

AUTO DEFAULT GATEWAY SETTINGS FOR VIRTUAL MACHINES IN SERVERS USING DEFAULT GATEWAY WEIGHT SETTINGS PROTOCOL (DGW)

Suman Dutta¹, Shouman Barua² and Jishu Sen³

¹IT Trainer, Logitrain.com.au

² PhD research student. University of Technology, Sydney

³ MSc research student. University of Technology, Sydney.

ABSTRACT

Availability is one of the most important concerns in the networking world. For any high available network, we need to maintain 99.99999% availability. That is why it is one of the most important factors to find out the single point of failure in the network architecture and eliminate that single point of failure (SPOF) from physical network and logical network. SPOF in our server infrastructure has been analysed in terms of communicating with the router for forwarding traffic with multiple routers. We have developed an algorithm that will automatically select default gateway into the network interface card of virtual machines. The proposed algorithm will automatically enable Default Gateway Weight settings (DGW) protocol among routers by configuring Network interface card with default gateway of all routers. The proposed protocol works based on weight settings for the multiple default gateway configuration in the host. There will be heartbeat communication and re-convergence will be performed within the shortest possible time. Lowest weight setting will select the path for packet forwarding through specified routers related with the default gateway from the virtual machine.

KEYWORDS

DGW protocol, Auto default gateway, Virtual Machine, High Availability, Weight settings.

1. INTRODUCTION

Virtual machine is the integral part to work as a server for different applications. In order to provide high availability for the virtual machine traffic, we can use network interface card (NIC) teaming switch independent mode for virtual network adapter of virtual machines. Virtual network interface card of virtual machines will work with automated default gateway settings using weight configuration among the virtual network adapter which will provide high availability among the virtual machines for application that will run into virtual machine. We will use an algorithm that will run with the protocol to converge the network with virtual machines for achieving high resiliency with multiple router and will resolve the problem of single point of failure. To implement our high reliability with virtual machines through automatic default gateway settings, we will use many networking and server virtualization concepts.

2. CONCEPT OF VIRTUALIZATION

Through the last decade, the enterprise data centre infrastructure design has been changed in a large scale to provide multifarious services. It is now an integral part of data centres to provide services to numerous clients including roaming devices, who are not only connected to the data centre from internal network of organization, but also connected from other geographic locations outside the organization. It means that organizations now need to provide much higher levels of availability and redundancy for internal services which will be accessed from the internet. Successful organizations generally can adapt rapidly to change business requirements, and can attain the high availability and resiliency.

2.1. High Availability with virtualization

The enterprise data centre provides services to different of potential clients, including organization employees who are internal and external, customers and business partners. From any place and at any time, the clients may need to access the data center service. Because of this, the most pivotal task is to make the service highly available and responsive. In the case of a service outage due to the network failure, it is very critical that the service can be restored within a shortest possible time frame.

To provide a highly availability, it is noteworthy that the system can failover or recover from the loss of any single component of the network. The system should be able to detect whenever a component will fail and there should be a mechanism to automatically restore from that failure. Generally, this is achieved by shifting the services from the failed component to a redundant component. It is also important that this failover should be happened automatically and that it does not require administrative attention or effort. But running Virtual machines for providing different services using multifarious applications subject to the constraint of high availability.

2.2. Virtual Switch

A virtual switch is a software program that works like a physical Ethernet switch that allows multiple virtual machines (VM) to inter communicate with each other. There is a difference between physical Ethernet switch and a virtual switch. Virtual switch is not only forward data packets, but it can intelligently direct communication on the network by inspecting packets before passing through the network. Few vendors has embedded virtual switches right into the virtualization software, but a virtual switch can also be included in a server's hardware as a firmware. Because of its intelligence, virtual switch can ensure the integrity of a VM profile that includes network and security settings.

