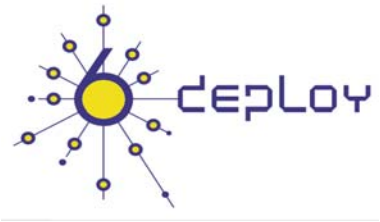





Title:	Document Version:
Deliverable D2.2.1 **Initial status of the available exercises to be used with the Lab equipment**	1.0

Project Number:	Project Acronym:	Project Title:
261584	6DEPLOY-2	IPv6 Deployment Support

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
28/02/2011	17/02/2012	R – PU

* Type: P – Prototype, R – Report, D – Demonstrator, O – Other

** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission Services), RE – Restricted to a group defined by the consortium (including the Commission Services), CO – Confidential, only for members of the consortium (including the Commission Services)

Responsible and Editor / Author:	Organization:	Contributing WP:
Simon Muyal	RENATER	WP2

Authors (organizations):

Simon Muyal (RENATER), Martin Potts (Martel)

Abstract:

This deliverable represents a summary of the hands-on exercises to be used with the IPv6 Lab equipment at the start of the 6DEPLOY-2 project.

Keywords:

ACL, Address, BGPv4, DHCP, DNS, FTP, IPv6, Linux, Management, OSPFv3, Routers, Security, Web, Windows.

Disclaimer

Executive Summary

One of the main activities in the 6DEPLOY-2 project is to produce and maintain a set of dissemination material for use in workshops to train the different Internet communities in the areas of IPv6 deployment, configuration, and usage. This material is partly produced within 6DEPLOY-2, but also exploits previous project activities within and outside the Framework Programmes of the European Commission.

This document describes the available set of hands-on exercises used with the IPv6 Lab equipment, either during the 6DEPLOY-2 workshops or by the Lab hosting organisation during their own training courses.

These hands-on exercises are always appreciated by the course participants and the remark is often given in the feedback forms that more such exercises would have been welcome.

Table of Contents

1. INTRODUCTION:

Workshops are one of the main mechanisms used by 6DEPLOY-2 to transfer information and to build collaboration. Each workshop is composed of a set of several theoretical presentations about aspects of the IPv6 protocol and also of practical hands-on exercises.

This document describes the different practical exercises modules which cover from the host operating system configuration to the end-to-end IPv6 connectivity (Routing, DNS, DHCP, services/applications, management and security).

Cisco has decided to install the same hardware and software in all the 6DEPLOY-2 IPv6 Labs, even renewing the “old” equipment in the already operational Labs in Paris, Sofia and Mauritius). This operation started in January 2011.

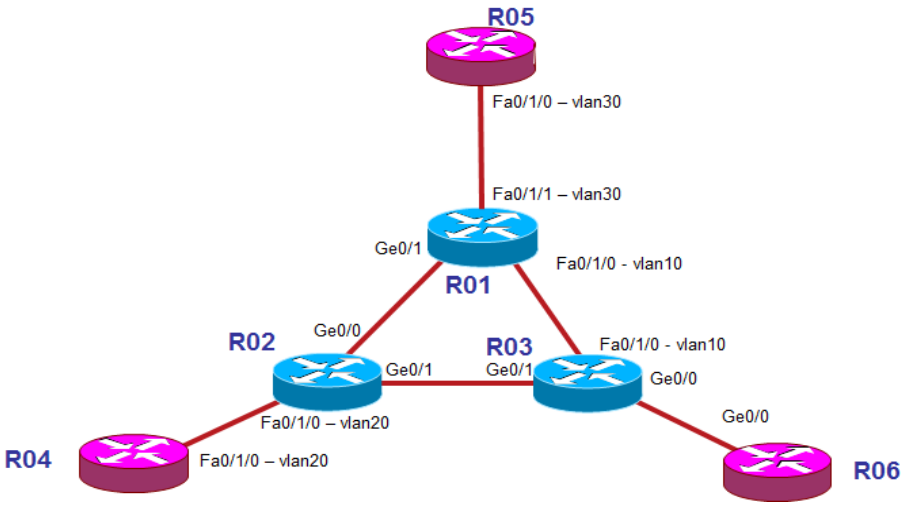
The Lab topology is therefore now standardized and documented.

