging synchronous

// log the messages to the console without interfering with your work in the console in Cisco IOS

line aux 0
line vty 0 4
login
!
!
end

```

Gateway

```
!
```

```
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds

service timestamps log datetime msec

// Indicates that the timestamp should be applied to logging messages include milliseconds

no service password-encryption
!
hostname GW

// Router named GW.

!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef

!
!
crypto isakmp policy 10
  encr aes

// Define Internet Key Exchange (IKE) policy

  authentication pre-share
  group 2

// pre-share authentication

crypto isakmp key IPSEC address 10.1.1.1

// Specify the shared secret.
!
!
crypto ipsec transform-set TUNNEL esp-aes esp-sha-hmac
```



```
// Define the IPsec transform set.

!
crypto ipsec profile TUNNEL
set transform-set TUNNEL

// Create an IPsec profile to be applied dynamically to the GRE over IPsec tunnels.

!
!
interface Tunnel0
ip address 192.168.200.1 255.255.255.0
tunnel source Serial0/0
tunnel destination 10.1.1.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile TUNNEL

// This is the configure of mGRE interface for dynamic GRE tunnels.

!
interface Serial0/0
ip address 192.168.100.1 255.255.255.0
serial restart-delay 0
!
interface Serial0/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial0/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial0/3
no ip address
shutdown
serial restart-delay 0
!
interface FastEthernet1/0
ip address 192.168.2.2 255.255.255.0
duplex auto
speed auto
!
router eigrp 10
network 192.168.2.0
network 192.168.200.0
```

```

auto-summary

// Configure of EIGRP routing protocol in number 10.

router ospf 10
log-adjacency-changes

// send a syslog message when an OSPF neighbor goes up or down.

network 192.168.2.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0

// Configure of OSPF routing protocol in area 10.

!
ip http server
no ip http secure-server
ip route 10.1.1.1 255.255.255.255 192.168.100.2

// This is static routing.

!
!
control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous

// log the messages to the console without interfering with your work in the console in Cisco IOS

line aux 0
line vty 0 4
login
!
!
end

```

Router 1

```

!
! No configuration change since last restart

```

```
! NVRAM config last updated at 00:08:04 UTC Fri Mar 1 2002 by cisco
!
version 12.4
no service pad

// Disable Packet Assembler/Disassembler (PAD) service, which is used for X.25 networks.

service tcp-keepalives-in
service tcp-keepalives-out

// Enable the generation of keepalive packets on idle incoming and outbound connections initiated from the device.

service timestamps debug datetime msec localtime show-timezone

// Indicates that the timestamp should be applied to debugging messages. Include milliseconds, relative to the local time zone, and time zone name in the time stamp.

service timestamps log datetime msec localtime show-timezone

// Indicates that the timestamp should be applied to logging messages. Include milliseconds, relative to the local time zone, and time zone name in the time stamp.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the router's NVRAM configuration files.

service sequence-numbers

// Insert sequence numbers into log files.

!
hostname R1

// Router named R1

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

security passwords min-length 6
```

// Configure the number of minimum password characters.

logging buffered 4096 debugging

// Configure the router to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit messages based on critical conditions.

enable secret 5 \$1\$7EOw\$SL9SuUt8FMBYRxRpThyjep/

enable password 7 1314001719181D

!

aaa new-model

// Enable AAA access control model.

!

!

aaa authentication login default group radius local

aaa authentication login local_auth local

aaa authentication login localauth local

aaa authentication ppp default if-needed group radius local

aaa authorization exec default group radius local

aaa authorization network default group radius local

aaa accounting delay-start

aaa accounting exec default start-stop group radius

aaa accounting network default start-stop group radius

!

aaa session-id common

// Configure of AAA RADIUS.

memory-size iomem 5

no ip source-route

// Disable IP source routing.

no ip gratuitous-arps

// disable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in a local pool.

!

!


```
ip cef
ip domain name test.com
!
!
no ip bootp server
ip inspect audit-trail

// Turn on CBAC audit trail messages, which will be displayed on the console after
each CBAC session closes.

ip inspect udp idle-time 1800

// Specify the UCP idle timeout.

ip inspect dns-timeout 7

// Specify the DNS idle timeout.

ip inspect tcp idle-time 14400

// Specify the TCP idle timeout.

ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600

// Define a set of inspection rules to override the global idle timeouts for the specified
protocol.

login block-for 3 attempts 3 within 10

// Configure your Cisco IOS device for login parameters that help provide DoS
detection.

!
!
key chain SECRET
key 10
  key-string 7 0037362531692E

// Specifies the key in encrypted form.
```

```
!  
!  
username cisco password 7 124814450558095038  
  
// Define username cisco and password.  
  
archive  
log config  
logging enable  
!  
!  
ip ssh time-out 60  
ip ssh authentication-retries 2  
  
// Configure Secure Shell (SSH) time out and the number of attempts after which the  
interface is reset.  
  
!  
interface Loopback0  
ip address 172.16.251.1 255.255.255.255  
!  
interface FastEthernet0/0  
ip address 172.16.1.1 255.255.255.0  
no ip redirects  
no ip unreachable  
no ip proxy-arp  
duplex auto  
speed auto  
no mop enabled  
!  
interface FastEthernet1/0  
ip address 172.16.200.2 255.255.255.0  
no ip redirects  
no ip unreachable  
no ip proxy-arp  
ip authentication mode eigrp 10 md5  
ip authentication key-chain eigrp 10 SECRET  
duplex auto  
speed auto  
no mop enabled  
!  
interface FastEthernet2/0  
no ip address  
no ip redirects  
no ip unreachable  
no ip proxy-arp
```

```

duplex auto
speed auto
no mop enabled
!
interface FastEthernet2/0.1
encapsulation dot1Q 1 native
ip address 172.16.253.2 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
!
interface FastEthernet2/0.99
encapsulation dot1Q 99
ip address 172.16.99.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
!
interface FastEthernet3/0
no ip address
no ip redirects
no ip unreachable
no ip proxy-arp
shutdown
duplex auto
speed auto
no mop enabled
!
router eigrp 10
passive-interface Loopback0

// Configure loopback 0 as a passive interface.

network 172.16.0.0
auto-summary
no eigrp log-neighbor-warnings

// Disable the logging of EIGRP neighbor warning messages.

!
no ip http server
no ip http secure-server
!
!
ip access-list extended autosec_firewall_acl
permit udp any any eq bootpc
deny ip any any

```

// Set an ACL extended rule to permit UDP bootstrap protocol client (bootpc) packets from any source to any destination.

logging trap debugging

// Limit the number of messages sent to the syslog servers at the debugging level.
logging facility local2

// Set the logging facility at critical level.

access-list 100 permit udp any any eq bootpc

// This ACL permits UDP bootstrap protocol client (bootpc) packets from any source to any destination.

no cdp run

// Disable CDP for the whole router

!
!

radius-server host 172.16.1.10 auth-port 1812 acct-port 1813 key 7
00150403164F1213062E5C

// Specify a RADIUS server host and encryption key values on a per-server basis.

!

control-plane

!

banner motd *^* Authorised Access only *^*

// The syntax for the banner.

!

line con 0

exec-timeout 0 0

logging synchronous

transport output telnet

line aux 0

transport output telnet

line vty 0 4

transport input telnet ssh

!

ntp authentication-key 1 md5 0832494D1B1C11 7

// The key string for NTP authentication key 1.

```

ntp authenticate

// Enables NTP authentication.

ntp master 1

// Makes the system an authoritative NTP server.
!
end

```

Router 2

```

!
version 12.4
no service pad

// Disable Packet Assembler/Disassembler (PAD) service, which is used for X.25
networks.

service tcp-keepalives-in
service tcp-keepalives-out

// Enable the generation of keepalive packets on idle incoming and outbound
connections initiated from the device.

service timestamps debug datetime msec localtime show-timezone

// Indicates that the timestamp should be applied to debugging messages. Include
milliseconds, relative to the local time zone, and time zone name in the time stamp.

service timestamps log datetime msec localtime show-timezone

// Indicates that the timestamp should be applied to logging messages. Include
milliseconds, relative to the local time zone, and time zone name in the time stamp.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the router's NVRAM configuration
files.

service sequence-numbers

// Insert sequence numbers into log files.

!
hostname R2

```



```
// Router named R2

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts
security passwords min-length 6

// Configure the number of minimum password characters.
logging buffered 4096 debugging

// Configure the router to send buffered logging of its events to the memory.
logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit
messages based on critical conditions.

enable secret 5 $1$9PBU$G0xJ2p9QZJG27m9C0IJAV0
enable password 7 00150403164F12

// Enable password in encryption form.

!
aaa new-model

// Enable AAA access control model.

!
!
aaa authentication login local_auth local

// Enables AAA local authentication.

!
aaa session-id common
memory-size iomem 5
no ip source-route

// Disable ip source routing.
no ip gratuitous-arps
```

// disable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in a local pool.

```
!
!
ip cef
ip domain name test.com
!
!
no ip bootp server
ip inspect audit-trail
```

// Turn on CBAC audit trail messages, which will be displayed on the console after each CBAC session closes.

```
ip inspect udp idle-time 1800
```

// Specify the UCP idle timeout.

```
ip inspect dns-timeout 7
```

// Specify the DNS idle timeout.

```
ip inspect tcp idle-time 14400
```

// Specify the TCP idle timeout.

```
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
```

// Define a set of inspection rules to override the global idle timeouts for the specified protocol.

```
login block-for 3 attempts 3 within 10
```

// Configure your Cisco IOS device for login parameters that help provide DoS detection.

```
!
!
```

```
username cisco password 7 101F184B1244175F1E
```

```
// Define username cisco and password.
```

```
archive  
log config  
logging enable
```

```
!
```

```
!
```

```
ip ssh time-out 60
```

```
ip ssh authentication-retries 2
```

```
// Configure Secure Shell (SSH) time out and the number of attempts after which the  
interface is reset.
```

```
!
```

```
!
```

```
interface Loopback0
```

```
no ip address
```

```
shutdown
```

```
!
```

```
interface FastEthernet0/0
```

```
ip address 192.168.1.2 255.255.255.0
```

```
no ip redirects
```

```
no ip unreachable
```

```
no ip proxy-arp
```

```
duplex auto
```

```
speed auto
```

```
no mop enabled
```

```
!
```

```
interface FastEthernet1/0
```

```
ip address 192.168.80.1 255.255.255.0
```

```
no ip redirects
```

```
no ip unreachable
```

```
no ip proxy-arp
```

```
duplex auto
```

```
speed auto
```

```
no mop enabled
```

```
!
```

```
interface FastEthernet2/0
```

```
ip address 192.168.2.1 255.255.255.0
```

```
no ip redirects
```

```
no ip unreachable
```

```
no ip proxy-arp
```

```
duplex auto
```

```
speed auto
```

```
no mop enabled
```

```

!
router eigrp 10
 network 192.168.0.0 0.0.255.255
 auto-summary
 no eigrp log-neighbor-warnings

// Configure EIGRP routing protocol number 10.
// Disable the logging of EIGRP neighbor warning messages.

!
router ospf 10
 log-adjacency-changes
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.80.0 0.0.0.255 area 0

// Configure OSPF routing protocol in area 10.
// send a syslog message when an OSPF neighbor goes up or down.

!
no ip http server
no ip http secure-server
!
!
ip access-list extended autosec_firewall_acl
 permit udp any any eq bootpc
 deny ip any any

// Set an ACL extended rule to permit UDP bootstrap protocol client (bootpc) packets
from any source to any destination.

logging trap debugging

// Limit the number of messages sent to the syslog servers at the debugging level.

logging facility local2

// Set the logging facility at critical level.

access-list 100 permit udp any any eq bootpc

// Set an ACL rule to permit UDP bootstrap protocol client (bootpc) packets from any
source to any destination.

no cdp run
// Disable CDP for the whole router

!

```

```

!
control-plane
!
!
banner motd ^ Authorised Access only ^

// The syntax for the banner.

!
line con 0
exec-timeout 0 0
logging synchronous
login authentication local_auth
transport output telnet
line aux 0
login authentication local_auth
transport output telnet
line vty 0 4
login authentication local_auth
transport input telnet ssh
!
!
end

```

Switch 1

```

!
! No configuration change since last restart
! NVRAM config last updated at 00:08:01 UTC Fri Mar 1 2002 by cisco
!
version 12.4
no service pad

// Disable Packet Assembler/Disassembler (PAD) service, which is used for X.25 networks.

service tcp-keepalives-in
service tcp-keepalives-out

// Enable the generation of keepalive packets on idle incoming and outbound connections initiated from the device.

service timestamps debug datetime msec localtime show-timezone

// Indicates that the timestamp should be applied to debugging messages. Include milliseconds, relative to the local time zone, and time zone name in the time stamp.

```



```
service timestamps log datetime msec localtime show-timezone
```

// Indicates that the timestamp should be applied to logging messages. Include milliseconds, relative to the local time zone, and time zone name in the time stamp.

```
service password-encryption
```

// Encrypts the Cisco IOS passwords stored in the router's NVRAM configuration files.

```
service sequence-numbers
```

// Insert sequence numbers into log files.

```
!  
hostname SW1
```

// Switch named SW1.

```
!  
boot-start-marker  
boot-end-marker  
!
```

```
security authentication failure rate 10 log
```

// Configure the number of allowable unsuccessful login attempts.

```
security passwords min-length 6
```

// Configure the number of minimum password characters.

```
logging buffered 4096 debugging
```

// Configure the router to send buffered logging of its events to the memory.

```
logging console critical
```

// Send system logging (syslog) messages to all available TTY lines and limit messages based on critical conditions.

```
enable secret 5 $1$8A5J$XhtVaSCWf131OL8GoeiKP1
```

```
enable password 7 095D590C0B110E
```

// Enable password in encryption form.

```
!  
aaa new-model
```

// Enable AAA access control model.

```

!
!
aaa authentication login default group radius local
aaa authentication login local_auth local
aaa authentication login localauth local
aaa authentication ppp default if-needed group radius local
aaa authentication dot1x default group radius
aaa authorization exec default group radius local
aaa authorization network default group radius local
aaa accounting delay-start
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
!
aaa session-id common

// Configure of AAA RADIUS.

memory-size iomem 5
no ip source-route

// Disable IP source routing.

no ip gratuitous-arps

// disable the transmission of gratuitous Address Resolution Protocol (ARP) messages  
for an address in a local pool.

!
!
ip cef
ip domain name test.com
!
!
no ip bootp server
ip inspect audit-trail
ip inspect udp idle-time 1800
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15

```

```
ip inspect name autosec_inspect tcp timeout 3600

// Define a set of inspection rules to override the global idle timeouts for the specified protocol.

login block-for 3 attempts 3 within 10

// Configure your Cisco IOS device for login parameters that help provide DoS detection.

!
dot1x system-auth-control
username cisco password 7 124814450558095038
archive
log config
logging enable
!
!
ip ssh time-out 60
ip ssh authentication-retries 2

// Configure Secure Shell (SSH) time out and the number of attempts after which the interface is reset.

!
!
interface FastEthernet0/0
switchport access vlan 99
dot1x port-control auto

// Define access port to vlan 99 with dot1x authentication.

!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
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
switchport mode trunk

// Define trunk port.

!
interface Vlan1
ip address 172.16.253.1 255.255.255.0

// Define ip address for vlan 1.

no ip redirects

// Disable the sending of redirect messages.

no ip unreachable

// Disable the generation of Internet Control Message Protocol (ICMP) unreachable
messages.

no ip proxy-arp

// disable proxy ARP on the interface
no mop enabled

// Disable mop which reduce LAN traffic, and are not in a DEC environment.
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.16.253.2

// This is static routing.
```

```

!
!
ip access-list extended autosec_firewall_acl
 permit udp any any eq bootpc
 deny ip any any

// Set an ACL extended rule to permit UDP bootstrap protocol client (bootpc) packets
from any source to any destination.

logging trap debugging

// Limit the number of messages sent to the syslog servers at the debugging level.

logging facility local2

// Set the logging facility at critical level.

access-list 100 permit udp any any eq bootpc

// Set an ACL rule to permit UDP bootstrap protocol client (bootpc) packets from any
source to any destination.

mac-address-table static 000c.294f.5d6d interface FastEthernet0/0 vlan 99

// Define static mac address for vlan 99 at port FastEthernet 0.

no cdp run

// Disable CDP for the whole router.

!
!
radius-server host 172.16.1.10 auth-port 1812 acct-port 1813 key 7
08305B4B1B0D1C021B041C

// Specify a RADIUS server host and encryption key values on a per-server basis.
!
control-plane
!
!
banner motd ^ Authorised Access only ^

// The syntax for the banner.

