Versuch 1: Einführung in Ethernet LANs und Analyse des ARP-Protokolls (Windows Version)

Dieser Versuch behandelt im ersten Teil die Grundprinzipien der Kapselung im TCP/IP Protokollstapel am Beispiel von ARP und dem Daytime Anwendungsprotokoll. Dazu verwenden Sie den Protokollanalysator „Wireshark“.

Versuchsvorbereitung

Zur Vorbereitung lesen Sie bitte diese Versuchsanleitung inklusive des Anhangs gründlich durch. Wiederholen Sie außerdem anhand der Vorlesungsunterlagen (Kapitel 2) die Grundprinzipien der Schichtenmodelle und die Verwendung der PDUs (Protocol Data Units) in den Schichten des TCP/IP-Modells. Informieren Sie sich auch über die grundsätzliche Struktur und Verwendung einer IP-Adresse (IP Version 4). Bearbeiten Sie dazu (bitte jeder und bitte schriftlich) die folgenden Aufgaben:

Aufgabe 1

1.1 Welche Schichten werden im TCP/IP Modell verwendet und welchen OSI-Schichten entsprechen sie?

1.2 Wie heißen die PDUs dieser Schichten?

Aufgabe 2:

Informieren Sie sich z.B. mit Hilfe der Vorlesung (Kapitel 7) über die grundsätzliche Aufteilung einer IP-Adresse (IPv4) in einen Netz-Anteil und einen Host-Anteil.

2.1 Wozu dient die Subnetzmaske?

2.2 Welche beiden Adressen eines Netzes dürfen nicht an die Geräte vergeben werden?

2.3 Was versteht man unter einem Default-Gateway (bzw. Standart-Gateway)? Um welches Netzelement handelt es sich und wozu wird es benötigt?

Aufgabe 3:

Wiederholen Sie die Funktionsweise des Address Resolution Protocols (ARP) und des ARP-Caches.

3.1 Wozu dient ARP?

3.2 Welche Zuordnung wird im ARP-Cache gespeichert?

Aufgabe 4:

Im ersten Teil des Versuches benutzen Sie den Protokollanalysator Wireshark. Laden Sie dieses Programm von www.wireshark.org und installieren es auf Ihrem Rechner.

Darüber hinaus benötigen Sie unter Windows 10 das Programm Eingabeaufforderung (unter *Programme->Windows System*), das als Administrator gestartet werden muss (erscheint nach Eingabe der Tastenkombination *Windowstaste-x*).

Windows 10 Benutzer müssen zusätzlich das Windows Feature Telnet Client (unter *Einstellungen->Apps und Features->Programme* und *Features->Windows Features aktivieren und deaktivieren->Telnet Client*) aktivieren.

Laden Sie die Dateien *V1-ARP.pcapng*, *V1-Daytime.pcapng* und *V1-ICMP.pcapng* aus dem Dateiordner unter OSCA auf Ihren Rechner.

Kommunikationsnetze Versuch 1

Marcel Syben, 920123

Aufgabe 1:

TCP/IP	OSI	PDU
Application	Application	Data
	Presentation	
	Session	
Transport	Transport	Segment
Internet	Network	Packet
Network Access	Data Link	Frame
	Physical	Bits

Aufgabe 2:

2.1

Die Subnetzmaske gibt die Bits an, die für den Netz-Anteil einer IP-Adresse reserviert ist.

2.2

Die Adressen 0 und 255 dürfen nicht vergeben werden, Die Netzadresse und die Broadcastadresse.

2.3

Mit Default Gateway ist der (meist einzige) Router gemeint, der das Ansprechen von Adressen ausserhalb des eigenen (Sub)-Netzes ermöglicht.

Aufgabe 3:

3.1

Durch ARP wird die MAC-Adresse des Ziel-Geräts in Erfahrung gebracht.

3.2

Im ARP-Cache werden temporär die angefragten MAC-Adressen den jeweiligen IP-Adressen zugeordnet.

Versuchsdurchführung

Internet-Anbindung und Protokollanalyse

1.1 Addressen

Machen Sie sich zunächst mit der Internet-Anbindung Ihres Rechners vertraut. Sollte Ihre Rechner sowohl über Ethernet und WLAN verbunden sein, deaktivieren Sie bitte die WLAN Verbindung.

Führen Sie in der Eingabeaufforderung das Kommando **`ipconfig /all`** aus. Notieren Sie folgende Adressen:

IP Adresse (IPv4)	192.168.178.85
MAC- oder physikalische Adresse	E0-D5-5E-4D-34-3D
Default-Gateway (Standard-Gateway)	192.168.178.1

Führen Sie in der Eingabeaufforderung das Kommando **`arp -a`** aus.