This consistency allows 6DEPLOY-2 to have:

- Standard Lab documentation and exercises
- Easier roll out of new Labs
- Easier roll out of new Lab exercises
- A Lab “cloud” concept (usage of multiple Labs for a single workshop)

2. STANDARD LAB TOPOLOGY DESCRIPTION

The standard Lab topology is composed of 6 routers (Cisco 1941) interconnected together as depicted in the topology below.



Each router runs in dual stack mode and is configured with static IPv4 and IPv6 standard Lab address ranges. Each Lab location has its own reserved IP static ranges.

The router naming convention is the following:

organisation_name-r0x where x = 1 to 6

Router #	Router Hostname	RENATER Example
Router1	organisation_name-r01	renater-r01
Router2	organisation_name-r01	renater-r02
Router3	organisation_name-r01	renater-r03
Router4	organisation_name-r01	renater-r04
Router5	organisation_name-r01	renater-r05
Router6	organisation_name-r01	renater-r06

Each Lab is also equipped with a terminal server router (Cisco 2911) that connects to the console port of each of the six routers using serial connection (out of band). The out of band connection is used to access the routers by telnet to a specific port on the terminal server.

End-devices such as student PC clients, DNS server, DHCP server, Web server, Wireshark, management applications, etc. are connected to the Lab routers via Fast Ethernet interfaces. These end-devices are used during the hands-on exercises and will be described later on in this document.

3. HANDS-ON MODULES SUMMARY

This section provides a list - and a short description - of the available hands-on modules.

The following hands-on exercises were developed originally within the 6DISS project and used extensively within 6DEPLOY:

- **Host configuration**: Two exercises illustrate how IPv6 works on Linux and Windows XP operating systems. The main focus is on IPv6 addressing (activation, configuration, connectivity check ...)
- **Stateful auto-configuration**: In this exercise, the trainees are requested to install a DHCPv6 client (Dibbler) and make a basic configuration.
- **Routing**: In this exercise, IPv6 routing protocols are configured by the trainees on the testbed routers. Internal Gateway Protocols (OSPF) and the External Gateway Protocol (BGP) are tested.
- **DNS**: In this exercise, the trainees have to manipulate IPv6 resource records (AAAA, PTR) of a DNS server. It is performed on Linux OS.
- **Services/Applications**: In this exercise, the trainees install IPv6 services such as web servers and FTP servers. This exercise is performed on Linux OS. The other trainees check that the configured services are available from their machine using IPv6 web/ftp clients (on Linux or Windows).
- **Management**: After having tested the services, the trainees are requested to install a management application (Argus) to supervise the routers, PCs and configured IPv6 services (web, ftp, etc.).
- **Security**: In this exercise, the trainees are required to add filters on the routers (ACL) and on the PCs (ip6tables) to allow/deny some PCs/services.

A further set of hands-on exercises was contributed to 6DEPLOY by Consulintel:

- IPv6 setup for several operating systems (Win2K/XP/2003/Vista and Linux)
- Basic Configuration, stateless/Stateful Autoconfiguration, Privacy, Static routes.
- Transition Mechanisms Configuration[1]
- Examples of applications
- IPv6 DNS

[1] [1] *In this hands-on exercise configuration of different transition mechanisms examples are given for different platforms, such as Linux and Windows. The main focus is on tunnelling mechanisms.*

- IPv6 and PPP
- Firewall IPv6
- IPv6 on Cisco routers and IPv6 ACLs
- SNMP over IPv6

The full set (see list below) is available at:
http://www.6deploy.org/index.php?page=hands-on

4. HANDS-ON MODULES DESCRIPTIONS

This section provides a description of the available hands-on modules.

4.1 Host Configuration

Objectives

- To activate and configure IPv6 on hosts running Windows XP and/or Linux
- To understand the basic IPv6 concepts
- To manually add/remove IPv6 addresses and display IPv6 information

Exercise description

The exercise consists of installing and modifying IPv6 addresses on Windows XP and/or Linux hosts.

