| Fachhochschule Jena<br>University of Applied Sciences Jena<br>Fachbereich<br>Elektrotechnik/ Informationstechnik | **Weitverkehrsnetze**<br>IP-Routing | Version 1.1 |
|---|---|---|

**Koppelrouter und NAT**

| | | | |
|---|---|---|---|
| Seminargruppe: | ..... | Datum: | ..... |
| Praktikumsgruppe: | ..... | Testat: | ..... |
| Teilnehmer: | ..... | | ..... |
| | ..... | | Unterschrift |

# 1 Versuchsziel

In diesem Versuch sollen die Eigenschaften von IP-Koppelroutern, ihre Konfiguration, die IP-Adressumrechnung und einige weitere Funktionen sowie die LAN-Einstellungen von PCs und diverse Hilfsmittel zur Netzwerkdiagnose untersucht werden.

# 2 Theoretische Grundlagen

## 2.1 Private Netze und die Kopplung zum Internet

Nachdem bis zum Ende der 90er Jahre des letzten Jahrhunderts Rechnernetze hauptsächlich an mittleren und größeren Unternehmens- und Behördenstandorten existierten, wurden nach 2000 zunehmend auch kleine und kleinste Standorte (SOHO[1]) mit Rechnernetzen ausgerüstet. Hinzu kamen dann auch Rechnernetze in Privathaushalten. Heute haben die allermeisten dieser „privaten“[2] Netze eine Kopplung zum (öffentlichen) Internet. Über diese Kopplung haben Nutzer des „privaten“ Netzes auch Zugang zum Internet. Netze in Privathaushalten dienen oft nur dem Zugang zum Internet.

Für die logische Kopplung der „privaten“ Netze zum Internet bietet der Provider in der Regel für jeden seiner Kunden[3] einen eigenen logischen Kanal zu einem Router im Netz des Providers an. In bestimmten Fällen kann auf Kundenseite ein Rechner direkt angeschlossen werden. In der Regel wird auf Kundenseite jedoch ein Router angeschlossen, der auf der „anderen Seite“ mit einem oder mehreren „privaten“ Netzen des Kunden verbunden ist. Diese Struktur zeigt Abbildung 2.1.

1 Small Office, Home Office
2 Privat bedeutet hier lediglich eine Abgrenzung zum Internet, das von Providern betrieben wird.
3 Kunde steht hier für jeden Nutzer der Leistungen des Providers.

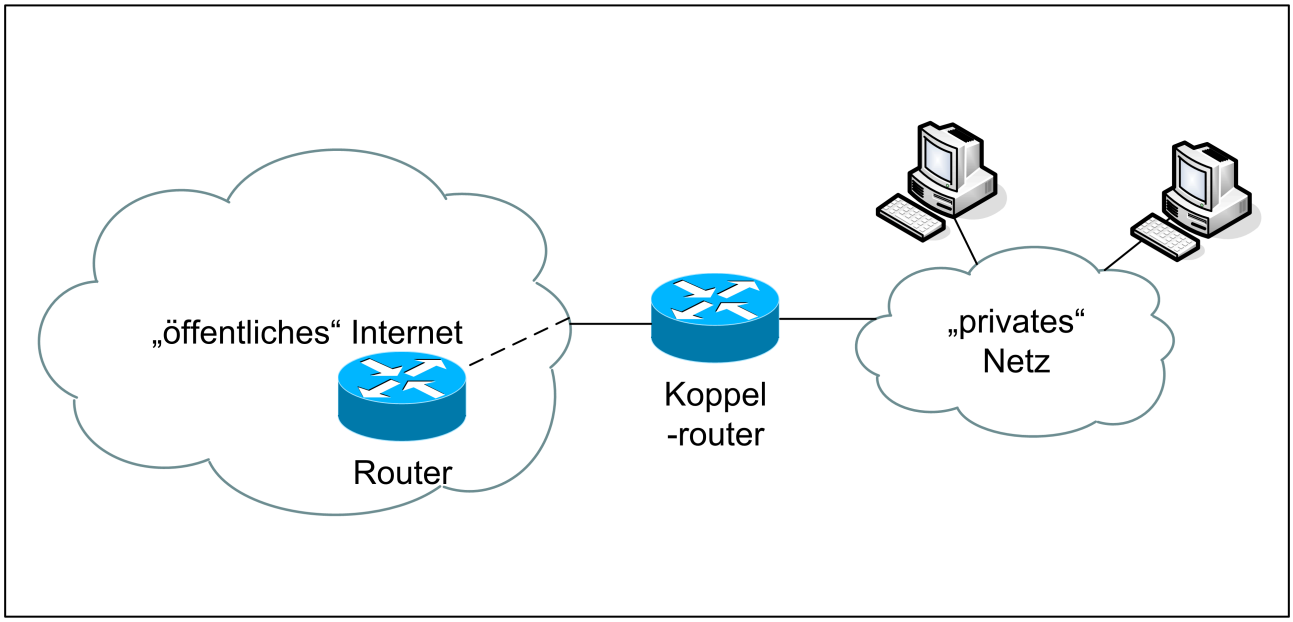

Abbildung 2.1: Kopplung des „privaten“ Netzes zum Internet

## 2.2 Routing und Adressierung

Router sind die Vermittlungsknoten der Rechnernetze. Je nach Adresse, zu der ein Datenpaket gehen soll, wählen Sie den geeigneten nächsten Router und somit den geeigneten Anschluss für die Weiterleitung der Daten aus. Dazu hat jeder Router eine Tabelle mit Adressen und dem zur jeweiligen Adresse passenden Anschluss. Praktisch sind in den Tabellen, soweit möglich, ganze Adressbereiche zusammengefasst. Ein Sonderfall dieser Zusammenfassung ist der Adressbereich des „default Gateway“. Zu diesem Bereich gehören alle Adressen, die nicht einzeln aufgeführt oder Teil eines anderen Adressbereiches sind.

