

Bachelor's Thesis (UAS)

Information Technology

2011

Kaiyuan Yang

Designing Protection System of LAN Security



TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology

2011 | 36 pages

Instructor: Patric Granholm

Kaiyuan Yang

Designing Protection System of LAN Security

ABSTRACT

Local Area Network (LAN) refers to the local area coverage of a computer network. In general, communication data packets which can be transmitted between any two network nodes based on broadcast transmission have been widely used in local area network at present. Not only can they be received by a network card in those two network nodes, but they can also be received by a network card in any other network node on the same Ethernet. Therefore, a hacker can track, unpack all packets and steal critical information in Ethernet when they access any node on the Ethernet. This poses security risks in Ethernet.

In order to ensure local area network security. This thesis analyzes several solutions which are used firewall technology, encryption technology, network segmentation and VLAN technology. The thesis introduces three ways of establishing a preliminary LAN Protection System which are: designing a LAN structure, designing LAN security management structure and configuring a firewall.

KEYWORDS:

VLAN, Illegal Access, Firewall

FOREWORD

The thesis introduces Local Area Network security. Each case study and the example for network security in this thesis is based on my practical training in China Mobile Corporation and school laboratory.

I'd like to thank my supervisor Patric Granholm and the people who gave me help and support.

2011 Turku Finland

Kaiyuan Yang

CONTENTS

1. INTRODUCTION	1
1.1. Development of computer network	1
1.2. Local Area network security technology overvie	3
1.2.1. Network segmentation and switching hubs application	3
1.2.2. VLAN	4
2. PROTECTING LAN IN THE INTERNAL NETWORK	6
2.1. VLAN Technology	6
2.2. VLAN Division	7
2.3. VLAN Communication	8
2.3.1. Router and Switch	9
2.3.2. Using a Switch Instead of a Router	10
3. PROTECTING LAN FROM THE EXTERNAL NETWORK	13
3.1. Unauthorized Access	13
3.2. Preventing Illegal Access	16
3.3. Designing Illegal Access Prevention	17
4. FIREWALL TECHNOLOGY	21
4.1. Packet Filtering Technology	21
4.2. Application of Proxy Technology	23
4.3. Preventing Computer Viruses from Spreading	25
5. A CASE STUDY	28
5.1. Designing VLAN Division and Configuration	28
5.2. Configuring Port Security on the Switch and the Router	30
6. SUMMARY	32
7. REFERENCES	33
8. APPENDIX	34

FIGURES

Figure 2-1. Router and switch connection structure	9
Figure 2-2. Switch connection structure	11
Figure 3-1. Media Access Control	15
Figure 3-2. Monitoring system structure	17
Figure 5-1 A company network structure	28
Figure 5-2 Switch port security	30

TABLES

Table 4-1. Virus attack prevention.....	26
---	----

1. Introduction

This chapter briefly describes the research background, main work and organizational structure of thesis. The background includes the development of computer network and an overview of Local Area Network security technology.

1.1. Development of computer network

A computer network is a resource sharing system which is a collection of computers and devices interconnected by communications channels that facilitate communications and allows sharing of resources and information among interconnected devices. The first computer network appeared in the 70s of the 20th century, in the United States. The development of computer network can be divided into four states:

1) Birth stage

In the 1960s the first generation computer network was a remote computer online system that had an independent computer as its center for the purpose of transmitting information to achieve remote information processing or further to resource sharing when the then network had already had a prototype.

2) Formative stages

From the 1960s to 1970s the second generation computer network had multiple hosts through an interface message processor to interconnect and provide services for users. During this period, the network concept was A computer group that every host is capable of sharing sources together while operating its own functions separately which formed the basic concepts of

computer network.

3) Interconnection stage

From the 1970s to 1990s the third generation computer network was unified network architecture in accordance with international standards and standardized network. Because the development of computer network was very fast, each leading computer company has launched their own independent network architecture. However, there was no common standard, and there was no proper communication between different network architectures. So there was a demand to find an open, common and standardized network environment. As a result two important international generic architecture were produced, the international organization for standardization OSI architecture and the famous TCP/IP architecture.

4) High-speed network technology stage

In the late 1990s the fourth generation computer network was developed. Because of the LAN technology developed high-speed fiber optic network technology, network connection speed, network terminals and the number of users has increased rapidly and gradually formed a network represented by the Internet.

Currently there are three types of network: LAN, MAN and WAN. LAN is Local Area Network. Which generally belongs to a department or a private network often used to connect internal computer resources to share resources and exchange information. LAN coverage is generally less than 10 kilometers. MAN is between WAN and LAN, a wide range high-speed network; its coverage typically is typically from a few to several ten kilometers and its transmission rate is 2 bps or more. WAN has coverage of a large wide area network such as several cities, countries, or even a global wide area network belongs to the

scope of WAN. Commonly, the Internet is the widest WAN of global application.[7]

1.2. Local Area network security technology overview

In general, communication data packets which can be transmitted between any two network nodes based on broadcast transmission have been widely used in local area network at present. Not only can they be received by a network card in those two network nodes, but they can also be received by a network card in any other network node on the same Ethernet. Therefore hackers can track, unpack all packets and steal critical information in Ethernet when they access to any node on the Ethernet to intercept. These are the security risks in Ethernet. Actually there are many free hacking tools in the Internet that could be intercept and attack a LAN. The current LAN security solutions are the following:

The main threat of modern computer network security is unauthorized access, posing as legitimate user, damaging to data integrity, interfering with normal operation of system, using the Internet to spread virus and line interception etc. LAN security solutions rely mainly on firewall technology, intrusion detection technology and network anti-virus technology. In the actual Designing network security often involves using a combination of the above three techniques. [1]

1.2.1. Network segmentation and switching hubs application

Network segmentation is generally considered an essential method for controlling a network broadcast storm, but it actually is an important measure for network security. The purpose is to prevent illegal users from intercepting sensitive networks. The network segmentation can be divided into physical and logical sub-sections. In general, the structure of most local area networks is to

use a switch as the center and a router as the border to apply the access control functions of the center switch and the functions of the three layers switch. Through dividing the network in a physical and logical sub-section, we can to achieve LAN security control. Although the LAN center switch network is segmented, the Ethernet is still in danger of being intercepted. Because the network user access is often through the use of branch hub and not the center switch, the most widely used branch hub is a shared hub. Thus, when the user data communicates with the host, the data packets (Uncast Packet) of two computers can still be intercepted by other users on same hub. A very dangerous situation is when a user uses Telnet as a host because Telnet lacks the encryption function. So when a user types each character (including user name, password and other important information), this provides an opportunity for hackers. Therefore the network should use a switching hub instead of a shared hub and unicast packets sent between two nodes, thus preventing the illegal interception. Of course, the switching hub can only control unicast packet but cannot control broadcast and multicast packets. Fortunately the critical information of broadcast and multicast packets is much less than that of unicast packets. [8]

