Quality of Service in home network: VLAN zeroconfiguration network

Aurelio La Corte* and Sabrina Sicari

Department of Informatics and Telecommunication Engineering,
University of Catania, Italy
Fax: +39 0957382397 E-mail: aurelio.lacorte@unict.it
E-mail: sabrina.sicari@unict.it
*Corresponding author

Abstract: The device proliferation jointly to the necessity of being constantly connected to the network is considered the cause of the need of 'Autoconfiguration'. At the same time, it is necessary to guarantee an adequate level of quality of service. So, we propose to use together zeroconfiguration protocols and Virtual LANs.

Keywords: Quality of Service (QoS); home network; zeroconfiguration network; autoconfiguration; Virtual LAN (VLAN).

Reference to this paper should be made as follows: La Corte, A. and Sicari, S. (2006) 'Quality of Service in home network: VLAN zeroconfiguration network', *Int. J. Internet Protocol Technology*, Vol. 1, No. 4, pp.228–235.

Biographical notes: Aurelio La Corte received the Degree in Electrical Engineering from the University of Catania and the PhD Degree in Electronic and Computer Science in 1988 and 1992, respectively. Since 1994, he has been at the University of Catania, where he is now an Associate Professor of Telecommunications Networks. His current research interests include mobile systems, QoS management, multimedia traffic modelling and digital signal processing.

Sabrina Sicari received her Degree in Electronic Engineering from University of Catania, Italy in 2002. In March 2006 she completed her PhD in Computer Science and Telecommunication Engineering at University of Catania. During this period she spent one year at DEI, Politecnico of Milan under the guidance of Professor Carlo Ghezzi. Now she works at University of Varese at the Department of Computer Science and Communication. Her current research interests include quality of service, mobile communication, network security and risk analysis.

1 Introduction

Today, the requirement of being constantly connected to the network and to satisfy, through applications and available services, varied requirements is always stronger. The customers wish to be able to choose among a wide suite, at their disposal, the service that better meets their needs, and this is the reason because they do not want to be bound to a single service provider. Customer may not want to reshape, every time there is the plug of a new device, or every time, in general terms, there is a change (Teger and Waks, 2002). At the same time, there is the necessity to integrate several telephone systems and several services, to share files and I/O devices, to protect systems and data from external attacks and to communicate with the external world. Today, the last requirement is extremely important, because people want to communicate with *anyone*, *anytime*, *anywhere* and *by anything*, possibly with the guarantee of an appropriate QoS. In this context, Home Digital Network, Home Automation, Smart Home, Home Network and Medium Home Network are various ways in order to refer to the intention, by now diffused, to extend the networking concept also to domestic environment (Wacks, 2002; Valtchev and Frankov, 2002). In last years, actually, there has been a growing proliferation of digital electronic objects that, in a more and more sophisticated way, every day, assist customer in the development of their home activity. The possibility to interrogate and to manage domestic devices from the outside and, at the same time, to connect various domestic devices so as to realise a distributed system and to be able to control them in an integrated way represents customer requirements, today.

Houses are wired; for this reason interconnection of several devices could be easy to realise. However, several types of cables are optimised for specific scopes: electrical wires to connect to power supply, telephone wires to provide telephone and coax cable to provide video from cable to satellite feeds. A lot of protocols cover several network layers, even including application layer. The number of communication technologies, used in order to interconnect these subnets, is in constant increase, including Bluetooth, HAVI, IEEE 802.11, IEEE802.15, IEEE 1394, Jini, Home PNA and UPnP (Dobrev et al., 2002).

At the state of art, there is no protocol in a position to satisfy all requirements, because of different physical characteristics and cost of the large heterogeneity of devices

and applications that are inside domestic world (Valtchev and Frankov, 2002). However, customers are interested in service they receive and they pay for and not in the communication protocol they use; the choice must turn out transparent to all (Dobrev et al., 2002). Our houses are full of stand-alone applications.

The target of home automation is not substitution of all existing applications with one only centralised machine that makes everything. Applications must be able to work independently, but, at the same time, they must be in a position to share resources. Home networks allow these applications to be integrated (Wacks, 2002). Integration of the home device into a home system allows creation of applications in a position to supply a lot of innovating services.

By the interoperability of several devices, it is possible to get a unit that is managed in an integrated and efficient way, so as to be able to optimise the use and consumption, to program operation on the base of the need and, even, to control and to monitor at distance.

