

Anhang A

Fehlertafeln

Bei der Fehlersuche helfen Ihnen oftmals Schemata (Tabelle A.1). Sie kommen dabei nicht in Versuchung, auf die Funktion von Netzwerkkomponenten zu vertrauen. Schritt für Schritt prüfen Sie, bis Sie den Fehler gefunden haben. Als Testgerät bei technischen Problemen verwenden Sie einen kleinen Mini-Switch. Bei LWL-Anlagen benutzen Sie einen mit Glasfaseranschluss. Bei funktionierender Netzverbindung leuchtet die Link-Anzeige des verbundenen Ports.

Fehler	Fehlertafel-Abbildung
Kupfernetz: Host ohne Verbindung	<u>Abbildung A.1</u>
LWL-Netz: Host ohne Verbindung	<u>Abbildung A.2</u>
DHCP: Host bekommt keine Adresse zugewiesen.	<u>Abbildung A.3</u>
1000Base-T: keine schnelle Verbindung möglich	<u>Abbildung A.4</u>

Tabelle A.1 Fehlertafeln

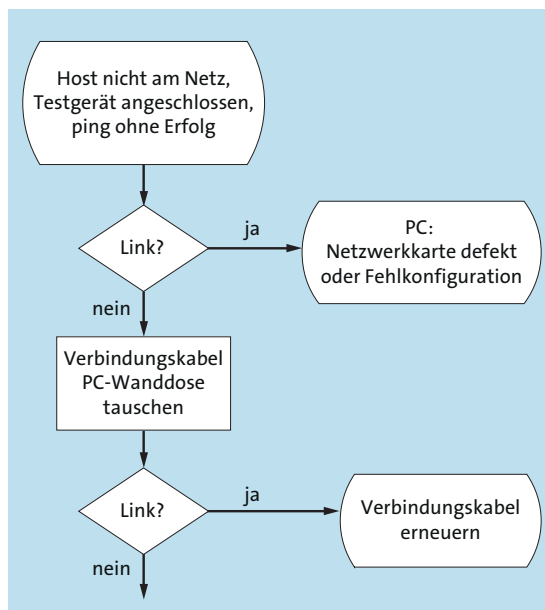


Abbildung A.1 Kupfernetz: Host ohne Verbindung

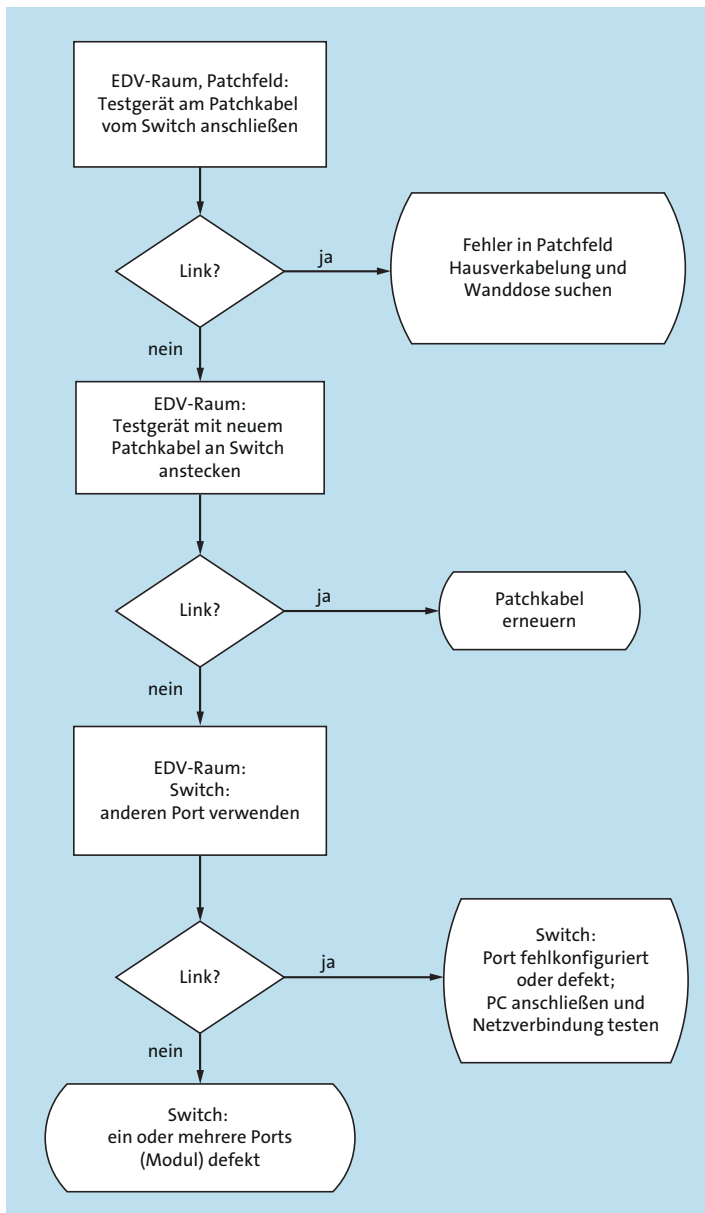


Abbildung A.1 Kupfernetz: Host ohne Verbindung (Forts.)

