Mobile IPv4 high availability

Ville Partanen
Helsinki University of Technology
vpartane@cc.hut.fi

Abstract

Mobile IPv4 specifies a protocol in order to enhance transparent routing of IP datagrams. The main objective of this protocol is to ensure an ability to communicate in a mobile environment where a node can change its place. An essential part of this protocol is a Home Agent, a router on the Mobile Nodes home network, which has a responsibility to tunnel datagrams to the node. In order to locate Home Agent some sort of high availability mechanism is needed. The scope of this paper is to describe these mechanisms. The goal is to compare and analyse high availability mechanisms. Effort is also put on suggesting future work and analysing remaining needs around this topic.

1 Introduction

In a mobile environment one basic part of the net is a Mobile Node. The idea is that a Mobile Node can move in a geographical area and in the same time maintain the connection to the Internet. In order to do this a Mobile Node has to have a router, which it is connected to and through which a Mobile Node will send and receive IP packets. This Mobile Nodes point of attachment to the Internet is called Foreign Agent. Since the Mobile Node might be in constant movement it might have to change its Foreign Agent. This results in a situation where the node has to change its IP address. In order to know which IP address the Mobile Node has, we have to have some kind of high availability mechanism that always knows to Mobile Nodes alternating IP address. In mobile IPv4 this is implemented by using a router, which is called a Home Agent.

Home agents task is to receive all packets sent to the Mobile Nodes original and static IP address and then tunnel them to the Mobile Nodes current and perhaps changing IP address. Thus the Home Agent is a single point of failure. This means that in a situation where a Mobile Node does not have a Home Agent it can not receive packets sent to its original IP address.

The purpose of this paper is to provide an overview of the Mobile IPv4 protocol and describe mechanism how to achieve high availability when using a Home Agent. This is done in chapters 3, 4 and 5. After this characteristics, which are important to high availability in the scope of this paper, are presented and high availability mechanisms are compared using these characteristics (chapter 6). In chapter 7 conclusions are summed up and finally in chapter 8 some effort is made suggesting future work and analysing remaining needs in the scope of high availability.

2 RFC 3344

2.1 Introduction

IP mobility support to IPv4 is introduced in RCF 3344 [9]. As it is essential to understand the basics of the protocol to apprehend the subject of this paper, a short introduction to RCF 3344 is given.

In IP version 4 it is assumed that the IP address uniquely identifies the point of attachment of the node to the Internet. In a mobile world this results to a significant problem, which could be solved by two alternatives: A node must change its IP address every time it changes its point of connection or host specific routes must be propagated to the Internet routing fabric. As we can clearly see none of these is an alternative since they both have major disadvantages. In the first alternative the high layer connection has to be closed and in the second one a severe scaling problem could appear. As an implication a more scalable mechanism is required: RFC 3344.

The goals of this protocol is to ensure that communication with other nodes can be sustained and IP address does not have to be changed even if the Mobile Node alters its point of connection in such a way that IP subnet is changed.

Mobile IP control messages are send with UDP[10] using a well know port number 434.

There are two types of messages: Registration Request and Registration Reply, both of which are used to register Mobile Nodes new address. Addition to these mobile IP uses existing Router Advertisement and Router Solicitation[2], which are used for Agent Advertisement and Solicitation.

In order to allow optional information to be carried Mobile IP defines a general extension mechanism. Up to 255 extensions are supported.

2.2 Architectural entities and terminology

- Mobile Node

  A host or a router, which changes its point of attachment from one subnet to another. When a Mobile Node is acting as a router it can have an entire network behind it. In such a case a network could be called a Mobile Network.

  A Mobile Node may communicate with other nodes to any location if the link layer connectivity is available.

  Every Mobile Node has to have a mobility security association for each of its Home Agents. Mobility security association applies security services when MN communicates with FA or HA. Such services include

for example authentication algorithm and a shared secret key. Security associations are indexed by SPI (Security Parameter Index) and IP addresses.

- Home Agent

  A router on a Mobile Nodes home network. Its main responsibly is to tunnel IP datagrams to the Mobile Node when it is not connected to its home network. Home Agent maintains the current location (IP address) of the Mobile Node in the Internet.

- Foreign Agent

  A router on a Mobile Nodes visited network. Foreign Agents main task is to detunnel datagrams that came from the Home Agent to the Mobile Node. Foreign Agent can also act as a default router for a Mobile Node.

