LF09:10:IPv4-Netzklassen und Segmentierung

1) IPv4-Adressklassen [→ ZP:Sheet:2]

Historisch gesehen wurden die 4.294.967.296 möglichen IPv4-Adressen auf 5 Klassen aufgeteilt:

1. **Klasse-A-Netze**:
    1. CIDR-Suffix: `/8` → `2^24` Adressen pro Klasse A-Netz
    2. Bereich: `0.0.0.0` (= `0x00000000`) - `127.255.255.255` (= `0x7FFFFFFF`)
    3. Bit-Erkennungsprefix: `0b0` gefolgt von 31 weiteren Bits: `0b0[01]{31}`
2. **Klasse-B-Netze**
    1. CIDR-Suffix: `/16` → `2^16` Adressen pro Klasse B-Netz
    2. Bereich: `128.0.0.0` (= `0x80000000`) - `191.255.255.255` (= `0xBFFFFFFF`)
    3. Bit-Erkennungsprefix: `0b10` gefolgt von 30 weiteren Bits: `0b10[01]{30}`
3. **Klasse-C-Netze**
    1. CIDR-Suffix: `/24` → `2^8` Adressen pro Klasse C-Netz
    2. Bereich: `192.0.0.0` (= `0xC0000000`) - `223.255.255.255` (= `0xDFFFFFFF`)
    3. Bit-Erkennungsprefix: `0b110` gefolgt von 29 weiteren Bits: `0b110[01]{29}`
4. **Klasse-D-Netze**
    2. Bereich: `224.0.0.0` (= `0xE0000000`) - `239.255.255.255` (= `0xEFFFFFFF`)
    3. Bit-Erkennungsprefix: `0b1110` gefolgt von 28 weiteren Bits: `0b1110[01]{28}`
5. **Klasse-E-Netze**
    2. Bereich: `240.0.0.0` (= `0xF0000000`) - `255.255.255.255` (= `0xFFFFFFFF`)
    3. Bit-Erkennungsprefix: `0b1111` gefolgt von 28 weiteren Bits: `0b1110[01]{28}`

Exkurs: Regular Expressions [→ ZP:Sheet:3]

- deutsch: Reguläre Ausdrücke
- abgekürzt: RegEx
- meint: eine grammatische Beschreibung erlaubter Sprachkonstrukte

1. An Position erlaubte Zeichen erscheint literal.
2. An einer Position erlaubte Varianten erscheinen in eckigen Klammern (`[A-Zabc]`):
    - Bereiche werden durch Bindestriche erfasst (`A-Z` meint alle Großbuchstaben).
    - Ansonsten werden alle Varianten direkt hintereinander geschrieben (`abc` meint nur `a`oder `b` oder `c`).

3. Quantoren werden danach in geschweiften Klammern erfasst (`[A-Zabc]`){2,5}:
    - 2 Zahlen werden als `min` bis `max`gelesen.
    - 1 Zahl bestimmt das genaue Vorkommen.
    - 1 Zahl gefolgt von Komma meint `mindestens, aber gern auch mehr`.
    - 0,n meint beliebig viele, aber höchstens n
4. Sonderquantoren werden ohne geschweifte Klammern direkt ans Zeichen angehängt (`A+`):
    - ? meint 0 oder einmal (= {0,1})
    - + mindestens 1 mal, aber sonst beliebig viele male (= {1,})
    - * beliebig oft, aber auch gar nicht (= {0,})

Hinweis: Manche Programme verwenden eine abgewandelte Syntax. `grep` z.B. gibt es auch als Tool `egrep`, was für *expanded global/regular expression" steht.

vgl.:

- https://de.wikipedia.org/wiki/Regulaerer_Ausdruck
- https://en.wikipedia.org/wiki/Regular_expression
- https://de.wikipedia.org/wiki/Grep