Im Fall des Koppelrouters in Abbildung 2.1 kennt der Koppelrouter den Adressbereich des „privaten“ Netzes. Alle Daten an andere Adressen werden zum Router des Providers geschickt, da diese Empfänger ja nicht im „privaten“ Netz sein können. Der Router des Providers ist für den Koppelrouter das default Gateway.

Hier werden nur Netze mit IP-Adressierung behandelt. Jedes Netz ist durch seine kleinste Adresse, der sogenannten Netzadresse, und die Netzmaske gekennzeichnet. Genaueres dazu kann den Vorlesungsunterlagen entnommen werden.

## 2.3 Adressumrechnung

Die Adressen im Internet sind weltweit koordiniert. Die jeweiligen Nutzer müssen solche Adressen über den Provider beantragen. Die Zuweisung erfolgt sparsam.

Wird ein „privates“ Rechnernetz ohne Kopplung zum Internet aufgebaut, so können hier sogenannte „private IP-Adressen“ verwendet werden. Dazu gibt es einige solche Adressbereiche, die aus dem möglichen Bereich aller IP-Adressen ausgeklammert wurden. Solche Adressen kann jeder ohne spezielle Zuweisung verwenden. Da diese Adressen weltweit nicht nur einmal verwendet werden, sind sie von der Weiterleitung im Internet ausgeschlossen.

„Private“ Adressen werden auch verwendet, wenn ein Nutzer weniger öffentliche IP-Adressen bekommen kann als er Adressen in seinem Netz benötigt.

Werden Netze mit „privaten“ Adressen mit dem Internet gekoppelt, so ist ein spezielles Verfahren notwendig, die Adressumrechnung (NAT – Native Address Translation oder Net Address Translation). Dieses Verfahren stellt eine Kopplung zwischen den „privaten“ Adressen und öffentlichen Adressen her.

Dem Kunden muss mindestens eine öffentliche Adresse zugeordnet werden. In einigen Fällen erhält er auch mehrere öffentliche Adressen.

Muss ein lokales Gerät (Rechner) Daten zu einer öffentlichen Adresse schicken, so bereitet seine private Absenderadresse im Internet Probleme. Deshalb wird im Koppelrouter diese private Absenderadresse gegen eine der zugeordneten öffentlichen Adressen ausgetauscht. Kommt aus dem Internet eine Datenpaket an diese öffentliche Adresse, so schickt der Koppelrouter die Daten an die entsprechende private Adresse weiter.

Hier werden drei wesentliche Betriebsweisen von NAT vorgestellt:

- 1 zu 1 NAT: Jeder privaten Adresse wird eine öffentliche Adresse fest zugeordnet.
- Pooled NAT: Jeder privaten Adresse, von der Daten in das Internet geschickt werden soll, wird für die benötigte Zeit eine freie öffentliche Adresse zugeordnet.
- Port-NAT: Jede private Adresse kann unter einer gemeinsamen öffentlichen Adresse Daten in das Internet schicken. Um die Daten, die aus dem Internet kommen, der richtigen privaten Adresse zuordnen zu können, wird zusätzlich die Portnummer des Lokalen Absenders verwendet. Die Portnummer ist ein Wert im Layer-4-Header (TCP oder UDP). Beim Umrechnen der lokalen Adresse bei zum Internet gehenden Daten wird die Portnummer des Absenders so geändert, dass die neue Portnummer eindeutig einem lokalen Gerät zugeordnet ist. Senden zwei oder mehr lokale Geräte mit der selben Absenderportnummer, so werden beim NAT Portnummern geändert. Der Koppelrouter merkt sich diese Änderung und kann Pakete aus dem Internet eindeutig dem jeweiligen lokalen Gerät zuordnen.

  Eine Einschränkung gibt es, wenn die Absenderportnummer bei einem bestimmten Dienst nicht geändert werden darf. Dann kann zur gleichen Zeit nur ein lokales Gerät diesen Dienst nutzen.

Die dritte Variante wird in der Regel immer bei Privatkundenanschlüssen und oft beim Anschluss sehr kleiner anderer Netze angewendet.

## 2.4 DHCP

Neben der eigentlichen Aufgabe des Routings übernehmen solche Koppelrouter noch einige andere Aufgaben. Fast immer ist DHCP (Dynamic Host Configuration Protocol) implementiert, das auch deaktiviert werden kann.

Mittels DHCP kann Rechnern eine freie IP-Adresse aus dem lokalen Adressraum zugewiesen werden. Zusätzlich werden einige weitere Parameter übertragen, die für die Netzwerkkopplung notwendig sind (meist Default Gateway, Adressen der DNS-Server).

In größeren Rechnernetzen übernimmt diese Aufgabe meist ein Server, der jedoch in kleinen und kleinsten Netzen meist nicht vorhanden ist.

## 2.5 DNS

DNS-Server erledigen die Namensauflösung. Zu einem Domänennamen aus dem Internet liefert der DNS-Server die passende IP-Adresse. Nur mit dieser kann dann der Zugriff erfolgen. DNS-Server betreiben verschiedene Institutionen.

Entweder kennt der Koppelrouter DNS-Serveradressen und teilt diese gegebenenfalls per DHCP den Rechnern im lokalen Netz mit, oder er stellt sich den lokalen Rechnern per DHCP selber als DNS-Server vor.

Im ersten Fall fragen die lokalen Rechner direkt bei den DNS-Servern im Internet nach. Im zweiten Fall fragen die lokalen Rechner beim Koppelrouter nach. Dieser muss dann natürlich auch Adressen von DNS-Servern im Internet kennen, bei denen er dann selber nachfragt. Er hat keinesfalls eine eigen große Datenbank mit allen möglichen Domänennamen.

Beziehen die lokalen Rechner ihre Netzwerkeinstellungen nicht per DHCP, so müssen die DNS-Adressen von Hand eingetragen werden. Es kommen auch die Adressen wie im ersten Fall oder die Adresse wie im zweiten Fall zum Einsatz.

