Lösung von Übungsblatt 10

Aufgabe 1 (Router, Layer-3-Switch, Gateway)

1. Beschreiben Sie den Zweck von **Routern** in Computernetzen.
(*Erklären Sie auch den Unterschied zu Layer-3-Switches.*)

   Router verbinden logische Netze. Zudem ermöglichen Sie die Verbindung des lokalen Netzes (LAN) mit einem WAN.

2. Beschreiben Sie den Zweck von **Layer-3-Switches** in Computernetzen.
(*Erklären Sie auch den Unterschied zu Routern.*)

   Layer-3-Switches verbinden logische Netze. Sie werden aber nur innerhalb lokaler Netze verwendet, um verschiedene logischen Adressbereiche zu realisieren. Sie ermöglichen keine Verbindung mit einem WAN.

3. Beschreiben Sie den Zweck von **Gateways** in Computernetzen.

   Gateways sind Protokollumsetzer. Sie ermöglichen Kommunikation zwischen Netzen, die auf unterschiedlichen Protokollen basieren und/oder unterschiedliche Adressierung verwenden.

4. Erklären Sie warum **Gateways** in der Vermittlungsschicht von Computernetzen heutzutage selten nötig sind.

   Moderne Computernetze arbeiten fast ausschließlich mit dem Internet Protocol (IP). Darum ist eine Protokollumsetzung auf der Vermittlungsschicht meist nicht nötig.

Aufgabe 2 (Adressierung mit IPv4)

1. Erklären Sie die Bedeutung von **Unicast** in der Vermittlungsschicht.

   Eine IP-Adresse ist einem einzelnen Empfänger zugewiesen.

2. Erklären Sie die Bedeutung von **Broadcast** in der Vermittlungsschicht.

   Über eines solche IP-Adresse werden alle Empfänger im Subnetzes erreicht.

3. Erklären Sie die Bedeutung von **Anycast** in der Vermittlungsschicht.

   Eine IP-Adresse wird verwendet, um ein einzelnes Gerät aus einer Gruppe von Geräten anzusprechen.

4. Erklären Sie die Bedeutung von **Multicast** in der Vermittlungsschicht.

   Eine IP-Adresse ist einer Gruppe von Empfängern zugewiesen.

5. Erklären Sie warum der **IPv4-Adressraum** nur 4.294.967.296 Adressen enthält.

   IPv4-Adressen sind 32 Bits (4 Bytes) lang. Daher können $2^{32} = 4.294.967.296$ Adressen dargestellt werden.

6. Erklären Sie warum das klassenlose Routing – **Classless Interdomain Routing (CIDR)** eingeführt wurde.

   Netzklassen verschwenden viele Adressen und es sie können nicht dynamisch an Veränderungen angepasst werden.

7. Beschreiben Sie in einfachen Worten die **Funktionsweise von CIDR**.
   Legen Sie den Schwerpunkt auf die Art und Weise, wie IP-Adressen behandelt und Subnetze erstellt werden.

   CIDR beschreibt die Unterteilung logischer Netze in Teilnetze (Subnetze). Alle Knoten in einem Netzwerk bekommen eine 32 Bits (4 Bytes) lange Netzmaske zugewiesen. Mit ihr wird die Anzahl der Subnetze und Hosts festgelegt. Die Netzmaske unterteilt die Hostadresse der IP-Adresse in Subnetznummer und Hostadresse. Einsen kennzeichnen den (Sub-)Netz-Nummernteil eines Adressraumes. Nullen kennzeichnen den Teil des Adressraumes, der für die Hostadressen zur Verfügung steht.

Aufgabe 3 (Adressierung mit IPv4)