In order to realise an effective integration of home devices, important standards and consortia programs have been developed since mid-1980 (Teger and Waks, 2002), with the objective of:

- Guaranteeing remote control of several devices.
- Developing a low-cost interface unit.
- Managing a lot of transmissions, guaranteeing, at same time, communication protocol independence from used technology, adopted for home devices.
- Providing a fair method for devices to access a shared medium; however, allowing time critical application higher priority in gaining communication services.
- Allowing applications and members to be added to the network and be removed in a transparent way for the customer. This feature is called 'Plug and Play'.

The interoperability of large variety of technologies and devices that are in a home environment is possible by using, as bridge of connection, the IP protocol. Through a convergent system based on IP, services are possible of remote control, diagnostics, management video on demand, interactive TV and so on.

Domestic customers have the necessity of devices that are able to autoconfiguration: each device must be able to find and to communicate with its peers – whether connected directly or indirectly over a Local Area Network (LAN), without special configuration or other technical effort by the user. The address autoconfiguration feature is built into the IPv6 protocol, enabling a large number of IP hosts to easily discover the network and get a new and globally unique IPv6 address, associated with their location. As the result, network devices could connect to the network without manual configuration and without any server, such as DHCP server (Fink, 1999).

In IPv4, such feature is not present, being necessary a manual configuration of network or through DHCP server. While waiting that IPv6 is diffused, in order to realise a *plug and play* system in an IPv4 environment, it is possible to use the *zeroconfiguration* networks (Guttman, 2001). These constitute a class of IP networks that does not need any administration or manual configuration. In July 2003, IETF zeroconfiguration-working group concluded its works and wrapped up because it could not come to a consensus. This WG produced one protocol specification, describing automatic generation and assignment of link-local IPv4 addresses in environments lacking host configuration (static or using DHCP) (http://www.zeroconf.org/zeroconf-charter.html). According to us, zeroconfiguration network represents a good solution to guarantee plug and play inside a home network; so we decided to use it in our work.

A lot of home devices have various requirements and ask the network for different levels of QoS. To guarantee QoS is one of the key issues in realisation of every telecommunication system, and, therefore, also, of a home network. The QoS term is used under many meanings ranging from user service perception.

In a LAN, in general terms, and in a zeroconfiguration network, in particular, the QoS guarantee is strictly linked to the mechanisms that can be implemented at the second level of the protocol architecture. The joint use of VLAN and priority policies to manage traffic generated from home devices can be a solution in order to guarantee various levels of quality to several home devices. In this paper, we propose the use of zeroconfiguration networks and VLAN in order to realise home networks, in which autoconfiguration problems are resolved by zeroconfiguration protocol, and QoS problems are solved by means of VLAN, assigned on the base of device type and IP address that the zeroconfiguration protocol has associated with the device.

According to us, zeroconfiguration network represents a good solution to guarantee plug and play inside a home network. Though the address autoconfiguration is a default feature of IPv6 protocol, there could be necessary many years before the total change of IPv4 and the total diffusion of IPv6, particularly in North America. So, while waiting that IPv6 is largely diffused, in order to realise a *plug and play* system in an IPv4 environment, it is possible to use the *zeroconfiguration* protocol. It is a 'good bridge solution' (Bound, 2001; IPv6, 2004): so we decide to use zeroconfiguration network in our work.

The paper is organised as follows. In Section 2 a synthetic overview on zeroconfiguration protocol is supplied. In particular, the principal motivations of such protocol, its areas of interest and the principle of operation are introduced. In Section 3, a short analysis on QoS problem is presented and how this is connected to data link level for VLAN implementation. In Section 4, the proposed solution is introduced in order to guarantee QoS in zeroconfiguration networks; it is called VLAN Zeroconfiguration network. To realise a zeroconfiguration network, the role of a VLAN Manager is a focal point, since on the base of IP address, home devices are linked to opportune VLAN. Section 5, finally, concludes the paper.

2 Overview zeroconfiguration network

In pervasive computing, customers use a large number of devices, many of which are only temporarily associated with a single individual. The increment in the number of network enabled nodes; thus the need to establish dynamic logins between such nodes renders manual configuration of nodes impossible to use (McAuley et al., 2001). Zeroconfiguration networks are a class of IP networks that do not demand any manual configuration or administration. This is a project that wants to provide a very simple and easy method to use network. The need for autoconfiguration is brought about by several factors, including (Perkins, 1999):

- the proliferation of computing features and options
- the large number of data formats in common use
- the sheer number of computers.