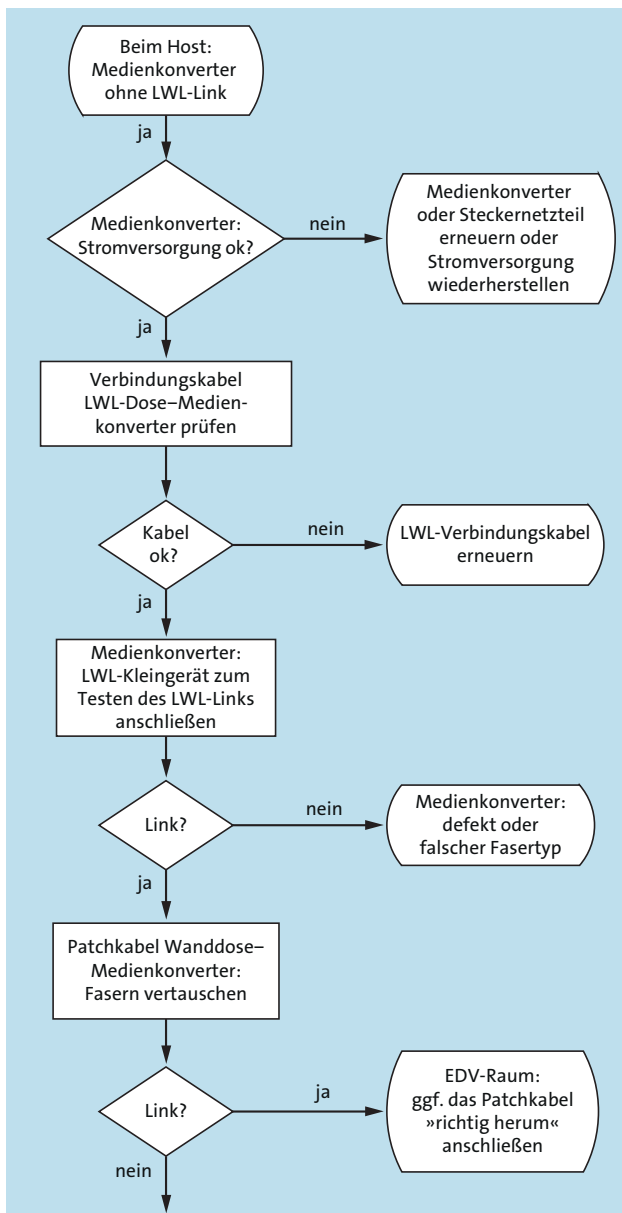


Abbildung A.2 LWL-Netz: Host ohne Verbindung

