

IPv6 BootCamp

Das Power-Programm

Die IPv6-Einführung in einem Unternehmensnetzwerk ist sehr facettenreich. 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.

Dieser IPv6-Komplettkurs beinhaltet sämtliche Themen der ExperTeach Networking Kurse IPv6, IPv6 im Enterprise Network und IPv6 und Security. 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

Jeder Teilnehmer erhält ausführliche Kursunterlagen aus der Reihe ExperTeach Networking in deutscher Sprache.

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.

Vormerkung und Buchung

Gerne merken wir für Sie für die Dauer von zwei Wochen kostenfrei und unverbindlich einen Kursplatz vor. Auf www.experteach.at können Sie unter *Anmeldung* bequem Vormerkung, Buchung und Hotelreservierung vornehmen. Oder rufen Sie uns einfach an unter 06074-4868-0.

Für geschlossene Teilnehmergruppen modifizieren wir diesen Kursinhalt gerne entsprechend Ihren Anforderungen. Bitte sprechen Sie uns an!



Auf Wunsch senden wir Ihnen gerne unseren kompletten Katalog zu, der Sie über alle Trainings und andere Dienstleistungen informiert.

5 Tage

€2.595,00 zzgl. MwSt.

Termin/Kursort

21.05.-25.05.12	Frankfurt	22.10.-26.10.12	München
18.06.-22.06.12	Düsseldorf	22.10.-26.10.12	Stuttgart
23.07.-27.07.12	München	19.11.-23.11.12	Frankfurt
23.07.-27.07.12	Wien	19.11.-23.11.12	Zürich
27.08.-31.08.12	Frankfurt	17.12.-21.12.12	Düsseldorf
24.09.-28.09.12	Berlin	21.01.-25.01.13	München
24.09.-28.09.12	Hamburg	18.02.-22.02.13	Frankfurt