The zeroconfiguration protocol is placed between two distinguished families of protocols: Internet Protocol on one side and vendor protocols on the other. Internet Protocol, as we know, emerges as standard for data transmission. The total communication is realised by means of proper configuration parameters that have only one meaning, assigned just by a network administrator. On the other hand, some network software vendors develop protocols able to manage an autoconfiguration of addresses, a decentralised service discovery, with the aim to facilitate local link communications, and resource sharing. To understand and take advantage of zeroconfiguration potentiality, it is necessary to specify that it is only a local-link technology. Such characteristic determines the absence of univocal value at the global level of IP addresses and logical names; for this reason application range of zeroconfiguration networks is limited to networks of small dimensions, either wired or wireless. On the other hand, the use of zeroconfiguration protocol turns out favourable in networks where to carry out set-up of devices by using the traditional technology of IP network, based on the aid of DNS or DHCP, is not convenient. With these bases, it clearly turns out that the use of zeroconfiguration in networks of average or great dimensions, in networks where a high degree of security and control is demanded, in public access networks, in networks with lowland bandwidth and high latency, is not advisable. If there are many cases in which it turns out that there is no opportunity to use zeroconfiguration (in networks of averages and great dimensions, in networks in which it is demanded an elevated level of security, and so on), the cases are equally numerous in which there is an effective advantage in zeroconfiguration implementation (in ad hoc networks for meeting and conferences, for an example). Actually, the traditional approaches are not sufficient and they are not able, therefore, to manage, in an adequate way, neither the mobility of ad hoc networks, nor are able to support a multi-hop communication, or splitting and merging of networks. The necessity of autoconfiguration becomes stronger when future home networks are considered, with IP-enabled appliances like microwave furnaces, thermostats, alarms and a lot of types of sensors. Clearly, it could not expect that user manages netmask and default gateways. A robust and fast plug and play solution is needed to provide reconfiguration when nodes exhibit individual or collective mobility (e.g., when nodes move to new rooms). Therefore, home network is a framework that suits with a zeroconfiguration application. Actually, we must remember that most users of home devices have no knowledge in computer science; so we must simplify the impact. Home networks implements a plug and play of several devices, eliminating the figure of network administrator and the need of a manual configuration.

For a home network user, this is a blessing: no longer do you have to spend time creating and addressing scheme and setting IP addresses and netmasks on devices that should just work. However, even the most trivial manual configuration task can become impossible when there are hundreds or thousands of devices needing attention.

The zeroconfiguration Working Group defines four areas of zeroconfiguration interest, and exactly *IP address configuration*, *Name to address translation*, *Service discovery* and *Multicast address allocation*.

Regarding the first area of interest, in zeroconfiguration networks, an automatic mechanism is used for a dynamic configuration of IP addresses, without any manual participation, or dependency from server. Automatic configuration for networking, naturally, follows from the more traditional uses of automatic configuration in stand-alone computers.

A good example of stand-alone use was the 'autoconfiguration' feature delivered with UC Berkley's version of Unix operating system. Since then, there have been more ambitious attempts to supply plug and play features for commodity laptop operating systems (Perkins, 1999).

The future of the internet is inextricably linked with the future availability of more autoconfiguration features for using it. The possibility to realise autoconfiguration is just contemplated in IPv6, but not in IPv4, although Stuart Cheshire, Bernard Aboba and Guttman have developed a method for "Dynamic configuration of IPv4 Local address" (Aboba and Cheshire, 2004). To such scope, IANA has classified a group of addresses (169.254/16) for local link. Node randomly chooses an address from the network 169.254/16; after it checks if the address is already in use. If the address is occupied, the algorithm starts again; otherwise it can be used. The selected addresses are tested with ARP.

The second area of zeroconfiguration interest is *Name to address translation*. Often lot of IP applications are identified with logical name, rather than with IP address. This operation supplies stability; actually, in case IP address changes, logical name remains unchanged. Zeroconfiguration protocol, in order to carry out name to address translation, needs mechanisms for obtaining IP address associated to logical name and determining the name associated with IP address, in DNS absence.

The third area of interest of zeroconfiguration protocol is *service discovery*, described in the 'DNS Service Discovery' (Cheshire, 2004). It does not require any change to the existing DNS protocol, of against it turns out absolutely compatible with existing DNS server. Actually, service discovery usually involves a client, service provider and a lookup or directory server.

