

# KOTE

## Selbststudium

### Aufgaben zum begleiteten Selbststudium

Version: 1.2

Autor: Mathias Gut

Zur besseren Lesbarkeit wird auf die gleichzeitige Verwendung der männlichen und weiblichen Sprachform verzichtet. Alle Bezeichnungen gelten gleichwohl für beide Geschlechter.

## Übersicht

Das Modul «KOTE – Kommunikationstechnik» bildet das Fundament für das darauf aufbauende Modul «NPDO - Netzwerk, Planung, Design und Optimierung» und dem abschliessenden Netzwerk Modul «NIUS - Netzwerkinstallation und Störungsbehebung». In diversen Konzepten der Netzwerksicherheit ist ein fundiertes Verständnis der Netzwerktechnik ebenfalls eine Grundvoraussetzung. Die offiziellen CISCO CCNA Lehrmittel werden dabei als Pflichtlehrmittel zur Vertiefung der Inhalte neben dem Folienskript verwendet.

Mit der Lernplattform «<https://www.netacad.com>» steht Dir zusätzlich eine umfassende Wissenssammlung zum freien Selbststudium bereit.

Das KOTE Modul verlangt von Dir neben dem Präsenzunterricht einen Selbststudium Anteil von **28 Lektionen**. Das Selbststudium wird mit den hier vorliegenden Aufgaben geführt und bei Fragen durch Deinen Dozenten im Unterricht begleitet. Die Aufgaben für den jeweiligen Modulblock sind dabei als Richtwert auf ca. 3 Lernstunden für das Selbststudium ausgerichtet. Solltest Du deutlich mehr Zeit für die Aufgaben benötigen, dann teile dies bitte Deinem Dozenten mit. Feedbacks sind immer herzlich willkommen!

Die hier angegebenen Kapitel und Seitenzahlen beziehen sich auf die genutzten Pflichtlehrmittel.

- ☐ Cisco CCNA 200-301 Official Cert Guide Volume 1, Wendell Odom, Pearson, ISBN: 978-0-13-579273-5 (Abkürzung **CCNA1**)
- ☐ Cisco CCNA 200-301 Official Cert Guide Volume 2, Wendell Odom, Pearson, ISBN: 978-1-58714-713-5 (Abkürzung **CCNA2**)

**Wichtig:** Beim Lesen der Inhalte muss nur die gewünschte Fachtiefe gemäss Taxonomie des Fachplans erreicht werden. Die Bücher werden für alle Netzwerkmodule genutzt. Die entsprechende Fachtiefe der Inhalte wird in den Nachfolgemodulen erreicht. Konzentriere dich auf das fundamentale Verständnis der Inhalte und versuche diese in deinem Arbeitsalltag einzuordnen. So ist der Lerneffekt am effektivsten.

## Modulblock 1

- ☐ Repetition der Folieninhalte des Modulblocks:  
Erstelle eine individuelle Zusammenfassung für das KOTE Modul.
- ☐ Kurze Übersicht der Lernhilfen:  
Verschaffe Dir eine allgemeine Übersicht der Lerninhalte in den Büchern und der Lernplattform «<https://www.netacad.com>».
- ☐ Lernstoff Vertiefung:
  - CCNA1 Kapitel 2 «Fundamentals of Ethernet LANs»
  - CCNA2 Kapitel 13 «LAN Architecture»
  - *optional CCNA2 Kapitel 4 «Security Architecture»*
- ☐ **Praxistransfer:**  
Versuche diese Fragen innerhalb Deiner Unternehmung zu klären und nimm die Antworten zur gemeinsamen Besprechung in den Unterricht mit.
  - Wer ist in deinem Unternehmen für das Netzwerk-Management zuständig?
  - Verwendet deine Firma den ISO/OSI-Managementmodell Ansatz? Wenn Nein, welcher andere Standard wird verwendet?
  - Verwendet deine Firma eine 2-Schichten oder 3-Schichten Netzwerkarchitektur?
- ☐ Vorbereitung auf das nächste Modul:
  - CCNA1 Buch Kapitel 1 «Introduction to TCP/IP Networking»
  - Installiere eine aktuelle KALI Linux™ VM ([kali.org](https://kali.org))

\* KALI LINUX™ is a trademark of Offensive Security.