!
line con 0
 exec-timeout 0 0

```



```

logging synchronous
transport output telnet
line aux 0
transport output telnet
line vty 0 4
transport input telnet ssh
!
ntp authentication-key 1 md5 03175E08140A35 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp trusted-key 1

// Tell the router which keys are valid for authentication.

ntp clock-period 17179866

// This command is added automatically to jump-start the NTP frequency compensation when the box is rebooted.

ntp server 172.16.251.1 key 1

// Make your time synchronize with a ntp master.

!
end

```

Switch 3

```

!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages. Include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to logging messages. Include milliseconds.

no service password-encryption

// Disable encrypts the Cisco IOS passwords stored in the router's NVRAM configuration files.

```

```
hostname SW3

// Switch named SW3.

!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
interface FastEthernet0/0
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
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 Vlan1
  no ip address
!
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
!
!
end

```

Switch 4

```

!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages. Include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to logging messages. Include milliseconds.

no service password-encryption
// Disable encrypts the Cisco IOS passwords stored in the router's NVRAM configuration files.

!
hostname SW4

// Switch named SW4.

!
boot-start-marker
boot-end-marker
!

```

```
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
interface FastEthernet0/0
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
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 Vlan1
no ip address
!
ip http server
no ip http secure-server
!
!
control-plane
```

```

!
!
line con 0
line aux 0
line vty 0 4
login
!
!
end

```

4.1.2 Final secure topology design

This final secure topology has the same security technology as the first secure topology and includes a lot of more technologies as the following:

- Inside network
 - Multilayer network or hierarchical network. (core, distribution and access)
 - Access Layer include the following:
 - Aggregating all the user endpoints.
 - Providing traffic conditioning functions such as marking and policing.
 - Providing network security services such as 802.1x and port security.
 - Providing redundant links toward the distribution layer.
 - Distribution Layer include the following:
 - Aggregating access layer switches.
 - Terminating virtual LANs (VLANs) that are defined within the Layer 2 domain.
 - Providing the first-hop gateway service for all the end stations.
 - Providing redundant links toward the core layer, if required.
 - Core Layer include the following:
 - Aggregating distribution layers to form an interconnected network.
 - Providing high-speed transfer of traffic among the distribution layers.
 - Providing a resilient IP routing environment.
 - **Hot Standby Routing Protocol (HSRP)**, HSRP allows one router to automatically assume the function of the second router if the second router fails. HSRP is particularly useful when the users on one subnet require continuous access to resources in the network.
 - **VLAN Trunk Protocol (VTP)** reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere.

- **Spanning Tree Protocol (STP)** is a Layer 2 protocol that runs on bridges and switches. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network. Loops are deadly to a network.
- Cisco **EtherChannel** technology provides a solution for network managers who require higher bandwidth between servers, routers, and switches than single-link Ethernet technology can provide.
- **PIX Firewall**
 - **Virtual Private Network (VPN)**
 - **IP Security (IPSec)** enable the following PIX Firewall VPN features:
 - **Data confidentiality** – the IPSec sender can encrypt packets before transmitting them across a network.
 - **Data integrity** – The IPSec receiver can authenticate IPSec peers and packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
 - **Data origin authentication** – The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
 - **Anti-replay** – The IPSec receiver can detect and reject replayed packets, helping prevent spoofing and man-in-the-middle attacks.
 - **Internet Security Association and Key Management Protocol (ISAKMP)**, ISAKMP defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation (e.g. denial of service and replay attacks).
 - **Site-to-Site VPN**, a company can connect multiple fixed sites over a public network such as the Internet.
 - **Remote-Access VPN**, a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations.
 - **Encapsulating Security Payload, ESP** used primarily in a VPN connection (like IPSec tunnel). The ESP protocol provides origin authenticity, integrity, and confidentiality protection of a packet. ESP also supports encryption-only and authentication-only configurations.
 - **Split-tunnel**, allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection.
 - **Access List Control (ACL)**, used for filtering outbound traffic and not allow outside network traffic comes inside.

- **Network Address Translation (NAT)**, NAT do so in order to enable multiple hosts on a private network to access the Internet using a single public IP address.
- **Service Sever**
 - **Dynamic Host Configuration Protocol (DHCP)**, a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
 - **Domain Name System (DNS)**, a database system that translates a computer's fully qualified domain name into an IP address. For example, on the web, it's much easier to remember the domain name www.amazon.com than it is to remember its corresponding IP address (207.171.166.48).
 - **MySQL**, a database system used on the web. Basically, a MySQL database allows you to create a relational database structure on a web-server somewhere in order to store data or automate procedures.
 - **Web Server (HTTP)**, delivers (serves) content, such as web pages, using the Hypertext Transfer Protocol (HTTP), over the World Wide Web.
 - **File Transfer Protocol Server (FTP)**, used to exchange and manipulate files over a TCP/IP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server applications.
- **OpenERP Server**, a company-wide computer software system used to manage and coordinate all the resources, information, and functions of a business from shared data stores.
- **Syslog Server**, used for computer system management and security auditing as well as generalized informational, analysis, and debugging messages.
- **AAA Server**, the process of authentication, authorization and accounting utilized by the Remote Authentication Dial In User Services (RADIUS) network protocol.
- **Kerberos Server**, allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed primarily at a client-server model, and it provides mutual authentication — both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

4.1.2.1 Show running-configure.

Table 4.2 Final secure network shows running configure.

```

A1
! No configuration change since last restart
! NVRAM config last updated at 00:18:34 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include milliseconds.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!
hostname A1

// Switch named A1

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit messages based on critical conditions.

!

```

```
aaa new-model
// Enable AAA access control model.
aaa authentication login default group radius local
aaa authentication login localauth local
aaa authentication ppp default if-needed group radius local
aaa authorization exec default group radius local
aaa authorization network default group radius local
aaa accounting delay-start
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius

// Configuration of AAA RADIUS.

!
aaa session-id common
memory-size iomem 5
!
!
ip cef
ip domain name mycompany.com
!
!
no ip bootp server
login block-for 3 attempts 3 within 60

// Configure your Cisco IOS device for login parameters that help provide DoS
detection.

!
!
vtp file nvram:vlan.dat
username cisco privilege 15 password 7 121A0C041104

// Define username cisco and password with privilege 15.

!
!
ip ssh time-out 60
ip ssh authentication-retries 2

// Configure Secure Shell (SSH) time out and the number of attempts after which the
interface is reset.

!
!
interface FastEthernet0/0
switchport mode trunk
```



```
!  
interface FastEthernet0/1  
  switchport access vlan 10  
!  
interface FastEthernet0/2  
  switchport access vlan 10  
!  
interface FastEthernet0/3  
  shutdown  
!  
interface FastEthernet0/4  
  shutdown  
!  
interface FastEthernet0/5  
  shutdown  
!  
interface FastEthernet0/6  
  shutdown  
!  
interface FastEthernet0/7  
  shutdown  
!  
interface FastEthernet0/8  
  shutdown  
!  
interface FastEthernet0/9  
  shutdown  
!  
interface FastEthernet0/10  
  shutdown  
!  
interface FastEthernet0/11  
  shutdown  
!  
interface FastEthernet0/12  
  shutdown  
!  
interface FastEthernet0/13  
  shutdown  
!  
interface FastEthernet0/14  
  shutdown  
!  
interface FastEthernet0/15  
  switchport mode trunk
```

// Define access and trunk mode for interfaces. Others interfaces are shutdown.

```
!  
interface Vlan1  
ip address 192.168.254.100 255.255.255.0  
!  
router eigrp 10  
network 192.168.254.0  
auto-summary  
!  
no ip http server  
no ip http secure-server  
!  
logging 192.168.50.100  
snmp-server community public RO  
  
// Define which Syslog server IP address is and enable the Read-only (RO) community  
string.  
  
!  
!  
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7  
03154C0E141B3859470609  
  
// Specify a RADIUS server host and to configure timeout, retransmit, and encryption  
key values on a per-server basis.  
  
!  
control-plane  
!  
!  
line con 0  
exec-timeout 0 0  
logging synchronous  
line aux 0  
line vty 0 4  
!  
ntp authentication-key 1 md5 014217564C58035B33 7  
  
// The key string for NTP authentication key 1.  
  
ntp authenticate  
  
// Enables NTP authentication.  
  
ntp trusted-key 1  
  
// Tell the switch which keys are valid for authentication.
```

```

ntp clock-period 17179870
ntp server 192.168.254.253 key 1

// Make your time synchronize with a ntp master.

!
end

```

A2

```

! No configuration change since last restart
! NVRAM config last updated at 00:18:37 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include milliseconds.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!
hostname A2

// Switch named A2

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.

logging console critical

```

```
// Send system logging (syslog) messages to all available TTY lines and limit  
messages based on critical conditions.
```

```
!  
aaa new-model
```

```
// Enable AAA access control model.
```

```
!  
!  
aaa authentication login default group radius local  
aaa authentication login localauth local  
aaa authentication ppp default if-needed group radius local  
aaa authorization exec default group radius local  
aaa authorization network default group radius local  
aaa accounting delay-start  
aaa accounting exec default start-stop group radius  
aaa accounting network default start-stop group radius
```

```
// Configuration of AAA RADIUS.
```

```
!  
aaa session-id common  
memory-size iomem 5  
!  
!  
ip cef  
ip domain name mycompany.com  
!  
!  
no ip bootp server  
login block-for 3 attempts 3 within 60
```

```
// Configure your Cisco IOS device for login parameters that help provide DoS  
detection.
```

```
!  
!  
vtp file nvram:vlan.dat  
  
username cisco privilege 15 password 7 1511021F0725
```

```
// Define username cisco and password with privilege level 15.
```

```
!  
!
```

```
ip ssh time-out 60
ip ssh authentication-retries 2

// Configure Secure Shell (SSH) time out and the number of attempts after which the
interface is reset.

!
!
interface FastEthernet0/0
switchport mode trunk
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 20
!
interface FastEthernet0/3
switchport access vlan 20
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
```



```
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown

// Define access and trunk mode for interfaces. Others interfaces are shutdown.

!
interface Vlan1
ip address 192.168.254.200 255.255.255.0
!
router eigrp 10
network 192.168.254.0
auto-summary
!
no ip http server
no ip http secure-server
!
!
logging 192.168.50.100
snmp-server community public RO

// Define which Syslog server IP address is and enable the Read-only (RO) community
string.

!
!
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
071E36495C1D00101E1D1B

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption
key values on a per-server basis.

!
control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
```

```

ntp authentication-key 1 md5 014217564C58035B33 7
// The key string for NTP authentication key 1.

ntp authenticate
// Enables NTP authentication.

ntp trusted-key 1
// Tell the switch which keys are valid for authentication.

ntp clock-period 17179854
ntp server 192.168.254.253 key 1
// Make your time synchronize with a ntp master.

!
end

```

A3

```

!
! No configuration change since last restart
! NVRAM config last updated at 00:18:24 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec
// Indicates that the timestamp should be applied to debugging messages include
milliseconds.

service timestamps log datetime msec
// Indicates that the timestamp should be applied to system logging messages include
milliseconds.

service password-encryption
// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!
hostname A3
// Switch named A3
boot-start-marker

```

```
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit
messages based on critical conditions.

!
aaa new-model

// Enable AAA access control model.

!
!
aaa authentication login default group radius local
aaa authentication login localauth local
aaa authentication ppp default if-needed group radius local
aaa authorization exec default group radius local
aaa authorization network default group radius local
aaa accounting delay-start
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius

// Configuration of AAA RADIUS.

!
aaa session-id common
memory-size iomem 5
!
!
ip cef
ip domain name mycompany.com
!
!
no ip bootp server
login block-for 3 attempts 3 within 60

// Configure your Cisco IOS device for login parameters that help provide DoS
detection.
```

```
!  
!  
vtp file nvram:vlan.dat  
  
username cisco privilege 15 password 7 030752180500  
  
// Define username cisco and password with privilege level 15.  
  
!  
!  
ip ssh time-out 60  
ip ssh authentication-retries 2  
  
// Configure Secure Shell (SSH) time out and the number of attempts after which the  
interface is reset.  
  
!  
!  
interface FastEthernet0/0  
switchport mode trunk  
!  
interface FastEthernet0/1  
switchport access vlan 30  
!  
interface FastEthernet0/2  
shutdown  
!  
interface FastEthernet0/3  
shutdown  
!  
interface FastEthernet0/4  
shutdown  
!  
interface FastEthernet0/5  
shutdown  
!  
interface FastEthernet0/6  
shutdown  
!  
interface FastEthernet0/7  
shutdown  
!  
interface FastEthernet0/8  
shutdown  
!  
interface FastEthernet0/9  
shutdown
```

```
!  
interface FastEthernet0/10  
shutdown  
!  
interface FastEthernet0/11  
shutdown  
!  
interface FastEthernet0/12  
shutdown  
!  
interface FastEthernet0/13  
shutdown  
!  
interface FastEthernet0/14  
shutdown  
!  
interface FastEthernet0/15  
shutdown  
  
// Define access and trunk mode for interfaces. Others interfaces are shutdown.  
  
!  
interface Vlan1  
ip address 192.168.254.230 255.255.255.0  
!  
router eigrp 10  
network 192.168.254.0  
auto-summary  
!  
no ip http server  
no ip http secure-server  
!  
!  
logging 192.168.50.100  
snmp-server community public RO  
  
// Define which Syslog server IP address is and enable the Read-only (RO) community  
string.  
  
!  
!  
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7  
1314001719181D3F222B38  
  
// Specify a RADIUS server host and to configure timeout, retransmit, and encryption  
key values on a per-server basis.  
!
```



```

control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 091D5F5B0E56124619 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp trusted-key 1

// Tell the switch which keys are valid for authentication.

ntp clock-period 17179881
ntp server 192.168.254.253 key 1

// Make your time synchronize with a ntp master.

!
end

```

A4

```

! No configuration change since last restart
! NVRAM config last updated at 00:18:19 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include milliseconds.

service password-encryption

```

// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!

hostname A4

// Switch named A4

!

boot-start-marker

boot-end-marker

!

security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit messages based on critical conditions.

!

aaa new-model

// Enable AAA access control model.

!

!

aaa authentication login default group radius local

aaa authentication login localauth local

aaa authentication ppp default if-needed group radius local

aaa authorization exec default group radius local

aaa authorization network default group radius local

aaa accounting delay-start

aaa accounting exec default start-stop group radius

aaa accounting network default start-stop group radius

// Configuration of AAA RADIUS.

!

aaa session-id common

memory-size iomem 5

!

```
!  
ip cef  
ip domain name mycompany.com  
!  
!  
no ip bootp server  
login block-for 3 attempts 3 within 60  
  
// Configure your Cisco IOS device for login parameters that help provide DoS  
detection.  
  
!  
!  
vtp file nvram:vlan.dat  
  
username cisco privilege 15 password 7 00071A150754  
  
// Define username cisco and password with privilege level 15.  
  
!  
!  
ip ssh time-out 60  
ip ssh authentication-retries 2  
  
// Configure Secure Shell (SSH) time out and the number of attempts after which the  
interface is reset.  
  
!  
!  
interface FastEthernet0/0  
switchport mode trunk  
!  
interface FastEthernet0/1  
switchport access vlan 40  
!  
interface FastEthernet0/2  
switchport access vlan 40  
!  
interface FastEthernet0/3  
shutdown  
!  
interface FastEthernet0/4  
shutdown  
!  
interface FastEthernet0/5  
shutdown  
!
```

```
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
switchport mode trunk

// Define access and trunk mode for interfaces. Others interfaces are shutdown.

!
interface Vlan1
ip address 192.168.254.240 255.255.255.0
!
router eigrp 10
network 192.168.254.0
auto-summary
!
no ip http server
no ip http secure-server
!
!
logging 192.168.50.100
snmp-server community public RO
```

```

// Define which Syslog server IP address is and enable the Read-only (RO) community
string.

!
!
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
03154C0E141B3859470609

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption
key values on a per-server basis.

!
control-plane
!
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 06571E735B1D0C4D17 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp trusted-key 1

// Tell the switch which keys are valid for authentication.

ntp clock-period 17179842
ntp server 192.168.254.253 key 1

// Make your time synchronize with a ntp master.

!
end

```

A5

```

! No configuration change since last restart
! NVRAM config last updated at 00:18:10 UTC Fri Mar 1 2002 by cisco

```



```
!  
version 12.4  
service timestamps debug datetime msec  
  
// Indicates that the timestamp should be applied to debugging messages include  
milliseconds.  
  
service timestamps log datetime msec  
  
// Indicates that the timestamp should be applied to system logging messages include  
milliseconds.  
  
service password-encryption  
  
// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.  
  