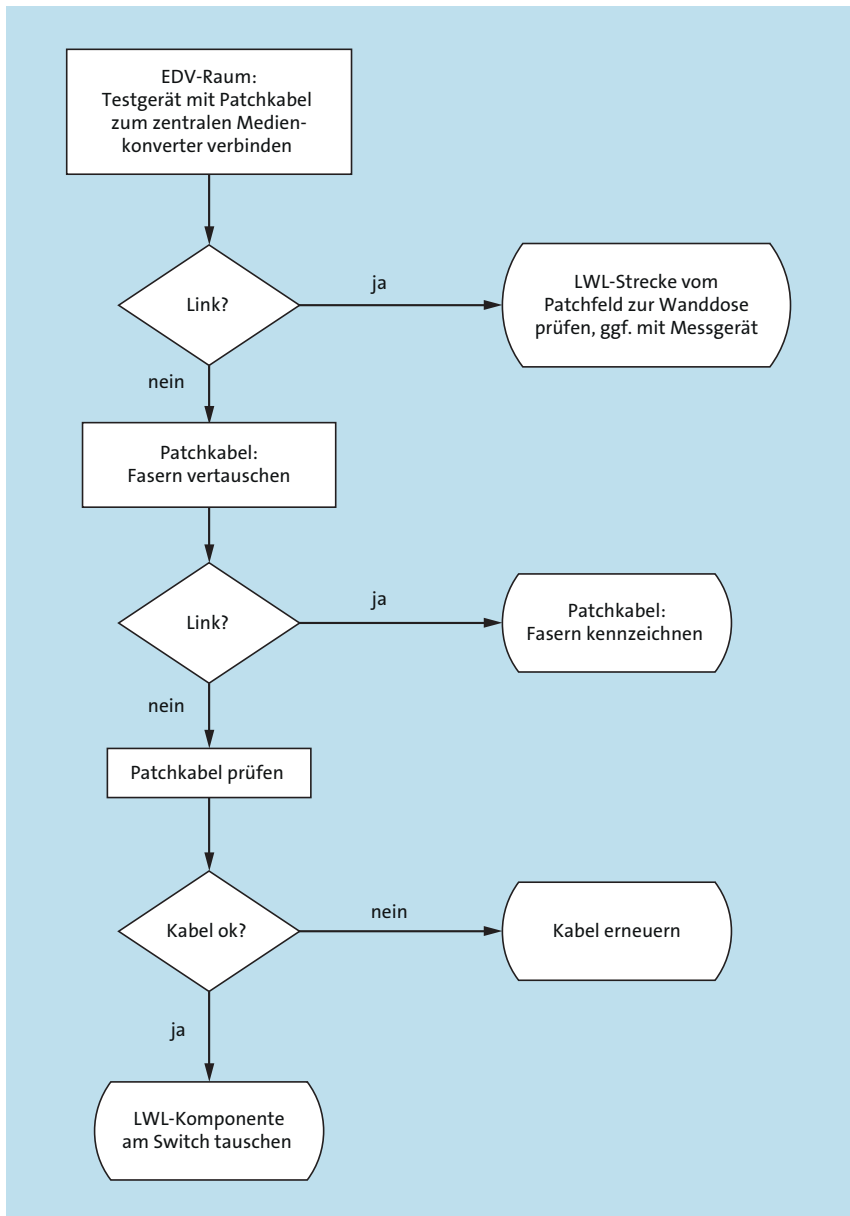


Abbildung A.2 LWL-Netz: Host ohne Verbindung (Forts.)

