

# PowerPackage IPv6

## Adressierung, Routing, Interworking, Security

Introducing IPv6 into an enterprise network is a very complex issue. Starting with the functioning of the IPv6 protocol and going on to discuss security aspects and useful migration strategies, this BootCamp will teach you everything you need to know to use this technology successfully.

This IPv6 all-in-one course includes all the subjects covered in the ExperTeach Networking courses IPv6, and IPv6 and Security. The knowledge you gain here will allow you to implement a structured, safe, and well-thought-out migration to IPv6.

### Course Contents

- What's New in IPv6
- IPv6 Headers, Extension Headers, and the Setup of IPv6 Addresses
- The IPv6 Communication and Its Shortcomings
- Stateless and Stateful Auto-Configuration
- Planning a Safe Migration from IPv4 to IPv6
- IPv6 in End Devices, Routers, and Firewalls
- Tunneling from IPv6 through IPv4
- Interworking between IPv6 and IPv4 (NAT64 and DNS64)
- Routing and Network Services (DNS, DHCP, RADIUS, and SNMP) with IPv6
- Applications: WWW, FTP, and E-mail with IPv6
- Internet Access and ISP Networks with IPv6
- Enterprise Networks and IPv6
- IPv6 in Mobile Communications
- Security and IPv6: New Points of Attack, Protection, Firewall, and VPN

**E-Book** You will receive the detailed documentation package from the series ExperTeach Networking – print, e-book and personalized PDF!

### Target Group

This course is designed for planners, administrators and security managers who intend to introduce IPv6 into a network and need to be able to assess potential security risks in advance.

### Prerequisites

This course is designed for planners, administrators and security managers who intend to introduce IPv6 into a network and need to be able to assess potential security risks in advance.

### This Course in the Web



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

[www.expertech-training.com/go/IP6B](http://www.expertech-training.com/go/IP6B)

### 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.	
Classroom training	5 Days	€ 2,595	
<b>Date/course venue</b>			
07/10-11/10/19 Berlin	08/06-12/06/20 Hamburg		
07/10-11/10/19 Hamburg	06/07-10/07/20 Frankfurt		
11/11-15/11/19 Düsseldorf	17/08-21/08/20 Düsseldorf		
09/12-13/12/19 Frankfurt	07/09-11/09/20 München		
09/12-13/12/19 Zürich	07/09-11/09/20 Stuttgart		
20/01-24/01/20 München	07/09-11/09/20 Wien		
20/01-24/01/20 Wien	05/10-09/10/20 Berlin		
17/02-21/02/20 Berlin	05/10-09/10/20 Hamburg		
17/02-21/02/20 Hamburg	02/11-06/11/20 Frankfurt		
23/03-27/03/20 Frankfurt	02/11-06/11/20 Zürich		
23/03-27/03/20 Zürich	07/12-11/12/20 Düsseldorf		
20/04-24/04/20 Düsseldorf	11/01-15/01/21 München		
11/05-15/05/20 München	11/01-15/01/21 Wien		
11/05-15/05/20 Stuttgart	08/02-12/02/21 Berlin		
11/05-15/05/20 Wien	08/02-12/02/21 Hamburg		
08/06-12/06/20 Berlin	08/03-12/03/21 Frankfurt		

