Theorie 6
Netzwerkschicht, IP und Sicherungsschicht

Fachgruppe Telekommunikationsnetze (TKN)

24. November 2023

Einleitung

Die folgenden Aufgaben werden gemeinsam im Tutorium bearbeitet. In der Veranstaltung Rechnernetze wird die SI-Notation verwendet. Beispiele für Präfixe: m = 10^{-3}, k = 10^{3}, M = 10^{6}, ki = 2^{10}, Mi = 2^{20}. „B“ bezeichnet Bytes, „bit“ Bits.

Übung 1 *Full-Stack*

Sie haben in der Vorlesung wichtige Komponenten, aus denen das Internet zusammengesetzt ist, kennengelernt. Beantworten Sie in diesem Kontext die folgenden Fragen und machen Sie sich klar, wo die Technologien jeweils verwendet werden:

1. Grenzen Sie die folgenden Begriffe gegeneinander ab. Auf welcherEbene des ISO/OSI Modells arbeiten die jeweiligen Elemente?
   - Repeater
   - Hub
   - Bridge
   - Switch
   - Router
2. Was ist eine IP-Adresse, was eine MAC-Adresse?
3. Welches sind die speziellen IPv4-Adressen für Loopback und (limited) Broadcast?
4. Wie funktioniert ARP?
5. Nennen und erklären Sie die 4 Arten von Delay in einem Netz mit Paket-Vermittlung.
6. Was ist ein Autonomes System (AS)?
7. Was ist der Unterschied zwischen Peering und Transit?

8. Was ist der Unterschied zwischen Routing und Forwarding?

Lösung

1.

Gerät	Schicht	Erläuterung
Repeater	Physical Layer	Reiner digitaler Signalverstärker, kennt nur Bits bzw. Symbole.
Hub	Physical Layer	Verbindet mehrere Eingänge physisch miteinander, sodass sie eine Kollisionsdomäne bilden.
Bridge	Link Layer	Verbindet LANs miteinander. Ports sind physisch voneinander isoliert. Die Netzwerke können unterschiedliche Geschwindigkeiten haben oder andere Protokolle benutzen (z.B. FastEthernet und Token-Ring). Frames werden gepuffert. Bridge lernt selbstständig wohin Frames geschickt werden müssen.
Switch	Link Layer	Unscharf definierte Begriff. Ähnlich zur Bridge (Folien definieren Switch als Oberbegriff) allerdings werden meist Hosts direkt miteinander verbunden anstatt Netzwerke.
Router	Network Layer	Bauen Routing-Tabellen auf und implementieren Routing-Algorithmen.

2.
- Beide adressieren Interfaces, nicht Hosts (mehre MAC/IP Adressen pro Host möglich)
- MAC Adressen benutzen flache Adressierung:
  - Adresse gibt keine Info darüber wo das Gerät ist.
  - Dadurch sind sind sie portabel.
- IP Adressen sind hierarchisch aufgebaut:
  - sie hängen vom Subnetz ab in dem man sich befindet.
  - Somit sind sie nicht portabel.
- MAC Adresse entspricht eher Sozialversicherungsnummer, IP Adressen sind eher wie Postanschriften.

3. Loopback: `127.0.0.1` Broadcast: `255.255.255.255`

4. Alle Hosts bauen eine ARP Tabelle auf mit Inhalt `[IP, MAC, Time-To-Live]`
   a) A sendet ARP Anfrage per Broadcast für die IP von B: `Who is 192.168.1.50?`

b) B antwortet per Unicast mit seiner MAC Adresse: `192.168.1.50 is AB:CD:DE:FF:AB:CD`

c) A speichert MAC Adresse in für Bs IP in seiner ARP-Tabelle bis TTL abläuft.

5. **Processing Delay** Benötigte Zeit um Frames/Pakete überprüfen und zum Bestimmen des korrekten Ausgangs.

   Queuing Delay Zeit, die ein Paket/Frame in Puffern warten muss bis es übertragen werden kann, aufgrund von Stau im Netzwerk.

   Transmission Delay Benötigte Zeit um Frame/Paket zu übertragen. Bestimmt durch Paketlänge und Bandbreite des Links.

