Fachschule für Technik

Schriftliche Abschlussprüfung

Fachrichtung Elektrotechnik
Walther-Rathenau-Gewerbeschule Freiburg

Fach:ITV		**Abschlussprüfung:**	**2016**
		Fachlehrer:	**Dienert**
Prüfungsdauer: 150 Min.		**Klasse:**	**FTI4T**
Hilfsmittel:	**4 A4-Seiten mit beliebigem Inhalt, Schriftgrösse nicht kleiner als 10pt. Schülerrechner mit Linux im Klassenarbeitsmodus.**		

Netzwerk

Abb. 2 zeigt eine Übersicht über das Netzwerk eines Instituts, das Strahlungsmesssonden betreibt. Eine Messsonde besteht aus einem Sensor (γ-Zählrohr), der an einen Messrechner angeschlossen ist. Der Messrechner wiederum ist über eine Fritzbox von AVM (Router AVM7490) mit dem Internet verbunden.

Der Internetzugang der Institutsräume erfolgt über einen Router mit Paketfilterung (Router *FW*).

Die Rechner im Institutsnetzwerk verwenden für die Internetadressierung das Dual-Stack-Verfahren, d.h. jeder Host hat eine IPv4- und eine IPv6-Adresse.

Auf dem Nameserver *NS* ist der *isc-dhcp-server* installiert, der die IPv4-Adressen aus dem Subnetz 10.20.30.0/24 an die 16 Laborrechner verteilt. Der Drucker, der Nameserver *NS* und der Router **NATTER** erhalten feste, manuell vergebene Adressen (siehe Bild 2).

Die Vergabe des IPv6-Routing-Prefixes erledigt der Dienst *radvd*, der ebenfalls auf *Natter* läuft. Er verteilt den Präfix:

```
2001:baff:caff::/64
```

Das Institut betreibt einen Webserver (*httpd*), von dem man die Messdaten der Sonden weltweit abrufen kann. Der Webserver hat die öffentliche Adresse

```
77.87.230.42/29
```

Die Switchports, an die der Webserver *httpd* und der Zugangsrouter *FW* angeschlossen sind, gehören zum VLAN10 auf dem Core-Switch.

Der Router *NATTER* ist an einem Tagged-Port (auch als Trunk-Port bezeichnet) nach der Spezifikation IEEE 802.1Q angeschlossen. Das Netzwerk-Interface des Routers *NATTER* arbeitet ebenfalls nach IEEE 802.1Q.

Der Uplink-Port zum Laborswitch befindet sich nur im VLAN46.

1 Aufgabe

Die Adresse 77.87.230.42 gehört dem Bund. Eine Anfrage an die RIPE - Datenbank liefert folgende Antwort:

```
inetnum:        77.87.224.0 - 77.87.231.255
netname:        BSI-IVBB
descr:          Bundesamt fuer Sicherheit in der Informationstechnik
country:        DE
```

1. RIPE gibt das Netz als Adressbereich (*inetnum*) aus. Geben Sie den Bereich in der Form *Netzadresse/Präfixlänge* an. 6 P

2. Wieviele Adressen hat dieses Netz und wieviele Hostrechner kann es maximal enthalten? 4 P

3. Teilen Sie das Netz in 16 gleich grosse Subnetze auf. Geben Sie die Präfixlänge und die Netzmaske dieser Subnetze an. Wie lautet die Netzadresse des letzten Teilnetzes? 8 P

2 Aufgabe

1. Im VLAN10 wird ein IPv4-Netz mit öffentlichen Adressen verwendet. Die Adresse des Webservers ist 77.87.230.42/29. Versehen Sie die Interfaces der Hosts *FW*, *httpd* und *NATTER* mit Adressen aus diesem Netz. Geben Sie jede Adresse in der CIDR-Schreibweise (Netzadresse/Präfixlänge) an. Der Internet-Router muss die höchste, mögliche Adresse im Subnetz haben, der Router NATTER die kleinste. Das Interface eth1.10 von NATTER ist dem VLAN10 zugeordnet. Verwenden Sie untenstehende Tabelle (Tab. 1). Tragen Sie auch die Netz- und Broadcastadressen ein. 8 P

