Akademie für
Lehrerfortbildung
und Personalführung

Digitale Transformation im Rahmen der Bildungsinitiative Networking

und

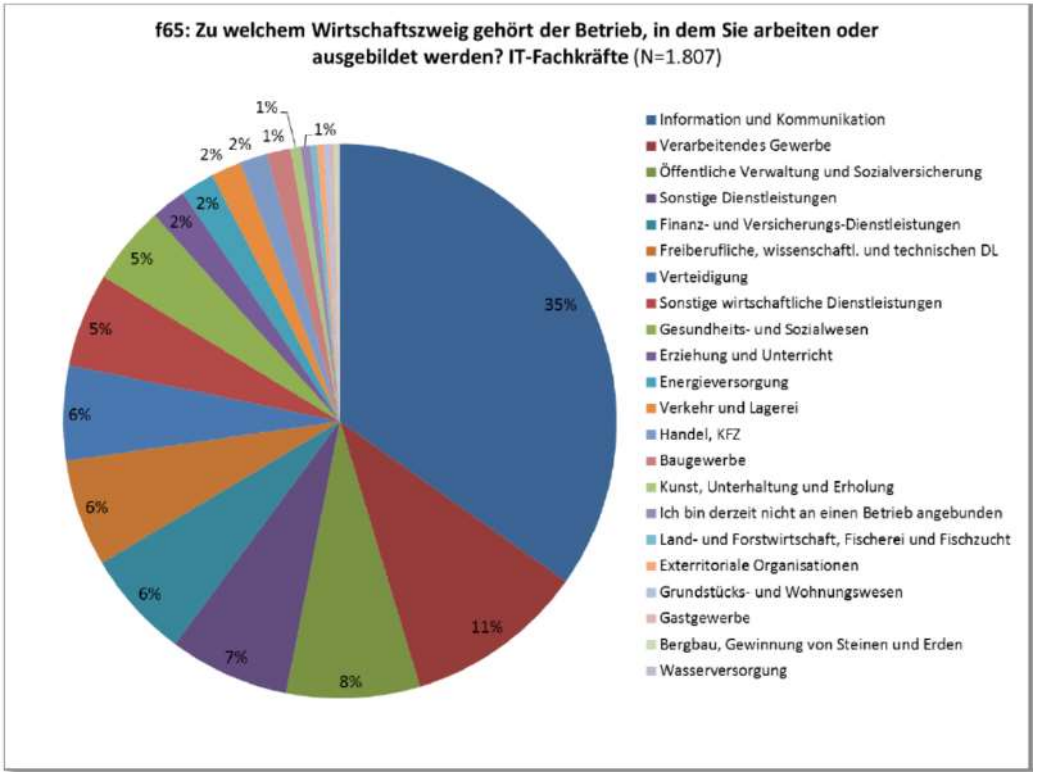
Regionalen Akademietag 2020 in Bayern

Fortbildungslehrgang Nr. 98/330

20.03.2020 Online statt in Würzburg - Klara-Oppenheimer-Schule

Datum 20.03.2020	Regionaler Akademietag, Live-Webkonferenz	Sprecher
08:45-09:00	Eintreffen der Workshop-Teilnehmer und Registrierung	
09:00-09:05	Eröffnung des regionalen Akademietages Bayern	Michael Lotter, ALP/~~(Wilhelm Ott)~~
09:05-09:45	Keynote: „A New Era in Networking“	Kristina Appelt, Manager System Engineering, Cisco
09:45-10:15	Transformation der IT-Ausbildung in Deutschland – Werkstattbericht aus dem Neuordnungsverfahren der	Carsten Johnson, Country Manager, Cisco
10:15-10:30	Pause	
10:30-11:40	Programm-Update & aktuelle Mitteilungen und Planungen der ASC/ITC (ALP) in Bayern	Michael Lotter, ALP
11:40-12:00	Packet Tracer 7.3 Demo	Eugene Morozov / Raquel Martinez, Technical Managers, Cisco
12:00	Verabschiedung	
Nachholung?	Automatisierung in der Systemintegration - über ETW-Workshops (Blended)	Almut Leykauff-Bothe, MMBBS Hannover
Nachholung?	IT Grundschutz und Schutzbedarfsanalyse – über BSI, 98/633B (Blended), 98/634B (Blended), ggf. 90 Minuten (Bericht eines IT-Grundschutzberater/-praktikers)	A.-M. Ruhland/Thomas Michalski steep GmbH/Inmodis GmbH
Nachholung?	Fachinformatiker im Umfeld cyber-physischer Systeme, 98/551A (M1.4 Präsenz), M1.2 (Herbst, Veranstalter Obb), M1.1 (Herbst), M1.3 (Januar, Veranstalter Mfr)	Michael Feike, Fürth III

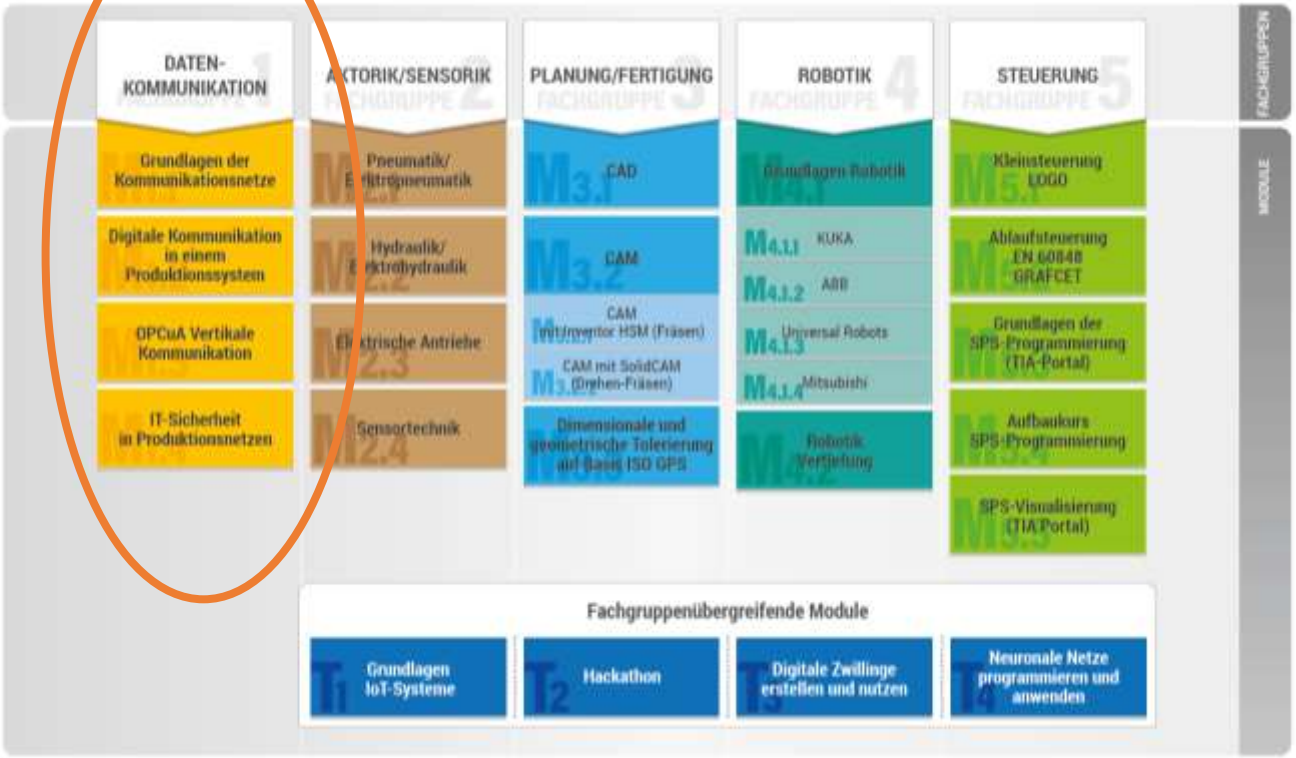
2016 BIBB- Abschlussbericht - Entwicklung der IT-Berufe



2016 - Orientierung an der bayme vbw-Studie

M+E Berufe und ausgewählte IT-Berufe im Industrie 4.0-Berufe-Atlas
(innerer Ring: Relevanz 5-10; äußerer Ring: Relevanz 2-5)

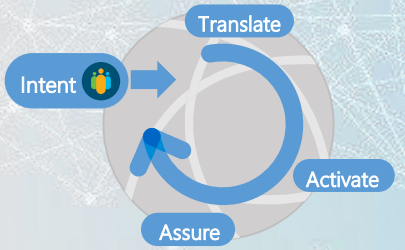
Fachinformatiker/-in –
„…. Dafür müssten die Produktionsprozesse jedoch in den Mittelpunkt des Berufes gestellt werden“


DATEN-KOMMUNIKATION
AKTORIK/SENSORIK
PLANUNG/FERTIGUNG
ROBOTIK
STEUERUNG
FACHGRUPPEN
MODULE
Grundlagen der Kommunikationsnetze
Digitale Kommunikation in einem Produktionssystem
OPCuA Vertikale Kommunikation
IT-Sicherheit in Produktionsnetzen
Pneumatik/ Elektropneumatik
Hydraulik/ Elektrohydraulik
Elektrische Antriebe
Sensortechnik
CAD
CAM
CAM Mitsubishi HSM (Fräsen)
CAM mit SolidCAM (Drehen-Fräsen)
Dimensionale und geometrische Tolerierung auf Basis ISO GPS
Grundlagen Robotik
KUKA
ABB
Universal Robots
Mitsubishi
Robotik Vertiefung
Kleinsteuerung LOGO
Ablaufsteuerung EN 60848 GRAFCET
Grundlagen der SPS-Programmierung (TIA-Portal)
Aufbaukurs SPS-Programmierung
SPS-Visualisierung (TIA Portal)
Fachgruppenübergreifende Module
Grundlagen IoT-Systeme
Hackathon
Digitale Zwillinge erstellen und nutzen
Neuronale Netze programmieren und anwenden

Treibende Veränderungen

Enabling IT to adapt fast and at scale

Cisco Leadership



Intent-Based Networks

Achieve business objectives using DevOps principles

Multi-Domain Networking

Unify and secure diverse networking domains

Programmable Networks

Drive automation, agility, and scale securely

Networking Academy

Program Updates

Cisco Networking Academy

Grundlage ist IPD Week im Dezember und Februar

Angepasst durch ALP OE 2.1.2

Michael Lotter

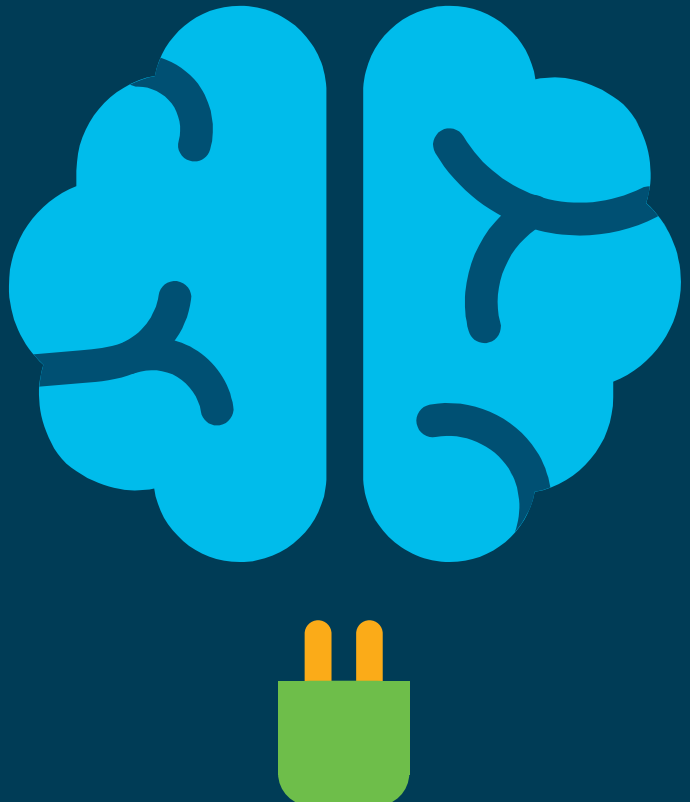
20.3.2020

NetAcad.com

Agenda

1. CCNAv7 Program Update
2. CCENT Exam Extension for Netacad
3. Laborausstattung
4. CCNP
5. Emerging Technologies Workshops
6. IoT Security v.1.1
7. Mitteilungen ASC/ITC Bayern
8. Emerging Technologie Workshops 1-3

