

PowerPackage IPv6

Adressierung, Routing, Interworking, Security

Die IPv6-Einführung in einem Unternehmensnetzwerk ist sehr facettenreich. Sie setzt ein detailliertes Verständnis der Änderungen und Neuerungen gegenüber IPv4 voraus. Aufbauend auf diesem Wissen kann eine Planung und Umsetzung der Migration erfolgen. Dabei sollten stets auch Sicherheitsaspekte bedacht werden.

Von der Funktionsweise des IPv6-Protokolls über Security-Aspekte bis hin zu sinnvollen Migrationsstrategien erfahren Sie in diesem BootCamp alles, was Sie zum erfolgreichen Einsatz dieser Technologie wissen müssen. Mit diesem Wissen werden Sie in die Lage versetzt, eine strukturierte und sicher durchdachte Migration zu IPv6 zu realisieren.

Kursinhalt

- Die Neuerungen in IPv6
- IPv6 Header, Extension Header und der Aufbau von IPv6-Adressen
- Die IPv6-Kommunikation und deren Schwächen
- Stateless und Stateful Autoconfiguration
- Planung der sicheren Migration von IPv4 auf IPv6
- IPv6 in Endgeräten, Routern und Firewalls
- Tunneln von IPv6 über IPv4
- Interworking von IPv6 mit IPv4 (NAT64 und DNS64)
- Routing und Netzwerkdienste (DNS, DHCP, RADIUS und SNMP) mit IPv6
- Applikationen: WWW, FTP und E-Mail mit IPv6
- Internet Access und ISP-Netze mit IPv6
- Enterprise-Netze und IPv6
- IPv6 in der Mobilfunkwelt
- Security und IPv6: Neue Angriffspunkte, Absicherung, Firewall und VPN

E-Book Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

Zielgruppe

Der Kurs eignet sich für Planer, Administratoren und Security-Beauftragte, die eine Einführung von IPv6 in einem Netzwerk durchführen sollen und mögliche Sicherheitsprobleme bereits im Vorfeld abschätzen wollen.

Voraussetzungen

Detaillierte Kenntnisse zu IPv4 sind für die erfolgreiche Teilnahme notwendig. Eine gute Vorbereitung ist der Besuch des Kurses TCP/IP.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/IP6B

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.	
Termine in Deutschland		5 Tage	CHF 2.635,-
Termine in Österreich		5 Tage	CHF 2.635,-
Termine in der Schweiz		5 Tage	CHF 3.150,-
Online Training		5 Tage	CHF 2.635,-
Termin/Kursort		Kurssprache Deutsch	
02.06.-06.06.25	Frankfurt	22.09.-26.09.25	Wien
02.06.-06.06.25	Online	20.10.-24.10.25	Frankfurt
30.06.-04.07.25	Hamburg	20.10.-24.10.25	Online
30.06.-04.07.25	Online	20.10.-24.10.25	Zürich
04.08.-08.08.25	München	17.11.-21.11.25	Berlin
04.08.-08.08.25	Online	17.11.-21.11.25	Hamburg
25.08.-29.08.25	Düsseldorf	17.11.-21.11.25	Online
25.08.-29.08.25	Online	15.12.-19.12.25	München
22.09.-26.09.25	Online	15.12.-19.12.25	Online

