NVS

Laborprotokoll – 06 –Wireshark & TCP/IP

Teffer christoph

2015

Inhaltsverzeichnis

[1. Aufgabenstellung für dieses Labor 2](#_Toc432359361)

[2. Fragen zum Labor 01 2](#_Toc432359362)

[3. Durchführung des Labors 2](#_Toc432359363)

[3.1. Installation der Hyper-V Plattform und Verwaltungstools 2](#_Toc432359364)

[3.2. Installation einer virtuellen Maschine mit Windows …. 4](#_Toc432359365)

TCP/IP und Wireshark

# Setup für das Labor

Für das Labor wird der nachfolgende Übungsaufbau mit den angegebenen IPv4 Adressen verwendet.

* Die Übung wird von VM-Lab01 durchgeführt. Auf diesem PC ist Wireshark installiert.
* Auf VM-Lab02 muss für den letzten Teil der Übung ein Web-Server installiert werden.

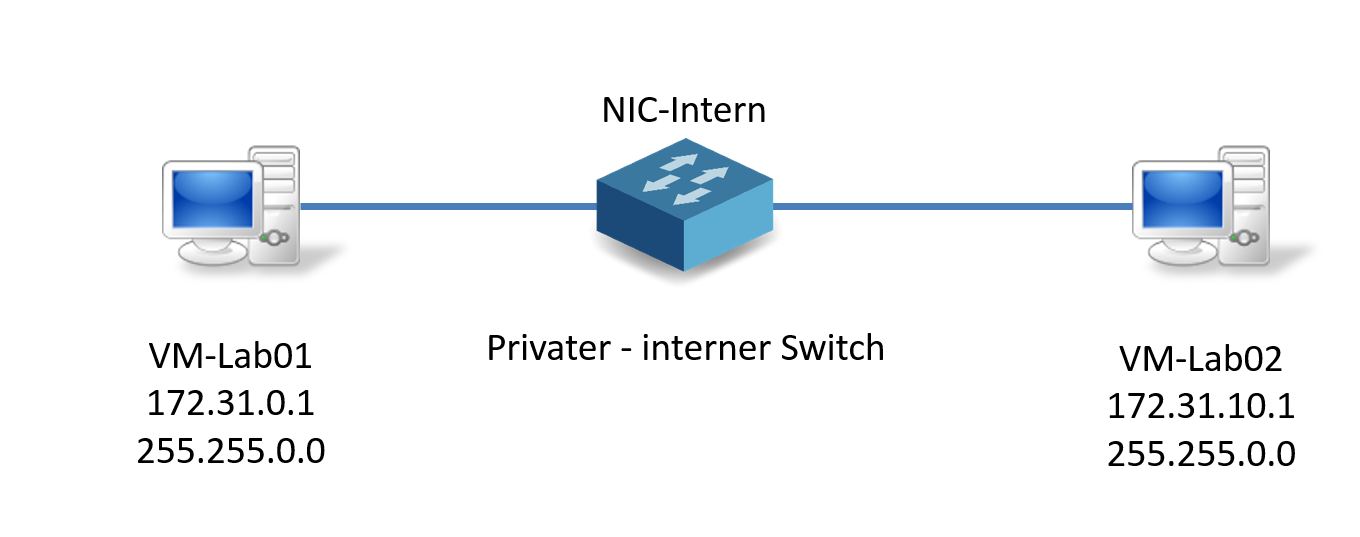


Abbildung: PCs und IP-Adressen für das Labor 06

# Aufgabenstellung für dieses Labor

In diesem Labor soll die Kommunikation zwischen PCs auf OSI Layer 2 bis 4 mit Hilfe von Wireshark untersucht werden.

Nachfolgende Übungen sollen durchgeführt und anschließend analysiert werden:

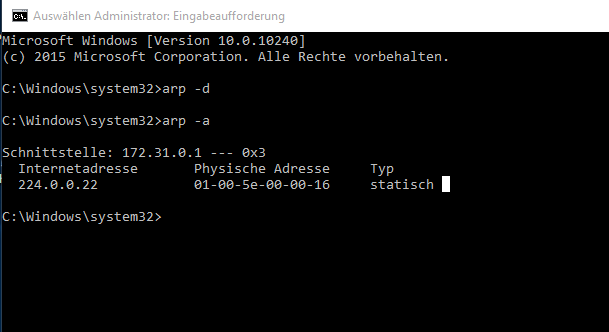
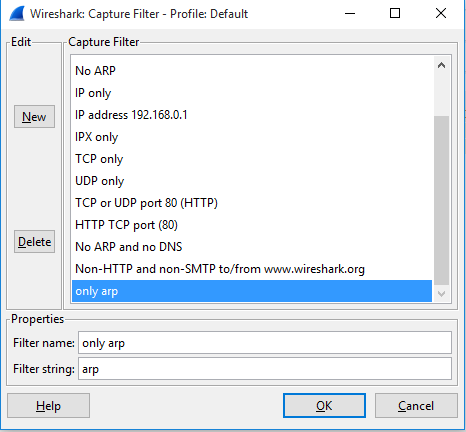
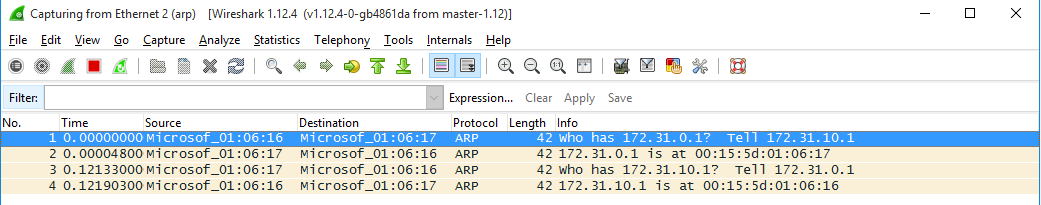
* Funktionsweise von ARP
* Kommunikation bei ICMPv4
* Kommunikation bei Verwendung von ICMPv6
* Drei Wege Handshake beim Aufbau einer TCP-Sitzung

# Durchführung des Labors

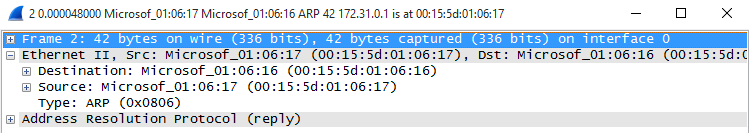
## Funktionsweise von ARP

Um einen Frame für das Netzwerk vorzubereiten muss die MAC-Adresse des Empfängers ermittelt werden. Dazu muss der PC durch aussenden eines ARP-Paketes die Zielempfänger MAC-Adresse ermitteln.

### Laborvorgangsweise für ARP

* Anmeldung auf VM-LAB01
* Lösche den Arp-Cache von VM-LAB01
* **
* Starte Wireshark
* Erstelle einen Caputre-Filter der nur das ARP-Protokoll aufzeichnet
* Starte die Aufzeichnung
* Führe nun einen Ping auf 172.31.10.1 aus (damit muss eine ARP-Auflösung erfolgen des Zielrechners erfolgen - nicht den Name VM-LAB02 verwenden)
* Beende die Aufzeichnung
* Speichere den Mitschnitt unter dem Dateinamen **06-LAB-01.pcapng**

### Analyse und Fragen zu ARP

1. Wie viele Datenpakete waren notwendig um die MAC Adresse von 172.31.10.1 zu ermitteln? Sehen Sie im Frame nach. 

Es waren 2 Datenpakete notwendig.

1. Welches Protokoll wurde verwendet?

- Das Protokoll, das verwendet wurde, heißt ARP(= Address Resolution Protocol).

1. An welche Ziel-MAC-Adresse wurde das erste Paket von 172.31.0.1 geschickt? Öffne dazu den Paket-Detail Bereich und analysiere den Mitschnitt des OSI Layer 2

- Das erste Paket wurde an das Ziel mit der MAC-Adresse 00:15:5d:01:06:17 geschickt.