Woher stammen die Daten? ARP-Cache / RAM Speicher

Bestimmen Sie aus der Ausgabe die MAC-Adresse des Default-Gateways:

5c-49-79-db-14-58

1.2 Erreichbarkeitstest

Mit Hilfe von Ping kann man die Erreichbarkeit eines entfernten Hosts testen. Dazu werden spezielle ICMP-Nachrichten (ICMP: Internet Control Message Protocol) verwendet. Ein ICMP Echo-Request wird dabei vom entfernten Host mit einem ICMP Echo-Reply beantwortet. Aus Sicherheitsgründen kann es aber sein, dass der entfernte Host nicht antwortet. Das Kommando Ping wiederholt je nach Implementation dieses Anfrage-Antwort Schema mehrfach.

Löschen Sie den ARP-Cache in der Eingabeaufforderung mit dem Kommando **`arp -d *`** (Achtung: Die Eingabeaufforderung benötigt dafür Administratorrechte!). Testen Sie anschließend **`ping www.microsoft.com`**.

Hinweis: Falls Ihr Rechner und ihr Router auch mit IPv6 arbeiten, sehen Sie diesen Vorgang möglicherweise auch mit IPv6- statt IPv4-Adressen (erkennbar an der viel längeren, hexadezimal dargestellten Adresse in der Antwort)

War der Test erfolgreich? Ja

Sehen Sie sich nun wieder den Inhalt des ARP-Cache mit **`arp -a`** an. Warum erscheint hier wieder ein Eintrag für das Default-Gateway?

Da bei „ping www.microsoft.com“ Pakete außerhalb des eigenen Netzes verschickt werden, laufen diese über den Standard-Gateway, dessen MAC-Adresse angefordert wurde, um die Kommunikation zu ermöglichen.

1.3 Analyse der ARP Protokolls

Starten Sie Wireshark. Entfernen Sie zunächst unter *Bearbeiten->Einstellungen->Name Resolution* den Haken bei *Resolve Mac Addresses*. Laden Sie dann die Datei *V1-ARP.pcapng*. Diese Datei enthält eine Aufzeichnung von ARP Frames in einem Netzwerk.

Hier wurde die Mac-Adresse für ein Default-Gateway per ARP bestimmt. Der Host hat dabei die MAC-Adresse 00:0c:29:6b:b8:c3, das Default-Gateway 00:50:56:f9:0d:54 (das Szenario sehen Sie im Anhang dieses Versuchs). Es wurden genau 2 Frames aufgezeichnet.

Sie können im oberen Teil des Fensters jeden dieser Frames einzeln auswählen und sehen dann unten die Detail-Informationen der PDUs. Die erste Zeile im darunterliegenden Teil enthält Informationen von Wireshark, die hier nicht von Interesse ist. Die zweite Zeile enthält die Information der Ethernet-PDU, die dritte die Informationen der Internet-Layer-PDU. Wenn in den PDUs Nutzdaten weiterer Layer enthalten sind, werden dann diese in weiteren Zeilen angezeigt. Durch Klicken auf das Dreieck am Anfang der Zeile erhält man die Details der PDU.

Welche Protokolle und PDUs sind an ARP beteiligt?

OSI Schicht	Verwendetes Protokoll	PDU-Name	Adresstyp
2	Ethernet	Frame	MAC
3	IPv4	Packet	IP

Analysieren Sie den ARP-Request und den zugehörigen Reply im Detail und tragen Sie die gewonnen Informationen in die folgenden Tabellen ein. Verwenden Sie für die Adressen die logischen Bezeichnungen Host.MAC, Gateway.Mac, Host.IP und Gateway.IP.

ARP-Request

Frame Header	Ziel MAC-Adresse	Gateway.MAC
	Absender MAC-Adresse	Host.MAC
	Type	Ethernet
ARP-PDU	Absender MAC-Adresse	Host.MAC
	Absender IP-Adresse	Host.IP
	Ziel MAC-Adresse	Broadcast.MAC
	Ziel IP-Adresse	Gateway.IP

ARP-Reply

Frame Header	Ziel MAC-Adresse	Host.MAC
	Absender MAC-Adresse	Gateway.MAC
	Type	Ethernet
ARP-PDU	Absender MAC-Adresse	Gateway.MAC
	Absender IP-Adresse	Gateway.IP
	Ziel MAC-Adresse	Host.MAC
	Ziel IP-Adresse	Host.IP

Aus welchem Feld des ARP-Reply entnimmt der Host die IP-Adresse des Gateways?