The integration into networked environments of home devices has determined a translation in a home environment of configuration problem and interaction of such multitude of devices. Service discovery technologies were developed to simplify the use of devices in a network by allowing them to be 'discovered'. Hosts are able to discover services on network without any previous configuration and any service of management and administration.

The configuration complexity of every element inside the network – clients, servers, peers and infrastructure – is a key problem by keeping in mind for network technology advance. As long as configuration remains difficult, network administration will be expansive, tedious and troublesome. Users will be unable to take advantage of full range of capabilities that a networked system could provide.

The IETF has standardised two mechanisms, SLPv2 and DNS, finalised to the service discovery on IP networks. SLPv2 supplies service discovery, making a query on service type and attributes: thus a client could characterise a specific server based on demanded features. Before SLP, service discovery protocols allowed users to discover only by the type. SLPv2 is compatible both with IPv6 and with IPv4.

SLP automatically discovers device position – supplying address, domain name and other information about configuration and demanded service. Clients can be connected and use services, thanks to SLP aid. To the state of art, without SLP, several applications must be manually shaped, demanding many times for manipulation of configuration parameters. With an SLP, a good level of scalability is guaranteed. It is important to notice that clients, using SLP, are in a position to discover several services without any specific configuration of SLP and any additional service. SLP discovery also has a place in the absence of DNS, DHCP, SLPDAs and routing. This is the main reason that renders SLP suitable for SOHO (*Small Office and Home*) environment.

The second service mechanism discovery is DNS SRV Resource Record, which permits clients to approach services via DNS. The rules, on the base on which search queries are realised, are service type, transport protocol and logical name.

The fourth protocol area of zeroconfiguration interest is *Multicast Address Allocation*, specified in *Zeroconfiguration Multicast Address Allocation Protocol* (ZMAAP) (Catrina, 2001). Some multicast applications only use a multicast address in order to avoid conflicts with other applications. A multicast address conflict can cause application failure in an analogous way to two hosts who use the same IP address. In ZMAAP, there is a method for peer-to-peer allocation of multicast address without a multicast server. There is no change required in the DNS protocol, rather a benefit of use of multicast for name resolution in an environment where a DNS server does not exist, actually it has a service name resolution without a name server. In the document local.arpa is proposed as a link local domain.

For implementation of a zeroconfiguration protocol, it is necessary to avoid that it interferes with other protocols. It is necessary to guarantee coexistence on the same network with no zeroconfiguration protocols. Zeroconfiguration working group has proposed different approaches in order to exceed differences between networks that contemplate the administrator figure and networks that do not contemplate it. A strategy realises transactions between global configuration and local one in such a way it is possible to simplify choice and allocation of IP addresses. Actually, we should use automatic IP address until DHCP server gives the final IP configuration parameters.

3 Quality of Service (QoS) and VLAN

QoS can be defined in many ways and can include various aspects and different sets of service requirements, such as performance, availability, reliability and security. The parameters that describe QoS can be defined in a deterministic and stochastic ways or through average values at suitable time intervals (Towsley et al., 2002).

QoS and its parameters can assume a meaning significantly different, changing the point of view from which you wish to evaluate it. Customers, service providers and telecommunication engineers all view QoS in a different way, using performance metrics to evaluate QoS that might be different from each other. In Hardy (2001), a general model is presented. In this model, the notions of *Intrinsic*, *Perceived* and *Assessed* QoS are illustrated. *Intrinsic* QoS is strictly determined by transport network design and the provision of network access, termination and connection (Hardy, 2001; Gozdecki et al., 2003). The approach used for defining QoS is similar to that used by IETF in the definition of QoS (Crawley et al., 1998; Braden et al., 1993; Blake ii et al., 1998) and to the approach used by ITU and ETSI for defining the concept of Network Performance (ETSI, 1994; ITU-T, 1993a, 1993b, 1999).