2.3. NIC teaming

In NIC teaming solution, multiple physical network adapters are connected to the NIC Teaming solution-multiplexing unit. This multiplexing unit presents one or more virtual adapters, which is also known as team network adapters to the operating system. There are different algorithms, which distribute inbound and outbound traffic between the physical network adapters. In non-Microsoft NIC Teaming solutions allows the team network adapters to divide traffic based on virtual local area network (VLAN) so that applications can connect to different VLANs.

2.4. Default Gateway

In computer networking, a default **gateway** is a router on a network, which serves as an access point to another network through which computers from a LAN network can communicate with outside world. In home computing network configurations, an ISP provides a physical device that both connects local network to the Internet and serves as a gateway. Such devices are digital subscriber line (DSL) routers and cable routers.

In organizational network infrastructure, a gateway is a node, which is used to routes the data packet from a workstation of one network to another network. The default gateway generally connects the internal networks and the outside network i.e., internet.

2.5. Requirements for Redundant Default Gateway Settings

When a host needs to communicate with a device on its local subnet, it needs to generate a broadcast message throughout the subnet which is an Address Resolution Protocol (ARP) request and wait for the unicast address resolution protocol reply and exchange packets. However, if the destination device is located on a different subnet then the sending device depends on an intermediate system (a router, for example) to forward packets to and from that subnet.

A sending workstation identifies its nearest router, which is also known as the default gateway or next hop, by its IP address. If the sending device comprehends something about routing, it considers that all packets destined off-net must be sent to the gateway's media access control (MAC) address instead of the other end's MAC address. Therefore, the sending device first sends an address resolution protocol (ARP) request to find the default gateway's MAC address. Then packets can be sent to the default gateway directly without looking for ARP entries for individual destinations which has been illustrated in Figure 1.

If the default gateway router becomes down, then hosts cannot communicate with the networks that is connected with the router. To avoid single point of failure, we can implement another default gateway within the same subnet to eliminate single point of failure that has been illustrated in Figure 2.

But there is a problem with this type of settings. If one router goes down, then we have to manually change the default gateway in the client PC's to forward packet through another default gateway router within the same LAN. To avoid this problem, we use our algorithm with new protocol default gateway weight settings (DGW).

2.6. Existing protocol that are used for redundant default gateway:

Hot standby router protocol is one of the protocol (HSRP) that is used to operate with an active/standby model. Two routers cooperate with each other using HSRP protocol to act as a default router. However, only one protocol will work as a default gateway at any time to actively support the end user traffic. The active router will carry the end user traffic for the other network. Then the other routers of the HSRP protocol will be in stand by state. It will wait to take over the control from the active router if active router face any problem which has been showed in Figure 3.