- Care-of address

  Termination point of the IP tunnel in the Mobile Nodes end. All IP datagrams are forwarded to this address while the Mobile Node is away from home. Protocol defines two possibilities:

  1. Foreign Agent care-of address
     Is an address of the Foreign Agent to which the Mobile Node has registered.
  2. Co-located care-of address
     Is an externally obtained address, which the Mobile Node has on its own network interface.

2.3 Example

Here is an simplified example how to set up an Mobile IP connection and how datagrams are sent.

1. Advertising

   Foreign agents and Home Agents advertise their presence and services by using Agent Advertisement messages, which can be sent in periodic time intervals. Such a message may also be asked by the Mobile Node by using an Agent Solicitation message.

   It is crucial that the Foreign Agent sends advertisements in order to the registered nodes to know that they are still in the area of the Foreign Agent.

   Mobile Node uses Agent Advertisements to identify its current point of attachment to the Internet.

   Authentication is not needed in Agent Advertisement and in Agent Solicitation messages.

   An Agent Advertisement is an ICMP Router Advertisement that has been extended. An Agent Solicitation is identical to an ICMP Router Solicitation but TTL set to 1.

2. Location definition

   Mobile Node receives advertisements and according to them the Mobile Node determines if it is connected to the home or to the foreign network or has it moved to another network.

   RCF 3344 presents two primary mechanisms to detect movement from one subnet to another.

   (a) Lifetime based

   If the Agent Advertisements lifetime expires and the Mobile Node fails to receive another advertisement from the same agent, it assumes that it has lost connection to the agent.

   If the Mobile Node has an older Agent Advertisement from another agent it can try to register with that agent. If the Mobile Node has no previous advertisements it will have to discover new agents.

   (b) Network prefix

   To check if the newly received Agent Advertisement was received on the same subnet as the Mobile Nodes current care-of address.

   In this case both the new and the old agent must include Prefix-length extension (indicates the number of bits in network prefix) in Agent Advertisements.

   Mobile Node knows it is at home network when it receives Agent Advertisement from its own Home Agent.

3. Addressing according to location

   There are two alternatives based on the Mobile Nodes point of connection to the Internet:

   (a) Home Network

   Mobile Node detects that it is located at its home network and as a result it operates without mobility. When returning home, Mobile Agent deregisters with its Home Agent.

   (b) Foreign Network

   Mobile Node detects that it has moved to a foreign network. Is this case it has to obtain care-of address from the network. Address can be advertised by Foreign Agent in the Mobilty Agent Advertisment Extension or it can be assigned for example with DHCP.[3]

4. Registration

   Mobile Node has to register its new care-of address with its Home Agent. Registration is done by using an Registration Request message and an Registration Reply message. This operation creates a binding with Mobile Nodes home address and its care-of address for a specific lifetime.

   In this process Mobile Node sends its current reachability information to the Home Agent. By doing so the Mobile Node informs its current care-of address. Mobile node can also requests that the Home Agent forwards services to a foreign network or Mobile Node can renew its registration. If the Mobile Node is at home network it deregisters at this stage.

   There are two alternative methods for registering:

   (a) Via Foreign Agent

   The Foreign Agent relays the registration to the Mobile Nodes home network. This is done when Mobile Node uses care-of address.

(b) Directly to Home Agent

Mobile Node communicates directly with the Home Agent. This is done when Mobile Node uses co-located care-of address.

Registration procedure has to be authenticated. Authentication is done by using extensions in the registration messages.

5. Tunnelling

   Datagrams sent to the Mobile Nodes home address are intercepted by the Home Agent. After interception the Home Agent tunnels the IP datagrams to the Mobile Node by using IP in IP encapsulation[8]. There are two possible endpoints for the tunnel based on the type of the Mobile Nodes address: Foreign Agent in the case of care-of address or the Mobile Node in the case of co-located care-of address. Advantage of using co-located care-of address is that the Mobile Node has the possibility to work without a foreign agent. Disadvantage is that this places significant demands on the size of the pool of addresses and since IPv4 does not have a vast address space this might be a problem in some situations.

   When Mobile Node is away from home its home address is hidden form the intervening routers between the home network and the current location by using protocol tunneling.

   The endpoint of the tunnel is care-of address. At this point the orginal datagram is removed from the tunnel and send to the Mobile Node.

