Application Session (Hands-on)

Athanassios Liakopoulos (GRNET)
aliako@grnet.gr

version 1.01
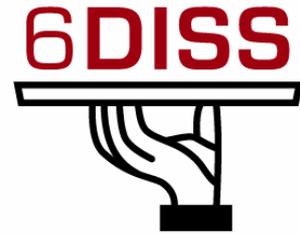
1. Lab information

Network Topology

The network topology is shown in Figure 1. PCs belong to different VLANs, each of them having a different IPv6 address prefix. For example, the first three PCs in the 2nd row belong in the VLAN 3 and use the 2001:w:z:3::/64[1] address space.
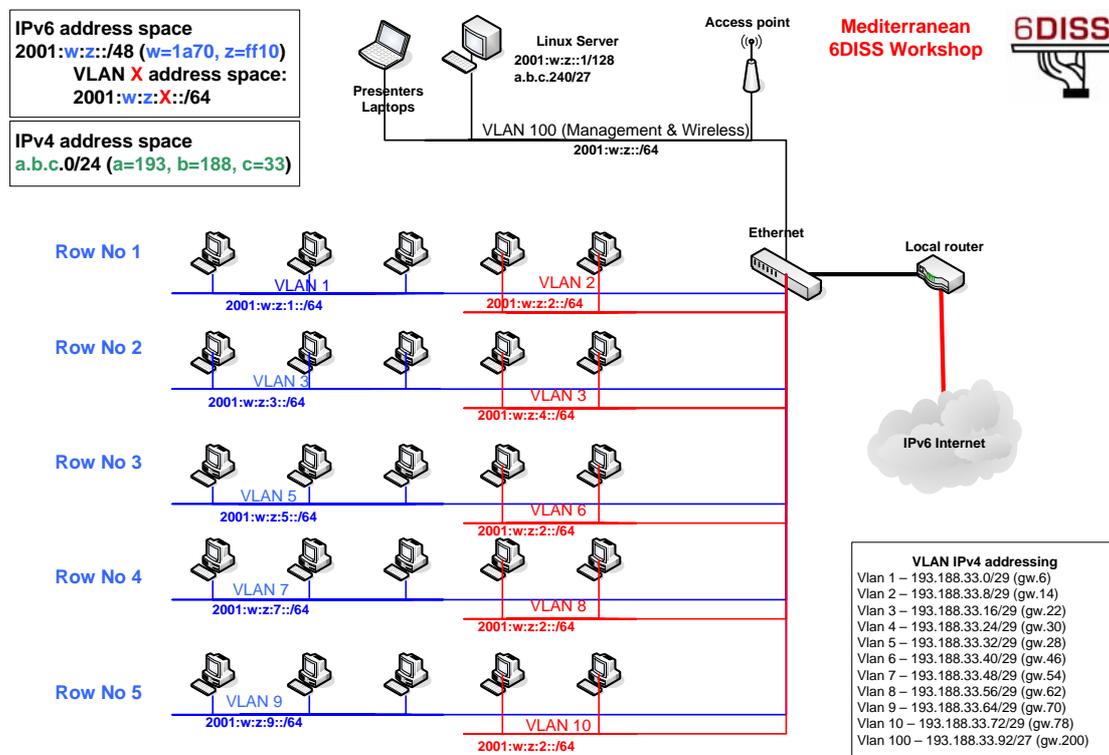

Figure 1: 6DISS lab topology.

Linux Server

A PC having Scientific Linux 4.2 (https://www.scientificlinux.org/) is running BIND 9.2.4 (http://www.isc.org/sw/bind/) and Apache HTTP Web Server 2.0.55 (http://httpd.apache.org/). Access to the linux server is allowed via **SSH/FTP** at the IPv6 address **2001:w:z:100::1/64** (or the IPv4 address a.b.c.240) using the **login/password:** *root/6diss*.

---

[1] Please refer to Figure 1 for the values of "w" and "z" at the IPv6 address.

