SAVONIA

Optical fiber network

Cisco part

Lu Chen

Bachelor’s Thesis

___.___.______   ________________________________

Acknowledgments

Firstly, I feel grateful for my supervisor Veijo Pitkänen sincerely. He has been fully support my bachelor's thesis and research. He showed the patience to my final project, and he gave me motivation and related knowledge. Without the help of him, I could not finish the final project and thesis smoothly and successfully.

In addition to my supervisor, I also want to thank other teachers: Arto Toppinen, Ulla Huttunen-Finta, they gave me a lot of help on the final project, not only in the aspect of the study, but also in the aspect of the truth in life.

Besides, there were another three students working in the group: Mirka Koivistoinen, Yuxuan Zhang and Chen Chen. We had discussions during the lab work and exchange opinions in the group. It was a great honor to work with them. I have learned a lot during the final project. Especially I gave the thanks to Mirka Koivistoinen, she was doing her work placement at the same time and gave us academic and professional advices in the part of Cisco network. We would not have finished the project so early during the spring without the help of Mirka. And I could not have finished the project efficiently without working with Yuxuan Zhang and Chen Chen.

At last, I would like to thank my family: my parents Yiming Chen, and Congxiao Cheng, they always support me in everywhere, and give me endless love during my life.

Lu Chen

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Abstract

Field of Study
Telecommunication Engineering

Degree Program
Information Technology

Author(s)
Lu Chen

Title of Thesis
Optical Fiber Network (Cisco part)

Date	28 March 2014	Pages/Appendices	46

Supervisor(s)
Veijo Pitkänen, Principal Lecturer

Client Organization/Partners
Savonia UAS, Engineering Kuopio

Abstract

This thesis describes a experimental optical fiber network. The thesis was based on the industrial placement work to design a laboratory network. The purpose of this thesis was to provide designs for setting an optical fiber network in the city of Kuopio.

The project work was started by searching information and usable technology in the books from the library and the Internet. Most of the broadband and/or fiber optical networks use OSPF together with MPLS as their networking protocols. The experiments of the present study involved the switches and routers from Cisco and Juniper. In this part, Cisco devices were focus on the laboratory network. Other parts of the laboratory network have been done by my two other student colleagues. Based on the knowledge I have learned in the CCNA and CCNP, the present study and evaluated methods were confirmed that were suited to my final project. The Cisco part of the laboratory network was also implemented and tested. Tests improved that the design and implementation had been done properly.

As a result of this thesis, it can conduced that in the laboratory network, two Cisco routers and switches connected to the Juniper base core network should be used. The result of this thesis indicated that in the laboratory network we should use two Cisco routers and switches that are connected to the Juniper based core network should be used. In that way, the aggregate and the access network segments can be simulated later in reality.

Keywords
Optical fiber network, Cisco, OSPF

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS Abstract**

Field of Study Telecommunication Engineering
Degree Program Information Technology
Author(s) Lu Chen
Title of Thesis Optical Fiber Network (Cisco part)

Date	28 March 2014	Pages/Appendices	46

Supervisor(s) Veijo Pitkänen, Principal Lecturer
Client Organization/Partners Savonia UAS, Engineering Kuopio

Abstract

Tiivistelmä
Työssä käsitellään kokeellista valokuituverkkoa, jonka laboratoriossa toteutettu malli perustuu käytössä oleviin järjestelmiin.

Tutkimuksen koeasetelmissa käytettiin Cisco- ja Juniper-merkkisiä kytkimiä ja reitittimiä. Minun osani tutkimuksesta keskittyy Ciscon laitteisiin, kaksi opiskelijatoveriani puolestaan keskittyivät tutkimuksen muihin osa-alueisiin. Perustuen CCNA:lta ja CCNP:ltä omaksumaani tietoon, tässä tutkimuksessa käytetyt menetelmät ovat osoitettu oikeiksi ja ovat soveltuneet lopputyöhöni. Tutkielman tulos oli, että kokeellisessa mallissa tulisi käyttää kaksi Cisco reititintä ja kytkintä, jotka ovat kytkettynä Juniper-runkoverkkoon. Tällä tavalla kokonaisuutta ja liityntäverkkojen osia voidaan simuloida jälkikäteen käytännössä. Kokeen Ciscon laitteita käsittelevä osa on myös toteutettu ja testattu, ja suunnittelu ja toteutus ovat osoittautuneet toimiviksi.

Keywords
Optical fiber network, Cisco, OSPF

Table of Contents

1 INTRODUCTION

The aim of this thesis is to create a similar fiber optical network as in Figure 1 in a laboratory by using resources found in school laboratories. This plan is supposed to work as a ground to the network that would later be executed together with Juniper devices. The final network system is shown in Figure 2.

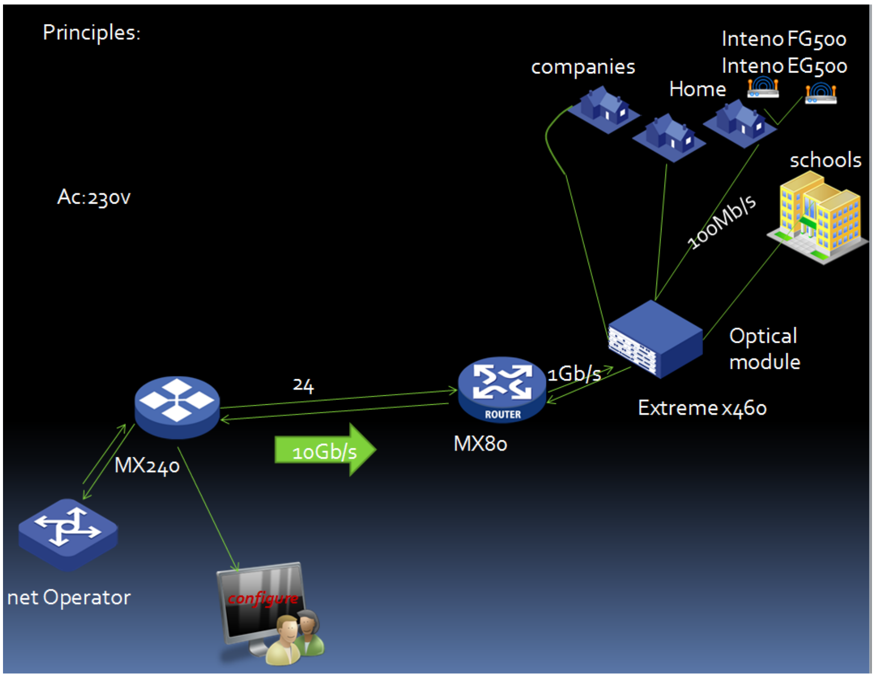


FIGURE 1. Original network design (Chen Chen& Zhang yuxuan, 2014.)

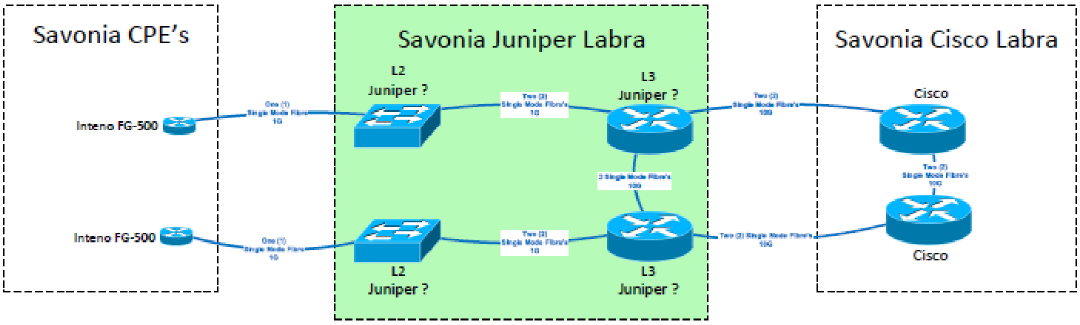

Savonia CPE's
Inteno FG-500
Inteno FG-500
One (1) Single Mode Fibre
1G
One (1) Single Mode Fibre
1G
Savonia Juniper Labra
L2
Juniper ?
L3
Juniper ?
Two (2) Single Mode Fibre's
1G
2 Single Mode Fibre's
10G
L2
Juniper ?
L3
Juniper ?
Two (2) Single Mode Fibre's
1G
Two (2) Single Mode Fibre's
10G
Two (2) Single Mode Fibre's
10G
Savonia Cisco Labra
Cisco
Two (2) Single Mode Fibre's
10G
Cisco

FIGURE 2. The final design (Juniper office, 2014.)

The project work will be started by searching information and usable technology in the books from the library and the Internet. Most of the broadband and/or fiber optical networks use OSPF together with MPLS as their networking protocols. The packet tracer will be used as the main software to test the configuring of the devices to figure out the problem in each port. Several designs will be propose during the project. Details of each design will be shown in the following chapter.

2 OPTICAL FIBER NETWORKS

With the steady development of the society, there are dramatic changes in the telecommunications industry. They got profound influence on our life styles. There are many reasons leading to these changes. The first and the most important is sustainable need for more capacity in the network system. There are many factors that can promote the demand. The significantly expanding of Internet and the World Wide Web, not only in the terms of the number of users, but also in the terms of requiring amount of time. Thus broadband taken by each user is the main influence factor. There is a simple example of the latter situation: A common voice phone call usually taken about 3 minutes, on the contrary, the users which using through dial-up lines connected to the Internet usually stay on for an average of 20 minutes, for example, Facetime, Skype, etc. Above all, six times or even more traffic can be bring via the Internet -phone-call into the Internet as the voice call. (Aneesh D & Jathin S D, 2012, 10.)