6. Communication

   In the reverse direction datagrams sent by the Mobile Node are delivered in a standard fashion way using IP. Traffic does not have to be routed through the Home Agent.

Fig. 1

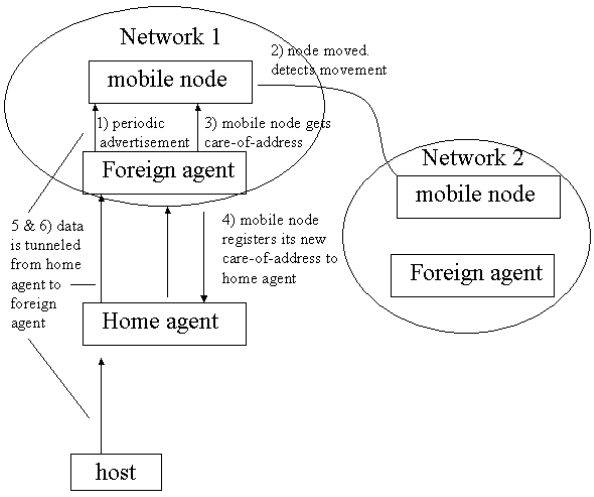

Figure 1: Mobile IP example when using care-of address

3 Dynamic Home Agent Assignment

3.1 Introduction

In RFC 3344 dynamic Home Agent discovery is done by Registration Request that is sent by using subnet-directed broadcast IP. This mechanism was designed for a Mobile Node, which has a static home address and subnet prefix. On the other hand subnet-directed broadcast includes one significant problem: Routers tend to drop these kind of packets by default so the Registration Request is unlikely to reach anything[6].

DHAA proposes a messaging mechanism for dynamic Home Agent assignment and Home Agent redirection during initial registration. The goal is to find optimal Home Agent for mobile IP session.

NAI (Network Access Identifier) must be used by the Mobile Node for home address assignment. In general NAI is used in order to AAA server to identify the client [1]. In the scope on Mobile IP and NAI, RFC 2794 specifies how to use Mobile Node NAI extension in the Mobile IP Registration Request, which is sent by the Mobile Node.

Reasons to use optimal Home Agent could be for example:

- Delay

  If the home network and Mobile Node are geographically within a long distance the delay that comes from tunnelling could be very significant.

- Simplicity

  In large scale mobile networks multiple Home Agent addresses cause bureaucracy.

- Load Balancing

  In order to avoid congestion in Home Agents. This could also be done at a group level.

3.2 Message mechanism

Here is a simplified example of DHAA procedure:

1. Home Agent Address field in the Registration Request is set to ALL-ZERO-ONE-ADDR (two possibilities). Message is sent by a Mobile Node.

   (a) IP address is 0.0.0.0

   Mobile Node needs a dynamic Home Agent from anywhere on the net.

   (b) IP address is 255.255.255.255

   Home Agent in assigned from the home domain.

2. The Mobile Node (if using co-located care-of address) or Foreign Agent (if using care-of address) sends the Registration Request to the Requested HA. In the latter case the orginal request comes from the Mobile Node and the destination address is Foreign Agent, which will forward the request onward to the requested Home Agent (note this is not the real Home Agent at this point).

3. Requested Home Agent processes the request by the rules of RFC 3344. A mobility binding is created. Mobile Node receives Registration Reply.
4. Mobile Node receives the Assigned Home Agent from the Registration Reply and starts using it.
5. Renewal may be done.

