Juhani Kaltio

IPv6 in SoHo Environment

A Study of Basic Functionality

Helsinki Metropolia University of Applied Sciences

Information and Communications Technology

Bachelor's Thesis

24 February 2016

Author(s)	Juhani Kaltio
Title	IPv6 in SoHo Environment
Number of Pages	32 pages
Date	24 February 2016
Degree	Bachelor of Engineering
Degree ProgrammeInformation and Communications Technology	Information and Communications Technology
Specialisation option	Networking
Instructor(s)	Pekka Sakara, ZyXEL Matti Puska, Principal Lecturer

The aim of this final year project was to increase understanding of configuring IPv6 for SoHo environment and to produce a short manual for ZyXEL Finland about IPv6. ZyXEL is a Taiwanese networking equipment manufacturer that has a global presence.

A ZyXEL USG-series firewall was used for most of the configuring tasks, since it is a popular product for small to medium size companies.

IPv6 is a successor protocol for IPv4, the current protocol used for networking. IPv6 offers more address space and additional features. In the project, a dual stack configuration was used, where IPv4 and IPv6 implementations co-exist. Such a scenario is likely to be common in the transition period from IPv4 to IPv6.

In the project, an IPv6 configuration manual was made for the ZyXEL CSO organization. In the manual, step-by-step instructions are given to configure IPv6 on a ZyXEL USG firewall. The manual outlook was based on ZyXEL CSO's wishes and it can later be modified if needed. The manual is intended to be sent to CSO's customers and to be used also in the CSO internal training.

Keywords	IPv6, ZyXEL

Tekijä(t) Otsikko Sivumäärä Aika	Juhani Kaltio IPv6 in SoHo enviroment 32 sivua + 0 liitettä 24.2.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Verkkotekniikka
Ohjaaja(t)	Pekka Sakara, ZyXEL Opettaja Matti Puska

Tämän opinnäytetyön tarkoitus on kartuttaa tekijän IPv6-tietämystä ja tuottaa lyhyt manuaali ZyXEL Suomen asiakaspalveluorganisaatiolle IPv6-verkkoprotokollan käytöönotosta. ZyXEL on taiwanilainen verkkolaitevalmistaja, jonka tuotteisiin kuuluvat sekä yritys- että kuluttajaverkkolaitteet. ZyXEL toimii maailmanlaajuisesti.

ZyXELin ZyWALL USG-sarjan palomuuria käytetään pääosin testien tekemiseen. ZyWALL USG on suosittu tuote pienten- ja keskisuurien yritysten tarpeisiin.

IPv6 on IPv4:n seuraajaprotokolla. IPv6 tarjoaa suuremman osoiteavaruuden ja lisäominaisuuksia IPv4:ään verrattuna. Tässä opinnäytetyössä käytetään dual-stack ympäristöä, koska se on todennäköisesti suosittu IPv6-toteutus siirtymä aikana IPv6:sta IPv4:ään.

Opinnäytetyön tulokena tehtiin IPv6-käyttöönottomanuaali ZyXELin asiakaspalveluorganisaatiolle. Manuaalissa annetaan kohta-kohdalta ohjeet IPv6:n käyttöönottamiseksi ZyXEL USG-palomuurilla. Manuaali tehtiin ZyXEL:in asiakaspalveluorganisaation toiveiden mukaisella ulkoasulla ja se on muokattavissa tarpeen vaatiessa. Manuaalia on tarkoitus käyttää sekä lähetettäväksi ZyXEL:in tukipalvelun asiakkaille että apuna tukiorganisaation sisäisessä koulutuksessa.

Avainsanat	IPv6, ZyXEL

Contents

Key Terms

SLAAC Stateless Address Autoconfiguration. Stateless is a way to configure clients with IPv6 address. The Subnet must have a /64 mask.

NDP Neighbor Discovery Protocol. “ARP for IPV6” and additional features. Uses ICMPv6 messages. A way to discover neighbor nodes in IPv6.

Prefix Delegation

A Way to give client routers a subnet address block to be used in their respective LAN network.

ICMPv6 Internet Control Message Protocol version 6. The Same as “ping” in IPv4, but with several additional features. IPv6 neighbor discovery for example uses ICMPv6 messages in their implementation.

Fragmentation

Technique of dividing big datapackets into smaller ones.

Fragmentation uses extension headers.

DUID DHCP Unique Identifier. An Identifier to distinguish DHCPv6 servers and clients. Each server and each client has one DUID.

IAID Identity Association Identifier. Distinguishes different groups of IPv6 addresses on an IPv6 node.

6in4Tunnel A tunneling method to tunnel IPv6 traffic in an IPV4 network. Used by some tunnelbrokers.

On-link In the same subnet.

VPN Virtual Private Network. Virtually attaches two separate LAN networks securely together over the public internet.

Multicast One sending operation is able to send a packet to multiple recipients. Uses special multicast addresses.

Dual-stack A networking scenario where IPv4 and IPv6 protocols exist on the same device and optionally also on the same network.

1 Introduction

IPv6 (Internet Protocol version 6) is a successor protocol for IPv4 (Internet Protocol version 4), the current IP (Internet Protocol) protocol used for networking. The main reason for this transition is that public IPv4 addresses have almost entirely been used, while the size of the internet grows. IPv6 offers more address space and additional features compared to IPv4. Even though IPv4 and IPv6 are likely to co-exist in the future, organizations still need to adjust to IPv6 in the coming years. [1;2.]. This migration is likely to cause challenges to networking professionals, end-users and organizations. IPv6 is similar to IPv4, but it still requires new skills to be learned. While some organizations have already migrated to the IPv6 environment, others are still not prepared for the change.

The aim of this study was to test the basic IPv6 configuration scenario for the SoHo (Small Office, Home Office) environment. On the basis of the configurations, a manual was made for ZyXEL Finland's CSO (Customer Service Organization). The manual can be emailed to customers and therefore it reduces some of the IPv6 workload coming to the service desk. The manual can also be distributed to other CSO organizations in Europe internally as a helper document when configuring IPv6.

The ZyXEL corporation is a Taiwanese networking equipment manufacturer. ZyXEL has a global presence. ZyXEL products are sold worldwide and the company employs over 2100 people. The ZyXEL product range consists of firewalls, switches, WLAN (Wireless Local Area Network) devices and consumer-grade CPEs (Customer-premises equipment). ZyXEL is also an OEM (Original Equipment Manufacturer) for other networking companies and ISPs. In addition, ZyXEL offers training and CSO services to its customers. [3;4.]

ZyXEL Finland is ZyXEL's Finnish branch office and also part of ZyXEL's European wide CSO organization. CSO offers service desk services to ZyXEL clients. ZyXEL CSO serves numerous customers daily, and as migration to IPv6 is drawing close, it is expected that IPv6 related service desk tickets will increase. The European CSO organization as a whole is also preparing for the migration with additional training.

A ZyXEL USG60 firewall is used for most of the configuring tasks, since it is a popular product for small to medium size companies. USG series firewalls are a key component of the ZyXEL networking equipment product range. USG60 firewall provides IPv4 and IPv6 connectivity, a statefull firewall, multiple VPN (Virtual Private Network) connections and multiple LAN (Local Area Network) network zones. It also has support for VLANs (Virtual Local Area Network). Configuration and testing steps done in USG60 can help to configure other ZyXEL professional grade networking equipment since the GUI (Graphical User Interface) is similar. Therefore ZyWALL USG60 was selected to be the testing device for this study [5,6.].

2 Basics of IPv6

IPv6 is a successor protocol for IPv4 developed by the IETF (Internet Engineering Task Force). IPv4 has limited 32 bit address space that was seen as adequate at the time of its invention. However, since then the size of the internet and the amount of networking equipment has grown and the world is running out of IPv4 addresses. This has caused several problems. The address depletion has created workarounds to manage the lack of IPv4 addresses. Such techniques include NAT (Network Address Translation) and CIDR (Classless Inter-Domain Routing). These in turn create additional complexity to the networking technology and the global networking infrastructure. Another problem with IPv4 is that global routing tables have grown too large.[2;7,691-692;8.]

IPv6 has been developed to repair these problems in its design. IPv6 has significantly larger address space that allows the use of an end-to-end address model. Techniques such as NAT are no longer necessary. Other features include compulsory support for IPsec(IP Security Architecture) that potentially makes IPv6 internet safer. The Header structure of IPv6 makes it faster for computers to route IPv6 packets. Also the global Internet routing table can be made smaller with the help of IPv6. [7;691-692;9,3-6.]

IPv6 also offers additional functionality that was not present in IPv4. In IPv6 an interface can have several IPv6 addresses at the same time. In IPv6 link-local addresses are created automatically. This means that IGPs (Interior Gateway Protocol) can communicate with each other automatically without first needing to assign an address to an interface manually. The large amount of IPv6 addresses enables user organizations to have dedicated IPv6 address space which does not change even if ISP changes. IPv6 also offers a stateless way of configuring devices with IPv6 address. This stateless address autoconfiguration enables easier delegation of IPv6 addresses to LAN nodes.[7,693.]

2.1 IPv6 Address and Header

The IPv6 address is used to identify interfaces in the IPv6 network. Figure 1 illustrates the notation of an IPv6 address.

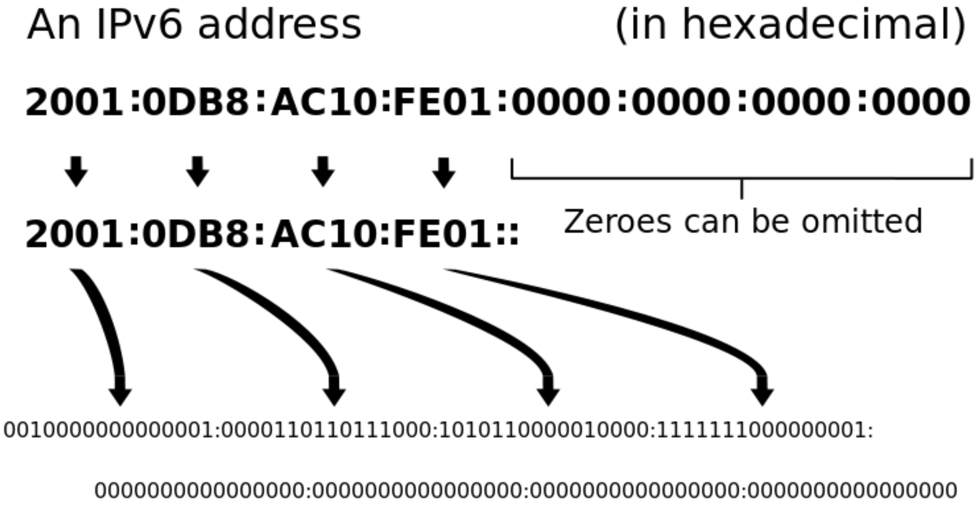


Figure 1. IPv6 address notation. Copied from [10].

Like figure 1 illustrates, the IPv6 address consists of 128 bits. Hexadecimal values are used and the address is divided into eight sections, each 4 hexadecimals or 16 bits long. Leading zeros in each section can be marked as one zero. As a result "2001:0000:0000:0000:0000:0000:0000:0000" can be marked as "2001:0:0:0:0:0:0:0". A Consecutive section of zeros can be marked as "::" once in every address. Thus the example presented before can also marked as "2001::". There are three primary classes of addresses in IPv6, unicast, anycast and multicast. Unicast refers to one interface in one node, like in IPv4. Both anycast and multicast addresses form a group of interfaces on different nodes. When packet is sent to a multicast address, all interfaces with that multicast address will receive the same packet. When the packet is sent to an anycast address, only the nearest interface with the anycast address will receive it. There is no broadcast in IPv6, but multicasting is used for the same task. [2;7;691-712;11.]. Multicasting and anycasting are further covered in chapter 2.6 of this thesis.

