

NVS Aufgabenblock 6

Abgabe von David Pape, 01634454. Zeitaufwand: 4h.

24. Erklären Sie die Struktur einer IPv4 Adresse. Welche Adress-Klassen gibt es? Welche Bereiche sind für spezielle Zwecke reserviert?

Eine IPv4-Adresse besteht aus 4 bytes, gewöhnlich als punkt-seperierte Dezimalzahlen dargestellt wie:

- 192.168.8.1
- 8.8.8.8

Dabei sind wir natürlich auf 2^{32} (~4bn) Adressen eingeschränkt, und weil das zu Anfangszeiten des Internets eine unglaublich große Zahl war, haben einige Firmen wie HP und Apple großzügigerweise Millionen von Adressen zugeteilt bekommen. Heute reicht diese Zahl nicht mehr und daher gibt es IPv6.

Subnets

Zwecks Organisation hat man IP-Adressen in Subnets aufgeteilt, indem man den ersten Teil einer IP-Adresse als das Subnetz identifizierende Prefix interpretiert (**network portion**), und nur den letzten Teil als eigentliche Adresse des Rechners (**host portion**). Es gibt 3 Klassen von Netzwerken:

1. **Class A:** Das erste Byte ist die network portion.
2. **Class B:** Die ersten zwei Bytes sind die network portion.
3. **Class C:** Die ersten drei Bytes sind die network portion.

Die **netmask** ist dabei die mittels logischem AND anzuwendende Bitmask, wenn man aus der ganzen IP nur die network portion will: für Class C z.B. 255.255.255.0

Reserved addresses

Special address blocks				
Address block	Address range	Number of addresses	Scope	Description
0.0.0.0/8	0.0.0.0–0.255.255.255	16 777 216	Software	Current network ^[3] (only valid as source address).
10.0.0.0/8	10.0.0.0–10.255.255.255	16 777 216	Private network	Used for local communications within a private network . ^[4]
100.64.0.0/10	100.64.0.0–100.127.255.255	4 194 304	Private network	Shared address space ^[5] for communications between a service provider and its subscribers when using a carrier-grade NAT .
127.0.0.0/8	127.0.0.0–127.255.255.255	16 777 216	Host	Used for loopback addresses to the local host. ^[3]
169.254.0.0/16	169.254.0.0–169.254.255.255	65 536	Subnet	Used for link-local addresses ^[6] between two hosts on a single link when no IP address is otherwise specified, such as would have normally been retrieved from a DHCP server.
172.16.0.0/12	172.16.0.0–172.31.255.255	1 048 576	Private network	Used for local communications within a private network. ^[4]
192.0.0.0/24	192.0.0.0–192.0.0.255	256	Private network	IETF Protocol Assignments. ^[3]
192.0.2.0/24	192.0.2.0–192.0.2.255	256	Documentation	Assigned as TEST-NET-1, documentation and examples. ^[7]
192.88.99.0/24	192.88.99.0–192.88.99.255	256	Internet	Reserved. ^[8] Formerly used for IPv6 to IPv4 relay ^[9] (included IPv6 address block 2002::/16).
192.168.0.0/16	192.168.0.0–192.168.255.255	65 536	Private network	Used for local communications within a private network. ^[4]
198.18.0.0/15	198.18.0.0–198.19.255.255	131 072	Private network	Used for benchmark testing of inter-network communications between two separate subnets. ^[10]
198.51.100.0/24	198.51.100.0–198.51.100.255	256	Documentation	Assigned as TEST-NET-2, documentation and examples. ^[7]
203.0.113.0/24	203.0.113.0–203.0.113.255	256	Documentation	Assigned as TEST-NET-3, documentation and examples. ^[7]
224.0.0.0/4	224.0.0.0–239.255.255.255	268 435 456	Internet	In use for IP multicast . ^[11] (Former Class D network).
233.252.0.0/24	233.252.0.0–233.252.0.255	256	Documentation	Assigned as MCAST-TEST-NET, documentation and examples. ^{[11][12]}
240.0.0.0/4	240.0.0.0–255.255.255.254	268 435 455	Internet	Reserved for future use. ^[13] (Former Class E network).
255.255.255.255/32	255.255.255.255	1	Subnet	Reserved for the "limited broadcast " destination address. ^{[9][14]}

Figure 1: https://en.wikipedia.org/wiki/Reserved_IP_addresses

25. Was versteht man unter „Classless Interdomain Routing (CIDR)“?

Es gab schlussendlich viel zu wenige (und viel zu riesige) Class A, und auch zu wenige Class C Netzwerke. Man hat mit CIDR dann auch “Zwischendinger” erlaubt, also n Bits als network portion und nicht nur n Bytes. Entsprechend gibt es netmasks der Form 255.255.255.252; da das unwieldy ist erlaubt man auch 192.168.8.1/30, wobei die /30 dafür steht, dass die Netmask 30 leading 1s hat.

26. Wie kann man den Verwalter einer IP-Adresse herausfinden?

Über die **whois**-Datenbanken der zuständigen Registrars, z.B. Denic für **.de**, oder bei Webseiten, die diese Information sammeln.

27. Beschreiben Sie, welche Schritte ein „Host“ durchführen muss, um ausgehende IPv4 Pakete zu „routen“– wie wird die sog. „routing table“ am Host abgearbeitet? Mit welchen OS-Programmen kann man die Routing-Tabellen ansehen/bearbeiten?

Man kann die routing table unter Linux mit `ip route show` einsehen (für IPv6 mit `ip -6 show`).

- First, the sender creates a packet with its IP as source, and the destination IP as destination
- The sender checks whether it's a local or remote destination
 - (by checking the subnet mask: $(\text{my_ip} \text{ AND } \text{netmask}) = (\text{destination_IP} \text{ AND } \text{netmask})$)
- If it's local find the destination's MAC address using ARP
- If it's remote, we'll look up our **routing table**
 - this is basically a list of known routes (an address with a netmask, and an associated address to go to)
 - we look for the “closest match” route that we can find:
 - * first, check if we have a direct route
 - that means netmask is /32
 - * then check if we have a route to the destination's subnet
 - meaning one for which $(\text{route} \text{ AND } \text{netmask}) = (\text{destination_IP} \text{ AND } \text{netmask})$ holds
 - * Otherwise use the default route
 - the default route is not guaranteed to exist, so we may get **Destination unreachable** here
 - if it exists, it's typically going to point to the local gateway (i.e. router)
 - The router is also going to have a routing table and repeat this same process.
 - We're basically making it the problem of our router
 - Routers know a bit more about the network topology, and may in turn be able to make this the problem of some backbone which is going to know even more, and so on; until the packet finally reaches its destination.

28. Ein 3000 Byte (inkl. IP Header) großes IPv4 Datagramm muss über eine Netzwerk-Verbindung (Link) mit einer maximalen Fragmentgröße (MTU) von 1500 Bytes übertragen werden. Erläutern Sie die Unterschiede der IP Header der einzelnen Fragmente zum IP Header des originalen Datagramms.

Folgende Felder werden sich unterscheiden:

- Total Length
- Identification
- Flags: das erste Fragment bekommt 001, das letzte 000
- Fragment Offset: das erste Fragment bleibt 0, das letzte bekommt einen Wert um 1500
- Header Checksum