Versuch 2: Basiskonfiguration von Routern und Switches

(Version für Packet-Tracer)

Ziel dieses Versuches ist es, die grundlegende Konfiguration von Switches und Routern für eine einfache Netztopologie vorzunehmen. Anschließend soll die Konfiguration mit geeigneten Befehlen überprüft und die Erreichbarkeit der Netzelemente getestet werden. Der Versuch basiert auf der Nutzung des Cisco Simulationstools Packet-Tracer.

Installation von Packet-Tracer

Dieser Versuch erfolgt auf Basis von Packet-Tracer. Packet-Tracer ist das Cisco Simulationstool für Netzwerke. Besorgen Sie sich Packet-Tracer, z.B. indem Sie sich unter www.netacad.com/courses/intro-packet-tracer/ für den Selbstlern-Kurs „**Introduction to Packet Tracer**“ (kostenlos) einschreiben. Dann können Sie Packet-Tracer herunterladen und installieren (vgl. auch Folie 14 in KN_00_Organisation).

Hinweis: Das vorliegende Praktikum funktioniert auch mit älteren Versionen von Packet-Tracer.

Im Folgenden wird davon ausgegangen, dass Sie Packet-Tracer nutzen können.

Versuchsvorbereitung

Eine Konfigurationsanleitung für das Praktikum finden Sie im Lernraum der Vorlesung. In der Konfigurationsanleitung sind sämtliche im Praktikum verwendeten Kommandos für Router und Switches zusammengefasst erläutert. Diese Konfigurationsanleitung benötigen Sie für den Versuch.

Lesen Sie die Versuchsanleitung gründlich durch und erarbeiten (und notieren) Sie sich bitte *schon während der Vorbereitung* (!) mit Hilfe der Konfigurationsanleitung zu jedem Konfigurationsschritt die jeweils erforderlichen IOS-Befehle.

Details zu nützlichen `show`-Befehlen und zu seriellen WAN Verbindungen finden Sie im Anhang dieser Versuchsunterlagen.

Beantworten Sie zur Vorbereitung zunächst die folgenden Fragen:

1. Betrachten Sie Versuchstopologie nach Abbildung 1.

   Welches Netzelement stellt für PC1 das Default Gateway dar und welches für PC2? Wie verhält es sich bei dem Switch S1? Welche IP-Adresse muss auf den Geräten jeweils als Default Gateway konfiguriert werden? Tragen Sie die Routernamen und IP-Adressen in die Tabelle ein!

Default Gateway für	Netzelement (welcher Router?)	mit welcher IP-Adresse?
PC1	R1	192.5.5.1
PC2	R2	219.17.100.1
Switch S1	R1	192.5.5.1

2. Machen Sie sich mit Hilfe von Anhang B mit der Verwendung der seriellen Verbindungen (als Ersatz für „echte“ Weitverkehrsverbindungen) vertraut. Was ist hinsichtlich des Befehls `clock rate` zu beachten?
3. Lesen Sie auch die optionalen Zusatzaufgaben. Welches Protokoll sollte man anstelle von Telnet verwenden, wenn man dabei verschlüsselt kommunizieren möchte?

Versuchsdurchführung

1. Aufbau der Netztopologie und IP-Konfiguration der PCs

1.1 Geräte Auswählen

Nach dem Starten von Packet-Tracer können Sie unten links Netzkomponenten/Geräte auswählen. Wählen Sie *Network Devices* und darunter *Routers* aus. Dann ziehen Sie zwei *2901 Router* auf die Arbeitsfläche Wählen Sie *Network Devices* und darunter *Switches* aus. Ziehen Sie einen *2960* Switch auf die Arbeitsfläche. Wählen Sie unten links *End Devices* aus und ziehen Sie 2 PCs (*Generic*) auf die Arbeitsfläche.

Auf der Arbeitsfläche haben Sie jetzt 2 PCs, ein Switch und 2 Router. Ordnen Sie die Geräte wie in Abb. 1 dargestellt an.

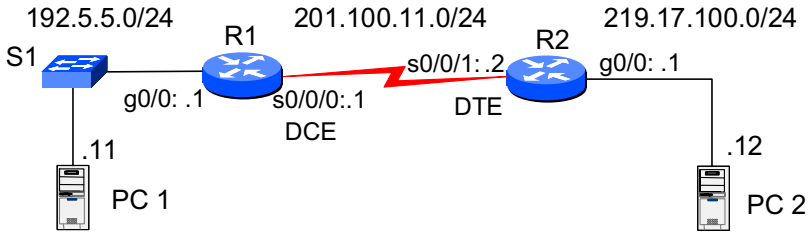


Abbildung 1: Topologie

		IP-Adresse	Subnetzmaske
PC1	FastEthernet0	192.5.5.11	255.255.255.0
PC2	FastEthernet0	219.17.100.12	255.255.255.0
R1	GigabitEthernet0/0	192.5.5.1	255.255.255.0
R2	GigabitEthernet0/0	219.17.100.1	255.255.255.0
R1	Serial0/0/0	201.100.11.1	255.255.255.0
R2	Serial0/0/1 (!)	201.100.11.2	255.255.255.0

1.2 Gerätenamen anpassen

Wenn Sie die Gerätebezeichnung anklicken, können Sie den angezeigten Gerätenamen ändern. Passen Sie die Gerätenamen an Abb.1 an, z.B. PC0 => PC1 und Router0 => R1.