!  
hostname A5  
  
// Switch named A5.  
  
!  
boot-start-marker  
boot-end-marker  
!  
security authentication failure rate 10 log  
  
// Configure the number of allowable unsuccessful login attempts.  
  
logging buffered 4096 debugging  
  
// Configure the switch to send buffered logging of its events to the memory.  
  
logging console critical  
  
// Send system logging (syslog) messages to all available TTY lines and limit  
messages based on critical conditions.  
  
!  
aaa new-model  
  
// Enable AAA access control model.  
  
aaa authentication login default group radius local  
aaa authentication login localauth local  
aaa authentication ppp default if-needed group radius local  
aaa authorization exec default group radius local
```

```
aaa authorization network default group radius local
aaa accounting delay-start
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius

// Configuration of AAA RADIUS.

!
aaa session-id common
memory-size iomem 5
!
!
ip cef
ip domain name mycompany.com
!
!
no ip bootp server
login block-for 3 attempts 3 within 60

// Configure your Cisco IOS device for login parameters that help provide DoS
detection.

!
!
vtp file nvram:vlan.dat

username cisco privilege 15 password 7 030752180500

// Define username cisco and password with privilege level 15.

!
!
ip ssh time-out 60
ip ssh authentication-retries 2

// Configure Secure Shell (SSH) time out and the number of attempts after which the
interface is reset.

!
!
interface FastEthernet0/0
 switchport mode trunk
!
interface FastEthernet0/1
 switchport access vlan 50
!
interface FastEthernet0/2
```

```
switchport access vlan 50
!
interface FastEthernet0/3
switchport access vlan 50
!
interface FastEthernet0/4
switchport access vlan 50
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
switchport mode trunk

// Define access and trunk mode for interfaces. Others interfaces are shutdown.

interface Vlan1
ip address 192.168.254.250 255.255.255.0
!
router eigrp 10
```

```
network 192.168.254.0
auto-summary
!
no ip http server
no ip http secure-server
!
!
logging 192.168.50.100
snmp-server community public RO

// Define which Syslog server IP address is and enable the Read-only (RO) community string.

!
!
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
1314001719181D3F222B38

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption key values on a per-server basis.

!
control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 040A1A541872491A1B 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp trusted-key 1

// Tell the switch which keys are valid for authentication.

ntp clock-period 17179914
ntp server 192.168.254.253 key 1

// Make your time synchronize with a ntp master.
```

```
!
end
```

D1

```
! No configuration change since last restart
! NVRAM config last updated at 00:18:30 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include milliseconds.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!
hostname D1

// Switch named D1

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit messages based on critical conditions.

!
aaa new-model
```



```
// Enable AAA access control model.
```

```
!  
!  
aaa authentication login default group radius local  
aaa authentication login localauth local  
aaa authentication ppp default if-needed group radius local  
aaa authorization exec default group radius local  
aaa authorization network default group radius local  
aaa accounting delay-start  
aaa accounting exec default start-stop group radius  
aaa accounting network default start-stop group radius
```

```
// Configuration of AAA RADIUS.
```

```
!  
aaa session-id common  
memory-size iomem 5  
!  
!  
ip cef  
ip domain name mycompany.com  
!  
!  
no ip bootp server  
login block-for 3 attempts 3 within 60
```

```
// Configure your Cisco IOS device for login parameters that help provide DoS detection.
```

```
!  
!  
spanning-tree vlan 10 priority 8192  
spanning-tree vlan 20 priority 16384
```

```
// Set STP for vlan with priority number.
```

```
vtp file nvram:vlan.dat
```

```
username cisco privilege 15 password 7 14141B180F0B
```

```
// Define username cisco and password with privilege level 15.
```

```
ip ssh time-out 60  
ip ssh authentication-retries 2
```

// Configure Secure Shell (SSH) time out and the number of attempts after which the interface is reset.

```
!  
!  
interface FastEthernet0/0  
  switchport mode trunk  
!  
interface FastEthernet0/1  
  switchport mode trunk  
!  
interface FastEthernet0/2  
  switchport mode trunk  
!  
interface FastEthernet0/3  
  switchport mode trunk  
!  
interface FastEthernet0/4  
  shutdown  
!  
interface FastEthernet0/5  
  shutdown  
!  
interface FastEthernet0/6  
  shutdown  
!  
interface FastEthernet0/7  
  shutdown  
!  
interface FastEthernet0/8  
  shutdown  
!  
interface FastEthernet0/9  
  shutdown  
!  
interface FastEthernet0/10  
  shutdown  
!  
interface FastEthernet0/11  
  shutdown  
!  
interface FastEthernet0/12  
  shutdown  
!  
interface FastEthernet0/13  
  shutdown  
!
```

```
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown

// Define trunk mode for interfaces. Others interfaces are shutdown.

!
interface Vlan1
ip address 192.168.254.10 255.255.255.0
!
interface Vlan10
ip address 192.168.10.10 255.255.255.0
ip helper-address 192.168.40.110

// Enable the forwarding of User Datagram Protocol (UDP) broadcasts, including
BOOTP, received on an interface.

standby 10 ip 192.168.10.1
standby 10 priority 200
standby 10 preempt

// Assigns an IP address to the interface with priority number and allows the router to
become the active router when the priority is higher than all other HSRP-configured
routers in the hot standby group.

!
interface Vlan20
ip address 192.168.20.20 255.255.255.0
ip helper-address 192.168.40.110

// Enable the forwarding of User Datagram Protocol (UDP) broadcasts, including
BOOTP, received on an interface.

standby 20 ip 192.168.20.1

// Assigns an IP address to the interface.

!
interface Vlan29
no ip address
!
router eigrp 10
network 192.168.10.0
network 192.168.20.0
network 192.168.254.0
```

```
auto-summary
!
no ip http server
no ip http secure-server
!
!
logging 192.168.50.100
snmp-server community public RO
mac-address-table static 0000.0c07.ac0a interface FastEthernet0/2 vlan 10

// Define which Syslog server IP address is and enable the Read-only (RO) community
string. Add static entries to the MAC address table.

!
!
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
12081212001F1511232434

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption
key values on a per-server basis.

!
control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 06571E735B1D0C4D17 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp trusted-key 1

// Tell the switch which keys are valid for authentication.

ntp clock-period 17179910
ntp server 192.168.254.253 key 1

// Make your time synchronize with a ntp master.
```

```
!
end
```

D2

```
! No configuration change since last restart
! NVRAM config last updated at 00:18:32 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include milliseconds.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!
hostname D2

// Switch named D2

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit messages based on critical conditions.

!
aaa new-model
```


// Enable AAA access control model.

!
!

aaa authentication login default group radius local
aaa authentication login localauth local
aaa authentication ppp default if-needed group radius local
aaa authorization exec default group radius local
aaa authorization network default group radius local
aaa accounting delay-start
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius

// Configuration of AAA RADIUS.

!

aaa session-id common
memory-size iomem 5

!

!

ip cef
ip domain name mycompany.com

!

!

no ip bootp server
login block-for 3 attempts 3 within 60

// Configure your Cisco IOS device for login parameters that help provide DoS detection.

!

!

spanning-tree vlan 10 priority 16384
spanning-tree vlan 20 priority 8192

// Set STP for vlan with priority number.

vtp file nvram:vlan.dat

username cisco privilege 15 password 7 00071A150754

// Define username cisco and password with privilege level 15.

ip ssh time-out 60
ip ssh authentication-retries 2

```
// Configure Secure Shell (SSH) time out and the number of attempts after which the
interface is reset.
!
!
interface FastEthernet0/0
 switchport mode trunk
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
!
interface FastEthernet0/6
 shutdown
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
```

```
shutdown
!
interface FastEthernet0/15
shutdown

// Define trunk mode for interfaces. Others interfaces are shutdown.

!
interface Vlan1
ip address 192.168.254.20 255.255.255.0
!
interface Vlan10
ip address 192.168.10.20 255.255.255.0
ip helper-address 192.168.40.110

// Enable the forwarding of User Datagram Protocol (UDP) broadcasts, including
BOOTP, received on an interface.

standby 10 ip 192.168.10.1

// Assigns an IP address to the interface.

!
interface Vlan20
ip address 192.168.20.10 255.255.255.0
ip helper-address 192.168.40.110

// Enable the forwarding of User Datagram Protocol (UDP) broadcasts, including
BOOTP, received on an interface.

standby 20 ip 192.168.20.1
standby 20 priority 200
standby 20 preempt

// Assigns an IP address to the interface with priority number and allows the router to
become the active router when the priority is higher than all other HSRP-configured
routers in the hot standby group.

!
router eigrp 10
network 192.168.10.0
network 192.168.20.0
network 192.168.254.0
auto-summary
no ip http server
no ip http secure-server
!
```

```

!
logging 192.168.50.100
snmp-server community public RO

// Define which Syslog server IP address is and enable the Read-only (RO) community string.

!
!
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
071E36495C1D00101E1D1B

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption key values on a per-server basis.

!
control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 08705D1C1E4A004300 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp trusted-key 1

// Tell the switch which keys are valid for authentication.

ntp clock-period 17179895
ntp server 192.168.254.253 key 1

// Make your time synchronize with a ntp master.

!
end

```

```
! No configuration change since last restart
! NVRAM config last updated at 00:18:21 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include milliseconds.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!
hostname D3

// Switch named D3

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit messages based on critical conditions.

!
aaa new-model
// Enable AAA access control model.
aaa authentication login default group radius local
aaa authentication login localauth local
aaa authentication ppp default if-needed group radius local
```



```
aaa authorization exec default group radius local
aaa authorization network default group radius local
aaa accounting delay-start
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius

// Configuration of AAA RADIUS.

!
aaa session-id common
memory-size iomem 5
!
!
ip cef
ip domain name mycompany.com
!
!
no ip bootp server
login block-for 3 attempts 3 within 60

// Configure your Cisco IOS device for login parameters that help provide DoS
detection.

!
vtp file nvram:vlan.dat

username cisco privilege 15 password 7 0822455D0A16

// Define username cisco and password with privilege level 15.

!
!
ip ssh time-out 60
ip ssh authentication-retries 2

// Configure Secure Shell (SSH) time out and the number of attempts after which the
interface is reset.

!
!
interface FastEthernet0/0
switchport mode trunk
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
```

```
switchport mode trunk
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown

// Define access and trunk mode for interfaces. Others interfaces are shutdown.

!
interface Vlan1
ip address 192.168.254.30 255.255.255.0
!
```



```

interface Vlan30
ip address 192.168.30.1 255.255.255.0
ip helper-address 192.168.40.110

// Enable the forwarding of User Datagram Protocol (UDP) broadcasts, including
// BOOTP, received on an interface.

!
router eigrp 10
network 192.168.30.0
network 192.168.254.0
auto-summary
!
no ip http server
no ip http secure-server
!
!
logging 192.168.50.100
snmp-server community public RO

// Define which Syslog server IP address is and enable the Read-only (RO) community
// string.

!
!
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
01021101491F1F1A28435E

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption
// key values on a per-server basis.

!
control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 014217564C58035B33 7

// The key string for NTP authentication key 1.
ntp authenticate

// Enables NTP authentication.

```

```
ntp trusted-key 1

// Tell the switch which keys are valid for authentication.

ntp clock-period 17179833
ntp server 192.168.254.253 key 1

// Make your time synchronize with a ntp master.

!
end
```

D4

```
! NVRAM config last updated at 00:18:17 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include
milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include
milliseconds.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!
hostname D4

// Switch named D4

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log
// Configure the number of allowable unsuccessful login attempts.
logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.
```

```
logging console critical
```

```
// Send system logging (syslog) messages to all available TTY lines and limit  
messages based on critical conditions.
```

```
!  
aaa new-model
```

```
// Enable AAA access control model.
```

```
!  
!  
aaa authentication login default group radius local  
aaa authentication login localauth local  
aaa authentication ppp default if-needed group radius local  
aaa authorization exec default group radius local  
aaa authorization network default group radius local  
aaa accounting delay-start  
aaa accounting exec default start-stop group radius  
aaa accounting network default start-stop group radius
```

```
// Configuration of AAA RADIUS.
```

```
!  
aaa session-id common  
memory-size iomem 5  
!  
!  
ip cef  
ip domain name mycompany.com  
!  
!
```

```
no ip bootp server  
login block-for 3 attempts 3 within 60
```

```
// Configure your Cisco IOS device for login parameters that help provide DoS  
detection.
```

```
!  
!  
spanning-tree vlan 40 priority 8192  
spanning-tree vlan 50 priority 16384  
// Set STP for vlan with priority number.  
vtp file nvram:vlan.dat
```

```
username cisco privilege 15 password 7 05080F1C2243
```



```
// Define username cisco and password with privilege level 15.
```

```
!  
!
```

```
ip ssh time-out 60
```

```
ip ssh authentication-retries 2
```

```
// Configure Secure Shell (SSH) time out and the number of attempts after which the  
interface is reset.
```

```
!  
!
```

```
interface FastEthernet0/0  
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/1  
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/2  
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/3  
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/4  
shutdown
```

```
!
```

```
interface FastEthernet0/5  
shutdown
```

```
!
```

```
interface FastEthernet0/6  
shutdown
```

```
!
```

```
interface FastEthernet0/7  
shutdown
```

```
!
```

```
interface FastEthernet0/8  
shutdown
```

```
!
```

```
interface FastEthernet0/9  
shutdown
```

```
!
```

```
interface FastEthernet0/10  
shutdown
```

```
!
```

```
interface FastEthernet0/11
```

```
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown

// Define trunk mode for interfaces. Others interfaces are shutdown.

!
interface Vlan1
ip address 192.168.254.40 255.255.255.0
!
interface Vlan40
ip address 192.168.40.10 255.255.255.0
standby 40 ip 192.168.40.1
standby 40 priority 200
standby 40 preempt

// Assigns an IP address to the interface with priority number and allows the router to
become the active router when the priority is higher than all other HSRP-configured
routers in the hot standby group.

!
interface Vlan50
ip address 192.168.50.20 255.255.255.0
standby 50 ip 192.168.50.1

// Assigns an IP address to the interface.

!
router eigrp 10
network 192.168.40.0
network 192.168.50.0
network 192.168.254.0
auto-summary
!
no ip http server
no ip http secure-server
!
```

```

!
!
!
logging 192.168.50.100
snmp-server community public RO
mac-address-table static 0000.0c07.ac28 interface FastEthernet0/2 vlan 40

// Define which Syslog server IP address is and enable the Read-only (RO) community string. Add static entries to the MAC address table.

!
!
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
01021101491F1F1A28435E

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption key values on a per-server basis.

!
control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 15431A5E13792E703A 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp trusted-key 1

// Tell the switch which keys are valid for authentication.

ntp clock-period 17179789
ntp server 192.168.254.253 key 1
// Make your time synchronize with a ntp master.
end

```

```
! NVRAM config last updated at 00:18:12 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include milliseconds.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!
hostname D5

// Switch named D5

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit messages based on critical conditions.

!
aaa new-model

// Enable AAA access control model.

aaa authentication login default group radius local
aaa authentication login localauth local
aaa authentication ppp default if-needed group radius local
```

```
aaa authorization exec default group radius local
aaa authorization network default group radius local
aaa accounting delay-start
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius

// Configuration of AAA RADIUS.

!
aaa session-id common
memory-size iomem 5
!
!
ip cef
ip domain name mycompany.com
!
!
no ip bootp server
login block-for 3 attempts 3 within 60

// Configure your Cisco IOS device for login parameters that help provide DoS
detection.

!
!
spanning-tree vlan 40 priority 16384
spanning-tree vlan 50 priority 8192

// Set STP for vlan with priority number.

vtp file nvram:vlan.dat

username cisco privilege 15 password 7 060506324F41

// Define username cisco and password with privilege level 15.

!
!
ip ssh time-out 60
ip ssh authentication-retries 2

// Configure Secure Shell (SSH) time out and the number of attempts after which the
interface is reset.

interface FastEthernet0/0
switchport mode trunk
!
```



```
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
// Define access and trunk mode for interfaces. Others interfaces are shutdown.

interface Vlan1
```

```

ip address 192.168.254.50 255.255.255.0
!
interface Vlan40
ip address 192.168.40.20 255.255.255.0
standby 40 ip 192.168.40.1

// Assigns an IP address to the interface.

!
interface Vlan50
ip address 192.168.50.10 255.255.255.0
standby 50 ip 192.168.50.1
standby 50 priority 200
standby 50 preempt

// Assigns an IP address to the interface with priority number and allows the router to
become the active router when the priority is higher than all other HSRP-configured
routers in the hot standby group.

