International Journal of
Science Inventions Today
www.ijsit.com
ISSN 2319-5436
Research Article

REDUNDANCY PROTOCOLS FOR CAMPOUS NETWORK

Kabita Sahoo* and Jagannath Ballav Goswami

*Centurion University of Technology and Management, BBSR.

DRIEMS, Tangi, Cuttack.

ABSTRACT

In this paper we are describing the redundancy protocols used in the campus network. Also focusing on how we will handle the failure. Redundancy protocol is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP sub network. we have discussed each of the protocol one by one and the features of each protocol.

Keywords: HSRP, VRRP, GLBP,CARP,ESRP,R-SMLT,NSRP,

First Hop Redundancy Protocol (FHRP):

A First Hop Redundancy Protocol (FHRP) is a computer networking protocol which is designed to protect the default gateway used on a sub network by allowing two or more routers to provide backup for that address in the event of failure of the/an active router, the backup router will take over the address, usually within a few seconds. Such protocols can also be used to protect other services operating on a single IP address, not just routers.

Examples of such protocols include:

1. Hot Standby Router Protocol (HSRP) - Cisco's initial, proprietary standard.
2. Virtual Router Redundancy Protocol (VRRP) - an open standard protocol.
3. Common Address Redundancy Protocol (CARP) - free, (patent) unencumbered alternative to Cisco's HSRP.
4. Gateway Load Balancing Protocol (GLBP) - a more recent proprietary standard from Cisco that permits load balancing as well as redundancy
5. Routed Split multi-link trunking (R-SMLT) - an Avaya redundancy protocol
6. Net Screen Redundancy Protocol (NSRP) - a Juniper Networks proprietary router redundancy protocol providing load balancing

Hot Standby Router Protocol (HSRP):

It is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway. The protocol establishes a framework between network routers in order to achieve default gateway failover if the primary gateway becomes inaccessible. HSRP-enabled routers, defining priority between the routers. The primary router with the highest configured priority will act as a virtual router with a pre-defined gateway IP address and will respond to the ARP request from machines connected to the LAN with the MAC address 0000.0C07.ACXX (or 0000.0C9F.FXXX for HSRPv2) where X will be hex representation of the (decimal) group ID. If the primary router should fail, the router with the next-highest priority would take over the gateway IP address and answer ARP requests with the same MAC address, thus achieving transparent default gateway failover. HSRP is not a routing protocol as it does not advertise IP routes or affect the routing table in any way. HSRP has the ability to trigger a failover if one or more interfaces on the router go down. This can be useful for dual branch routers each with a single serial link back to the head end. If the serial link of the primary router goes down, the backup router will take over the primary functionality and thus retain connectivity to the head end.

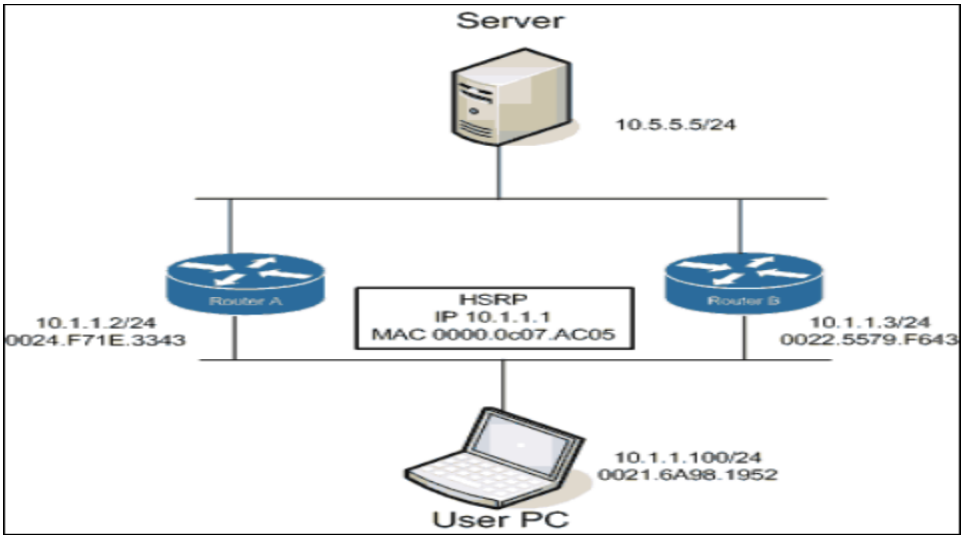


Figure for HSRP

Advantages of HSRP:

The HSRP supports configurable MAC addresses. This lets client computers and destination networks use HSRP as the first destination to start routing IP traffic. Peer-to-peer networking applications have significantly used the HSRP protocol, which also allows IP redundancy and maintains maximum redundancy.

