

Seminargruppe: .....	Datum: .....
Praktikumsgruppe: .....	<b>Testat:</b> .....
Teilnehmer: .....	.....
.....	Unterschrift

# Praktikum lokale Netze

Thema: „Layer 3 - Routing“

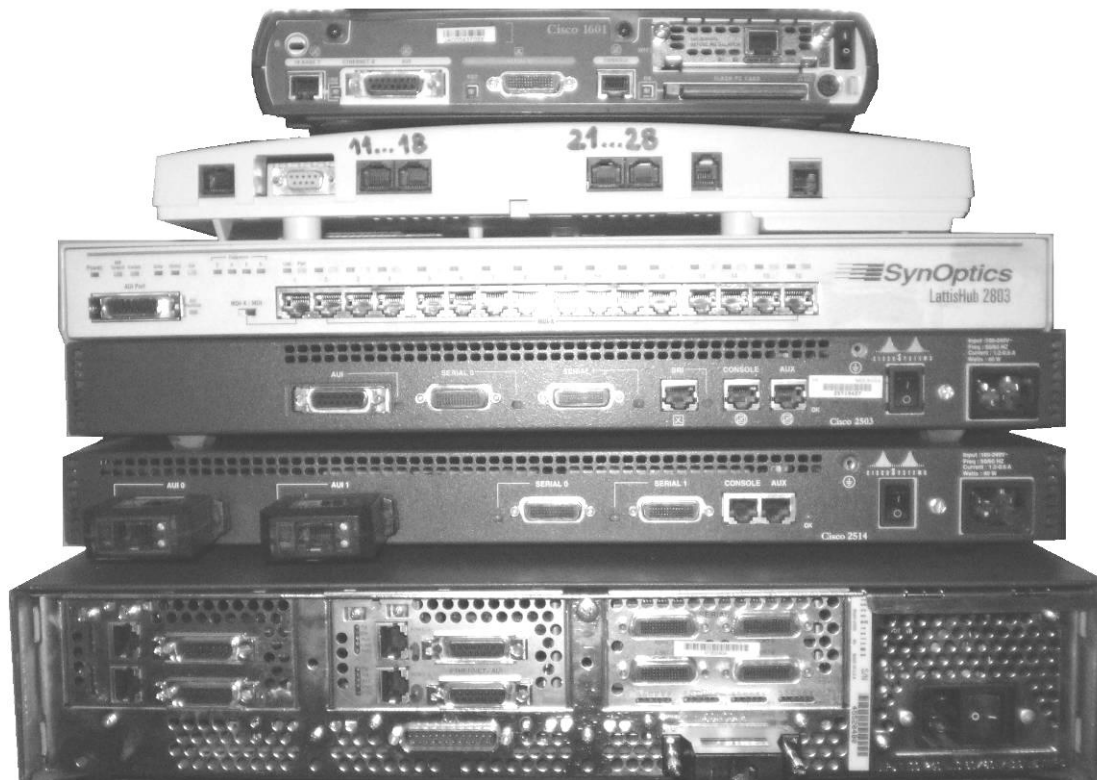


Abbildung 1: Hardware am Arbeitsplatz

## Inhaltsverzeichnis

<b>1</b>	<b>Versuchsziel .....</b>	<b>4</b>
<b>2</b>	<b>Theoretische Einführung.....</b>	<b>4</b>
2.1	<i>OSI-Modell.....</i>	4
2.1.1	(3) Vermittlungsschicht.....	4
2.1.2	(2) Sicherungsschicht .....	5
2.1.3	(1) Bitübertragungsschicht .....	5
2.1.4	Fehlersuche .....	5
2.2	<i>Router &amp; Routing .....</i>	5
2.2.1	Definition Router .....	5
2.2.2	Definition Routing .....	5
2.2.3	Routing tables & topology database.....	6
2.2.4	Routerfunktionen.....	6
2.2.5	3 Arten des Routing .....	6
2.3	<i>Routingprotokolle.....</i>	6
2.3.1	Distance Vector Routing .....	6
2.3.2	Link State Routing .....	7
2.3.3	Im Versuch benutzt: OSPF.....	7
2.4	<i>Cisco Hardware .....</i>	7
2.4.1	Cisco Router: Aufbau.....	7
2.4.2	Cisco Router: Interfacetypen.....	8
2.4.3	Cisco Router: Verbindungskabel.....	8
2.5	<i>IPv4 Adressierung.....</i>	9
2.5.1	IP Adressklassen .....	9
2.5.2	Subnetting .....	10
2.5.3	Subnetmasken & Wildcardmasken .....	10
<b>3</b>	<b>Benutzung der Hardware und Software .....</b>	<b>11</b>
3.1	<i>Router, Hub, ISDN-Tk_Anlage.....</i>	11
3.2	<i>PC / Laptop .....</i>	11
3.3	<i>Software .....</i>	12
3.3.1	Router IOS .....	12
3.3.2	Tera Term.....	12
3.3.3	telnet über Windows Commandline .....	13
3.3.4	Wireshark .....	14
<b>4</b>	<b>Versuchsdurchführung.....</b>	<b>15</b>
4.1	<i>Szenario und Aufgabenstellung .....</i>	15
4.2	<i>IP-Adress-Schema .....</i>	16
4.3	<i>Versuch 1: Inbetriebnahme des Routers „R1_Gotha“ .....</i>	16
4.4	<i>Versuch 2: Inbetriebnahme des Routers „R2_Weimar“ .....</i>	18
4.5	<i>Versuch 3: Querverbindung R1_Gotha zu R2_Weimar .....</i>	19
4.6	<i>Versuch 4: Inbetriebnahme des Routers „Jena“ .....</i>	20
4.7	<i>Versuch 5: Backup-ISDN-Verbindung R3_Jena zu R2_Weimar .....</i>	21
4.7.1	Konfiguration der ISDN-Interfaces.....	22
4.7.2	Test der Backup-Funktion.....	23
4.8	<i>Versuch 6: Snifferanalyse von OPSF-Routingupdates.....</i>	24

---

4.9	<i>Rücksetzen der Einstellungen:</i> .....	25
<b>5</b>	<b>Anhang</b> .....	<b>25</b>
5.1	<i>Literaturverzeichnis</i> .....	25
5.2	<i>Abbildungsverzeichnis</i> .....	25

## 1 Versuchsziel

Im Praktikum steht ein Arbeitsplatz zur Verfügung, der mit folgenden Geräten ausgerüstet ist:  
(im Titelbild von oben nach unten)

Cisco-Router 1601, ISDN-Telefonanlage Eumex 322, ein 10MBit-Ethernet-Hub, Cisco-Router 2503, Cisco-Router 2514, Cisco-Router 4500M.

In der Versuchsdurchführung sollen grundlegende Aspekte des Layer 3 des OSI-Modells am praktischen Beispiel eines Routernetzwerkes veranschaulicht werden.

Die Basiskonfigurationen von Cisco-Routern werden ebenso wie einfache Analysen von Routinginformationen anhand eines realitätsnahen Testszenarios vermittelt.

## 2 Theoretische Einführung

In der Einführung werden alle grundlegenden für den Versuch benötigten Begriffe erklärt. Dies ist ein rein informativer Abschnitt, der zur Versuchsvorbereitung und Auffrischung unbedingt gelesen werden sollte.

### 2.1 OSI-Modell

Das OSI-Modell wurde entwickelt, um die komplexen Vorgänge einer Kommunikation in verschiedene hierarchische Ebenen zu unterteilen und sie damit besser beschreibbar und standardisierbar zu machen.

	<b>OSI-Schicht / Layer</b>	<b>Einheiten</b>	<b>Kopplungselemente</b>
7	Anwendung / application		
6	Darstellung / presentation		
5	Sitzung / session		
4	Transport / transport	Segmente	Layer4-7-Switch, ContentSwitch
<b>3</b>	<b>Vermittlung / network</b>	<b>Pakete</b>	<b>Router, Layer3-Switch</b>
2	Sicherung / data link	Rahmen / frames	Bridge, Switch
1	Bitübertragung / physical	Bits	Hub, Repeater

Jede elektronische Kommunikation durchläuft im Prinzip vom Sender bis zum Empfänger alle Schichten in der Reihenfolge:

7-6-5-4-3-2-1---Übertragungsmedium---1-2-3-4-5-6-7

Sind ein oder mehrere Vermittlungsknoten auf dem Weg zwischen Sender und Empfänger zu durchlaufen, ergibt sich folgendes Bild:

7-6-5-4-3-2-1---ÜM---1-2-3-Router-3-2-1---ÜM---1-2-3-Router-3-2-1---ÜM---1-2-3-4-5-6-7

In diesem Versuch geht es vorwiegend um Funktionalitäten der Vermittlungsschicht = Layer 3. Dennoch ist auch ein grundlegendes Verständnis der darunter liegenden Schichten 2 und 1 erforderlich.

#### 2.1.1 (3) Vermittlungsschicht

Die Vermittlungsschicht (engl. Network Layer) sorgt bei paketorientierten Diensten für die Weitervermittlung von Datenpaketen. Die Datenübertragung geht über das gesamte Kommunikationsnetz hinweg und schließt die Wegesuche (Routing) zwischen den Netzknoten mit ein. Da nicht immer eine direkte Kommunikation zwischen Absender und Ziel

möglich ist, müssen Pakete von Knoten, die auf dem Weg liegen, weitergeleitet werden. Weitervermittelte Pakete gelangen nicht in die höheren Schichten, sondern werden mit einem neuen Zwischenziel versehen und an den nächsten Knoten gesendet.

### 2.1.2 (2) Sicherungsschicht

Die Aufgabe der Sicherungsschicht ist es, eine weitgehend fehlerfreie Übertragung zu gewährleisten und den Zugriff auf das Übertragungsmedium zu regeln. Dazu dient das Aufteilen des Bitdatenstromes in Blöcke und das Hinzufügen von Folgenummern und Prüfsummen. Fehlerhafte, verfälschte oder verloren gegangene Blöcke können vom Empfänger durch Quittungs- und Wiederholungsmechanismen erneut angefordert werden. Die Blöcke werden auch als Frames oder Rahmen bezeichnet.

Eine „Datenflusskontrolle“ ermöglicht es, dass ein Empfänger dynamisch steuert, mit welcher Geschwindigkeit die Gegenseite Blöcke senden darf.

### 2.1.3 (1) Bitübertragungsschicht

Die Bitübertragungsschicht (engl. Physical Layer) stellt mechanische, elektrische und weitere funktionale Hilfsmittel zur Verfügung, um physikalische Verbindungen zu aktivieren und Bits darüber zu übertragen.

