

1.12 Praktische Aufgaben

1.12.1 Der Versuchsaufbau

Abbildung 15 zeigt das Netz, welches nach Abschluß der Übungen dieses Kapitels entstehen soll.

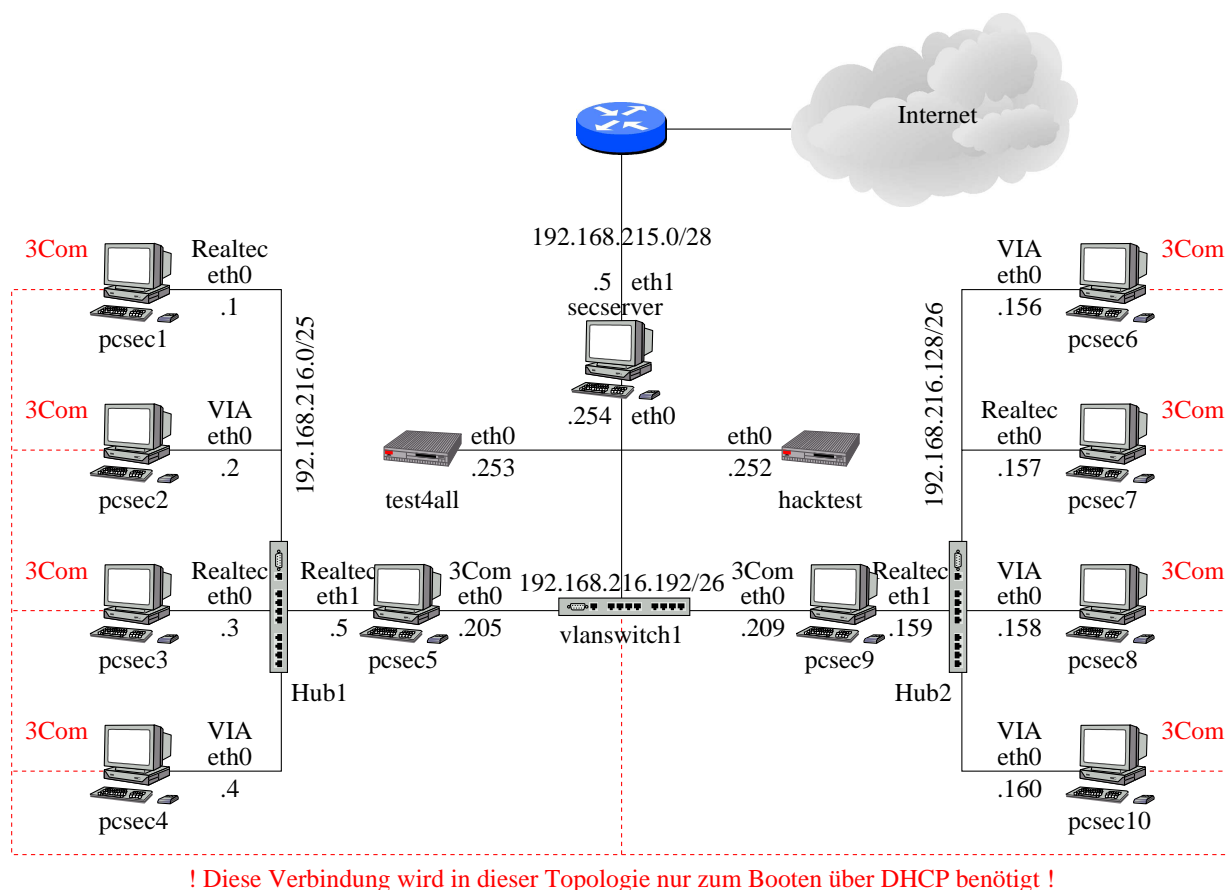


Abbildung 15: Der Versuchsaufbau

Der Rechner `test4a11` kann für Tests der Konfigurationen verwendet werden (Benutzer `secpgast`, Passwort `pcsec`).

Sobald der Netzzugang zum `secserver` funktioniert haben Sie über NFS⁹ Zugriff auf die SuSE 8.0 CDs unter `/opt/SuSE8.0-CDs`. Im YaST tragen Sie zur Installation neuer Software die IP-Adresse des `secserver` sowie den Pfad `/opt/SuSE8.0-CDs/CD1` als Installationsquelle ein.

⁹Network File System zum Einhängen von entfernten Dateisystemen am lokalen Rechner über das Netzwerk.

Des Weiteren können Sie den `secserver` als Internet-Proxy verwenden. Tragen Sie dazu die IP-Adresse der `secserver` und den Port 3128 in Ihrem Browser als HTTP/HTTPS/FTP-Proxy ein.

1.12.2 IP-Adressen und Netzmasken

Bestimmen Sie für die Netze des Versuchsaufbaues aus Abbildung 15 die in den Netzen verwendbaren IP-Adressen und die Broadcast-Adresse.

