African Research Review

An International *Multidisciplinary Journal, Ethiopia*
Vol. 6 (1), Serial No. 24, January, 2012
ISSN 1994-9057 (Print) ISSN 2070--0083 (Online)

DOI: http://dx.doi.org/10.4314/afrrev.v6i1.6

Network Gateway Technology: The Issue of Redundancy towards Effective Implementation

(Pp. 71-81)

Imiefoh, Pedro - Computer Science Department, University of Benin,
P. M. B. 1154, Benin City, Nigeria
E-mail: pimiefoh@yahoo.com
Phone: +2348034438481

Abstract

The Internet has provided advancement in the areas of network and networking facilities. Everyone connected to the Internet is concerned about two basic things: the availability of network services and the speed of the network. Network gateway redundancy technology falls within these categories and happens to be one of the newest technologies which only few companies, such as mobile companies and other corporate business ventures have adopted. Network gateway redundancy technology makes it possible for computer devices to have access to multiple exit and entry points in the network, thus, eliminates the problem of a single point failure in both Ethernet and Internet networking systems. For effective implementation of network gateway redundancy, however, ideal focus should be on the success factors, such as ease of configuration, stability of large systems, and flow identification.

Introduction

The computer network, according to Microsoft Encarta, (2009) is a system used to link two or more computers, where users are able to share files, printers and other resources, send electronic messages and programs on other computers and networks.

A network has three layers of components, namely: application software, network software and network hardware. The application software consists of computer programs that interface with network users and permit the sharing of information such as files, graphics, videos and other resources such as printers and disks. A typical example of application software is client – server. Client computers can send request for information or requests to use resources to other computers called servers that control data and applications. Network software consists of computer programs that establish protocols or rules for computers to communicate with one another. These protocols are carried out by sending and receiving formatted instructions of data called packets. Protocols make logical connections between network applications, direct the movement of packets through the physical network and minimize the possibility of collisions between packets sent at the same time. Network hardware is made up of the physical components that connect the computers. Two important components are the transmission media, that carry the computers signals, typically on wires or fibre – optic cables and the network adaptors, which address the physical media that link computers, receive packets from network software and transmit instructions and requests to other computers. Transmitted information is in the form of binary digits or bits, that is, 0s and 1s, which the computers electronic circuitry can process.

It is against this background that this paper attempts to describe the characteristics of network gateway technology, and how to make a network gateway redundancy available, effective and manageable. To achieve this ultimate goal, the paper is presented in a five-section structure and this includes: introduction; background of network gateway redundancy, which discusses brief overview of gate way redundancy in modern technology; redundancy configuration; management strategies and tools; and a conclusion that summarises the central arguments of the paper.

Background of network gateway redundancy

A gateway is a network point that acts as an entrance to another network. Both the computers of Internet users and the computers that serve pages to users are host nodes, while the nodes that connect the networks in between are gateways. For example, the computers that control traffic between company networks or the computers used by Internet Service Providers (ISPs) to connect users to the Internet are gateway nodes.

In the network for an organisation, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

In general, a gateway is an essential feature of most routers, although other devices such as personal computers or servers can function as a gateway. However, a computer running Microsoft Windows describes standard networking feature as Internet Connection Sharing (ICS), which will act as a gateway, offering a connection between the Internet and an internal network. Such a system might also act as a Dynamic Host Configuration Protocol (DHCP) server. DHCP is a Protocol used by networked devices (clients) to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network.

Network gateway redundancy deals with the technology and protocols involved in providing high availability of access to multiple exit and entry points in a computer network. The relevance of network gateway redundancy is that it provides resilience and reliability for the network. That is, the ability of the network to react to network failure seamlessly so that from the perspective of the computer users or end users devices, it would seem as if nothing has happened and the network interruption or failure at the gateway never gets noticed by the user, except the network administrator who is required to go through the system logs periodically.

Network gateway redundancy eliminates the problem of a single point of failure when computer systems use the network gateway to connect to other parts of an Internet. That is, network gateway redundancy makes it possible for computer devices in a network to make use of several networking devices (gateways) to exit a network.

According to Institute of Electrical and Electronics Engineers (IEEE), network redundancy is involved mainly with two protocols, namely: Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). The STP allows networks to be wired in almost any topology and provides network recovery times from 30 – 60 seconds. The RSTP is an updated form of STP and provides faster recovery times from 1 – 2 seconds. Network recovery time is the time it takes to restore the network after a cable failure. Thus, the faster the recovery time the better.

Redundancy configuration

The network layering and configuration consist of three main network redundancy protocols, namely: Hot Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and Virtual Router Redundancy Protocol (VRRP). The HSRP and GLBP are Cisco proprietary while VRRP is an open source standard. The major network devices used in network gateway redundancy configuration are the routers and multilayer switches. They are used as active and backup devices depending on the type of network topology. Whenever the active gateway fails, in the event of hardware failure, software problem, IP address issue, the backup gateway links in and takes over the responsibility of the active gateway, thus providing continuous network connectivity to the remote network branches.