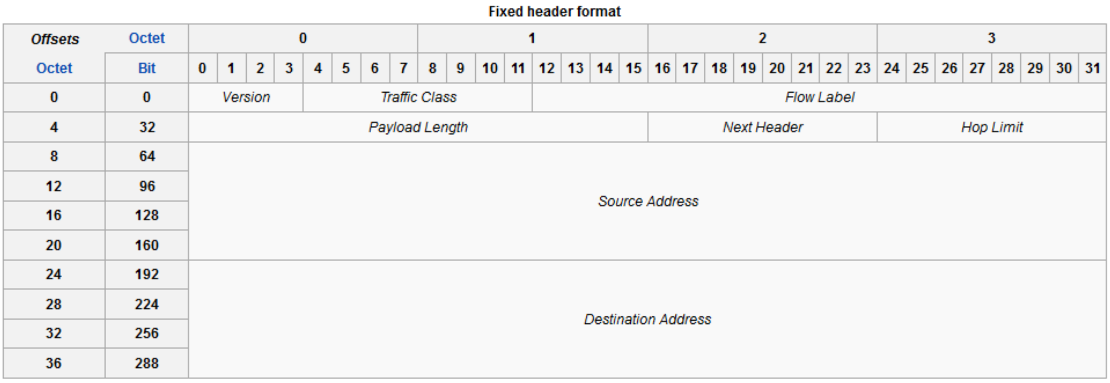
IPv6 addresses can be grouped by their functionality like IPv4 addresses. Some of the most common functionalities are:

- 2000::/3 are global unicast addresses. This means that they are the "normal" routed IPv6 addresses. They are similar to IPv4 public addresses.
- Multicast addresses are marked as ff00::/8.

- Unique Local Address (ULA) is marked as fc00::/7. ULAs are meant to be used in closed networks such as LAN's. They are not meant to be routed globally and are not unique.
- Link-local addresses are marked as fe80::/10 and are meant to be routed on specific link only. Link-local addresses are assigned automatically to an interface.
- Loopback is marked as ::1/128.

In addition to type, the IPv6 address also has a scope. The Scope defines the network part where it can be used. Global addresses are routed globally and have marking E. Node scope has marking 1, link scope has marking 2, site scope has marking 5 and organizational scope has marking 8. For example IPv6 address “ff02::/8” is a multicast address that is used in in the link local scope.[7,692-712;12.]

An IPv6 packet has several sections. Figure 2 illustrates the IPv6 header structure.



Fixed header format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class								Flow Label																			
4	32	Payload Length																Next Header								Hop Limit							
8	64	Source Address																															
12	96																																
16	128																																
20	160																																
24	192	Destination Address																															
28	224																																
32	256																																
36	288																																

Figure 2. IPv6 Header. Copied from [13].

As figure 2 illustrates, the IPv6 header has 40 octets or 320 bits. The Offset of each section is marked in figure 2 and each section has a specific task:

- Version describes the IP version that is used. It is four for IPv4 and six for IPv6.
- A Traffic class is used when QoS (Quality of Service) is implemented.
- A Flow label is also used in QoS and in packet handling. The Packet that belongs to a specific flow can be forwarded on the basis of that flow, instead of on the basis of each packet. This makes switching operations faster.
- Payload length describes the size of the payload.

- The Next header indicates what kind of a header is in the IPv6 packet *after* the IPv6 header. If extension headers are used, this field marks the location of the next extension header.
- Hop limit indicates how many hops this packet can travel in a network.
- Source address is the IPv6 address of an interface in the sending node.
- Destination address is the IPv6 address of the destination node.
- If extension headers are used, they are placed after all other header fields, before the actual payload.[7,692-798;11;13.]

IPv6 extension headers deliver extra information in the IPv6 packet and are optional. Figure 3 illustrates the placement of extension headers in the IPv6 packet header.

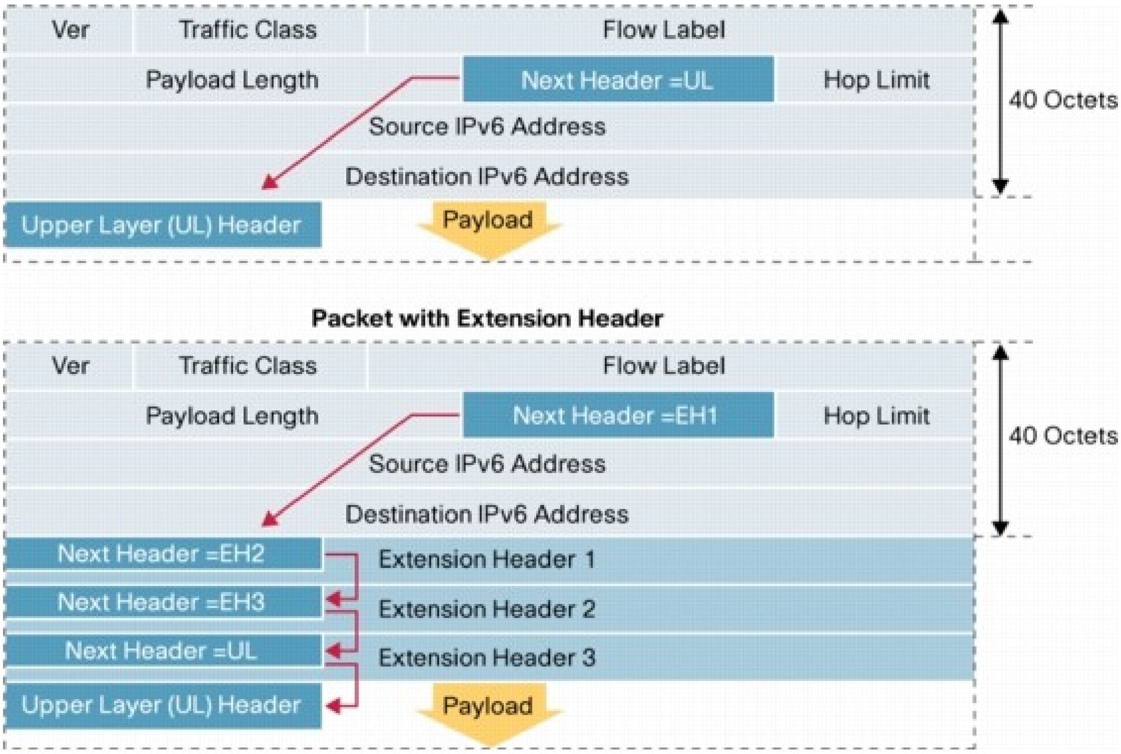


Figure 3. IPV6 extension header. Copied from [14].

Extension headers have similar use as the IPv4 options field of the IPv4 header. As figure 3 illustrates, the IPv6 packet can have several extension headers. The next header field in the IPv6 header marks where the extension header starts, but if there are no extension headers, the next header marks the point where the UL (Upper Layer) header starts. Extension headers are placed one after another before the upper layer header in a specific order. Extension headers are organized so that they are fast to process. For example the hop-by-hop extension header is the first in the sequence, because it will be checked by all nodes when the packet travels to its destination.

There are different types of extension headers and they have different purposes. For example the hop-by-hop extension header is used by the MLD (Multicast Listener Discovery) protocol. The Routing extension header holds information about routing and also mobility. IPv6 fragmentation also uses a extension header called fragment extension header. IPsec (IP Security Architecture) employs the AH (Authenticating Headers) extension header for authentication and ESP (Encapsulating Security Payload) for encryption. The Destination header, when it is not used with with hop-by-hop header, is parsed on the destination node. [7;695-698;14.]

2.2 IPv6 Subnetting

IPv6 subnetting is similar to IPv4 subnetting, except for the fact that the IPv6 address is longer. Because of the large IPv6 address space, there is no need to conserve addresses when subnetting IPv6. Therefore it is recommended to make the configuration simple and try to minimize the size of the routing tables. It is recommended to use a 64 bit subnet mask with IPv6, even with point-to-point links. Many IPv6 features require a 64 bit mask, for example neighbor discovery, privacy extension, and some parts of mobile IPv6. If a 64 bit mask is not used for subnets, these technologies will not work. However, different subnet masks such as 128 bits can be used. Because IPv6 does not have broadcasting, a 128 bit subnet mask will give one address. If addresses need to be conserved, a 126 bit mask can be used for point-to-point links; however, this might make the configuration more complicated. [15.]

In this study a Welho/DNA cable connection was used. Welho gave an address block of /56 with prefix delegation. If a 64 bit mask is used, a /56 prefix gives 256 subnets of / 64. If a fictional company would have 2 or more sites, the /56 block could be delegated to smaller portions, say /58. Each of the four sites would still get 64 blocks of /64 subnets.

As an example a fictional ISP has provided address block of 2001:14ba:2fe:ea00::/56. The last two zeros are the subnet, so the block ranges between "2001:14ba:2fe:ea**00**::/64" – "2001:14ba:2fe:ea**ff**::/64".

When subnetting IPv6, it easy to start the subnet from 1 or 0, as in subnetting IPv4.
An Example of IPv6 subnetting is given below:

- LAN1 IPV6 subnet is 2001:14ba:2fe:ea**01**::/64
- LAN2 IPV6 subnet is 2001:14ba:2fe:ea**02**::/64
- LAN3 IPV6 subnet is 2001:14ba:2fe:ea**03**::/64

In case VLANs are needed, same procedure can be used:

- VLAN10 IPV6 subnet is 2001:14ba:2fe:ea**0a**::/64
- VLAN20 IPV6 subnet is 2001:14ba:2fe:ea**14**::/64
- and so on

[16.]

Like IPv4 subnets, IPv6 subnets can also be summarized. Summarization is also called aggregation. Summarization is used to make the routing table smaller by creating one big subnet from smaller subnets that are contiguous. When routing tables are smaller, routers use less memory and CPU. For example an ISP can summarize all of its customer networks into one large subnet and then only one routing table entry can describe several smaller customer networks.[7,698-701;17,26-27,49-50.]

As an example IPv6 subnet, “2001:1111:1111:1234::/64” and “2001:1111:1111:4567::/64” can both be summarized into “2001:1111:1111::/48” address. Another example is an fictional ISP that delegates 56 bit address blocks to its customers. The ISP can summarize 256 subnets of a mask 56 with a supernet mask of 48 bits.[16.]

2.3 Address Delegation in IPv6

In IPv6 addresses can be delegated to client nodes either with SLAAC (stateless address autoconfiguration), DHCPv6 (Dynamic Host Configuration Protocol version 6) or manually with static configuration. Static configuration is similar to IPv4. [18.]

SLAAC is a stateless way to configure an IPv6 address. Stateless means the router does not know the address each client has. In SLAAC, the router only advertises the prefix to be used in a specific subnet and the prefix must be 64 bit long. The Client then creates the suffix address using the EUI-64 (Extended Unique Identifier 64 bit) method. Together the prefix from the router and the EUI-64 suffix created by the client form the SLAAC address. Figure 4 describes the EUI-64 method.[7,701-704;19,3;20,74.]

