Simulation of Reliable Communication in Large-scale LAN

Zuozheng Lian

*Compute Center, Qiqihar University,
Qiqihar 161006, Qiqihar, China*

Haizhen Wang

*School of Computer and Control Engineering,
Qiqihar University, Qiqihar 161006, Qiqihar, China*

Abstract
Reliable communication is a challenging problem when planning and designing large-scale LAN. It is also a key issue in network planning and the designing of courses. In this paper, we propose a network communication model in a large-scale LAN based reliable technology, which is efficient from simulation point of view. First, a HCL simulator is adopted to design a network model with a three-layer architecture using switches as the key components. Second, network reliability technology is applied to configure all devices, e.g. link aggregation and virtual router redundancy protocol (VRRP), together with Virtual Local Area Networks (VLAN), multiple spanning tree protocol (MSTP) and OSPF protocols. Finally, the communication reliability is verified and the result is analyzed, the result shows that this model can provide reliable communication and also be helpful for students to understand and apply such technologies, i.e., VLAN and VRRP technology and the knowledge of routing protocols.

Key words: LARGE-SCALE LAN, HCL SIMULATOR, RELIABILITY COMMUNICATION

1. Introduction

The increasing demand for information exchange and improved computing power exceeded the load limits of traditional LAN, so Ethernet switch technology has emerged in 1990s [1]. In the beginning, it was only implemented with the protocol of the lowest two layers in the OSI model. With the development of switch technology, the protocols from three or more layers in the OSI model have been implemented as well. At present, most of LAN using Ethernet topology, because it has the following four advantages [2]. 1) It can reduce costs when upgrading a user's network due to the replacement of share-based HUBs and switches. 2) It allows for collaboration between different networks due to its easy transition between high-speed networks and low-speed networks. 3) It provides more channels and bandwidth than traditional share-based concentrators do. 4) It has relatively low cost, high bandwidth and high-speed routers. Hence, when switch-based Ethernet technology is applied to a LAN, i.e. a switch-based Ethernet, it can greatly improve the performance of traditional LAN.

With widespread applications of switch-based Ethernet technology, switch based VLAN have also been developed [3]. VLAN is a type of logical group [4] consisting of several LAN segments whose physical locations are irrelevant, it has become a key technology in large-scale LAN [5, 6]. Addition to the VLAN technical, network topology structure design and application of related redundancy technology are very import to ensure reliable communication in large-scale LAN. Generally, the network is more reliable with mesh topology, typical redundancy techniques include link aggregation, VRRP, STP, etc., and in recent years, researchers have carried out the related research. Link aggregation technology were applied to network high availability for Ethernet services in literature [7], MSTP were applied to partitioning networks in literature [8, 9], and VRRP were improved and applied to load balance in literature [10], but single technology is limit to impoved reliable communication, there is little research on integrated application to these techniques.

With various two- and three-layer switches are frequently used in large LAN networking, it has become increasingly critical to use these switches to achieve reliable communication. The critical problem effects the success of large-scale LAN planning and design, and this is a key pedagogical point in network planning and design courses, which could help students understand important knowledge and develop their innovation ability if they were able to combing the study of actual device operation with software simulation in their courses [11]. In this paper, a HCL simulator is used to design a large-scale LAN model with emphasis on network reliability. VLAN technology, link aggregation, MSTP and VRRP are adopted to configure reliable communication in the network model. In this configuration process, students could obtain a better understanding of the challenges in reliable communication technologies in large-scale LAN by practicing, analyzing and solving problems directly.

2. Design of Reliable Communications solutions in Large-scale LAN

Generally, a large-scale LAN contains multiple departments, each of which needs to implement reliable communication among 500-1000 points of information (POI). Moreover, it also requires high processing capability, VLAN division supporting switches, simple and effective network structures that can utilize quintillion links as workhorses, and must achieve gigabit bandwidth to desktop computers. Therefore, VLAN and network reliability technology are two of the challenging problems to achieve reliable communication in large-scale LANs. In this section, the technical issues and their solutions are analyzed.

2.1 Technical Issues

2.1.1 Technical Issues of Network Reliability

1. Network Reliability Design

Network reliability is quantified by the percentage of service uptime provided by network. As any network component may malfunction, network reliability is generally achieved by a certain amount of redundancy. Nevertheless, the main components in the communication network are network devices and links, so network reliability design is mainly related to the design of these two elements.

The structures of large-scale networks are complicated, so a layered model design is usually applied, i.e., dividing a network into several layers with each layer concentrating on a certain function. This approach turns a complicated problem into several smaller and simpler problems. Three-layer network architectures have a core layer, a convergence layer and an access layer, with their respective functions explained as follows.

CORE LAYER. This is a group of network high-speed switches. It plays an important role in the entire network connectivity, so is usually considered the “Network Center”. It must have high reliability, high efficiency, redundancy, fault tolerance, manageability, adaptability and low latency, etc. Therefore, gigabit switches with high bandwidth should be used. Dual redundant hot backup technology and load balancing technologies are usually applied to improve network performance as well.