   Propagation Delay Benötigte Zeit um den Link zu durchqueren. Nur bestimmt durch Länge des Links (nicht Paket!) und der Ausbreitungsgeschwindigkeit im Link.

6. **Autonomes System (AS)** Mehrere miteinander verbundene Netzwerke unter einer Administration. Ein AS benutzt immer das gleiche Intradomain-Routing Protokoll. Zum Beispiel das Netz eines ISPs (obwohl ein ISP auch mehrere AS betreiben kann).

7. **Peering** Vereinbarung die ISPs ermöglicht gegenseitig auf die Kunden des jeweils anderen Zugriff zu erhalten.

   Transit Bezahlte Vereinbarung, bei der ein ISP den Zugang zu allen Zielen seiner Routing Tabellen verkauft aka. Zugang zum Rest der Welt.

8. **Routing** beschreibt den Aufbau der Forwarding Tabelle mittels Routing-Algorithmen.

   Forwarding beschreibt den Prozess des Weiterleitens von Paketen basierend auf der Forwardingtabelle und dem Paketheader.

Übung 2 *IPv4*

Beantworten Sie im Kontext von IP die folgenden Fragen:

1. Was sind Class A, B und C Netze? Welcher Teil der Adresse gehört jeweils zu Host bzw. Netzwerk?

2. Überprüfen Sie, ob die IPv4-Adresse `149.77.115.54` im Netzwerk `149.77.112.0` mit der Netzwerkmaske `255.255.252.0` liegt.

3. Nennen Sie zwei Ansätze, mit dem Problem der knappen Internet-Adressen umzugehen.

4. Wie hilft das heute verwendete Classless Inter-Domain Routing (CIDR), das Problem zu lösen?

Lösung

1.
   - Class A (erstes Bit 0): $2^7 - 2$ Netze, da `0.x.x.x` und `127.x.x.x` für lokalen Host reserviert ist. Für jedes Netz: $2^8 \cdot 2^8 \cdot 2^8 - 2$ Interfaces, da `x.255.255.255` für Broadcasts und `x.0.0.0` für den Netznamen reserviert ist.

     $126 \cdot (256 \cdot 256 \cdot 256 - 2) = 2113928946$
   - Class B (erste Bits: 10): $2^6 \cdot 2^8$ Netze a $2^8 \cdot 2^8 - 2$ Interfaces.

     $64 \cdot 256 \cdot (256 \cdot 256 - 2) = 1073709056$
   - Class C (erste Bits: 110): $2^5 \cdot 2^8 \cdot 2^8$ Netze a $2^8 - 2$ Interfaces.

     $32 \cdot 256 \cdot 256 \cdot 254 = 532676608$
   - Class D (erste Bits: 1110): $2^4 \cdot 2^8 \cdot 2^8 \cdot 2^8 - 2$ Interfaces.

     $16 \cdot 256 \cdot 256 \cdot 256 - 2 = 268435454$
   - Class E (erste Bits: 1111): $2^4 \cdot 2^8 \cdot 2^8 \cdot 2^8 - 2$ Interfaces.

     $16 \cdot 256 \cdot 256 \cdot 256 - 2 = 268435454$
   - Summe: 4257185536.

   Man könnte noch die privaten Adressen nach RFC 1918 abziehen.[a]

2. Anwenden von Bit-weisem UND:

   ```
       10010101.01001101.01110011.00110110
   AND 11111111.11111111.11111100.00000000 =
       10010101.01001101.01110000.00000000
   ```

3.
   - IPv6
   - Network Address Translation (NAT)
   - dynamische Vergabe von IP-Adressen durch Internet Service Provider (ISP)

4. Bei der klassenbasierten Vergabe wurden oft ganze B-Netze vergeben von denen nur ein Bruchteil wirklich gebraucht wurde. Mit CIDR können nun auch kleinere Blöcke vergeben werden.

[a] `https://en.wikipedia.org/wiki/Private_network#Private_IPv4_address_spaces`

Übung 3 *NAT*

Angenommen Sie greifen auf das Internet über einen Router zu. Beantworten Sie die folgenden Fragen:

1. Sie schalten Ihren Rechner an und erhalten automatisch eine IP-Adresse. Die dafür benutzte Technologie nennt sich DHCP. Wie sieht die initiale Anfrage nach einer Adresse aus?
2. Sie haben eine Adresse zugewiesen bekommen. Wie lange ist diese gültig?
3. Was macht Ihr Rechner, damit die Adresse länger gültig bleibt? Wann tut er dies?
4. Ihr Router stellt das Internet über NAT bereit. Was bedeutet das?