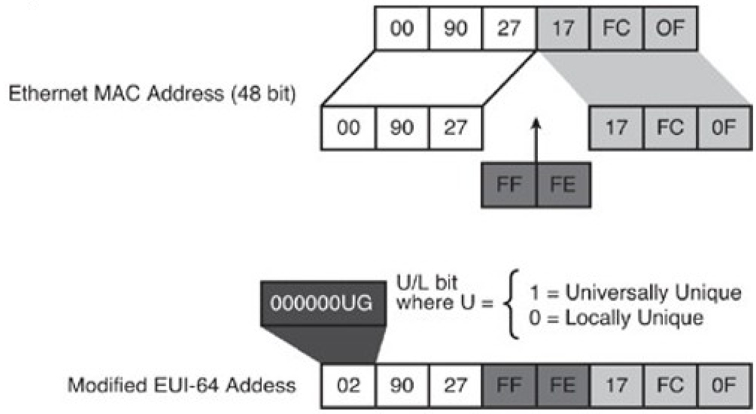


Figure 4. EUI-64 format. Copied from [7,702].

As figure 4 illustrates, in the EUI-64 method the client MAC address (Media Access Control) is used to create the EUI-64 suffix by adding “ff:fe” in the midlle of the MAC-address and flipping the seventh bit of client MAC-address when reading from left to right. If “2000:1234:5678:0000::/64” is the prefix that a router is giving out to clients, and client MAC address is “00:20:12:34:56:78” then the client EUI-64 suffix would be “:0220:12ff:fe34:5678“. The EUI-64 suffix is added to the subnet prefix and the complete SLAAC address would be 2000:1234:5678:0000:0220:12ff:fe34:5678/64. [7,701-704.]

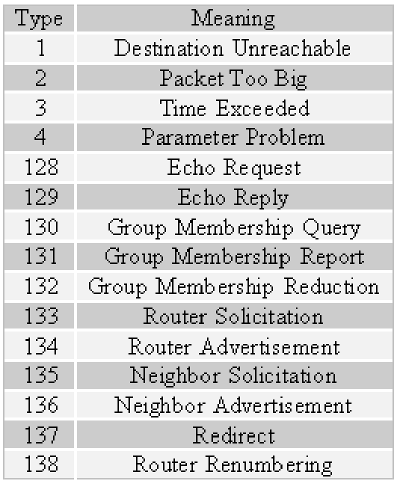
The benefit of SLAAC is that it is easy to configure, and it does not require configuration on the client side. Clients can be identified by their SLAAC address when they are using the EUI-64 format. This can be a good thing, but it also has a downside. The advantage is that clients can be identified for example in a LAN network using their MAC-address. The Downside is that since the MAC-address is visible also globally, some information can be deducted from the IPv6 address that uses the EUI-64 SLAAC address format. Client traffic can also be tracked because the suffix of the SLAAC address is the same. To prevent this, a so called privacy extension to the SLAAC is defined in the RFC document 4941. When using privacy extension, the MAC-address will not be used in the SLAAC address but instead the suffix part of the SLAAC is created randomly. The suffix part also changes over time. Windows 10, for example, uses privacy extension by default. [7,701-704;18;21,7,10-16.]

DHCPv6 is somewhat similar to DHCPv4. DHCPv6 offers both a stateless and statefull way of distributing addresses to client nodes. Statefull means that the delegating server knows which client has which IPv6 address.[20,74]. DHCPv6 can also be used in a stateless mode, in which it will not provide any addresses to clients, only other information such as DNS (Domain Name Server) or NTP (Network Time Protocol) servers. In addition to addresses, DHCPv6 can be used to delegate the IPv6 address block to a router. This is called prefix delegation and is used by some ISPs. These client routers in turn distribute addresses to LAN clients from the delegated address block either with SLAAC of DHCPv6. In this study an IPv6 address block was received from Welho/DNA using the prefix delegation technique. DNS and NTP servers and other options can also be delegated to clients using DHCPv6 either in a statefull or stateless mode. An Important difference to DHPCv4 is that DHCPv6 will not give a default gateway to clients. DHCPv6 and SLAAC can both work at the same time in the same network. It is possible for example to use SLAAC to create the IPv6 address for clients and DHCPv6 to give them DNS and NTP server information. [19,167;22,55-56,191-193;23,11-12,19,23-24.]

DUID (DHCP unique identifier) is a numeric identifier used to distinguish servers and clients. DUID should be unique and not change even if the hardware configuration of a IPv6 node changes. DHCPv6 clients and servers all have one DUID assigned to them. Routers distinguish clients based on DUID and clients can separate DHCPv6 servers form each other with DUID. Because in IPv6 an interface can have several IPv6 addresses assgined to it, DHCPv6 clients have IA (identity-association) on every interface that it wants to request an address from the DHCPv6 server. The DHCPv6 server can together with IA and DUID tell which interface has a specific IPv6 address and the node where the interface is located. IAID (Identity association identifier) separates the IA's of a client from each other. The IAID is assigned by the client to every IA it has. In other words, IA describes usually one interface on the DHCPv6 client and the interface can have several IPv6 addresses assigned to it. The Client can have several IAs if it has several interfaces. An IA is identified by IAID. [22,55-56,191-193;23,11-12,19,23-24.]

2.4 ICMPv6

ICMPv6 (Internet Control Message Protocol version 6) is a protocol for sending informational and error messages. ICMPv6 is defined in the RFC (Request For Comments) document 4443. Figure 5 illustrates ICMPv6 message types. [24.]



Type	Meaning
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect
138	Router Renumbering

Figure 5. ICMPv6 message types. Copied from [25].

As can be seen in figure 5, ICMPv6 message types smaller than 128 are error messages, and messages greater or equal to 128 are informational messages. ICMPv6 has also been designed in a fashion that additional features can be added to it in the future. ICMPv6 is a key component in IPv6. It and several other protocols use ICMPv6 messages for communication such as MLD (Multicast Listener Discovery) and path MTU (Maximum Transmission Unit) discovery. ICMPv6 is also used for neighbor discovery. [7,698;22,48-49;24,3-4;25;26,59.]

2.5 IPv6 Neighbor and Router Discovery

NDP (Neighbor Discovery Protocol) is used for neighbor discovery in IPv6 and it is defined in RFC 2461. NDP uses ICMPv6 messages of type 133 (router solicitation), 134 (router advertisement), 135 (neighbor solicitation), 136 (neighbor advertisement) and 137 (redirect). ICMPv6 messages and their types can be seen in figure 5. Router solicitation messages are used by IPv6 hosts to make routers respond to them with router advertisement messages. Routers in turn respond to router solicitation messages instantly with router advertisement messages, or send them when a certain time period has passed. Neighbor solicitation messages are used to ask the link-layer address of another node to provide the node with the link-layer address of the sender node or to ensure that the other node is still responding. Multicast is used in the link-layer address resolution and unicast is used when ensuring reachability. Neighbor advertisement messages are sent when a node receives a neighbor solicitation message. They can also be sent without first receiving neighbor solicitation messages if the node wants to give out new information. Redirect messages are sent by routers to hosts if there is a better first-hop route available to its destination.[27,3,17-26.]

NDP is used to achieve a number of different goals. With router discovery nodes can learn about the existence of neighbor router and about on-link address prefixes. Stateless address autoconfiguration uses also router discovery messages. Link-layer address resolution and neighbor unreachability detection are also tasks of NDP. In link-layer address resolution link-layer address of a neighbor node is discovered using its IPv6 address. In duplicate address detection a node sends a message with the address that it suspects might be a duplicate as a destination address. If another node responds with a neighbor advertisement message, the node can deduct that address is already in use. [27,38-39,59,60,68,78]

Neighbor discovery on IPv6 is process of finding out link-layer address of another router when the IPv6 address of the neighbor is known. Neighbor discovery is also used to make sure that the neighbor device is reachable. Neighbor discovery happens in the link-local scope. Figure 6 illustrates the IPv6 neighbor discovery process.

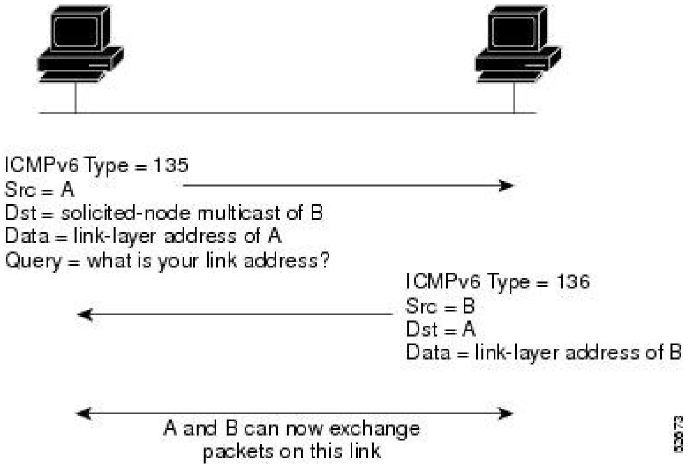

ICMPv6 Type = 135
Src = A
Dst = solicited-node multicast of B
Data = link-layer address of A
Query = what is your link address?
ICMPv6 Type = 136
Src = B
Dst = A
Data = link-layer address of B
A and B can now exchange packets on this link
82873

Figure 6. IPv6 neighbor discovery process. Copied from [26,82].

As it can be seen on figure 6, the neighbor discovery uses ICMPv6 messages. The neighbor discovery process starts when a node sends out a router solicitation message to the solicited-node multicast address of the node of which link-layer address it wants to discover. The solicited-node multicast address is explained in chapter “2.6 IPv6 multicast and anycast” of this study. The sending node includes its own link-layer address in the neighbor solicitation message and the message source is the IPv6 address of the sender. Next step occurs when the node that has the IPv6 address that correspond to the solicited-node multicast address responds to the requesting node with neighbor advertisement message. This message has the IPv6 address of the requesting node as the destination address and the message include the link-layer address of the second node. When the requesting node gets the neighbor advertisement message, both nodes can communicate on that link. When the link-layer address is obtained, neighbor solicitation messages are sent to the unicast address of the other node to make sure it still reachable. [26,81-83.]

In router discovery host and routers become aware of each other's presence and exchange information. Figure 7 illustrates the router discovery process in IPv6.

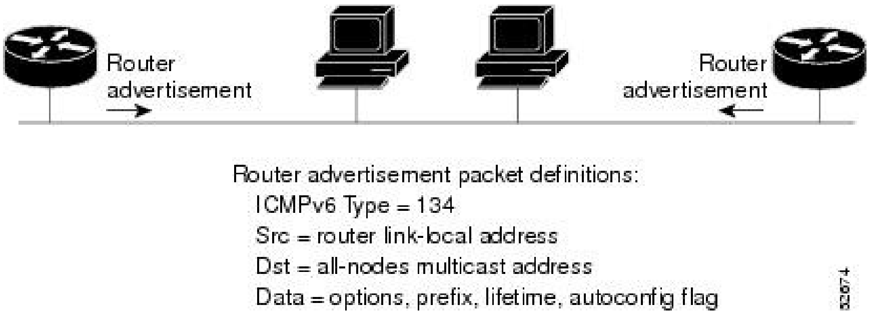

Router advertisement
Router advertisement
Router advertisement packet definitions:
ICMPv6 Type = 134
Src = router link-local address
Dst = all-nodes multicast address
Data = options, prefix, lifetime, autoconfig flag
52674

Figure 7. IPv6 router discovery. Copied from [26,84].

Router discovery in IPv6 works in the following fashion. As can be seen in figure 7, routers send router advertisement messages to link-local all-nodes multicast address of ff02::1. This happens in certain time periods. Router advertisement messages are also sent when a router receives router solicitation messages and in that case the response is sent to unicast address of the sender. Nodes send router solicitation messages when they start to the link-local scope all-routers multicast address “ff02::2”. If the client node already has a unicast address, it uses that as a source address; otherwise, address “0:0:0:0:0:0:0:0” is used as a source. With router advertisement messages extra information such subnet prefix, default router, autoconfiguration information, MTU, default gateway and routes can be given. [22,55,66;26;28,38,45.]