CONVERGENCE LAYER. This is the intermediary between the access layer and the core layer. It converges first before the workstation can access the core layer. This serves to alleviate the device load in the core layer. Many functions are gathered in the convergence layer, such as implementation strategy, security, workstation access, inter-VLAN routing, and source/destination address filtration. Hence, the convergence layer should also adopt a three-layer switch technology and VLAN switches to achieve network isolation and division.

ACCESS LAYER. This can provide workstation access for local network segments, decrease the number of workstations in the same network segment, and provide high-speed bandwidth for workgroups. At the access layer, ordinary switches that do not support VLAN and three-layer switching technologies are allowed.

By converting the network architecture from a two-layer switch technology to a three-layer switch technology, an improvement in network performance can be easily obtained. With the help of network management software, the network security can also be greatly enhanced. By allocating core switches appropriately, the hardware performance of core switches could be taken fully exploited. By adjusting the positions of the core switches in the bandwidth and network traffic handling capabilities, good scalability can be achieved. By dividing VLAN according to business requirements to control broadcasting areas, the whole performance and security of LANs can be enhanced.

2. Network Reliability Related Technologies

In this paper, reliability technologies including link aggregation, MSTP and VRRP are applied, and we now introduce these concepts below.

(1)MSTP

MSTP is generated based on a Spanning Tree Protocol (STP), and its technical issues are analyzed below. There are multiple interlinked switches in LAN. In order to avoid broadcast storms, loop circuits in networks are not allowed. STP can form a loop-less tree in all links. However, all STP VLANs share the same spanning tree and the topological structures are the same. Thus, all VLANs in one Trunk remain in either the forwarding state or the blocked state, some links are wasted and cannot provide load sharing of VLAN traffic.

MSTP could define multiple spanning tree objects in a network, and each object corresponds to multiple VLANs, maintaining its own spanning tree. This avoids resource over-consumption that is associated with maintaining its own spanning tree for each VLAN, while still being able to maintain different spanning tree topologies for different VLANs. Furthermore, different VLANs can have different states in different ports. As shown in Figure 1, switches are interconnected, a region is divided and two spanning tree instances are configured: one is the link between SW2 and SW1 taking SW2 as root (indicated by the dotted arrow), and the other is the link between SW3 and SW1 taking SW3 as root (indicated by the solid arrow). Instance 1 allows communication between VLAN 1~10 and the Server, while Instance 2 allows communication between VLAN 11~20 and the Server. Therefore, MSTP is generally applied to large-scale LAN with multiple VLANs, effectively improving the load balance of multiple VLANs while providing network links and device backups.

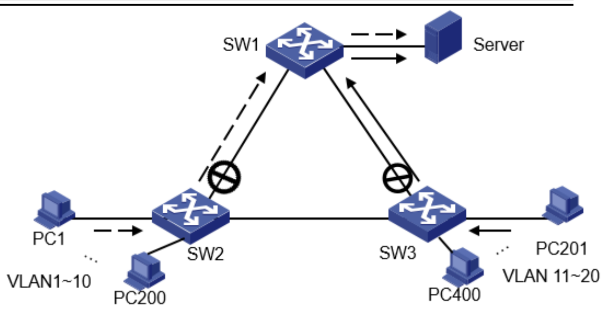

Figure 1. Configuration of multiple VLANs load sharing by MSTP

(2) VRRP

In general, hosts’ gateway in same broadcast domain is set to next hop of gateway’s default routing. The default routing provides a convenient way to configure host for the user, but which also requires high stability for gateway equipment, increasing the number of gateway equipment is a common method to improve the network reliability. VRRP could be able to join a group of gateway functions routers to the backup group to form virtual routers, and from which, the election mechanism of VRRP may elect a gateway router.

The main features of VRRP backup group are as follows. 1) Virtual routers have IP address, namely virtual IP address. Hosts in LAN only needs to know the virtual IP address, which is set to the next hop of the default routing. 2) Hosts in LAN communication with external network by the virtual router. 3) Routers in the backup group firstly select master router according to the priority (The highest priority router becomes the master router, if the priority is same, then the biggest IP address router becomes the master router) to bear gateway function, other routers as backup routers, when the master router failure, the backup routers replace master router to performance the gateway duties, so as to ensure the hosts in LAN to communicate uninterrupted with external network. According to the characteristics of VRRP, the VRRP is applied to the convergence layer switches and the network reliability is improved.

(3) Link Aggregation

Link aggregation converges multiple LAN lines with the same characteristics to form one logical link. The converged links load-share transmission data, and when a line in a certain link aggregation malfunctions, other links could still function and share data. This provides LAN link backup and ensures the reliability of the link design.

2.1.2 Principles of VLAN Technology

VLAN technology is essential to LAN. It’s most challenging technologies, VLAN tag operation and VLAN routers, are introduced in this section.

1. VLAN Tag Operation

In VLAN technologies, a tag added to the Ethernet frame indicates to which VLAN the frame can propagate. Thus, not only should MAC address be searched to determine which port to forward, but also the tag on ports should be checked to ascertain whether it is matched with a specific port when switching the transmission data frame. Furthermore, the attributes of different switch ports need to be configured manually in order to make switches that achieve a tag match. Each port of the switch that supports VLANs could be configured with one of three attributes: Access, Trunk or Hybrid. An Access port can only be assigned to one VLAN. The transmission frame is used to connect to a PC. The frame is not tagged and commonly does not receive a tagged frame. A Trunk port can be assigned to multiple VLANs. Generally, the received frames are always tagged. The tagged frames are used in transmitting multiple VLAN frames among multiple switches to provide the same VLAN communication for multiple switches. A Hybrid port has the functions of both Access and Trunk ports, and can be assigned to multiple VLANs. It is mainly used for building VLANs based on protocols. In this paper, the attribute ports of switch configurations are Access ports and Trunk ports.