1.3 Die Router mit seriellen Interfaces ausstatten

Wenn Sie mit der Maus auf ein Gerät gehen (ohne zu Klicken), werden die Interfaces des Geräts angezeigt. Bei den Routern sehen Sie, dass diese lediglich über GigabitEthernet-Interfaces verfügen. Um den Router mit seriellen Interfaces auszustatten, klicken Sie auf R1 und wählen Sie *Physical*. Mit *Zoom In* können Sie die Darstellung vergrößern. Netzwerkkarten können Sie nur ergänzen, wenn der Router ausgeschaltet ist.

Lokalisieren Sie den Netzschalter und schalten Sie den Router durch einen Klick auf den Netzschalter aus.

Links wird eine Auswahl von Netzwerkkarten angezeigt. Wir verwenden die Netzwerkkarte HWIC-2T. Klicken Sie auf HWIC-2T und ziehen Sie die Netzwerkkarte in den rechten freien Slot des Routers. Anschließend schalten Sie den Router wieder ein.

Verfahren Sie in gleicher Weise mit R2.

Gehen Sie in der Arbeitsfläche mit der Maus nacheinander auf die Router und kontrollieren Sie, dass die Interfaces Serial 0/0/0 und Serial 0/0/1 bei beiden Routern angezeigt werden.

1.4 Komponenten verkabeln

Klicken Sie im Packet-Tracer unten links auf *Connections*. Rechts daneben werden dann verschiedene Verbinder angezeigt, unter anderem *Copper Straight-Through* und *Copper Cross-Over*. Klicken Sie den gewünschten Verbinder an. Anschließend klicken Sie (Linke Maustaste) auf das Gerät, das Sie anschließen möchten. Es erscheint eine Übersicht über die Schnittstellen des Geräts. Wählen Sie die gewünschte Schnittstelle aus… und der Stecker sitzt. Verfahren Sie ebenso mit dem anderen Ende des Verbinders.

Verkabeln Sie die Topologie wie in Abb. 1 angegeben.

Beim Switch nutzen Sie selbstgewählte FastEthernet Interfaces, bei den Routern die in der Topologie angegebenen Interfaces g0/0 (= GigabitEthernet 0/0).

Für die serielle Verbindung wählen Sie Serial DCE. Achten Sie darauf, dass DCE an Serial 0/0/0 von R1 angeschlossen wird und das andere Ende an Serial0/0/1 von R2.

Welche Art von Kabel verwenden Sie zum Anschluss eines PCs an einen Switch? Straight-Through

Welche Art von Kabel verwenden Sie zum Anschluss eines Switch an einen Router? Straight-Through

Welche Art von Kabel verwenden Sie zum Anschluss eines PCs an einen Router? Cross-Over

1.5 IP-Konfiguration der PCs

Klicken Sie auf einen PC. Es öffnet sich ein Fenster mit mehreren Reitern. Unter *Desktop* => *IP Configuration* erfolgt die IP-Konfiguration des PCs. Konfigurieren für jeden PC

1. IP-Adresse, **2. Subnetzmaske** und **3. Default-Gateway**

gemäß der Topologie und der Tabelle aus Ihrer Versuchsvorbereitung. Achten Sie darauf, dass die *IP-Configuration* auf *Static* steht.

2 Allgemeines zur Konfiguration von Routern und Switches

Router und Switches haben in der Regel weder eine Tastatur noch einen Bildschirm. Die Erstkonfiguration der Geräte erfolgt i.d.R. über einen Konsolenanschluss. Dazu wird das Gerät über ein Konsolenkabel (Rollover-Kabel) mit der seriellen Schnittstelle (COM) eines PCs verbunden. Die Konfiguration erfolgt dann auf der Kommandozeile über einen Terminal Emulator vom PC aus.

Bei der Simulation mit Packet-Tracer gelangen Sie über einen Klick auf das Gerät und Auswahl von CLI (Command Line Interface) direkt auf die Kommandozeile/Konsole des Geräts. Hier erfolgt die Konfiguration auf Basis des *Cisco Internetwork Operating System* (*IOS*). Dabei sind die meisten Befehle der Basiskonfiguration für Router und Switches identisch.

3 Basiskonfiguration des Switches

Zur Konfiguration des Switches klicken Sie auf den Switch und wählen Sie CLI (Command Line Interface). Nach dem Betätigen von <Enter> sind wird der Prompt `Switch>` angezeigt. Sie befinden sich an der Konsole des Switches im User-Exec-Mode (kurz User-Mode).

3.1 Wechsel der Befehlsmodi

Für die Bedienung des Cisco IOS ist es wichtig zu wissen, dass bestimmte Aufgaben immer nur in den dafür vorgesehenen Befehlsmodi ausgeführt werden können. Neben dem User Mode, der in erster Linie nur einfache Befehle zum Ansehen und Testen zur Verfügung stellt, kennt das Cisco IOS weitere Befehlsmodi, in denen der volle Funktionsumfang, insbesondere auch die Befehle zur Konfiguration zur Verfügung stehen.

