universität wien

PR Netzwerktechnologien
Sommersemester 2014

Aufgabenblatt 4

Abgabetermin: Montag, 16.06.2014 09.00 Uhr

Team-Abgabe als PDF im CEWebS

Aufgabe 4.1: *Forwarding*

15 Punkte

Ein Router in einem IPv4-Netzwerk hat vier Schnittstellen, über die er ankommende Pakete weiterleitet.

Ziel-Adressbereich	Schnittstelle
11000000 00000000 00000000 00000000 bis	0
11000000 00000000 11111111 11111111	
11000000 00000001 00000000 00000000 bis	1
11000000 00000001 11111111 11111111	
11000000 00000010 00000000 00000000 bis	2
11000001 11111111 11111111 11111111	
alle anderen	3

1. Konvertieren Sie die Einträge in die Dotted-Decimal-Adress/Subnetzmasken-Schreibweise.
2. Geben Sie die Forwarding Tabelle für Longest Prefixes Matching an.
3. Über welche Schnittstelle werden Pakete mit den Zieladressen 191.168.0.1, 192.0.1.1, 192.1.0.1, 193.168.0.1, und 224.0.13.7 weitergeleitet?

Aufgabe 4.2: *Routing und NAT*

30 Punkte

1. Zwei Computer befinden sich je hinter einem eigenem NAT. Beschreiben Sie Wege, wie diese miteinander via TCP kommunizieren können, ohne dass das NAT dafür konfiguriert werden muss.
2. Beschreiben Sie die Routing-Ansätze von OLSR (RFC 3626) und vergleichen sie das Protokoll mit aus der Vorlesung bekannten Ansätzen wie RIP oder OSPF. Wieso verwenden Community-Netze wie funkfeuer.at und Freifunk bevorzugt OLSR und verwandte Ansätze?
3. Erstellen Sie ein Netzwerk-Topologie mit mindestens $v = 11$ Knoten, $e = v + 3$ Kanten und zufällig gewählten Kantengewichten. Bestimmen Sie nun die Routing-Tabellen für zwei dieser Knoten nach dem Link State-Verfahren. Zeigen Sie den Herleitungsweg der Tabellen auf.

4. Erklären Sie anhand eines möglichst kleinen Netzwerks das *count-to-infinity*-Problem und zwei Gegenmaßnahmen zu diesem.

Aufgabe 4.3: *Sicherungs- und Bitübertragungsschichtschicht*

15 Punkte

1. Wie lange wartet ein Netzwerkadapter, der CSMA/CD verwendet, nach einer Kollision, bevor er erneut versucht zu senden? Wie hängen Datenrate, minimale Framegröße und maximale räumliche Ausdehnung des Netzwerks zusammen? Wie lange ist die Wartezeit für $K = 997$ bei einer 10 Mibit s^{-1} Verbindung?

2. Welche Rolle spielen Beacon-Frames in 802.11? Welchen Inhalt haben Sie?

3. Ein 802.11b Sender möchte 1200 B Daten über einen leeren Kanal mit 9 Mibit s^{-1} übertragen. Wie lange dauert es, bis die Übertragung abgeschlossen ist, wenn der Kanal vorher reserviert werden soll? Fertigen Sie dazu auch ein Sequenzdiagramm an. Wieso können Kanalreservierungen nötig sein?

Aufgabe 4.4: *Netzwerksicherheit*

40 Punkte

1. Berechnen Sie den MD4-Hash eines beliebig gewählten Wortes und beschreiben Ihre Vorgehensweise. Warum sollten Sie dieses Verfahren heute nicht mehr und welche Verfahren stattdessen verwenden?

2. Erklären Sie je anhand eines Beispiels aus der Netzwerktechnik einen *Side Channel Attack* und einen *Man-in-the-Middle Attack* und diskutieren Sie Gegenmaßnahmen. Kann Man-in-the-Middle auftreten, wenn symmetrische Verschlüsselung benutzt wird?

3. Verwenden Sie RSA mit fünfstelligen Primzahlen Ihrer Wahl um ein Wort Ihrer Wahl zu verschlüsseln und danach wieder zu rekonstruieren.

4. Beschreiben Sie anhand eines Sequenzdiagramms den vollständigen Verbindungsaufbau von IMAP (RFC 3501) mit STARTTLS (RFC 2595).

5. Beschreiben Sie die Bedeutung von Forward Secrecy für die Vertraulichkeit von Kommunikation. Beschreiben Sie außerdem kurz ein Verfahren, dass dies sicher stellen kann.

6. Beschreiben Sie kurz das Kerckhoffs'sche Prinzip[1]. Wenden Sie das Prinzip auf einige aktuelle Instant Messaging Systeme an. Wie schneiden diese ab?

Gesamt: 100 Punkte

[1] `http://www.petitcolas.net/fabien/kerckhoffs/`