

## L2 1. Zentrale Bestandteile eines Netzwerks

### 1.3 Datenaustausch – „Was passiert bei einem ping?“

Beachten Sie das Informationsmaterial *L2 1.3 Informationsmaterial Datenaustausch.docx*.

#### 1.3.1 Voraussetzung

*LS 1.2 Arbeitsauftrag Ping* ist abgeschlossen und noch innerhalb *Filius* geladen.

#### 1.3.2 Datenaustausch beim *ping*-Befehl

Lassen Sie sich nach der Ausführung des *ping*-Befehls (LS 1.2) den *Datenaustausch* vom *Notebook 1* anzeigen.

Beachten Sie das Informationsmaterial *L2 1.3 Informationsmaterial Datenaustausch.docx*.

Datenaustausch

Notebook 1 - 192.168.0.10

Nr.	Zeit	Quelle	Ziel	Protokoll	Schicht	Bemerkungen
1	15:47:19.514	192.168.0.10	192.168.0.11	ARP	Vermittlung	Suche nach MAC für 192.168.0.11, 192.168.0.10: 30:3F:39:75:86:DB
2	15:47:19.639	192.168.0.11	192.168.0.10	ARP	Vermittlung	192.168.0.11: 6E:0A:F3:AD:54:57
3	15:47:19.639	192.168.0.10	192.168.0.11	ICMP	Vermittlung	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 1
4	15:47:19.763	192.168.0.11	192.168.0.10	ICMP	Vermittlung	ICMP Echo Reply (pong), TTL: 64, Seq.-Nr.: 1
5	15:47:20.718	192.168.0.10	192.168.0.11	ICMP	Vermittlung	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 2
6	15:47:20.843	192.168.0.11	192.168.0.10	ICMP	Vermittlung	ICMP Echo Reply (pong), TTL: 64, Seq.-Nr.: 2
7	15:47:21.924	192.168.0.10	192.168.0.11	ICMP	Vermittlung	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 3
8	15:47:22.049	192.168.0.11	192.168.0.10	ICMP	Vermittlung	ICMP Echo Reply (pong), TTL: 64, Seq.-Nr.: 3
9	15:47:23.127	192.168.0.10	192.168.0.11	ICMP	Vermittlung	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 4
10	15:47:23.239	192.168.0.11	192.168.0.10	ICMP	Vermittlung	ICMP Echo Reply (pong), TTL: 64, Seq.-Nr.: 4

#### 1.3.2.1 Warum sind bereits zehn Zeilen eingetragen, obwohl nur ein ping-Befehl eingegeben wurde?

Es werden 5 Nachrichten versendet und 5 Nachrichten empfangen.

#### 1.3.2.2 Welchen Zweck haben die einzelnen Nachrichten?

Nachricht 1 dient dazu, zur IP-Adresse (192.168.0.11) die MAC-Adresse zu erfragen.

Nachricht 2 ist die Antwort darauf und liefert die MAC-Adresse. (Sie besteht aus 48 Bits bzw. 6 Bytes)

Nachricht 3, 5, 7 und 9 sind die vier *pings*, die durch einen ping-Befehl erzeugt werden.

Nachricht 4, 6, 8 und 10 sind die Antworten (*pong*).

### 1.3.3 Nachrichteninhalt

1.3.3.1 Notieren Sie den Inhalt des **ersten** Eintrags (ARP) und versuchen Sie die Bedeutung zu erklären.

```
Nr.: 1 / Zeit: 15:47:19.514
├─ Netzzugang
│   ├── Quelle:      30:3F:39:75:86:DB
│   ├── Ziel:       FF:FF:FF:FF:FF:FF
│   └─ Bemerkungen: 0x806
├─ Vermittlung
│   ├── Quelle:     192.168.0.10
│   ├── Ziel:      192.168.0.11
│   ├── Protokoll:  ARP
│   └─ Bemerkungen: Suche nach MAC für 192.168.0.11, 192.168.0.10: 30:3F:39:75:86:DB
```

