
Bachelor's Thesis

Information Technology

2010

Chi Zhang

HIGH AVAILABILITY (HA) TESTING OF KING GUARD FIREWALL

– for Lenovo Security Technologies (Beijing), Inc.



TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Telecommunication and e-Business | Information Technologies

April 2010 | 85

Vesa Slotte

Chi Zhang

HIGH AVAILABILITY (HA) TESTING OF KING GUARD FIREWALL

Presently, the importance of networking enjoys popular support all over the world. Accordingly, networking companies have been trying to meet or even surpass the requirements of clients in order to strengthen their customer relationships. For the clients, obtaining the maximum of profit and minimizing operational cost is the essential problem. Therefore, networking companies should conduct a reliable and continuously available system for their customers to avoid downtime risks or hardware failure.

The High-Availability (HA) is a reliable technique of system. It is capable of protecting the system by involving redundant equipment to set up a standby group, which could ensure that if one forwarding piece of equipment failed, another backup piece of equipment would be activate to take over the work immediately. In this thesis, the KingGuard firewall is utilized to test the performance of High-Availability technique which belongs to the Lenovo Security Technologies, Ltc. This thesis is expected to simulate the real user environment now in the company, as well as deal with different situations of fault tolerance. The whole testing procedure combined with the HA testing topology simulates the availability of KingGuard firewall in real-world scenario, with the purpose of creating a relatively comprehensive way for HA testing in networking.

KEYWORDS:

Firewall, High-Availability (HA), Heartbeat Link, Software Testing, Single Point of Failure(SPOF), Recovery and Pre-empts.

TABLE OF CONTENTS

1	INTRODUCTION	9
1.1	Background	9
1.2	Product information	10
1.3	Thesis aim and Objective	12
1.4	Thesis questions	12
1.5	Limitation of the thesis	13
1.6	Thesis structure	13
2	TESTING ENVIRONMENT	15
2.1	Introduction	15
2.2	Users' network environment	15
2.2.1	Network topology for simulating user environment	16
2.3	Flow analysis	17
2.4	Users' specific demands on testing	18
2.5	Focus and problems	18
2.6	Summary	19
3	TESTING DESIGN AND METHODS	20
3.1	Introduction	20
3.2	Time arrangement of the test	20
3.3	Introduction to testing design	20
3.4	Testing methods and terminology	21
3.4.1	CISCO's three-layered system structure	21
3.4.2	HSRP (Hot Standby Router Protocol)	26
3.4.3	Some concepts related to HA testing	30
3.5	Summary	33
4	TESTING PROCEDURES AND RESULTS	34
4.1	Introduction	34
4.2	Network topologies	34
4.2.1	Physical topological diagram	35
4.2.2	Logical topology diagram	36
4.2.3	Routing topology diagram	37
4.3	Normal network flow and direction diagram	39
4.4	Malfunction testing of firewall and switches	41

4.4.1 Test 1: Malfunction in firewall Master 1	41
4.4.2 Test 2: Malfunction in firewall Back 1	43
4.4.3 Test 3: Malfunction in firewall Master 2	45
4.4.4 Test 4: Malfunction in firewall Back 2	47
4.4.5 Test 5: Malfunction 1 in switch Master A	48
4.4.6 Test 6: Malfunction 2 in switch Master A	50
4.4.7 Test 7: Malfunction 1 in switch Back A	52
4.4.8 Test 8: Malfunction 2 in switch Back A	54
4.5 Malfunction recovery and preempt	55
4.5.1 Test 9: Master 1 recovery and preempt 1	55
4.5.2 Test 10: Back 1 recovery and preempt 1	58
4.5.3 Test 11: Master 1 recovery and preempt 2	61
4.5.4 Test 12: Back 1 recovery and preempt 2	64
4.5.5 Test 13: Situation 1 of Master A recovery and preempt	67
4.5.6 Test 14: Situation 2 of Master A recovery and preempt	70
4.5.7 Test 15: Situation 3 of Master A recovery and preempt	73
4.5.8 Test 16: Situation 4 of Master A recovery and preempt	76
4.6 Summary	79
5 CONCLUSIONS	80
5.1 Review of the answers to the research questions	80
5.2 The problems occurring in the testing process	81
5.2 Summary of the testing process	82
REFERENCES	83
APPENDIX	85

LIST OF FIGURES

List of Figures

Figure 1.1	KingGuard 9000 series security gateway	11
Figure 1.2	8x8 matrix parallel processing system	11
Figure 2.1	Network topology for simulated user environment	17
Figure 3.1	CISCO three layered hierarchical model	23
Figure 3.2	An example of virtual MAC and IP address of HSRP	29
Figure 3.3	An example of firewall in transparent mode	31
Figure 4.1	Physical topological diagram	35
Figure 4.2	Logical topology diagram	36
Figure 4.3	Routing topology diagram	37
Figure 4.4	HSRP is enabled between Master A and Back A	39
Figure 4.5	The results of normal network flow	40
Figure 4.6	The direction of the network flow under normal situation	40
Figure 4.7	The situation 1 of malfunction in Master 1	41
Figure 4.8	The net flow direction under Master 1 malfunction	42
Figure 4.9	The PING duration under Master 1 malfunction	42
Figure 4.10	The situation 1 of malfunction in Back 1	43
Figure 4.11	The net flow direction under Back 1 malfunction	44
Figure 4.12	The PING duration under Back 1 malfunction	44
Figure 4.13	The situation of malfunction in Master 2	45
Figure 4.14	The net flow direction under Master 2 malfunction	46
Figure 4.15	The PING duration under Master 2 malfunction	46
Figure 4.16	The situation of malfunction in Back 2	47
Figure 4.17	The situation 1 of malfunction in Master A	48
Figure 4.18	The net flow direction under Master A malfunction 1	49
Figure 4.19	The PING duration under Master A malfunction 1	49
Figure 4.20	The situation 2 of malfunction in switch Master A	50
Figure 4.21	The net flow direction under Master A malfunction 2	51
Figure 4.22	The PING duration under Master A malfunction 2	51
Figure 4.23	The situation 1 of malfunction in switch Back A	52
Figure 4.24	The net flow direction under Back A malfunction 1	53
Figure 4.25	The PING duration under Back A malfunction 1	53
Figure 4.26	The situation 2 of malfunction in switch Back A	54

Figure 4.27	The situation of Master 1 before recovery	55
Figure 4.28	The net flow direction of Master 1 before recovery	55
Figure 4.29	The situation of Master 1 after recovery	56
Figure 4.30	The net flow direction of Master 1 after recovery	56
Figure 4.31	The PING duration under Master 1 after recovery	57
Figure 4.32	The flow direction shift under Master 1 after recovery	57
Figure 4.33	The situation of Back 1 before recovery	58
Figure 4.34	The net flow direction of Back 1 before recovery	58
Figure 4.35	The situation of Back 1 after recovery	59
Figure 4.36	The net flow direction of Back 1 after recovery	59
Figure 4.37	The PING duration under Back 1 after recovery	60
Figure 4.38	The flow direction shift under Back 1 after recovery	60
Figure 4.39	The situation 2 of Master 1 before recovery	61
Figure 4.40	Netflow direction in situation 2 of Master 1 before recovery	61
Figure 4.41	The situation 2 of Master 1 after recovery	62
Figure 4.42	Netflow direction in situation 2 of Master 1 after recovery	62
Figure 4.43	The PING duration in situation 2 of Master 1 after recovery	63
Figure 4.44	Flow direction shift in situation 2 of Master 1 after recovery	63
Figure 4.45	The situation 2 of Back 1 before recovery	64
Figure 4.46	Netflow direction in situation 2 of Back 1 before recovery	65
Figure 4.47	The situation 2 of Back 1 after recovery	65
Figure 4.48	Netflow direction in situation 2 of Back 1 after recovery	66
Figure 4.49	The PING duration in situation 2 of Back 1 after recovery	66
Figure 4.50	Flow direction shift in situation 2 of Back 1 after recovery	66
Figure 4.51	The situation 1 of switch Master A before recovery	67
Figure 4.52	Netflow direction in situation 1 of Master A before recovery	67
Figure 4.53	The situation 1 of switch Master A after recovery	68
Figure 4.54	Netflow direction in situation 1 of Master A after recovery	68
Figure 4.55	The PING duration in situation 1 of Master A after recovery	69
Figure 4.56	Flow direction shift in situation 1 of Master A after recovery	69
Figure 4.57	The situation 2 of switch Master A before recovery	70
Figure 4.58	Netflow direction in situation 2 of Master A before recovery	70
Figure 4.59	The situation 2 of switch Master A after recovery	71
Figure 4.60	Netflow direction in situation 2 of Master A after recovery	71
Figure 4.61	The PING duration in situation 2 of Master A after recovery	72

Figure 4.62	Flow direction shift in situation 2 of Master A after recovery	72
Figure 4.63	The situation 3 of switch Master A before recovery	73
Figure 4.64	Netflow direction in situation 3 of Master A before recovery	73
Figure 4.65	The situation 3 of switch Master A after recovery	74
Figure 4.66	Netflow direction in situation 3 of Master A after recovery	74
Figure 4.67	The PING duration in situation 3 of Master A after recovery	75
Figure 4.68	Flow direction shift in situation 3 of Master A after recovery	75
Figure 4.69	The situation 4 of switch Master A before recovery	76
Figure 4.70	Netflow direction in situation 4 of Master A before recovery	76
Figure 4.71	The situation 4 of switch Master A after recovery	77
Figure 4.72	Netflow direction in situation 4 of Master A after recovery	77
Figure 4.73	The PING duration in situation 4 of Master A after recovery	78
Figure 4.74	Flow direction shift in situation 4 of Master A after recovery	78

LIST OF ABBREVIATION

HA	High Availability
TCP/IP	Transmission Control Protocol/Internet Protocol
VSP	Versatile Security Platform
CPU	Central Processing Unit
vCPU	Micro-CPU
HSRP	Hot Standby Router Protocol
ACL	Access Control List
LAN	Local Area Network
VLAN	Virtual-LAN
MAC	Media Access Control
IOS	Internetwork Operating System
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
NAT	Network Address Translation
OSPF	Open Shortest Path First
SPOF	Single Point of Failure

1 INTRODUCTION

1.1 Background

Networking is playing an increasingly significant role in this information age. Therefore, constructing a reliable and continuously available system and network is a major problem companies are facing. One way to solve this problem is to design a system with high availability. The purpose of HA is to ensure and deliver a network that can protect the system from downtime risks or hardware failure, thereby minimizing operational cost. A high availability network can be achieved through a variety of techniques, e.g., fast re-route, network re-route, load-sharing and dual network devices management, etc. In this thesis, the focus is to test whether a system fulfills the characteristics and conditions of high availability.

Network Security is an especially essential part for some sensitive organizations , e.g., government, police , etc. Instead of protecting all sensitive information by performing the functions of firewall on each computer, we could combine all the security services into one piece of equipment or a group of equipment specifically. In this way, we could save more computing resources and shorten the time for connection and authentication of local area. For security, the firewall devices become the control point next to the external internet for filtering all the packets and preventing hacking. ([1]) Thus, it is important to provide high availability for the firewall devices, which means that if the main communication link crashes, another backup device could be started immediately and automatically.

To realize high availability, we need at least two firewall devices to compose the HA Cluster which links them together. ([2]) One is configured as the master device; the other one is configured as the backup device. By default, the master device is in active status for routing and sending packets and the backup device is in passive status. However, when the master device crashes, the backup device will immediately become active to take over the work to

maintain the availability of network communication. Furthermore, to synchronize the information between the master and backup devices, there is a heartbeat link to ensure that the information of the configuration and status of each node in the cluster are sent to the other nodes periodically. ([3])

This thesis introduces eight different fault situations in HA testing, four of which relate to the firewall, and the others relate to the switches. It also presents an individual analysis of all situations and how the problems are dealt with automatically. In addition, the Cisco three-layer hierarchical model, consisting of the core layer, the distribution layer, and the access layer, used to implement the tests, is discussed, as well.

1.2 Product information

This test was based on the project of Digital Beijing, which involved testing new series of firewall products developed by different companies. The purpose of this project was to select the security machines with highest performances and flexibilities among all related products.

As a member of the testing group sent by Lenovo Security Technologies (Beijing), Inc., the author is responsible for the HA testing with another member, Zhigang Liu. The product we used this time is the new series of firewall products, KingGuard. Our task is to simulate the customers' environment, create the platform and then test all possible situations that would happen.

The KingGuard security gateway was launched in June, 2008, the capabilities of which network security processing could reach up to 20 Gbps throughput. Based on the Versatile Security Platform (VSP) of Lenovo's independent innovation, KingGuard contains a multi-core, multi-thread processor and hardware structure with high reliability.



Figure 1.1 KingGuard 9000 series security gateway

“KingGuard applies several innovative technologies like unique matrix parallel processing and dynamic load balancing multi-core CPU to improve security network processing capability and reliability of the whole system.”[product literature]

KingGuard security gateway uses a matrix parallel processing system, in which the 64 micro-CPU (vCPU) was divided into $8 * 8$ matrix, processing and pipelining the data in a parallel way. In order to achieve efficient processing of the data, Lenovo Security Technologies developed the “Windrunner” matrix parallel processing algorithms, which can dynamically predict the bottleneck of the CPU-matrix and make a real-time schedule of the micro-CPU resources.

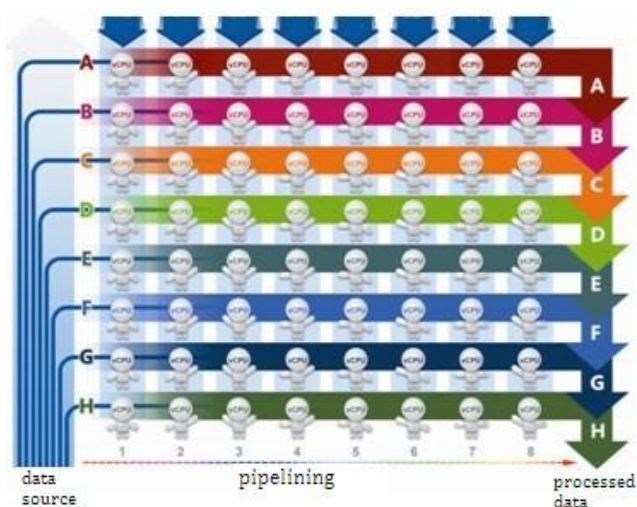


Figure1.2 8x8 matrix parallel processing system ([4])

1.3 Thesis aim and objective

The primary focus of this thesis is testing the HA performance of the KingGuard firewall. This study simulates the user environment, as well as deals with different situations of fault tolerance. The whole testing procedure combined with the HA testing topology simulates the availability of KingGuard firewall in a real-world scenario, with the purpose of creating a relatively comprehensive method for HA testing in networking.

As mentioned earlier, high availability enables organizations to provide redundant systems for customers to keep their services available all the time, without needing to worry about connection failure or loss of information. In this way, organizations can better maintain efficient communication and a good relationship with their customers. Therefore, it is necessary to consider not only the testing procedure, but also the commercial practicality.

This thesis mainly utilizes the Cisco three-layer hierarchical model as segmentation and Hot Standby Router Protocol (HSRP) to make a virtual IP gateway on the distribution layer to keep the stability of the network. In addition, all testing firewalls are of HA active/standby type in transparent mode, which means that the firewall interprets all the packets crossing through it without any change in the configuration. The purpose of this thesis is to investigate the usefulness of this HA testing method for further development.

1.4 Thesis questions

This thesis attempts to provide ways for customers and test engineers to achieve the thesis' aim as previously mentioned with the following thesis questions:

- How could the Cisco three-layer hierarchical model be used?
- Can this testing procedure be used for a company's malfunction analysis in reality?
- Does the malfunction analysis procedure in this thesis comprehensively simulate all the possibilities that would happen?

The expected result is a workable HA testing method that can help test engineers and customers to diagnose the situation efficiently when the system fails in some node.

1.5 Limitation of the thesis

The focus of this thesis is to test the usability of the method to know whether it could simulate the malfunction immediately and the product could take over the communication link automatically. However, its reliability testing is beyond the scope of this study, which means that we cannot obtain the peak value of reliability through this testing procedure. Another limitation might be the performance. Only those malfunctions related to specific functions of the products, but not such malfunctions as the connection interruption caused by other physical factors, will be taken into consideration of our study.

1.6 Thesis structure

This thesis is divided into six chapters:

Chapter 1 introduces the thesis. It starts with the overall objective, thesis questions and limitations.

Chapter 2 introduces the testing environment, which includes the network topology that simulates the user environment, the actual reduced graph, the network flow analysis, and the counter-measures we create to meet users' specific needs. Some details that we should pay special attention to are put forward at the end of this chapter.

Chapter 3 describes the test design and method, which includes the introduction to the test design, the proper testing method that we make according to the design ideas, and the test duration. In addition, some terminologies involved in the testing process will also be explained in this chapter.

Chapter 4 shows the major steps of the testing. The first step is to formulate typologies according to the customers' individual situation, and set up the network environment based on the route topology. The second step is to analyze the data flow direction in a normal situation, draw up the flow graph, and ensure that the established network runs properly. The third step is to set up different fault nodes in a normally-running network to test the network's performance. Here, we pay special attention to classifying all possible single point failures, and altogether make a list of eight categories of various firewall faults and switch faults. Finally, the network flow direction in the circuit is tested when the malfunction occurs, so as to check whether the master and backup devices are successfully synchronized.

Chapter 5 deals with fault recovery and preempt, which is also the focus of this test. We will recover all possible major fault nodes, i.e., the eight different categories of faults mentioned in Chapter 4 in sequence, observe and analyze the network activities after the recovery, and ensure that the master device instantly perform preempt tasks and return into active state after the fault recovery.

In Chapter 6, answers are first given to the thesis questions proposed in Chapter 1 in the preliminary stage of testing, and the weak points in the products discovered in the testing process are listed out. Finally, comments are made on the whole testing process.

In the Appendices of this thesis, the configuration information of some devices related on both distribution layer and core layer are presented for reference.

2. TESTING ENVIRONMENT

2.1 Introduction

Companies design their projects and make product design strategies in accordance with customer needs, on the basis of which we design the test. Therefore, only when we understand the customers' core demand and use environment in depth can we satisfy their needs completely and accurately in the testing design. And a clear design diagram could accurately express design scheme, enabling designers and non-professionals to better understand the whole designing concept.

In order to better agree with the users' environment and demands, the user environment is introduced first. Then rational plans and the topology of the testing are made accordingly. Next, a tentative analysis of the packets forwarding direction under normal conditions is made, and, finally, some details that we should pay attention to in the following testing process are listed.

2.2 Users' network environment

Configuring a testing environment is an important step in conducting the test. Whether the testing environment is suitable will severely affect the reliability and validity of the test. It is our hope that the testing environment is infinitely close to the actual environment the customers will be using. However, due to the limitation of various sources, we could only conduct the testing in an approximate simulation environment.

In the planning phase of the testing, fully understanding of customers' needs and knowing the basic characteristics of the products well is important as this helps to design the testing environment, coordinate and use all kinds of sources reasonably. In addition, it facilitates the process of acquiring temporarily unavailable resources, thereby ensuring the smooth implementation of the plan.

An inappropriate environment in the testing plan could slow down the whole development of the project.

In addition, simulating and fully understanding the actual user environment is of profound importance in a testing project, for the following reasons:

1. To ensure the performance stability of the device. For example, if the maximum number of concurrent users in system peak hour is known, we could check whether all transactions could meet the customers' needs within the response time through Stress Testing, whether the performance indexes of the system are within normal scope under this stress, and whether such adverse reaction as abnormal program termination occurs due to the stressed system.
2. To test fault tolerance. Through simulating some possible abnormal situations, for example, unexpected server power cut, intermittent internet connection, we could check whether there is an auto-processing mechanism that could guarantee the normal operation of the system and whether there are measures to restart the operation.

Therefore, we should attach great importance to the testing environment. We should try our utmost to reduce the unfavorable effect of the testing environment to the minimum, and avoid problems arising from the testing environment.

2.2.1 Network topology for simulating user environment

According to the customer's request to simulate the connection from offices of all floors to the server cluster, two switches are to be used. One of the switches is used as a floor aggregation switch, and the other will be connected with the server cluster.

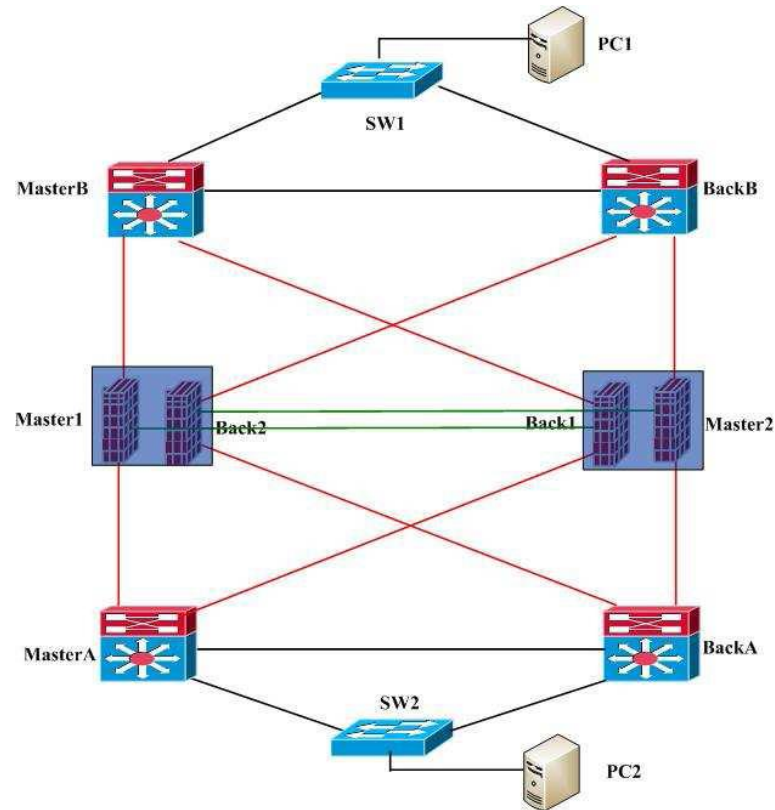


Figure 2.1. Network topology for simulated user environment

In Figure 2.1, Master B and Back B are core switches, Master1, Back1, Back2, and Master2 are the KingGuard's 10 gigabit firewalls, and Master A and Back A are aggregation switches. The customer required that SW2 was connected with the server cluster and SW1 was the floor aggregation switch. KingGuard firewall is of HA Active/Standby type in transparent mode. In the Figure above, the red line is 10 gigabit Ethernet, the black is the gigabit link while the green one is the heartbeat link.

2.3 Flow analysis

When the structure and design of the network are completed, we need to make further analysis of the whole network situation, get to know the data flow direction, and how the flow will change when there is something wrong with a certain node. Only in this way can we better simulate the user environment and accordingly make a proper estimate of possible effects on customers.