Hot Standby Redundancy Protocol (HSRP)

Hot Standby Redundancy Protocol is for establishing a fault-tolerant default gateway. That is, reliable, fault-tolerant network devices for hardware and software reliability to automatically identify and overcome failures. This is to achieve high network availability to ensure no single point of failure and change control for optimum use of network devices and maintenance of documentation of changes.

The active router assumes and maintains its active role through the transmission of hello messages in the group. The standby router is to initialize and maintain the highest priority. It also monitors the operational status of the HSRP group and quickly assume packet forwarding responsibility if the active router becomes inoperable. It also transmits hello messages to inform all other routers in the group of its standby router role and status. The virtual router (switch in this case) presents a consistent available router (default gateway) to the host. This assigns its own IP and Virtual addresses.

When the active router fails, and the other HSRP routers stop receiving hello messages, the standby router assumes the role of the active router, thereby forwarding packets received to the virtual router. In a situation where both active and standby routers fail, all routers in the HSEP group contend for the active and standby router roles. Even when the former active router with the higher priority regains service in the network, the active router remains the forwarding router.

Gateway Load Balancing Protocol (GLBP)

One outstanding feature of the GLBP is that the routers can support multiple MAC addresses on the physical interfaces. Gateway Load Balancing Protocol group has many member routers acting as IP default gateways known as Active Virtual Forwarders (AVFs). AVF determines the router that handles the forwarding and ensure that each station has a forwarding path in the event of failures to gateways or tracked interfaces.

Members of a GLBP group elect one gateway to be the Active Virtual Gateway (AVG) for the group. Other group members provide backup for the AVG in the event that the AVG becomes unavailable. The AVG assigns a virtual MAC address to each member of the group. Each gateway assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These gateways are known as Active Virtual Forwarders (AVFs) for their virtual MAC address.

In Figure 2, Router A is the AVG for the GLBP group and is responsible for the virtual IP address and also the AVF for the virtual MAC address. Router B is a member of the group and is designated as AVF for the virtual MAC address. Client 1 has a default gateway IP address and a gateway MAC address while client 2 shares same default gateway IP address but receives the gateway MAC address because Router B is sharing the traffic load with Router A.

If Router A becomes unavailable, client1 will not lose access to the WAN because Router B will assume responsibility for forwarding packets sent to the virtual MAC address of Router A and for responding to packets sent to its own virtual MAC address. It will also assume the role of the AVG for the entire GLBP group, hence communication for the group members continues despite the failure of a router in the group.

Virtual Router Redundancy Protocol

Like HSEP, Virtual Router Redundancy Protocol (VRRP) is a default gateway redundancy method and it has similar functionality to HSRP. The virtual router, representing a group of routers, is known as VRRP group.

Figure 3 depicts a VRRP configured LAN topology where Router A is default gateway for hosts 1 and 2 while Router B is default gateway for hosts 3 and 4. This acts as backup virtual routers to each other if either router fails. That is, if the master virtual router fails, the router configured with the higher priority will become the master virtual router and provide uninterrupted service for the LAN hosts. When Router A recovers, it becomes the master virtual router again.

For the advantage VRRP has over HSRP is that for the backup of VRRP, it does not send advertisements and VRRP master is not aware of the current backup router.

Implementation techniques

An attempt has been made for the illustration of the three main network redundancy protocols. This development is based on a computer network environment characterized by guidelines of the Institute of Electrical and Electronics Engineers (IEEE).

It can take a short time to design a computer network, but only a few minutes to lose it. Network failures happen. Planning is essential. A well planned operation has few failures, and when they occur, recovery is far more controlled and timely.

Ease of configuration

Configuring routers in a networking system is hard work. Misconfigured routers can be hard to detect and can cause nearly untraceable performance problems. For example, bugs in the configuration of proxy ARP on routers manifest themselves only as a mysterious increase in network delay (Keshav, 2003). But simple and intuitive abstractions of the underlying network functionality would go a long way in solving these problems.

Configuration becomes harder if the functionality, such as limiting the amount of multicast traffic in a network, requires the simultaneous configuration of more than one router in the network interaction between inconsistent configurations can cause network–wide problems and failures. It is not always possible to visually examine configuration files to discover mistakes and inconsistencies. However, the next generation of configuration tools will need rule-based and simulation–based sub-systems to test a configured router before installing it in the field.

