

# IPv6 and Security

## How to Properly Secure Networks and End Devices

The introduction of IPv6 gives rise to new security questions both for providers of enterprise networks and for private customers. After all, IPv6 offers new options to compromise a network. On the one hand, this includes variants of existing types of attack, on the other hand, IPv6 opens up new security gaps. To protect an IPv6 network, it is not merely required to clarify these basic security issues but also to find out whether the components used so far—i.e. firewalls, proxies or intrusion prevention systems (IPS)—are actually equipped for IPv6. Which is the correct method for migration under security aspects? Which changes occur due to the permanent availability of public addresses after the elimination of NAT? Which gaps appear in Windows operating systems due to tunneling mechanisms, such as Teredo, without even migrating to IPv6 and how can these gaps be mended? This course gives a detailed overview of these highly topical questions. The students will learn to assess the level of danger introduced in their networks by IPv6 and to plan comprehensive security measures.

### Course Contents

- New points of attack through IPv6
- Securing IPv6 addressing
- The auxiliary protocols ICMPv6 and DHCPv6 from a security perspective
- IPv6 and First Hop Security
- Securing IPv6 networks
- Securing endpoints
- Securing routers for IPv6
- Adapt firewalls to IPv6
- Securing the migration

**E-Book** You will receive the comprehensive documentation package of the ExperTeach Networking series – printed documentation, e-book, and personalized PDF! As online participant, you will receive the e-book and the personalized PDF.

### Target Group

This course is designed for planners, administrators and security managers intending to design, prepare, or assist in a migration to IPv6. Attendance at this course can be credited for T.I.S.P. recertification.

### Prerequisites

The students require sound know-how of the traditional IP world and need to be familiar with the new protocol. Participation in the course IPv6 - Addressing, Routing is often recommendable as a preparation. A further requirement is that the students know and understand common security concepts.

### This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

[www.experteach-training.com/go/IP6S](http://www.experteach-training.com/go/IP6S)

### Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

### Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

### Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training	Prices, excl. of V.A.T.	
<b>Classes in Germany</b>	<b>2 Days</b>	<b>€ 1,595</b>
<b>Classes in Austria</b>	<b>2 Days</b>	<b>€ 1,595</b>
<b>Classes in Switzerland</b>	<b>2 Days</b>	<b>€ 2,150</b>
<b>Online Training</b>	<b>2 Days</b>	<b>€ 1,595</b>
<b>Date/course venue</b>	<b>Course language German</b>	
19/09-20/09/24 Berlin	13/02-14/02/25	Online
19/09-20/09/24	13/02-14/02/25	Zürich
19/09-20/09/24	13/03-14/03/25	Düsseldorf
24/10-25/10/24	13/03-14/03/25	Online
24/10-25/10/24	10/04-11/04/25	Berlin
24/10-25/10/24 Zürich	10/04-11/04/25	Hamburg
21/11-22/11/24	10/04-11/04/25	Online
21/11-22/11/24	08/05-09/05/25	Online
19/12-20/12/24	08/05-09/05/25	Wien
19/12-20/12/24	05/06-06/06/25	Frankfurt
16/01-17/01/25	05/06-06/06/25	Online
16/01-17/01/25	03/07-04/07/25	Hamburg
13/02-14/02/25	03/07-04/07/25	Online