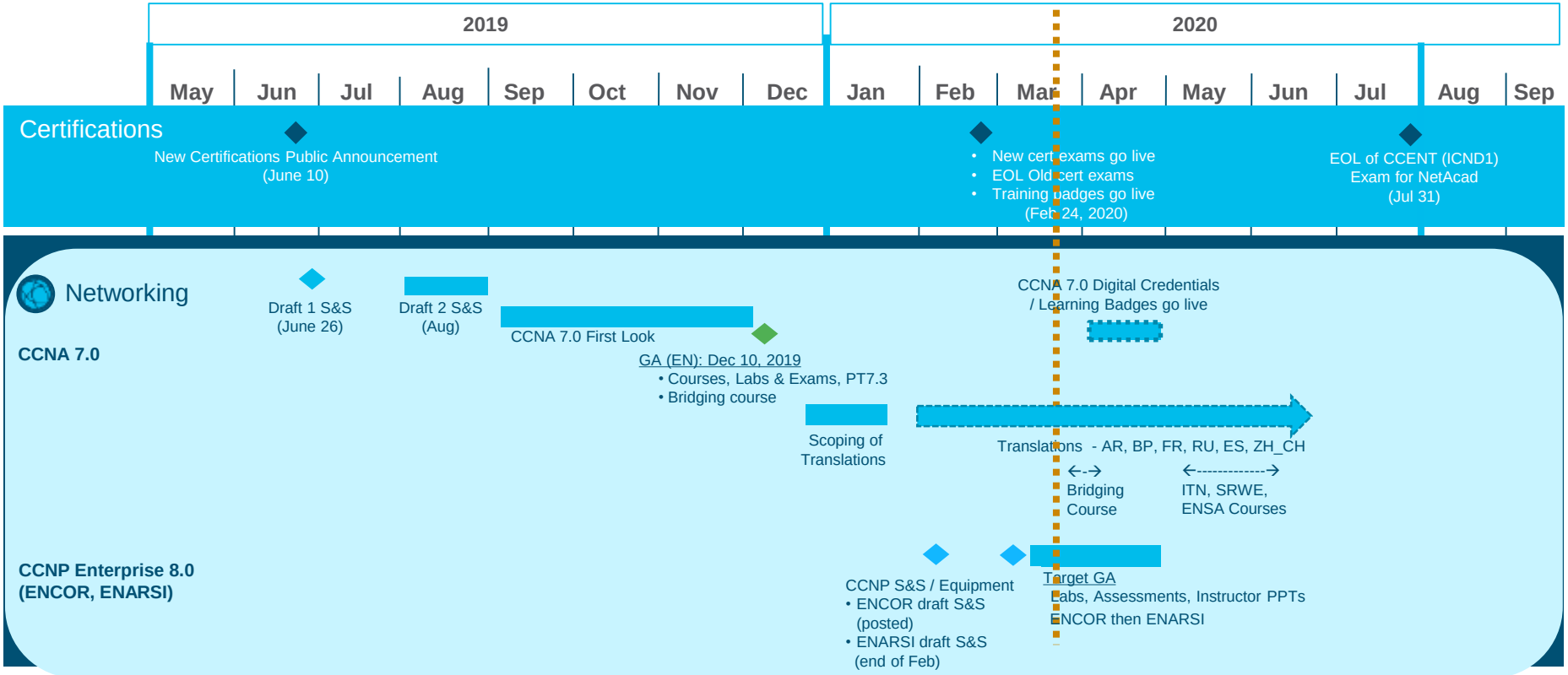
Updated Courses



CCNAv7 Program Update

1. Meilensteine & Zeitschiene
2. CCNA Vergleich (v6 zu v7)
3. Umstieg auf CCNA v7
4. Laborausstattung
5. CCNP

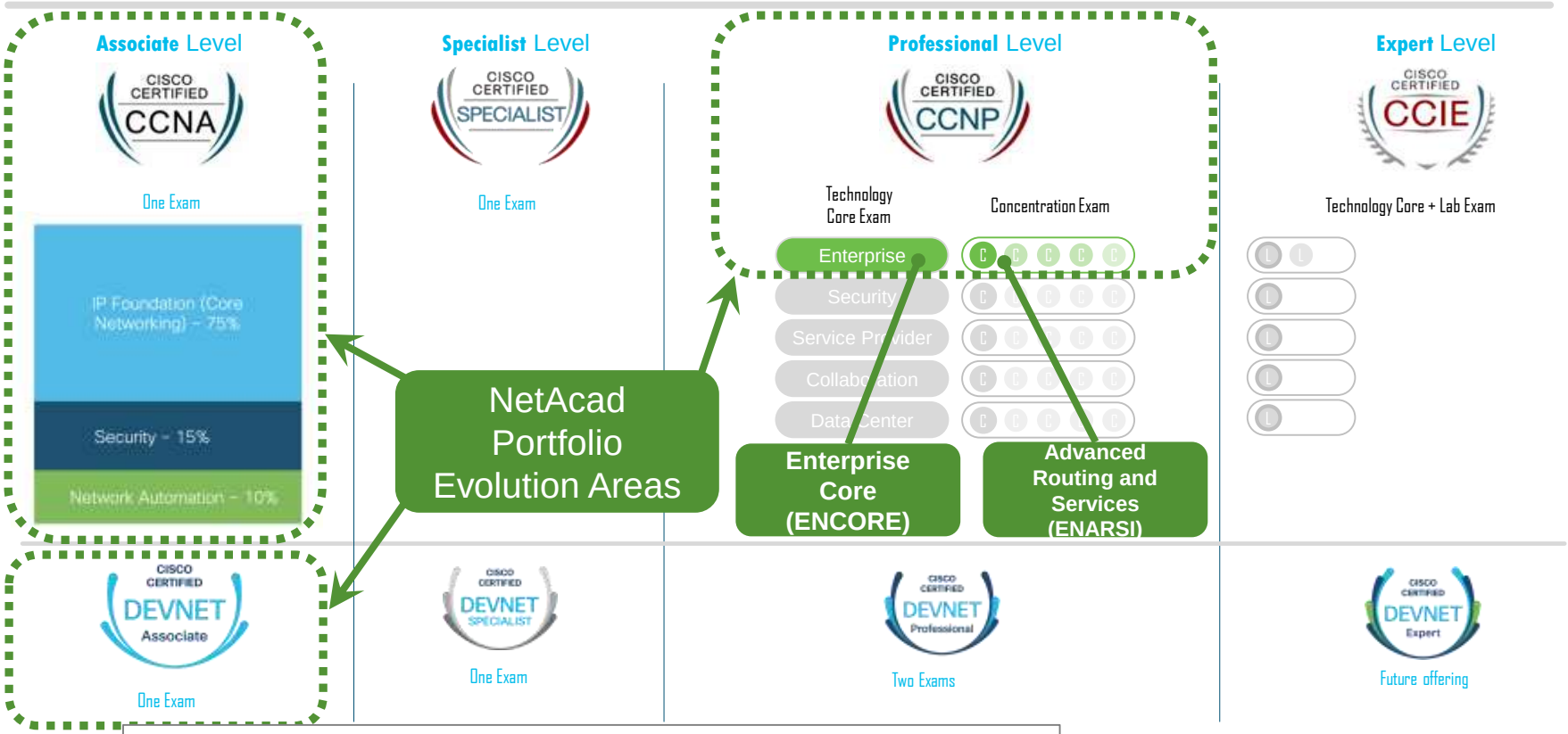
Key Milestones & Timeline



Networking Academy

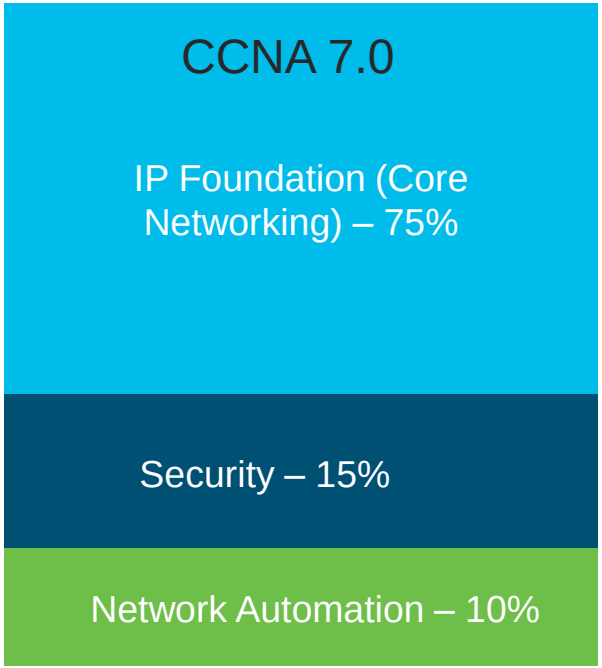
CCNA Vergleich (v6 to v7)

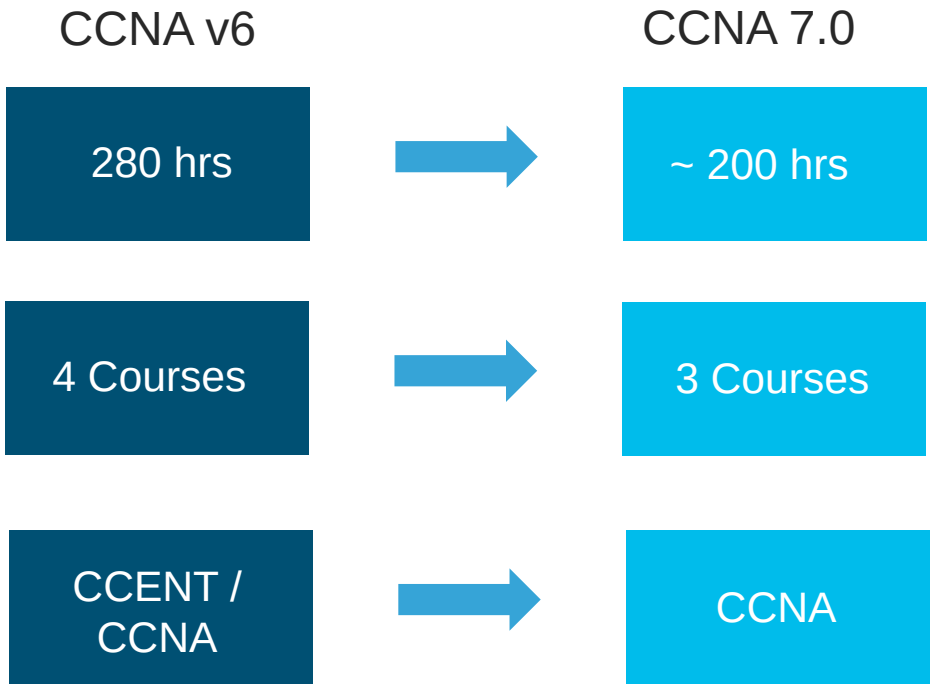
Cisco’s erweitertes Zertifizierungsangebot



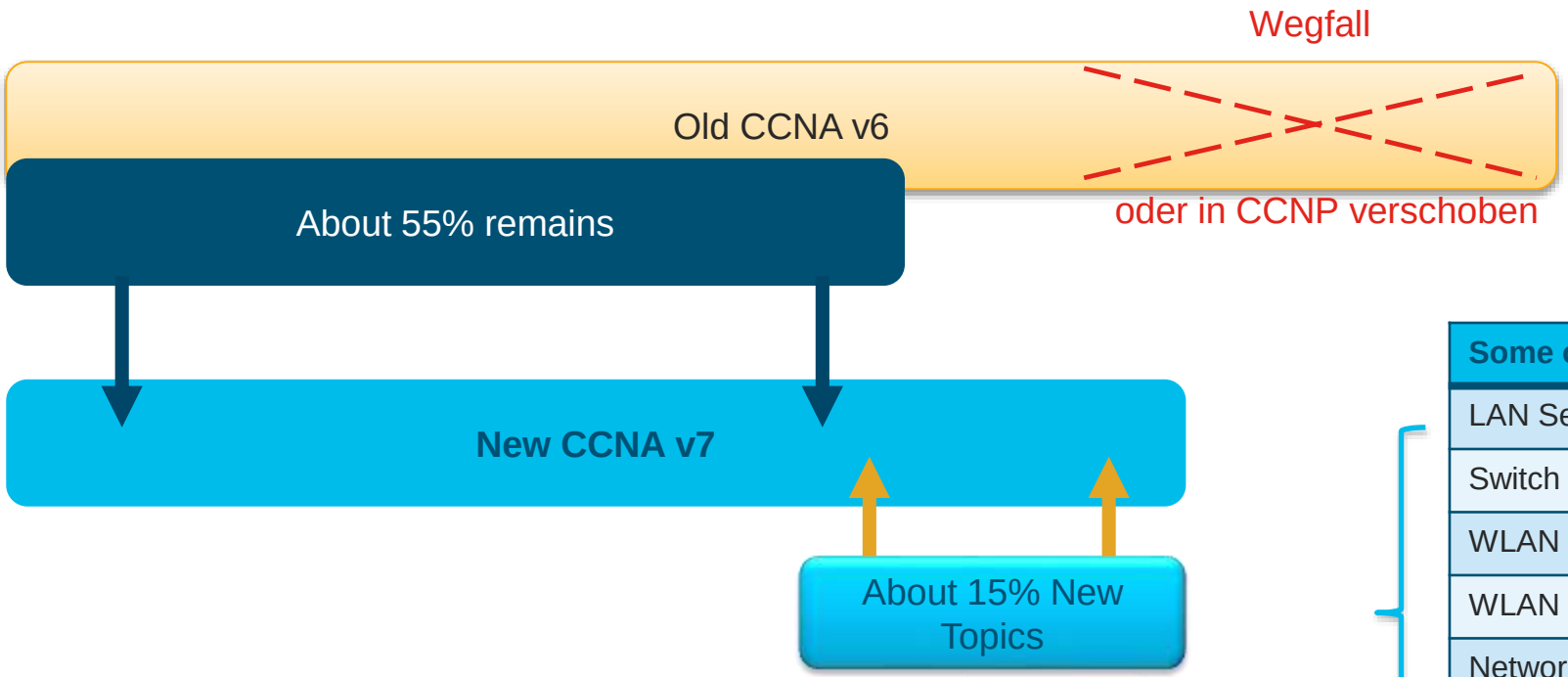
Anforderungen an CCNA Exam v1.0 (200-301)

CCNA 7 Schwerpunkte und Unterschiede





Relativer Größenvergleich



Some of new Topics
LAN Security
Switch Security
WLAN Concepts
WLAN Configuration
Network Security
VPN & IPSec
Network Automation

CCNA 7.0 Entwicklung

CCNAv7 Intro to Networks (ITN)	CCNA v7 Switching, Routing, and Wireless Essentials (SRWE)	CCNA v7 Enterprise Networking, Security and Automation (ENSA)
Based on CCNA 6.0 Intro to Networking (ITN)	Blend of CCNA 6.0 … ✓ Routing and Switching Essentials (RSE) ✓ Scaling Networks (ScaN) ✓ + New topics*	Blend of CCNA 6.0 … ✓ Routing and Switching Essentials (RSE) ✓ Scaling Networks (ScaN) ✓ Connecting Networks (CN) ✓ + New topics**
Minor updates and refinements	*Addition of WLAN and Security topics	**Addition of Automation, Programmability, VPN, and Security topics

CCNA 7.0 Kursüberblick

Networking Academy

Intro to Networks (ITN)
Networking Today
Basic Switch and End Device Configuration
Protocol Models
Physical Layer
Number Systems
Data Link Layer
Ethernet Switching
Network Layer
Address Resolution
Basic Router Configuration
IPv4 Addressing
IPv6 Addressing
ICMP
Transport Layer
Application Layer
Network Security Fundamentals
Build a Small Network