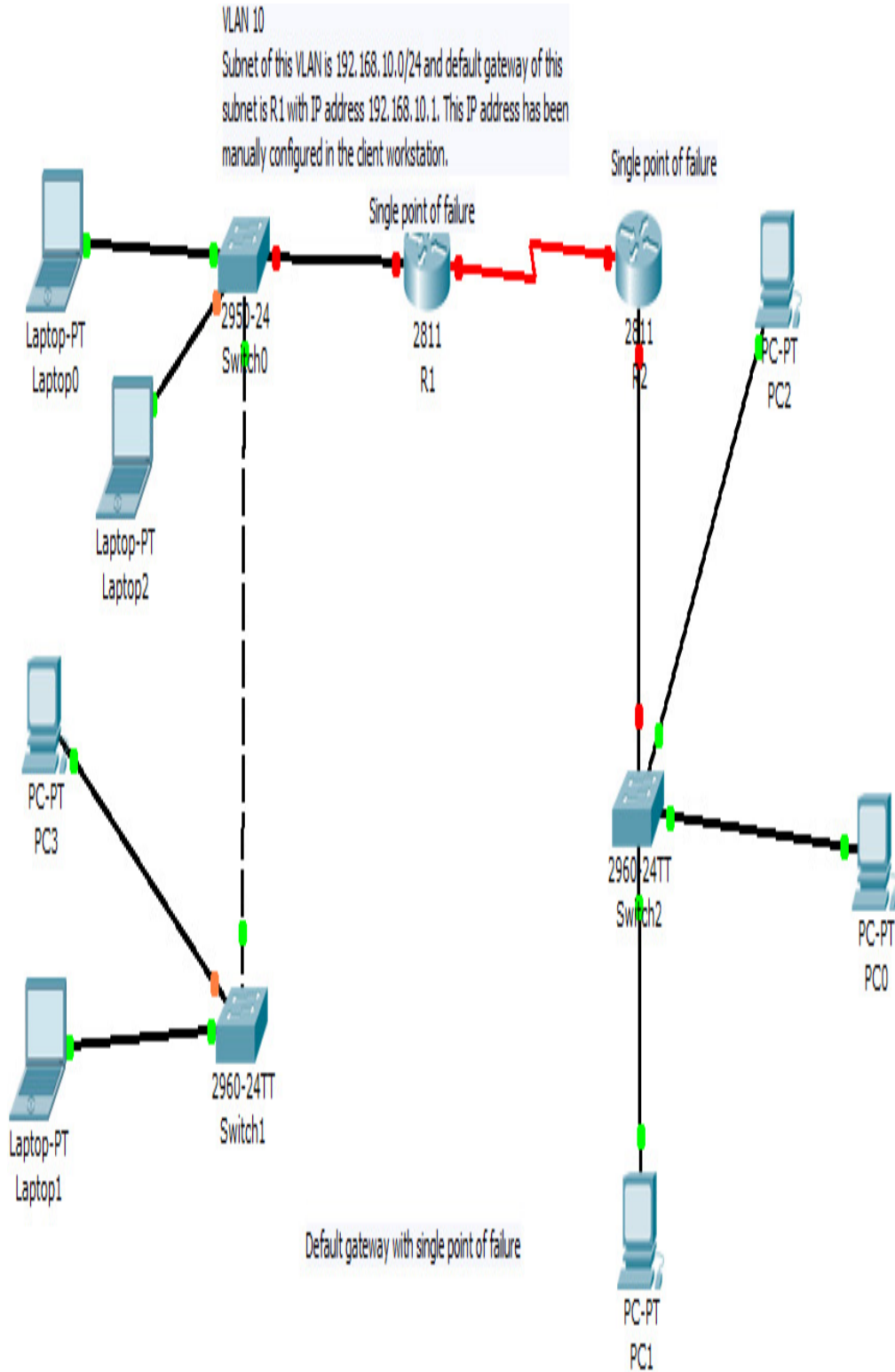


Figure 1: Default gateway with single point of failure

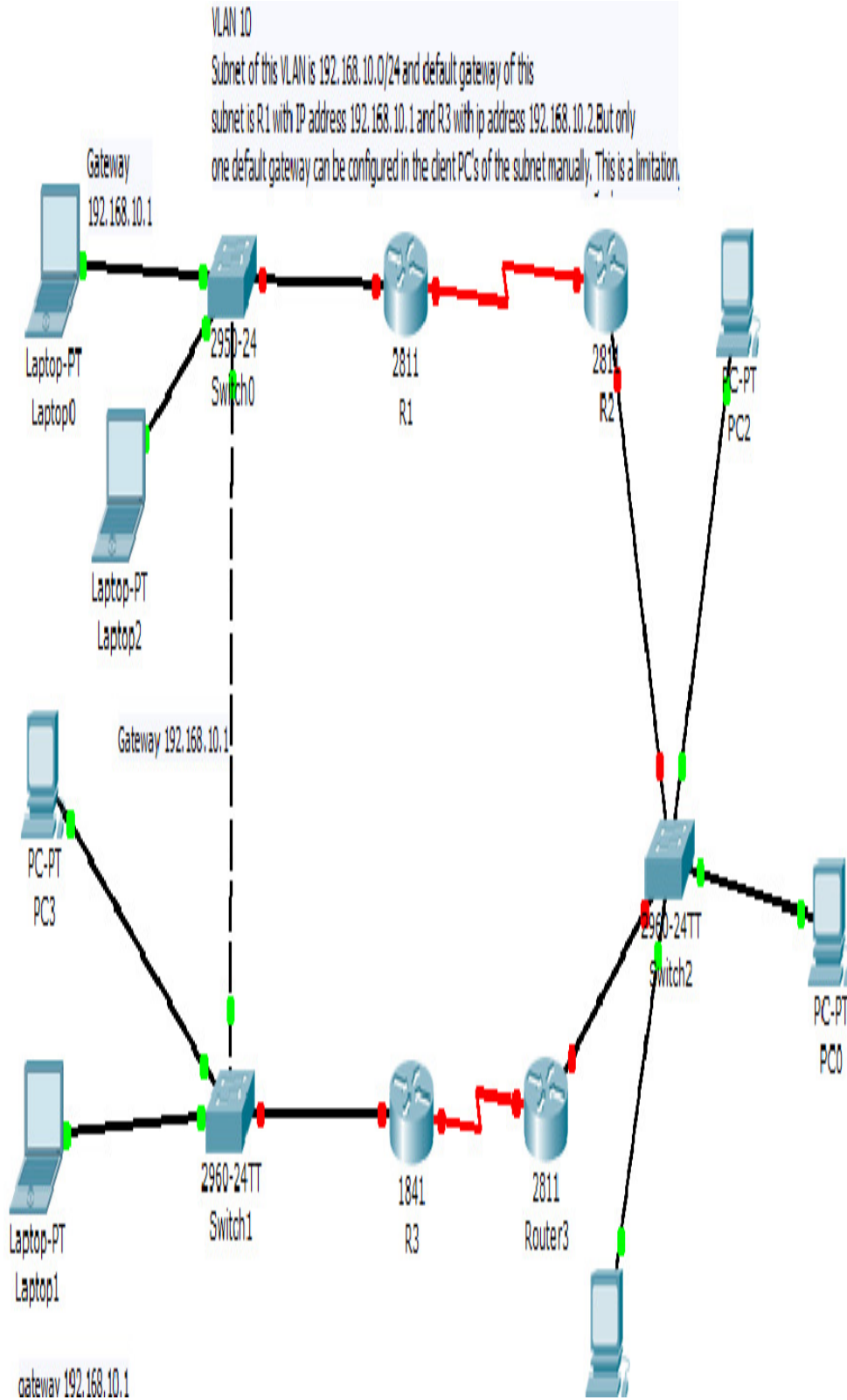


Figure 2: Redundant default gateway with manual default configuration

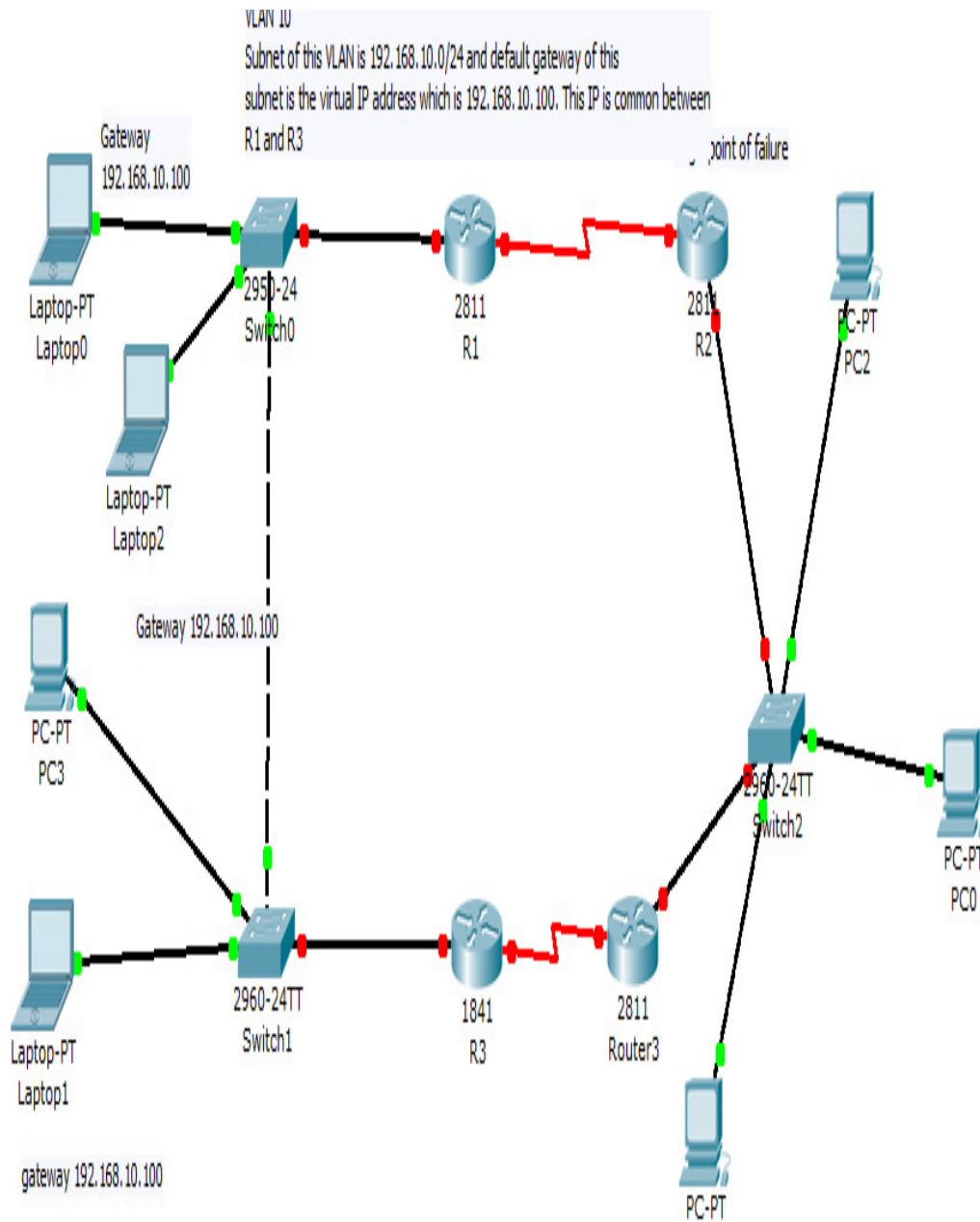


Figure 3: Default gateway with HSRP protocol

The HSRP protocol works with the virtual IP address. Active router controls the virtual IP address. This virtual IP address is part of the HSRP configuration. This IP address is the additional address in the fast Ethernet interface of the active and standby routers. All the IP address belongs to the same subnet. The router then automatically creates virtual MAC address. All the co-operating HSRP routers know these virtual address, but only active default gateway will use virtual IP address at any one point of time.

2.7. DGW protocol

DGW protocol needs to be enabled into the routers Fast Ethernet interface that is connected with the local area network (LAN) switch. The number of routers that would be connected with the LAN switch should be minimum two. Host Server will be connected with switch thorough multiple network interface cards. All network interface cards should be combined together to form virtual network adapter, which is also known as the NIC teaming to provide the fault tolerance and high availability for the server.

The server is running with hypervisor where multiple virtual machine can be configured for different service. To implement our protocol for automatic default gateway, all IP address should be configured within a single subnet of all virtual machines and routers Ethernet interface of the LAN which has been showed in Figure 4.

On the network interface card of virtual machine, we need to configure the options for our DGW protocol for Ethernet interface that needs to be performed with the driver software update of different vendor specified network interface card.