## 2.6 Firewall

Im Zusammenhang mit der Kopplung zum Internet treten Sicherheitsfragen auf. Aus dem Internet ist immer

mit Angriffen zu rechnen. Zum Schutz werden Firewalls verwendet. Auf üblichen Koppelroutern sind in den meisten Fällen solche Firewalls installiert, die auf OSI-Layer 3 und / oder 4 arbeiten (Paketfilter).

Zum einen sind das statische Filter und zum anderen dynamische.

Statische Filter werden fest eingetragen (oder sind es vom Hersteller her).

Die dynamische Filterung erfolgt mittels Stateful Packet Inspection. Pakete aus dem Internet werden nur dann zum Kundennetz geroutet, wenn sie zu einem aus dem Kundennetz initiierten Datenfluss passen.

Praktisch werden die beiden Techniken oft auch kombiniert. So können zusätzlich zur dynamischen Filterung noch per statischem Filter Datenarten festgelegt werden, die auch ohne Veranlassung aus dem lokalen Netz durchgelassen werden.

Die Firewall kann oft auch deaktiviert bzw. für alle Daten aus dem Internet durchlässig gemacht werden, wovon allerdings dringend abgeraten wird.

## 2.7 Protokolle

Aktionen innerhalb des Routers sind von außen höchstens an den Folgen zu erkennen. Diese werden teilweise nicht wahrgenommen (z. B. unverlangte Daten aus dem Internet werden nicht weitergeleitet oder Versuch der Konfiguration des Routers aus dem Internet) oder die Ursache ist unklar (z. B. Grund für das Ausbleiben im Internet angeforderter Daten). Um solche Aktionen erkennbar und analysierbar zu machen, kann in Routern in der Regel ein Log erzeugt werden. Dieses wird entweder über die Bedienschnittstelle direkt auf dem Router gelesen oder über ein Protokoll an einen externen Server geschickt, von dem die Informationen abrufbar sind.

Typische Protokolle zum Weiterleiten von Logdaten sind

- Syslog - eher bei „größeren“ Routern
- SMTP - eher bei kleinen Routern, wie den hier behandelten.

Mittels SMTP werden ein oder mehrere Logeinträge in eine Email gepackt und an eine festgelegte Adresse geschickt.

Die Einträge im Log sind in der Regel mit einem Datums- und Zeitstempel versehen. Der Router hat dazu eine interne Uhr. Diese kann meist mittels NTP oder SNTP synchronisiert werden.

## 2.8 Test- und Analysewerkzeuge

Diese werden hier anhand von Windows beschrieben.

### 2.8.1 IPCONFIG

Zeigt und beeinflusst die Netzwerkeinstellungen des PC.

### 2.8.2 PING

Fordert den Host mit einer angegebenen IP-Adresse auf, mit einem Pong zu antworten und dient zum Test der Erreichbarkeit des Hosts. Bei einer Antwort ist er erreichbar. Die fehlende Antwort bedeutet, dass der Host nicht erreicht wird oder dass der Host die Quelle des Ping nicht erreicht (Rückrichtung) oder dass der Host auf Ping nicht antwortet.

### 2.8.3 TRACERT

TraceRoute ermittelt die Route zum Gerät mit einer angegebenen IP-Adresse

### 2.8.4 ARP

Zeigt den Inhalt des ARP-Cache auf dem PC oder beeinflusst diesen.

### 2.8.5 Netzwerkeinstellungen des PC

Dient zur Einstellung diverser Netzwerkparameter auf dem PC. Hier kann auch der automatische Bezug dieser Daten per DHCP aktiviert oder deaktiviert werden.

### 2.8.6 Wireshark

Wireshark (früher Ethereal) ist ein Programm, mit dem auf einem PC der Netzwerkverkehr der einzelnen Netzwerkanschlüsse mitgeschnitten und dekodiert werden kann. Entweder ist es der Netzwerkverkehr, den der PC mit dem Netzwerk selber austauscht oder ein von außen nur zur Diagnose zugeführter Netzwerkverkehr.

Der Netzwerkverkehr ab OSI-Schicht 2 aufwärts wird angezeigt.

### 2.8.7 Ethernet-Tester MX120

Dieses Gerät dient zum Test von Ethernet-Netzwerken. Zusätzlich können auch auf höheren OSI-Schichten Funktionen genutzt werden. Hier interessiert die Möglichkeit des Ping (vergleiche 2.8.2) auf ein anderes Gerät im Netzwerk.

# 3 Versuchsvorbereitung

## 3.1 Konfigurationszugang zu Routern

Informieren Sie sich im Kompakthandbuch (23 Seiten) des Routers ZYXEL Prestige 324 (P-324) (www.zyxel.com) über den Konfigurationszugang zum Router.

- Welches ist die Werkseinstellung des Routers auf der LAN-Seite (Netzadresse, Netzmaske)?
- Wenn Sie den Konfigurationszugang hier mit den im Fach „LAN“ im Skript unter 3.11 beschriebenen Arten vergleichen, um welche Art handelt es sich?
- Wie können Sie die LAN-Konfiguration des Routers ermitteln, wenn keine Unterlagen vorhanden sind? Hilft Ihnen DHCP weiter? Wenn ja, wie?

## 3.2 Verwaltung der LAN-Adressen im Router (DHCP)

- Wie funktioniert DHCP im Prinzip?

Die LAN-Seite eines Routers gehört zu einem IP-Netz mit 256 Adressen.

- Was ist bei der Einstellung des Adressbereiches für den DHCP-Server zu beachten?
- Was ist zu beachten, wenn auch Adressen manuell in diesem Netz vergeben werden sollen?

## 3.3 Einstellung der lokalen Adressen im Router

In einem DSL-Router soll auf der LAN-Seite ein anderes IP-Netz eingestellt werden.