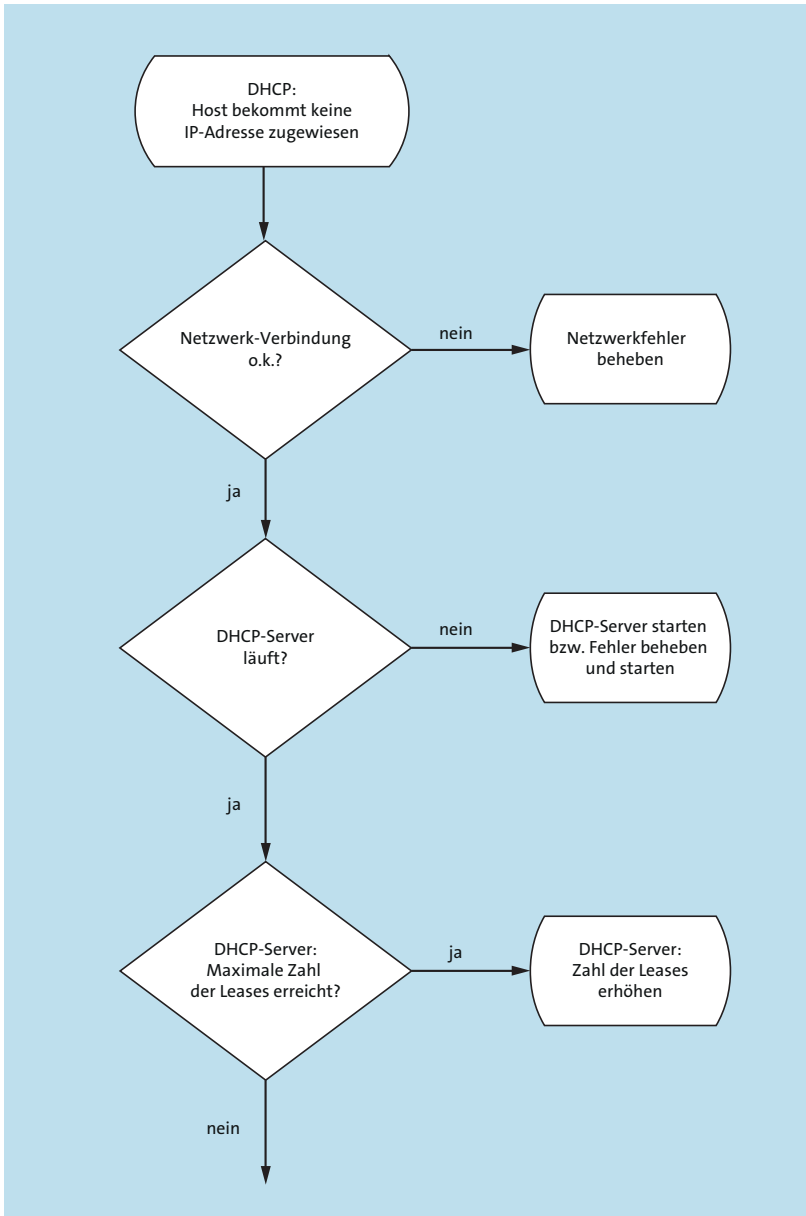


Abbildung A.3 DHCP: Host bekommt keine Adresse zugewiesen.

