Rechnernetze, Übung 6

Henry Haustein

Aufgabe 1

(a) Dijkstra-Algorithmus

permanente Knoten	**Arbeitsknoten**	$d(B)$	$d(C)$	$d(D)$	$d(E)$	$d(F)$
A	A	$\underline{3}$	4	∞	∞	∞
A, B	B	3	$\underline{4}$	8	5	∞
A, B, C	C	3	4	$\underline{5}$	5	∞
A, B, C, D	D	3	4	5	$\underline{5}$	9
A, B, C, D, E	E	3	4	5	5	$\underline{9}$

Jetzt sind alle Knoten markiert und der kürzeste Weg von A nach F geht über A → C → D → F und ist 9 Einheiten lang.

(b) Dijkstra-Algorithmus

permanente Knoten	**Arbeitsknoten**	$d(B)$	$d(C)$	$d(D)$	$d(E)$	$d(F)$
A	A	$\underline{3}$	4	∞	∞	∞
A, B	B	3	$\underline{4}$	∞	5	∞
A, B, C	C	3	4	∞	$\underline{5}$	∞
A, B, C, E	E	3	4	∞	5	$\underline{11}$

Knoten D wird nie markiert. Der kürzeste Weg von A nach F geht nun über A → B → E → F und ist 11 Einheiten lang.

Aufgabe 2

(a) Subnetze sind Teilnetze eines größeren Netzwerks. Das Internet bildet dabei das größte, weltumspannende Rechnernetzwerk und besteht aus unzähligen Subnetzen, welche wiederum selbst mehrere Subnetze enthalten können. Damit wird ein hierarchisches Routing ermöglicht.
⇒ Vorteile: keine neuen Netzwerkadressen erforderlich, Subnetzadressen müssen außerhalb der Organisation nicht bekannt sein, Routingtabellen nicht unnötig vergrößert, Basis für klassenloses Routing (CIDR – Classless Interdomain Routing); variable Netzmasken nutzen Adressbereiche besser aus

(b) Subnetzadresse = Adresse AND Subnetzmaske

Adresse	129	44	0	7	10000001	00101100	00000000	00000111
Subnetzmaske	255	255	128	0	11111111	11111111	10000000	00000000
Subnetzadresse	129	44	0	0	10000001	00101100	00000000	00000000

Adresse	129	44	0	7	10000001	00101100	11100000	00001111
Subnetzmaske	255	255	128	0	11111111	11111111	11000000	00000000
Subnetzadresse	129	44	192	0	10000001	00101100	11000000	00000000

(c) Die Subnetzmaske M_1 besteht aus 17 Einsen, maximal können 32 Einsen als Adresse verteilt werden. Das bedeutet es können noch $2^{32-17} = 2^{15}$ Adressen im Subnetz verteilt werden. Ähnlich für M_2, hier können noch $2^{32-18} = 2^{14}$ Adressen verteilt werden.

Aufgabe 3

(a) Es gilt

Netz	**IP von**	**IP bis**	**Netzadresse**	**Subnetzmaske**	**CIDR**	**Hosts**
A	141.30.0.0	141.30.255.255	141.30.0.0	255.255.0.0	/16	2^{16}
B	172.16.0.0	172.17.255.255	172.16.0.0	255.254.0.0	/15	2^{17}
C	141.76.40.0	141.30.43.255	141.76.40.0	255.255.252.0	/22	2^{10}

Immer 2 Adressen sind in einem Subnetz reserviert, die Anzahl an Endgeräten verringert sich damit um 2.

(b) Weiterleitungstabelle für Router ZIH

Typ	**Filter**		**Gateway**	**Interface**	**Bemerkung**
C	10.10.10.0	30		eth3	Transitnetz zu Router INF
C	141.30.0.0	16		eth1	angeschlossenes Subnetz A
S	141.76.0.0	16	10.10.10.2		Subnetz INF über Router INF (Gateway)
C	172.16.0.0	15		eth2	angeschlossenes Subnetz B
D*	0.0.0.0	0	= DFN x (188.1.x.x)		Standardroute (default route) über DFN

(c) Weiterleitungstabelle für Router INF

Typ	**Filter**		**Gateway**	**Interface**	**Bemerkung**
C	10.10.10.0	30		eth1	Transitnetz zu Router INF
S	141.76.40.0	22	141.76.29.33		Statische Route (Umleitung über Firewall)
D	0.0.0.0	0	10.10.10.1		Standardroute (default route)

(d) Weiterleitung von Paketen

Zieladresse	Router INF	Router ZIH
172.17.56.78	Weiterleitung an ZIH	Zustellung an Subnetz B
141.76.42.42	Weiterleitung an Firewall	Weiterleitung an INF
9.9.9.9	Weiterleitung an ZIH	Weiterleitung an DFN

Aufgabe 4

(a) Ermittlung von MAC-Adressen

- Sender sendet eine ARP-Anforderung (ARP Request) inkl. der gesuchten IP-Adresse an Broadcast-Adresse (ff:ff:ff:ff:ff:ff)
- Host mit angefragter IP-Adresse hat sich gemeldet und seine MAC-Adresse in ARP-Antwort (ARP Reply) zurückgesendet (alternativ: keine Antwort → Timeout)
- Information wird ARP-Tabelle (ARP Cache) vorübergehend gespeichert, sodass künftige Anfragen schneller beantwortet werden können.

