Network-Level Redundancy for Campus LAN

Khaing Khaing Wai

Department of Information Technology Support and Maintenance, University of Computer Studies, Mandalay, Myanmar

How to cite this paper: Khaing Khaing Wai "Network-Level Redundancy for Campus LAN" Published in International Journal of Trend in Scientific Research and Development (IJTSRD), ISSN: 2456-6470, Volume 3 | Issue 5, August 2019, pp.1738-1743, https://doi.org/10.31142/ijtsrd26768

Copyright © 2019 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0/)

1. INTRODUCTION

The sole concept of network redundancy is to provide alternate and efficient paths for data to travel along in case a cable is broken or a connector accidentally unplugged. Ethernet as standard does not have rings or loops in the network because it will cause broadcast storms and can ultimately cause the network to stop functioning. To withstand with redundancy, network building structure mainly the switches and routers [6] used in the network must support redundancy protocols designed to avoid the usual problems of putting loops into a network.

Today, business requires reliable network connectivity and access to corporate resources. Connections to and from business units, vendors and SOHOs are all equally important to keep the continuity when needed. Business runs all day, every day and even in off hours. Most companies run operations around the clock, seven days a week so it's important to realize that to keep a solid business continuity strategy, redundancy technologies should be considered and should be implemented [3].

Network redundancy is a simple concept to understand. If you have a single point of failure and it fails you, then you have nothing to rely on. If you put in a secondary (or tertiary) method of access, then when the main connection goes down, you will have a way to connect to resources and keep the business operational [5].

The purpose of this system is to build the redundancy system. Redundancy means that there are backup components in place to ensure that if a networking card, power supply, or Ethernet cable fails, your business will not suffer because a source is in place to take over if the primary source fails [6]. Another term used to describe redundancy is high availability, because of the increased availability to your resources. We have achieved redundancy by ensuring your server has everything that it needs (including power and network source). So in the case of networking, a redundant connection would include two Ethernet cables going to two separate routers from two separate network cards connecting to our backbone ISP providers.

The more common approach a highly available directory service is to use redundant server components. Redundant solutions are usually less expensive, easier to implement, and easier to manage. During a failure, a redundant system might provide poor availability. Imagine, for example, an environment in which the load is shared between two redundant server components. The failure of one server component might put an excessive load on the other server, making this server respond more slowly to client requests.

A slow response might be considered a failure for clients that rely on quick response times. In other words, the availability of the service, even though the service is operational, might not meet the availability requirements of the client.

2. PROPOSED SYSTEM

Figure 1 shows infrastructure design for campus buildings. The campus A is running ether channels and redundancy protocols. At the upper edge routes are running NAT and they can connect to the outside internet. In the campus B, we use the VoIP phones and it can communicate with the other networks in the redundancy campus.
3. IMPLEMENTATION

In this design, four Cisco 1900 series routers, four Cisco 2960 series switches, personal computers (PCs), two IP phones are used as main networking components. Gateway Load Balancing Protocol (GLBP) is used for redundancy. Ether channel is a form of link aggregation used in switched networks. It also provides redundancy because the overall link is viewed as a logical connection by Spanning Tree Protocol (STP). If one physical link within channel goes down, this does not cause a change in the topology and does not require STP recalculation. RPVST+ supports RPVST+ and works as IEEE 802.1q and Vlan VTPs and RPVST+ are used to avoid the loop among switches. In this system OSPF protocol is used to route and to get connections between the different networks. NAT is also used the system to connect with outside network.

3.1 Redundancy Configuration

R02(config)#interface g0/1
R02(config-if)#glbp 1 ip 192.168.1.254
R02(config-if)#glbp 1 preempt
R02(config-if)#glbp 1 priority 150
R02(config-if)#glbp 1 load-balancing round-robin
R03(config)#interface g0/0
R03(config-if)#glbp 1 ip 192.168.1.254

3.2 EtherChannel Configuration on Switches

SW01(config)#interface range f0/3-4
SW01(config-if)#shutdown
SW01(config-if)#channel-group 1 mode desirable
SW01(config-if)#no shut
SW01(config-if)#interface port-channel 1
SW01(config-if)#switchport mode trunk
SW01(config-if)#interface range f0/5-6
SW01(config-if)#shutdown
SW01(config-if)#channel-group 3 mode desirable
SW01(config-if)#no shut
SW01(config-if)#interface port-channel 3
SW02(config-if)#switchport mode trunk

SW02(config)#interface range f0/3-4
SW02(config-if)#shutdown
SW02(config-if)#channel-group 1 mode desirable
SW02(config-if)#no shut
SW02(config-if)#interface port-channel 1
SW02(config-if)#switchport mode trunk

SW03(config)#interface range f0/1-2
SW03(config-if)#shutdown
SW03(config-if)#channel-group 2 mode desirable
SW03(config-if)#no shut
SW03(config-if)#interface port-channel 2
SW03(config-if)#switchport mode trunk
SW03(config)#interface range f0/5-6
SW03(config-if)#shutdown
SW03(config-if)#channel-group 3 mode desirable
SW03(config-if)#no shut
SW03(config-if)#interface port-channel 3
SW03(config-if)#switchport mode trunk