Here through the theoretical analysis we have obtained typical-usage scenarios and alternative solutions before the test commences. “Typical-usage” here means the normal data flow direction with all lines connected, and “alternative solutions” means the solution which the system automatically adopts to replace the normal flow when a certain node in the line is interrupted and the flow direction has to be changed. ([5])

The network’s normal flow direction here is: PC1→Master B→master1→master A→PC2. When there is a firewall malfunction, network traffic flow direction will be:

- ① PC1→Master B→Back1→master A→PC2
- ② PC1→Back B→Master2→Back A→PC2
- ③ PC1→Back B→Back2→Back A→PC2

2.4 Users’ specific demands on testing

Considering that customers have a high demand for the stability of their business and for quick recovery ability after malfunction occurs, we have adopted corresponding measures in the beginning of the test design:

1. The concept of double-redundancy is adopted in all devices in the network design.
2. The devices in the network can achieve fast re-routing and the network stability is assured.
3. In actual environment, all firewalls are with dual Network Interface Card. They are directly linked to Master A and Master B.

2.5 Focus and problems

In order to obtain more characteristic, comprehensive, and valuable testing results, we should pay special attention to some technical details that are worth noticing in the testing process. ([6])

Below we have listed seven points that deserve our attention in the testing procedures:

1. The application of HA master/backup mode in transparent environment and its problems;
2. The time the network needs to shift to stable condition either with or without traffic;
3. The synchronization of the session between master and backup firewall;
4. When there is network flow, which protocols will be used and what size the packets are;
5. How to deal with the unsuccessful synchronization of the configuration between Master 1, Back 1 and Master 2, Back 2;
6. Malfunction analysis and location: in the later stage of network maintenance, how to identify network malfunction quickly and how to know the actual data flow direction in the network.

2.6 Summary

In this chapter, we have simulated and analyzed the user environment, produced a feasible testing graph to the needs of customers, made a theoretical analysis of the network data flow direction, and listed the customers' particular demands in the testing process for reference. Finally, we have made a survey of all the problems that require special attention, making preparation for later results. We will elaborate on the testing procedures from the next chapter on.

3. TESTING DESIGN AND METHODS

3.1 Introduction

After we have fully understood the user environment and their needs, we will start with design mentality and testing methods. An excellent designing mentality is a prerequisite to a high availability testing result. It is the link between customer demand and testing process. A good designing mentality should produce a solution that is to the best benefit and the most satisfaction of the customers' demand, according to such factors as customer demand, network layer structure, security, and feasibility. Meanwhile, an outstanding design frame assists users and other non-professionals in making sense of the designers' thoughts.

In this Chapter, we first introduce the testing mentality and on the basis of it, work out appropriate testing approaches. After that, we will explain some terminologies which are mentioned in the testing mentality or involved in the testing process.

3.2 Time arrangement of the test

Due to the limitation of available devices in the company, every testing group needs to pre-plan the time they will use, to the convenience of the company's coordination. After the testing plan is made, we estimate that the testing duration will be five working days. On the first day, we will set up the network environment, configure the network interface and protocols. From the second to the fourth day, we will conduct the test. On the last day, we will summarize the testing and review the configuration files. The detailed description of the testing process is to be found in Chapter Four.

3.3 Introduction to testing design

According to the Cisco network structure model, the internal network is divided into core layer, distribution layer, and access layer. In this environment, both

Master B and Back B are devices on the core layer, Master A and Back A are devices on distribution layer, while SW1 and SW2 are on the access layer. In the light of the latest network application report, we adopt the three-layered network structure, i.e., the route protocol on the devices from the distribution layer to the core layer, which ensures network stability and quick location and recovery of malfunctions. As for the access layer devices, we adopt HSRP (Hot Standby Router Protocol), which is used on the network devices on the distribution layer. In this way, there is a virtual gateway for every device on the access layer to guarantee network stability.

We will explicate the Cisco network model and HRSP mentioned above in detail later in this chapter. Due to device restriction, we could only simulate a 100-megabit fast network environment, while the customers' core network environment is of the 10-gigabit network environment. So our main goal is only to verify the high availability of the network design. Although products' continuous operation ability under the maximum number of concurrent users and fault tolerance are also important criteria to evaluate product quality, we will not take them into account in this thesis.

3.4 Testing methods and terminology

3.4.1 Cisco's three-layered system structure

Concept of hierarchy

The Cisco three-layered model was first proposed 20 years ago by Cisco Systems, Inc. At that time, the local networks, composed of some servers, PCs and printers, constitute the first generation of campus networks. For those small-scaled networks, the malfunction on a certain section will influence the whole network. In order to solve these problems, Cisco introduced the programming design standard based on hierarchy and modularity.

A structured system is based on two complementary principles: hierarchy and modularity. Any large complex system must be built using a set of modularized components that can be assembled in a hierarchical and structured manner. (Cisco, Enterprise Campus 3.0).

This hierarchical system divide all physical and logical components in to three layers and each layer which represents a certain area in the network structure functions differently. It simplifies the process of maintaining a reliable and

large-scale network, because it constructs three functional areas in the network rather than the packets. Thus, the whole network is clear and easily manageable. The administrator can manage and control the data by setting limits to the name lists getting in and out on some layers, and when there is something wrong with the network, we could make an analysis of a certain layer easily.

However, with the increasing demands from customers, this three-layer model may not help enterprises locate and retrieve information or communicate with each other conveniently and securely. For this reason, Cisco has introduced a more comprehensive enterprise architecture, which utilizes five elements (*Campus, Data Center, Branch, Teleworker, WAN*) to create models for enterprise operation flow. However, the introduction of this architecture is beyond the scope of this thesis. For more specific information about the Cisco Enterprise Architecture, please refer to CCNP2 online academic materials, Chapter 1.1.1 and 1.1.2.

Three-layered model

Every layer in Cisco's three-layered model has its individual configuration methods and responsibilities. When we configure the physical implementations of a hierarchy network, we can allocate either one or multiple devices on a certain layer to achieve the same function. At the same time, we could use one device to simulate the different functions achieved on two layers. The three layers are as follows:

- The core layer
- The distribution layer
- The access layer

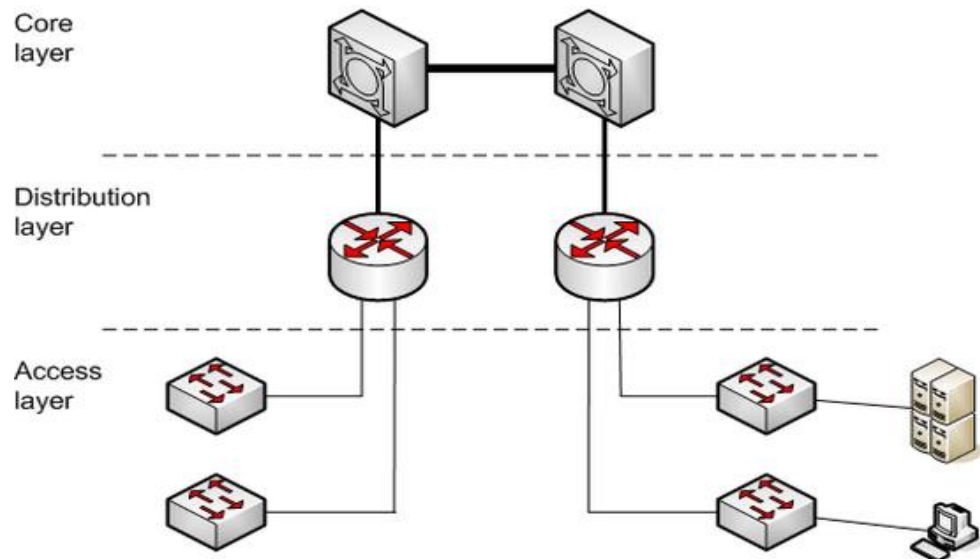


Figure 3.1. Cisco three-layered hierarchical model

Now we are going to explain the three layers in detail:

The core layer

As the backbone of network, the core layer could be utilized to connect multiple buildings or multiple sites, and it can connect a server cluster, such as the Internet, VPN, WAN, etc., as well. It shoulders the responsibility to transfer a great quantity of data quickly and reliably. The designing engineers must ensure that the core layer is fault-tolerant. When unexpected malfunctions occur in the system, the core layer could respond to it shortly and continue running within tolerant condition and scope without any shift or diversion. Due to the fact that a malfunction in the core layer would inevitably affect all users in the network, efficiency is the key for the core layer. The realization of core layer functions can reduce network complexity, facilitate management and cut malfunction elimination workload.

The objective of the core layer, macroscopically, is to enable data to be transferred among different parts of the network efficiently and rapidly. Concretely, the designing objective of the core layer is to provide 100% normal operation time, improve throughput to the utmost, and support the rapid growth of the network.

The distribution layer

As a workgroup layer, the distribution layer is correlated with path selection and filtering, and it is considered as the communication point between the access and the core layer. So the designing engineers have to take the needs of the other two layers into consideration while designing this layer. The access layer is usually organized using the second layer switching technology while the distribution layer uses the third layer devices. The objectives to be achieved on this layer are as follows:

1. Filter and manage data flow. Receive and send data packets according to pre-established transferring mechanism and rules; transfer data to assigned destination according to source and target address information; update information data timely; utilize access control list (ACL) to limit access and prohibit undesired data getting into core network. ACL is a conditional list, which is used to monitor the network traffic that tries to go across the route interface, and it designates data groups to be received, and groups to be rejected and excluded by the router.
2. Carry out access control strategies. Read the received data packets, classify and send them according to priority, so as to control the data packet access.
3. Gather route information before informing the core layer of the route. The distribution layer is also a convergence node to the access layer. It gathers route information before sending data to the core layer, forming a connecting link between the access layer and the core layer.
4. Prevent the malfunction or interruption on the access layer from affecting the core layer. On the distribution layer devices, there are redundant connections with access layer switches and core layer devices. Once a malfunction occurs on a certain connection or device, these redundant connections can provide a substitute route. By adopting an appropriate routing protocol on the distribution

layer, the third layer could respond quickly to the connection malfunctions, so as to prevent them from affecting the whole network operation.

5. Routing among access layer VLAN. It can be realized among virtual LANs and other workgroup on the distribution layer.

The relay link is used to connect the access layer and distribution layer, which means that the same link can be used among devices to transfer multiple VLAN data flow. Redundant links might exist among devices on the distribution layer, and we could configure these devices so that load balancing, which is another way to add available broad brand to application programs, could be achieved on multiple links.

The access layer

The access layer is sometimes called desktop layer. It is the network edge that is connected with terminal devices, used to control users' access to Internet sources. Access layer services and devices are usually located in every building, every remote site, server cluster, and enterprise edge. Users can get access through Internal wired facilities, or wireless access point. Devices that are connected to the access layer could be used for personal computers, printers, IP phones, cameras, and video conferencing etc., and all these services could be merged into a single basic facility on the access layer.

The access layer is to perform the following functions:

- Filter MAC address. By configuring switches, some specified systems are allowed to be connected to related LANs.
- Divide conflict area. The switch can improve system performance through setting up a new conflict area.
- Share broad brand. All data are allowed to be processed in one shared network link. The collision domain describes a portion of an Ethernet network at layer 1 of the OSI model where any communication sent by a node can be sensed by any other node on the network. ([7])

- Manage device bandwidth. Data in one network link can be transferred to another network link to achieve load balancing.

3.4.2 HSRP (Hot Standby Router Protocol)

Introduction of HSRP

As Internet becomes more popular, people grow more and more dependent on it. This tendency requires more stable network, and thus device-based standby structure comes into being, which is with the same reason why the dual hard disk structure is adopted in the server to enhance data security. Router or three-layered switches are the core and heart of the whole network.

If some deadly malfunction occurs in the router, the whole local network will collapse. Be it the bone router, a larger scope of the network would be affected and the loss caused would be unimaginable. Therefore, a hot standby device is an inevitable choice to improve network reliability. When one router fails and cannot run, Cisco's HSRP permits another router to take over the failed router automatically, and realize IP route fault tolerance. HSRP allows two or more routers configured with HSRP to use the MAC address and IP address of one virtual router.

HSRP's operating principle

To realize HSRP, multiple routers in the system are indispensable. They constitute a "hot standby group", which forms a virtual router. Only one router in the group is active at any time, and is used to transfer data packet. If the active router breaks down, it will be replaced by another chosen standby router. However, the host in this network will not notice the change in the virtual router. Thus, the host stays connected and is free from the influence of malfunctions which solves the problem of router shift well.

In order to lessen network traffic, only the active router and the standby router can send HSRP reports regularly after being configured. If the active router fails, the standby router will take over to be the active one. And if the standby

router fails, or it replaces the active router, another router will be chosen to be the standby router.

In an actual particular local area network, there may be several hot standby groups existing side by side or overlapping. Each hot standby group simulates one virtual router working, and each owns a well-known-MAC address and an IP address. The IP address, router interface address within the group, and the host share a subnet, but they are not the same. When multiple hot standby groups exist in one LAN, distributing hosts to different hot standby groups will enable load sharing.

HSRP adopts a prioritized solution to decide which router configured with HSRP will be the default active router. If the priority of a router is configured higher than that of other routers, this router will become the active router. The default priority of a router is set as 100, so if only one router is configured higher than 100, this router will be the active router.

HSRP selects its current active router by broadcasting HSRP priority among those routers with HSRP configuration. If an active router fails to send a “hello” message within a pre-set period of time, the standby router with the highest priority becomes the active router. The packet transmission among routers is transparent for all hosts in the network.

Routers with HSRP configuration exchange the following three multi-node broadcasting messages:

- ◆ Hello—The hello message is to notify other routers to send their HSRP priority and status information. Routers send out a hello message every 3 seconds by default;
- ◆ Coup—A standby router sends out the coup message when it wishes to become the active router.
- ◆ Resign—When the active router receives a hello message with a higher HSRP priority sent by another router, it sends out a “resign” message.

An HSRP-configured router is in one of the following four statuses at any moment:

- ◆ Initial –The router is of this status before its HSRP starts. Normally, the router enters this status when changing configuration or initiating ports.
- ◆ Learning – The router, neither active nor standby, has already been assigned a virtual IP address. It keeps monitoring the HELLO messages sent from the active and standby router.
- ◆ Listen -- The router is monitoring HELLO messages. It knows the virtual IP address, but neither active nor standby status.
- ◆ Speak –With this status, the router sends HELLO messages at regular intervals, and takes an active part in selecting an active or standby router.
- ◆ Standby—The router is ready to take over packet transferring when the active router fails.
- ◆ Active—The router is forwarding packets.

The application of HSRP in this testing

In this test, we generate the virtual network by configuring the devices with HSRP on the distribution level, to guarantee the stability of the network. A virtual router is not a physical being. It represents a public router object which can provide fault tolerance. What we need to do is configure the two or more devices, which constitute a hot standby group, with the MAC and IP address of the virtual router. See the figure below:

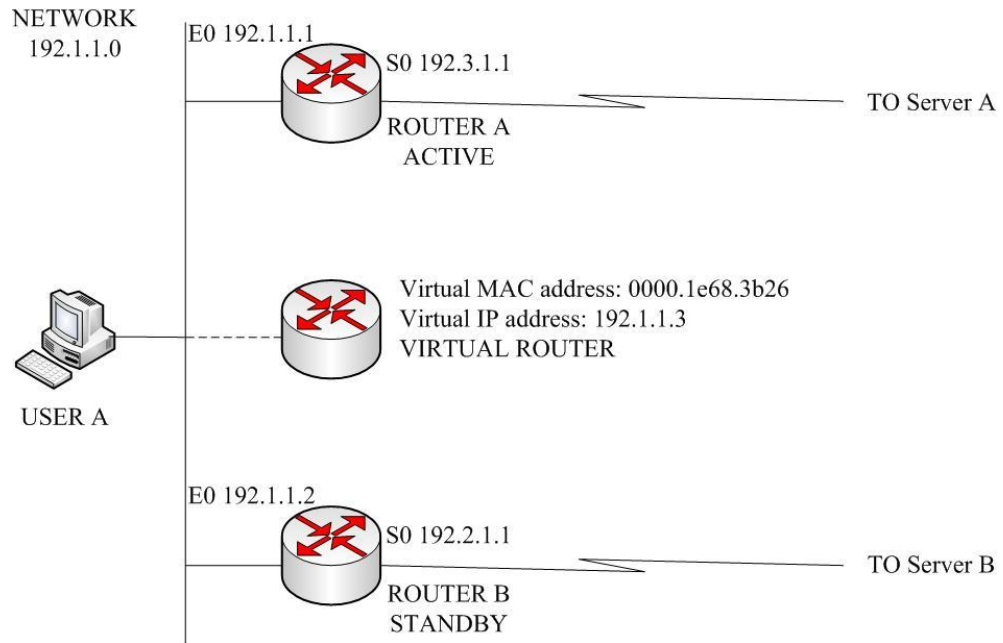


Figure 3.2. An example of virtual MAC and IP address of HSRP

We assume the MAC address of the virtual router is 0000.1e68.3b26. When the router is configured with HSRP, it will automatically choose from the address pool of Cisco IOS software a virtual MAC address, which is within the MAC address scope of Cisco Company. The default router that connects to user interface network is configured with the IP address of the virtual router instead of that of router A. The packets sent to server by users are sent to the MAC address of the virtual router. Router A is initially set as active router and router B is set as standby router. Both router A and B are allocated the IP address and MAC address of the virtual router. If router A stops transferring data packets due to some reason, the route protocol is converged, router B will take over from A to be the active router. That is to say, router B responds to the virtual MAC address and the virtual IP address. Users will continue to use the IP address of the virtual router to send packets to the server and router B will receive these packets and send them to the target network through interface B.

3.4.3 Some other concepts related to HA testing

Active/standby mode

HA solutions are mainly based on the redundancy mechanism of the system components. If a component fails on account of something, the system is still able to operate on another redundant device. The level of HA is dependent on its configuration mode and replication strategy. ([8])

HA has two different models: active/standby model and active/active model. In the active/standby model, the master and standby devices help and cooperate with each other in working. Under normal circumstances, the master is the priority device. Once the master fails, the standby devices will automatically modulate its internal organizing patterns and take the master's place to keep the continuous operation of both the internal and external network, and thus avoiding loss. The active/active model is to achieve the function of load balancing and hot standby with all devices in the HA clusters running at the same time. In this testing process, the active/active model is beyond the scope of our study, so we are not going to discuss further this model.

The HA active/standby model is a failover model. That is to say, once there is a malfunction, a standby device will take over from the failed device. In the HA cluster, only one active device is processing all network traffic, while another one or more devices are in passive status, and they do not process any network traffic, only monitor in real-time whether the active device is still running normally. The main job of the standby devices is to:

- Synchronize configuration with active device in real-time;
- Listen the status of the active device;

If the function of “session pick-up” is enabled, the standby device needs to synchronize the sessions of the active device. So when there is something wrong with the active device, it could take over from the active device transparently. In addition, none of the sessions established earlier on the active

devices needs to be re-established. The “session pick-up” function supports all TCP/UDP/ICMP/multicast/broadcast traffic when the firewall access control list is disabled.

However, if the function of session pick-up is not enabled, the standby device will not synchronize the sessions established on the active device in real-time. So when HA shifts, all the sessions established earlier on the active device will have to be re-established.

Transparent mode

The second concept involved in HA we need to mention here is the application of transparent mode in the testing. Traditionally speaking, the firewall is regarded as a routed hop in the line, and it plays the role of user default gateway. However, in transparent mode, the firewall is used as a second-layer device. It can accomplish the communication between the internal and external network without users’ noticing its physical existence. The firewall in transparent mode is like a network bridge. It cannot select a path and configure NAT, but it can analyze every data packet (such as upper-layer data packet as IP traffic included) crossing through it, and forbid or permit their flow, by means of Access Control List (ACL). In this way, it not only raises the network security but also reduces the complexity of user management.

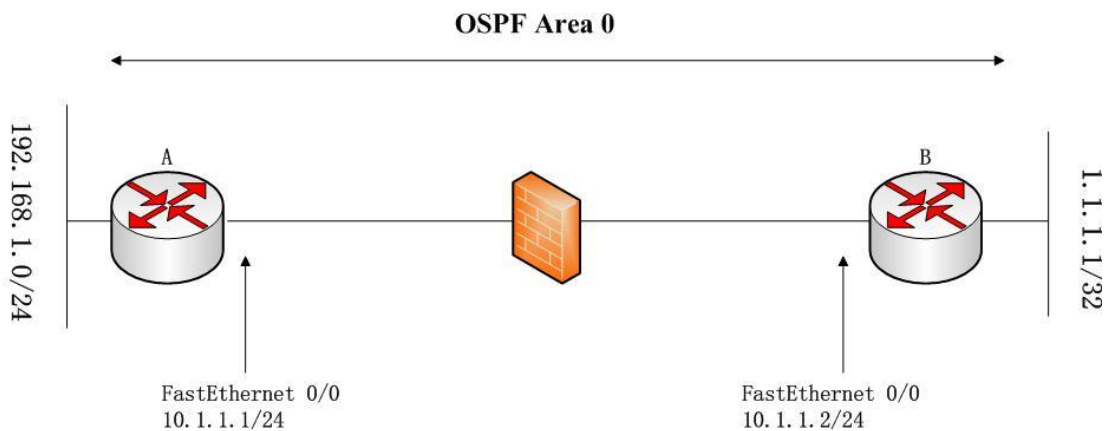


Figure 3.3. An example of firewall in transparent mode

When the firewall is running in transparent mode, the outlet of data packets is determined by its MAC address, instead of the three-layered route. The firewall can be directly installed and put into use, and the users do not need to reset and modify the route, which is just as in the case of switches, the users do not need to configure the IP address. That is to say, the networks that are connected to it are within the same subnet as shown in Figure 3.3. The only difference is their VLAN number. Suppose A is an internal network client, B is an external network server, and C is the firewall in transparent mode. When A requests connection to B, the TCP connection request is intercepted and monitored by the firewall. If A's address is found to be in the Access Control List, A's request is permitted, and the connection, from A to C and then to B, is established. As users see it, A and B are directly connected, while actually A is connected to B through the firewall C. Conversely, the same applies when B requests to connect with A. However, if B's address is not in the firewall's ACL, B cannot transfer data to A. These connections are completed automatically, and there is no need to manually configure anything in the client. Moreover, users do not know the existence of the medium. Therefore, we say the firewall is transparent for users.

In this HA test, our focus is to test the feasibility of HA testing approaches, so we have adopted the interface in transparent mode, with which there is no need to change the users' original network typologies, and helps to simplify the firewall configuration. Actually, there are other modes for the firewall except for transparent mode, which are beyond this test, so we will make no further analysis of them here.

Heartbeat link

The concept of heartbeat link

A heartbeat link is a network cable used to link server A and server B. In these two servers, A, the active server, and B, the standby server, are connected by a heartbeat link. Any server can monitor the other's operating condition in real-time through a heartbeat link. Once the running master A fails because of

various hardware malfunctions, for example, power failure, failure of main components, or failure of boot disk, etc., the heartbeat link will report to the standby host, and host B can get into work immediately. In this way, the normal operation of the network is best guaranteed.

The operating principles of heartbeat link

The heartbeat link is the core element in HA-related solutions. The purpose of establishing a heartbeat link is for 2 main devices to check whether the other device is alive or not. That is to say, the two devices send request packets to each other at regular intervals. If the other device fails to respond to the requests several times, it will be deemed as dead by the request side. When this happens, if the request side is the backup device, it will be activated and take over all services. That is the operating principle of the heartbeat link.