Optical network always provides a common infrastructure in order to offer all kinds of services more than itself, besides this, it also makes a contribution for large capacity in network. These networks can provide the bandwidth at any time and any place if needed. The bandwidth of the optical fibers networks is much more than the copper cable. Optical fibers offer much higher bandwidth than copper cables and it is not easy to be interference by the factors such as electromagnetic. It is selected as the excellent medium for data transmissions especially based on these advantages. In addition to these. It is also has the advantage of realizing short-distance, high-speed interconnections inside large systems. (Aneesh D & Jathin S D,2012,10.) In the past few decades, optical fiber transmission technology has a rapid development in providing longer and farther distance transmission. It also successfully created the high fiber rate and high bit rate. A huge increased bandwidth of optical fiber network is due to the deployment of optical fiber communication systems. Figure 3 shows the basic path of the optical fiber communication system.

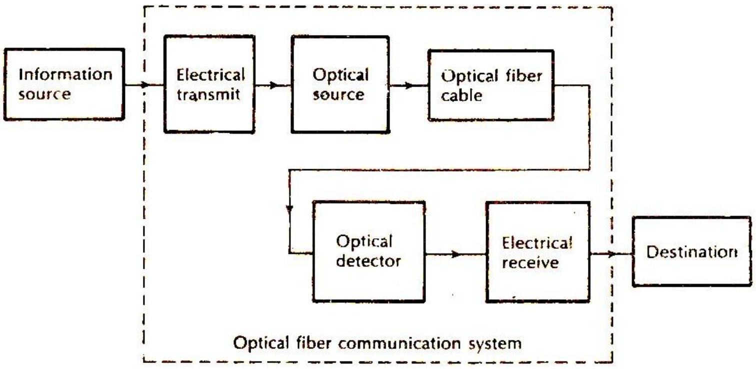


FIGURE 3. Optical fiber communication system (Ahmed, 2002.)

2.1 Optical fiber network overview

An optical fiber is made of high quality silica or plastic, it is a transparent fiber which slightly thicker than a human hair. Optical fiber widely applied in optical fiber communication system, it allows farther distances and higher bandwidth of the transmission. On account of these features, optical fiber can be used in the computer network system due to the flexibility. Compared to other transport, the most favorable characteristics of the optical fiber is the long-distance communications. There is almost no attenuation of light through the optical fiber transmission compared with the electrical cables. Therefore, long distance transmission can be delivered through repeaters. (Fiber optics.)

When comes to the optical fiber network, the fiber access system (FTTx) should be mentioned at first. FTTx stands for Fiber-to-the-X system. The X can be any place such as “building”, ”home”, ”curb”, ”premises”, etc. FTTx brings the high-quality optical fiber network more closer to the user, it should be the best choice for the network transmission system. In the modern technology, the maximum information capacity of an optical fiber exceeds 100 Tb/s, it be used to be the coherent detection in a typical DWDM system. (Broadbandcommunities, 2013, 9th Edition.)

A fiber access system can be divided into two parts: point-to-point (P2P) and point-to-multi-point (P2MP). In addition, an active remote distribution node can be used to be an Ethernet switch or a simple passive splitter as the remote distribution node used in power splitting passive optical network (PONs).

2.2 Advantages of optical fiber and optical fiber network

2.2.1 Advantages of optical fiber

Since 1980s, with the development of the network technology, many kinds of materials have been put into use for information transmission in the building. From then on, the optical fiber has been comprehensively put into global business operation. Optical fiber is flexible glass as thin as human hair which can be used for telecommunications. It easily carries digital signals with light. Even though it is made of glass, it can be either bend or twist without any demand of the communication system. The most familiar material in the daily life is the fiber optic cable, it tens of thousands of fibers which are arranged in bundles or twist into a shares. The special protective coating covering on glass cables is called cladding. It is made from a material that reflects the light back into the core or center of the cable. This cladding creates a mirror-lined wall. The final outer layer is a buffer coating which aims to protect this special glass cable from any damage and moisture. (ifiber,2012,2.)

The optical fiber cable uses light instead of electricity to transmit signals. From the perspective of physics, light transmission is the fastest way. However, not being interference by electrical is the additional advantage of the optical fiber cable, therefore, it can be run almost anywhere. Moreover, fiber optic cable can be run over very long distances without processing the signal since there is almost no resistance in light. Some signals have been transmitted to faraway places ahead of processing.

2.2.2 Advantages of optical fiber network

At present, it has ultra-low loss fibers (0.001dB/km), so that the optical signals can be transmitted over very long distances with low loss through the fiber. Hence, the optical fibers can transmit the optical signals or data with a very low attenuation and low dispersion. If it uses the silicon laser pulses, it can transmit the signals almost without any loss dispersion. Therefore, the optical fiber network can achieve very high bandwidth and data rate through fiber optic cables. Nowadays, many kinds of fibers have been published into the market, for example, dispersion free fibers, dispersion compensation fibers, etc. The advantages of optical fiber communication compared to other communication system are as follows: (science guy, 2009, 1.)

2.2.2.1 Enormous bandwidths

Bandwidths represent the size of the transmission capacity. The higher the carrier frequency is, the greater bandwidth of the transmitted signal will be. The optical carrier frequency is in the range of Hz while the radio frequency is around Hz. Although the frequency band is affected due to the optical fibers of different frequencies have different losses. But the bandwidth can also up to the minimum loss region 30000GHz, it is enough for the daily use. (Baidu web page.)

2.2.2.2 Low transmission loss

In the system of coaxial-cable, the transmission loss per Km are more than 40 dB when transfer 800MHz. In contrast, the transmission loss is much smaller in the optical fiber system. Therefore, the data can transmit much farther distance through the optical fiber. Furthermore, there are two characteristics in optical fiber transmission loss, one is that the transmission loss is the same among the cable channels, another is that the loss hardly affected by the temperature of the environment.

2.2.2.3 Strong anti-interference ability

Because the basic component is quartz, the optical fiber can only transmit light, it is non-conductive so it cannot be effected from electromagnetic fields. Because of this, the signal transmitted in the fiber can not be easily tapped, it is useful for data confidentiality. (Baidu web page.)

2.2.2.4 Electric isolation

Optical fibers are made from silica which is an electric insulator. Therefore they do not affected by any electromagnetic wave or any high current lighting. It is also suitable in explosive environment.

2.2.2.5 Small size and weigh

The optical fiber is very thin, the core diameter of a single mode fiber is generally 4um ~ 10um, and the outside diameter is only 125 um. It is much smaller than a standard coaxial-cable. Because it is made of silica, it has a small diameter, light weight, and easy for installation. (Baidu web page.)

2.2.2.6 Signal security

The transmitted signal through the fiber does not radiate. Different from the copper cables, a transmitted signal cannot change without being tampered. Thus, the optical fiber communication provides a 100% signal security.

2.2.2.7 Ruggedness and flexibility

The fiber cable can be easily bent or twisted without damaging it. Further, the fiber cables are superior than the copper cables in terms of handling, installation, storage, transportation, maintenance, strength and durability.

2.2.2.8 Low cost and availability

Since the material of producing the optical fiber is very abundant, with the progress of technology, the cost of the production will be further reduced.

2.2.2.9 Reliability

The reliability of a system related to the number of the devices in the system. The more equipment in the system, the more chance of failure will happen. Because the optical fiber system contains a small number of devices, the reliability of the fiber will be higher. (Science guy, 2009, 1.)

3 LAB WORK (CISCO PART)

3.1 General

According to the devices we got. The designs of Cisco part have been tested several times. As a result of the devices from the Company Juniper are not in the lab at these moments. So only the part of Cisco lab can be illustrated in this chapter .And the extra part of Juniper will be explained in another thesis by another group member.

This part is divided into two sections. And the theory and the practical will be combined together in this chapter.

3.2 Equipment in the lab work

Most of the equipment is from Cisco Company, and all the devices have been provided by the Cisco classroom. The most suitable devices were chosen to conduct the experiment.

3.2.1 Router (Cisco 2900 series)

Cisco 2900 Series Integrated Services Routers (ISR) is designed to meet the demands of today's medium-sized branches and it is based on the cloud services. The high performance of the router is from connecting to the wide area network, it offers concurrent services at up to 75 Mbps. Figure 4 shows the appearance of the router that has been used in the lab.

FIGURE 4. Cisco 2900 series used in the lab work (cisco.)

All Cisco 2900 Series Routers have a long product line in the business. They have modular design that can be suitable for each use in the market. Meanwhile, they maximize protect the investing of the existing module, they offer (cisco):

- Agile Application Services, they have the ability to host Cisco and multiple third-party applications on UCS-E Series server modules for mission-critical applications at the branch office, moreover, they that can optimize all types of data, voice, and video applications.
- Using WAN Connectivity, including T1/E1, T3/E3, 4G/LTE, xDSL, copper, and fiber Gigabit Ethernet
- Cisco 2900 series have highly Integrated Security, using a completed VPN technology with IPSec and SSL. They strengthen the function of the defense by the support of firewall and intrusion prevention system (IPS) options in VPNs it also support for encryption of next-generation and cloud-based security.
- Cisco 2900 series perfectly support call processing and voicemail services and offer a high-quality analog and digital voice through on-board integrated digital signal processors (DSPs) and analog voice cards. They also highly support resilient call management to overcome WAN service interruptions.
- Cisco 2900 series deliver a more visual, social, and personal experience through video networking solutions.
- Cisco 2900 series highly support the performance with powerful and energy-efficient multicore processors, a multigigabit fabric, and high-performance services modules. Multiple concurrent services can be run at high throughputs in an extensible way.

3.2.2 Switch---Cisco Catalyst 2950 Series

The switches have been used as different parts in this lab work. Two of the switches have been put into use. Figure 5 shows the performance of the switch 2950 series used in the lab work.

