Title: **Deliverable D2.2.2** **Update of the available exercises to be used with the Lab equipment**	**Document Version:** 1.0

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

Contractual Delivery Date: 28/02/2011	**Actual Delivery Date:** 22/02/2012	**Deliverable Type* - Security**:** 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: Simon Muyal/Bernard Tuy	**Organization:** RENATER	**Contributing WP:** WP2

Authors (organizations):

Simon Muyal (RENATER), Bernard Tuy (RENATER)

Abstract:

This deliverable represents an update of the hands-on exercises described in D2.2.1 to be used with the IPv6 Lab equipment from the beginning of 6DEPLOY-2 project and the new possibilities offered by the deployment of virtual machines on the labs.

Keywords:

ACL, Addressing, BGPv4, DHCP, DNS, FTP, IPv6, Linux, Management, OSPFv3, Routers, Security, ToIP, Virtual Machines, Web, Windows.

Disclaimer

The 6DEPLOY-2 project number 261584 is co-funded by the European Commission under Framework Programme 7. This document contains material, which is the copyright of certain 6DEPLOY-2 beneficiaries and the EC, and may not be reproduced or copied without permission. The information herein does not necessarily express the opinion of the EC. The EC is not responsible for any use that might be made of data appearing herein. The 6DEPLOY-2 beneficiaries do not warrant that the information contained herein is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using this information.

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.

Some material was already available from previous project activities. Some work has been done from the beginning of the project to extend this material: Since IPv6 deployment in the different sectors of activities is speeding up, 6DEPLOY-2 partners have felt the need to propose new hands-on topics to the IPv6 workshop attendees. The effort was focused mainly on transition mechanisms, voice and video services and new exercises based on virtual machines. Before writing these new exercises, it was necessary to adapt lab infrastructure. New servers have been deployed in some labs to be able to host virtual machines. A SIP based Telephony over IP (ToIP) call manager was also installed in RENATER lab.

This document summarises the available set of possibilities trainers can use with the IPv6 Labs installed on the different continents around the globe, either during the 6DEPLOY-2 workshops or by the Lab hosting organisation during their own training courses.

Table of Contents

Table of Figures

1. INTRODUCTION:

Workshops are one of the main mechanisms used by 6DEPLOY-2 to transfer information and know-how 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 and provided a much better way to use these resources.

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)

To start creating this large 6DEPLOY lab cloud, it has been decided to split the labs into three category types:

- IPv6 **standard lab** sites which together constitute the **6DEPLOY lab cloud**
- **Potential** (or near future) IPv6 **standard lab** sites
- **Regional** IPv6 labs

2. STANDARD LAB TOPOLOGY DESCRIPTION

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

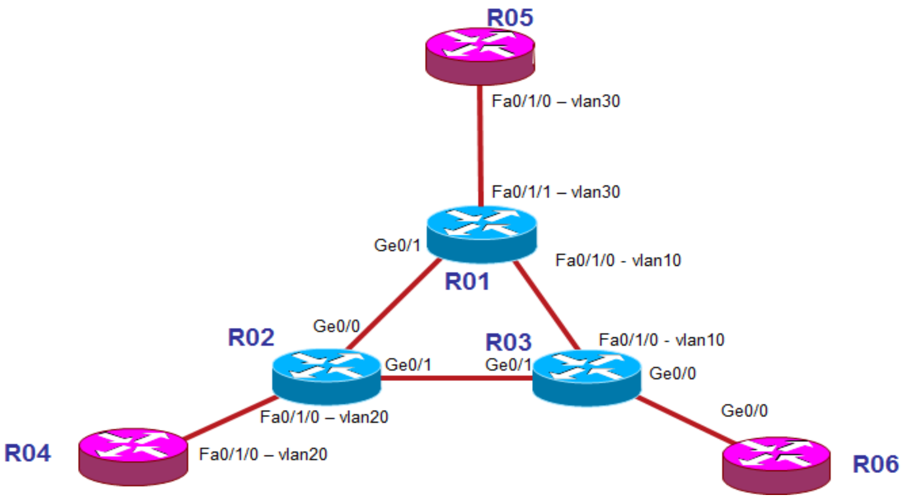


Figure 2-1: Standard lab topology

Each router runs in dual stack mode and is configured with static IPv4 and IPv6 standard Lab address 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
…		
Router6	organisation_name-r01	renater-r06

VLANs numbering:

Where Switched Virtual Interfaces (SVIs) are used, they use a numbering scheme made up of the two devices that the SVI connects, lowest first then highest. Specifically, this means:

- Vlan 14 connects R01 to R04
- Vlan 25 connects R02 to R05
- Vlan 36 connects R03 to 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 a serial connection (out-of-band). This out-of-band connection is used to access the routers by telnet to a specific port on the terminal server.