2. Auf dem Host *NATTER* wurde der Datenverkehr an der Schnittstelle eth1.10 mitgeschnitten. Die ersten 18 Bytes eines Frames sehen so aus:

   ```
   c860 00c7 0b1f 90e2 ba21 cc8c 8100 000a 0800
   ```

   Erklären Sie die Bedeutung der einzelnen Felder dieses Ethernet-Frames. Beschreiben Sie, worin sich dieser Frame-Header von einem EthernetII-Frame-Header unterscheidet. 4 P

3. Wie sieht der Header des Ethernet-Frames dieser Nachricht aus, wenn er an *eth0* des Hosts *httpd* eintrifft? Verwenden Sie Tabelle 2 für die Lösung. 4 P

Name, Vorname:		
Hostname	Interface	Adresse/Präfix
Netzadresse	-	
FW		
httpd		
NATTER		
BC-Adresse	-	

Tabelle 1: Servernetz

Name, Vorname:

Tabelle 2: Ethernet-Frame-Header

3 Aufgabe

1. Auf dem Host *NS* läuft unter anderem ein Dienst, der automatisch IPv4-Adressen an die am Laborswitch angeschlossenen Rechner vergibt (dhcp - dynamic host configuration protocol). Beschreiben Sie den Ablauf der Adressvergabe an einen neu eingschalteten Client-Host.

   Der Host hat nach Ablauf der Adressvergabe die IPv4-Adresse **10.20.30.101**.

   Geben Sie dabei die Layer2- (MAC-) und Layer3 (IP-) Adressen in den hin- und hergehenden dhcp-Nachrichten an. Die Layer4 (Port-)-Adressen müssen nicht angegeben werden. 8 P
   Vorgaben:

Layer3-Adresse des Servers NS:	**10.20.30.10**
Layer3-Adresse die der Client erhält:	**10.20.30.101**
Layer2-Adresse des Netzwerkinterfaces des Servers NS:	**4c:5e:0c:b1:74:73**
Layer2-Adresse des Netzwerkinterfaces des Client-Hosts:	**90:e2:ba:21:cc:8c**

2. Die IP-Adressen des Druckers, des Nameservers NS und des Routers NATTER sind manuell konfiguriert. Der Router hat die höchste, mögliche Adresse im Subnetz 10.20.30.0/24.
   Welche Informationen ausser der IP-Adresse muss der dhcp-Server an die Clients noch verteilen, damit die Laborrechner Zugang zum Internet herhalten?
   Geben Sie Art und konkrete Werte dieser Informationen an. 6 P

4 Aufgabe

1. Welche beiden IPv4-Einträge stehen nach dem Abschluss der dhcp-Adressvergabe in den Routingtabellen der Laborrechner? Die Laborrechner haben alle nur ein Netzwerkinterface mit dem Namen *eth0*. Tragen Sie die Lösung in Tabelle 3 ein. 4 P

2. Geben Sie die komplette IPv4-Routingtabelle des Routers NATTER an. Verwenden Sie die Tabelle 4. Es sind evtl. mehr Zeilen vorhanden, als Sie benötigen werden. 6 P

3. Die Adressen im Labornetz gehören zum Klasse-A-Netz 10.0.0.0/8. Welches sind die Besonderheiten dieses Netzes? Beschreiben Sie ein Verfahren, mit dem es möglich wird, mit Adressen aus dem Netz 10.0.0.0/8 bei Hosts im Internet anzufragen (zu “surfen”). 4 P

4. Um dieses Verfahren einzuschalten, sollen auf NATTER zwei iptables-Kommandos abgesetzt werden. Ergänzen Sie die beiden Kommandos in der Abbildung 1 handschriftlich um die richtigen Netzwerkschnittstellen. 6 P