1.2.2. VLAN

To overcome the broadcasting problem of Ethernet, the network uses VLAN (Virtual LAN) technology to change Ethernet into point-to-point communication to prevent interception. Currently there are three kinds of VLAN:

- 1) Switch-based VLAN: It is more mature and in the practical application, results are obvious and popular, but less flexible.
- 2) MAC address-based VLAN: It provides the possibility for mobile computing, but also suffers risks of MAC fraud attack.
- 3) Protocol-based VLAN: It is very good in theory, but the practical application

is not mature yet.

In a centralized network environment, people usually design all host systems of center into one VLAN, but the VLAN does not allow any user node to better protect sensitive host resources. In a distributed network environment, we can divide VLAN by physical sections? such as departments in a company. All internal server and user nodes are in their respective VLAN which offers mutual non-interference. [5]

The way of VLAN internal connection is using switch, however the VLAN connection is achieved through routing. Currently, most switches support the international standard routing protocols which are RIP and OSPF. If there are some special requirements other routing protocols can be used. The router rather than the switch could achieve VLAN communications. [5]

2. Protecting LAN in the internal network

In the traditional Local Area Network (LAN), broadcast storms issue have become an important factor affecting network performance because of the shared transmission channel and the third layer in the network. To solve this problem, bridges and routers are widely used in the LAN. The sites of bridges have same address on the network layer which belongs to same logic network. In this network structure, the hub and cables constitute the physical network and logical subnet and the network divides the broadcast domain through the physical network. One IP subnet is part of one physical network. Because the site is bound in the physical network, it cannot be arbitrarily divided as needed into appropriate logical subnet. When the physical structure of network changes, this increases the burden of network management, leading to a comprehensive decline of network performance and reducing network stability and security. At same time, heavy traffic and low delay requirements demand more and more network bandwidth which is an issue in the traditional LAN which brings us to the concept of VLAN. [8]

2.1. VLAN Technology

VLAN is Virtual Local Area Network used widely in computer network technology. VLAN is a technology through which LAN devices are divided into network segments based on logical instead of physical what? It is the logical segmentation of network users that connect to the second layer on the switch port. The network segmentation does not limit the physical location of network users. It is according to the user needs, for example, a VLAN could be based on the location of network users, roles, departments, users of the network applications and protocols used for grouping.

VLAN technology allows network managers of a VLAN to physically divide it into different broadcast domains logically. Each VLAN contains the same properties of a group. However, it is logically, not physically divided. Although some workstations belong to the same VLAN, there is no need to place them in the physical VLAN segment. [5]

VLAN solves the Ethernet issue which is about broadcasting and security. It increases the VLAN ID base on the Ethernet. The VLAN ID could be for users divided into smaller working groups to limit the second layer of user exchange visits from different working groups. Each working group is a VLAN. The advantage of VLAN limits broadcast range and forms virtual working groups to a dynamic manage network. [5]

2.2. VLAN Division

A port divided-VLAN is divided according to the several number of switch ports of the VLAN in the network. Computers belonging to the same VLAN have same network address, but different communication between VLAN needs to go through layer 3 routing protocols. VLAN uses this approach in work process when the network node migrates. If the old and the new port are not within the same VLAN, then the user must reset the port. For accessing each different network unit, VLAN uses the router and the filtering port of the MAC address to prevent illegal access and stealing IP address. [5]

MAC address divided-VLAN: regardless of whether the node is moved in the network or not, the administrator does not have to re-configure VLAN when this way is used to divide VLAN. Because MAC address is not changed. [5]

IP address divided-VLAN: The VLAN does not need not complicated configurations when a new node is added to the network. The switch will automatically allocate the node into different VLAN according to its IP address. This is best intelligent method to divide VLAN, but it is also complicated. The IP address will be unavailable when the VLAN is deleted, thus preventing unauthorized users use of resources on network through modifying the IP address. [5]

Protocol divided-VLAN: This method divided VLAN according to the protocol fields of layer 2 data frames. Determining the upper layer run of the network protocol is through the protocol fields of layer 2(such as IP protocol or IPX protocol). If there are IP, IPX and others protocols running in a physical network, this method is best way. [5]

2.3. VLAN Communication

Designing a VLAN is a requisite in a current network structure. Considering the security performance and transmission speed of network, the VLAN communication problem is also very important aspect because the network product of development and application is very fast and inter-VLAN communication has no uniform standard. Each network equipment manufacturer ha their own strong point for inter-VLAN communication technologies. Therefore, the specific network planning should be based on characteristics of network devices and applications of network to decide which method to use. [5]

2.3.1. Router and Switch

There are two ways to achieve communication between router and switch. The first way is through different physical interfaces on the router connecting to each VLAN on the switch. The second way is to use the logical sub-interfaces of the router connect to each VLAN on the switch.