!
router eigrp 10
network 192.168.40.0
network 192.168.50.0
network 192.168.254.0
auto-summary
!
no ip http server
no ip http secure-server
!
!
logging 192.168.50.100
snmp-server community public RO
mac-address-table static 0000.0c07.ac32 interface FastEthernet0/2 vlan 50

// Define which Syslog server IP address is and enable the Read-only (RO) community
string. Add static entries to the MAC address table.

!
!
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
00150403164F1213062E5C

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption
key values on a per-server basis.
control-plane
!
!

```

```

line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 144603591B572F7F36 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp trusted-key 1

// Tell the switch which keys are valid for authentication.

ntp clock-period 17179890
ntp server 192.168.254.253 key 1

// Make your time synchronize with a ntp master.

!
end

```

C1

```

! No configuration change since last restart
! NVRAM config last updated at 00:18:14 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include
milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include
milliseconds.

service password-encryption
// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.
hostname C1

// Switch named C1

```

```

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit
messages based on critical conditions.

!
aaa new-model

// Enable AAA access control model.

!
!
aaa authentication login default group radius local
aaa authentication login localauth local
aaa authentication ppp default if-needed group radius local
aaa authorization exec default group radius local
aaa authorization network default group radius local
aaa accounting delay-start
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius

// Configuration of AAA RADIUS.

!
aaa session-id common
memory-size iomem 5
!
!
ip cef
ip domain name mycompany.com
!
no ip bootp server
login block-for 3 attempts 3 within 60

```

```
// Configure your Cisco IOS device for login parameters that help provide DoS
detection.

!
!
vtp file nvram:vlan.dat

username cisco privilege 15 password 7 0822455D0A16

// Define username cisco and password with privilege level 15.

!
!
ip ssh time-out 60
ip ssh authentication-retries 2

// Configure Secure Shell (SSH) time out and the number of attempts after which the
interface is reset.

!
!
interface Port-channel1
switchport mode trunk
!
interface FastEthernet0/0
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet0/1
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport mode trunk
!
interface FastEthernet0/6
switchport mode trunk
!
```



```
interface FastEthernet0/7
  switchport mode trunk
!
interface FastEthernet0/8
  shutdown
!
interface FastEthernet0/9
  shutdown
!
interface FastEthernet0/10
  shutdown
!
interface FastEthernet0/11
  shutdown
!
interface FastEthernet0/12
  shutdown
!
interface FastEthernet0/13
  shutdown
!
interface FastEthernet0/14
  shutdown
!
interface FastEthernet0/15
  shutdown

// Define Etherchannel group and trunk mode for interfaces. Others interfaces are
// shutdown.
!
interface Vlan1
  ip address 192.168.254.1 255.255.255.0
!
router eigrp 10
  network 192.168.254.0
  auto-summary
!
no ip http server
no ip http secure-server
!
!
logging 192.168.50.100
snmp-server community public RO

// Define which Syslog server IP address is and enable the Read-only (RO) community
// string.
```

```

radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
1314001719181D3F222B38

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption
key values on a per-server basis.

!
control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 0055025413080E521D 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp trusted-key 1

// Tell the switch which keys are valid for authentication.

ntp clock-period 17179882
ntp server 192.168.254.253 key 1

// Make your time synchronize with a ntp master.

!
end

```

C2

```

! No configuration change since last restart
! NVRAM config last updated at 00:18:26 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include
milliseconds.

```

```
service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include
milliseconds.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!
hostname C2

// Switch named C2

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the switch to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit
messages based on critical conditions.

!
aaa new-model

// Enable AAA access control model.

!
!
aaa authentication login default group radius local
aaa authentication login localauth local
aaa authentication ppp default if-needed group radius local
aaa authorization exec default group radius local
aaa authorization network default group radius local
aaa accounting delay-start
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
// Configuration of AAA RADIUS.
```

```
!  
aaa session-id common  
memory-size iomem 5  
!  
!  
ip cef  
ip domain name mycompany.com  
!  
!  
no ip bootp server  
login block-for 3 attempts 3 within 60  
  
// Configure your Cisco IOS device for login parameters that help provide DoS  
detection.  
  
!  
!  
vtp file nvram:vlan.dat  
  
username cisco privilege 15 password 7 121A0C041104  
  
// Define username cisco and password with privilege level 15.  
  
!  
!  
ip ssh time-out 60  
ip ssh authentication-retries 2  
  
// Configure Secure Shell (SSH) time out and the number of attempts after which the  
interface is reset.  
  
!  
!  
interface Port-channel1  
switchport mode trunk  
!  
interface FastEthernet0/0  
switchport mode trunk  
channel-group 1 mode on  
!  
interface FastEthernet0/1  
switchport mode trunk  
channel-group 1 mode on  
!  
interface FastEthernet0/2  
switchport mode trunk  
!
```

```
interface FastEthernet0/3
switchport mode trunk
!
interface FastEthernet0/4
switchport mode trunk
!
interface FastEthernet0/5
switchport mode trunk
!
interface FastEthernet0/6
switchport mode trunk
!
interface FastEthernet0/7
switchport mode trunk
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown

// Define EtherChannel group and trunk mode for interfaces. Others interfaces are
shutdown.

!
interface Vlan1
ip address 192.168.254.2 255.255.255.0
!
router eigrp 10
```




```

network 192.168.254.0
auto-summary
!
no ip http server
no ip http secure-server
!
!
logging 192.168.50.100
snmp-server community public RO

// Define which Syslog server IP address is and enable the Read-only (RO) community string.

!
!
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
071E36495C1D00101E1D1B

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption key values on a per-server basis.

!
control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 075E301E595A1C5105 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp trusted-key 1

// Tell the switch which keys are valid for authentication.

ntp clock-period 17179823
ntp server 192.168.254.253 key 1
// Make your time synchronize with a ntp master.
end

```

R1

```
! No configuration change since last restart
! NVRAM config last updated at 00:18:28 UTC Fri Mar 1 2002 by cisco
!
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include milliseconds.

service password-encryption

// Encrypts the Cisco IOS passwords stored in the NVRAM configuration files.

!
hostname R1

// Router named R1

!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log

// Configure the number of allowable unsuccessful login attempts.

logging buffered 4096 debugging

// Configure the router to send buffered logging of its events to the memory.

logging console critical

// Send system logging (syslog) messages to all available TTY lines and limit messages based on critical conditions.

!
aaa new-model

// Enable AAA access control model.
```

```
aaa authentication login default group radius local enable
aaa authentication login localauth local enable
aaa authentication ppp default if-needed group radius local
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius if-authenticated
aaa accounting delay-start
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
```

// Configuration of AAA RADIUS.

```
!
aaa session-id common
memory-size iomem 5
!
!
ip cef
ip domain name mycompany.com
!
!
no ip bootp server
login block-for 3 attempts 3 within 60
```

// Configure your Cisco IOS device for login parameters that help provide DoS detection.

```
!
!
username cisco privilege 15 password 7 070C285F4D06
```

// Define username cisco and password with privilege level 15.

```
!
!
ip ssh time-out 60
ip ssh authentication-retries 2
```

// Configure Secure Shell (SSH) time out and the number of attempts after which the interface is reset.

```
!
!
interface FastEthernet0/0
switchport mode trunk
!
interface FastEthernet0/1
switchport mode trunk
```

```
!  
interface FastEthernet0/2  
  switchport mode trunk  
!  
interface FastEthernet0/3  
  shutdown  
!  
interface FastEthernet0/4  
  shutdown  
!  
interface FastEthernet0/5  
  shutdown  
!  
interface FastEthernet0/6  
  shutdown  
!  
interface FastEthernet0/7  
  shutdown  
!  
interface FastEthernet0/8  
  shutdown  
!  
interface FastEthernet0/9  
  shutdown  
!  
interface FastEthernet0/10  
  shutdown  
!  
interface FastEthernet0/11  
  shutdown  
!  
interface FastEthernet0/12  
  shutdown  
!  
interface FastEthernet0/13  
  shutdown  
!  
interface FastEthernet0/14  
  shutdown  
!  
interface FastEthernet0/15  
  shutdown  
!  
interface FastEthernet1/0  
  no ip address  
  shutdown  
  duplex auto
```

```

speed auto
// Define trunk mode for interfaces. Others interfaces are shutdown.

!
interface Vlan1
ip address 192.168.254.253 255.255.255.0
!
router eigrp 10
network 192.168.254.0
auto-summary
!
no ip http server
no ip http secure-server
!
!
radius-server host 192.168.50.110 auth-port 1812 acct-port 1813 key 7
1406050E1E10333E2D2723

// Specify a RADIUS server host and to configure timeout, retransmit, and encryption
key values on a per-server basis.
!
control-plane
!
!
line con 0
exec-timeout 0 0
logging synchronous
line aux 0
line vty 0 4
!
ntp authentication-key 1 md5 03554A59115C24185C 7

// The key string for NTP authentication key 1.

ntp authenticate

// Enables NTP authentication.

ntp master 1

// Makes the system an authoritative NTP server

!
end

```


R2

```
version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include milliseconds.

no service password-encryption
!
hostname R2

// Router named R2

!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 172.16.10.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 10.1.3.1 255.255.255.0
duplex auto
speed auto
!
router eigrp 10
```

```

network 10.1.1.0 0.0.0.255
network 10.1.3.0 0.0.0.255
network 172.16.10.0 0.0.0.255
no auto-summary
!
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
!
!
end

```

ISP

```

version 12.4
service timestamps debug datetime msec

// Indicates that the timestamp should be applied to debugging messages include milliseconds.

service timestamps log datetime msec

// Indicates that the timestamp should be applied to system logging messages include milliseconds.

no service password-encryption
!
hostname ISP

// Router named ISP

!
boot-start-marker
boot-end-marker
!
!

```

```
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
interface FastEthernet0/0
ip address 172.16.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 172.16.20.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 172.16.30.2 255.255.255.0
duplex auto
speed auto
!
router eigrp 10
network 172.16.10.0 0.0.0.255
network 172.16.20.0 0.0.0.255
network 172.16.30.0 0.0.0.255
no auto-summary
!
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
!
!
end
```

FW1

```
PIX Version 8.0(4)
!
hostname mycompanyFW

// Pix firewall named mycompanyFW

enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted

// Enable password in encryption form.

names
name 192.168.10.0 vlan10
name 192.168.20.0 vlan20
name 192.168.30.0 vlan30
name 192.168.40.0 vlan40
name 10.1.2.0 remote
name 192.168.40.110 DB
name 10.1.3.254 DMZ-WEB

// Identify a host by a text name.

!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.254.254 255.255.255.0
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 no security-level
 no ip address
!
```

```

interface Ethernet4
 nameif Manage
 security-level 100
 ip address 172.16.1.1 255.255.255.0
 !
 ftp mode passive
 object-group network vlan-group
 network-object vlan10 255.255.255.0
 network-object vlan20 255.255.255.0
 network-object vlan30 255.255.255.0
 network-object vlan40 255.255.255.0

// Defines object groups that you can use to optimize your configuration, and then you
can issue a single command using the group name to apply to every item in the group.

 access-list outside_access_in extended permit icmp any object-group vlan-group
 access-list outside_access_in extended permit ip host DMZ-WEB host DB
 access-list outside_1_cryptomap extended permit ip object-group vlan-group remote
 255.255.255.0
 access-list inside_nat0_outbound extended permit ip object-group vlan-group remote
 255.255.255.0
 access-list inside_nat0_outbound extended permit ip 192.168.254.0 255.255.255.0
 192.168.254.0 255.255.255.128
 access-list mycompany-vpn_splitTunnelAcl standard permit 192.168.254.0
 255.255.255.0
 access-list inside_access_in extended permit ip any any

// ACL rules to permit vlan group from outside to remote access.

 pager lines 24
 mtu outside 1500
 mtu inside 1500
 mtu Manage 1500

// Specify the maximum transmission unit (MTU) for an interface.

 ip local pool vpn-ip 192.168.254.60-192.168.254.65 mask 255.255.255.0

// Creates a pool of local addresses to be used for assigning dynamic IP addresses to
remote VPN clients.

 icmp unreachable rate-limit 1 burst-size 1
 asdm image flash:/asdm-625.bin
 no asdm history enable
 arp timeout 14400
 global (outside) 101 interface
 nat (inside) 0 access-list inside_nat0_outbound

```



```

nat (Manage) 101 0.0.0.0 0.0.0.0

// Specify the NAT configuration.

access-group outside_access_in in interface outside
access-group inside_access_in in interface inside

// Binds the access list to an interface.

!
router ospf 20
network 10.1.1.0 255.255.255.0 area 0
area 0
log-adj-changes
!
router eigrp 10
no eigrp log-neighbor-warnings
network 10.1.1.0 255.255.255.0
network 192.168.254.0 255.255.255.0
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

// Set the maximum idle time duration.

dynamic-access-policy-record DfltAccessPolicy
http server enable
http 172.16.1.2 255.255.255.255 Manage
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group1

```

```

crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set transform-set
ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5
ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-
DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set security-
association lifetime seconds 28800
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set security-
association lifetime kilobytes 4608000
crypto map outside_map 1 match address outside_1_cryptomap
crypto map outside_map 1 set pfs group1
crypto map outside_map 1 set peer 172.16.30.1
crypto map outside_map 1 set transform-set ESP-3DES-SHA
crypto map outside_map 1 set security-association lifetime seconds 28800
crypto map outside_map 1 set security-association lifetime kilobytes 4608000
crypto map outside_map 1 set reverse-route
crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTOMAP
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
crypto isakmp policy 65535
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

// Crypto map and policy for remote access with split tunnel VPN.

telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
group-policy mycompany-vpn internal
group-policy mycompany-vpn attributes
dns-server value 192.168.40.110
vpn-tunnel-protocol IPSec
split-tunnel-policy tunnelall
// This defines the group policy and specify the networks that should pass through the
tunnel.

```

```

username user password XEaJpJFaYvDqZKxJ encrypted privilege 0
username user attributes
  vpn-group-policy mycompany-vpn
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15

// The username and password associated with this VPN connection.

tunnel-group 172.16.30.1 type ipsec-l2l
tunnel-group 172.16.30.1 ipsec-attributes
  pre-shared-key *
tunnel-group mycompany-vpn type remote-access
tunnel-group mycompany-vpn general-attributes
  address-pool vpn-ip
  default-group-policy mycompany-vpn
tunnel-group mycompany-vpn ipsec-attributes
  pre-shared-key *

// Bind the configurations defined in this configuration to the tunnel.

!
class-map inspection_default
  match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:90693e5dfce84cf78f2be04f9c4d4db7
: end

```

FW2

```
PIX Version 8.0(4)
!
hostname BranchFW

// Pix firewall named BranchFW

enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted

// Enable password in encryption form.

names
name 192.168.10.0 vlan10
name 192.168.20.0 vlan20
name 192.168.30.0 vlan30
name 192.168.40.0 vlan40

// Identify a host by a text name.
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 172.16.30.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.2.1 255.255.255.0
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet4
 nameif Manage
 security-level 100
```



```

ip address 172.16.1.3 255.255.255.0
!
ftp mode passive
object-group network vlan-group
network-object vlan10 255.255.255.0
network-object vlan20 255.255.255.0
network-object vlan30 255.255.255.0
network-object vlan40 255.255.255.0

// Defines object groups that you can use to optimize your configuration, and then you
can issue a single command using the group name to apply to every item in the group.

access-list outside_access_in extended permit icmp any 10.1.2.0 255.255.255.0
access-list outside_1_cryptomap extended permit ip 10.1.2.0 255.255.255.0 object-
group vlan-group
access-list inside_nat0_outbound extended permit ip 10.1.2.0 255.255.255.0 object-
group vlan-group

// ACL rules to permit access vlan group.

pager lines 24
mtu outside 1500
mtu inside 1500
mtu Manage 1500

// Specify the maximum transmission unit (MTU) for an interface.

icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-625.bin
no asdm history enable
arp timeout 14400
global (outside) 101 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (Manage) 101 0.0.0.0 0.0.0.0

// Specify the NAT configuration.

access-group outside_access_in in interface outside

// Binds the access list to an interface.

!
router ospf 20
network 10.1.2.0 255.255.255.0 area 0
network 172.16.30.0 255.255.255.0 area 0
area 0
log-adj-changes

```



```

!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute

```

// Set the maximum idle time duration.

```

dynamic-access-policy-record DfltAccessPolicy
http server enable
http 172.16.1.2 255.255.255.255 Manage
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto map outside_map 1 match address outside_1_cryptomap
crypto map outside_map 1 set pfs group1
crypto map outside_map 1 set peer 10.1.1.1
crypto map outside_map 1 set transform-set ESP-3DES-SHA
crypto map outside_map 1 set security-association lifetime seconds 28800
crypto map outside_map 1 set security-association lifetime kilobytes 4608000
crypto map outside_map 1 set reverse-route
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
crypto isakmp policy 65535
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

```

// Crypto map and policy for remote access with split tunnel VPN.