2. Inter-VLAN Routing

Inter-VLAN routing technologies are introduced to provide communication between different VLANs. There are several implementation models, e.g., a two-layer switch plus router, a one-armed router, and a three-layer switch. Comparatively, built-in three layer forwarding engines in three layer switches have the advantages of high speed, large throughput, latency avoidance, instability generated by external physical connections, and better transmission performance than inter-VLAN routing using routers. Hence, in this paper, three-layer switches are used for inter-VLAN routing.

2.2 Solutions

2.2.1 Networking Model Design

In this paper, an H3C simulator (HCL) is used to de sign the network model for a three-layer structure large-scale LAN, as shown in Figure 2.

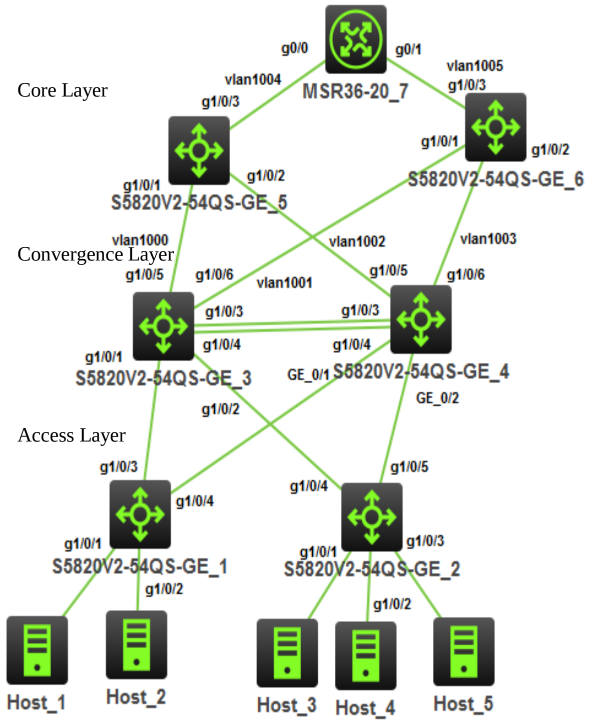

Figure 2. Networking model

In Figure 2, S5820V2-54QS-GE_1 (expressed as SW1) and S5820V2-54QS-GE_2 (expressed as SW2) are Access layer switches, separately divided into two VLANs and three VLANs, and representing five different departments, i.e., Host_1, Host_2, Host_3, Host_4 and Host_5. The five hosts represent the managing users of these five departments, and they all require mutual communication. S5820V2-54QS-GE_3 (expressed as SW3) and S5820V2-54QS-GE_4 (expressed as SW4) are convergence layer switches, while S5820V2-54QS-GE_5 (expressed as SW5) and S5820V2-54QS-GE_6 (expressed as SW6) are core layer switches. MSR36-20_7 (express as R1) is the router to connect the external network. No actual external network is designed because this paper focuses only on LAN design.

To guarantee reliable communication between these five VLANs, the network needs to configure link aggregation and VRRP among the convergence layer switches, and configure MSTP among Convergence layer and Access layer switches, avoiding data transfer loops and realizing load sharing. In this way, data can be transferred more reliably. The network can maintain routing information automatically by configuring OSPF-routing protocols in core layer switches and router, while simplifying manual configuration routing. Note that the link between g1/0/6 port of SW3 and g1/0/1 port of SW6 is backup link, whose cost is bigger than others, it works only when the link between g1/0/5 port of SW3 and g1/0/2 port of SW5 malfunctions. The link between g0/1/6 port of

SW4 and g0/1/2 port of SW5 is also backup link, the function is same as above link.

2.2.2 Device Configuration Solution

To avoid loops in data forwarding and provide link and device backup, a redundant connections is set up between SW3~SW4 and SW5~SW6, and five VRRP backup groups and link aggregation are set up between SW3 and SW4, and MSTP is set up among SW1~SW4. Thus, data can be transferred more reliably. After configuring the OSPF protocol among SW5~SW6 and R1, the IP addresses of each device are shown in Table 1.