VRRP:

Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork.

The protocol achieves this by creation of virtual routers, which are an abstract representation of multiple routers, i.e. master and backup routers, acting as a group. The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the master router.

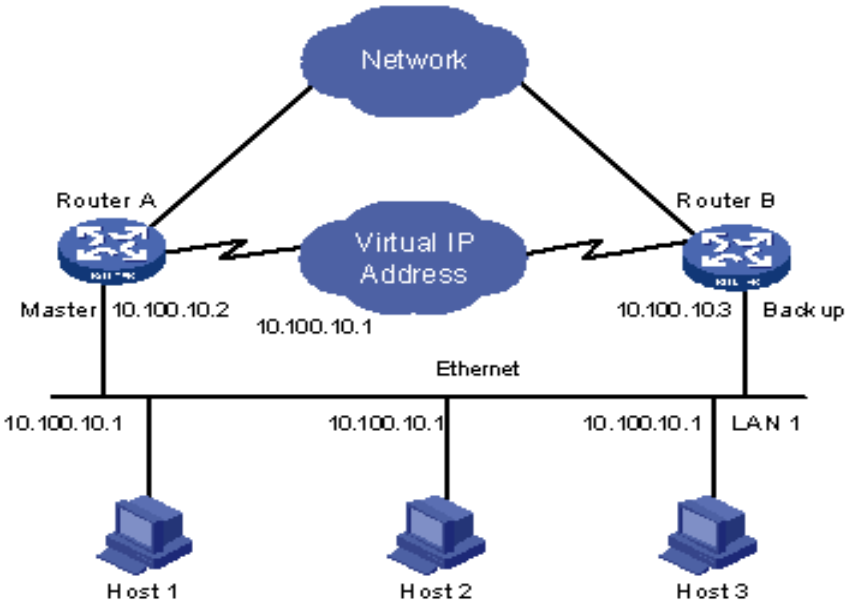


Figure for VRRP

How VRRP Works:

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration. Examples of dynamic router discovery are as follows:

- Proxy ARP—The client uses Address Resolution Protocol (ARP) to get the destination it wants to reach, and a router responds to the ARP request with its own MAC address.
- Routing protocol—The client listens to dynamic routing protocol updates (for example, from Routing Information Protocol [RIP]) and forms its own routing table.
- IRDP (ICMP Router Discovery Protocol) client—The client runs an Internet Control Message Protocol (ICMP) router discovery client.

The dynamic discovery protocols incur some configuration and processing overhead on the LAN client. This could be detrimental also, in the event of a router failure, the process of switching to another router can be slow.

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is

detached from the rest of the network.

VRRP can solve the static configuration problem. VRRP is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork. Enables a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group. VRRP is supported on Ethernet, Fast Ethernet, BVI, and Gigabit Ethernet interfaces, on MPLS VPNs, VRF-aware MPLS VPNs and VLANs.

Benefits of VRRP:

Redundancy:

VRRP enables you to configure multiple routers as the default gateway router, which reduces the possibility of a single point of failure in a network.

Load Sharing:

You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.

Multiple Virtual Routers:

VRRP supports up to 255 virtual routers (VRRP groups) on a router physical interface, subject to the platform supporting multiple MAC addresses. Multiple virtual router support enables you to implement redundancy and load sharing in your LAN topology.

Multiple IP Addresses:

The virtual router can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on an Ethernet. it is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork surface you can configure VRRP on each subnet.

Preemption:

The redundancy scheme of VRRP enables you to preempt a virtual router backup that has taken over for a failing virtual router master with a higher priority virtual router backup that has become available.

Authentication:

VRRP message digest 5 (MD5) algorithm authentication protects against VRRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.

Advertisement Protocol:

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA assigned VRRP the IP protocol number 112.

VRRP Object Tracking:

VRRP object tracking provides a way to ensure the best VRRP router is virtual router master for the group by altering VRRP priorities to the status of tracked objects such as interface or IP route states.