In Rechnernetzen wird Information zumeist in Form von Bitfolgen übertragen.

Die Definition der Werte 0 und 1 in Bezug auf das elektrische, optische oder elektromagnetische Medium wird auf der Bitübertragungsschicht definiert.

### 2.1.4 Fehlersuche

Treten Kommunikationsfehler auf, wird sinnvollerweise ein troubleshooting vom physical layer zum application layer hin durchgeführt. Für den Versuch bedeutet das:

L1) Ist ein Kabel gesteckt? Wird ein Link durch eine leuchtende LED signalisiert?

L2) Ist eine MAC-Adresse sichtbar? Sind cdp neighbors sichtbar?

L3) Funktionieren ping und traceroute?...



Merke: **First check the physical!**

## 2.2 Router & Routing

### 2.2.1 Definition Router

Ein Router ist logisch ein Netzknoten und physisch ein Netzwerkgerät, das aus Sicht des Clients im LAN ein Gateway darstellt und als quasi „Vermittlungsstelle“ zwei wesentliche Funktionen erfüllen muss: Wegefindung (path determination) und Datentransport zwischen Netzen / LANs (packet forwarding). In den schematischen Netzplänen wird ein Router mit diesem Symbol dargestellt:



### 2.2.2 Definition Routing

Routing ist ein Prozess, der unter Benutzung eines Layer3-Gerätes Datenpakete zwischen Netzen oder Teilnetzen (subnets) transportiert. Der Routingprozess nutzt Routingtabellen (routing tables), Protokolle und Algorithmen, um den effizientesten Pfad für die Weiterleitung von IP-Paketen zu finden.

Router erhöhen die Skalierbarkeit von Netzen, indem sie die Layer2-Collisions- und Broadcastdomänen auf kleine Teilnetze begrenzen.

### 2.2.3 Routing tables & topology database

Anhand von zwischen mehreren Routern periodisch ausgetauschten Informationen erlangt jeder Router Kenntnis über die Struktur angeschlossener und benachbarter Netzwerke. Das wird in der topology database abgebildet.

Bei Veränderungen im Netz (z.B. Hinzufügen neuer Netze, Leitungsunterbrechungen, Nichterreichbarkeit von LANs etc.) werden Routingupdates sofort an alle benachbarten Router propagiert.

Router berechnen anhand der Topologie und weiterer Parameter (z.B. Hopanzahl, Bandbreite, delay etc.) den optimalen Weg vom Quellnetz zum Zielnetz.

Diese Routen werden in der routing table abgelegt.

### 2.2.4 Routerfunktionen

Router benutzen die routing table um festzulegen, zu welchem Interface ein empfangenes Datenpaket geschickt werden muss, um das Zielnetz zu erreichen. Dazu muss im Datenpaket die destination IP address ausgelesen werden. Das erfordert eine De-encapsulation; ein „Auspacken“ des Datenpakets aus den Headern (Umhüllungen) der Layer 1 und 2. Danach entscheidet der Router, ob dieses Datenpaket für den Router selbst bestimmt ist oder weitergeleitet werden muss.

Wenn eine Weiterleitung erfolgen muss, durchsucht der Router seine routing table, um festzulegen, wohin das Paket geschickt werden muss.

Wenn das Zielnetz ein direkt angeschlossenes Netz ist, bestimmt der Router mittels ARP request die MAC-Adresse des Zielhosts und sendet das Paket in das Zielnetz.

Wenn das Zielnetz über einen anderen Router erreicht werden muss, nutzt der Router die MAC-Adresse des Nachbarrouters (next hop router) und sendet das Paket zum entsprechenden Interface.

Bevor das Paket in Richtung Ziel vom outgoing Interface auf das Medium Kabel gebracht wird, muss das Paket wieder mit den Headern für Layer 2 und 1 eingepackt = encapsulated werden.

### 2.2.5 3 Arten des Routing

Static routing: Hier werden vom Administrator manuell Informationen in die routing table geschrieben. Der Router benutzt generell den vorgegebenen Weg, um das Ziel zu erreichen.

Dynamic routing: Hier werden die Rechenergebnisse des Routingalgorithmus in die routing table eingefügt. Der optimale Weg zum Ziel ist abhängig von den aktuell verfügbaren Verbindungen.

Default route: Hier kennt der Router nur seine direkt angeschlossenen Netze und schickt alle Pakete mit unbekanntem Ziel einfach zu seinem übergeordneten Router; sozusagen an das Hauptpostamt.

## 2.3 Routingprotokolle

### 2.3.1 Distance Vector Routing

Hierbei speichert jeder Router eine Tabelle mit der besten Entfernung (z. B.: Anzahl hops, Verzögerung in ms, Bandbreite der Verbindung) zu jedem Ziel und dem dazugehörigen Ausgangsinterface. In der Praxis hat dieses Verfahren eine zu langsame Konvergenz, d.h. es vergeht zu viel Zeit, bis alle Router den aktuellen Zustand des Netzes korrekt in den routing tables abbilden können. Grundprinzip: „Teile deinen Nachbarn mit, wie für dich die Welt aussieht.“ Distanzvektor-Protokolle sorgen dafür, dass sich die Router untereinander nur mitteilen, wie „gut“ sie an verschiedene Zielknoten angebunden sind. Durch Auswahl des für ein bestimmtes Ziel optimalen Nachbarn wird die Berechnung des optimalen Weges somit auf mehrere Router verteilt. Typischer Vertreter: RIP (Routing Information Protocol)



### 2.3.2 Link State Routing

Hier erstellt sich jeder Router eine baumförmige Struktur des Netzes anhand seiner und von den Nachbarn erhaltenen Informationen. Grundprinzip: „Teile der Welt mit, wer deine Nachbarn sind.“ Link-State-Routing-Protokolle sorgen dafür, dass nach einiger Zeit jeder Router die vollständige Topologie des Netzwerkes kennt und sich die kürzesten Wege darin selbst ausrechnen kann.

Typischer Vertreter: OSPF (Open Shortest Path First)

### 2.3.3 Im Versuch benutzt: OSPF

Beim Erstellen oder Aktualisieren der topology database und der routing table eines OSPF-Routers werden folgende Schritte vollzogen:

- Entdecken neuer Nachbarn mittels HELLO-Paket
- Messung von Verzögerung und Kosten zu jedem Nachbarn mittels ECHO-Paket
- Erstellung eines LINK-STATE-Paketes mit allen gelernten Daten (Sender, Liste der Nachbarn mit Verzögerung, Alter, ...), das periodisch oder ereignisgesteuert (z. B.: neuer Nachbar, Ausfall, ...) erzeugt wird
- Versenden dieses Pakets an alle Nachbarn
- Berechnung des kürzesten Pfades zu allen anderen Routern (mit dem Shortest-Path-First-Algorithmus von Dijkstra)

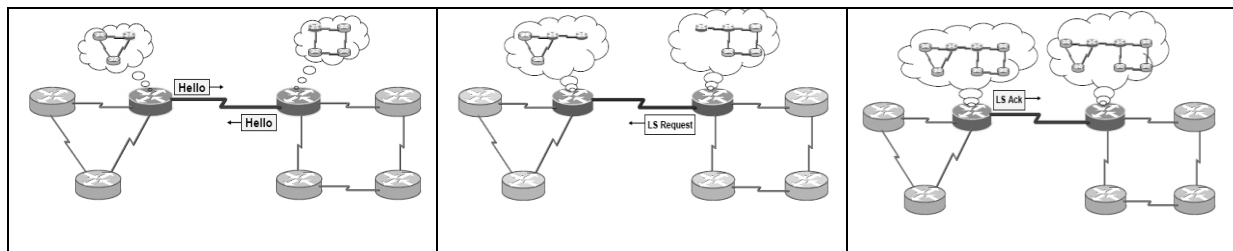


Abbildung 2: Einige Schritte des OSPF-Prozesses

## 2.4 Cisco Hardware

### 2.4.1 Cisco Router: Aufbau

Ein Router besteht wie jedes Datenverarbeitungsgerät aus Interfaces, Prozessor und Speicher, die auf einem Motherboard in einem Chassis untergebracht sind.

Im Router gibt es mehrere Speichermodule:

**NVRAM** (Non Volatile Random Access Memory): beschreibbarer Speicher, in dem die startup-configuration und die Einstellungen des Config-Registers permanent abgelegt werden

**RAM**: speichert routing tables und die running-configuration, fungiert als cache

**Flash**: permanenter Speicher für das Cisco IOS image = Betriebssystemsoftware

**ROM**: beinhaltet ein Mini-Bootimage für den Fall des IOS-Verlustes

Beim Bootvorgang vollzieht der Router mit Informationen aus dem ROM einen power-on-self-test, entpackt das IOS aus dem Flash in den RAM, holt aus dem NVRAM (Config-Register) die Information, ob die startup-config vom NVRAM als running-config in den RAM geladen werden soll. Im Normalfall geschieht das Laden der startup-conf und der Router ist betriebsbereit. Bei Fehlern bleibt der Router im ROM-Monitor stehen, d.h. nur ein Mini-IOS ist geladen und für die Fehlersuche oder das Nachladen eines IOS verfügbar.