Table 1. The IP address list

Device	Port	IP adress
Host_1	VirtualBox Host-Only Ethernet Adapter	192.168.1.2/24
Host_2	VirtualBox Host-Only Ethernet Adapter #2	192.168.2.2/24
Host_3	VirtualBox Host-Only Ethernet Adapter #3	192.168.3.2/24
Host_4	VirtualBox Host-Only Ethernet Adapter #4	192.168.4.2/24
Host_5	VirtualBox Host-Only Ethernet Adapter #5	192.168.5.2/24
SW3	vlan10	192.168.1.1/24
	vlan20	192.168.2.1/24
	vlan30	192.168.3.1/24
	vlan40	192.168.4.1/24
	vlan50	192.168.5.1/24
	vlan1000	172.16.1.1/24
	vlan1001	10.1.1.1/24
	virtual IP 1	192.168.1.254/24
	virtual IP 2	192.168.2.254/24
	virtual IP 3	192.168.3.254/24
	virtual IP 4	192.168.4.254/24
	virtual IP 5	192.168.5.254/24
SW4	vlan10	192.168.1.253/24
	vlan20	192.168.2.253/24
	vlan30	192.168.3.253/24
	vlan40	192.168.4.253/24
	vlan50	192.168.5.253/24
	vlan1002	10.1.2.1/24
	vlan1003	172.16.2.1/24
	virtual IP 1~5	同SW3
SW5	vlan1000	172.16.1.2/24
	vlan1002	10.1.2.2/24
	vlan1004	200.1.1.1/24
SW6	vlan1002	10.1.1.2/24
	vlan1003	172.16.2.2/24
	vlan1005	200.1.2.1/24
R1	GigabitEthernet0/0	200.1.1.2/24
	GigabitEthernet0/1	200.1.2.2/24

As show in Figure 2, the networking model includes the following device: Host_1~Host_5, SW1~SW6, R1. The configurations of SW1 and SW2 are similar, as are those of SW3 and SW4, SW5 and SW6. Taking the configurations of SW2, SW4 and SW6 as examples, the configuration process is explicitly stated below.

1. The Configuration of SW2

```
[H3C]sysname SW2
[SW2]vlan 30        # create vlan30, vlan40 and vlan50, and add relevant ports
[SW2-vlan30]port g1/0/1
[SW2-vlan30]vlan 40
[SW2-vlan40]port g1/0/2
[SW2-vlan40]vlan 50
[SW2-vlan50] port g1/0/3
[SW2-vlan50]quit
[SW2]interface g1/0/4    # configure g1/0/4 port as trunk port
[SW2-GigabitEthernet1/0/4]port link-type trunk
[SW2-GigabitEthernet1/0/4]port trunk permit vlan 30 40 50
[SW2-GigabitEthernet1/0/4]quit
[SW2]interface g1/0/5   # configure g1/0/5 port as trunk port
[SW2- GigabitEthernet1/0/5]port link-type trunk
[SW2- GigabitEthernet1/0/5]port trunk permit vlan 30 40 50
```

```
[SW2]stp region-configuration  # configure MSTP
[SW2-mst-region]region-name bf
[SW2-mst-region]instance 1 vlan 10 20
[SW2-mst-region]instance 2 vlan 30 40 50
[SW2-mst-region]active region-configuration
[SW2-mst-region]quit
```