An overview of commonly used terminology related to QoS in IP networks and a comparison among the approaches used by IETF, ITU and ETSI for defining QoS are shown in Gozdecki et al. (2003). In the case of the home networks, keeping in mind the network dimensions and types of devices that may be connected, QoS is tied to parameters that must be considered in any type of connection. These QoS parameters depend on technical aspects and are determined by the type of projected transport network, from connection to termination. QoS is expressed in terms of bit rate, available for service or target throughput that may be achieved, delay and delay variation (jitter), experienced by user information units while along the path and loss rate of user information unit (Gozdecki et al., 2003). In order to guarantee an acceptable

QoS level, different for a lot of end-system typologies, traffic must be guaranteed certain bandwidth, latency and jitter requirements. In general, QoS provides better (and more predictable) network services by providing the following features:

- support-dedicated bandwidth
- improve loss characteristics
- avoid and manage network congestion
- shape network traffic
- set traffic priorities across the network.

In a home network to guarantee QoS is not simple, for it concerns variety of networks – from an architectural point of view that protocol one – and application heterogeneity. In a home network, different technologies coexist, realising a communication heterogeneous environment. There are wireless and wired networks, analog and digital networks and so on. Today, in a communication environment, based on internet Protocol, QoS could be controlled and guaranteed, also, through the use of techniques of resource reservation and techniques that allow to support the priority of the traffic (Towsley et al., 2002). In the scientific literature, they a multitude of techniques are brought back for the maintenance and the guarantee of QoS – some simple, remarkably sophisticated others. In home network case, based on zeroconfiguration protocol, techniques that guarantee QoS must be simple and do not demand any participation by customer to realise configuration because they are able to implement a *plug and play*. Taking also into account home network features, the use of VLAN appears suitable to scope. A VLAN consists of several end systems, either hosts or network equipment, all of which are members of a single logical broadcast domain. A VLAN has no longer physical proximity constraints for the broadcast domain.

VLAN first-generation is based on various OSI second layer bridging and multiplexing mechanisms, such as IEEE 802.10, LAN Emulation (LANE), and Inter-Switch Link (ISL), that allow the formation of multiple, disjointed, overlaid broadcast groups on a single network infrastructure. VLAN can be used to group a set of related end-systems, regardless of their physical connectivity. End-systems belonged to a VLAN can communicate with end-systems belonged to another VLAN through a router. VLANs permit to control broadcast traffic; they increase level of network security because they allow the logical separation of devices that do not have to directly communicate between them, improve network performances and simplify management of the same one. VLANs permit to classify traffic and to assign various priority levels.

VLANs require an opportune organisation of services and devices. As it is known, there are several ways in which VLAN membership can be defined: port grouping, MAC layer grouping and network layer grouping. Taking into account zeroconfiguration requirements inside a home environment, according to us, it is better to implement VLANs on the base of layer 3 information. Actually, port grouping is still the most common method of defining VLAN membership. However, the primary limitation of defining VLAN by port is that network manager must reconfigure VLAN membership when a user moves from one port to another. So, clearly, this technique does not satisfy mobility requirements that are characterised of a zeroconfiguration network. In opposition, VLANs, based on MAC address, enable network managers to move a workstation that automatically retains its VLAN membership. A drawback of MAC address-based VLAN solution is the requirement of initial manual configuration. Another VLAN drawback, only based on a MAC layer addresses, emerges in environment, as home environment, that uses a lot of notebook PCs with some docking stations. The problem is that docking station and integrated network adapter, with its hard-wired MAC layer address, usually remain on the desktop, while the notebook travels with user. When user moves to a new desk and docking station, MAC-layer address changes, making VLAN membership impossible to track. In such an environment, VLAN membership must be constantly updated as the user moves around and uses different docking stations. Instead, VLANs, based on third layer information, take into account the protocol type or network-layer address to determine VLAN memberships.

So, this solution improves self-configuring network requirement. According to us, there are many several advantages to define VLANs at third layer. First, it enables partitioning by protocol type. Second, users can physically move their workstation without having to reconfigure each workstations network address.

So, VLANs, based on IP address, reduce handling cost of user moves and changes inside a home. Normally, when a user moves to a different subnet, IP address must be manually updated in workstation. VLANs eliminate this disadvantage, because VLAN membership is not tied to a workstation.

4 VLAN zeroconfiguration network

In a home network, a good QoS level is linked to capacity to plan and to implement, in opportune way, VLANs over zeroconfiguration networks. Keeping in mind the requirements of both zeroconfiguration networks and VLANs, a VLAN zeroconfiguration network guarantees customer the following services:

- absence of service manual configuration
- discovery
- support in case of high mobility
- easy and friendly networking
- support and management of different traffic classes owing to large heterogeneity of home devices.

