PowerPackage IPv6

Adressierung, Routing, Interworking, Security

Dieses PowerPackage kombiniert die Inhalte der Kurse IPv6 und IPv6 und Security in einer Veranstaltung.

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 Sie erhalten das ausführliche deutschsprachige Unterlagenpaket aus der Reihe ExperTeach Networking – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

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.de/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**	**€ 2.395,-**
Termine in Österreich	**5 Tage**	**€ 2.395,-**
Termine in der Schweiz	**5 Tage**	**€ 3.150,-**
Online Training	**5 Tage**	**€ 2.395,-**

Termin/Kursort — Kurssprache Deutsch

08.07.-12.07.24	HY München	21.10.-25.10.24	HY Online
08.07.-12.07.24	HY Online	21.10.-25.10.24	Zürich
16.09.-20.09.24	Berlin	18.11.-22.11.24	HY Düsseldorf
16.09.-20.09.24	HY Hamburg	18.11.-22.11.24	HY Online
16.09.-20.09.24	HY Online	16.12.-20.12.24	HY Online
21.10.-25.10.24	HY Frankfurt	16.12.-20.12.24	HY Wien

Stand 23.04.2024

Inhaltsverzeichnis

PowerPackage IPv6 – Adressierung, Routing, Interworking, Security

1 Motivation für IPv6
1.1 Die Motivation für IPv6
1.2 Entwicklungen im Internet
1.2.1 IPv4 Adressraum
1.2.2 Größe der Routingtabellen
1.2.3 Effizienz
1.2.4 Komplexität durch Hilfsprotokolle
1.3 Mobilfunk
1.3.1 Mobiles Internet
1.4 Das Internet of Things (IoT)
1.4.1 IoT Zugangs-Technologien
1.5 Anforderungen an das neue IP
1.6 Vergleich IPv4 und IPv6
1.7 Die IPv6 Einführung
1.7.1 Die Einführung in Enterprise-Netzen
1.7.2 Der Mehrwert für Firmennetze
1.7.3 Widerstand gegen IPv6

2 Adressierung mit IPv6
2.1 IPv6 Adressen
2.2 Struktur einer IPv6 Adresse
2.2.1 Bilden der Interface ID
2.2.2 Privacy Extensions nach RFC 4941
2.3 IPv6 Gültigkeitsbereiche
2.4 Unicast Adressen
2.5 Global Unicast Adressen
2.6 Link Local Adressen
2.7 Unique Local Adressen
2.7.1 Vor und Nachteile privater Adressen
2.8 Multicast Adressen
2.8.1 Bekannte Multicast Adressen
2.8.2 Solicited-Node Multicast Adresse
2.8.3 Präfix basierte Multicast Adressen
2.9 Anycast Adressen
2.10 Weitere Adresstypen
2.11 Die Vergabe der IPv6 Präfixe
2.11.1 Adressvergabe IANA-RIR
2.11.2 Adressvergabe der RIRs – LIRs – Kunden
2.11.3 Kontrolle

3 Der IPv6 – Header
3.1 Das Header-Format
3.1.1 Version, Payload Length und Hop Limit
3.1.2 Traffic Class
3.2 Flow Label
3.2.1 RFC 6294: Route Caching und Load Sharing
3.2.2 RFC 6294: Weitere Nutzung des Flow Labels
3.3 Erweiterungen mit dem Next Header
3.3.1 Erweiterungen für die Router
3.3.2 Erweiterungen für die Endsysteme
3.3.3 Erweiterung IPsec
3.4 Mobile IPv6
3.4.1 Mobile IPv6 Begriffe

4 Nachbarschaftsprozesse
4.1 ICMPv6
4.2 ICMPv6 Meldungen
4.2.1 Typ 1: Destination Unreachable
4.2.2 Typ 2: Packet to Big
4.2.3 Typ 3: Time Exceeded
4.2.4 Typ 4: Parameter Problem
4.2.5 Typ 128/129: Echo Request und Reply
4.3 Neighbor Discovery
4.4 Neighbor Unreachability Detection
4.5 Duplicate Address Detection
4.6 Router Discovery
4.7 Multicast Listener Discovery
4.8 Redirect

5 Adressvergabe mit IPv6
5.1 Adressvergabe bei IPv6
5.2 Statische Adressvergabe
5.3 Router Advertisements deaktivieren?
5.4 Dynamische Adressvergabe
5.5 Stateless Autoconfiguration (SLAAC)
5.5.1 Prozesse während SLAAC
5.6 IPv6 RDNSS Configuration
5.7 DHCPv6
5.7.1 DHCPv6 – Varianten
5.7.2 Stateless DHCPv6
5.7.3 Stateful DHCPv6
5.7.4 Lifetime und Erneuerung von Adressen
5.7.5 DHCPv6-Timing – ohne Server
5.7.6 DHCPv6 – Client- und Server-Identifier (DUID)
5.8 DHCPv6 Relay Agent
5.9 DHCPv6 Prefix Delegation
5.10 Die richtige Adressvergabe wählen
5.11 IPv6 Adressdesign
5.11.1 IPv6 Plan für ein Campus Netzwerk
5.11.2 Adresskonzept VLAN Benennung