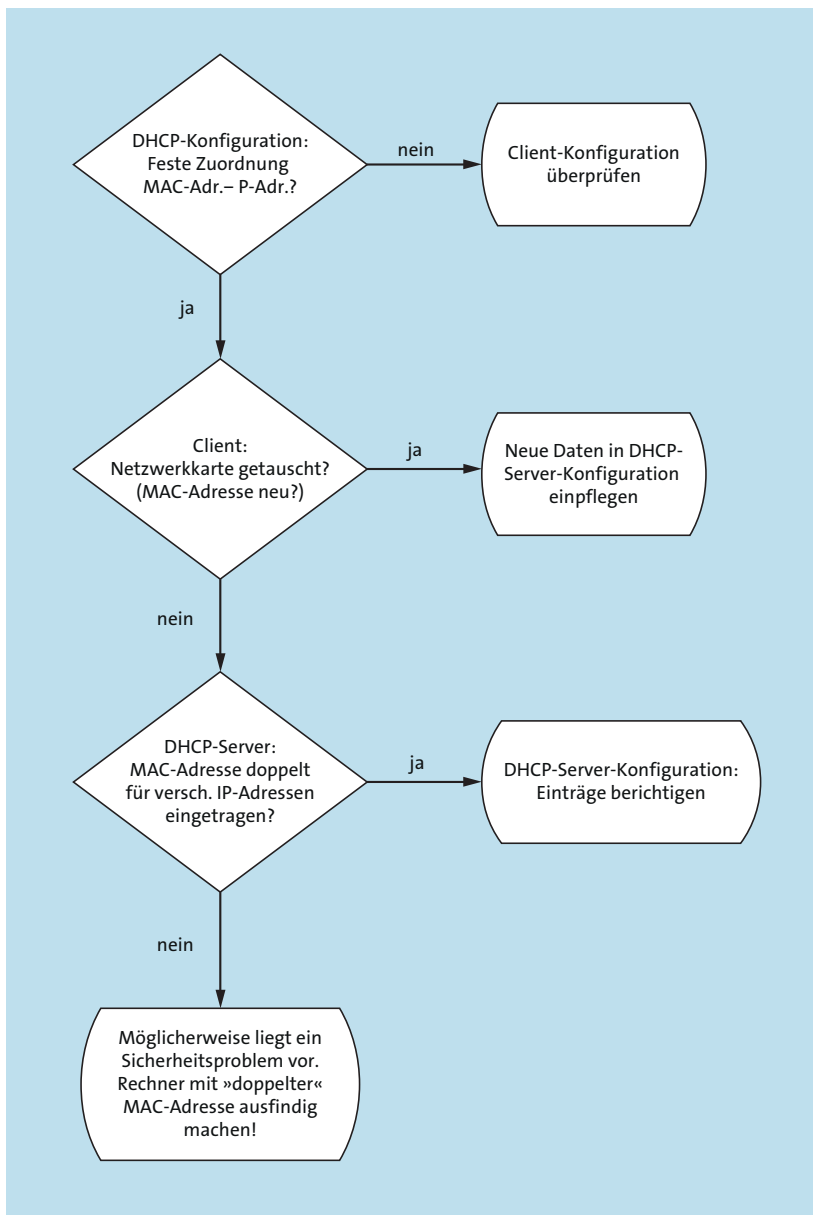


Abbildung A.3 DHCP: Host bekommt keine Adresse zugewiesen. (Forts.)