Name, Vorname:		
Zielnetz/Präfix	Next-Hop	Exit-Interface

Tabelle 3: Routingtabelle Laborrechner

Name, Vorname:		
Zielnetz/Präfix	Next-Hop	Exit-Interface

Tabelle 4: Routingtabelle NATTER

Name, Vorname:

```
iptables -A FORWARD -o _______ -i _______ -s 10.20.30.0/24 \
-m conntrack --ctstate NEW -j ACCEPT



iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED \
-j ACCEPT iptables -t nat -A POSTROUTING -o _______ -j MASQUERADE
```

Abbildung 1: iptables

5 Aufgabe

1. Der vom Router verteilte Präfix ist `2001:baff:caff::/64`. Geben sie die **ersten 64 bit** des Präfixes **hexadezimal** inklusive aller Nullen an (Tabelle 5). 4 P

Name, Vorname:

Tabelle 5: 64-bit IPv6 Präfix

2. Die Laborrechner arbeiten im Dual-Stack-Betrieb, d.h. sie haben eine IPv4- und eine IPv6-Adresse. Geben Sie die IPv6-Adressen des Hosts mit der MAC-Adresse **90:e2:ba:21:cc:8c** an. Verwenden Sie die Tabelle 6. Es sind evtl. mehr Zeilen vorhanden, als Sie benötigen werden. 8 P

Name, Vorname:
IPv6/Präfixlänge

Tabelle 6: IPv6-Adressierung

6 Aufgabe

Der Router **FW** soll das Netzwerk gegen Angriffe aus dem Internet absichern. Dazu sollen Firewallregeln aufgestellt werden, die nur den Zugriff auf den Webserver- und den ssh-Dienst auf der Maschine mit der IPv4 77.87.230.42/29 erlauben. Alle weiteren Zugriffe auf alle Adressen aus dem Netz 77.87.239.40/29 sollen verboten werden.

Die Firewall arbeitet nach dem *Stateful Inspection* - Prinzip. Es sind bereits Regeln eingerichtet, die die *established* und *related*-Pakete durchlassen.

Die Firewallregeln werden mit dem Kommando `add` der Filterkette hinzugefügt.

`add` hat folgende mögliche Bedingungen:

```
action = accept | drop
chain = input | forward | output
dst-address = <ipv4>/[<praefix-laenge>]
dst-port = <portadresse>
protocol = tcp | udp
src-address = <ipv4>/[<praefix-laenge>]
src-port = <portadresse>
```

1. Welche tcp-Ports gehören zu den Diensten http und ssh ? 8 P
2. Geben Sie die Kommandos an, mit der die oben geforderten Firwallregeln eingetragen werden. 12 P

7 Anbindung der Messrechner

Der Messrechner ist über einen DSL-Router und Source-NAT ständig ans Internet angeschlossen.

Die Messdaten werden mit *ssh* auf den Webserver übertragen. Auch wird der Messrechner hierüber gewartet.

Leider findet das Institut immer schwieriger Mitarbeiter, die noch einen Kommandozeileninterpreter (eine sog. *Shell*) bedienen können und Sie als Administrator sollen die Wartung der Messrechner über Programme mit grafischer Benutzerschnittstelle ermöglichen.

Beschreiben Sie die sog. VPN-Technologie die es ermöglicht, den Messrechner in das Netzwerk 10.20.30.0/24 einzubinden, ohne dass zusätzliche Hardware angeschafft werden muss. Denken Sie dabei auch an evtl. notwendige, zusätzliche Firewall-Regeln.