```

telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list

```

```
no threat-detection statistics tcp-intercept
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15
tunnel-group 10.1.1.1 type ipsec-l2l
tunnel-group 10.1.1.1 ipsec-attributes
pre-shared-key *

// Bind the configurations defined in this configuration to the tunnel.

!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6f700053200da2c5f5237e3420bb7ce7
: end
```

CHAPTER 5: LAB INTERACTION ON VIRTUALIZATION ARCHITECTURE SYSTEM AND NETWORK SECURITY

Introduction:

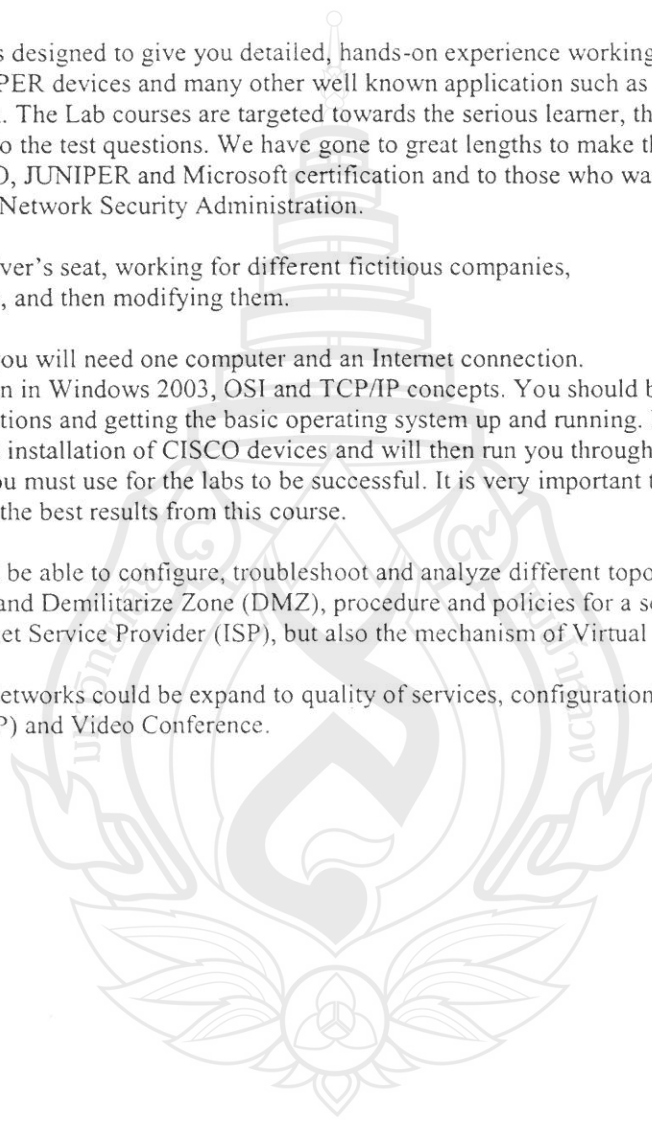
This series of labs on the model is designed to give you detailed, hands-on experience working with Windows 2003, UBUNTU, CISCO devices, JUNIPER devices and many other well known application such as OpenERP, TACACS+, RADIUS and so forth. The Lab courses are targeted towards the serious learner, those who want to know more than just the answers to the test questions. We have gone to great lengths to make this series appealing to both those who are seeking CISCO, JUNIPER and Microsoft certification and to those who want an excellent overall knowledge of System and Network Security Administration.

Each of our labs put you in the driver's seat, working for different fictitious companies, deploying complex configurations, and then modifying them.

To complete these labs yourself, you will need one computer and an Internet connection. You also need to have a foundation in Windows 2003, OSI and TCP/IP concepts. You should be comfortable with installing network, system applications and getting the basic operating system up and running. Each of the labs in this series will start from a default installation of CISCO devices and will then run you through the basic configurations and settings that you must use for the labs to be successful. It is very important that you follow these guidelines exactly, in order to get the best results from this course.

At the end of this tutorial you will be able to configure, troubleshoot and analyze different topologies on the LAN and WAN environments. Understand Demilitarize Zone (DMZ), procedure and policies for a secure network, multi homing with more than one Internet Service Provider (ISP), but also the mechanism of Virtual Private Network.

This virtualization Systems and Networks could be expand to quality of services, configuration of ISP policies, integration of Voice over IP (VoIP) and Video Conference.



1. Table of contents

1. Table of Contents

1.	LAB1: Secure topology with Branch office using through WAN connection.....	170
2.	LAB2: Configure AAA Authentication on Cisco Routers.....	Error! Bookmark not defined.
3.	LAB3: Inside Internet : BGPv4 and Internet Service Provider	4
4.	Server Security (LAB_4).....	7
5.	Internet Gateway (LAB_5).....	10
6.	DHCP Servers (LAB_6).....	14



LAB 1: Secure topology with Branch office using through WAN connection

This topology use PIX firewall to protect inside network from outside network. DMZ is allowed outside network to access HTTP server. VPN tunneling and IPSec tunnel mode involve establishing and maintaining a logical network connection, support authentication and encryption to keep the tunnels secure between Branch office and GW router. EIGRP routing protocol has used on R1 and R2 router.

Network Time Protocol (NTP) has used to synchronize time keeping among a set of distributed time servers and clients. Inside Server is installed AAA Radius server manage user profiles for authentication (verifying user name and password) for secure R1 and R2 router when enter username and password.

Introduction

The network topology shows for a small or medium company topology with an extension of one branch office. You will configure NTP and Syslog on all routers. You will configure SSH.

What is NTP?

Network Time Protocol (NTP) allows routers on the network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single source have more consistent time settings and Syslog messages generated can be analyzed more easily.

The Syslog Server will provide message logging in this lab. You will configure the routers to identify the remote host (Syslog server) that will receive logging messages.

You will need to configure timestamp service for logging on the routers. Displaying the correct time and date in Syslog messages is vital when using Syslog to monitor a network.

You use the CLI to configure the router to be managed securely using SSH instead of Telnet.

SSH is a network protocol that establishes a secure terminal emulation connection to a router or other networking device.

The servers have been preconfigured for NTP and Syslog services. NTP will not require authentication.

The routers have been preconfigured with the following:

Enable password: **mfulabpass75**

Password for vty lines: **mfulabvtypass75**

Routing: EIGRP Routing protocol

Activity LAB1: Configure NTP, SSH and Syslog

Topology Diagram: Topology: Secure topology with Branch office using through WAN connection

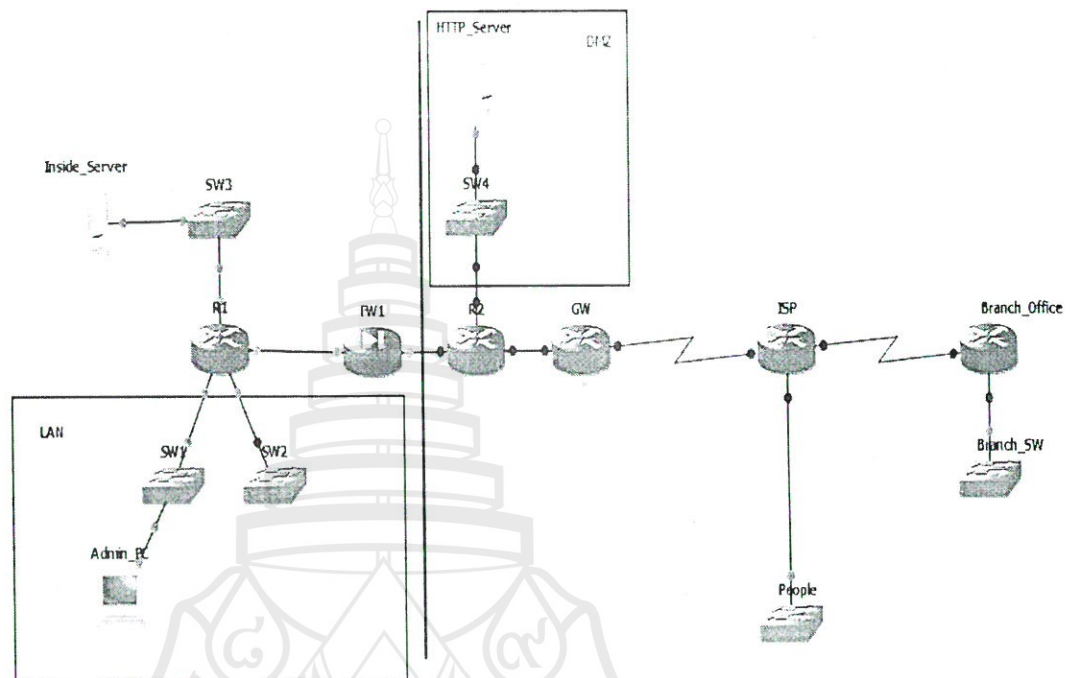


Figure 1

Addressing Table

Accessing to the routers

IOS version for this Network Security lab is 12.2(33)

- Telnet to a host 10.68.116.11 with TCP port number = 101xx, where xx is a router, switch and server or PC client numbers
- For example, telnet 10.68.116.11 10101 to get console access to a SW1.

Devices	Names	Telnet MAP
Switch	SW1	01
Switch	SW2	02
Switch	SW3	03
Switch	SW4	04
Switch	Branch_SW	04
Switch	People	05
Router	Branch_Router	06
Router	ISP	07
Router	GW(Gateway)	08
Router	R2	09
Router	R1	10
Router	FW1(Firewall)	11

SERVER	Inside Server	12
SERVER	HTTP_Server	13
PC	Admin_PC	14

Learning Objectives

- Configure routers as NTP clients.
- Configure routers to update the hardware clock using NTP.
- Configure routers to log messages to the syslog server.
- Configure routers to timestamp log messages.
- Configure local users.
- Configure VTY lines to accept SSH connections only.
- Configure RSA key pair on SSH server.
- Verify SSH connectivity from PC client and router client.

Task 1: Configure routers as NTP Clients.

Step 1. Test Connectivity

Ping from PC-C to R3.

Ping from R2 to R3.

Telnet from PC-C to R3.

Telnet from R2 to R3.

Step 2. Configure R1, R2 and R3 as NTP clients.

Verify client configuration using the command show ntp status.

Step 3. Configure routers to update hardware clock.

Configure R1, R2 and R3 to periodically update the hardware clock with the time learned from NTP.

Verify that the hardware clock was updated using the command show clock.

Step 4. Configure routers to timestamp log messages.

Step 5. Configure timestamp service for logging on the routers.

Task 2: Configure routers to log messages to the Syslog Server.

Step 1. Configure the routers to identify the remote host (Syslog Server) that will receive logging messages.

Step 2. Verify logging configuration using the command show logging.

Step 3. Examine logs of the Syslog server.

From the Config tab of the Syslog server's dialogue box, select the Syslog services button.
Observe the logging messages received from the routers.

Task 3: Configure R3 to support SSH connections.

Step 1. Configure a domain name.

Configure a domain name of mfusecurity.com on R3.

Step 2. Configure users for login from the SSH client on R3.

Create a user ID of SSHadmin with the highest possible privilege level and a secret password of Mfusshpass75.

Step 3. Configure the incoming VTY lines on R3.

Use the local user accounts for mandatory login and validation. Accept only SSH connections.

Step 4. Erase existing key pairs on R3.

Step 6. Verify the SSH configuration.

Use the **show ip ssh** command to see the current settings. Verify that the authentication timeout and retries are at their default values of 120 and 3.

Step 7. Configure SSH timeouts and authentication parameters.

The default SSH timeouts and authentication parameters can be altered to be more restrictive.

Set the timeout to 90 seconds, the number of authentication retries to 2, and the version to 2. Issue the **show ip ssh** command again to confirm that the values have been changed.

LAB2: Configure AAA Authentication on Cisco Routers

(Use the topology of Figure 1)

Configure a local user account on R1 and authenticate on the console and VTY lines using local AAA.

- Verify local AAA authentication from the R1 console and the PC-A client.
- Configure a server-based AAA authentication using TACACS+.
- Verify server-based AAA authentication from PC-B client.
- Configure a server-based AAA authentication using RADIUS.
- Verify server-based AAA authentication from PC-C client.

Introduction

The TACACS+ server has been pre-configured with the following:

Finally, you will configure router R3 to support server-based authentication using the RADIUS protocol.

The RADIUS server has been pre-configured with the following:

Task1: Basic configurations a verification AAA server

Step 1. Configure a local username on R1.

Configure a username of Admin and secret password of adminpass75.

Step 2. Configure local AAA authentication for console access on R1.

Enable AAA on R1 and configure AAA authentication for console login to use the local database.

Step 3. Configure the line console to use the defined AAA authentication method.

Step 4. Verify the AAA authentication method.

Verify the user EXEC login using the local database.

