Recommendations for IPv6 addressing plan for the HE sector

Best Practice Document

Produced by UNINETT-led working group
on campus networking
(UFS 137)

Authors: Trond Skjesol, Rune Sydskjør,
Einar Lillebrygfjeld, Gunnar Bøe

March 2013

Document No:	GN3-NA3-T4-UFS137
Version / date:	1.0/2013-03-14
Original language:	Norwegian
Original title:	“Anbefaling for IPv6 addresseplan i høyere utdanning”
Original version / date:	1.0 of 2012-02-09
Contract:	campus@uninett.no

UNINETT bears responsibility for the content of this document. The work has been carried out by a UNINETT-led working group on campus networking as part of a joint-venture project within the HE sector in Norway.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 238875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Executive Summary

Based on best practice in the higher education in Norway, this document gives a to the point recommendation on how you should allocate your IPv6 address space in your campus environment. Emphasis is on simplicity and readability. The plan carefully considers the recommended campus network security architecture. Prefix allocations within the same security zones crossing multiple campuses should facilitate summarized expressions in respective filtering rules. The document recommends static addresses for routers, switches and servers according to a proposed numbering scheme. Clients should rely on DHCPv6. An example IPv6 addressing plan is included.

1. Recommendations for IPv6 address use in the HE sector

Approximately 30 % of Norwegian HE institutions have implemented IPv6 in the course of 2012. For many, it has been a challenge to decide which address plan should be selected for IPv6. Work is in progress in Norway to implement an ICT security architecture and this should be considered in connection with the address plan for IPv6. However, this document can be used even if one is not going to implement a security architecture. An example of an IPv6 address plan has been included in the appendix.

The Dutch research and education network, SURFnet, has created a recommendation for the use of IPv6 addresses. This valuable document, containing extensive treatment of possible options for address plans, has been translated into English and adopted by RIPE. The inherent challenge is in knowing which option is most suitable for the HE sector. An abridged version of the SURFnet document has therefore been created for the HE sector in Norway. Download the complete RIPE version at [RIPE IPv6].

2. Address allocation for zones

The extensive IPv6 address space for subnets makes it possible to be creative in establishing a numbering plan. IPv6 addresses are normally written as hexadecimal numbers and using the VLAN number directly, number for number, in subnet addresses makes it easier to recognise an address and subnet.

[UFS122] provides recommendations for zoning in a network and should be referred to when creating an address plan for IPv6.

If an institution consists of several campuses with separate connections to UNINETT, one /48 prefix will be assigned to each campus or location (for example Haugesund University College has one prefix for Stord and a different one for Haugesund). The same address plan may be used for the subnets at each location. The /48 prefix indicates which campus the address belongs to. The goal is to create simple access control lists (ACLs).

Firewallbuilder [fwbuilder] is an open source product and a good tool to help managing ACLs and firewall rules because it maintains common access lists for IPv4 and IPv6. The basic premise of [UFS122] is that servers with the same security requirements shall be located in the same VLAN. If one re-uses the same VLAN at different campuses without a Layer 2 connection, the campuses must be separated as described above.

At initial deployment of IPv6 it is natural to use a dual stack, but with IPv6 it is no longer necessary to consider the size of the subnets (secondary networks are no longer needed). The same subnet/VLAN is used for IPv4 and IPv6. The RIPE document [RIPE IPv6] specifies the subnet as LLLL-BBBB-BBBB-BBBB;

2001:700:db8:	LLLL-BBBB-BBBB-BBBB	::/64

where “db8” is the element of the address which signifies the campus/location.

Remember that each hexadecimal number consists of four bits. If one does not need to use all four bits (LLLL) in the location/building/area element, it may be of interest to split up the first four-bit element (nibble) into two parts to distinguish, for example, the student network from other networks. Other divisions may also be used. The effect can then be very simple access lists that for example make it possible to block access by all students to special subnets. If one uses “U” to specify the area of use or zone, one can either use ULLL or UULL. It is already common to use low VLAN numbers for those networks which are most secure or best protected. We therefore suggest using U=0 (or UU=00) for the most secure networks and U=F for the most open.

2001:700:db8:	UULL-BBBB-BBBB-BBBB	::/64

As an example, in a single campus the following may be used for two zones:

Use	Bit	Description
UU	00	Secure zone
UU	01	Internal zone
UU	10	Not in use
UU	11	Open zone

The first two bits specify the area of use or zone and here is a more extensive example:

VLAN number	IPv6 network	Description	First Hex number
5	2001:700:db8:0005::/64	Central shared servers / Safe Zone	UULL=0000 ⇒ 0
10	2001:700:db8:4010::/64	Internal servers / Internal Zone	UULL=0100 ⇒ 4
30	2001:700:db8:4030::/64	Printer network / Internal Zone	UULL=0100 ⇒ 4
40	2001:700:db8:8040::/64	Employee network	UULL=1000 ⇒ 8
250	2001:700:db8:C250::/64	Student network / Open Zone	UULL=1100 ⇒ C

Address space in access lists for IPv6 on Cisco equipment can only be specified by means of prefix lengths and not by using random bit masks for matching. This means that it is not possible to use bit masks containing non-consecutive sequences of 0s and 1s.