Fig. 2

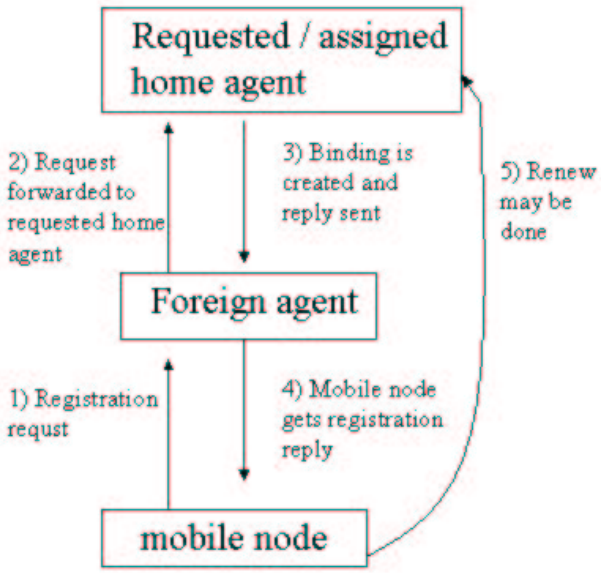

Figure 2: DHAA example

In some cases Registration Request may be rejected. This could happen for a many reasons such an administrative restriction. In this case an optional redirection message can be sent by the Home Agent: REDIRECT-HA-REQ. In this message an alternate HA is suggested at the REDIRECT-HA-ADDRESS extension, which is mandatory when a redirection message is sent. After receiving this REDIRECT-HA-REQ Mobile Node obtains new Home Agent address from the message and may try to register with that Home Agent.[6]

4 Virtual router redundancy protocol

4.1 Introduction

Virtual Router Redundancy Protocol is introduced in the RFC 2338[5]. It has been designed to eliminate the single point of failure in a static default routed environment. It is an electation protocol, which dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN[5].

The router controlling the IP addresses that are associated with a virtual router is called the master and it has the responsibility to forward packets to the IP addresses it controls.

If the master becomes unavailable any of the virtual routers IP addresses can be used as a first hop router. Master selection can be done for instance according to link capacity, performance or reliability.

The idea of VRRP is to provide quick and efficient transition from backup to master in order to minimize service interruption and to provide efficient optimisation for choosing the right master. The election process is quick (less than 1 second), a few active protocol states are used and only a single message is sent.

Each router has a priority number varying from 1 to 255, 255 being the highest (master). Default value is 100.

VRRP is intended for use with IPv4 only.

4.2 Terminology

- VRRP router

  A Router running the VRRP.

- Virtual Router

  An abstract object managed by VRRP. This router acts as a default router for other hosts. Virtual router is composed of a Virtual Router Identifier and a set of associated IP addresses it can use. VRRP router can backup virtual router.

- IP address Owner

  A VRRP router that has a real IP interface address that is associated with a virtual router.

- Primary IP address

  An IP address selected from a set of addresses. In VRRP advertisements primary IP address is always the source of IP packets.

- Virtual Router Master

  VRRP router that has the responsibility to send packets to IP addresses that are associated with a Virtual Router. A Virtual Router Master also responses to ARP request sent from associated IP addresses.

- Virtual Router Backup

  A set of VRRP routers available to do forwarding if the master should fail.

4.3 Example

A virtual router is defined by an identifier (VRID) and a set of IP addresses. This mapping between VRID and set of addresses must be coordinated among all routers. In order to minimize traffic only the master can send periodic advertisement messages. If the master is unavailable a router with the highest priority becomes master.

Here is an example of two VRRP routers and a set of nodes connected to them. Router 1 is the Master Router (MR) and it has the ID number 1 and permanent IP addresses A, which is associated to ID number (VRID=1, IP_Address=A). In according router 2 has the IP address (B) associated with its ID number. Router 2 acts as a Backup Router for router one (VRID=1, IP_Address=A).

Since router 1 has the priority of 255 it will become a master and router 2 will become backup router.

If router 2 would have connection to nodes that have IP addresses B then also router 2 would be a master. Then the routers would have different ID numbers and they would backup each other. In this case router 1 would have (VRID=1, IP_Address=A) and router 2 (VRID=2, IP_Address=B) and router 1 would backup router 2 (BR VRID=2) and router 2 would backup router 1 (BR VRID=1).

If backup router becomes master (i.e the router has IP addresses and its priority number is 255) it has to send advertisement messages and broadcast ARP request to each of its associated IP addresses. By this way all of the nodes will receive the masters MAC address.

Backup routers main task is to monitor the availability and state of the master router.