The signal of heartbeat link is running on the TCP/IP network, as well. However, HA without non-TCP/IP network can not differentiate TCP/IP failure from node failure, thus network failure will result in isolated node, and the backup device will take over the resources by mistake.)

3.4 Summary

In this chapter, in view of customer demands mentioned in Chapter 2 , we have discussed the designing mentality, including the Cisco three-layered structure, HSRP, HA active/standby model, transparent mode, heartbeat link configuration, and the reasons why we use those specifications and protocols. Moreover, we have explained the terminologies involved in the testing methods. In next chapter, we will start conducting the test and give an analysis of all results.

4. TESTING PROCEDURES AND RESULTS

4.1 Introduction

This chapter presents the topologies created in the thesis for the testing segmentation and customer profitability analysis. For example, physical topologies give a complete description of the devices in the test; logical topologies and route topologies, which cover three-layered topologies with IP address distributions, facilitate network administrators to check and administrate. In the second stage, we will simulate the malfunctions in the main elements of the network and analyze them.

4.2 Network topologies

The network nowadays is becoming more and more complex, with different network devices produced by various manufactures distributed among all departments of a company. Sometimes, the distribution is within a city or several cities across the country, and the physical range of distribution becomes larger and larger as the company's business expands. Purely manual administration and passive monitoring and checking cannot guarantee the normal operation of the whole system. Network administrators are now facing the problem of how to deal with event reports sent by so many devices, and how to detect the fault node in the shortest time when a network malfunction happens. In order to maintain the normal operation of network, and to better serve the business system of the company, we urgently need active monitoring on the network, automatic detection and resolution of the network malfunction.

4.2.1 Physical topological diagram

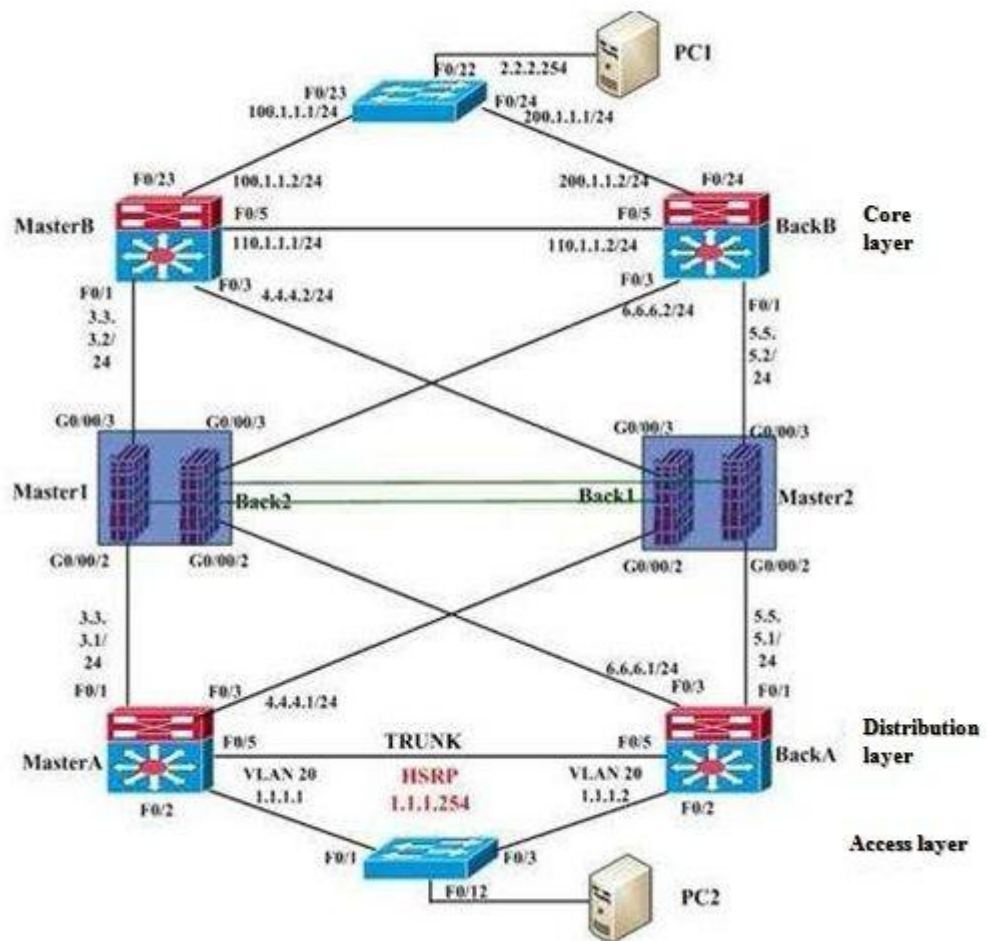


Figure 4.1. Physical topological diagram

As shown in Figure 4.1, PC1 simulates the outlet device, PC2 simulates the server cluster. Master B and Back B are core switches. Master 1 and Back 2 constitute a KingGuard 9202 10-gigabit firewall, while Back 1 and Master 2 make up another KingGuard 9202 10-gigabit firewall. Among them, Master 1 and Black 1 are active/standby devices to each other, same as in the case of Master 2 and Back 2. They all adopt transparent mode. Master A and Back A are two distribution layer switches. The black line represents a 10 gigabit interconnecting wire, and the green line represents the heartbeat link.)

4.2.2 Logical topology diagram

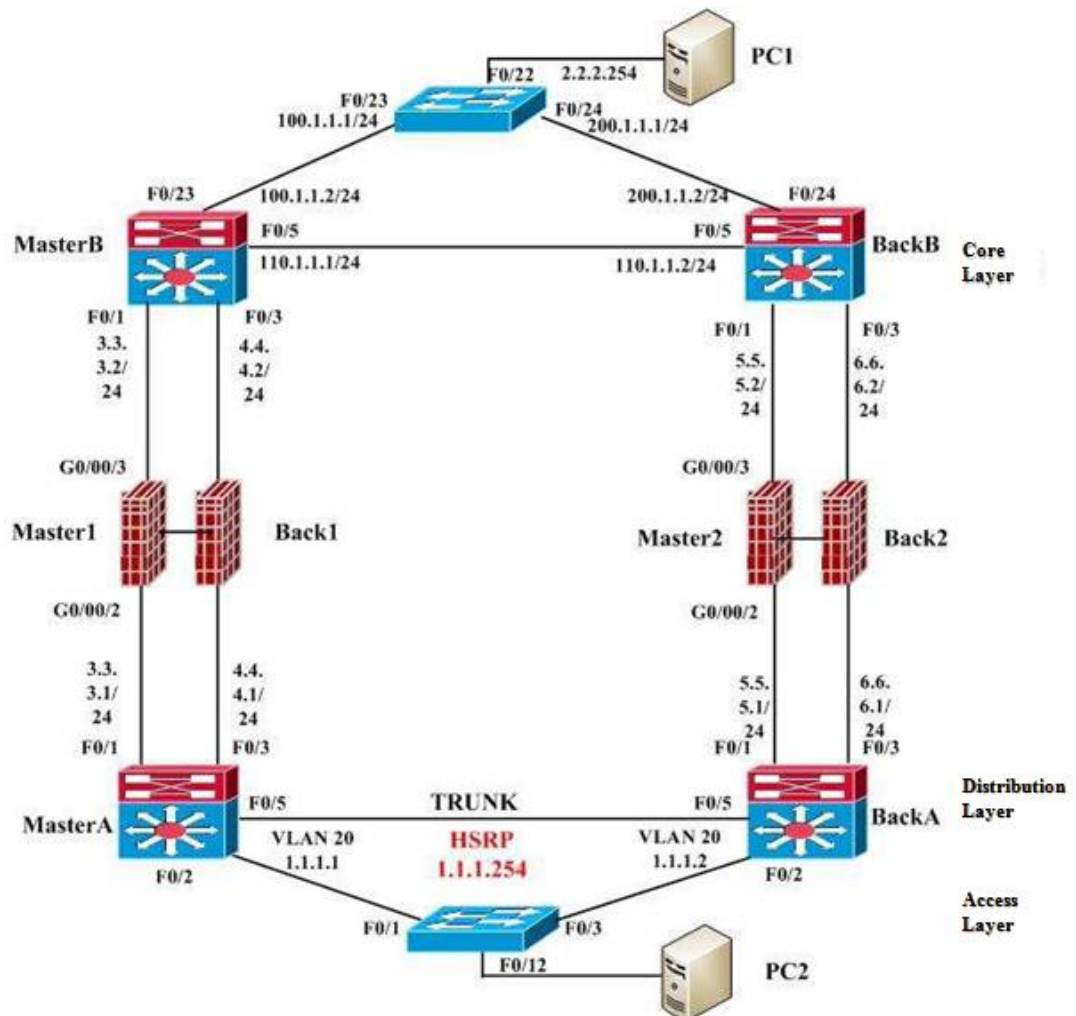


Figure 4.2. Logical topology diagram

Physical topologies can be converted to logical topologies shown in Figure 4.2. Master 1 and Back 1 constitute a KingGuard 9202 10-gigabit firewall. Among them, Master 1 and Back 1 are active/standby devices to each other, and Master 2 and Back 2 are active/standby devices to each other. They are all used in transparent mode.

4.2.3 Routing topology diagram

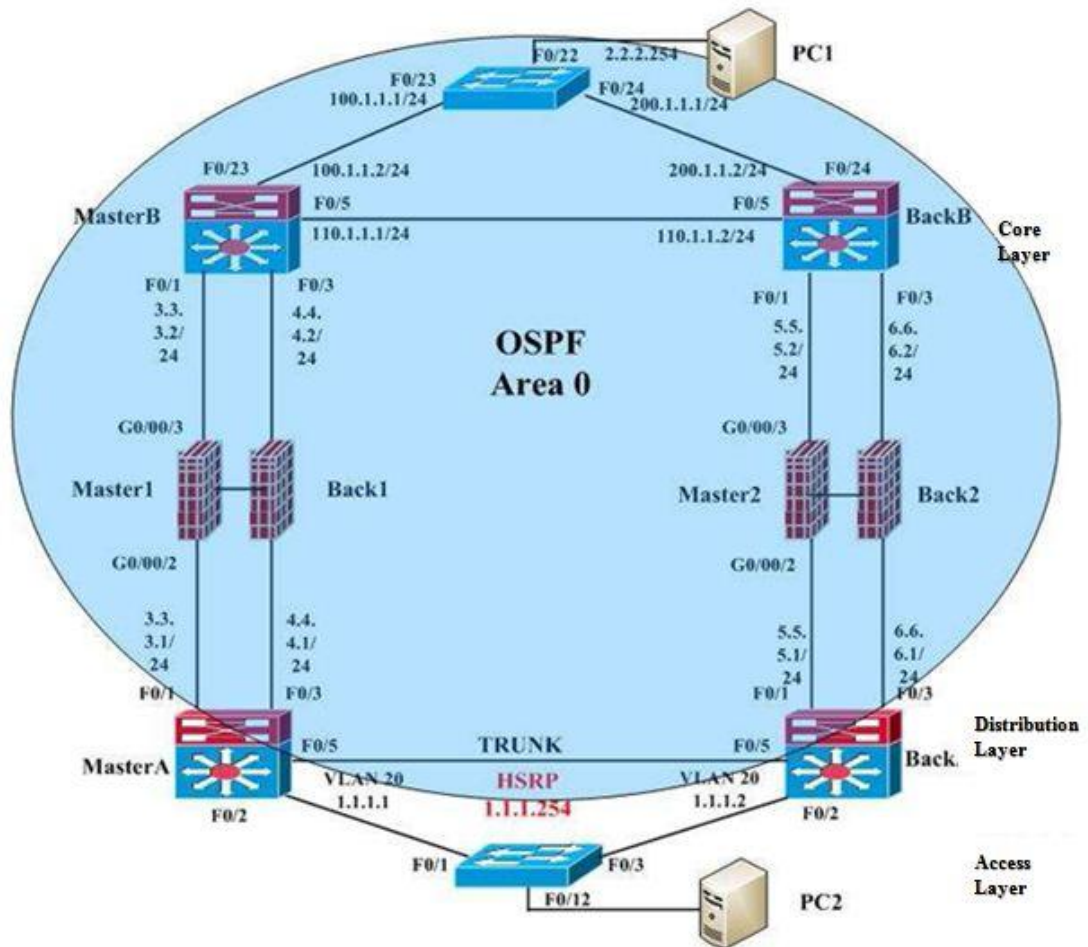


Figure 4.3. Routing topology diagram

The three-layered routing protocol is adopted from the distribution layer to the core layer, and from the core layer to the outlet. In the core layer device, the port and IP address of Master B core switch can be seen as below: All ports on the three-layers comply with the OSPF routing protocol.

F0/1: 3.3.3.2/24
 F0/3: 4.4.4.2/24
 F0/5: 110.1.1.1/24
 F0/23: 100.1.1.12/24

The port and IP address of Back B core switch are as below: All ports on the three-layers comply with the OSPF routing protocol.

F0/1: 5.5.5.2/24
F0/3: 6.6.6.2/24
F0/5: 110.1.1.2/24
F0/24: 200.1.1.12/24

The port and IP address of egress switch are:

F0/23: 100.1.1.1/24
F0/24: 200.1.1.1/24
F0/22: 2.2.2.254 (the Internet gateway that is used to test PC1)

On the distribution layer devices, the port and IP address of distribution layer switch Master A are as below:

F0/1: 3.3.3.1/24
F0/3: 4.4.4.1/24

The IP address of VLAN 20 is 1.1.1.1/24.

It is configured with the HSRP virtual router redundancy protocol, and its IP address is 1.1.1.254/24. Ports F0/2 and F0/5 are the TRUNK ports.

The port and the IP address of Switch Back A on the distribution layer are:

F0/1: 5.5.5.1/24
F0/3: 6.6.6.1/24

The IP address of VLAN 20 is 1.1.1.2/24.

It is configured with same HSRP configuration as Master A, and the virtual IP address is 1.1.1.254/24. On the devices of access layer, port F0/1 and F0/3 connected to switches are linked to two distribution switches. Port F0/12 is the upper port, and it is part of VLAN 20.

4.3 Normal network flow and direction diagram

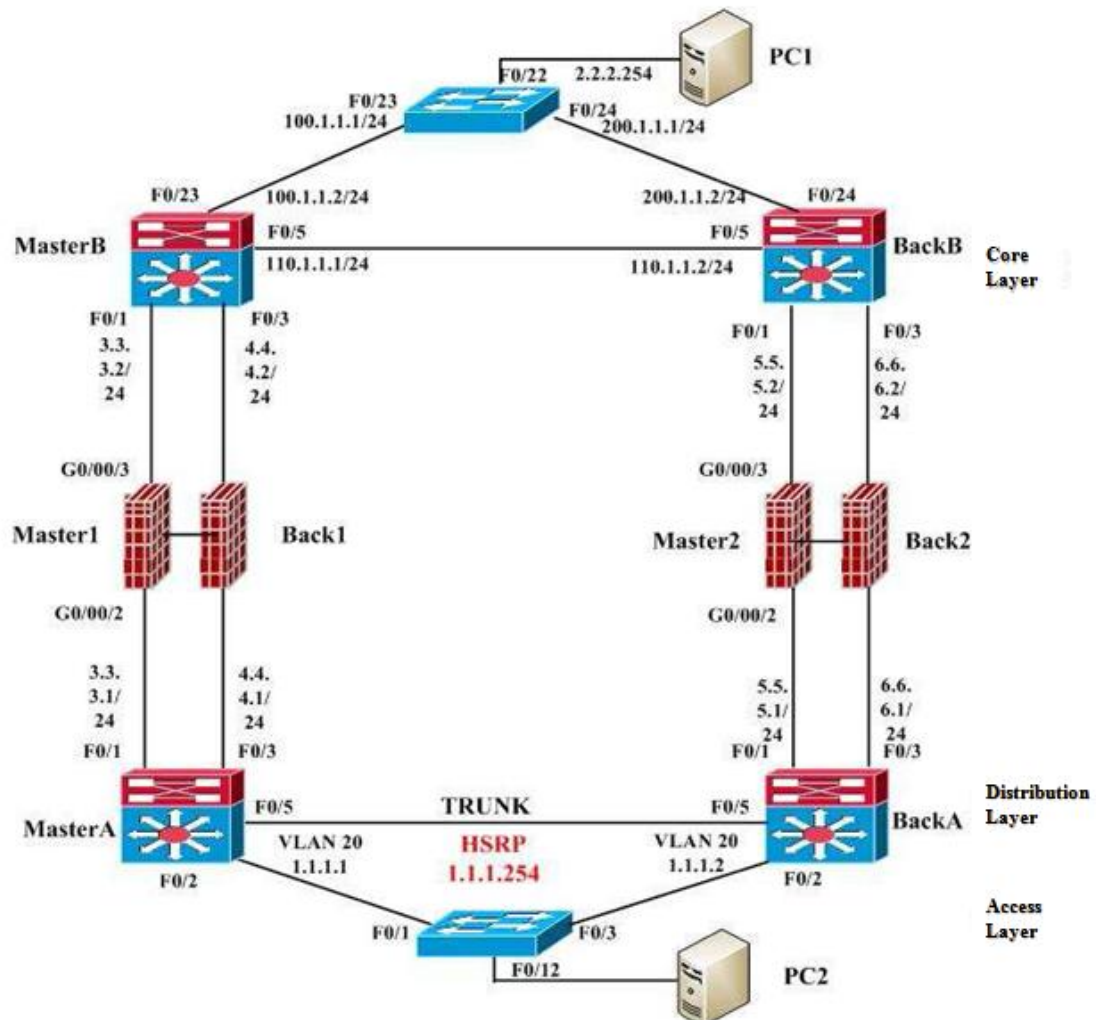
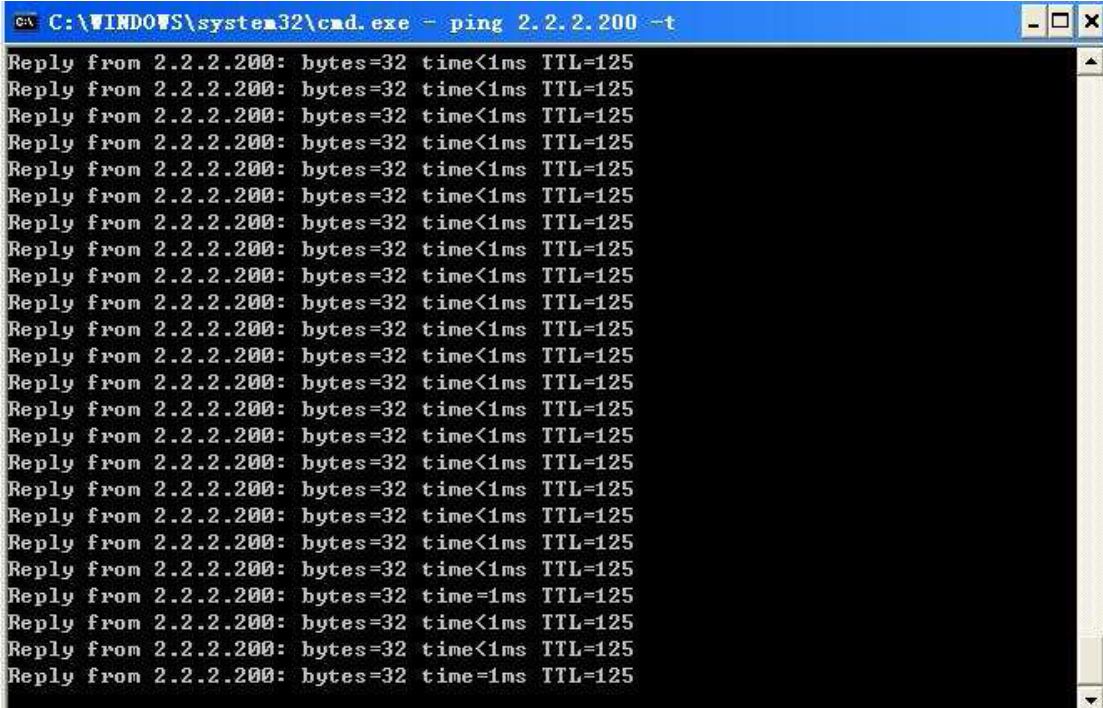


Figure 4.4. HSRP is enabled between Master A and Back A

As seen in Figure 4.4, HSRP is enabled among switches on the distribution layer. Switch Master A is configured with a high priority, i.e. under normal circumstances, switch Master A is the active switch and configured with preempt mode. Back A is configured with the default priority, i.e. under normal circumstances, Back A is the standby switch and is configured with preempt mode, as well. HA is enabled in the firewall. The normal data flow direction in the network is: PC2→Master A→Master1→Master B→PC1. The testing result can be seen from Figure 4.5 and Figure 4.6.



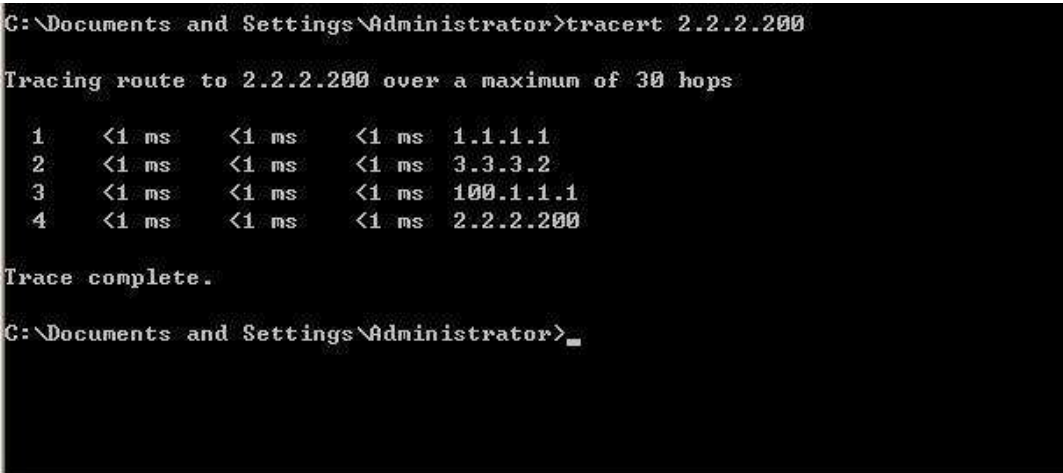
```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125

```

Figure 4.5. The results of normal network flow

As shown in Figure 4.5, PC2 can ping PC1, which proves that the network connection is normal and available at the moment.



```

C:\Documents and Settings\Administrator>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    3.3.3.2
  2  <1 ms    <1 ms    <1 ms    100.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

C:\Documents and Settings\Administrator>

```

Figure 4.6. The direction of the network flow under normal situation

Figure 4.6 shows that the network flow direction is: PC2→Master A→Master1→Master B→PC1.

4.4 Malfunction testing of firewall and switches

One word that we cannot avoid referring to is SPOF when speaking of high availability. SPOF, i.e., Single Point of Failure, is used in the situation when one component malfunction of the system leads to the failure of the whole system, and then this component is called SPOF of the system. We provide redundancy hardware device in the network to reduce SPOF probability, and its consequences on to the enterprises to the minimum. And that is the original intention of HA. ([9])

In this study, our goal is to test the high availability of the tested product performance, so the possible physical damage in the product hardware components, such as power supply failure, will not be taken into account.