## 2.4.2 Cisco Router: Interfacetypen

Beispiel Cisco 2503, Interfaces von links nach rechts

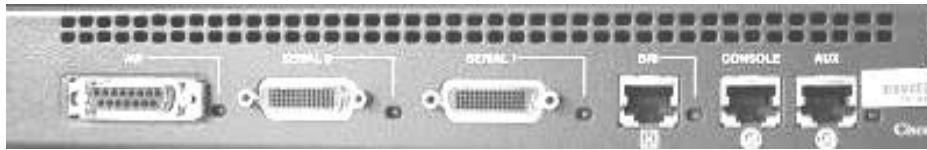


Abbildung 3: Interfaces am Cisco 2503

Ethernet-Interface: im Versuch **ausschließlich 10MBit half duplex**, Anschlusstyp AUI (15polig Sub-D) oder 10BaseT (RJ45-Stecker)

Serielles Interface: im Versuch bis 2MBit, synchron, 60polig

ISDN-Interface: BRI = im Versuch: BasicRateInterface 2x 64kbit

Console: serielles Interface zum Konfigurieren

Auxillary port = Anschlussmöglichkeit für Modem

Weitere Interfacetypen anderer Router informativ:

Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, asynchronus serial,

## 2.4.3 Cisco Router: Verbindungskabel

Folgende Kabel stehen für den Versuch zur Verfügung:


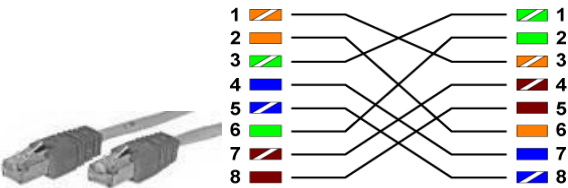



<p>Ethernet Patchkabel (PC&lt;-&gt;Router, PC&lt;-&gt;Hub)</p> <p>Farbe: grau oder blau</p>	
<p>Ethernet Crosskabel (Router&lt;-&gt;Router)</p> <p>Farbe grau mit <b>grünem</b> Stecker</p>	
<p>ISDN -Kabel (Router-BRI&lt;-&gt;Tk_Anlage)</p> <p>Farbe: schwarz</p>	
<p>Serielle Kabel DTE-DCE (Router&lt;-&gt;Router)</p> <p>Farbe: Cisco-blaugrün</p>	
<p>Consolekabel (PC_COM1&lt;-&gt;Routerconsole)</p> <p>Farbe: hellblau</p>	

Abbildung 4:Verbindungskabel



## 2.5 IPv4 Adressierung

IP-Adressen werden in Computernetzen, die auf dem Internetprotokoll (IP) basieren, verwendet, um Daten von ihrem Absender zum vorgesehenen Empfänger transportieren zu können. Aufgrund dieser Adresse können die Router entscheiden, in welche Richtung das Paket weiter transportiert werden soll.

Eine IP-Adresse kann einen einzelnen, aber in manchen Fällen auch eine Gruppe von Empfängern bezeichnen (Multicast, Broadcast).

Die übliche Notation der IPv4-Adressen besteht aus vier Dezimalzahlen, die jeweils zwischen 0 und 255 liegen und mit einem Punkt getrennt werden.

Beispiel 127.0.0.1

In anderer Schreibweise ist diese Adresse eine 32-stellige Binärzahl der Form 01111111 00000000 00000000 00000001.

Jede Gruppe von 8 Bits wird als Oktett bezeichnet. In einem Oktett haben die einzelnen Bits folgende Wertigkeiten:

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

Addiert man die Wertigkeiten der einzelnen Bits zusammen, erhält man den Dezimalwert des Oktetts.

0	1	1	1	1	1	1	1
$0*128 +$	$1*64 +$	$1*32 +$	$1*16 +$	$1*8 +$	$1*4 +$	$1*2 +$	$1*1 =$

127

### 2.5.1 IP Adressklassen

Ursprünglich wurden die IP-Adressen in Netzklassen von A bis C mit verschiedenen Netzmasken eingeteilt.

Netzklasse	Präfix	Adressbereich	Netzmaske	Netzlänge	Hostlänge	Netze	Hosts pro Netz	
Klasse A	0...	0.0.0.0 – 127.255.255.255	255.0.0.0	8 Bit	24 Bit	128	16.777.214	
Klasse B	10...	128.0.0.0 – 191.255.255.255	255.255.0.0	16 Bit	16 Bit	16.384	65.534	
Klasse C	110...	192.0.0.0 – 223.255.255.255	255.255.255.0	24 Bit	8 Bit	2.097.152	254	
Klasse D	1110...	224.0.0.0 – 239.255.255.255	Verwendung für Multicast -Anwendungen					
Klasse E	1111...	240.0.0.0 – 255.255.255.255	reserviert					

Aufgrund der immer größer werdenden Routing-Tabellen wurde 1993 das klassenlose Routing CIDR (Classless Interdomain Routing) eingeführt. Damit spielt es keine Rolle mehr, welcher Netzklasse eine IP-Adresse angehört, wobei der Adressbereich der Klasse D auch nach Abschaffung der Netzklassen weiter für Multicast-Anwendungen herangezogen wird.

## 2.5.2 Subnetting

Eine IP-Adresse, sowohl in binärer als auch in dezimaler Schreibweise, ist ohne Angabe einer Subnetzmaske nicht eindeutig lesbar. Analogie: Eine Postanschrift ist ohne eindeutige Unterscheidung von Zielort und Straße/Hausnummer nicht verwendbar.

Grundsätzlich gilt:

Jede über ein Routerinterface erreichbare Menge von Hosts gehört zu einem einzigen (Teil-) Netz.

Die erste IP-Adresse kennzeichnet das Netz.

Die zweite bis  $n$ -te IP-Adresse erhalten die Hosts.

Die letzte IP-Adresse kennzeichnet die Broadcastadresse.

Wie groß der Zahlenraum für das ganze (Teil-)Netz ist, wird durch die Subnetzmaske gekennzeichnet.

Jede IP-Adresse, ganz gleich ob in Dezimal- oder Binärschreibweise, hat einen Anteil, der das Netz und einen Anteil, der den Host bezeichnet.

Jene Bits, die die Subnetzmaske mit 1 kennzeichnet, gehören zum Netzanteil.

Jene Bits, die die Subnetzmaske mit 0 kennzeichnet, gehören zum Hostanteil.

Beispiel:

gegeben: 172.16.3.11 255.255.255.128 (alternative Schreibweise 172.16.3.11/25)

Es werden **25** Bits für den Netzanteil und  $(32-25=)$  7 Bits für Hosts verwendet.

Auflösung in binäre Schreibweise:

```
10101100 00010000 00000011 00001011 .. IP-Adresse
11111111 11111111 11111111 10000000 .. Subnetzmaske
Das ergibt
10101100 00010000 00000011 00001011
NETZANTEIL                                HOSTANTEIL
```

Die Netzadresse lautet somit 172.16.3.0

Die Hosts können in folgendem Ziffernraum Adressen verwenden:

172.16.3.1 bis 172.16.3.126

Die Broadcast-Adresse lautet 172.30.16.127

## 2.5.3 Subnetmasken & Wildcardmasken

Bei der Verwendung des Routingprotokolls OSPF auf Cisco-Routern muss nicht nur das Netz benannt werden, das geroutet werden soll, sondern auch die dazugehörige Maske. Allerdings wird hier nicht die herkömmliche Subnetzmaske der Form 255.x.x.x, sondern eine invertierte Maske, die sogenannte Wildcard-Maske verwendet.

Einfach gesagt, sind hier Nullen und Einsen vertauscht. Dezimal ergibt sich dann eine Form der Wildcardmask von 0.x.x.x.

Hier eine Tabelle zur Übersicht, damit bei der Routerkonfiguration im Versuch auf langwieriges dezimal-binäres Rechnen verzichtet werden kann:

Bits für den Netzanteil	Subnetmask dezimal	Subnetmask binär	Wildcard-mask = inverse Subnetmask	Wildcardmask dezimal
8	255.0.0.0	11111111 00000000 00000000 00000000	00000000 11111111 11111111 11111111	0.255.255.255
9	255.128.0.0	11111111 10000000 00000000 00000000	00000000 01111111 11111111 11111111	0.127.255.255
10	255.192.0.0	11111111 11000000 00000000 00000000	00000000 00111111 11111111 11111111	0.63.255.255
11	255.224.0.0	11111111 11100000 00000000 00000000	00000000 00011111 11111111 11111111	0.31.255.255
12	255.240.0.0	11111111 11110000 00000000 00000000	00000000 00001111 11111111 11111111	0.15.255.255
13	255.248.0.0	11111111 11111000 00000000 00000000	00000000 00000111 11111111 11111111	0.7.255.255
14	255.252.0.0	11111111 11111100 00000000 00000000	00000000 00000011 11111111 11111111	0.3.255.255
15	255.254.0.0	11111111 11111110 00000000 00000000	00000000 00000001 11111111 11111111	0.1.255.255
16	255.255.0.0	11111111 11111111 00000000 00000000	00000000 00000000 11111111 11111111	0.0.255.255
17	255.255.128.0	11111111 11111111 10000000 00000000	00000000 00000000 01111111 11111111	0.0.127.255
18	255.255.192.0	11111111 11111111 11000000 00000000	00000000 00000000 00111111 11111111	0.0.63.255
19	255.255.224.0	11111111 11111111 11100000 00000000	00000000 00000000 00011111 11111111	0.0.31.255
20	255.255.240.0	11111111 11111111 11110000 00000000	00000000 00000000 00001111 11111111	0.0.15.255
21	255.255.248.0	11111111 11111111 11111000 00000000	00000000 00000000 00000111 11111111	0.0.7.255
22	255.255.252.0	11111111 11111111 11111100 00000000	00000000 00000000 00000011 11111111	0.0.3.255
23	255.255.254.0	11111111 11111111 11111110 00000000	00000000 00000000 00000001 11111111	0.0.1.255
24	255.255.255.0	11111111 11111111 11111111 00000000	00000000 00000000 00000000 11111111	0.0.0.255
25	255.255.255.128	11111111 11111111 11111111 10000000	00000000 00000000 00000000 01111111	0.0.0.127
26	255.255.255.192	11111111 11111111 11111111 11000000	00000000 00000000 00000000 00111111	0.0.0.63
27	255.255.255.224	11111111 11111111 11111111 11100000	00000000 00000000 00000000 00011111	0.0.0.31
28	255.255.255.240	11111111 11111111 11111111 11110000	00000000 00000000 00000000 00001111	0.0.0.15
29	255.255.255.248	11111111 11111111 11111111 11111000	00000000 00000000 00000000 00000111	0.0.0.7
30	255.255.255.252	11111111 11111111 11111111 11111100	00000000 00000000 00000000 00000011	0.0.0.3
31	255.255.255.254	11111111 11111111 11111111 11111110	00000000 00000000 00000000 00000001	0.0.0.1
32	255.255.255.255	11111111 11111111 11111111 11111111	00000000 00000000 00000000 00000000	0.0.0.0

Abbildung 5: Subnet- u. Wildcardmasken

### 3 Benutzung der Hardware und Software

#### 3.1 Router, Hub, ISDN-Tk-Anlage

Die Geräte sind pfleglich zu behandeln. Es ist darauf zu achten, dass die Netzkabel vorsichtig und ohne Gewalt nach dem Herunterdrücken der Verankerung herausgezogen oder eingesteckt werden. Besonders acht zu geben ist darauf, dass keiner der 60 Pins der seriellen Kabel verbogen wird.

Auf dem zentralen Router „Erfurt“ sind keine Konfigurationsarbeiten notwendig. Der Zugriff ist für Studenten gesperrt!

Zugriff auf die Router „Gotha“, „Weimar“ und „Jena“ erlangt man zunächst über Console und nach erfolgter Basiskonfiguration auch über telnet. Der http-Zugriff ist deaktiviert! Es wird nur das CLI=Command Line Interface benutzt.