2. The Configuration of SW4

```
[H3C]sysname SW4
[SW4]interface g1/0/1    # configure g1/0/1 port as trunk port
[SW4- GigabitEthernet1/0/1]port link-type trunk
[SW4- GigabitEthernet1/0/1]port trunk permit vlan 10 20
[SW4- GigabitEthernet1/0/1]quit
[SW4]interface g1/0/2    # configure g1/0/2 port as trunk port
[SW4- GigabitEthernet1/0/2]port link-type trunk
[SW4 GigabitEthernet1/0/2]port trunk permit vlan 30 40 50
[SW4- GigabitEthernet1/0/2]quit
[SW4]interface Bridge-Aggregation 1  # configure link aggregation
[SW4-Bridge-Aggregation1]quit
[SW4]interface g1/0/4
[SW4- GigabitEthernet1/0/4]port link-aggregation group 1
[SW4- GigabitEthernet1/0/4]quit
[SW4]interface g1/0/3
[SW4- GigabitEthernet1/0/3]port link-aggregation group 1
[SW4- GigabitEthernet1/0/3]quit
[SW4]interface Bridge-Aggregation 1
[SW4-Bridge-Aggregation1]port link-type trunk
[SW4-Bridge-Aggregation1]port trunk permit vlan all
[SW4-Bridge-Aggregation1]vlan 1002 #configure the IP address of vlan1002 and vlan1003 ports
[SW4-vlan1002]port g1/0/5
[SW4-vlan1002]interface vlan 1002
[SW4-Vlan-interface1002]ip address 10.10.2.1 24
[SW4-Vlan-interface1002]vlan 1003
[SW4-vlan1003]port g1/0/6
[SW4-vlan1003]interface vlan 1003
[SW4-Vlan-interface1003]ip address 172.16.2.1 24
[SW4] track 1 interface vlan-interface 1002 #create a track item 1, monitor the physical state of the uplink interface vlan-interface 1002
[SW4] track 2 interface vlan-interface 1003 #create a track item 2, monitor the physical state of the uplink interface vlan-interface 1003
[SW4]vlan 10  # configure vlan10, vlan20, vlan30, vlan40 and vlan50's gateway
[SW4-vlan10]interface vlan 10
[SW4-Vlan-interface10]ip address 192.168.1.253 24
[SW4-Vlan-interface10]vrrp vrid 1 virtual-ip 192.168.1.254  # create a backup group 1, and configure it's virtual IP address
[SW4]vlan 20
[SW4-vlan20]interface vlan 20
[SW4-Vlan-interface20]ip address 192.168.2.253 24
[SW4-Vlan-interface20]vrrp vrid 2 virtual-ip 192.168.2.254  # create a backup group 2, and configure it's virtual IP address
[SW4]vlan 30
[SW4-vlan30]interface vlan 30
[SW4-Vlan-interface30]ip address 192.168.3.253 24
[SW4-Vlan-interface30]vrrp vrid 3 virtual-ip 192.168.3.254  # create a backup group 3, and configure it's virtual IP address
[SW4-Vlan-interface30] vrrip vrid 3 priority 110
[SW4-Vlan-interface30] vrrip vrid 3 track 1 reduced 20  #when track item 1 status is negative SW4 in VRRP group 3 priority reduced by 20, so that the priority of SW3 is higher than SW4, SW4 becomes master gateway
[SW4-Vlan-interface30] vrrip vrid 3 track 2 reduced 20  #when track item 2 status is negative SW4 in VRRP group 3 priority is reduced by 20, so that the priority of SW3 is higher than SW4, SW4 becomes master gateway.
[SW4-Vlan-interface30]vlan 40
[SW4-vlan40]interface vlan 40
[SW4-Vlan-interface40] ip address 192.168.4.253 24
[SW4-Vlan-interface40]vrrp vrid 4 virtual-ip 192.168.4.254  # create a backup group 4, and configure it's virtual IP address
[SW4-Vlan-interface40] vrrip vrid 4 priority 110
[SW4-Vlan-interface40] vrrip vrid 4 track 1 reduced 20  #the function is same as VRRP backup group 3
[SW4-Vlan-interface40] vrrip vrid 4 track 2 reduced 20  #the function is same as VRRP backup group 3
[SW4-Vlan-interface40]vlan 50
[SW4- vlan50] interface vlan 50
[SW4-Vlan-interface50] ip address 192.168.5.253 24
[SW4-Vlan-interface50]vrrp vrid 5 virtual-ip 192.168.5.254  # create a backup group 5, and configure it's virtual IP address
[SW4-Vlan-interface50] vrrip vrid 5 priority 110
[SW4-Vlan-interface40] vrrip vrid 5 track 1 reduced 20  #the function is same as VRRP backup group 3
[SW4-Vlan-interface40] vrrip vrid 5 track 2 reduced 20  #the function is same as VRRP backup group 3
[SW4-Vlan-interface40]quit
```

```
[SW4]stp region-configuration   #configure MSTP
[SW4-mst-region]region-name bf
[SW4-mst-region]instance 1 vlan 10 20
[SW4-mst-region]instance 2 vlan 30 40 50
[SW4-mst-region]active region-configuration
[SW4-mst-region]quit
[SW4]stp instance 1 root secondary
[SW4]stp instance 2 root primary
[SW4]interface g1/0/5 #turn off STP function on the uplink interface
[SW4- GigabitEthernet1/0/5] undo stp enable
[SW4- GigabitEthernet1/0/5]quit
[SW4]interface g1/0/6
[SW4- GigabitEthernet1/0/6] undo stp enable
[SW4] ospf    # configure ospf protocol
[SW4-ospf-1] area 0
[SW4-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[SW4-ospf-1-area-0.0.0.0] network 172.16.2.0 0.0.0.255
[SW4-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SW4-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[SW4-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[SW4-ospf-1-area-0.0.0.0] network 192.168.4.0 0.0.0.255
[SW4-ospf-1-area-0.0.0.0] network 192.168.5.0 0.0.0.255
[SW4-ospf-1-area-0.0.0.0]quit
[SW4] interface vlan-interface 1002  #as the speed of each interface is 1000M, according to the ospf the cost of each interface value is 108 divided by 1000M(namely 0.1), interface g1 / 0/5 is configured to  backup interface, so its cost is set to a value greater than 0.1.
[SW4-Vlan-interface1002]ospf cost 5
```

3. The Configuration of SW6

```
[SW6]vlan 1001    # configure the IP address of vlan1001 port
[SW6-vlan1001]port g1/0/1
[SW6-vlan1001]interface vlan 1001
[SW6-Vlan-interface1001]ip address 10.1.1.2 24
[SW6-Vlan-interface1001]vlan 1003   # configure the IP address of vlan1003 port
[SW6-vlan1003]port g1/0/2
[SW6-vlan1003]interface vlan 1003
[SW6-Vlan-interface1003]ip address 172.16.2.2 24
[SW6-Vlan-interface1003]vlan 1005
[SW6-vlan1005]interface vlan 1005
[SW6-Vlan-interface1005] ip address 200.1.2.1 24
[SW6-Vlan-interface1005]quit
[SW6] ospf     # configure ospf protocol
[SW6-ospf-1] area 0
[SW6-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SW6-ospf-1-area-0.0.0.0] network 172.16.2.0 0.0.0.255
[SW6-ospf-1-area-0.0.0.0] network 200.1.2.0 0.0.0.255
```

4. The Configuration of R1

```
[H3C]sysname R1
[R1]interface g0/0   # configure the IP address of g0/0 port
[R1-GigabitEthernet0/0]port link-mode route
[R1-GigabitEthernet0/0]combo enable copper
[R1-GigabitEthernet0/0]ip address 200.1.1.2 24
[R1]interface g0/1   # configure the IP address of g0/1 port
[R1-GigabitEthernet0/1]port link-mode route
[R1-GigabitEthernet0/1]combo enable copper
[R1-GigabitEthernet0/1]ip address 200.1.2.2 24
[R1] ospf    # configure ospf protocol
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0] network 200.1.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0] network 200.1.2.0 0.0.0.255
```

5. The Configuration of hosts

hosts configuration is more complex in HCL simulator, the main configuration steps are as follows.