Windows XP host:

- Enable IPv6
- Display and identify existing IPv6 addresses
- Usage of IPv6 related tools (ping, netsh ...)
- Add/remove IPv6 addresses
- Netsh command line utility usage/description

Linux host:

- Verify IPv6 support in your Linux version
- Display and identify existing IPv6 addresses
- Usage of IPv6 related tools (ping, ifconfig ...)
- Add/remove IPv6 addresses
- Analyse IPv6 message using tcpdump and route commands
- Usage of the IPv6 tcpdump tool utility
- Set variables and values in the kernel virtual file system

4.2 Stateful Auto-configuration

Objectives

- To configure DHCPv6 clients
- To get experience of both auto-configuration methods (stateless and stateful)

Exercise description

The exercise consists of configuring a Linux client to obtain a global IPv6 address from a DHCPv6 server (Dibbler) on the same VLAN.

With a protocol analyser (Wireshark), the trainees will capture and analyse the DHCPv6 messages to understand the way DHCPv6 is working.

Two scenarios are used:

- DHCPv6 with Router Advertisement messages (stateless)
- DHCPv6 without Router Advertisement messages (stateful)

4.3 Routing

Objectives

- To get experience in configuring IPv6 routing on Cisco routers

Exercise description

The routing exercise is composed of two sub-modules:

- Lab configuration:
    - Configure IPv6 interface addresses according to a provided table
    - Configure OSPFv3 on all the routers in a single area
    - Check IPv6 routing table and connectivity
    - Configure IPV6 eBGP and iBGP
    - Check IPv6 routing table and connectivity
- Cisco router configuration and command summary
    - Contains a short summary of the Cisco configuration commands and the outputs of *show* commands
    - Summary of the CLI commands to configure Cisco routers
    - List of commands to configure IPv6 routing (Static, OSPF, BGP, Access-lists) and a list of the show commands

4.4 DNS

Objectives

- To configure a DNS server for IPv6
- To create a *forward zone* and insert IPv6 related records
- To make A and AAAA queries to the server

Exercise description

The exercise consists of host addresses being assigned by DHCP.

A DHCP server (BIND 9.3) is running on a Linux (Ubuntu) laptop.

Trainees are requested to:

- Create an IPv6 *forward zone* (AAAA) file and insert IPv6 records
- Create an IPv6 reverse record (PTR) in a *reverse zone*

The trainees should validate the DNS queries by using their Lab PC.

The module also contains an example of a configuration file for DNS.

4.5 Services / Applications

Objectives

- To configure and run an IPv6 Web server and an FTP server
- To test services with IPv6 clients (web, ssh, ftp)

Exercise description

The exercise consists of configuring a server with some services. A workstation is then used to ensure the services are running properly.

Trainees should first configure their Server Operating System with a pre-defined IPv6 address and update the DNS server accordingly.

a) Server configuration

- Configure and launch a Web server (Apache2)
  - Install the Apache2 Web server to listen to both IPv4 and IPv6
  - Launch the Apache2 Web server
- Configure and launch an FTP server
  - Install a compliant IPv6 FTP server (Proftpd).
  - Launch the FTP server

b) Client configuration

- Install a Web browser supporting IPv6 (FireFox)
- Check that you can reach the Web Server using IPv6 and analyse the packet flow with Wireshark
- Install and test the FTP client (FileZilla)
- Enable IPv6 on FileZilla
- Check that you can reach the FTP server and analyse the packet flow with Wireshark

4.6 Management Tools

Objectives

- To monitor the routers, PCs and services (Web, FTP)
- To install monitoring tools

Exercise description

The exercise consists of installing and using monitoring tools.

- Install/configure a tool (Argus) to manage the routers, PCs and services (Web, FTP)
- Use the tool to monitor the routers, PCs and services
- Test additional monitoring tools, such as AS-Path-Tree, Looking-Glass ...

The exercise also contains an example of a configuration file for Argus.

4.7 Security

Objectives

- To secure the servers
- To secure the network

Exercise description

The exercise consists of securing:

- The servers, by configuring the ip6tables file to allow/deny some PCs/services
- The routers, by configuring Access Control Lists (ACLs) to allow/deny some PCs/services.