2.6 IPv6 Multicast and Anycast

Multicast plays a central role in IPv6. IPv6 does not use broadcasting. In multicast packets sent to a multicast address are sent to all those interfaces that are part of the mutlicast group. Interfaces that listen to certain multicast traffic are part of that multicast group. Multicast addresses start with “ff” in hexadecimal and they are defined by scope, flag and group ID. The Scope defines where in the network the address can be used. Scope was described in the chapter 2.1 of this thesis. The T-flag indicates whetever the multicast address is defined fixed or not. The Group ID indicates the multicast group. For example, multicast address “ff02::2” means it is in link-local scope and the group ID of 2 means all routers. In other words, a packet sent to this multicast address will be received by all routes in the link-local scope, but not beyond that.[7;704-712;29,29-32,43-45.]

A special type of multicast address is a solicited node multicast address. The Solicited node multicast address is created by adding the last 24 bits of IPv6 unicast address to the multicast address “ff02::1:ff00::/104”.[30] The Solicited-node multicast address is used by the neighbor discovery protocol to the get link-layer address of another node, when only the IPv6 address of that node is known. Using the solicited-node multicast address in link-layer address resolution means less traffic and better performance for the network. The Neighbor discovery process is explained in chapter 2.5 of this study. [7;704-712;30,14;31.]

In anycast a packet is sent to the nearest interface that has the anycast address assigned. Anycast addresses are like IPv6 unicast addresses. When a device has the same unicast address on more than one interface, the address will become an anycast address. Configuration is also needed on the device so it can understand it has an anycast address assigned. For example, mobile IPv6 employs anycast. [7;704-712.]

The MLD (Multicast Listener Discovery) protocol is used for managing multicast group members. Routers use the MLD protocol to find out which nodes want to receive specific multicast traffic on directly attached links. MLD uses ICMPv6 messages for communication. ICMPv6 message type 130 is a query message, and routers use it to find out if any node wants receive multicast traffic on a link. A query can be general, which means that it queries all groups or group-specific which means that a specific group is queried. If no one is listening, the router can stop the specific multicast traffic. Nodes can send report messages of ICMPv6 type 131 if they want to join a certain multicast group. Report messages are also sent if a node has first received a query message. MLDv1 done messages of ICMPv6 type 132 are sent by a node when it does not want to receive multicast traffic anymore. MLDv2 uses an ICMPv6 type 143 report message instead. There are different versions of MLD, MLDv1 and MLDv2. Version 1 of MLD is similar to IGMPv2 (Internet Group Management Protocol) and version 2 of MLD is similar to IGMPv3. Even though MLDv1 and MLDv2 have difference in the MLD messages, MLDv2 needs to support also MLDv1 messages. This means that MLDv1 and MLDv2 can operate together. [29;30;32;33,2,13-19.]

2.7 IPsec

IPsec (IP Security Architecture) consists of a group of protocols that help to make IPv6 more secure using authentication and encryption. Authentication means that the sender of the packet can be verified. Encryption means that the data that was sent cannot be read by someone else. IPsec also provides integrity for the data, meaning it cannot be changed during transmission. IPsec is designed by IETF (Internet Engineering Task Force) and operates in the network layer of the OSI (Open Systems Interconnection Reference) model. IPsec uses AH (authentication header) for authentication and ESP (Encapsulating Security Payload) both for authentication and/or encryption. IKE (Internet Key Exchange) is used for secure exchange of keys. IKE works in two phases. In first phase of IKE a secure channel is formed between two endpoints. In the second part, SAs (Security Associations) that protect the packets are created.
[7,631-633;9,311-314;19,199-209;34;35.]

IPsec can operate in tunnel mode or transport mode. The transport mode encapsulates the packet, but not the headers. The Transport mode is usually used between two hosts. The Tunnel mode encapsulates the payload of the packet and also the headers under a new header. The Tunnel mode is usually used when the IPsec traffic goes through one or two gateways. The gateways encapsulate and decapsulate the packets and then send the packet to a host behind the gateway.
[19,199-209;35;36.]

In this thesis, IPsec is used to create VPN (Virtual Private Network) tunnels between firewalls or a client computer and a firewall. VPN configuration for the USG firewall is described in chapter 3.4 of this thesis.

2.8 IPv6 Transition Mechanisms

There are a number of different methods to transition from IPv4 to IPv6. In dual-stack configuration both IPv4 and IPv6 exist at the same time on the same device. The Downside of dual-stacking is that it uses more system resources. Maintaining a dual-stack device can also be more demanding as both protocols need to be configured and maintained. A network can also be dual-stacked if it enables both IPv4 and IPv6. Tunneling is a technique in which a certain protocol is encapsulated inside another protocol through a network that does not support the first protocol. The transport protocol carries the passenger protocol over the network. IPv6 traffic can be routed inside IPv4 packets, through an IPv4 network. In such a case, IPv6 is the passenger protocol and IPv4 is the transport protocol. In tunneling scenarios the network does not need to be dual-stacked, but the devices at the tunnel end-points require dual-stacking. Tunnels can be created between gateways or gateways and host. Both manually and automatically configured tunnels exist. IPv6 and IPv4 packets can also be translated from IPv4 to IPv6 and from IPv6 to IPv4 using a translating device. This kind of a scenario is useful for old devices that do not have IPv6 capability. [7,691-696,824-830;37,2-4;19,33;38.]

In this thesis 6in4 tunneling and dual-stacking are discussed because they are used in the practical part of the study. In 6in4 tunneling IPv6 packets are transported in IPv4 packets through the IPv4 internet. 6In4 tunneling is also called proto-41-tunneling because of the IP protocol number 41 that is used in the in IPv4 packet header when it encapsulates the IPv6 packets. 6In4 tunneling is static tunneling method. Tunnelbrokers are special service providers that offer IPv6 tunneling over the IPv4 network. In this study the Hurricane Electrics tunnelbroker service is used. [38;39;40.]

3 IPv6 in SoHo Enviroment

The goal of this study is to create a manual for ZyXEL Finland's CSO organization about IPv6 configuration with the ZyXEL USG60 firewall. The manual is based on testing done mainly with the USG60 firewall. The following sections describe the testing methods, equipment and scenarios.

3.1 Testing and Equipment

Based on testing a manual was made for CSO internal usage and also to be delivered to clients. Six different testing scenarios were conducted: getting an IPv6 address from ISP and from TunnelBroker, delegating the address to LAN, and three VPN testings. Together these IPv6 scenarios formed a base for IPv6 deployment in the SoHo environment.

The testing was done in dual-stack environment. In a dual-stack scenario both IPv4 and IPv6 exist on the same network and on the same device. The Dual-stack environment is likely to become a common deployment scenario in the transitioning period from IPv6 to IPv4.[7,824-828.] Scenarios were meant to be basic so that main functionality of IPv6 would be made clear. This information could also be used when configuring other ZyXEL products.

The ZyXEL USG60 firewall was decided to be used for the testing. Figure 8 illustrates the USG 60 firewall.

Figure 8. ZyXEL USG60 firewall. Copied from [41].

The USG60 VPN firewall has support for dual-stack IPv6, IPv6 addressing, DHCPv6, tunneling, static and policy routing, IPsec VPN and IPv6 firewall. USG60 can be configured either using GUI (graphical user interface) or with CLI (command line interface). As can be seen in figure 8, USG60 has two WAN (Wide Area Network) ports and four LAN ports. USG-series firewalls are designed for small-to-medium sized businesses and are a popular ZyXEL security product. [5,42,43] Many of the calls coming to ZyXEL Finland's CSO concern ZyXEL USG-series firewalls.

The tests were done using a DNA/Welho home subscriber cable connection, since it supports IPv6 natively[44,45]. The Cisco EPC3825 cable modem in bridged mode was used to connect the USG60 to Welho/DNA cable connection. When testing site-to-site VPN, an additional USG110 firewall was used to act as the VPN remote site. For client-to-site VPN testing, the ZyXEL LTE3301 LTE router in bridged mode was used along with Saunalahti 3G data connection. Figure 9 illustrates the LTE3301 LTE router.

Figure 9. ZyXEL LTE3301 LTE router. Copied from[46].

As can be seen in figure 9, LTE 3301 is an LTE router with external antennas. LTE3301 allowed the client computer to have IPv6 connectivity[46]. After acquiring the IPv6 address with LTE3301, the client computer could be configured to form a VPN tunnel to USG60 that acquired IPv6 connectivity from the Welho/DNA cable connection.

For each testing scenario a setup was created, testing conducted and testing steps documented for the manual. The Parts of the thesis that describe the study are divided into three chapters, each chapter describing similar testing scenarios and reasons for the testing.

3.2 Getting a Global IPv6 Address

The First part of the testing was to acquire a global IPv6 address for the USG60. Some ISP's already support IPv6 in Finland, and DNA delegates IPv6 addresses with prefix delegation in its cable subscriber connections[44]. Getting the IPv6 address from a tunnelbroker was also included in the testing and the manual. Hurricane Electric provides 6in4 tunnels that allow IPv6 packets to be encapsulated in IPv4 packets to be transported through the IPv4 internet. This would benefit clients whose ISP would not support IPv6. Hurricane Electric was chosen for the tunnelbroker because it is free and it also supports multiple tunnels. Previous testing in ZyXEL CSO was also done with Hurricane Electrics tunnels.[38;40;47;48.]

The First step in configuration was to create an account on the tunnelbroker.net website. In the website five tunnel could be created for free. The website also gave instructions on how to configure tunnels[40]. Figure 10 describes the testing scenario for the 6in4 tunnel using the Hurricane Electric's tunnel.