Dieses sind der Priviledged EXEC Mode und die darin verfügbaren Modi zur Konfiguration, der globale Konfigurationsmodus für einfache Konfigurationsaufgaben und viele spezifische Konfigurationsmodi für speziellere Aufgaben.

Wechseln Sie zwischen den verschiedenen Modes hin und her (=> Konfigurationsanleitung 1.3). Tragen Sie die Kommandos zum Wechsel zwischen den Modes in Abb. 2 ein.

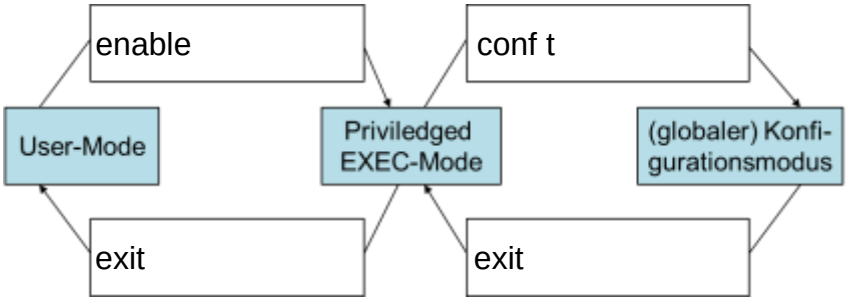


Abb. 2 Befehlsmodi und Befehle zum Wechseln

3.2 Abschalten der DNS-Clientfunktionalität

Schalten Sie die DNS-Clientfunktionalität des Switches ab (=> KonfigAnleitung 1.4, achten Sie auf den korrekten Modus!).

Das sollten Sie bei der Konfiguration im Praktikum immer zuerst machen, weil sonst bei einem Tipp-Fehler bei der Befehlseingabe häufig erst eine langwierige DNS-Namensauflösung versucht wird.

Hintergrund: Das IOS interpretiert einen unbekannten Begriff zunächst als Versuch ein Gerät dieses Namens per Telnet zu erreichen und muss daher eine (hier) erfolglose DNS-Abfrage starten.

3.3 Kontextbasierte Hilfefunktion

Das Cisco IOS stellt eine nützliche Hilfefunktion zu den jeweils verfügbaren Befehlen und deren Syntax zur Verfügung. Machen Sie sich anhand der Konfigurationsanleitung 2.1 mit der Hilfefunktion des Fragezeichens `[?]` und der Autovervollständigung von Kommandos vertraut.

Geben Sie folgende Kommandos in der angegebenen Reihenfolge ein und vervollständigen Sie die Tabelle:

Kommando-Eingabe	Welches Kommando wurde erkannt bzw. ausgeführt?	Bemerkungen
`Switch>show clock [enter]`	show clock	Uhrzeit/Datum
`Switch>show clo [enter]`	show clock	Uhrzeit/Datum
`Switch>show cl [enter]`	show clock	Uhrzeit/Datum
`Switch>show c?`	show c?	Hilfe-Funktion

`Switch>show clo [Tab]`	show clock	Vervollständigung

Wie lautet das hinsichtlich der Zeichenanzahl kürzeste Kommando, um in den Konfigurationsmode zu wechseln?

conf t

3.4 Konfiguration des Gerätenamens

Geben Sie dem Switch den Namen S1 (Konfigurationsanleitung 1.5).

3.5 Basiskonfiguration: Zugangsschutz – Setzen lokaler Passwörter

Ein Netzelement sollte natürlich nicht für jedermann zugänglich sein. Dieses gilt bereits für den User Mode und umso mehr noch für den Priviledged Mode, in dem man die Konfiguration dann sogar verändern könnte. Dazu bedarf es eines Zugangsschutzes, der über das Setzen von Passwörtern realisiert wird. Häufig gibt es ein zweistufiges Konzept für die Zugangserlaubnis: Ein gewisser Personenkreis darf den User Mode nutzen und ein noch strenger eingeschränkter Kreis kennt auch noch das Passwort für den Priviledged Mode.

*Der Einfachheit halber und um nicht durcheinander zu kommen, verwenden wir für die Praktika **ausschließlich Standard-Passwörter**. Diese Passwörter lauten:*

-> ***cisco*** *-> für alle Passwörter, außer:*

-> ***class*** *-> nur für das enable secret password.*

Das Vorgehen zum Zugangsschutz finden Sie in der Konfigurationsanleitung 1.6.

- ⇨ Setzen Sie *cisco* als Passwort für den Konsolenzugang (User-Mode).
- ⇨ Wie viele virtuelle Zugänge (Telnet-Zugänge) unterstützt der Switch? 16
- ⇨ Setzen Sie für alle diese Zugänge *cisco* als Passwort.
- ⇨ Setzen Sie *class* als Passwort für den Priviledged Mode.