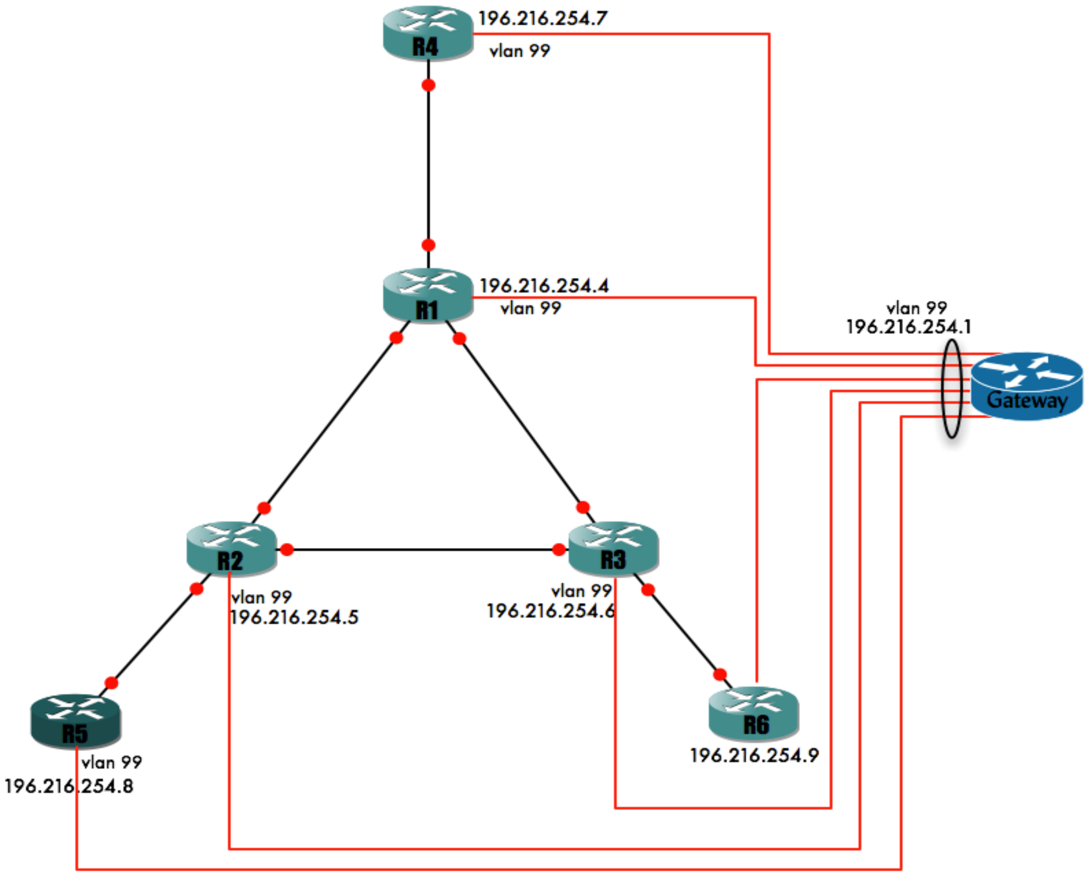


Figure 2-2: Out-of-band connection: AfriNIC example

In order to connect to the lab routers devices such as DNS server, DHCP server, Web server, Wireshark or management application hosts, dedicated hardware hosting virtual machines has been deployed in some labs. It is easier now to organise workshops as a trainer does not need to prepare previously the configurations on local machines. The Virtual Machine infrastructure is 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 …). Note that the routers are provided with IPv4 configuration only, since the trainees have to configure the IPv6 part.
- **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, the trainees on the test bed routers configure IPv6 routing protocols. 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) on 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. Every trainee checks that the configured services by the other trainees are available from his/her machine using IPv6 web/ftp clients (running either Linux or Windows).
- **Management**: After having tested the services, the trainees are requested to install a management application (Argus) to supervise the routers, hosts 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 Linux hosts (ip6tables) to allow/deny some machines/services.

