IP addresses configuration in spontaneous networks

RAQUEL LACUESTA GILABERTE
Systems Engineering and Computer Department
Zaragoza University
Ciudad escolar s/n 44003 Teruel. Aragón.
SPAIN

LOURDES PEÑALVER HERRERO
Systems Computer Department
Valencia Politecnic University
Camino de Vera s/n Valencia
SPAIN

Abstract: - To participate in IP networking, a host needs to be configured with IP addresses for its interfaces, either manually by the user or automatically from a source on the network such as a Dynamic Host Configuration Protocol (DHCP) server.

Many common TCP/IP protocols [1] such as DHCP [2], DNS [3][4], MADCAP [5], and LDAP [6] must be configured and maintained by an administrative staff. Other times, administrative staff won't be necessary, however we'll need the help of central servers to configure the network. This is unacceptable for emerging networks such as home networks, automobile networks, airplane networks, or ad hoc networks at conferences, emergency relief stations, and many others. Such networks may be nothing more than two isolated laptop PCs connected via a wireless LAN. For all these networks, neither will exist an administrative staff nor possibly will exist central servers that help to configure this data, then the users of these networks neither have the time nor inclination to learn network administration skills. Instead, these networks need protocols that require zero user configuration and administration. Spontaneous networks are an example of these networks, in which central servers don't usually exist, for this reason, the nodes will be in charge of both forming the network and configuring their IP address. In this article we deal with the problematic of IP addresses configuration in a particular case: spontaneous networks, we'll have into account the identifier ownership problems.

Key Words: - Spontaneous networking, IP configuration.

1 Introduction

The constant growth of the information technologies net infraestructure, in which a bigger number of devices such as PDAs, cellular telephones, televisions, and even appliances, is being constantly integrated, implies a demand of new methods to control, administer and integrate in a simple and flexible way all this amount of devices. The common techniques of manual configuration of parameters and also the installation of the software don't satisfy the necessity of more mobility, dynamism and users' friendliness [7]. The methods that are being studied at the moment not only for devices but also for services in spontaneous nets are based on imitating the behavior of the human relationships, which could be a solution to this situation.

We could define a spontaneous net as a net that is formed temporarily, with a small dependence or without any, on a central administration, and without expert users' intervention, to solve a problem or to develop a certain task. This net will be formed by a number of independent nodes that are in the same time and place and that can communicate among them. The nodes can go and come. An ad hoc network can be implemented over different kind of nets and not only over an ad hoc environment as for example over a wireless net with access point or even a wired net. Its objective is the integration of both services and devices in an environment that allows a user to have an immediate service without any manual intervention.

Among the tasks to carry out in the configuration of these nets will be included: the identification of nodes, authorization of these, assignment of addresses, service of names, operation and security.

2 Problematic

When configuring a spontaneous network one of the main problems that appear is the generation of unique IP addresses. Most of the routing protocols assume that the mobile nodes are configured a priori with an only IP address before becoming a part of the net, which is not true.

The problem arises due to the lack of knowledge of the topology of the net, neither when being initialized nor when its later modified. A node can be disconnected or can connect without any previous warning and at any time, To do so a protocol should be able to negotiate the generation of these IP addresses. The protocol should also be able to detect the existence of a duplicated IP address, which can arise when two subnets have joined, when a node has abandoned a subnet to which it belonged with an IP which was unique, or when forgery attacks take place.

Mobile nodes will need a unique address to communicate. This address could be shorter than 32 bits for the communication in the net; however most of the nodes bear IP addresses which are more suitable since the nodes could want to communicate with members from the Internet.

In a wired network the configuration is typically carried out by means of the protocol DHCP (Dynamic Host Configuration Protocol), which requires the existence of a central server to generate the IP addresses. Spontaneous networks don’t have central servers. Therefore this protocol or others aimed at nets with infrastructure won't be able to be used.