3.6 Zugangsschutz – Rechtlicher Hinweis (Login Banner)

Häufig ist es rechtlich erforderlich, vor dem Zugang zu einem System mit einer entsprechenden Warnmeldung vor den rechtlichen Konsequenzen eines unauthorisierten Zugriffs zu warnen. Dieses wird unter Cisco IOS mit einem Login Banner, auch „message of the day (MOTD)” genannt, realisiert. Der zugehörige Befehl erfordert zur Begrenzung der Nachricht ein identisches Start- und Endezeichen, dass nicht im Banner vorkommen darf. (Konfigurationsanleitung 1.7). Konfigurieren Sie als Banner die Nachricht: *Zugang nur für <Ihr Name> !*

3.7 Test des Zugangsschutzes

Loggen Sie sich aus, in dem Sie 2x hintereinander `exit` eingeben. Kontrollieren Sie, dass vor der Passworteingabe das Banner angezeigt wird und loggen Sie sich ein, bis in den Priviledged Mode.

3.8 Anzeigen der aktuellen Konfiguration (running-config)

Ein wichtiger Befehl, mit dem Sie die ausgeführten Konfigurationsänderungen überprüfen können, ist `show running-config`. Damit wird die aktuelle Konfiguration angezeigt.

Geben Sie im Priviledged Mode den Befehl `show run` ein. Die Konfiguration wird Ihnen seitenweise angezeigt, Sie können bei `--More--` mit [enter] jeweils eine weitere Zeile, mit der Leertaste eine weitere Seite anzeigen lassen oder mit jeder anderen Taste die Ausgabe abbrechen. Sie sehen nun (neben einigen vorgegebenen Konfigurationen) alle Befehle, die Sie bisher konfiguriert haben. Bitte achten Sie insbesondere auf die Darstellung des Passwortes bei der Verwendung von enable secret: Es wird verschlüsselt dargestellt, damit man es in der Ausgabe und der Textdatei zur Konfiguration nicht lesen kann.

3.9 Speichern der aktuellen Konfiguration

Üblicherweise möchte man die Konfiguration eines Netzelementes auch abspeichern, damit Sie bei einem möglichen Neustart wieder verwendet wird und nicht wieder neu eingegeben werden muss. Bei Cisco Geräten wird die Startkonfiguration in der `startup-config` Datei gespeichert.

Testen Sie zunächst, ob eine Startkonfiguration vorhanden ist:

```
S1# show startup-config
```

Anschließend speichern Sie die aktuelle Konfiguration als Startkonfiguration:

```
S1#copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
```

3.10 Anzeige der Interfaces und ihrer Zustände

Um den Zustand der Interfaces (up oder down) in einer übersichtlichen, tabellarischen Form abzurufen, verwendet man am besten den Befehl:

```
S1#show ip interface brief
```

Man erhält eine Übersicht über die Interfaces des Geräts und den Status der OSI-Schichten 1 (Physical Layer) und 2 (Schicht 2 Protokoll). Für ein funktionsfähiges Interface müssen beide „up“ lauten, andernfalls liefert die Anzeige des Status erste Hinweise für eine Fehlersuche.

Warum ist nur ein Interfaces des Switches „up“? Welches?

0/1, da nur ein PC angeschlossen ist

3.11 Konfiguration von IP-Adresse und Default Gateway für den Switch

Auf konfigurierbaren Switches, wie den hier verwendeten, kann häufig auch eine IP-Adresse für die Management-Instanz vergeben werden, damit die Switches über das Netz remote konfiguriert werden können (z.B. per Telnet oder SecureShell).

Konfigurieren Sie auf Switch S1 die IP-Adresse 192.5.5.20 /24 (Subnetzmaske: 255.255.255.0) für VLAN 1. (KonfigAnleitung 5.1).

Zur Erläuterung: In diesem Versuch wird auf dem Switch noch nicht zwischen sog. VLANs (virtuellen LANs) unterschieden (die erst später in der Vorlesung behandelt werden). Alle Interfaces des Switches gehören hier noch zu einem LAN (mit der Default-Kennung VLAN 1) und damit auch die Management-Instanz, für das auf diesem Wege ein virtuelles Interface erzeugt wird.

Prüfen Sie mittels ping von der *Konsole des Switches*, ob Sie PC1 erreichen können.

Kommando: ping 192.5.5.20

Wie viele Anfragen erzeugt ein Ping unter Cisco IOS standardmäßig? 4

Mit welchem Zeichen wird ein erfolgreicher Versuch dargestellt? ✓

Mit welchem Zeichen wird ein nicht erfolgreicher Versuch dargestellt? X

Damit der Switch selbst auch Netzelemente in entfernten Netzen erreichen kann, benötigt er auch ein Default Gateway (wie auf jedem Host: Der Routerport im eigenen Netz, der zur Verbindung mit anderen Netzen verwendet werden soll).

Konfigurieren Sie auf S1 das Default Gateway (KonfigAnleitung 5.2) mit der IP-Adresse aus der Tabelle aus Ihrer Versuchsvorbereitung.

4 Basiskonfiguration der Router

Die Konfiguration der Router verläuft in weiten Teilen identisch zur Konfiguration des Switches.

