

Lehrveranstaltungshandbuch IN

Internetworking und Netzsicherheit

Version: 7 | Letzte Änderung: 29.04.2022 13:03 | Entwurf: 0 | Status: vom verantwortlichen Dozent freigegeben

– Allgemeine Informationen

Langname	Internetworking und Netzsicherheit
Anerkennende LModule	<u>IN_BaTIN</u> , <u>IN_BaET</u>
Verantwortlich	Prof. Dr. Andreas Grebe Professor Fakultät IME
Gültig ab	Sommersemester 2022
Niveau	Bachelor
Semester im Jahr	Sommersemester
Dauer	Semester
Stunden im Selbststudium	60
ECTS	5
Dozenten	Prof. Dr. Andreas Grebe Professor Fakultät IME

Literatur

J. Kurose, K. Ross: Computernetzwerke - Der Top-Down-Ansatz, Pearson Studium, 6. Auflage, 2014

A. Tanenbaum: Computernetzwerke, Pearson Studium, 5. Auflage 2012

G. Schäfer: Netzsicherheit: - Grundlagen & Protokolle - Mobile & drahtlose Kommunikation - Schutz von Kommunikationsinfrastrukturen, dpunkt.verlag, 2. Auflage 2014

W. Stallings: Foundations of Modern Networking, Pearson Education, 2016

J. Doherty: SDN and NFV Simplified, Pearson Education, 2016

J. Edelman: Network Programmability and Automation, O'Reilly 2018

Internet-Standardisierung: IETF Standards (RFCs), www.ietf.org

LAN-Standards: IEEE, ieeexplore.ieee.org (freier Zugang über TH Köln)

Telekommunikationsstandards: ITU-T Standards, www.itu.int

Web-Standardisierung: W3C Standards, www.w3c.org

Abschlussprüfung

Voraussetzungen

Kenntnisse und Kompetenzen des Moduls "Netze und Protokolle (NP)"
alternativ: Kenntnisse und Anwendung von grundlegenden Internetworking Techniken
Grundlegende Vernetzungstechniken
TCP/IP Protokollfamilie
ISO/OSI Schichtenmodellierung
IPv4/IPv6 Routing
Switchingtechniken
TCP/UDP
Transporttechniken
Anwendungsprotokolle
Umgang mit Netzelementen (Client, Server, Switch, Router)

Unterrichtssprache

deutsch

**separate
Abschlussprüfung**

Ja

Details

Die Studierenden weisen in einer abschließenden Prüfung (schriftlich, optional mündlich) summarisch ihre Kompetenzen nach. Die Prüfung umfasst folgende Teilbereiche, in denen sechs Taxonomiestufen (Wiedergeben, Verstehen, Anwenden, Analysieren, Synthetisieren, und Bewerten) enthalten sind.

1.) Sichere Beherrschung grundlegender Begrifflichkeiten, Konzepte und Techniken. Typische Aufgabenformen sind Multiple-Choice-Fragen, offene Fragen, Bewertung von Aussagen hinsichtlich ihrer Korrektheit
2.) Anwendung von Planungs- und Bewertungstechniken. Typische Aufgabenformen sind Planungsaufgaben von Netzen oder Teilsystemen.
3.) Prüfung von Lösungsvorschlägen auf Korrektheit, Identifikation von Fehlern in Aussagen oder vorgegebenen Netzen. Typische Aufgabenformen enthalten die Analyse vorgegebener Netzarchitekturen und Sysetmaussagen.

Mindeststandard

Erreichen der individuellen Mindestpunktzahl je Klausur, typisch 50% der maximalen Punktzahl.

Prüfungstyp

Klausur

– Vorlesung / Übungen

Lernziele

Zieltyp	Beschreibung
Kenntnisse	Grundlagen zum Aufbau von hierarchisch strukturierten Netzen, Unternehmensnetzen mit Redundanztechniken, Wireless LAN (WLAN), standortübergreifende Kommunikation, WAN-Techniken. Einführung in die Netzsicherheit mit Vertiefungen zu Angriffen, Sicherheitszielen, kryptographischen Verfahren, Verschlüsselung, Paketfilter, sichere Infrastrukturen, virtuelle private Netze. Einführung in verteiltes Netzmanagement und Servicequalitätstechniken. Techniken zur Netzvirtualisierung, Software-defined Networking und Netzautomatisierung.
Fertigkeiten	Studierende erhalten die Kompetenzen, mittelgroße, standortübergreifende Unternehmensnetze unter Einsatz geeigneter Tools analysieren, geeignete Architekturen auszuwählen und entsprechende Netze zu planen und zu implementieren. Sie benennen und identifizieren Gefährdungslagen für Unternehmensnetze. Geeignete Sicherheitsmechanismen sind auszuwählen, zu designen und zu implementieren. Aufgaben und Methoden softwaregesteuerter Netze inklusive und Virtualisierungen werden benannt und Mechanismen zur Netzautomatisierung geplant und umgesetzt.