VRRP Object Tracking:

Object tracking is an independent process that manages creating, monitoring, and removing tracked objects such as the state-of-the line protocol of an interface. .

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes such as VRRP use this number to track a specific object.

The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down.

VRRP object tracking gives VRRP access to all the objects available through the tracking process. The tracking process provides the ability to track individual objects such as a the state of an interface line protocol, state of an IP route, or the reachability of a route.

VRRP provides an interface to the tracking process. Each VRRP group can track multiple objects that may affect the priority of the VRRP router. Specify the object number to be tracked and VRRP will be notified of any change to the object. VRRP increments (or decrements) the priority of the virtual router based on the state of the object being tracked.

VRRP Authentication:

VRRP ignores unauthenticated VRRP protocol messages. The default authentication type is text

authentication. We can configure VRRP text authentication, authentication using a simple MD5 key string, or MD5 key chains for authentication.MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each VRRP group member to use a secret key to generate a keyed MD5 hash of the packet that is part of the outgoing packet. A keyed hash of an incoming packet is generated and if the generated hash does not match the hash within the incoming packet, the packet is ignored. The key for the MD5 hash can either be given directly in the configuration using a key string or supplied indirectly through a key chain. A router ignores incoming VRRP packets from routers that do not have the same authentication configuration for a VRRP group. VRRP has three authentication schemes:

- No authentication
- Plain text authentication
- MD5 authentication

VRRP packets are rejected in any of the following cases:

- The authentication schemes differ on the router and in the incoming packet.
- MD5 digests differ on the router and in the incoming packet.
- Text authentication strings differ on the router and in the incoming packet.

GLBP:

Gate way Load Balancing Protocol (GLBP), which is a Cisco proprietary FHRP that provides not only first-hop redundancy like HSRP and VRR is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork but also more integrated load-balancing capabilities.

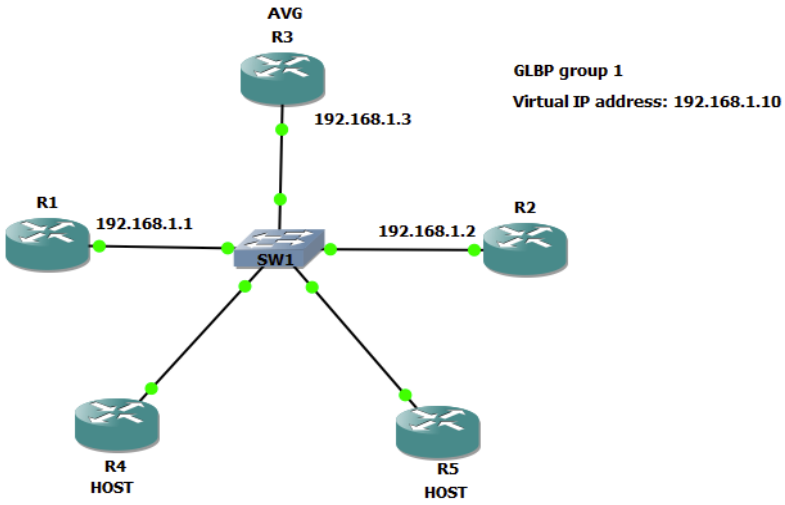


Figure for GLBP

How Does GLBP Work?

The purpose of GLBP development was to bridge a gap that existed with the Hot Standby Router Protocol (HSRP)—that is, easy implementation of load balancing. With HSRP (and VRRP, the standard version of HSRP), the problem that exists is that only a single device within a group is ever forwarding traffic at any given time. When only a single device is actually forwarding data, a large amount of idle bandwidth is left sitting off the interfaces of the standby devices. There is a way to get around this by configuring multiple HSRP groups on the devices, but this also requires that half the hosts be configured with one gateway and the other half with another that increases the amount of administration and is still a crude solution to the problem.

GLBP works a bit differently from these other protocols. To understand this, there are two terms for GLBP device roles that need to be defined: Active Virtual Gateway (AVG) and Active Virtual Forwarder (AVF). The AVG is responsible for managing the traffic to all of the configured GLBP Active Virtual Forwarder (AVF) devices. That is done by controlling the ARP process. When GLBP comes up, the AVG is elected, and one of its first duties is to take responsibility for the virtual IP address and assign each of the configured GLBP devices with a virtual MAC address (including itself). When an ARP message is seen by the AVG, it responds and gives out these virtual MAC addresses in a round-robin format; this way, each of the AVFs is assigned an even amount of traffic from the devices requesting access. Up to four different virtual MAC addresses and thus AVFs can actively exist.