The key element, from infrastructural point of view, for the realisation of a VLAN zeroconfiguration network, is a residential gateway, also known as Home Gate (Wacks, 2002). Actually, in domestic environment, it is necessary to

take advantage of a gateway aid to support large heterogeneity of protocols, allowing communication in a transparent way for customer. To the state of the art, Residential Gateway's architectures, with different features, are several. Between the others, there is OSGi standard (Open Service Gateway Initiatives) (Dobrev et al., 2002) that realises a gateway with an architecture divided into functional blocks. OSGi service platform is a JAVA general-purpose secure software framework that allows the development of service applications, said *bundles*. OSGi architecture allows (Valtchev and Frankov, 2002):

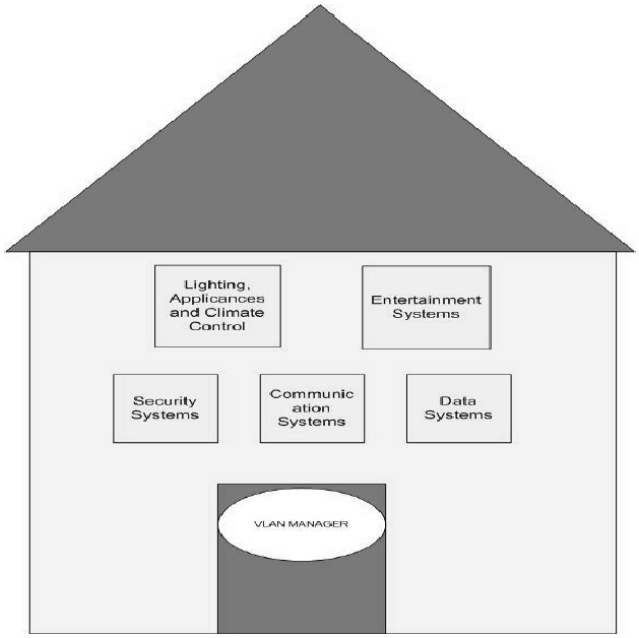
- remote control and diagnostic
- dynamic software update
- remote management
- building systems that are open to third-party software.

OSGi gateway has the function of coordination centre for home network management. It is important to emphasise that OSGi only specifies the Application Program Interface (API), does not allow implementation. API allows not only to interact with devices that support the same protocol, but also with devices that use different protocols. On the base of these characteristics, OSGi Gateway is considered the optimal solution in order to guarantee an adequate level of performances inside home network; judgement reached after a careful analysis of its architecture. The adoption of open specifications promotes the development of applications that increase interoperability; reason for which inside a residential gateway should be possible to define API, finalised to management and implementation of VLANs on the base of IP address. In such way, residential gateway will have also logical function of VLAN Manager. From an architectural point of view, VLAN manager is a focal point inside VLAN zeroconfiguration network. Actually, VLAN manager carries out the following functions:

- organisation of home devices in logical micronetworks
- allocation of every micronetwork to different VLANs
- resources allocation for every VLAN, according to traffic requirements
- negotiation with a new home device, to associate it to an opportune VLAN.

Inside a home, opportunely grouping several devices, five different types of micronetworks can be characterised: Lighting, Appliances and Climate Control Systems; Security Systems; Entertainment Systems; Communication Systems and Data System (Valtchev and Frankov, 2002) (Figure 1). IP-based network is the network that interconnects, integrates and guarantees interoperability among such micronetworks.

Figure 1 Organisation of home devices in VLAN



OSGi can be considered as a platform that interconnects these micronetworks. VLAN manager associates one VLAN to every micronetworks, on the base of IP address. In order to create an association between IP addresses and micronetwork type, the class of IP addresses, 169.254/16, put to disposition from IANA for local link (Aboba and Cheshire, 2004), is divided in sub-classes, equal to the number of subnetworks, typical for a domestic environment. The house manufacturers will have to indicate device belonging class, in conformity with the carried out subdivision. Thanks to such architecture of support, when new device realises a plug operation, system answers in the following way: taking advantage itself of the aid of zeroconfiguration protocol, new device acquires an IP address – *Temporary IP address* – by means of which it could establish a communication with VLAN manager. VLAN manager is located after a service discovery operation – function contemplated inside zeroconfiguration protocol. Discovery techniques allow third party to tailor services based on dynamic configurations of home networking elements, intelligently responding to presence or absence of certain devices within home. This effectively reduces complexity, perceived by end-user, and, at the same time, it increases flexibility of offered service, and enables more rapid deployment of home networking services (Dobrev et al., 2002). After to have discovered VLAN manager, home device communicates to VLAN manager the own belonging class, indicated by house manufacturer. The communication between VLAN Manager and home device is analogous to autonegotiation between two network interfaces. Autonegotiation is a mechanism that allows to

discover the different operational possibilities of a device and to configure, in automatic way, the higher performance. The autonegotiation philosophy is comparable, from an infrastructural point of view, to a switch.