When we enable our protocol into the router Ethernet interface and virtual machine Ethernet interface, this will generate a multicast hello message within that subnet using the default multicast address 224.254.254.254. With this hello messages routers will send their LAN interface IP address configuration. Every router will analyze the hello messages to identify whether all IP address of the routers belong to the same subnet in the LAN network. Using the multicast message, DGW protocol will work between the routers. DGW protocol will select only one active router and standby routers based on the uptime of routers. Uptime will be calculated from the routers. The routers with the highest uptime will become the active router and weight will be set to 0 and for the standby routers weight will be set according to the chronological orders. For example 1, 2, 3...etc. Now this auto weight settings of the routers will be send to the virtual machines though the multicast message of neighbor advertisement using DGW protocol. Here the multicast message would be 224.253.253.253.

DGW protocol will always run on the background of network interface card (NIC) card of the virtual network adapter of the virtual machines. The neighbor advertisement message of the DGW protocol will put the default gateway settings. In the NIC card, there should be the options of multiple default gateway settings with different weight i.e., IP address with weight

The DGW protocol, which will also run in the network interface card, will be used to route packets with the lowest weight settings of the router IP address. DGW protocol will always send multi casted keep alive messages using the multicast address 224.253.253.253 to active default gateways at every 100 millisecond. If two keep alive messages are missed between host virtual machine and active default gateway router, then DGW protocol will automatically choose next lowest weight settings as the default gateway in the virtual NIC card of virtual machine. At the same time, this router with the weight settings 1 will become the active router and all other router will become the standby routers.

In this way, virtual machine will provide the fault tolerance with automated default gateway setting using DGW protocol with maximum down time of 200 milliseconds.