4.4.1 Test 1: Malfunction in firewall Master 1

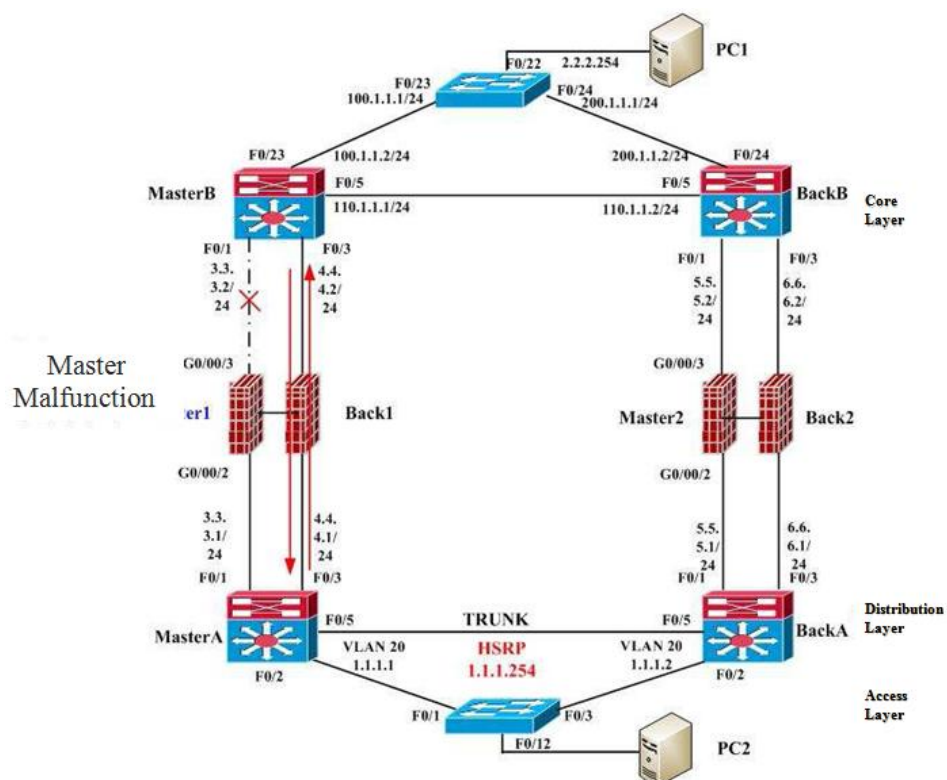
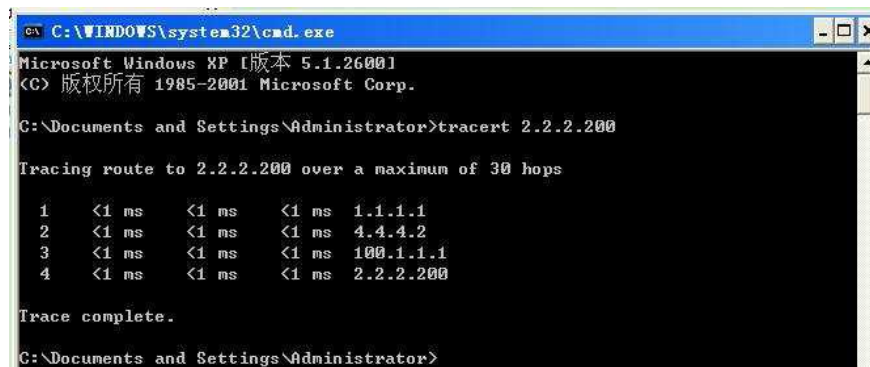


Figure 4.7. The situation 1 of malfunction in Master 1

Figure 4.7 shows the situation that when port G0/0/3 of Master 1 is down, the actual flow direction in the network will change. Master 1 is pre-set as them in firewall, and Back 1 as the backup firewall. So when the G0/0/3 port of Master1 is down, Back 1 will automatically shift to the main firewall through the monitoring of the heartbeat link. The network traffic direction should be: PC2→Master A→ Back 1→Master B→PC1. And the testing result could be seen in Figure 4.8 and Figure 4.9.

Note: In actual testing, there is a transient handoff among switches on the distribution layer.



```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms   1.1.1.1
  1  <1 ms    <1 ms    <1 ms   4.4.4.2
  2  <1 ms    <1 ms    <1 ms  100.1.1.1
  3  <1 ms    <1 ms    <1 ms  2.2.2.200

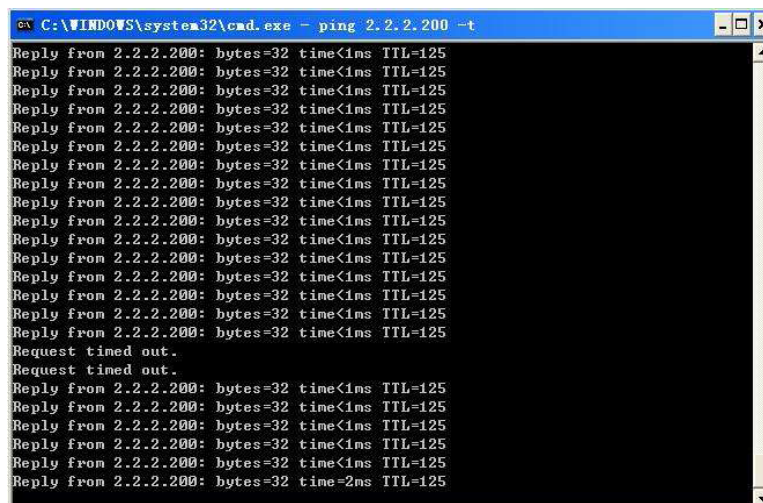
Trace complete.

C:\Documents and Settings\Administrator>

```

Figure 4.8. The net flow direction under Master 1 malfunction

As shown in Figure 4.8, the network flow direction after the network handoff is: PC2→Master A→ Back 1→Master B→PC1.



```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Request timed out.
Request timed out.
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=2ms TTL=125

```

Figure 4.9. The ping duration under Master 1 malfunction

Figure 4.9 shows that PC2 in the network continues to ping PC1's address. The handoff time from the figure above, time of ping duration, is about 1s, while the interruption interval is about 2s.

The configuration of Master1 and HA status can be found in the Appendix.

4.4.2 Test 2: malfunction in firewall Back 1

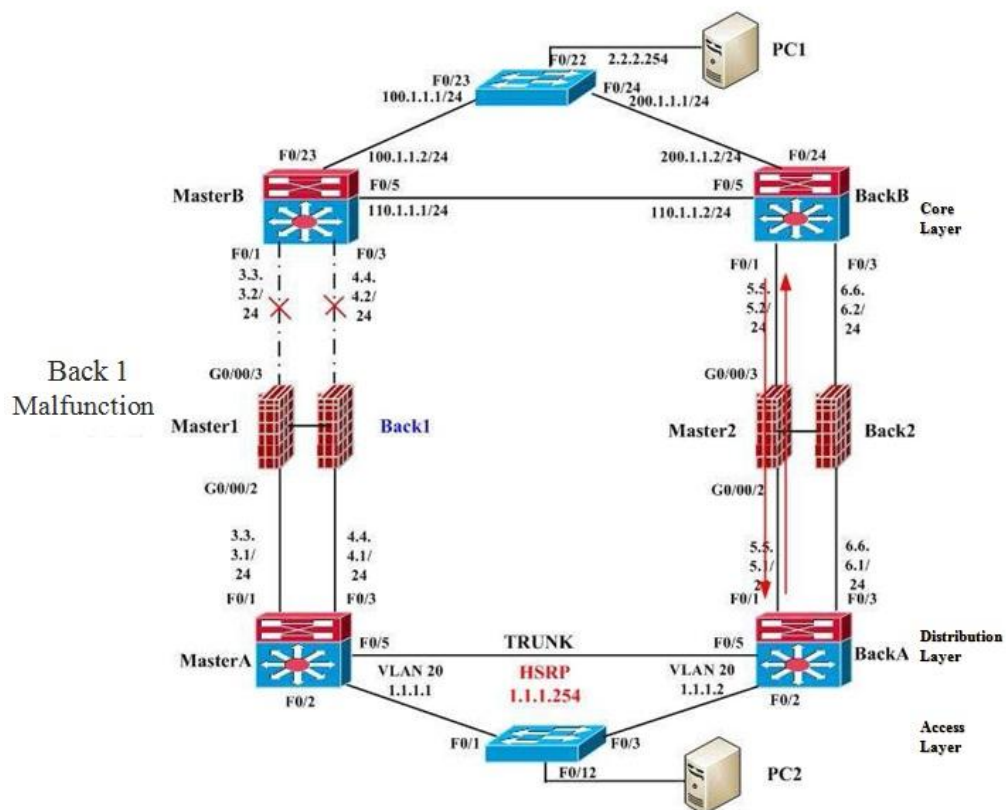
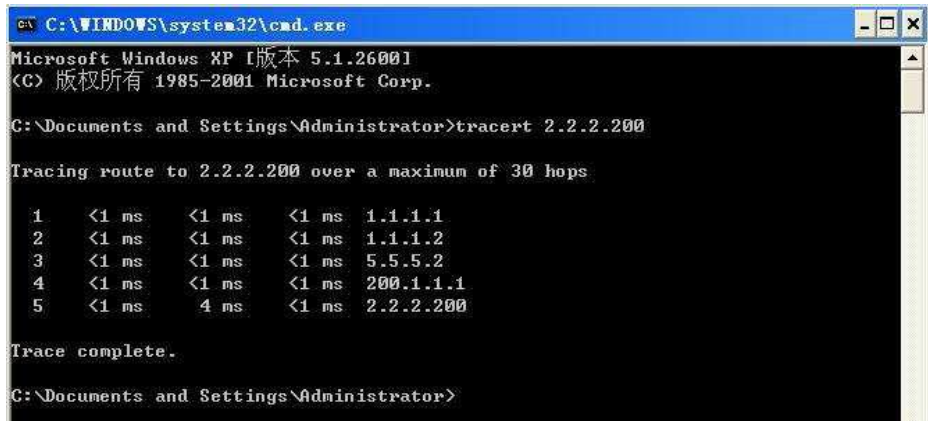


Figure 4.10. The situation 1 of malfunction in Back 1

When Master 1 is down, the network flow is shifted to Back 1. If there is something wrong with the G0/0/3 port of Back 1, the port will be down as seen in Figure 4.10. And at this time, the actual network flow direction changes. Both Master A and Back A on the distribution layer have been configured with HSRP, with Master A possessing a higher priority. Since malfunctions have occurred on both Master1 and Back 1, Back A switch becomes the active switch. The

network flow direction now is: PC2→Back A→ Master 2→ Back B→PC1. The testing result is shown in Figure 4.11 and Figure 4.12.



```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2  <1 ms    <1 ms    <1 ms    5.5.5.2
  3  <1 ms    <1 ms    <1 ms    200.1.1.1
  4  <1 ms    4 ms     <1 ms    2.2.2.200

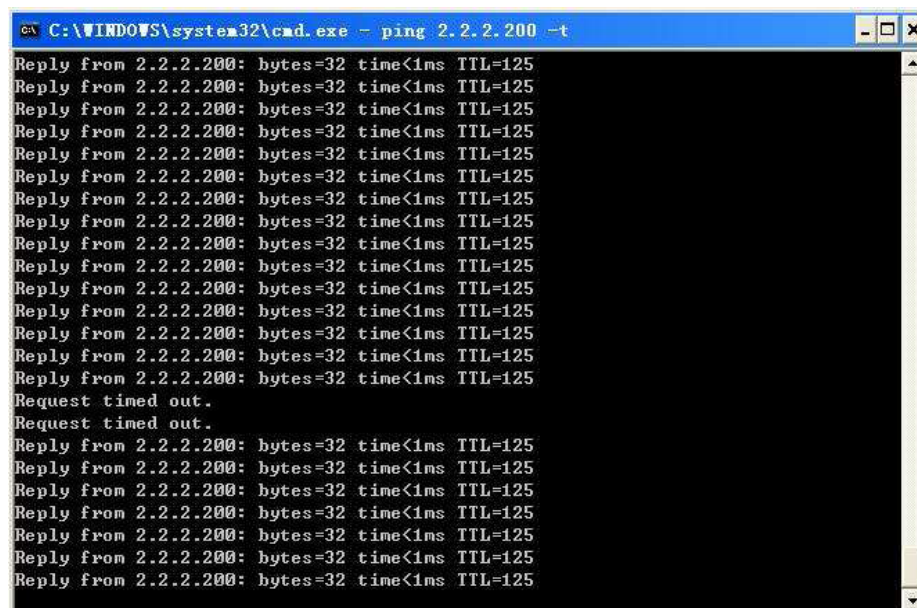
Trace complete.

C:\Documents and Settings\Administrator>

```

Figure 4.11. The net flow direction under Back 1 malfunction

As shown in Figure 4.11, the network flow direction after network handoff is: PC2→Back A→ Master 2→ Back B→PC1.



```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Request timed out.
Request timed out.
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125

```

Figure 4.12. The ping duration under Back 1 malfunction

The Figure 4.12 shows that PC2 in the network continues to ping PC1's address. We can see the handoff time, the time of ping duration is about 1s, while the interruption interval is about 2s. The configuration of the firewall of Master 2 and status testing can be found in the Appendix.

4.4.3 Test 3: malfunction in firewall Master 2

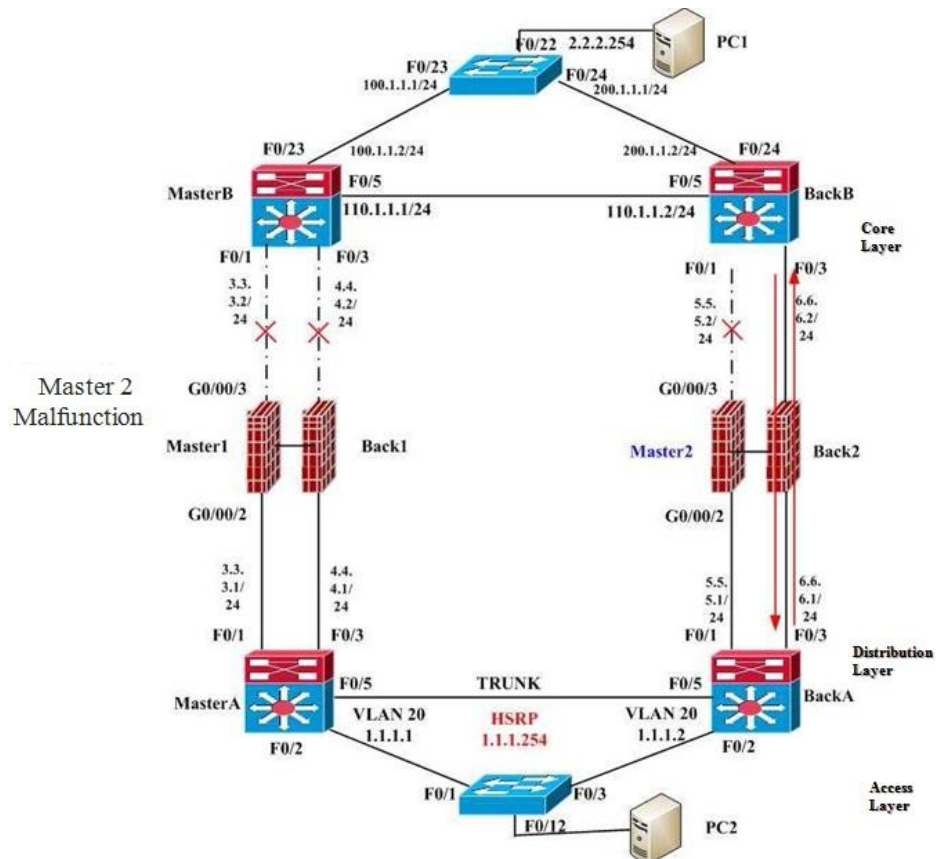


Figure 4.13. The situation of malfunction in Master 2

When the port is down due to the malfunction in port G0/0/3 of Master 2, like the situation in Figure 4.13, the actual flow direction in the network will change. Master 2 is pre-set as the main firewall, and Back 2 as the backup firewall. So when port G0/0/3 of Master 2 is down, Back 2 will automatically shift to the main firewall through the monitoring of the heartbeat link. The network traffic direction should be: PC2→Back A→ Back 2→Back B→PC1. The testing results are shown in the Figure 4.14 and Figure 4.15.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2  <1 ms    <1 ms    <1 ms    6.6.6.2
  3  <1 ms    <1 ms    <1 ms    200.1.1.1
  4  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

C:\Documents and Settings\Administrator>

```

Figure 4.14. The net flow direction under Master 2 malfunction

As shown in Figure 4.14, the network flow direction after network handoff is: PC2→Back A→ Back 2→ Back B→PC1.

```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=3ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Request timed out.
Request timed out.
Request timed out.
Reply from 1.1.1.1: Destination host unreachable.
Reply from 1.1.1.1: Destination host unreachable.
Reply from 1.1.1.1: Destination host unreachable.
Reply from 1.1.1.1: Destination host unreachable.
Reply from 1.1.1.1: Destination host unreachable.
Reply from 1.1.1.1: Destination host unreachable.
Reply from 1.1.1.1: Destination host unreachable.
Reply from 1.1.1.1: Destination host unreachable.
Reply from 1.1.1.1: Destination host unreachable.
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=4ms TTL=125

```

Figure 4.15. The ping duration under Master 2 malfunction

Figure 4.15 shows that PC2 in the network continues to ping PC1's address. We can see the handoff time, the time of ping duration is about 1s, while the interruption interval lasts about 12s.

The configuration of the firewall of Back 2 and status testing can be found in the Appendix.

4.4.4 Test 4: malfunction in firewall Back 2

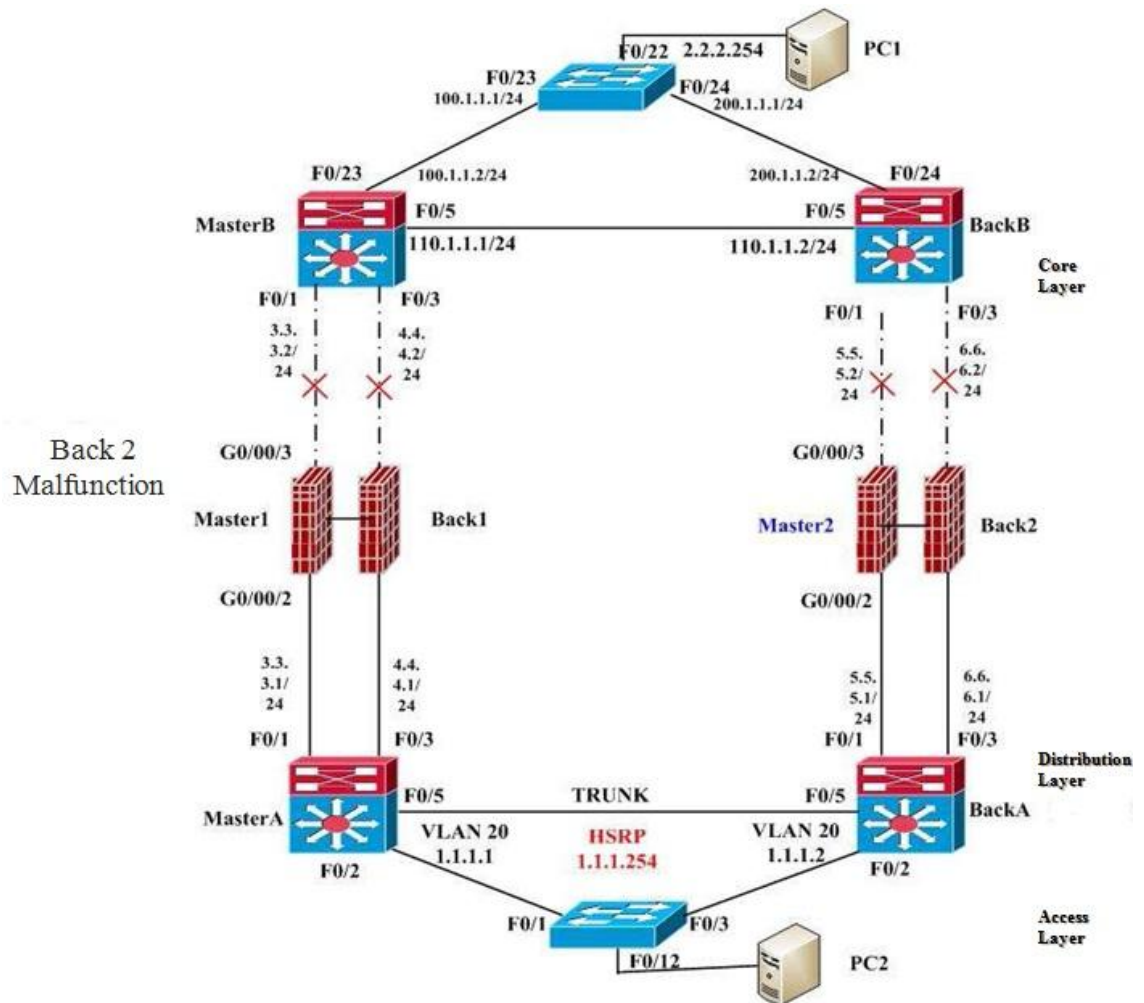


Figure 4.16. The situation of malfunction in Back 2

As shown in Figure 4.16, when port F0/3 of the firewall Back 2 in the network is down, the network is interrupted.

4.4.5 Test 5: malfunction 1 in switch Master A

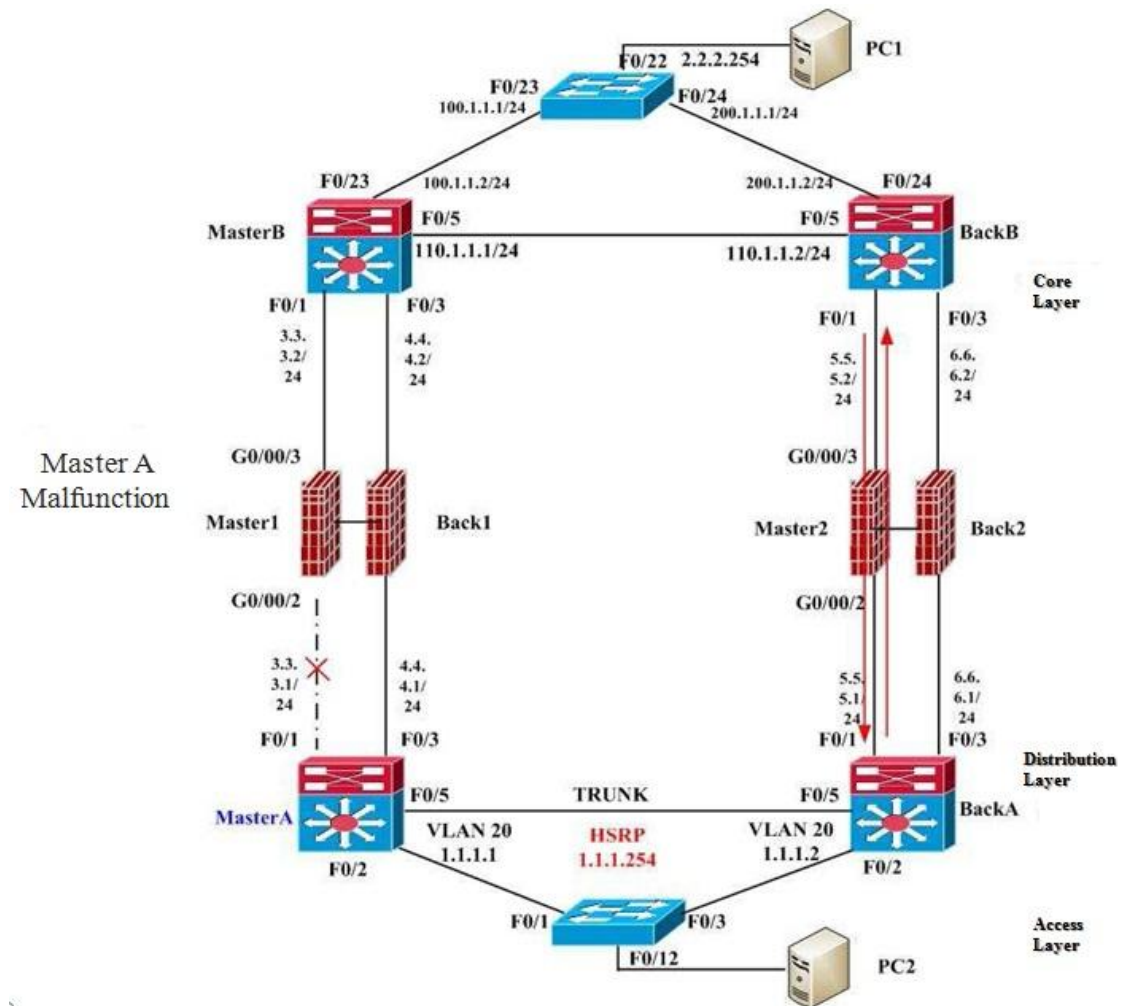


Figure 4.17. The situation 1 of malfunction in Master A

As shown in Figure 4.17, the switches on the distribution layer are configured with HSRP. They monitor their upper port F0/1 and F0/3. Master A with a high priority becomes the active switch while Back A with a lower priority becomes the backup switch. For VLAN 20, when the monitoring port F0/1 of Master A is down, the Back A switch on the distribution layer becomes the active switch. And the network traffic direction should be: PC2→Back A→ Master 2→ Back B→PC1. The testing results are shown in Figure 4.18 and Figure 4.19.