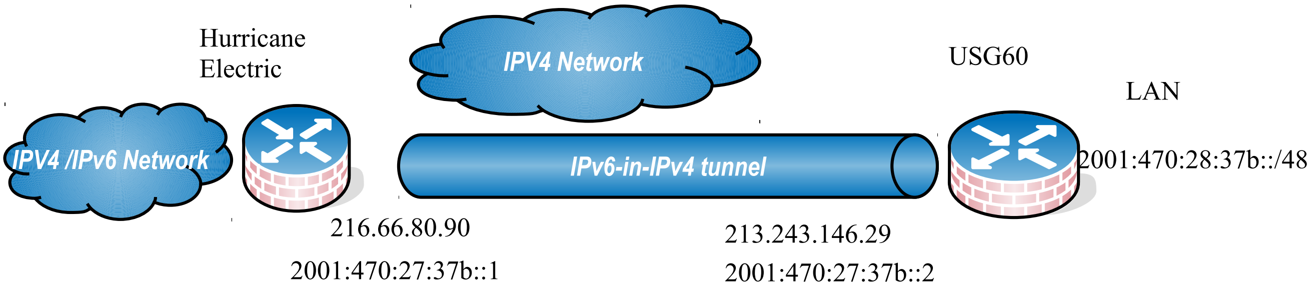
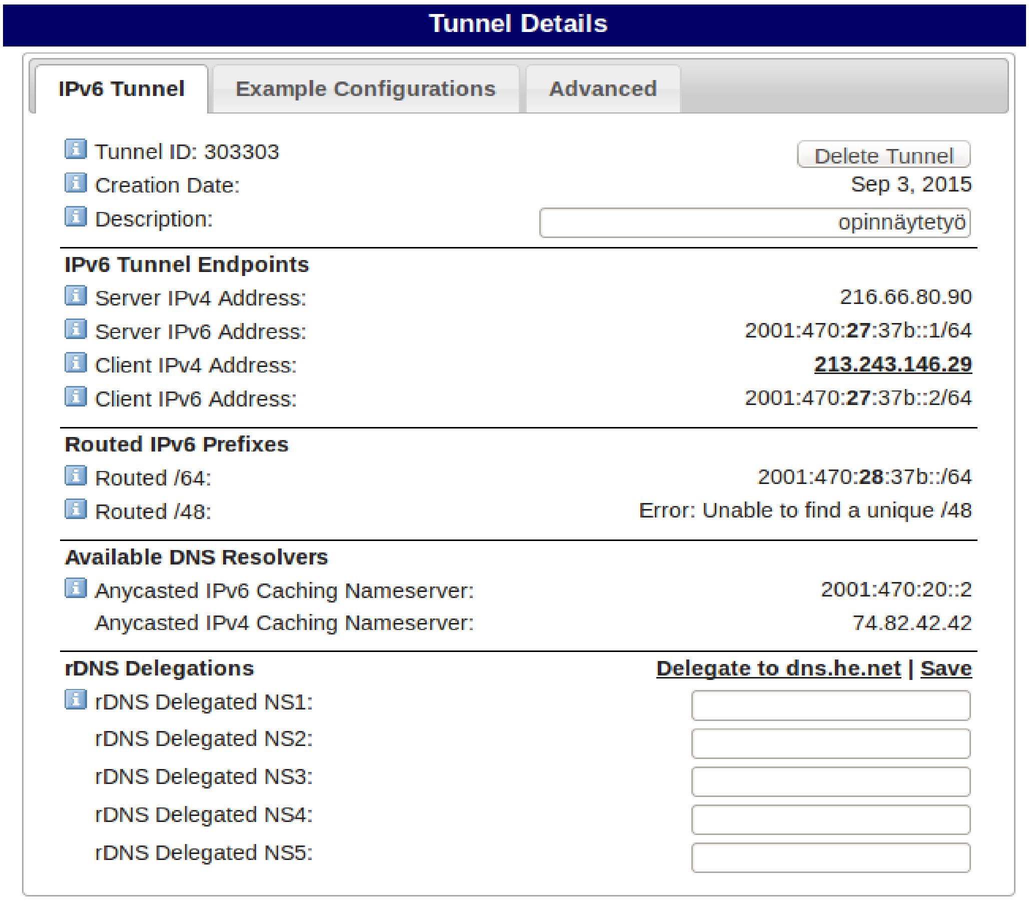


Figure 10. Tunnelbroker setup.

As can be seen in figure 10, USG60 is the other tunnel endpoint of the 6in4 tunnel and the Hurricane Electric is the other. Packets travel in 6in4 tunnel across the IPv4 internet to Hurricane Electric and from there to the IPv6 internet.[38;40] Figure 11 illustrates the settings on the Hurricane Electric's side of the tunnel.



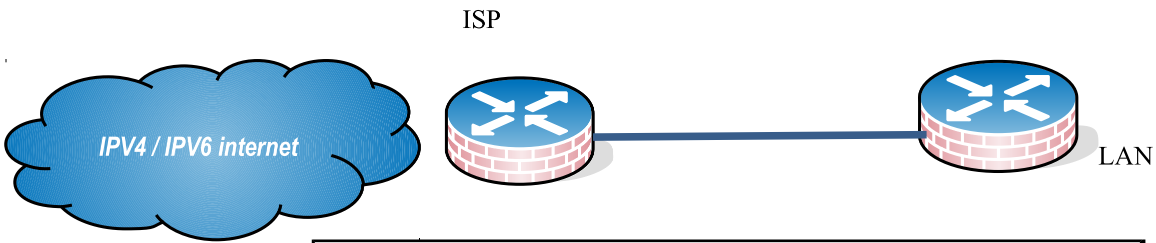
Tunnel Details

Tunnel ID: 303303	
Creation Date:	Sep 3, 2015
Description:	opinnäytetyö
IPv6 Tunnel Endpoints	
Server IPv4 Address:	216.66.80.90
Server IPv6 Address:	2001:470:**27**:37b::1/64
Client IPv4 Address:	**213.243.146.29**
Client IPv6 Address:	2001:470:**27**:37b::2/64
Routed IPv6 Prefixes	
Routed /64:	2001:470:**28**:37b::/64
Routed /48:	Error: Unable to find a unique /48
Available DNS Resolvers	
Anycasted IPv6 Caching Nameserver:	2001:470:20::2
Anycasted IPv4 Caching Nameserver:	74.82.42.42
rDNS Delegations	**Delegate to dns.he.net | Save**
rDNS Delegated NS1:	
rDNS Delegated NS2:	
rDNS Delegated NS3:	
rDNS Delegated NS4:	
rDNS Delegated NS5:	

Figure 11. Settings of the Hurricane Electric Tunnelbroker. Copied from[49].

As can be seen in figure 11, the Hurricane Electrics 6in4 tunnel has the IPv4 address and also the IPv6 address. The tunnelbroker delegates an IPv6 address block of /64 to its clients. First, the tunnel was created on the Hurricane Electric web page. After that USG60 was configured as the other end of the 6in4 tunnel. After the configuration was complete, USG had global IPv6 connectivity. IPv6 addresses could also be delegated to USG LAN clients and with the help of routing rules client nodes were able to reach IPv6-only website. Configuration steps to create the tunnel were added to the manual. [40.]

DNA offers natively supported IPv6 to its cable subscriber clients as do some other ISP's in Finland. DNA uses prefix delegation to deliver the IPv6 address block to clients and as this is likely to be a common method of getting the IPv6 address in the future, it was therefore tested and added to the manual. Figure 12 illustrates the testing scenario for getting the IPv6 address from ISP. [7,824-828;44.]



Address block from ISP	2001:14ba:2fe:ea00::/56
Prefix for LAN1	2001:14ba:2fe:ea01::/64
LAN1 static address	2001:14ba:2fe:ea01::3/64

Figure 12. Getting IPV6 address from ISP.

DNA assigned one /128 address for the communication between USG and itself. Then a separate prefix address block was delegated to the USG. This address block was delivered using the prefix delegation technique. As can be seen in the figure 12, the prefix obtained from the ISP, /56 in this case, could be further used to give out addresses to LAN clients and to configure a static address to the LAN1 interface. During testing it was also discovered that the USG WAN interface must request a SLAAC address as well to get a default IPv6 gateway from the ISP.
[44,50.]

ZyXEL CSO also had a security concerns with the USG60 default IPv6 configuration. By default USG allows RA, RS, NA and NS ICMPv6 messages to be delivered from WAN to itself. These default settings were configured in the factory to the default configuration of USG. It was necessary to see if all the messages were actually necessary for the functionality of USG when requesting the address from the ISP. Allowing unnecessary traffic to reach the firewall could be a security issue. By trial and error it was discovered that RS messages could be blocked without an adverse effect for the firewall functionality when requesting the address block. Also the MLD protocol could be blocked. However, these findings were not added to the manual.

3.3 Routing and LAN Network

When IPv6 connectivity had been obtained for the USG60, the second step was to test how IPv6 addresses could be delegated to LAN clients in order to create a functioning network. The Routing of IPv6 was also tested. USG60 supports DHCPv6 and SLAAC methods to delegate addresses to LAN clients.[42,43] SLAAC required fewer configuration steps on the USG side, but for DHCPv6 additional address objects were configured. A Windows 10 PC (Personal Computer) was used as the LAN client.

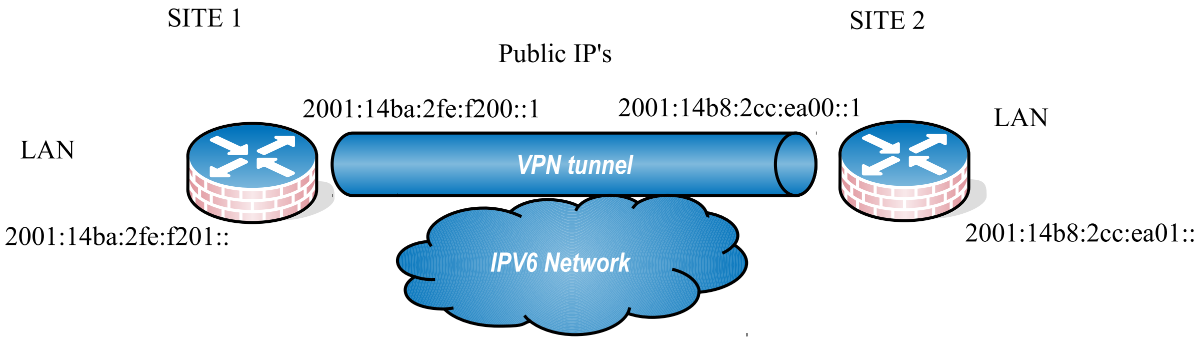
Figure 12 shows the subnetting scenario for the LAN testing. The Address block of “2001:14ba:2fe:ea00::/56” was obtained from ISP with prefix delegation. Then the addresses were delegated to LAN clients with DHCPv6 and also using the SLAAC method. USG60 supported both of these methods simultaneously. DHPCv6 also had the possibility to distribute DNS (Domain Name Server) servers to clients. This feature was also tested. Based on the testing it could be concluded that DHCPv6 and SLAAC worked on the USG60. [19,167.]

USG series firewalls do not route IPV6 addresses automatically so it was necessary to create routing policies manually. Otherwise, LAN clients would not have connectivity beyond USG. After manual routing policies were added, LAN clients were able to have IPv6 connectivity. [42,43.]

3.4 IPv6 VPN

Many ZyXEL CSO customers are using site-to-site or client-to-site VPN connections in IPv4, and support cases concerning their configuration are frequent. ZyXEL Finland's CSO wished that IPv6 VPN was tested with the ZyXEL device and that configuration steps were added to the manual. USG60 supports client-to-site and site-to-site IPsec IPv6 VPN's. Both scenarios were tested.

Site-to-site VPN connect two LAN networks (”sites”) behind firewalls[51]. Two USG's were needed for this test. The USG's were connected to a bridged cable modem, so both got public a IPv6 address block. The Scenario was not ideal, but there was no alternative solution available to get two firewalls with a public IPv6 address at the time of testing. The Configuration of IPv6 site-to-site VPN was similar to IPv4 site-to-site VPN, and there were no major difficulties. When the tunnel was up, verification was done by pinging the interface address behind the USG firewall. This ensured that VPN tunnel was indeed working. Figure 13 shows the testing scenario for the site-to-site IPsec VPN.[51,17-25.]