The autonegotiation supplies:

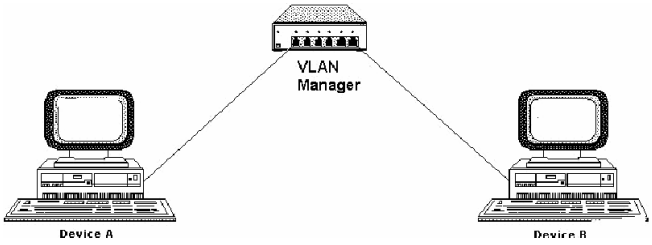
- automatic connection
- management interface.

Automatic connection allows, as is clearly from the same name, login of device without any participation, either of a customer, or an administrator, or even a management software. Automatic connection property of autonegotiation mechanisms is consistent with zeroconfiguration protocol requirements and, in particular, with autoconfiguration capacity.

The management interface allows to:

- determine reasons of refusal of a demanded logon
- find possibility offered from network
- change connection rate
- find and resolve fault status
- exchange arbitrary information with partner link (Figure 2).

Figure 2 Autonegotiation

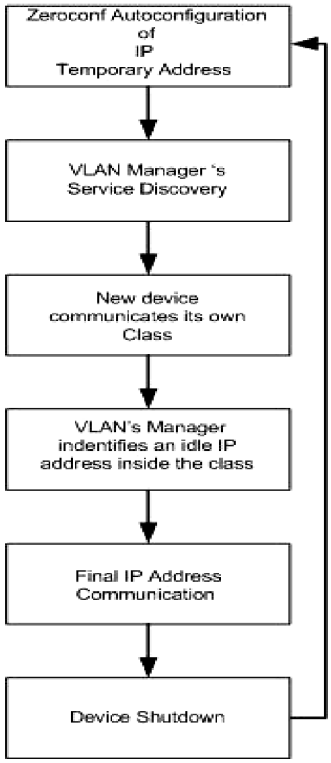


Autonegotiation mechanism, thanks to its intrinsic simplicity, low cost and flexibility, totally satisfies requirements of domestic environment. The functionalities that are included in the management interface will permit a corrected exchange of information between VLAN manager and new device, realising a corrected subdivision of devices in respective VLANs and guaranteeing a proper QoS level inside home environment. Actually, VLAN manager assigns IP address-*Final IP address* – among those available in the belonging class. VLAN manager randomly chooses an address from the subnetwork, after it checks if address is already in use. If address is occupied, VLAN manager repeats the operation, otherwise communicate it to the device.

Taking in mind these actions, we define a VLAN ZeroConfiguration algorithm as a step–by-step procedure that allows a new device to plug and play inside a home network with an adequate level of QoS. In detail, when a new device is added to the network, at first step, thanks to the IP address configuration feature of ZeroConfiguration protocol, it receives a Temporary IP address; at second step, it must discover the VLAN Manager; at third step, the device communicates its own class to the VLAN manager; at fourth step, the VLAN manager finds an idle IP address inside the belonging class and at fifth step, VLAN manager communicates the IP address, that is, called Final IP address, to the device; so the device changes address from Temporary IP address to the Final IP address.

In this way, the device can work with an adequate level of QoS assigned to the belonging class. When the device finishes its work, it is shutdown (final step) and if it is plugged again, the algorithm starts again from the first step (Figure 3).

Figure 3 VLAN zeroconfiguration algorithm



Therefore, in conformity to OSGi, such architecture allows several home devices to be installed and uninstalled *on the Fly* without having to reinitialised entire system.