Der Hub und die Tk-Anlage brauchen nicht konfiguriert zu werden und müssen unverändert bleiben.

#### 3.2 PC / Laptop

Der PC / Laptop wird für 4 Zwecke benötigt:

- als Terminal zur Routerkonfiguration via COM -> Console; benutzte Software: *Hyperterminal* oder *TeraTerm*
- als Host im LAN der jeweiligen Niederlassungsrouter (*ping*, *tracert*, *telnet*)
- ggf. ein 2. PC als TFTP-Server am Zentralrouter
- als Traffic-Sniffer mit Software *Wireshark*

## 3.3 Software

### 3.3.1 Router IOS

Das IOS = Internetworking Operation System kann als das Betriebssystem eines Routers bezeichnet werden.

Die verfügbaren Befehle sind abhängig von den Userrechten und der Tiefe der Konfigurationsebene.

Nach einem login über Console oder telnet wird das login-Passwort abgefragt.

Im Versuch heißt das Passwort **cisco**

Hat der Router noch keine Konfiguration, entfällt diese Abfrage.

Nun befindet man sich im User-mode.

Hier sind durch Eingabe von **?** die wenigen verfügbaren Befehle abrufbar. Mehr ist nur im Enable-Modus möglich. Dahin gelangt man durch Eingabe des Befehls **ena**.

Im Versuch heißt das Passwort ebenfalls **cisco**.

Konfigurationsänderungen können nur im config-Mode durchgeführt werden.

Dahin gelangt man durch Eingabe des Befehls **configure terminal**. Kurz: **conf t**.

Beide Formen sind möglich. Eine Ebene zurück kommt man mit **end** oder **exit**.

Das Speichern der sofort aktiven Befehle (running config) in die Startup-config erfolgt mit dem Befehl **copy running-config startup-config**. Kurz: **copy run start**.

Alle weiteren notwendigen Befehle werden in der Versuchsdurchführung genannt.



#### Merke:

- Jede Eingabe eines Befehls ist mit <ENTER> abzuschließen.
- Sind mehrere Befehle in der Versuchsbeschreibung mit Komma getrennt angegeben, sind die Befehle natürlich nacheinander und jeweils mit >ENTER> abgeschlossen einzugeben.
- Eingegebene Befehle werden SOFORT und ohne Sicherheitsabfrage wirksam.
- Ist die Bildschirmausgabe eines Befehls länger als 80 Zeilen, können mit der Leertaste die nächsten Zeilen angezeigt werden.

### 3.3.2 Tera Term

TeraTerm ist eine Freeware und ermöglicht Terminalsessions über telnet (hier wird über die Netzwerkkarte des PCs gearbeitet) oder über ein serielles Interface des PCs (z.B. COM1), das direkt mit dem Consoleport des Routers verbunden ist. Geben Sie bei der Wahl einer neuen Verbindung die IP-Adresse Ihres Ziels an und wählen Sie „Telnet“ wie im linken Bild gezeigt.

In Abhängigkeit von der Hardwareausstattung des verwendeten PCs oder Laptops wählen Sie für eine Console-Verbindung „Serial“. Hat Ihr PC oder Laptop eine herkömmliche 9polige serielle Sub-D-Schnittstelle, so wählen Sie COM\_1.

Sind Sie mit einem USB-Seriell-Adapter ausgerüstet, wählen Sie das entsprechende simulierte COM\_1-Interface wie rechts im Bild gezeigt.

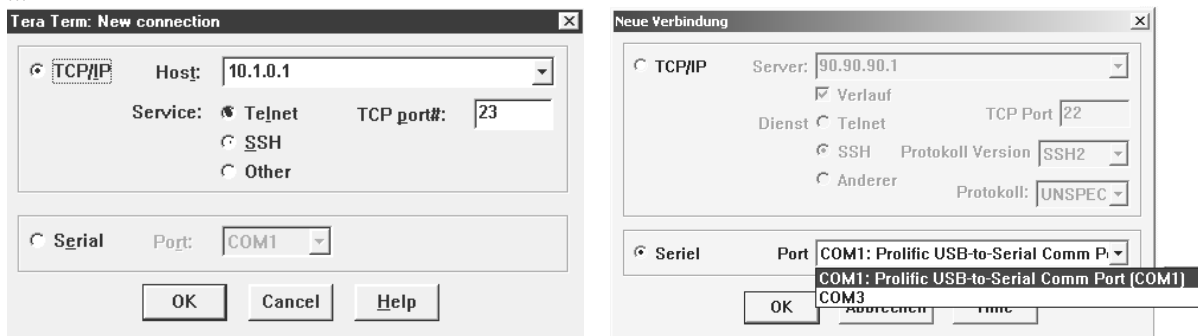


Abbildung 6: TeraTerm Startscreen – Telnet oder seriell

### 3.3.3 telnet über Windows Commandline

Eine Telnetsession kann entweder über die zuvor beschriebene Software TeraTerm oder die Windows-Commandline des PCs/Laptops aufgebaut werden. Diese wird über „Start -> Ausführen“ und den Befehl „*cmd*“ gestartet. Danach lautet der Befehl **telnet <IP-Adresse>**.

Um alle IP- Informationen des Rechners zu bekommen, ist ebenfalls die Windows Command Line zu verwenden. Nützliche Befehle sind hier:

- ipconfig /all** komplette Netzwerkinformationen
- ping <IP-Adresse>** ICMP-Testpaket, Test der Erreichbarkeit eines Ziels
- tracert <IP-Adresse>** Routenverfolgung zu einem Ziel

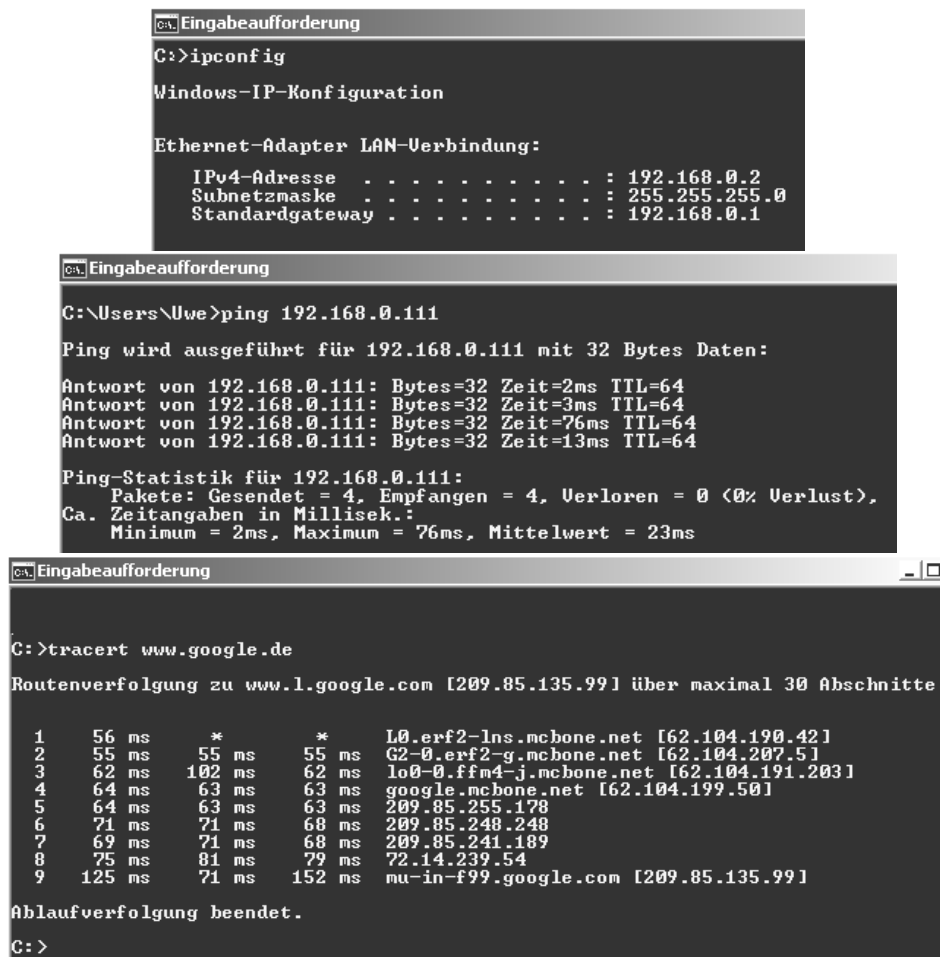


Abbildung 7: Windows Command Line mit Beispielen für ipconfig, ping und traceroute

### 3.3.4 Wireshark

Das Programm Wireshark wird im Praktikum zum Auswerten des Netzwerktraffics verwendet. Der Start erfolgt auf dem Laptop über das Desktop Symbol „Wireshark“. Nach dem Programmstart kann der Capture Vorgang über die linke Grafik „List the available capture interfaces.“ in der Symbolleiste gestartet werden. Durch die Buttons rechts daneben kann man den Capture Vorgang stoppen oder erneut starten.

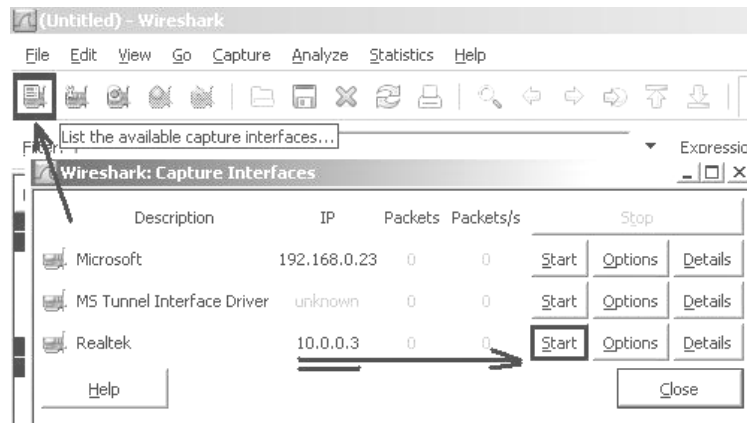


Abbildung 8: Wireshark Startbildschirm

Danach muss nur noch der Startknopf der entsprechenden Netzwerkkarte betätigt werden. Dann werden drei Fensterbereiche angezeigt.