Site1	
WAN	2001:14ba:2fe:f200::1/56
LAN1	2001:14ba:2fe:f201::/64
PHASE1	
Pre-shared key	1234test
Local ID	::1111
Encryption	AES128
Authentication	SHA1
Key Group	DH1
Phase2	
Local policy	2001:14ba:2fe:f201::/64
Remote Policy	2001:14b8:2cc:ea01::/64
Active protocol	ESP
Encapsulation	Tunnel
Encryption	AES128
Authentication	SHA1
Key Group	DH1

Site2	
WAN	2001:14b8:2cc:ea00::1/56
LAN1	2001:14b8:2cc:ea01::/64
Phase1	
Pre-shared key	1234test
Local ID	::2222
Encryption	AES128
Authentication	SHA1
Key Group	DH1
Phase2	
Local policy	2001:14b8:2cc:ea01::/64
Remote Policy	2001:14ba:2fe:f201::/64
Active protocol	ESP
Encapsulation	Tunnel
Encryption	AES128
Authentication	SHA1
Key Group	DH1

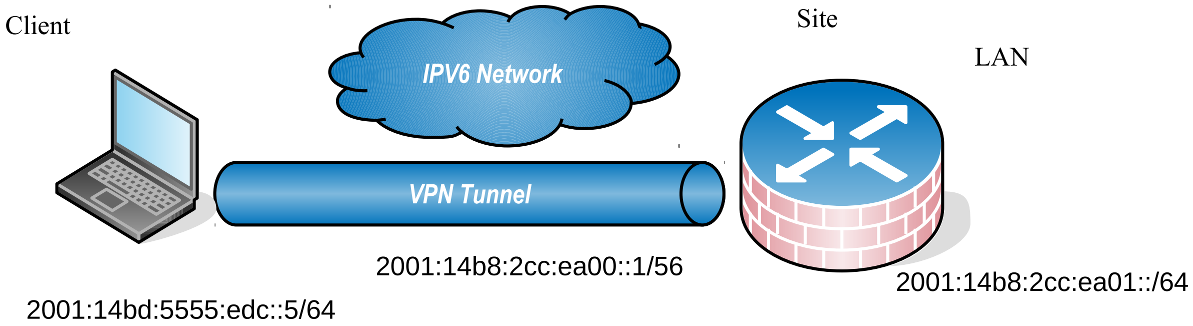
Figure 13. Site-to-site IPsec VPN scenario and VPN settings.

As can be seen in figure 13, both ends of the tunnel needed to be configured similarly. Encapsulation, encryption and authentication methods needed to match between the tunnel endpoints. IPsec VPN tunnel creation consisted of two phases. In phase 1 the pre-shared key and encryption algorithms were configured. Then phase 1 settings were added to the phase 2 settings. In phase 2 local and remote policies were defined. These policies dictate the address space that the user on the other side of the tunnel can have connectivity to. Phase 2 settings also defined the security zone that the particular VPN was part of. If the VPN connection was not part of any zone, routing rules could not be applied to that VPN connection.[51,17-25.]

In USG60 VPN traffic also needed AH, IKE and ESP protocols to pass trough the USG firewall. However when using USG's default firewall settings, these protocols were already allowed to pass, so no further configuration was needed. [51.]

Client-to-site IPv6 IPsec VPN was also tested. Client-to-site VPN's are used to create a secure connection, for example, to company, headquarters office from a remote location. A Teleworker might be at his or her home doing remote work or he/she might be using LTE (Long Term Evolution) connection in a hotel to access the company server. In these cases a client-to-site VPN connection is required [7,8;51,54;52.]. Many CSO clients use also client-to-site VPN connections and therefore this scenario was included in the testing and the manual.

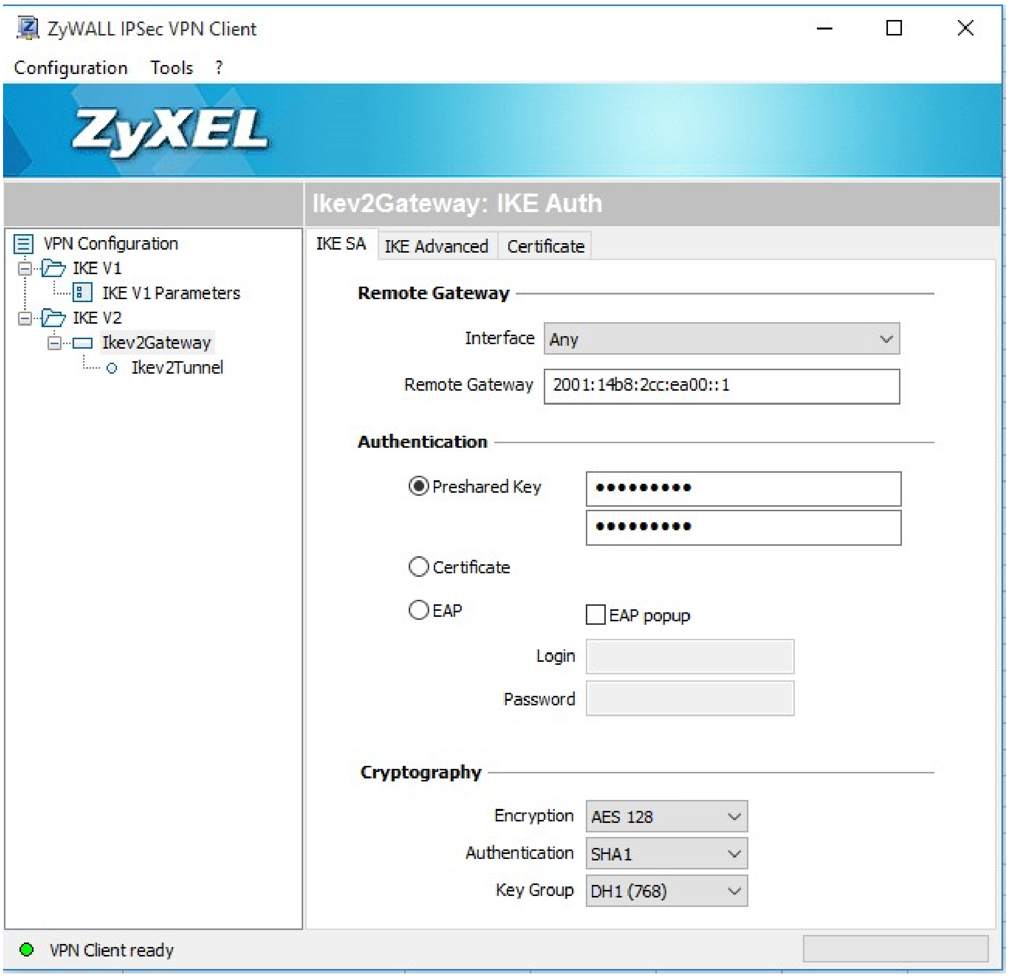
Client-to-site IPsec VPN configuration differs from site-to-site IPsec VPN and it was important to test it as well. It also gave an opportunity to test ZyXELL VPN client software in the IPv6 enviroment. Figure 14 show the client-to-site IPsec VPN testing scenario and settings. First, client computer needed to get a global IPv6 address, and this was accomplished by connecting the client computer to a Saunalahti 3G network from which it obtained the IPv6 address. ZyXEL LTE3301 LTE router was used to get 3G connectivity. Then the ZyXEL VPN software client version 3.4 was installed on the Windows 10 client machine so it could establish the connection to the USG60. In general ZyXEL VPN client software is made by Greenbow and requires a license to be bought to be used after a 30-day trial has expired. Many ZyXEL clients use the ZyXEL VPN client. [52.]



WAN	2001:14b8:2cc:ea00::1/56
LAN1	2001:14b8:2cc:ea01::/64
Client address ”virtual”	2001:14ba:1111:2222::5/64
Client address	2001:14bd:5555:edc::5/64
PHASE1	
Pre-shared key	1234test
Local ID	::5555
Encryption	AES128
Authentication	SHA1
Key Group	DH1
Phase2	
Local policy	2001:14b8:2cc:ea01::/64
Active protocol	ESP
Encapsulation	Tunnel
Encryption	AES128
Authentication	SHA1
Key Group	DH1

Figure 14. Client-to-site VPN scenario and settings.

As can be seen in figure 14, the client-to-site VPN also consists of phase 1 and 2 settings. Phase 1 settings define the pre-shared key and encryption and authentication algorithms. Phase 1 settings are attached to phase 2 settings and a local policy is defined. The Local policy defines to which subnet the remote user can have connectivity. In the study, the settings were first configured on the USG60 side of the tunnel and then on VPN client software in Windows 10 client. Figure 15 illustrates the phase 1 settings on the ZyXEL VPN client software.



Ikev2Gateway: IKE Auth

Remote Gateway

Interface: Any

Remote Gateway: 2001:14b8:2cc:ea00::1

Authentication

● Preshared Key: •••••••••• / ••••••••••

○ Certificate

○ EAP □ EAP popup

Login:

Password:

Cryptography

Encryption: AES 128

Authentication: SHA1

Key Group: DH1 (768)

● VPN Client ready

Figure 15. Greenbow VPN client. Copied from [53].

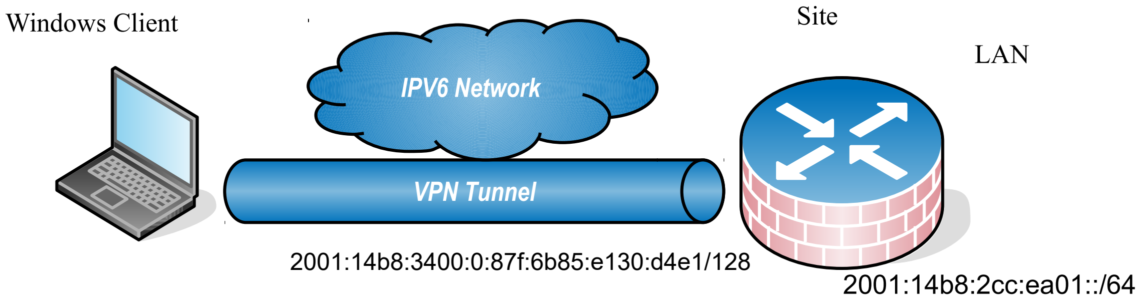
As can be seen in figure 15, the ZyXEL VPN client software offers a graphical way to configure the VPN client settings. Cryptography settings needed to match the phase 1 security settings on the USG60 side of the tunnel. Remote gateway was the IPv6 address of the USG60 firewall.

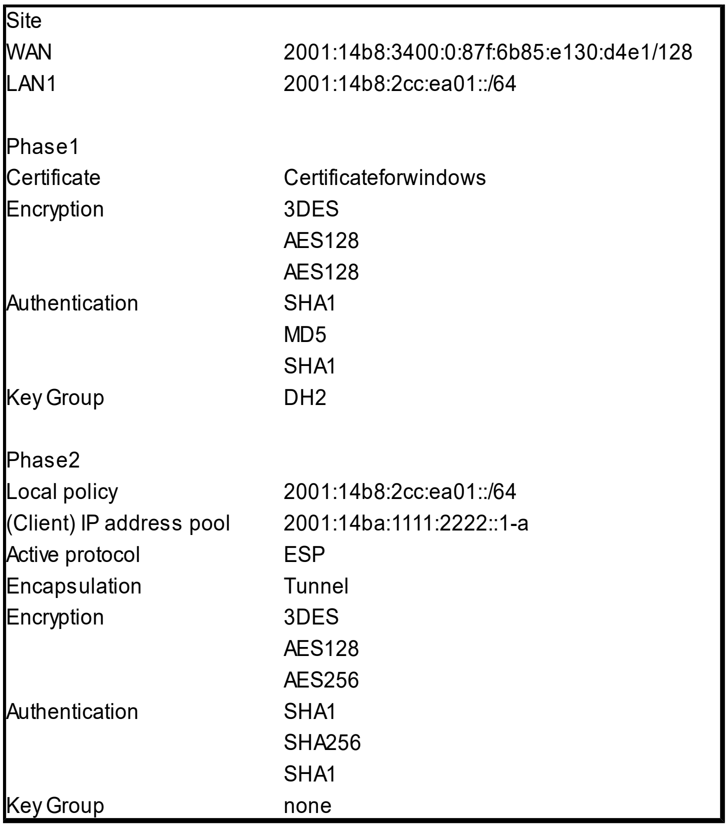
When it come to the ZyXEL USG60 firewall it was possible to test the IKEv2 configuration payload feature. With this feature it was possible to provide the client with DNS server and an IPv6 address from the VPN server. The Functionality of this feature was also tested. In general, configuration payload reduces some of the teleworker configuration efforts when establishing the tunnel.[54.]