GLBP Redundancy:

With GLBP, there are actually two different types of redundancy: AVG redundancy and AVF redundancy. AVG redundancy works almost exactly the same as HSRP or VRRP redundancy; a single AVG is elected when GLBP comes up and keeps that role until it goes down or until another router takes the role from it. Like HSRP and VRRP, GLBP uses a priority to elect the AVG; in the case of a tie (the default is 100), the highest IP address is used. GLBP (AVG) pre-emption is disabled by default; what this means is that the current AVG must fail for another device to take over the role even if it has a higher priority.

AVF redundancy is a little different; if the device that is responsible for a specific virtual MAC address fails, one of the other current AVFs takes over the forwarding duties by taking over the specific virtual MAC address. This change is communicated to the current AVG, and over a series of timeouts, the traffic is transferred from that specific virtual MAC address to other, currently up, AVFs. Pre-emption for AVFs is enabled by default. This enables the other devices within GLBP to keep track of when an AVF fails and take over the duties proactively.

GLBP Weighting and Interface Tracking:

GLBP uses a concept of weighting to determine the load capacity of each of the AVFs. By default, each of the AVFs is configured with a weighting of 100 (values range from 1 to 254). By default, the load balancing behaviour of GLBP is to use round robin, which will always result in a distribution of hosts to AVFs. If this load balancing behaviour was altered to use weighting, then depending on the current weighting assigned to an AVF, each specific forwarder would get a specific load of the traffic.

The weighing can also be configured with lower and upper levels. These are then used to determine if an AVF should be forwarding. For example, if configured with a lower limit of 40 and an upper limit of 80, when the weighting on a device changed to be lower than 40, the AVF would stop forwarding. It would remain in this state until its weighting increased to above 80.

The weighting of specific AVFs can be controlled both statically and dynamically. When configured statically, the network administrator/engineer will configure a specific weighting to each AVF. When configured dynamically, GLBP uses the status of a track object to determine the current AVF weighting. Track objects can use a number of different criteria to determine their state (up or down). The most basic of these is interface line protocol state and interface IP routing.

Common Address Redundancy Protocol:

CARP is the Common Address Redundancy Protocol. Its primary purpose is to allow multiple hosts on the same network segment to share an IP address. CARP is a secure, free alternative to the Virtual Router

Redundancy Protocol and the Hot Standby Router Protocol.

CARP works by allowing a group of hosts on the same network segment to share an IP address. This group of hosts is referred to as a "redundancy group". The redundancy group is assigned an IP address that is shared amongst the group members. Within the group, one host is designated the "master" and the rest as "backups". The master host is the one that currently "holds" the shared IP; it responds to any traffic or ARP requests directed towards it. Each host may belong to more than one redundancy group at a time.

One common use for CARP is to create a group of redundant firewalls. The virtual IP that is assigned to the redundancy group is configured on client machines as the default gateway. In the event that the master firewall suffers a failure or is taken offline, the IP will move to one of the backup firewalls and service will continue unaffected.

While highly redundant and fault-tolerant hardware minimizes the need for CARP, it doesn't erase it. There's no hardware fault tolerance that's capable of helping if someone knocks out a power cord, or if your system administrator types reboot in the wrong window. CARP also makes it easier to make the patch and reboot cycle transparent to users, and easier to test a software or hardware upgrade--if it doesn't work, you can fall back to your spare until fixed.

There are, however, situations in which CARP won't help. CARP's design does require that the members of a group be on the same physical subnet with a static IP address, although with the introduction of the carp dev. directive, there is no more need for IP addresses on the physical interfaces. Similarly, services that require a constant connection to the server (such as SSH or IRC) will not be transparently transferred to the other system--though in this case, CARP can help with minimizing downtime. CARP by itself does not synchronize data between applications, for example, manually duplicating data between boxes with sync, or whatever is appropriate for application.

CARP supports both IPv4 and Ipv6.