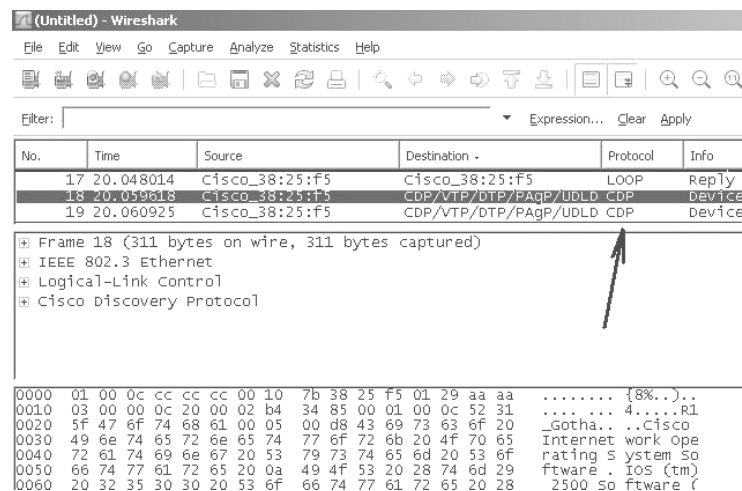


Abbildung 9: Wireshark im Einsatz

Im oberen Fenster werden alle empfangen und gesendeten Netzwerkpakete dargestellt. Der Pfeil zeigt auf die Spalte „Protokoll“. Hier ist im Versuch nach OSPF zu suchen!

In der Mitte erfolgt eine Zusammenfassung des im oberen Fenster ausgewählten Paketes. Im unteren Fenster wird der Hexadezimalblock des Paketes angezeigt.



## 4 Versuchsdurchführung

Zu Beginn des Versuches finden Sie folgende Ausgangssituation vor:

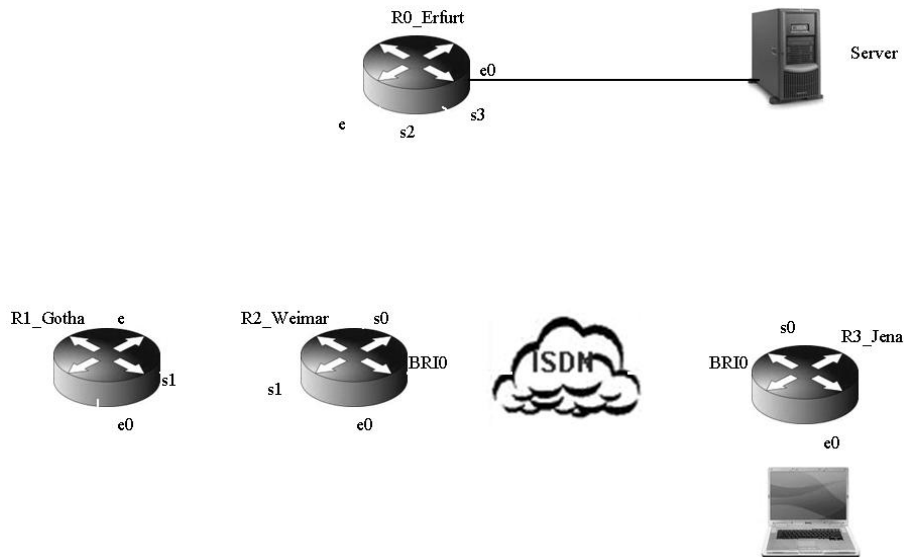


Abbildung 10: Ausgangssituation Arbeitsplatz

### 4.1 Szenario und Aufgabenstellung

Sie sind als Service Engineer beauftragt, die neuen Firmenniederlassungen Gotha und Weimar mit der Zentrale in Erfurt zu vernetzen und mittels Querverbindung die Ausfallsicherheit zu erhöhen. User in allen Lokationen müssen in der Lage sein, den Server in Erfurt zu erreichen. Später ist noch ein Büro in Jena in das Netz einzubinden und mit einer ISDN-Backup-Leitung nach Weimar abzusichern. Durch Mitlesen (Sniffen) des Netztraffics zwischen Erfurt und Gotha soll nachgewiesen werden, dass bei Ausfall von WAN-Leitungen sofort Ersatzrouten durch OSPF-Routingupdates propagiert werden.

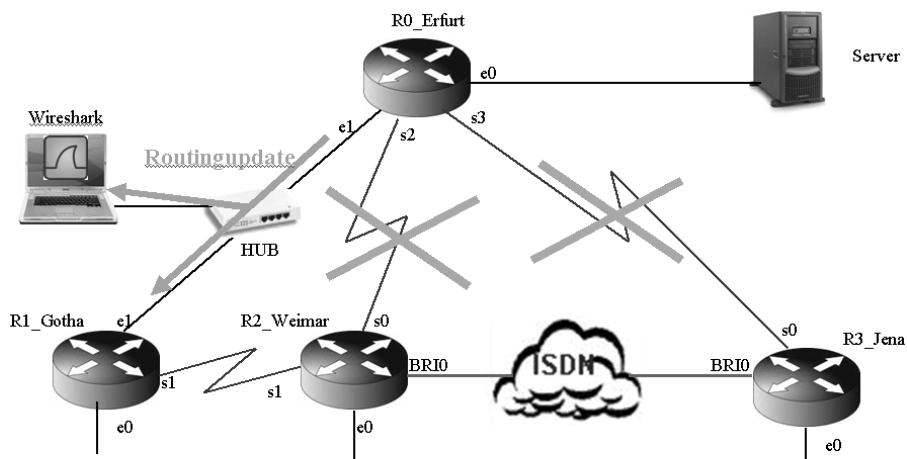


Abbildung 11: Endsituation Arbeitsplatz

## 4.2 IP-Adress-Schema

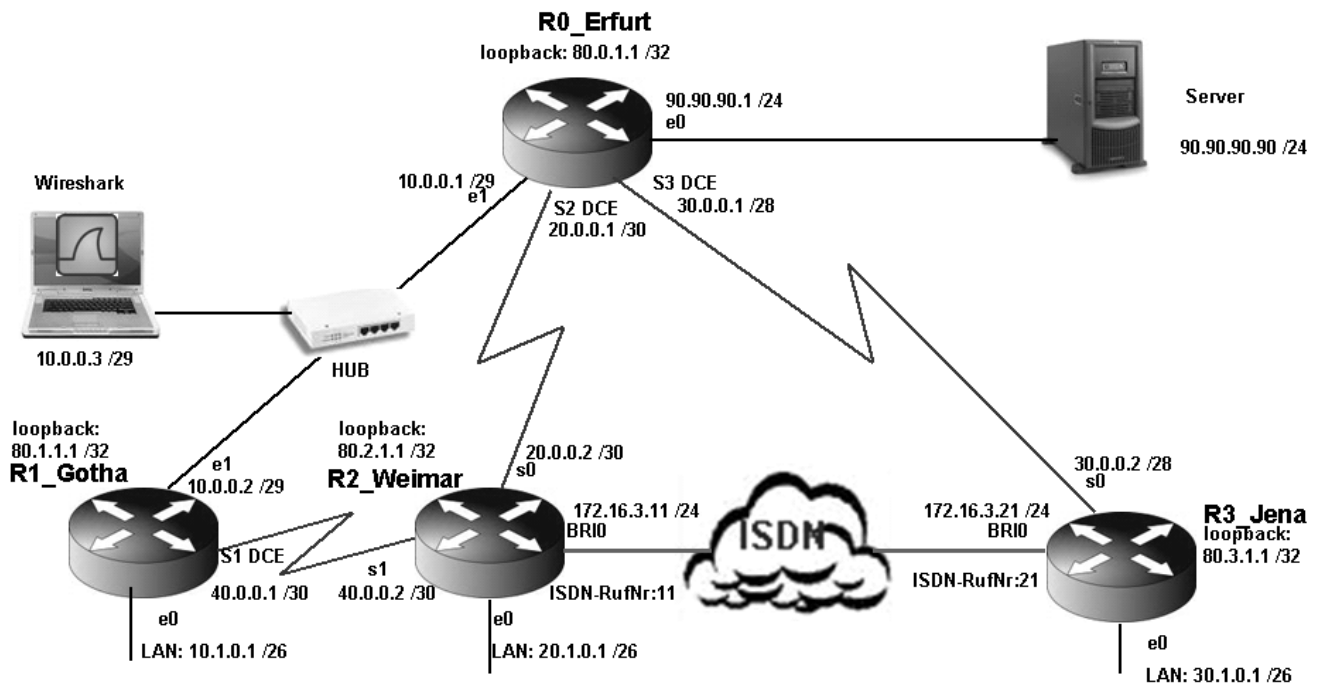


Abbildung 12: IP-Adress-Schema

## 4.3 Versuch 1: Inbetriebnahme des Routers „R1\_Gotha“

Router R0\_Erfurt einschalten.

Laptop verbinden mit console des Routers R1\_Gotha

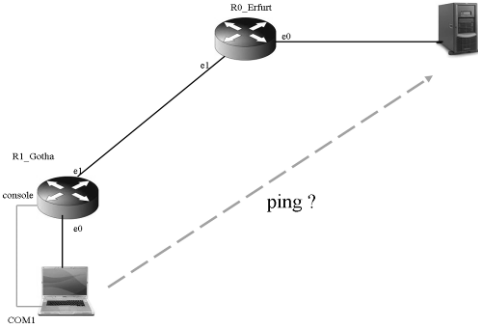
Nutzen Sie das Terminalprogramm *hyperterminal* oder *TeraTerm* mit den Einstellungen *com1* (oder die vom USB-Interface simulierte COM) 9600 8bit kein stopbit

1. Router R1\_Gotha einschalten, booten lassen. Der Router ist ohne jegliche Konfiguration. Ignorieren Sie die Vorschläge zur menügeführten Konfiguration: *use configure dialog: no*, *terminate autionstall: yes*. Der Router ist bereit, wenn der Prompt wie folgt aussieht:  
**Router>**

2. Um den erweiterten Befehlssatz zur Verfügung zu haben und konfigurieren zu können, gehen Sie in den enable-Modus: **enable**
3. **show version** (a: Welche Interfaces sind vorhanden? b: Welches IOS ist geladen?)

4. Gehen Sie in den config-Modus **configure terminal** (kurz: **conf t**)
5. Vergeben Sie den Routernamen **hostname R1\_Gotha**
6. config-Modus beenden mit **end**
7. Stellen Sie Datum und Uhrzeit ein mit **clock set hh:mm:ss DAY MONTH YEAR!**
8. **show interface e1** (Wie ist der Status von Interface und Protokoll?)

