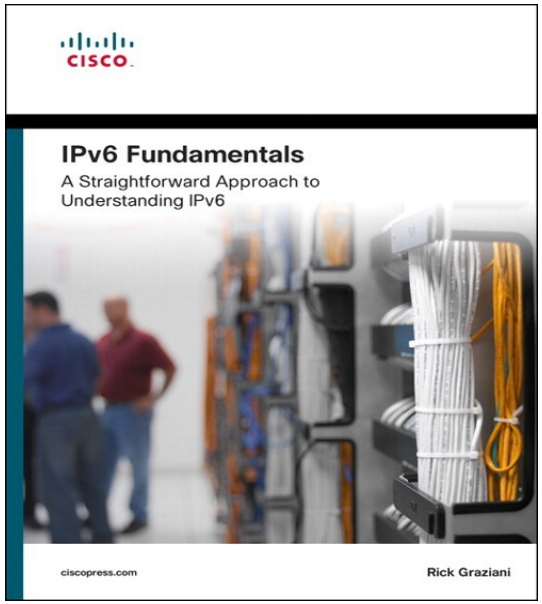
Practical Network Defense

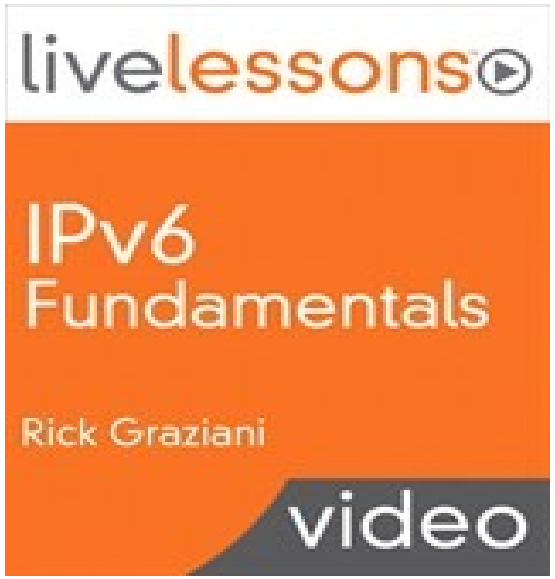
Master's degree in Cybersecurity 2024-25

IPv6: addressing and ICMPv6 lab

Angelo Spognardi
spognardi@di.uniroma1.it
Dipartimento di Informatica
Sapienza Università di Roma

Material taken from Rick Graziani IPv6 courses





Recap last lectures

- IPv6 address types
  - Global Unicast Address
  - Local-link Unicast Address
- IPv6 dynamic assignment options
- Multicast Addresses
  - Permanent addresses (“well known multicast groups”)
  - Scope of multicast addresses
- IPv6 packet header
- IPv6 Extension headers

Lab activity

Main tasks

- DHCPv6 with prefix delegation
- ICMPv6 MTU discovery
  - With ping and tracepath
- Tunnelbroker
- RIPE NCC IPv6Security-Exercises

To do the activities

- We will use Kathará (formerly known as netkit)
  - A container-based framework for experimenting computer networking: http://www.kathara.org/
- A virtual machine is made ready for you
  - https://drive.google.com/file/d/1W6JQzWVyH5_LKLD20R6XH1ugPDP5LWP5/view?usp=sharing
- For not-Cybersecurity students, please have a look at the Network Infrastructure Lab material
  - http://stud.netgroup.uniroma2.it/~marcos/network_infrastructures/current/cyber/
    - Instructions are for netkit, we will use kathara

The kathara VM

- It should work in both Virtualbox and VMware
- It should work in Linux, Windows and MacOS
- There are some alias (shortcuts) prepared for you
  - Check with **`alias`**
- All the exercises can be found in the git repository:
  - https://github.com/vitome/pnd-labs.git
  - DON'T FORGET TO UPDATE → `~/pnd-labs$ git pull`
- You can move in the directory and run lstart
  - **NOTE**: launch docker first or the first lstart attempt can (...will...) fail

Lab activity: ex4

Exercise 4: pnd-labs/lab2/ex4

DHCPv6 with prefix delegation

- One router with two lan, both with 2 pcs. The router is connected with an ISP router.
- TASK: configure the topology to use IPv6 addresses
  - The ISP makes use of a DHCPv6 server for address and prefix distribution
  - The router has to ask prefixes to its ISP and has to distribute addresses inside the two lans, using SLAAC.
    - At least two options:
      - dibbler DHCPv6 client + radvd
      - wide-dhcp + dnsmasq
- The ISP is already configured to provide prefixes, while the router and the pcs have to be configured.
  - the router has always 1 in the host part of its own link local address