Der Aufbau der Verbindung *messrechner-Labornetz* soll vom Messrechner aus gestartet werden. 12 P

8 IPv6 Namensauflösung

Im Labornetz soll testweise IPv6 verwendet werden. Der Rechner `labor-16.testnetz.de` hat die globale unicast IPv6-Adresse

```
2001:baff:caff::ca60:ff:fec7:b1f/64
```

Das Kommando

```
dig -x 2001:baff:caff::ca60:ff:fec7:b1f
```

liefert folgendes Ergebnis (unwichtige Zeilen der Ausgabe wurden weggelassen):

```
;; QUESTION SECTION:
;f.1.b.0.7.c.e.f.f.f.0.0.0.6.a.c.0.0.0.0.f.f.a.c.f.f.a.b.1.0.0.2.ip6.arpa. IN PTR
```

1. Was bewirkt der Schalter **-x**4 des dig-Kommandos? Welche Datensätze werden angefragt? 4 P

2. Obige Anfrage liefert noch keine “ANSWER”-Section. Welcher Eintrag muss in der Zonendatei für die Rückwärtsauflösung stehen, damit die Anfrage auch eine Antwort liefert. 4 P

3. Die weiteren Rechner des Testnetzes sollen auch in die Zonendateien aufgenommen werden. Der Administrator hat dazu folgenden Eintrag vorgenommen:

   ```
   $ORIGIN 0.0.0.0.f.f.a.c.f.f.a.b.1.0.0.2.ip6.arpa.
   ```

   Erklären Sie die Funktionsweise von `$ORIGIN`. Wie würde sich der Eintrag in die Zonendatei ändern, wenn `$ORIGIN` den angegebenen Wert hat? 8 P

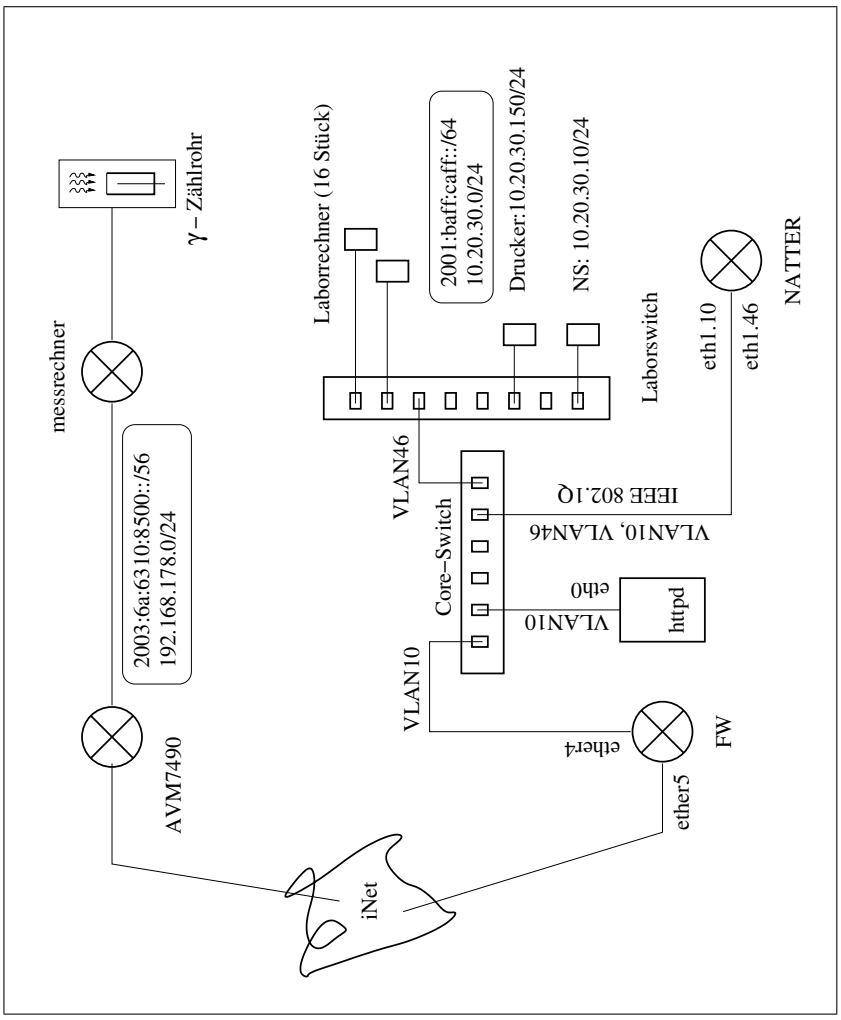

Abbildung 2: Netzwerktopologie

9 Lösungen

1 Aufgabe

1.1

Es sind insgesamt $8 \cdot 256 = 2048$ Adressen, man benötigt also eine Präfixlänge von $31 - 11 = 21$ bit. Bereich in CIDR: ***77.87.224.0/21***

1.2

insgesamt ***2048*** Adressen, bleiben ***2046*** für Hostrechner.