Task 2: Configure Local AAA Authentication for VTY Lines on R1

Step 1. Configure a named list AAA authentication method for VTY lines on R1.

Configure a named list called TELNET-LOGIN to authenticate logins using local AAA.

Step 2. Configure the VTY lines to use the defined AAA authentication method.

Configure the VTY lines to use the named AAA method.

Step 3. Verify the AAA authentication method.

Verify the Telnet configuration. From the command prompt of PC-A, Telnet to R1.

Task 3: Configure Server-Based AAA Authentication Using TACACS+ on R2

Step 1. Configure a backup local database entry called Admin.

For backup purposes, configure a local username of Admin and secret password of adminpass75.

Step 2. Verify the TACACS+ Server configuration.

Select the TACACS+ Server. From the Config tab, click on AAA and notice that there is a Network configuration entry for R2 and a User Setup entry for Admin2.

Step 3. Configure the TACACS+ server specifics on R2.

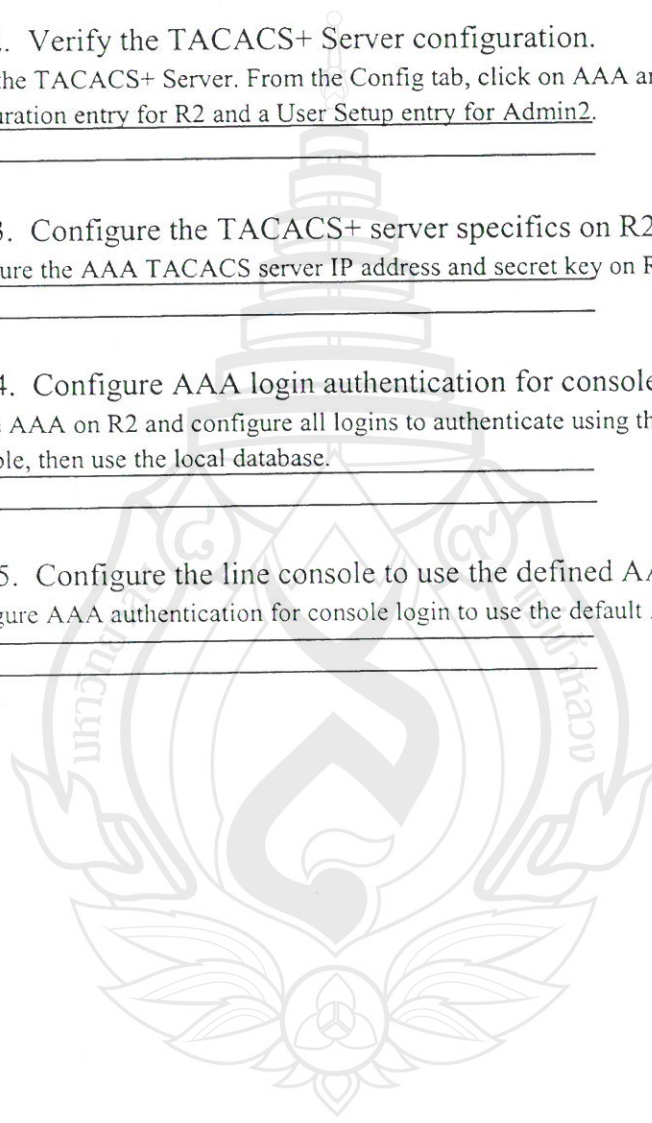
Configure the AAA TACACS server IP address and secret key on R2.

Step 4. Configure AAA login authentication for console access on R2.

Enable AAA on R2 and configure all logins to authenticate using the AAA TACACS+ server and if not available, then use the local database.

Step 5. Configure the line console to use the defined AAA authentication method.

Configure AAA authentication for console login to use the default AAA authentication method.



Accessing to the routers
IOS version for this Network Security lab is 12.2(33)

- Telnet to a host 192.168.30.11 with TCP port number = 101xx, where xx is a router, switch and server or PC client numbers
- For example, telnet 192.168.30.11 10101 to get console access to a SW C1.

Devices	Names	Telnet MAP
Switch	A1 (Access Layer)	01
Switch	A2 (Access Layer)	02
Switch	A3 (Access Layer)	03
Switch	A4 (Access Layer)	04
Switch	A5 (Access Layer)	05
Switch	D1 (Distribution Layer)	06
Switch	D2 (Distribution Layer)	07
Switch	D3 (Distribution Layer)	08
Switch	D4 (Distribution Layer)	09
Switch	D5 (Distribution Layer)	10
Switch	C1 (Core Layer)	11

Switch	C2 (Core Layer)	12
Switch	SW1	13
Switch	SW1	14
Switch	SW2	15
Switch	SW3	16
Switch	SW4	17
Switch	People	18
Router	Branch_Router	19
Router	ISP	20
Router	R2	21
Router	R1	22
Router	FW1(Firewall)	23
Router	FW2(Firewall)	24
SERVER	Inside Server	25
SERVER	HTTP_Server	26
SERVER	SERVER KERBEROS	27
SERVER	SERVER RADIUS	28
SERVER	SERVER SYSLOG	29
SERVER	SERVER IDS Software	30
SERVER	SERVER SERVICES	31
SERVER	SERVER OpenERP	32
SERVER	SERVER WEB	33
PC1	USER 1 Accounting Dept.	34
PC2	USER 1 Accounting Dept.	35
PC3	USER 2 Financial Dept.	36
PC4	USER 2 Financial Dept.	37
PC5	BranchPC	38
PC6	ThisMachine	39
PC7	VPN Remote Access	40

Introduction:

In this case scenario you will be confronted to different situation for troubleshooting, and analyzing the secure topology. You configure and repair connections, in a secure environment. As well as configure and troubleshooting Virtual Private Network. Find mistakes and errors by enforcing security with some indispensable command. This LAB allows you to report any change on the Network and verifying policies of the company. At the end of this LAB, you will be able to follow and integrating any Network administrator team. This is very important step for Network administration; you will learn the Network Security Model and what kind of attacks we can deal with on the production time.

Configure a local user account on R1 and authenticate on the console and VTY lines using local AAA.

- Verify Layer 2 Security.
- Verify Layer 3 Security.
- Verify RADIUS and TACACS+ servers.
- Verify NTP is well synchronized.
- Verify OpenERP accessibility, if not troubleshootin..
- Verify HDLC protocol is well secured, if not what is the best solution to protect layer 2 encapsulation protocol
- Verify if the policies of the companies is strong enough
- Verify design of the DMZ

- Verify the proxy WEB server if is connected to the inside servers
- Verify Firewall configuration FW1 and FW2
- Verify IPS software configuration and test the logging server response and counter attack
- Verify connection between the Branch office and the Head Quarter is secured
- Analyze the topology and change if necessary

Introduction

The TACACS+ server has been pre-configured with the following:

Finally, you will configure router R3 to support server-based authentication using the RADIUS protocol.

The RADIUS server has been pre-configured with the following:

Task1: Verify Layer 2 Security.

Step 1. Check all port unused in A1, A2, A3, A4, A5 Access layer switches.

Step 2. Configure STP blocked port.

Enable AAA on R1 and configure AAA authentication for console login to use the local database.

Step 3. Configure the line console to use the defined AAA authentication method.

Step 4. Disable all unnecessary services for Layer 2 ACCESS layer.

Task2: Verify Layer 3 Security.

Step 1. Connect via telnet and modify to an encrypted remote access using SSH

Step 2. Disable all unnecessary services for Layer 3 Distribution layer.

Step 3. Verify that Routing protocols are protected.

Step 4. Verify that HSRP Redundancy is activated on the distribution layer.

Task3: Verify RADIUS and TACACS+ servers.

Step 1. Configure a backup local database entry called Admin.

For backup purposes, configure a local username of Admin and secret password of adminpass75.

Step 2. Verify the TACACS+ Server configuration.

Select the TACACS+ Server. From the Config tab, click on AAA and notice that there is a Network configuration entry for R2 and a User Setup entry for Admin2.

Step 3. Configure the TACACS+ server specifics on R2.

Configure the AAA TACACS server IP address and secret key on R2.

Step 4. Configure AAA login authentication for console access on R2.

Enable AAA on R2 and configure all logins to authenticate using the AAA TACACS+ server and if not available, then use the local database.

Step 5. Configure the line console to use the defined AAA authentication method.

Configure AAA authentication for console login to use the default AAA authentication method.

Task4: Verify NTP is well synchronized.

Step 1. Verify that all devices are configure as client NTP and only the NTP server master and A backup NTP server exist in this topology

Step 2. Who are they?

Task5: Verify OpenERP accessibility, if not troubleshooting.

Step 1. Connect with a Account from Financial Department

Step 2. Check that the connection is only prohibited for Accounting Department

Task6: Verify HDLC protocol is well secured, if not what is the best solution to protect layer 2 encapsulation protocol.

Step 1. Why HDLC is not protected?

Step 2. Which encapsulation layer 2 secure protocol should you change?

Task7: Verify if the policies of the companies is strong enough.

Step 1. Analyze the topology and find out more about the policies.

Step 2. Is the password policies strong enough?

Step 3. If not change it?

Task8: Verify design of the DMZ

Step 1. Analyze the topology and find out more about the DMZ.

Step 2. Verify CBAC

Step 3. Check if the access list is well protected?

Task9: Verify the proxy WEB server if is connected to the inside servers

Step 1. Can we connect to the proxy WEB server?

Step 2. If not, why?

Step 3. Look at the access list in FW1 and make change on order to get connection

Task10: Verify Firewall configuration FW1 and FW2.

Step 1. Do a show command on both Firewall

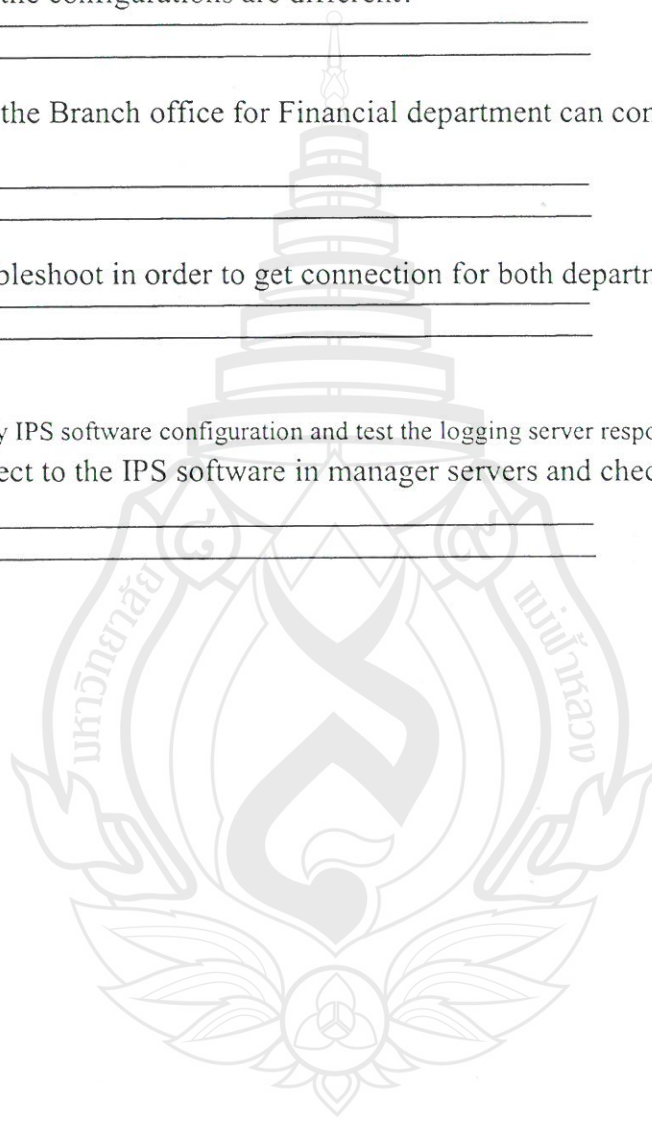
Step 2. Why the configurations are different?

Step 3. Why the Branch office for Financial department can connect and accounting department cannot?

Step 4. Troubleshoot in order to get connection for both departments?

Task11: Verify IPS software configuration and test the logging server response and counter attack

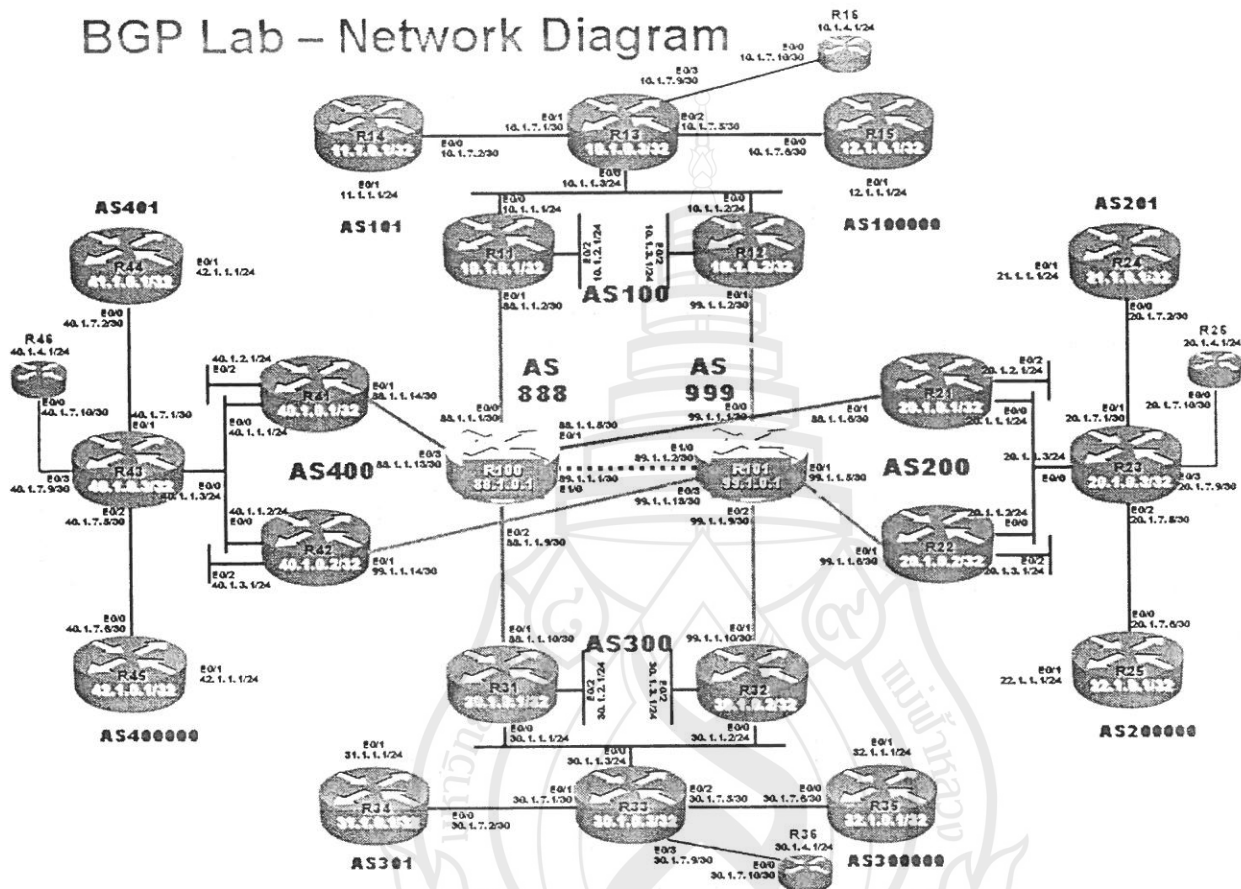
Step 1. Connect to the IPS software in manager servers and check if virus signature is updated.



LAB 3: Inside Internet: BGP (Version 4) and Internet Service Provider

TOPOLOGY DIAGRAM:

BGP Lab – Network Diagram



Introduction:

This LAB is for advance network skill students or very motivated student. In this LAB you have to configure step by step all CISCO routers inside many Internet Service Providers. You will analyze how Autonomous System interact each other and how the customer can be a passive or an active Autonomous System. As while how to protect data for the customer but also protect network against the customer.

We will discuss and analyze on multi homing and in which case we should increase the bandwidth or enforce the redundancy in order to reach 100 % internet connection.

Accessing to the routers

- Telnet to a host 10.68.116.11 with TCP port number = 101xx, where xx is a router number
- For example, telnet 10.68.116.11 10111 to get console access to a router R11.

BGP Lab Scenario

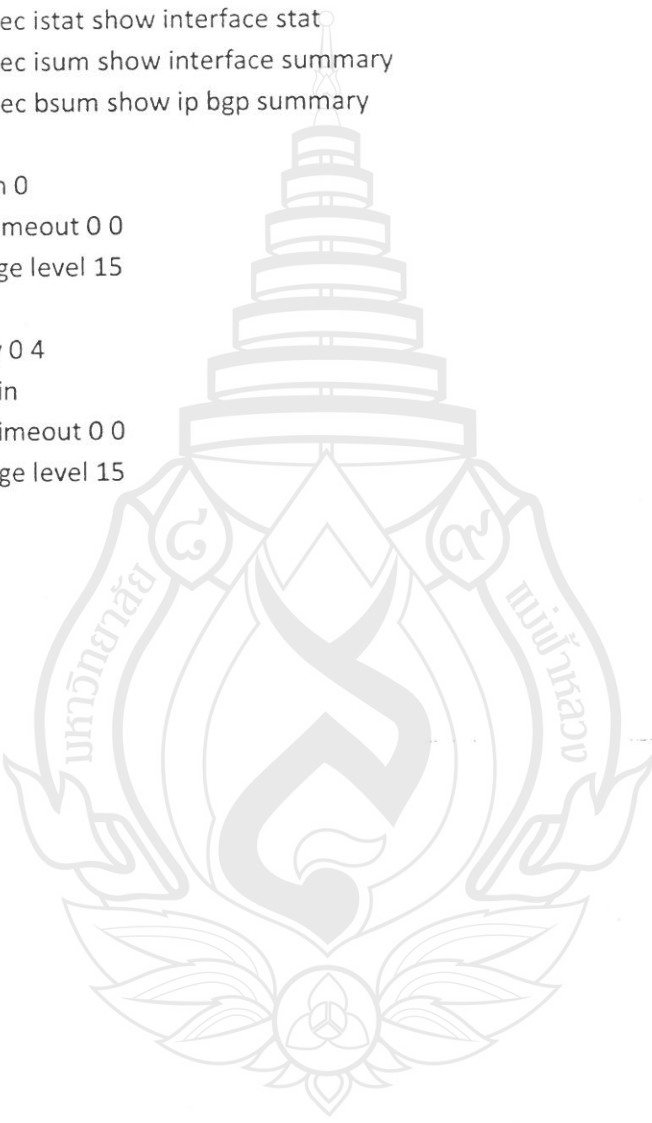
- Each ISP will be connecting to TWO Upstream Providers AS 888 and 999 respectively
- Each ISP has THREE Routers running OSPF/BGP Routing
Prefixes = x0.1.0.0/24 – x0.1.7.0/24
- Each ISP has TWO customers connecting and running eBGP.
ASx01 Prefixes = x1.1.0.0/24 – x1.1.1.0/24
ASx02 Prefixes = x2.1.0.0/24 – x2.1.1.0/24
- Each ISP has ONE customer with Static Routing.
Prefixes = x0.1.4.0/24

ALL routers' BASIC configuration