9. Verbinden Sie R1\_Gotha e1 mit R0\_Erfurt e1. Welcher Kabeltyp muss verwendet werden?
10. Interface e1 aktivieren (**conf t, int e1, no shut**) Wie oft ändert sich der Prompt?

11. mit **end** den config-modus verlassen
12. Ermitteln des Nachbars mittels Cisco Discovery Protokoll **show cdp neighbor detail** (Welche IP-Adresse hat der benachbarte Router?)  
.....
13. Aktivieren des Routingprotokolls OSPF, Instanz 1 (**conf t, router ospf 1, end**)
14. routing table anzeigen lassen **sh ip route** (Warum ist die Tabelle leer?)  
.....
15. Router Gotha interface e1 mit IP-Adresse konfigurieren: **conf t, no ip classless, int e1, ip address 10.0.0.2 255.xxx.xxx.xxx** (Welche Subnetmask muss hier angegeben werden, wenn die Netzadresse 29 Bits hat?)  
.....
16. Zulassen der Verwendung des Null-Subnetzes mit **ip subnet-zero**
17. das Netzwerk 10.0.0.0. zum Routing hinzufügen (**router ospf 1, network 10.0.0.0 0.0.0.xxx area 0**) Welche Wildcardmask gehört zu einer 29-Bit Netzadresse?  
.....
18. routing table anzeigen lassen **end, sh ip route** (a: Woher kommen die neuen Einträge, die nicht das Netz 10.0.0.0 betreffen? b: Wieviele?)  
.....
19. Ist das Interface des Nachbarn R0\_Erfurt erreichbar? **ping 10.0.0.1** Welche Antwortzeiten in Millisekunden bringt der ping?  
.....
20. Interface e0 von R1\_Gotha mit IP versehen: 10.1.0.1 / 26 **conf t, int e0, ip add 10.1.0.1 255.255.255.192**, Interface hochfahren **no shut**, das Netzwerk dem Routing hinzufügen **router ospf 1, network 10.1.0.0 0.0.0.63 area 0**, Laptop mit LAN-Karte an R1\_Gotha e0 anschließen (Welches Kabel?)  
.....
21. IP am Laptop einstellen = 10.1.0.3/26, GW=10.1.0.1 und vom DOS-Prompt des Laptops **ping 90.90.90.90** zum Server ausführen. Ersatzweise kann, wenn kein Server vorhanden ist, das Servergateway 90.90.90.1 gepingt werden. Welche Antwortzeiten in Millisekunden bringt der ping? .....  

22. **sh int e0** (a: Welchen speed hat das Interface? Vgl. Punkt 2.4.2) .....  
 (b: Welchen duplex-mode? Vgl. Punkt 2.4.2) .....  
 (c: error-counters: Woher kommen / kämen die collisions, falls vorhanden?)  
 .....  
 (d: Welche counters ändern sich noch?) .....
23. Vom DOS-Prompt des Laptops **ping -t -l 1000 90.90.90.90** einen Dauerping mit Last von 1000 Bytes zum Server ausführen. Ziehen Sie das Ethernetkabel an R1\_Gotha e0 ab und stecken Sie es erneut. a: Was hat sich an den error-counters geändert?

.....

b: Warum? .....

24. Erzeugen Sie ein immer erreichbares virtuelles Loopback-Interface 80.1.1.1 / 32 `conf t, int loop0, ip add 80.1.1.1 255.255.255.255`, Interface hochfahren `no shut`, das Netzwerk dem Routing hinzufügen `router ospf 1, network 80.1.1.1 0.0.0.0 area 0, end`
25. Damit dieser Router nicht nur über die Console, sondern auch per telnet aus dem Netz und von anderen Routern aus erreichbar ist, öffnen Sie den telnet-Zugang `conf t, line vty 0 4`, sichern Sie ihn mit dem Password „cisco“ `password cisco` und erzwingen Sie eine password-Abfrage `login`.
26. Sichern Sie den enable-Modus mit dem selben Password `enable password cisco, end !`
27. running config anzeigen lassen `sh run`
28. lokales Speichern der running config: `copy running-conf startup-conf`

#### 4.4 Versuch 2: Inbetriebnahme des Routers „R2\_Weimar“

Laptop verbinden mit console des Routers R2\_Weimar

Nutzen Sie das Terminalprogramm *hyperterminal* oder *TeraTerm* mit den Einstellungen *com1* (oder die vom USB-Interface simulierte COM) *9600 8bit kein stopbit*

1. Router R2\_Weimar einschalten, booten lassen. Der Router ist ohne jegliche Konfiguration. Ignorieren Sie die Vorschläge zur menügeführten Konfiguration: use configure dialog: **no**, terminate autionstall: **yes**. Der Router ist bereit, wenn der Prompt wie folgt aussieht: **Router>**
2. Um den erweiterten Befehlssatz zur Verfügung zu haben und konfigurieren zu können, gehen Sie in den enable-Modus: **enable**
3. **show version** ( a: Welche Interfaces sind vorhanden? b: Welches IOS ist geladen?)

.....

4. Gehen Sie in den config-Modus `configure terminal` (kurz: `conf t`)
5. Vergeben Sie den Routernamen `hostname R2_Weimar`
6. config-Modus beenden mit `end`.
7. Stellen Sie Datum und Uhrzeit ein
8. `sh int s0` (Wie ist der Status von Interface und Protokoll?)

.....

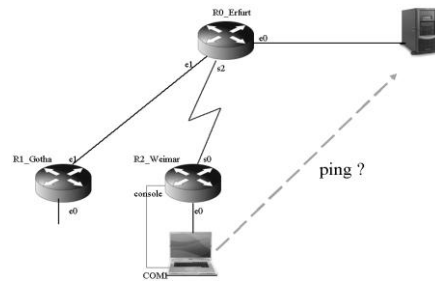
9. Verbinden Sie R2\_Weimar s0 mit Erfurt s2. Router Erfurt gibt die Clockrate vor. (a: Welcher Kabeltyp? b: Welche Steckerseite muss an welchen Router?)

.....

10. Interface s0 aktivieren (`conf t, int s0, no shut`), interface s0 mit IP-Adresse konfigurieren: `ip address 20.0.0.2 255.xxx.xxx.xxx` (30 Bits Netzanteil)  
Bandbreite der seriellen Leitung festlegen: `bandwidth 2048`
11. Das variablen Subnettings ip classless ist in diesem IOS per default aktiv.
12. Zulassen der Verwendung des Null-Subnetzes mit `ip subnet-zero`
13. Aktivieren des Routingprotokolls OSPF ( `router ospf 1`)
14. das Netzwerk 20.0.0.0. zum Routing hinzufügen (`network 20.0.0.0 0.0.0.xxx area 0`) Welche Wildcardmask gehört zu einer 30-Bit Netzadresse?

.....

15. Interface e0 von R2\_Weimar mit IP versehen: 20.1.0.1 / 26 `conf t, int e0, ip add 20.1.0.1 255.255.255.192`, Interface hochfahren `no shut`, das Netzwerk dem Routing hinzufügen `router ospf 1, network 20.1.0.0 0.0.0.63 area 0, end`,
16. Laptop mit LAN-Karte an R2\_Weimar e0 anschließen, IP am Laptop einstellen = 20.1.0.3/26, GW=20.1.0.1 und vom DOS-Prompt des Laptops `ping 90.90.90.90` zum Server ausführen. Ersatzweise kann, wenn kein Server vorhanden ist, das Servergateway 90.90.90.1 gepingt werden. Welche Antwortzeiten in Millisekunden bringt der ping? .....
17. Erzeugen Sie ein immer erreichbares virtuelles Loopback-Interface 80.2.1.1 / 32 `conf t, int loop0, ip add 80.2.1.1 255.255.255.255`, Interface hochfahren `no shut`, das Netzwerk dem Routing hinzufügen `router ospf 1, network 80.2.1.1 0.0.0.0 area 0, end`
18. Damit dieser Router nicht nur über die Console, sondern auch per telnet aus dem Netz und von anderen Routern aus erreichbar ist, öffnen Sie den telnet-Zugang `conf t, line vty 0 4`, sichern Sie ihn mit dem Passwort „cisco“. `password cisco` und erzwingen Sie eine Passwort-Abfrage `login`.
19. Sichern Sie den enable-Modus `enable password cisco, end`,
20. running config anzeigen lassen: `sh run`
21. lokales Speichern der running config: `copy running-config startup-config`

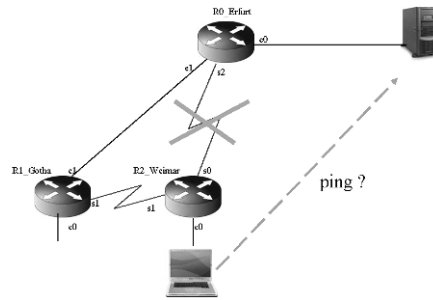


#### 4.5 Versuch 3: Querverbindung R1\_Gotha zu R2\_Weimar

1. Verbinden von R1\_Gotha s1 mit R2\_Weimar s1 mit serielllem Kabel. Router Weimar interface s1 mit IP-Adresse konfigurieren: `int s1, ip address 40.0.0.2.255.255.255.252, bandwidth 128, no shut`
2. Router Gotha interface s1 mit IP-Adresse und als DCE konfigurieren: `int s1, ip address 40.0.0.1.255.255.255.252, bandwidth 128, clock rate 20000, no shut` Warum muss einer der beiden Router als DCE arbeiten?  
.....
3. das Netzwerk 40.0.0.0. auf R1\_Gotha und R2\_Weimar zum Routing hinzufügen (`conf t, router ospf 1, network 40.0.0.0 0.0.0.3 area 0`)
4. Login in Router R2\_Weimar, routing table anzeigen lassen `sh ip route` (Woher kommen die Einträge für die 80er Netze und das 90er Netz?)  
.....  
.....
5. Sind die loopback-Interfaces der Nachbarn erreichbar? `ping 80.0.1.1` (R0\_Erfurt loop0), `ping 80.1.1.1` (R1\_Gotha loop0) Welche Antwortzeiten in Millisekunden bringt der ping? .....
6. Ermitteln Sie den Weg eines ICMP-Paketes vom lokalen Ethernet in Weimar zum Tftp-Server. Stecken Sie dazu den Laptop mit dessen Netzwerkkarte an R2\_Weimar e0, geben Sie dem Laptop die IP 20.1.0.2, Gateway 20.1.0.1 Mask 255.255.255.192; vom DOS\_Fenster aus geben Sie folgenden Befehl: `tracert 90.90.90.90` ..... (ersatzweise

auch 90.90.90.1) Welche Routerinterfaces werden passiert?