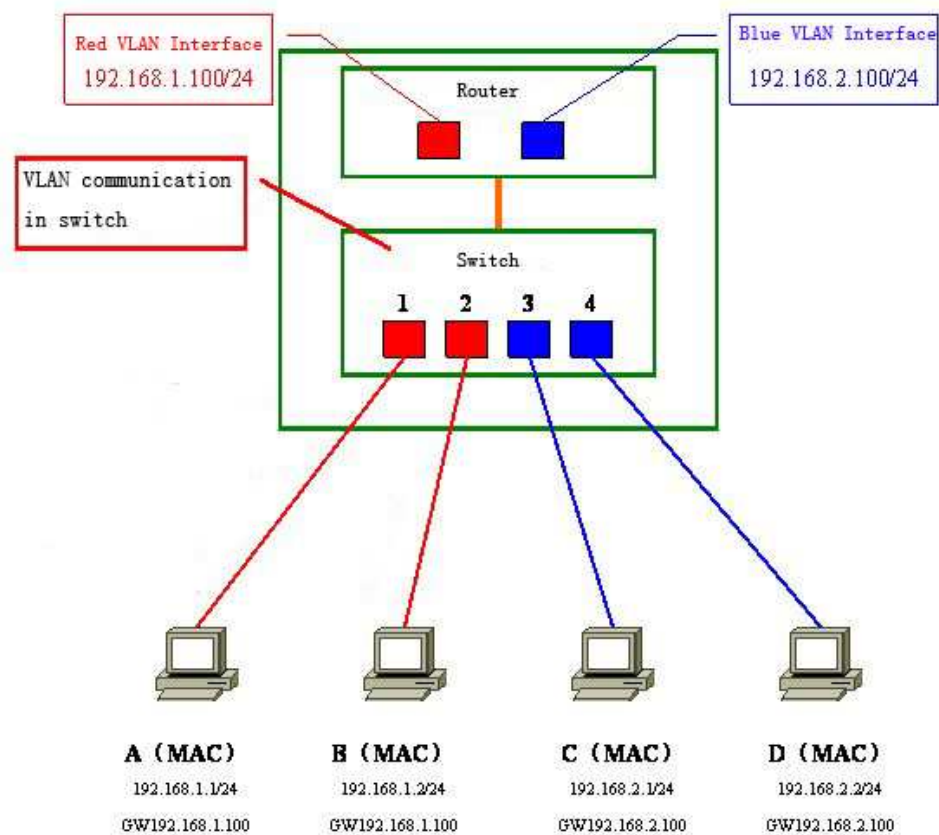


Figure 2-1. Router and switch connection structure

Through different physical interfaces, the router connects to each VLAN on a switch. The advantage of this approach is that it is easy to manage but the disadvantage is that it is too difficult to expand network. For each new VLAN,

the VLAN not only needs to take up a router port and access links on the switch, but it also needs to re-layout a network cable. However, the routers usually do not have too many LAN interfaces. In order to expand the VLAN corresponding to the required port, the router has to upgrade high-end products with multiple LAN interfaces. These costs have made this connection method expensive. [3]

The logical sub-interfaces of the router connect to each VLAN on the switch. This connection method requires the port of the router and the switch support aggregation links and the protocols used in aggregation links must be same. Then configure each VLAN logical sub-interfaces E1.1 and E1.2 on the router. Because this method is set on a multi-port which is logical sub-interfaces on one physical interface, the network expansion is simple and low cost, but the router configuration is too complicated. [3]

2.3.2. Using a switch instead of a router

Currently on the market, there are many switches which are more than layer 3. In these switches, the manufacturers use hardware or software technologies to achieve routing functionality integrated into the switch. The switch is mainly used for campus and company networks, because campus and company networks are simple but they require fast speed of data exchange and transmission. In large campuses and company networks using switches instead of routers is an indisputable fact. There are two ways to use a switch instead of a router to achieve VLAN communication. The first one is enabling routing function in the switch; it is same function as using a router. The second one is using a high-end switch with dedicated VLAN functions which support the implementation of inter-VLAN communication. [3]

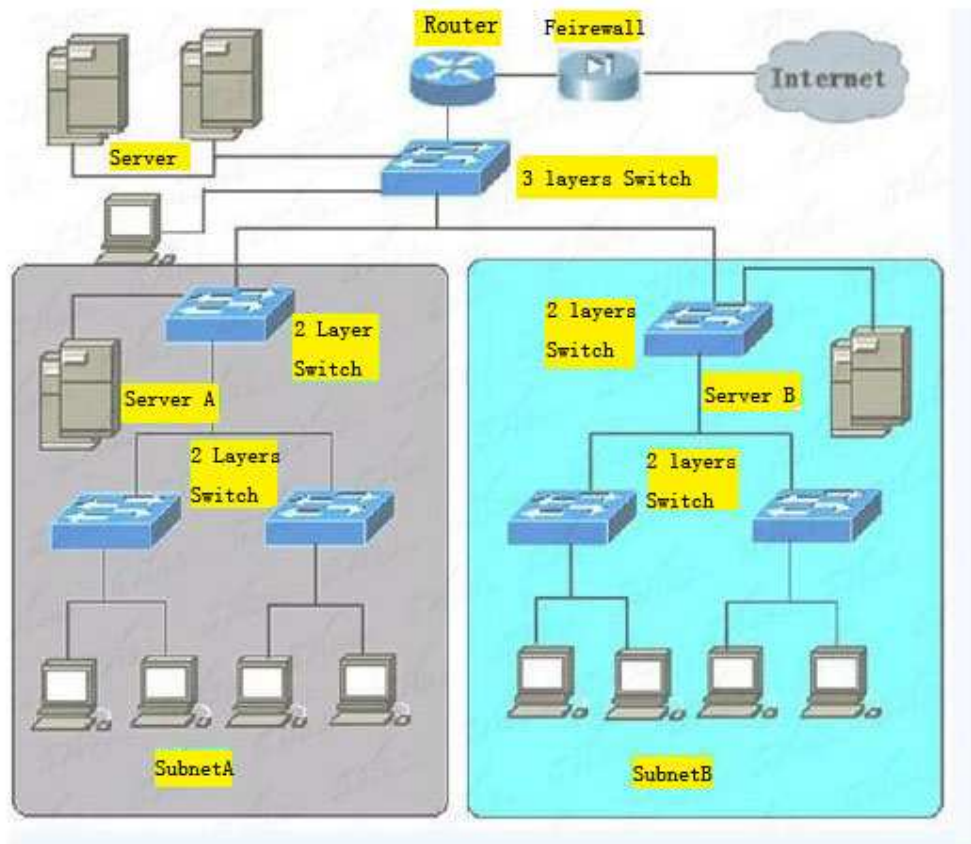


Figure 2-2. Switch connection structure

The dedicated VLAN is divided into three kinds of ports which are primary port, isolated port and community port. Only a primary port can connect with a router or a layer 3 switch. The port of the primary VLAN can communicate with all the port of the isolated and community VLAN. The port of the isolated VLAN only can communicate with the primary VLAN, internal ports are mutually isolated. The port of the community VLAN not only can communicate to primary VLAN, but also internal ports can communicate with each other. [3]