Berechnen Sie für jede Teilaufgabe die **erste und letzte Hostadresse**, die **Netzadresse** und die **Broadcast-Adresse** des Subnetzes.

```
IP-Adresse:          151.175.31.100   10010111.10101111.00011111.01100100
Netzmaske:           255.255.254.0    11111111.11111111.11111110.00000000
Netzadresse?         151.175.30.0     10010111.10101111.00011110.00000000
Erste Hostadresse?   151.175.30.1     10010111.10101111.00011110.00000001
Letzte Hostadresse?  151.175.31.254   10010111.10101111.00011111.11111110
Broadcast-Adresse?   151.175.31.255   10010111.10101111.00011111.11111111

IP-Adresse:          151.175.31.100   10010111.10101111.00011111.01100100
Netzmaske:           255.255.255.240  11111111.11111111.11111111.11110000
Netzadresse?         151.175.31.96    10010111.10101111.00011111.01100000
Erste Hostadresse?   151.175.31.97    10010111.10101111.00011111.01100001
Letzte Hostadresse?  151.175.31.110   10010111.10101111.00011111.01101110
Broadcast-Adresse?   151.175.31.111   10010111.10101111.00011111.01101111
```

```
IP-Adresse:          151.175.31.100   10010111.10101111.00011111.01100100
Netzmaske:           255.255.255.128  11111111.11111111.11111111.10000000
Netzadresse?         151.175.31.0     10010111.10101111.00011111.00000000
Erste Hostadresse?   151.175.31.1     10010111.10101111.00011111.00000001
Letzte Hostadresse?  151.175.31.126   10010111.10101111.00011111.01111110
Broadcast-Adresse?   151.175.31.127   10010111.10101111.00011111.01111111
```

binäre Darstellung	dezimale Darstellung	binäre Darstellung	dezimale Darstellung
10000000	128	11111000	248
11000000	192	11111100	252
11100000	224	11111110	254
11110000	240	11111111	255

Aufgabe 4 (Adressierung mit IPv4)

In jeder Teilaufgabe überträgt ein Sender ein IP-Paket an einen Empfänger. Berechnen Sie für jede Teilaufgabe die **Subnetznummern von Sender und Empfänger** und geben Sie an, ob das IP-Paket **während der Übertragung das Subnetz verlässt** oder nicht.

```
Sender:      11001001.00010100.11011110.00001101    201.20.222.13
Netzmaske:   11111111.11111111.11111111.11110000    255.255.255.240
             ----------------------------------
                                      0000        => 0

Empfänger:   11001001.00010100.11011110.00010001    201.20.222.17
Netzmaske:   11111111.11111111.11111111.11110000    255.255.255.240
             ----------------------------------
                                      0001        => 1
```

```
Subnetznummer des Senders? 0

Subnetznummer des Empfängers? 1

Verlässt das IP-Paket das Subnetz [ja/nein]? ja
```

```
Sender:       00001111.11001000.01100011.00010111    15.200.99.23
Netzmaske:    11111111.11000000.00000000.00000000    255.192.0.0
              ----------------------------------
                        11                           => 3

Empfänger:    00001111.11101111.00000001.00000001    15.239.1.1
Netzmaske:    11111111.11000000.00000000.00000000    255.192.0.0
              ----------------------------------
                        11                           => 3

      Subnetznummer des Senders? 3

      Subnetznummer des Empfängers? 3

      Verlässt das IP-Paket das Subnetz [ja/nein]? nein
```

Aufgabe 5 (Adressierung mit IPv4)

Berechnen Sie für jede Teilaufgabe **Netzmaske** und beantworten Sie die **Fragen**.

1. Teilen Sie das Klasse C-Netz `195.1.31.0` so auf, das 30 Subnetze möglich sind.

`Netzadresse:` `11000011.00000001.00011111.00000000` `195.1.31.0`
`Anzahl Bits für Subnetznummern?` 30 Subnetze $\Longrightarrow$ 32 Adressen $= 2^5 \Longrightarrow$ 5 Bits für Subnetze
`Netzmaske:` `11111111.11111111.11111111.11111000` `255.255.255.248`
`Anzahl Bits für Hostadressen?` 3
`Anzahl Hostadressen pro Subnetz?` $2^3 = 8$. Davon sind zwei Adressen (Broadcast-Adresse und Netzdeskriptor) nicht nutzbar.

2. Teilen Sie das Klasse A-Netz `15.0.0.0` so auf, das 333 Subnetze möglich sind.

`Netzadresse:` `00001111.00000000.00000000.00000000` `15.0.0.0`
`Anzahl Bits für Subnetznummern?` 333 Subnetze $\Longrightarrow$ 512 Adressen $= 2^9 \Longrightarrow$ 9 Bits für Subnetze
`Netzmaske:` `11111111.11111111.10000000.00000000` `255.255.128.0`
`Anzahl Bits für Hostadressen?` 15
`Anzahl Hostadressen pro Subnetz?` $2^{15} = 32768$. Davon sind zwei Adressen (Broadcast-Adresse und Netzdeskriptor) nicht nutzbar.

