Ethernet

Markus Götzl

Zusammenfassung
Ethernet ist eine weit verbreitete Netzwerktechnologie, die in vielen privaten und geschäftlichen Umgebungen für die Datenübertragung verwendet wird. Ethernet besteht aus einer Gruppe von Standards und Protokollen, die in lokalen Netzwerken (Local Area Networks, LANs) zur Verbindung von Computern und anderen Netzwerkgeräten verwendet werden. Es wurde erstmals in den 1970er Jahren von Xerox, DEC und Intel entwickelt.

Keywords
Ethernet — LAN — Netzwerktechnologie

Inhaltsverzeichnis

Vorbereitungen **1**
1 Ethernet Rahmen **1**
1.1 *Display-Filter* 2
1.2 Ethernet-Standard 2
1.3 *I/G* und *L/G Bits* 2
1.4 Type-Feld 2
1.5 *Padding* 2
2 Ethernet Rahmengröße **2**

Vorbereitungen

Wenn mit einem eigenen Mitschnitt gearbeitet wird (*Empfehlung!*) muss der Rechner, natürlich, an ein *Ethernet* Netzwerk angebunden sein, kabelgebunden (IEEE 802.3) oder per WLAN (IEEE 802.11). Alternativ können auch die Labormitschnitte verwendet werden. Zudem muss die eigene MAC Adresse (Media Access Control Address) bekannt sein, dafür muss das aktive Netzwerkgerätes (Network Interface Controller) ermittelt werden (u.U. lassen sich diese Information auch über Wireshark ermitteln):

- NIC Name:
  - Linux:
    ```
    ip addr \
    | awk '/state UP/ {print $2}' \
    | sed 's/.$//'
    ```
  - Windows:
    ```
    netsh interface show interface
    ```
  - macOS:
    ```
    route get default \
    | grep interface \
    | awk 'print $2'
    ```
- MAC Adresse:
  - Linux:
    ```
    ip a show <NIC Name> \
    | grep ether \
    | awk 'print $2'
    ```
  - Windows:
    ```
    getmac /v
    ```
  - macOS:
    ```
    ifconfig <NIC Name> \
    | grep ether \
    | awk 'print $2'
    ```

Bei den Labormitschnitten ist die eigene (Quell-MAC Adresse): `00:23:32:da:19:8c`

1. Ethernet Rahmen

Wählen Sie einen beliebigen *Frame* aus. Folgendes fällt auf:

- Die Rahmen in diesem Mitschnitt sind DIX Ethernet Rahmen, diese werden in *Wireshark 'Ethernet II'* genannt.
- Es gibt keine *Präambel*. Die *Präambel* ist ein Mechanismus aus der Bitübertragungsschicht (Physical Layer), der der NIC hilft, den Anfang eines Rahmens zu identifizieren. Die *Präambel* enthält keine nützlichen Daten und wird nicht wie die anderen Felder angezeigt bzw. im Mitschnitt aufgeführt.
- Es gibt eine Zieladresse und eine Quelladresse. Wireshark dekodiert einige dieser Bits im OUI-Teil(Organizationally Unique Identifier) der Adresse, um den Anbieter der NIC anzugeben, z. B. *Dell* oder *Apple* (siehe Wireshark Mitschnittsoptionen - Namensauflösung).
- Es gibt ein *Type-Feld*. Für manche ist der Ethernet-Typ: *'IPv4'*, was bedeutet, dass die Ethernet-Payload ein IP-Paket ist. Es gibt kein Längenfeld wie im IEEE 802.3-Format. Stattdessen wird die Länge eines DIX-Ethernet-Rahmens durch die Hardware einer empfangenden NIC bestimmt,

die nach gültigen Frames sucht, die mit einer Präambel beginnen und mit einer korrekten Prüfsumme enden, und zusammen mit dem Paket an höhere Schichten übergeben.

- Manchmal werden *Pad-Bytes* angezeigt. *Pad-Bytes* werden eingefügt, wenn die Rahmengröße andernfalls weniger als 64 Bytes, die minimale Ethernet-Rahmengröße, betragen würde. Auch die *Pad-Bytes* werden bereits auf Hardwareebene entfernt und tauchen im Mitschnitt nicht auf.
- Es wird keine Prüfsumme angezeigt. Auch diese wird bereits auf Hardwareebene berechnet oder überprüft und ist nicht im Mitschnitt enthalten.
- Es gibt auch keine VLAN-Felder. Wenn VLANs verwendet werden, werden die VLAN-Tags durch die *Switch-Ports* hinzugefügt bzw. entfernt, so dass sie auf den Endgeräten, die das Netzwerk verwenden, nicht sichtbar sind.

1.1 *Display-Filter*

Wenden Sie einen *Display Filter* an um ausschließlich Ethernet-Rahmen anzeigen zu lassen, welche einen ARP (Address Resolution Protocol) Payload enthalten.

1.2 Ethernet-Standard

Wählen Sie einen beliebigen Rahmen aus:

- Welchem Ethernet-Standard entspricht der ausgewählte Rahmen und warum?

1.3 *I/G* und *L/G Bits*

Lassen Sie den *Display-Filter* bestehen und wählen Sie einen *Broadcast-Rahmen* aus:

- Sehen Sie sich die *I/G* und *L/G Bits* der Zieladresse an. Inwiefern sind die plausibel?
- Die Quelladresse ist, natürlich, eine *Unicast-Adresse*. Inwiefern sind die *I/G* und *L/G Bits* hier plausibel?

1.4 Type-Feld

Bei Ethernet-Rahmen mit *ARP Payload* wird im Type-Feld jeweils der Wert: *0x0806* angegeben. Diese Werte wurden durch IEEE bzw. die IANA festgelegt (die IEEE führt *0x800 = IPv4* nicht auf).

- *0x800 = IPv4* ist der niedrigste Wert der in diesen Listen aufgeführt wird, warum?

1.5 *Padding*

Wählen Sie einen Rahmen mit *ARP Payload* aus, der *nicht* von Ihrem Rechner stammt:

- Dieser Rahmen wird mit einer Rahmengröße von 60 Byte angegeben und erreicht damit sie geforderte Mindestgröße von 64 Byte beim Transport im Netzwerk (+ 4 Byte Prüfsumme, die nicht angezeigt werden!). Zeigen Sie wie diese Rahmengröße erreicht wird indem Sie die Header und Payload-Größen angeben/addieren.

2. Ethernet Rahmengröße

Wählen Sie einen Rahmen mit *ARP Payload* aus, der Ihrem Rechner erzeugt wurde:

- Warum wird dieser Rahmen mit lediglich 42 Byte angegeben?

Literatur