

Protokoll-Header Analyse

June 18, 2024

Aufgabe 1: Protokoll-Header

IPv4-Paket-Analyse

Filter: ip

Gefundenes IPv4-Paket:

```
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 52
  Identification: 0x0000 (0)
  010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 127.0.0.1
  Destination Address: 127.0.0.1
```

IPv4-Header-Kategorien:

- **Version:** 4
- **Header Length:** 20 bytes (5 words)
- **Type of Service (ToS):** 0x00
- **Total Length:** 52
- **Identification:** 0x0000 (0)
- **Flags:** 0x2 (Don't fragment)
- **Fragment Offset:** 0
- **Time to Live (TTL):** 64
- **Protocol:** TCP (6)
- **Header Checksum:** 0x0000 (unverified)
- **Source Address:** 127.0.0.1
- **Destination Address:** 127.0.0.1

UDP-Paket-Analyse

Filter: udp

Gefundenes UDP-Paket:

User Datagram Protocol, Src Port: 12345, Dst Port: 80

Source Port: 12345

Destination Port: 80

Length: 32

Checksum: 0x1f2e

UDP-Header-Kategorien:

- **Source Port:** 12345
- **Destination Port:** 80
- **Length:** 32
- **Checksum:** 0x1f2e

TCP-Paket-Analyse

Filter: tcp

Gefundenes TCP-Paket:

Transmission Control Protocol, Src Port: 49255, Dst Port: 58356, Seq: 1, Ack: 1, Len: 0

Source Port: 49255

Destination Port: 58356

Sequence Number: 1 (relative sequence number)

Acknowledgment Number: 1 (relative ack number)

1000 = Header Length: 32 bytes (8)

Flags: 0x010 (ACK)

.... 0... = Acknowledgment: Set

Window: 6379

Checksum: 0xfe28 [unverified]

Urgent Pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

TCP Option - No-Operation (NOP)

Kind: No-Operation (1)

TCP Option - No-Operation (NOP)

Kind: No-Operation (1)

TCP Option - Timestamps: TSval 3801576600, TSecr 2818559571

Kind: Time Stamp Option (8)

Length: 10

Timestamp value: 3801576600

Timestamp echo reply: 2818559571

TCP-Header-Kategorien:

- **Source Port:** 49255
- **Destination Port:** 58356
- **Sequence Number:** 1 (relative sequence number)
- **Acknowledgment Number:** 1 (relative acknowledgment number)
- **Data Offset:** 32 bytes (8 words)
- **Flags:** 0x010 (ACK)
- **Window:** 6379
- **Checksum:** 0xfe28 (unverified)
- **Urgent Pointer:** 0
- **Options:** No-Operation (NOP), Timestamps (TSval 3801576600, TSecr 2818559571)

Aufgabe 2: CIDR

Die Notation 103.161.122.83/18 ist eine CIDR (Classless Inter-Domain Routing)-Notation. Im Folgenden werden die einzelnen Bestandteile und die Berechnung der Subnetzmaske, Broadcastadresse und Netzwerkadresse beschrieben.

Beschreibung der CIDR-Notation

- **103.161.122.83:** Dies ist die IP-Adresse des Hosts.
- **/18:** Dies ist die Länge des Netzwerkpräfixes in Bits.

Berechnung der Subnetzmaske

Die Subnetzmaske besteht aus den ersten 18 Bits, die auf 1 gesetzt sind, gefolgt von 14 Bits, die auf 0 gesetzt sind. Dies ergibt die folgende Subnetzmaske:

11111111.11111111.11000000.00000000

In dezimaler Darstellung:

255.255.192.0

Berechnung der Netzwerkadresse

Die Netzwerkadresse erhält man, indem man die Hostadresse bitweise mit der Subnetzmaske UND-verknüpft:

IP-Adresse:	103.161.122.83	-> 01100111.10100001.01111010.01010011
Subnetzmaske:	255.255.192.0	-> 11111111.11111111.11000000.00000000
Netzwerkadresse:	103.161.64.0	-> 01100111.10100001.01000000.00000000

Die Netzwerkadresse lautet also:

103.161.64.0

Berechnung der Broadcastadresse

Die Broadcastadresse erhält man, indem man alle Host-Bits auf 1 setzt. Das bedeutet, dass die ersten 18 Bits der Netzwerkadresse unverändert bleiben und die letzten 14 Bits auf 1 gesetzt werden:

Netzwerkadresse:	103.161.64.0	-> 01100111.10100001.01000000.00000000
Broadcastadresse:	103.161.127.255	-> 01100111.10100001.01111111.11111111

Die Broadcastadresse lautet also:

103.161.127.255

Vergleich der Netzwerke

Liegt 103.161.122.83/18 im selben Netz wie 103.161.193.83/18?

Um dies zu bestimmen, berechnen wir die Netzwerkadresse für 103.161.193.83/18:

IP-Adresse:	103.161.193.83	-> 01100111.10100001.11000001.01010011
Subnetzmaske:	255.255.192.0	-> 11111111.11111111.11000000.00000000
Netzwerkadresse:	103.161.192.0	-> 01100111.10100001.11000000.00000000

Die Netzwerkadresse von 103.161.193.83/18 lautet:

103.161.192.0

Da die Netzwerkadressen von 103.161.122.83/18 (103.161.64.0) und 103.161.193.83/18 (103.161.192.0) unterschiedlich sind, liegen diese beiden IP-Adressen nicht im selben Netzwerk.

Zusammenfassung der Ergebnisse

- **Subnetzmaske:** 255.255.192.0
- **Netzwerkadresse:** 103.161.64.0
- **Broadcastadresse:** 103.161.127.255
- **Netzwerkvergleich:** Die IP-Adresse 103.161.122.83/18 liegt nicht im selben Netzwerk wie 103.161.193.83/18.