3 IPv4 vs IPV6

IPv4 presents several deficiencies, more remarkable every day that could be solved through the IPv6 protocol [8,9]. The Ipv6 maintains the good characteristics from IP, and discards and reduces the bad ones, and it adds new ones where they are needed.

Among the main characteristics of the Ipv6 it should be stood up that the addresses are 16 bytes long (128 bits versus the 32 bits of Ipv4), which solves the expected problem, to provide a practically limitless quantity of Internet addresses. The second main improvement of the Ipv6 is the simplification of the head, which only contains 7 fields (versus 13 in the Ipv4). This change allows the routers to process the packets at a higher speed and to improve, therefore, the efficiency. The third important improvement is a better support in the options. This change was essential with the new head, because fields that were before compulsory are now optional. It is also different the way the options are presented, doing it simpler to the routers not to pay attention to options that are not directed to them. This characteristic improves the processing time of packets. A fourth area in which Ipv6 represents an important advance is the security. The authenticity verifications and the confidentiality are the main characteristic of the new IP. Finally, a bigger attention has to be paid than the one paid in the past. Ipv4 in fact has a field of 8 bits dedicated to this matter, but with the prospective growth of multimedia traffic in the future, much more is expected to be required.

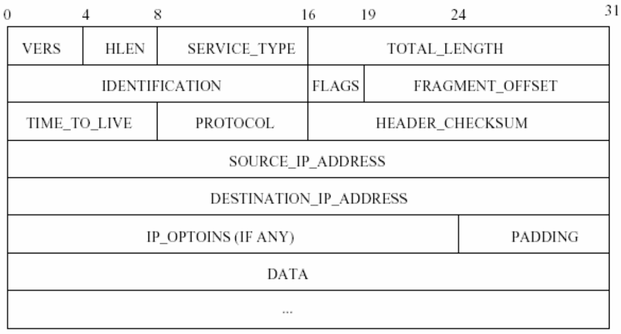

Fig.1. IPv4 packet header.

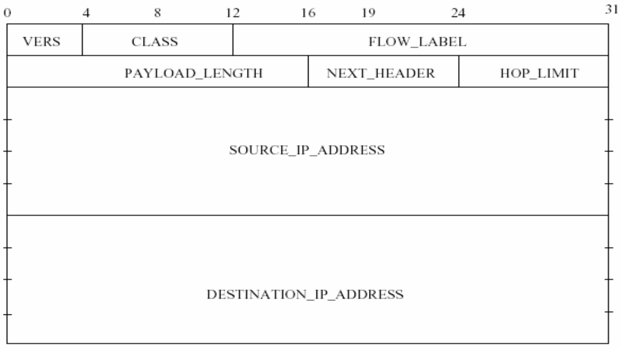

Fig.2. IPv6 packet header.

4 Current studies

The investigation area in autoconfiguration of addresses is based mainly on three problems: addresses generation, partition and union of nets and detection of duplicated addresses. In this last point the possibility of attacks of forgery addresses will be kept in mind; mechanisms that allow us to assure that a node is the owner of an address will settle down when we accept information from it.

Next some of the proposals outlined by the investigators in these areas will be treated.

In the protocol presented in [10] the address using a variable size can do assignment to the nodes. In this proposal when two nets join it is necessary that the nodes change their address if the number of nodes is bigger than the current size of their addresses.

In [11] a proposal of autoconfiguration protocol is presented using IPv4 both for the acquisition of the addresses and its maintenance as well as for the detection of duplicated addresses. Also, the nodes will execute the protocol DAD (Duplicate yourself

Address Detection) to guarantee the oneness of the selected address.