Some clients do not want to buy the IPsec VPN client software license, but they still need a client-to-site VPN connection. In such situations it is possible to use the Windows built-in IPsec IKEv2 VPN with certificate authentication to create the client-to-site tunnel, and no third-party software or licenses are needed. This feature has been in Windows since Windows 7. USG60 also supports IPsec IKEv2 VPN with certificate authentication. In this study a self-signed 2048 bit X.509 certificate needed to be created on the USG60 and imported to the Windows client to be used for the authentication. This was the final part of the testing.[51,25-40.]

The X.509 certificate is used to tie a public key to a name, DNS entry, IP or email address. In this way it can be verified that when the client is connecting to a certain web resource, for example a website that the resource is the one the client actually wants to connect to, and not an impostor. A Self signed X.509 certificate is not signed by a CA (Certificate Authority), but by the same device to which connection is made. In this case, the identity of the target device cannot be verified but the certificate is still used for securing the communication between the client and the target device.
[50;51,25-40;55;56;57;58.]

Figure 16 illustrates the configuration scenario for IPsec IKEv2 VPN with a certificate authentication testing scenario[51,25-40.].

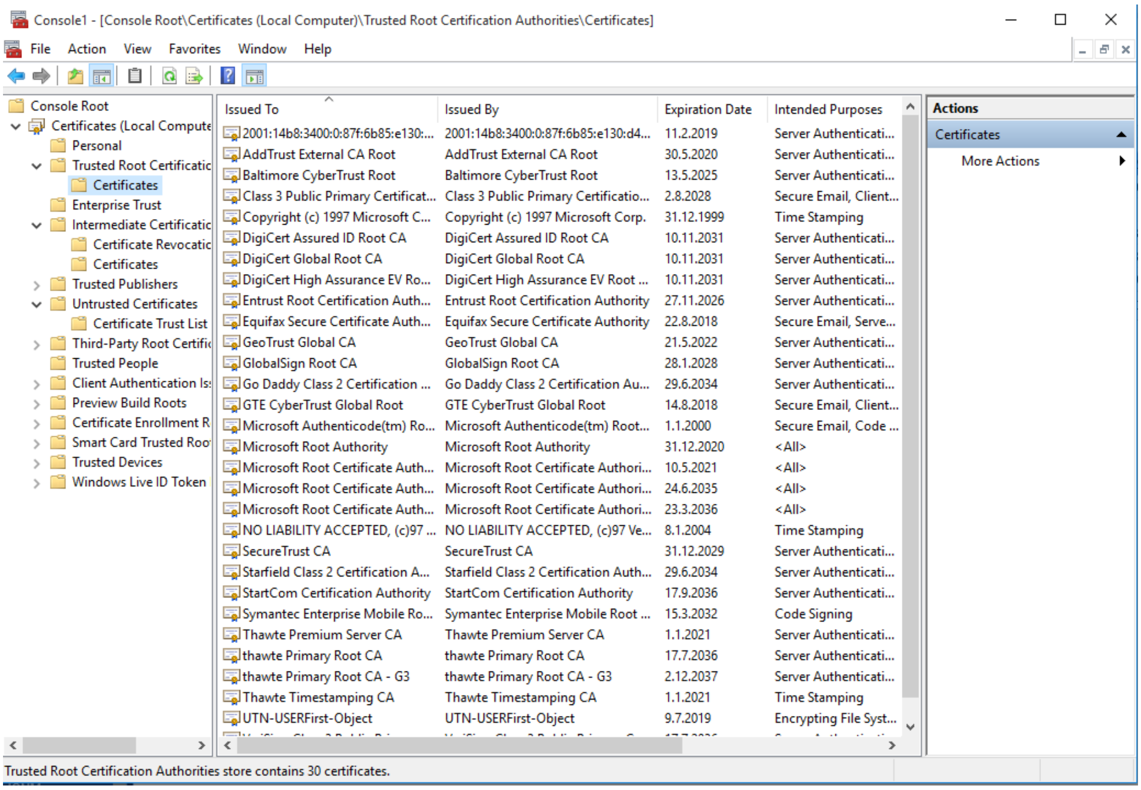




Site	
WAN	2001:14b8:3400:0:87f:6b85:e130:d4e1/128
LAN1	2001:14b8:2cc:ea01::/64
Phase1	
Certificate	Certificateforwindows
Encryption	3DES AES128 AES128
Authentication	SHA1 MD5 SHA1
Key Group	DH2
Phase2	
Local policy	2001:14b8:2cc:ea01::/64
(Client) IP address pool	2001:14ba:1111:2222::1-a
Active protocol	ESP
Encapsulation	Tunnel
Encryption	3DES AES128 AES256
Authentication	SHA1 SHA256 SHA1
Key Group	none

Figure 16. IPsec IKEv2 VPN with certificate authentication testing scenario and settings.

As can be seen in figure 16, the self-signed certificate (“Certificateforwindows”) was used for authentication in phase 1. After the certificate had been created on the USG60, VPN phase 1 and phase 2 were configured. Otherwise, the configuration of the VPN tunnel on the USG60 side was similar to configuring the IPsec client-to-site VPN. After the tunnel was ready on the USG60, the certificate was downloaded to the Windows client machine and imported with the MMC (Microsoft Management Console) program. Figure 17 illustrates the MMC program on the Windows client. In general MMC allows adding certificates to the Windows client and associating them with a user account or with the computer itself. This way Windows client holds the certificate created in the USG60. [51;59.]



Issued To	Issued By	Expiration Date	Intended Purposes
2001:14b8:3400:0:87f:6b85:e130:...	2001:14b8:3400:0:87f:6b85:e130:d4...	11.2.2019	Server Authenticati...
AddTrust External CA Root	AddTrust External CA Root	30.5.2020	Server Authenticati...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13.5.2025	Server Authenticati...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	2.8.2028	Secure Email, Client...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31.12.1999	Time Stamping
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10.11.2031	Server Authenticati...
DigiCert Global Root CA	DigiCert Global Root CA	10.11.2031	Server Authenticati...
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10.11.2031	Server Authenticati...
Entrust Root Certification Auth...	Entrust Root Certification Authority	27.11.2026	Server Authenticati...
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	22.8.2018	Secure Email, Serve...
GeoTrust Global CA	GeoTrust Global CA	21.5.2022	Server Authenticati...
GlobalSign Root CA	GlobalSign Root CA	28.1.2028	Server Authenticati...
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	29.6.2034	Server Authenticati...
GTE CyberTrust Global Root	GTE CyberTrust Global Root	14.8.2018	Secure Email, Client...
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	1.1.2000	Secure Email, Code ...
Microsoft Root Authority	Microsoft Root Authority	31.12.2020	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	10.5.2021	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	24.6.2035	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23.3.2036	<All>
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	8.1.2004	Time Stamping
SecureTrust CA	SecureTrust CA	31.12.2029	Server Authenticati...
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	29.6.2034	Server Authenticati...
StartCom Certification Authority	StartCom Certification Authority	17.9.2036	Server Authenticati...
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	15.3.2032	Code Signing
Thawte Premium Server CA	Thawte Premium Server CA	1.1.2021	Server Authenticati...
thawte Primary Root CA	thawte Primary Root CA	17.7.2036	Server Authenticati...
thawte Primary Root CA - G3	thawte Primary Root CA - G3	2.12.2037	Server Authenticati...
Thawte Timestamping CA	Thawte Timestamping CA	1.1.2021	Time Stamping
UTN-USERFirst-Object	UTN-USERFirst-Object	9.7.2019	Encrypting File Syst...

Trusted Root Certification Authorities store contains 30 certificates.

Figure 17. The MMC program on Windows client. Copied from[60].

As can be seen in figure 17, the certificate from USG60 is placed under the trusted root authentication authorities in the MMC program. The certificate holds the USG60 WAN IPv6 address. In this study it was important to test and document the use of the MMC program and add the instructions to the manual so that the CSO clients could also configure the IKEv2 VPN on the Windows client as well. This testing was complicated and required several steps to complete. After all configurations were complete, the tunnel was tested. However, no connection could be established. After debugging procedures, reason was found to be NATT (Network Address Translation-Traversal) protocol. Generally speaking NATT is used to create and maintain a connection between networks behind NATted gateways. When UDP (User Datagram Protocol) port 4500 was opened on the USG60 firewall in the study, the tunnel was formed and VPN was established[61]. Therefore it was necessary to include the firewall rule in the CSO manual. Using USG60 application notes document was helpful when configuring the VPN settings.

3.5 Manual

When all testing was finished, a step-by-step manual was created. The Manual is for ZyXEL CSO internal use and to be distributed to customers. The Manual consists of five sections. The First section describes the use of a tunnelbroker service to receive the global IPv6 address. The Second part describes the use of natively supported IPv6 from ISP and address delegation. The Third part describes the use and configuration of site-to-site VPN connection. Parts 4 and 5 describe the configuration of client-to-site IPsec VPN and client-to-site IPsec VPN with certificate authentication, respectively.

The manual gives illustrated step-by-step instructions to configure each step of the process. It also includes additional information about IPv6 to help the reader to understand what he/she was actually configuring. The Manual is intended to be used inside the European CSO organization if information about IPv6 is needed. The Manual can also be emailed to ZyXEL Finland's CSO customers when they are in need of IPv6 instructions. Using the manual to help customers configure things themselves saves a lot of time for the customer service agents, allowing them to handle the calls and emails of other clients. The basic structure of the manual is based on an IPv4 VPN manual created by ZyXEL Finland's CSO and also instructions created by ZyXEL corporation in Taiwan.

The Manual is intended to be clear and precise and to describe the basic functionality of IPv6 features. Extra effort was placed on describing the reader why each configuration step was taken. The Manual uses a lot of images and is illustrative and clear. The Manual was saved in PDF (Portable Document Format) but a copy of the original word file has also been given to the ZyXEL Finland's CSO. Later, possible corrections can be made to the document and new instructions can also be added.

4 Conclusions

The aim of this study was to get useful information of configuring IPv6 for the SoHo environment and to produce a short manual for ZyXEL Finland about IPv6.

Several test were conducted. After testing was completed, it could be shown that basic IPv6 functionality worked in ZyXEL devices. A manual was made for ZyXEL Finland CSO describing the configuration steps of five different IPv6 deployment scenarios. The manual consisted of step-by-step instructions to configure each scenario. Based on the initial testing phase, it could be concluded that IPv6 was not as straightforward as it first appeared.

The ZyXEL devices also lacked some IPv6 features that IPv4 already has. One such feature was automatic routing. Once the testing was done, the manual was created. The manual also proved to be more work than anticipated. Making the manual clear, informative and not too long took time. Having earlier instructions created by ZyXEL CSO at hand was important in making the manual uniform. It can be concluded that creating documents that match company standards is detail oriented work. A lot of effort must be placed on the correctness of the information but also on the layout of the document. It is also important to plan testing the scenarios and the document layout beforehand. This significantly reduces the time to produce the manual.

The implementation phase of the study itself did not take as much time as originally planned. It can therefore be concluded that planning, setting clear goals and communication are important factors when creating documentation and testing for a company. However, testing and the manual provided valuable information about the migration process to IPv6.

The manual was submitted to ZyXEL Finland's CSO to be used as a training material and also to be delivered to customers working in the IPv6 environment. Further modifications, corrections and additional scenarios could be added to the manual in the future if needed.