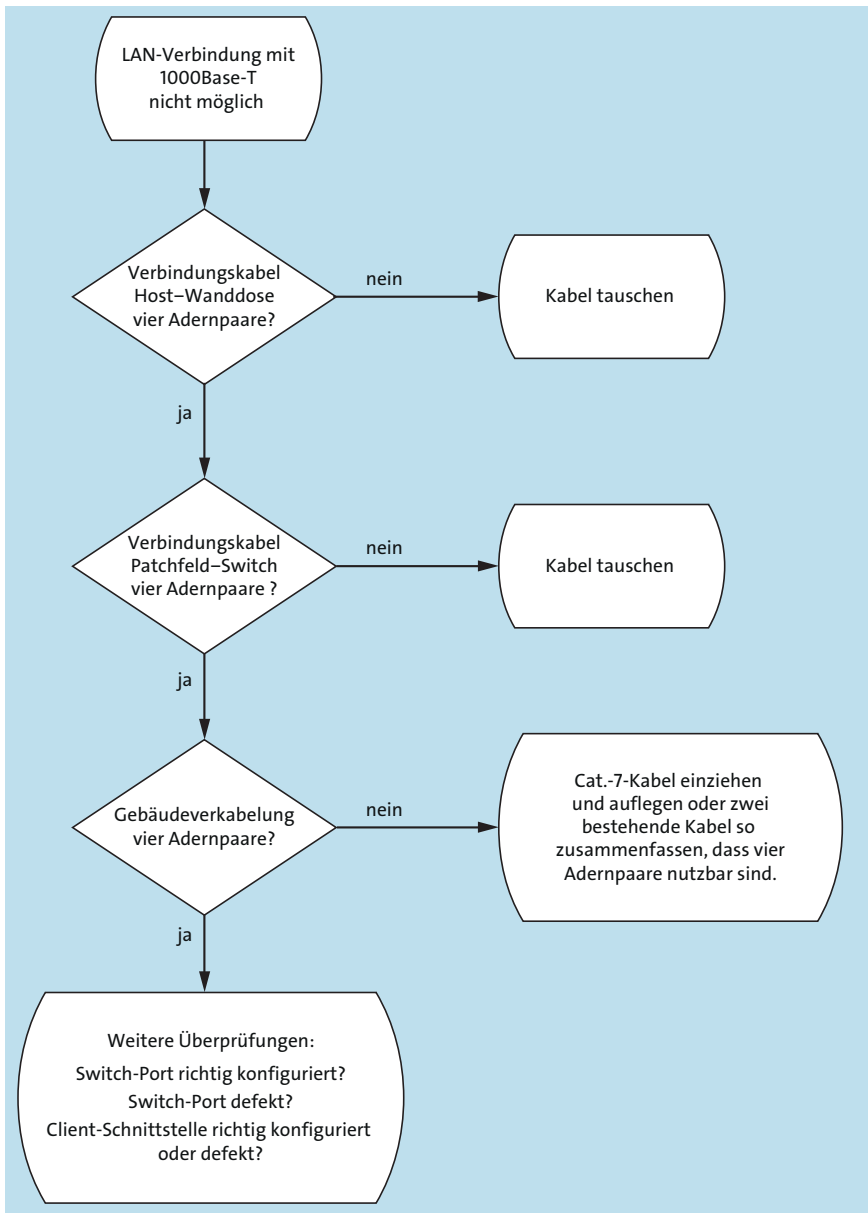


Abbildung A.4 1000Base-T: keine schnelle Verbindung möglich

Anhang B

Auflösungen zu den Prüfungsfragen

Fragen aus Kapitel 3, »Adressierung im Netzwerk – Theorie«

Abschnitt 3.8.1, »Berechnungen«

1. Maximale Hosts: 510
2. Netzwerkadresse: 192.168.4.0/23
3. 192.168.4.1 – 192.168.5.254

Abschnitt 3.8.2, »IP-Adressen«

Es handelt sich um eine Link-local Unicast-Adresse, die nicht in das Internet durchgeroutet wird.

Übungen aus Kapitel 4, »MAC- und IP-Adressen in der Praxis«

Abschnitt 4.9.1, »Glasfasern«

1. 9-µm-Monomode
2. Das Licht wird nicht mehr vom Übergang vom Kern zum Glasmantel reflektiert und tritt zum Primärcoating hin aus.
3. Vorteile:
 - Führung auch zusammen mit Stromkabeln möglich
 - größere Reichweite
 - hohe Investitionssicherheit, da bisher keine technischen Grenzen hinsichtlich der Übertragungsgeschwindigkeit erreicht wurden
 - relativ hohe Abhörsicherheit
 - keine störenden Beeinflussungen von außen möglich
4. Bei einem der SC-Duplex-Verbinder lösen Sie die Steckerklammer und stecken die nun einzelnen Stecker vertauscht am Medienkonverter wieder an. Vorher waren die LWL-Ausgänge TX mit TX und RX mit RX verbunden, nun jeweils »über Kreuz«.

Abschnitt 4.9.2, »TP-Verkabelung«

1. Kabelkategorie: nach Möglichkeit Cat. 7
2. Kabelkanäle: Nein. Kabelkanäle mit mehreren Kammern sind zulässig, wenn dabei die Stromkabel vom Netzwerkkabel getrennt geführt werden.
3. Längenüberschreitung: Selbst wenn die Signalspannung am anderen Ende der Verbindung ausreicht, werden die Signalfanken zu schwach. Der damit zu langsame Flankenanstieg macht die Informationen für die Endgeräte unlesbar. Sie können die Reichweite mit einem Repeater erhöhen (siehe Abschnitt 2.5, »Weitere Netzwerkkomponenten«).