Stand 07.05.2025



Inhaltsverzeichnis

PowerPackage IPv6 – Adressierung, Routing, Interworking, Security

1	Motivation für IPv6	5.7.1	DHCPv6 – Varianten	8.4.3	Sicherheitsrelevanz der Erweiterungsheader
1.1	Die Motivation für IPv6	5.7.2	Stateless DHCPv6	8.4.4	Die Filterung von IPv6
1.2	Entwicklungen im Internet	5.7.3	Stateful DHCPv6	8.5	Die Sicherheit testen - Tools für IPv6 Vulnerability Tests
1.2.1	IPv4 Adressraum	5.7.4	Lifetime und Erneuerung von Adressen	8.5.1	NMAP
1.2.2	Größe der Routingtabellen	5.7.5	DHCPv6-Timing – ohne Server	8.5.2	Nessus und OpenVAS
1.2.3	Effizienz	5.7.6	DHCPv6 – Client- und Server-Identifizierer (DUID)	8.5.3	Paket-Generatoren
1.2.4	Komplexität durch Hilfsprotokolle	5.8	DHCPv6 Relay Agent	8.5.4	Die THC Toolsammlung
1.3	Mobilfunk	5.9	DHCPv6 Prefix Delegation	8.5.5	SIG Tools
1.3.1	Mobiles Internet	5.10	Die richtige Adressvergabe wählen		
1.4	Das Internet of Things (IoT)	5.11	IPv6 Adressdesign	9	IPv6-Adressierung aus Sicherheitsicht
1.4.1	IoT Zugangs-Technologien	5.11.1	IPv6 Plan für ein Campus Netzwerk	9.1	Sicherheitsrelevanz von NAT
1.5	Anforderungen an das neue IP	5.11.2	Adresskonzept VLAN Benennung	9.1.1	IPv6-IPv4 Network Prefix Translation (NAT66)
1.6	Vergleich IPv4 und IPv6			9.2	Sicherheitsbetrachtungen zu den Adressarten
1.7	Die IPv6 Einführung	6	IPv6 im Betrieb	9.2.1	EUI 64 – Großer Wiedererkennungswert
1.7.1	Die Einführung in Enterprise-Netzen	6.1	Parallelbetrieb IPv6 und IPv4	9.2.2	Temporäre Adressen
1.7.2	Der Mehrwert für Firmennetze	6.1.1	Vor- und Nachteile von Dual Stack	9.3	IPv6-Adressen auskundschaften
1.7.3	Widerstand gegen IPv6	6.1.2	DNS machts möglich	9.3.1	Passive Sniffing
2	Adressierung mit IPv6	6.1.3	Was wird bevorzugt?	9.3.2	Detect-New-IP6
2.1	IPv6 Adressen	6.1.4	Happy Eyeballs	9.3.3	Multicast Enumeration
2.2	Struktur einer IPv6 Adresse	6.2	Betriebssysteme und IPv6	9.3.4	Alive6
2.2.1	Bilden der Interface ID	6.2.1	Microsoft	9.3.5	Registrierungs-Abfrage
2.2.2	Privacy Extensions nach RFC 4941	6.2.2	Linux	9.3.6	IPv6 Netze scannen
2.3	IPv6 Gültigkeitsbereiche	6.2.3	Mac OS X	9.3.7	IPv6-Adressen erraten
2.4	Unicast Adressen	6.2.4	Android	9.3.8	DNS Reconnaissance
2.5	Global Unicast Adressen	6.2.5	iOS		
2.6	Link Local Adressen	6.3	Router und IPv6	10	IPv6 und First Hop Security
2.7	Unique Local Adressen	6.3.1	Hersteller	10.1	Neighbor-Discovery-Angriffe
2.7.1	Vor und Nachteile privater Adressen	6.3.2	Cisco Systems	10.1.1	Trust Models and Threats
2.8	Multicast Adressen	6.3.3	Juniper	10.1.2	NDP Spoofing
2.8.1	Bekannte Multicast Adressen	6.4	IPv6 und Virtualisierung	10.1.3	Neighbor Unreachability Detection (NUD)
2.8.2	Solicited-Node Multicast Adresse	6.5	Cloud Services	10.1.4	DoS_New_IP6
2.8.3	Präfix basierte Multicast Adressen	6.6	Routingprotokolle IPv6	10.1.5	NDP Exhaustion Attack
2.9	Anycast Adressen	6.6.1	Statische Routen	10.1.6	Neighbor Advertisement Flooding
2.10	Weitere Adresstypen	6.6.2	RIPng	10.2	SLAAC Angriffe
2.11	Die Vergabe der IPv6 Präfixe	6.6.3	OSPF und IS-IS	10.2.1	Rogue Router
2.11.1	Adressvergabe IANA-RIR	6.6.4	BGP-4	10.2.2	Man in the Middle mit RAS
2.11.2	Adressvergabe der RIRs – LIRs – Kunden	6.7	IPv6 beim Zugang	10.2.3	Faked Default Gateway