In the traditional local area network, because any computer can intercept data packages between other computers transmitted in the same LAN, there are security vulnerabilities. Different VLAN cannot communicate with each other when the VLAN is divided. It has to forward data through a router. If there is not a router in network, then the VLAN is separated by other equipment. It is likes independent LAN. This way the network security can be improved, other way would be to configure the router to achieve security control of network access between VLANs. Using VLAN technologies prevent the invasion of most network monitoring tools. [3]

In the traditional IP network, network administrators have to spend a lot of time to deal with network change. If a user wants to move to a different IP subnet, the IP address for each network workstation must be manually adjusted. However, after the division of VLAN, if a VLAN on the network workstation has to be moved to other port of the network, the administrators only need to specify the new port to the VLAN. With network management software, the administrator can easily control the network. [3]

Because the different VLANs are independent broadcast domains, the broadcast is only working in the local VLAN. Thus, the bandwidth usage is greatly reduced and its transmission efficiency is improved. In this way the generation of broadcast storm on network could be effectively avoided.

Designing a LAN structure and VLAN configurations is described in Section 5.1.

3. Protecting LAN from the external network

In applications of Local Area Network, the intranet of independent external internet applications is widespread. In many enterprises and scientific research institutions, there are many computers which save national secrets, private customer information and important information within the company and these computers cannot connect to the Internet. [4]

The purpose of illegal external monitoring is to enable administrators to understand the status of protected environment, and thus to establish a monitoring process, timely response, and alarm for illegal external access conduct on the internal LAN, to protect the internal network security, to further take effective technical means to provide support and resolve the problem. [4]

3.1. Unauthorized Access

Unauthorized access means unauthorized use of computers and mobile devices directly accessed through the intranet. As long as there occurs use of IP without distribution, strange network MAC address or the IP address and MAC address in one device is different from the intranet legal list, these are all instances of illegal access. Usually the unauthorized access is not generally a violent invasion, however, these kinds of unauthorized access to an intranet could spread viruses and Trojans to the network host and devices; in serious cases they may intercept confidential information of intranet. The occurrence of such incidents is often incomplete because the intranet hardware and software management is not good, or security administrator awareness is weak. The prevention is difficult in practice. Misappropriation of IP address is a primary means of illegal access behavior. This behavior strongly violates the interests of validated users on the network. Nevertheless, it causes great trouble and

affects the network's regular operation and security. So solving this problem is urgent. [2]

IP address theft takes many forms, but it occurs more commonly in two ways. The first one is unauthorized by administrator to configure IP address. The second one is modifying local host IP and MAC address to match the legitimate pairing information when sending and receiving data packets to modify the IP address. [2]

Unauthorized by administrator modify unallocated IP addresses. Except for dynamic IP addresses that access an intranet, there is no need for users to manually configure their own IP address. For general secret intranets, the use of IP addresses is allocated in accordance with the regulations. When the host IP is determined without authorization, the user is allowed to change the IP address of the local host. But for the IP address in the Windows system, in the absence of technical constraints, the users are free to set their own IP address of computer. If this kind of behavior was not limited, then it would cause confusion on the intranet management. Nevertheless, even though the users modify their host IP address, this only changes their own IP address of the network segment. The IP address of the host changing to another IP address of network segment is meaningless, not only can it not communicate with other computers of network segment but also it cannot communicate with local computers. [2]

Modifying the IP and MAC address of local computer

If local network users modify local computer IP address in intranet computers, this is actually not strictly illegal access behavior, but it is IP tampering. This situation will not cause too many threats in the intranet because the host is also

an intranet host. But if the IP and MAC address of computer are modified at the same time, the security administrator is unable to determine which host belongs to the intranet equipment or to unauthorized access devices. Actually, when such a situation is discovered, it should be regarded as an act of illegal access. Because a MAC address is the address of hardware device, in general the MAC address is imprinted inside the network card. The hardware address is constituted by 48 bits (6 bytes), 16 hexadecimal digits. The 0-23 bit is organizationally unique; this is the identification of the LAN node. The 24-47 bit is allocated by manufacturers and the number 40 bit is the marker bit of multicast address.

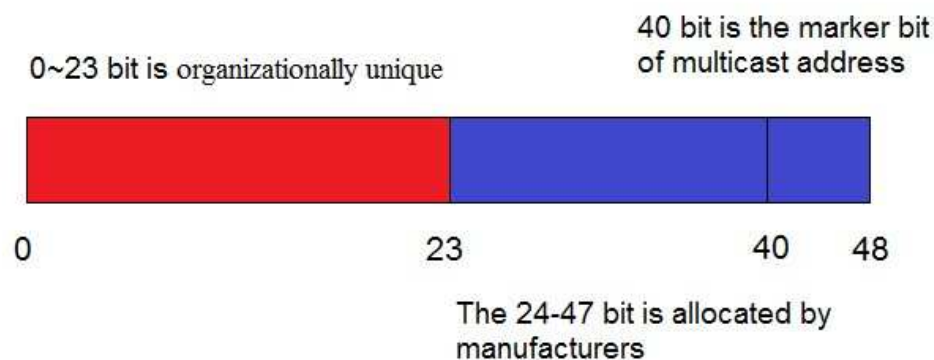


Figure 3-1. Media Access Control

In general, the physical address of network card is imprinted into the EPROM chip (one kind of flash memory chips) of the NIC by the manufacturers. Originally it could not be modified, but now some MAC address modifying software has been able to modify the MAC address of the NIC and on the other hand, some NIC also provide this function. [2]

3.2. Preventing Illegal Access

In general the solution for the problem of illegal access is based on the switch and the router. The principle is according to the layer of theft of the IP and MAC address corresponding to the layer of the network device.

Switch port control is a very effective method to solve the problem of illegal access. Because the general problem of illegal access occurs mainly on the second layer in switch, the control from the second layer is the root of the problem. The principle of this approach is the use of the switch port to provide single address access mode. This means that any one of the hosts must be through the switch port to access the network which the port is fixed. When the port has a specified IP and MAC address, any other IP and MAC address of computer specified not fulfilled with the switch port will be rejected. This method requires that the network must use all switches to provide host access at same time requiring deployment of the intranet switch. The switch port must support the physical address and the MAC address function. The current high-end switches also offer this function. Configuring the port security on the switch and the router is described in Section 5.2.

