



RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Virtual IPv6 Security Lab Environment

Hands-on Learning

Ondřej Caletka | 18 November 2021 | UKNOF 48

RIPE NCC Learning & Development



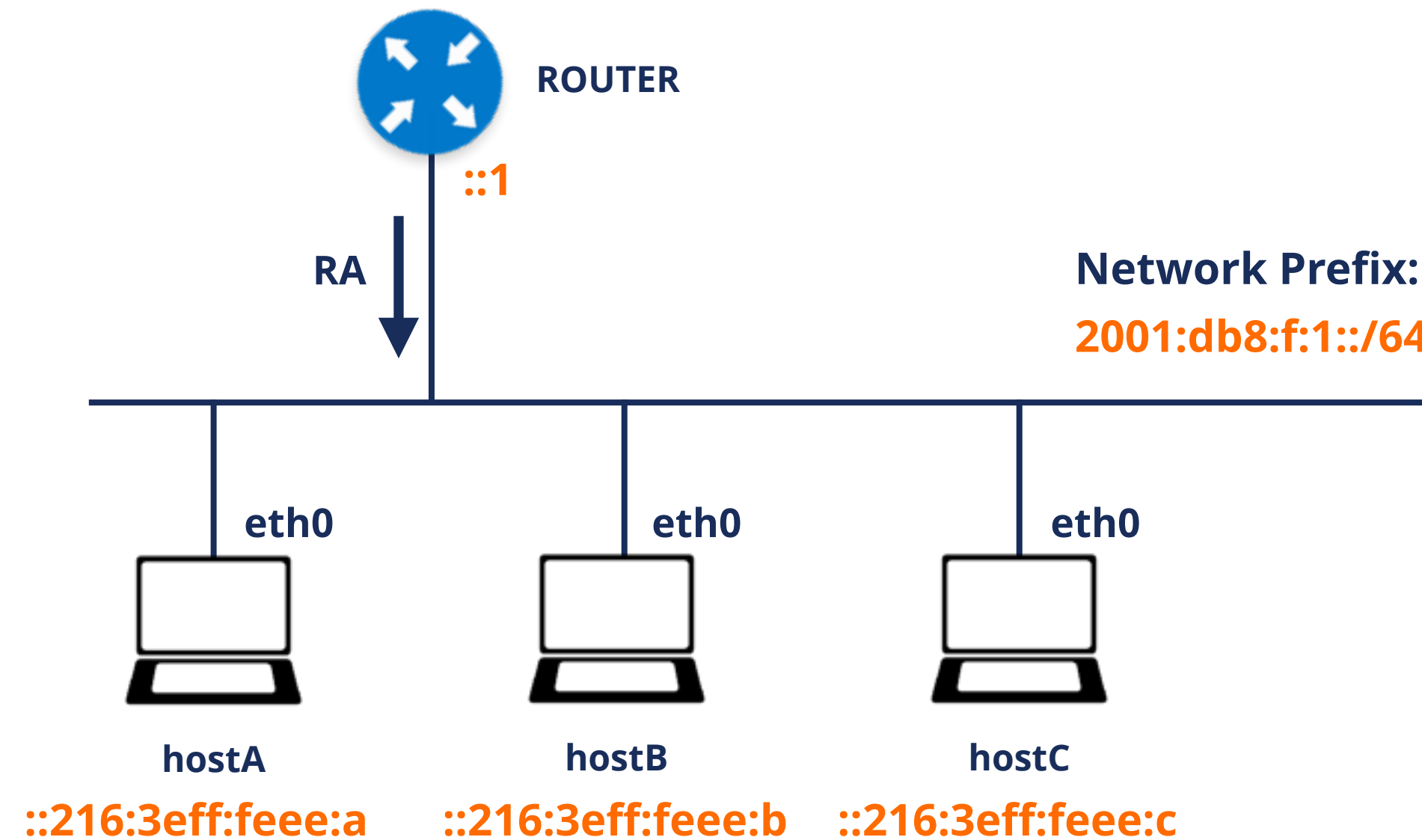
- Former Training Services of RIPE NCC
- Face-to-face trainings for LIRs
 - Temporary suspended due to COVID-19
- Webinars for LIRs
 - Live interactive sessions lasting one or two hours
- RIPE NCC Academy
 - E-learning platform accessible to everyone
- RIPE NCC Certified Professionals
 - Prove your skills and receive a digital badge



IPv6 Security E-learning Course



- The newest addition to IPv6 Security trainings and webinars
- Preparation for IPv6 Security Certified Professional exam
- First time with hands-on labs



Delivering Lab Environment



- Should be universally scalable
- Should not cost us too much money
- Should allow enough time to play with it
- Should be easy to use
- We decided to **deliver a Virtual Machine image**



Image: Markus Meier, FSFE, CC-BY-SA 4.0

Virtual Machine Challenges



- Different virtualisation technology on each platform
 - The only *common* solution is **Oracle VM VirtualBox**, available on Windows, macOS or Linux
 - Still suboptimal compared to native solutions like Hyper-V or KVM
- No common keyboard layout or screen resolution
 - Therefore, we deliver the VM headless with everything accessible over a web interface
- Deploying a VM image is hard
 - We try to make it easier by using **Vagrant**

Running The Labs



- Install VirtualBox
- Install Vagrant
- Open terminal and type:
vagrant init ripencc/ipv6seclab
vagrant up
- Open web browser on
<http://localhost:8080/>

The screenshot shows the RIPE NCC Academy dashboard in a web browser. The dashboard is divided into several sections:

- Host A:** A terminal window showing the installation of Scapy. The user runs `pip3 install scapy` and the output shows the installation of Scapy version 2.4.5. The user then runs `scapy` and sends a packet.
- Host B:** A terminal window showing the output of the `top` command, displaying system statistics and a list of running processes.
- Host C:** A terminal window showing the output of the `tcpdump` command, displaying a list of captured packets. The first packet is highlighted, showing its source and destination addresses.
- Available tools:** A list of tools available for the lab, including Scapy, THC-IPV6, SIB IPv6 Toolkit, and Tormshark.
- Hints:** A list of hints for using the lab, including instructions on how to resize terminal windows and how to scroll inside the tmux window.
- Scratchpad:** A text area for taking notes.

Under The Hood



- Based on Ubuntu 20.04 LTS
- Three containers managed by **LXD**
- Consoles accessible from web browser using **ttyd** and **tmux**
- Static website and WebSocket proxy by **NGINX**
- Everything deployed using **Ansible**
- **Public development** in RIPE NCC's GitHub repository

<https://github.com/RIPE-NCC/ipv6-security-lab/>

Further Steps



- Collect feedback from the users
- Expand the lab to use a more real networking gear
 - Some routers are now available as containers
 - Uncertain licence conditions

Try out our new IPv6 security e-learning course!

<https://academy.ripe.net>





Questions



Ondrej.Caletka@ripe.net
@ripencc