Status 09/19/2019



# Table of Contents

## PowerPackage IPv6 – Adressierung, Routing, Interworking, Security

<b>1 IPv6 - The Protocol</b>		
1.1 Weak Points of IPv6		
1.1.1 Efficiency		
1.1.2 Address Space		
1.1.3 Size of the Routing Tables		
1.1.4 Complexity due to Auxiliary Protocols		
1.2 Demands Made on the New IP		
1.3 The RFCs		
1.4 The Header Format		
1.4.1 Version, Payload Length, and Hop Limit		
1.4.2 Traffic Class		
1.4.3 Flow Label		
1.5 Extensions with the Next Header		
1.5.1 Extensions for the Routers		
1.5.2 Extensions for the End Systems		
1.6 Mobile IPv6		
<b>2 The Migration in an Overview</b>		
2.1 IPv6—Act Now		
2.1.1 Benefits for an ISP		
2.1.2 Added Value for Corporate Networks		
2.1.3 IPv6 at Home—Why?		
2.1.4 Motivation for IPv6 in Mobile Communications Networks		
2.2 Migration Procedure		
2.2.1 Networks with Dual Stack Nodes		
2.2.2 Native IPv6 Networks		
2.2.3 Tunnel		
2.3 Migration Strategies		
2.3.1 Backbone First		
2.3.2 Edges First		
2.4 Planning the Migration		
2.4.1 Determining an Aim		
2.4.2 Analyzing the Current State		
2.4.3 Inventory and Analysis		
2.4.4 An IPv6 Test Environment		
2.5 Migrating—but when?		
<b>3 Addressing with IPv6</b>		
3.1 IPv6 Addresses		
3.1.1 Address Types		
3.1.2 End Device IDs		
3.2 Global Unicast Addresses		
3.2.1 IPv6 Address Request		
3.2.2 Control		
3.3 IPv6 Address Design		
3.3.1 Site Concept		
3.3.2 Concept of Use		
3.3.3 Size of the Network Sections		
3.3.4 Subgroups		
3.4 Unique Local Unicast		
3.4.1 Setup of Unique Local Addresses		
3.4.2 Advantages and Disadvantages of Private Addresses		
3.5 The Benefit of Anycast		
3.6 Multicast Addresses		
3.7 Neighbor Solicitation		
3.8 Address Assignment		
3.8.1 Static		
3.8.2 Stateless Auto-configuration		
3.8.3 Stateful with DHCPv6		
<b>4 The Dual Stack Variant</b>		
4.1 Two Parallel Networks		
4.1.1 Advantages and Disadvantages of Dual Stack		
4.1.2 DNS Makes It Possible		
4.1.3 What is preferred?		
4.2 End Devices and IPv6		
4.2.1 Microsoft		
4.2.2 Linux		
4.2.3 Mac OS X		
4.2.4 IPv6 and Virtualization		
4.3 Routers and IPv6		
4.3.1 Ready for IPv6 or not?		
4.3.2 Migrating the Routing		
4.4 IPv6 during Dial-In		
4.4.1 Configuration of the WAN End		
4.4.2 Configuration of the LAN End		
<b>5 Tunneling Variants</b>		
5.1 Static Tunnels—6in4		
5.1.1 Tunnel Setup		
5.1.2 Routing through the Tunnels		
5.1.3 IPv6 in GRE		
5.2 Dynamic Tunnels—6to4		
5.2.1 Address Format of 6to4		
5.2.2 Communication with the IPv6 Internet		
5.3 Teredo—Dial-in into the IPv6 Internet		
5.3.1 Problems with Tunnels and NAT		
5.3.2 The Solution of Teredo		
5.3.3 Communication between Teredo Clients		
5.4 Tunnel Broker		
5.4.1 Tunnel Broker—The Procedure		
5.4.2 Tasks of the Tunnel Broker		
5.4.3 Tunneling Protocols		
5.5 Intra-Site—ISATAP		
5.5.1 The ISATAP Address		
5.5.2 Communication with the IPv6 Internet		
<b>6 Provider Aspects of IPv6</b>		
6.1 Offering IPv6 to the Customer		
6.1.1 Native IPv6 Access		
6.1.2 MPLS and IPv6		
6.2 Multi-Homing of Customers		
6.3 Communication from IPv6 to IPv4		
6.3.1 NAT64		
6.3.2 DNS64		