(1) Setting up the Oracle VM VirtualBox

Starting the Oracle VM VirtualBox, then opening “management” menu, selecting “global settings”, and then selecting “network” in the VirtualBox settings dialog, clicking “adding Host-Only network” button, adding four virtual network cards, and separately configuring IP address and mask, IP addresses are 192.168.1.2, 192.168.2.2, 192.168.3.2, 192.168.4.2, 192.168.5.2, their mask are 255.255.255.0.

(2) Starting HCL

Starting HCL, creating host, and then adding the connection, selecting different virtual network card for each host.

(3) Configuration gateway

Opening Network Center, and configuration gateway for each virtual network adapter, the gateway are separately 192.168.1.254, 192.168.2.254, 192.168.3.254, 192.168.4.254, 192.168.5.254.

3. Results Analysis

In order to verify whether this model can achieve reliable communication, OSPF protocol, MSTP, link aggregation and VRRP are verified and the results are analyzed as well in this section.

3.1 Verification and Analysis of MSTP and link aggregation

The link aggregation between SW3 and SW4 has improved network reliability at the price of generating link redundancy. This can cause loops in data transfer. MSTP can avoid this loop problem.

3.1.1 Verification and Analysis of MSTP

In the test, SW3 and SW4 work normally, MSTP is verified and analyzed.

Step 1. Check the state of the spanning tree on SW1.

As shown in Table 2. MSTP generates two examples, with MSTID equal to 0 and 1, respectively. In Example 1, the role of GigabitEthernet1/0/4(namely g1/0/4) port is ALTE, i.e., a blocked port.

Table 2. The state of the spanning tree on SW1

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/3	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/4	DESI	FORWARDING	NONE
1	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
1	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
1	GigabitEthernet1/0/3	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/4	ALTE	DISCARDING	NONE

Step 2. Check the state of spanning tree on SW2.

The state of spanning tree on SW2 as shown in Table 3, MSTP generates two examples, with MSTID equal to 0 and 2, respectively. In Example 0, the role of GigabitEthernet1/0/5 port is ALTE, i.e., a blocked port.

Table 3. The state of the spanning tree on SW2

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/3	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/4	ROOT	FORWARDING	NONE
0	GigabitEthernet1/0/5	ALTE	DISCADING	NONE
2	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
2	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
2	GigabitEthernet1/0/3	DESI	FORWARDING	NONE
2	GigabitEthernet1/0/4	ALTE	DISCADING	NONE
2	GigabitEthernet1/0/5	ROOT	FORWARDING	NONE
2	GigabitEthernet1/0/1	DESI	FORWARDING	NONE

Step 3. Check the state of spanning tree on SW3.

It follows from Table 2 that MSTP Example 1 includes SW1, SW3 and SW4, in which GigabitEthernet1/0/3 of SW1 is the root port, GigabitEthernet1/0/4 is ALTE port, to realize the forwarding data transfer, and other ports must be forwarding ports. As shown by the state of the spanning tree on SW3 in Table 4, the roles of all ports are either DESI or ROOT, i.e., forwarding ports.

Table 4. The state of the spanning tree on SW3

MSTID	Port	Role	STP State	Protection
0	Bridge-Aggregation1	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/1	ROOT	FORWARDING	NONE
0	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
1	Bridge-Aggregation1	DESI	FORWARDING	NONE
1	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
2	Bridge-Aggregation1	DESI	FORWARDING	NONE

2	GigabitEthernet1/0/2	DESI	FORWARDING	NONE

Step 4. Check the state of spanning tree on SW4

Table 3 shows the results of MSTP Example 2, and includes SW2, SW3 and SW4, in which Bridge-Aggregation1 of SW4 and GigabitEthernet1/0/5 of SW2 are the root ports, GigabitEthernet1/0/4 is the ALTE port. To implement the forwarding of data traffic, other ports must be forwarding ports. Looking into the states of spanning tree on SW4, as shown in Table 5, it shows that all ports are forwarding ports.

Table 5. The state of the spanning tree on SW4

MSTID	Port	Role	STP State	Protection
0	Bridge-Aggregation1	ROOT	FORWARDING	NONE
0	GigabitEthernet1/0/1	ALTE	DISCARDING	NONE
0	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
1	Bridge-Aggregation1	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/1	ALTE	DISCARDING	NONE
2	Bridge-Aggregation1	DESI	FORWARDING	NONE
2	GigabitEthernet1/0/2	DESI	FORWARDING	NONE

As shown from Table 2 to Table 5, MSTP Example 0 includes SW1, SW2, SW3 and SW4, its configuration can be found from the network models in Figure 2, Table 2, where GigabitEthernet1/0/5 port of SW2 is blocked ports. As such, this configuration forwards no data traffic and avoids data transfer loops.