## Modulblock 2

- ☐ Repetition der Folieninhalte des Modulblocks:  
Ergänzen deiner individuellen Zusammenfassung
- ☐ Lernstoff Vertiefung:
  - CCNA1 Kapitel 1 «Introduction to TCP/IP Networking»
  - CCNA1 Kapitel 3 «Fundamentals of WANs and IP Routing»
  - *optional CCNA2 Kapitel 14 «WAN Architecture»*
- ☐ Lernvideos «Youtube»:  
Suche ein gutes Lernvideo über Wireshark und nimm deinen Vorschlag in den Unterricht für den gemeinsamen Austausch mit.

□ **Praxistransfer:**

Analysiere die Webseite deiner Firma mit Wireshark. Nutze dazu Linux. Bringe die Ergebnisse der Aufzeichnungen zur Besprechung in den Unterricht mit.

Versuche folgendes zu filtern:

- Welche DNS-Querys werden beim Öffnen der Webseite gemacht?
- Welches TLS-Protokoll wird für die Webseite genutzt.
- Im TLS-Handshake befindet sich das SNI-Feld. Filtere alle SNI Informationen, welche beim Öffnen der Webseite angezeigt werden.
- Wozu wird SNI «Server Name Indication» bei TLS genutzt?

Auf «<https://github.com/OCSAF/freesvcheck>» findest du ein BASH-Skript, welchen du für deine Zwecke für die Analyse mittels tshark anpassen kannst.

□ Vorbereitung auf das nächste Modul:

Lese dich mittels der HELP und der Manpage in die DNS-Tools **dig** und **nslookup** ein.

## Modulblock 3

□ Repetition der Folieninhalte des Modulblocks:

Ergänzen deiner individuellen Zusammenfassung

□ Lernstoff Vertiefung:

- CCNA2 Kapitel 1 «Introduction to TCP/IP Transport and Applications»
- «[https://de.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](https://de.wikipedia.org/wiki/Transmission_Control_Protocol)»
- «[https://de.wikipedia.org/wiki/User\\_Datagram\\_Protocol](https://de.wikipedia.org/wiki/User_Datagram_Protocol)»
- «[https://de.wikipedia.org/wiki/Domain\\_Name\\_System](https://de.wikipedia.org/wiki/Domain_Name_System)»

□ **Praxistransfer:**

Analysiere die DNS-Zone der Domain deiner Firma mittels **dig** und beantworte die nachfolgenden Fragen. Bringe die Ergebnisse und die genutzten Befehlszeilen deiner Analyse zur Besprechung in den Unterricht mit.

- Wie lautet der A-Record Eintrag?
- Wie lautet der AAAA-Record Eintrag für IPv6?
- Mit welchen dig Optionen kannst du direkt **nur** die IP-Adresse des A-Record als Ausgabe anzeigen?
- Hat es für den A-Record einen «in-addr.arpa» Eintrag?
- Wie lauten die MX-Einträge?
- Welche IP-Adressen sind im MX enthalten?
- Ist ein SPF-Eintrag gesetzt?
- Welche TXT-Einträge sind in der Zone enthalten?
- Ist ein DMARC-Eintrag gesetzt?
- Wird DNSSEC verwendet?