Exercise A: IPv6 DNS

Objectives

There are IPv4 DNS (A, PTR) entries in the `/var/named/` directory for all lab PCs. Participants are asked to create the relevant IPv6 DNS (AAAA, PTR) entries.

Requirements

Participant should have basic knowledge of DNS and the BIND application.

DNS configuration basics

A DNS server is configured via the `/etc/named.conf` file. The "forward- or reverse-zone" files, i.e. the files that contain the (IPv4) DNS entries, are defined using via the following syntax in the `/etc/named.conf`:

```
zone "testbed.6diss.org" in {
      type master;
      file "db.6diss";
};
zone "<c>.<b>.<a>.in-addr.arpa" in {
      type master;
      file "db.<a>.<b>.<c>";
};
```

In order to add IPv6 DNS entries for PCs belong in VLAN **X**, the zone file `db.6diss`**X**[2] and the reverse-zone `db.`**X.z.w**[3]`.2001` have to be created by the system administrator. Furthermore, the file `/etc/named.conf` should also contain the appropriate entries for the aforementioned files, as follows:

```
zone "testbed.6dissX.org" in {
      type master;
      file "db.6dissX";
};

zone "X.0.0.0.<z>.<w>4.1.0.0.2.ip6.arpa" in {
      type master;
      file "db.X.<z>.<w>.2001";
};
```

Exercises steps

1. Reboot one PC per VLAN using the Scientific Linux partition and install BIND 9.2.4 (http://www.isc.org/index.pl?/sw/bind/). This PC will become the "server" for the group.

---

[2] The IPv4 and IPv6 forward zone files could be the same. However, in the 6DISS training the forward-zone files for IPv4 and IPv6 are separated in order to allow different groups to create their own configuration.

[3] Please refer to Figure 1 for the values of "w" and "z" at the IPv6 address.

[4] Example: zone "1.0.0.0.0.1.f.f.0.7.a.1.1.0.0.2.ip6.arpa"

- Make sure that you removed any configuration from the previous exercise that could harm the IPv6 connectivity or routing.
- Set the IPv6 address of the linux server as `2001:`**`w:z:`**`VLAN_X:1`
- Note down the IPv4 address of the server.

2. Create and populate the files "`testbed.6diss`**`X`**`.org`" and "**`X`**`.0.0.0.`**`<z>.<w>`**`.1.0.0.2.ip6.arpa`"
   - (Tip: See configuration examples at the end of the document)
3. Validate the configuration files using the command "`named-checkzone`"
   - (Tip (example): `# named-checkzone testbed.6diss1.org db.6diss1`)
4. Restart DNS server
   - (Tip: `kill -HUP` `` `cat /var/run/named/named.pid` `` or `rndc reload`)
5. Check DNS server logs
   - (Tip: `grep named /var/log/messages`)
6. Validate DNS queries using the other PC in the VLAN. Do the same using the local linux server. What is the transport protocol for the DNS queries?
   - (Tip: Use the `nslookup` and change the DNS server to IPv4 address of the local linux server in the VLAN)
7. Use IPv6 as DNS queries transport protocol. What is the problem in the DNS queries at the PCs with WinXP? Is there the same problem in DNS queries in the Linux machines?
   - (Tip: Add the following configuration lines at the `named` configuration file `Allow IPv6 transport listen-on-v6 port 53 {any;};`)
   - (Tip: Use the `nslookup` and change the DNS server to `2001:w:z:VLAN_X:1`)

Exercise B: Enable an Apache server

Objectives

Lab participants are asked to set up and IPv6-enabled server. In addition, different IPv6 and IPv4 web pages are created while IPv4-only web sites are accessed via an IPv6 proxy.

Apache HTTP configuration basics

An Apache web server is configured via the `/etc/httpd/conf/http.conf` file. Access privileges to pages are defined in the `/etc/httpd/conf.d` directory. Further information can be found at http://httpd.apache.org/docs-2.0/.