Consulintel contributed a further set of hands-on exercises to 6DEPLOY:

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

- Examples of applications
- IPv6 DNS
- IPv6 and PPP
- Firewalling with IPv6
- IPv6 on Cisco routers and IPv6 ACLs
- SNMP over IPv6 (transport and MIBs)

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 configuring 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 on 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 protocols 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 adding a record for 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 a 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 install monitoring tools
- To monitor the routers, hosts and services (Web, FTP)

Exercise description

The exercise consists of installing and using monitoring tools.

- Install/configure a tool (Argus) to manage the routers, hosts and services (Web, FTP)
- Use the tool to monitor the routers, hosts 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 machines/services
- The routers, by configuring Access Control Lists (ACLs) to allow/deny some machines/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 (see the list in section 3).

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 running machines. It includes:

- Setting up/ Deleting a 6in4 tunnel between two hosts

- 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 …).

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 Firewalling with 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:

- Enabling *Telnet* over IPv6 transport
- Enabling *ssh* over IPv6 transport
- Enabling IPv6 on an interface
- Showing IPv6 information
- Configuring a 6in4 tunnel

- Filtering IPv6 traffic with an Access Control List (ACL)
- Creating 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. LAB INFRASTRUCTURE EVOLUTION

A set of enhancements has been implemented during recent months in order to offer new hands-on material opportunities.

5.1 Virtual Machines

Cisco is providing 2 servers on each lab that belongs to the 6DEPLOY lab cloud. The deployment of these servers is in progress. The goal is to create Virtual Machines (VMs) connected to the set of routers in a given IPv6 lab. These VMs will help in setting up new hands-on activities for the trainees (e.g. IPv6 multicasting or IPv6 flow monitoring).

