Computer Science Department

IPv6 Address Plan

October 9, 2018

Goal

With the depletion of IPv4 addresses and the need to move forward to the next generation of the TCP/IP, the department has made the decision to adopt IPv6 as soon as possible.

While there is no pressing internal need for the department to adopt IPv6 due to depletion of IP addresses, we realize that the rest of the world is moving forward to IPv6 due to this depletion on their part. In order to stay well connected and prepared for the pervasive role of IT systems we are adopting a project to incorporate IPv6 in our infrastructure. This document is the start of this project.

This document describes a set of proposed decisions for the adoption of IPv6. It is very possible that these may have to be reconsidered or adjusted in the actual project implementation.

General information about IPv6 is abundantly available at this point but we have used the guidelines in the documents in the references below to formulate this specific address plan.

IPv6

- IPv4 and IPv6 are two technically separate protocols and there is no fundamental intercommunication between them.
- Our UCY allocated address space is 2001:1A18:1::/48
- Access (edge) sub-nets, to which hosts/printers/PC etc are connected, are (typically recommended as) /64 in size (therefore 64 bits of host space). Which means that there are 64 bits in each sub-net for host use. This is more than enough for our purposes (ie 2^{64} = 1.844674407×10^{19} of hosts). Due to this large number in each sub-net/VLAN there is no need for enlarging or splitting any of the sub-nets, a practice very common in IPv4.
- Therefore, there are 16 bits of sub-net space ie 2^{16} or 65536 sub-nets available to the Department which is more than enough for our purposes. It should be noted that theoretically speaking we own an address space of 72 bits which amounts to a provision for 4.722366483×10^{21} hosts!
- The enormous number of available IPv6 addresses allows us to concentrate on organizing the network along convenient concepts (groups, services, automation, security etc) rather than economizing on the address space.

Host Configuration

- The spirit of IPv6 is embraced in full. It provides for auto-configuration of hosts and a “provide a connection when needed” approach. The challenges (see below) that this approach presents will be dealt in the IPv6 spirit not in the old IPv4 methodologies.
- There are four methodologies adopted that hosts can use. These are, from the most recommended to the least recommended:

- EUI-64. Host requests information from its network (address, netmask) from its gateway router using the ICMPv6 protocol and constructs an IPv6 address for itself based on its MAC address. No DHCP server is needed and no statically assigned address.
- RFC-4941. With the support of EUI-64 the host randomly assigns an IPv6 address for itself that is not related to its MAC address. The address is changed regularly or when host is restarted. The address is valid for the network in which the host is located. Provides more security.
- Static configuration. Reserved for server machines or services that need to be registered in the DNS systems (ex web server, mail server etc). With IPv6 static addresses can be assigned to services even if the services are on the same machine.
- DHCPv6. Hosts can use the DHCPv6 services, if needed, to get more information (DNS, PXE etc). Hosts are not required to use it and its use is currently limited.

Private Addresses

- There is no plan to use private addresses. Therefore the NAT (network address translation) methodology will eventually be made obsolete.
- There is no plan to use IPv6 ULAs (Unique Local Addresses).
- Security issues that arise from the above will be dealt in the multilevel security policies that the department has already in place: 1) edge/entry point level, 2) VLAN level and 3) host level.

Address Assignments

As indicated above each VLAN will be assigned a /64 address space. Therefore each entity (server farm, teaching lab, research lab etc) will have a large address space to use.

A preliminary address assignment table is provided in the Appendix. It should be noted that the assignments are not of extreme importance since with IPv6 methodologies hosts will auto-configure themselves in whatever network they find themselves.

IPv4 interoperability

- It is expected that IPv6 and IPv4 co-existence will last for many years.
- In the interim when both IPv6 and IPv4 exist on our networks:
  - the network fundamental services (ex DNS) will provide name resolution in both IPv6 and IPv4
  - hosts will operate in a dual stack mode ie they will have both IPv6 and IPv4 addresses. An IPv6 host will use IPv6 services by priority over IPv4 services falling back to IPv4 when needed. The dual stack will be invisible to users.