Es gilt: **[→ ZP:Sheet:4]**

1. Adressen aus **Klasse-A-Netzen** = frei routbar - außer
    1. `0.0.0.0` :- reserviert als kontextsensitiver Platzhalter
    2. `10.0.0.0` (= `0x0A000000`)- `10.255.255.255` (= `0x0AFFFFFF`) :- privat
    3. `127.0.0.0` (= `0x7F000000`)- `127.255.255.255` (= `0x7FFFFFFF`) :- superprivat
2. Adressen aus **Klasse-B-Netzen** = frei routbar - außer
    1. `169.254.0.1` (= `0xA9FE0001`) - `169.254.255.255` (= `0xA9FEFFFF`) :- APIPA = DHCP-Fallback
    2. `172.16.0.0` (= `0xAC100000`) - `172.31.255.255` (= `0xAC1FFFFF`) :- privat
3. Adressen aus **Klasse-C-Netzen** = frei routbar - außer
    1. `192.168.0.0` (= `0xC0A80000`) - `192.168.255.255` (= `0xC0A8FFFF`) :- privat
4. Adressen aus **Klasse-D-Netzen** = Multicastadressen / dürfen nicht als Rechneridentifikatoren genutzt werden
5. Adressen aus **Klasse-E-Netzen** = Testadressen / dürfen nicht ins Internet geroutet werden.

Legende:

- **frei routbar** :- können netzübergreifend als IP-Adresse / 'Rechnername' verwendet werden

- **privat** :- dürfen Adressen in einem privaten Netz eingesetzt, aber nicht ins Internet geroutet werden
- **superrivat** :- dürfen innerhalb eines Rechners als Loopbackadressen für seine Interfaces eingesetzt, aber nicht nach außen geroutet werden, auch nicht in private Netze
- **APIPA** :- steht für *Automatic Private IP Addressing*. Erlaubt Rechnern beim DHCP-Ausfall eine Adresse aus diesem Pool zu nehmen. Doppelte IP-Adresse werden in Kauf genommen: besser als gar nicht kommunizieren zu können.

IPv4-Adressen werden

- von der **IANA** (= Internet Assigned Numbers Authority https://www.iana.org/) (meist blockweise) an *Registrare* vergeben
- von **Registraren** als Blöcke an *Provider* weitergereicht
- von **Providern** einzeln, als Mengen oder als Blöcke (an Kunden) weitergereicht

Regeln:

- Wer einen IPv4-Adressblock delegiert,
  - spezifiziert den Block mittels der (Sub)Netzwerkadresse und der zugehörigen (Sub)Netzmaske
  - stellt via IP-Adresse u.a. ein Gateway zur Verfügung, an den Router aus dem verteilten Adressbereich ihre unzustellbaren 'Weiterleitungsaufträge' abgeben können.
- Wer einen IPv4-Adressblock empfängt, darf
  - diesen weiter segmentieren.
  - die neuen Segmente weiterreichen (Netzwerkadresse + erweiterte Subnetzmaske), sofern er seinen 'Kunden' ein Gateway anbietet.

2) IPv4-Segmentierung [→ ZP:Sheet:5]

- Ausgangspunkt einer Segmentierung sind Netzadresse und Subnetzmaske:
  - z.B. `192.168.1.0/24` bzw.
  - `192.168.1.0 & 255.255.255.0`
- Subnetze können nur in `2^x`-Segmente vom Netzbereich abgespalten werden:
  - z.B. `192.168.1.0/25` bzw. `192.168.1.0 & 255.255.255.128`
  - z.B. `192.168.1.128/25` bzw. `192.168.1.128 & 255.255.255.128`

Was bedeutet das? [→ ZP:Sheet:6]