3.1.2 Verification and Analysis of link aggregation

In the test, we assumed that SW4 Malfunctions, SW3 works normally. Namely the link aggregation port g1/0/4 of SW3 was shut down, and the information of the aggregation group is checked. As shown in Table 6, it is found that the state of GigabitEthernet1/0/4 port is “U”, i.e., in an unselected state, meaning it does not work. It can be shown from Table 7 that Host_5 can ping Host_1, indicating that link aggregation works and one line failure does not affect communication.

Table 6. The information of the link aggregation group

MSTID	Port	Role	STP State	Protection
0	Bridge-Aggregation1	ROOT	FORWARDING	NONE
0	GigabitEthernet1/0/1	ALTE	DISCARDING	NONE
0	GigabitEthernet1/0/2	DESI	FORWARDING	NONE
1	Bridge-Aggregation1	ROOT	FORWARDING	NONE
1	GigabitEthernet1/0/1	ALTE	DISCARDING	NONE
2	Bridge-Aggregation1	DESI	FORWARDING	NONE
2	GigabitEthernet1/0/2	DESI	FORWARDING	NONE

Table 7. The packets statistics information from pinging Host_1 with Host_5

value of parameter	packets sequence			
	1	2	3	4
ttl	127	127	127	127
times, ms	10ms	3ms	3ms	3ms

3.2 Verification and Analysis of VRRP

3.2.1 Analysis the VRRP Information when SW3 and SW4 Work Normally

The VRRP on SW3 and SW4 works if the link aggregation malfunctions between them. When SW3 and SW4 worked normally, the VRRP information on SW3 and SW4 was checked and reorganized, the import information are separately as shown Table 8 and Table 9. As shown in Table 11 and Table 12, five backup groups are created on SW3 and SW4, their virtual IP address are 192.168.1.254, 192.168.3.254, 192.168.4.254, 192.168.5.254, SW3 is the Master gateway and SW4 is the Backup gateway of VLAN 10, and 20, and SW4 is the Master gateway and SW3 is the Backup gateway of VLAN 30, 40 and 50.

Table 8. The import VRRP information on SW3

VRID	Admin Status	State	Config Pri	Preempt Mode
1	Up	Master	110	Yes
2	Up	Master	110	Yes
3	Up	Backup	100	Yes
4	Up	Backup	100	Yes
5	Up	Backup	100	Yes

Table 9. The import VRRP information on SW4

VRID	Admin Status	State	Config Pri	Preempt Mode
1	Up	Backup	100	Yes
2	Up	Backup	100	Yes
3	Up	Master	110	Yes
4	Up	Master	110	Yes
5	Up	Master	110	Yes

3.2.2 SW3 Malfunctions, SW4 Works Normally

In this test, SW3 was closed, and the VRRP information was checked on SW4, the import information are as shown Table 10. AS shown in Table 10, instead of SW3, SW4 become Master gateway of all VLANs, which shows SW3 failure does not affect network communication, and improves the network reliability.

Table 10. The import VRRP information on SW4 when SW3 malfunctions

VRID	Admin Status	State	Config Pri	Preempt Mode
1	Up	Master	100	Yes
2	Up	Master	100	Yes
3	Up	Master	110	Yes
4	Up	Master	110	Yes
5	Up	Master	110	Yes

3.3 Verification and Analysis of OSPF Protocol

3.3.1 Ping between devices

By configuring the OSPF protocol among SW3~SW6, R1, each node could ping each other individually. Taking SW3 and R1 as examples (the others are similar), the results for pinging g0/1 port of R1 with SW3 are shown in Table 11. This demonstrates that SW3 could ping R1, and that the packet loss is 0.00%, which indicates OSPF protocol works normally.

Table 11. The packets statistics information from pinging R1 with SW3

value of the parameter	packets sequence				
	0	1	2	3	4
Bytes	56	56	56	56	56
Ttl	255	255	255	255	255
times, ms	1.365	1.115	1.619	1.096	1.885
packets transmitted	5				
packets received	5				
packets loss, %	0.00				

3.3.2 Analysis of the link performance

When g1/0/5 and g0/1/6 ports of SW3 work normally, the ospf routing is checked, and the main information is shown in Table 3. As shown in Table 12, the next hop of SW3 reaching destination 200.1.2.0/24 is 172.16.1.2, and cost is 2, namely

SW3 transmits packets from g1/0/5 port, through g1/0/3 port of SW5, and g0/1 port of R1, finally reaches the destination.

Table 12. The main ospf routing information

Destination	Cost	Type	NexHop	AdvRouter	Area
200.1.1.0/24	2	Transit	172.16.1.2	200.1.1.1	0.0.0.0
200.1.2.0/24	3	Transit	172.16.1.2	200.1.2.1	0.0.0.0
172.16.1.0/24	1	Transit	0.0.0.0	200.1.1.1	0.0.0.0
172.16.2.0/24	2	Stub	192.168.1.253	192.168.5.253	0.0.0.0
10.1.1.0/24	5	Transit	0.0.0.0	200.1.2.1	0.0.0.0
10.1.2.0/24	2	Stub	172.16.1.2	200.1.1.1	0.0.0.0

To check the reliability of backup link, in this test, g1/0/5 port of SW3 is shut down, the ospf routing is checked, and the main information is shown in Table 13. As shown in Table 4, because of g1/0/5 port is shut down, namely the link is down, compared with Table 12, the routing of reaching to destination 172.16.1.0/24 is lost, and the next hop of SW3 reaching destination 200.1.2.0/24 is 10.1.1.2, namely SW3 transmits the packet from g1/0/6 port, through g1/0/1 and g1/0/3 ports of SW6, finally reaches the destination.