Stability of Large Systems

Router hardware can be made more reliable by adding hot spares, dual power suppliers, and duplicate data paths. But software reliability remains a challenging problem. Stability of router software is a necessary prerequisite for the reliability of a large network. But software stability is hard to achieve because software state is affected by interaction among different features. For example, the addition of an exterior routing attribute, may affect the calculation of routes exported to interior routing protocols. (Mckeown, 2005). The interaction between bugs from different vendors can also lead to persistent instabilities in the network. That is, simulation may not be very helpful as it is difficult to reproduce bugs in implementation.

For effective implementation however, the one solution to software reliability may lie in adding features to protocol implementations, similar to the support for multicast trace route in mrouted, which allow users to detect and isolate problems.

Flow Identification

It is very useful to think of the set of packets travelling through the Internet between a given source and given destination, close together in time as constituting a flow. Flows last for a while, and so it is a useful optimization to pin resources, such as cache entries, associated with the set of current flows. Flows can also be associated with real – time performance guarantees. We can identify these flows by matching incoming packet headers with a set of pre-specified filters.

Classification needs to be done for each incoming packet, hence, we need fast classification algorithms. For instance, the most generic classifier is one that masks the source and destination IP addresses and parts and the protocol number, thus requiring a lookup on bits of the packet. Though this sort of classifier seems difficult to implement at high speed, coming up with a concise description of a classified and a way to match the best classifier among the several thousands that may be present at a router is advisable.

Conclusion

The essence of network gateway redundancy protocol is very crucial to the Internet. Network gateway redundancy makes it possible for computer devices to access to multiple exit and entry points in the network. For instance, routers and multilayer switches can function as network gateways and eliminate the problem of a single point failure in the network.

A good network system concentrates on the operational aspects and their success is dependent on the availability, accessibility and performance of the system. That is, the effective implementation of network gateway redundancy should ideally focus on these success factors and lie on ease of configuration, stability of large systems and flow identification.

Reference

Cisco Systems (2003). *Network Devices*: *Routers and Multilayer Switches*. Cisco Systems Inc., West Tasman Drive, San Jose, California, USA.

Contemporary Control System Incorporation (2004). *Ethernet Redundancy: Contemporary Controls*, ARC Control and Incorporation, USA.

Highleyman, W. H. (2008). *The Availability Digest: Virtual Router Redundancy Protocol.* Sombers Associates. Available at www.availabilitydigest.com

John, L. J. (2004) *Virtual Router Redundancy Protocol for Gateway Redundancy.* Task Force Network Working Group. Available at www.ieff.org/rfc/rfc3768

Keshav, and Sharma, R. (2003) *Issues and Trends in Router Design.* Department of Computer Science, Cornel University, New York. Sheshav ajcs.cornell.edu;sharmaajcs.cornell.edu

Lubomir, N. (2002). *White Paper: Hot Standby Redundancy Protocols, Gateway Load Balancing Protocols and Virtual Redundancy Protocol.* Oxford Press. London.

Mckeown, N. (1995). Scheduling *Algorithms for Input-Queued Cell Switchs.* PhD Thesis, University of California at Berkeley, May 1995

Rick, G. (2006). *Implementing High Availability Options in MLS with HSRP, CCNP3.* Cabrillo College, Spring.

Ronald, J. G (2008). *Fundamentals of Data Communication and Computer Networks* (Second Edition). Engineering Research Facility, California.

Ted, D. (2008). *Effective Internet Presence.* Creative Commons License, United States Available at http://www.effectiveinternetpresence.com

The Wikipedia Foundations Incorporation (Online). *How Staff Works and Network Gateway*. (www.wikipedia.org)