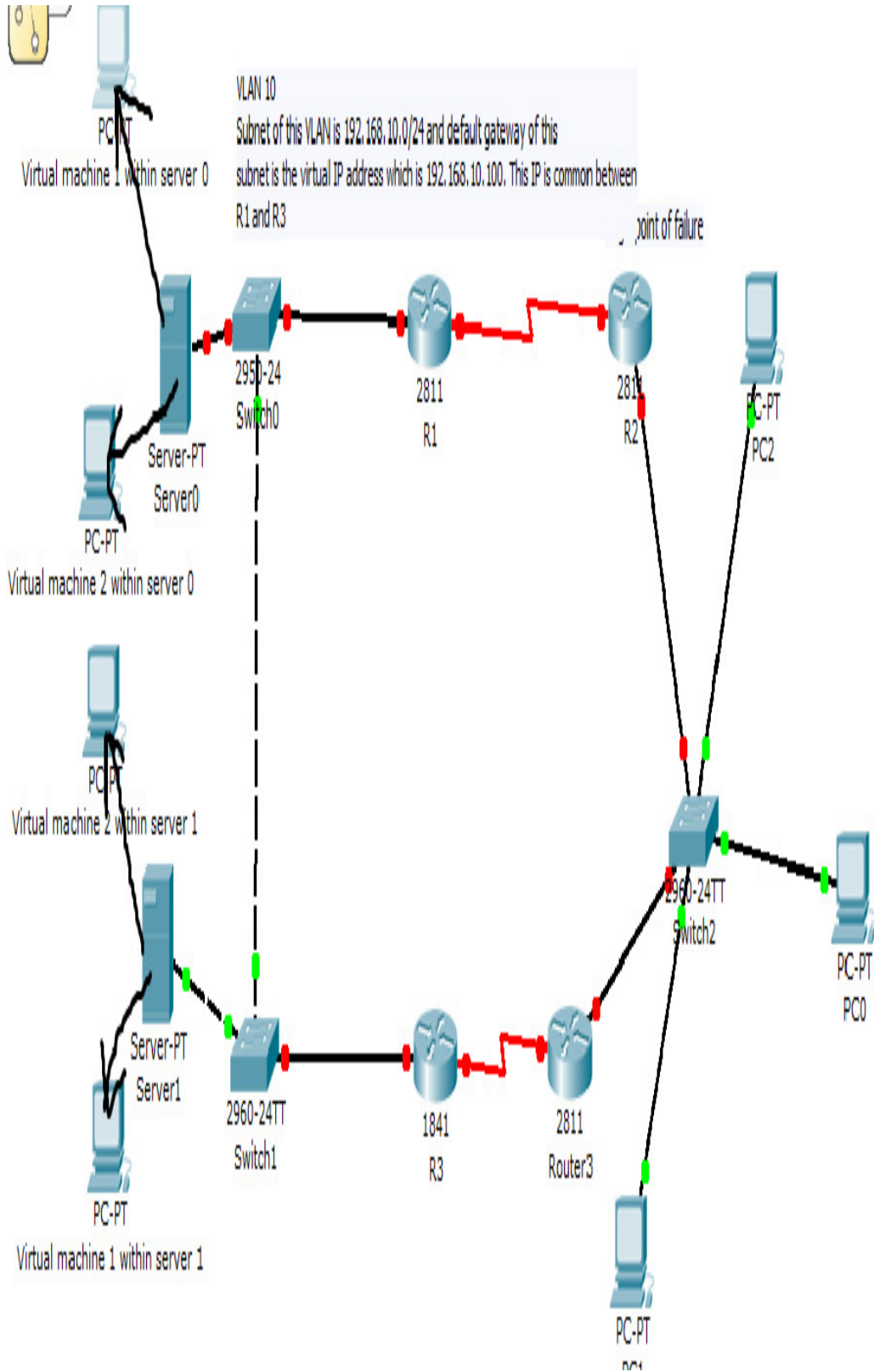


Figure 4: DGW protocol with redundant default gateway.

same time, this router with the weight settings 1 will become the active router and all other router will become the standby routers.

In this way, virtual machine will provide the fault tolerance with automated default gateway setting using DGW protocol with maximum down time of 200 milliseconds

2.7. Pseudo code of DGW:

Router_weight_settings()

```
{
  1. The routers will generate multicast Hello messages using IP address 224.254.254.254
     using the Ethernet interface.
  2. Every router will analyze their network address by calculating through the subnet mask.
     If all routers will belong to the same network address then they will establish neighbor
     ship with each other.
  3. Collect the uptime of each router by using the multicast messages.
  4. Everybody will compare their own uptime with the uptime of the other routers and the
     higher one will win.
  5. Assign weight 0 with the IP address of the highest uptime of router.
  6. Increment the weight number or next higher uptime routers and continue it for all
     remaining routers.
  7. Router with lowest weight settings will hold a copy of weight settings of all routers.
  8. Send output to the function weight_settings
     End of function.
}
```

Weight_settings()

```
{
  1. Contains the list of outputs.
}
```

Multicast_message_generation_virtual_machine()

```
{
  1. Virtual machines in server generates multicast message with destination IP
     255.253.253.253.
  2. Only routers will sense that multicast message and determine whether source IP address
     belong to the same network of the routers LAN interface.
  3. If source IP address belong to the same network, then
  4. {
  5. Lowest weight settings router will send a unicast reply messages to the virtual machine of
     the same network which will contain list of default gateways with different weight
     settings virtual machine function
     }
  6. All virtual machines within the same network will get the list of default gateways.
  7. Selecting default gateway by invoking the function select_default()
}
```

Select_default()

```
{  
  1. Select the lowest weight settings of the default gateway list and place lowest weight  
     settings as the default gateway of that virtual machine network adapter.  
  2. Start function monitoring_default_gateway()  
}
```

Monitoring_default_gateway()

```
{  
  1. Start sending and receiving keep_alive_messages between host and selected default  
     gateway at every 100 millisecond  
  2. If two consecutive keep_alive_messages are missed then  
  3. Track the default gateway with the lowest weight settings.  
  4. Send this default gateway to the function calculate_new_gateway()  
}
```

Calculate_new_gateway()

```
{  
  1. Invoke function weight_settings().  
  2. Select next lower default_gateway from the list of default_gateway.  
  3. Invoke function Monitoring_default_gateway()  
}
```

