Distributed Systems

RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

Klausur
"Sichere Verteilte Systeme"
SS 2010

Name, Vorname: «NACHNAME», «VORNAME»

Matrikelnummer: «MATNR»

Zur Beachtung:

- Die Klausur besteht aus 6 Aufgaben und 18 Seiten.
- Bitte legen Sie Ihren Personalausweis/Reisepass und Studentenausweis auf den Tisch, damit wir die Überprüfung ohne Störung während der Klausur durchführen können.
- Es dürfen keine weiteren Hilfsmittel verwendet werden.
- Schreiben Sie Ihre Lösungen – soweit möglich – nur in die entsprechenden Stellen der Aufgabenblätter.
- Fassen Sie Ihre Antworten kurz und präzise.
- Die Klausur dauert 120 Minuten und es gibt insgesamt 120 Punkte.
- Bewahren Sie ihre Klausurnummer auf. Nur unter dieser werden die Ergebnisse veröffentlicht.

Ich bestätige, dass ich die Klausur selbstständig bearbeitet habe.

_____

(Unterschrift)

Punkte:

Aufgabe	1 (16 P)	2 (17 P)	3 (12 P)	4 (34 P)	5 (11 P)	6 (30 P)	**Σ (120P)**	**Note**
Punkte								
Kürzel								

Aufgabe 1: Allgemeine Grundlagen (7 + 3 + 4 + 2 = 16 Punkte)

a) *Skizzieren* Sie die beiden in der Vorlesung vorgestellten Protokollreferenzmodelle und benennen Sie die einzelnen Schichten. Angenommen all die Protokollfunktionalität sei in einer einzigen Schicht implementiert. Ergeben sich damit irgendwelche Vorteile gegenüber den Schichtenmodellen? Wenn ja, welche?

b) Nennen Sie *drei typische Gemeinsamkeiten* der Sicherungs- und Transportschicht am Beispiel von Ethernet und TCP. *Erläutern* Sie diese mit jeweils einem Satz.

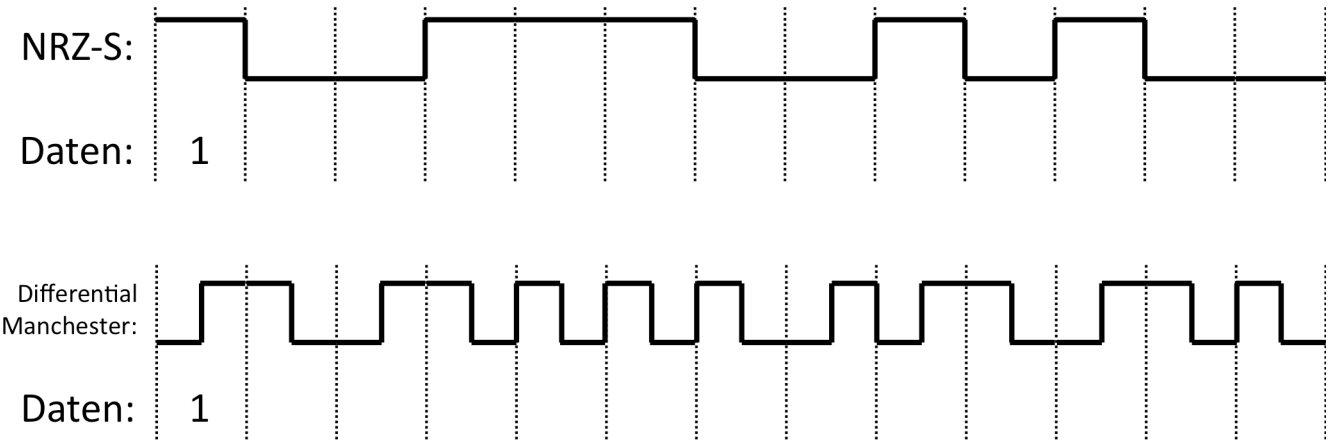
c) *Formulieren* Sie das Abtasttheorem von Shannon und Rabe. Geben Sie ein in der Vorlesung vorgestelltes Beispiel aus der Praxis, wo das Theorem in der Bitübertragungsschicht seine Anwendung findet.

d) Welche der beiden folgenden IPv4-Subnetzmasken ist gültig und welche ungültig? Warum?