Abschnitt 4.9.3, »Switches«

1. STP gegen Schleifen
2. Sie können hier sowohl normale Patchkabel als auch Crosskabel verwenden bzw. die Verkabelung sowohl nach EIA/TIA-568A als auch nach EIA/TIA-568B verwenden.
3. Vorteile von VLANs:
 - Eindämmung von Broadcasts und damit Verringerung der Netzlast
 - Abbildung betrieblicher oder organisatorischer Strukturen
 - Einteilung nach Anwendung (Daten/IP-Telefonie, Multimedia)

Abschnitt 4.9.4, »MAC- und IP-Adressen«

1. einen DHCP-Server
2. Leasetime: Gültigkeitsdauer der Adresszuweisung

Abschnitt 4.9.5, »Namensauflösung«

1. Die Namen unerwünschter Hosts werden in die *hosts*-Datei eingetragen und zeigen darin auf 127.0.0.1 bzw. ::1.
2. IPv6-Hosts: AAAA
3. Sie konfigurieren die Datei */etc/host.conf* wie folgt:

```
order hosts, bind
multi on
```

Abschnitt 4.9.6, »Routing«

1. Der Default-Router leitet alle Datenpakete an Hosts außerhalb des eigenen Netzes nach außen weiter.
2. Abbildung 4.40: Für die Netzwerkkarte *eth0* gilt 192.168.0.1 als Default-Gateway, die andere Route gilt dem Netz 192.168.0.0.

Die Netzwerkkarte *eth1* hat zusätzlich eine feste Route auf den Host *lp*, was man am Flag *H* erkennt.

3. Löschen der Route zu *lp*: `route del -host 192.168.0.54`

Abschnitt 4.9.7, »Sicherheit im lokalen Netz«

1. Nein, denn diese lässt sich leicht bei fast allen Betriebssystemen verändern.
2. Wenn Sie keinen ARP-Proxy in Ihrem Netzwerk einsetzen, liegt ARP-Spoofing vor. Es besteht die große Gefahr einer Man-in-the-Middle-Attacke. Sie müssen sämtlichen Netzwerkverkehr sofort unterbrechen.
3. Physikalische Sicherung: Entweder ziehen Sie das Kabel zwischen Patchfeld und Switch im Rechnerraum ab und/oder deaktivieren den entsprechenden Port am Switch.
4. Sicherheit erhöhen: siehe Abschnitt 3.6.6, »Kryptografisch erzeugte Adressen (CGA)«
5. Ausfall DNS: Ergänzen Sie die *hosts*-Datei um die Ihnen wichtigen Hosts und deren IP-Adressen.

Fragen aus Kapitel 6, »Datentransport mit TCP und UDP«

Abschnitt 6.8.1, »TCP-Protokoll«

1. Mit dem Flag zum Abweisen von Verbindungswünschen: RST
2. Sequenznummern dienen der richtigen Reihung der Datenpakete am Ziel und deren Kontrolle hinsichtlich ihrer Vollständigkeit.

Abschnitt 6.8.2, »Ports und Sockets«

1. Webserver mit abweichender Port-Nummer: *http://192.168.7.100:8182*
2. Sockets: nur TCP
3. Programmausgabe Portscan: Auf dem Rechner netzbuch läuft ein Webserver, der über den Port 80 Anfragen entgegennimmt. Er benutzt hierfür TCP.
4. Portscanner: Mit einem TCP-SYN-Scan sendet der Portscanner ein Paket mit SYN-Flag zur vermeintlichen Verbindungsaufnahme.
5. Keine Antwort: Ein Paketfilter lässt weder Anfrage noch Antwort passieren.
SYN/ACK-Flag-Paket: Der Port ist offen.
RST-Flag-Paket: Der Port ist geschlossen.

Abschnitt 6.8.3, »Firewall«

Allgemeines Sicherheitsproblem: Gewöhnliche Firewalls überprüfen nicht, ob freigegebene Ports auch gemäß ihrer Bestimmung genutzt werden. Hier können Sicherheitsregeln umgangen werden.