- Until the central University network is ready to adopt IPv6 and provide the necessary services to carry IPv6 traffic the department will make use of a tunnel to an IPv6 service provider to access the IPv6 internet. This is very important since the UCY network is not yet ready and in the initial testing phases. The use of tunnels is currently free of charge.

Challenges

- Accountability and trace-ability. Due to international norms but also due to legal obligations, communication on the Department network must be traceable to the machine and individual originating the communication. A system of network authentication needs to be adopted.
- Security. The NAT methodology provided some form of security since hosts with internal IPv4 addresses were hard to discover from the outside networks. IPv6 addresses will be public and therefore directly reachable from the outside.
- Security. A network access control system is recommended to both allow for accountability but also to protect networks from intentional or unintentional access.
- Security. The existing Departmental security model should be expanded to incorporate a more elaborate and multilevel security policy. This is essential in the IPv6 world.

Possible solutions

- Adoption of 802.1x with user and/or machine authentication
- Adopting MAC authentication/fixing for machines that do not support 802.1.x

References

- [RFC7381] – Enterprise IPv6 Deployment Guidelines
- Recommendations for IPv6 addressing plan for the HE sector (GEANT)
- IPv6 at Cambridge
- Preparing an IPv6 address plan (SURFNET)

Appendix – Address Assignments

Network	VLAN ID.	IPv6 assignment 2001:1A18:0001:00xx/64	Comment
Infrastructure Systems 1		**0X**	
Point-to-Point and other network infrastructure connections	N/A	00	/127
Server Farm-1		01	
Server Farm-2		02	
Server Farm-3 (reserved)		03	
Server Farm-4 (reserved)		04	
Server Farm-5 (reserved)		05	
DMZ1		06	
DMZ2		07	
rDMZ1		08	
rDMZ2 (reserved)		09	
Wireless		0A	
VPN1		0B	
VPN2		0C	
iSCSI		0D	
Reserved		0E	
Reserved		0F	

Appendix – Address Assignments

Network	VLAN ID.	IPv6 assignment 2001:1A18:0001:00xx/64	Comment
Infrastructure Systems 2		**1x**	
Openstack 1		10	External
Openstack 2		11	PXE
Openstack 3		12	Storage
Openstack 4		13	Reserved
Openstack 5		14	Reserved
Reserved		15-19	
Testing Networks		1A-1E	
Management Network		1F	
User Access Systems		**2x**	
Faculty and Staff		20	
Printers and Office machines		21	
User access Testing		22	
Reserved		23	
Teaching Labs			

Appendix – Address Assignments

Network	VLAN ID.	IPv6 assignment 2001:1A18:0001:00xx/64	Comment
Linux Lab I (B103)		24	
Linux Lab II (103)		25	
Windows Lab I (B121)		26	
Windows Lab II (123)		27	
Digital Lab (101)		28	
Graduate Lab (201)		29	
Walk-in Lab		2A	
Reserved		2B-2F	
Research Labs		**3x**	
Computational Intelligence and Neuroscience research group (CIN)		30	
Computer Architecture System Performance Evaluation Research (CASPER)		31	
Ξ - Computer Architecture Research Group (Ξ - CARCH)		32	
Computer Graphics and Virtual		33	

Appendix – Address Assignments

Network	VLAN ID.	IPv6 assignment 2001:1A18:0001:00xx/64	Comment
Reality Research Laboratory			
Data Management in Mobile and Adaptive Computing (DMAC)		34	
Data Management Systems Laboratory (DMSL)		35	
E-Health Laboratory		36	
Laboratory for Internet Computing		37	
Networks Research Laboratory (NetRL)		38	
Research Laboratory for Foundations of Computing Systems and Theoretical Computer Science		39	
Software Engineering and Internet Technologies (SEIT) Laboratory		3A	
Reserved		3B-3F	

Appendix – Address Assignments

Network	VLAN ID.	IPv6 assignment 2001:1A18:0001:00xx/64	Comment
Research Systems (clusters or groups)		**4x**	
Departmental general clusters and small lab clusters		40	
GRID		41	
LINC		42	
Reserved		43-4F	