The initial address is selected randomly from the range of address 169.254/16. A difference with the protocol proposed in [12] where all the nodes maintain a list of all the IP addresses used in the net, is that in this proposal an address authority will be the one in charge of maintaining the existing routing information and of detecting partitions and unions. It won't trust (contrary to [13]) in a central node for the assignment of addresses but rather each node will obtain an only IP independently. The authority will have the function of helping to guarantee the oneness of this address, to negotiate the information of the node for a new use of the address and the maintenance of the net. Contrary to the proposals presented in [22,23] based on Ipv6 for the autoconfiguration of ad hoc nets, where a net identifier is obtained from an agent and the address of local connection is generated based on its MAC address. In this protocol it won't be able to introduce the MAC since Ipv4 will be used.

To solve address conflicts the protocol uses two versions, one is strong DAD in which double addresses cannot exist at any time. The other one is weak DAD in which in a given moment duplicated addresses can exist and measures are taken to prevent that a packet is sent to an erroneous destination. In this protocol a dynamic configuration of IPs is pursued, maintaining uniqueness, robustness, light overload and spreading.

To assure a correct routing each node will have a unique IP address and each independent net will have its corresponding unique identifier.

This solution doesn't work correctly in complex scenarios, as when a net can be the object of partitions and mixtures.

In [14] the steps a host takes in deciding how to autoconfigure its interfaces in IP version 6 are specified. The autoconfiguration process includes creating a link-local address and verifying its uniqueness on a link, determining what information should be autoconfigured (addresses, other information, or both), and in the case of addresses, whether they should be obtained through the stateless mechanism, the stateful mechanism, or both. This document defines the process for generating a link-local address, the process for generating site-local and global addresses via stateless address autoconfiguration, and the Duplicate Address Detection procedure.

In Ipv6 stateless autoconfiguration no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers are required. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. Combining the two forms an address is generated. In the absence of routers, a host can only generate link-local addresses. However, link-local addresses are sufficient for allowing communication among nodes attached to the same link.

To negotiate nodes mobility is usually proposed the use of servers DHCP [15].

On the other hand, the work group of Zero Configuration [24] [25] of IETF is defining a standard to allow to work in nets without the need of configuration without administration. Their work is focused on small nets (home or small offices) to endow them with such functions as the addresses handling, names assignment, and localization of services, with some equivalent requirements of security to the fixed nets. These functionalities are those required in the spontaneous nets, nevertheless, the mechanisms can be different. Zero Configuration can support a router at least. They also operate in more static environments, therefore the configuration works in a more stationary state. Ipv6 has already considered some of these functionalities.

If we analyze the problem of forgery addresses in spontaneous nets it is possible to observe that many of the consulted authors use techniques of IP generation from data that allow them to identify the nodes. For example, in [16] to establish the IP address the idea that is adopted was designed originally to solve the problem of address property in mobile Ipv6. The IP address is derived by starting from the public key of the node. First it is done a hash to this key and later on from this value the IP address of the node is built. The advantage is that it doesn't exist the necessity of certificates to join the address of the node with its public key and it doesn't exist since one has been derived from the other in a verifiable way. Once a secure association has settled down and it has been verified that the address of the node matches its public key the author proposes the use of symmetrical keys to continue the communication.

In MIPv6 (Mobile Ipv6) [17][18] a mechanism is described so that a mobile node can move freely along the net links and to remain accessible the whole time through a home address that is statistically located in its initial net. When the node is far from its first net it begins to make use of the care-of address located dynamically in the net where it is at that moment. A well-known proxy as the initial agent will be the responsible for sending packets that should arrive to the initial net through the care-of address of the mobile node. The mobile node will inform at any time to its initial agent where it is sending a necessary message to upgrade. In it its initial address, its current care-of address, and a lifetime has to be attached. Each initial agent will maintain an obligatory cache.

MIPv6 demands the use of the authentication IPSEC (IPSEC AH) for the obligatory upgrade and knowledge messages (ACK). This prevents an impostor to cause that the whole traffic for a mobile node is not well forwarded emitting false obligatory upgrades since the objective of the ACK messages will be to counterattack DOS (Denial of Service) attacks.

