



TI III: Operating and Communication Systems



WS 2007/08 Übungsblatt Nr. 7

Georg Wittenburg, M.Sc., AG Technische Informatik, Freie Universität Berlin

Ausgabe am 25.1.2008 — Abgabe spätestens 8.2.2008, 10:00 Uhr

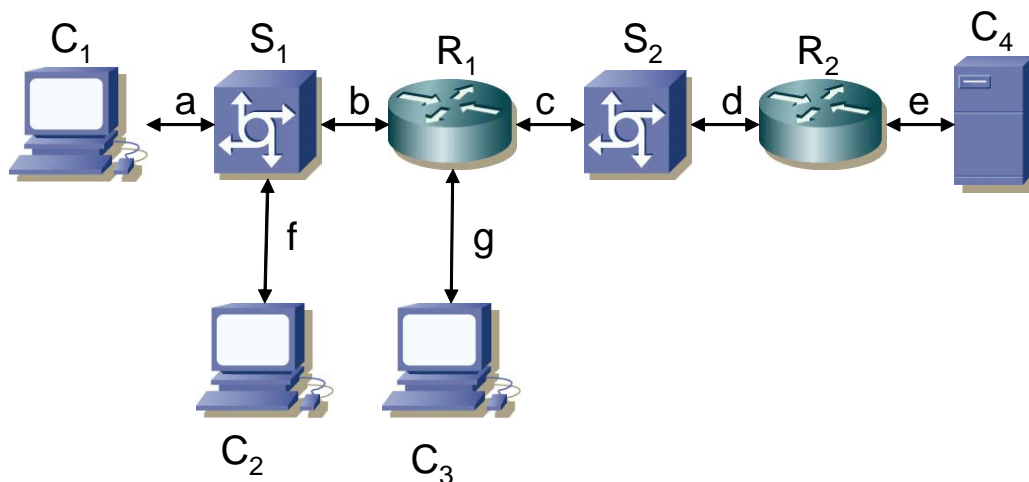
Bitte bei der Abgabe beide Namen/Matr.Nr. der Mitglieder einer Gruppe, NUMMER DER ÜBUNG/TEILAUFGABE und DATUM auf den Lösungsblättern **nicht vergessen!** Darauf achten, dass die Lösungen beim richtigen Tutor/der richtigen Tutorin abgegeben werden.
Achten Sie bei Programmieraufgaben außerdem darauf, dass diese im Linuxpool kompilierbar sind.
Zu spät abgegebene Lösungen werden nicht mehr berücksichtigt!

1. Aufgabe: Begriffe (7 Punkte)

Beschreiben Sie jeden der folgenden Begriffe durch maximal zwei Sätze: Port, Cipher, Public Key Infrastructure, Bastion Host, Proxy, NAT, IPsec

2. Aufgabe: Zwischensysteme (9 Punkte)

Für die gesamte Aufgabe soll von folgendem einfachen Firmennetz ausgegangen werden:



Knotentyp		MAC-Adresse	IP-Adresse
Computer	C ₁	AE3F	129.13.42.67
	C ₂	1F3D	129.13.42.78
	C ₃	4E37	129.13.37.67
	C ₄	345C	129.13.128.200
Switch	S ₁	268F	10.1.1.17
	S ₂	1A2C	10.1.1.29
Router	R ₁	Port b: 3A24	10.1.1.2
		Port c: 5D67	Port b: 129.13.42.1
		Port g: 7F29	Port c: 129.13.71.14
			Port g: 129.13.37.1
	R ₂		10.1.1.45
		Port d: AE34	Port d: 129.13.71.27
		Port e: B2A5	Port e: 129.13.128.1

Alle Verbindungen a, b, ..., g sollen vom Typ 100 Mbit/s-Ethernet sein. Die MAC-Adressen wurden vereinfacht, um unnötiges Schreiben zu vermeiden. Ansonsten wird eine ganz normale Internet-Protokollwelt mit IPv4 angenommen. Switches arbeiten wie transparente Brücken und können noch mehr als die gezeigten Ports besitzen. Ebenso wurden bei den Routern nur die für die Aufgabe benötigten Ports gezeigt. C_3 sei allen Komponenten als DNS-Server bekannt, ebenso die Default-Gateways. Ein Management-Netz wurde der Übersicht halber weggelassen.

