

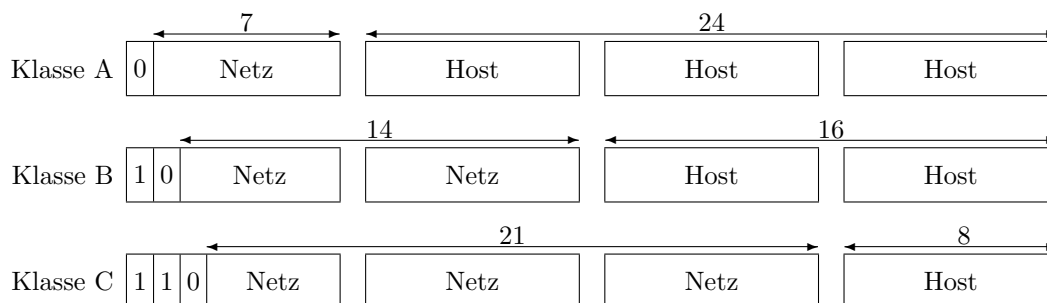
Übungen zur Vorlesung
Betriebssysteme, Rechnernetze und verteilte Systeme II
 Im Wintersemester 2008/2009
Blatt 7

Aufgabe 1: IP-Netzklassen und IP-Subnetze (3 Punkte) Zum Routing von IP-Datagrammen von einem Netz zu einem anderen ist es nötig, zu wissen, welcher Teil der 32 Bit-IP-Adresse das Netz kodiert, an das der Host angeschlossen ist, und welcher Teil die Adresse des Hosts innerhalb dieses Netzes darstellt. In der Literatur finden Sie die beiden Verfahren, die dies ermöglichen:

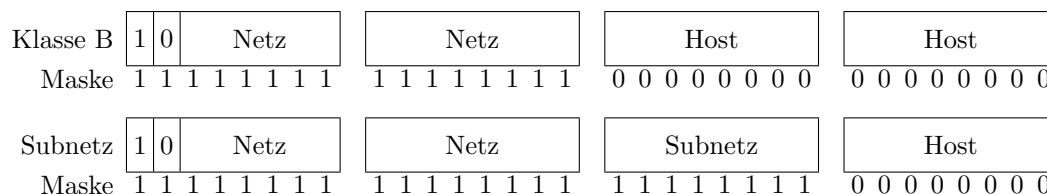
IP-Address-Classes IP kennt fünf Adress-Klassen: A, B, C, D und E. Nur Netze der Klassen A, B und C werden kommerziell verwendet. Klasse-D-Adressen sind Multicast-Gruppen, Klasse-E-Netze sind experimentell.

Die 32 Bit-Adressen werden üblicherweise als vier Gruppen von jeweils acht Bits (Octets) oder dezimal in dem bekannten *Dotted Decimal Format* dargestellt. Die höchstwertigsten Bits der Adresse identifizieren, wie in der Tabelle angegeben, die Netz-Klassen. Daraus ergeben sich die Adressbereiche und die maximale Anzahl von Hosts pro individuellem Netz.

IP-Addr.-Klasse	Format ¹	Höchstwertigste Bits	Adressbereich	Max. Anzahl Hosts pro Netz
A	N.H.H.H	0	1.0.0.0 – 126.0.0.0	16 777 214
B	N.N.H.H	10	128.1.0.0 – 191.254.0.0	65 534
C	N.N.N.H	110	192.0.1.0 – 223.255.254.0	254
D	—	11110	224.0.0.0 – 239.255.255.255	—
E	—	11111	240.0.0.0 – 254.255.255.255	—



IP-Subnet-Addressing IP-Netze können (unabhängig von ihren eigentlichen Klassen) in (kleinere) Subnetze unterteilt werden. Die IP-Adresse wird durch eine Subnetzmaske in Netz- und Host-adresse aufgeteilt. Subnetzmasken haben das gleiche Format wie IP-Adressen. Jedoch bedeuten Einsen, dass der entsprechende Teil der IP-Adresse das Netz (oder Subnetz) angibt, und Nullen, dass der entsprechende Teil der IP-Adresse den Host innerhalb des (Sub-)Netzes adressiert. Die Grenze zwischen Netz- und Hostteil ist nicht an Octet-Grenzen gebunden.



¹N = Netz, H = Host

Private Adressbereiche Die RFC 1597 legt drei „private“ Adressbereiche fest, die nicht zentral vergeben werden und im öffentlichen Internet nicht geroutet werden:

11.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

- a) Wo liegen die Vor- und Nachteile beider Methoden?
- b) Ist die Subnetzmaske 255.255.255.15 möglich? Begründen Sie
- c) In einem Klasse-C-Netz stehen laut Tabelle nur 254 Adressen zur Verfügung, obwohl man erwarten könnte, dass $2^8 = 256$ Adressen möglich sind. Was ist der Grund für diese Abweichung?
- d) Wozu dient das Netz 127.0.0.0? Welchen Host bezeichnet die Adresse 127.0.0.1?