FIGURE 5. Cisco Catalyst 2950 Series used in the lab work (Cisco.)

The Cisco Catalyst 2950 Series Switch is a fixed-configuration, stackable standalone switch that provides wire-speed Fast Ethernet and Gigabit Ethernet connectivity. This switch offers two distinct sets of software features and a range of configurations to allow small, midsize, and enterprise branch offices and industrial environments to select the right combination for the network edge.

Standard Image Software offers Cisco IOS Software functions for basic data, voice, and video services.

Available for the Catalyst 2950 Series, the Cisco Network Assistant is a free centralized management application that simplifies the administration task of Cisco switches, routers, and wireless access points. Cisco Network Assistant offers user-friendly GUI interface to easily configure, troubleshoot, enable and monitor the network. (Cisco)

3.2.3 Switch (Cisco Catalyst 3560 PoE-24)

The Catalyst 3560 switches are used as the R1 and R2 in the following lab work. Figure 6 shows the front side of the switch 3560.

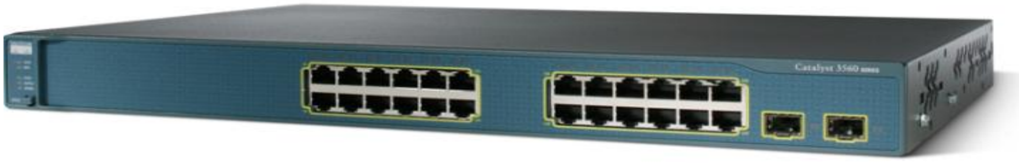


FIGURE 6. Cisco Catalyst 3560 PoE-24 (Cisco)

The Cisco Catalyst 3560 Series have the efficient energy; they are Layer 3 Fast Ethernet switches. These new switches support Cisco Energy Wise technology, which helps companies manage power consumption of the network infrastructure, thereby reducing their energy costs and their carbon footprint.

The new switches consume less power than any other switches that have been put into use. And they are ideal access layer switches for enterprise, and branch-office environments. They can maximize productivity and provide investment protection by using a unified network from data, voice, and video. (Cisco web page)

3.2.4 Switch (Inteno Broadband technology AB)

The switch Inteno has been schemed in the third part of the final design but not in the Cisco part lab work, but during the lab work, the Inteno device has been tested in the Cisco lab connected with other Cisco devices. Figure 7 shows the picture that has been taken in the laboratory.

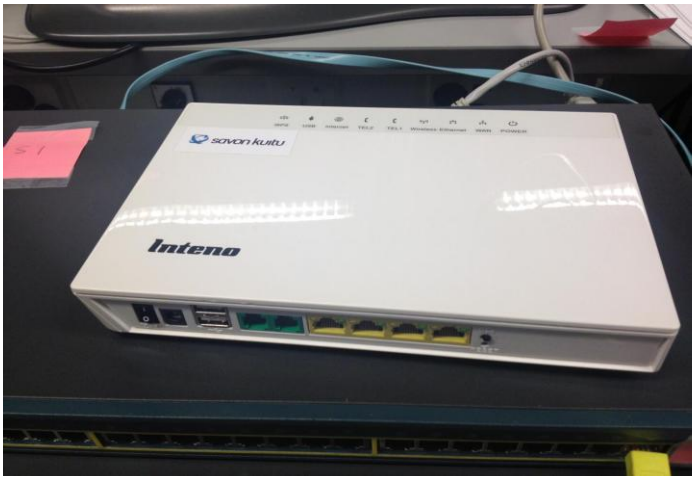


FIGURE 7. Inteno Broadband technology AB (model: FG 500) (photograph by Chen Lu, 2014.)

The features of Inteno FG500-R are as follows :(Inteno instruction book, 2008, 15)

- Ethernet interface automatic speed-sensing and crossover correction supports up to 1000 Mbps downstream and 1000 Mbps upstream rates
- Integrated four-port 10/100/1000BaseTX Ethernet switch with speed-sensing and crossover detection automatically
- 802.11b/g/n WLAN supports up to 300 Mbps transmission rate
- Provides wireless secure transmitting encryption by either 802.1x; WEP; WEP2; WPA; WPA2; TKIP; AES; 802.11i
- Supports 2 FXS ports for VoIP application including call waiting, call forward, call transfer and so on
- Support voice CODECs like G.711, G.726, G.729AB, BV16, ILBC, T.38 etc.; programmable G.168 echo cancellation, adaptive jitter buffer and packet loss concealment
- Supports Voice activity detection (VAD), comfort noise generation (CNG) and caller ID
- Supports DTMF tone detection and generation; Fax / Modem detection and pass-through
- Support SIP signaling protocol and bonus services like call forwarding, call waiting, call transfer, call busy, call return, enquiry service, CLIP/CLIR and three way conference
- Support Networking protocols such as PPP, Routing, DHCP server / relay / client
- Network address translation (NAT) functions to provide security for your LAN and multiple PCs surfing Internet simultaneously.
- Configuration and management by Web-browser through the Ethernet interface and remotely through WAN interface
- Firmware Support TR-069
- Upgradeable through HTTP / TFTP

The connector definitions of Inteno are show in Table 1:

TABLE 1: The function of each button in Inteno (instruction book of Inteno, 2008, 14)

Label	Function
Antenna	Connects to the 802.11b/g/n enabled wireless devices in LAN
Power Switch	ON/OFF switch
Power Jack	Connects to the supplied power adapter
USB	Connects to the USB devices
TEL 1 ~ TEL2	Connects to analog telephones for VoIP service
LAN1 ~ LAN4	Connects the device via Ethernet to your devices in LAN
WPS	Press to enter wireless WPS mode
RES	A reset button to reset the device or reset to default settings
SFP	Connects to the fiber broadband network
Antenna	Connects to the 802.11b/g/n enabled wireless devices in LAN
Power Switch	ON/OFF switch
Power Jack	Connects to the supplied power adapter
USB	Connects to the USB devices
TEL 1 ~ TEL2	Connects to analog telephones for VoIP service
LAN1 ~ LAN4	Connects the device via Ethernet to your devices in LAN
WPS	Press to enter wireless WPS mode
RES	A reset button to reset the device or reset to default settings
SFP	Connects to the fiber broadband network

3.2.5 Others

The IP address of the computers in the lab work has been used to be the Internet Services Provider (ISP) and the clients. The network between the computers in the lab work was completed testing from the packet tracer. The devices were taken from the Cisco classroom as well as the cross cables, straight cables, and power cables. They all have been one part of the whole lab work.

3.3 Experimentation

The lab work was designed and tested for several times, and finally two designs have been come out. They will be illustrated in this chapter. At the same time the differences and the functions of each design will be presented.

3.3.1 The first design

Figure 8 shows the preliminary design of the first design:

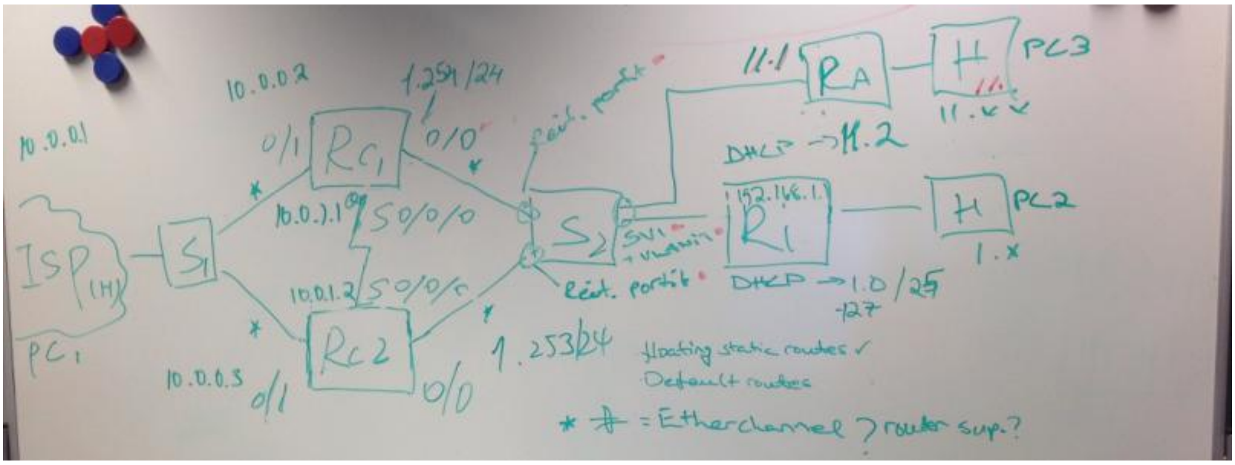


FIGURE 8. The first preliminary design in lab (Chen, 2014.)

Another schematic diagram about the design was drawn up by using the packet Tracer as shown in the Figure 9.

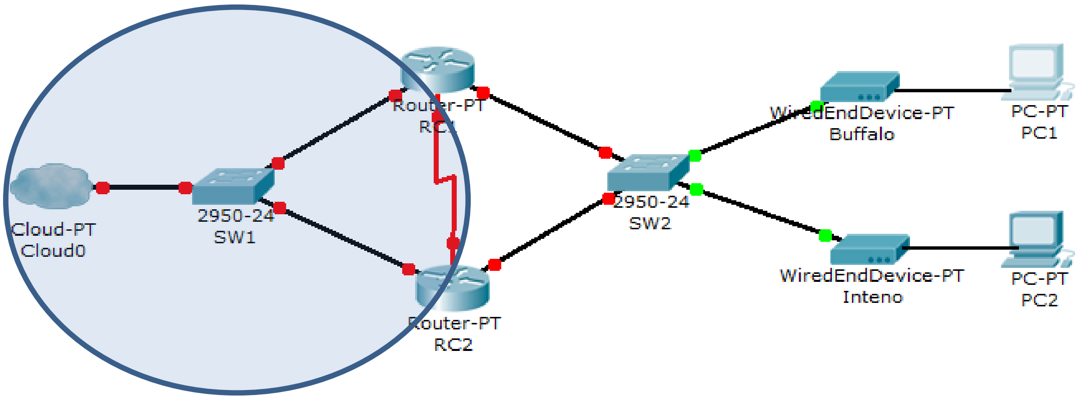


FIGURE 9. Schematic diagram on the packet tracer (Chen Lu, 2014.)