- Eine **symmetrische Netzwerksegmentierung** teilt den Adressbereich in gleich große Subnetze auf.
- Eine **asymmetrische Netzwerksegmentierung** spaltet vom verbliebenen Adressbereich verschieden große Subnetze je einer Größe von `2^n` ab:
  - Zuerst den größten Bereich abspalten;
  - danach sukzessive die je kleineren Bereiche
- Die Anzahl der in einem Subnetz prinzipiell zuweisbaren IPv4-Adressen ist `2^n - 2`:
  - Netzadresse und Broadcastadresse dürfen nicht zugewiesen werden.
- Das kleinste sinnvoll abspaltbare Subnetz hat die Größe `2^2` mit
  - 1 Netzadresse
  - 1 Broadcastadresse
  - 1 Router-/Gatewayadresse
  - 1 Adresse für einen Arbeitsrechner

Beispiel im großen Aufriss [→ ZP:Sheet:7]

- Klasse C-Netz `192.168.42.y` aufgespalten in `1 \25` und `2 \26` Subnetze
  - `192.168.42.0/25`
  - `192.168.42.128/26`
  - `192.168.42.192/26`
- Achtung:
  - Aufspaltung hat nichts mit Hopping zu tun

Segmentierung als Prozess: [→ ZP:Sheet:8]

- **Step 1**: **Initiale Bedarfsanalyse** + Segmentierungshypothese:
  - *Heuristik A*: Rechner, die viel miteinander kommunizieren, gehören in dieselbe Broadcastdomäne! *(Denn jedes Hopping verlangsamt die Kommunikation, weil dabei zusätzlich Layer-3-Berechnungen nötig werden)*
  - *Heuristik B*: Rechner, denen der Zugriff auf eine andere Broadcastdomäne mittels Firewallregeln erlaubt bzw. verboten werden soll, gehören in dieselbe Broadcastdomäne! *(Denn aufgesplittete Firewallregeln, die auf einzelne Rechner zugreifen, verlangsamen die Zugriffsberechnung. Und sie erschweren Netzwerkupdates)*
  - *Aber:* Wenn A+B nicht gemeinsam erfüllbar sind, finde die kleinste mögliche Abweichung.
- **Step 2**: **Netzwerkdesign**

  - mit dem **MVP** (Minimal Viable Product) beginnen
  - sukzessive Anforderungen hinzufügen

- **Step 3**: Netzwerkdesign bedingte **Bedarfsbereinigung**
- **Step 4**: **Adressinstantiierung**

Hinweis:

1. Eine korrekte **Segmentierung** verlängert die gegebene Subnetzmake (Bits hinzufügen):
    1. Sie darf diese nie verkürzen (Bits aus der gegebenen Maske entfernen (damit im Netz keine Dubletten von IP-Adressen auftreten.)
    2. = *CIDR-Suffix* nur erhöhen, nicht verringern.
2. Wer wie viele 'Gatewayrouter' wem mit welcher Verfügbarkeit zur Verfügung stellt, ist eine Frage der je bilateralen Verträge:
    1. Der oberstere Provider könnte alle Router aus allen neu segmentierten Subnetzen in sein übergeordnetes Netzmit mit Gateway einbinden.
    2. Der oberstere Provider könnte seinem Kunden, der Subnetze heraussegmentiert, anbieten, einen speziellen Kunden-Router bei sich einzubinden: Dann bräuchte der Segmentierer ein gesondertes Netz, in das alle Router seiner Subnetze als normalen Mitglieder eingebunden sind und in dem der Kunden-Router als Gateway fungiert.

ÜBUNG LF09:10:Segmentierung:01

Nehmen wir an, ich hätte überraschend doch noch 256 routbare, unverbrauchte IPv4-Adressen 'gefunden', nämlich `192.110.0.0/24`. Die würde ich dann gerne in Teilblöcken an Sie weitergeben:

- ☐ Segmentieren Sie die Bereiche so, dass
    - ☐ ich ein kleines Verwaltungsnetz bekomme, in das ich meinen Router nach außen als Gateway für innen, einen eigenen Rechner und die je für Ihre Subnetze zuständigen Router einbinden kann
    - ☐ jeder von Ihnen ein möglichst großes Subnetz bekommt
- ☐ Erstellen Sie mit *drawio* ein Netzdiagramm. Geben Sie dabei alle Netzspezifikatoren und verwendeten IPv4-Adressen an.