Lösung

TODO

1. **Wie sieht die initiale Anfrage nach einer Adresse aus?**
   - Ihr Rechner startet den lokalen DHCP Client. Dieser weiß nur die lokale MAC Adresse des Rechners.
   - Dieser sendet nun ein DCHPDISCOVER an alle DHCP Server als Broadcast.
   - Sie erhalten eine (oder mehrere) DHCPOFFER als Antwort, mit einer IP Adresse.
   - Der DHCP Client wählt nun eine der angebotenen Ip Adressen aus und sendet eine DHCP Request um diese zu beantragen.
   - Er erhält ein DHCPACK als Antwort und kann nun die gewählte IP Adresse nutzen.
2. **Wie lange ist diese gültig?**
   - Entsprechend der "Lease Time".
3. **Was macht Ihr Rechner, damit die Adresse länger gültig bleibt? Wann tut er dies?**
   - Wenn 50% der Lease Time abgelaufen ist, findet eine Erneuerung statt.
   - Dafür sendet der DHCP CLient erneut eine DHCPREQUEST mit der Adresse.
   - Erhält er erneut ein DHCPACK, kann er die Adresse wieder fpr eine gewisse Lease Time nutzen

4. **Was bedeutet das?**

   - NAT umgeht die Adressknappheit.
   - Die Idee ist die folgende: man unterscheidet zwischen IP Addressen, die im Internet identifiziert werden können, und den Rechnern, die intern im Netzwerk genutzt werden.
   - Dafür gibt es private, global ungültige Addressen.
   - Das Netzwerk selber benutzt aber eine global gültige IP-Adresse.

Übung 4 *DHCP*

Angenommen, Ihr Rechner befindet sich in einem Zustand, in dem er – bis auf seine eigene MAC-Adresse – über keine weiteren Information über das Netzwerk zu dem er sich gerade verbunden hat, verfügt.

Nun soll untersucht werden, welche Schritte nötig sind, bevor Ihr Rechner eine Verbindung zum Standardgateway und somit zum Internet aufbauen kann. Wir haben Ihnen dazu eine Trace-File auf ISIS bereitgestellt.

1. Welches Protokoll ist dafür verantwortlich, dass Ihr Rechner eine IP-Adresse bekommt? Welche Pakete dieses Protokolls finden Sie in dem Trace-File? Was ist in diesen Paketen als Source- und Destination IP-Adresse eingetragen und warum? Welche Adresse möchte der Rechner gerne bekommen? Wird diesem Wunsch entsprochen? Wie lange ist die Adresse gültig? Was ist der zuständige DNS-Server?

2. Was sind die Pakete 1 und 4-7 und wozu dienen sie?

3. Nun verfügt der Rechner über alle nötigen Information, um Daten ins Internet zu schicken. Er ruft jetzt eine Webseite über eine URL auf. Nach welchem Hostnamen wird zunächst per DNS gefragt? Was ist die entsprechende Antwort des DNS-Servers?

4. Nun wird der HTTP-Server kontaktiert. Welche vollständige URL wird angefragt? Welcher Browser wird genutzt? Welche Server-Software antwortet? Handelt es sich um eine persistente Verbindung?

5. Nun wird eine zweite Verbindung aufgebaut. Welcher DNS-Name wird diesmal aufgelöst? Auf welchen Ports (Client/Server) wird die Verbindung aufgebaut? W elchem Protokoll entspricht das standardmäßig? Schauen Sie sich den Datenaustausch zwischen Server und Client an. Warum können Sie keine sinnvollen Daten erkennen?

6. Mit dem Hintergrund, dass nicht nur Sie Ihren eigenen Netzwerkverkehr mitschneiden können, sondern auch jeder andere, der sich in Ihrem Netzwerk befindet, bzw.

in Reichweite ihrer WLAN Karte aufhält, welche potentiellen Sicherheitsrisiken fallen Ihnen bei der Verwendung von Protokollen wie z.B. HTTP, FTP, SMTP, etc. ein?