Nach dem Abschluss des Bootvorgangs mit <enter> werden Sie auf der CLI werden Sie gefragt, ob Sie einen Konfigurationsdialog verwenden wollen. Hier geben Sie bitte im gesamten Praktikum immer **no** ein.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Führen Sie anschließend in derselben Weise wie auf dem Switch für die beiden Router folgende Konfigurationen durch:

- ⇨ Schalten Sie die DNS-Clientfunktionalität ab.
- ⇨ Konfigurieren Sie R1 bzw. R2 als Gerätenamen.
- ⇨ Setzen Sie *cisco* als Passwort für den User-Mode (Konsole) und für alle virtuellen Zugänge.
- ⇨ Setzen Sie *class* als Passwort für den Priviledged Mode.
- ⇨ Konfigurieren Sie als Zugangsmeldung „*Zugang nur für <Ihr Name>!*“
- ⇨ Prüfen Sie, ob die Router eine Startkonfiguration aufweisen.
- ⇨ Speichern Sie die aktuelle Konfiguration als Startkonfiguration.

4.1 Konfiguration der Ethernet Interfaces auf den Routern

Konfigurieren Sie das GigabitEthernet 0/0 Interface (kurz g0/0) auf den Routern R1 **und** R2 mit den IP-Adressen und Netzmasken aus der Tabelle unter Abb. 1. Wählen Sie dabei eine eigene Beschreibung (description). Die Konfigurationsbefehle finden Sie in Abschnitt 4.1 der Konfigurationsanleitung.

Der Befehl `no shutdown` dient zum Einschalten des Interfaces.

Hieran wird eine bei Cisco übliche Konfigurationsweise deutlich: Eingegebene Befehle können durch die Wiederholung des Befehls mit vorangestelltem `no` rückgängig gemacht werden. Interfaces werden angeschaltet, in dem man ihren ausgeschalteten Zustand rückgängig macht.

Lassen Sie sich die Interfaces mit `show ip int brief` anzeigen und kontrollieren Sie, ob das Interface g0/0 auf R1 und auf R2 eingeschaltet ist und die korrekte IP-Adresse hat.

4.2 Kontrolle der Ethernet-Verbindung

Wenn bis hierhin alles korrekt konfiguriert wurde, müssten die PCs jetzt ihre Default-Gateways per Ping erreichen können. Gehen Sie auf PC1 auf Desktop => CommandPromt (ggf. vorher die IP-Configuration schließen). Pingen Sie von PC1 aus R1 an: `ping 192.5.5.1`

Pingen Sie von PC2 aus R2 an. Kommando: ping 219.17.100.1

Beides sollte funktionieren. Falls nicht, suchen und beheben Sie den Fehler.

4.3 Konfiguration der seriellen Verbindung zwischen den Routern

Die Konfiguration serieller Interfaces ist sowohl im Anhang als auch in der Konfigurationsanleitung 4.2 beschrieben. DCE ist das Interface s0/0/0 auf R1, DTE ist s0/0/1 auf R2.

Konfigurieren Sie die Interfaces so, dass die Kommunikation mit einer Taktrate von 128.000 Bit pro Sekunde erfolgt!

In welcher Einheit (bit/s / kbit/s) gibt man die Geschwindigkeit jeweils an:

	Einheit (bit/s, kbit/s)	Konfigurierter Wert
`clock rate`	bit/s	128000
`bandwidth`	kbit/s	128

Ordnen Sie die Befehle `clock rate` und `bandwidth` den folgenden Aussagen zu:

Legt die Übertragungsgeschwindigkeit der Leitung physikalisch fest	clock rate
Reicht diesen Wert an Routing-Protokolle etc. weiter	bandwidth

Welchen der Befehle dürfen Sie nur auf der **DCE-Seite** eingeben? clock rate

Lassen Sie sich die Interfaces mit `show ip int brief` anzeigen und kontrollieren Sie, ob die konfigurierten seriellen Interface s0/0/0 auf R1 und s0/0/1 auf R2 eingeschaltet sind und die korrekte IP-Adresse aufweisen.

Kontrollieren Sie die Funktion, in dem Sie auf R1 versuchen R2 per Ping zu erreichen.

Kommando: `R1#ping` 201.100.11.2

Falls der Ping nicht erfolgreich ist, suchen und beheben Sie den Fehler.

4.4 Erreichbarkeitstests für entfernte Netze

Versuchen Sie, von PC1 aus R2 an zu pingen. Erhält PC1 eine Antwort von R2? Nein

Schauen Sie sich mit `show ip route` auf R2 die Routing-Tabelle an. In dieser sind sämtliche Netze angegeben, die R2 kennt.

Weshalb kann R2 den PC1 nicht erreichen? R2 kennt PC1 nicht.

Versuchen Sie, von R1 aus PC2 an zu pingen. Erhält R1 eine Antwort von PC2? Nein

Schauen Sie sich mit `show ip route` auf R1 die Routing-Tabelle an. In dieser sind sämtliche Netze angegeben, die R1 kennt.

Weshalb kann R1 den PC2 nicht erreichen? R1 kennt PC2 nicht.

