Zero Configuration Networking, autumn 2002

EERIKKI AULA
Helsinki University of Technology, Espoo

Traditionally networking has required exhaustive configuring. There has been several vendor specific solutions for easily configured networks. Zeroconf WG is working for IP based, global protocol for automatically configured networking.

Automatically configured networks working parallel with traditional networks open possibilities for completely new kind of networking. It isn't feacible to connect small appliances to internet without some easy way to configure them. Zeroconf proposes to produce a protocol enabling this.

1. INTRODUCTION

Internet Protocol was originally designed for scalability, and it has worked well. However, current networking requires a lot of configuration. For large networks this is feasible, but there is a growing demand for smaller networks: home networks, adhoc networks and networks with domestic appliacens. There must be an easier way to configure these.

Zeroconf Working Group[1] is working to produce protocols for automatic configuration of IP networks. With no need for exhaustive configuration, even small devices with limited computing capacity can be attached to IP networks.

This paper introduces the requirements for zero configuration networking. First the paper goes briefly through all the fields of study of the Zeroconf WG: IP autoconfiguration, Domain Name Configuration, Service Discovery, Automatic Allocation of Multicast addresses and security implications of automatic networking. On later sections the paper goes deeper into IP autoconfiguration and security issues.

2. MAJOR FIELDS OF ZERO CONFIGURATION

This section gives short introduction to all the different parts of automatic networking the Zeroconf WG is studying. On later sections the paper goes deeper into IP Address Configuration and Security implications.

2.1 IP Address Configuration

Traditionally, even dynamically configured IP hosts need to configure several options. Both static and dynamic configuration need professional system administrators. Automatic configuration aims for easier joining to small networks.

Hosts with automatically configured settings must be able to come up with unique IP addresses in the scope of the autoconfigured networks. They must also have some uniform configurations such as netmask: every host in the same subnet must have the same netmask. Additionally, networks must work even if there are no services available, such as DNS or routers. As two subnets might merge at any time, hosts must periodically watch for conflicts, checking for conflicts only on joining isn't enough.

2.2 Domain Name Configuration

When IP addresses are automatically configured, hosts IP address may change in the middle of the session. Host names are used to keep connection persistent when IP addresses change. There must be an automatic way to map these names to IP addresses. In the absense of DNS server hosts must handle the name to address translations themselves.

There might be conflicts in the chosen names, so hosts must detect and resolve conflicts in names, just like they do with IP addresses. As with IP addresses, hosts must detect conflicts with names and resolve them constantly as new hosts join and leave network.

Author's contact information: Eerikki.Aula@hut.fi

Published in *Internet Protocols for Mobile Computing - Seminar on Internetworking, Autumn 2002*, by Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory. The complete publication can be found at http://www.tml.hut.fi/Studies/T-110.551/2002/papers/December/index.html.
ISBN 951-22-6272-X - ISSN 1455-9749 - HUT - TML - TML-C9

There are two different solutions for name to address translation. First involves Multicast DNS[2]. This means all the hosts actively listenn to DNS queries and reply if their own name is requested.

Second solution works only in IPv6. It upses ICMP messages for "IPv6 Node Information Queries". This works quite similar to the first solution.[3]

2.3 Service Discovery

In order to any networking to be happening the hosts must be able to discover the address of other hosts. Usually they need some kind of service, which they must be able to find automatically. There are two distinct cathegories in services. First cathegory is global services such as DNS, where the host doesn't care which server responds, as long as somebody does. The second cathegory includes services such as printers, where host needs to access some specific service provider. The addresses of servers can be found in one of several methods. We'll go briefly through some possibilities.

If the network has DHCP[4] server, it might be able to provide some addresses of different services. This would perhaps be in addition to the other protocols. And, even the DHCP server itself could be located automatically with the other protocols.

Service Location Protocol, SLP[5], uses queries for different services. These queries help clients to request for different types of services with different parameters.

Lightweight Directory Access Protocol LDAP[6] is used for sharing files and directories. This lightweight protocol suits well to the resource limited autoconf networks.

