NETCOR

Troubleshooting Bundle

Kombination aus Allegro Network Multimeter und Wireshark Schulung

Das Allegro Network Multimeter liefert Ihnen vielfältige Analysen auf Schicht 2 bis 7. Diese liegen alle in Echtzeit mit Graphen vor, können aber auch rückwirkend für ein Zeitintervall dargestellt werden. Zudem werden pro IP und MAC viele Informationen korreliert dargestellt, wie z.B. der dekodierte DNS-, DHCP- oder HTTP-Hostname oder der SSL Common Name. Zudem kann in den Tabellen frei nach den korrelierten Informationen gefiltert werden. Alle Daten können für eine Analyse in Wireshark exportiert werden. Fit im Umgang mit Wireshark werden Sie durch die im Bundle enthaltene Wireshark Schulung.

Ein vertrauter Umgang mit dem Messgerät und eine effiziente Analyse sowie Auswertung der ermittelten Daten sind die Voraussetzung für eine schnelle Fehlerbehebung. Daher umfasst unser Bundle neben dem Allegro Packet Multimeter auch eine 2-tägige Online-Schulung, in der Sie in die Bedienung des Gerätes eingewiesen werden und die wichtigen Faktoren kennenlernen, die die Performance von Anwendungen in Netzwerken beeinflussen.
Dabei werden nicht nur theoretische Kenntnisse vermittelt, sondern auch viele praktische Übungen unter Einsatz des Wireshark Protokollanalysators durchgeführt. Die genauen Inhalte der Schulung erhalten Sie auf Seite 2.

	Allegro 200	Allegro 1000
In-Memory-Datenbank	2 GB	16 GB ECC
Speicherplatz	optional via USB	1 TB
Maximaler Durchsatz	2 GBit/s	20 GBit/s
Durchschnittlicher Durchsatz	2 GBit/s	10 GBit/s
Durchschnittliche Paketanzahl pro Sekunde	300.000	1.2 Millionen
Maximale parallele Verbindungen	200.000	1 Million
Monitoring Ports	2 x 1000BaseT	3x 1GBaseT 2x 10GBaseT 2x SFP+ Ports
Management Ports	1 x 1000BaseT via USB 3 Adapter 1 x WiFi 802.11n via USB 2 Adapter	1 x 1000BaseT out of band 1 x WiFi 802.11n via USB Adapter 1 x 1000BaseT IP KVM remote management
Anzahl Schulungstage Wireshark	2	2
Anzahl Teilnehmer	bis zu 4	bis zu 4
Online-Schulung	ja	ja
Bundlepreis (netto)	5.495,00 EUR	14.980,00 EUR

Die aufgeführten Preise sind gültig bis einschließlich 31.03.2021.

NETCOR GmbH - Innungsstr. 14 - 21244 Buchholz in der Nordheide - Telefon +49 4181 9092-01 - Telefax +49 4181 9092-345 - www.netcor.de - eMail netcor@netcor.de

Inhalte der Wireshark-Schulung

Dieses Training vermittelt systematische und methodische Ansätze der Fehleranalyse in Netzwerken. Die Teilnehmer lernen die wichtigsten Faktoren kennen, die die Performance von Anwendungen auf dem Netzwerk beeinflussen. Dabei lernen sie u.a. mit dem Wireshark Protokollanalysator Laufzeiten und Verzögerungszeiten von Diensten und Anwendungen zu erfassen und auswerten zu können. Die theoretischen Kenntnisse werden mit praktischen Übungen vertieft. Auf Basis von typischen Fehlerszenarien und bekannten Stolperfallen erlernen die Teilnehmer, wie sie Probleme gezielt diagnostizieren und beheben können.

Historische Entwicklung Wireshark

Einführung und Arbeitsweise des Netzwerkanalysators / Workflow Datenbeschaffung

- Datenquellen
  - Datenaufzeichnung in drahtgebundenen, 802.11-basierenden Netzen
  - Live Capture (Promiscuous Mode) und Live Capture Einstellungen
  - Offline Datenquellen
- Arbeiten mit Capture Filter und Display Filter
- Anpassen der lokalen Ordner

Philosophie, wann, warum und wie mit dem Wireshark messen?