- .....
7. Erzeugen Sie eine „WAN-Störung“ durch Lösen der Kabelverbindung an R2\_Weimar s0
  8. Ermitteln Sie den Weg eines ICMP-Paketes vom lokalen Ethernet in Weimar zum Tftp-Server  
**tracert 90.90.90.90**  
(ersatzweise auch 90.90.90.1)  
Welche Routerinterfaces werden passiert?



- .....
9. Routingtable anzeigen lassen **sh ip route** (Welchen Unterschied zur vorherigen Routingtable in Schritt 4 stellen Sie fest?)
- .....
- .....

10. Stellen Sie die Kabelverbindung an R2\_Weimar s0 wieder her.
11. running config anzeigen lassen **sh run**
12. Speichern der running config lokal: **copy running-conf startup-conf**

#### 4.6 Versuch 4: Inbetriebnahme des Routers „Jena“

Laptop verbinden mit console des Routers R3\_Jena.  
Nutzen Sie das Terminalprogramm *hyperterminal* oder *TeraTerm* mit den Einstellungen *com1* (oder die vom USB-Interface simulierte COM) *9600 8bit kein stopbit*

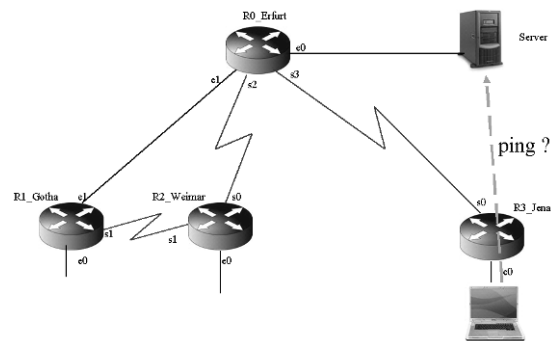
1. Router R3\_Jena einschalten, booten lassen. Der Router ist ohne jegliche Konfiguration. Ignorieren Sie die Vorschläge zur menügeführten Konfiguration: use configure dialog: **no**, terminate autionstall: **yes** . Der Router ist bereit, wenn der Prompt wie folgt aussieht:  
**Router>**
  2. Um den erweiterten Befehlssatz zur Verfügung zu haben und konfigurieren zu können, gehen Sie in den enable-Modus: **enable**
  3. **show version** (a: Welche Interfaces sind vorhanden? b: Welches IOS ist geladen?)
- .....
4. Gehen Sie in den config-Modus **configure terminal** (kurz: conf t)
  5. Vergeben Sie den Routernamen **hostname R3\_Jena**
  6. config-Modus beenden mit **end**
  7. Stellen Sie Datum und Uhrzeit ein.
  8. **sh int s0** (Wie ist der Status von Interface und Protokoll?)
- .....
9. Verbinden Sie R3\_Jena s0 mit Erfurt s3. Router Erfurt gibt die Clockrate vor. (a: Welcher Kabeltyp? b: Welche Steckerseite muss an welchen Router?)
- .....
10. Zulassen der Verwendung des Null-Subnetzes mit **ip subnet-zero**



11. Interface s0 aktivieren (`conf t, int s0, no shut`), interface s0 mit IP-Adresse konfigurieren: `ip address 30.0.0.2 255.xxx.xxx.xxx` (30 Bits Netzanteil)
12. Warum meldet der Router „bad mask“?

- .....
13. Aktivieren des des variablen Subnettings mit `ip classless`(Dieser Router hat ein älteres IOS, bei dem ip classless per Hand aktiviert werden muss)
  14. Wederholen: Interface s0 aktivieren (`int s0, no shut`), interface s0 mit IP-Adresse konfigurieren: `ip address 30.0.0.2 255.xxx.xxx.xxx` (30 Bits Netzanteil)
  15. Bandbreite der seriellen Leitung festlegen: `bandwidth 2048`
  16. Aktivieren des Routingprotokolls OSPF (`router ospf 1`)
  17. das Netzwerk 30.0.0.0. zum Routing hinzufügen (`network 30.0.0.0 0.0.0.xxx area 0`) Welche Wildcardmask gehört zu einer 28-Bit Netzadresse?

- .....
18. Interface e0 von R3\_Jena mit IP versehen: 30.1.0.1 / 26 `conf t, int e0, ip add 30.1.0.1 255.255.255.192`, Interface hochfahren `no shut`, das Netzwerk dem Routing hinzufügen `router ospf 1, network 30.1.0.0 0.0.0.63 area 0, end`, Laptop mit LAN-Karte an R2\_Weimar e0 anschließen, IP am Laptop einstellen = 30.1.0.3/26, GW=30.1.0.1 und vom DOS-Prompt des Laptops `ping 90.90.90.90` zum Server ausführen. Ersatzweise kann, wenn kein Server vorhanden ist, das Servergateway 90.90.90.1 gepingt werden.



Welche Antwortzeiten in Millisekunden bringt der ping? .....

19. Erzeugen Sie ein immer aktives virtuelles Loopback-Interface 80.3.1.1/32 : `conf t, int loop0, ip add 80.3.1.1 255.255.255.255`, Interface hochfahren `no shut`, das Netzwerk dem Routing hinzufügen `router ospf 1, network 80.3.1.1 0.0.0.0 area 0, end`
20. Damit dieser Router nicht nur über die Console, sondern auch per telnet aus dem Netz und von anderen Routern aus erreichbar ist, öffnen Sie den telnet-Zugang `conf t, line vty 0 4`, sichern Sie ihn mit dem Passwort „cisco“ `password cisco` und erzwingen Sie eine Passwort-Abfrage `login`
21. Sichern Sie den enable-Modus mit dem selben Passwort `enable password cisco, end`,
22. Speichern der running config lokal: `copy running-config startup-config`

#### 4.7 Versuch 5: Backup-ISDN-Verbindung R3\_Jena zu R2\_Weimar

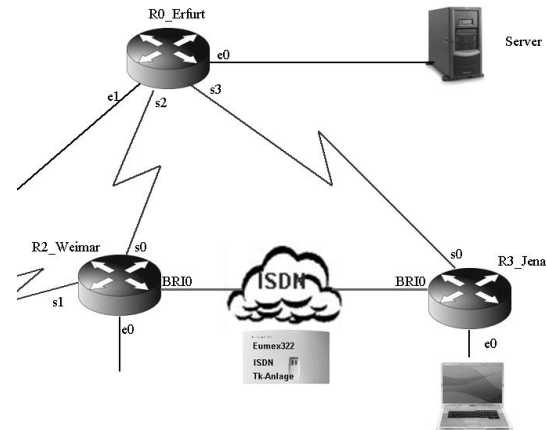
Zwischen Weimar und Jena soll zur Erhöhung der Ausfallsicherheit eine Querverbindung aufgebaut werden. Nun jedoch nicht als serieller WAN-Link, weil gemietete Providerleitungen einige hundert Euro schon allein im Ortsnetz kosten.

In Abhängigkeit der km-Entfernung zwischen 2 Orten können die Leitungskosten leicht tausend Euro pro Monat überschreiten. Es bietet sich an, hier eine Wählverbindung über ISDN einzurichten, die nur bei Bedarf aktiv wird.

Diese Technologie heißt „dial on demand routing = DDR“.

Das öffentliche Telefonnetz wird im Versuch durch eine Telefonanlage Eumex322 dargestellt. Diese Telefonanlage arbeitet mit Werkseinstellungen und braucht bzw. darf **nicht** konfiguriert oder verändert werden!

Die ISDN-Interfaces der Router Weimar und Jena sind mit „BRI“ gekennzeichnet und werden mit den 4adrigen Kabeln an die Telefonanlage Port 11..18 bzw. Port 21..28 angeschlossen. Damit nicht jeder uninteressante Traffic ein Hochfahren der ISDN-Leitung bewirkt, muss mit Access-Listen auf dem BRI-Interface der Traffic gefiltert werden. Dieses und das Thema der Dialer-Interfaces bzw. dialermaps soll im Versuch nicht vertieft werden. Die notwendigen Befehle werden mit Kommentar zur Verfügung gestellt.



#### 4.7.1 Konfiguration der ISDN-Interfaces

- Gehen Sie auf R3\_Jena in den config-Modus **configure terminal** und fügen Sie folgende Befehle dem **interface Serial0** hinzu:  
**description** zu R0\_Erfurt s3  
**backup delay 5 5** (wenn int s0 down geht, aktiviere nach 5 sec. das Backup. Backup nach 5 sec wieder down, sobald das int s0 wieder aktiv ist)  
**backup interface BRI0** (benutze das int BRI0 als Backup)
- Fügen Sie folgende Befehle dem **interface BRI0** hinzu:  
**description Backup zu R2\_Weimar\_eigene\_RufNr=21** (ist nur eine Beschriftung)  
**ip address 172.16.3.21 255.255.255.0** (ist die IP-Adresse des Interfaces)  
**encapsulation ppp** (ppp= point to multipoint)  
**dialer idle-timeout 60** (Verbindungstrennung nach 60 sec. ohne Traffic)  
**dialer map ip 172.16.3.11 name R2\_Weimar broadcast 11**  
 (um die IP 172.16.3.11 zu erreichen, wähle die Rufnummer 11 und stelle sicher, dass sich dort R2\_Weimar meldet)  
**dialer-group 1**  
 (zeigt auf die Dialer-Liste 1, in welcher erlaubter Traffic notiert ist)  
**ppp authentication chap**  
**no shut**  
**ppp multilink, exit**
- Konfigurieren Sie den Router R3\_Jena mit dem Befehl **isdn switch-type basic-net3** (damit wird dem ISDN-Interface des Routers der Anschlussstyp „Euro-ISDN“ zugewiesen)
- Fügen Sie das Netz 172.16.3.0 dem OSPF-Routingprozess hinzu: **router ospf 1, network 172.16.3.0 0.0.0.255 area 0**
- Konfigurieren Sie den Router R3\_Jena mit dem Befehl **username R2\_Weimar password 0 ISDNPASS** (damit wird dem User „R2\_Weimar“ erlaubt, mittels nicht (0) verschlüsseltem Chap-Passwort „ISDNPASS“ sich mit den Router R3\_Jena zu verbinden)
- Fügen Sie folgende Befehle dem Router hinzu:  
**ip route 0.0.0.0 0.0.0.0 172.16.3.11 254** (damit wird eine minderwertige [Metrik 254] Defaultroute nach 172.16.3.11 gesetzt, die nur dann gilt, wenn keine besseren Routen vorhanden sind)  
**dialer-list 1 protocol ip list 100** (damit wird der Traffic durch die Accessliste 100 gefiltert)  
**access-list 100 deny ospf any any** (damit wird OSPF-Traffic über ISDN verboten)  
**access-list 100 permit ip any any** (damit wird jeder andere IP-Traffic über ISDN erlaubt)
- config-Modus beenden mit **end** und Speichern mit **copy run start**
- Verbinden Sie das BRI-Interface mittels 4poligem Kabel zur Telefonanlage S<sub>0</sub>-Port „11...18“