Welche kleinst mögliche Netzadress/Netzmasken-Kombination beinhaltet alle IP-Adressen der drei internen Netze?

1.12.3 Konfiguration der Netzwerkkarten

1. Lassen Sie sich die ARP- (`man arp`, vgl. Abbildung 4) und die Routing-Tabelle (`man netstat`, vgl. Abbildung 7) sowie die Liste aller konfigurierten Interfaces (`man ifconfig`) Ihres Rechners anzeigen.
2. Nennen Sie ein Beispiel für die praktische Verwendung des Loopback-Interfaces.
3. Konfigurieren Sie nun die Netzwerkkarte(n) Ihres Rechners. Die Rechner sind mit zwei bzw. drei unterschiedlichen Karten ausgerüstet. Welche der Karten Sie wie konfigurieren müssen entnehmen Sie bitte der Abbildung 15. Die dort nicht aufgeführten Karten werden in dieser Topologie nicht benötigt. Die rot eingezeichnete Verbindung dient nur zum Booten und ist für die Versuche nicht weiter von Bedeutung. Versuchen Sie, andere Rechner im Netz zu erreichen. Welche Rechner antworten, welche nicht? Welche Meldung erhalten Sie, wenn sie versuchen, einen Rechner außerhalb Ihres Subnetzes zu erreichen?
4. Wie haben sich ARP- und Routing-Tabelle verändert?

1.12.4 Konfiguration der statischen Routen

1. Konfigurieren Sie nun die statischen Routen (mit `YaST`) des Rechners so, daß sie alle Rechner im Netz erreichen können. Arbeiten Sie dabei nicht mit Host-Routen für die einzelnen Rechner sondern mit Netzrouten für die Netze aus Abbildung 15 und verwenden Sie keine Default-Route. Lassen sich Routen zusammenfassen?
2. Auf den Rechnern, die als Router arbeiten sollen, muß auch das Routing aktiviert werden¹⁰ (`YaST`).

¹⁰Einige Firewall-Produkte erledigen das Routing unabhängig vom Betriebssystem. Das Routing des Betriebssystems darf in so einem Fall nicht aktiv sein um auszuschließen, daß bei nicht laufender Firewall-Software Pakete ungefiltert weitergeleitet werden.

3. Überprüfen Sie nochmal ARP- und Routingtabelle. Welche Änderungen stellen Sie fest?

1.12.5 Überwachung des Netzwerkverkehrs

Für die folgenden Versuche müssen auf Ihren Rechnern noch der FTP- und Telnet-Server-Prozess installiert werden. Installieren Sie dazu mit YaST die Pakete `ftpd` und `telnet-server` und aktivieren Sie die beiden Dienste ggf. in der Datei `/etc/inetd.conf`.

1. Starten Sie nun in einem weiteren Terminal-Fenster das Programm `tcpdump` oder `ngrep`. Sinnvolle Optionen entnehmen Sie bitte den Man-Pages.
2. Loggen Sie sich mit `ftp` auf einem benachbarten Rechner ein und laden Sie einige der dort gespeicherten Dateien herunter (User: `secpgast` Passwort: `pcsec`). Achten Sie dabei darauf, sich keine lokalen Dateien zu überschreiben. Was sehen Sie mit `tcpdump/ngrep` bei aktiver und nicht aktiver `ftp`-Verbindung? Versuchen Sie, das `ftp`-Passwort aufzuzeichnen.
3. Was können Sie daraus bzgl. der Schicht 2-Infrastruktur in Ihrem Netzsegment schließen?
4. Zeichnen Sie den TCP-Verbindungsauf- und -abbau zu einem beliebigen über IP erreichbaren Rechner im Netz (`<Ziel-IP>` auf und kennzeichnen Sie die mitgeschnittenen Pakete als zugehörig zu
 - Verbindungsaufbau
 - Datenübertragung
 - Verbindungsabbau.

Starten Sie dazu in einem Terminal-Fenster zuerst das Kommando

```
tcpdump -n host <Ziel-IP>
```

Über folgende Kommandos (Beispiel in Abbildung 16) können Sie nun in einem weiteren Terminal-Fenster eine TCP-Verbindung (`telnet`, Port 23) zur (`<Ziel-IP>`) sauber auf- und wieder abbauen.

```
telnet <Ziel-IP>
Control-5 oder Control-AltGr-9
quit
```

`tcpdump` können Sie mit `Control-C` abbrechen.

```
linux:~# telnet 10.11.12.13
Trying 10.11.12.13...
Connected to linuxserver.
Escape character is '^]'.
Welcome to SuSE Linux 7.0 (i386) - Kernel 2.2.16 (0).

linuxserver login:
telnet> quit
Connection closed.
linux:~#
```

Abbildung 16: TCP-Verbindungsauf- und Abbau