If, for example, one uses “11LL” to denote users on all student networks, machines may be denied access to the student network using:

```
deny ipv6 2001:700:db8:C000::/50 any ! (UULL = 1100(binary) = C(hex))
```

3. Multiple areas in the same campus (Layer 3 routing)

If one also wishes to use internal location (building) or other structural information, one may use the first number in the subnet address for this purpose and limit VLAN numbering to the range 1-999. Here we have chosen not to take zoning into account.

Use	Bit	Description
UU	00	Central functions
UU	01	Internal servers/services
UU	10	Employees
UU	11	Students

Two bits specify the use and two bits specify the location:

2001:700:db8:	UULL-BBBB-BBBB-BBBB	::/64

Remember that each hexadecimal number consists of four bits. UULL is only the first hexadecimal number.

VLAN number	IPv6 network	Description	First Hex number
5	2001:700:db8:0005::/64	Central shared servers	UULL=0000 ⇒ 0
10	2001:700:db8:5010::/64	Internal servers at Location 1	UULL=0101 ⇒ 5
10	2001:700:db8:6010::/64	Internal servers at Location 2	UULL=0110 ⇒ 6

30	2001:700:db8:5030::/64	Printer network at Location 1	UULL=0101 ⇒ 5
40	2001:700:db8:A040::/64	Employee network at Location 2	UULL=1010 ⇒ A
250	2001:700:db8:D250::/64	Student network at Location 1	UULL=1101 ⇒ D
250	2001:700:db8:E250::/64	Student network at Location 2	UULL=1110 ⇒ E

“db8” is used as an example of the block one has been allocated for one’s location. Here we have assumed that there is only one prefix assigned by UNINETT and that UULL is used internally for area of use and location.

Example of a Cisco IPv6 VLAN configuration is given below. Please not that this configuration is added to the existing IPv4 configuration:

```
interface Vlan10
   description lokal vlan, internal servers at location 1
   ipv6 address 2001:700:db8:0010::1/64
   ipv6 traffic-filter vlan10-out out
```

The concept of “secondary addresses” in IPv4 is no longer used in IPv6, but one may use several IPv6 addresses at the same interface (e.g. when renumbering).

4. Addressing

There are several ways of allocating IPv6 addresses:

- SLAAC, stateless automatic configuration
  The client is then allocated an IPV6 address consisting of an assigned prefix obtained from the router (RA) and the machine element of the address generated from the MAC address (more specifically EUI-64). If the client is to be allocated a name server, a DHCPv6 server which provides DHCPv6 stateless information must be used.

- DHCPv6 stateful
  As for IPv4, this provides both an IPv6 address and other information, but no gateway address is allocated. This is obtained from the router by means of Router Announcement (RA). (Remember the relay agent)

- Static address allocation
  Similar as for IPv4

Various methods should be used for different types of equipment or services. Servers should be set up using fixed or static addresses. We still recommend using `<prefix>::1` as the gateway address, or alternatively Router Announcement (RA) may be used.

Since SLAAC also depends on a DHCPv6 server, we recommend the use of DHCPv6 stateful address allocation (see below). An exception to this may be in the case of large student networks.

4.1 Host addresses for servers and network equipment

Static addresses must be allocated to servers, switches and routers. An example of a static address is:

2001:700:db8:0010::2/64

In the case of servers one should use RA from the router. If one is using HSRPv6 one must use RA or specify the Link Local Address of the HSRP router as static.

4.2 Host addresses for clients

It is recommended to use DHCPv6 for address allocation to clients if one needs information which connects the address to the client. If one combines this with dynamic registration in a DNS reverse look-up, one will achieve a great deal. DHCPv6 must be used under any circumstances to distribute other information needed by clients, such as the DNS server[1], SIP server, NTP server, etc. Because a gateway address is not allocated in DHCPv6, RA from the router must be used to obtain one.

An example of a configuration for this is:

```
ipv6 address 2001:700:db8:0040::1/64
```

[1] DNS server can also be announced by RA if RFC6106 is supported.

Appendix: Example of an IPv6 address plan

This appendix contains an example of an IPv6 address plan based on the principles described in this document. The same address plan can be downloaded in excel format from:

https://openwiki.uninett.no/_media/gigacampus:bpd_ipv6_example_adr_plan_vlan_v2.xls

Three zones are used: Open, Internal and Secure. By using other bit patterns, one may have more zones or different allocations.