Switching, Routing, and Wireless Essentials (SRWE)
Basic Device Configuration
Switching Concepts
VLANs
Inter-VLAN Routing
STP
Etherchannel
DHCPv4
SLAAC and DHCPv6 Concepts
FHRP Concepts
LAN Security Concepts
Switch Security Configuration
WLAN Concepts
WLAN Configuration
Routing Concepts
IP Static Routing
Troubleshoot Static and Default Routes

Enterprise Networking, Security and Automation (ENSA)
Single-Area OSPFv2 Concepts
Single-Area OSPFv2 Configuration
WAN Concepts
Network Security Concepts
ACL Concepts
ACLs for IPv4 Configuration
NAT for IPv4
VPN and IPsec Concepts
QoS Concepts
Network Management
Network Design
Network Troubleshooting
Network Virtualization
Network Automation

Neue Inhalte

Ergänzende Optionen

CCNP Enterprise (ENCOR, ENARSI)

or

CCNA Security / CCNA CyberOps

or

DevNet Associate

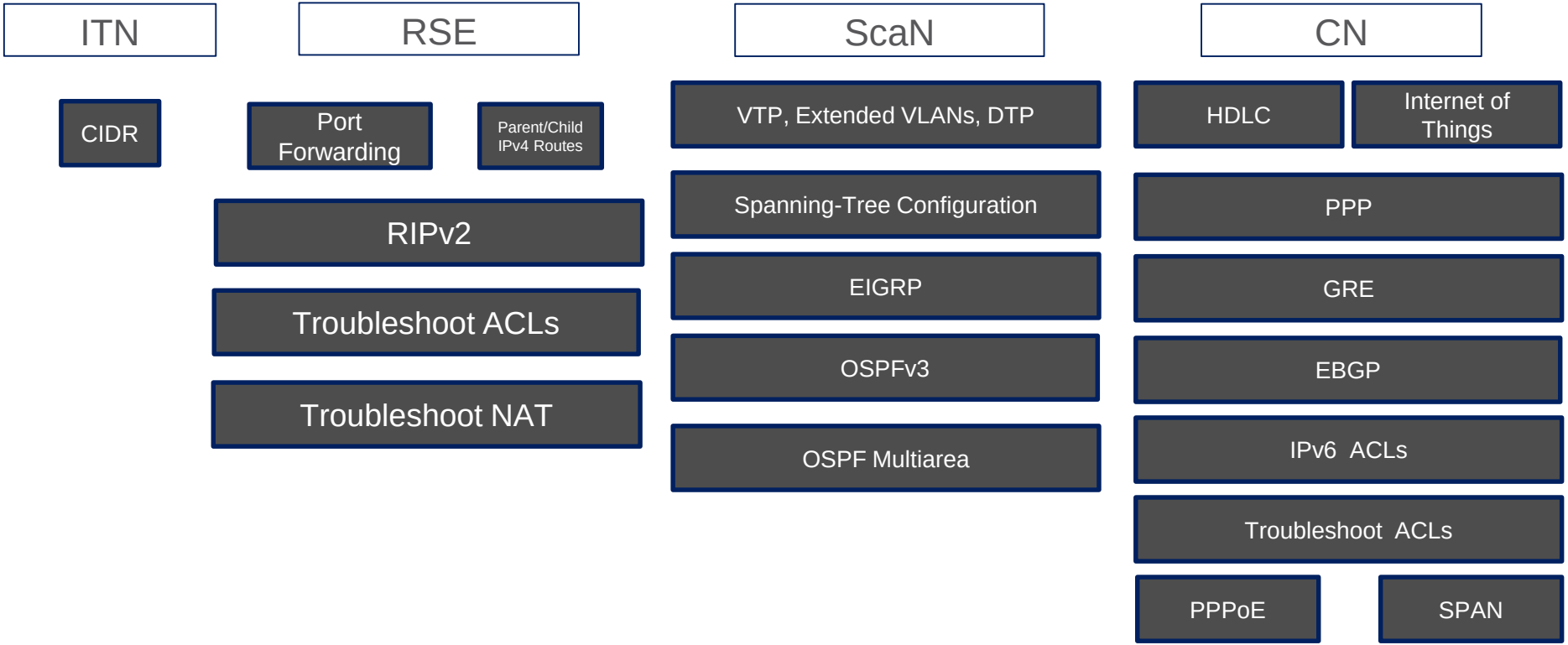
or

Python / ETWs

or lead with

IT Essentials

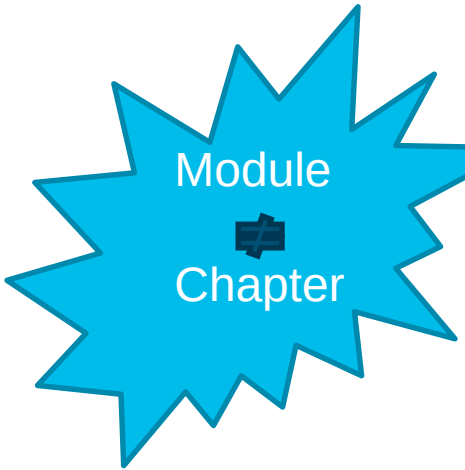
CCNA R&S v6 Content Removed (reference by size)



CCNA R&S v6

Chapters

Introduction to Networks (ITN) v6.0
Explore the Network
Configure a Network Operating System
Network Protocols and Communications
Network Access
Ethernet
Network Layer
IP Addressing
Subnetting IP Networks • CIDR
Transport Layer
Application Layer
Build a Small Network



CCNA-1 v7

17 Modules

Introduction to Networks (ITN) v.7.0
Networking Today
Basic Switch and End Device Configuration
Protocol Models
Physical Layer
Number Systems • Hexadecimal
Data Link Layer
Ethernet Switching
Network Layer
Address Resolution
Basic Router Configuration
IPv4 Addressing (Reduced and Updated)
IPv6 Addressing • Network Discovery
ICMP
Transport Layer
Application Layer
Network Security Fundamentals
Build a Small Network

	New
	Removed

New
from RSE
From ScaN

CCNA R&S v6

Chapters

Routing & Switching Essentials (RSE) v6.0
Routing Concepts
Static Routing
Dynamic Routing
Switched Networks
Switch Configuration
VLANs
Access Control List
DHCP
NAT for IPv4
Device Discovery, Management & Maintenance

Scaling Networks (ScaN) v6.0
LAN Design
Scaling VLANs
STP
EtherChannel and HSRP
Dynamic Routing
EIGRP (CCNP)
EIGRP Tuning and Troubleshooting
Single-Area OSPF
Multiarea OSPF
OSPF Tuning and Troubleshooting

CCNA-2 v7

17 Modules

Switching, Routing, and Wireless Essentials (SRWE) v7.0
Basic Device Configuration (from RSE)
Switching Concepts (from RSE)
VLANs (from RSE & ScaN)
Inter-VLAN Routing (from ScaN)
STP (from ScaN)
EtherChannel (From ScaN)
DHCPv4 (from RSE)
SLAAC and DHCPv6 Concepts (from RSE)
FHRP Concepts (From ScaN)
LAN Security Concepts (New)
Switch Security Configuration (New)
WLAN Concepts (New)
WLAN Configuration (New)
Routing Concepts (from RSE)
IPv4 Static Routing (from RSE)
IPv6 Static Routing (from RSE)
Troubleshoot Static and Default Routes (from RSE)

New
from CN
from ScaN
from RSE

CCNA R&S v6
Chapters

Scaling Networks (ScaN) v6.0
LAN Design
Scaling Networks
STP
EtherChannel
Dynamic Routing
EIGRP
EIIGRP Tuning and Troubleshooting
Single-Area OSPF
Multiarea OSPF
OSPF Tuning and Troubleshooting

Connecting Networks (CN) v6.0
WAN Concepts
Point-to-Point Connections
Branch Connections
Access Control Lists
Network Security and Monitoring
Quality of Service
Network Evolution
Network Troubleshooting

CCNA-3 v7
14 Modules

Enterprise Networks, Security and Automation (ENSA) v7.0
Single-Area OSPFv2 Concepts (from ScaN)
Single-Area OSPFv2 Configuration (from ScaN)
WAN Concepts (from CN)
Network Security Concepts (New)
ACL Concepts (from CN)
ACL for IPv4 Configuration (from CN)
NAT for IPv4 (from RSE)
VPN and IPsec Concepts (New)
QoS Concepts (from CN)
Network Management (RSE & CN)
Network Design (RSE & ScaN)
Network Troubleshooting (from CN)
Network Virtualization (from CN)
Network Automation (New)

CCNA 7.0 Strategie der Lernzielkontrollen

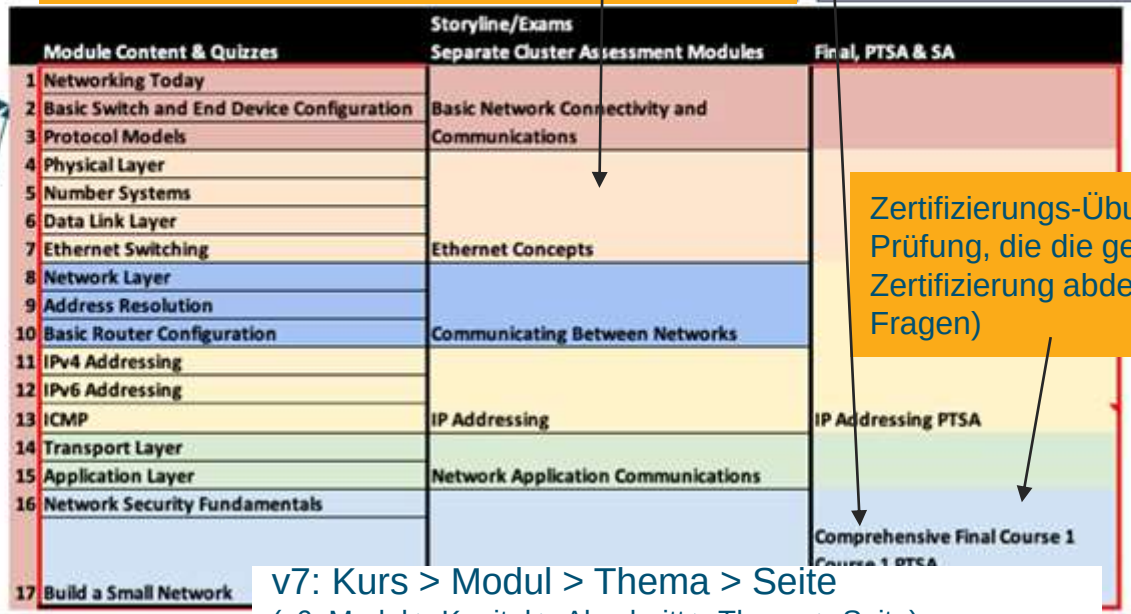
Modul-Quiz, ein in die GUI eingebettetes Quiz pro Modul, das den Inhalt des Blocks abdeckt (17x 10 Fragen)

Überprüfen Sie Ihr Verständnis - ein Quiz zur Selbstevaluation am Ende jedes Themas (3-5 Fragen)

Cluster-Prüfungen - Eine Prüfung, die mehrere Module umfasst, in denen eine Fähigkeit abgeprüft wird. (6x 10-20 Fragen)

Abschlussprüfungen - eine Prüfung, die den gesamten Kurs abdeckt. (50-60 Fragen)

Zertifizierungs-Übung - eine Prüfung, die die gesamte CCNA-Zertifizierung abdeckt. (50-60 Fragen)



v7: Kurs > Modul > Thema > Seite

(v6: Modul > Kapitel > Abschnitt > Thema > Seite)

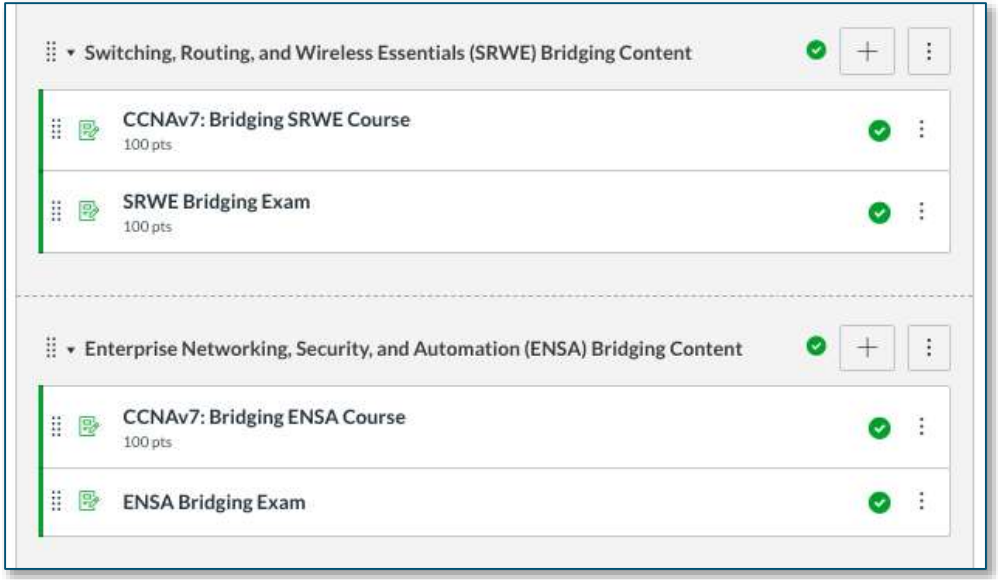
CCNA Instructor Qualification Mapping

Keine Verpflichtung, nur eine Empfehlung für den Anspruch die CCNA-Zertifizierung anbieten zu können