Status 07/14/2024



# Table of Contents

## IPv6 and Security – How to Properly Secure Networks and End Devices

<b>1 Basic safety considerations</b>	3.1.3 Neighbor Unreachability Detection (NUD)	4.2.5 Fortinet
1.1 Basic considerations	3.1.4 DoS_New_IP6	4.2.6 Juniper
1.1.1 Security measures	3.1.5 NDP Exhaustion Attack	4.2.7 Barracuda
1.1.2 Personnel and service providers	3.1.6 Neighbor Advertisement Flooding	4.2.8 Customize objects
1.2 IPv4 and IPv6 security in comparison	3.2 SLAAC Attacks	4.2.9 Adding rule sets
1.2.1 Differences between IPv4 and IPv6	3.2.1 Rogue router	4.2.10 Bogon filtering
1.3 The current security situation	3.2.2 Man in the Middle with RAs	4.3 Radius and IPv6
1.3.1 Vulnerable IPv6 stacks	3.2.3 Faked Default Gateway	4.3.1 Establishing IPv6 connectivity
1.3.2 The firewall	3.2.4 RA flooding	4.3.2 Freeradius and IPv6
1.3.3 Intrusion Prevention System	3.3 DHCPv6 attacks	4.3.3 Microsoft - Network Policy Server
1.4 The IPv6 header from a security point of view	3.3.1 DHCPv6 Starvation	4.3.4 RADIUS IPv6 attributes
1.4.1 The Flow Label - Covert Channel	3.3.2 Rogue DHCPv6 server	4.4 IPS in IPv6 networks
1.4.2 Extension Header Parsing	3.4 ICMPv6 attacks	4.5 Proxies in IPv6 networks
1.4.3 Security relevance of the extension headers	3.4.1 Amplification attack	4.6 IPsec in IPv6 networks
1.4.4 The filtering of IPv6	3.4.2 Redirect attacks	4.6.1 Possible uses of IPsec
1.5 Testing the security - Tools for IPv6 Vulnerability Tests	3.5 ACLs for security	4.6.2 Host to Host Scenario
1.5.1 NMAP	3.5.1 Rogue router exclusion	4.6.3 IPv6 VPNs
1.5.2 Nessus and OpenVAS	3.5.2 Prevent rogue DHCP servers	4.6.4 IPv6 VPDN with IPsec
1.5.3 Packet generators	3.5.3 RA Guard	4.6.5 IPsec RAS VPNs and IPv6
1.5.4 The THC tools collection	3.5.4 DHCPv6 Guard/Shield	<b>5 Security during migration</b>
1.5.5 SI6 tools	3.5.5 NDP snooping	5.1 Mental move to IPv6
<b>2 IPv6 addressing from a security point of view</b>	3.5.6 NDP Inspection	5.2 IPv6 Latent Threats
2.1 Security relevance of NAT	3.6 SEND	5.3 Dual Stack - Double Protection Required
2.1.1 IPv6-IPv6 Network Prefix Translation (NAT66)	3.6.1 Securing RAs with SEND	5.3.1 Endpoint Security from an IPv6 Perspective
2.2 Security considerations for address types	3.6.2 SEND and stateful autoconfiguration	5.4 Questioning the benefits of tunnel technologies
2.2.1 EUI 64 - Large recognition value	<b>4 Security of IPv6 networks</b>	5.4.1 Questioning tunnel security
2.2.2 Temporary addresses	4.1 Securing routers in IPv6 networks	5.4.2 Secure Configured Tunnel
2.3 Exploring IPv6 addresses	4.1.1 Setting up IPv6 ACLs	5.4.3 Encrypt tunnel traffic
2.3.1 Passive sniffing	4.1.2 Inbound traffic	<b>A Lab Exercises</b>
2.3.2 Detect-New-IP6	4.1.3 Address filtering	A.1 Lab Exercises in the Course
2.3.3 Multicast enumeration	4.1.4 Filtering ICMPv6	A.1.1 Lab Setup
2.3.4 Alive6	4.1.5 Securing routing protocols	A.2 Exercises Chapter 2
2.3.5 Registry query	4.1.6 Authentication for routing protocols	A.3 Exercises Chapter 3
2.3.6 IPv6 network scanning	4.1.7 BGP-4 - Using Link Local Unicasts	<b>B Lab exercises online</b>
2.3.7 IPv6 address guessing	4.1.8 Preventing IP spoofing	B.1 Lab exercises in the course
2.3.8 DNS Reconnaissance	4.2 Adapt firewalls	B.1.1 Lab setup
<b>3 IPv6 and First Hop Security</b>	4.2.1 Questioning IPv6 capability	B.2 Exercises Chapter 2
3.1 Neighbor Discovery Attacks	4.2.2 Check Point	B.3 Exercises Chapter 3
3.1.1 Trust Models and Threats	4.2.3 Cisco ASA	
3.1.2 NDP Spoofing	4.2.4 Palo Alto	