1.3

$2048/16 = 128 \Rightarrow$ Präfixlänge ist $32 - 7 = 25$ bit. Maske: ***255.255.255.128***, letztes Teilnetz: ***77.87.231.128/25***

2 Aufgabe

2.1

Hostname	Interface	Adresse/Präfix
Netzadresse	-	77.87.230.40/29
FW	ether4	77.87.230.46/29
httpd	eth0	77.87.230.42/29
NATTER	eth1.10	77.87.230.41/29
BC-Adresse	-	77.87.230.47/29

Tabelle 7: Lösung Servernetz

2.2

c860 00c7 0b1f Layer2-Zieladresse

90e2 ba21 cc8c Layer2-Quelladresse

8100 (tag protocol identifier). Fester Wert, der den Frame für nicht 802.1q-fähige Geräte ungülig macht.

000a Flags (hier alle Null) und 12bit VLAN-ID, hier $0a_{hex} = 10_{dez}$

0800 Ethertype, hier 0800_{hex} für IPv4

2.3

Das VLAN-Tag (16bit) wird komplett entfernt:

```
c860 00c7 0b1f 90e2 ba21 cc8c 0800
```

3 Aufgabe

3.1

dhcp-Adressvergabe in 4 Schritten:

DHCPDISCOVER Quell-IP=0.0.0.0, Ziel-IP=255.255.255.255, Quell-MAC=90:e2:ba:21:cc:8c, Ziel-MAC=ff:ff:ff:ff:ff:ff

DHCPOFFER Quell-IP=10.20.30.10, Ziel-IP=10.20.30.101, Quell-MAC=4c:5e:0c:b1:74:73, Ziel-MAC=90:e2:ba:21:cc:8c

DHCPREQUEST Quell-IP=10.20.30.101, Ziel-IP=10.20.30.10, Quell-MAC=90:e2:ba:21:cc:8c, Ziel-MAC=4c:5e:0c:b1:74:73

DHCPACK Quell-IP=10.20.30.10, Ziel-IP=10.20.30.101, Quell-MAC=4c:5e:0c:b1:74:73, Ziel-MAC=90:e2:ba:21:cc:8c

3.2

Die Clients benötigen für den Internetzugang ausser einer eigenen Adresse noch die Adresse des DNS-Servers **10.20.30.10/24** und des Gateways **10.20.30.254/24**

4 Aufgabe

4.1

Zielnetz/Präfix	Next-Hop	Exit-Interface
10.20.30.0/24	*	eth0
0.0.0.0/0	10.20.30.254	eth0

Tabelle 8: Lösung Routingtabelle Laborrechner

4.2

Zielnetz/Präfix	Next-Hop	Exit-Interface
10.20.30.0/24	*	eth1.46
77.87.230.40/29	*	eth1.10
0.0.0.0/0	77.87.230.46/29	eth1.10

Tabelle 9: Lösung Routingtabelle NATTER

4.3

10.0.0.0/8 ist ein privates Class-A-Netz, dessen Adressen nicht geroutet werden.

Mit Hilfe von Source-NAT / PAT können die Rechner hinter dem Router *Natter* jedoch Anfragen ins Internet schicken. Der Router Natter tauscht dabei die Quelladresse eines Clients gegen seine eigene Adresse aus und kennzeichnet die Anfragen (tcp oder udp) mit jeweils einer eigenen Portadresse. So können die Antworten der Server im Internet vom Router wieder den richtigen Clients zugeordnet werden.