Vlan ID	Name of VLAN	Description	#addr.	IPv4	IPv6 2001:db8:3e11::/48	First Hex digit	
Location #0					**Subnet=:UULL<vlan>:**		
Zone Open							
120	DMZ	External reachable servers (DNS, Exchange, VPN, etc.)	64	10.0.122.64/26	2001:db8:3e11:C120::/64	UULL=1100	C
50	eduroam guest	Student's / employee's visitors	64	10.0.123.128/27	2001:db8:3e11:C050::/64	UULL=1100	C
60	Guest network	Other external guests	128	10.0.19.128/25	2001:db8:3e11:C060::/64	UULL=1100	C
70	Student eduroam	Our own students with eduroam access (HiX-student)	512	10.0.248.0/23	2001:db8:3e11:C070::/64	UULL=1100	C
20	Student servers	File server for student's home area	32	10.0.68.0/27	2001:db8:3e11:C020::/64	UULL=1100	C
90	Lab-network	All machines in lab, incl all PC/MAC rooms	256	10.0.126.0/24	2001:db8:3e11:C100::/64	UULL=1100	C
110	Realtime	IP telephony, video conference	256	10.0.16.0/24	2001:db8:3e11:C110::/64	UULL=1100	C
130	Quarantine	Infected machines, or other special reasons	16	10.0.17.0/28	2001:db8:3e11:C130::/64	UULL=1100	C
Zone Internal							
80	eduroam employees	Wireless network for employees (HiX-employee)	256	10.0.251.0/24	2001:db8:3e11:8080::/64	UULL=1000	8
10	Internal servers	Server farm for HiX	64	10.0.122.0/26	2001:db8:3e11:8010::/64	UULL=1000	8
40	Employees network	Vlan for employee's workstations	256	10.0.250.0/24	2001:db8:3e11:8040::/64	UULL=1000	8
30	Print	VLAN for printers og multifunction machines	128	10.0.122.128/25	2001:db8:3e11:8030::/64	UULL=1000	8
150	Sound	VLAN for sound equipment at HiX	128	10.0.123.0/25	2001:db8:3e11:8150::/64	UULL=1000	8
160	Lights	VLAN for light equipment at HiX	128	10.0.123.128/25	2001:db8:3e11:8160::/64	UULL=1000	8
Zone Secure							
5	Personal/HR	Network for HR department	256	10.0.251.0/24	2001:db8:3e11:0005::/64	UULL=0000	0
8	Research	Servers with special research data	64	10.0.122.0/26	2001:db8:3e11:0008::/64	UULL=0000	0
140	Management net	VLAN for switches, monitoring equipment etc	256	10.0.252.0/24	2001:db8:3e11:0140::/64	UULL=0000	0

Alternative with one extra "location" at the same campus: Location #1

Zone Open

120	DMZ	External reachable servers (DNS, Exchange, VPN, etc.)	2001:db8:3e11:D120::/64	UULL=1101	D
50	eduroam guest	Student's/employee's visitors	2001:db8:3e11:D050::/64	UULL=1101	D
60	Guest network	Other external guests	2001:db8:3e11:D060::/64	UULL=1101	D
70	Student eduroam	Our own students with eduroam access (HiX-student)	2001:db8:3e11:D070::/64	UULL=1101	D
20	Student servers	File server for student's home area	2001:db8:3e11:D020::/64	UULL=1101	D
90	Lab-network	All machines in lab, incl all PC/MAC rooms	2001:db8:3e11:D100::/64	UULL=1101	D
110	Realtime	IP telephony, video conference	2001:db8:3e11:D110::/64	UULL=1001	D
130	Quarantine	Infected machines, or other special reasons	2001:db8:3e11:D130::/64	UULL=1101	D

Sone Intern

80	eduroam employees	Wireless network for employees (HiX-employee)	2001:db8:3e11:9080::/64	UULL=1001	9
10	Internal servers	Server farm for HiX	2001:db8:3e11:9010::/64	UULL=1001	9
40	Employees network	Vlan for employee's workstations	2001:db8:3e11:9040::/64	UULL=1001	9
30	Print	VLAN for printers and multifunction machines	2001:db8:3e11:9030::/64	UULL=1001	9
150	Sound	VLAN for sound equipment at HiX	2001:db8:3e11:9150::/64	UULL=1001	9
160	Lights	VLAN for light equipment at HiX	2001:db8:3e11:9160::/64	UULL=1001	9

Zone Internal

140	Management net	VLAN for switches, monitoring equipement etc	2001:db8:3e11:1140::/64	UULL=0001	1

Usage	Bit	Description
UU	00'	Secure zone
UU	01'	Internal zone
UU	10'	Not in use
UU	11'	Open zone

References

[fwbuilder] Firewallbuilder: http://www.fwbuilder.org/

[RIPE IPv6] Preparing an IPv6 Addressing Plan http://www.ripe.net/lir-services/training/material/IPv6-for-LIRs-Training-Course/IPv6_addr_plan4.pdf.

[UFS122] UFS122 Recommended ICT Security Architecture in the HE Sector http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs122.pdf

Glossary

ACL	Access Control List
BPD	Best Practice Document
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name Service
HE	Higher Education
HSRP	Hot Standby Router Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
NTP	Network Time Protocol
RA	Routing Announcement
SIP	Session Initiation Protocol
SLAAC	StateLess Address AutoConfiguration
VLAN	Virtual Local Area Network

Complete BPDs available at www.terena.org/campus-bp/

campus-bp-announcements@terena.org