Network layer control

This method is controlling the third layer device (such as router and three layer switches). The principle is based on the NIC physical address property of being globally unique and irreversible. The SNMP regularly scans ARP of the router in the intranet to obtain the IP and MAC address to compare them with the existing addresses; if different, this means that there are illegal access devices. In this way the original IP and MAC address stored on the router is very important, so spending some time using static setting instead of the APR protocol obtain is more safe.

3.3. Designing Illegal Access Prevention

Combining the internal network platform with the external network platform prevents any illegal access being wrongly reported or left out. The program consists of an internal network platform and an external network platform. The internal network platform includes the internal access monitoring server and the illegal access monitoring proxy. The external network platform is separate from the illegal access inspection center. In the main structure of the network platform, the administrators can know any behavior of unauthorized access in the internal network on time. The complete system structure is shown in Figure 3-2.

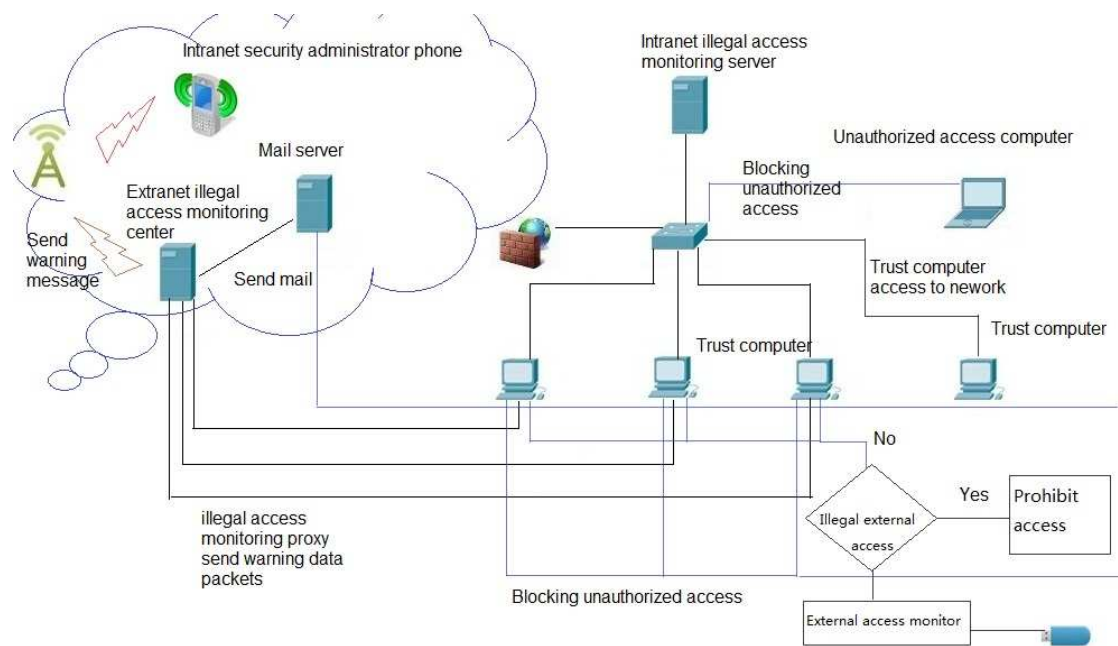


Figure 3-2. Monitoring system structure

The illegal access monitoring server of the intranet is mainly to complete the following major work:

- 1) The ARP/TCP scan on-line host and network devices obtains data and add data to the database for network security management building initial data by the provided trusted host list.
- 2) Sending ARP packets to intranet illegal access devices and controlling unauthorized access.
- 3) Sending illegal access security policy data to the host of the unauthorized access monitoring proxy.
- 4) Receiving information of security incident from the unauthorized access monitoring proxy host reports.
- 5) Detecting hosts of suspected illegal access act and sending alarm to the network security administrator.
- 6) Viewing basic information and operational information of the host from the unauthorized access monitoring proxy host.
- 7) Monitoring action of tampering in the intranet through the ARP scan.
- 8) Upgrading the program of the unauthorized access monitoring proxy.
- 9) Providing an operational interface for security administrators audit security incidents.

The users cut off connection with intranet physically to achieve connection to the internet. This situation often leads to the security administrators being unable to discover behavior of user unauthorized access. The traditional solution is the often neglected monitor for unauthorized access. This system goes through two operations to achieve monitoring: setting up data packets of the anti-illegal access monitoring center and t using the E-mails and SMS of the monitoring center to timely inform the security administrator to block this illegal access.

The monitoring center regularly scans to check if the host is online or not. If the host is offline, the security administrator has to find out the reason. The normal reason for being of offline should be that the host is shut down. However, if host is not shut down, it may be that the host has shut down the connection port of illegal access monitoring proxy and intranet monitoring server, or the user cut off the physical connection between the host and the intranet. Although in both cases it is not clear illegal access has occurred, there has occurred a suspect incident of illegal access. We call this kind of illegal access suspect situation. When the system finds suspect cases of illegal access, the security administrator could further troubleshoot the causes. This way constitutes an effective implementation of the management and technologies.

The host anti-illegal access monitoring proxy is the core of the whole system operation. It mainly completes the following tasks.

- 1) Monitoring the situation of host anti-illegal access.
- 2) Informing of security incidents to the intranet illegal access monitoring server and the extranet illegal access monitoring center.
- 3) Regularly reporting of the host illegal access monitoring proxy operational state to the intranet illegal access monitoring server.
- 4) Regularly sending host operational information to the intranet illegal access monitoring server.
- 5) Through sending ARP cheating packages to the host of illegal access achieving control over the action of illegal access.
- 6) After the user has physically cut off the connection with the security intranet, the intranet illegal access monitoring proxy would generate a suspect action log of illegal access. When a user carries out illegal access, the agent will

report to the extranet illegal access inspection center, or when the user re-connects to the intranet, the agent will report to the intranet illegal access inspection server.

- 7) Regularly scanning the online host and network devices in the intranet and reporting to the intranet illegal access monitoring server.

The extranet illegal access monitoring center as an assistant system working in whole system is a very important part for system. When the intranet illegal access monitoring server does not work, the extranet anti-illegal access monitoring center can timely receive log information of illegal access from the illegal access monitoring proxy after that through using security E-mails and SMSs to inform the security administrator.