Aufgabe 2: IP-Routing (3 Punkte) Auf Seite 3 f. finden Sie die Skizze eines IP-Netzes und die Routing-Tabellen der einzelnen Hosts bzw. Router.

- a) Welchen Weg nimmt ein IP-Datagramm von Host G nach Host N ?
- b) Welchen Weg nimmt ein IP-Datagramm von Host A nach Host D ?
- c) Welche Hosts kann Host P erreichen, von welchen Hosts kann Host P erreicht werden?

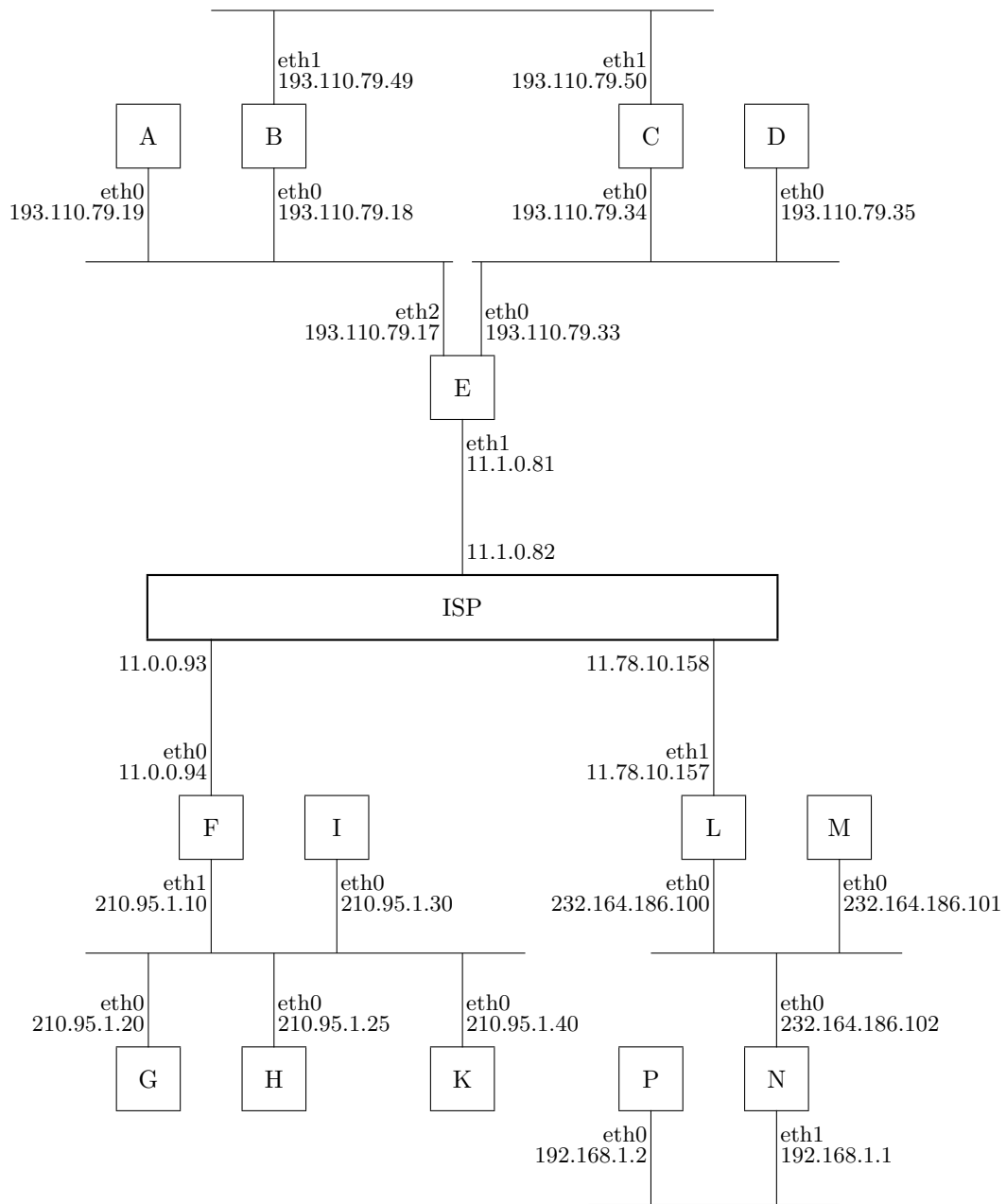
Aufgabe 3: CRC-Codes (4 Punkte) 6 Bit-Wörter $D(x)$ werden CRC-codiert mit dem 3 Bit-Generatorpolynom $G(x) = 101$.