```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    1.1.1.2
  1  <1 ms    <1 ms    <1 ms    5.5.5.2
  2  <1 ms    <1 ms    <1 ms    200.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

C:\Documents and Settings\Administrator>

```

Figure 4.18. The net flow direction under Master A malfunction 1

As shown in Figure 4.18, the network flow direction after network handoff is: PC2→Back A→ Master 2→ Back B→PC1.

```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t

Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Request timed out.
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125

```

Figure 4.19. The ping duration under Master A malfunction 1

Figure 4.19 shows that PC2 in the network continues to ping PC1's address. We can see the handoff time, the time of ping duration is about 1s, while the interruption interval takes up about 1s.

The configuration of Master A on the distribution layer can be found in the Appendix.

4.4.6 Test 6: malfunction 2 in switch Master A

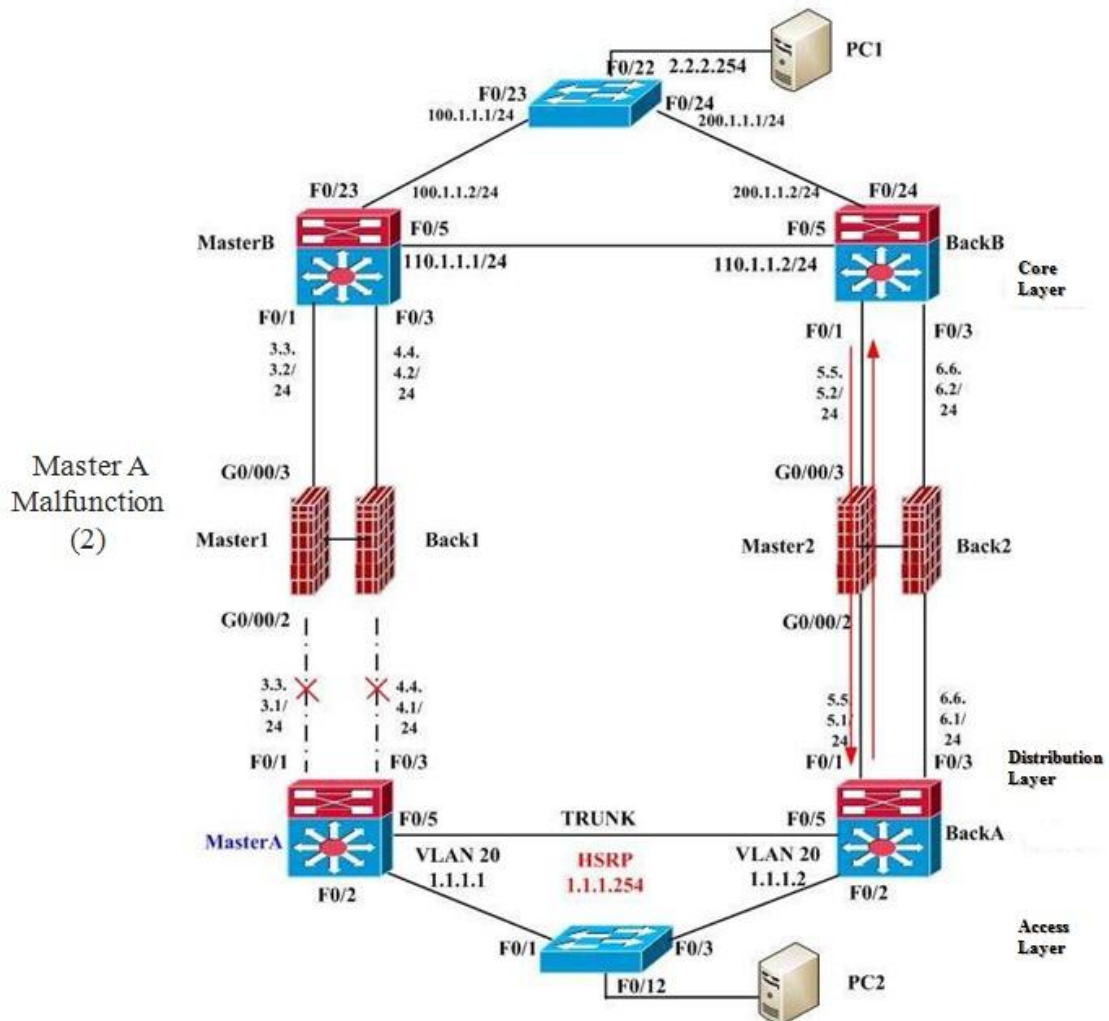


Figure 4.20. The situation 2 of malfunction in switch Master A

As seen in Figure 4.20, the switches on the distribution layer are configured with HSRP. They monitor their upper port F0/1 and F0/3. Master A with a high priority becomes the active switch while Back A with a lower priority becomes the backup switch. For VLAN 20, when the monitoring port F0/3 of Master A is down, the Back A switch on the distribution layer becomes the active switch. The network traffic direction should be: PC2 → Back A → Master 2 → Back B → PC1. The testing results are as shown in Figure 4.21 and Figure 4.22.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.2
  1  2 ms     <1 ms    <1 ms    5.5.5.2
  2  <1 ms    <1 ms    <1 ms    200.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

C:\Documents and Settings\Administrator>

```

Figure 4.21. The net flow direction under Master A malfunction 2

As shown in Figure 4.21, the network flow direction after network handoff is: PC2→Back A→ Master 2→ Back B→PC1.

```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=5ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=2ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125

```

Figure 4.22. The ping duration under Master A malfunction 2

Figure 4.22 shows that PC2 in the network pings PC1's address continuously. The configuration of Master A and status testing result can be found in the Appendix.

4.4.7 Test 7: malfunction 1 in switch Back A

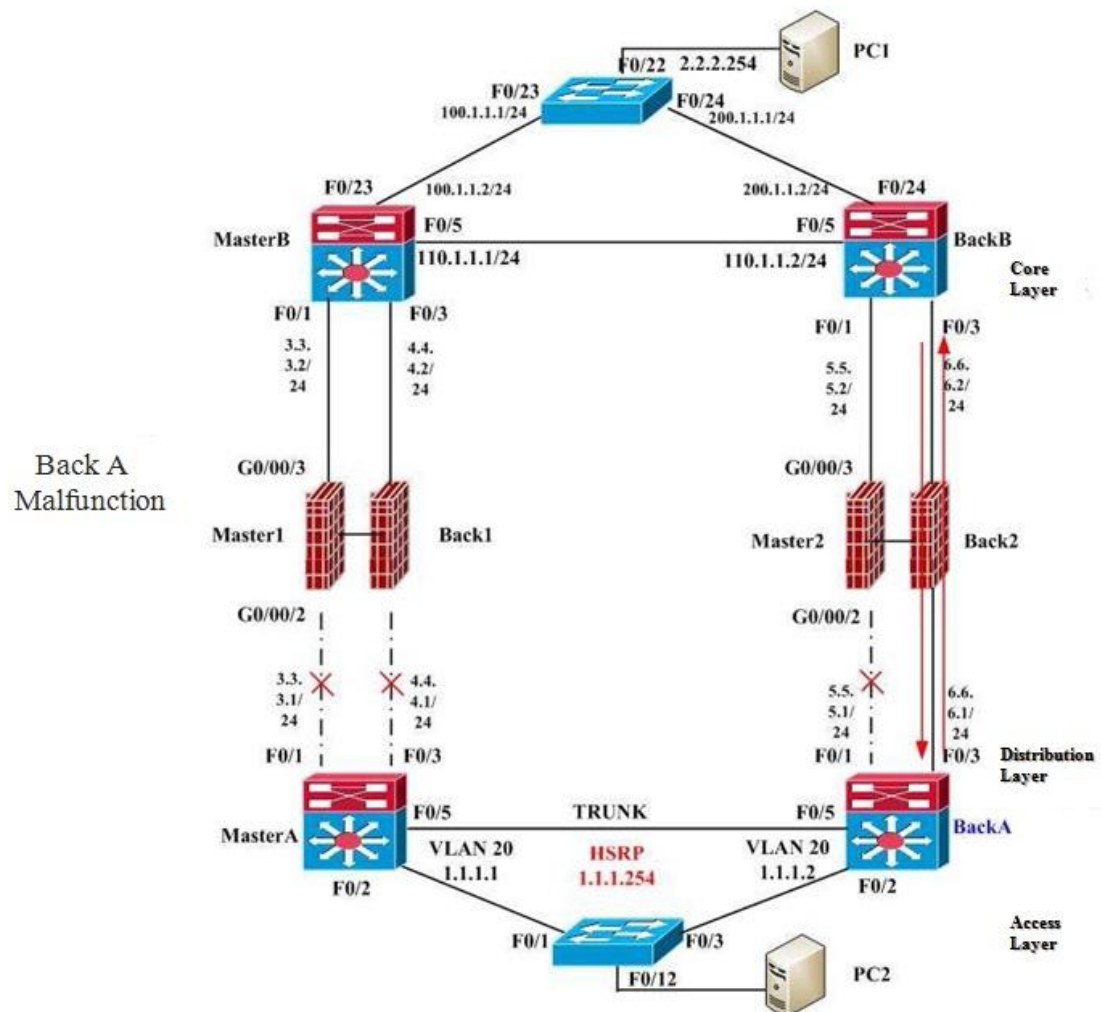


Figure 4.23. The situation 1 of malfunction in switch Back A

As shown in Figure 4.23, when the switch Back A on the distribution layer is the active switch, if malfunction occurs in port F0/1, the port will be down. Master 2 is pre-set as the main firewall, while Back 2 is the backup firewall. When port F0/1 of Back A is down, Back 2 will shift to active firewall automatically through the monitoring of the heartbeat link. The network traffic direction should be: PC2→Back A→Back 2→Back B→PC1. The testing results are shown in Figure 4.24 and Figure 4.25.

```

C:\Documents and Settings\Administrator>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.2
  1  <1 ms    <1 ms    <1 ms    6.6.6.2
  2  1 ms     <1 ms    <1 ms    200.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

C:\Documents and Settings\Administrator>

```

Figure 4.24. The net flow direction under Back A malfunction 1

As shown in Figure 4.24, the network flow direction after network handoff is: PC2→Back A→Back 2→Back B→PC1.

```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t

Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Request timed out.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Reply from 1.1.1.2: Destination host unreachable.
Request timed out.
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=3ms TTL=125

```

Figure 4.25. The ping duration under Back A malfunction 1

PC2 in the network continues to ping PC1's address. We can see the handoff time from Figure 4.25, the time of ping duration 1s, while the interruption interval lasts about 14s.

The configuration of the firewall of Back 2 and the status testing result can be found in the Appendix.

4.4.8 Test 8: Malfunction 2 in switch Back A

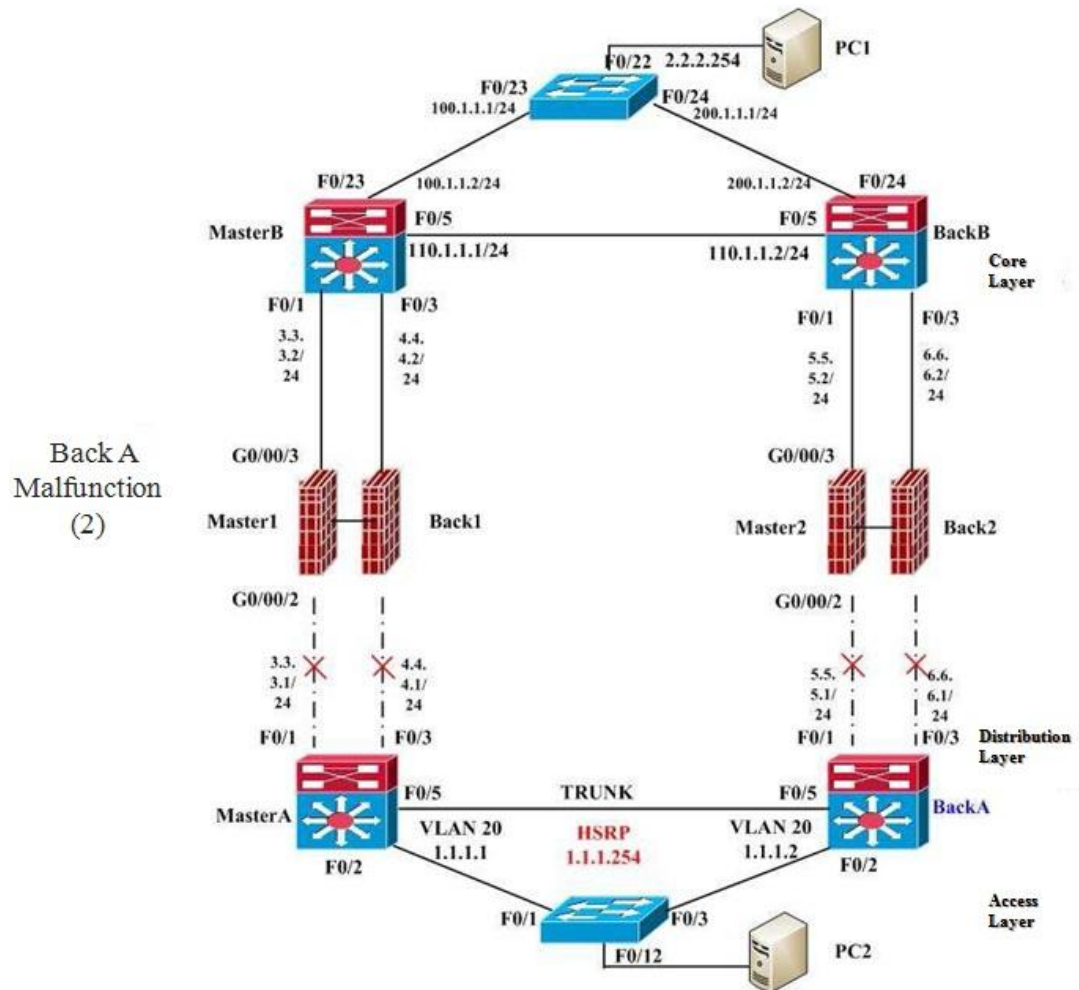


Figure 4.26. The situation 2 of malfunction in switch Back A

When port F0/3 of switch Back A in the network is down, the network is interrupted as shown in Figure 4.26.

4.5 Malfunction recovery and preempt

4.5.1 Test 9: Master 1 recovery and preempt

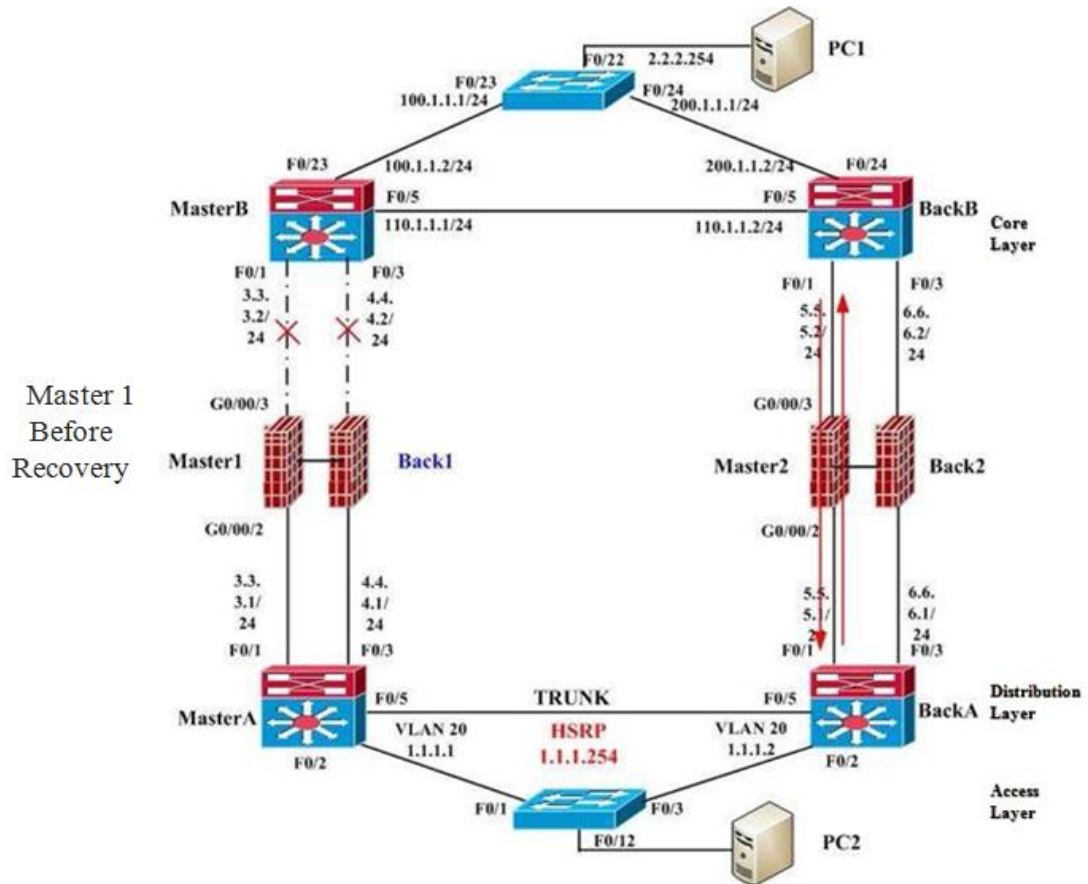


Figure 4.27. The situation of Master 1 before recovery

Originally when port G0/0/3 within the firewall of Master1 and Back 1 is down as seen in Figure 4.27, the network flow direction is:PC2→Back A→Master 2→Back B→PC1. The testing result is as seen in Figure 4.28.

```
D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms  <1 ms  <1 ms  1.1.1.1
  2  <1 ms  <1 ms  <1 ms  1.1.1.2
  3  <1 ms  <1 ms  <1 ms  5.5.5.2
  4   1 ms  <1 ms  <1 ms  200.1.1.1
  5  <1 ms  <1 ms  <1 ms  2.2.2.200

Trace complete.
```

Figure 4.28. The net flow direction of Master 1 before recovery

Now if the G0/0/3 port of Master 1 becomes active again as in Figure 4.29, the network flow direction will change to: PC2→Master A→Master 1→Master B→PC1. And the testing result can be seen in Figure 4.30.

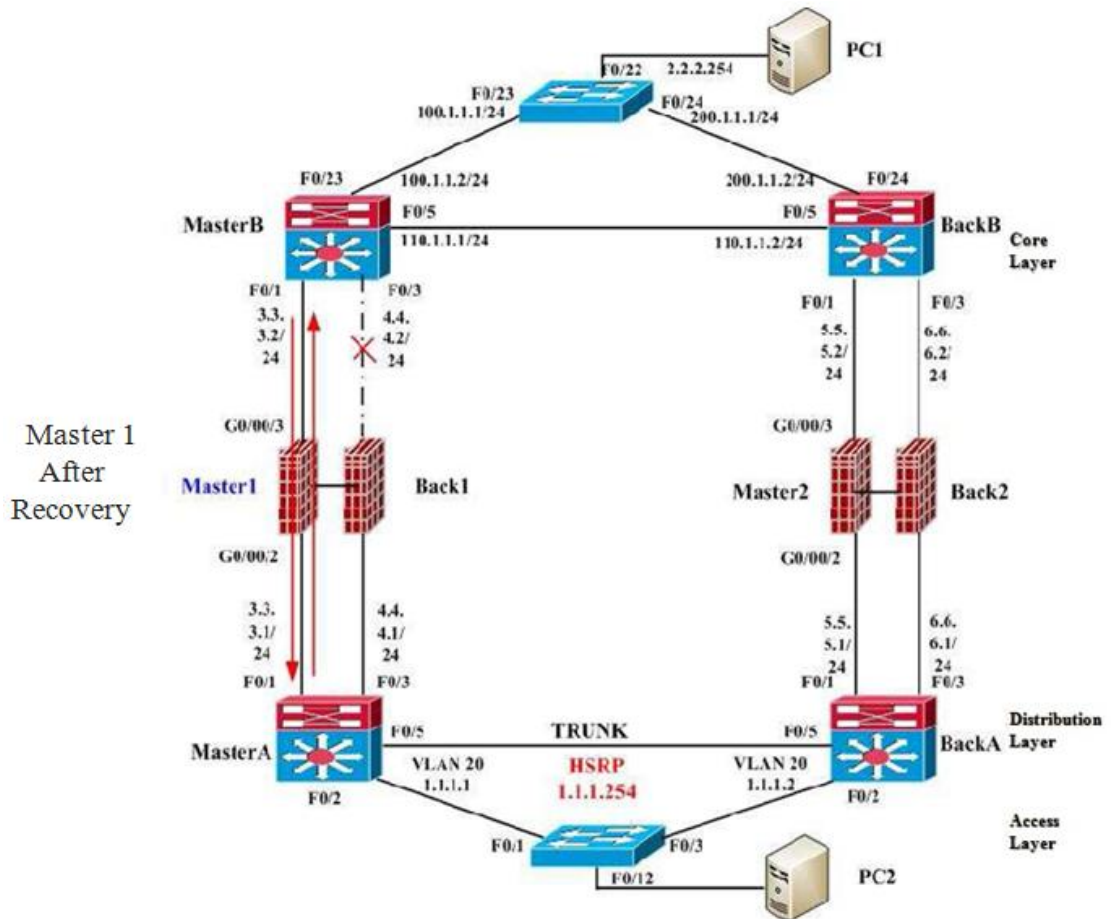


Figure 4.29. The situation of Master 1 after recovery

```
D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    3.3.3.2
  2  <1 ms    <1 ms    <1 ms    100.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.
```

Figure 4.30. The net flow direction of Master 1 after recovery

As shown in Figure 4.30, the network flow direction after the network handoff is: PC2→Master A→Master 1→Master B→PC1.


```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=4ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125

```

Figure 4.31. The ping duration under Master 1 after recovery

Figure 4.31 shows that PC2 in the network continues to ping PC1's address, without interruption. The flow direction shift information can be seen in Figure 4.32.

```

D:\>tracert 2.2.2.200
Tracing route to 2.2.2.200 over a maximum of 30 hops
  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2  <1 ms    <1 ms    <1 ms    5.5.5.2
  3  1 ms     <1 ms    <1 ms    200.1.1.1
  4  <1 ms    <1 ms    <1 ms    2.2.2.200
Trace complete.

D:\>tracert 2.2.2.200
Tracing route to 2.2.2.200 over a maximum of 30 hops
  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    3.3.3.2
  2  <1 ms    <1 ms    <1 ms    100.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200
Trace complete.