Table 13. The main ospf routing information when the g1/0/5 is shut down

Destination	Cost	Type	NexHop	AdvRouter	Area
200.1.1.0/24	2	Transit	172.16.1.2	200.1.1.1	0.0.0.0
200.1.2.0/24	3	Transit	172.16.1.2	200.1.2.1	0.0.0.0
172.16.1.0/24	1	Transit	0.0.0.0	200.1.1.1	0.0.0.0
172.16.2.0/24	2	Stub	192.168.1.253	192.168.5.253	0.0.0.0
10.1.1.0/24	5	Transit	0.0.0.0	200.1.2.1	0.0.0.0
10.1.2.0/24	2	Stub	172.16.1.2	200.1.1.1	0.0.0.0

4. Verification communication between hosts and R1 by Ping

The above analysis shows the network model shown in Figure 2 has better reliability, Table 14 shows hosts and g0/1 port of R1 ping time, which shows they may communicate each other.

Table 14. The packets statistics information from pinging R1 with hosts

ping time,ms	packets sequence			
	1	2	3	4
Host_1 ping R1	5	2	2	2
Host_2 ping R1	3	2	3	2
Host_3 ping R1	4	3	2	2
Host_4 ping R1	8	3	3	3
Host_5 ping R1	5	2	3	3

4. Conclusions

Multiple two-layer or three-layer switches have been widely used in large-scale LAN planning and design. The key pedagogical issues in network planning and design courses are the division of VLANs and how to ensure reliable communication. In this paper, HCL simulator has been used to build a three-layer structure large-scale LAN model based mesh topology, and MSTP, link aggregation, VRRP, ospf have been applied to the model, which has broken up the reliable technologies into smaller pieces for students to understand, and help the students to observe and discover potential problems more easily. Future work will study the security of the network.

Acknowledgements

This work was supported by the Heilongjiang Nature Science Foundation of China (No. F201212), Qiqihar university young teachers' scientific research started to support projects foundation (2011 k - M05), Qiqihar Science and Technology Bureau of industrial projects foundation (GYGG-201315, GYZD-2013007), Heilongjiang Education Science "Twelfth Five Year Plan"(GBC1213078) , and Qiqihar University education and scientific research project (2014018).

References

1. Jadperneite, J., Neumann, P. (2001) Performance Evaluation of Switched Ethernet in Real-Time Applications. *Proc. Conf. on*

Fieldbus Systems and their Applications, Nancy, France, p.p. 141-151.

2. D.W. Pritty, J.R. Malone, D.N. Smeed, S. K. Banerjee, N.L. Lawrie (1995) A Real-Time Upgrade for Ethernet Based Factory Networking. *Proc. Conf. on Industrial Electronics, Control, and Instrumentation*, Orlando, FL, USA, p.p. 1631-1637.
3. Mathias Hein, David Griffiths, Orna Berry. (1996) Switching technology in the local network: From LAN to switched LAN to virtual LAN. Thomson Executive: Cincinnati.
4. GilbertHeld (2003) Ethernet Networks: Design, Implementation Operation, Management. John Wiley& Sons, Ltd.: England.
5. Jose A Ventura, Xiaohua Weng (1993) A new method for constructing minimal broadcast networks. *Networks*, 23(5), p.p.481-497.
6. Steven S King, Stephen Saunders (1995) Virtual LANs Get Real. *Data Communications*, 24(3), p.p. 87-100.
7. Matthew Bocci, Ian Cowburn, Jim Guillet, Alcatel-Lucent (2008) Network High Availability for Ethernet Services Using IP/MPLS Networks. *IEEE Communications Magazine*, 46(3), p.p. 90-96.
8. Farhad Faghani, Ghasem Mirjalily.(2009) An Analytic Comparison of Shortcut Switching Strategy and Spanning Tree Protocol. *Proc. Conf. on International Colloquium Computing Communication Control Management*, Hubei, China p.p. 619-623.
9. K.H. Yeung, F. Yan, T.C. Leung (2006) Improving Network Infrastructure Security by Partitioning Networks Running Spanning Tree Protocol. *Proc. Conf. on Internet Surveillance and Protection*. Cap Esterel, Cote d'Azur, France p.p.19.
10. Jen-Hao Kuo, Siong-Ui. Te.(2006) An Evaluation of the Virtual Router Redundancy Protocol Extention with Load Balancing. *Proc. Conf. on Pacific Rim International Symposium on Dependable Computing*, Changsha, China, p.p. 133-139.
11. Zhang Tengyu. (2014) Analysis and application of simulation teaching mode based Multisim. *Computer Simulation*, 31(6), p.p. 230-232.