```

service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
!
enable password cisco
!
```

```
no ip domain-lookup
!  
alias exec cc clear counter  
alias exec r show ip route  
alias exec b show ip interface brief  
alias exec istat show interface stat  
alias exec isum show interface summary  
alias exec bsum show ip bgp summary  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
!  
line vty 0 4  
  no login  
  exec-timeout 0 0  
  privilege level 15  
!
```



OSPF-01 Configuration (1)

- Configure IP addresses according to the Diagram and “NO Shutdown” under the interfaces being used.
- Configure CEF (config# ip cef)
- Configure a Static Default Route on Rx1 and Rx2 to the Upstream Provider AS 888 and AS 999 respectively.

- Configure OSPF Routing on Rx1, Rx2 and Rx3 using OSPF Process ID = 1, and Area = 0.
- Configure Loopback0 as OSPF Router ID
- Configure Message Digest 5 Authentication for Area 0 with Key ID 1 = cisco
- Configure OSPF Network only for the Local Subnets including Loopback0's Subnet. DO NOT Advertise OSPF Packets to the Interfaces connecting to Customers.
- Configure Rx1 and Rx2 to Advertise the Default Route via OSPF.
- Configure a Static Default Route on Rx6 to Rx3.
- Configure a Static Route on Rx3 for Rx6's Network.
- Configure Rx3 to Advertise a Static Route to Rx6's Network via OSPF
- Verify the connectivity (*ping, trace, show interface, show cdp neighbors, show ip route*)
- Verify the OSPF neighbors (*show ip ospf neighbor*)
- Verify the OSPF Interface Parameters (Network type, Cost etc.) (*show ip ospf interface*)

OSPF-01 OSPF Configuration (2)

***** Rx1 *****

```
interface Loopback0
ip address x0.1.0.1 255.255.255.255
!
interface Ethernet0/0
ip address x0.1.1.1 255.255.255.0
ip ospf message-digest-key 1 md5 cisco
```

***** Rx2 *****

```
interface Loopback0
ip address x0.1.0.2 255.255.255.255
!
interface Ethernet0/0
ip address x0.1.1.2 255.255.255.0
ip ospf message-digest-key 1 md5 cisco
!
```


<pre> ! interface Ethernet0/1 ip address 88.1.1.yy 255.255.255.252 ! interface Ethernet0/2 ip address x0.1.2.1 255.255.255.0 ! ip route 0.0.0.0 0.0.0.0 88.1.1.y ! router ospf 1 router-id x0.1.0.1 log-adjacency-changes area 0 authentication message-digest passive-interface default no passive-interface Ethernet0/0 network x0.1.0.1 0.0.0.0 area 0 network x0.1.1.1 0.0.0.0 area 0 network x0.1.2.1 0.0.0.0 area 0 default-information originate </pre>	<pre> interface Ethernet0/1 ip address 99.1.1.yy 255.255.255.252 ! interface Ethernet0/2 ip address x0.1.3.1 255.255.255.0 ! ip route 0.0.0.0 0.0.0.0 99.1.1.y ! router ospf 1 router-id x0.1.0.2 log-adjacency-changes area 0 authentication message-digest passive-interface default no passive-interface Ethernet0/0 network x0.1.0.2 0.0.0.0 area 0 network x0.1.1.2 0.0.0.0 area 0 network x0.1.3.1 0.0.0.0 area 0 default-information originate </pre>
--	--

- Recommended Command “description <Interface description>”

BGP-01 Configuration (1)

```

***** Rx1 *****
router bgp x00
no synchronization
bgp log-neighbor-changes
neighbor x0.1.0.2 remote-as x00
neighbor x0.1.0.2 update-source Loopback0
neighbor x0.1.0.3 remote-as x00
neighbor x0.1.0.3 update-source Loopback0
neighbor 88.1.0.1 remote-as 888
neighbor 88.1.0.1 ebgp-multihop 2
neighbor 88.1.0.1 update-source Loopback0
no auto-summary
!
ip route 88.1.0.1 255.255.255.255 88.1.1.y

```

```

***** Rx2 *****
router bgp x00
no synchronization
bgp log-neighbor-changes
neighbor x0.1.0.1 remote-as x00
neighbor x0.1.0.1 update-source Loopback0
neighbor x0.1.0.3 remote-as x00
neighbor x0.1.0.3 update-source Loopback0
neighbor 99.1.1.y remote-as 999
no auto-summary

```

```

***** Rx3 *****
router bgp x00
no synchronization
bgp log-neighbor-changes
neighbor x0.1.0.1 remote-as x00
neighbor x0.1.0.1 update-source Loopback0
neighbor x0.1.0.2 remote-as x00
neighbor x0.1.0.2 update-source Loopback0
neighbor x0.1.7.2 remote-as x01
neighbor x0.1.7.6 remote-as x00000
no auto-summary

```

```

***** Rx4 *****
router bgp x01
no synchronization
bgp log-neighbor-changes
neighbor x0.1.7.1 remote-as x00
no auto-summary

```

```

***** Rx5 *****
router bgp x00000
no synchronization
bgp log-neighbor-changes
neighbor x0.1.7.5 remote-as x00
no auto-summary

```

- Recommended Command “neighbor <x.x.x.x> description <desc>”

BGP-02 Configuration (1)

- Configure Rx1, Rx2 and Rx3 to advertise the following Prefixes :

x0.1.0.0/24

x0.1.1.0/24

x0.1.2.0/24

x0.1.3.0/24

x0.1.4.0/24

x0.1.7.0/24.

- Configure Rx4 to advertise the Prefixes - x1.1.0.0/24 and x1.1.1.0/24
- Configure Rx5 to advertise the Prefixes - x2.1.0.0/24 and x2.1.1.0/24
- Configure the Static Routes to the above Prefixes to NULL0 with Higher Metric.
- Verify the BGP Prefixes and Neighbors
 - *show ip bgp*
 - *Show ip bgp <prefix>*
 - *show ip route*
 - *show ip bgp summary*
 - *show ip bgp neighbors <neighbor> routes*
 - *show ip bgp neighbors <neighbor> advertised-routes*

BGP-02 BGP Configuration (2)

***** Rx1, Rx2 and Rx3 *****

```
router bgp x00
 network x0.1.0.0 mask 255.255.255.0
 network x0.1.1.0 mask 255.255.255.0
 network x0.1.2.0 mask 255.255.255.0
 network x0.1.3.0 mask 255.255.255.0
 network x0.1.4.0 mask 255.255.255.0
 network x0.1.7.0 mask 255.255.255.0
!
ip route x0.1.0.0 255.255.255.0 Null0 250
ip route x0.1.1.0 255.255.255.0 Null0 250
ip route x0.1.2.0 255.255.255.0 Null0 250
ip route x0.1.3.0 255.255.255.0 Null0 250
ip route x0.1.4.0 255.255.255.0 Null0 250
ip route x0.1.7.0 255.255.255.0 Null0 250
```

***** Rx4 *****

```
router bgp x01
 network x1.1.0.0 mask 255.255.255.0
 network x1.1.1.0 mask 255.255.255.0
!
ip route x1.1.0.0 255.255.255.0 Null0 250
ip route x1.1.1.0 255.255.255.0 Null0 250
```

***** Rx5 *****

```
router bgp x00000
 network x2.1.0.0 mask 255.255.255.0
 network x2.1.1.0 mask 255.255.255.0
!
ip route x2.1.0.0 255.255.255.0 Null0 250
ip route x2.1.1.0 255.255.255.0 Null0 250
```

BGP-03 Configuration (1)

- Configure Rx1, Rx2 and Rx3 the command “neighbor <neighbor> next-hop-self” for Neighbors - Rx1, Rx2 and Rx3.
- Configure Rx1-5 the command “neighbor <neighbor> soft-reconfiguration in” for all Neighbors.
- Configure Rx3 to advertise the default-route (0.0.0.0/0) to Rx4 and Rx5
- Verify the BGP Prefixes and Neighbors
 - *show ip bgp*
 - *show ip route*
 - *show ip bgp summary*
 - *show ip bgp neighbors <neighbor> routes*
 - *show ip bgp neighbors <neighbor> advertised-routes*
 - *show ip bgp neighbors <neighbor> received-routes*



***** Rx1 *****

```
router bgp x00
neighbor x0.1.0.2 next-hop-self
neighbor x0.1.0.2 soft-reconfiguration inbound
neighbor x0.1.0.3 next-hop-self
neighbor x0.1.0.3 soft-reconfiguration inbound
neighbor 88.1.0.y soft-reconfiguration inbound
```

***** Rx2 *****

```
router bgp x00
neighbor x0.1.0.1 next-hop-self
neighbor x0.1.0.1 soft-reconfiguration inbound
neighbor x0.1.0.3 next-hop-self
neighbor x0.1.0.3 soft-reconfiguration inbound
neighbor 99.1.1.y soft-reconfiguration inbound
```

***** Rx3 *****

```
router bgp x00
neighbor x0.1.0.1 next-hop-self
neighbor x0.1.0.1 soft-reconfiguration inbound
neighbor x0.1.0.2 next-hop-self
neighbor x0.1.0.2 soft-reconfiguration inbound
neighbor x0.1.7.2 soft-reconfiguration inbound
neighbor x0.1.7.6 soft-reconfiguration inbound
neighbor x0.1.7.2 default-originate
neighbor x0.1.7.6 default-originate
```

***** Rx4 *****

```
router bgp x01
neighbor x0.1.7.1 soft-reconfiguration inbound
```

***** Rx5 *****

```
router bgp x00000
neighbor x0.1.7.5 soft-reconfiguration inbound
```

BGP-04 Configuration (1)

- Configure Rx3 to Filter ONLY the Prefixes and AS-Path from Rx4 and Rx5.
- Configure Rx1 and Rx2 to Advertise ONLY the Local Prefixes and Customer's Prefixes OUT to AS 888 and AS 999.
- Verify the BGP Prefixes and Neighbors
 - *show ip prefix-list <name>*
 - *show ip as-path-access-list <number>*
 - *show route-map <name>*
 - *show ip bgp*
 - *show ip bgp regexp <regexp>*
 - *show ip bgp neighbors <neighbor> received-routes*
 - *show ip bgp neighbors <neighbor> routes*
 - *show ip bgp neighbors <neighbor> advertised-routes*
 - *Clear ip bgp <neighbor> soft in*
 - *Clear ip bgp <neighbor> soft out*

```

***** Rx1 *****
ip as-path access-list 1 permit ^$
ip as-path access-list 2 permit _x01$
ip as-path access-list 2 permit _x00000$
!
route-map MY-PREFIXES permit 10
  match as-path 1
!
route-map MY-PREFIXES permit 20
  match as-path 2
!
router bgp x00
  neighbor 88.1.0.y route-map MY-PREFIXES out

```

```

***** Rx2 *****
ip as-path access-list 1 permit ^$
ip as-path access-list 2 permit _x01$
ip as-path access-list 2 permit _x00000$
!
route-map MY-PREFIXES permit 10
  match as-path 1
!
route-map MY-PREFIXES permit 20
  match as-path 2
!
router bgp x00
  neighbor 99.1.1.y route-map MY-PREFIXES out

```

```

***** Rx3 *****
ip as-path access-list 1 permit _x01$
ip as-path access-list 2 permit _x00000$
!
ip prefix-list ASx01 seq 5 permit x1.1.0.0/24
ip prefix-list ASx01 seq 10 permit x1.1.1.0/24
!
ip prefix-list ASx00000 seq 5 permit x2.1.0.0/24
ip prefix-list ASx00000 seq 10 permit x2.1.1.0/24
!
route-map FILTER-ASx01 permit 10
  match ip address prefix-list ASx01
  match as-path 1
!
route-map FILTER-ASx00000 permit 10
  match ip address prefix-list ASx00000
  match as-path 2
!
router bgp 100
  neighbor x0.1.7.2 route-map FILTER-ASx01 in
  neighbor x0.1.7.6 route-map FILTER-ASx00000 in

```

BGP-05 Configuration (1)

- Configure Rx1 and Rx2 to Summarize the Prefixes Advertisement to AS888 and AS999 as x0.1.0.0/21.
- Verify the BGP Prefixes
 - *show ip prefix-list <name>*
 - *show ip as-path-access-list <number>*
 - *show route-map <name>*
 - *show ip bgp*
 - *show ip bgp regexp <regexp>*
 - *show ip bgp neighbors <neighbor> received-routes*
 - *show ip bgp neighbors <neighbor> routes*
 - *show ip bgp neighbors <neighbor> advertised-routes*
 - *Clear ip bgp <neighbor> soft in*
 - *Clear ip bgp <neighbor> soft out*

```

***** Rx1 *****
ip as-path access-list 1 permit ^$
ip as-path access-list 2 permit _x01$
ip as-path access-list 2 permit _x000000$
!
ip prefix-list SUMMARY-PREFIX seq 5 permit x0.1.0.0/21
!
route-map MY-PREFIXES permit 10
  match ip address prefix-list SUMMARY-PREFIX
  match as-path 1
!
route-map MY-PREFIXES permit 20
  match as-path 2
!
ip route x0.1.0.0 255.255.248.0 Null0 250
!
router bgp 100
  network x0.1.0.0 mask 255.255.248.0
  neighbor 88.1.0.y route-map MY-PREFIXES out

```

```

***** Rx2 *****
ip as-path access-list 1 permit ^$
ip as-path access-list 2 permit _x01$
ip as-path access-list 2 permit _x000000$
!
ip prefix-list SUMMARY-PREFIX seq 5 permit x0.1.0.0/21
!
route-map MY-PREFIXES permit 10
  match ip address prefix-list SUMMARY-PREFIX
  match as-path 1
!
route-map MY-PREFIXES permit 20
  match as-path 2
!
ip route x0.1.0.0 255.255.248.0 Null0 250
!
router bgp 100
  network x0.1.0.0 mask 255.255.248.0
  neighbor 99.1.1.y route-map MY-PREFIXES out

```

BGP-06 Configuration (1)

- Configure Rx1 and Rx2 to advertise a Prefix x0.1.2.0/24 to AS 888 and AS 999, and the incoming traffic to this prefix should come from AS 888.
- Configure Rx1 and Rx2 to advertise a Prefix x0.1.3.0/24 to AS 888 and AS 999, and the incoming traffic to this prefix should come from AS 999.
- Verify the BGP Prefixes
 - *show ip prefix-list <name>*
 - *show route-map <name>*
 - *show ip bgp*
 - *show ip bgp neighbors <neighbor> received-routes*
 - *show ip bgp neighbors <neighbor> routes*
 - *show ip bgp neighbors <neighbor> advertised-routes*
 - *Clear ip bgp <neighbor> soft in*
 - *Clear ip bgp <neighbor> soft out*

```

***** Rx1 *****
ip as-path access-list 1 permit ^$
ip as-path access-list 2 permit x01$
ip as-path access-list 2 permit _x00000$
!
ip prefix-list SUMMARY-PREFIX seq 5 permit x0.1.0.0/21
ip prefix-list PREFIX-X0-1-2 seq 5 permit x0.1.2.0/24
ip prefix-list PREFIX-X0-1-3 seq 5 permit x0.1.3.0/24
!
route-map MY-PREFIXES permit 10
match ip address prefix-list SUMMARY-PREFIX
match as-path 1
!
route-map MY-PREFIXES permit 20
match as-path 2
!
route-map MY-PREFIXES permit 30
match ip address prefix-list PREFIX-X0-1-2
!
route-map MY-PREFIXES permit 40
match ip address prefix-list PREFIX-X0-1-3
set as-path prepend x00 x00 x00
!
ip route x0.1.0.0 255.255.248.0 Null0 250
ip route x0.1.2.0 255.255.255.0 Null0 250
ip route x0.1.3.0 255.255.255.0 Null0 250
!
router bgp x00
network x0.1.0.0 mask 255.255.248.0
network x0.1.2.0 mask 255.255.255.0
network x0.1.3.0 mask 255.255.255.0
neighbor 88.1.0.y route-map MY-PREFIXES out

```


BGP-06 BGP Configuration (2)

```
***** Rx2 *****

ip as-path access-list 1 permit ^$
ip as-path access-list 2 permit _x01$
ip as-path access-list 2 permit _x00000$
!
ip prefix-list SUMMARY-PREFIX seq 5 permit x0.1.0.0/21
ip prefix-list PREFIX-X0-1-2 seq 5 permit x0.1.2.0/24
ip prefix-list PREFIX-X0-1-3 seq 5 permit x0.1.3.0/24
!
route-map MY-PREFIXES permit 10
  match ip address prefix-list SUMMARY-PREFIX
  match as-path 1
!
route-map MY-PREFIXES permit 20
  match as-path 2
!
route-map MY-PREFIXES permit 30
  match ip address prefix-list PREFIX-X0-1-2
  set as-path prepend x00 x00 x00
!
route-map MY-PREFIXES permit 40
  match ip address prefix-list PREFIX-X0-1-3
!
ip route x0.1.0.0 255.255.248.0 Null0 250
ip route x0.1.2.0 255.255.255.0 Null0 250
ip route x0.1.3.0 255.255.255.0 Null0 250
!
router bgp x00
  network x0.1.0.0 mask 255.255.248.0
  network x0.1.2.0 mask 255.255.255.0
  network x0.1.3.0 mask 255.255.255.0
  neighbor 99.1.1.y route-map MY-PREFIXES out
```


BGP-07 Configuration (1)

- Configure Rx1 to receive the a prefixes from R100, and the outgoing traffic to the prefixes source from AS Y01 should go out via R100.
- Configure Rx2 to receive the a prefixes from R101, and the outgoing traffic to the prefixes source from AS Y00000 should go out via R101.
- Verify the BGP Prefixes
 - *show route-map <name>*
 - *show ip bgp*
 - *show ip bgp neighbors <neighbor> received-routes*
 - *show ip bgp neighbors <neighbor> routes*
 - *show ip route <prefix>*
 - *Clear ip bgp <neighbor> soft in*
 - *Clear ip bgp <neighbor> soft out*

```

***** Rx1 *****
ip as-path access-list 3 permit A01$
ip as-path access-list 3 permit B01$
ip as-path access-list 3 permit C01$
!
route-map LOCAL-PREF permit 10
  match as-path 3
  set local-preference 200
!
route-map LOCAL-PREF permit 20
!
router bgp x00
  neighbor 88.1.0.y route-map LOCAL-PREF in

```

```

***** Rx1 *****
ip as-path access-list 3 permit A01$
ip as-path access-list 3 permit B01$
ip as-path access-list 3 permit C01$
!
route-map LOCAL-PREF permit 10
  match as-path 3
  set local-preference 200
!
route-map LOCAL-PREF permit 20
!
router bgp x00
  neighbor 88.1.0.y route-map LOCAL-PREF in

```

QoS-08 Bandwidth Limit Configuration (1)

- Configure Rx3 to limit the Upstream and Downstream Bandwidth from ASx01 to 250 Kbps.
- Configure Rx3 to limit the Upstream and Downstream Bandwidth from ASx02 to 500 Kbps.