3. Teilen Sie das Klasse B-Netz `189.23.0.0` so auf, das 20 Subnetze möglich sind.

`Netzadresse:` `10111101.00010111.00000000.00000000` `189.23.0.0`
`Anzahl Bits für Subnetznummern?` 20 Subnetze $\Longrightarrow$ 32 Adressen $= 2^5 \Longrightarrow$ 5 Bits für Subnetze
`Netzmaske:` `11111111.11111111.11111000.00000000` `255.255.248.0`
`Anzahl Bits für Hostadressen?` 11
`Anzahl Hostadressen pro Subnetz?` $2^{11} = 2048$. Davon sind zwei Adressen (Broadcast-Adresse und Netzdeskriptor) nicht nutzbar.

4. Teilen Sie das Klasse C-Netz `195.3.128.0` in Subnetze mit je 17 Hosts auf.

`Netzadresse:` `11000011.00000011.10000000.00000000` `195.3.128.0`
`Anzahl Bits für Hostadressen?` 17 Hosts $\Longrightarrow$ 32 Adressen $= 2^5 \Longrightarrow$ 5 Bits für Hosts
`Anzahl Bits für Subnetznummern?` $8 - 5 = 3$ Bit für Subnets
`Anzahl möglicher Subnetze?` $2^3 = 8$
`Netzmaske:` `11111111.11111111.11111111.11100000` `255.255.255.224`

5. Teilen Sie das Klasse B-Netz `129.15.0.0` in Subnetze mit je 10 Hosts auf.

`Netzadresse:` `10000001.00001111.00000000.00000000` `129.15.0.0`
`Anzahl Bits für Hostadressen?` 10 Hosts $\Longrightarrow$ 16 Adressen $= 2^4 \Longrightarrow$ 4 Bits für Hosts
`Anzahl Bits für Subnetznummern?` $16 - 4 = 12$ Bit für Subnets
`Anzahl möglicher Subnetze?` $2^{12} = 4096$
`Netzmaske:` `11111111.11111111.11111111.11110000` `255.255.255.240`

binäre Darstellung	dezimale Darstellung	binäre Darstellung	dezimale Darstellung
10000000	128	11111000	248
11000000	192	11111100	252
11100000	224	11111110	254
11110000	240	11111111	255

Aufgabe 6 (Private IP-Adressbereiche)

Nennen Sie die drei privaten IP-Adressbereiche.

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Aufgabe 7 (IPv6)

1. Erklären Sie das Konzept der Scopes in IPv6. *IPv6 unterscheidet nicht nur zwischen privaten und öffentlichen Adressen (wie IPv4), sondern auch mehrere Gültigkeitsbereiche (sog. Scopes). Der Gültigkeitsbereich ist der Teil eines Netzes, in dem die zugehörige Adresse als gültig betrachtet und weitergeleitet wird.*

2. Erklären, was der Host-Scope ist.

   Der Host Scope umfasst die Loopback-Adresse `::1/128`.

3. Erklären Sie, was der Link-Local Scope ist.

   Der Link-Local-Bereich umfasst Link-Local (Unicast)-Adressen (LLA). Jede Netzwerkschnittstelle benötigt zu jeder Zeit eine Link-Local-Adresse. Link-Local-Adressen fe80::/10 sind nur im lokalen Netz gültig. Router leiten keine Pakete mit diese Adressen weiter.

4. Erklären Sie, was der Unique-Local Scope ist.

   Der Unique-Local-Bereich umfasst Unique Local Addresses (ULA). Router sollten Pakete mit diesen Adressen nicht außerhalb des lokalen Verwaltungsbereichs (Organisation oder Standort) weiterleiten. Es handelt sich um private Adressen, die für die lokale Kommunikation innerhalb einer administrativen Domäne gedacht sind, aber global gültig (eindeutig) sein können, wenn sie von einem Anbieter zugewiesen werden. Lokal generierte ULA sind höchstwahrscheinlich eindeutig.

5. Erklären Sie, was der Global Scope ist.

   Der globale Bereich umfasst globale Unicast-Adressen. Router leiten Pakete mit diesen Adressen weiter.

6. Geben Sie an, was die IPv6-Adresse `::1/128` anspricht.

   Es ist die Loopback-Adresse.

7. Geben Sie den Namen des Bereichs der IPv6-Adresse `::1/128`.

   Host Scope.

8. Geben Sie den Namen des Bereichs der Adressen mit dem Präfix `fe80::/10`.

   Link-Local Scope.

9. Geben Sie den Namen des Bereichs der Adressen mit dem Präfix `fc00::/7`.

   Unique-Local Scope.