CCNA R&S v6 Course Current Qualification(s)	CCNA v7 Course Qualification(s) Earned	Materials to Review*
CCNA 1 (Intro to Networks)	CCNA 1 (Intro to Networks)	No additional
CCNA 1 (Intro to Networks) CCNA 2 (Routing & Switching Essentials)	CCNA 1 (Intro to Networks) CCNA 2 (Switching, Routing, and Wireless Essentials)	CCNA 2 (SRWE) v7
CCNA 1 (Intro to Networks) CCNA 2 (Routing & Switching Essentials) CCNA 3 (Scaling Networks)	CCNA 1 (Intro to Networks) CCNA 2 (Switching, Routing, and Wireless Essentials) CCNA 3 (Enterprise Networking, Security, and Automation)	CCNA3 (ENSA) v7 + Bridging Course (4 new topics SRWE)
CCNA 1 (Intro to Networks) CCNA 2 (Routing & Switching Essentials) CCNA 3 (Scaling Networks) CCNA 4 (Connecting Networks)	CCNA 1 (Intro to Networks) CCNA 2 (Switching, Routing, and Wireless Essentials) CCNA 3 (Enterprise Networking, Security, and Automation)	Bridging Course
CCNA 2 (Routing & Switching Essentials)	CCNA 2 (Switching, Routing, and Wireless Essentials)	CCNA2 (SRWE) v7
CCNA 3 (Scaling Networks)	CCNA 3 (Enterprise Networking, Security, and Automation)	CCNA3 (ENSA) v7
CCNA 4 (Connecting Networks)	CCNA 3 (Enterprise Networking, Security, and Automation)	CCNA3 (ENSA) v7

CCNAv7 Bridging Course

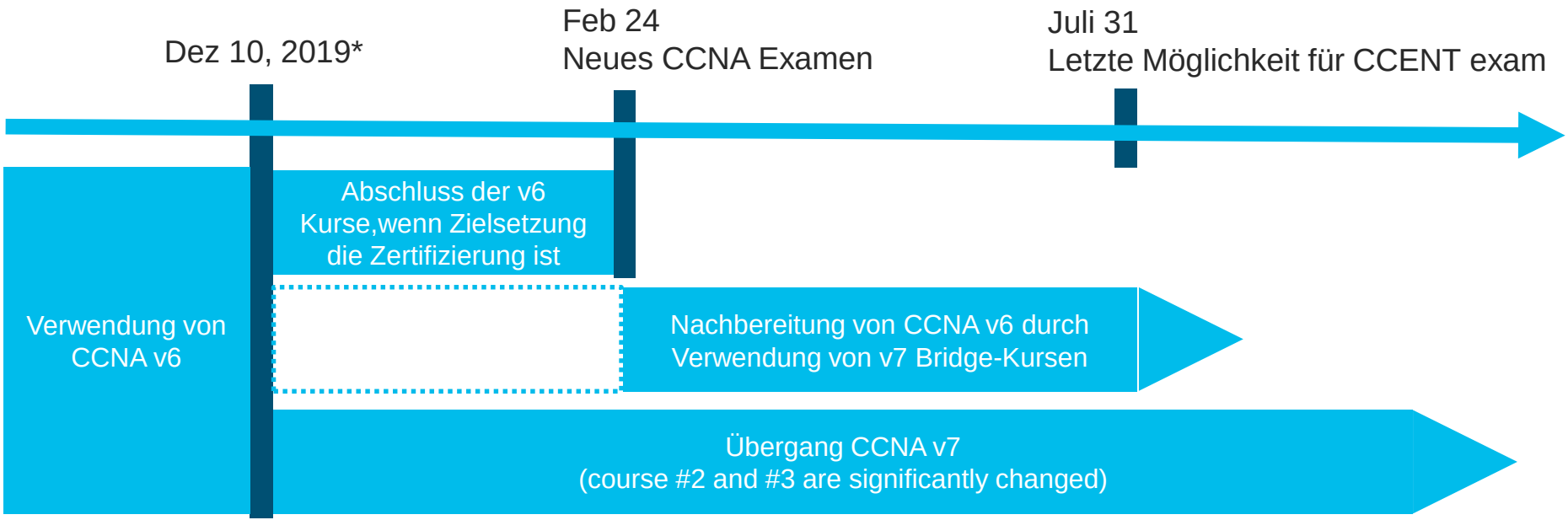
- Verfügbar seit Oktober, 2019
- Umfasst 7 neue Module in einer Kursraumvorlage
- Verfügbarkeit kann nach Kursen 2 und 3 gesteuert werden (CCNAv7 SRWE - 4 Module oder CCNAv7 ENSA – 3 Module)



Networking Academy

Umstieg auf CCNA v7

CCNA v7 Migration – Vorgehen (Zertifizierung)



Die Zeitleiste ist spezifisch für die englische Version von CCNA 7.
Für andere Sprachen unterrichten Sie weiterhin v6, bis v7 verfügbar ist.

Wann kommt deutsche Übersetzung?

CCNA v7 Migration – Vorgehen (z. B. ALP/ITC)

Dezember 2019

24. Februar 2020
Neues CCNA Examen

~~30.3.-09.04.2020~~
~~98/376~~

20.7.-31.7.2020
98/568

Juli 31
Letzte Möglichkeit für CCENT exam

Verwendung von CCNA v6

Verwendung von CCNA v7 (Kurs 1-3 und CyberOps) und individuelle Anpassung an die Teilnehmerzusammensetzung

98/568

Vernetzte IT-Systeme - Aktuelle Angebote der Bildungsinitiative Networking

28.7.2020, 14:00 Uhr – 31.7.2020, 12:00 Uhr

Ort: Kardinal-von-Waldburg-Str. 6-7, 89407 Dillingen a.d. Donau

Leitung: Michael Lotter

Bewerbung bis: 31.5.2020

Ziele:
Ziel des Lehrgangs ist eine grundlegende Qualifizierung im Wissensgebiet der Netzwerktechnik und die Einbettung industrieller Qualifizierungsangebote in den Lernfeldunterricht beruflicher Schulen.

Inhalt:
Folgende Module können wahlweise belegt werden. Bitte geben Sie in Ihrer Bewerbung an, welches Modul Sie belegen möchten:

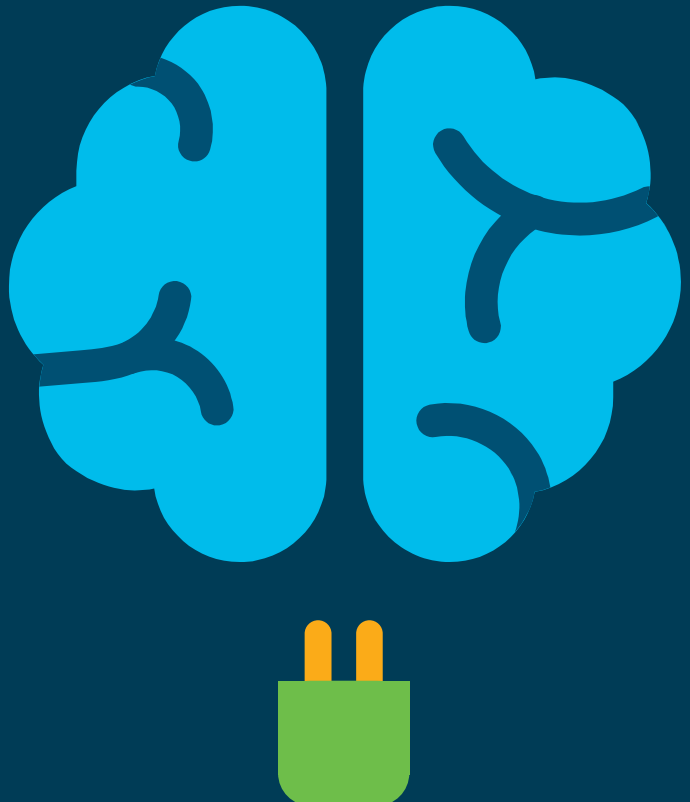
- Modul 1: Grundlagen Netzwerkprotokolle - Standards des OSI-Schichtenmodell (Umfang 70 Stunden, Modulbeschreibung)
- Modul 2: Switching, Routing und Grundlagen WLAN (Umfang 70 Stunden, Modulbeschreibung)
- Modul 3: Anforderungen an Unternehmensnetze, IT-Sicherheit, Automatisierung von Konfigurationsaufgaben (Umfang 70 Stunden, Modulbeschreibung)
- Zusatzmodul: Angriffsszenarien in cyber-physischen Systemen unterscheiden und antizipieren / Anomalien in vernetzten Systemen feststellen und Schutzmaßnahmen einleiten (Cybersecurity Operations, Umfang 70 Stunden, Modulbeschreibung)

CCNA v7 Migration – Vorgehen (z. B. BS/CA)

Ersatz für 98/376 Vernetzte IT-Systeme – Aktuelle Angebote der Bildungsinitiative Networking

Nummer	Titel	Zeitraum
98/635A	Kurs 1: Introduction to Networks (5 Fortbildungstage)	Online bis 17.7.20 Prüfung z. B. in 98/558
98/636A	Kurs 2: Switching, Routing und Grundlagen WLAN (SRWE) (5 Fortbildungstage)	Siehe oben
98/637A	Kurs 3: Anforderungen an Unternehmensnetze, … (ENSA) (5 Fortbildungstage)	Siehe oben
98/638A	Neuerungen im Angebot der Bildungsinitiative Networking / Bridge-Kurs (1 Fortbildungstag)	Siehe oben
98/633B	Erkennen von sicherheitsrelevanten Ereignissen und Behandlung von Sicherheitsvorfällen (CyberOps) (5)	Siehe oben
98/568	Vernetzte IT-Systeme – Aktuelle ...	Präsenz

CCENT Verlängerung



CCENT (ICND1 - 100-105)

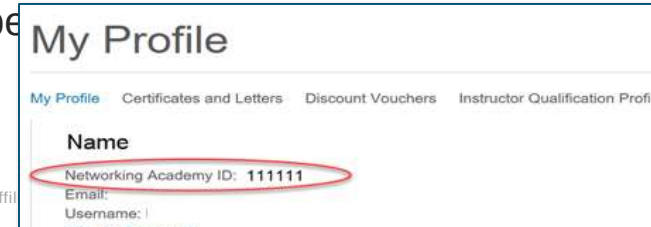
Verlängerung gilt nur für Networking-Akademie-Studenten & Instruktoren

Letzter Tag an dem eine CCENT-Prüfung stattfinden kann: 31. Juli 2020

Veränderte Prüfungsbezeichung

100-110 INVITATION ONLY - CCENT, Interconnecting Cisco Networking Devices

- Voucher (Gutscheine) haben eine Gültigkeit von 6 Monaten und müssen spätestens 3 Monate vor der Prüfung beantragt werden. Alle CCENT-Gutscheine laufen zum 31. Juli 2020 ab.
- Die Rabatte für Networking Academy-Kurse werden ab dem 10. Juli 2020 nicht mehr gewährt.
- Networking Academy Studenten und Instruktoren müssen bei der Anmeldung zur Prüfung ab dem 24. Februar 2020 ihre Networking Academy ID angebe



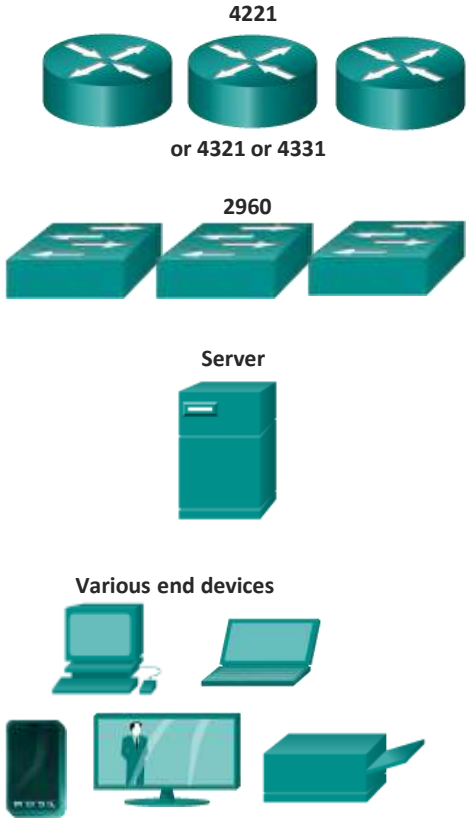
Umfrage: Wie gehen Sie vor? / Wie werden Sie vorgehen?

1. Bieten/Boten Sie Ihren Schülern das CNAP primär an, um auf die CCNA-Zertifizierung v6 vorzubereiten?
2. Werden Sie das CNAP Ihren Schülern primär anbieten, um auf die CCNA-Zertifizierung v7 vorzubereiten?
3. Integration der CCNA v6-Inhalte in den Regelunterricht?
   a. vollständig
   b. teilweise
4. Integration der CCNA v7-Inhalte in den Regelunterricht?
   a. Vollständig
   b. Teilweise
5. Die Inhalte des CCNA biete ich grundsätzlich außerhalb des Regelunterrichts an.

Networking Academy

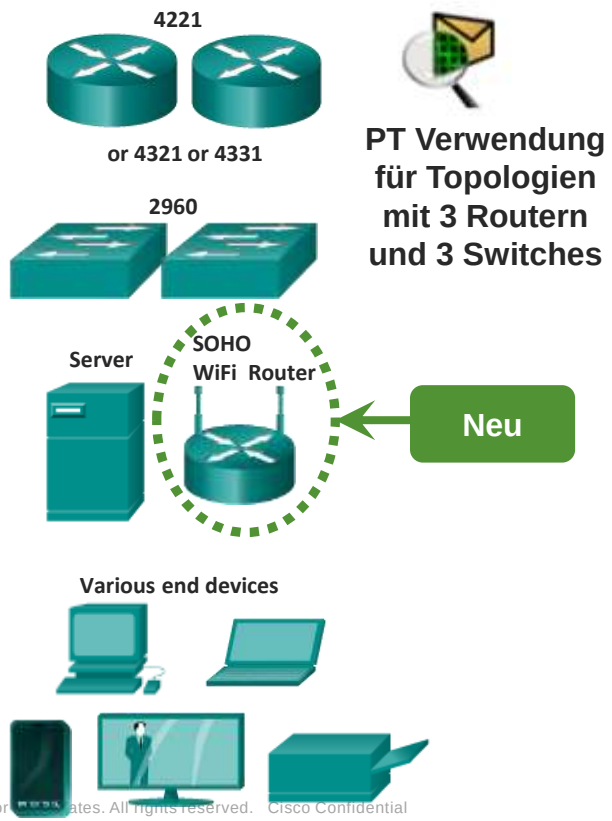
CCNA v7 Laborausstattung

CCNA 6.0 vs 7.0 – Laborausstattung



Bitte für v7 berücksichtigen:

- **Serial Ports werden nicht benötigt**
- **PT Version 7.3 erforderlich**



PT Verwendung für Topologien mit 3 Routern und 3 Switches

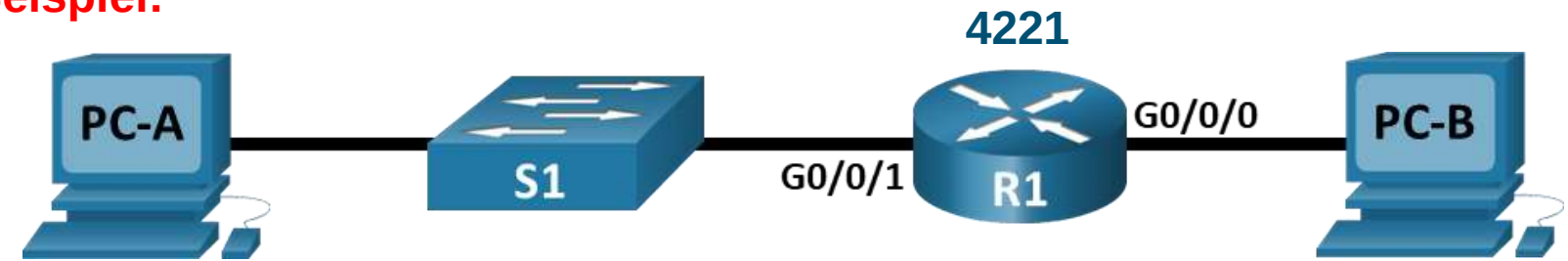
SOHO Wi-Fi Router im CCNA 7.0

- 1 Wireless Router (egal welches Produkt, plain vanilla) der WPA2 unterstützt
- Inhalte beschränken sich auf Standardkonfigurationen eines kleinen WLANs (Infrastruktur BSS)
- PT bietet auch Übungen mit WLAN-Controller

Kann ich die v7 auch mit 1941/2901 Routern anbieten?