- Was ist alles umzustellen und zu beachten, wenn der Router auch als DHCP-Server arbeitet? Informieren Sie sich dazu im Handbuch.
- Spielt die Reihenfolge der Eingaben eine Rolle?

## 3.4 Relevante Konfigurationen an Rechnern

- Wie werden auf einem PC (oder Notebook) die Basiseinstellungen für den IP-Netzwerkzugang vorgenommen? Informieren Sie sich auf einem Windows-PC.
- Welche Werte werden typischerweise eingestellt?

– Welche Werte müssen auf dem PC eingestellt werden, wenn der PC zur LAN-Seite eines Routers ZYXEL Prestige 324 eine Netzwerkverbindung erhalten soll? Der Router hat die Werkseinstellungen und der PC arbeitet mit DHCP?

– Welche Werte müssen auf dem PC manuell eingestellt werden, wenn der PC im Gegensatz zum vorigen Punkt kein DHCP nutzen soll?

## 3.5 Weitere Grundkonfiguration des Routers

### 3.5.1 Netzwerkdaten am WAN-Anschluss

Es gibt für den WAN-Anschluss mehrere Betriebsarten. Die auszuwählende Betriebsart hängt von der Anschlussart ab, die der Internetprovider bereitstellt. Gebräuchlich sind in Deutschland folgende Betriebsarten:

- PPPoE / PPPoA meist bei ADSL-Anschlüssen, Netzwerkdaten werden bei der jeweiligen Anmeldung im Netz automatisch vom Provider an den Koppelrouter übertragen
- feste IP meist bei kommerziellen Anschlüssen, über SDSL oder andere „Leitungen“, die Netzwerkdaten werden vom Provider bereitgestellt, bleiben gleich und werden „für immer“ fest im Koppelrouter eingestellt.

Im Versuch wird die zweite Variante verwendet.

– Wie kann erreicht werden, dass vom Router jeglicher Netzwerkverkehr in Richtung Internet zum nächsten Knoten im Internet geschickt wird? In unserem Fall ist das der PC im WAN, Abbildung 4.1, links im Bild.

– Bestimmen Sie den Wert der Netzmaske aus Abbildung 4.1 in der anderen Schreibweise. Wie lautet auf der WAN-Seite die Netzadresse und welches ist die höchste nutzbare Adresse in diesem Netz?

### 3.5.2 NAT

Der Router P-324 beherrscht mehrere Varianten von NAT. Hier wird nur NAPT untersucht.

– Was versteht man unter NAPT? Wie wirkt es?

### 3.5.3 Firewall

– Was versteht man unter einer Firewall?

– Wie funktioniert SPI?

### 3.5.4 Filter

– Wozu werden im Router Filter verwendet?

### 3.5.5 Log

– Wozu dient im Router das Log?

## 3.6 Einsatz und Bedienung von Test- und Analysewerkzeugen

### 3.6.1 IPCONFIG

Im DOS-Fenster / an der Eingabeaufforderung

`ipconfig` Netzwerkdaten des PC anzeigen

| | |
|---|---|
| `ipconfig /all` | detaillierte Netzwerkdaten des PC anzeigen |
| `ipconfig /release` | über DHCP bezogene Adresse seitens des PC freigeben und lokale Einstellungen löschen |
| `ipconfig /renew` | DHCP Adresse durch den PC neu anfordern bzw. Zuteilung verlängern |

### 3.6.2 PING

Im DOS-Fenster / an der Eingabeaufforderung

| | |
|---|---|
| `ping <address>` | Antwort vom Knoten mit der IP-Adresse <address> anfordern, 4 mal |
| `ping <address> -t` | Antwort vom Knoten mit der IP-Adresse <address> anfordern, fortlaufendend |
| `<ctrl> C` | ping <address> -t beenden |

### 3.6.3 TRACERT

Im DOS-Fenster / an der Eingabeaufforderung

| | |
|---|---|
| `tracert <address> -d` | Route zu <address> anzeigen, keine Namensauflösung |

### 3.6.4 ARP

Im DOS-Fenster / an der Eingabeaufforderung

| | |
|---|---|
| `arp -a` | Anzeige der Einträge in der ARP-Tabelle des PC |
| `arp -d` | löscht alle Einträge der ARP-Tabelle des PC |

### 3.6.5 Netzwerkeinstellungen des PC

unter START – SYSTEMSTEUERUNG – NETZWERK- UND FREIGABECENTER - ADAPTEREINSTELLUNGEN ÄNDERN – LAN – (Kennwort) – Internetprotokoll Version 4 – Eigenschaften öffnen

automatischer Bezug aktivierbar

automatischer Bezug deaktivierbar, dann Einstellungen manuell vornehmen

Fenster bestätigen

### 3.6.6 Wireshark

Der Start erfolgt 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.

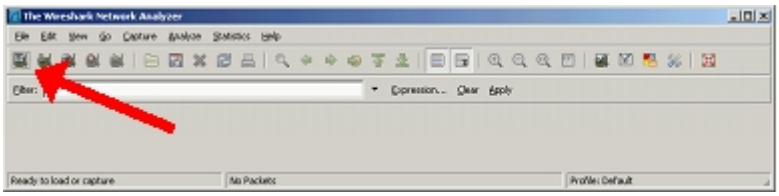


Abbildung 3.1: Wireshark Startbildschirm

Danach muss nur noch der Startknopf der entsprechenden Netzwerkkarte betätigt werden.

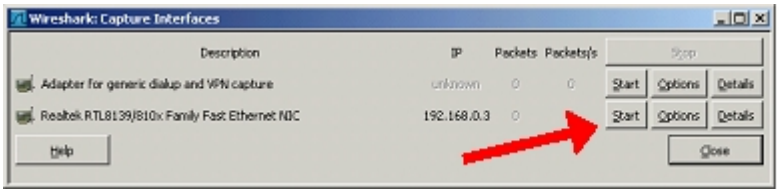

Abbildung 3.2: Wireshark Interface Auswahl

Jetzt werden drei Fensterbereiche angezeigt.

