

Wireshark & IPv6

IPv6-Netzwerke analysieren

IPv6 findet zunehmend Verbreitung – in Firmennetzwerken wie auch bei Providern. Selbst wenn Verantwortliche mit der Einführung von IPv6 noch zögern, ist IPv6 schon dabei, unsere Netzwerke zu erobern. Dieser Kurs gibt Netzwerktechnikern die Möglichkeit, IPv6 mit Hilfe von Wireshark zu entdecken und die wichtigsten Protokolle und Abläufe an praktischen Beispielen kennenzulernen. Der Kurs wiederholt kurz die Grundlagen von Wireshark und IPv6. Anhand von Trace Files lernen Teilnehmer IPv6 aus der Sicht von Wireshark kennen und über Decodes, Filter und Profile auszuwerten. Weitere Schwerpunkte des Kurses liegen in den praktischen Übungen im Live-Netz. Dabei werden die typischen Abläufe von IPv6 sowie häufige Fehler in IPv6-Netzwerken mit Wireshark analysiert.

Kursinhalt

- Grundlagen von Wireshark und IPv6 im Kurzüberblick
- Wireshark-Auswertungen für IPv6
- Wireshark Capture und Display Filter für IPv6
- IPv6-Adressierung
- Automatische Adresszuweisung mit SLAAC und DHCPv6
- Nachbarschaftsprozesse mit ICMPv6
- IPv6 Namensauflösung über DNS
- IPv6-Prozesse beim Booten von Clients
- IPv6 Tunnel – Statisch oder dynamisch
- Typische Fehlerszenarien bei IPv6-Netzwerken analysieren
- Praktische Übungen zur Analyse und Fehlersuche am Live-Netz und mittels Trace-Files

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

Zielgruppe

Dieser Workshop eignet sich für Netzwerker, die sich mit IPv6 während Planung, Implementierung und Betrieb beschäftigen und mit Hilfe von Wireshark diese Netze kennenlernen, auswerten, sichern und entstören möchten.

Voraussetzungen

Die Teilnehmer sollten über ein solides Wissen im Bereich TCP/IP sowie in der Bedienung und der Netzwerkanalyse mit Wireshark verfügen. Zudem sind grundlegende Kenntnisse zum IPv6-Protokoll erforderlich. Der vorherige Besuch der Kurse Wireshark Protokollanalyse – Praktischer Einsatz im Netzwerk sowie IPv6 – Adressierung, Routing und IPv4-Interworking sind sehr zu empfehlen.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/WIS6

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 der Schweiz	3 Tage CHF 2.850,-
Online Training	3 Tage CHF 2.415,-
Termine auf Anfrage	