Byte 28-31: Sender IP address

Welche unterschiedlichen Adressierungsarten werden im ARP-Request und ARP-Reply verwendet?

	Adressierungsart	Begründung
ARP-Request	broadcast	MAC des Ziels unbekannt
ARP-Reply	unicast	MAC bekannt

1.4 Analyse des Daytime Protokolls

Bei dem Daytime-Dienst handelt es sich um ein einfaches, TCP-basiertes Anwendungsprotokoll. Dabei wird der anfragenden Client-Anwendung die lokale Zeit der entfernten Server-Anwendung als lesbare Zeichenkette übermittelt. Daytime verwendet die Portnummer 13. Der Ablauf des Protokolls ist folgender:

- Die Client-Anwendung öffnet eine TCP-Verbindung zur Serveranwendung.
- Die Serveranwendung sendet auf dieser Verbindung einen Zeitstempel an die Client-Anwendung zurück.
- Die Server-Anwendung schließt die TCP-Verbindung.

Unter Windows gibt es keine spezielle Anwendung für Daytime. Stattdessen kann man das Kommando **`telnet`** in der Eingabeaufforderung verwenden.

Probieren Sie in der Eingabeaufforderung den Befehl **`telnet time.fu-berlin.de 13`** aus. Welche Antwort erhalten Sie?

Aktuelles Datum, Zeit und Zeitzone.

Laden Sie nun die Datei *V1-Daytime.pcapng*. Diese Datei enthält den Mitschnitt der Frames für diese Anwendung. Host und Default-Gateway haben wieder die MAC-Adressen wie in 1.3.

Wählen Sie den Frame mit den Nutzdaten für Daytime aus. Sie können ihn an der Bezeichnung in der Spalte **`Protocol`** erkennen.

Welche Protokolle und PDUs sind an der Realisierung des Daytime-Protokolls beteiligt? Analysieren Sie in welcher Reihenfolge diese eingekapselt werden und zu welcher OSI-Schicht sie jeweils gehören. Geben Sie für die PDUs jeweils auch den Adresstyp an.

OSI-Schicht	Names des Protokolls	PDU-Name	Adresstyp
2	Ethernet	Frame	MAC
3	IP	Packet	IP
4	TCP	Segment	Port

Welche Adressen werden in dem Frame verwendet? Benutzen Sie hier wieder die Bezeichnungen Host.Mac, Host.IP, Server.Mac, Server.IP, Gateway.MAC, Gateway.IP. Tragen Sie für die Schicht 4 die entsprechenden Port-Nummern ein.

OSI-Schicht	Ziel-Adresse	Absende-Adresse
2	Host.MAC	Gateway.MAC
3	Host.IP	Server.IP
4	49737	13

Warum passen die Absende-Adressen in Schicht 2 und 3 nicht zusammen?

Die Adressen passen nicht zusammen, da sich der Server in einem anderen Netz befindet. Der MAC-Adresstyp agiert allerdings nur im eigenen Netz, deshalb wird die MAC-Adresse des Servers mit der Adresse des Gateways ersetzt.

Ein wichtiges Merkmal des TCP/IP-Protokollstapels besteht darin, dass in den OSI-Schichten 2 und 3 im Header der PDUs angezeigt wird zu welchem Protokoll die Informationen im Nutzfeld gehören. Identifizieren Sie die Inhalte den Headerfelder „Type“ und „Protocol“ in den PDUs und notieren Sie die Werte:

OSI-Schicht	Headerfeld	Inhalt und Bedeutung
2	IPv4	0x0800
3	TCP	6

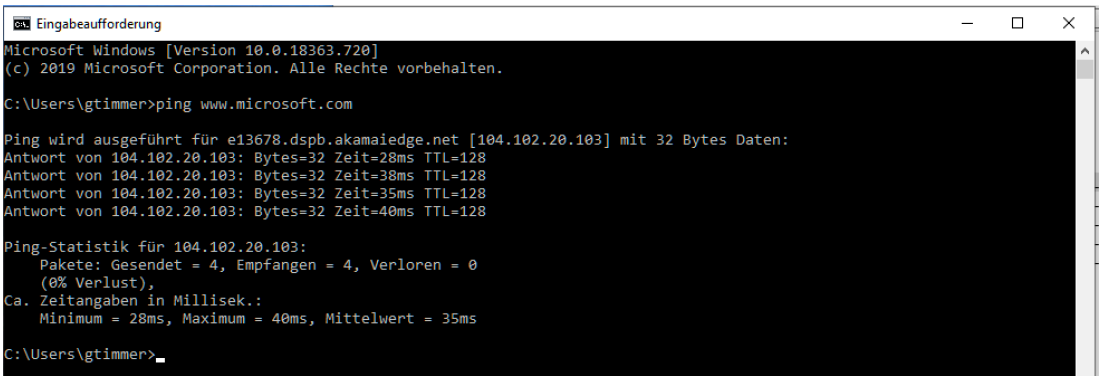
Warum wird in der OSI-Schicht 4 ein vergleichbares Feld nicht benötigt?