Figure 1: HSRP Group Layering

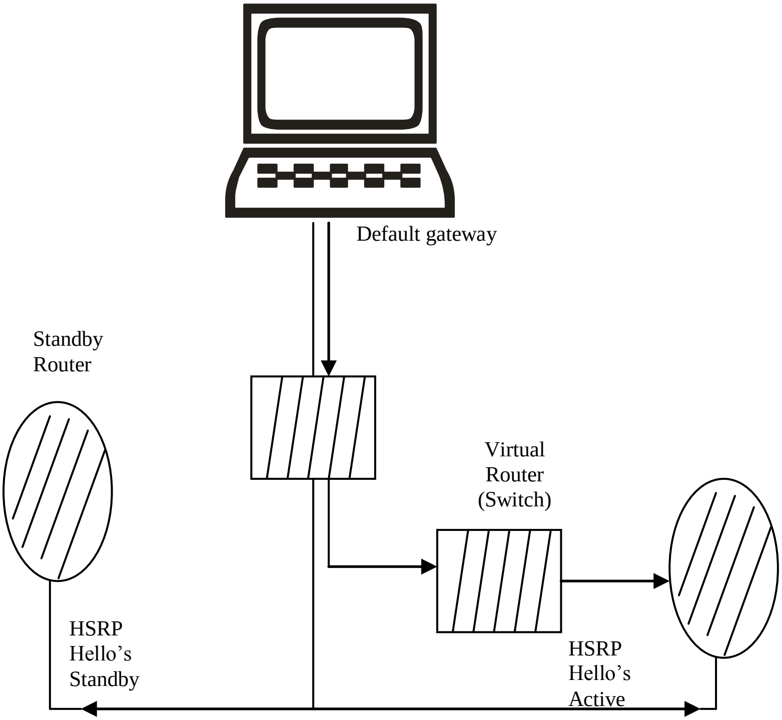


Figure 2: GLBP Group Layering

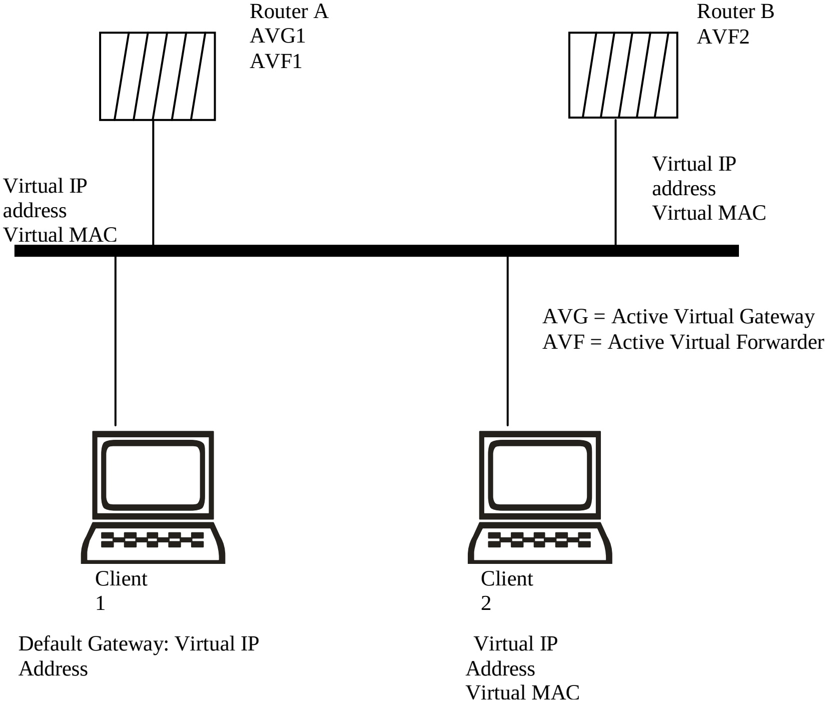
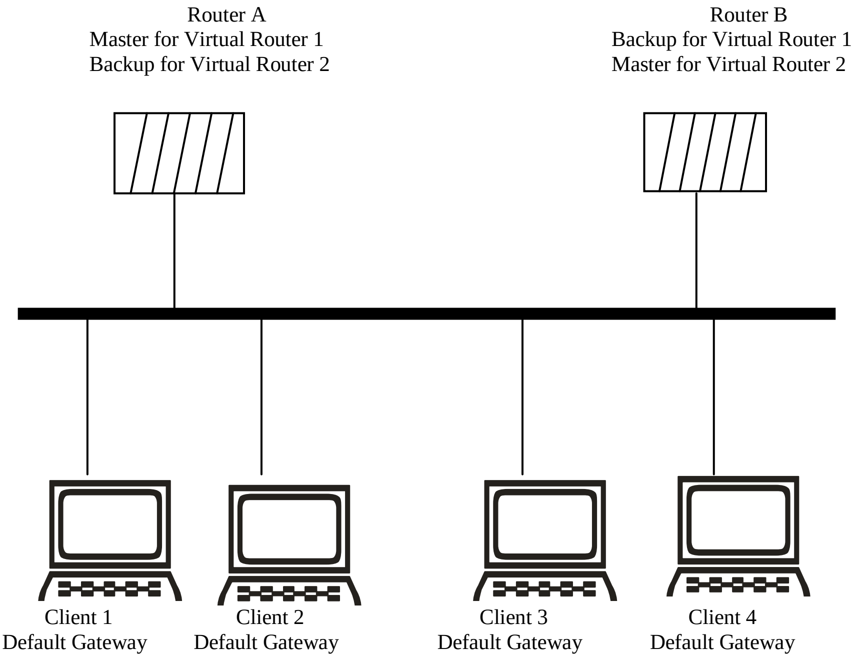


Figure 3: VRRP Group Layering


Router A
Master for Virtual Router 1
Backup for Virtual Router 2
Router B
Backup for Virtual Router 1
Master for Virtual Router 2
Client 1
Default Gateway
Client 2
Default Gateway
Client 3
Default Gateway
Client 4
Default Gateway