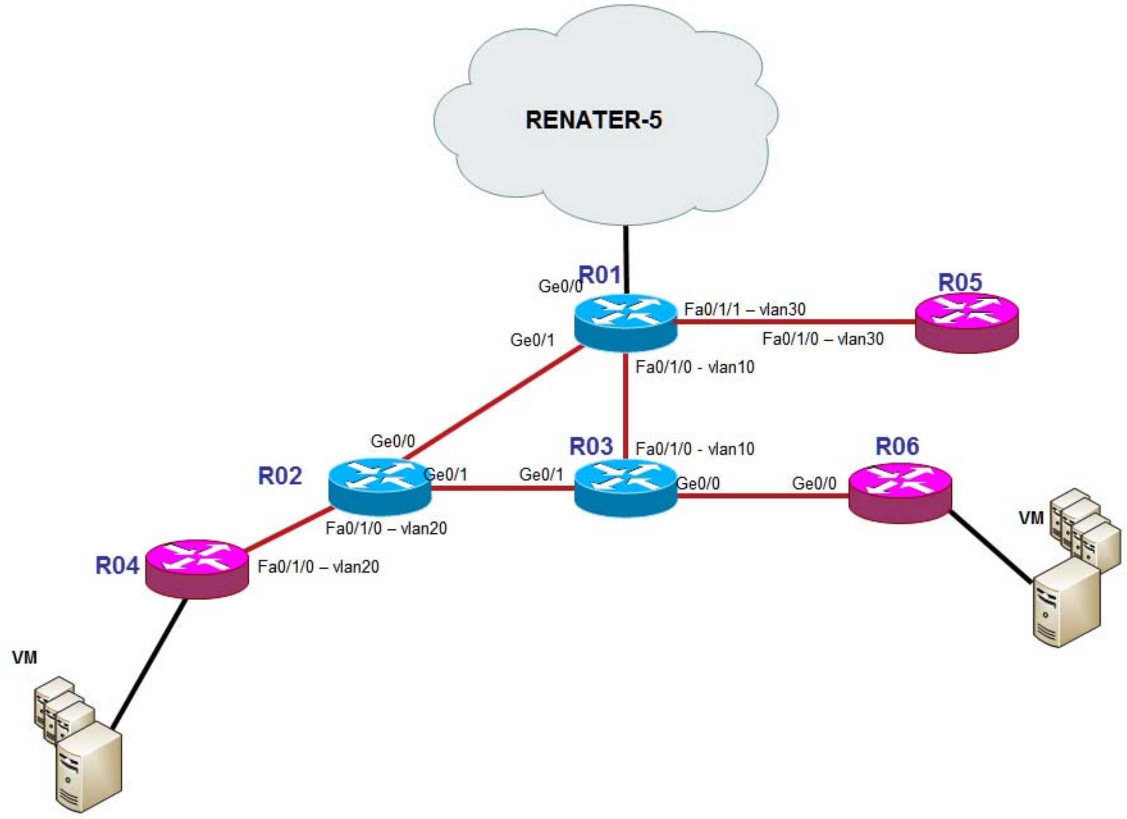
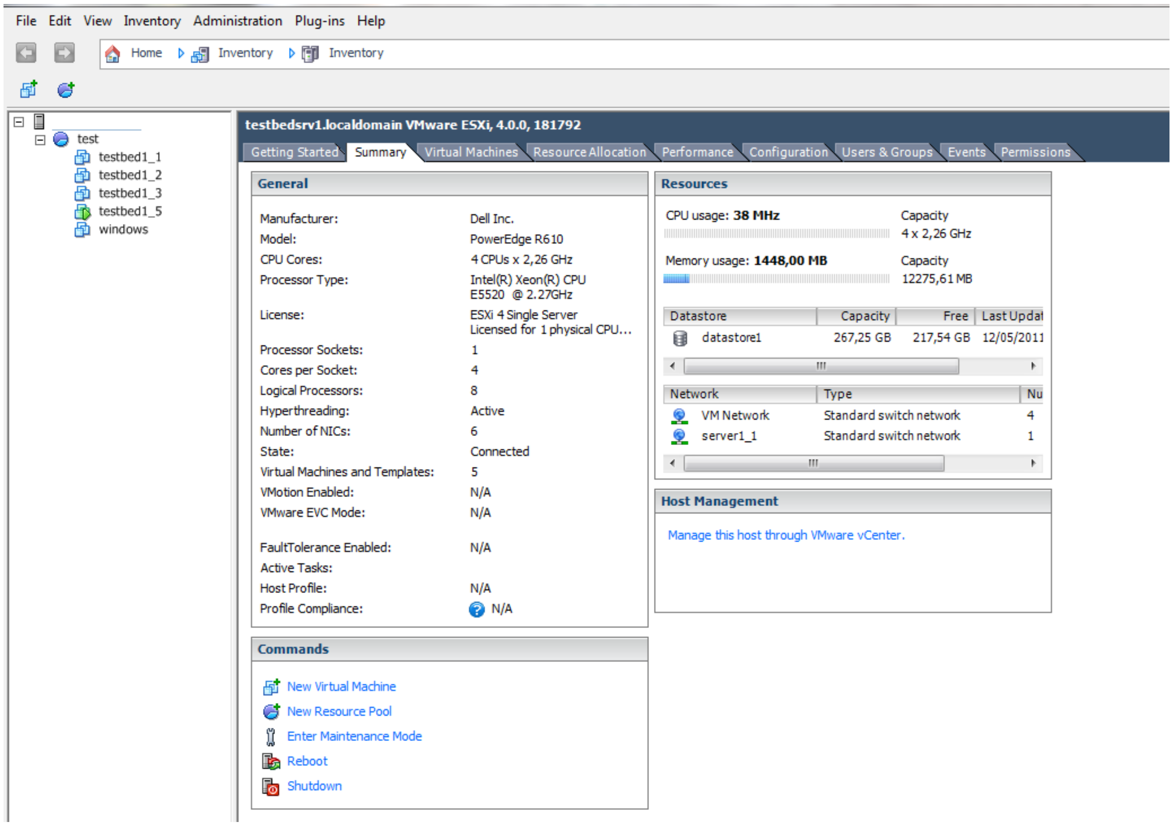


Figure 5-1: RENATER lab with VM servers deployed

Alternately each VM could serve as a terminal for a trainee. In this way, no previous installation is needed on local computers. This would reduce to a minimum the effort of preparation and configuration for a trainer, since each piece of equipment could be configured beforehand.