The reason for using two routers on top of each other was that in case of other router failing the second one would still be functional. Most of the broadband and/or fiber optical networks should be using Open Shortest Path First (OSPF) together with Multiprotocol Label Switching (MPLS) as their networking protocols.

For the first experiment, the two routers (series 2900) and two switches (series 2950) were put into use. All of the equipment in the packet tracer including Buffalo and Inteno which needed to be added in the final lab work were tested. The IP address of the computers was using to be the client and the ISP. Furthermore, the technology which using in the lab work consist of the basic configuring, OSPF, etc. Created a normal OSPF network in the lab caused that the series 2900 routers do not support the MPLS. And the idea and the theory will be explained in the next chapter.

The basic configuration was done by our group after putting the cables in the ports and setting the IP address for each port that has been used. The IP address for the essential ports can be seen from the picture in front. The software KiTTY was used to do the basic configuration.

The blue area should uses the address space 10.0.0.0, address space 192.168.0.0. was chosen to be the best address that will be used in the rest of the network , PC1 and PC2 gain their addresses from Inteno and Buffalo home routers as they would in a normal networking environment at home. In this case Inteno was using ip address 192.168.1.1.

#ip address configuration of RC1:

```
!
interface Serial0/0/0

ip address 10.0.1.1 255.255.255.0

no fair-queue

clock rate 64000
```

```
no shutdown
!
```

#ip address configuration of RC2:

```
interface GigabitEthernet0/0

ip address 192.168.1.253 255.255.255.0

duplex auto

speed auto
!

interface GigabitEthernet0/1

ip address 10.0.0.3 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/0

ip address 10.0.1.2 255.255.255.0

!
```

Next task was to achieve routing to and from different subnets. The used protocol was OSPF.

#networking configuration for RC1:

```
router ospf 1

network 10.0.0.0 0.0.255.255 area 1

network 192.168.0.0 0.0.255.255 area 1

!
```

#networking configuration for RC2:

```
router ospf 1

network 10.0.0.0 0.0.255.255 area 1
network 192.168.0.0 0.0.255.255 area 1
```

!

To achieve redundancy in case of a link failure towards end users (networks 192.168.1.0 or 192.168.11.0), a floating static route with administrative distance of 120 to the serial link has been added between RC1 and RC2. This means that if a normal route (from RC1 through interface GigabitEthernet0/0 or from RC2 through interface GigabitEthernet0/0) somehow fails the serial line between two routers is used.

#Configurations of RC1 and RC2

```
ip route 10.0.0.0 255.0.0.0 Serial0/0/0 120

ip route 192.168.0.0 255.255.0.0 Serial0/0/0 120
```

#Default routes were also inserted to both routers:

```
ip route 0.0.0.0  0.0.0.0 Ga0/1
```

As a result , the network was working successfully.

3.3.2 The second design

Based on the first lab work and the final goal we made a change about the topology. The three switches (2950series, 2950 series, and 3560series), two routers (2900 series, 2900 series) and the cables were using in the lab work. And the Inteno has been using between the switches and the customer computer.

The topology has the same function as in the first design. The network can go smoothly when one of the switches is power off, another switch will automatically be put into use instead of the first one.

After finishing this part, the Juniper devices would be added to the left of the Cisco Routers to extend the network area.

The basic configuring, create another OSPF among the routers, the SVIs on the switches, trunk between the switch 2 and switch 3 are the main protocols of the lab work, further, the Portfast would be used to security the network similar to the part to set the key among the network in the CCNA 1.For the abbreviation that mentioned in the lab part in this chapter, it can be illustrated into details in the next chapter. Figure 10 shows the second design of the Cisco part which is the most suitable one for the final goal.

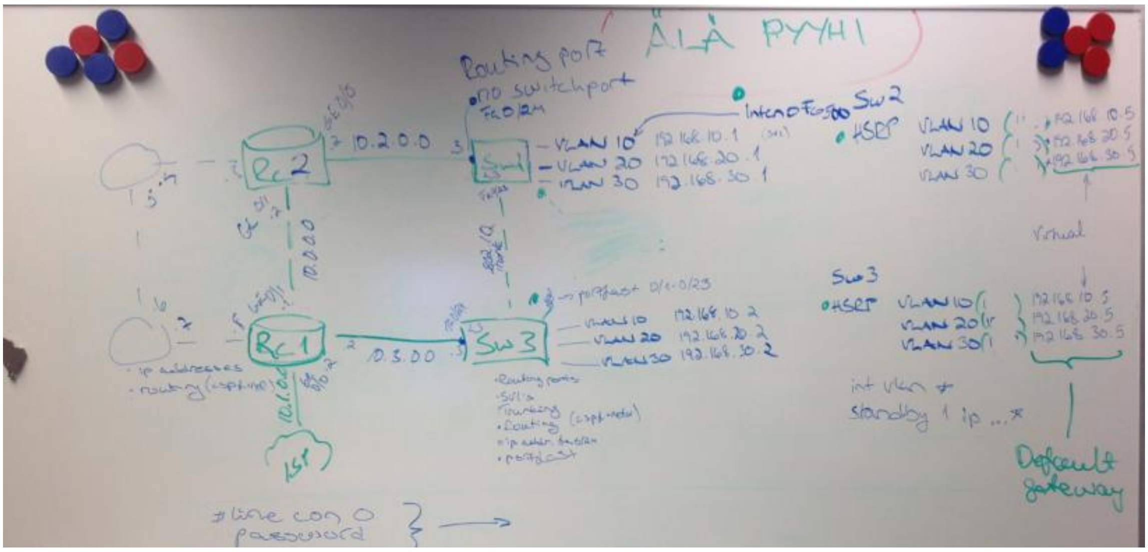


FIGURE10. The second preliminary design in lab (Chen Lu, 2014.)

Another schematic diagram about the design has been draw by using the packet Tracer as shown in the Figure 11.The design was altered a bit to simulate circular shape of actual optical fiber network. This is the final design of the network.

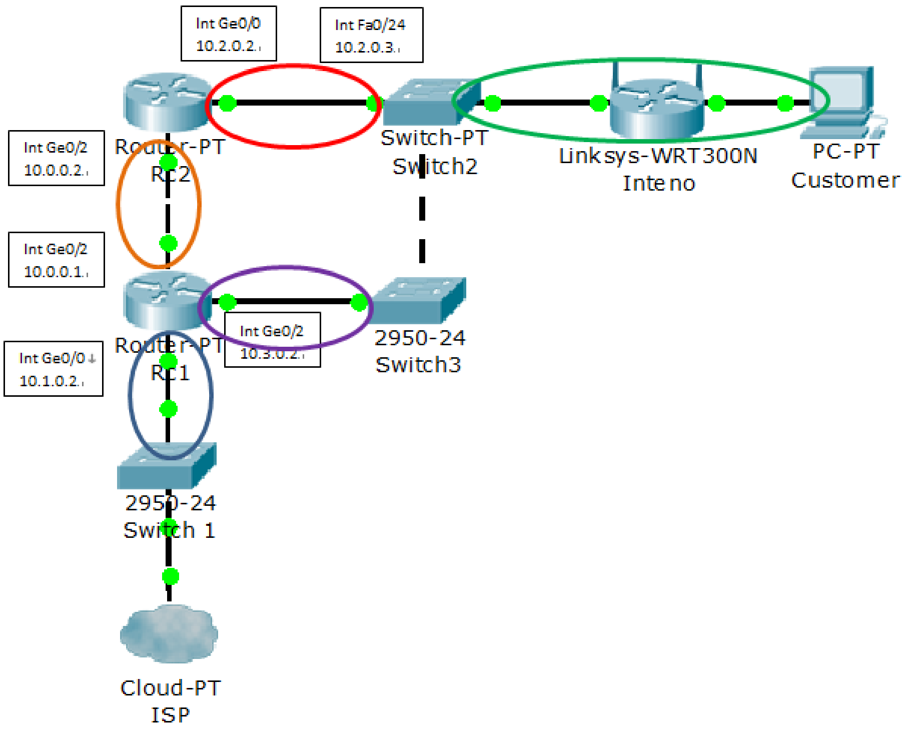


FIGURE 11. The schematic diagram on the packet tracer (Chen Lu, 2014.)

Different colors of simulate circular mark different network areas:

- The network covered by the blue circle is 10.1.0.0/24
- The network covered by the orange circle is 10.0.0.0/24
- The network covered by the red circle is 10.2.0.0/24
- The network covered by the violet circle is 10.3.0.0/24
- The network covered by the green circle is 192.168.10.0/24

The Interface addresses can be seen in the Figure 11. Here are the configurations that has done for the network setting.

- OSPF

#networking configuration for RC1:

```
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
!
```

#Networking configuration for RC2:

```
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
!
```

On switches 2 and 3 layer 3 routing was also enabled and SVIs were used to achieve inter-VLAN routing. Three VLANs (10, 20, 30) were created on both switches and routing protocol was also OSPF. Same OSPF area (area 0) was used for entire network.