- Ja, das geht. Folgendes ist jedoch zu beachten:
  - Die Labs und die praktischen Lernerfolgskontrollen sind für den 4221 geschrieben und erprobt worden.
  - Die Interface-Nummerierungen sind 3- statt 2-stellig.
  - Es kann kleine Abweichungen bei der Funktion mancher IOS-Befehle geben.

Beispiel:



1941/2901 – Interface names G0/0 & G0/1

CCNA v7 Equipment List – ISR4K IOS-XE

- **Dei aktuelle Equipmentlist schlägt das Betriebssystem IOS-XE vor**

Equipment List (Option 1)

The Cisco 4221 router shown in Option 1 should be ordered with IOS-XE Image with Payload Encryption:
e.g. SISR4200UK9-xxx (select a current version for xxx), Cisco ISR 4200 Series IOS XE Universal

Qty	Product Number	Description	Notes
2	ISR4221/K9	Cisco ISR 4221 (2GE, 2NIM, 8G FLASH, 4G DRAM,IPB) See note above regarding IOS-XE image.	1,2

- **Die Auswahlliste im CCO-Account bietet 3 Registerkarten zu Auswahl von Images an. Für das korrekte Image sollte die 2. Registerkarte (Image with Payload Encryption) gewählt werden. Standardauswahl wäre nicht korrekt.**

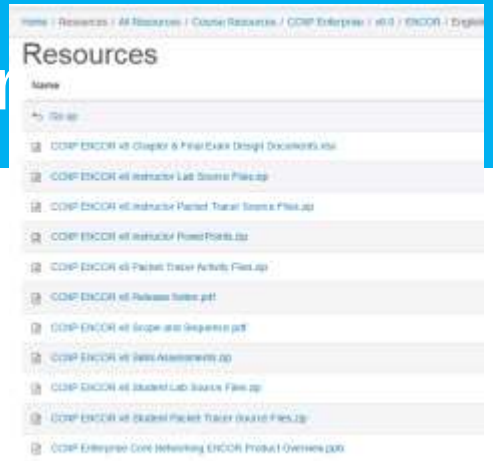
Networking Academy

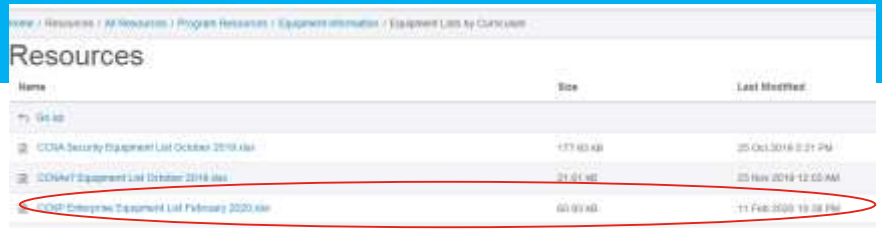
CCNP 8.0 Updates

CCNA 6.0 Content Shifted to CCNP

CCNA v6	CCNP Enterprise Core
Old CCNA-2 (RSE Course)	Troubleshoot ACLs
	Troubleshoot NAT
Old CCNA-3 (ScaN Course)	Spanning Tree Configuration
	Distance Vector Dynamic Routing
	Link-State Dynamic Routing
	EIGRP Characteristics
	Implement EIGRP for IPv4
	EIGRP Operation
	Implement EIGRP for IPv6
	Tune EIGRP
	Troubleshoot EIGRP
	Single-area OSPFv3
	Multiarea OSPF Operation
	Implement Multiarea
	Troubleshooting Single-Area OSPF Implementations
Old CCNA-4 (CN Course)	GRE
	eBGP
	Introducing IPsec
	IPv6 ACLs
	Troubleshoot ACLs
	Cisco Switch Port Analyzer (SPAN)
	NetFlow

CCNP Enter





Alte Zertifizierungen

SWITCH

ROUTE

TSHOOT

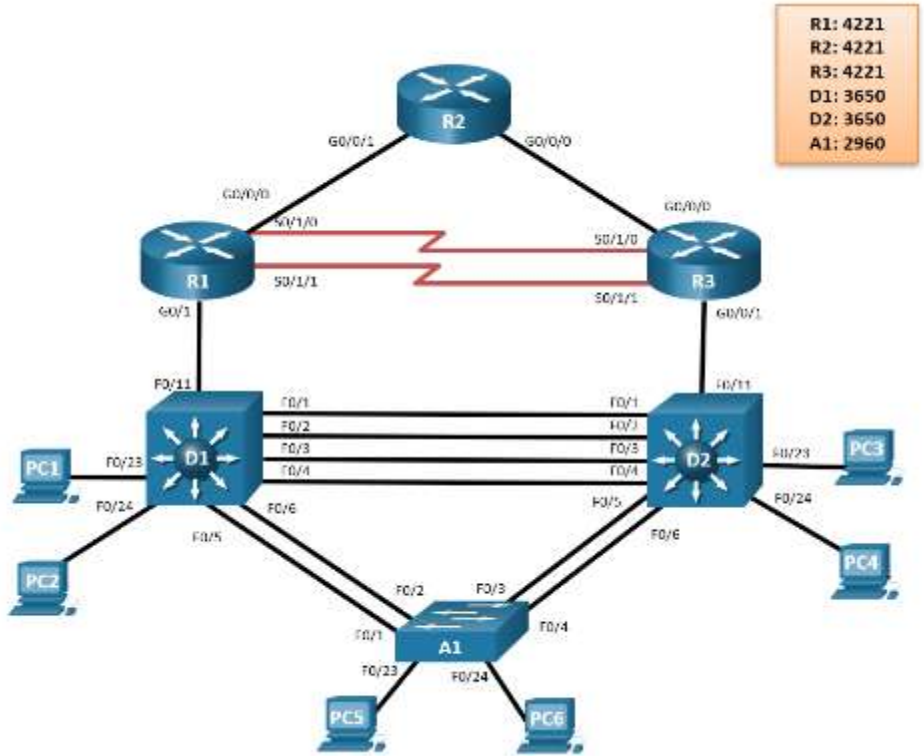
Neue Zertifizierungen

Enterprise Core

Enterprise Advanced Routing & Services

- Neue Labs und Zertifizierungsprüfungen, kein Online-Curriculum
  - ENCOR ~ Veröffentlichung seit Januar (Cisco Press)
  - ENARSI ~ Veröffentlichung seit (Cisco Press)
- Digital Badges für den Abschluss von Laboren und Prüfungen und das Bestehen von Prüfungen
- Ziel:
  - Equip list (seit Dezember)
  - ENCOR - PPT, Labs ... (seit dieser Woche)
  - ENARSI – PPT, Labs … ASAP

CCNP Enterprise – Baseline Physical Topology
(ENCOR and ENARSI)



This is the same basic topology as used by CCNPv7.1;
Some connections are changed around, and there is one less 2960 L2 Switch and one less ISR4221

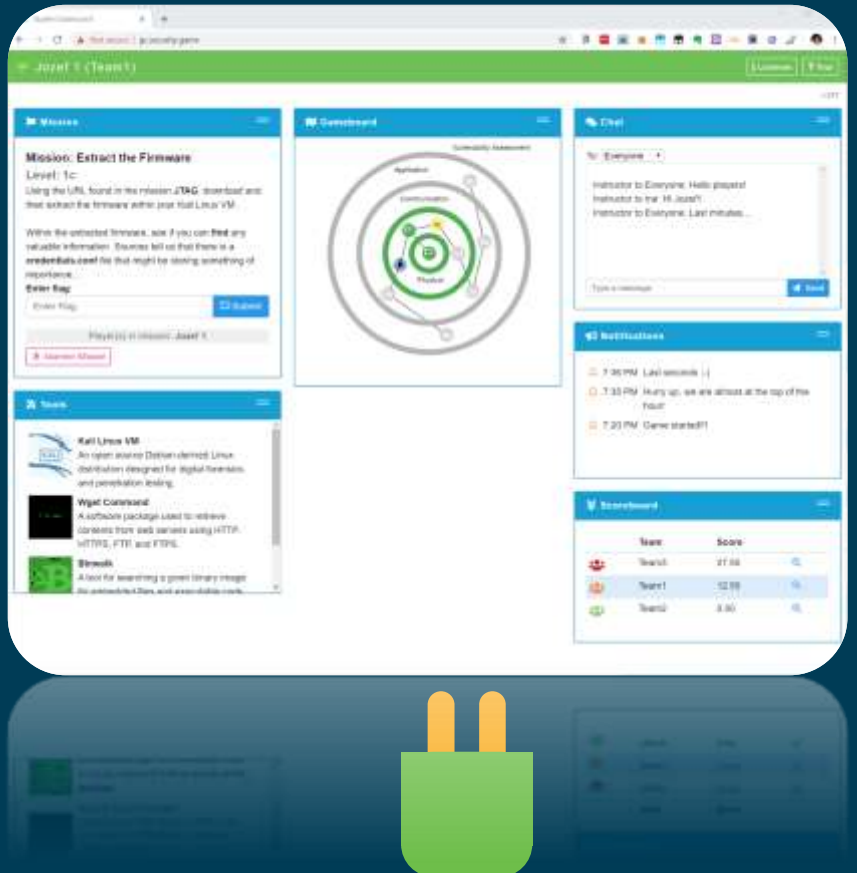
Most current labs can be adapted, and the LP labs can be used directly or adjusted for the topology

CCNP Baseline Equipment Recommendation
3x Cisco 4221 with SEC license (2 with NIM-2T)
2x Cisco Catalyst 3650 Switches (WS-C3650-24TS-E)
1x Cisco Catalyst 2960+ Switch (WS-C2960+24TC-L)
Ethernet cables as shown in the topology
2x CAB-SS-V35MT= (10' DTE Serial Cable)
2x CAB-SS-V35FC= (10' DCE Serial Cable)

Computers (Virtual or Physical)
Minimum 1x PC workstation host (Linux or Windows)
Minimum 1x PC server host (Linux or Windows)

IoT Security 1.1

- With Gamification



IoT Security v1.1

Überblick

Die Zunahme von IoT-Geräten ermöglicht die branchenübergreifende Digitalisierung, erhöht aber auch das Risiko von Sicherheitsbedrohungen. Nach Abschluss können Schwachstellen- und Risikobewertungen durchgeführt werden und Strategien zur Risikominderung für gängige Sicherheitsbedrohungen in IoT-Systemen empfohlen werden.

Nutzen

Lerner, die ihr zukünfiges Arbeitsumfeld im schnell wachsenden IoT-oder IT-Sicherheitsbereich sehen lernen praktische Werkzeuge zur Bewertung von Sicherheitsschwachstellen kennen, führen eine unternehmensbezogene Einschätzung von Schadenspotenzialen (Modellierung) durch und verwenden Risikomanagement-Frameworks (z. B. NIST CVSS, Schutzbedarfsbewertung des BSI IT-Grundschutz (Basis/Standard/Kern), um Maßnahmen zur Bedrohungsabwehr zu empfehlen.