Stand 27.02.2024



EXPERTeach



Inhaltsverzeichnis

Wireshark & IPv6 – IPv6-Netzwerke analysieren

- 1 Einführung**
 - 1.1 Motivation für IPv6
 - 1.1.1 Entwicklungen im Internet
 - 1.1.2 IPv4 Adressraum
 - 1.1.3 Header und Routingtabellen
 - 1.1.4 Komplexität durch Hilfsprotokolle
 - 1.1.5 Anforderungen an das neue IP
 - 1.2 Veränderungen mit IPv6
 - 1.2.1 Protokollheader
 - 1.3 IPv6-Adressen und Adresstypen
 - 1.3.1 Adressierungskonzept
 - 1.3.2 Struktur von IPv6-Adressen
 - 1.3.3 Bilden der Interface ID
 - 1.3.4 Gültigkeitsbereiche und Reichweiten
 - 1.3.5 Besondere Adressen
 - 1.3.6 Struktur von Unicast-Adressen
 - 1.4 Wireshark im Kurzüberblick
 - 1.4.1 Installation und Betrieb des Npcap-Treibers
 - 1.4.2 Messen in Ethernet Netzwerken
 - 1.4.3 Aufzeichnen mit Wireshark
 - 1.4.4 Mitschnittfilter – Capture Filter
 - 1.4.5 Einstellungen - Preferences
 - 1.4.6 Voreinstellungen und Profile
 - 1.4.7 Display Filter – Anzeigefilter
 - 1.5 Grundlagen der Netzwerkanalyse
 - 1.5.1 Messen im Switched Ethernet
 - 1.5.2 Port Monitoring – SPAN
 - 1.5.3 Test Access Point – TAP
 - 1.5.4 Wireshark auf dem Endgerät
- 2 IPv6 mit Wireshark auswerten**
 - 2.1 IPv6 in Wireshark finden und filtern
 - 2.1.1 IPv6 - Anzeigefilter (Display Filter)
 - 2.1.2 IPv6 – Capture Filter
 - 2.1.3 DNS für IPv6
 - 2.2 Wireshark lernt IPv6-Adressen
 - 2.2.1 Globale Unicast Adressen
 - 2.2.2 Link Local Unicast Adressen
 - 2.2.3 Die Interface ID
 - 2.2.4 Adressen im Router
 - 2.2.5 Adressen in Windows
 - 2.2.6 Adressen in Linux
 - 2.2.7 Multicast-Adressen
 - 2.3 ICMPv6
 - 2.3.1 ICMPv6 Echo und Echo Reply
 - 2.3.2 ICMPv6-Fehlermeldungen
 - 2.3.3 ICMPv6 Destination Unreachable
- 2.3.4** ICMPv6 Time Exceeded
- 2.4** Routingprotokolle am Beispiel von OSPFv3
 - 2.4.1 Die theoretischen Grundlagen
 - 2.4.2 OSPF und IPv6
 - 2.4.3 Hello-Prozedur
 - 2.4.4 Das Link-State-Protokoll
- 3 Nachbarschaftsprozesse**
 - 3.1 ICMPv6
 - 3.2 Neighbor Discovery
 - 3.3 Neighbor Unreachability Detection
 - 3.4 Duplicate Address Detection
 - 3.5 Router Discovery
 - 3.6 Multicast Listener Discovery
 - 3.7 Redirect
- 4 Adressvergabe mit IPv6**
 - 4.1 Adressvergabe bei IPv6
 - 4.1.1 Steuerung durch Router Advertisements
 - 4.1.2 Router Advertisements deaktivieren?
 - 4.2 Statische Konfiguration
 - 4.3 Stateless Autoconfiguration
 - 4.4 DHCPv6
 - 4.4.1 DHCPv6 – Varianten
 - 4.4.2 DHCPv6 – Abläufe im Überblick
 - 4.4.3 Stateless DHCPv6
 - 4.4.4 Stateful DHCPv6
 - 4.4.5 Lifetime und Erneuerung von Adressen
 - 4.4.6 DHCPv6 – Client- und Server-Identifizier (DUID)
 - 4.4.7 DHCPv6 Relay Agent
 - 4.4.8 DHCPv6 Prefix Delegation
- 5 Praxis und Fehlersuche**
 - 5.1 Praktische Fehlersuche im IPv6-Testnetz
 - 5.1.1 Problemstellungen im Testnetz
 - 5.1.2 Vorgehensweise
 - 5.2 Lab Übung – Adressierungsprobleme
 - 5.3 Lab Übung – Probleme mit der Verfügbarkeit
 - 5.4 MTU, Path-MTU, Fragmentierung
 - 5.4.1 MTU
 - 5.4.2 IPv6 Fragmentierung
 - 5.4.3 PMTU und PMTU-Discovery
 - 5.4.4 Anpassung der MSS
- 6 Tunnel und VPN**
 - 6.1 Migrationsverfahren und Parallelbetrieb
 - 6.1.1 Vor- und Nachteile von Dual Stack
 - 6.1.2 DNS als Bindeglied
 - 6.2 Tunnel und Tunnelverfahren
 - 6.2.1 Statische Tunnel – 6in4
 - 6.2.2 IPv6 in GRE
 - 6.2.3 Dynamische Tunnel – 6to4
 - 6.3 IPsec in IPv6-Netzen
 - 6.3.1 Host to Host
 - 6.3.2 Gateway-to-Gateway
 - 6.3.3 IPsec – Die IPv6-Erweiterungsheader
 - 6.3.4 Beispiel für IPsec in Wireshark
- A Wireshark & IPv6 – IPv6-Netzwerke analysieren Lab-Übungen und Lösungen**
 - A.1 Das Testnetz mit Labor CSRS
 - A.2 Das Testnetz mit Labor INIP
 - A.2.1 Anschluss von Vor-Ort Clients
 - A.2.2 Lab Übung – Aufzeichnen von IPv6 mit Wireshark
 - A.3 Lab Übungen – Kapitel 2
 - A.3.1 Lab Übung – ICMPv6
 - A.3.2 Lab Übungen – Kapitel 3
 - A.3.2.1 Lab Übung – Neighbor Discovery
 - A.3.2.2 Lab Übung – Neighbor Unreachability Detection
 - A.3.2.3 Lab Übung – Duplicate Address Detection
 - A.3.2.4 Lab Übung – Router Discovery
 - A.3.2.5 Lab Übung – Multicast Listener Discovery
 - A.4 Lab Übungen – Kapitel 4
 - A.4.1 Lab Übung – Statische Konfiguration
 - A.4.2 Lab Übung – Stateless Address Autoconfiguration
 - A.4.3 Lab Übung – Stateless DHCPv6
 - A.4.4 Lab Übung – Stateful DHCPv6
 - A.4.5 Lab Übung – DHCPv6 Relay Agent
 - A.5 Lab Übungen – Kapitel 5
 - A.5.1 Praktische Fehlersuche im IPv6-Testnetz
 - A.5.2 Lab Übung – Adressierungsprobleme
 - A.5.3 Lab Übung – Fragmentierung
 - A.5.4 Lab Übung – PMTU Discovery
 - A.5.5 Lab Übung – Black Hole
 - A.5.6 Lab Übung – MSS-Adjustment
 - A.5.7 Lösungen der Lab Übungen
 - A.5.7.1 Lösungen der Lab Übungen – Kapitel 1
 - A.5.7.2 Lösungen der Lab Übungen – Kapitel 2
 - A.5.7.3 Lösungen der Lab Übungen – Kapitel 3
 - A.5.7.4 Lösungen der Lab Übungen – Kapitel 4
 - A.5.7.5 Lösungen der Lab Übungen – Kapitel 5