References

1.IPv4 Address Depletion [online]. Internet Protocol Journal;3(10). Cisco.
URL: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-3/103_addr-dep.html. Accessed 10 February 2016.

2.IPv6 [online]. Wikipedia. Last modified on 22 February 2016.
URL: https://en.wikipedia.org/wiki/IPv6. Accessed 27 February 2016.

3.ZyXEL Company [online]. Wikipedia.last modified on 14 December 2015.
URL: https://en.wikipedia.org/wiki/ZyXEL. Accessed 27 February 2016.

4.Company Overview [online]. ZyXEL
URL: http://www.zyxel.com/fi/fi/about_zyxel/company_overview.shtml.
Accessed 10 February 2016.

5.ZyXEL Products [online]. ZyXEL
URL:http://www.zyxel.com/fi/fi/products_services/smb-security_appliances_and_services.shtml. Accessed 12 December 2015.
Accessed 10 February 2016.

6.ZyXEL ZyWALL USG 60 palomuuri [online]. Verkkokauppa.com
URL: https://www.verkkokauppa.com/fi/product/29205/fngdt/ZyXEL-ZyWALL-USG-60-palomuuri Accessed 12 December 2015.
Accessed 10 February 2016.

7.Teare Diane. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide.Indianapolis, IN: Cisco Press; 2010

8.IPv4 Address Exhaustion [online]. Wikipedia. Last modified on 25 February 2016.
URL: https://en.wikipedia.org/wiki/ipv4_address_exhaustion. Accessed 27 February 2016.

9.Stockebrand Benedikt.IPv6 in Practice. New York: Springer; 2007.

10.Picture of IPv6 Address [online]. Wikipedia. Created on 2 February 2010.

URL: https://en.wikipedia.org/wiki/IPv6#/media/File:Ipv6_address_leading_zeros.svg. Accessed 27 February 2016.

11.IPv6 Address [online]. Wikipedia. Last modified on 22 February 2016.
URL: https://en.wikipedia.org/wiki/IPv6_address. Accessed 27 February 2016.

12.IPv6 Reference Card [online]. RIPE network coordination centre.
URL; https://www.ripe.net/participate/member-support/new-lir/ipv6_reference_card.pdf. Accessed 10 February 2016.

13 IPv6 Packet [online]. Wikipedia. Last modified on 19 November 2015.
URL: https://en.wikipedia.org/wiki/IPv6_packet. Accessed 27 February 2016.

14. IPv6 Extension Headers Review and Considerations [online]. White Paper. Cisco.
URL:http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html. Accessed 10 February 2016.

15.IPv6 Addressing Guide [online]. Cisco.com.
URL:http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-government/sbaBN_IPv6addrG.pdf. Accessed 11 February 2016.

16.IPv4/IPv6 Subnet Calculator [online]. GestióIP.net.
URL: http://www.gestioip.net/cgi-bin/subnet_calculator.cgi. Accessed 11 February 2016.

17.Paquet Catherine, Teare Diane. CCNP Self-Study: Building Scalable Cisco Internetworks (BSCI) (2nd Edition) (Self-Study Guide). Indianapolis, IN:
Cisco Press; 2005.

18.Privacy Extensions for IPv6 SLAAC [online]. Internet Society.
URL:http://www.internetsociety.org/deploy360/resources/privacy-extensions-for-ipv6-slaac/. Accessed 11 February 2016.

19.Van Beijnum Iljitsch. Running IPv6. New York, NY: Apress; 2005.

20.Mun Youngsong, Keren Lee Hyewon. Understanding IPv6. New Yourk, NY: Spirnger; 2005.

21.Narten T, Draves R,Krishnan S. RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6 [online].
Internet Engineering Task Force; September 2007.
URL:https://tools.ietf.org/html/rfc4941
Accessed 11 February 2016.

22.Horley, Edward . Practical IPv6 for Windows Administrators. New York, NY: Apress; 2013.

23.Droms R,Bound J,Volz B,Lemon T, Perkins C, Carney M. RFC3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [online].
Internet Engineering Task Force; July 2003.
URL:https://tools.ietf.org/html/rfc3315
Accessed 11 February 2016.

24.Conta A,Deering S,Gupta M. RFC 4443 Internet Control Message Protocol (ICMPv6)for the Internet Protocol Version 6 (IPv6) Specification [online].
Internet Engineering Task Force; March 2006.
URL:https://tools.ietf.org/html/rfc4443#page-3.
Accessed 11 February 2016.

25.Das Kaushik. What is ICMPv6?[online]. IPv6.com.
URL:http://ipv6.com/articles/general/ICMPv6.htm. Accessed 11 february 2016.

26.IPv6 Configuration Guide, Cisco IOS Release 15.2M&T [online].
Cisco. 2012.
URL:http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-15-2mt-book.pdf.
Accessed 11 February 2016.

27.Narten T,Nordmark E,Simpson W.RFC2461 Neighbor Discovery for IP Version 6 (IPv6) [online].
Internet Engineering Task Force; December 1998.
URL:https://www.ietf.org/rfc/rfc2461.txt.
Accessed 11 February 2016.

28.Narten T,Nordmark E, Simpson W, Daydreamer, Soliman H. RFC 4861 Neighbor Discovery for IP version 6 (IPv6) [online].
Internet Engineering Task Force; September 2007.
URL:https://tools.ietf.org/html/rfc4861
Accessed 11 February 2016.

29. IP Multicast: LSM Configuration Guide, Cisco IOS XE Release 3S [online].
Cisco 2012
URL:http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_lsm/configuration/xe-3s/imc-lsm-xe-3s-book.pdf
Accessed 12 February 2016.

30.Martin Tim. IPv6 Multicast Primer [online].
Cisco; 2013
URL:http://www.txv6tf.org/wp-content/uploads/2013/07/Martin-IPv6-Multicast-TM-v3.pdf.
Accessed 12 February 2016.

31.Multicast IPv6 Addresses [online]. technet.microsoft.com.
URL:https://technet.microsoft.com/en-us/library/cc781068%28v=ws.10%29.aspx.
Accessed 12 February 2016.

32.Multicast Listener Discovery (MLD) [online]. Technet.microsoft.com.
URL:https://technet.microsoft.com/en-us/library/cc776494%28v=ws.10%29.aspx.
Accessed 12 February 2016.

33.Vida R, Costa L, Ed.RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6 [online].
Internet Engineering Task Force; June 2004.
URL:https://tools.ietf.org/html/rfc3810.
Accessed 12 February 2016.

34.Implementing IPsec in IPv6 Security [online]. Cisco.com,
URL:http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-ipsec.html.

Accessed 12 February 2016.

35.Das Kaushik. IPSec & IPv6 - Securing the NextGen Internet [online].
URL:http://ipv6.com/articles/security/IPsec.htm.
Accessed 12 February 2016.

36.Tunnel mode [online]. technet.microsof.com
URL:https://technet.microsoft.com/en-us/library/cc737154%28v=ws.10%29.aspx
Accessed 12 February 2016.

37.Nordmark E, Gilligan R. RFC4213 Basic Transition Mechanisms for IPv6 Hosts and Routers [online].
Internet Engineering Task Force; October 2005.
URL:https://tools.ietf.org/html/rfc4213.
Accessed 12 February 2016.

38.6in4 [online]. Wikipedia. Last modified on 7 March 2015
URL:https://en.wikipedia.org/wiki/6in4
Accessed 27 February 2016.

39.Tunnel Broker [online]. Wikipedia. Last modified on 25 January 2016
URL:https://en.wikipedia.org/wiki/Tunnel_broker
Accessed 27 February 2016.

40.Hurricane Electric Internet Services [online].
URL:https://tunnelbroker.net/
Accessed 27 February 2016.

41.Picture of USG60 Firewall [online] www.zyxel.ch
http://www.zyxel.ch/de/products/zyxel-usg60/
Accessed 13 February 2016.

42.USG Firewall Series [online]. ZyXEL.com
URL:http://www.zyxel.com/us/en/products_services/usg60w_60_40w_40.shtml?t=p
Accessed 13 February 2016.

43.USG60 Datasheet [online]. ZyXEL.
URL:ftp://ftp.zyxel.com/USG60/datasheet/USG60_7.pdf
Accessed 13 February 2016.

44.Niskanen Lauri. IPv6-tekniikka suomalaisissa kuluttajaliittymissä [online].
URL:https://ape3000.com/ipv6/
Accessed 13 February 2016.

45.IPv6 tulee, olemme valmiita [online]. DNA.
URL:https://www.dna.fi/fi/ipv6
Accessed 13 February 2016.

46.ZyXEL LTE 3301 LTE Router [online]. Verkkokauppa.com.
URL:https://www.verkkokauppa.com/fi/product/61289/gbckq/ZyXEL-LTE3301-LTE-modeemi-ja-WiFi-tukiasema
Accessed 10 February 2016.

47.Hurricane Electric [online]. Hurricane Electric.
URL:http://he.net/
Accessed 13 February 2016.

48.List_of_IPv6_tunnel_brokers [online]. Wikipedia. Last modified on 2 February 2016.
URL:https://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers
Accessed 27 February 2016.

49.Hurricane Electric Tunnel Details [online]. tunnelbroker.net.
URL:https://tunnelbroker.net/tunnel_detail.php
Accessed 27 February 2016.

50.Suominen Kimmo. IPv6 with Prefix Delegation and VRFs [online].
URL:https://kimmo.suominen.com/blog/2015/07/ipv6-with-prefix-delegation-and-vrfs/
Accessed 13 february 2016.

51.ZyWALL USG Series Application Notes [online]. ZyXEL.
URL:ftp://ftp.zyxel.com/USG60/application_note/USG60_2.pdf
Accessed 13 February 2016.

52.ZyWALL IPsec VPN client [online]. ZyXEL
URL:ftp://ftp.zyxel.com/ZyWALL_IPSec_VPN_Client/datasheet/ZyWALL%20IPSec%20VPN%20Client_3.pdf
Accessed 13 February 2016.

53.Greenbow VPN client [computer program]. Version 3.4. Greenbow; 2015

54.Kaufman C. RFC 4306 Internet Key Exchange (IKEv2) Protocol
Internet Engineerin Task Force; December 2005
URL:https://tools.ietf.org/html/rfc4306
Accessed 13 February 2016.

55.X.509 [online]. Wikipedia. Last modified on 25 February 2016.
URL:https://en.wikipedia.org/wiki/X.509
Accessed 27 February 2016.

56.What Is an X.509 Certificate? [online] access.redhat.com.
URL:https://access.redhat.com/documentation/en-US/Fuse_ESB_Enterprise/7.1/html/ActiveMQ_Security_Guide/files/X509CertsWhat.html
Accessed 13 February 2016.

57.When Are Self-signed Certificates Acceptable [online]?
https://www.sslshopper.com/article-when-are-self-signed-certificates-acceptable.html
Accessed 13 February 2016.

58.Self-signed Certificate [online]. Wikipedia. Last modified on 23 December 2015.
URL:https://en.wikipedia.org/wiki/Self-signed_certificate
Accessed 27 February 2016.

59.Microsoft Management Console - Overview [online]. technet.microsoft.com.
URL:https://msdn.microsoft.com/en-us/library/bb742441.aspx
Accessed 13 February 2016.

60.Microsoft Management Console [software]. Microsoft; 2015

61.NAT Traversal [online]. Wikipedia.com. Last modified on 6 January 2016.
URL:https://en.wikipedia.org/wiki/NAT_traversal
Accessed 27 February 2016.