The software used to offer the VM infrastructure is ESXI 4.0. With this software, we can easily deploy a new VM or replicate an existing one.



testbedsrv1.localdomain VMware ESXi, 4.0.0, 181792

General

Manufacturer: Dell Inc.
Model: PowerEdge R610
CPU Cores: 4 CPUs x 2,26 GHz
Processor Type: Intel(R) Xeon(R) CPU E5520 @ 2.27GHz
License: ESXi 4 Single Server Licensed for 1 physical CPU...
Processor Sockets: 1
Cores per Socket: 4
Logical Processors: 8
Hyperthreading: Active
Number of NICs: 6
State: Connected
Virtual Machines and Templates: 5
VMotion Enabled: N/A
VMware EVC Mode: N/A
FaultTolerance Enabled: N/A
Active Tasks:
Host Profile: N/A
Profile Compliance: N/A

Resources

CPU usage: **38 MHz** Capacity 4 x 2,26 GHz
Memory usage: **1448,00 MB** Capacity 12275,61 MB

Datastore	Capacity	Free	Last Updat
datastore1	267,25 GB	217,54 GB	12/05/2011

Network	Type	Nu
VM Network	Standard switch network	4
server1_1	Standard switch network	1

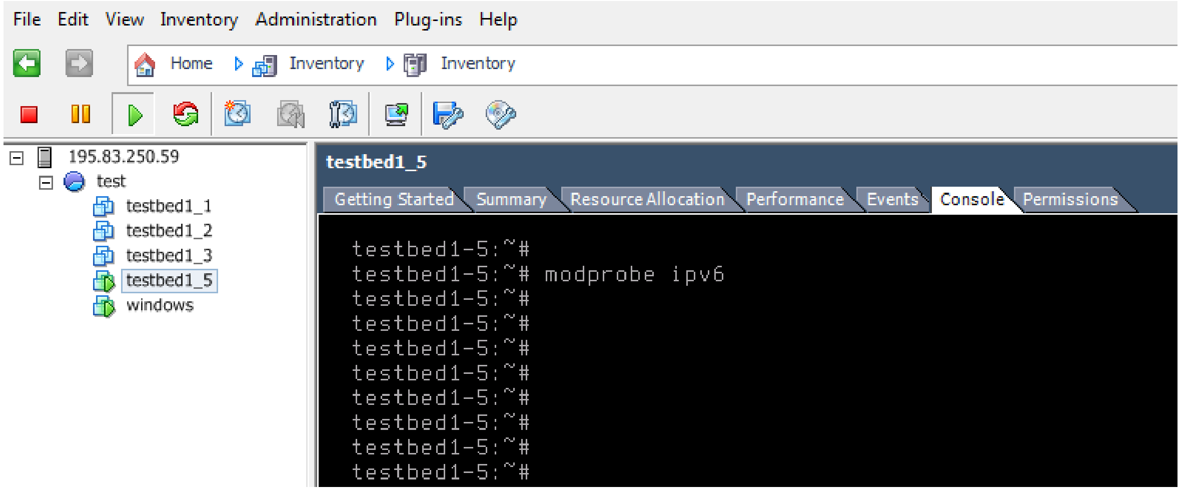
Host Management

Manage this host through VMware vCenter.