Nameservers are a crucial part of normal internet. In the bigger automatically configured networks there most likely is one or more DNS servers available. Using DNS SRV[7], domain name servers can advertise different kinds of services. They could be asked for a certain type of service, and if they know a server providing it, they could provide the address and the parameters of the server.

2.4 Automatic allocation of Multicast Addresses

Another field needing special solutions is multicast addressing. Zeroconf Multicast Address Allocation Protocol ZMAAP[8] provides solutions on how hosts can allocate unique multicast addresses. These addresses must be defended against collisions just like normal automatic IP addresses. Multicast addresses are more complicated to handle than normal IP addresses, as they are a shared resource.

Zeroconf multicast networking concentrates on small scale multicasting, so scalability isn't quite as much an issue as in regular multicasting.

2.5 Security Issues

This subsection goes briefly through the security issues imposed by zero configuration networking. Security will be addressed more deeply in section 5. Naturally, automatically configured networks have all the same security issues as statically and dynamically configured networks. Zero configuration also brings new things to be considered.

Because this protocol will be part of the Internet Protocol suite, it musn't be less secure than the existing solutions. How this is archieved, is yet to be solved.

Security runs opposite to zero configuration. As security cannot be omitted, zeroconf networks require at least some configuration. The goal of Zeroconf WG is to make the options as easy as possible to configure. However, things will never be totally automatic.

3. IP ADDRESS CONFIGURATION

As shown earlier in this paper, automatic configuration of network addresses is needed for new applications, adhoc networks, small networks and networks of home appliances and other small devices new to networking. There are several vendor-spesific products, but global standard of IP based solution is needed for universal manufacturer-indepent networks.

This section covers in detail, how the automatic configuration of IP hosts is to be done. First the paper goes through how the different settings are negotiated. Then there is explanation on how onnections are kept alive in dynamic situations. Although Zeroconf WG works both on IPv4 and IPv6, there are some differences in different places. The last part of this section covers the differences and similarities of automatic configuration with IPv4 and IPv6.

3.1 Requirements

The main goal of Zeroconf WG is to produce RFC:s to describe how automatic configuration should be done. The actual protocols will be designed later, after the requirements are ready. When this paper was written, Zeroconf WG hadn't yet published any RFC:s, only Internet-Drafts. The work on requirements is still in progress. [9]

3.2 Persistence

Hosts leaving and joining the networks should be assigned constant addresses, if possible. When host rejoins a network, it should be assigned the same IP it had the previous time, if it's available. This can be accomplished, for example, by choosing the address with pseudo-number generator with consistent seed. The seed can be eg. the hosts hardware-interfaces address. If the host has some kind of RAM, it could also remember the previous address, and try to acquire it when rejoining.

The protocol for choosing address is different in IPv4 and IPv6, as the address space in IPv4 is much more limited.

3.3 Routing

Automatic networking must work even when there are no routers available. This means every host must actively participate in the routing process. Because the hosts in zeroconf networks usually are in the same physical link, this doesn't propose a big problem.

3.4 Collision detection

As networks are constantly changing, several networks might be joined at any time. Hosts musn't rely on their IP addresses to remain collision free after acquiring them. Instead, every host must actively participate in collision detection: they must constantly watch for conflicts and be ready to automatically solve them.

Collision detection can be done by ARP messages. When host receives ARP packet from hosts own IP address with different 'sender hardware address', host must resolve this conflict. This can be done in two different manners: either by changing own IP address immeditially, or by defending the address.

Collision detection opens new kind of denial-of-service attack, where malicious host sends arp-replies to all IP:s reserved in the network in question. This causes all the hosts to circle through addresses trying to find free one. Zeroconf WG must find a way to prevent this kind of attack. How this is to be accomplished is a mystery.

4. CONNECTION TO GLOBAL INTERNET

One of the major motivations of IP based automatic network configuration is the connection to global internet. This opens several new possibilities for future applications. It is required that the automaticly configured network is as safe as dynamic or static networks. How this is to be accomplished is yet unknown. We'll see more on security on section 5.