```

Figure 4.32. The flow direction shift under Master 1 after recovery

4.5.2 Test 10: Back 1 recovery and preempt

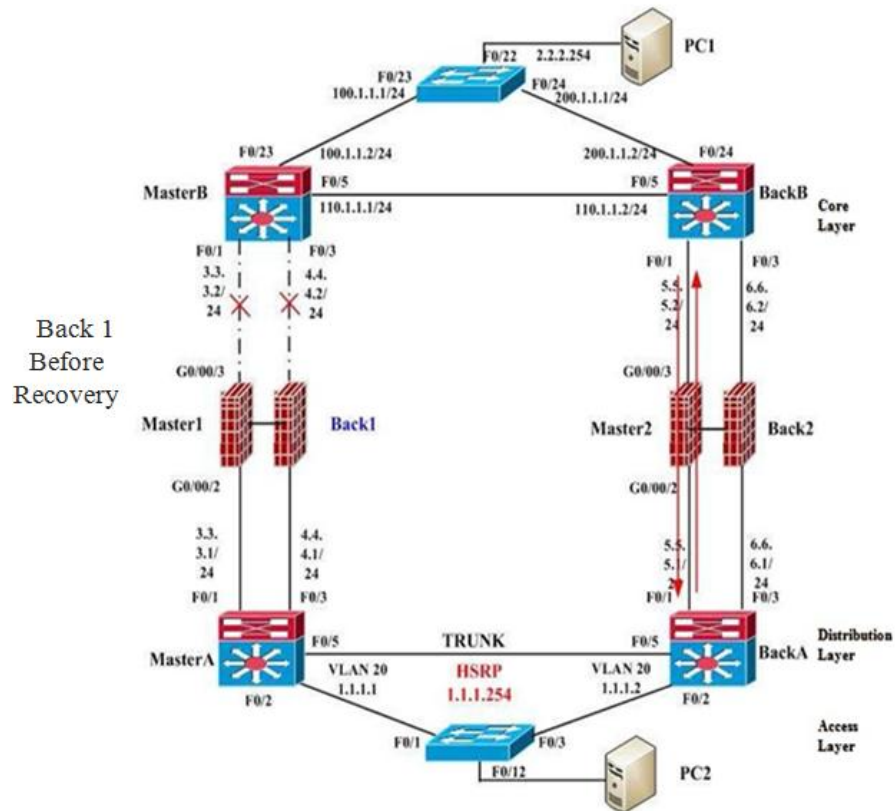


Figure 4.33. The situation of Back 1 before recovery

As shown in Figure 4.33, when port G0/0/3 within the firewall of Master1 and Back 1 are down, the network flow direction should be: PC2→Back A→Master 2→Back B→PC1. The testing result is shown in Figure 4.34.

```
D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2  <1 ms    <1 ms    <1 ms    5.5.5.2
  3  1 ms     <1 ms    <1 ms    200.1.1.1
  4  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.
```

Figure 4.34. The net flow direction of Back 1 before recovery

As shown in Figure 4.34, now when the G0/0/3 port of Back 1 is up, the network flow direction changes to: PC2→Master A→Back 1→Master B→PC1. The testing result is seen in Figure 4.36.

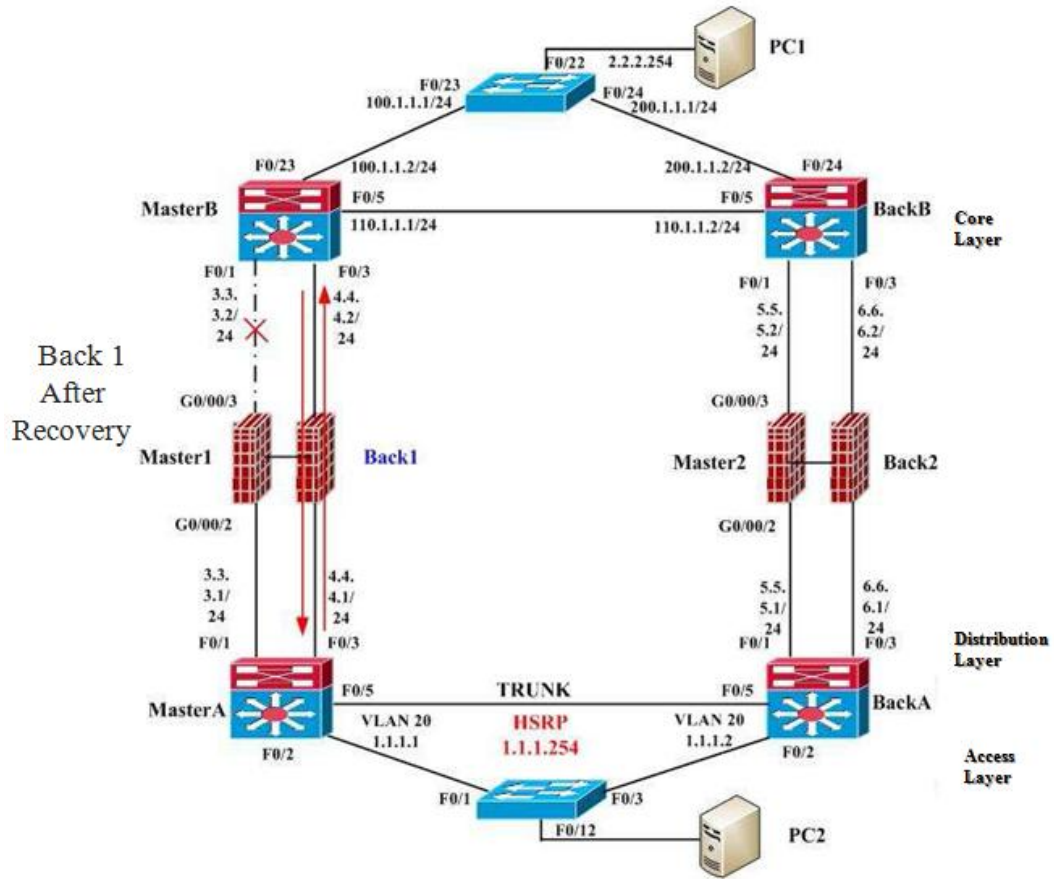


Figure 4.35. The situation of Back 1 after recovery

```
D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms  <1 ms  <1 ms  1.1.1.1
  2  <1 ms  <1 ms  <1 ms  4.4.4.2
  3   1 ms  <1 ms  <1 ms  100.1.1.1
  4  <1 ms  <1 ms  <1 ms  2.2.2.200

Trace complete.
```

Figure 4.36. The net flow direction of Back 1 after recovery

In Figure 4.36, we can see that the network flow direction after network handoff is:PC2→Master A→Back 1→Master B→PC1.

```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=3ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125

```

Figure 4.37. The ping duration under Back 1 after recovery

PC2 in the network continues to ping PC1's address, as shown in Figure 4.37. And the flow direction shift result can be seen in Figure 4.38.

```

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2  <1 ms    <1 ms    <1 ms    5.5.5.2
  3  <1 ms    <1 ms    <1 ms    200.1.1.1
  4  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    4.4.4.2
  2  <1 ms    <1 ms    <1 ms    100.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

```

Figure 4.38. The flow direction shift under Back 1 after recovery

4.5.3 Test 11: Master 1 recovery and preempt 2

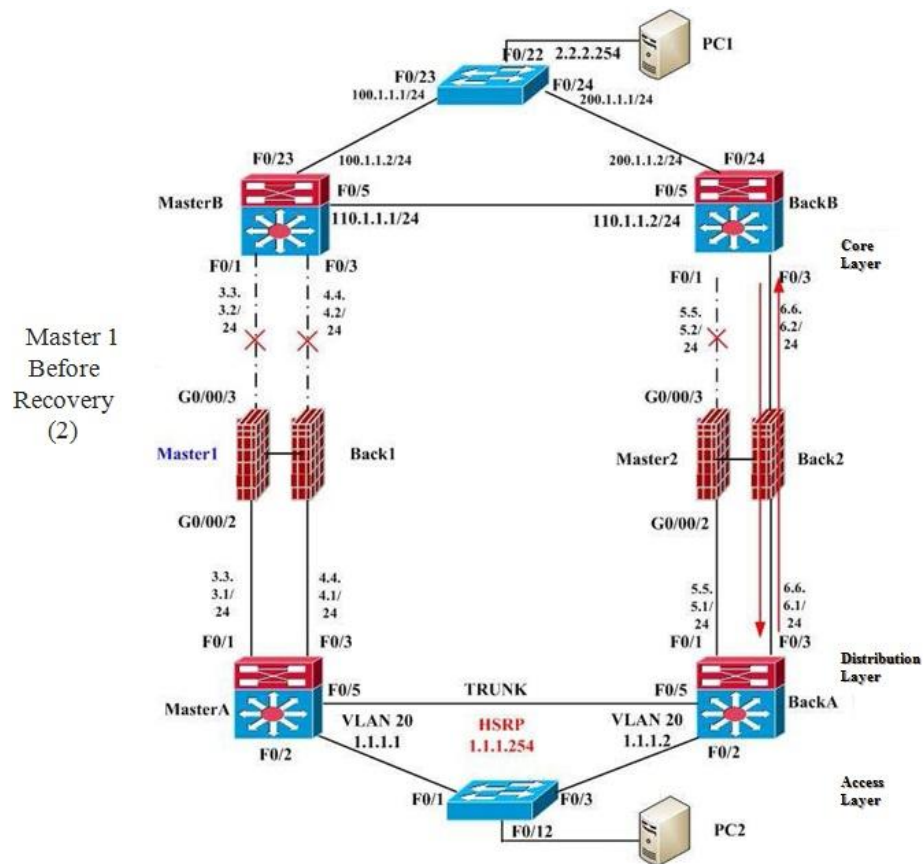


Figure 4.39. The situation 2 of Master 1 before recovery

As shown in Figure 4.39, if port G0/0/3 of Master1 and Back 1 are both down, and also port G0/0/3 of Master 2 is down, the network flow direction should be: PC2→Back A→Back 2→Back B→PC1. The testing result is as shown in Figure 4.40.

```
D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2   1 ms    <1 ms    <1 ms    6.6.6.2
  3   1 ms     4 ms    <1 ms    200.1.1.1
  4   1 ms    <1 ms    <1 ms    2.2.2.200
```

Figure 4.40. The net flow direction under the situation 2 of Master 1 before recovery

As shown in Figure 4.41, now if the G0/0/3 port of Master 1 becomes active again, the network flow direction changes to: PC2→Master A→Master 1→Master B→PC1. The testing result is shown in Figure 4.42.

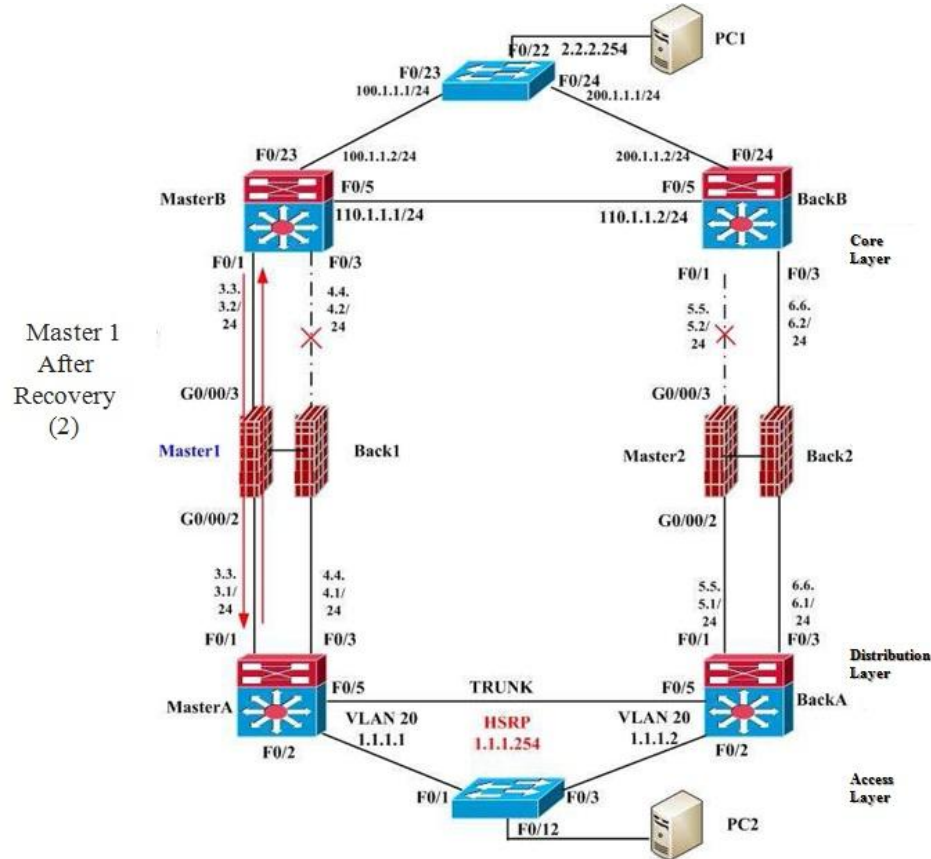


Figure 4.41. The situation 2 of Master 1 after recovery

```
D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    3.3.3.2
  2  <1 ms    <1 ms    <1 ms    100.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.
```

Figure 4.42. The net flow direction in the situation 2 of Master 1 after recovery

As shown in Figure 4.42, we can see that the network flow direction after network handoff is: PC2→Master A→Master 1→Master B→PC1.

```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=4ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125

```

Figure 4.43. The ping duration under the situation 2 of Master 1 after recovery

PC2 in the network continues to ping PC1's address, as shown in Figure 4.43.

And the flow direction shift information is shown in Figure 4.44.

```

D:\>tracert 2.2.2.200
Tracing route to 2.2.2.200 over a maximum of 30 hops
  1  <1 ms  <1 ms  <1 ms  1.1.1.1
  2  <1 ms  <1 ms  <1 ms  1.1.1.2
  3  <1 ms  <1 ms  <1 ms  6.6.6.2
  4   7 ms   1 ms  <1 ms  200.1.1.1
  5  <1 ms  <1 ms  <1 ms  2.2.2.200
Trace complete.

D:\>tracert 2.2.2.200
Tracing route to 2.2.2.200 over a maximum of 30 hops
  1  <1 ms  <1 ms  <1 ms  1.1.1.1
  2  <1 ms  <1 ms  <1 ms  3.3.3.2
  3   1 ms  <1 ms  <1 ms  100.1.1.1
  4  <1 ms  <1 ms  <1 ms  2.2.2.200
Trace complete.

```

Figure 4.44. The flow direction shift in situation 2 of Master 1 after recovery

4.5.4 Test 12: Back 1 recovery and preempt 2

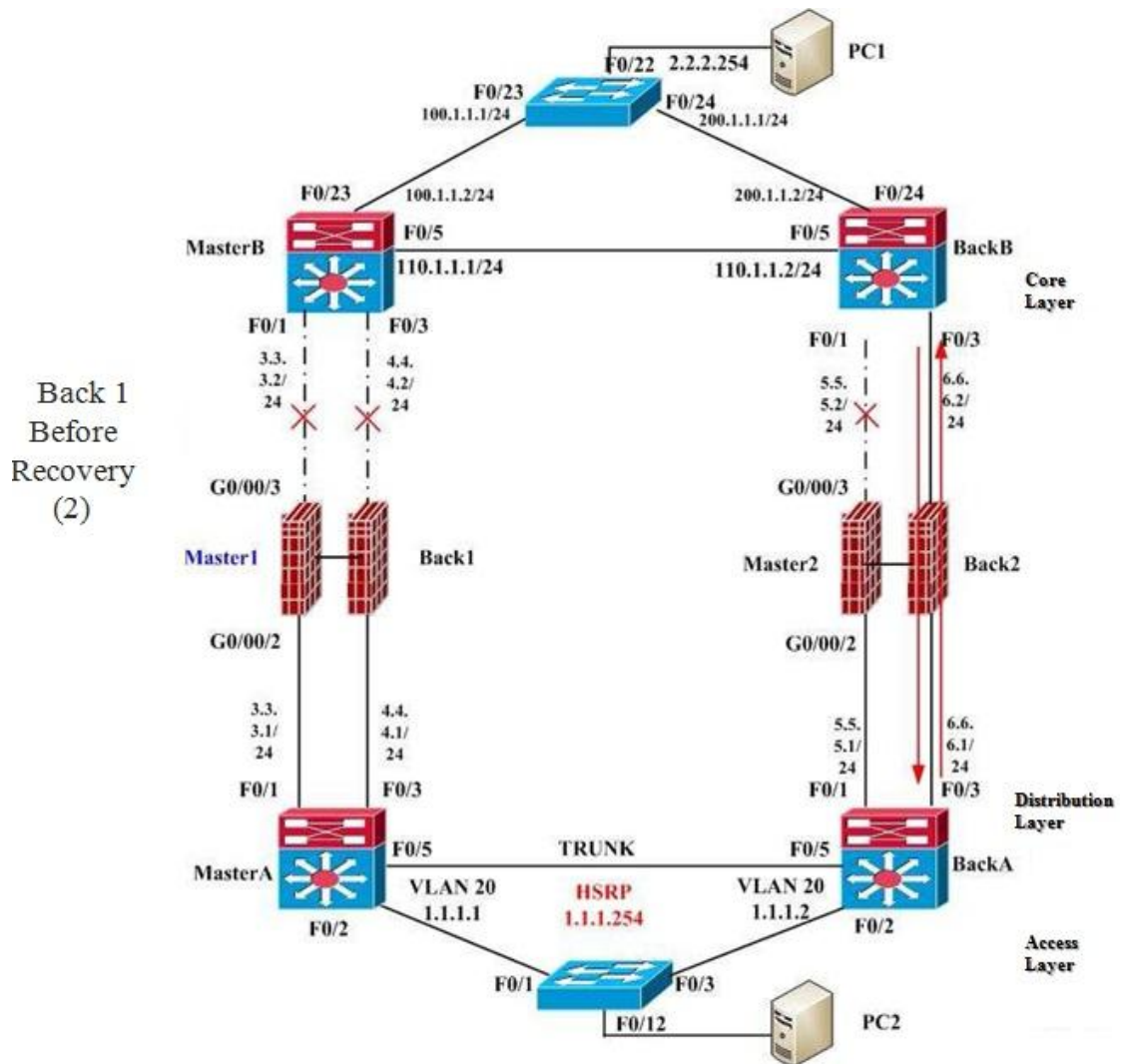


Figure 4.45. The situation 2 of Back 1 before recovery

As shown in Figure 4.45, if port G0/0/3 of Master1 and Back 1 are both down and also port G0/0/3 of Master 2 is down, the network flow direction should be: PC2→Back A→Back 2→Back B→PC1. The testing result is shown in Figure 4.46.


```

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    1.1.1.1
  2  <1 ms    <1 ms    <1 ms    1.1.1.2
  3   1 ms    <1 ms    <1 ms    6.6.6.2
  4   1 ms     4 ms    <1 ms    200.1.1.1
  5   1 ms    <1 ms    <1 ms    2.2.2.200
    
```

Figure 4.46. The net flow direction in situation 2 of Back 1 before recovery

As shown in Figure 4.47, now if port G0/0/3 of Back 1 becomes active again, the network flow direction should change to: PC2→Master A→Back 1→Master B→PC1. The testing result can be seen in Figure 4.48.