4.4

```
iptables -A FORWARD -o eth1.10 -i eth1.46 -s 10.20.30.0/24 \
-m conntrack --ctstate NEW -j ACCEPT

iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED \
-j ACCEPT iptables -t nat -A POSTROUTING -o eth1.10 -j MASQUERADE
```

5 Aufgabe

5.1

2001:baff:caff:0000

Tabelle 10: Lösung 64-bit IPv6 Präfix

5.2

IPv6/Präfixlänge
fe80::92e2:baff:fe21:cc8c/64
2001:baff:caff::92e2:baff:fe21:cc8c/64
alternativ: 2001:baff:caff:0000:92e2:baff:fe21:cc8c/64

Tabelle 11: Lösung IPv6-Adressierung

6 Aufgabe

6.1

http: Port **80**
ssh: Port **22**

6.2

add chain=forward dst-address=77.87.230.42 dst-port=22 protocol=tcp action=accept
add chain=forward dst-address=77.87.230.42 dst-port=80 protocol=tcp action=accept
add chain=forward dst-address=77.87.230.40/29 dst-port=22 action=drop

Die Regel mit *action=drop* **muss** als letzte in der Kette stehen. Die Reihenfolge der Optionen innerhalb eines **add**-Kommandos ist beliebig.

7 Aufgabe

7.1

Durch die Verwendung eines sog. *Tunnels* oder *VPN* können die Messrechner direkt ins Labornetzwerk eingebunden werden. Das könnte z.b. mit *openvpn* erfolgen.

Bei einem Tunnel werden IP-Pakete (oder Layer2-Frames; im Unterricht nicht behandelt) als Nutzlast eines UDP-Segments nochmals in ein IP-Paket verpackt.

Wird als inneres Protokoll *IP* verwendet, hat der Tunnel an den Enden die Adresse 10.8.0.1 bzw. 10.8.0.2 (default-Adressen von openvpn). An den Endpunkten des Tunnels wird dann jeweils ins eigene Netz geroutet.

Wird als inneres Protokoll *Ethernet* verwendet, könnte der Client über sein Tunnelinterface eine Adresse vom dhcp-Server des Labornetzes beziehen (im Unterricht nicht behandelt).

Der *openvpn*-Server muss im Labornetz stehen, damit vom Messrechner aus der Tunnel aufgebaut werden kann. Dazu muss auf der Firewall eine Port-Weiterleitung zum *openvpn*-Server eingerichtet werden.

Auf dem *messrechner* läuft der *openvpn*-Client, der über den Router NATTER eine Verbindung zum Server aufbaut. *openvpn* verwendet standardmässig den udp-port 1194.

8 Aufgabe

8.1

Der Schalter **-x** erzeugt aus der IP-Adresse einen FQDN (full qualified domain name). Bei IPv6 liegen diese Namen in der Domäne `ip6.arpa.` .

Bei IPv6 wird dabei jede Hexadezimalziffer der IPv6-Adresse in ein DNS-Label umgewandelt, einschliesslich aller Nullen.

Die Labels sind wie die rückwärts gelesene IPv6-Adresse angeordnet.

Wird dig mit **-x** aufgerufen, werden PTR-Records angefragt.

8.2

Zeile in der Zonendatei; wichtig sind die Punkte am Ende des Namens (root-domain) und am Ende des FQDN in **ip6.arpa.** .

```
f.1.b.0.7.c.e.f.f.f.0.0.0.6.a.c.0.0.0.0.f.f.a.c.f.f.a.b.1.0.0.2.ip6.arpa. IN PTR labor-16.testnetz.de.
```

8.3

Ist die Variable `$ORIGIN` gesetzt werden alle Einträge, die nicht mit einem Punkt enden, um den Inhalt von `$ORIGIN` ergänzt.

Neuer Eintrag (hier kein Punkt nach ...0.6.a.c):

```
f.1.b.0.7.c.e.f.f.f.0.0.0.6.a.c IN PTR labor-16.testnetz.de.
```