10. Geben Sie den Namen des Bereichs der Adressen mit dem Präfix `2000::/3`.

    Global Scope.

11. IPv6 hat keine Broadcast-Adressen, aber für einige Zwecke ist eine Broadcast-ähnliche Funktionalität erforderlich. Erklären Sie, wie IPv6 die Broadcast-Funktionalität emuliert.

    In IPv6 werden Multicast-Adressen verwendet, um die Broadcast-Funktionalität zu emulieren. Die Adresse `ff02::1` hat den Link-Local Scope und adressiert alle Knoten im lokalen Netz.

12. Geben Sie das Präfix von Multicast-Adressen an.

    Bei Multicast-Adressen haben die ersten 8 Bits den Wert `11111111`. Sie haben also das Multicast-Präfix `ff::/8`.

13. Nennen Sie drei Möglichkeiten zur Konfiguration der Schnittstellen-ID.

    - *Statische manuelle Adressierung*
    - *Zustandslose automatische Adresskonfiguration – Stateless Address Autoconfiguration (SLAAC)*
    - *Netzwerkkonfiguration via DHCPv6*

14. Erklären Sie, was Stable Privacy Addresses ist und warum es manchmal im Zusammenhang mit der Konfiguration der Interface-ID verwendet wird.

    Stable Privacy ist eine optionale Erweiterung von SLAAC (Stateless Address Autoconfiguration). Es definiert die Adressgenerierung ohne Verwendung einer MAC-Adresse. Ein zufälliger geheimer Schlüssel wird erstellt und für die Generierung der Interface-ID verwendet. Der geheime Schlüssel ist eine 128-Bit lange hexadezimale Zeichenfolge, die aussieht wie eine IPv6-Adresse.

    Ein Vorteil (im Vergleich zu SLAAC) ist verbesserte Sicherheit, da keine MAC-Adresse für die Erzeugung verwendet wird. Die MAC-Adresse des Knotens wird nicht preisgegeben. Dies ermöglicht Anonymität.

    Ein weiterer Vorteil (im Vergleich zu Privacy Extension) ist, dass die Adresse des Knotens stabil ist. Einmal generiert, ändert sich die Schnittstellen-ID bis zum Neustart nicht mehr.

15. Erläutern Sie, was Privacy Extension ist und warum sie manchmal im Zusammenhang mit der Konfiguration der Interface-ID verwendet wird.

    Privacy Extension ist eine weitere optionale Erweiterung von SLAAC (Stateless Address Autoconfiguration). Die Interface-ID wird nur vorübergehend verwendet. Eine neue Interface-ID wird in regelmäßigen Zeitabständen erzeugt. Alte Interface-IDs bleiben für bestehende Verbindungen gültig.

Ein Vorteil (im Vergleich zu SLAAC) ist verbesserte Sicherheit, da keine MAC-Adresse für die Generierung verwendet wird. Die MAC-Adresse des Knotens wird nicht offengelegt. Dies ermöglicht Anonymität. Und da regelmäßig eine neue Interface-ID generiert wird, ist der Grad der Anonymität im Vergleich zu Stable Privacy noch besser.

Ein Nachteil ist, dass die Adresse verfällt. Sie ist nicht stabil.

16. Wenn ein Knoten eine Interface-ID über SLAAC erstellt hat, muss er sicherstellen, dass kein anderer Knoten im Netz die gleiche Interface-ID hat. Erklären Sie, wie dies in der Praxis gemacht wird.

    Wenn ein Knoten eine IPv6-Adresse für sich selbst generiert hat, muss er überprüfen, dass kein anderer Knoten im Netz diese Adresse bereits verwendet. Dieser Vorgang heißt Duplicate Address Detection (DAD). Der Knoten sendet eine Neighbor Solicitation (NS)-Nachricht an die Adresse, die er selbst verwenden möchte. Die Absenderadresse ist die unspezifische Adresse (`::` ($\Longrightarrow$ 128 Null-Bits). Wenn ein Knoten im lokalen Netz die IP-Adresse bereits verwendet, handelt es sich um ein Duplikat. Der Knoten antwortet mit einer Neighbor Advertisement (NA)-Nachricht, die an die Link-Local-Multicast-Adresse `FF02::1` gesendet wird (jeder Knoten im lokalen Netz erhält diese Nachricht). Der Knoten, der die Neighbor Solicitation (NS) Nachricht gesendet hat, muss eine neue Adresse generieren und die Duplicate Address Detection erneut durchführen. Wird für eine gewisse Zeit keine Neighbor Advertisement (NA)-Nachricht empfangen , kann die Adresse verwendet werden ($\Longrightarrow$ kein Duplikat).