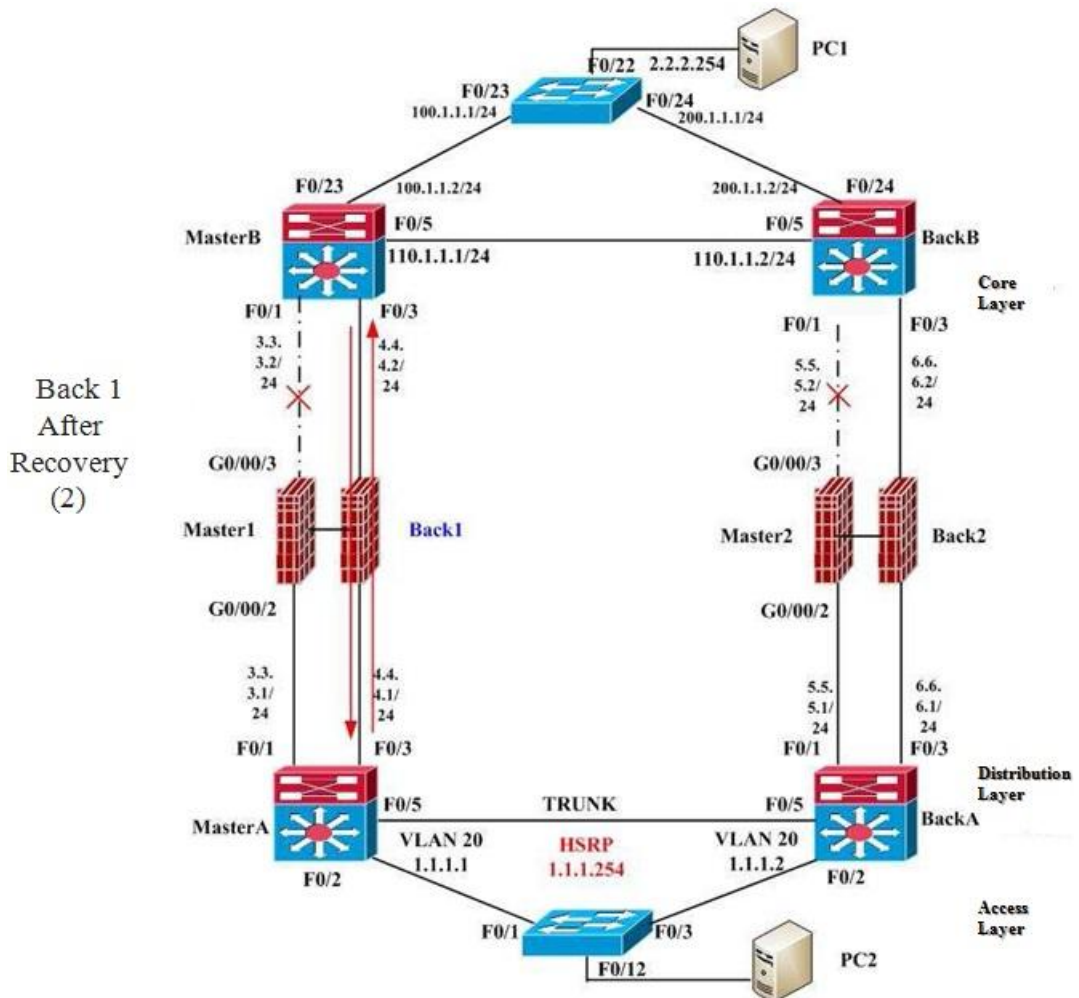


Figure 4.47. The situation 2 of Back 1 after recovery

```

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    1.1.1.1
  2  <1 ms    <1 ms    <1 ms    1.1.1.2
  3  <1 ms    <1 ms    <1 ms    6.6.6.2
  4   1 ms    <1 ms    <1 ms    200.1.1.1
  5  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

```

Figure 4.48. The net flow direction in situation 2 of Back 1 after recovery

As shown in Figure 4.48, we can see that the network flow direction after network handoff is: PC2→Master A→Back 1→Master B→PC1.

```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125

```

Figure 4.49. The ping duration in situation 2 of Back 1 after recovery

PC2 in the network continues to ping PC1's address, as shown in Figure 4.49. And the flow direction shift information is shown in Figure 4.50.

```

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    1.1.1.1
  2  <1 ms    <1 ms    <1 ms    1.1.1.2
  3  <1 ms    <1 ms    <1 ms    6.6.6.2
  4   4 ms    1 ms     <1 ms    200.1.1.1
  5  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    1.1.1.1
  2  <1 ms    <1 ms    <1 ms    4.4.4.2
  3   1 ms    <1 ms    <1 ms    100.1.1.1
  4  <1 ms    <1 ms    <1 ms    2.2.2.200

```

Figure 4.50. The flow direction shift in situation 2 of Back 1 after recovery

4.5.5 Test 13: Situation 1 of Master A recovery and preempt

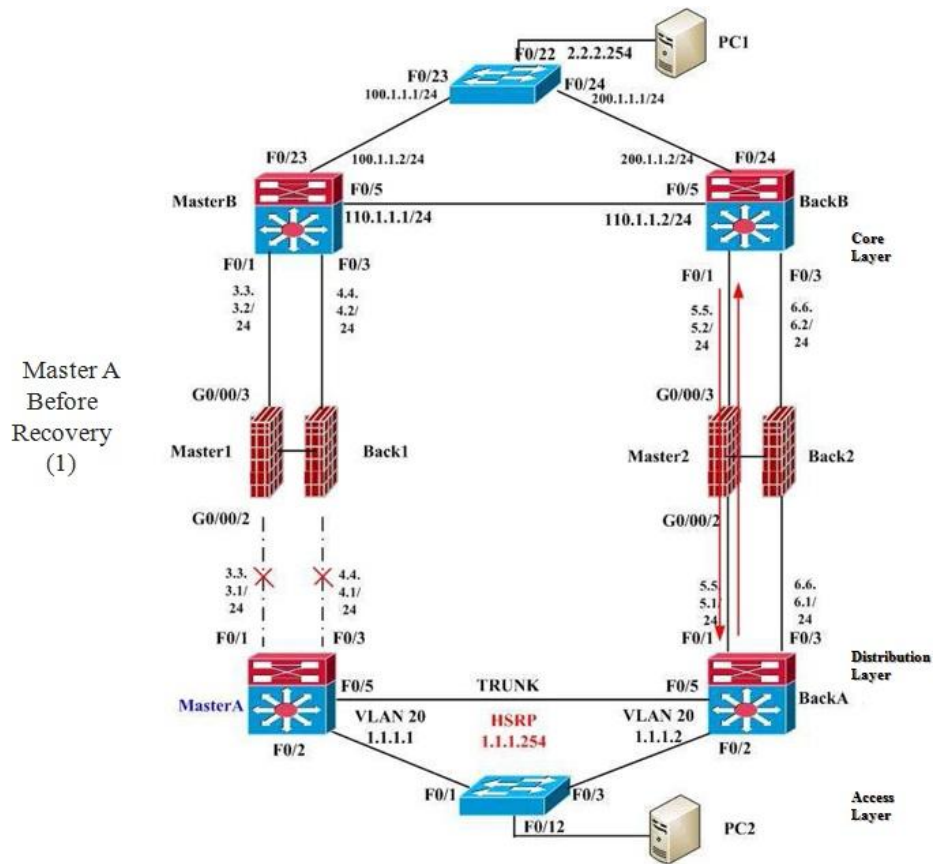


Figure 4.51. The situation 1 of switch Master A before recovery

In Figure 4.51, originally when port F0/3 and F0/1 of Master A in the network are down, the network flow direction is: PC2→Back A→Master 2→Back B→PC1 as shown in Figure 4.52.

```
D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2  <1 ms    <1 ms    <1 ms    5.5.5.2
  3  1 ms     <1 ms    <1 ms    200.1.1.1
  4  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.
```

Figure 4.52. The net flow direction in situation 1 of Master A before recovery

Now if both port F0/1 and port F0/3 of Master A become active again as shown in Figure 4.53, and neither Master1 nor Back 1 has enabled preempt, whichever of them enables HA first would be the main firewall. Therefore, there are two possible situations in the network. Situation 1: when the HA of port F0/1 in Master A is enabled sooner than that of port F0/3, the network traffic direction would be: PC2→Master A→Master 1→Master B→PC1. The testing result can be seen in Figure 4.54.

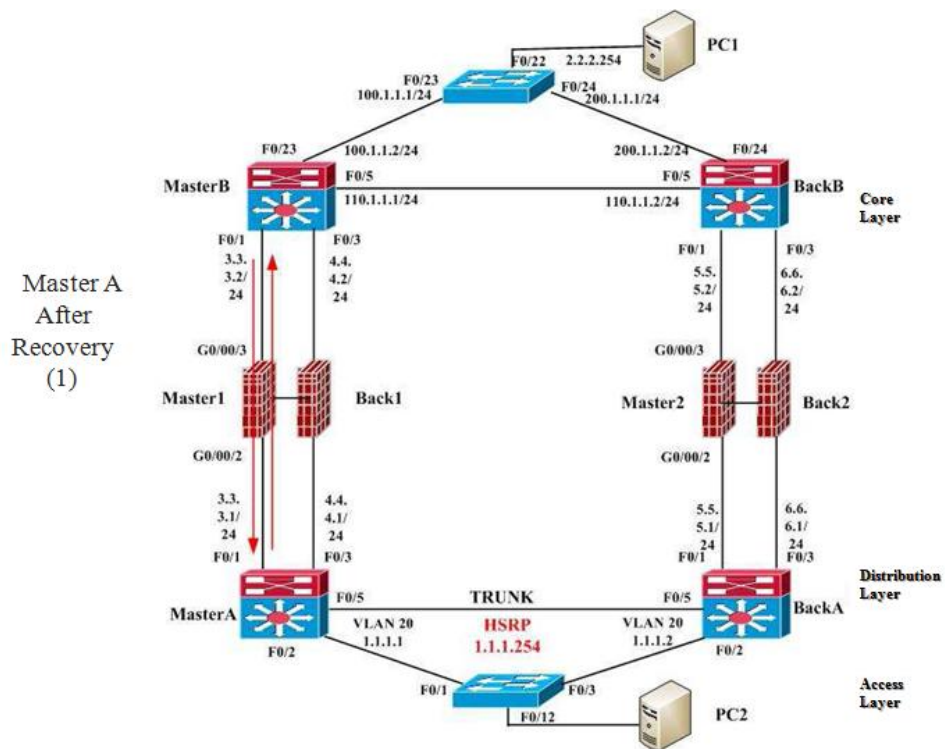


Figure 4.53. The situation 1 of switch Master A after recovery

```
D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    1.1.1.1
  2  <1 ms    <1 ms    <1 ms    3.3.3.2
  3  <1 ms    <1 ms    <1 ms    100.1.1.1
  4  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.
```

Figure 4.54. The net flow direction in situation 1 of switch Master A after recovery

As we can see from Figure 4.54, the network flow direction after network handoff is: PC2→Master A→Master 1→Master B→PC1.

```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=4ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125

```

Figure 4.55. The ping duration in situation 1 of switch Master A after recovery PC2 in the network continues to ping PC1's address, as shown in Figure 4.55. And the flow direction shift information is shown in Figure 4.56.

```

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops
  0  <1 ms  <1 ms  <1 ms  1.1.1.1
  1  <1 ms  <1 ms  <1 ms  1.1.1.2
  2  <1 ms  <1 ms  5 ms  5.5.5.2
  3  1 ms  1 ms  <1 ms  200.1.1.1
  4  <1 ms  1 ms  4 ms  2.2.2.200

Trace complete.

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops
  0  <1 ms  <1 ms  <1 ms  1.1.1.1
  1  <1 ms  <1 ms  <1 ms  1.1.1.2
  2  <1 ms  <1 ms  <1 ms  100.1.1.1
  3  <1 ms  4 ms  <1 ms  2.2.2.200

Trace complete.

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops
  0  <1 ms  <1 ms  <1 ms  1.1.1.1
  1  <1 ms  <1 ms  <1 ms  3.3.3.2
  2  <1 ms  <1 ms  <1 ms  100.1.1.1
  3  <1 ms  <1 ms  <1 ms  2.2.2.200

```

Figure 4.56. The flow direction shift in situation 1 of Master A after recovery

4.5.6 Test 14: Situation 2 of Master A recovery and preempt

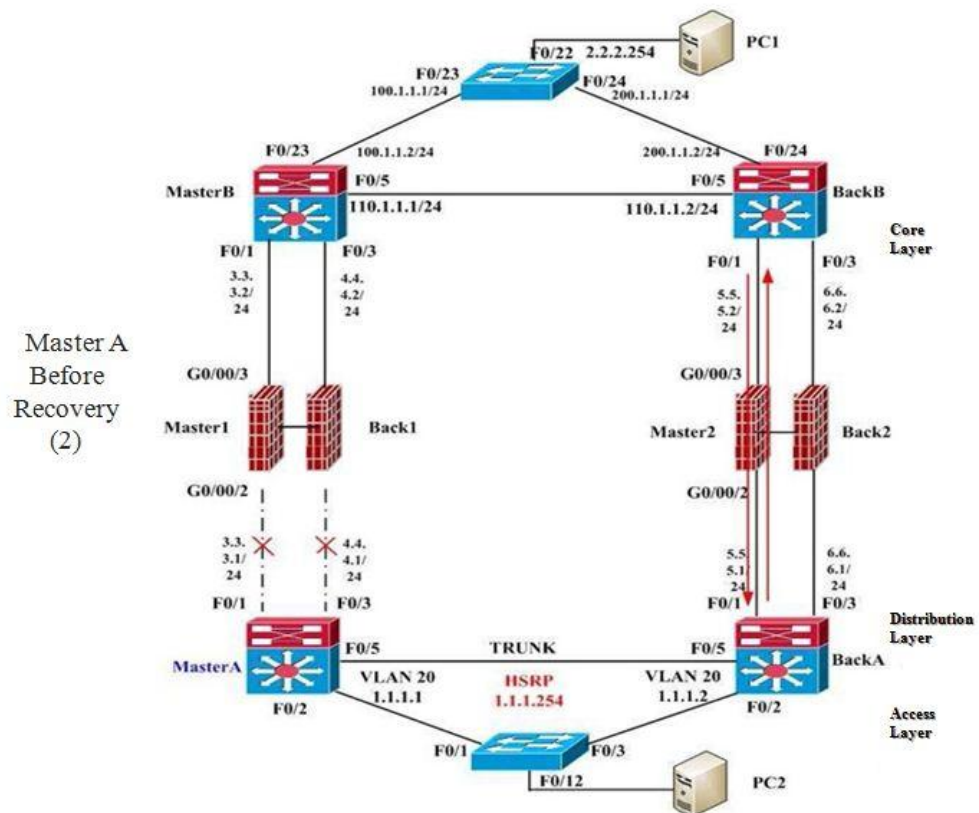


Figure 4.57. The situation 2 of switch Master A before recovery

In Figure 4.57, originally when port F0/3 and F0/1 of Master A in the network are down, the network flow direction is: PC2→Back A→Master 2→Back B→PC1 as shown in Figure 4.58.

```
D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    1.1.1.1
  2  <1 ms    <1 ms    <1 ms    1.1.1.2
  3  <1 ms    <1 ms    <1 ms    5.5.5.2
  4   1 ms    <1 ms    <1 ms    200.1.1.1
  5  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.
```

Figure 4.58. The net flow direction in situation 2 of Master A before recovery

Now if both port F0/1 and port F0/3 of Master A become active again as shown in Figure 4.59, and neither Master1 nor Back 1 has enabled preempt, whichever of them enables HA first would be the main firewall. Therefore, there are two possible situations in the network. Situation 2: when the port F0/3 in Master A is enabled sooner than that of port F0/1, the network traffic direction will be: PC2→Master A→Back 1→Master B→PC1. The testing result can be seen in Figure 4.60.

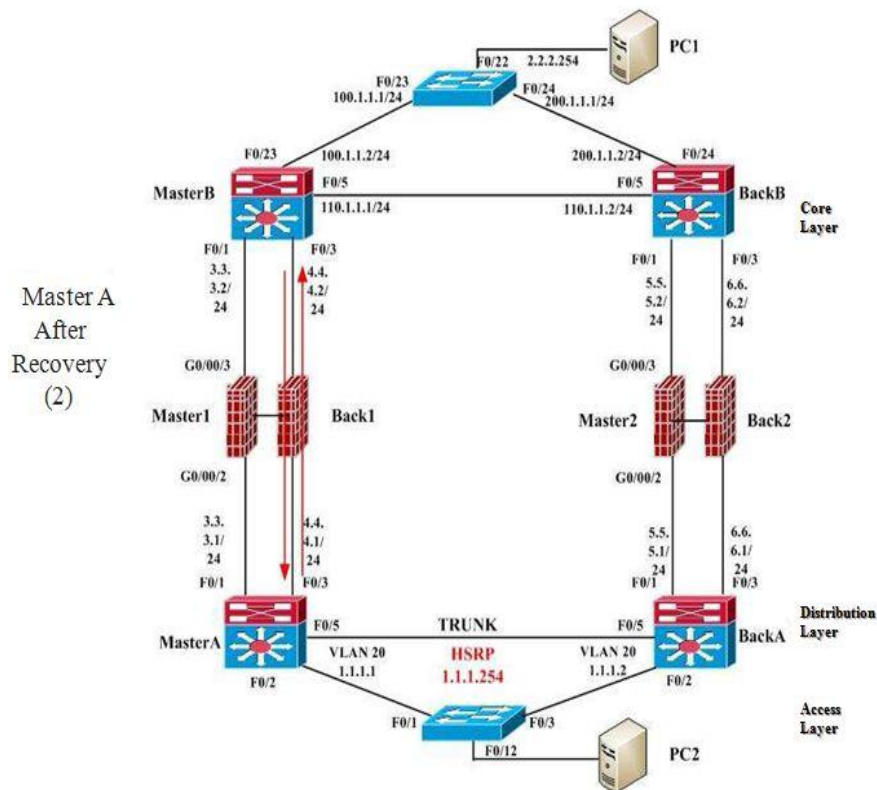


Figure 4.59. The situation 2 of switch Master A after recovery

```
D:\>tracert 2.2.2.200

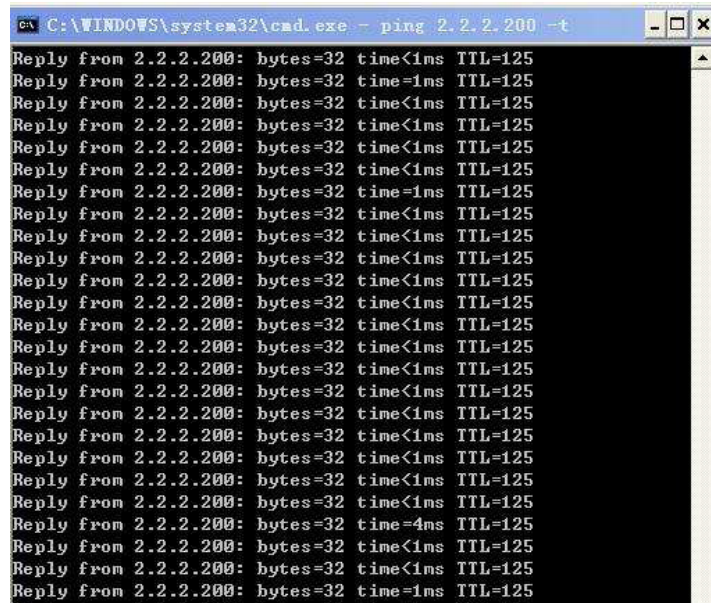
Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    4.4.4.2
  2   1 ms    <1 ms    <1 ms    100.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.
```

Figure 4.60. The net flow direction in situation 2 of Master A after recovery

As shown in Figure 4.60, the network flow direction after network handoff is: PC2→Master A→Back 1→Master B→PC1.

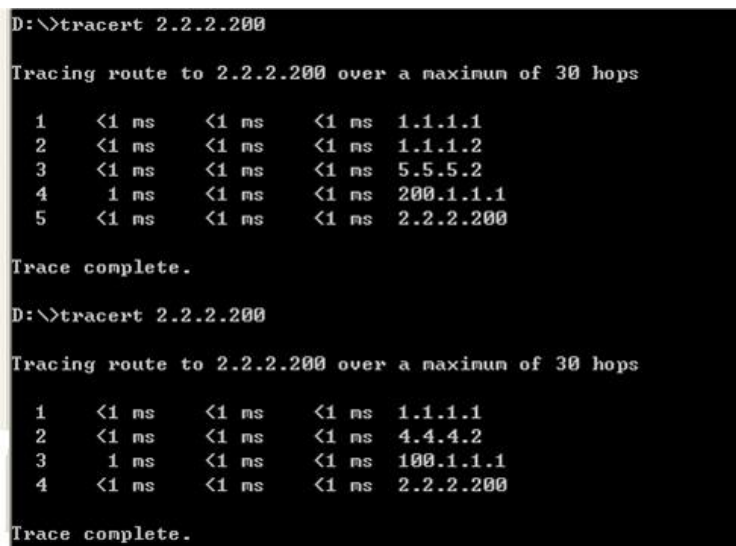


```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=4ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125

```

Figure 4.61. The ping duration in situation 2 of switch Master A after recovery PC2 in the network continues to ping PC1's address, as shown in Figure 4.61. And the flow direction shift information is shown in Figure 4.62.



```

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2  <1 ms    <1 ms    <1 ms    5.5.5.2
  3   1 ms    <1 ms    <1 ms    200.1.1.1
  4  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    4.4.4.2
  2   1 ms    <1 ms    <1 ms    100.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

```

Figure 4.62. The flow direction shift in situation 2 of switch Master A after recovery

4.5.7 Test 15: Situation 3 of Master A recovery and preempt

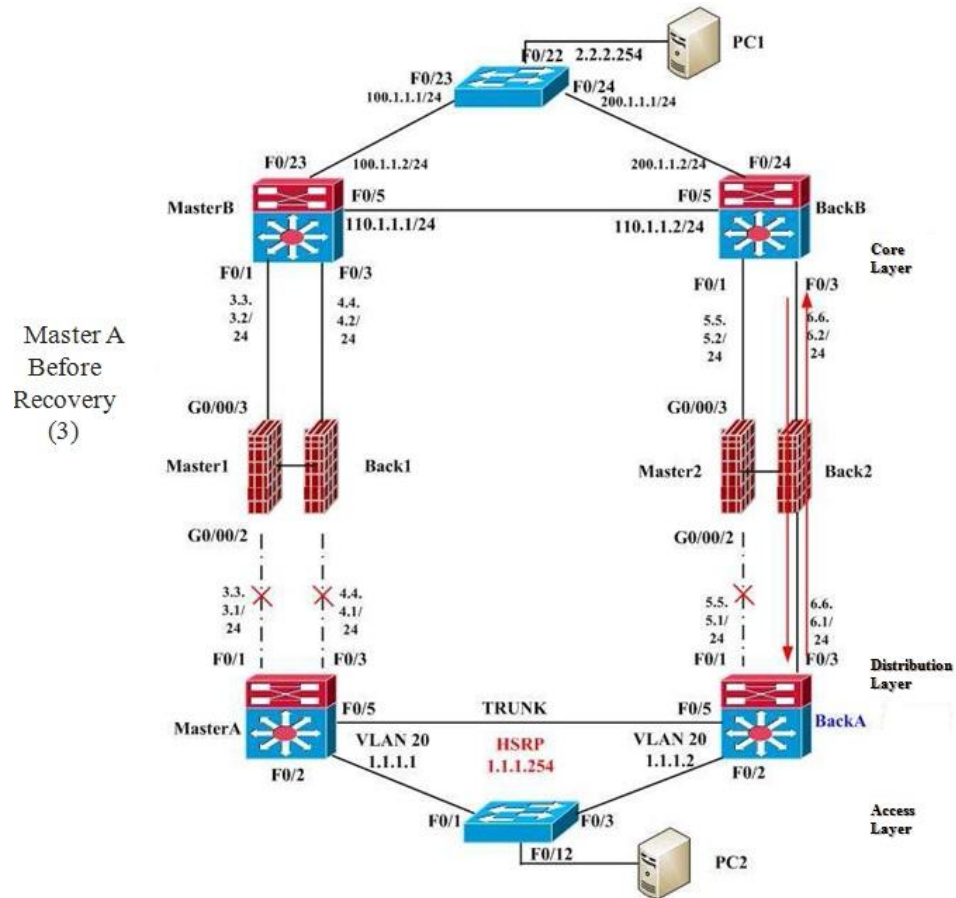


Figure 4.63. The situation 3 of switch Master A before recovery

In Figure 4.63, originally when port F0/3 and F0/1 of Master A in the network are down, and the port F0/1 of Back A is also down, the network flow direction is: PC2→Back A→Back 2→Back B→PC1 as shown in Figure 4.64.

```

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    1.1.1.1
  2  <1 ms    <1 ms    <1 ms    1.1.1.2
  3   1 ms    <1 ms    <1 ms    6.6.6.2
  4   1 ms     4 ms    <1 ms    200.1.1.1
  5   1 ms    <1 ms    <1 ms    2.2.2.200
    
```

Figure 4.64. The net flow direction in situation 3 of switch Master A before recovery

Now if both port F0/1 and port F0/3 of Master A become active again as shown in Figure 4.65, and neither Master 1 nor Back 1 has enabled preempt, whichever of them enables HA first would be the main firewall. Therefore, there are two possible situations in the network. Situation 1: when port F0/1 in Master A is enabled sooner than that of port F0/3, the network traffic direction will be: PC2→Master A→Master 1→Master B→PC1. And the testing result is shown in Figure 4.66.