Besondere Voraussetzungen

keine

Begleitmaterial

Onlinematerialien:
Vortragsfolien zur Vorlesung
Übungsaufgaben
Tutorials für Tools (u.a. Wireshark)
Materialsammlungen wie IOS-Befehlsliste, ASCII-Zeichentabelle
Optional:
Netzsimulatortool Cisco PacketTracer

Optional ist die Teilnahme an zwei Cisco Academy CCNA (Cisco Certified Network Associate) Modulen möglich. Die Inhalte der Module CCNA 2 und CCNA 3 stehen dann zusätzlich als Material zur Verfügung.

Separate Prüfung

Nein

Kenntnisse Auszug der Inhalte:
Hierarchische Netze, Redundanz,
STP, EtherChannel, FHRP, Single-
area und Multiarea OSPF, OSPF
Sicherheitstechniken, WLAN, WAN-
Anschluss, PPP, xDSL
Netzicherheit mit
Sicherheitszielen, kryptographische
Verfahren, Algorithmen, Paketfilter,
ACL, NAT, FireWall, DMZ, VPN,
IPsec
SNMP, Syslog, QoS – Quality-of-
Service
Software Defined Networking
(SDN), SDN Controller, Cloud,
Virtualisierung, Ansible, JSON,
YAML, REST API

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Vorlesung	2
Übungen (ganzer Kurs)	2
Übungen (geteilter Kurs)	0
Tutorium (freiwillig)	0

– Praktikum

Lernziele

Zieltyp	Beschreibung
Kenntnisse	Konzepte und Technologien für mittelgroße, standortübergreifende Unternehmensnetze benennen, strukturieren, einordnen. Netzanalysetechniken und Tools beherrschen, Netzdesignschritte kennen und Methoden zur Netzplanung kennen. Sicherheitsrelevante Netzaspekte identifizieren und geeignete Massnahmen zur Netzsicherheit und deren Umsetzung kennen. Aufgaben der Netzautomatisierung und Virtualisierung kennen und für geeignete Netzbereiche deren Umsetzung beherrschen.
Fertigkeiten	Planung, Implementierung und Analyse von VLAN-Architekturen, WLAN-Netzen, standortübergreifende VPN und Paketfilter-Firewall. Implementierung und Analyse von Netzmanagement mit SNMP und Syslog. Implementierung und Analyse von Netzautomatisierung an Netzelementen (u.a. Router, Switch, Host, SDN-Controller) über REST API mit Python-Scripting oder Ansible YAML Skripting.

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Praktikum	1
Tutorium (freiwillig)	0

Besondere Voraussetzungen

Bestandenes Praktikum ULP NP oder vergleichbare Kenntnisse

Begleitmaterial

Online verfügbare Materialien:
Selbstlernaufgaben
Praktikumsanleitung je Versuchstermin
Tutorials für Tools (u.a. Wireshark)
Materialsammlungen wie IOS-Befehlsliste, ASCII-Zeichentabelle RFC standards (www.ietf.org)
Optional:
Netzsimulatortool Cisco PacketTracer

Optional ist die Teilnahme an zwei Cisco Academy CCNA (Cisco Certified Network Associate) Moduln CCNA2 und CCNA3 möglich. Der erfolgreiche Abschluss der Modulbegleitenden Labs wird für das Praktikum anerkannt.

Separate Prüfung

Ja

Separate Prüfung

Prüfungstyp

praxisnahes Szenario bearbeiten (z.B. im Praktikum)

Details

Es sind mehrer
Praktikumstermine mit
verschiedenen
Aufgaben
wahrzunehmen.
Für jeden Termin sind
folgende Aufgaben zu
bearbeiten:
Selbstständige Lösung
der vorbereitenden
Selbstlernaufgaben
(Hausaufgabe).
Lösung der
Netzdesign-,
Implementierungs- und
Analyseaufgaben im
Kleinteam (typisch 2
Studierende), ggf. unter
Inanspruchnahme von
Hilfestellungen.
Optional ist die
Teilnahme an Cisco
Academy CCNA (Cisco
Certified Network
Associate) Moduln
möglich. Der
erfolgreiche Abschluss
von ausgewählten Labs
von CCNA 1 und CCNA
2 wird für das Praktikum
anerkannt.

Mindeststandard

Erfolgreiche Teilnahme
an allen
Praktikumsterminen.
Jeweils korrekte Lösung
aller Selbstlernaufgaben
und jeweils Abschluss
aller Aufgaben des
Praktikumtermins.