Lösung

1.
   - DHCP
   - DHCP Request, DHCP Ack
   -
     - Paket 2: Source: 0.0.0.0 (weil noch keine IP Adresse) Dest: 255.255.255.255 (für einen limited Broadcast für die DHCP Request)
     - Paket 3: Source: 192.168.1.1 (Antwortender DHCP Server) Dest: 192.168.1.109 (neue Client IP Adress)
   - 192.168.1.109 wird als Requested IP angegeben
   - ja, der bekommt sie
   - Lease Time ist 43200s (12 Stunden)
   - 192.168.1.1
2.
   - ARP (Adress Resolution Protocol) Pakete, genutzt zur Abbildung einerIP-Adresse auf eine Adresse im lokalen Netzwerk (LAN)
   - hier wird die MAC Adresse vo, DNS Server und Ihrem Rechner erfragt
3.
   - www.tkn.tu-berlin.de
   - ace-hauptblock4.tubit.tu-berlin.de
4.
   - http://www.tkn.tu-berlin.de/
   - Browser: Lynx
   - Server-Software: Apache
   - Persistente Verbindung: nein, die Verbindung läuft ab am 20.6.2014
5.
   - hyperion.tkn.tu-berlin.de
   - Server:22 Client: 39506
   - 22: SSH port
   - SSHv2 sorgt für Verschlüsselung, es gibt einen Key-Exchange usw.
6.
   - Sender, Empfänger mitlesen
   - Inhalte unverschlüsselt, ausspionierbar
   - potentielle Manipulierung von Absender/Empfänger/Inhalten

Übung 5 *CRC*

Gegeben sei das Generatorpolynom $x^5+x^4+x^1+x^0$. Sie wollen den Bitstring `10010101011` verschicken.

1. Welche CRC-Checksumme müssen Sie an den Bitstring anhängen?
2. Wie wird auf Empfängerseite ein empfangenes Paket überprüft?

Lösung

Siehe auch `https://de.wikipedia.org/wiki/Zyklische_Redundanzpr%C3%BCfung`

- Generatorpolynom:
  $P = 1 * x^5 + 1 * x^4(+0 * x^3 + 0 * x^2) + 1 * x^1 + 1 * x^0$
  $= 110011$‘
- Grad(P) = 5 = n = # Bits des Generatorpolynoms - 1
- Bitstring: `1001 0101 011`
- Anhang: `00000`
- Bitstring mit Anhang: `1001 0101 0110 0000`

```
1001|0101|0110|0000  XOR  110011
1100|11  |    |
----|--- |    |
 101|100 |    |
 110|011 |    |
 ---|----|    |
  11|1111|    |
  11|0011|    |
  --|----|    |
    |1100|01  |
    |1100|11  |
    |----|--  |
         |1010|00
         |1100|11
          ----|----
           110|110
           110|011
           ---------
           000|1010
           --------
           --------

# Rest: 01010 wird angehangen
```

Alternativ mit ausführlicher Rechnung:

```
1001|0101|0110|0000  XOR  110011
1100|11  |    |
----|---  |    |
 101|100  |    |
 110|011  |    |
 ---|----|    |
  11|1111|    |
  11|0011|    |
  --|----|    |
   0|1100|0   |
   0|0000|0   |
   -|----|-   |
    |1100|01  |
    |1100|11  |
    |----|--  |
    | 000|101 |
    | 000|000 |
    |----|--- |
       00|1010|
       00|0000|
       --|----|
        0|1010|0
        0|0000|0
        --------
         |1010|00
         |1100|11
          ----|----
           110|110
           110|011
           ---------
           000|1010
           000|0000
           ---|----
            00|1010
            -------
            -------

# Rest: 01010 wird angehangen
```

```
***************
CRC Check
***************
1001|0101|0110|1010  XOR  110011
1100|11  |    |
----|--- |    |
 101|100 |    |
 110|011 |    |
 ------- |    |
  11|1111|    |
  11|0011|    |
  --|----|--  |
    |1100|01  |
     1100|11  |
     -------  |
          1010|10
          1100|11
          ----|--
           110|011
           110|011
           ---|----
           000|0000
           --------
           --------

# Rest ist 0 --> Keine Bitfehler
```