4. Firewall Technology

The firewall is an important security technology. It mainly consists of software and hardware devices. The firewall establishes a safety shield that is used in the intranet and extranet of a unit and enterprise or private network and public network. The firewall establishes a security gateway between Internets to prevent illegal invasion, destruction and theft of data from outside users. The firewall mainly consists of service access control rules, authentication policy and packet filtering and application gateway. From technical point of view, currently there are 2 more mature architectures of firewall: packet filtering firewall and proxy type firewall (application gateway-based). At present considering comprehensive security and low-cost, the firewall market are mainly dominated by packet filtering firewall products. [7]

4.1. Packet Filtering Technology

The function of packet filtering firewall is running on network layer and transport layer on network. According to source address, destination address, port number, protocol type and mark of group packet determined whether to allow a packet to pass. Only data packets of satisfying filtering rules are forward to the appropriate destination port, the other data packets are drop from the data stream. These information sources are from IP, TCP or UDP data packet header. [6]

The packet filtering technology is a universal, cheap and effective security technology. There are 3 advantages to it:

- 1) The packet filtering does not need each specific network service to take special treatment.

- 2) Most routers have already been provided with packet filtering functions, so the application of technology is very mature and wide.
- 3) This security technology could to a large extent meet the security needs of enterprises and institutions.

The packet filtering firewall software is based on IP packet blocking all external connection requests to protect the internal network. If Web server is put inside the firewall, then the firewall needs to allow access for the Web server and the TCP port. Determining whether the packet filtering allows some packets transmit on network is based on following potions:

- 1) The destination address of packet.
- 2) The source address of packet.
- 3) The transmission protocol of packet.

Most packet filtering systems do not care about the specific content of the packet when the system determines the packet. The firewall packet filtering system only allows us to operate similar according to the following conditions:

- 1) It does not allow any user login from the external network using Telnet.
- 2) It allows any user to send e-mails to the internal network using SMTP.
- 3) It allows specific hosts to send information to the internal network using NNTP.

Not only does the packet filtering system not recognize user information of data packets, but also it cannot recognize file information of data packets. The main feature of the packet filtering system is that a user can use one computer in

order to provide protection for the whole network. In the Telnet example, if a limited user uses Telnet, the administrator could shut down the Telnet service of computers on the network. However when there are new host added on the network, the administrator cannot guarantee the Telnet service of new hosts that have been shut down or other users that have never re-installed the Telnet service. If using the packet filtering system, the administrator only configures the system a little, then there is no Telnet problem. [6]

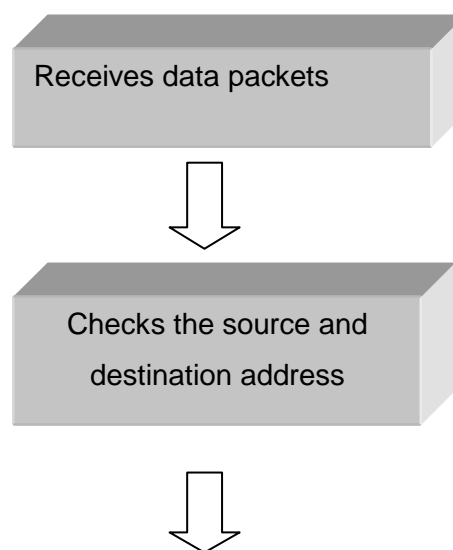
The router provides a useful point of obstruction for all users passing in and out the data flow of the network. However, only the filtering router of a specific position on the network can provide protection. For example, let us consider the safety rules which allow the network to reject any packet that contains internal mail. Because intruders always like to use this kind of packet to cheat internal network, we use filtering routers to achieve our design security rules, and the only way is through packet filtering routers of the parameters network. Only the packet filtering router in this position can be looking over the source address of packet to determine whether this packet comes from the internal network or the external network. [6]

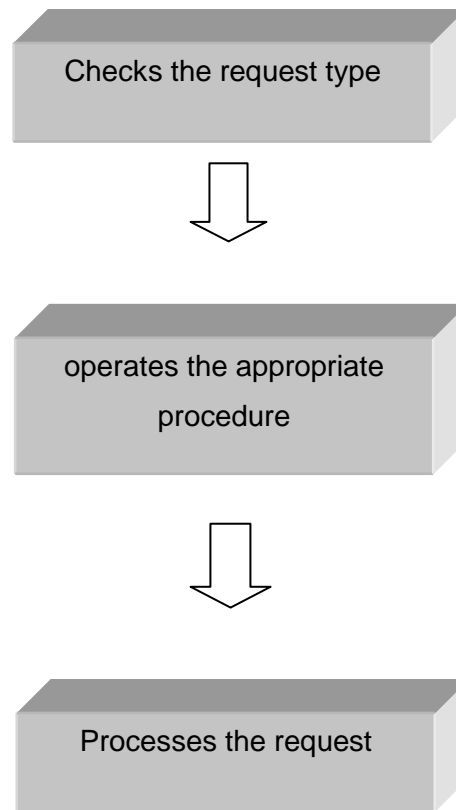
4.2. Application of proxy Technology

The application proxy firewall is also known as application gateway. It is the isolation point of internal network and external network to monitor and isolate communication of the application layer. The proxy firewall works in the highest layer of the OSI model (application layer) and controls all information as security decisions in system. Its function is to completely “isolate” communication traffic of the network for each application service through establishing special proxy preparation to achieve control and monitor the communication traffic of the application layer. [6]

The proxy firewall for each application protocol provides appropriate proxy services, through the proxy server (proxy host) it accesses the internal and external network and returns the results to its proxy client. In the standard HTTP protocol proxy service, the client's browser must configure the proxy IP address. The proxy server does not distinguish internal network or external network, but the proxy server uses name resolution on the Internet to determine the location of the WEB server. However, the normal firewall usually using the internal address which also determines the normal proxy firewall does not support requests for external network access to the Web server's HTTP on the internal network. [6]

Because the internal network and external network are separate on the network layer, the application communication between the internal and external network must be based on the network layer. The proxy system is an intermediary agent between the client host and the real server. It completely controls and records the flow rate between the client host and the real server. Currently, the proxy firewall products generally have a packet filtering function. The application proxy firewall according to following standards for processing data packets works as illustrated:





4.3. Preventing computer viruses from spreading

The functions of virus firewall technologies are as follows:

- 1) To prevent viruses from spreading by installing real-time virus filtering software in the firewall and virus monitoring software on the PC
- 2) To check and clear viruses by using anti-virus software to check and clear viruses.
- 3) To upgrade the virus database. The virus database should be continuously updated.
- 4) To install JAVA and ACTIVE X control scanning software in the firewall to

prohibit unauthorized downloading by installing and using pirate software on network.