- a) Berechnen Sie die zu übertragenden Code-Wörter $T(x)$ zu folgenden Nutzinformatioenen.
 - i) $D(x) = 100110$
 - ii) $D(x) = 101010$
- b) Überprüfen Sie, ob die Code-Wörter $T(x)$ korrekt empfangen wurden.
 - i) $T(x) = 10011001$
 - ii) $T(x) = 01100110$

Aufgabe 4: Hamming-Code (Zusatzaufgabe 4 Punkte)

- a) Begründen Sie, dass die Formel $r = \min\{l \mid m + l + 1 \leq 2^l\}$ die minimale Anzahl r von Check-Bits bestimmt, um die ein Wort der Länge m ergänzt werden muss, damit 1 Bit-Fehler korrigierbar sind.
- b) Warum werden die Positionen 1, 2, 4, ... als Position der Check-Bits gewählt?
- c) Bilden Sie den Hamming-Code (gerader Parität) für folgende 8 Bit-Wörter:
 - i) 01010101
 - ii) 11110000
- d) Sie empfangen folgende Wörter im Hamming-Code (mit gerader Parität). Korrigieren Sie eventuelle 1 Bit-Fehler.
 - i) 000011100011
 - ii) 000100001111
 - iii) 111111110000

zu Aufgabe 2



Node A

Destination	Gateway	Genmask	Flags	Iface
0.0.0.0	193.110.79.17	0.0.0.0	UG	eth0
193.110.79.16	0.0.0.0	255.255.255.240	U	eth0
193.110.79.48	193.110.79.18	255.255.255.240	UG	eth0
193.110.79.32	193.110.79.18	255.255.255.240	UG	eth0

Node *B*

Destination	Gateway	Genmask	Flags	Iface
0.0.0.0	193.110.79.17	0.0.0.0	UG	eth0
193.110.79.16	0.0.0.0	255.255.255.240	U	eth0
193.110.79.48	0.0.0.0	255.255.255.240	U	eth1
193.110.79.32	193.110.79.50	255.255.255.240	UG	eth1

Node *C*

Destination	Gateway	Genmask	Flags	Iface
0.0.0.0	193.110.79.33	0.0.0.0	UG	eth0
193.110.79.48	0.0.0.0	255.255.255.240	U	eth1
193.110.79.32	0.0.0.0	255.255.255.240	U	eth0
193.110.79.16	193.110.79.49	255.255.255.240	UG	eth1

Node *D*

???

Node *E*

Destination	Gateway	Genmask	Flags	Iface
0.0.0.0	11.1.0.82	0.0.0.0	UG	eth1
11.1.0.80	0.0.0.0	255.255.255.252	U	eth1
193.110.79.48	193.110.79.18	255.255.255.240	UG	eth2
193.110.79.32	0.0.0.0	255.255.255.240	U	eth0
193.110.79.16	0.0.0.0	255.255.255.240	U	eth2

Node *F*

Destination	Gateway	Genmask	Flags	Iface
0.0.0.0	11.0.0.93	0.0.0.0	UG	eth0
11.0.0.92	0.0.0.0	255.255.255.252	U	eth0
210.95.1.0	0.0.0.0	255.255.255.0	U	eth1

Nodes *G, H, I, K*

Destination	Gateway	Genmask	Flags	Iface
0.0.0.0	210.95.1.10	0.0.0.0	UG	eth0
210.95.1.0	0.0.0.0	255.255.255.0	U	eth0

Node *L*

Destination	Gateway	Genmask	Flags	Iface
0.0.0.0	11.78.10.158	0.0.0.0	UG	eth1
11.78.10.156	0.0.0.0	255.255.255.252	U	eth1
232.164.186.0	0.0.0.0	255.255.255.0	U	eth0
192.168.1.0	232.164.186.102	255.255.255.0	UG	eth0

Node *M*

???

Node *N*

Destination	Gateway	Genmask	Flags	Iface
0.0.0.0	232.164.186.100	0.0.0.0	UG	eth0
232.164.186.0	0.0.0.0	255.255.255.0	U	eth0
192.168.1.0	0.0.0.0	255.255.255.0	U	eth1

Node *P*

Destination	Gateway	Genmask	Flags	Iface
232.164.186.0	192.168.1.1	255.255.255.0	UG	eth0
192.168.1.0	0.0.0.0	255.255.255.0	U	eth0