This section tells how the communication between automatically configured and regular networks is done. As automatically configured addresses are only valid in the local scope, hosts willing to access the global Internet must acquire global IP settings. We'll see two different solutions on transformation from automatically configured to static/dynamic addressing. Originally the transition was to be done exclusively: when host acquires global IP settings it discards the automatic configurations. New protocol is to maintain both addressings parallel.

4.1 Global settings overriding autoconfigured settings

This was the original idea. However when host discards automatially acquired settings, it also discards all the connections based on them. Also, there might be hosts only capable of automatically gained settings, which are unreachable when using global settings. There already are some implementations using this type of addressing, so it cannot be discarded from the protocol.

4.2 Autoconfigured settings parallel to global settings

New protocol suggests hosts to keep automatically acquired settings upon acquiring global settings. This way all the services and connections in automatically configured network stay the same, while the global settings enable new connections to normal Internet.

Because hosts can use both types of addressing, the transition from zeroconf networking to global network is smooth. However, this requires all hosts to keep two different IP stacks, one for both types of networking. For IPv6 hosts this is easy, because they are already required to be able to handle several IP addresses.

5. SECURITY ISSUES

As mentioned earlier, automatic configuration isn't possible with the requirement for security. This section first addresses the status of security in zeroconf. Then there are some spesific issues conserning automatic configuration. Last is a thought about security and the need of a change in the way people think about computer security.

5.1 Status of security in Zeroconf WG

There are a lot of issues unsolved about security. Several aspects are only requirements, with no solutions on how to address the issues. There has been no suggestions on how to make automatically configured networks as safe as traditional networks.

The need for configuration is yet to be addressed. The configuration should be as simple as possible, but how this is to be done is yet to be solved. It is important to find out the different security problems in order to come up with solutions to them. Next we'll see some of the security issues characteristics to zeroconf, most of which are unsolved for the time being.

5.2 Security issues in automatic configuration networks

ARP vulnerabilities
Every host is required to probe for conflicts with ARP messages[10]. This proposes a new denial of services attack, where malicious host replies to all queries with IP reserved message. This means all the hosts in that connection are in endless loop through IPs trying to reserve one. This problem must be solved, but, as in the most of the other security issues, the solution is yet unresolved. [11]

Eavesdropping
As many of the automatically configured networks are wireless, the risk of eavesdropping is big. There must be ways to both be able to protect the connections. IPsec[12] is one solution, but it might require too much computing for some devices.

5.3 Security in the Internet

The hosts connecting both with automatic configuring mustn't be any less secure than traditional hosts. Zeroconf WG is currently working on the requirements on what is needed to be done. How these requirements are to be met is an open question.

5.4 Security solutions

IPsec is a good way to protect the traffic in unprotected links. This of course requires some kind of configuration, but often it is worth it. However, IPsec requires more calculation power than some of the small hosts might have.

With physical link hosts often can rely on the physical security. For example, home heating system might be physically connected to a computer, which can be safely accessed from outside. It is reasonable to trust that the physical link is safe enough in this kind of cases.

5.5 Security in practice

Currently security in computers is considered as necessary evil that somebody else is hired to ensure. The attitude towards security must be changed so, that everybody thinks it necessary, and normal cause of action.

People are used to trust physical security in computer world too. With wireless networks this doesn't hold true anymore. Everybody must start protecting the connections as automatically as locking doors when going out. [13]

6. USERS VIEW

This section views automatically configured networks from normal users perspective. First there is some discussion about the motives of zeroconf networking. Then the section tells about current situation and last there are some possible future scenarios.

6.1 Motives of Zeroconf Networking

Traditional networks are cumbersome to configure. With automatically configured networks user can set up a small home network just as easily as plugging in a television set. In the future zeroconf networks enable a large amount of different uses, eg. the traditional example of refridgerator automatically ordering missing groceries. Many of the future uses are propably something nobody has yet thought of.

6.2 Small networks

Already today there are solutions on automatically configured networking. Earlier Apple versions had protocols for automatically connecting to another Apple, but new Mac OS X Operating System uses Zeroconf protocols under trademark Rendezvous. This enables users to form IP networks with both Apples, and other Zeroconf compatible hosts.