Fig. 3

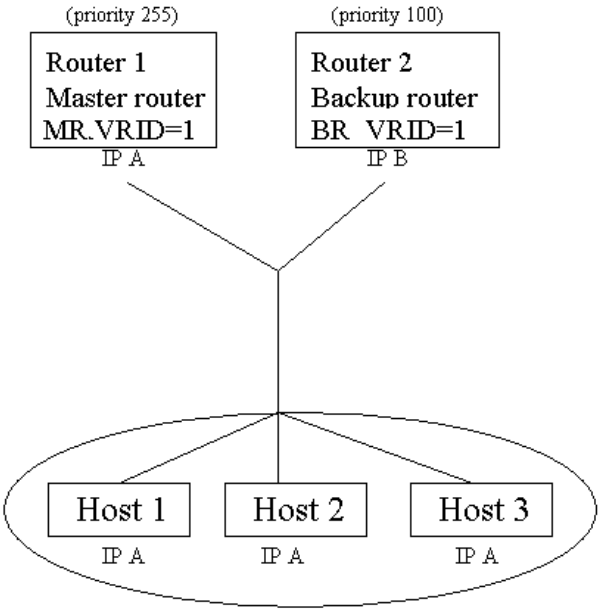

Figure 3: VRRP example

4.4 VRRP and mobile IP

The basic idea is that in the home network at least two routers act as Home Agents. They both have the same IP and MAC addresses. In order to maintain up to date information in the backup routers, backup routers information has to be updated. This is done in the boot sequence by sending data dump request to master router, which responds with VRRP data dump message, which contains all the associated IP addresses. After this the master router sends all received registration to the backup router using VRRP data forward messages. Thus is the case of failure the backup router will have all the necessary information. A common setup is done in such a way that two routers have one virtual network for each one and they backup each other.[4] [5]

5 Cisco Hot Standby Router Protocol

Cisco solution solves the problem when HA fails and thus mobility binding information is lost. The solution is based on Hot Standby Router Protocol (HSRP), which designates one router to be the active HA and another to be the standby HA.

The basic idea is very similar to VRRP. Two or more routers share the same IP and MAC address and in the case of Mobile Node movement exchange of mobility binding information is done.

Standby protocol runs over UDP. Packets are sent to multicast address 224.0.0.2.

Messages have clear-text eight character authentication data.

5.1 Terminology

- HSRP group

  A set of working routers acting as one virtual router. This creates an illusions that there is only one router. On one LAN there can be many groups, but they always operate independently.

- Active router

  The router that forward packets.

- Standby router

  A primary back-up router.

- Standby Group

  A set of routers all of which belong to a HSRP group.

- Hello time

  An interval between HSRP messages from a router.

- Hold time

  An interval between the time from the point when hello message arrives and assumption that the sending router has failed.

After the active router fails one standby router becomes active and another router is selected as a standby router if it is not already done so. Acting in a active group routers periodically advertise their state.

5.2 HSRP states

Routers advertise hello messages in order to indicate that they are capable of becoming a active or a standby router. If a router would like to become an active router it has to send Coup message and if it wishes not to be a active router it can send Resing message.

The main idea is that each router in a HSRP Standby Group executes state machine. All together there are six states:

1. Initial

   Starting stage. HSRP not running. This stage is entered when interface comes up.

2. Learn

   Router has not seen authenticated Hello message and it has not determined the virtual router IP address. Router is waiting to hear the active router.

3. Listen

   Router knows virtual IP address but is still waiting to hear from the active router. Virtual IP address can be learned from the Hello message of it can be configured to a router.

4. Speak

   Router participates in the election to be a active and/or a standby router. Router sends periodic Hello Messages and it has a virtual IP address.

5. Standby

   Candidate to the next active router. Periodic hello messages are sent. There can be only one standby router in one group.

6. Active

   Router forwards packages that are sent to the gruops virtual MAC address. Periodic hello messages are sent. There can be only one active router in one group.

A router has three timers

1. Active timer

   Used to monitor the active router. Started when the authenticated hello message is received from the active router. Expiries when Holdtime is 0.

2. Standby timer

   Used to monitor standby router. Started when the authenticated hello message is received from the standby router. Expiries when Holdtime is 0.

3. Hello timer

   Expires once per Hellotime period. If the router must send hello message it will do that after timer is zero.

Transitions between states happen in according to actions. In total there are nine actions, which contain starting active and standby timers (two actions), stoping the same timers (two actions), learning parameters from the hello message (one action) and sending Hello, Coup, Resign or ARP message (four actions).[7]

6 Comparison

In this section DHAA, VRRP and HSRP high availability mechanisms are compared with the following criterias: security, fail over and new relocation of HA, optimisation and load balancing.

6.1 Security

6.1.1 Overall security of Mobile IP

Overall Mobile IP security can be divided into four parts[4]:

1. Foreign Network where the MN is visiting.
2. Intermediate Network between HA and FA.
3. Home Network after HA router.
4. Correspondent Node Network where the node is connected.