IPv6: Neighbor Discovery Protocol übernimmt die Aufgaben von ARP.

(b) Gratuitous ARP bezeichnet Antwortpakete (ARP Response) für die es keine Anfrage gab. ⇒ Risiko: Man-in-the-Middle

Aufgabe 5

(a) Die Pakete verlassen den Rechner in der Annahme dass die MTU auf dem Weg dem üblichen Standard (bei Ethernet: 1500 Byte Nutzdaten) entspricht. Pakete mit dieser Standard-MTU passen jedoch nicht mehr durch den Link zwischen den VPN-Gateways und müssen daher fragmentiert werden.

(b) Bei IPv4 erfolgt die Fragmentierung auf dem Weg, also auf dem Router, der feststellt, dass die MTU eines Links zu klein ist. Falls das Don't-fragment-Bit gesetzt ist erfolgt eine ICMP-Fehlermeldung (T:3/C:4). Bei IPv6 werden zu große Pakete auf dem Weg nicht fragmentiert, stattdessen erhält der Sender direkt die ICMP-Nachricht Packet too big, welche auch die maximale MTU auf dem Pfad (Path MTU) enthält. Der Sender des ursprünglichen Pakets muss das Paket nun entsprechend der PMTU fragmentieren und erneut senden.

Aufgabe 6

(a) IPv4 benutzt 32-Bit-Adressen. Somit sind maximal ca. 4,3 Mrd Adressen möglich. Auf Grund der anfänglichen Einteilung der Adressen in Klassen entfallen jedoch sehr viele Adressen ungenutzt. IPv6 verwendet 128-Bit-Adressen, was $3,4 \cdot 10^{38}$ (340 Sextillionen) Adressen erlaubt. (um Faktor $7,9 \cdot 10^{28}$ mal mehr als bei IPv4).

(b) Vorteile

- Vergrößerung des Adressraums
- Vereinfachung Header → weniger Rechenaufwand in Vermittlungsstellen, insb. Router
- automatische, zustandslose Konfiguration (Zuweisung von Adressen)
- Vereinfachung von mobiler Netzwerkteilnahme
- Implementierung von Sicherheitsmerkmalen (IPsec) innerhalb des IPv6-Standards.

- Qualitäts- und Mehrzielmerkmale werden unterstützt

Herausforderungen beim Übergang von IPv4 zu IPv6

- Berechnungen in Netzwerkgeräten (insb. Vermittlungsstellen) sind i.d.R. aus Effizienzgründen in Hardware realisiert. → Umstellung von 32-Bit-Berechnung auf 128-Berechnungen somit nicht trivial und von Hardware abhängig.
- Viele Altgeräte erlauben keine Hardwareänderungen. → Immenses Kostenproblem durch Phasing-out von Altgeräten
- Selbst wenn die Hardware unproblematisch wäre, kann IPv4 nicht von heute auf morgen abgeschaltet und durch IPv6 ersetzt werden. → Gleichzeitiger Übergangsbetrieb notwendig (bspw. Dual-Stack).
- Erwerb von IP-Adressen ist immer mit Verwaltung und Kosten verbunden. → Provider wollen Geld verdienen (Kunden schröpfen), nicht Geld ausgeben (Investieren).
- Weiterbildung der Administratoren

(c) Für IPv6 wird kein DHCP mehr benötigt, um einen Host mit einer IP-Adresse zu versehen.

- Link-lokale IPv6-Adresse erzeugen (erzeugt automatisch eine zugehörige Multicast-Gruppe)
- Nachricht an erzeugte Multicast-Gruppe senden, fehlende Antwort signalisiert, dass Adresse frei ist
- Host sendet an ff02::2/128 (alle Router) eine Anfrage zur Mitteilung der Konfiguration
- Router antwortet mit Konfiguration, insb. vorhanden(en) Präfix(en)
- Globale Unicast-Adresse wird erzeugt (erzeugt automatisch eine zugehörige Multicast-Gruppe)
- Nachricht an erzeugte Multicast-Gruppe senden, fehlende Antwort signalisiert, dass Adresse frei ist
- Adresszuweisung und Bekanntmachung

Aufgabe 7

(a) Feld: Protocol, Wert: 1 (ICMP), Internet Control Message Protocol, Austausch von Informations- und Fehlermeldungen, hier: ICMP Echo Request ist Host erreichbar? (Ping), jedes Protokoll hat eine durch die IANA festgelegte Nummer, z.B. UDP = 17, TCP = 6

(b) Felder: Source und Destination, Sender = 192.168.1.102, Empfänger = 128.59.23.100

(c) ja, wegen TTL – Time to Live in der Nachricht ist TTL auf 1 gesetzt, jeder Router verringert TTL um mindestens 1, wenn TTL 0 erreicht ist, sendet der Router ICMP Typ 11 (Time-to-live exceeded), hier ist das schon beim 1. Router auf dem Weg zum Empfänger der Fall

(d) Paket ist nicht fragmentiert, da "more fragments" nicht gesetzt ist

(e) source und destination bleiben gleich, totalLength kann sich ändern, identification muss sich ändern (hochzählen), TTL kann sich ändern (typischerweise hochgezählt für das hier verwendete traceroute-Beispiel), header checksum kann sich ändern, wird sich meist ändern, da immer mindestens 1 Feld verändert wird