The module contains in the Appendix examples of:

- An ip6tables example file for a Linux machine
- Access Control Lists example for a Cisco router

4.8 Hands-on exercises from Consulintel

There is also a further set of 9 hands-on exercises written by Consulintel which complement the original exercises from the 6DISS project. These exercises are:

- IPv6 setup for several operating systems (Win2K/XP/2003/Vista, Linux)
- Basic Configuration, stateless/Stateful Autoconfiguration, Privacy, Static routes
- Transition Mechanisms Configuration
- Examples of applications
- IPv6 DNS
- IPv6 and PPP
- Firewall IPv6
- IPv6 on Cisco routers and IPv6 ACLs
- SNMP over IPv6

The set of Consulintel exercises is called "IPv6 Startup" and is composed of 164 pages of different practical exercises which can be used on the standard Lab topology.

These exercises are described in the following subsections 4.8.1 - 4.8.9:

4.8.1 IPv6 setup for several operating systems (Win2K/XP/2003/Vista, Linux)

This exercise explains how to enable and setup IPv6 on:

- Win2K/XP/2003/Vista
- Linux (Red Hat, SUSE, Ubuntu and BSD)

4.8.2 Basic Configuration, stateless/Stateful Autoconfiguration, Privacy, Static routes

This exercise includes:

- The basic configuration command descriptions for Win2K/XP/2003/Vista and Linux, such as:
    - IPv6 specific commands

- Troubleshooting commands
- Adding/Deleting/Showing static routes
- Tunnel configuration

- A set of exercises for Autoconfiguration (Stateless + Stateful with a DHCP server)
- Descriptions of address Privacy Extensions for Stateless Autoconfiguration

4.8.3 Transition Mechanisms Configuration

This exercise explains how to configure of a set of Transitions Mechanisms on WinXP/2003, Linux and BSD. It includes:

- Setting up a 6in4 tunnel between two hosts
- The deletion of a 6in4 tunnel
- Setting up IPv6 connectivity via a Tunnel Broker
- Setting up IPv6 connectivity with a 6to4 tunnel
- Setting Up a 6to4 Relay with Win2003
- Setting up a Teredo Client
- The use of IPv4/IPv6 Proxies

4.8.4 Examples of applications

This exercise shows some IPv6 applications such as DNS lookups, Putty, Wireshark, VLC media player (multimedia), Microsoft Windows Media Player and Server, ISABEL (collaboration tool), BitTorrent (File Sharing), VNC (remote control SW), Web servers (Apache2, IIS 6+), Web browsers (Firefox, IE, Safari ...), FreeBSD.

There are also some specific exercises with these applications.

4.8.5 IPv6 DNS

This exercise includes the installation, configuration and testing of BIND DNS with the Linux Operating System, and the configuration and testing of DNS IPv6 with Windows 2003.

4.8.6 IPv6 and PPP

This exercise explains PPP implementation with Windows/Linux/Unix. It includes an

example of configuring pppd and the use of pppd in RASs and VPNs.

4.8.7 Firewall IPv6

This exercise shows how to set up IPv6 Firewalls on XP/2003 and Linux.

4.8.8 IPv6 on Cisco routers and IPv6 ACLs

This exercise shows examples of CLI configuration on Cisco routers to:

- Enable Telnet over IPv6 transport
- Enable SSH over IPv6 transport
- Enable IPv6 on an interface
- Show IPv6 information
- Configure a 6in4 tunnel
- Filter IPv6 traffic with an Access Control List (ACL)
- Create an ACL and show its functionality through an example with an application on an interface

4.8.9 SNMP over IPv6

This exercise explains how to configure SNMP over IPv6 on Cisco routers.

There is also an exercise to check with SNMP the IPv6 traffic on interfaces using a graphical tool like MRTG.

5. CONCLUSIONS

This document has described the available set of hands-on exercises used with the IPv6 Lab equipment, either during the 6DEPLOY-2 workshops or by the Lab hosting organisation during their own training courses.

These practical hands-on exercises are an essential aspect of learning new technologies since they illustrate and complement the theoretical modules presentations.

The practical exercises modules cover a range of installation and configuration procedures from the host operating system (Win2K/XP/2003/Vista, Linux …), through end-to-end IPv6 connectivity, up to applications and services.

We are developing new standard hands-on exercises for IPv6 Transitioning Mechanisms.