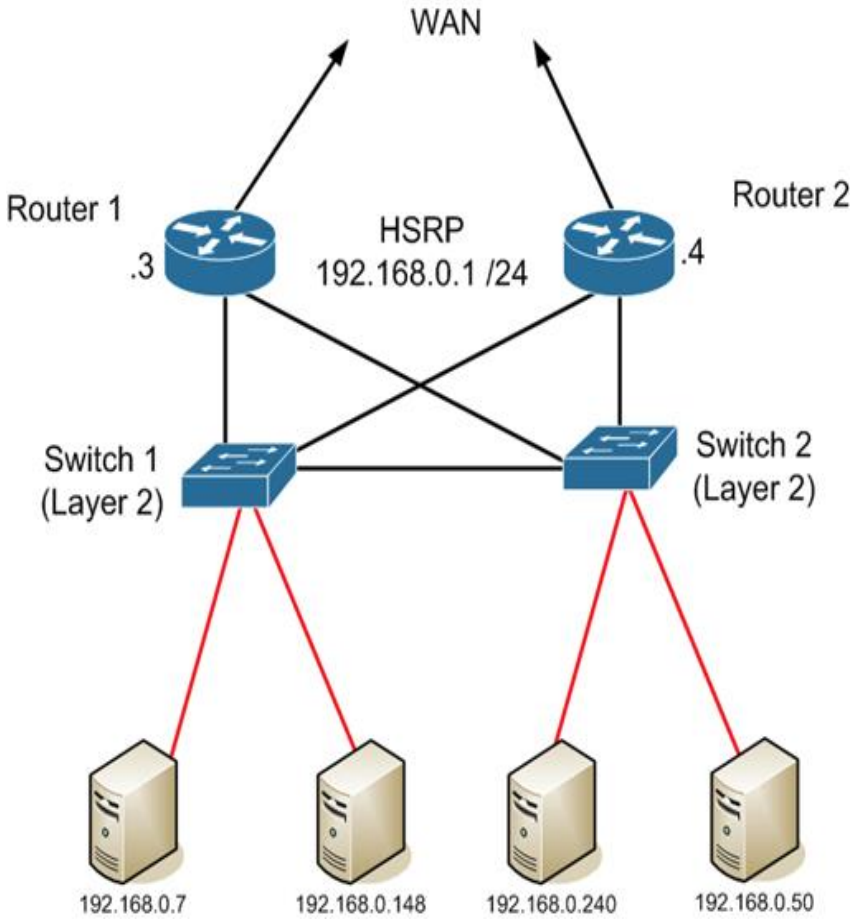


Figure for CARP

R-SMLT:

It is a computer networking protocol developed at Nortel as an enhancement to split multi-link trunking (SMLT) enabling the exchange of Layer 3 information between peer nodes in a switch cluster for resiliency and simplicity for both L3 and L2.

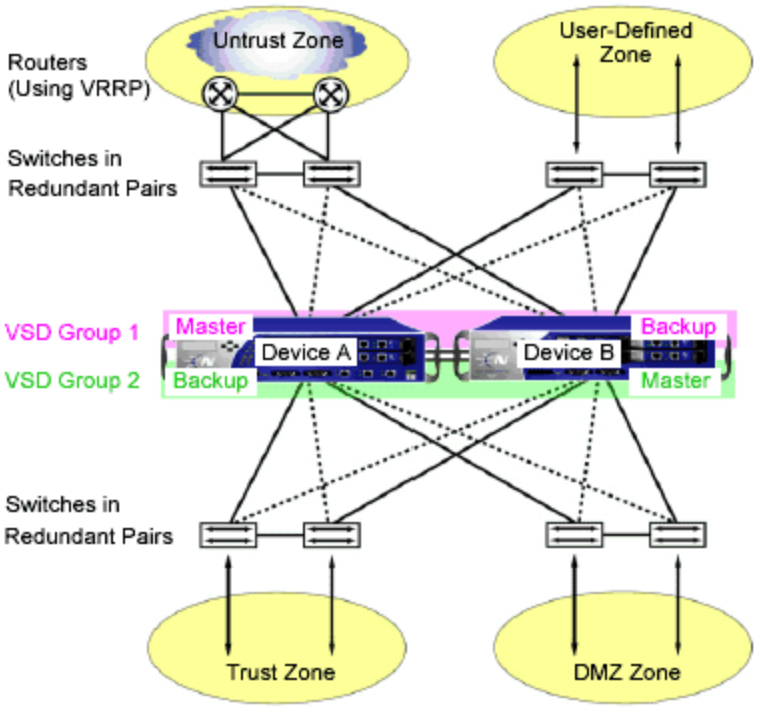
In many cases, core network convergence-times after a failure is dependent on the length of time a routing protocol requires to successfully converge (change or re-route traffic around the fault). Depending on the specific routing protocol, this convergence time can cause network interruptions ranging from seconds to minutes. The R-SMLT protocol works with SMLT, and distributed Split Multi-Link Trunking (DSMLT) technologies to provide sub-second failover (normally less than 100 millisecond so no outage is noticed by end users. This high speed recovery is required by many critical networks where outages can cause loss of life or very large monetary losses in critical networks.