Commands

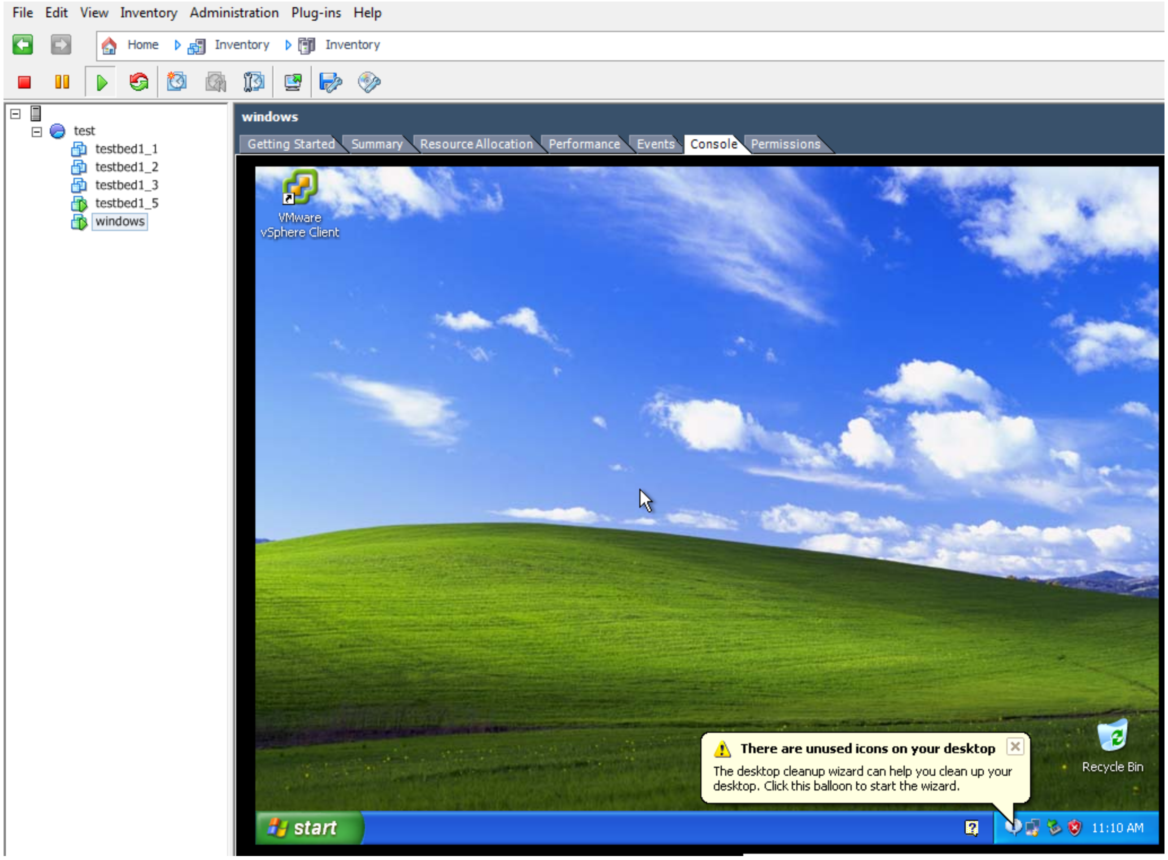
Figure 5-2: VM management: ESXI4.0 interface

It is possible to run Linux and Windows Operating Systems on each VM, and each server can host up to 6 VMs. In this way, 24 trainees can use a single lab if we consider there are 2 trainees per VM.



```
testbed1-5:~#
testbed1-5:~# modprobe ipv6
testbed1-5:~#
testbed1-5:~#
testbed1-5:~#
testbed1-5:~#
testbed1-5:~#
testbed1-5:~#
testbed1-5:~#
testbed1-5:~#
```

Figure 5-3: VM running Linux OS



There are unused icons on your desktop

The desktop cleanup wizard can help you clean up your desktop. Click this balloon to start the wizard.

Figure 5-4: VM running Windows OS

Once the deployment on the servers is finished, it will be possible to adapt and create new hand-on exercises to run on the VM infrastructure. This will be done in the second quarter of 2012.

5.2 Voice and video infrastructure

5.2.1 Call manager and IP phones

In order to investigate another important area: Telephony over IPv6 (ToIPv6), Cisco has started to provide two IP phones to each lab and a call manager (CUCM) was installed in RENATER's lab premises.

The goal is to use this new CUCM and UCL's CUCM to connect IP phones installed in all the standard lab locations. Therefore, lab managers - and later on trainees - will be able to perform telephone calls over IPv6 using the new signalling protocol, SIP.