Table 4-1. Virus attack prevention

Method of Attack	Safety switch protection strategies	Protection results
ARP attack	<ol style="list-style-type: none"> 1. Using VLAN isolated users. Each user corresponds to a VLAN. 2. Limiting user's number of APR packets and total flow of ARP packets per unit time. 	<p>Controlling APR storm of the entire secondary network.</p> <p>Ensuring the normal operation of the network devices</p>
IIICMP and network traffic attack	<ol style="list-style-type: none"> 1. Limiting the number and time of user access to other users per unit time. 2. Limiting bandwidth for each user 	<p>Suppressing worm attack speed.</p> <p>Ensuring legitimate users can normally access Internet.</p>
DDOS-Syn flood attack	Exact matching source IP address and MAC address, discarding packets if any one does not match.	Discarding a large number of illegal attack packets, basically eliminating DDOS attack to network.
Worm spread in host	ACL provides temporary protection; prohibits all RPC ports used by worm spreading.	Controlling worm spread to provide sufficient time for the network administrator to operate

		anti-virus and repair and then opening the corresponding RPC ports.
Administrators unaware of the worm situation	PORTAL provides mandatory business, whether it is WEB, PPPOE or 802.1 X authentication when the user can get online information of worm, patches and anti-virus links.	Non-spread users can simply download and install patches. Removing the worm from the spread users, downloading and installing anti-virus programs .

Firewall technology includes dynamic packet filtering, application proxy service, user authentication, network address forwarding, and IP anti-counterfeiting and warning mode sound analysis. It can effectively isolate the internal from the external network to protect the local area network from unauthorized access.

5. A case study

Designing VLAN Division and Configuration

There are 100 computers in a company network, mainly used by the following departments: Production department (20), Finance department (15), Human Resource department (8) and information center (12).

The basic structure of network is as follows: The network required resources use 3 switches (Cisco 2960, named as: Switch1, Switch2, Switch3). One router (2800), the network would connect to the Internet through the router.

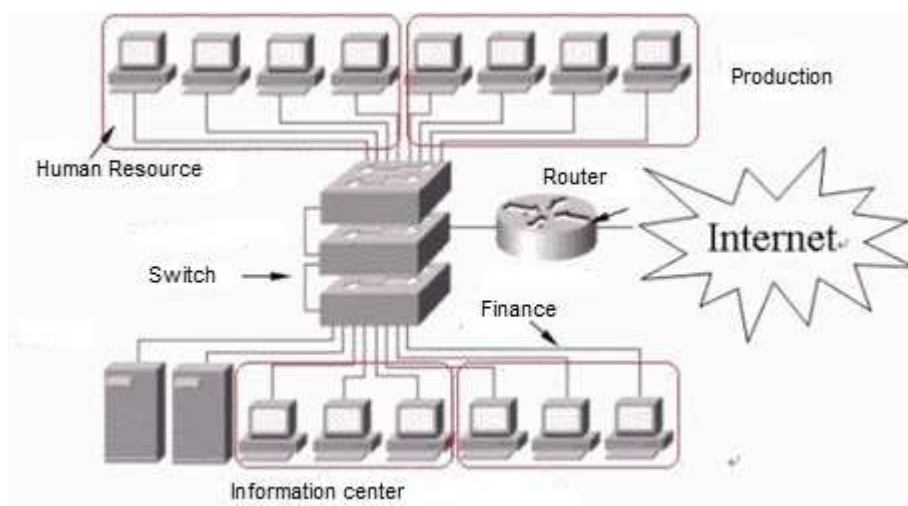


Figure 5-1 A company network structure

The connected users are mainly distributed in four parts: Production, Finance, Information Center and Human Resources. VLAN is divided for the user of the four departments to ensure the network resources of appropriate department are not stolen or destroyed. Network resource security requires sensitive company departments such as the Finance and the Human Resources department, are not easily accessed by other users.. So the company used the VLAN method to solve the problem. Divided by VLAN, the network can be mainly divided into: Production, Finance, Human Resources and Information

Center, corresponding to VLAN group name: Prod, Fina, Human and Info. The segment of each VLAN group is as follows:

VLAN	VLAN Name	Number of port
2	Prod	Switch 1 2-21
3	Fina	Switch2 2-16
4	Human	Switch3 2-9
5	Info	Switch3 10-21

The switch VLAN number starts from "2", because the switch has a default VLAN that is "1" which includes all connected users on the switch. Actually, the basic VLAN configuration process is very simple:

1. We configuring the VLAN name
2. We dividing the VLAN to a corresponding switch port

The switch configurations are as follows:

Step 1: We use ">" prompt to enter privilege mode command "enable", the command is entered as ">enable". Then we enter switch privilege mode.

```
#config t
```

We enter configuration commands, one per line and end with CNTL/Z

Step 2: For safety and convenience, we respectively configure the name and set privilege mode login passwords for the 3 switches. The following description is only an example for Switch1.

Step 3: We set the VLAN name. Because 4 VLAN belongs to different switch, we configure a name and different VLAN number on Switch1, Switch2 and Switch 3.

Step 4: We configure the switch port for each switch and to verify configuration, we use the privilege mode "show vlan" command to check if it is correct.

Step 5: We configure the trunk port on Switch1, Switch2 and Switch3.

Step 6: We enable storm control for broadcasts on the trunk port with a 50 rising suppression level for each switch

The configuration commands can be seen in Appendix 1.