Naturally the overall security is important and it should be as wide as the connection, which means end-to-end security. The problem is, however, that all the networks may belong to a different administrative domain and so they do not implement a single security scheme. The other problem is that security should be simple to use and if possible invisible. This means that the user does not have to make various security measures in order to trust the overall security.

Mechanism used in different layers with mobile IP security could be for example[4]:

1. Mobile IP specific security between nodes that participate in mobility. Usually a challenge - response system.
2. AAA (Authentication, Authorization and Accountability) to authenticate end-user and authorise tasks.
3. IPSec / IKE in the network layer.
4. Transport level security (secure socket).
5. Application level (for example PGP).

From these for example IPSec and PGP can be used without setting any demand for network hop-to-hop security.[4]

A significant problem might be between the Intermediate and Home Network. This is because the HA usually is behind a firewall inside in an administrative area. In such cases careful planning of the firewall rules must be done since the end point of the tunnel is not the actual node but the firewall. This means that the firewall must participate in key exchange and other security measures.

Overall the mobile environment is very vulnerable to many security attacks such as passive eavesdropping, active replay attack and other active attacks [9]

6.1.2 DHAA, VRRP and HSRP security in scope of HA

DHAA HA will process the incoming registration as stated in RFC-3344 [6]. Due to this HA supports authentication by using HMAC-MD5 algorithm.

However in DHAA in a Home Agent redirection situation authentication model is not precise. The problem is that MD5 algorithm is based on a secret key that both parties are aware of. Thus is a situation, where Mobile Node is redirected to a another Home Agent, we cannot be certain that the Mobile Node knows the key. To overcome this there are at least two solutions: The Mobile Node shares secrets with every HA or every key pair is configured manually. The first solution would perhaps be acceptable is a single administrative domain but the security would still be inferior to mobile IPv4. The second solution is better in the terms of security but it would demand major administrative work.

VRRP does not include any kind of authentication. This is significant problem since hostile routers can act as masters, which can lead to false ARP. VRRP does not also provide any kind of confidentiality. On the other hand VRRP has a mechanism to stop injection VRRP packets from another

network by setting the TTL to the value of 255. This limits the threat to local network [5].

HSRP offers no security at all, since the authentication field is clear-text. On the other hand HSRP uses multicast IP address 224.0.0.2 and thus it is unlikely that an attack from outside LAN would do any harm, since most of the routers tend to drop packets sent to this address[7].

In conclusion: DHAA is the only protocol, which has security measures implantedbut it also has unresolved problems when using MD5 algorithm. VRRP and HSRP on the other hand are feasible only in a closed administrative domain and additional security measures should be used with them.

6.2 Failover of old HA and relocation of new HA

When using DHAA and Home Agent becomes unavailable Mobile Node will have to try to find new Home Agent. In the worst case scenario a message is first sent to the HA that for example in administrative reasons will not accept the request. In such a case Home Agent might send an optional redirect-HA message to the Mobile Node that has to wait for the message and then contact the suggested Home Agent. In the case where originally requested Home Agent does not suggest alternative Home Agent a whole new Registration Request must be sent. In any case traffic will always have to router through MN and so time is lost. Time is also consumed during the authentication procedure.

The active connection is lost if the HA is changed. The time needed to find a new HA depends greatly on the network and the number of available Home Agents. An assumption can be made that this may take everything from a few seconds up to tens of seconds.

In VRRP a failure of master router (primary HA) is quickly compensated as the backup router (secondary HA) has the same routing table and can act as a master straight after the failure of master.

In HSRP HA failure is also compensated quickly since there are always standby routers (secondary HA), which have the same information as the active routers (primary HA).

In both VRRP and HSRP the secondary HA should be running as a primary HA in a few seconds. Because the time is so small and the secondary router has the same MAC address as the primary router it is possible that no packets are lost and so connection is maintained [11].

As a conclusion it is fair to say that VRRP and HSRP offer faster transition from primary Home Agent to secondary Home Agent than DHAA and they might maintain connection.

6.3 Home Agent optimisation

The fundamental difference with DHAA to VRRP and HSRP is that DHAA offers flexible redirection message in order to optimise routing. This redirection could be done for several reasons such as better bandwidth, lower latency or reliable router.