Exercises steps

1. Reboot at least one PC per VLAN using the Scientific Linux partition. Install the Apache HTTP server 2.0.55 (http://httpd.apache.org/). As the server supports both IPv6/4, you do not have to do any change in the configuration.
   - Make sure that you removed any configuration from the previous exercise that could harm the IPv6 connectivity or routing.
   - Set the IPv6 address of the linux server as `2001:w:z:VLAN_X::1`
   - Note down the IPv4 address of the server.

2. Create two directories to store HTML files. The directory `/var/www/html6` will be used for accessing the server via IPv6 while the directory `/var/www/html4` will be used for accessing the server via IPv4.
   a) Create the following HTML files:
   a) `<html> <body> You have successfully accessed an HTML page over <b>IPv6</b>! <br> 6DISS Workshop In Malta </body></html>`
   b) `<html> <body> ERROR: THIS PAGE IS ACCESSED OVER IPv4. PLEASE USE an <a href=http://[2001:648:2320:1000::1]><b>IPv6</b></a> LINK TO SEE THE CONTENT OF THIS WEB SITE <br> </body></html>`
3. Create a virtual host for accessing the web server via IPv4.
   - (Tip: Add the following lines to `httpd.conf` file: `<VirtualHost a.b.c.K`[5]`:80> DocumentRoot /var/www/html4 </VirtualHost>`
4. Restart the server and access the HTTP server over IPv4
   - (Tip: Use the command `# service httpd restart or # apachectl restart`)
5. Allow proxying to another web site.
   - (Tip: Add the following lines to `httpd.conf` file: `ProxyPass /6diss/ http://www.6diss.org/ <Location /6diss/> ProxyPassReverse / </Location>`
6. Restart the server.

Exercise C: Examples of various IPv6 applications

Objectives

Lab participants are asked to use simple IPv6 applications and verify their proper operation.

Exercises steps

1. Access an IPv6 web site and capture traffic using `ethereal` tool.
2. Access an IPv6-enabled FTP server. Verify that the connection is established via IPv6.
   - Which FTP server is IPv6-enables; ftp.ntua.gr or ftp.auth.gr?
3. Access an `AS Path` web site. Find the number of IPv6 AS numbers and the number of routing entries in the IPv6 routing table. Identify the IPv6 upstream provider for local NREN. What is worth noticing?
   - (Tip: `http://www.join.uni-muenster.de/bgp/bgp.html`)
4. Use a `Looking Glass` web site. Identify the same information as in previous step.
   - (Tip: `http:// http://netmon.grnet.gr/lg.shtml`)

---

[5] Use the IPv4 address noted in step 1.

Supporting info

Appendix A: DNS supporting info

Examples BIND files

Forward-zone file for `testdomain.org`

```
testdomain.org. IN SOA server.testdomain.org. root.server.testdomain.org. (
                        1       ; Serial
                        10800   ; Refresh after 3 hours
                        3600    ; Retry after 1 hour
                        604800  ; Expire after 1 week
                        86400 ) ; Minimum TTL of 1 day


;
; Name servers
;
testdomain.org.  IN NS  server.testdomain.org.
;
; Define $ORIGIN
; $ORIGIN testdomain.org.
;
; If an $ORIGIN directive is not defined - BIND uses the zone name in the named.conf
; file as the initial ORIGIN
; @                          IN NS  server.testdomain.org.


;
; Host addresses
;
localhost.testdomain.org.    IN A    127.0.0.1
laptop.testdomain.org.       IN A    10.10.10.1
server.testdomain.org.       IN A    10.10.10.202
camera.testdomain.org.       IN A    10.10.10.201
;
; Multi-homed hosts
;
router.testdomain.org.       IN A    10.10.10.200
;
; Aliases
;
www                     IN CNAME server
;
; IPv6 host addresses
;
localhost.testdomain.org.    IN AAAA    ::1
laptop.testdomain.org.       IN AAAA    2001:648:E000:1000::1
server.testdomain.org.       IN AAAA    2001:648:E000:1000::2
```