Im oberen Fenster werden alle empfangenen und gesendeten Netzwerkpakete dargestellt.

In der Mitte erfolgt eine Dekodierung des im oberen Fenster ausgewählten Paketes.

Im unteren Fenster wird das im oberen Fenster ausgewählten Paket hexadezimal angezeigt.

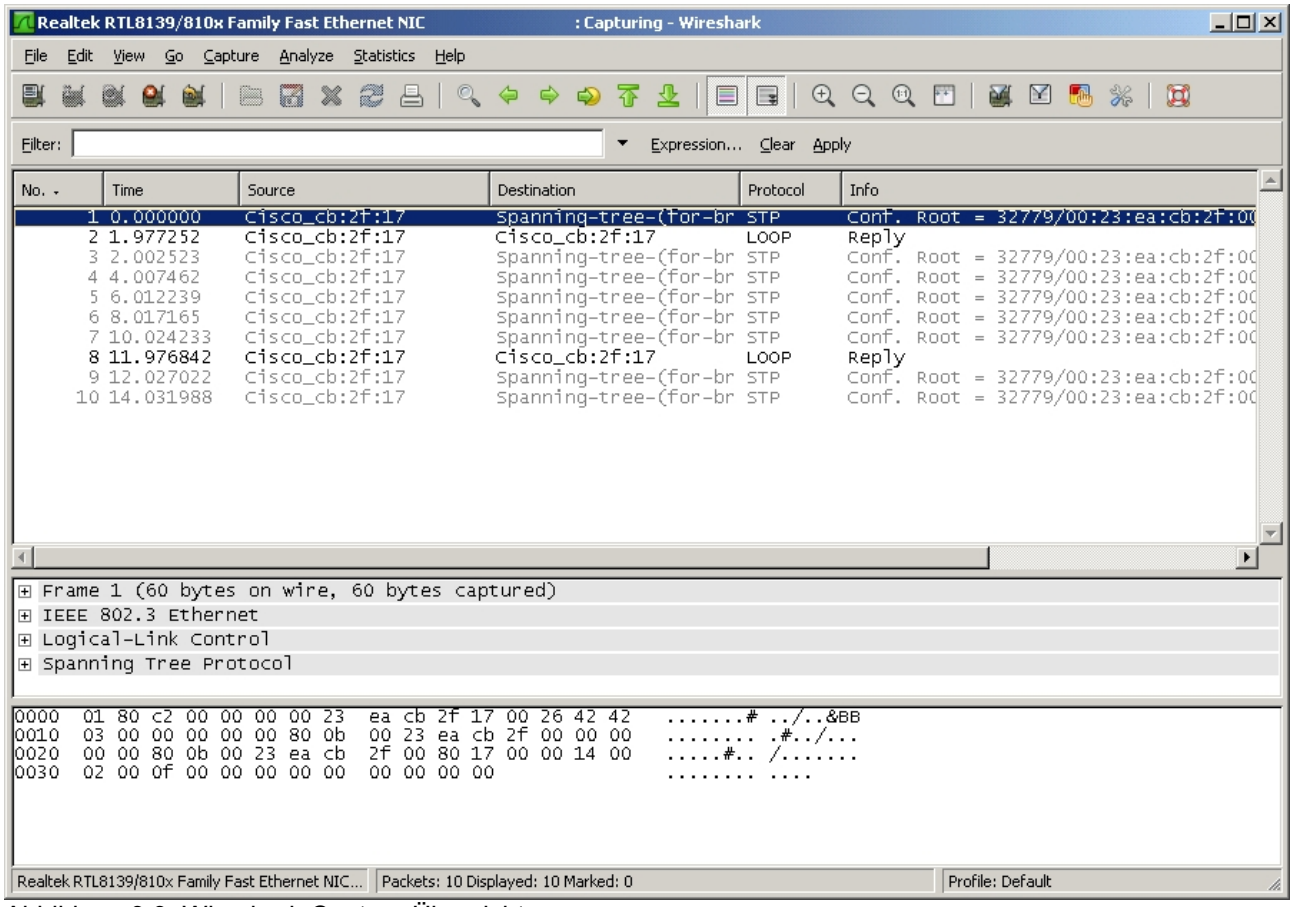

Abbildung 3.3: Wireshark Capture Übersicht

Die Anzeige erfolgt für OSI-Schicht 2 und höher. Der FCS-Wert ist nicht zu sehen. Bei gesendeten Frames erfolgt ein eventuelles Byte-Padding im Ethernet erst im LAN-Adapter, also unterhalb von Wireshark. Deshalb können gesendete Frames scheinbar zu kurz sein.

Durch weitere Buttons in der Symbolleiste kann man den Capture-Vorgang stoppen oder neu starten.

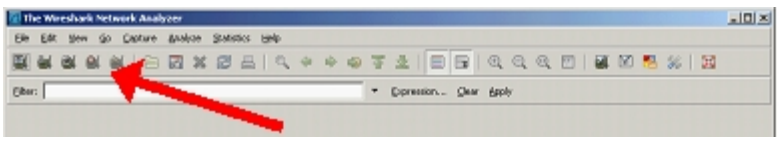
Abbildung 3.4: Wireshark Capture Buttons

### 3.6.7 Ethernet-Tester MX120

**Achtung!**

**Der zu verwendende Netzwerkanschluss befindet sich an der rechten Seite des Gerätes unter einer Gummiabdeckung.**

**Zur Bedienung bitte die transparente Abdeckung des Displays nach oben klappen und nur den Kunststoffstift aus der oberen Gehäuseklappe zum Antippen des Displays verwenden.**

Mit der roten Taste wird das Gerät eingeschaltet (mehrere Sekunden drücken). Nach dem Booten befindet man sich im Hauptmenü (Abbildung 3.5).