Networking configuration for Switch2:

```
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
network 192.168.0.0 0.0.255.255 area 0
!
```

Networking configuration for Switch3:

```
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
network 192.168.0.0 0.0.255.255 area 0
!
```

- SVIs

Setting the vlan ports for each switches and then use the ports connected to the customers. Ports fa0/1-22 was configured to be access ports for VLANs 10, 20 and 30. The port fa0/1 was using for vlan 10, port fa0/7 was using for vlan 20 and port fa0/13 was using for vlan 30 in each switch.

#SVIs for Switch2:

```
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan30
 ip address 192.168.30.1 255.255.255.0
!
```

#SVIs for Switch3:

```
!
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.2 255.255.255.0
!
interface Vlan30
 ip address 192.168.30.2 255.255.255.0
!
```

Figure 12 shows the reality of the ports from the lab work:

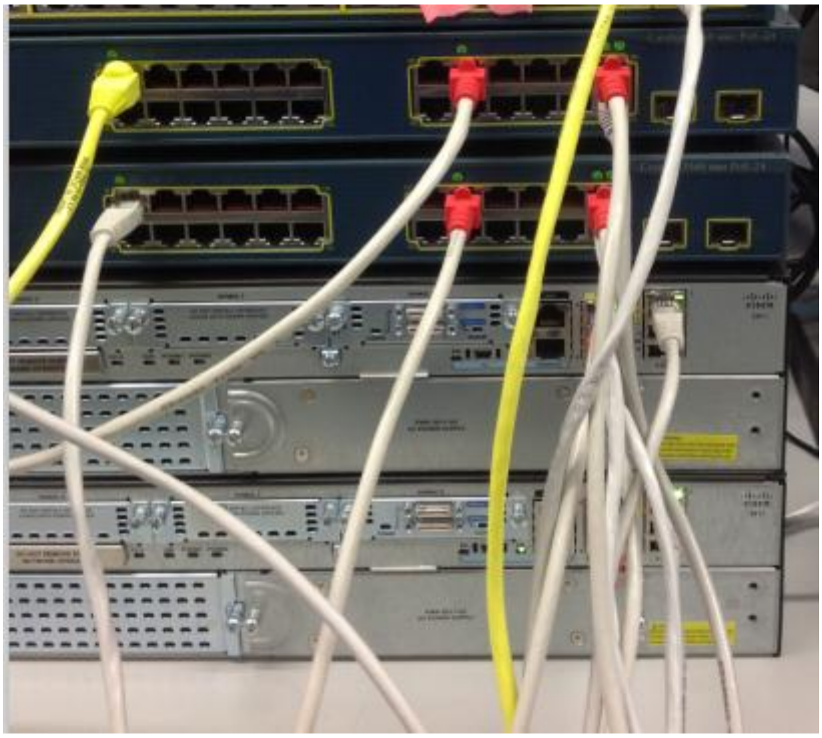


FIGURE 12. setting the ports on the switches to make the virtual interface. (Photograph by Chen Lu, 2014.)

Switches fa0/24 ports were configured as routing ports and assigned with ip ddresses**.**
#Configuration of port 24 on switch 2:

```
interface FastEthernet0/24
!
no switchport
ip address 10.2.0.3 255.255.255.0
```

#Configuration of port 24 on switch 3:

```
interface FastEthernet0/24
!
no switchport
ip address 10.3.0.3 255.255.255.0
```

#Configuration of ports:

```
!
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 30
switchport mode access
```

- Trunking

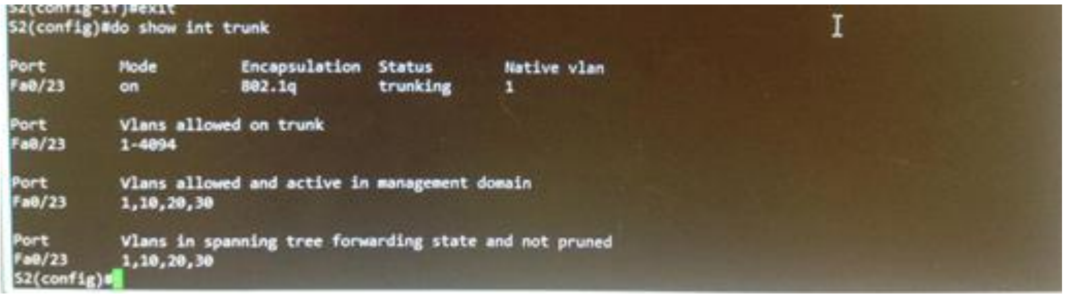
The ports fa0/23 on switches 2 and 3 are used for trunking to carry different VLANs and crossover cable was used between them. Used the protocol for trunking was chose to be 802.1Q, because it is supported also on non Cisco switches and it is a standardized protocol.

#Configuration of trunk ports:

```
!
interface FastEthernet0/23
switchport trunk encapsulation dot1q
switchport mode trunk
```

Use the code# do show int trunk to test the trunking has been connected or not.Figure13 shows

the screen of the testing.



```
S2(config-if)#exit
S2(config)#do show int trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/23      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/23      1-4094

Port        Vlans allowed and active in management domain
Fa0/23      1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/23      1,10,20,30
S2(config)#
```

FIGURE13. type the #do show int trunk to show the connecting information (Printscreen by Chen Lu,2014.)

After all the setting for the second design have been done completely. The IP addresses have been set for the ISP computer, client computers, and then it shows everything all goes well and when one of the switches was powered off. The network can also goes through the ISP to the client via another switch.

3.3.3 Extra part (HSRP)

3.3.3.1 Instructions

HSRP is the abbreviation of the Hot Standby Router Protocol .HSRP is a redundancy protocol developed by Cisco to provide gateway redundancy without any additional configuration on the end devices in the subnet. With HSRP configured between a set of routers, they work in concert to present the appearance of a single virtual router to the hosts on the LAN (Baidu, 2006.), as shown in Figure 14.

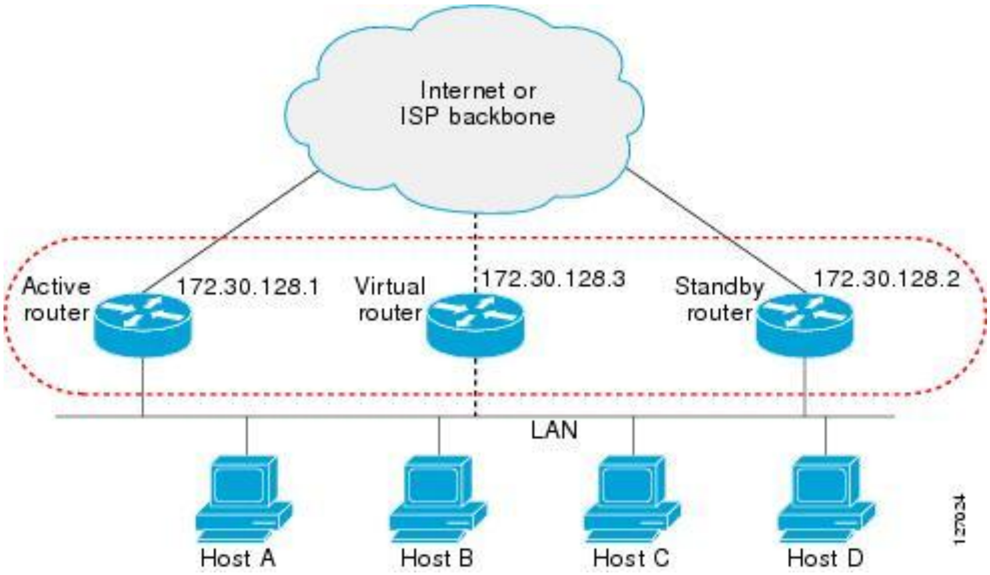


FIGURE 14. Normal ISP network (Cisco configuring HSRP.)

There are several routers in the protocol including a group of the HSPR. They inform a “hot backup group” All the routers in an HSRP group have specific roles and interact in specific manners (Baidu, 2006.):

- Active router: Within an HSRP group, one router is elected to be the active router. These routerphysically forwards packets sent to the MAC address of the virtual router. There is only one active router in an HSPF group. Just like the left router shown in the figure above.

- Virtual router: An IP and MAC address pair that end devices have configured as their default gateway. The active router processes all packets and frames sent to the virtual router address. The virtual router processes no physical frames. There is also only one virtual router in an HSRP group.

At any one time, there is only one router within a group is active, and it will forward packets in the system. If the active router is power off, the router will select a backup to replace the active router. But from the side of the hosts within the network, virtual router has not been changed. So the host remains connected, failure does not affect the process of the system. It effectively reduces the probability of disruption in the communication.

To reduce the data traffic during the network, after setting the router and the backup router to become active, only the active router and the backup router ends HSRP packets periodically. If the active router fails, the backup router takes over the active router. If the backup router fails or becomes the active router, the backup router was chosen by another extra router.

HSRP provides the mechanism for determining which router should take the active role in forwarding traffic. HSRP also has a mechanism to determine when that active role must be taken over by a standby router. The transition from one forwarding router to another is transparent to the end devices.

When the active router or the links between the routers fail, the standby router stops seeing hello messages from the active router. The standby router then assumes the role of the forwarding router. Because the new forwarding router assumes both the IP and MAC address of the virtual router, the end stations see no disruption in service.

The active router responds to traffic for the virtual router. If an end station sends a packet to the virtual router MAC address, the active router receives and processes that packet. If an end station sends an ARP (address res) request with the virtual router IP address, the active router replies with the virtual router MAC address.

3.3.3.2 Configuring HSRP

The description of each command in the configuring of the HSRP will be show in the Table 2.