2.7. Comparison between DGW protocol and other existing protocols

There are copious advantages of using this DGW protocol over the current hot standby redundant protocol (HSRP) and Virtual Redundant router Protocol (VRRP). Both HSRP and VRRP protocol supports active and standby mode of routers. These protocol requires virtual IP address and needs manual configuration into the routers. Moreover, these protocol can be implemented only with two routers. Furthermore, to switch between the routers, it takes 3-5 seconds. The DGW protocol will automatically start functioning with the routers and hosts. There is no requirement of manual default gateway configuration in the hosts. This protocol is not limited to the number of routers and it can be re-converged within 200 milliseconds. So, DGW protocol provides seamless redundancy and fault tolerance among the virtual machines of the servers which ensures high availability of applications and service through virtualization. In spite of being planned for virtual machines, this protocol can also supports physical machines.

3. CHALLENGES FOR IMPLEMENTING DGW PROTOCOL

Network interface card driver need to reprogrammed for supporting the algorithm of this protocol and router interworking operating system (IOS) also needs to be updated to support this protocol.

4. CONCLUSIONS

The main purpose of the default gateway weight setting protocol is to ensure the high reliability, availability, and high fault tolerance for the default gateway of virtual network adapter settings in the virtual machines of the host. The DGW protocol will work at the virtual network interface card of virtual machine as well as physical network interface card of physical machines.

REFERENCES

- [1] Cisco. Nexus 1000V Series Switches. <http://www.cisco.com/en/US/products/ps9902>, July 2009.
- [2] P. Congdon. Virtual Ethernet Port Aggregator Standards Body Discussion. <http://www.ieee802.org/1/files/public/docs2008/new-congdon-vepa-1108-v01>. Pdf, Nov.2008.
- [3] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. Xen and the Art of Virtualization. In Proc. of SOSPO, Oct. 2003.
- [4] A. Bavier, N. Feamster, M. Huang, L. Peterson, and J. Rexford. In VINI Veritas: Realistic And Controlled Network Experimentation. In Proc. of SIGCOMM, 2006.
- [5] M. Casado, T. Koponen, D. Moon, and S. Shenker. Rethinking Packet Forwarding Hardware. In Proc. of HotNets, Nov. 2008.
- [6] Altar Networks. <http://altornetworks.com>, July 2009.
- [7] T. Anderson, L. Peterson, S. Shenker, and J. Turner. Overcoming the Internet Impasse through Virtualization. Computer, 38(4):34–41, 2005.
- [8] F. Anhalt and P. V.-B. Primet. Analysis and Evaluation of a Xen Based Virtual Router. Technical Report 6658, Inria, Sept. 2008.
- [9] R. Davoli. VDE: Virtual Distributed Ethernet. In Proc. Of TRIDENTCOM, Feb. 2005.

Authors

Suman Dutta – Suman Dutta is an IT trainer holds a B.Sc in computer Science and Engineering from Chittagong University of Engineering and Technology in 2004. He served for many reputed companies as a telecommunication and IT consultant for more than 10 years. Apart from his consultancy, he is involved with related research work. His area of focus is planning, designing, deploying, optimizing core and data network of telecommunication systems.



Shouman Barua – PhD research student. University of Technology, Sydney. email: shouman.barua@uts.edu.au Shouman Barua is a Phd research scholar at the university of Technology, Sydney. He received his B.Sc in Electrical and Electronic Engineering from Chittagong University of Engineering and Technology, Bangladesh and MSc in information and communication Engineering from Technische University Darmstadt (Technical University of Darmstadt), Germany in 2006 and 2014 respectively. He holds also more than five years extensive working experience in Telecommunication sector in various roles including network planning and operation.



Jishu Sen – MSc research student. University of Technology, Sydney. email: jishu.sen@uts.edu.au. He did his Bachelor of Engineering from Chittagong University of Engineering and technology, Bangladesh. Moreover, he has seven years of working experience in a Multinational telecommunication Company Robi Axiata Ltd. Specialized in core network operation, transmission operation and networking.