Inhalte

- Schutzbedarfe in einem IoT-System feststellen und bewerten.
- Schwachstellen mit Penetrations-Test-Werkzeugen entdecken (Kali Linux)
- praktische Übungen mit IoT-Prototypen (Raspberry Pi)
- Einblick in neue Techologien der IT-Sicherheit (Blockchain)
- **Spielerisches Lernen, White Hat Hacker-Rolle in einem Teamspiel einüben**

Beitrag zur Kompetenz “Schutzbedarfsanalyse im eigene Arbeitsbereich durchführen“

Beitrag zur Kompetenz “durch eine Risikoanalyse den Schutzbedarf eines vernetzten Systems ermitteln, und Schutzmaßnahmen planen, umzusetzen und dokumentieren“

Merkmale

Zielgruppe: BFS, BS, FS

Voraussetzungen:

- IoT Fundamentals: Connecting Things (Grundlagen IoT)
- Netzwerktechnik und IT-Sicherheit auf dem Niveau von z. B. Networking Essentials und Cybersecurity Essentials

Sprache: English

Kursbereitstellung: Instruktorgeführt

Zeitumfang: 50 Stunden

IoT Security v1.1

IT-Grundschutz (BSI)	Handlungsprodukte	Ausgewählte Laborübungen	PT-Übungen
Sicherheitsmanagement	Leitlinie, Sicherheitskonzept, Verantwortlichkeiten, Rollenverteilung	Shodan Search	
Strukturanalyse	Dokumentation der Geschäftsprozesse, der IT-Anwendungen, der Topologie nach Schutzbedarf, der IT-Systeme, Plattformen und Dienste, der Räume  	Evaluate Home Automation Products Evaluate the IoT Security Risk in an Industry Sector Create an IoT Sensor-Actuator System	• Explore the Smart Home • Threat Modeling at the IoT Device Layer • Threat Modeling at the IoT Communication Layer • Threat Modeling at the IoT Application Layer • Threat Modeling to Assess Risk in an IoT System Bsp. Thread Modeling Device L 1. Schutzziele festlegen 2. Darstellung des physischen Netzwerks 3. Zuordnung Vermögenswerte und Angriffsoberfläche für physische Geräte 4. Identifizieren potenzieller Bedrohungen mit dem STRIDE-Modell 
Schutzbedarfsfeststellung	Einteilung der Struktur nach Schutzzielen (CIA) und Schutzkategorien mit Unternehmensbezug	Investigate Vulnerability Assessment Tools Investigate IoT Security Requirements	
Modellierung	Zuordnung der IT-Grundschutzbausteine zu Zielobjekten und Anpassung der unternehmensspezifischen Anforderungen		
Risikoanalyse	zusätzlicher Analysebedarf (erhöhter Schutzbedarf, kein passender Baustein, Einsatzumgebung des Zielobjekts ist untypisch)	Compromise IoT Device Firmware/Hardware Sniffing Bluetooth with the Raspberry Pi Hacking MQTT	
…			
IT-Grundschutzzertifizierung	ISO 27001-Zertifizierung		

IoT Security Game

Überblick

Das Spiel ist an CTF (CTF = Catch The Flag, Erobere die Fahne) angelehnt.

Der Spielort ist ein IoT-System in dem Schülerteams gegeneinander antreten und ihre White Hat Hacker-Fähigkeiten unter Beweis stellen dürfen, d. h. sie führen Schwachstellenanalysen durch und geben Empfehlungen zur Schadensbegrenzung.

Nutzen

Die Spieler trainieren ihre Fähigkeiten im Bereich der White Hat Hacker-Cybersicherheit durch eine Reihe von Herausforderungen im Team. In 10 Missionen entdecken sie verschiedene Schwachstellen auf Geräte-, Kommunikations- und Anwendungsebene und empfehlen Maßnahmen zur Schadensbegrenzung.

Inhalte/Komponenten

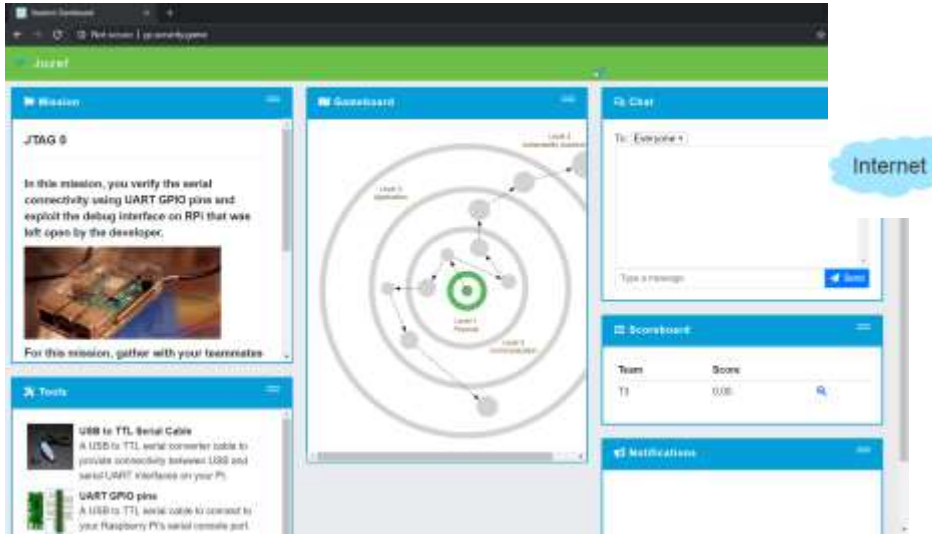
- Game Controller
- Cloud Services Simulator
- Internet Gateway
- IoT End Device
- Kali Linux VM

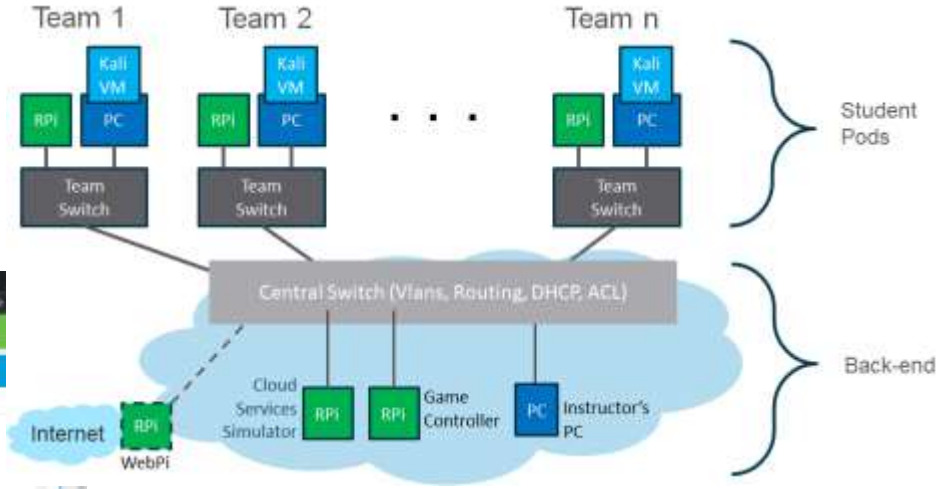
Merkmale

Integraler Bestandteil des IoT-Security Kurses

- 10 herausfordernde Missionen
- Praxis im Umgang mit Werkzeugen für Penetrationstests
- Unterhaltsame und einnehmende Erfahrung
- Teamarbeit und Kommunikation

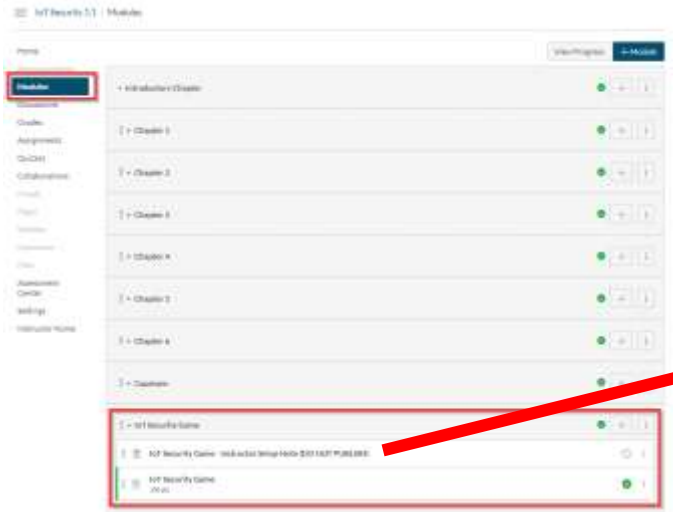
IoT Security Game

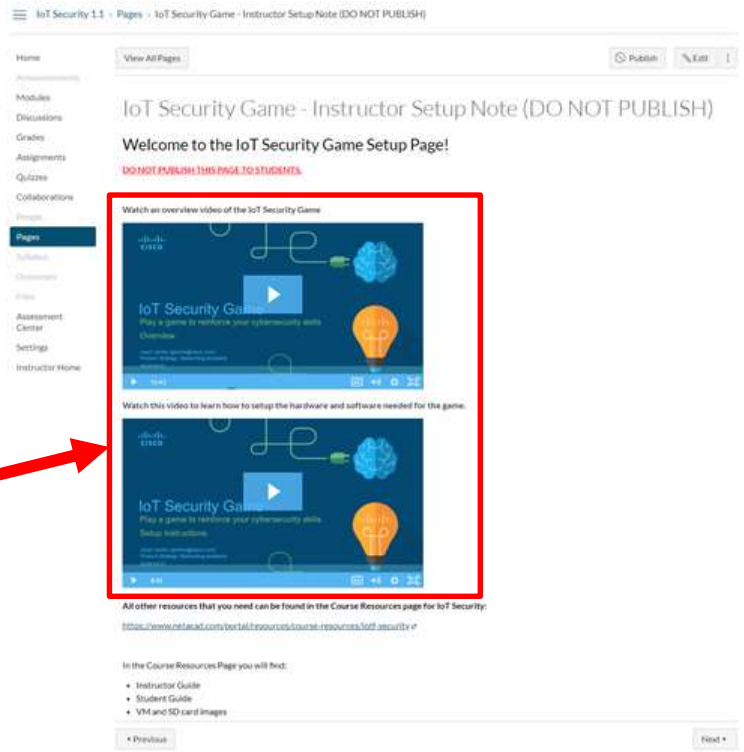




Verfügbarkeit auf der Plattform?

1. Einen Kursraum v1.1 einrichten
2. Navigieren Sie im Menü "Module" zum IoT-Sicherheitsspiel
3. Sie sehen die beiden Video-Tutorials (Spielanleitung und Spielvorbereitung)





Verfügbarkeit des Spielmaterials?

1. Navigieren Sie zu [IoT Security Course Instructor's Resources Page]
2. Wählen Sie den Ordner "Kursressourcen".
3. Laden Sie die Dateien des IoT-Sicherheitsspiels herunter
4. Folgen Sie dem *Instructor's Setup Guide* für die Einrichtung

IoT-Sec./Connecting Things

Nummer	Titel	Zeitraum
99/237R	Digitale Transformation: Neuerungen in der Informationstechnologie	31.08.-04.09.2020 Präsenz
98/634B 99/679	Basisschutz im Internet der Dinge – IoT-Security	Jedes Halbjahr online

Nummer	Titel	Zeitraum
98/630	Digitale Transformation: Grundlagen IoT-Systeme, Modul T1.2 (Connecting Things)	Jedes Halbjahr online
	Digitale Transformation: Grundlagen der IoT- (Internet of Things) Systeme T1.2	Jedes Jahr im Februar/März Präsenz

Aktuelle Mitteilungen und Planungen des ASC/ITC Bayern

Fortbildungslehrgang Nr. 98/330

Angebote der ALP zur Unterstützung der Personal- und Unterrichtsentwicklung für die neugeordneten IT-Berufe

				Angebote der ALP	Format/Verfügbarkeit	Bewertung der Eignung maximal 3x +							
				siehe Legende	siehe Legende	Lehrerqualifizierung	Fachinformatiker				IT-SE	System-Management	Digitalisierung smanagement
							AE	SY	DP	DV			
	LF	Titel	Umfang										
1. Jahr	1	Das Unternehmen und die eigene Rolle im Betrieb beschreiben	80										
	2	Arbeitsplatz nach Kundenwunsch ausstatten	80	IT-Essentials	Blended, jährlich 2x	+++	+++	+++	+++	+++	+++	+++	+++
	3	Clients in Netzwerke einbinden	80	CCNA - Kurs 1 Grundlagen Netzwerkprot	Blended, jährlich 2x	+++	+++	+++	+++	+++	+++	+++	+++
				M1.1.x Grundlagen der Kommunikationsnetze in einem CPS	Blended, halbjährlich	+++				+++			
				Grundlagen Vernetzung, Schulnetzinitiat	präsenz, halbjährlich	+++	+++	+++	+++	+++	+++	+++	+++
	4	Schutzbedarfsanalyse im eigene Arbeitsbereich durchführen	40	IT-Grundschutz Online-Kurs des BSI *	online, on demand	+++	+++	+++	+++	+++	+++	+++	+++
				Cyber Security Essentials	online, on demand	+++	+++	+++	+++	+++	+++	+++	+++
				Basisschutz im Internet der Dinge - IoT Security	online, halbjährlich	+++	+++	+++	+++	+++	+++	+++	+++
				M1.4.x IT-Sicherheit in	Blended, jährlich	+++				+++			
				Cybersicherheit - Erkennen von sicherheitsrelevanten Ereignissen und Behandlung von Sicherheitsvorfällen	Bended, jährlic								
	5	Software zur Verwaltung von Daten anpassen	80	Grundlagen C und C++	online, on dem								+
				Grundlagen der Python-Programmierung	online, on dem								+
				Einsatz von SAP-Software	präsenz, halbjä								+++
				Grundlagen von Java - Kurs I	präsenz, jährlic								+++

IT-Essentials

Der Kurs IT -Grundlagen (ITE) führt die Teilnehmer in die Grundlagen der Computer Hard- und Software, der mobilen Geräte, der Sicherheits- und Netzwerkkonzepte sowie in die Verantwortlichkeiten eines IT-Profis ein. Die neueste Version umfasst mobile Geräte, Linux und cloudbasierte Virtualisierung sowie erweiterte Informationen über Microsoft Windows-Betriebssysteme, Sicherheit, Netzwerke und Fehlerbehebung.

Am Ende des Kurses werden die Teilnehmer in der Lage sein:

- die internen Komponenten eines Computers zu beschreiben und ein Computersystem zusammenzubauen.
- Betriebssysteme auf Computern und mobilen Geräten zu installieren und zu verstehen.
- sich mit dem Internet zu verbinden und Ressourcen in einer Netzwerkumgebung gemeinsam zu nutzen.
- Fehler mit Hilfe von Systemwerkzeugen und Diagnosesoftware zu beheben.

Der 70-stündige Kurs umfasst Aktivitäten mit Packet Tracer und praktische Laborarbeit. Für die Nutzung ist eine Qualifizierung an einem ITC erforderlich (Blended).