- ☐ Vorbereitung auf das nächste Modul:
  - CCNA1 Buch Kapitel 11 «Perspectives on IPv4 Subnetting»

## Modulblock 4

- ☐ Repetition der Folieninhalte des Modulblocks:  
Ergänzen deiner individuellen Zusammenfassung
- ☐ Lernstoff Vertiefung:
  - CCNA1 Kapitel 11 «Perspectives on IPv4 Subnetting»
  - CCNA1 Kapitel 12 «Analyzing Classful IPv4 Networks»
  - CCNA1 Kapitel 13 «Analyzing Subnet Masks»
  - *optional* CCNA1 Kapitel 18 «Troubleshooting IPv4 Routing»
- ☐ Löse die Subnetz Aufgaben im CCNA1 Buch Kapitel 12 Seite 296-297
- ☐ Lernvideos «Youtube»:  
Suche ein gutes Lernvideo über die IPv4 Subnettierung und nimm deinen Vorschlag in den Unterricht für den gemeinsamen Austausch mit.
- ☐ **Praxistransfer:**  
Versuche diese Fragen innerhalb deiner Unternehmung zu klären und nimm die Antworten zur gemeinsamen Besprechung in den Unterricht mit.
  - Wie sieht das IP-Adressenkonzept mit der dazugehörenden Subnettierung aus?
  - Gibt es verbindliche Regeln für die Subnettierung?
  - Welche Routing Protokolle werden in der Unternehmung verwendet (oder statisches Routing)?
- ☐ Vorbereitung auf das nächste Modul:
  - CCNA1 Buch Kapitel 4 «Using the Command-Line Interface»
  - Installiere den **CISCO Pakettracer** für den nächsten Modulblock

## Modulblock 5

- ☐ Repetition der Folieninhalte des Modulblocks:  
Ergänzen deiner individuellen Zusammenfassung
- ☐ Lernstoff Vertiefung:
  - CCNA1 Buch Kapitel 4 «Using the Command-Line Interface»
- ☐ Lernvideos «Youtube»:  
Suche ein gutes Lernvideo über Switching und nimm deinen Vorschlag in den Unterricht für den gemeinsamen Austausch mit.

□ **Praxistransfer:**

1. Übe mit dem **CISCO Pakettracer** die grundlegenden CLI-Befehle aus dem Modulblock 5:

- Erstelle im Pakettracer einen Cisco 2911 Router
- Nenne den Router R1. Notiere den dazu verwendeten Befehl.
- Konfiguriere das erste Interface (0/0) mit folgender IP-Adresse 10.10.10.1/30 und notiere die dazu verwendeten Befehle.
- Erstelle ein sicheres «enable» Passwort. Notiere den dazu verwendeten Befehl.
- Richte den CLI Zugriff mittels SSH ein. Notiere die dazu verwendeten Befehle.
- Speichere deine Cisco-Router Konfiguration und notiere den dazu genutzten Befehl.
- Prüfe in der Cisco Konfigurationsdatei, dass alle Passwörter «gehashed» sind und notiere den zur Anzeige der Konfigurationsdatei genutzten Befehl.
- Prüfe nun ob alle Passwörter «gehashed» sind. Notiere deine Hashes.
- Speichere die Notizen und die Pakettracer Lösung für die anschliessende Diskussion im nächsten Modulblock.

2. **Optional zur Vertiefung** - Das Protokoll SSH (Secure Shell) wird im Netzwerkbereich besonders häufig genutzt. Du benötigst für dieses optionale LAB eine Linux VM als SSH-Server und als SSH-Client eine zweite Linux VM und eine Windows VM:

- Installiere und aktiviere den SSH-Server auf deiner ersten Linux VM. Notiere den dazu verwendeten Command.
- Verbinde mittels SSH von deiner zweiten Linux VM auf dein Linux SSH-Server System. Notiere den dazu verwendeten Command.
- Installiere auf deiner Windows VM das Tool Putty (putty.org) und verbinde via SSH auf dein Linux SSH-Server System. Erstelle eine entsprechende Installationsanleitung.
- Welche Sicherheitstipps gibt es aus deiner Sicht für die Verbindung mittels SSH? Notiere deine persönlichen Sicherheitstipps.