2.11.3	Kontrolle	6.7.1	IPv6 und PPP	10.2.4	RA Flooding
3	Der IPv6 – Header	6.7.2	Konfiguration der WAN-Seite	10.3	DHCPv6 Angriffe
3.1	Das Header-Format	6.7.3	Konfiguration der LAN-Seite	10.3.1	DHCPv6 Starvation
3.1.1	Version, Payload Length und Hop Limit	6.7.4	Adressierung interner Links	10.3.2	Rogue DHCPv6 Server
3.1.2	Traffic Class	7	Die Migration im Überblick	10.4	ICMPv6-Angriffe
3.2	Flow Label	7.1	Migrationsverfahren	10.4.1	Amplification Attack
3.2.1	RFC 6294: Route Caching und Load Sharing	7.1.1	Netze mit Dual Stack Nodes	10.4.2	Redirect-Angriffe
3.2.2	RFC 6294: Weitere Nutzung des Flow Labels	7.1.2	Native IPv6-Netze	10.5	ACLs zur Sicherung
3.3	Erweiterungen mit dem Next Header	7.2	Tunnel	10.5.1	Rogue Router ausgrenzen
3.3.1	Erweiterungen für die Router	7.2.1	IPv6 in IPv4 Tunneling	10.5.2	Rogue DHCP Server verhindern
3.3.2	Erweiterungen für die Endsysteme	7.2.2	Statische Tunnel – 6in4	10.5.3	RA Guard
3.3.3	Erweiterung IPsec	7.2.3	Tunnel bauen	10.5.4	DHCPv6 Guard/Shield
3.4	Mobile IPv6	7.2.4	Routing durch Tunnel	10.5.5	NDP Snooping
3.4.1	Mobile IPv6 Begriffe	7.2.5	IPv6 in GRE	10.5.6	NDP Inspection
4	Nachbarschaftsprozesse	7.2.6	Dynamische Tunnel – 6to4	10.6	SEND
4.1	ICMPv6	7.2.7	Adressformat bei 6to4	10.6.1	RAS mit SEND absichern
4.2	ICMPv6 Meldungen	7.3	Migrationsstrategien	10.6.2	SEND und Stateful Autoconfiguration
4.2.1	Typ 1: Destination Unreachable	7.3.1	Backbone First		
4.2.2	Typ 2: Packet to Big	7.3.2	Edges First	11	Sicherheit von IPv6-Netzen
4.2.3	Typ 3: Time Exceeded	7.4	Die Migration planen	11.1	Router in IPv6 Netzwerken sichern
4.2.4	Typ 4: Parameter Problem	7.4.1	Das Ziel festlegen	11.1.1	IPv6 ACLs aufsetzen
4.2.5	Typ 128/129: Echo Request und Reply	7.4.2	Den Ist-Zustand erfassen	11.1.2	Eingehender Verkehr
4.3	Neighbor Discovery	7.4.3	Inventarisierung und Auswertung	11.1.3	Adressen Filtern
4.4	Neighbor Unreachability Detection	7.4.4	Eine IPv6-Testumgebung	11.1.4	ICMPv6 filtern
4.5	Duplicate Address Detection	7.4.5	Abschluss der Tests	11.1.5	Sicherung der Routingprotokolle
4.6	Router Discovery	7.5	Umstellen – Aber wann?	11.1.6	Authentisierung bei Routing Protokollen
4.7	Multicast Listener Discovery	8	Grundlegende Sicherheitsüberlegungen	11.1.7	BGP-4 – Verwendung von Link Local Unicast
4.8	Redirect	8.1	Grundsätzliche Überlegungen	11.1.8	IP Spoofing verhindern
5	Adressvergabe mit IPv6	8.1.1	Sicherheitsmaßnahmen	11.2	Firewalls anpassen
5.1	Adressvergabe bei IPv6	8.1.2	Personal und Dienstleister	11.2.1	IPv6-Fähigkeit hinterfragen
5.2	Statische Adressvergabe	8.2	IPv4 und IPv6 – Sicherheit im Vergleich	11.2.2	Check Point
5.3	Router Advertisements deaktivieren?	8.2.1	Unterschiede zwischen IPv4 und IPv6	11.2.3	Cisco-ASA
5.4	Dynamische Adressvergabe	8.3	Die aktuelle Sicherheitslage	11.2.4	Palo Alto
5.5	Stateless Autoconfiguration (SLAAC)	8.3.1	Vulnerable IPv6 Stacks	11.2.5	Fortinet
5.5.1	Prozesse während SLAAC	8.3.2	Die Firewall	11.2.6	Juniper
5.6	IPv6 RDNSS Configuration	8.3.3	Intrusion Prevention System	11.2.7	Barracuda
5.7	DHCPv6	8.4	Der IPv6-Header aus Sicherheitsicht	11.2.8	Objekte anpassen
		8.4.1	Das Flow Label – Covert Channel	11.2.9	Regelwerke ergänzen
		8.4.2	Extension Header Parsing	11.2.10	Bogon Filtering