Relevante Lernfelder

- Arbeitsplatz nach Kundenwunsch ausstatten

Relevante Berufsbildpositionen (exemplarisch)

Informieren und Beraten von Kunden

- Bedarfe von Kunden feststellen sowie Zielgruppen unterscheiden
- Kunden unter Beachtung von Kommunikationsregeln informieren und Sachverhalte präsentieren und dabei deutsche und englische Fachbegriffe anwenden
- Informationsquellen auch in englischer Sprache aufgabenbezogen auswerten und für die Kundeninformation nutzen

Beurteilen marktgängiger IT-Systeme und kundenspezifischer Lösungen

- Marktgängige IT-Systeme für unterschiedliche Einsatzbereiche hinsichtlich Leistungsfähigkeit, Wirtschaftlichkeit und Barrierefreiheit beurteilen
- Angebote zu IT-Komponenten, IT-Produkten und IT-Dienstleistungen einholen und bewerten sowie Spezifikationen und Konditionen vergleichen
- Technologische Entwicklungstrends von IT-Systemen feststellen sowie ihre wirtschaftlichen, sozialen und beruflichen Auswirkungen aufzeigen
- Veränderungen von Einsatzfeldern für IT-Systeme aufgrund technischer, wirtschaftlicher und gesellschaftlicher Entwicklungen feststellen

[Link zur Ergebnisdokumentation]

Lernfeldübersicht

1. Ausbildungsjahr

Lernfeld 1	Lernfeld 2	Lernfeld 3	Lernfeld 4	Lernfeld 5
40 Std. Das Unternehmen und die eigene Rolle im Betrieb beschreiben	80 Std. Arbeitsplätze nach Kundenwunsch ausstatten	80 Std. Clients in Netzwerke einbinden	40 Std. Schutzbedarfsanalyse im eigenen Arbeitsbereich durchführen	80 Std. Software zur Verwaltung von Daten anpassen

2. Ausbildungsjahr

Lernfeld 6	Lernfeld 7	Lernfeld 8	Lernfeld 9
40 Std. Serviceanfragen bearbeiten	80 Std. Cyber-physische Systeme ergänzen	80 Std. Daten systemübergreifend bereitstellen	80 Std. Netzwerke und Dienste bereitstellen
exemplarische Lernsituation ☑	exemplarische Lernsituation ☑		

3. Ausbildungsjahr

Lernfeld 10a	Lernfeld 11a	Lernfeld 12a
80 Std. Benutzerschnittstellen gestalten und entwickeln	80 Std. Funktionalität in Anwendungen realisieren	120 Std. Kundenspezifische Anwendungsentwicklung

Nutzung freiwilliger oder verbindlicher Grundlage?

- Die Teilnahme ist grundsätzlich freiwillig und bedarf der individuellen Zustimmung zu den Nutzungsbedingungen durch den/die Schüler/in.
- Freiwilligkeit bedingt durch Registrierungsverfahren
- Mit diesem Einschreibeverfahren stimmen die Nutzer durch das setzen eines Hakens den Nutzungsbedingungen zu.
- Diese sind neben der Datenschutzerklärung sichtbar auf der Website hinterlegt.

Werden Einwilligungserklärungen von den Schülerinnen und Schülern (bzw. bei Minderjährigen von den Eltern) eingeholt?

- Die Richtlinien der Bildungsinitiative Networking enthalten für Lehrkräfte den Hinweis, dass eine Einwilligungserklärung der Erziehungsberechtigten durch die Lehrkraft einzuholen ist, bevor mit den Kursen der Lernplattform gearbeitet werden kann. Entsprechende Formulare werden angeboten. (“Parent/Guardian Consent for Cisco Networking Academy Course”)
- Unter Verwendung eines Pseudonyms ist eine Einwilligungserklärung im Punkt Datenverarbeitung nicht zutreffend.

Ihr Zeichen / Ihre Nachricht vom

Unser Zeichen (bitte bei Antwort angeben)
I.4-BS1356.5/158/7

München, 12.03.2020
Telefon: 089 2186 2319
Name: Herr Leicht

Einsatz digitaler Medien im Fall von längerfristiger Unterrichtsbeeinträchtigung aufgrund des Corona-Virus

Schließt die Schule Auftragsverarbeitungsverträge mit dem jeweiligen Auftragsverarbeiter?

- Die Schulleitung oder ein von der Schulleitung beauftragter Vertreter oder z. B. ein Verantwortlicher des Fördervereins stimmt einer Vereinbarung über die Mitgliedschaft zu. Darin enthalten ist die Auftragsverarbeitung.

- Diese Vereinbarung definiert Verantwortlichkeiten für den Schutz personenbezogener Daten und den Bereich der Anbieterverantwortung (Cisco Networking Academy Agreement). In dem Dokument bestehen Querbezüge zu den Nutzungsbedingungen (Term and Conditions for use of Cisco Networking Academy Sites and Services)

Wie steht Bayerns Landesbeauftragte für den Datenschutz dazu?

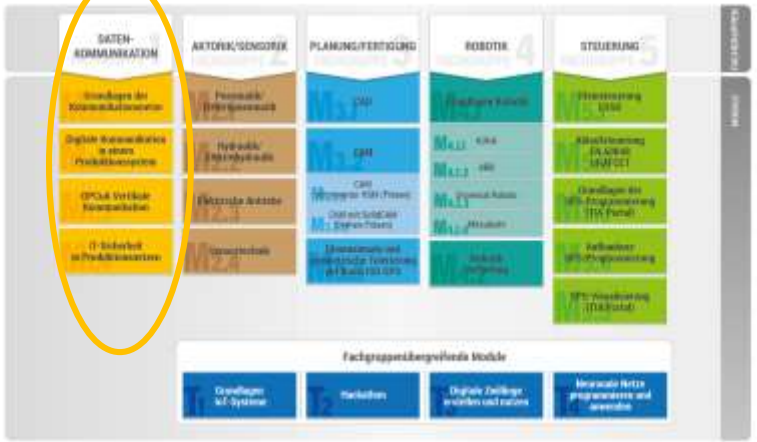
https://www.datenschutz-bayern.de/0/privacy_shield/privacy_shield.html

… Auch wenn sich Medienberichte zum Privacy Shield durchgängig auf Datenübermittlungen durch Unternehmen beziehen, kann der Privacy Shield für bayerische Behörden relevant werden. …

… Auf Grundlage des bindenden Beschlusses der Europäischen Kommission kann der Privacy Shield genutzt werden, um personenbezogene Daten aus der Europäischen Union an bereits zertifizierte Unternehmen in den USA zu transferieren. Die für den Datenexport verantwortlichen Stellen haben dabei stets darauf zu achten, dass das datenempfangende US-Unternehmen auch tatsächlich auf der Liste des US-Handelsministeriums *(externer Link)* geführt wird.

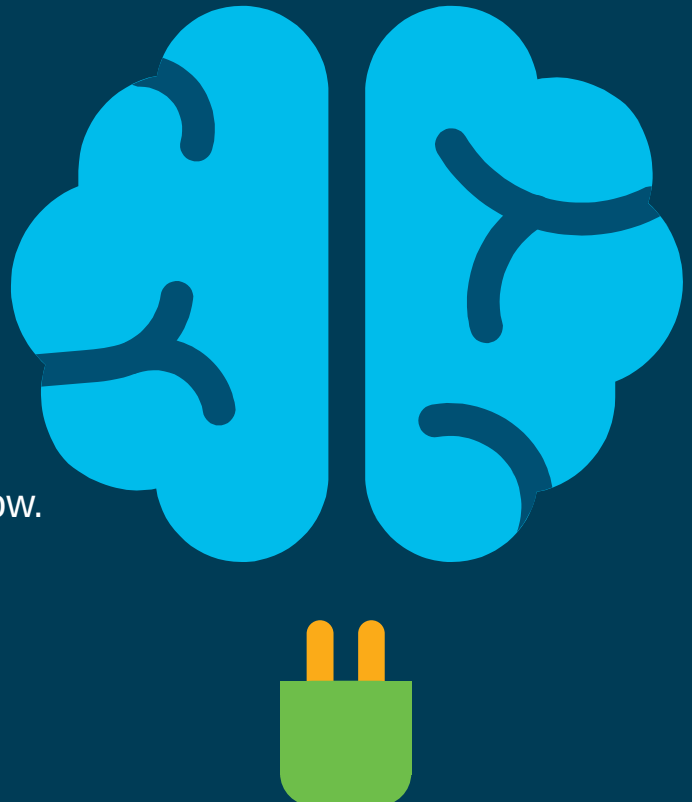
Nummer	Titel	Zeitraum
98/255R	Digitale Transformation: Neuronale Netze mit Python (Phase 1)	13.05.-15.05.20 (wird voraussichtlich verschoben)
98/267R	Digitale Transformation: Cybersicherheit in Produktionsnetzen, Modul 1.5 (Phase 2)	~~23.03.-24.03.20~~

https://links.alp.dillingen.de/iot



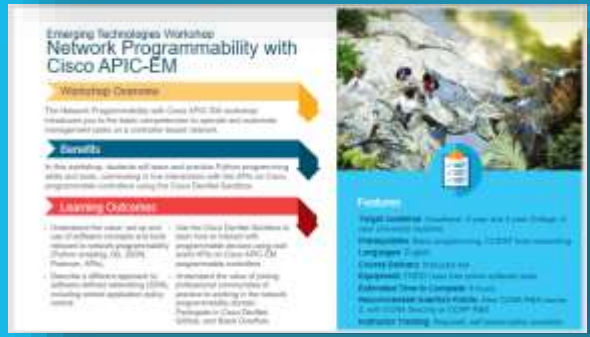
Emerging Technologies Workshops (ETW 1-3)

- Start your #NetDevOps journey with hands-on experience now.



ETWs an der ALP

Nummer	Titel	Zeitraum
99/237R	Digitale Transformation: Neuerungen in der Informationstechnologie	31.08.-04.09.2020 (Blended)
99/239R	Workshop: Künftige Technologien in der Netzwerktechnik	23.11.-27.11.2020 (Blended)
98/6xx	Bei Bedarf Online-Anteil als Lehrgang der ALP	Ab 31.März



Zusatz

Easiest and cleanest transition is after CCNA R&Sv6 ITN students can move to CCNAv7 SRWE then ENSA

Course Migration Options

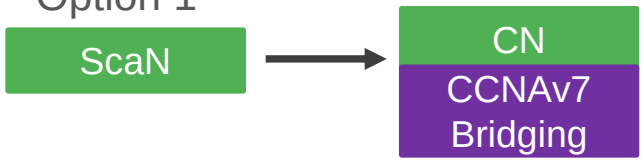
Completed CCNA R&S v6

ITN

+

RSE

Option 1



Advantage: Simplest and feasible to ‘fit’ Bridging topics into CN.
Disadvantage: Large # of topics taught not on new certification. (RIPv2, EIGRP, multi-area OSPF, OSPFv3, GRE, eBGP, Tshoot ACL, IPv6 ACLs, Tshoot NAT, STP Configuration, VTP, Extended VLANs, DTP, PPP & more)

Option 2

Advantage: Small amount of topics taught not on new certification. No Bridging course required.
Disadvantage: Major topic overlap between RSE & SRWE (possibly up to 40% overlap)

Option 3

*Challenge to fit Bridging modules plus missed topics into ENSA course (>70 hrs)

Advantage: Small amount of topics taught but not on certification.
Disadvantage: Topics on certification exam not covered in these courses, Ex: Scaling VLANs, Inter-VLAN routing, STP, Etherchannel, FHRP concepts

Course Migration Options

Completed CCNA R&S v6

ITN

+

RSE

+

ScaN

Option 1

CN

CCNAv7 Bridging

Advantage: Simplest and feasible to ‘fit’ Bridging topics into CN.
Disadvantage: Large # of topics taught not on new certification. (RIPv2, EIGRP, multi-area OSPF, OSPFv3, GRE, eBGP, Tshoot ACL, IPv6 ACLs, Tshoot NAT, STP Configuration, VTP, Extended VLANs, DTP, PPP & more)

Option 2

ENSA

CCNAv7 Bridging 4 Modules*

Advantage: Small amount of topic overlap.
Disadvantage: Significant # of topics covered but not on new certification. (RIPv2, EIGRP, multi-area OSPF, OSPFv3, Tshoot ACL, Tshoot NAT, STP Configuration, VTP, Extended VLANs, DTP & more)

*Challenge to fit Bridging modules into ENSA course (>70 hrs)

ETW – Model Driven Programmability

Überblick

Mit der zunehmenden Größe des modernen Netzwerks und der Häufigkeit der vom Unternehmen geforderten Anpassungen ist die Verwaltung und Automatisierung von Netzwerken über die Kommandozeilenschnittstelle (CLI) ineffizient und fehleranfällig. Ein neuer Ansatz, der die „Model Driven Programmability“ nutzt, ermöglicht transaktionale Änderungen durch die Definition standardisierter Gerätemodelle und APIs. Konfigurations- und Verwaltungsaufgaben mit standardisierten YANG-Geräteklassen und den RESTCONFIG- und NETCONFIG-APIs auf Geräteeben automatisieren

Nutzen

- YANG als Sprache für die Modellierung eines Netzwerkgerätes nutzen
- Networkmanagement Protokolle wie RESTCONFIG und NETCONFIG nutzen
- Python-Skripte schreiben, um ein Netzwerk zu verwalten

Inhalte

- Relevante Werkzeuge nutzen (Python, Git, JSON, Postman, APIs)
- Zentrale Steuerung von Richtlinien
- Gerätekonfigurationen abrufen und aktualisieren
- Netwerk-Wissen nutzen (DEVNet, GitHub, Stack Overflow)

Merkmale

Zielgruppe: Berufsschule, Bachelor, Techniker

Voraussetzungen: Grundlagen der Programmierung, CCNA
Sprache: Englisch

Kursverfügbarkeit: Instruktor geführt

Ausstattung: Virtueller Cisco SW Router, DevNet Sandbox, oder Realequipment mit Cisco ISR 4xxx Router

Zeitaufwand: 8 Stunden

Empfohlene Einstiegshilfen: nach CCNA M2 und Security oder CCNP

Intruktorenqualifizierung: erforderlich, als Selbstlernkurs verfügbar

ETW

– Experimentieren mit REST-APIs mit Hilfe von Webex-Teams

Überblick

Der Workshop "Experimentieren mit REST-APIs mit Webex-Teams" führt in die Erstellung von Anwendungen und die Automatisierung von Aufgaben mit REST-APIs ein.

Nutzen

Innerhalb eines Tages lernen und üben die Teilnehmer Python-Programmierfähigkeiten und -Werkzeuge, bis hin zu Live-Interaktionen mit den APIs über die Online-Plattform Webex Teams.