6 IPv6 im Betrieb
6.1 Parallelbetrieb IPv6 und IPv4
6.1.1 Vor- und Nachteile von Dual Stack
6.1.2 DNS machts möglich
6.1.3 Was wird bevorzugt?
6.1.4 Happy Eyeballs
6.2 Betriebssysteme und IPv6
6.2.1 Microsoft
6.2.2 Linux
6.2.3 Mac OS X
6.2.4 Android
6.2.5 iOS
6.3 Router und IPv6
6.3.1 Hersteller
6.3.2 Cisco Systems
6.3.3 Juniper
6.4 IPv6 und Virtualisierung
6.5 Cloud Services
6.6 Routingprotokolle IPv6
6.6.1 Statische Routen
6.6.2 RIPng
6.6.3 OSPF und IS-IS
6.6.4 BGP-4
6.7 IPv6 beim Zugang
6.7.1 IPv6 und PPP
6.7.2 Konfiguration der WAN-Seite
6.7.3 Konfiguration der LAN-Seite
6.7.4 Adressierung interner Links

7 Die Migration im Überblick
7.1 Migrationsverfahren
7.1.1 Netze mit Dual Stack Nodes
7.1.2 Native IPv6-Netze
7.2 Tunnel
7.2.1 IPv6 in IPv4 Tunneling
7.2.2 Statische Tunnel – 6in4
7.2.3 Tunnel bauen
7.2.4 Routing durch Tunnel
7.2.5 IPv6 in GRE
7.2.6 Dynamische Tunnel – 6to4
7.2.7 Adressformat bei 6to4
7.3 Migrationsstrategien
7.3.1 Backbone First
7.3.2 Edges First
7.4 Die Migration planen
7.4.1 Das Ziel festlegen
7.4.2 Den Ist-Zustand erfassen
7.4.3 Inventarisierung und Auswertung
7.4.4 Eine IPv6-Testumgebung
7.4.5 Abschluss der Tests
7.5 Umstellen – Aber wann?

8 Grundlegende Sicherheitsüberlegungen
8.1 Grundsätzliche Überlegungen
8.1.1 Sicherheitsmaßnahmen
8.1.2 Personal und Dienstleister
8.2 IPv4 und IPv6 – Sicherheit im Vergleich
8.2.1 Unterschiede zwischen IPv4 und IPv6
8.3 Die aktuelle Sicherheitslage
8.3.1 Vulnerable IPv6 Stacks
8.3.2 Die Firewall
8.3.3 Intrusion Prevention System
8.4 Der IPv6-Header aus Sicherheitssicht
8.4.1 Das Flow Label – Covert Channel
8.4.2 Extension Header Parsing
8.4.3 Sicherheitsrelevanz der Erweiterungsheader
8.4.4 Die Filterung von IPv6
8.5 Die Sicherheit testen - Tools für IPv6 Vulnerability Tests
8.5.1 NMAP
8.5.2 Nessus und OpenVAS
8.5.3 Paket-Generatoren
8.5.4 Die THC Toolsammlung
8.5.5 SI6 Tools

9 IPv6-Adressierung aus Sicherheitssicht
9.1 Sicherheitsrelevanz von NAT
9.1.1 IPv6-IPv6 Network Prefix Translation (NAT66)
9.2 Sicherheitsbetrachtungen zu den Adressarten
9.2.1 EUI 64 – Großer Wiedererkennungswert
9.2.2 Temporäre Adressen
9.3 IPv6-Adressen auskundschaften
9.3.1 Passive Sniffing
9.3.2 Detect-New-IP6
9.3.3 Multicast Enumeration
9.3.4 Alive6
9.3.5 Registrierungs-Abfrage
9.3.6 IPv6 Netze scannen
9.3.7 IPv6-Adressen erraten
9.3.8 DNS Reconnaissance

10 IPv6 und First Hop Security
10.1 Neighbor-Discovery-Angriffe
10.1.1 Trust Models and Threats
10.1.2 NDP Spoofing
10.1.3 Neighbor Unreachability Detection (NUD)
10.1.4 DoS_New_IP6
10.1.5 NDP Exhaustion Attack
10.1.6 Neighbor Advertisement Flooding
10.2 SLAAC Angriffe
10.2.1 Rogue Router
10.2.2 Man in the Middle mit RAs
10.2.3 Faked Default Gateway
10.2.4 RA Flooding
10.3 DHCPv6 Angriffe
10.3.1 DHCPv6 Starvation
10.3.2 Rogue DHCPv6 Server
10.4 ICMPv6-Angriffe
10.4.1 Amplification Attack
10.4.2 Redirect-Angriffe
10.5 ACLs zur Sicherung
10.5.1 Rogue Router ausgrenzen
10.5.2 Rogue DHCP Server verhindern
10.5.3 RA Guard
10.5.4 DHCPv6 Guard/Shield
10.5.5 NDP Snooping
10.5.6 NDP Inspection
10.6 SEND
10.6.1 RAs mit SEND absichern
10.6.2 SEND und Stateful Autoconfiguration

11 Sicherheit von IPv6-Netzen
11.1 Router in IPv6 Netzwerken sichern
11.1.1 IPv6 ACLs aufsetzen
11.1.2 Eingehender Verkehr
11.1.3 Adressen Filtern
11.1.4 ICMPv6 filtern
11.1.5 Sicherung der Routingprotokolle
11.1.6 Authentisierung bei Routing Protokollen
11.1.7 BGP-4 – Verwendung von Link Local Unicasts
11.1.8 IP Spoofing verhindern
11.2 Firewalls anpassen
11.2.1 IPv6-Fähigkeit hinterfragen
11.2.2 Check Point
11.2.3 Cisco-ASA
11.2.4 Palo Alto
11.2.5 Fortinet
11.2.6 Juniper
11.2.7 Barracuda
11.2.8 Objekte anpassen
11.2.9 Regelwerke ergänzen
11.2.10 Bogon Filtering
11.3 Radius und IPv6
11.3.1 IPv6-Konnektivität herstellen

ExperTeach Gesellschaft für Netzwerkkompetenz mbH
Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach.de