```

policy-map <policy-name>
  class class-default
    police <rate bps> <burst-size bytes>
    ! <burst size> = <rate> x 1.5 /8
    !
  interface <interface>
    service-policy input <policy-map-name>
    service-policy output <policy-map-name>

```

- Verify the QoS Configuration and Monitoring
 - *show class-map <class>*
 - *show policy-map <policy>*
 - *show policy-map interface <interface>*
 - *show interface <interface>*
 - *show interface summary*

```

***** Rx3 *****

policy-map 250K
  class class-default
    police 250000 50000
  !
policy-map 500K
  class class-default
    police 500000 100000
  !
interface Ethernet0/1
  load-interval 30
  service-policy input 250K
  service-policy output 250K
!
interface Ethernet0/2
  load-interval 30
  service-policy input 500K
  service-policy output 500K

```

QoS-09 Class-Based Policing (1)

- Configure Rx3 to limit the Upstream/Downstream Bandwidth between ASx01 and Local Prefixes to 200 Kbps.
- Configure Rx3 to limit the Upstream/Downstream Bandwidth between ASx01 and Other Prefixes to 100 Kbps.
- Verify the QoS Configuration and Monitoring
 - *show access-list*
 - *show class-map <class>*
 - *show policy-map <policy>*
 - *show policy-map interface <interface>*
 - *show interface <interface>*

```

***** Rx3 *****
ip access-list extended ASx01-Local
 permit ip x1.1.0.0 0.0.1.255 x0.1.0.0 0.0.7.255
 permit ip x1.1.0.0 0.0.1.255 x2.1.0.0 0.0.1.255
!
ip access-list extended ASx01-Other
 deny ip x1.1.0.0 0.0.1.255 x0.1.0.0 0.0.7.255
 deny ip x1.1.0.0 0.0.1.255 x2.1.0.0 0.0.1.255
 permit ip any any
!
ip access-list extended Local-ASx01
 permit ip x0.1.0.0 0.0.7.255 x1.1.0.0 0.0.1.255
 permit ip x2.1.0.0 0.0.1.255 x1.1.0.0 0.0.1.255
!
ip access-list extended Other-ASx01
 deny ip x0.1.0.0 0.0.7.255 x1.1.0.0 0.0.1.255
 deny ip x2.1.0.0 0.0.1.255 x1.1.0.0 0.0.1.255
 permit ip any any
!
class-map match-all ASx01-Local-Class
 match access-group name ASx01-Local
!
class-map match-all ASx01-Other-Class
 match access-group name ASx01-Other
!
class-map match-all Local-ASx01-Class
 match access-group name Local-ASx01
!
class-map match-all Other-ASx01-Class
 match access-group name Other-ASx01

```

```

***** Rx3 *****
policy-map ASx01-QOS-IN
 class ASx01-Local-Class
  police 200000 37500
 class ASx01-Other-Class
  police 100000 18750
!
policy-map ASx01-QOS-OUT
 class Local-ASx01-Class
  police 200000 37500
 class Other-ASx01-Class
  police 100000 18750
!
interface Ethernet0/1
 load-interval 30
 NO service-policy input 250K
 NO service-policy output 250K
 service-policy input ASx01-QOS-IN
 service-policy output ASx01-QOS-OUT

```

Netflow-10 Netflow Configuration (1)

- Configure Rx1, Rx2 and Rx3 for Netflow Ingress Accounting on All interfaces.
- Configure Netflow Export and Top Talkers.
- Verify Netflow Configuration and Monitoring
 - *show ip cache flow*
 - *show ip flow export (verbose)*
 - *show ip flow top-talkers (verbose)*

```
***** Rx2 *****  
interface Ethernet0/0  
  ip flow ingress  
!  
interface Ethernet0/1  
  ip flow ingress  
!  
interface Ethernet0/2  
  ip flow ingress  
!  
interface Ethernet0/3  
  ip flow ingress  
!  
ip flow-export destination 99.99.99.99 9996  
!  
ip flow-top-talkers  
  top 100  
  sort-by bytes
```

6. Books, materials, tools:

- [1] Larry Peterson, Bruce Davie, Computer networks - A systems approach, 3rd Edition, Morgan Kauffman, 2004.
- [2] Samuel T. King, George W. Dunlap, Peter M. Chen, Operating System Support for Virtual Machines, Proceedings of the 2003 USENIX Technical Conference, pp 71-84, June 9-14, San Antonio, TX, USA, 2003.
- [3] R. Goldberg. Architectural Principles for Virtual Computer Systems. PhD thesis, Harvard University, February 1973.
- [4] Fermín Galán, David Fernández, Javier Rúiz, Omar Walid, Tomás de Miguel. "A Virtualization Tool in Computer Network Laboratories", 5th International Conference on Information Technology Based Higher Education and Training (ITHET'04), Istanbul, Turkey, May 2004.
- [5] Netkit project (Web site), <http://www.netkit.org>, retrieved 2006.
- [6] M. Zec, M. Mikuc, Operating System Support for Integrated Network Emulation in IMUNES, Proceedings of the 1st Workshop on Operating System and Architectural Support for the on demand IT InfraStructure / ASPLOS-XI, Boston, USA, October 2004.
- [7] Einar project (Web site), URL:<http://www.isk.kth.se/proj/einar/>, retrieved 2006.
- [8] B. Kneale, A. Y. De Horta, I. Box, Velnet: virtual environment for learning networking, Proceedings of the sixth conference on Australian computing education - Volume 30, p 161-168, Dunedin, New Zealand, 2004.
- [9] Microsoft Virtual PC 2004 (Web site), URL:<http://www.microsoft.com/windows/virtualpc/default.mspx>, 2006.
- [10] Dobrilovic D., Odadžić B., OSPF protocol simulation in virtual network laboratory (in Serbian), Proceedings of the 5th conference Infoteh-Jahorina 2006, March 22-24, Jahorina, Bosnia & Herzegovina, 2006.
- [11] Sylvia Ratnasamy, Andrey Ermolinskiy and Scott Shenker, Revisiting IP Multicast, ACM SIGCOMM Computer Communication Review, Vol. 36, Issue 4, pp. 15-26, October 2006.
- [12] Jon Crowcroft, Steven Hand, Richard Mortier, Timothy Roscoe and Andrew Warfield, QoS's Downfall: At the bottom, or not at all !, Proc. of the ACM SIGCOMM workshop on Revisiting IP QoS: What have we learned, why do we care?, pp. 109-114, 2003.
- [13] Open source: OpenERP, ERP, GNS3, VirtualPC, VMware
- [14] GNS3, an open source multiplatform graphical network simulator (2009). GNS3 overview. Available: <http://www.gns3.net/> [2010, February 12].
- [15] Mark Ciampa. (2005). Security + Guild to Network Security Fundamentals Second Edition. USA: Course Technology.
- [16] Ulrich Windl, et al., NTP Group. (2006) Network time protocol(NTP). Available: <http://www.ntp.org/ntpfaq/NTP-s-def.htm> [2010, February 13].
- [17] Peter J. Welcher. (2002). PIX firewall. Available:<http://www.netcraftsmen.net/resources/archived-articles/369-cisco-pix-firewall-basics.html>[2010, February 14].
- [18] ESET (2009). What is identification and authentication? Available: <http://www.eset.com/download/whitepapers/EsetWP-SocialSecurityNumbers20090810.pdf> [2010, February 26].
- [19] Routing TCP/IP – Jeff Doyle CCIE #1919 Volume I Techmedia, 2002 Delhi India.
- [20] TCP/IP Illustrated -- Richard Stevens Volume II Pearson Education 2001, Delhi, India.

- [21] Designing and Developing Scalable IP Networks By Guy Davies, Telindus, UK John Wiley & Sons publishers
- [22] The Free RADIUS Server Project. (2009). RADIUS server overview.
Available: http://wiki.freeradius.org/Main_Page [2010, February 13]
- [23] Cisco Systems, Inc. (2010). TACACS+ and RADIUS comparison.
Available: https://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml [2008, February 13]



Research Team

1. Khaled KESSALI (95%)

School of Information Technology

Mae Fah Luang University

Chiang Rai, Thailand

Email: kessalik@yahoo.fr, khaled@mfu.ac.th

Tel. 0849878640

2. Dr. Guy Saidana Consultant

Chief leader, Consultant, Trainer Network and TELECOM Security

ALCATEL LUCENT FRANCE

Paris, France

Email: guy.saidana@gmail.com

Tel. 0855462682, +33

3. Dr. Thongchai Yooyativong Consultant

School of Information Technology

Mae Fah Luang University

Chiang Rai, Thailand

Tel. 053-916741

Email: thongchai@mfu.ac.th

CONCLUSION

The result that we used GNS3 to simulate network security topology, it has high efficient because GNS3 use real IOS file form Cisco router except some commands of switch layer 2 doesn't work. The benefit of GNS3 is in some situation, we cannot connect and try to configure security protocol or routing protocol in real device so, it's better to try it on GNS3 and then implement the complete structure and configure it to real device:

Advantages

- Emulation from real Cisco IOS so, it has full functional as Cisco device.
- GNS3 can communication to other PC.
- It can communication to virtual NIC on PC.
- It is multiplatform software.
- It is good for network security practice.
- It is open source software.
- It has Qemu for PIX firewall emulation.
- It support package capture program such as Wireshark.

Disadvantages

- It doesn't fully support with ASA firewall.
- GNS3 use router 16 ports modules to work as switch layer 2 so, few commands in switch layer 2 doesn't work.
- It need high performance computer to run a large network design.
- Sometimes GNS3 closes automatically or crashed.
- It hard to transfer project file to other machine.
- Mac OS has less function in GNS3 than Windows.
- It has not IDS or IPS devices support.
- It has limited of IOS device support.

In the other hand, interaction with our simulation shows that student interact quiet well, because of the real enterprise network. Students are exciting especially when we simulate scenarios as a game. We are still focus on how students can learn funny with some network connection application connected to the simulator server. This will be my next article.



REFERENCE

Books, materials, tools:

- [1] Larry Peterson, Bruce Davie, Computer networks - A systems approach, 3rd Edition, Morgan Kaufman, 2004.
- [2] Samuel T. King, George W. Dunlap, Peter M. Chen, Operating System Support for Virtual Machines, Proceedings of the 2003 USENIX Technical Conference, pp 71-84, June 9-14, San Antonio, TX, USA, 2003.
- [3] R. Goldberg. Architectural Principles for Virtual Computer Systems. PhD thesis, Harvard University, February 1973.
- [4] Fermin Galán, David Fernández, Javier Rúiz, Omar Walid, Tomás de Miguel. "A Virtualization Tool in Computer Network Laboratories", 5th International Conference on Information Technology Based Higher Education and Training (ITHET'04), Istanbul, Turkey, May 2004.
- [5] Netkit project (Web site), <http://www.netkit.org>, retrieved 2006.
- [6] M. Zec, M. Mikuc, Operating System Support for Integrated Network Emulation in IMUNES, Proceedings of the 1st Workshop on Operating System and Architectural Support for the on demand IT InfraStructure / ASPLOS-XI, Boston, USA, October 2004.
- [7] Einar project (Web site), URL:<http://www.isk.kth.se/proj/einar/>, retrieved 2006.
- [8] B. Kneale, A. Y. De Horta, I. Box, Velnet: virtual environment for learning networking, Proceedings of the sixth conference on Australian computing education - Volume 30, p 161-168, Dunedin, New Zealand, 2004.
- [9] Microsoft Virtual PC 2004 (Web site), URL:<http://www.microsoft.com/windows/virtualpc/default.mspx>, 2006.
- [10] Dobrilovic D., Odadžić B., OSPF protocol simulation in virtual network laboratory (in Serbian), Proceedings of the 5th conference Infoteh-Jahorina 2006, March 22-24, Jahorina, Bosnia & Herzegovina, 2006.
- [11] Sylvia Ratnasamy, Andrey Ermolinskiy and Scott Shenker, Revisiting IP Multicast, ACM SIGCOMM Computer Communication Review, Vol. 36, Issue 4, pp. 15-26, October 2006.
- [12] Jon Crowcroft, Steven Hand, Richard Mortier, Timothy Roscoe and Andrew Warfield, QoS's Downfall: At the bottom, or not at all !, Proc. of the ACM SIGCOMM workshop on Revisiting IP QoS: What have we learned, why do we care?, pp. 109-114, 2003.
- [13] Open source: OpenERP, ERP, GNS3, VirtualPC, VMware
- [14] GNS3, an open source multiplatform graphical network simulator (2009). GNS3 overview. Available: <http://www.gns3.net/> [2010, February 12].
- [15] Mark Ciampa. (2005). Security + Guild to Network Security Fundamentals Second Edition. USA: Course Technology.
- [16] Ulrich Windl, et al., NTP Group. (2006) Network time protocol(NTP). Available: <http://www.ntp.org/ntpfaq/NTP-s-def.htm> [2010, February 13].
- [17] Peter J. Welcher. (2002). PIX firewall. Available: <http://www.netcraftsmen.net/resources/archived-articles/369-cisco-pix-firewall-basics.html> [2010, February 14].
- [18] ESET (2009). What is identification and authentication? Available: <http://www.eset.com/download/whitepapers/EsetWP-SocialSecurityNumbers20090810.pdf> [2010, February 26].
- [19] Routing TCP/IP – Jeff Doyle CCIE #1919 Volume I Techmedia, 2002 Delhi India.

- [20] TCP/IP Illustrated -- Richard Stevens Volume II Pearson Education 2001, Delhi, India.
- [21] Designing and Developing Scalable IP Networks By Guy Davies, Telindus, UK John Wiley & Sons publishers
- [22] The Free RADIUS Server Project. (2009). RADIUS server overview.
Available: http://wiki.freeradius.org/Main_Page [2010, February 13]
- [23] Cisco Systems, Inc. (2010). TACACS+ and RADIUS comparison.
Available: https://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml [2008, February 13]



Research Team

1. Khaled KESSALI (95%)

School of Information Technology

Mae Fah Luang University

Chiang Rai, Thailand

Email: kessalik@yahoo.fr, khaled@mfu.ac.th

Tel. 0849878640

2. Dr. Guy Saidana Consultant (5%)

Chief leader, Consultant, Trainer Network and TELECOM Security

ALCATEL LUCENT FRANCE

Paris, France

Email: guy.saidana@gmail.com

Tel. 0855462682, +33

3. Dr. Thongchai Yooyativong Captain/Dr. and Consultant

School of Information Technology

Mae Fah Luang University

Chiang Rai, Thailand

Tel. 053-916741

Email: thongchai@mfu.ac.th

ABOUT THE AUTHOR

Khaled KESSALI has over 20 years of experience in working with multiple aspects of computers and data communications in industry and education. He is the technical consultant and teacher at Mae Fah Luang University, an international education company in Chiang Rai (Thailand). Khaled is also a senior instructor with Global Knowledge. In that role, he has authored and managed three highly successful courses—hands-on data communication network, network security system and microprocessor application. Khaled is involved on virtualization research of next generation of LAN/MAN/WAN, including business applications, security systems and mobile devices.