RSMLT routing topologies providing an active-active router concept to core SMLT networks. The protocol supports networks designed with SMLT or DSMLT triangles, squares, and SMLT or DSMLT full mesh topologies, with routing enabled on the core VLANs. R-SMLT takes care of packet forwarding in core router failures and works with any of the following protocol types: IP Unicast Static Routes, RIP1, RIP2, OSPF, BGP and IPX RIP.

NSRP:

An NSRP cluster consists of a group of security devices that enforce the same overall security policy and share the same configuration settings. When you assign a device to an NSRP cluster, any changes made to the configuration on one member of the cluster propagate to the others

With the Screen OS device in Route or NAT mode, you can also configure both devices in a redundant cluster to be active, sharing the traffic distributed between them by routers with load-balancing capabilities running a protocol such as the Virtual Router Redundancy Protocol (VRRP). This is accomplished using the Net Screen Redundancy Protocol (NSRP) to create two virtual security device (VSD) groups, each with its own virtual security interfaces (VSIs). Device A acts as the master of VSD group 1 and as the backup of VSD group 2. Device B acts as the master of VSD group 2 and as the backup of VSD group 1. This configuration is known as active/active. Because of device redundancy, there is no single point of failure.



Issues in FHRP:

As Index 7 of RFC 2281 tells that these protocols do not provide security; the authentication field found within the message is useful for preventing misconfiguration. The protocols are easily subverted by an active intruder on the LAN. This can result in a packet black hole and a denial-of- service attack. It is difficult to subvert the protocols from

Outside the LAN as most routers will not forward packets addressed to the all-routers multicast address (224.0.0.2) [1]. This issue of HSRP can be resolved using MD5 algorithm with it because MD5 algorithm provides hash functions which can't be re-engineered. So it will be appropriate solution of this problem. Thus LAN can be made more secure and it can be saved from internal attacks holds 10 seconds.

CONCLUSION

In this paper, we have discussed about some first hop redundancy protocols their working scenario . Every protocol works in its own specific way and contains different type specialty within it.

Future Scope:

In future work, we will implement the authentication of md5 algorithm And after that we will work upon the various issue within it. Furthermore we will define more precise technique for it which will be able to provide more security.

REEFERENCES

1. Review of First Hop Redundancy Protocol and TheirFunctionalities Priyanka Dubey , Shilpi Sharma, Aabha Sachdev.(IJETT) – Volume 4 Issue 5- May 2013
2. High Availability with Redundancy Control Protocol.Rupinder kaur, M.Vijaya Raju, B.Arun kumar. International Journal of Data & Network SecurityVolume 2 No.2 March15, 2013, ISSN 2319-1236
3. T. Li Juniper Networks, B. Cole Juniper Networks, P. Morton CiscoSystems, D. Li Cisco Systems, RFC 2281 March 1998.
4. R. Rivest MIT Laboratory for Computer Science and RSA Data security, Inc. RFC 1321,April 1992
5. Deering, S., "ICMP Router Discovery Messages", RFC 1256,

6. en.wikipedia.org

7. United States Patent. Patent Number: 5,473,599. Standby RouterProtocol. Date of Patent: Dec. 5, 1995.

8. www.cisco.com/c/en/us/td/.../fhp-12-4-book.pdf tools.ietf.org/html/rfc3768

9. First Hop Redundancy Protocolsconfiguration Guide, Cisco IOS Release12.4

10. CCNP SWITCH Exam - Router Redundancy ProtocolsPosted by Kelson Lawrence on Wed, Feb 09, 2011