9. Gehen Sie direkt vom Prompt R1\_Gotha via telnet auf R2\_Weimar . Geben Sie dazu einfach die loopback-Adresse von Weimar m aPrompt in Gotha ein: **80.2.1.1** . Gehen Sie in den config-Modus: **configure terminal**
10. Fügen Sie folgende Befehle dem **interface BRI0** hinzu:
 

```

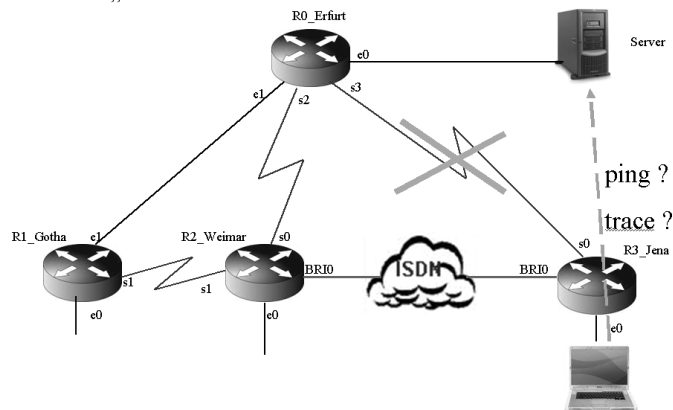
description Backup zu R3_Jena_eigene_RufNr=11 (ist nur eine Beschriftung)
ip address 172.16.3.11 255.255.255.0 (ist die IP-Adresse des Interfaces)
encapsulation ppp (ppp= point to multipoint)
dialer idle-timeout 60 (Verbindungstrennung nach 60 sec. ohne Traffic)
dialer map ip 172.16.3.21 name R3_Jena broadcast 21
      (um die IP 172.16.3.21 zu erreichen, wähle die Rufnummer 21 und stelle sicher, dass sich dort R3_Jena meldet)
dialer-group 1 (zeigt auf die Dialer-Liste 1, in welcher erlaubter Traffic notiert ist)
ppp authentication chap
no shut
ppp multilink, exit
      
```
11. Konfigurieren Sie den Router R2\_Weimar mit dem Befehl **isdn switch-type basic-net3** (damit wird dem ISDN-Interface des Routers der Anschlussstyp „Euro-ISDN“ zugewiesen)
12. Fügen Sie das Netz 172.16.3.0 dem OSPF-Routingprozess hinzu: **router ospf 1, network 172.16.3.0 0.0.0.255 area 0**
13. Konfigurieren Sie den Router R2\_Weimar mit dem Befehl **username R3\_Jena password 0 ISDNPASS** (damit wird dem User „R3\_Jena“ erlaubt, mittels nicht (0) verschlüsseltem Chap-Passwort „ISDNPASS“ sich mit den Router R2\_Weimar zu verbinden)
14. Fügen Sie folgende Befehle dem Router hinzu:
 

```

dialer-list 1 protocol ip list 100 (damit wird der Traffic durch die Accessliste 100 gefiltert)
access-list 100 deny ospf any any (damit wird OSPF-Traffic über ISDN verboten)
access-list 100 permit ip any any (damit wird jeder andere IP-Traffic über ISDN erlaubt)
      
```
15. config-Modus beenden mit **end** und Speichern mit **copy run start**
16. Verbinden Sie das BRI-Interface mittels 4poligem Kabel zur Telefonanlage S<sub>0</sub>-Port „21...28“. Stellen Sie sicher, dass die Telefonanlage mit Strom versorgt wird.

#### 4.7.2 Test der Backup-Funktion

Wenn Sie über die Console verbunden sind, können Sie alle Routermeldungen sofort mitlesen. Wenn Sie über telnet verbunden sind, müssen Sie die Anzeige der Consolemeldung auf Ihre Terminalsession weiterleiten. Dazu dient der Befehl **terminal monitor**. Ausschalten geht mit **terminal no monitor** .



Damit Sie alle Aktivitäten des ISDN-Interfaces sehen können, nutzen Sie den Befehl **debug isdn events**. Um den Status und die Historie der ISDN-Verbindungen sehen zu können, nutzen Sie **show isdn activ** oder **show isdn history** .

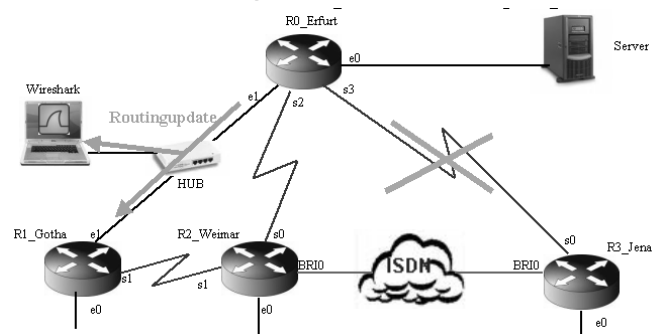
1. Trennen Sie den PC von R3\_Jena e0. Loggen Sie sich via Console auf dem Router R3\_Jena ein.
2. Debuggen Sie mit dem Befehl **debug isdn events**.
3. Trennen Sie die serielle WAN-Verbindung zwischen Jena und Erfurt.
4. a: Wird die ISDN-Leitung aktiv? ..... b: Warum? .....
5. Senden Sie einen ping auf 90.90.90.90 oder 90.90.90.1

6. a: Wird die ISDN-Leitung aktiv? ..... b: Warum? .....
7. Machen Sie einen traceroute zum Server. Welche Routerinterfaces werden passiert?  
.....
8. a: Welcher Router baut die ISDN-Verbindung auf ? ..... b: Called number: .....
9. Stellen Sie die serielle WAN-Verbindung zwischen Jena und Erfurt wieder her.

Bis hierher haben Sie nun das Routernetzwerk in Betrieb genommen und die Backup-Verbindungen erfolgreich getestet. Alle seriellen Verbindungen sind aktiv, Routinginformationen werden zwischen den Niederlassungsroutern und dem Zentralrouter ausgetauscht; alle Ethernet-LANs der Niederlassungen erreichen den Server 90.90.90.90.

#### 4.8 Versuch 6: Snifferanalyse von OSPF-Routingupdates

Durch Mitlesen (Sniffen) des Netztraffics zwischen Erfurt und Gotha soll nachgewiesen werden, dass bei Ausfall der WAN-Leitung zwischen Jena und Erfurt sofort Ersatzrouten durch OSPF-Routingupdates propagiert werden. Dazu wird ein Hub in die Ethernetverbindung zwischen Erfurt und Gotha eingeschleift. Der Hub gibt jedes ankommende Datenpaket auf allen Ports weiter. Damit kann ein Netzwerkscanner jedes Paket mitlesen. Ein Switch kann hier nicht eingesetzt werden, da er Pakete im Standartmodus nur an den einen Zielport sendet.



1. Nehmen Sie dazu den Hub in Betrieb. Verbinden Sie den Hub mit  
R0\_Erfurt e1 - Crosskabel, Hubport 1  
R1\_Gotha e1 – Patchkabel, Hubport 2  
Laptop-Netzwerkkarte IP 10.0.0.3 Mask 255.255.255.192, GW=10.0.0.1, Hubport 3



Achtung! Der Port1 am Hub kann mit dem winzigen Schalter darunter zwischen MDX und MDI-X umgeschaltet werden. Achten Sie auf die richtige Wahl der Ethernetkabel. Am Hub muss für jeden gesteckten Port eine Link-LED grün leuchten.

2. Testen Sie von der Laptop- DOS-Console per ping die Verbindung zu 10.0.0.1 und 10.0.0.2
3. Aktivieren Sie auf Ihrem Laptop das sniffertool *Wireshark*®. Siehe Punkt 3.3.4
4. Lesen Sie aus den Wireshark-Daten die OSPF-Pakete aus und schauen Sie sich die Art der OSPF-Pakete im Normalzustand des Netzes an. Hier dürften nur HELLO-Pakete kommen.
5. Erzeugen Sie durch Trennen der seriellen WAN-Leitung zwischen Jena und Erfurt ein OSPF-Update.
6. Lesen Sie aus den Wireshark-Daten die OSPF-Pakete aus. Welche Arten von OSPF-Paketen kommen bei einem Update wegen Topologieänderung?  
.....

## 4.9 Rücksetzen der Einstellungen:

Nach dem Ende der praktischen Arbeiten setzen Sie die Router R1, R2 und R3 wieder auf die Ausgangskonfiguration zurück. Löschen Sie dazu die startup-config der Router mit **write erase** . Danach schalten Sie den Router aus.

Schalten Sie noch einmal den Router ein und vergewissern Sie sich, dass keine config geladen ist. Danach schalten Sie den Router endgültig aus.

Trennen Sie den Hub und die Telefonanlage ebenfalls vom Stromnetz, da letztere keinen Netzschalter hat.

Lösen Sie alle Ethernet-, seriellen und ISDN-Kabel.

## 5 Anhang

### 5.1 Literaturverzeichnis

- Cisco Website <http://www.cisco.com>
- Cisco Press: Wendell Odom CCNA INTRO. Prüfungshandbuch
- Wikipedia
- Wireshark Dokumentation

### 5.2 Abbildungsverzeichnis

Abbildung 1: Hardware am Arbeitsplatz .....	1
Abbildung 2: Einige Schritte des OSPF-Prozesses.....	7
Abbildung 3: Interfaces am Cisco 2503.....	8
Abbildung 4:Verbindungskabel.....	8
Abbildung 5: Subnet- u. Wildcardmasken .....	11
Abbildung 6: TeraTerm Startscreen – Telnet oder seriell .....	13
Abbildung 7: Windows Command Line mit Beispielen für ipconfig, ping und traceroute .....	13
Abbildung 8: Wireshark Startbildschirm .....	14
Abbildung 9: Wireshark im Einsatz.....	14
Abbildung 10: Ausgangssituation Arbeitsplatz .....	15
Abbildung 11: Endsituation Arbeitsplatz .....	15
Abbildung 12: IP-Adress-Schema.....	16