Die Benutzung des Gerätes erfolgt am einfachsten per Touchpad. Für dieses ist **nur** der im Deckel befindliche Stift zu benutzen.

Zum Ändern von angezeigten Werten wird das Feld mit den Werten angetippt. Das öffnet ein Eingabefenster, in dem der jeweilige Wert editiert werden kann.

Mit der „Home“-Taste (Haussymbol) kommt man jederzeit zurück ins Anfangsmenü.

Die Nutzung des eingebauten Browsers erfolgt über „Tools“ - „IP Tools“ (roter Pfeil in Abbildung 3.6).

Zuerst werden in der Maske „Network“ (Abbildung 3.7 die eigenen Netzwerkparameter eingestellt und dann am unteren Bildrand die blaue Taste „Connect“ betätigt. Nach dem Durchlauf, der einige Sekunden dauert, ist Abbildung 3.8 zu sehen. Jetzt wird in die Maske WEB/FTP (Abbildung 3.9) gewechselt. In dieser erfolgt die Einstellung der Zieladresse und der Start über die blaue Taste am unteren Bildschirmrand.

Abbildung 3.5: Hauptmenü

Abbildung 3.6: Menü Tools

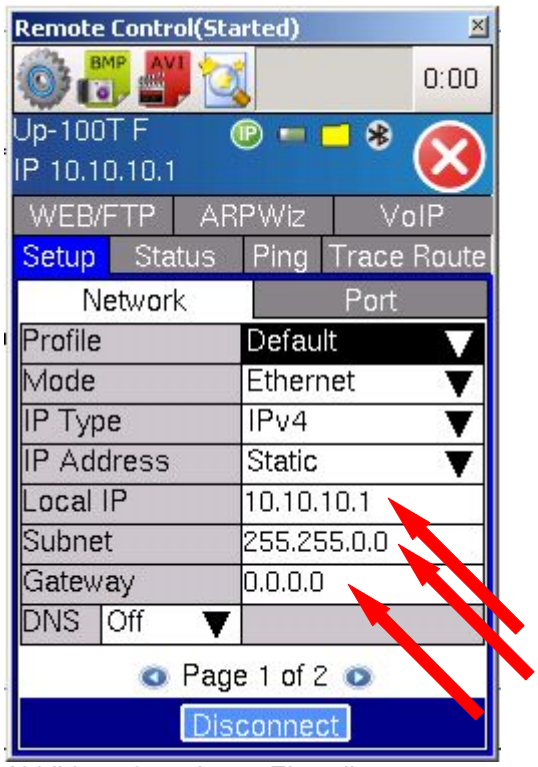


Abbildung 3.7: eigene Einstellungen


Abbildung 3.8: IP gestartet

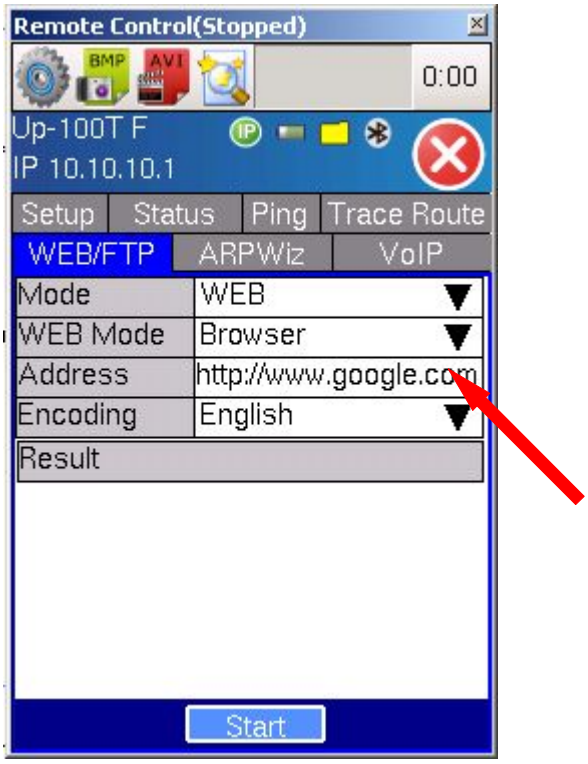


Abbildung 3.9: vor Start Browser

# 4 Versuchsdurchführung

## 4.1 Benötigte Technik

- PC „Internet“
- PC privat
- DSL-Router SMC BARRICADE (mit ADSL-Modem)
- DSL-Router ZYXEL Prestige 324
- Ethernettester VeEX M120
- diverse LAN-Kabel