Wird nicht benötigt, da in der 4. Schicht mit Ports gearbeitet wird.

1.5 Analyse der PDUs bei der Ping-Anwendung (optional)

Wie unter 1.2 schon dargestellt kann man mit Ping die Erreichbarkeit eines entfernten Hosts überprüfen. Ping verwendet das ICMP-Protokoll. ICMP-Nachrichten werden dabei direkt in IP-Pakete eingekapselt.

Führen Sie in der Eingabeaufforderung wie unter 1.2 das Kommando **`ping www.microsoft.com`** aus. (*Hinweis: möglicherweise geschieht dies in IPv6 – vgl. 1.2*) Das Kommando sendet unter Windows genau 4 ICMP-Echo Requests und wartet auf die Antworten. Anschließend wird eine Statistik über die 4 Durchläufe mit den entsprechenden Antwortzeiten ausgegeben.



Laden Sie mit Wireshark die Datei *V1-ICMP.pcapng*. Sie enthält den Mitschnitt der Frames für diesen Ablauf für IPv4.

Wie heißen die ICMP-Nachrichten, die eine ping-Anfrage und die zugehörige Antwort realisieren?

	Name der ICMP-Nachricht
Anfrage	Echo (ping) request
Antwort	Echo (ping) reply

Das ICMP-Protokoll gehört ebenfalls zur OSI-Schicht 3, als Ergänzung des IP-Protokolls für Steuer- und Fehlernachrichten. Die ICMP-PDU wird dabei direkt in ein IP-Paket eingekapselt. Wie wird unter Wireshark diese Einkapselung dargestellt?

OSI-Schicht	Protokoll
3	ICMP
3	IP
2	Ethernet

Welcher Wert steht nun im Feld Protocol des IP-Headers? ICMP

Welchen Grund wird das haben?

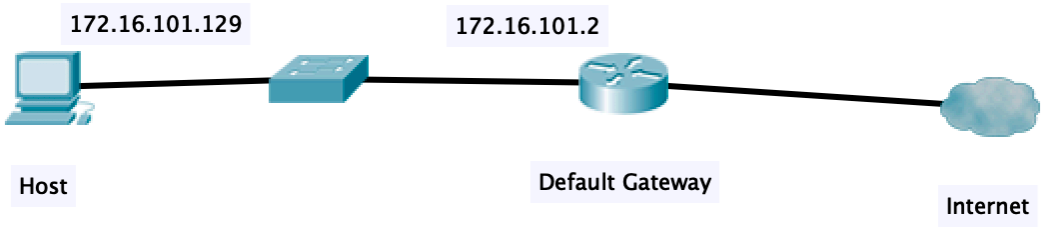
Das ICMP-Protokoll wird im Datenfeld des IP-Paketes übertragen.

Zusatz: Sehen Sie sich den Inhalt der ICMP Nachrichten an und überlegen Sie, wie es der Ping-Anwendung gelingt, eine Anfrage der richtigen Antwort zuzuordnen. Es ist möglich das Antworten nicht in der Reihenfolge der Anfragen eintreffen. Dann würden die Antwortzeiten nicht korrekt ermittelt.

Durch die Felder "Sequence number" können die Frames zugeordnet werden.

Anhang: Beschreibung zur Erstellung der Wireshark Mitschnitte

Die Mitschnitte wurden auf einem Rechner in folgendem Netz vorgenommen:



Dazu wurde in Wireshark eine Aufzeichnung durchgeführt. Dazu wurde im Menü Aufzeichnen->Optionen zunächst die passende Schnittstelle ausgewählt und dann mit unterschiedlichen Mitschnittfiltern die Aufzeichnung gestartet.

Netzwerkverkehr	Filterstring für Mitschnittfilter
ARP	`arp`
Daytime	`tcp port 13`
Ping	`icmp`

Erst danach wurden die einzelnen Anwendungen wie oben dargestellt gestartet und dann die Aufzeichnung angehalten.