Ipsec [26], on the other hand, is an extension to the IP protocol that provides security to IP and the upper layer protocols. It was developed for the new standard IPv6 and later IPv4 carried it out. The architecture IPsec is described in [8].

To protect the integrity of the IP datagrams, the IPsec protocol uses codes of message authentication based on hash (HMAC - Hash Message Authentication Codes). To calculate these, HMAC protocols use algorithms such as MD5 and SHA to calculate a hash based on a secret key and in the contents of the IP datagram. The HMAC is included in the head of the IPsec protocol and the receiver of the packet can check the HMAC if it has access to the secret key.

To protect the confidentiality of the IP datagrams the IPsec protocol uses standard symetrical algorithms to encode.

The manual configuration of the association of security is prone to errors, and it is not very safe. The secret keys and encoding algorithms should be shared among all the participants of the VPN. One of the critical problems of those that the administrator of systems faces is the exchange of keys: how to exchange symmetrical keys when any type of encoding has not been settled down yet?

To solve this problem the key exchange protocol was developed by Internet (IKE - Internet Key Exchange Protocol). This protocol authenticates the participants in a first phase. In a second phase the associations of security are negotiated and the symmetrical secret keys are chosen through an exchange of Diffie Hellmann key. The IKE protocol is even in charge of renovating the keys periodically to assure its confidentiality

The authentication of the participants in the first phase is usually based on previously shared keys (PSK - Pre-shared keys), RSA key and certified X.509.

In [19] a protocol is provided that takes into account both problems, the generation of IPs and the detection of duplicated addresses. Each mobile node uses a partial hash of its key. It publishes it to generate its IPv6 address. The proposed protocol, CAM (Child-hood Authentication for MIPv6), integrates the distribution of keys and it protects against the forgery of net addresses.

This protocol aims to improve the security of MIPv6 in absence of IPSEC. It is built on characteristic of the implementations of Ipv6 and IPSEC and according to their authors it is a light protocol as it doesn't need any manual configuration and it incurs in a minimum exchange of messages in relation to IPSEC and IKE [20]

In this system the mobile node chooses an initial address incorporating a cryptographic hash of its public key. Contrary to other authors the whole hash is not used here but a part of it. The possession of an IP address is established by demonstrating the knowledge of the private key. Also, this address will be difficult to forge due to the difficulty of finding a given hash of public-private couple of keys, however this address will be easy to verify. The detection of repeated packets will be carried out through the synchronization of clocks.

For the detection of published addresses Ipv6 will be used. The conflicts will be able to be solved without the need of the mobile node to do anything. For that a modifier i will be generated and remembered (of one or two bits). This will be added later on to the public key before the generation of the hash. If the problem doesn´t disappear this should be done again until it does.

This protocol doesn't defend against the DoS attack (Denial of Service) in which an attacker wants to overload the net through a great number of messages. In this case, some alternative protocol should be implemented as IKE.

CAM only considers the authenticity of the obligatory upgrades and the option of maintenance of home addresses. The rest of shippings of information are not guaranteed. Because of this, CAM will only be used when the number of required packets for authentication is small, otherwise the use of IKE and IPSEC AH will be better , since in this case CAM will be less efficient. CAM could be used for example as the base for the establishment of the associations of IPSEC security.

In [21] the routing attacks to Ipv6 again are studied, in this case they focus on the DdoS attack (Distributed Denial of Service)

In some of these attacks source forgery addresses are used and can even have the same prefixes that the real addresses of the committed nodes used for the attacks. This article is focused on the difficulty of distinguising between the behavior of committed nodes that carry out prefix forgery attacks and the behavior of the nodes that use temporary addresses. Due to this it becomes difficult to identify the DdoS attacks.

To avoid these attacks they outline the modification of private extensions for the address autoconfiguration. This way, identifier of the interface will be modified and with it, the addresses of the nodes for the different transactions. With this it will become more difficult to carry out eavesdropping and it will be easier the detection of the attackers nodes whose IPs aren't modified in the different transactions.