Inhalte

- Relevante Werkzeuge nutzen (JSON, Postman, APIs)
- Relevanz der REST-APIs-Architektur erkennen und Automatisierung durchführen
- Gerätekonfigurationen abrufen und aktualisieren
- Netwerk-Wissen nutzen (DEVNet, GitHub, Stack Overflow)

Merkmale

Zielgruppe: Berufsschule, Bachelor, Techniker

Voraussetzungen: Grundlagen der Programmierung

Sprache: Englisch

Kursverfügbarkeit: Instruktor geführt

Ausstattung: frei verfügbare Software

Zeitaufwand: 8 Stunden

Empfohlene Einstiegshilfen: PCAP Programming, Grundlagen Python, Connecting Things

Intruktorenqualifizierung: erforderlich, als Selbstlernkurs verfügbar

ETW – Netzwerkprogrammierung mit Cisco APIC-EM

Überblick

Einführung in den Betrieb und die Automatisierung in einem Controller-basierten Netzwerk ein.

Nutzen

Teilnehmer lernen Python und die Verwendung der Cisco DevNet Sandbox, um mit Controller zu interagieren.

Inhalte

- Relevante Werkzeuge nutzen (Python Scripting, Git, JSON, Postman, APIs)
- Software Defined Networking zur Umsetzung von Richtlinien
- Nutzung einer Sandbox
- Netwerk-Wissen nutzen (DEVNet, GitHub, Stack Overflow)

Merkmale

Zielgruppe: Berufsschule, Bachelor, Techniker

Voraussetzungen: Grundlagen der Programmierung, CCNA

Sprache: Englisch

Kursverfügbarkeit: Instruktor geführt

Ausstattung: frei verfügbare Software

Zeitaufwand: 8 Stunden

Empfohlene Einstiegshilfen: CCNA, CCNA Security oder CCNP

Intruktorenqualifizierung: erforderlich, als Selbstlernkurs verfügbar

CCNA 7.0 Downloadable - Policy

From CCNA 7.0 FAQ..

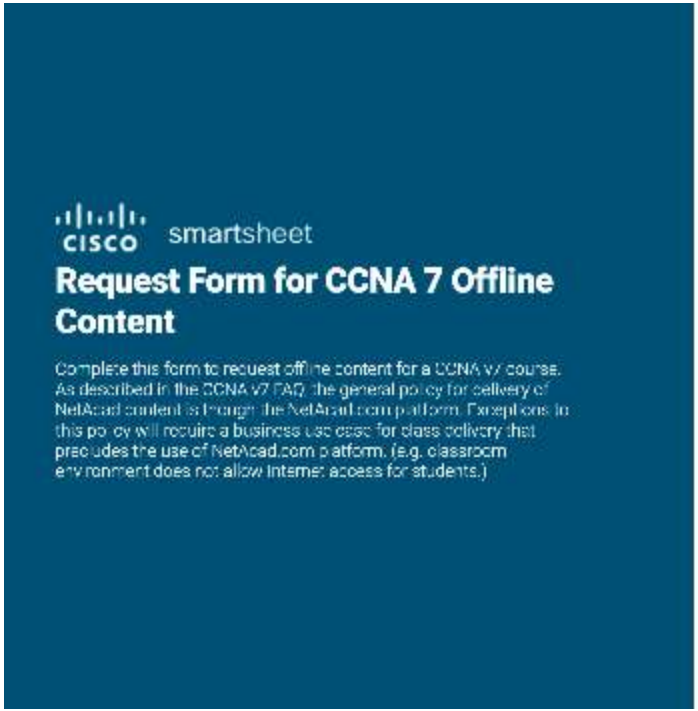
Q22. *Is there an option to download CCNA 7.0 course content to be used offline?*

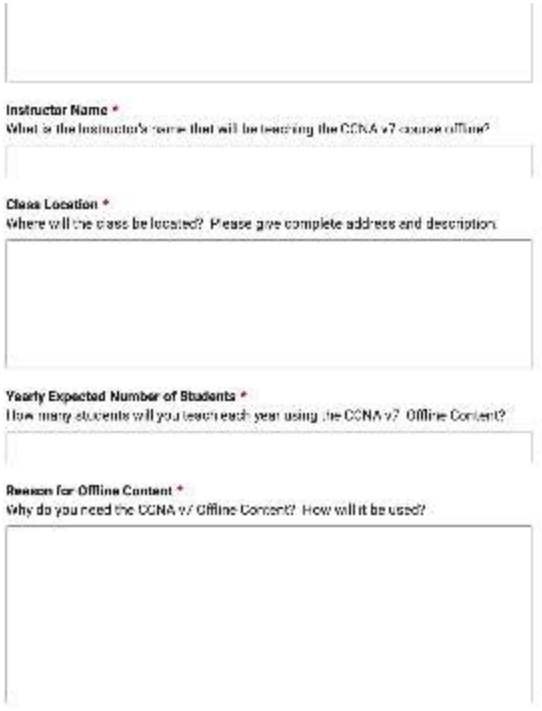
A: *The general policy regarding course delivery is described in the NetAcad Membership Guide (Section 2.2) Academies must ensure that all students taking the class are enrolled in the Cisco NetAcad.com learning platform and use the Networking Academy materials including assessments. NetAcad courses are designed to be delivered using the NetAcad.com platform in order to provide an effective and* ***optimal learning experience*** *for students as well as to* ***protect Cisco's intellectual property*** *contained within these courses. For business cases that cannot comply with this policy and require exception, we will provide a link to an Offline Content Request form that will be available in Jan 2020 and can be used to submit details regarding the need for offline content. If approved, you will be notified with information regarding how to obtain access to the offline content.*

CCNA 7.0 Downloadable - Intended Use Cases

- Primäre Anwendungsfälle – Zugang zu NetAcad.com ist nicht möglich (z.B. Gefängnisse und eingeschränkte militärische Umgebungen)
- Nicht für Anwendungsfälle mit geringer Bandbreite vorgesehen (angepasste Lösung ist in Arbeit)
- Ausführbare Datei für Inbetriebnahme auf Endgeräten (Windows, Mac, Linux)
- Die Lösung wird gerätebezogen installiert (nicht übertragbar)
- Weitere Einschränkungen:
  - Enthält keine Abschluss- oder Modulgruppenprüfungen
  - Es ist nicht möglich, ein Abschlusszertifikat, ein Anerkennungsschreiben oder einen digitalen Nachweis (digital Batch) zu erhalten.
  - Link zum Antrag: http://cs.co/90011eGtR

CCNA 7.0 Downloadable Request Form





Eine Anleitung für die Inbetriebnahme wird mit der Genehmigung zur Verfügung gestellt

New Module: LAN Security Concepts

- **Endpoint Security**: Network attacks, Security devices, Endpoint Protection, Email and Web Security
- **Access Control**: Local Password, Authentication, Authorization, Accounting, 802.1x
- **Security Threats**: Layer 2 Vulnerabilities, Switch Attack Categories, Switch attack mitigation techniques
- **MAC Address Table Attacks** and mitigation
- **LAN Attacks**: VLAN Hopping, VLAN Double Tagging, DHCP Attacks, ARP Attacks, Address Spoofing attacks, STP Attacks, CDP Reconnaissance

New Module: Switch Security Configuration

- **Implement Port Security**: Secure unused ports, Mitigate MAC Address Table Attacks, Enable Port Security, Limit and Learn MAC Addresses, Port Security Aging, Port Security Violation Modes, Ports in err-disabled state, Verify Port Security
- Mitigate **VLAN** Attacks: Mitigate VLAN Hopping
- Mitigate **DHCP** Attacks: DHCP Snooping, Configuration
- Mitigate **ARP** Attacks: Dyn ARP Inspection, DAI Implementation
- Mitigate **STP** Attacks: PortFast and BPDU Guard, Configuration

New Module: WLAN Concepts

- **Introduction to Wireless**: Benefits of Wireless, Type of Wireless networks, Wireless Technologies, 802.11, Radio Frequencies, Wireless Standards Organizaions
- **WLAN Components**: Wireless NIC, Wireless Home Router, Wireless Access Point, AP Categories, Wireless Antennas
- **WLAN Operation**: 802.11 Modes, BSS and ESS, 802.11 Frame Structure, CSMA/CA, Client and AP Association, Passive and Active discovery
- **CAPWAP Operation:** Introduction to CAPWAP, Split MAC Architecture, DTLS Encryption, FlexConnect APs
- **Channel Management:** Frequency Channel Saturation, Channel Selection, Planning a WLAN Deployment
- **WLAN Threats**: DoS attacks, Rouge Access Points, MITM Attack
- **Secure WLANs**: SSID Cloaking and MAC Filtering, 802.11 Original Auth. Methods, Shared Key auth. Methods, Authenticating a home user, Encryption Methods, Auth. In the Enterprise, WPA3

New Module: WLAN Configuration

- **Remote Site WLAN Configuration**: Wireless Router, Log in to Wireless Router, Basic Network setup, Configure a wireless mesh network, NAT for IPv4, QoS
- **Configure a Basic WLAN on the WLC**: WLC Topology, Log into the WLC, View AP Information, Advanced Settings, Configure a WLAN
- **Configure a WPA2 Enterprise WLAN on the WLC**: SNMP and RADIUS, Configure SNMP Server Information, Configure RADIUS Server Information, Configure a VLAN for a New WLAN, Configure a new Interface, Configure a DHCP in a new WLAN, Configure DHCP Scope, Configure WPA2 Enterprise WLAN
- **Troubleshoot WLAN Issues:** Wireless Client not connecting, Network is slow, Updating Firmware

New Module: Network Security Concepts

- **Current State of Cybersecurity**: Current state of Affairs, Vectors of network attacks, Data Loss
- **Threat Actors**: The Hacker, Evolution of Hackers, Cyber Criminals, Hacktivists, State-Sponsored Hackers
- **Threat Actor Tools**: Attack Tools, Evolution of Security Tools, Attack Types
- **Malware**: Viruses and Trojan Horses, Types of Malware
- **Common Network Attacks**: Reconnaissance, Access, Social Engineering, Dos and DDoS
- **IP Vulnerabilities and Threats**: ICMP, Amplification and Reflection, Address Spoofing Attacks
- **TCP and UDP Vulnerabilities**: TCP and UDP Segment Header, TCP Services, TCP Attacks, UDP Attacks
- **IP Services**: ARP Vulnerabilities, ARP Cache poisoning, DNS Attacks, DNS Tunneling, DHCP Attacks
- **Network Security Best Practices**: CIA, Defence-in-Depth approach, Firewalls, IPS, Content Security Appliances
- **Cryptography**: Securing communication, Data Integrity, Hash Functions, Origin Auth., Data Confidentiality, Symmetric Encryption, Asymmetric Encryption, Deffie-Helman

New Module: VPN and IPsec Concepts

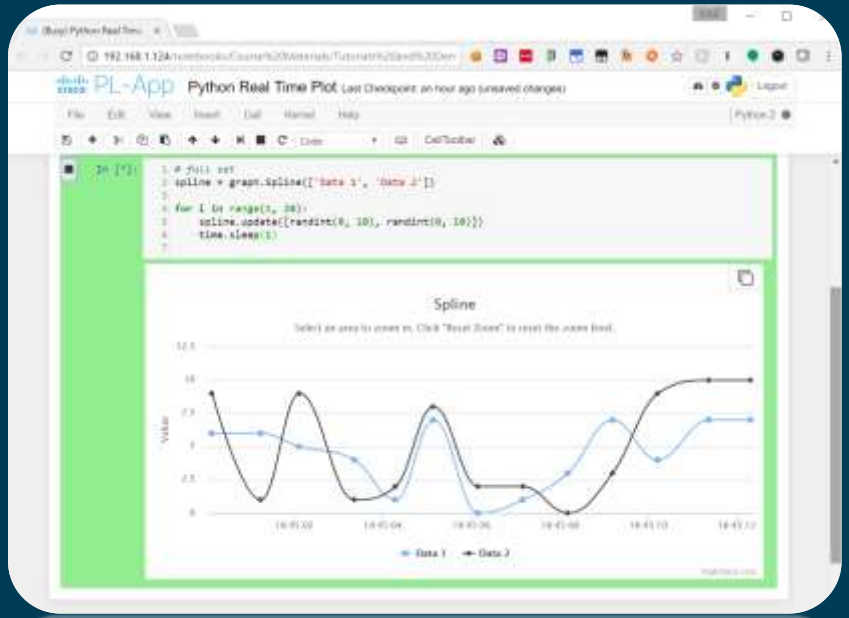
- **VPN Technology**: VPN Benefits, Site-to-Site and Remote-access VPN, Enterprise and Service provider VPN
- **Types of VPN**: Remote-access, SSL, Site-to-Site IPsec, GRE over IPsec, DMVPN, IPsec Virtual Tunnel Interface, Service Provider MPLS
- **IPsec**: IPsec concepts, IPsec technologies, IPsec protocol encapsulation, Confidentiality, Integrity, Authentication, Secure Key Exchange with DH, IPsec transport and Tunnel modes

New Module: Network Automation

- **Automation Overview**
- **Data Formats**: Data formats concept, data format rules, JSON, YAML, XML
- **APIs**: API Concept, API Example, Open, Internal and Partner APIs, Types of Web Service APIs
- **REST**: REST and RESTful API, RESTful implementation, URI/URN/URL, Anatomy of RESTful Request, RESTful API Applications
- **Configuration Management Tools**: Traditional Network Configuration, Network Automation, Ansible, Chef, Puppet, SaltStack
- **IBN and Cisco DNA Center**: Intent Based Networking, Network Infrastructure as Fabric, Cisco DNA, CDA Center

IoTF: PL-App

- Update



Updated PL-App SD-card Images

- New PL-App Image
  - Version 2.2.0 (based on Raspbian Buster)
- **NEW: Support for the new Raspberry Pi 4**
  - **USB-C for power!**
  - Faster CPU & More RAM options (1,2,4GB)
  - Dual Micro-HDMI ports
- Download the updated PL-App Images:
  - Instructor's Resources Page for IoTF: Prototyping Lab
  - Connecting Things (page 3.2.2.3)
  - Big Data & Analytics (page 1.3.2.8)
  - IoT Security (page 1.2.3.1)
  - Hackathon Playbook (page 2.1.2.5)
  - Introduction to IoT (page 2.2.2.5)