Reverse-zone file for `testdomain.org`

```
0.0.0.1.0.0.0.E.8.4.6.0.1.0.0.2.ip6.arpa. IN SOA server.testdomain.org.
root.server.testdomain.org. (
                        1       ; Serial
                        10800   ; Refresh after 3 hours
                        3600    ; Retry after 1 hour
                        604800  ; Expire after 1 week
                        86400 ) ; Minimum TTL of 1 day
;
; Name servers
;
0.0.0.1.0.2.3.2.8.4.6.0.1.0.0.2.ip6.arpa.  IN NS  server.testdomain.org.


;
; Addresses point to canonical name
;
```
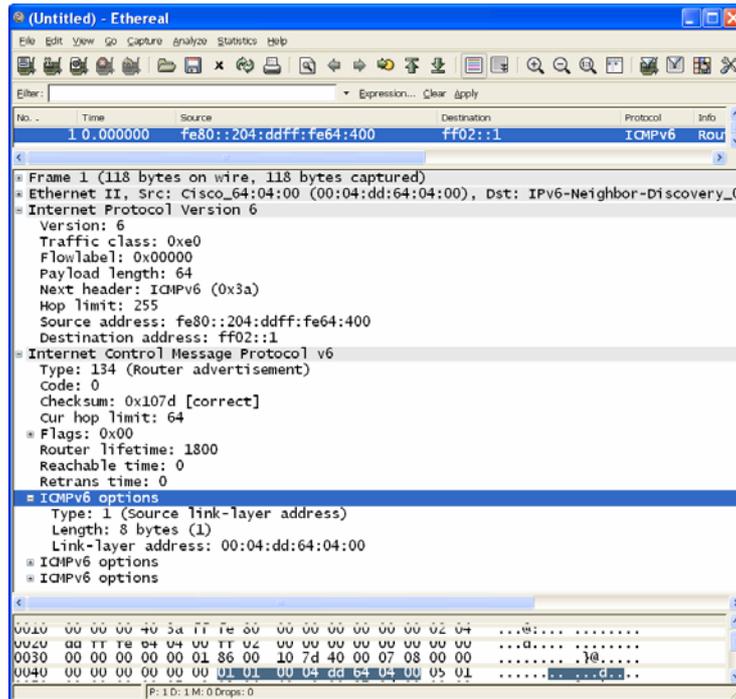
```
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.E.8.4.6.0.1.0.0.2.ip6.arpa.       IN PTR
laptop.testdomain.org.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.E.8.4.6.0.1.0.0.2.ip6.arpa.       IN PTR
server.testdomain.org.
```

Localhost
```
0.0.0.0.ip6.arpa. IN SOA server.aliako.gr. root.server.aliako.gr (
                        1        ; Serial
                        10800    ; Refresh after 3 hours
                        3600     ; Retry after 1 hour
                        604800   ; Expire after 1 week
                        86400 )  ; Minimum TTL of 1 day
0.0.0.0.ip6.arpa.  IN NS  server.aliako.gr.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa.  IN PTR
localhost.
```

Appendix B: Compact "Ethereal" documentation

Ethereal is used by network professionals around the world for troubleshooting, protocol analysis, software and protocol development, and education. Its open source license allows talented experts in the networking community to add enhancements. It runs on all popular computing platforms, including Unix, Linux, and Windows. See further information at http://www.ethereal.com/.

In order to capture packets, use the menu (Capture -> Start)
If you want to capture only a specific set of packets, use *capture filters* (Capture->Options), as shown in Figure 2.

Figure 2: Ethereal packet capture filters

(Tip: Use the capture filter "`ip6`" to capture only IPv6 packets or "`icmp6`" capture only ICMPv6 packets)

After having captured some traffic, you can also filter the results using the "Filter" option, as shown in the Figure 3.

Figure 3: Ethereal interface

(Tip: Use the filter "`ip6`" to show only IPv6 packets, "`icmpv6.code==0`" to show ICMP packets of specific code or "`http`" to show HTTP traffic.)

Appendix C: Lab specifications

PCs are running WinXP (SP2) and Scientific Linux 4.2. Workshop local router is a Cisco 1811 using `c181x-advipservicesk9-mz.124-2.XA.bin`. Ethereal Version 0.10.13 is also installed at the WinXP partition.