Nach der Interface Konfiguration kennen die Router nur die direkt angeschlossenen Netze.

Woran sind direkt angeschlossenen Netze in der Routing-Tabelle erkennbar?
"*IP* is directly connected"

4.5 Konfiguration eines Routing Protokolls

Jetzt konfigurieren Sie die Router so, dass sie sich untereinander über die nicht direkt angeschlossenen Netze informieren und diese in ihre Routingtabellen aufnehmen. Dieses wird in der Vorlesung noch zu einem späteren Zeitpunkt vertieft. Sie verwenden das Routingprotokoll RIP (=> KonfigAnleitung 4.6).

Auf Router R1:

```
R1(config)#router RIP
R1(config-router)#network 192.5.5.0
R1(config-router)#network 201.100.11.0
```

Auf Router R2:

```
R2(config)#router RIP
R2(config-router)#network 201.100.11.0
R2(config-router)#network 219.17.100.0
```

Zur Erläuterung: Mit dem Befehl `router RIP` aktivieren Sie RIP als Routing-Protokoll auf Ihrem Router. Danach müssen Sie festlegen, welche der direkt angeschlossenen Netze des Routers am Routing mit RIP teilnehmen sollen (in diesem Fall jeweils beide). Das geschieht im Router-Konfigurationsmodus (`(config-router)#`) für jedes betroffene Netz mit dem `network`-Befehl unter Angabe der Netzadresse.

Überprüfen Sie die Routing-Tabellen nun noch einmal mit `show ip route`. Sind nun jeweils drei Netze vorhanden?

4.6 Überprüfung der Konfiguration mit Hilfe der show-Befehle

Für die weitere Prüfung der Konfiguration bieten sich insbesondere die folgenden Befehle an:

a) Überprüfen Sie Ihre Router-Konfiguration mit dem Befehl `show running-config`.

b) Überprüfen Sie den Status der Routerinterfaces mit `show ip interface brief`. Sind alle benötigten Interfaces aktiviert und alle nicht benötigten deaktiviert?

c) Sehen Sie sich außerdem auch die detailliertere Ausgabe des Befehls `show interfaces <Interfacebezeichner>` an. Auch hier erhalten Sie neben vielen anderen Informationen über das betreffende Interface eine Auskunft zu dessen Status (up/down). Sehen Sie hier bitte speziell nach der IP-Adresse und der MAC-Adresse der Ethernet-Interfaces.

Hinweis: Damit ein Interface sich im Status „up“ befindet, ist es jeweils erforderlich, dass dieses mit einer ebenfalls aktivierten Gegenseite verbunden ist. Sie werden also ggf. noch Interfaces im Zustand „down“ vorfinden, falls das entsprechende Interface der Gegenseite Nachbarrouters noch nicht vollständig konfiguriert oder aktiviert wurde. Dies gilt insbesondere für die seriellen Verbindungen, die auf beiden Seiten korrekt (DCE/DTE) konfiguriert und aktiviert sein müssen.

4.7 Testen der Erreichbarkeit mit ping und traceroute

Abschließend sollen Sie die Erreichbarkeit der Netzelemente in der Topologie testen. Die PCs, der Switch und die Routerinterfaces sollten nun untereinander erreichbar sein. Falls ein Element nicht erreichbar sein sollte, überlegen Sie, woran es liegen könnte und versuchen Sie den Fehler zu beheben.

a) Testen Sie, ob Sie die Routerports von beiden PCs aus mittels `ping` erreichen können.

b) Testen Sie, ob von jedem PC auch der andere PC und der Switch erreichbar sind.

c) Testen Sie die Verbindung zwischen den PCs mit Hilfe von `tracert`. (dem Windows-Befehl für die Traceroute-Anwendung).

Optionale Zusatzaufgaben

5 Konfiguration einiger zusätzlicher Sicherheitsaspekte (Zusatzaufgabe)

Die im Praktikum immer gleich verwendeten Passwörter „cisco“ und „class“ sind natürlich nur für einen reibungslosen Praktikumsbetrieb sinnvoll und in der Praxis völlig ungeeignet. (Überlegen Sie einige Schwächen, warum das so ist.) Das Cisco IOS sieht zahlreiche Maßnahmen vor, den Zugangsschutz sicherer zu gestalten. Einige davon lernen Sie hier kennen:

5.1 Strengere Vorgaben für Passwörter (z.B. Mindestlänge)

Bei der Konfiguration von Passwörtern unter Cisco IOS kann die Sicherheit dadurch erhöht werden, dass eine Mindestlänge in Zeichen (hier z.B.: 10 Zeichen) vorgegeben wird. Dann werden bei der Konfiguration aller Zugangspasswörter keine kürzeren Passwörter mehr akzeptiert. (bitte hier nicht ausprobieren, das Ergebnis sollte klar sein):

```
R1(config)#security passwords min-length 10
```

Hinweis: Bereits vorher konfigurierte Passwörter mit weniger Zeichen bleiben bestehen; erst bei nach Eingabe des Befehls neu konfigurierten Passwörtern wird die vorgegebene Mindestlänge eingefordert.