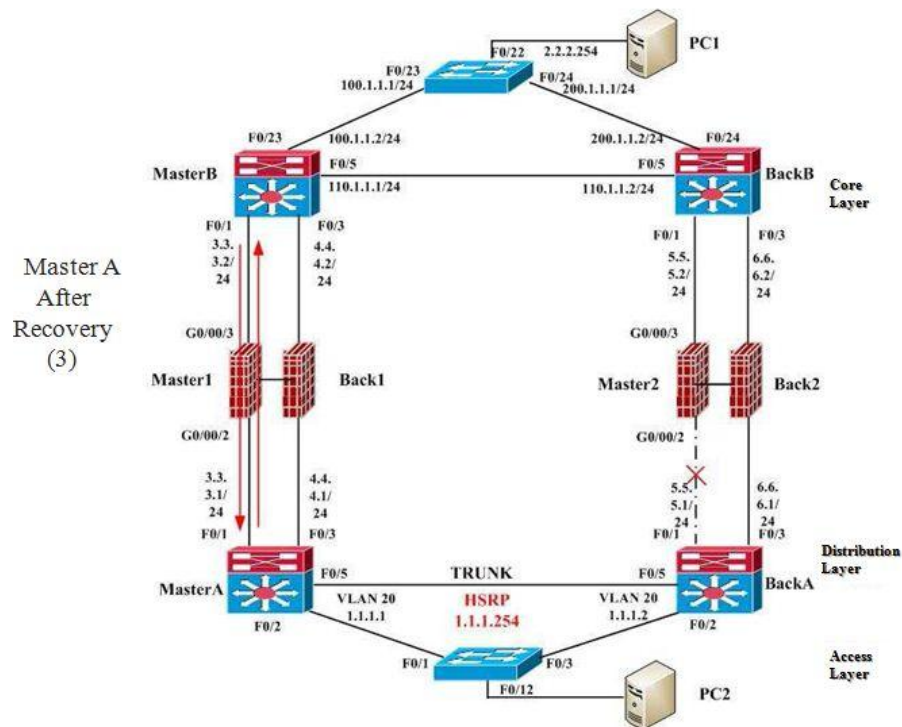


Figure 4.65. The situation 3 of switch Master A after recovery

```
D:\>tracert 2.2.2.200

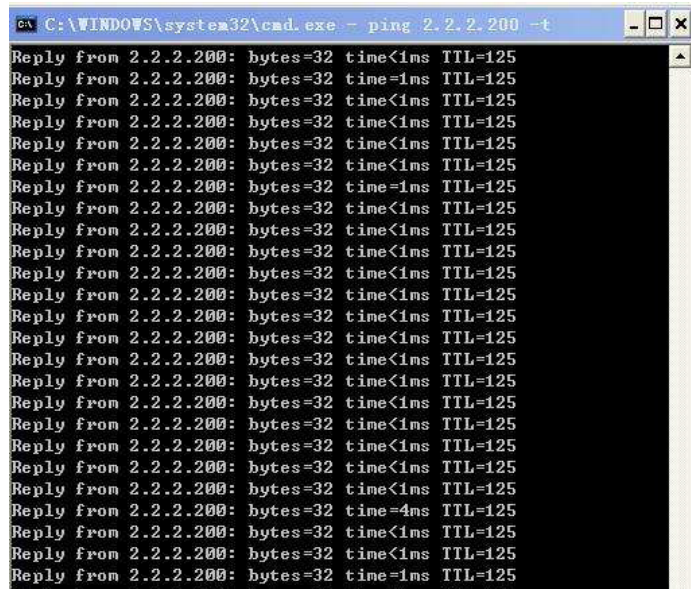
Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    1.1.1.1
  2  <1 ms    <1 ms    <1 ms    3.3.3.2
  3  <1 ms    <1 ms    <1 ms    100.1.1.1
  4  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.
```

Figure 4.66. The net flow direction in situation 3 of switch Master A after recovery

As shown in Figure 4.66, the network flow direction after network handoff is: PC2→Master A→Master 1→Master B→PC1.



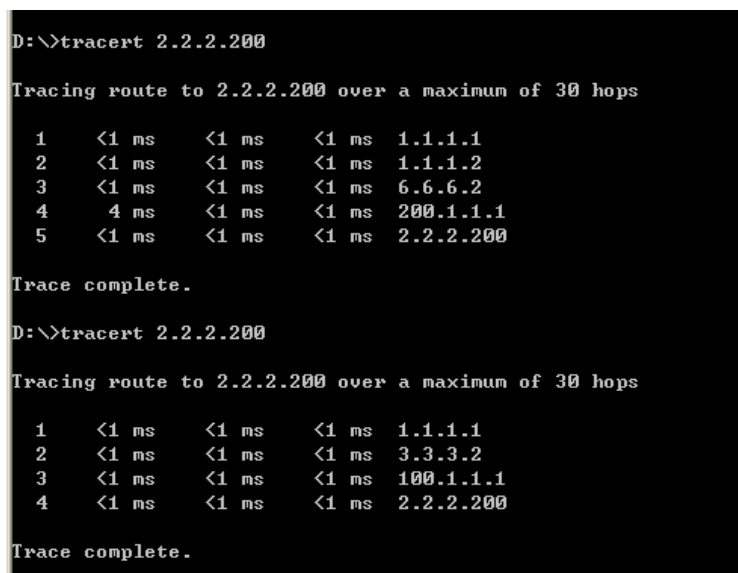
```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=4ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125

```

Figure 4.67. The ping duration under the situation 3 of switch Master A after recovery

PC2 in the network continues to ping PC1's address, as shown in Figure 4.67, and the flow direction shift information is shown in Figure 4.68.



```

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2  <1 ms    <1 ms    <1 ms    6.6.6.2
  3  4 ms     <1 ms    <1 ms    200.1.1.1
  4  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    3.3.3.2
  2  <1 ms    <1 ms    <1 ms    100.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.

```

Figure 4.68. The flow direction shift in situation 3 of switch Master A after recovery

4.5.8 Test 16: Situation 4 of the recovery and preempt of Master A

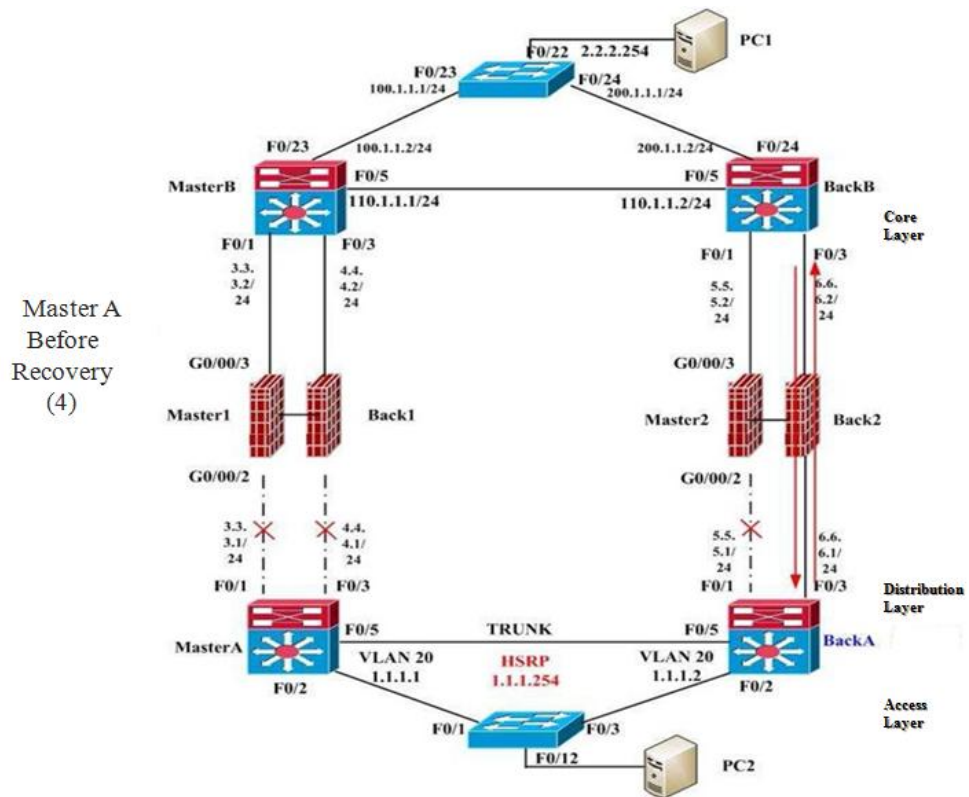


Figure 4.69. The situation 4 of switch Master A before recovery

In Figure 4.69, originally when port F0/3 and F0/1 of Master A in the network are down, and port F0/1 of Back A is also down, the network flow direction is: PC2→Back A→Back 2→Back B→PC1. The testing result of net flow direction is shown in Figure 4.70.

```

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  1  <1 ms  <1 ms  <1 ms  1.1.1.1
  2  <1 ms  <1 ms  <1 ms  1.1.1.2
  3   1 ms  <1 ms  <1 ms  6.6.6.2
  4   1 ms   4 ms  <1 ms  200.1.1.1
  5   1 ms  <1 ms  <1 ms  2.2.2.200
    
```

Figure 4.70. The net flow direction in situation 4 of switch Master A before recovery

Now if both port F0/1 and port F0/3 of Master A become active again as shown in Figure 4.71, and neither Master 1 nor Back 1 has enabled preempt, whichever of them enables HA first will be the main firewall. Therefore, there are two possible situations in the network. Situation 2: when port F0/3 in Master A is enabled sooner than that of port F0/1, the network traffic direction will be PC2→Master A→Back 1→Master B→PC1 and the testing result is shown in Figure 4.72.

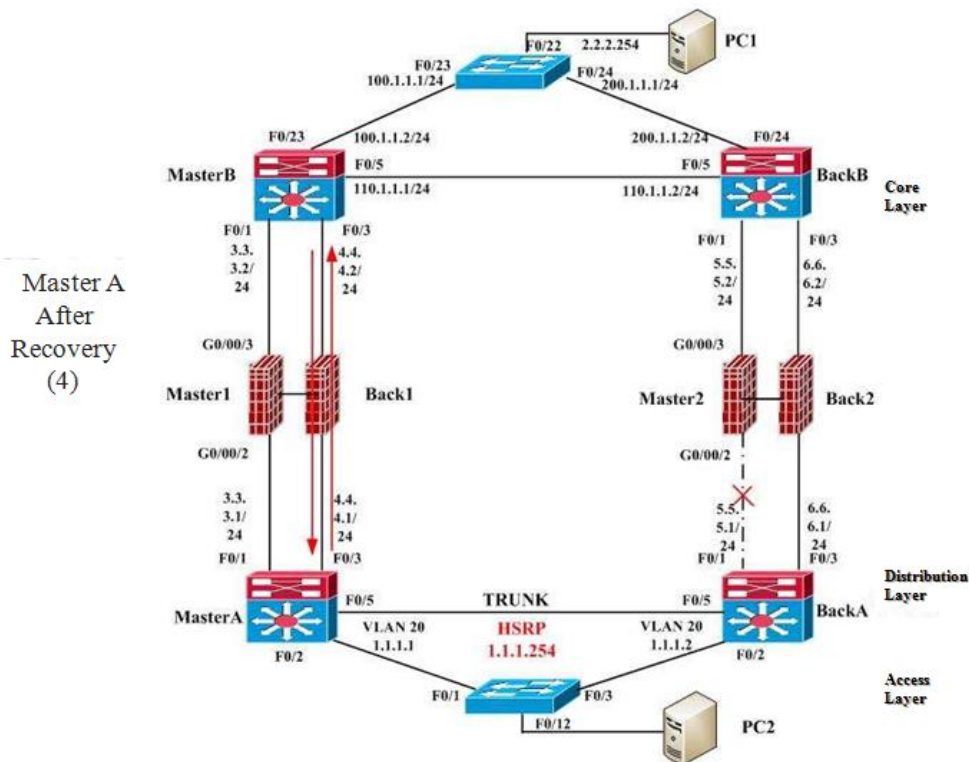


Figure 4.71. The situation 4 of switch Master A after recovery

```
D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    4.4.4.2
  2   1 ms    <1 ms    <1 ms    100.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

Trace complete.
```

Figure 4.72. The net flow direction in situation 4 of switch Master A after recovery

As shown in Figure 4.72, the network flow direction after network handoff is: PC2→Master A→Back 1→Master B→PC1.

```

C:\WINDOWS\system32\cmd.exe - ping 2.2.2.200 -t
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time=4ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125
Reply from 2.2.2.200: bytes=32 time<1ms TTL=125

```

Figure 4.73. The ping duration in situation 4 of switch Master A after recovery PC2 in the network continues to ping PC1's address, as shown in Figure 4.73. And the flow direction shift information can be seen in Figure 4.74.

```

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2  1 ms     <1 ms    <1 ms    6.6.6.2
  3  1 ms     <1 ms    4 ms    200.1.1.1
  4  1 ms     <1 ms    <1 ms    2.2.2.200

Trace complete.

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    1.1.1.2
  2  1 ms     <1 ms    <1 ms    100.1.1.1
  3  3 ms     <1 ms    <1 ms    2.2.2.200

Trace complete.

D:\>tracert 2.2.2.200

Tracing route to 2.2.2.200 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms    1.1.1.1
  1  <1 ms    <1 ms    <1 ms    4.4.4.2
  2  <1 ms    <1 ms    <1 ms    100.1.1.1
  3  <1 ms    <1 ms    <1 ms    2.2.2.200

```

Figure 4.74. The flow direction shift in situation 4 of switch Master A after recovery

4.6 Summary

In this chapter, we have presented the specific procedures of the testing. We have covered the topologies based on the second and third layer of the network, the network traffic direction and its changes when a certain port connected to the main device is interrupted due to some reason. The last part of this chapter was about the test of main device operation after malfunction recovery. That means we checked whether the network could order the priorities of links, get the main link back into use rapidly after the recovery of main devices and main ports, and reduce the backup line into passive status. In the next chapter, conclusions will be drawn from the testing results.

5. CONCLUSION

This chapter gives a conclusive review of the study carried out in this thesis. The answers to the research questions are given first, followed by a concise description of what has been achieved. At the end of this chapter, the implications and recommendations for future research are briefly discussed.

5.1 Review of the answers to the research questions

The main thesis questions are:

- How can the Cisco three-layer hierarchical model be used?
- Can this testing procedure be used for company's malfunction analysis in reality?
- Does the malfunction analysis procedure in this thesis comprehensively simulate all the possibilities that will happen?

How can the Cisco three-layer hierarchical model be used?

In Cisco's three-layered structure, the network is divided into core layer, distribution layer, and access layer. The core layer belongs to the third layer network, so we need to allocate IP addresses to them and configure the routing protocols to the network. We put the firewall and switches near the egress into the core layer. The two-layered structure in the network locates the network malfunction according to the spanning-tree protocol while in actual operation the network malfunction is mainly attributable to disoperation. So we change the two-layered network environment into the three-layered one. That is to say, the switches on each floor which are actually put into use are defined as three-layered switches, while the two two-layered switches that provide client access become the access layer devices.

Can this testing procedure be used for company's malfunction analysis in reality?

In this test, we have mainly analyzed the user environment of customers, and in the light of customer demand and Cisco's three-layered model, we have designed the physical and logical topologies that tally with the actual situation. Besides, we have analyzed eight possible malfunction situations, and conducted the testing of the eight active preemptions after the recovery of device malfunction. HA feasibility is proven successful with this test, and it fundamentally guarantees the high redundancy of link with full consideration of possible malfunction situations. The whole testing process can be applied universally to HA performance testing, so it can be taken for the standard of HA malfunction analysis for the company. In the meanwhile, it is hoped that more efforts could be made to further improve this test to seek a more accurate and comprehensive HA testing theory.

Does the malfunction analysis procedure in this thesis comprehensively simulate all the possibilities that will happen?

This thesis mainly discusses the testing of HA performance, i.e., testing the HA feasibility when the new product of the company is employed in the customers' actual environment. The testing environment in this thesis is only a simulation of the actual company environment, so the testing and its results are only accomplished with the purpose of testing the feasibility of the HA function on the consideration of the feasibility of the HA function. In effect, in the real user environment, other factors such as the stability and the stress capacity of the device, and the fault tolerance capacity in some special cases will affect the HA performance in one way or another. However, they are beyond the scope of the test in this thesis.

5.2 The problems occurring in the testing process

There are four problems that were detected during the testing procedure:

1. In the transparent mode of HA active/standby model, the standby firewall is not configured with the HA tracking port, but it can still synchronize the configuration.
2. In the transparent mode of the HA active/standby model, the device name could be synchronized on to the standby device, as well.
3. The HA firewall in the active/standby model could only synchronize with the config.cfg file.
4. The configuration of synchronization can only be realized manually not automatically between Master 1, Back 1 and Master 2, Back 2.

5.3 Summary of the testing process

The goal of this test was to try the utmost to prevent the occurrence of SPOF (Single Points of Failure), so the redundancy devices were configured both on firewalls and switches. Nevertheless, we could still see the occurrence of SPOF, such as power supply device failure, or storage device failure etc.

This test was mainly to verify the high availability of the network design, for the reason that we could only simulate the 100-megabit network environment, while the customers' core network environment is of the 10-gigabit network environment. Synchronization could not be realized in the routing environment of the HA active/standby model and the 10-gigabit network of HA active/active model, which falls short of customer demand. Therefore in the testing plan, the main testing point was set as the application of HA active/standby model in transparent mode.

Through the testing, we found out that network flow could automatically shift the network link in multiple malfunction situations and during malfunction recovery, to ensure fluent connection. Thus, we can conclude that the application of the HA active/standby model in transparent mode in this network design is feasible.

REFERENCES

- [1] Matthew Strebe. (2004). *Network Security Foundations* (1st ed.). San Francisco: Sybex.
- [2] Candace Leiden and Marshall Wilensky. (2009). *TCP/IP for Dummies*. Hoboken, NJ:Wiley.
- [3] Sander van Vugt. (2009). *Pro Ubuntu Server Administration*. Berkeley, CA : Apress ; New York : Distributed to the book trade by Springer-Verlag.
- [4] Lenovo Security Technologies, Inc. (2009).
[\[http://www.leadsec.com.cn/Product/?RootID=359&ParentID=360&ClassID=hide\]](http://www.leadsec.com.cn/Product/?RootID=359&ParentID=360&ClassID=hide)
 Available at www.leadsec.com.cn. Retrieved November 2, 2009.
- [5] James D.McCabe. (2007). *Network Analysis, Architecture, and Design*. San Francisco Calif. : Morgan Kaufmann.
- [6] Joseph F. Lamond, and J. H. Pielert. (2006). *Significance of Tests and Properties of Concrete and Concrete-making Materials*. West Conshohocken, Pa.: ASTM
- [7] The Cisco Three-Layered Hierarchical Model. (2004).
[\[http://www.semsim.com/ccna/ccna-study-guide.asp?ain=57\]](http://www.semsim.com/ccna/ccna-study-guide.asp?ain=57) Available at:
<http://www.SemSim.com> .Retrieved November 2, 2009..
- [8] C.Engelmann and S.L.Scott. *Concepts for High Availability in Scientific High-End Computing*. Oak Ridge National Laboratory: Oak Ridge, TN 37831, USA.
- [9] Kevin Dooley. (2002). *Designing Large-scale LANs*. Beijing ; Köln [u.a.] : O'Reilly.

[10] HA Cluster Plugin User Guide. (1995).

[www.nexenta.com/static/ha-cluster-userguide-2.1]. Available at:

<http://www.high-availability.com>. Retrieved October 10, 2009

Appendix--Configuration Files

A. The configuration of Master1 and HA status

```
KingGuard(config)#show ha configuration
ha mode active-standby
ha local node-id 2
ha hello-interval 500
ha priority 100
ha enable
KingGuard(config)#show ha status
ha is running.
node-id      status      metric
-----
1            Fault      100
2            Active    200
```

B. Configuration of the firewall of Master 2 and status output

```
KingGuard(config)#show ha configuration
ha mode active-standby
ha local node-id 3
ha hello-interval 500
ha priority 100
ha enable
KingGuard(config)#show ha status
ha is running.
node-id      status      metric
-----
3            Active    200
4            Standby   200
```

C. Configuration of the firewall of Back 2 and status information

```
KingGuard(config)#show ha configuration
ha mode active-standby
ha local node-id 4
ha hello-interval 500
ha priority 100
ha enable
KingGuard(config)#show ha status
ha is running.
node-id      status      metric
-----
3            Fault      100
4            Active    200
```

D. The status information of Master A shown for 4.4.5

```
masterA#
2d06h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to down
```

```

masterA#
2d06h: %STANDBY-6-STATECHANGE: Vlan20 Group 1 state Active -> Speak
2d06h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
masterA#
2d06h: %OSPF-5-ADJCHG: Process 1, Nbr 110.1.1.1 on FastEthernet0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached
masterA#
2d06h: %OSPF-5-ADJCHG: Process 1, Nbr 110.1.1.1 on FastEthernet0/3 from LOADING to
FULL, Loading Done

masterA#show sta
masterA#show stan
Vlan20 - Group 1
  Local state is Standby, priority 95 (confgd 105), may preempt
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 2.656
  Virtual IP address is 1.1.1.254 configured
  Active router is 1.1.1.2, priority 100 expires in 8.880
  Standby router is local
  56 state changes, last state change 00:01:13
  IP redundancy name is "hsrp-Vl20-1" (default)
  Priority tracking 2 interfaces or objects, 1 up:
    Interface or object      Decrement      State
    FastEthernet0/1         10             Down   (line protocol down)
    FastEthernet0/3         10             Up

```

E. The status information of Master A shown for 4.4.6.

```

masterA#
2d06h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
to down
masterA#
2d06h: %STANDBY-6-STATECHANGE: Vlan20 Group 1 state Active -> Speak
2d06h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
masterA#
2d06h: %OSPF-5-ADJCHG: Process 1, Nbr 110.1.1.1 on FastEthernet0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached
masterA#
2d06h: %OSPF-5-ADJCHG: Process 1, Nbr 110.1.1.1 on FastEthernet0/3 from LOADING to
FULL, Loading Done

masterA#show sta
masterA#show stan
Vlan20 - Group 1
  Local state is Standby, priority 95 (confgd 105), may preempt
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 2.656
  Virtual IP address is 1.1.1.254 configured
  Active router is 1.1.1.2, priority 100 expires in 8.880
  Standby router is local
  56 state changes, last state change 00:01:13
  IP redundancy name is "hsrp-Vl20-1" (default)
  Priority tracking 2 interfaces or objects, 1 up:
    Interface or object      Decrement      State

```

FastEthernet0/1	10	Down	(line protocol down)
FastEthernet0/3	10	Down	(line protocol down)