ÜBUNG LF09:10:Segmentierung:02

[→ ZP:Sheet:9]

Setzen Sie bitte für Ihre Firma ein IPv4-basiertes Netzwerk auf. Ihre Firma hat dazu folgende Eigenarten und Wünsche:

1. Im Bereich 'Finance' arbeiten 5 Mitarbeiterinnen mit je 1 Rechner. Zusammen nutzen sie 1 Server als ihren Datenhost
2. Im Bereich HR arbeiten 3 Mitarbeiterinnen mit je 1 Rechner. Sie legen ihre Daten auf 3 bereichseigenen Servern ab.
3. In der Geschäftsleitung arbeiten 5 Personen mit je 1 Rechner.
4. In der Softwareentwicklung arbeiten 10 Entwicklerinnen mit je 2 Rechnern.
5. In der Produktion stehen 5 Server. Sie stellen die Services für Kunden bereit.
6. In den Bereichen Finance, HR, Geschäftsleitung und Softwareentwicklung können die jeweiligen Mitarbeiterinnen jeweils auf alle bereichseigenen Rechner zugreifen.
7. Die Geschäftsleitung kann jeden Firmenrechner kontaktieren, außer denen in Finance und Production
8. Die Softwareentwicklerinnen können auf die Production-Rechner Software aufspielen.
9. Die Firma rechnet damit, im nächsten Jahr in allen Bereichen um je 100% zu wachsen. Im übernächsten sollen jeweils nochmals 50% des heutigen Wertes hinzukommen.
10. Alle Server können ohne Änderung auch die hinzukommenden Mitarbeiterinnen bedienen.
11. Die Firma möchte sicherheitshalber 2 Gateways ins Internet haben, eines für die Produktionsrechner, eines für die Rechner der Mitarbeiterrinnen. Dafür hat sie 2 öffentliche IPv4-Adressen organisiert.
12. Die Firma möchte zwecks Komplexitätsreduktion nur höchstens 256 private IPv4-Adressen verwenden.
13. Die Firma möchte außerdem ein einziges, räumlich übergreifendes WLAN für alle Mitarbeiterinnen bereitstellen. Sie geht davon aus, dass jeder 2 WLAN-fähige Geräte mitbringt (BYOD). Alle anderen o.a. Rechner sind ans LAN angeschlossen.

Bitte planen Sie ein Netz, dass die Wünsche durch eine geeignete Segmentierung samt dazu passender Router-Gateway-Vernetzung unterstützt:

- Nehmen Sie an, dass jeder Router einen Außenport, einen Switch mit 64 Binnenports und eine Firewall enthält.
- Markieren Sie, wo und wozu ggfls. Firewalls aktiviert werden sollten.
- Setzen Sie dabei voraus, dass die Firewalls mindestens einzelne Rechner anhand ihrer IPv4-Adressen und Rechnergruppen anhand ihrer Netzadresse aussperren oder zulassen können.

Lösung:

LF09:02:02 [→ ZP:Sheet:10] Initiale Bedarfsanalyse

- *Abkürzungen*
  - **E** = Employees / Mitarbeiter
  - **S** = Server
  - **Ad** = Number of department specific addresses
  - **As** = Number of additionally structurally required addresses
  - **SEG** = Type of segmentation
- *Berechnungen*
  - Die Summe der fachlich benötigten IP-Adressen Ad ergibt sich per

```
(Anzahl_Mitarbeiter * Faktor_Mitarbeiterrechner) + Anzahl_Bereichserver
```