5.2 Sitzungen bei Inaktivität automatisch beenden

Für den Konsolen- und die Telnet bzw. SSH-Zugänge kann ein Timer konfiguriert werden, nach dessen Ablauf eine Sitzung bei Inaktivität beendet wird (im Bsp.: nach 5 Minuten, 0 Sekunden):

```
R1(config)#line console 0
R1(config-line)#exec-timeout 5 0
R1(config-line)#line vty 0 4
R1(config-line)#exec-timeout 5 0
R1(config-line)#exit
```

5.3 Login-Versuche blockieren

Außerdem können die Zugänge bei wiederholten fehlerhaften Login-Versuchen blockiert werden, um sog. Brute Force Angriffe (= wiederholtes Ausprobieren der Zugangsdaten) zu unterbinden. Beispielsweise wird mit dem Befehl

```
R1(config)#login block-for 30 attempts 2 within 120
```

der Zugang für 30s blockiert, wenn in 120 Sekunden 2 fehlerhafte Versuche registriert wurden.

Konfigurieren Sie den Router so, dass die Zugänge für 15s blockiert werden, wenn 3 fehlerhafte Versuche in 60 Sekunden unternommen wurden. Überprüfen Sie dieses mit `R1#show login`.

5.4 Passwörter in der Ausgabe verschlüsselt darstellen

Mit dem Befehl `R1(config)#service password-encryption` kann außerdem vorgegeben werden, dass alle konfigurierten Passwörter in den Konfigurationsdateien verschlüsselt angezeigt werden (Dies hat aber keine Auswirkung auf die Übertragung!). Sehen Sie sich das Resultat mit `R1#show running-config` an. Jetzt wird nicht nur das `enable secret` verschlüsselt dargestellt, sondern auch die vorher unverschlüsselt angezeigten Passwörter für die Konsole und die Telnet-Zugänge.

5.5 Konfiguration eines SSH-Zugangs

Die Verwendung von Telnet ist hinsichtlich der IT-Sicherheit insofern problematisch, dass alle Daten zwischen den Geräten unverschlüsselt ausgetauscht werden. **Secure Shell (SSH)** bietet gegenüber Telnet eine Verschlüsselung der ausgetauschten Daten und zusätzlich eine stärkere Authentifizierung der Teilnehmer, indem z.B. neben Passwörtern auch Benutzernamen abgefragt werden. Zur Konfiguration eines SSH-Zugangs sind 4 Schritte erforderlich:

1. Es muss ein Domain Name für das Gerät vergeben werden (hier z.B. Router1.com**)**.

   ```
   R1(config)#ip domain-name Router1.com
   ```

2. Die Authentifizierung der zugelassenen Benutzer kann lokal auf dem Gerät oder zentral mit entsprechenden Servern im Netz (z.B. Radius, Diameter) vorgenommen werden. Um diese lokal auszuführen, benötigt man eine lokale Datenbank, in der die Benutzernamen und zugehörigen Passwörter abgelegt sind, zum Beispiel:

   ```
   R1(config)#username bob secret cisco
   ```

3. Die vty lines müssen nun für die Nutzung von SSH Verbindungen und die Nutzung der lokalen Authentifizierung konfiguriert werden:

   ```
   R1(config)#line vty 0 15
   R1(config-line)#transport input ssh
   R1(config-line)#login local
   R1(config-line)#exit
   ```

4. Außerdem müssen für die Verschlüsselung jeweils Sitzungsschlüssel generiert werden, Dieses erfolgt mit Hilfe der sogenannten RSA-Verschlüsselung. Verwenden Sie die Schlüssellänge von 1024 Bit.

   ```
   R1(config)#crypto key generate rsa
   ```

5. Starten Sie von PC1 aus eine SSH-Sitzung auf R1.

   ```
   C:\> ssh –l bob 192.5.5.1
   ```

Hinweis: Das beschriebene Vorgehen zur SSH-Konfiguration ist auf Packet Tracer abgestimmt. Gerade bei der Schlüsselgenerierung gibt es real weitere Konfigurationsmöglichkeiten. Als SSH-Client auf PCs wird häufig die Software PUTTY genutzt.

6 Zurücksetzen von Routern und Switches

Ein Zurücksetzen von Routern und Switches erfolgt durch Löschen der gespeicherten Start-Konfiguration (startup-config) und einem nachfolgenden Warmstart (=> KonfigAnleitung 2.5).