6.4 Providing IPv4 Further on		
6.4.1 NAT444		
6.4.2 NAT464		
6.4.3 Dual Stack Lite		
<b>7 Adapting Applications</b>		
7.1 Changes in UDP and TCP		
7.2 DNS and IPv6		
7.2.1 Forward Lookup		
7.2.2 Reverse Lookup		
7.3 Network Management in IPv6 Networks		
7.4 Radius and IPv6		
7.5 IPv6 in Applications		
7.5.1 IPv6-Enabled Open Source Software		
7.5.2 IPv6 in Microsoft Networks		
<b>8 Basic Security Considerations</b>		
8.1 IPv4 and IPv6—Security in Comparison		
8.1.1 Differences between IPv4 and IPv6		
8.1.2 The Current Security Situation		
8.2 Vulnerable IPv6 Stacks		
8.3 Security Aspects of the IPv6 Header		
8.3.1 Extension Header Parsing		
8.3.2 Security Relevance of Extension Headers		
8.3.3 Filtering IPv6		
8.4 Testing Security—Tools for IPv6 Vulnerability Tests		
8.4.1 NMAP		
8.4.2 Nessus and OpenVAS		
8.4.3 Packet Generators		
8.4.4 The THC Tool Collection		
8.4.5 SI6 Tools		
<b>9 Security Aspects of IPv6 Addressing</b>		
9.1 Security Relevance of NAT		
9.2 Security Aspects of the Address Types		
9.2.1 EUI 64—Addresses Which Are Recognized		
9.2.2 Temporary Addresses		
9.2.3 ULA—Entirely Private		
9.3 Discovering IPv6 Addresses		
9.3.1 Passive Sniffing		
9.3.2 Multicast Enumeration		
9.3.3 Registration Query		
9.3.4 Scanning IPv6 Networks		
9.3.5 Guessing IPv6 Addresses		
9.3.6 DNS Reconnaissance		
<b>10 Security during Migration</b>		
10.1 IPv6 Latent Threats		
10.2 Dual Stack—Double Protection Required		
10.2.1 End Device Security from the Viewpoint of IPv6		
10.3 Questioning the Tunnel Security		
10.3.1 Protecting a Configured Tunnel		
10.3.2 ACLs for Dynamic Tunnels		
10.4 Encrypting the Tunnel Traffic		
<b>11 IPv6 and First Hop Security</b>		
11.1 Neighbor Discovery Attacks		
11.1.1 NDP Exhaustion Attack		
11.1.2 Neighbor Advertisement Flooding		
11.1.3 NDP Spoofing		
11.2 SLAAC Attacks		
11.2.1 Rogue Router		
11.2.2 Man-in-the-Middle with RAs		
11.2.3 Faked Default Gateway		
11.2.4 RA Flooding		
11.3 DHCPv6 Attacks		
11.3.1 DHCPv6 Starvation		
11.3.2 Rogue DHCPv6 Server		
11.4 ICMPv6 Attacks		
11.4.1 Amplification Attack		
11.4.2 Redirect Attacks		
11.4.3 DoS_New_IPv6		
11.5 Security Measures		
11.5.1 SEND		
11.5.2 ACLs for Protection		
11.5.3 RA Guard		
11.5.4 DHCPv6 Guard/Shield		
11.5.5 NDP Spoofing		
<b>12 Security in IPv6 Networks</b>		
12.1 Protecting Routers in IPv6 Networks		
12.1.1 Configuration of IPv6 ACLs		
12.1.2 Filtering ICMPv6		
12.1.3 Protecting Routing Protocols		
12.1.4 Preventing IP Spoofing		
12.2 Adapting Firewalls		
12.2.1 Testing the IPv6-Capability		
12.2.2 Adapt Objects		
12.2.3 Completing Sets of Rules		
12.2.4 Bogon Filtering		
12.3 Radius and IPv6		
12.3.1 Testing the IPv6-Capability		
12.3.2 RADIUS IPv6 Attributes		
12.4 IPS in IPv6 Networks		
12.5 Proxies in IPv6 Networks		
12.6 IPsec in IPv6 Networks		
12.6.1 Host-to-Host Encryption		
12.6.2 IPv6 VPNs		
12.6.3 IPv6 VPN with IPsec		
12.6.4 IPsec RAS VPNs and IPv6		
<b>A List of Abbreviations</b>		



### ExperTech GmbH

Waldstraße 94 • 63128 Dietzenbach • Telefon: +49 6074 4868-0 • Fax: +49 6074 4868-109  
info@expertech.de • www.expertech.de