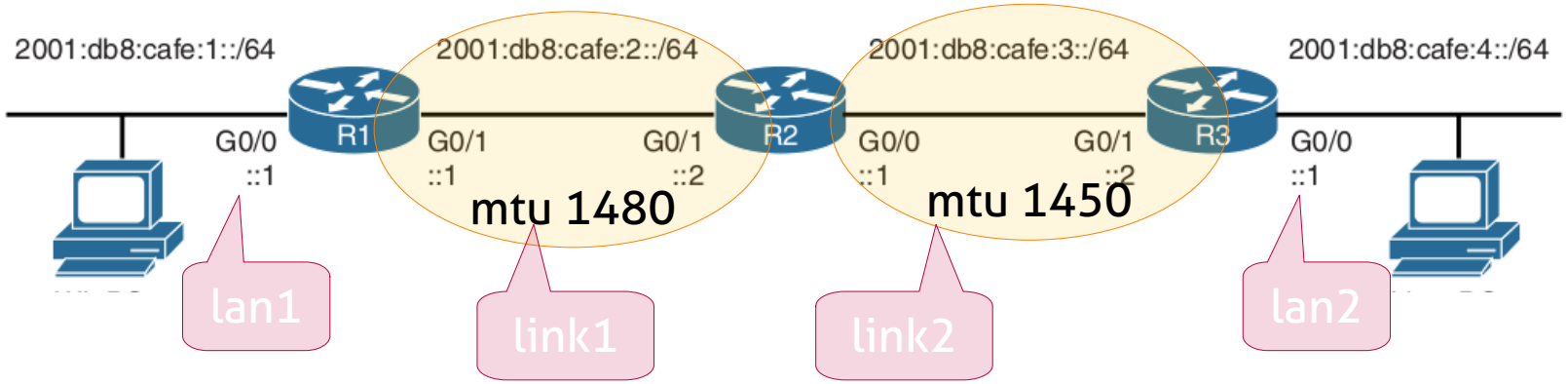
DHCPv6-PD: Reference links

- Linux ipv6 configuration: ipv6 sysctl
  - https://www.kernel.org/doc/Documentation/networking/ip-sysctl.txt
- DHCPv6:
  - dibbler+radvd:
    - useful guide: https://k3a.me/setting-up-ipv6-using-a-dhcp-client/
    - man pages:
      - https://manpages.debian.org/testing/radvd/radvd.conf.5.en.html
      - https://klub.com.pl/dhcpv6/doc/dibbler-user.pdf
  - wide-dhcp+dnsmasq:
    - useful guide: https://github.com/torhve/blag/blob/master/using-dnsmasq-for-dhcpv6.md
    - man pages:
      - https://thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html
      - https://manpages.debian.org/stretch/wide-dhcpv6-client/dhcp6c.8.en.html
      - https://manpages.debian.org/stretch/wide-dhcpv6-client/dhcp6c.conf.5

Lab activity: ex5

Exercise 5: pnd-labs/lab2/ex5

- Three routers connecting two LANs with one PC each.
- Configure the topology to use static addressing for the routers and SLAAC IPv6 addresses for the two LANs. See the README file for the details.
- Moreover, you have to play with the MTU of the links between the routers to generate and capture ICMPv6 packets (Packet too big or MTU discovery).
- You have to use **`tracepath`** and **`ping`** to test connectivity and MTU
- You can use the **`ip link set mtu XXXX dev YYY`** on both the end points of a link to alter the MTU



Lab activity: ex6

Exercise 6: create an IPv6 capable connection

- The task is to create an virtual interface for providing capable IPv6 Internet connection
  - IPv6 native: the entire infrastructure supports IPv6
    - Namely, your ISP provides you IPv6 addresses
  - IPv6 capable: the infrastructure can support IPv6 services and technologies by taking advantage of IPv6 transition technologies
    - Namely, you use a Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
      - Tunnel IPv6 messages inside an IPv4 header
  - IPv4 only: the infrastructure can not support IPv6
- Reference: https://developers.redhat.com/blog/2019/05/17/an-introduction-to-linux-virtual-interfaces-tunnels/

ISATAP: howto, using hurricane-electric services

- Go to https://www.tunnelbroker.net/ and register
- On the left, select Create regular tunnel
- Setup everything following the form directions
  - You can also refer to https://ipv6.he.net/certification/faq.php or http://ipv6.he.net/presentations.php and http://tunnelbroker.net/forums/
  - Beware if you are in a NAT'd network (this is highly likely)
- Important: your host has to be reachable from outside using protocol 41 → IPv6 Encapsulation (RFC 2473)
  - Virtual server, forward or DMZ in your home router

Steps to follow (sketch)

```
ip tunnel add he-ipv6 mode sit remote 216.66.80.98\
        local 192.168.100.13 ttl 255
ip link set he-ipv6 up
ip addr add 2001:a23f:f25:14c9::2/64 dev he-ipv6
ip route add ::/0 dev he-ipv6
ip -f inet6 addr
```

Lab activity: ex7

Exercise 7: IPv6Security-Exercises

- The task is to replicate the exercises of the RIPE NCC security lab
- The topology is the same, but the names are different:
  - hostA → pc1, hostB → pc2, hostC → pc3, router → r1
- Scapy is on pc3
- THC-IPV6 and the IPv6-toolkit must be built in pc1 and pc2
  - You can follow the README
  - In a nutshell: copy from shared, unzip, cd and make install

That’s all for today

- **Questions?**
- References:
  - https://developers.redhat.com/blog/2019/05/17/an-introduction-to-linux-virtual-interfaces-tunnels/
  - http://www.tcpipguide.com/free/t_InternetProtocolVersion6IPv6IPNextGenerationIPng.htm
  - https://www.6diss.org/e-learning/
  - http://www.cabrillo.edu/~rgraziani/ipv6-presentations.html
  - Book chapter 11 (even if quite obsoleted)