First users of zeroconf networks are propably different games: players only need to connect two hosts directly, or several hosts through a hub, and everything works automatically. Another use is meetings in companies. Participants just need to plug their laptops to the hub in conference room, and network is set without the need of configuration.

6.3 Networks for small appliances

Currently there are some nice bluetooth applications, eg. bluetooth cellural phone with carkit installed. When the owner gets in his/her car, bluetooth automatically transfers the calls to the cars phonesystem.

In the future, there will be similar IP based applications. However, with IP products, the car might notice the arrival to the garage and notify the phone to transfer control to the house phone system. Also, with standardized IP networks, even the passagers could perhaps be able to connect to the car they are currently riding with.

7. CONCLUSIONS

Traditional ways of configuring networks aren't sufficient for the new emerging small networks. There are several vendor specific solutions, but a global IP based solution is required for networks compatible with different types of hosts. Already there is support for automatic configured networks in new operating systems: Apple has implemented Zeroconf's protocols under the trademark of Rendezvous.

The possibilities in the future are countless, from small gaming networks to home network. There could be home network where VCR negotiates with television set about when the programs begin, and user can access both of them from work through home control computer. However, there are a lot of things to solve before this is reality. Currently not even all the requirements are ready, not to mention the protocols meeting the requirements. Security is still a big issue, and long way before everything is solved..

Currently Zeroconf WG is refining the Internet Drafts about the protocols. In the near future Zeroconf will be working both on new requirements, and solutions to unsolved ones. The goal is to produce finished RFC:s once the protocol suite is mature enough.

REFERENCES

[1] Zero Configuration Networking Working Group charter page,
URL: http://www.ietf.org/html.charters/zeroconf-charter.html

[2] STUART CHESHIRE, Performing DNS queries via IP Multicast, Internet draft, Joint effort of Zeroconf WG and DNS Extensions WG, Jul. 2002; Work in progress.

[3] THOMSON S., NARTEN T., IPv6 Stateless Address Autoconfiguration, RFC 2462, December 1998, URL: http://www.ietf.org/rfc/rfc2462.txt

[4] DROMS R., Dynamic Host Configuration Protocol, RFC 2131, March 1997, URL: http://www.ietf.org/rfc/rfc2131.txt

[5] GUTTMAN, E., PERKINS, C, VEIZADES, J., AND DAY, M., Service Location Protocol, Version 2, RFC 2608, June 1999, URL: http://www.ietf.org/rfc/rfc2608.txt

[6] WAHL, M., HOWES, T, AND KILLE, S., Lightweight Directory Access Protocol v3, RFC 2251, Dec 1997, URL: http://www.ietf.org/rfc/rfc2251.txt

[7] GULBRANDSEN, A., VIXIE, P., A DNS RR for specifying the location of services (DNS SRV), RFC 2052, October 1996, URL: http://www.ietf.org/rfc/rfc2052.txt

[8] CATRINA OCTAVIAN, THALER DAVE, ABOBA BERNARD, GUTTMAN ERIK, Zeroconf Multicast Address Allocation Protocol (ZMAAP), Internet draft, Zeroconf WG, Oct. 2002; work in progress.

[9] GUTTMAN ERIC, Autoconfiguration for IP NETWORKING: Enabling Local Communications, Online, updated May 2001.
URL: http://www.zeroconf.org/w3onwire-zeroconf.pdf

[10] WILLIAMS, A, Requirements for Automatic Configuration of IP Hosts, Internet draft, Zeroconf WG, OCT. 2002; work in progress.

[11] CHESHIRE STUART, IPv4 Address Conflict Detection, Internet draft, Zeroconf WG, Oct. 2002; Work in progress.

[12] IP Security Protocol Working Group charter page,
URL: http://www.ietf.org/html.charters/ipsec-charter.html

[13] GUTTMAN ERIC, Zero Configuration Networking, Online, Oct 2002,
URL: http://www.isoc.org/isoc/conferences/inet/00/cdproceedings/3c/3c_3.htm