## 4.2 Grundaufbau

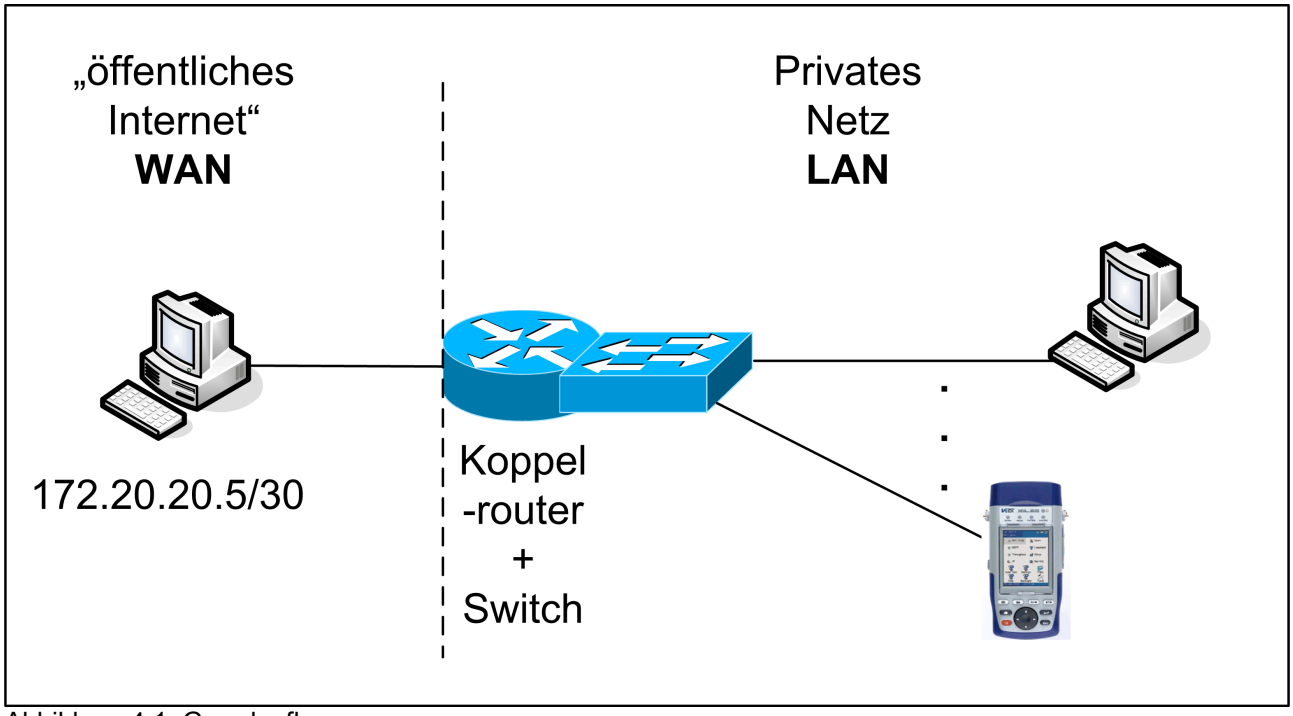


Abbildung 4.1: Grundaufbau

**Anmerkung:** Die IP-Adressen im „öffentlichen Internet“ sind eigentlich Adressen für private Netze. In unserem Versuch können sie auch im „öffentlichen“ Netz verwendet werden, in der Realität jedoch nicht.

## 4.3 Zugang zum Router 1 (SMC)

Der Router SMC BARRICADE wird verwendet. Dieser Router hat ein eingebautes ADSL-Modem, welches hier nicht genutzt wird. Der WAN-Anschluss (ADSL-Port) bleibt frei.

### 4.3.1 PC bezieht LAN-Einstellungen

Hier wird das Beziehen von Netzwerkeinstellungen durch den PC untersucht.

Folgender Ablauf wird empfohlen:

1 Auf PC LAN-Anschluss auf automatischen Bezug der Einstellungen setzen (2 Stellen)

2 Verbindungen herstellen, Router einschalten, ca. 30 Sekunden warten (Hochfahren des Routers)

3 Wireshark starten, Capturing mit Standardwerten auf LAN-Port starten, Ausgaben noch nicht auswerten

4 Auf PC IP-Adresse freigeben

5 Auf PC IP-Angaben im Detail abrufen und dokumentieren

6 Auf PC ARP-Cache löschen, ARP-Cache anzeigen → muss leer sein

7 Auf PC IP-Adresse freigeben

8 Wireshark: Restart capturing

9 Auf PC IP-Einstellungen per DHCP beziehen

10 nach ca. 30 Sekunden in Wireshark Mitschnitt stoppen

11 Auf PC ARP-Tabelle auslesen und dokumentieren

12 Auf dem PC die IP-Daten detailliert auslesen und dokumentieren

13 Mitschnitt auf dem Desktop abspeichern

14 Im Mitschnitt die Frames bis vor dem ersten mit dem Protokoll NBNS analysieren (beide Adressen, Protokoll, Info, DHCP-Felder mit t=1, 3, 6, 12, 50 – soweit vorhanden) und dokumentieren

### 4.3.2 Managementzugang zum Router

Per HTTP wird das Management des Routers aufgerufen (Routeradresse kann aus den IP-Daten des PC entnommen werden, ist dort die Adresse des Standardgateway).

Die Zugangsdaten lauten: **`admin smcadmin`**

Folgende Seiten sollen aufgerufen und genauer angesehen werden:

| | |
|---|---|
| Home (rechts oben) | Bereich LAN analysieren |
| LAN (links) | Daten dokumentieren |
| NAT (links) | dokumentieren, was aktiv ist |
| System Log (links) | ansehen |
| Status (rechts oben) | |
| LAN-Status (links) | Daten dokumentieren |
| TCP-Status (links) | Daten ansehen, erklären |

### 4.3.3 Auswertung

Setzen Sie die in 4.3.1 und 4.3.2 gewonnenen Daten zueinander in Bezug.

## 4.4 Zugang zum Router 2 (Zyxel)

**Achtung:**

**Vor weiteren Arbeiten ist der Router vorsorglich auf die Fabrikeinstellungen zu setzen. Der Ablauf steht im Arbeitsblatt, welches auf dem Laborplatz liegt.**

**In der grafischen Benutzeroberfläche müssen alle Konfigurationsänderungen vor dem Verlassen der jeweiligen Konfigurationsseite bestätigt werden. Wenn die Seite ohne Bestätigung verlassen wird, gehen die Änderungen ohne Wirkung verloren.**

Stellen Sie im lokalen PC die Netzwerkparameter fest von Hand ein. Wählen Sie dazu aus dem im Handbuch des Routers für die Werkseinstellungen genannten Netz eine passende Adresse für den PC aus.

Testen Sie die Erreichbarkeit des Routers vom lokalen PC mittels Ping.

Öffnen Sie das Management des Routers 2 über HTTP. Die IP-Adresse des Routers finden Sie im Handbuch oder wie unter 4.3.2 beschrieben. Verändern Sie das Passwort nicht. Lesen Sie im Handbuch nach, wie dabei zu verfahren ist.