- 255.255.96.0
- 255.255.128.0

Aufgabe 2: Bitübertragungsschicht (4 + 2 + 3 + 8 + 4 = 21 Punkte)

a) Im Folgenden erhalten Sie zwei physikalische Signale. Das erste ist in Non-Return-to-Zero-Space (NRZ-S), das zweite in Differential Manchester codiert. Decodieren Sie die Signale in Bitfolgen.



b) Angenommen, bei der Übertragung dieser beiden Signale liegt die Anzahl der Pegelwechsel bei jeweils 25000 Wechseln pro Sekunde. Wie hoch ist jeweils die Datenübertragungsrate in bit/s?

c) Wie hoch ist die Datenrate eines Kanals mit einer Bandbreite von 50KHz und 256 verschiedenen Signalstufen?

d) Angenommen, der unter c) angegebene Kanal bietet einen Signal-Rausch-Abstand von 20dB. Kann dies zu Problemen führen? Begründen Sie ihre Antwort! Wie viele Bits pro Schritt sind unter diesen Umständen maximal codierbar?

e) Wieso wurde bei der Spezifikation der „schnelleren“ Ethernet-Variante (FastEthernet, damit 100 Mbit/s statt 10 Mbit/s) die maximale Segmentlänge auf 100m reduziert? *Begründen* Sie ihre Antwort.

Aufgabe 3: Sicherungsschicht

(3 + 4 + 2 + 3 = 12 Punkte)

a) Wodurch unterscheiden sich gerade und ungerade Parität? Zeigen Sie dies durch die Berechnung der beiden Paritäten für die Bitfolge 1001.

b) Ein Verfahren zur Sicherung der Übertragung ist die Kreuzparität. Führen Sie das Kreuzparitätsverfahren für die unten angegebenen Daten aus. Dabei soll die Querparität gerade und die Blockparität ungerade sein. Das mit X gekennzeichnete Feld müssen Sie nicht ausfüllen.

	Byte 0	**Byte 1**	**Byte 2**	**Byte 3**	**Byte 4**	**Parität**
Bit 0	0	0	0	1	1	
Bit 1	1	1	1	0	0	
Bit 2	1	0	0	0	1	
Bit 3	1	0	1	0	0	
Bit 4	1	1	0	1	0	
Bit 5	0	0	1	0	0	
Bit 6	1	0	0	1	0	
Parität						X

c) Welchen Vorteil bietet das Kreuzparitätsverfahren gegenüber einfacher Parität? Welchen Nachteil?

d) Forward Error Correction erlaubt die Wiederherstellung von inkorrekt empfangenen oder verlorenen Paketen. Nutzen Sie ein aus der Vorlesung bekanntes Verfahren, bei dem zusätzlich zu den Nutzdaten ein weiteres Paket mit Wiederherstellungsinformationen übertragen wird. Drei Pakete sind gegeben:

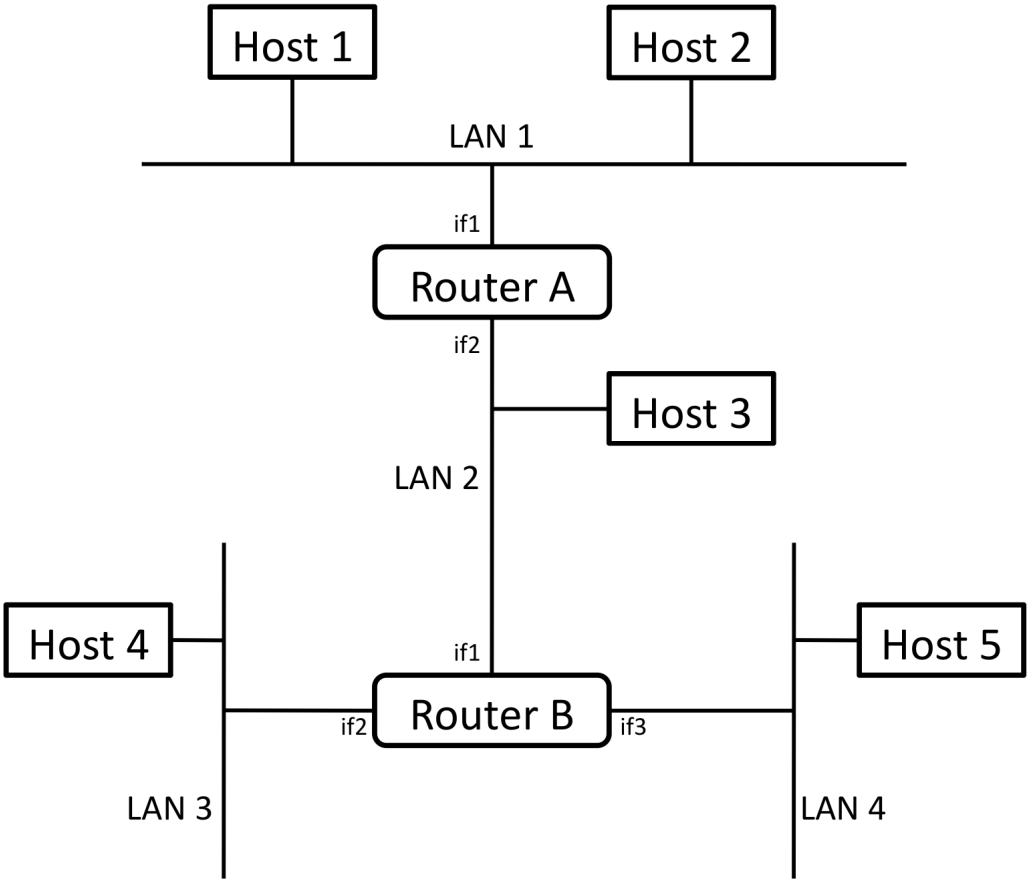
   a. P1: `10011101`
   b. P2: `01010110`
   c. P3: `11100110`

   Mit welchem Verfahren wird P4 berechnet? Geben Sie P4 an.

Aufgabe 4: Netzwerkschicht

(10 + 4 + 6 + 3 + 10 + 1 = 34 Punkte)

Gegeben sei das in der folgenden Grafik dargestellte Netz. Dabei sind in jedem Subnetz (LAN1-LAN4) exemplarisch ein oder zwei Hosts dargestellt.



Für Aufgabenteil d) benötigen Sie die MAC-Adressen der einzelnen Interfaces:

Host 1	01:02:03:04:05:11
Host 2	01:02:03:04:05:12
Host 3	01:02:03:04:05:13
Host 4	01:02:03:04:05:14
Host 5	01:02:03:04:05:15
Router A, if1	01:02:03:04:05:A1
Router A, i2	01:02:03:04:05:A2
Router B, if1	01:02:03:04:05:B1
Router B, if2	01:02:03:04:05:B2
Router B, if3	01:02:03:04:05:B3

a) Sie haben zur Konfiguration dieses Netzes den Adressbereich 134.130.56.0/21 erhalten. LAN 1 enthält ca. viermal so viele Rechner wie (jeweils) LAN 2, 3 und 4. Konfigurieren Sie die Subnetze entsprechend. Geben Sie eine kurze Begründung für ihre Aufteilung.

	Adresse (Netz-ID)	Maske
LAN 1		
LAN 2		
LAN 3		
LAN 4		

(Beispiel für einen Eintrag: Adresse „213.133.49.0“, Maske „/16“ oder „255.255.0.0“)

b) Teilen Sie jedem Interface eine gültige IPv4-Adresse zu.

Host 1	
Host 2	
Host 3	
Host 4	
Host 5	
Router A, if1	
Router A, if2	
Router B, if1	
Router B, if2	
Router B, if3	

c) Zum Internetworking ist es erforderlich, dass die Router wissen, wie sie Pakete weiterzuleiten haben. Geben Sie die Routingtabellen für beide Router an. Kennzeichnen Sie direkte Verbindungen mit einem Stern (*).