5 Conclusions

In this paper, we mean to offer a possible application scenario in order to test the potentiality of an integrated VLAN Zeroconfiguration solution. Our work wants to analyse functionalities, just contemplated from zeroconfiguration protocols, extending and upgrading the same protocol with an opportune QoS guarantees. QoS problem is faced by means of an adequate traffic segmentation, realised by VLANs. Home environment is turned out a suitable condition to apply VLAN zeroconfiguration networks, because it is able to guarantee plug and play requirement to home users that have always no familiarity and acquaintances within of computer science. Necessity of being constantly connected, in no best effort way, pushes telecommunication engineering to characterise integrated and convergent solutions, as VLAN zeroconfiguration networks, in order to satisfy

heterogeneous requirements of equally heterogeneous users. The advantages of proposed solution are undeniable, in terms of management easiness of different devices, better performance and too lower costs. At the moment, the authors try to implement a home network in which the devices use the protocol introduced in this paper. In this way it is possible to evaluate performance. The results will be showed in future works.

References

Aboba, B. and Cheshire, S. (2004) 'Dynamic configuration of IPv4 local address', *Internet Draft, Zeroconf Working Group*, July.

Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z. and Weiss, W. (1998) 'An architecture for differentiated services', *IETF RFC 2475*, December.

Bound, J. (2001) 'IPv6 Deployment', *Internet Society*, September.

Braden, R., Clark, D. and Shenker, S. (1993) 'Integrated services in the internet architecture: an overview', *IETF RFC 1633*, July.

Catrina, O. (2001) 'Zeroconf Multicast Address Configuration Protocol (ZMAAP)', *Internet Draft, Zeroconf Working Group*, March.

Cheshire, S. (2004) 'Discovering Named Instances of Abstract Services using DNS'. *Internet Draft*.

Crawley, E., Nair, R., Rajagopalan, B. and Sandick H. (1998) 'A framework for QoS-based routing in the internet', *IETF RFC 2386*, August.

Dobrev, P., Famolari, D., Kurzke, C. and Miller, B.A. (2002) 'Device and service discovery in home networks with OSGi', *IEEE Communication Magazine*, Vol. 40, No. 8, August, pp.86–92.

ETSI (1994) 'Network Aspects (NA): general aspects of Quality of Service (QoS) and Network Performance (NP)', *Technical Report ETR003, 2nd ed.*, October.

Fink, R.L. (1999) 'Ipv6', *The Internet Protocol Journal*, Vol. 2, No. 1, March.

Gozdecki, J., Jajszczyk, A. and Stankiewicz, R. (2003) 'Quality of Service terminology in IP networks', *IEEE Communication Magazine*, Vol. 41, No. 3, March, pp.153–159.

Guttman, E. (2001) 'Autoconfiguration for IP networking', *IEEE Internet Computing*, Vol. 5, No. 3, June, pp.81–86.

Hardy, W.C. (2001) *QoS Measurement and Evaluation of Telecommunications Quality of Service*, Wiley, New York.

IPv6 (2004) http://www.ipv6style.jp/en/special/20040726/index.shtml.

ITU-T (1993a) 'General aspects of Quality of Service and Network Performance in digital networks, including ISDN', *ITU-T Rec. E.350*, March.

ITU-T (1993b) 'Terms and definitions related to Quality of Service and Network Performance including dependability', *ITU-T Rec. E.800*, August.

ITU-T (1999) 'Internet protocol data communication service – IP packet transfer and availability performance parameters', *ITU-T Rec. Y.1541*, February.

McAuley, A., Das, S.K., Misra, A. and Das, S. (2001) 'Autoconfiguration, registration and mobility management for pervasive computing', *IEEE Personal Communications*, Vol. 8, No. 4, August, pp.24–31.

Perkins, C.E. (1999) 'Autoconfiguration. Plug and play internet: Protocols for extending the net', *IEEE Internet Computing*, Vol. 3, No. 4, pp.42–44.

Teger, S. and Waks, D.J. (2002) 'End-user perspectives on home networking', *IEEE Communication Magazine*, April, pp.114–119.

Towsley, D., Firoiu, V., Le Boudec, J. and Zhang, Z.L. (2002) 'Theories and models for internet Quality of Service', *Proceedings of the IEEE*, special issue in Internet Technology, Vol. 90, No. 9, August, pp.1565–1591.

Valtchev, D. and Frankov, I. (2002) 'Service gateway architecture for a smart home', *IEEE Communications Magazine*, Vol. 4, No. 4, April, pp.126–132.

Wacks, K. (2002) 'Home systems standards: achievements and challenges', *IEEE Communications Magazine*, Vol. 4, No. 4, April, pp.152–159.

Website

IETF Zero Configuration Working Group, *Zeroconfiguration Networking*, http://www.zeroconf.org/zeroconf-charter.html.