TABLE 2: Configuring of the HSRP

command	Description
Switch(config-if)# **standby** Group-number **ip** ip-address	Configures HSRP on this interface. Group number is optional and indicates the HSRP group to which this interface belongs. Specifying a unique group number in the

	standby command enables the creation of multiple HSRP groups.
Switch(config-if)# **no standby** Group-number **ip** ip-address	Disable HSRP on the interface

3.3.3.3 Design of the HSRP in the project

To gain some redundancy in case of link failure HSRP- Hot Standby Routing Protocol HSRP was configured for VLAN10, the virtual router address was 192.168.10.5. Configurations were added on switch 2 and 3.The idea was, that if a link between switch 2 and 7 became unusable, the switch 3 would be used. The same configurations can be done for all the VLANs in the network with their own standby ip numbers. Figure 15 shows the real network design of the HSRP.

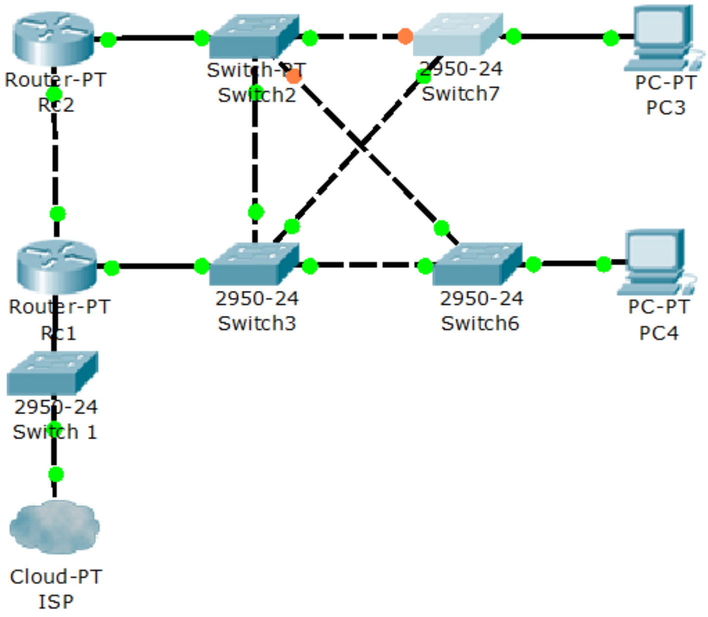


FIGURE 15: Design the HSRP of the network (Chen Lu,2014.)

Example of switch 2 configuration:

```
S2#show standby
Vlan10 - Group 1
State is Active
5 state changes, last state change 02:13:01
Virtual IP address is 192.168.10.5
```

```
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.297 secs
Preemption disabled
Active router is local
Standby router is 192.168.10.2, priority 100 (expires in 8.976 sec)
Priority 100 (default 100)
IP redundancy name is "hsrp-Vl10-1" (default)
```

3.4 Theoretical explanation

In this chapter, the functions of the abbreviations which mentioned in the previous section will be illustrated, and more theories will be put here to fulfill the chapter.

3.4.1 OSPF

OSPF substitutes the Open Shortest Path First routing protocol. It is a fairly complex protocol made up of several protocol handshakes, database advertisement, and packet types. In this part, the basic configuration and verification of OSPF will be described.(Baidu,2006.)

3.4.1.1 Instructions

Open Shortest Path First is a kind of Interior Gateway Protocol (IGP), it is using in a simple autonomous system. It achieve a link-state routing protocol belongs to the IGP because of the manner in which they distribute routing information and calculate routes. Figure 16 shows the link-state protocol operation in the OSPF.

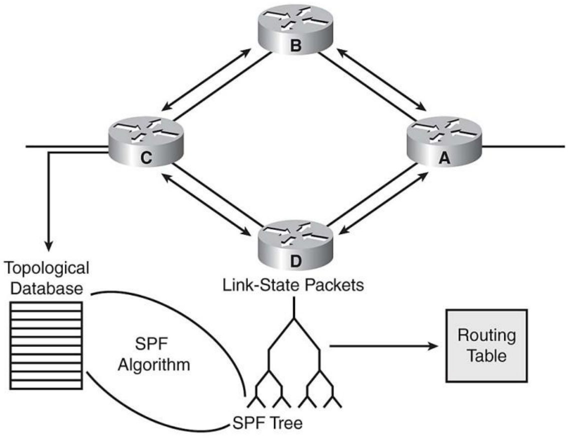


Figure 16. Link-state Protocol operation (Baidu web page.)

Routers running link-state routing protocols collect routing information from all other routers in the network, and then each router independently calculates its best paths to all destinations in the network, using the Dijkstra’s(SPF)algorithm. Incorrect information from any particular router is less likely to cause confusion because each router maintains its own view of the network. Compared with RIP, OSPF is a link-state protocol, while RIP is a distance vector protocol. And the administrative distance are not the same for the different systems in the companies. For example, the AD for the Cisco Protocol is 110.

3.4.1.2 Terminology and protocol

3.4.1.2.1 Router-ID

Image that the people in the world have their own special name differ from others. So if you want to find someone, it is easier to look for them by providing his or her name. It seems that the special name is the connection among people. OSPF is similar to the situation above, each OSPF router in the network are equivalent to one person, the notice to each other between the OSPF link state router likes that when someone else intend to contact you. In this way, if the points between the routers do not recognize who they are, there is not possible to determine their identity. So it seems that the link status is meaningless. It is necessary to define each OSPF router an identity, it looks the same to the person's name, which is the router-ID, and router -ID in the network must not have duplicate names. Otherwise from the received link state router, you cannot determine the identity of the initiator, it cannot be determined by link status information network location. Link status will be issued in writing OSPF router on its own router-ID, It should be understood likes the signature of link status, link status generated by different routers would not get the same signature.

An OSPF router ID uniquely identifies each OSPF router in the network. The OSPF routing process chooses a router ID for itself when it starts up. The router ID is a unique number in IP address format that can be assigned in the following ways:

By default, the highest IP address of any active physical interface when OSPF starts is chosen as the router IS. The interface does not have to be part of the OSPF process, but it has to be up. There must be at least one “up” IP interface on the router for OSPF to use as the router ID.

Alternatively, if a loopback interface exists, its IP address will always be preferred as the router ID instead of the IP address of a physical interface, because a loopback interface never goes down. If there is more than one loopback interface, the highest IP address on any active loopback interface becomes the router ID.

Alternatively, if the router-id ip-address OSPF router configuration command is used, it will override the use of the address of a physical or loopback interface as the router ID. Using the router-id command is the preferred procedure for setting the router ID. (Baidu web page.)

If a router receives a link state but cannot reach the location of the Router-ID. So it is impossible for you to reach the target network link status. Router-ID can only calculate when OSPF getting start, or after resetting the OSPF process.

3.4.1.2.2 Link

It is the interface on the router. In this part, it refers to the interface on the running OSPF.

3.4.1.2.3 Link-State

Link state (LSA) is the description of the interface information, Such as the IP address on the interface, subnet mask, network type, Cost values, etc. The routing tables are not exchanged between routers in the OSPF, but the link state (LSA) does. OSPF calculating the precise path reaching to each destination network by acquiring the entire link state information .OSPF router will send all the issued link states unreservedly to all neighbors. And the neighbors will put all the receiving link-states into the Link-State Database, the neighbors pass the information one by one to another in the transmission process without any changes. By this process, all the OSPF network routers will receive all the network link state and the link status of all routers should be able to depict the same network topology.

It seems that to have a metro map in our daily life. When you choose a station as your starting point, what information you need to draw a metro map is that you need to know all the stations from your starting point from the near to the distant. However, the OSPF is using all the interface information from the routers to calculate the network topology.

3.4.1.2.4 OSPF areas

As the OSPF routers (LSA) will interchanged the link between states without reservation, when the network expand to a certain extent, LSA will form an enormous database, it will left a huge pressure on the calculating of OSPF .In order to reduce the complexity of calculating the OSPF, and caching calculated pressure, OSPF will calculate using the sub region, which means to divide the OSPF routers in the network into different regions, each regions responsible for their respective LSA transmission and precise route calculation, and then simplify the LSA in a region and aggregate them together then finally forwarding to another area. In this way, within the region, it receive the precise LSA in a different area of a network .It pass simplified LSA effectively. In order to try to divide the area into a non-ring network design, using the Hub-Spoke topology architecture will be the best way which shows in the figure 17, which stands for the core of topology and branch.

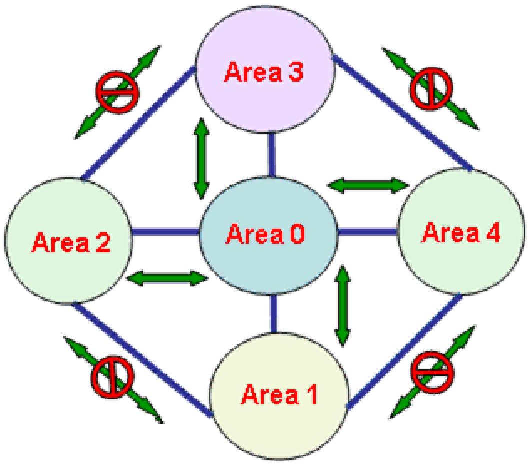


FIGURE 17. Hub-Spoke network (Baidu web page.)

Integer numbers can be used to name the area, such as 1,2,3,4. It is also possible to take the form of an IP address to name it, such as 0.0.0.1, 0.0.0.2. Because of using the Hub-Spoke architecture, it is necessary to define a core, and then other parts will connected to the core. OSPF area 0 is the core of all regions, it is called the backbone area, and the other areas are called as Normal area (general area). In theory, all of the general area should be directly connected to the general area and the general area can only exchange Link-state area (LSA) with backbone area .There is no LSA exchanged between the two general areas even if directly connected to each other.

As Figure 17 shows Area 1, Area 2, Area 3, Area 4 and Area 0 can only exchange LSA, and then be forwarded by Area 0. Area 0 is like a transit point, two general areas need to exchange LSA, it can only be sent first to the area 0, then forwarded by the area 0, but it cannot be forwarded to each other between the general areas.