	Ziel	Interface	Gateway
Router A			
Router B			

d) Host 2 hat eine HTTP-Verbindung zu Host 5 aufgebaut und verschickt ein Paket mit HTTP-Daten. Welchen Weg nimmt das Paket? Geben Sie für jedes Teilstück der Strecke die Ziel-MAC-Adresse und Ziel-IP-Adresse an. (Hinweis: sollten Sie Aufgabenteil b) nicht lösen können, so tragen Sie in die dortige Tabelle beliebige IP-Adressen ein, und nutzen diese hier.)

e) Nehmen Sie an, das in Teilaufgabe d) versendete IP-Paket habe eine Payload von 1200 Byte. Die MTU für LAN1 und LAN 2 betrage 1400 Byte, für LAN 3 und LAN4 576 Byte. Führen Sie die notwendige Fragmentierung durch. Geben Sie für jedes Fragment die folgenden Werte an:

- Größe der Payload in Bytes
- Wert des MF-Flags
- Wert im Fragment-Offset-Feld

Gehen Sie dabei von einem Standard-IPv4-Paket ohne Headeroptionen aus.

f) Was geschieht mit dem Paket, wenn Host 2 das DF-Flag auf 1 gesetzt hat?

Aufgabe 5: Transport- und Anwendungsschicht

(2 + 2 + 3 + 4 = 11 Punkte)

a) Woran und auf welcher Schicht erkennt ein Endsystem, für welche Anwendung ein bestimmtes Paket bestimmt ist?

b) Bei der Verwendung von negativen Bestätigungen (NAK) signalisiert der Empfänger dem Sender, wenn er ein Paket nicht oder nicht korrekt erhalten hat. Wie erkennt dies der Sender, falls keine NAKs verwendet werden?

c) Ein großer Vorteil von TCP gegenüber UDP ist die gesicherte Datenübertragung. Deshalb wird UDP hauptsächlich in Bereichen eingesetzt, in denen es nicht auf 100%ige Übertragungssicherheit ankommt, wie zum Beispiel Multimediastreaming. Daneben kommt UDP aber auch noch anderen wichtigen Anwendungsschichtprotokollen aus anderen Gründen zum Einsatz. Nennen Sie ein solches Protokoll, und erläutern Sie, worin in dem Fall der Vorteil besteht.

d) In der Vorlesung wurden zwei Protokolle behandelt, mit denen ein Host im Netz die Zuweisung einer IP-Adresse erbitten kann. Nennen Sie die beiden Protokolle. Welches ist das umfassendere? Nennen Sie eine zusätzliche Information, die Sie im umfassenderen Protokoll zusätzlich zur zugewiesenen IP-Adresse erhalten.

Aufgabe 6: Sicherheit (6 + 4 + 10 + 10 = 30 Punkte)

a) *Beschreiben* Sie kurz die Sicherheitsfunktionen von *Authentication Header* (*AH*) in IPSec. *Skizzieren* Sie, wie AH in das normale IP-Protokoll integriert wird.

b) Was versteht man unter dem Begriff *Spoofing*? Welche Internet-Protokolle sind davon betroffen? Nennen und erläutern Sie 4 Beispiele.

c) Das Needham-Schroeder Protokoll enthielt in seiner frühen Version die folgende Sicherheitslücke: Nachdem Herausfinden des Schlüssels von Alice zum KDC konnte der Angreifer vom KDC einen geheimen Schlüssel (ein Ticket) für Bob anfordern. Wenn Alice ihren Schlüssel nach dem Angriff änderte, blieb das Ticket für Bob trotzdem gültig. *Beschreiben* Sie wie es zu dieser Schwachstelle gekommen ist und *skizzieren* Sie wie diese in einer weiteren Version des Protokolls geschlossen wurde.

d) Ein bekanntes asymmetrisches Verfahren ist *RSA*. Sie belauschen eine per RSA gesicherte Kommunikation und erhalten den verschlüsselten Text c. Der öffentliche Schlüssel, der zur Verschlüsselung verwendet wurde, ist <e = 29, n = 221>. *Ermitteln Sie den privaten Schlüssel d mit dem erweiterten euklidischen Algorithmus*. *Erläutern* Sie durch Angabe des Rechenwegs, wie die verschlüsselte Nachricht damit entschlüsselt werden kann.