## 4.5 Grundkonfiguration Router 2

### 4.5.1 LAN-Adresse

Lokal soll das Netz **192.168.0.0 / 24** verwendet werden. Stellen Sie das im Router so ein, dass der Router per DHCP auch 50 LAN-Adressen vergeben kann. Die Adressen von .101 aufwärts sollen außerhalb von DHCP verwendbar sein.

Dokumentieren Sie die einzelnen Schritte der Konfiguration und die jeweils eingestellten Werte.

Stellen Sie nach erfolgreicher Konfiguration des Routers den lokalen PC auf automatische Netzwerkkonfiguration um und beziehen Sie die Netzwerkeinstellungen vom Router. Das sollte automatisch nach der Umstellung erfolgen und kann etwa 20...30 Sekunden dauern. Das Ergebnis sehen Sie per ipconfig.

Dokumentieren Sie die Einstellungen detailliert mittels ipconfig.

Testen Sie die Erreichbarkeit des Routers mittels Ping vom lokalen PC und notieren Sie das Ergebnis. Suchen Sie bei fehlender Erreichbarkeit den Fehler.

### 4.5.2 WAN-Adresse

Der Router erhält die Adresse 172.20.20.6. (Die restlichen benötigten Werte können Abbildung 4.1 entnommen werden.) Dokumentieren Sie diese Werte und stellen Sie diese im Router ein.

Testen Sie vom WAN-PC aus per Ping, ob der Router erreichbar ist. Suchen Sie bei fehlender Erreichbarkeit den Fehler.

Testen Sie vom lokalen PC aus per Ping, ob der WAN-PC erreichbar ist. Suchen Sie bei fehlender Erreichbarkeit den Fehler.

## 4.6 Klassisches Routing durch Router 2

### 4.6.1

Schalten Sie im Router auf der Konfigurationsseite „WAN --- WAN IP“ NAT aus (Wert ist None).

Ermitteln Sie mittels tracert den Pfad vom lokalen PC zum WAN-PC und dokumentieren Sie diesen.

### 4.6.2

Starten Sie auf dem WAN-PC und dem lokalen PC jeweils einen Trace (Wireshark) und schicken Sie Ping vom lokalen PC auf den WAN-PC. Halten Sie den Trace an und werten Sie diesen aus. Das Auswerten je eines Ping-Paketes jeder Richtung ist ausreichend. Dokumentieren Sie die Quell- und Zieladressen auf OSI Layer 2 und auf OSI Layer 3 der Ping-Pakete auf beiden PC und stellen Sie diese Werte gegenüber.

### 4.6.3

Starten Sie auf dem WAN-PC einen Trace (Wireshark) und rufen Sie über den Browser SeaMonkey vom lokalen PC die Internetseite 10.10.10.10 auf. (Diese Adresse einfach dort eintragen, wo sonst die Adresse der Internetseite eingetragen wird). Diese Adresse wird natürlich nicht erreicht. Die Aufrufe laufen aber bis zum „Internet-PC“ und werden dort protokolliert. Etwa gleichzeitig dazu soll diese Adresse über den Browser im MX120 aufgerufen werden. Halten Sie dann den Trace an und werten Sie diesen aus. Das Auswerten je

eines Aufruf-Paketes jeder Verkehrsbeziehung ist ausreichend. Dokumentieren Sie, soweit jeweils vorhanden, die Quell- und Zieladressen und den Quell- und Zielport auf OSI Layer 2, OSI Layer 3 und auf OSI-Layer 4 und stellen Sie diese Werte gegenüber.

## 4.7 Adressumrechnung auf Router 2

### 4.7.1

Schalten Sie auf der Konfigurationsseite „WAN --- WAN IP“ NAT ein (Wert ist SUA[4] Only, entspricht NAPT).

Ermitteln Sie mittels tracert den Pfad vom lokalen PC zum WAN-PC und dokumentieren Sie diesen.

### 4.7.2

Starten Sie auf dem WAN-PC und dem lokalen PC jeweils einen Trace (Wireshark) und schicken Sie Ping vom lokalen PC auf den WAN-PC. Halten Sie den Trace an und werten Sie diesen aus. Das Auswerten je eines Ping-Paketes jeder Richtung ist ausreichend. Dokumentieren Sie die Quell- und Zieladressen auf OSI Layer 2 und auf OSI Layer 3 der Ping-Pakete auf beiden PC und stellen Sie diese Werte gegenüber.

### 4.7.3

Starten Sie auf dem WAN-PC einen Trace (Wireshark) und rufen Sie über den Browser SeaMonkey vom lokalen PC die Internetseite 10.10.10.10 auf. (Diese Adresse einfach dort eintragen, wo sonst die Adresse der Internetseite eingetragen wird). Diese Adresse wird natürlich nicht erreicht. Die Aufrufe laufen aber bis zum „Internet-PC“ und werden dort protokolliert. Etwa gleichzeitig dazu soll diese Adresse über den Browser im MX120 aufgerufen werden. Halten Sie dann den Trace an und werten Sie diesen aus. Das Auswerten je eines Aufruf-Paketes jeder Verkehrsbeziehung ist ausreichend. Dokumentieren Sie, soweit jeweils vorhanden, die Quell- und Zieladressen und den Quell- und Zielport auf OSI Layer 2, OSI Layer 3 und auf OSI-Layer 4 und stellen Sie diese Werte gegenüber.

### 4.7.4 Vergleich zum klassischen Routing

Stellen Sie die Werte aus 4.6.2 und 4.7.2 tabellarisch zusammen und vergleichen Sie diese. Erklären Sie Unterschiede zwischen den beiden Versuchen.

Stellen Sie die Werte aus 4.6.3 und 4.7.3 tabellarisch zusammen und vergleichen Sie diese. Erklären Sie Unterschiede zwischen den beiden Versuchen.

# 5 Literatur


– Skript zur Vorlesung LAN, Teil TCP/IP

– Kompakthandbuch zum Router ZYXEL Prestige 324


4 single user address