

PUNKTEVERTEILUNG:

19	20	21		Σ
----	----	----	--	---

Aufgabe (19)

- (a) Host 1: Default-Router: 160.25.10.254, Broadcast: 160.25.10.255, Netmask: 255.255.255.0
 Host 3: Default-Router: 160.25.52.254, Broadcast: 160.25.25.255, Netmask: 255.255.255.0

- (b) Ein beliebiger Router hat genau einen Eintrag für das Netz 160.25.0.0/16. Er muss über die einzelnen Subnetze nichts wissen und hat dementsprechend keinen Eintrag für die einzelnen Subnetze. Dadurch ändert sich die Zahl der Einträge nicht, wenn ein zusätzliches Subnetz in 160.25.0.0/16 hinzugefügt wird.

- (c) Es wird der spezifischere Eintrag verwendet, in dem Fall also 78.7.7.0/24.

- (d) Schicht 2: *MAC-Adresse* adressiert ein physisches Interface eines Geräts

Schicht 3: *IP-Adresse* für die logische Adressierung eines Geräts

Schicht 4: *Port*, sorgt dafür, dass mehrere Prozesse unabhängig voneinander die gleiche IP nutzen können.

Schicht 7: *Protokoll*, wie z.B. HTTP. Spezifiziert, wie ein Programm die Daten interpretiert.

- (e) Das Netz ist ein 160.25.0.0/16-Netz, daher bleiben noch 16 Bit übrig zur Einteilung. Um 8000 IP-Adressen einteilen zu können, benötigt man 13 Bit (8192 Adressen). Dann bleiben noch 3 Bit übrig, also sind 8 solcher Netze möglich.

Die Netze sind dementsprechend dann 160.25.0.0/19, 160.25.32.0/19, 160.25.64.0/19, 160.25.96.0/19, 160.25.128.0/19, 160.25.160.0/19, 160.25.192.0/19, 160.25.224.0/19.

- (f) Die Netzmaske ist jeweils 255.255.96.0 (11111111.11111111.11100000.00000000), da die Subnetze alle die gleiche Struktur haben.

Der erste Rechner des ersten Subnetzes hat die IP-Adresse 160.25.0.1, was binär 10100000.00011001.00000000.00000001 entsprechen würde. Der 4000. Rechner hat die IP-Adresse 160.25.15.160, binär 10100000.00011001.00001111.10100000.

Im zweiten Subnetz hat der erste Rechner die IP-Adresse 160.25.32.1, binär 10100000.00011001.00100000 der 4000. Rechner hingegen 160.25.47.160, was binär 10100000.00011001.00101111.10100000 entspricht.

Aufgabe (20)

- (a)

ARP	who-has 192.168.1.254?
Ethernet	from af:fe:14:af:fe:20 to ff:ff:ff:ff:ff:ff
- | | |
|----------|---|
| ARP | 192.168.1.254 is af:fe:14:af:fe:21 |
| Ethernet | from af:fe:14:af:fe:21 to af:fe:14:af:fe:20 |
- | | |
|----------|---|
| Payload | |
| IP | from 192.168.1.1 to 217.205.134.65 |
| Ethernet | from af:fe:14:af:fe:20 to af:fe:14:af:fe:21 |
- | | |
|----------|---|
| ARP | who-has 192.168.5.34? |
| Ethernet | from af:fe:14:af:fe:22 to ff:ff:ff:ff:ff:ff |

ARP	192.168.5.34 is af:fe:14:af:fe:23
Ethernet	from af:fe:14:af:fe:23 to af:fe:14:af:fe:22

Payload	
IP	from 192.168.1.1 to 217.205.134.65
Ethernet	from af:fe:14:af:fe:22 to af:fe:14:af:fe:23

ARP	who-has 217.205.134.65?
Ethernet	from af:fe:14:af:fe:24 to ff:ff:ff:ff:ff:ff

ARP	217.205.134.65 is af:fe:14:af:fe:25
Ethernet	from af:fe:14:af:fe:25 to af:fe:14:af:fe:24

Payload	
IP	from 192.168.1.1 to 217.205.134.65
Ethernet	from af:fe:14:af:fe:24 to af:fe:14:af:fe:25

- (b) Im ARP-Protokoll sind keine Sicherheitsfeatures vorgesehen daher ist es mittels *ARP-Spoofing* möglich, das Netzwerk mit gefälschten ARP-Paketen zu fluten, um gezielt die Zuordnung von MAC-Adresse zu IP-Adresse zu stören und Pakete auf andere Rechner wie zum Beispiel den eigenen zu leiten, etwa für Man-in-the-Middle-Angriffe.
- (c) Zuerst wird ein 1020 Byte großes Paket an Router 1 geschickt (1000 Byte Nutzdaten plus 20 Byte Header, es wird davon ausgegangen, dass keine Options gesetzt sind).