Nr. : 1	Inhalt	Bedeutung
<b>Netzzugang</b>	<b>Quelle:</b> 30:3F:39:75:86:DB	MAC-Adresse des Senders
	<b>Ziel:</b> FF:FF:FF:FF:FF:FF	„An alle“. (Broadcast, entspricht der höchsten MAC-Adresse)
<b>Vermittlung</b>	<b>Quelle:</b> 192.168.0.10	IP-Adresse des Senders
	<b>Ziel:</b> 192.168.0.11	IP-Adresse des Empfängers

Das Address Resolution Protocol (**ARP**) ist ein Netzwerkprotokoll, das zu einer Netzwerkadresse die physische Adresse (MAC-Adresse) der Netzzugangsschicht ermittelt.

1.3.3.2 Was ist in der **zweiten** Nachricht (ARP-Antwort) anders als in der ersten?

```
Nr.: 2 / Zeit: 15:47:19.639
├─ Netzzugang
│   ├── Quelle:      6E:0A:F3:AD:54:57
│   ├── Ziel:       30:3F:39:75:86:DB
│   └─ Bemerkungen: 0x806
├─ Vermittlung
│   ├── Quelle:     192.168.0.11
│   ├── Ziel:      192.168.0.10
│   ├── Protokoll:  ARP
│   └─ Bemerkungen: 192.168.0.11: 6E:0A:F3:AD:54:57
```

Quelle und Ziel sind IP-Adresse getauscht, weil der Empfänger der ersten Nachricht darauf antwortet. „An alle“ wird bei der Antwort nicht gesendet, da der ursprüngliche Sender bekannt ist.

1.3.3.3 Notieren Sie den Inhalt des **dritten** Eintrags (ICMP) und versuchen Sie die Bedeutung zu erklären.

Nr.: 3 / Zeit: 15:47:19.639

```

Netzzugang
├── Quelle:      30:3F:39:75:86:DB
├── Ziel:       6E:0A:F3:AD:54:57
└── Bemerkungen: 0x800
Vermittlung
├── Quelle:     192.168.0.10
├── Ziel:      192.168.0.11
├── Protokoll: ICMP
└── Bemerkungen: ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 1
    
```

Nr.: 3	Inhalt	Bedeutung
<b>Netzzugang</b>		
<b>Quelle:</b>	30:3F:39:75:86:DB	MAC-Adresse des Senders
<b>Ziel:</b>	6E:0A:F3:AD:54:57	MAC-Adresse des Empfängers
<b>Vermittlung</b>		
<b>Quelle:</b>	192.168.0.10	IP-Adresse des Senders
<b>Ziel:</b>	192.168.0.11	IP-Adresse des Empfängers

1.3.3.4 Was ist in der **vierten** Nachricht (ICMP-Antwort) anders als in der dritten?

Nr.: 4 / Zeit: 15:47:19.763

```

Netzzugang
├── Quelle:     6E:0A:F3:AD:54:57
├── Ziel:      30:3F:39:75:86:DB
└── Bemerkungen: 0x800
Vermittlung
├── Quelle:     192.168.0.11
├── Ziel:      192.168.0.10
├── Protokoll: ICMP
└── Bemerkungen: ICMP Echo Reply (pong), TTL: 64, Seq.-Nr.: 1
    
```

Quelle und Ziel sind bei MAC-Adresse und IP-Adresse getauscht, weil der Empfänger der ersten Nachricht darauf antwortet.

In den Bemerkungen steht *pong* für Antwort auf *ping*!

**Das ICMP-Protokoll ermöglicht den Austausch von Kontroll- und Fehlerpaketen im Netz.**

1.3.3.5 Versuchen Sie den Datenaustausch bei *einem ping-Befehl* zusammenzufassen.

Zunächst wird die MAC-Adresse zur im ping-Befehl angegebenen IP-Adresse erfragt. Dabei wird die Adresse des Senders mitgeteilt. Der Besitzer der gesuchten MAC-Adresse antwortet und teilt dem Absender des pings seine MAC-Adresse mit. Jetzt ist ein Datenaustausch möglich. Anschließend wird vier Mal ein ping gesendet. Die Übertragungszeit wird gemessen.