- Wenn jeder Bereich sein eigenes Subnetz haben soll, muss zur fachlichen bedingten Zahl noch die Zahl der strukturell nötigen Adressen(Netzwerkadresse, Broadcastadresse, mindestens 1 Routeradresse) addiert werden, um die Anzahl der von einem Bereich insgesamt benötigten IP-Adressen zu erhalten.
- Außerdem muss die Anzahl der pro Bereichsnetz aus Gründen des Netzwerkdesigns zusätzlich notwendigen Router eingerechnet werden.
- *Herausforderungen*
  - 1.) Der Ansatz, jedem Bereich sein eigenes Netz zu geben, ist der 2^x-Regel wegen mit den gewünschten Werten in einem Klasse-C-Netz nicht unerfüllbar.
  - 2.) Durch zusätzliche Vernetzungen der Subnetze mittels zusätzlicher Router kann sich die Anzahl der insgesamt benötigten IP-Adressen je nach Netzwerkdesign noch erhöhen.

→ Das Netzwerkdesign wird zu einem mehrstufigen, iterativen Prozess.

LF09:02:02 [→ ZP:Sheet:11] initiales Netzwerkdesign

- *Minimal Viable Product* : 1 Core-Netz, alle Rechner im Core-Netz, 1 Router im Core-Netz mit Hopping heraus ins Internet (Core-Dateway).
- *Erweiterungen*:
  - 1.) HR kriegt eigenes Netz → 1 HR-Netz dazu, alle HR-Rechner im HR-Netz, 1 HR-Router mit Hopping ins Core-Netz (nicht direkt ins Internet, weil nur 2 routbare IP-Adressen)
  - …
  - n.) DEV kriegt eigenes Netz → 1 DEV-Netz dazu, alle DEV-Rechner im DEV-Netz, 1 DEV-Router mit Hopping ins Core-Netz

  - m.) PROD kriegt eigenes Netz → 1 PROD-Netz dazu, alle PROD-Rechner im PROD-Netz, 1 PROD-Router mit Hopping ins ?UPPS?:
    * A) CORE2-NETZ dazu, 1 Router im Core2-Netz mit Hopping heraus in Internet (CORE2-Gateway)
    * B) PROD-Router auch ins CORE2-Netz, aber NICHT im CORE1-Netz
  - X:) 2. Router in DEV mit Interface nach PROD
  - Z:) Goldplating: Router in MNG mit Interface nach HR und DEa etc.

LF09:02:02 [→ ZP:Sheet:12] Bereinigte Bedarfsanalyse

- *Abkürzungen*
  - **E** = Employees / Mitarbeiter
  - **S** = Server
  - **Ad** = Number of department specific addresses
  - **As** = Number of additionally structurally required addresses
  - **As** = Number of additionally added secondary routers
  - **SEG** = Type of segmentation
- *Berechnungen* (s.o.)
- *Lösung der Herausforderungen*
  - Im WLAN können bei dieser Lösung gleichzeitig nur etwa so viele WLAN-Geräte eingeloggt sein, wie es Mitarbeiter gibt.
    * Da erfahrungsgemäß nicht alle Mitarbeiter wirklich 2 Geräte haben und nicht alle Mitarbeiter immer vor Ort sind, sollte das funktionieren.
    * Dafür werden dann alle anderen Anforderung erfüllt.
  - Andere Lösungen dafür sind ebenso möglich
    * Der Wachstum wird mit einem Faktor über alle Bereiche entsprechend beschränkt.
    * Das WLAN- und das Development-Subnetz werden so designt, dass sie nur den aktuellen Bedarf abdecken. Die unverbrauchten IP-Adressen kommen in einen Pool, aus dem dann je nach tatsächlichem Bedarf ein WLAN2- und eine Development2-Netz abgespalten wird.
  - Die Zugriffe müssen zusätzlich zu Netzwerkstruktur per Firewall-Regeln in den zuständigen Routern begrenzt werden.

LF09:02:02 [→ ZP:Sheet:13] Adressinstantiierung

LF09:02:02 [→ ZP:Sheet:14] Finales Netzwerkdesign