Aktuelle Informationen finden Sie auf www.experteach.at IP6B





IPv6 BootCamp – Das Power-Programm

1 Die Motivation	3.2.5 IPv6 und Virtualisierung	8.2 EUI 64 – Adressen mit Wiedererkennungswert
1.1 Schwachstellen von IPv4	3.3 Router und IPv6	8.2.1 Sicherheit durch Privacy Extensions
1.1.1 Effizienz	3.3.1 IPv6 ready oder nicht	8.2.2 Sicherheitsrelevanz von NAT
1.1.2 Adressraum	3.3.2 Das Routing migrieren	8.3 ICMPv6 aus Sicherheitssicht
1.1.3 Größe der Routingtabellen	3.4 IPv6 bei der Einwahl	8.3.1 NDP-Angriffe
1.1.4 Komplexität durch Hilfsprotokolle	3.4.1 Konfiguration der WAN-Seite	8.3.2 SEND
1.2 Anforderungen an das neue IP	3.4.2 Konfiguration der LAN-Seite	8.3.3 Router Advertisements
1.2.1 Was war mit IPv5?		8.3.4 Weitere ICMP-Angriffe
1.2.2 Die RFCs		8.3.5 Die Filterung von ICMPv6
1.3 Das Header-Format	4 Tunnelvarianten	8.4 Sicherheit von DHCPv6
1.3.1 Version, Payload Length und Hop Limit	4.1 Statische Tunnel – 6in4	
1.3.2 Traffic Class	4.1.1 Tunnel bauen	
1.3.3 Flow Label	4.1.2 Durch die Tunnel routen	
1.3.4 Erweiterungen mit dem Next Header	4.1.3 IPv6 in GRE	
1.3.5 Erweiterungen für die Router	4.2 Dynamische Tunnel – 6to4	
1.3.6 Erweiterungen für die Endsysteme	4.2.1 Adressformat bei 6to4	
1.3.7 Der Nutzen für einen ISP	4.2.2 Kommunikation mit dem IPv6-Internet	
1.3.8 Der Mehrwert für Firmennetze	4.3 Teredo – Einwahl in das IPv6-Internet	
1.3.9 IPv6 zu Hause – Warum?	4.3.1 Probleme mit Tunneln und NAT	
1.3.10 Gründe für IPv6 in Mobilfunknetzen	4.3.2 Die Lösung von Teredo	
1.3.11 Mobile IPv6	4.3.3 Kommunikation zwischen Teredo Clients	
1.4 Migrationsverfahren	4.4 Tunnel Broker	
1.4.1 Netze mit Dual Stack Nodes	4.4.1 Tunnel Broker – Der Ablauf	
1.4.2 Native IPv6-Netze	4.4.2 Aufgaben des Tunnel Brokers	
1.4.3 Tunnel	4.4.3 Tunnelprotokolle	
1.5 Migrationsstrategien	4.5 In einer Site – ISATAP	
1.5.1 Backbone First	4.5.1 Die ISATAP-Adresse	
1.5.2 Edges First	4.5.2 Kommunikation mit dem IPv6-Internet	
1.6 Die Migration planen		
1.6.1 Das Ziel festlegen	5 Provideraspekte zu IPv6	
1.6.2 Den Ist-Zustand erfassen	5.1 Dem Kunden IPv6 bieten	
1.6.3 Inventarisierung und Auswertung	5.1.1 Der native IPv6 Zugang	
1.6.4 Eine IPv6-Testumgebung	5.1.2 MPLS und IPv6	
1.7 Umstellen – Aber wann?	5.2 Multihoming von Kunden	
	5.3 Kommunikation IPv6 zu IPv4	
2 Adressierung mit IPv6	5.3.1 NAT64	
2.1 Die IPv6-Adressen	5.3.2 DNS64	
2.1.1 Adresstypen	5.4 Weiterhin IPv4 ermöglichen	
2.2 Global Unicast Adressen	5.4.1 NAT444	
2.2.1 Die IPv6-Adressanforderung	5.4.2 NAT464	
2.2.2 Kontrolle	5.4.3 Dual Stack Lite	
2.3 IPv6-Adressdesign		
2.3.1 Standortkonzept	6 Applikationen anpassen	
2.3.2 Nutzungskonzept	6.1 Änderungen bei UDP und TCP	
2.3.3 Größe der Netzbereiche	6.2 DNS und IPv6	
2.3.4 Untergruppen	6.2.1 Forward Lookup	
2.4 Die Endgeräte-Kennung	6.2.2 Reverse Lookup	
2.4.1 Aufbau von Unique-Local-Adressen	6.3 Network Management in IPv6-Netzen	
2.4.2 Vor- und Nachteile privater Adressen	6.4 Radius und IPv6	
2.4.3 Multicast-Adressen	6.5 IPv6 in der Anwendung	
2.5 Der Nutzen von Anycast	6.5.1 IPv6 Enabled OpenSource Software	
2.6 Adresszuweisung	6.5.2 IPv6 in Microsoft-Netzen	
2.6.1 Statisch		
2.6.2 Stateless Autoconfiguration	7 Grundlegende Sicherheitsüberlegungen	
2.6.3 Stateful mit DHCPv6	7.1 IPv4 und IPv6 – Sicherheit im Vergleich	
3 Die Dual Stack Variante	7.2 Derzeitiges Angriffspotential	
3.1 Zwei parallele Netze	7.2.1 Informationsbeschaffung	
3.1.1 Vor- und Nachteile von Dual Stack	7.2.2 IPv6 Netze auskundschaften	
3.1.2 DNS machts möglich	7.2.3 Layer 3 und Layer 4 Spoofing	
3.1.3 Was wird bevorzugt?	7.2.4 Mangelnde Applikationssicherheit	
3.2 Endgeräte und IPv6	7.3 Die Sicherheit testen - Tools für IPv6 Vulnerability Tests	
3.2.1 Microsoft		
3.2.2 Linux	8 IPv6 Sicherheit von Protokollen und Abläufen	
3.2.3 Sun Solaris	8.1 IPv6 – Das Protokoll und seine Schwächen	
3.2.4 Mac OS X	8.1.1 Schwächen des Headers	
	8.1.2 Schwächen der Erweiterungsheader	
	8.1.3 Multicast Angriffe	
	8.2 EUI 64 – Adressen mit Wiedererkennungswert	
	8.2.1 Sicherheit durch Privacy Extensions	
	8.2.2 Sicherheitsrelevanz von NAT	
	8.3 ICMPv6 aus Sicherheitssicht	
	8.3.1 NDP-Angriffe	
	8.3.2 SEND	
	8.3.3 Router Advertisements	
	8.3.4 Weitere ICMP-Angriffe	
	8.3.5 Die Filterung von ICMPv6	
	8.4 Sicherheit von DHCPv6	
	9 Sicherheit von Geräten und Netzen	
	9.1 IPv6 in Endgeräten	
	9.1.1 Microsoft	
	9.1.2 IPv6-Sicherheit im Linux-Umfeld	
	9.1.3 Sun Solaris	
	9.1.4 Mac OS X	
	9.2 Router in IPv6 Netzwerken sichern	
	9.2.1 Access Listen aufsetzen	
	9.2.2 IPv6-Filter auf Perimeter Routern	
	9.3 Sicherung der Routingprotokolle	
	9.3.1 RIPng	
	9.3.2 OSPF	
	9.3.3 IS-IS	
	9.3.4 BGP-4	
	9.4 Firewalls, IDS und Proxies anpassen	
	9.4.1 Einige Hersteller — Cisco	
	9.4.2 Checkpoint	
	9.4.3 Palo Alto	
	9.4.4 Blue Coat	
	10 Sicherheit während der Migration	
	10.1 Problemfall unvorbereiteter Umstieg	
	10.1.1 IPv6 Latent Threats	
	10.1.2 Schutz gegen IPv6	
	10.2 Dual Stack – Zwei Welten	
	10.2.1 Schutz gegen Dual Stack-Angriffe	
	10.3 IPv4 zum Transport: Tunnelmechanismen	
	10.3.1 Wie sicher ist der Tunnel?	
	10.3.2 Statische Tunnel – 6in4	
	10.3.3 Dynamische Tunnel – 6to4	
	10.3.4 6RD	
	10.3.5 In einer Site – ISATAP	
	10.3.6 Teredo	
	10.3.7 Tunnel Broker	
	10.4 NAT64	
	10.4.1 DNS64	
	10.4.2 NAT64 – Sicherheitsprobleme	
	11 IPv6-Sicherheit mit IPsec	
	11.1 IPsec – Sicherheit für IP	
	11.1.1 IPsec und IPv6	
	11.1.2 IPsec – Die IPv6-Erweiterungsheader	
	11.2 Internet Key Exchange	
	11.2.1 Die Phasen von IKEv1	
	11.2.2 IKEv2 – Schneller und einfacher	
	11.3 IPsec in IPv6-Netzen	
	11.3.1 Host to Host	
	11.3.2 Gateway-to-Gateway	
	11.3.3 IPsec und dynamische Einwahl	
	A Abkürzungsverzeichnis	
	B Index	



ExperTeach GmbH Training Center Wien

Millennium Tower, 24. Etage
Handelskai 94-96 • A-1200 Wien
Telefon +43 66 43 45 39 64
info@experteach.at • www.experteach.at

© ExperTeach GmbH, alle Angaben ohne Gewähr

Stand 11.05.2012