OSPF areas are divided based on the interfaces of the routers rather than on the entire division router, a router may not only belong to a single region, but also can belong to more than one area. As shown in the Figure 18 :

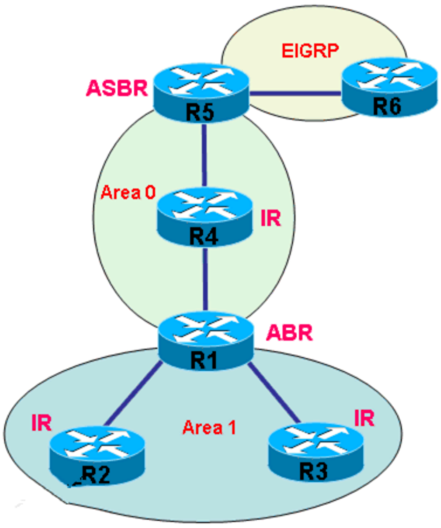


FIGURE 18. OSPF area (Baidu.)

If the OSPF router belongs to a single area, it means that the interfaces of the OSPF router all belong to the same region. Then this router is called on Internal Router (IR), such as the R2, R3 and R4 in Figure 18. If the OSPF router belongs to more than one area, it means the interfaces of the router do not belong to a region, then this router is called area Border Router (ABR), As the R1 in the figure 18 above. Finally, ABR can summarize the LSA, then forwarded to another area. If an OSPF router redistributes external routing protocol into OSPF, then this router is called Autonomous System Boundary Router (ASBR), as shows in the figure 18 above, R5 will redistribute the EIGRP into OSPF, so R5 is called ASBR, but if the router can only redistributes the OSPF into other routing protocols, it cannot be called ASBR. Any OSPF routers all can be configured into ABR or ASBR. (Baidu web page.)

Because OSPF has a variety of areas, and therefore the OSPF routing in the routing table also exist in many forms, it can be divided into the following categories:

- If they are in the same routing area, it is called the Intra-Area Route; the O is represented in the routing table.
- If they are in the different routing area, it is called the Inter-Area Route Summary Route, using O IA represented in the routing table.
- If they are not in the OSPF routing area, or a different OSPF routing process, only to be redistributed to OSPF, it can be called the External Route, using O E2 or OE 1 which is represented in the routing table.

A router can run multiple OSPF processes or not should be considered during the configuring. OSPF with different processes can be regarded as no-relationship, if they need to exchange routing information with each other, and the only way is to re-distribution. Each OSPF process can have multiple zones, while the router's link state database is divided into sub-regional processes and to be stored.

3.4.1.2.5 Neighbor

OSPF will only exchange between neighboring LSA, the router sends all content from link state database to all the neighbors unreservedly. You must first form OSPF neighbor, then exchange LSA between OSPF routers, and OSPF neighbor establish and maintain by sending Hello packets. Hello packets are sent periodically at the start of the OSPF interfaces on different networks, the interval for sending Hello packets will be different, when there are more than four times for the Hello time, which means neighbor's Hello packet is not received after the Dead time. If the two OSPF routers in order to be the OSPF neighbor, they need to fulfill the four conditions as following, of which they need to be the same:

Which they need to be the same:

- Area-id
- Hello and Dead Interval
- Authentication
- Stub Area Flag

3.4.1.2.6 Adjacency

Two OSPF can have a relationship to be neighbors, but not necessarily mutually exchange LSA. As long as the exchange of LSA, the relationship is called adjacency (Adjacency).Between neighbors, they only exchanged the Hello packets, but between adjacency, they can not only exchange the Hello packets, but also the LSA.

3.4.1.2.7 DR/BDR

When multiple OSPF routers connected to the same multi-access network, if the LSA are interchanged between each two routers, then the segment will be filled with many LSA entries. In order to minimize the number of LSA spread through multi-access, a core router should be selected, and it is called DR (Designated Router).

All OSPF network routers and DR interchange LSA. In this way, DR contains all the LSA, and forwarded all the LSA to each router. DR is like a transit station of the LSA segment. All routers are interchanging LSA with the transfer station. If the DR fails, it will result in the loss of the LSA and incomplete. So when we choose a router to be the DB among the multi-access network, we also need to select another router called BDR (Backup Designated Router) which will put into use when the DB is out of use.

3.4.1.3 Network Types

There are five defined networks in the OSPF (Baidu):

- Point-to-point: Proposed by the Cisco network type, the neighbor can be discovered automatically, it does not need to select DR / BDR, 10s for the hello time.
- Broadcast: Proposed by the Cisco network type, the neighbor can be discovered automatically, it does not need to select DR / BDR, 10s for the hello time.
- Non-broadcast: Proposed by the RFC, the neighbors can be configured manually, it does the DR / BDR election, 30s for hello time.
- Point-to-multipoint: Proposed by the RFC, the neighbor can be discovered automatically, it does not need to select DR / BDR, 30s for the hello time.
- Point-to-point non-broadcast: Proposed by the Cisco network type, the neighbor can be configured manually. It does not need to select DR / BDR, 30s for the hello time.

3.4.1.4 OSPF LSA types

There are many types in the OSPF LSA, each of them has different features. It will show as follows :(Baidu web page.)

3.4.1.4.1 Router LSA

Each router will have a Router LSA. The LSA only spread this in the region, it describing all the links and router interfaces, status, and overhead.

3.4.1.4.2 Network LSA

In each multi-access network, DR will produce this Network LSA. And it only describes all routers which connected to it in the production area of this Network LSA flooding (including the DR itself).

3.4.1.4.3 Network Summary LSA

It is originating from the ABR router, it used to advertise the destination address outside the region. It will not run the SPF algorithm after the other routers when received from the ABR Network Summary LSA.

3.4.1.4.3 ASBR Summary LSA

It is issued by the ABR, the ASBR summary LSA is an ASBR rather than an network, and the features will be the same as Network Summary LSA.

3.4.1.4.4 AS External LSA

It is started from the ASBR router. It used to advertise to reach the external destination of the OSPF autonomous system or the external LSA default route in the OSPF autonomous system.

3.4.1.4.5 Other types

Group Membership LSA,NSSA External LSA, External Attributes LSA, Opaque LSA(link-local scope),Opaque LSA(area-local scope),Opaque LSA(AS scope).etc.

3.4.1.5 OSPF metric

In Cisco routers, using the formula 100Mbit / bandwidth (in units of Mbit) to calculate, but the bandwidth is equal to 100Mbits. It is not a good value when the value in the link is greater than 100Mbits.

```
RouterA (config-if) # ip ospf cost interface-cost

The lower the costs, the better the link

RouterA (config-router) # auto-cost reference-bandwidth ref-bw

Which cost: 1 ~ 65535 ref-bw: 1 ~ 4294967
```

Because not all the routers need information from outside of the network, in order to reduce the LSA Pan magnanimity and routing table entries, a peripheral area should be created. The ABR which located in the border of Stub will declare a default route to the internal router.

3.4.1.5.1 Stub area restrictions

All the routers in the stub area must maintain LSDB information synchronization, and they will set the E bit (E-bit) with a value of 0 in the Hello packets. These routers are not receiving Hello packets when the value of E bit is 1. It can be explained that routers which have not been configured in the stub area will not establish adjacency relationships with other routers which have been configured as stub router.

You cannot configure a virtual link in the stub area, and also the virtual links cannot cross the stub area.

- The routers in the stub area cannot be the ASBR.
- Stub area could have more than one ABR, but due to the default of the route, ABR internal router cannot determine which is the best choice to reach the ASBR .
- The external routing allowed to be declared for the OSPF domain by NSSA, meanwhile the characteristics of the stub area can be retained.
- Totally stub area is the whole region of the stub, and even the type of LSA 3 cannot be receiving.

3.4.1.5.2 Basic commands in the OSPF

The commands of single-area and multi-zone configuration will be show as following:

LOOPBACK interface address configuration

```
ROUTER (config) # interface loopback 0

ROUTER (config) # ip address IP address mask
```

Configure the ospf area

```
router ospf 100

network 192.168.1.0 0.0.0.255 area 0

router-id 192.168.2.1 manually set the router-id

area 1 default-cost 50 to manually set the overhead

# clean ip ospf process network 192.168.1.0 0.0.0.255 area 0

router-id 192.168.2.1 /*manually set the router-id */

area 1 default-cost 50  /*manually set the overhead */

# clean ip ospf process
```

configure ospf Plaintext authentication

```
interface s0

ip ospf authentication

ip ospf authentication-key <; password>
```

Configure ospf authentication ciphertext

```
interface s0

ip ospf authentication

ip ospf message-digest-key 1 md5 7 <; password>
```

debug ip ospf adj and open debug ospf

```
show ip protocols

show ip ospf interface s0
```

Configure the interface manually, the bandwidth and priority

```
inter s0

ip ospf cost 200

bandwidth 100

ip ospf priority 0
```

Configure virtual link

```
router ospf 100

area <area-id> virtual-link <router-id>

show ip ospf virtual-links

Show ip ospf border-routers

Show ip ospf process-id

Show ip ospf database

show ip ospf database nssa-external
```

OSPF routing induction

```
Router ospf 1 /*routing induction for ASBR external routes for */

Summary-address 200.9.0.0 255.255.0.0

Router ospf 1 /* routing induction from AREA1 to AREA0 */

Area 1 range 192.168.16.0 255.255.252.0
```

Configure Stub area

```
IR area <area-id> stub
```

```
ABR area <area-id> stub
```

Configure totally stubby area

```
IR area <area-id> stub
```

```
ABR area <area-id> stub no-summary
```

Configure NSSA

```
ASBR router ospf 100

area 1 nssa

ABR router ospf 100

area 1 nssa default-information-originate
```

3.4.1.6 Conclusion

The OSPF using in the final project aims to complete network because of the advantages. And it will be summarized into several points as following:

- OSPF is a real LOOP-FREE (no route from the ring) routing protocol. The advantages derived from the algorithm itself.
- OSPF has the fast convergence. It will pass route changes to the entire autonomous system in the shortest and possible time.
- After proposing the concept of regionalism, the autonomous system is divided into different areas. Through a summary the routing information between areas, the number of routing information that needs to pass has been reduced greatly. Also the routing information will not expanding rapidly with the expansion of network.
- OSPF controls the overhead of the protocol to a minimum.
- OSPF has go through four divisions in the level routing, a more credible route selection can be provided.
- OSPF has good security, and it supports the plaintext and md5 verification based on the interfaces.