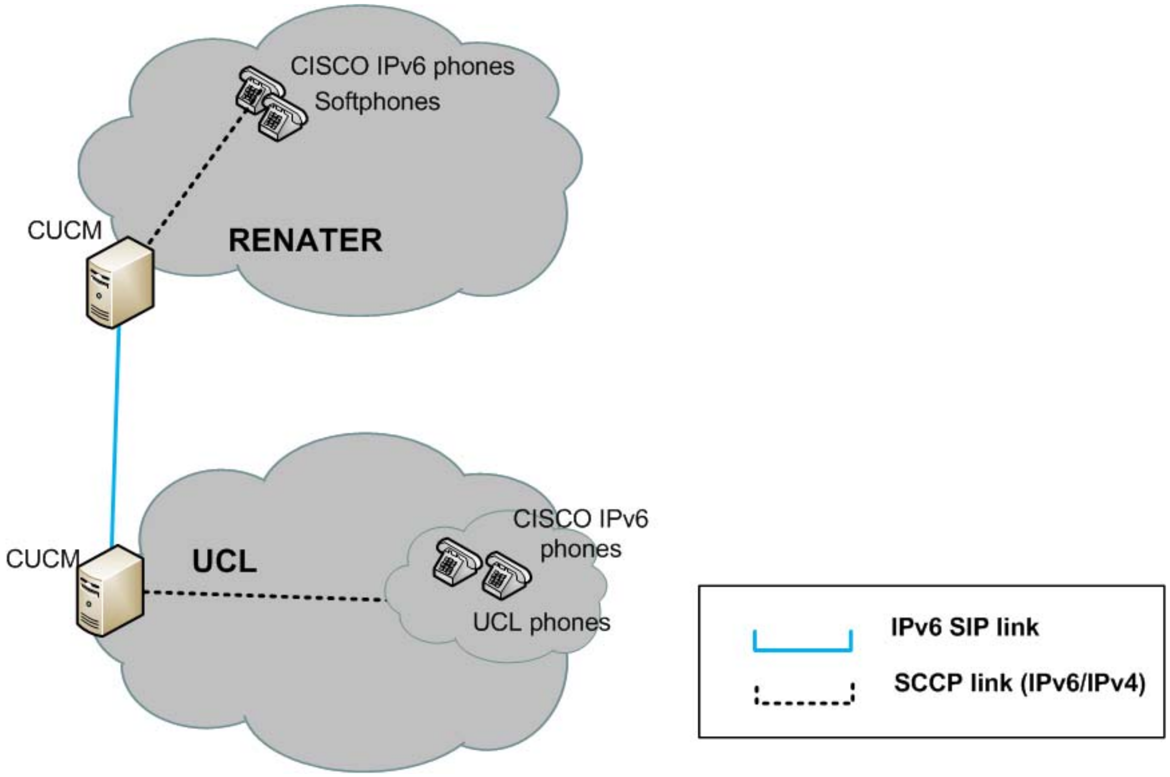


Figure 5-5: Call manager and IP phones

With this infrastructure, we can also imagine hands-on exercises where softphones running on VM infrastructure can be attached to CUCMs.

5.2.2 IPv6 cameras

To promote video services, Cisco has started to provide one IPv6 camera per lab. These cameras are directly connected to the lab or in the partner's offices when there is no possibility to have a camera in the datacentre hosting the lab.

These cameras are reachable over IPv6 Internet. It is a good application to show during a training session how this standard service can be reached using IPv6.

6. TRANSITION MECHANISMS

At the beginning of the 6DEPLOY-2 project, we considered there was a lack of transition mechanism hand-on exercises. Therefore, we took the decision to create exercises to cover this important topic. The first step was to decide which transition mechanisms have to be taken into account. The list of transitions scenarios analysed were:

- 6to4 and 6RD
- TEREDO and ISATAP
- 6PE or 6VPE

Considering the possibilities of the Cisco platforms installed in the standard labs and the advantages of each mechanism, we decided in the General Assembly meeting in Madrid (July 2011) to write scenarios for 6RD and 6PE/6VPE. We also decided to use the VM infrastructure to run some scenarios based on tunnelling mechanisms.

The different architectures have been defined in the document available on the wiki page: http://wiki.6deploy.eu/uploads/TBManagers/TransMechs_Labs.pdf (Note, however, that the lab topology has changed from the Madrid meeting)

7. CONCLUSIONS

This document has described the available set of hands-on exercises used with the IPv6 Lab equipment (routers and Virtual Machines), 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.

With the new infrastructure deployed, standard hands-on exercises for transitioning mechanisms and voice/video topics will be ready in the next months.