- Gezielter Einsatz des Wireshark-Analyzers: wann soll man messen und wann nicht
- Anwendungsgebiet der Paketanalyse
- Systematischer Ablauf einer Fehlersuche

Paketanalyse in geswitchten und virtuellen Netzen

- SPAN/Mirror-Port, die Vor- und Nachteile
- Inline-Netzwerkmessung mittels TAPs: Breakout-, Aggregation- und Filter-TAPs
- Filter- und Aggregation (Matrix) Switches
- Zusammenfassen und Modifizieren von großen Trace-Dateien

Grundlagen IP

- Aufbau des IP Headers
- IP Adressierung / Subnetting
- IP Fragmentierung
- Einführung in QoS mittels DiffServ

Grundlagen TCP

- Aufbau des TCP Headers
- Funktionsweise TCP Receive Window and Congestion Window (Window Scaling)
- Überlaststeuerung/Staukontrolle
  - Algorithmus zur Überlaststeuerung
  - Slow Start und Congestion Avoidance
  - Window Scaling
  - Fast-Retransmit und Fast-Recovery
  - Selective ACKs (SACK)
- Die Auswirkung des Bandwidth-Delay-Product auf den Datendurchsatz

Pakete mit Wireshark aufzeichnen

- Wichtige Optionen für die Datenaufzeichnung
- Datenaufzeichnung mit mehr als einer Netzwerkkarte
- Langzeitnetzwerkanalyse mit Wireshark
- Datenaufzeichnung mit Wireshark in hochperformanten Netzen, wo sind hier die Grenzen?
- Wichtiges zu Checksum Offloading und CRC Fehler
- Wie funktioniert die SSL-Analyse?

Benutzeroberfläche des Wireshark-Analyzers individuell anpassen

- Fonts, Farben, Spalten, Aufteilung der Ansichten
- Standard Vorgaben, Verzeichnisse, Profile
- Namensauflösung
- Protokollanpassungen
- Navigation in Trace Dateien
- Richtig und effektiv markieren, sortieren der Pakete
- Zeitdarstellungen: Relativ vs. Delta
- Kolorierung der Konversationen
- Eigene Farbanpassungen und regeln der Kolorierung

Display Filter für die Fehlersuche effektiv nutzen

- Grundlagen der Filterdefinitionen:
  - Möglichkeiten um Filter zu definieren
  - Expressions
  - Expert Filtereinstellungen
  - Text on Wire Filter
  - Filter exportieren
- Was ist bei der Filterdefinition zu beachten
- Typische Fehler in der Filtererstellung

Wireshark Statistiken für die Analyse und Fehlersuche einsetzen

- Statistiken zu Verbindungen und Endpunkten
- Das Zeitwertediagramm IOStats
- Flowdiagramme und Ermitteln von Antwortzeiten
- Zeitanalyse für das CIFS-Protokoll
- Erweiterte Statistiken

Anwendung der Zeitwertegrafiken bei der Performanceanalyse

- Vorgehensweise der Performanceanalyse mit Zeitwertegrafiken
- Analyse und Ermitteln von schlechter Performance
- Welche Auswirkung haben Paketverluste auf die Performance und wie werden sie im Zeitwertediagramm dargestellt?

Netzwerkprobleme vs. Applikationsprobleme - Eingrenzen von Fehlersituationen

- Ursachen von schlechter Performance
  - Vorgehensweise bei der Problemaufnahme
  - Interpretieren der Informationen um Ursachen zu erkennen
  - Welche Auswirkung hat die Bandbreite resp. Retransmissions auf die Performance?
- Typische Netzwerkprobleme
- Paketverluste richtig interpretieren und verstehen
  - Den Verursacher ermitteln
  - Interpretation der Paketverluste im Wireshark
  - Hinweise zu Paketverlusten richtig verstehen
  - Das Duplex-Problem: nicht kleinzukriegen
- Ermitteln von Laufzeiten
  - Mit Wireshark die RTT Acked Data Transferzeit messen
  - Durchsatz vs. Laufzeit

NETCOR GmbH - Innungsstr. 14 - 21244 Buchholz in der Nordheide - Germany
Telefon +49 4181 9092-01 - Telefax +49 4181 9092-345 - www.netcor.de - eMail netcor@netcor.de