VRRP and HSRP on the other hand are used to backup the primary router with a router that functions with the same IP and MAC addresses as the primary router. Therefore VRRP and HSRP do not offer real time optimisation. On the other hand VRRP offers optimisation by giving a possibility to prioritise secondary routers by a number. In reality this means that routers current situation (for example load) must be monitored and according to routers state is will be given a priority number. Thus in a situation where Home Agent fails a router with the highest priority number will become the Home Agent.

HSRP does not implement such kind of system.

In conclusion in terms of optimisation it is fair to say that only DHAA supports a flexible selection of secondary Home Agent selection. VRRP also has a possibility to implement optimisation but it requires some kind of real time monitoring system for all routers. HSRP does not offer optimisation.

6.4 Load balancing

In DHAA routers (HA) can inform that they will not accept any more MN but they still can continue to serve current MN. In this way DHAA supports dynamic load balancing[6].

With VRRP it is possible to do load balancing since different routers can have different ID numbers and a set of IP address attach to them. In a same way HSRP can support load balancing between different HSRP groups.

Therefore we can come up to the conclusion that DHAA is the only one of these protocols that supports dynamic load balancing. VRRP and HSRP support static load balancing but they require the change of static information: in VRRP VRID number and a set of IP addresses connected to them must be changed and in HSRP new HSRP groups must be formed and hosts must be distributed to these groups.

7 Conclusion

In the beginning of this paper Mobile IPv4 was presented and a Single Point of Failure, the Home Agent, introduced. After that three protocols to eliminate the single point of failure were represented: HDAA, VRRP and HSRP and finally they were compared with a few key characteristics.

As a final conclusion we might say that DHAA is the most advanced protocol of these three. It supports dynamic load balancing, dynamic optimisation and it implements security measures. But, as most of the protocols, this one has its weaknesses: in the relocation procedure we can not be sure that the Mobile Node knows assigned Home Agents HD5 key that it needs in order to authenticate messages.

VRRP presents also a significant refinement to the single point of failure problem by presenting an efficient way of transferring from primary (failed) Home Agent to a secondary Home Agent. These protocols also support load balancing and optimisation although not in real time as HDAA did.

HSRP was also a moderate solution to a high availability problem, but this protocol merely offers a way to backup Home Agent.

Current redundancy protocols such as VRRP and HSRP are a significant part of the future but their role lies perhaps

only in a single administrative area where their main function is to guarantee efficient backup of routing tables of the HA. In this domain their implementation is easy and it will not have any effect on the network behind HA.

8 Future work

Mobile IP itself has been working application for many years. On the other hand mobile IP faces demanding requirements in the future since mobility will certainly increase.

In the future emphasis must be on the real time service development. What this basically means is that optimisation and load balancing without a break more than few second must be achieved. An early example of this is DHAA, which answers to many demanding needs: dynamic load balancing and authentication. Future work after DHAA is needed and the emphasis should be on the situation where devices do not belong to a single administrative domain.

Perhaps the most significant obstacle will be the need of support for the future protocols. Since these might require modification to current hardware and their software one can not be certain that high availability in IPv4 will be a huge success story without significant problems.

References

[1] P. Calhoun and C. Perkins. Mobile IP Network Access Identifier Extension for IPv4. Technical Report RFC 2794, IETF, 2000.

[2] S. Deering. ICMP router Discovery Message. Technical Report RFC 1256, IETF, 1991.

[3] R. Droms. Dynamic Host Configuration Protocol. Technical Report RFC 2131, IETF, 1997.

[4] U. Gustafson and J. Forslöw. Network design with Mobile IP. In *INET 2001 - Proceedings*, 2001.

[5] R. Hinden. Virtual Router Redundancy Protocol. Technical Report RFC 2338, IETF, 2004.

[6] M. Kulkaerni, A. Petel, and K. Leung. Mobile IPv4 Dynamic Home Agent Assignment. Technical report, IETF, 2004.

[7] T. Li, B. Cole, P. Morton, and D. Li. Cisco Hot Standby Router Protocol. Technical Report RFC 2281, IETF, 1998.

[8] C. Perkins. IP encapsuation within IP. Technical Report RFC 2003, IETF, 1996.

[9] C. Perkins. IP mobility Support for IPv4. Technical Report RFC 3344, IETF, 2002.

[10] J. Postel. User Datagram Protocol. Technical Report RFC 768, IETF, 1980.

[11] G. Vincent. Managing Multiple Routers at a Single Site. *InformIt*, 2001.