17. Geben Sie eine kurze Erklärung für einen konkreten Anwendungsfall der ICMPv6-Nachricht Router Advertisement (RA) in der Praxis.

    Router senden in regelmäßigen Abständen (die Zeit kann in der Benutzeroberfläche eingestellt werden) Router Advertisement (RA)-Nachrichten in verbundene Netzwerke, um über ihre Anwesenheit, das Netzwerk-Präfix, die Präfix-Länge und u.a., die MTU zu informieren. Die Zieladresse im IPv6-Paket ist die Link-Local Multicast-Adresse `FF02::1`, um alle Knoten im lokalen Netz zu erreichen.

18. Geben Sie eine kurze Erklärung für einen konkreten Anwendungsfall der ICMPv6-Nachricht Router Solicitation (RS) in der Praxis.

    Wenn ein Knoten nicht auf eingehende Router Advertisement (RA)-Nachrichten warten möchte, kann er RA-Nachrichten anfordern, indem er RS-Nachrichten sendet. Die Zieladresse im IPv6-Paket ist die Link-Local Multicast-Adresse `FF02::2`, um alle Router im lokalen Netz zu erreichen.

19. Geben Sie eine kurze Erläuterung für einen konkreten Anwendungsfall der ICMPv6-Nachricht Neighbor Solicitation (NS) in der Praxis.

Die Nachricht Neighbor Solicitation (NS) ist die IPv6-Alternative zu einer ARP-Anfrage bei Verwendung von IPv4. Sie wird verwendet, um die MAC-Adresse eines Nachbarn anzufordern.

20. Geben Sie eine kurze Erklärung für einen konkreten Anwendungsfall der ICMPv6-Nachricht Neighbor Advertisement (NA) in der Praxis.

    Die Nachricht Neighbor Advertisement (NA) ist die IPv6-Alternative zu einer ARP-Antwort bei Verwendung von IPv4. Sie wird verwendet, um auf eine Neighbor Solicitation (NS)-Nachricht zu antworten (Senden der MAC-Adresse einer IPv6-Adresse).

21. Erklären Sie, wie ein Knoten erfährt, ob er einen DHCPv6-Server für die Anforderung einer Adresskonfiguration verwenden soll (zustandsabhängige Adresskonfiguration) oder ob er eine Interface-ID selbst erstellen darf (zustandslose Adresskonfiguration).

    Die in regelmäßigen Abständen gesendete Nachricht Router Advertisement (RA) enthält u.a. das Flag `managed`*. Wenn es gesetzt ist, soll der Client die Adresse nicht zustandslos einstellen, sondern die Adresskonfiguration von einem DHCPv6-Server (zustandsabhängig) anfordern.*

Aufgabe 8 (IPv6 – Adressen vereinfachen)

1. Vereinfachen Sie die folgende IPv6-Adressen:

   - `1080:0000:0000:0000:0007:0700:0003:316b`

     Lösung: `1080:7:700:3:316b`

   - `2001:0db8:0000:0000:f065:00ff:0000:03ec`

     Lösung: `2001:db8::f065:ff:0:3ec`

   - `2001:0db8:3c4d:0016:0000:0000:2a3f:2a4d`

     Lösung: `2001:db8:3c4d:16::2a3f:2a4d`

   - `2001:0c60:f0a1:0000:0000:0000:0000:0001`

     Lösung: `2001:A60:F0A0::1`

   - `2111:00ab:0000:0004:0000:0000:0000:1234`

     Lösung: `2111:ab:0:4::1234`

2. Geben Sie alle Stellen der folgenden vereinfachten IPv6-Adressen an:

   - `2001::2:0:0:1`

Lösung: `2001:0000:0000:0000:0002:0000:0000:0001`

- `2001:db8:0:c::1c`

  Lösung: `2001:0db8:0000:000c:0000:0000:0000:001c`

- `1080::9956:0:0:234`

  Lösung: `1080:0000:0000:0000:9956:0000:0000:0234`

- `2001:638:208:ef34::91ff:0:5424`

  Lösung: `2001:0638:0208:ef34:0000:91ff:0000:5424`

- `2001:0:85a4::4a1e:370:7112`

  Lösung: `2001:0000:85a4:0000:0000:4a1e:0370:7112`