3.3 OSPF Configuration on Routers

R01(config)#router ospf 10
R01(config-router)#router-id 1.1.1
R01(config-router)#log-adjacency-changes
R01(config-router)#network 192.168.3.0 0.0.0.255 area 0
R01(config-router)#network 192.168.2.0 0.0.0.255 area 0
R01(config-router)#network 192.168.10.0 0.0.0.255 area0
R01(config-router)#network 192.168.11.0 0.0.0.255 area0
R01(config-router)#network 192.168.12.0 0.0.0.255 area0
R01(config-router)#network 203.81.64.192 0.0.0.7 area 0

R02(config)#router ospf 10
R02(config-router)#router-id 2.2.2.2
R02(config-router)#log-adjacency-changes
R02(config-router)#network 192.168.2.0 0.0.0.255 area 0
R02(config-router)#network 192.168.4.0 0.0.0.255 area 0
R02(config-router)#network 192.168.10.0 0.0.0.255 area0
R02(config-router)#network 192.168.11.0 0.0.0.255 area0
R02(config-router)#network 192.168.12.0 0.0.0.255 area0
R03(config)#router ospf 10
R03(config-router)#router-id 3.3.3.3
R03(config-router)#log-adjacency-changes
R03(config-router)#network 192.168.3.0 0.0.0.255 area 0
R03(config-router)#network 192.168.4.0 0.0.0.255 area 0
R03(config-router)#network 192.168.10.0 0.0.0.255 area0
R03(config-router)#network 192.168.11.0 0.0.0.255 area0
R03(config-router)#network 192.168.12.0 0.0.0.255 area0

3.4 VoIP Services Configuration

R04(config)#telephony-service
R04(config-telephony)#max-ephones 5
R04(config-telephony)#max-dn5
R04(config-telephony)#ip source-address 192.168.11 port 2000
R04(config-telephony)#auto assign 1 to 9
R04(config-ephone-dn)#number 100
R04(config-ephone-dn)#number 200
R04(config-ephone-dn)#number 300
R04(config)#ip nat inside source list 1 interface Serial0/1/0 overload
R01(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1/0

3.5 NAT Configuration
R01(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R01(config)# interface GigabitEthernet0/1
R01(config-if)# ip address 192.168.3.1 255.255.255.0
R01(config-if)# ip nat inside
R01(config)# interface GigabitEthernet0/0
R01(config-if)# ip address 192.168.2.1 255.255.255.0
R01(config-if)# ip nat inside
R01(config)# interface Serial0/1/0
R01(config-if)# ip address 203.81.64.193 255.255.255.248
R01(config-if)# ip nat outside
R04(config)# interface GigabitEthernet0/0
R04(config-if)# ip address 192.168.1.1 255.255.255.0
R04(config-if)# ip nat inside
R04(config)# interface Serial0/1/0
R04(config-if)# ip address 203.81.64.194 255.255.255.248

3.6 RPVST+ Configuration on Switches
SW01(config)# spanning-tree mode rapid-pvst
SW01(config)# spanning-tree vlan 10 root primary
SW01(config)# spanning-tree vlan 11-13 root secondary
SW01(config)# spanning-tree mode rapid-pvst
SW02(config)# spanning-tree vlan 11 root primary
SW02(config)# spanning-tree vlan 10,12,13 root secondary
SW02(config)# spanning-tree mode rapid-pvst
SW03(config)# spanning-tree vlan 12 root primary
SW03(config)# spanning-tree vlan 10,11,13 root secondary

3.7 Testing Result
The following figures show the result for the system.

Figure 2. Ether channel Testing in Switch SW01

Figure 3. Ether channel Testing in Switch SW02
Figure 4. Ether channel Testing in Switch SW03

Figure 5. OSPF Testing on Cisco Router 01
### Figure 6. Testing Result for VLAN

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>active</td>
<td>Fa0/0, Fa0/5, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Gi0/1, Gi0/2, Gi0/5, Gi0/6, Gi0/7</td>
</tr>
<tr>
<td>10 Teacher</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>11 Student</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>12 Staff</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1005 trnet-default</td>
<td>active</td>
<td></td>
</tr>
</tbody>
</table>

### Figure 7. Redundancy Protocol GLBP Testing

GigabitEthernet0/1 - Group 1
State is Standby
10 state changes, last state change 00:07:52
Virtual IP address is 192.168.4.3
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.264 secs
Redirect time 600 sec, forwarder timeout 14400 sec
Preemption disabled
Active is 192.168.4.1, priority 150 (expires in 8.480 sec)
Standby is local
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
- cccf.484f.5a61 (192.168.4.1)
- f872.ea57.e9a1 (192.168.4.2) local
There are 2 forwarders (1 active)

Forwarder 1
State is Active
5 state changes, last state change 00:08:22
MAC address is 0007.b400.0101 (default)
Owner ID is f872.ea57.e9a1
Preemption enabled, min delay 30 sec
Active is local, weighting 100

Forwarder 2
State is Listen
5 state changes, last state change 00:08:02
MAC address is 0007.b400.0102 (learned)
Owner ID is cccf.484f.5a61
Time to live: 14397.952 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 192.168.4.1 (primary), weighting 100 (expires in 9.536 sec)
4. CONCLUSION
Redundant devices, such as multilayer switches or routers, provide the capability for a client to use an alternate default gateway when the primary default gateway fails. First Host Redundancy protocols, such as HSRP, VRRP, and GLBP provide alternate default gateways for hosts in the redundant router or multilayer switched environment. In this system, a network redundancy is a key factor to consider for maintaining network reliability. So, Layer 3 redundancy will be needed to consider to ensure that hosts maintain connectivity in the event of link failure of one device serving as a default gateway for a VLAN or set of VLANs.

5. REFERENCES