Anhang A: Einige nützliche `show`-Befehle

Dieser Anhang soll Ihnen einen Überblick über einige nützliche `show`-Befehle zur Anzeige von Informationen und Konfigurationsdetails geben. Häufig verwendete Kommandos sind:

- `show running-config` (oder kurz: `sh run`) ist der wohl umfassendste Befehl, um den aktuellen Status einer Konfiguration zu beurteilen, denn er stellt das aktuelle Konfigurationsfile aus dem RAM dar.
- `show startup-config` (oder kurz: `sh start`) stellt die Backup-Konfiguration dar, die im nichtflüchtigen Speicher (NVRAM) gespeichert ist. Dieses File wird beim Booten (Kalt- oder Warmstart) des Routers benutzt, indem es dabei, sofern vorhanden, in das RAM kopiert wird.
- `show flash` wird benutzt, um den zur Verfügung stehenden Flash-Speicher anzuzeigen, wieviel davon in Gebrauch ist, und welche Files, z.B. welche IOS-Images oder VLAN-Dateien (nur Switches), dort vorhanden sind.
- `show arp` zeigt die Address-Resolution-Table eines Gerätes an.
- `show interfaces` zeigt detaillierte Informationen zu den Interfaces an, u.a. den Status, deren MAC-Adressen und - sofern konfiguriert – auch deren IP-Adressen.
- `show protocols` zeigt den globalen und Interface-spezifischen Status der konfigurierten Layer-3-Protokolle (wie z.B. IP, IPX) an.
- `show ip interface brief` gibt eine sehr nützliche Zusammenfassung von Statusmeldungen der Interfaces in einer Übersicht.
- `show ip route` (nur Router) zeigt den Inhalt der Routing-Tabelle eines Routers an. Der wohl nützlichste Befehl, um sich in einer größeren Topologie erst einmal einen Überblick zu verschaffen, welche der erwarteten Netze möglicherweise aufgrund von Fehlern noch fehlen.

Anhang B: Serielle WAN-Verbindungen

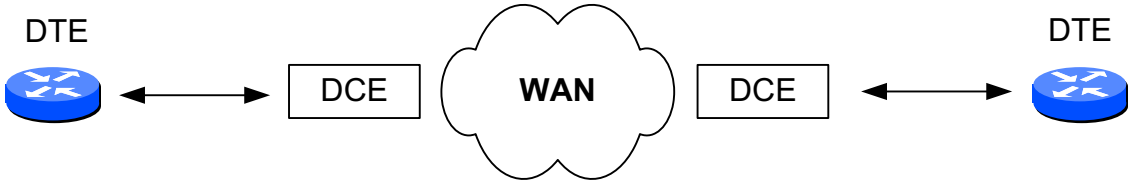
Router, die über eine Serielle Verbindung mit einem Weitverkehrsnetz (WAN) verbunden werden, werden häufig an ein spezielles Gerät, z.B. ein Modem oder einen Mietleitungsabschluss angeschlossen. Dabei wird die Netzseite, die u.a. den Takt für die Verbindung vorgibt, als DCE (Data Circuit Equipment) bezeichnet und die Kundenseite als DTE (Data Terminal Equipment). Diese übernimmt den Takt von der DCE-Seite. Aus der Sicht des WANs werden dort angeschlossene Router als Endgeräte der Benutzer angesehen, die den Takt vom Netz übernehmen (DTE).

Data Terminal Equipment (DTE)

- benutzerseitiges Ende
- bezieht den Takt von der DCE-Seite

Data Circuit Equipment (DCE)

- Netzabschluss des WAN-Providers
- stellt den Takt zur Verfügung



In den Laborversuchen im Praktikum werden keine realen WAN-Verbindungen genutzt. Stattdessen werden die Router direkt über serielle Verbindungsleitungen miteinander verbunden, mit denen eine WAN-Verbindung nachgebildet wird. Daher muss hier jeweils ein Router-Interface der Seriellen Verbindung die **DCE-Rolle** übernehmen, die sonst auf der Netzseite liegt, und entsprechend zur Bereitstellung des Taktes konfiguriert werden.

Dazu muss auf der DCE-Seite der seriellen Verbindung (und nur dort) neben der grundsätzlich üblichen Konfiguration einer IP-Adresse, der bandwidth (wir in kbit/s (!) angegeben) und ggf. einer Beschreibung (description) zusätzlich die Geschwindigkeit der Verbindung über die Taktrate eingestellt werden (Befehl: clockrate (wird in bit/s angegeben).

Beispiel:

```
Router(config)#Interface s0/0
Router(config-if)#ip address 1.2.3.4 255.255.255.0
Router(config-if)#description WAN Interface
Router(config-if)#clock rate 2048000 <- stellt als Geschwindigkeit 2,048 Mbit/s ein
Router(config-if)#bandwidth 2048      <- Übergabe des Wertes z.B. an Routing-Protokolle
Router(config-if)#no shut
```

Hintergrund: Anders als bei Ethernet-Interfaces wird die tatsächliche Geschwindigkeit nicht automatisch erkannt und z.B. für Metrik-Berechnungen herangezogen, sondern sie muss dazu mit dem bandwidth Befehl angegeben werden, sonst wird immer der Default-Wert (1,544 Mbit/s) für solche Berechnungen verwendet.

Darüber hinaus ist bei den Kabeln für die seriellen Verbindungen ebenfalls darauf zu achten, dass diese eine Richtung aufweisen. Die DCE und DTE Seite sind jeweils gekennzeichnet und müssen entsprechend der Konfiguration verwendet werden.

Weitere Informationen zu den seriellen Verbindungen finden Sie im Anhang A der Vorlesung oder im CCNA 2 Routing & Switching Essentials Curriculum Version 6 im Kapitel 1.1.