IPv6 SECURITY

This one-day course provides an overview of the most relevant IPv6 security topics. The participant will gain insight into industry best practice and gain a high-level understanding of the most pressing IPv6 security concerns today. The course includes theory and hands-on exercises.

Goals

- Identify what is IPv6 Security and what it isn't
- Identify and protect your network from IPv6-related threats
- Understand how the IPv6-associated protocols work. Identify, and protect your network from the related threats
- Recognise the existing security solutions to protect your IPv6 network
- Understand how to apply packet filtering in IPv6
- Understand how Internet-wide IPv6 threats could happen, such as DDoS or via transition mechanisms
- Understand the many complexities of IPv6 that must be taken into account from a security point-of-view

Pre-Requisites

This is an advance course that requires the participants to understand:

- IPv4 networking and security
- IPv6 networking equivalent to that covered in the RIPE NCC Basic IPv6 Course or the RIPE NCC Academy IPv6 Fundamentals Course
- Basic Internet security concepts
- For the labs: CLI and command tools

Course Content

- Introduction
- Basic IPv6 Protocol Security
  - Basic header
  - Extension Headers
  - Addressing
- IPv6 Associated Protocols Security
  - ICMPv6
  - NDP
  - MLD
  - DNS
  - DHCPv6
- Internet wide IPv6 Security
  - Filtering
  - DDoS
  - Transition Mechanisms
- Tips and Tools
  - Up-to-date information
  - Security Tools
  - Device features

- Training Material: **https://www.ripe.net/training-material**
- Feedback Survey: **https://www.ripe.net/feedback/v6s/**
- Contact us: **learning@ripe.net**
- Learning and Development Services: **www.ripe.net/support/training**

Training Material

RIPE NCC