5.2 Configuring port security on the switch and the router

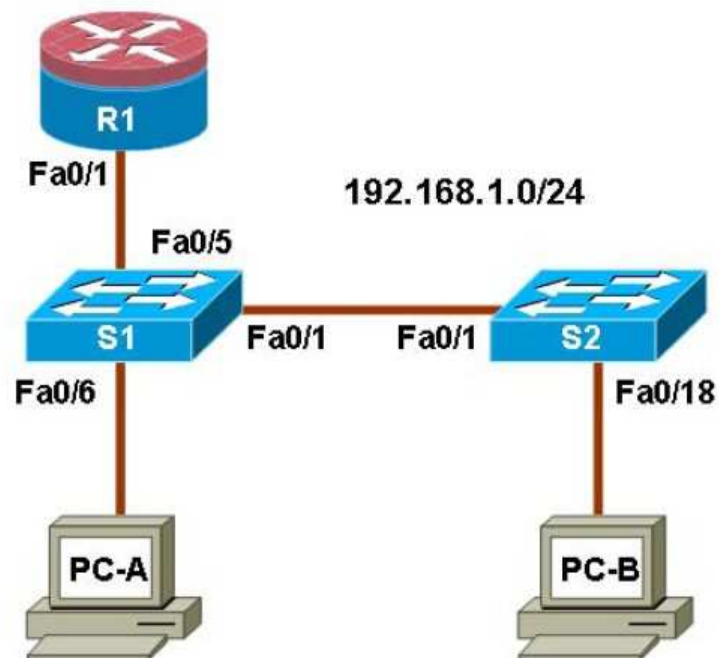


Figure 5-2. Switch port security

First we need to know the R1 MAC address use command

R1#show interface fa0/1, now we can see R1 MAC address.

```
FastEthernet0/1 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256f (bia 001b.5325.256f)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
```

We configure the switch port security settings. Note that a switch must be an access port

S1(config)#interface FastEthernet 0/5

S1(config-if)#switchport mode access //enable f0/5 is access port.

S1(config-if)#shutdown

S1(config-if)#switchport port-security //enable security on the port

S1(config-if)#switchport port-security mac-address 001b.5325.256f //
001b.5325.256f is MAC address of R1 f0/1

S1(config-if)#no shutdown

Now R1 could ping and access to S1. But if we change the R1 MAC address or change other router,

R1(config)#interface FastEthernet 0/1

R1(config-if)#shutdown

R1(config-if)#mac-address abcd.efgh.ijkl

R1(config-if)#no shutdown

R1(config-if)#end

this time the R1 cannot ping and access to S1.

6. Summary

The thesis mainly introduces an analysis of network security technology applied in LAN. It also introduces how to establish a preliminary LAN Protection System using VLAN technology to protect and design a LAN structure from the internal network. Based on LAN security management structure, administrators can monitor and prevent illegal access from the external network. Configuring a firewall prevents viruses from spreading.

Network information security is a very important and extensive topic, which contains a large amount of information. It can be greatly helpful for our society's development and play a crucial role in people's lives. We need to research and master more and more technologies that can be used to guarantee network information security. Some technologies, such as firewall technology, anti-virus technology, against external technology and VLAN technology, are useful for every LAN. Based on methods that the thesis mentioned, we are capable of initially establishing a LAN security protection system. It makes great improvement on a network's security. If all the methods are applied in the same network, the effect of security protection is obvious. However, there are several problems that cannot be ignored. The establishment technology of the anti-virus protection system is not completed. According to the establishment of anti-virus system, we generally decide to use technologies, such as anti-virus software and VLAN-isolated technology, to construct an anti-virus system. However, in this way cannot achieve our purposes. The main problems are that each host has its own security vulnerabilities, but clients do not update their hosts in time, which causes their hosts become targets of virus attacks.

References

- [1]. Andrew S. Tanenbaum, *Computer Network [M]*. 4th Edition, USA: Prentice Hall, Sep 2003
- [2]. Chen Bing, “Computer Engineering and Application” *Research on Architecture of Network Security [J]*, Vol38, No7, 2002.
- [3]. Eric Maiwald, *Network Security: a beginner's guide*. USA: Osborne/McGraw-Hill, 2001.
- [4]. Feng Dengguo, *Computer Engineering and Technology [M]*. 2th Edition, China: Science Press, 2010
- [5]. Hu Daowen, Min Jinhua, *Network Security [M]*. Bei Jing: Qing Hua Press, 2004
- [6]. Marcus Goncalves, *Firewalls complete*. USA: McGraw-Hill Companies, 1998
- [7]. Wu Gongyi, *Computer Network [M]*. Bei Jing: Qing Hua Press, 2009.
- [8]. Zhang Shiyong, *Network Security Principles and Applications [M]*. China: Science Press, May 2003.

Appendix

```
(Config)#hostname Switch1
```

```
Switch1(config)#line console 0
```

```
Switch1(config-line)#password XXXXXX
```

```
Switch1(config-line)#login
```

```
Switch1(config-line)#line vty 0 15
```

```
Switch1(config-line)#password XXXXXX
```

```
Switch1(config-line)#login
```

```
Switch1(config-line)#exit
```

```
Switch1 (config) #
```

Step 3: Set VLAN name. Because 4 VLAN belong to different switches, we configure names and different VLAN number on Switch1, Switch2 and Switch 3.

```
Switch1 (config) # vlan 2 name Prod
```

```
Switch2 (config) # vlan 3 name Fina
```

```
Switch3 (config) # vlan 4 name Human
```

```
Switch3 (config) # vlan 5 name Info
```

Step 4: configure switch port for each switch:

For Prod

```
Switch1(config)#int f0/2
```

Switch1(config-if)#vlan 2

Switch1(config-if)#int f0/3

Switch1(config-if)#vlan 2

Switch1(config-if)#int f0/4

Switch1(config-if)#vlan 2

.....

Switch1(config-if)#int f0/20

Switch(config-if)#vlan 2

Switch1(config-if)#int f0/21

Switch1(config-if)#vlan 2

Switch1(config-if)#

Also, we can use simple command to configure switch

For Fina

Switch 2(config)#int range f0/2-16

Switch 2(config-if-range)#switchport access vlan 3

For Human

Switch 3(config)#int range f0/2-9

Switch 3(config-if-range)#switchport access vlan 4

For Info

Switch 3(config)#int range f0/10-21

Switch 3(config-if-range)#switchport access vlan 5

To verify the configuration of use privilege mode we use the "show vlan" command to check if it is correct.

Step 5: configure trunk port on Switch1, Switch2 and Switch3. Example for Switch1

Switch 1(config)#int range f0/2-21

Switch 3(config-if-range)#switchport mode trunk

Step 6: Enable storm control for broadcasts on the trunk port with a 50 rising suppression level for each switch

Switch 1(config)#int range f0/2-21

Switch 3(config-if-range)#storm- control broadcast level 50