5 Conclusions

The generation of not duplicated IP addresses is one of the tasks that requires special attention when we talk about spontaneous nets configuration. Because of these, mechanisms that get the IP of a node from random numbers, MAC address, public keys of the nodes or hash functions are used. In spontaneous nets, due to the existence of central nodes, it will not be fundamental that the nodes self-manage this configuration. To do so in first place, techniques that minimize the possibility of conflicts in the IPs assignment should be looked for and later on techniques that allow to detect and solve the possible duplicated IP addresses. The routing problem is increased if other nodes can forge these IPs; if this happens a node will be able to attack the net by making itself appear to be a part of the net. For it, it is necessary the establishment of mechanisms that allow nodes to check the authenticity of the IP addresses of the nodes. The mechanisms outlined to generate these addresses help to the later authentication of these addresses. In this article this problem has been studied as well as some of the solutions outlined in the bibliography

References:

[1] A.Williams, "Requirements for Automatic Configuration of IP Hosts". Internet-Draft. Zero Configuration Networking. September 2002.

[2] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[3] Mockapetris, P.,"Domain names- concepts and facilities", STD 13, RFC 1034,
November 1987.

[4] Mockapetris, P.,"Domain names- implementation and specification", STD 13, RFC 1035, November 1987.

[5] Hanna, S., Patel, B. and M. Shah, "Multicast Address Dynamic Client Allocation Protocol (MADCAP)", RFC 2730, December 1999.

[6] Wahl, M.,Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[7] Stephan Preu, Clemens. H. Cap. Overview of Spontaneos Networking-Envolving Concepts and Technologies.

[8] Robotiker. "Introducción e historia del Ipv6" Vigilancia Tecnológica. Revista Nº 12.

[9] Manuel de la Parra, Verónica Rico, Carlos Villaseñor, Conchita Mendoza. Ipv6-Task Force.

[10] J. Boleng. Efficient Network Layer Addressing for Mobile Ad Hoc Networks. March 1999.

[11] Yuan Sun, Elizabeth M.Belding-Royer. "Dynamic Address Configuration in Mobile Ad Hoc Networks"

[12] S. Mesargi and R. Prakash. "MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network".2002.

[13] P. Patchipulusu. "Dynamic Address Allocation Protocols for Mobile Ad Hoc Networks". August 1997.

[14] Thomson, S. and T. Narten, "Ipv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[15] G. Montenegro, "Reverse Tunneling for Mobile IP", January 2001

[16] G. Montenegro and C. Castelluccia. "Statistically unique and cryptographically verifiable (SUCV)"

[17] Johnson, D. and Perkins, C. Mobility Support in Ipv6. Internet Draft. April 2000.

[18] Kent, S. and Atkinson, "R. Security Architecture for the Internet Protocol" RFC2401. November 1998.

[19] G. O'Shea, M. Roe "Child-proof Authentication for MIPv6 (CAM)" Microsoft Research Ltd, Cambridge

[20] Harkins, D. and Carrel, D. "The Internet Key Exchange (IKE)". RFC 2409. November 1998

[21] T. Narten, R.Draves "Privacy Extensions for Stateless Address Autoconfiguration in Ipv6" RFC3041. January 2001.

[22]M. Gunes and J. Reibel. An IP Address Configuration Algorithm for Zeroconf. Mobile Multi-hop Ad-Hoc Networks. September 2002.

[23] K. Weniger and M. Zitterbart. Ipv6 Autoconfiguration in Large Scale Mobile Ad-Hoc Networks. February 2002.

[24] A. Willians, "Requirements for Automatic Configuration of IP Hosts draft-ietf-zecoconf-reqts-12.txt. Internet-Draft,September 2002

[25] A. Willians, “Zeroconf ip host requirements draft-ietf-zeroconf-reqtts-10.txt.Internet Draft, 2002

[26] http://www.ipsec-howto.org/spanish/x161.html