- Welche Adressklassen gibt es im Internet und welche davon werden hier verwendet? Welche Adressbereiche werden für das öffentliche und welche für das private Netz eingesetzt? (3 Punkte)
- Gehen Sie davon aus, dass noch kein Rechner C_1 mit einem anderen Rechner kommuniziert hat. Ein Anwender klickt im Web-Browser auf C_1 auf einen URL, welcher auf eine Datei verweist, die auf C_4 gespeichert sei. Welche Art Pakete sind die ersten, die jeweils über Teilstrecke a, b und e übertragen werden? Warum werden diese Pakete benötigt? (4 Punkte)
- Nach jahrelangem Dienst fällt S_1 aus. Der Switch wird umgehend durch einen neuen ersetzt und die angeschlossenen Komponenten sollen möglichst nichts davon bemerken. Nach Einschalten des neuen S_1 sendet C_2 , wie gewöhnlich und unabhängig von der Existenz eines neuen Switches, eine DNS-Anfrage an C_3 . Geben Sie den jeweiligen Paketkopf (nur Quell-/Zieladresse) auf Schicht 2 von Teilstrecken a, b, c, f und g an. (2 Punkte)

3. Aufgabe: Sicherheitsziele (8 Punkte)

Weisen Sie den Sicherheitszielen Vertraulichkeit, Erhalt der Datenintegrität, Verantwortlichkeit und Serviceerreichbarkeit jeweils einen typischen Angriff zu, der versucht diese zu unterlaufen. Erläutern sie diese in maximal zwei Sätzen.

4. Aufgabe: Fifty/Fifty (6 Punkte)

Entscheiden Sie, ob folgenden Aussagen zutreffend oder nicht zutreffend sind, und begründen Sie Ihre Entscheidung:

- Eine Denial-of-Service-Attacke ist schon dann gegeben, wenn absichtlich so viele erlaubte Anfragen an einen Server gestellt werden, dass die Anfragen anderer Benutzer erst nach langer Zeit ausgeführt werden können.
- Mit dem Aufkommen von asymmetrischen Codes sind symmetrische Codes überflüssig geworden, da diese einen vorherigen Schlüsselaustausch benötigen.
- UDP wird für Multimedia-Dienste mit Echtzeit-Anforderungen eingesetzt.

5. Aufgabe: Port-Scanner (8 Punkte)

Implementieren Sie in C einen Port-Scanner, der als Kommandozeilenparameter einen Rechnernamen und zwei Portnummern erhält. Das Programm soll nun versuchen, zu allen Ports, die sich in dem von den zwei weiteren Parametern gegebenen Intervall befinden, eine Verbindung aufzubauen. Die Ausgabe des Port-Scanners ist eine Liste der offenen Ports und die jeweilige Ausgabe des Servers auf diesem Port, falls es denn eine gibt. Welche Rückschlüsse über den gescannten Rechner lassen sich aus einem Scan der untersten 1024 Ports ziehen?

6. Aufgabe: IP-Stack (12 Punkte)

Der auf dem 6. Übungsblatt in Aufgabe 5 verwendete Linux-Kernel kann keine Netzwerkverbindung zur Außenwelt herstellen, weil der Emulator in der verwendeten einfachen Konfiguration keine Netzwerkunterstützung anbietet. Dennoch bietet er Einblicke in die Implementierung eines TCP/IP Stacks.

- Welche Ausgabe erhalten Sie verschiedene IP-Adressen mit dem Befehl **ping** auf Erreichbarkeit testen? Testen Sie das Verhalten mit der Loopback-Adresse, der eigenen IP-Adresse (zu ermitteln mit dem Befehl **ifconfig**), einer IP-Adresse in demselben Subnetz und einer IP-Adresse außerhalb des Subnetzes. (2 Punkte)
- An welcher Stelle im Kernel (Implementierung von TCP/IPv4 in `net/ipv4/`) werden die jeweiligen Fehlerzustände erkannt bzw. an welcher Stelle wird auf ein Timeout gewartet? Ordnen Sie die jeweiligen Stellen in der Implementierung dem ISO/OSI-Schichtenmodell zu. (4 Punkte)
- Gegen Sie an den jeweiligen Schnittstellen zwischen den beteiligten Schichten die kompletten, von der jeweils unteren Schicht zu übertragenden Pakete im Hexadezimalformat auf der Console aus. Identifizieren Sie jeweils für ein Paket pro Schnittstelle die Felder im Paketkopf. (6 Punkte)