Total length	1020
Identifier	0
Flags	000
Fragment Offset	0
Source Address	192.168.1.1
Destination Address	217.205.134.65

Dieses Paket ist größer als die MTU zwischen den Routern, also wird von Router 1 in zwei Pakete aufgeteilt. Diese Pakete werden von Router 2 unverändert weitergeleitet und erst beim Empfänger zusammengesetzt.

Das erste Paket enthält 560 Byte Nutzdaten (plus 20 Byte Header), was zusammen genau der MTU entspricht. Es bleiben also noch 440 Byte Nutzdaten, die im zweiten Paket übertragen werden müssen.

Total length	580
Identifier	0
Flags	001
Fragment Offset	0
Source Address	192.168.1.1
Destination Address	217.205.134.65

Das zweite Fragment enthält als Offset $560/8 = 70$ und notiert in den Flags, dass es das letzte Fragment ist, der Identifier ist der selbe wie im ersten Fragment, damit klar wird, zu welchem IP-Datagramm das Fragment gehört.

Total length	460
Identifier	0
Flags	000
Fragment Offset	70
Source Address	192.168.1.1
Destination Address	217.205.134.65

Aufgabe (21)

	Einheit	Bedarf	CIDR	CIDR-verschwendet	Class	Class-verschwendet
(a)	Klein GmbH	5	/29 (8)	1	C (256)	249
	Mittel AG	700	/22 (1024)	322	B (65536)	64834

- (b) Ohne CIDR kann man an den ersten 4 Bits des ersten Bytes erkennen, in welcher Klasse sich ein Netz befindet. Wenn die Netze nach Klassen sortiert sind, kann man die Suche nach einem Netz auf einen kleineren Bereich einschränken und konnte beim ersten Treffer die Suche beenden.

Mit CIDR können die Subnetze in kleinere Teilnetze gegliedert werden und dementsprechend eine eigene Route bekommen. Die Suche kann nun leider nicht mehr beim ersten Treffer abgebrochen werden sondern muss so lange weitergeführt werden bis die spezifische Route gefunden wurde.

- (c) Die linke Hälfte des Bildes entspricht den Klasse-A-Netzen. Die untere Hälfte der rechten Hälfte entspricht den Klasse-C-Netzen und die obere Hälfte der rechten Hälfte stellt die Klasse-C-Netze dar.
- (d) Auf dem Bild erkennt man die Adressverschwendung recht gut an Klasse-A-Netzen die Firmen wie HP, Ford, GE, Xerox, etc gehören (Blöcke die ziemlich schwarz sind). Diese Firmen haben zu Beginn der IPv4-Vergabe große Blöcke bekommen, welche sie jedoch scheinbar nicht benötigen.
- (e) RIPE, ARIN, APNIC, LACNIC und AfriNIC sind die 5 großen *Regional Internet Registries*. Sie sind für die Verwaltung und Verteilung der IP-Adressen auf den verschiedenen Kontinenten der Erde zuständig. RIPE für Europa, ARIN für Nordamerika, APNIC für Asien und Pazifik-Region, LACNIC für Lateinamerika und die Karibik sowie AfriNIC für Afrika.
- (f) Vermutlich wurden solche Bereiche durch CIDR vergeben, wenn das „Muster“ in der Grafik nicht zur jeweiligen Netzklasse passt. Beispielsweise findet man im LACNIC-Netz (189.x.x.x) Cluster mit Größen zwischen 16 und 24 Bits (vermutlich 19-20). Solche Netzgrößen sind nur mit CIDR möglich.
- (g) 2006 waren es 56 nicht allokierte /8-Blöcke während es heute nur noch 16 sind. Wenn der Trend anhält, dann sind die letzten IPv4-Adressen demnächst weg. Dies ist momentan auch das Hauptargument für IPv6, das dem Adressmangel mit längeren Adressen entgegenwirkt.