□ Vorbereitung auf das nächste Modul:

- CCNA1 Buch Kapitel 5 «Analyzing Ethernet LAN Switching»
- CCNA1 Buch Kapitel 6 «Configuring Basic Switch Management»
- CCNA1 Buch Kapitel 8 «Implementing Ethernet Virtual LANs»

## Modulblock 6

- Repetition der Folieninhalte des Modulblocks:  
Ergänzen deiner individuellen Zusammenfassung
- Lernstoff Vertiefung:
  - CCNA1 Buch Kapitel 5 «Analyzing Ethernet LAN Switching»
  - CCNA1 Buch Kapitel 6 «Configuring Basic Switch Management»
  - CCNA1 Buch Kapitel 8 «Implementing Ethernet Virtual LANs»
- Lernvideos «Youtube»:  
Suche ein gutes Lernvideo über Switching und nimm deinen Vorschlag in den Unterricht für den gemeinsamen Austausch mit.
- **Praxistransfer:**  
Erstelle mit dem **CISCO Pakettracer** ein Beispiel-Netzwerkdesign. Konzentriere dich dabei auf das Switching. Wir besprechen im Unterricht gemeinsam die verschiedenen Designvorschläge, Konzeptvorgaben und eigenen Erfahrungen. Du kannst dazu ein bekanntes Beispielnetzwerk verwenden oder ein eigenes Beispiel entwickeln.
  - Mache bei allen Switchen eine Grundkonfiguration gemäss den Folieninhalten. Nutze dabei die aus deiner Sicht sinnvollen Geräte im Pakettracer auch wenn die «simulierten» CISCO Switche nicht mehr aktuell sind. *«Konzentriere Dich vor allem auf das Design.»*
  - Beantworte mindestens folgende Fragen:
    - Beachtest du unternehmenseigene Vorgaben beim Konzept?
    - Was ist dir im Konzept wichtig?
    - Wo siehst du die Herausforderungen?
    - Verwendest du dabei VLANs nach 802.1Q?
    - Weist dein Switch-Design Redundanzen auf und ist so vor Ausfällen von Netzwerkverbindungen und Switchen geschützt?
  - Welche Switche verwendet ihr in eurem Unternehmen und wie werden diese konfiguriert, verwaltet und überwacht?
- Vorbereitung auf das nächste Modul:
  - CCNA1 Buch Kapitel 9 «Spanning Tree Protocol Concepts»
    - Verschaffe dir hier nur eine kurze Übersicht betreffend STP. Die Vertiefung der Thematik erfolgt erst im Nachfolgemodul – «NPDO - Netzwerk, Planung, Design und Optimierung»

## Modulblock 7

- ☐ Repetition der Folieninhalte des Modulblocks:  
Ergänzen deiner individuellen Zusammenfassung
- ☐ Lernstoff Vertiefung:
- ☐ - CCNA1 Buch Kapitel 9 «Spanning Tree Protocol Concepts»
  - Verschaffe dir hier nur eine kurze Übersicht betreffend STP. Die Vertiefung der Thematik erfolgt erst im Nachfolgemodul – «NPDO - Netzwerk, Planung, Design und Optimierung»
- ☐ **Praxistransfer:**  
Erstelle mit dem **CISCO Pakettracer** ein Beispiel-Netzwerkdesign für eine KMU mit mehreren Switchen und einem Router. Konfiguriere das gesamte Netzwerk mit zwei VLANs und Subnetzen.
  - Wir besprechen verschiedene Designs im Unterricht. Versuche möglichst viel mit Textfeldern direkt im Pakettracer zu dokumentieren.
- ☐ Vorbereitung auf das nächste Modul:  
Repetition der Cisco CLI Commands

## Modulblock 8

- ☐ Repetition der Folieninhalte des Modulblocks:  
Ergänzen und finalisieren deiner individuellen Zusammenfassung