- OSPF adapt to a variety of networks, and up to thousands.

3.4.2 SVI

SVI is stand for switch virtual interface, it interactive three management Vlan address. SVI is the ip interface to contact the vlan, only one SVI link to one vlan.

There are two types of SVI:

- Host management interface. Administrators can use this interface to manage the switch.
- Gateway Interface. It is using for inter-vlan routing between three switches. In specific use interface vlan interface configuration command to create SVI, then you can achieve the function of routing to configure ip address.

A switch virtual interface (Switch Virtual Interface, SVI) represents VLAN constituted by the switch port (in fact, commonly refers to VLAN interfaces). It proposes to achieve the functions of system routing and bridging. A switch virtual interface corresponds to a VLAN. When needed protocols that between traffic routing or bridging between non-routable virtual LANs, and provides a connection to the switch's IP host, you need to configure the virtual switch to the appropriate virtual LANs Interfaces. Actually, it commonly refers to SVI VLAN interface, but it is a virtual interface. It has been used to connect the entire VLAN and generally refers to the interface which is a Layer 3 interface. (Baidu web page.)

SVI interfaces were created when typing specific VLAN ID after global-configure the interface vlan command. You can use the **no interface vlan vlan_id** global configuration command to delete the interface has been default for remote switch management.

All VLANs should been configured with the SVI interfaces for routing traffic between VLAN. The function of SVI interface is purpose to provide inter-VLAN communication routes. If you need to get the traffic route between VLAN, you need to configure a VLAN interface (which is mentioned here SVI) for each VLAN, and an IP address assigned to each SVI interfaces.

SVI has a feature as exclude automatic status which called Auto state Exclude. SVI interfaces were open when SVI line state with multiple VLAN on the port meets with the following conditions:

VLAN are existing, furthermore, it is active in the VLAN database switch. VLAN interface are existing and administrable.

By default, there are multiple ports in a VLAN, VLAN, and SVI interfaces will be closed after all ports have closed.

SVI can be used the exclude port state automatically to configure the interfaces, it does not include considering the status of SVI interface.

3.4.3 HSRP

HSRP is the abbreviation of Hot Standby Router Protocol. It is a unique technology of the Cisco platform and also a Cisco proprietary protocol. Figure 19 shows a basic topology of the HSRP.

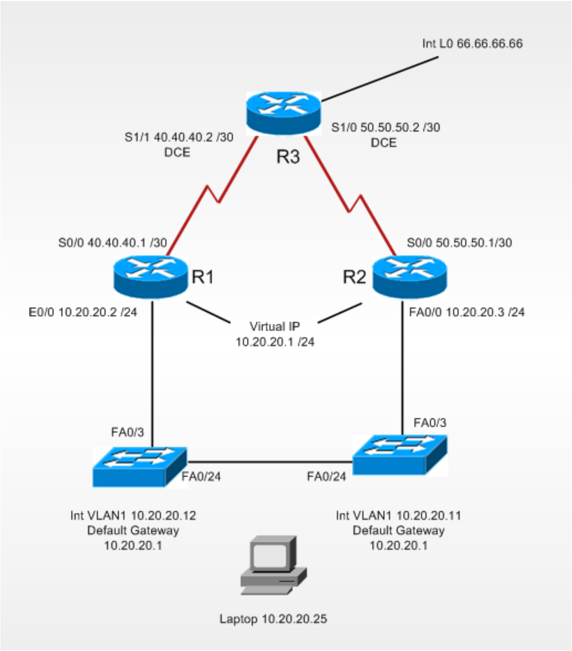


FIGURE 19. Cisco HSRP (Cisco configuring HSRP.)

The protocol contains multiple routers which corresponding to a HSRP group. There is only one router take charge of the forwarding traffic among the users, which called the active router. When the active router fails, the backup router will assume the role as a new active router. This is the principle of thermal backup.

The condition of achieving a HSRP is that there should be more than one router in the system, and they will form a "hot backup group", then the group forms a virtual router. At any time, only one router within a group is active, and it will forward the packets. If the active router fails, the router will select a backup to replace the active router. But from the points of the host in the network, the virtual router has not been changed. So the host remains connected to the router, the previous failure does not affect any subject.

To reduce the errors in the data traffic of the network, only the active router and the backup router sends HSRP packets periodically after setting the router and the backup router to the activity status. If the active router fails, the backup router takes over the active router.

In a real particular LAN, there are may be more than one hot backup groups coexist or overlap. Each hot backup group works simulate as a virtual router, it has a Well-known-MAC address and an IP address. The IP address, the interface of the routers within the group and the host can be in the same subnet, but they cannot use the same address. When the multiple hot standby groups existing in a LAN, the host will be distributed to different hot backup groups, the load will be balanced.

There is another technology called VRRP (Virtual Router Redundancy Protocol), it is similar to the HSRP in function. But from the security aspect, VRRP has a major advantage: it allows the group to participate in the establishment of the inter-device, as explained earlier, the HSRP virtual router cannot be one of the router's ip addresses, but VRRP allows to happen. On the other hand, the VRRP is better than the HSRP. There are six states (initial (Initial) status, learning (Learn) state, listening (Listen) state, the dialogue (Speak) state backup (Standby) status, activity (Active) status) and eight events in the HSRP, but only VRRP has three states (initial state (Initialize), the main state (Master), backup status (Backup)) and five events.(Baidu web page.)

The reason to favor to use the HSRP in the network is that it has outstanding features. It will be illustrated as follows:

- HSRP has a high reliability. When using the HSRP protocol between two routers, when either router is down or the router Wide Area Network (WAN) is port down, it will quickly switch to the other one.
- HSPR can effectively achieve load balancing.
- HSRP makes the utmost of the multi-port Ethernet router functions on divided multi-service network. Only multi-port Ethernet router HSRP applications can achieve load sharing between two routers, which is the greatest advantage of a router with four Ethernet ports.
- By setting the VLAN on the switch, HSPR can effectively control the security of two subnets.
- There will not be any failure in a single point of the HSRP.

4 CONCLUSION

Based on the experiment I did from the beginning of January to the middle of February, the whole part of Cisco was finished successfully. The Juniper devices can be added to continue the experiment.

The aim of the research was to provide a design of an optical fiber network in the city of Kuopio. This study presented a combination of theory and practice. The Cisco books provided knowledge to be used in the Cisco part. The presented project was conducted by using the Cisco devices. It was professional experience for me to work with my classmate Chen Chen and Zhang Yuxuan. The final project lays a foundation for me whether to further my studies or work in a technical company in the future.

REFERENCES

Black Box. Fiber optical technology. [electronic file]. [accessed 18 February 2014]. Available from:

http://www.blackbox.com/resource/genpdf/White-Papers/Fiber-Optic-Technology.pdf

Baidu. HSPR. [web document]. [accessed 18 February 2014]. Available from:

http://baike.baidu.com/view/51200.htm?fr=aladdin

Baidu. OSPF. [web document]. [accessed 18 February 2014]. Available from:

http://baike.baidu.com/view/6234950.htm?fromId=64365&fr=wordsearch

Cisco Quick Product Reference Guide 2013. [electronic file].2013. [accessed 18 February 2014]. Available from:

http://www.bradreese.com/reference-guide-january-2013.pdf

Cisco web page. [webpage]. [accessed 18 February 2014]. Available from:

www.cisco.com

Cisco-kid.co.uk. Hot Standby Routing Protocol (HSRP). [web publication]. [accessed 18 February 2014]. Available from:

http://cisco-kid.co.uk/routing/hsrp

Froom,R., Sivasubramanian,B.& Frahim,E. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide. 2011

Interno FG500-R. Installation Guide. [electronic file]. [accessed 18 February 2014]. Available from:

http://www.intenogroup.com/Portals/0/IntenoFiles/ProductDocs/5/5/Quickguide_FG500.pdf_20111127213037.pdf

Kaminow, I.,Li,T.& Willner,E.A. "Fiber-Optic Communications Systems" . 2013. 3rd edition

Rahim,M.S.B.A. Optical fiber audio communication system. [electronic file]. 2007. [accessed 18 February 2014]. Available from:

http://eprints2.utem.edu.my/1918/1/Optical_Fiber_Audio_Communication_System_-_24_pages.pdf

Ramaswami, R & Sivarajan, R.K. Optical Networks. [electronic book]. [accessed 18 February 2014]. Available from:

http://dc185.4shared.com/doc/ZpewkEQC/preview.html

Science guy. Optical fiber communication advantages. [web publication].2009. Computer Pheripherals and General info.

Sivasubramanian,B. The formation of multi-cisco switched networks. 2007

Teare,D. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide: Foundation learning for the ROUTE 642-902. 2010

Volume VIA . Optical Fiber Telecommunications. 6th Edition

Wikipedia. Optical fiber. [webpage] [accessed 18 February 2014] . Available from:

http://en.wikipedia.org/wiki/Optical_fiber#Optical_fiber_communication