1. Welchen OP-Code, Bezeichnung/ Nummer hatte das erste Paket der ARP-Anfrage? Öffne dazu den Paket-Detail Bereich und analysiere den Mitschnitt des OSI Layer 3

- Der OP-Code lautet: request

1. Zu welcher OSI-Schicht gehört die MAC-Adresse?

- Die MAC-Adresse ist Bestandteil der OSI-Schicht 2 (= Sicherungsschicht)

1. Zu welcher OSI-Schicht gehört die IP-Adresse?

- Die IP-Adresse ist Bestandteil der OSI-Schicht 3 (= Vermittlungsschicht)

1. Zu welcher TCP/IP-Schicht gehört die MAC-Adresse?

- Die MAC-Adresse ist Bestandteil der TCP/IP-Schicht 1 (= Netzzugangsschicht)

1. Zu welcher TCP/IP-Schicht gehört die IP-Adresse?

- Die IP-Adresse ist Bestandteil der TCP/IP-Schicht 2 (= Internetschicht)

1. Auf welcher Schicht des OSI bzw. TCP/IP Schichtmodels gehören ARP und RAP?

- ARP: OSI = Sicherungsschicht ; TCP/IP = Netzzugangsschicht

1. Unter welchen Umständen ist die Ziel-MAC-Adresse eines Datenpaketes nicht mit der MAC-Adresse des PCs identisch?

- Da das Datenpaket über das Internet u.a. einen NAT-Server passieren muss und dieser NAT-Server eine andere MAC-Adresse, als der Zielhost hat, kann dies vorkommen.

1. Was wäre, wenn die MAC-Adresse des Absenders auf Layer 2 und in ARP-Paket nicht identisch wären?
   1. Ist dies überhaupt möglich?

- Ja

* 1. Wenn ja, wie nennt man dieses „**gefälschte**“ Datenpaket.

- Dieses Datenpaket kommt u.a. bei Arp-Spoofing vor und hat keine genaue Bezeichnung

### Recherchen zu ARP

1. Auf dem Rechner VM-LAB01 wurde gerade ein Ping auf 172.31.10.1 gemacht. Es wird nochmals Wireshark mit einem Caputre-Filter arp gestartet. Es wieder ein erneuter Ping auf 172.31.10.1 abgesetzt. Werden in Wireshark nochmals Daten mitgeschnitten? Falls nein, warum nicht?

- Nein, weil die Adresse schon aufgelöst worden ist und erkannt wird.

1. Wozu wird RARP verwendet?

- RARP (= Reverse Access Resolution Protocol) wird zur Zuordnung von MAC-Adressen zu Internetadressen verwendet.

1. Gibt es ein Windows-Tool mit dem RARP verwendet werden kann und falls nicht, habe Sie dafür eine hinreichende Begründung

- Es gibt kein Windows-Tool mit dem RARP verwendet werden kann, da RARP nicht dynamisch ist und durch DHCP ersetzt wurde.

1. Welche Form der Adressierung wird auf OSI-Layer 2 verwendet? Es sind zwei Antworten gültig!
   1. Logische Adressierung
   2. Physische Adressierung
   3. MAC-Adressierung
   4. IP-Adressierung
   5. Port-Adressierung
2. Wie nennt man die PDU´s auf OSI-Layer 2, 3, 4 und 5 bis 7? **PDU steht für Protocol Data Unit**, dies sind die Daten einer bestimmten Schicht. Die PDU für die Schicht 1 wird allgemein **Bit** oder **Symbol** bezeichnet.

- OSI-Schicht 2: Frame

- OSI-Schicht 3: Paket

- OSI-Schicht 4: Segment

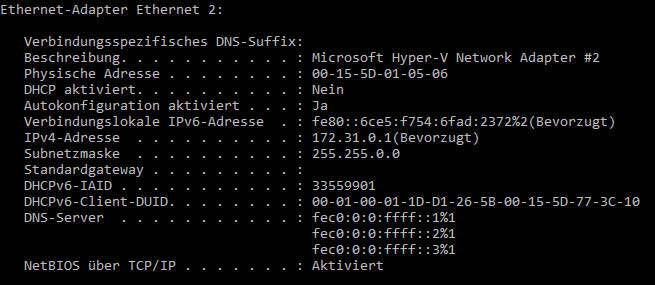
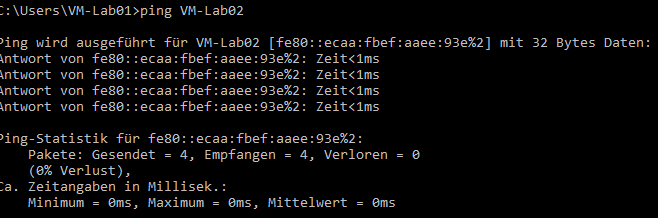
- OSI-Schicht 5: Daten

- OSI-Schicht 7: Daten

## Kommunikation bei ICMPv4

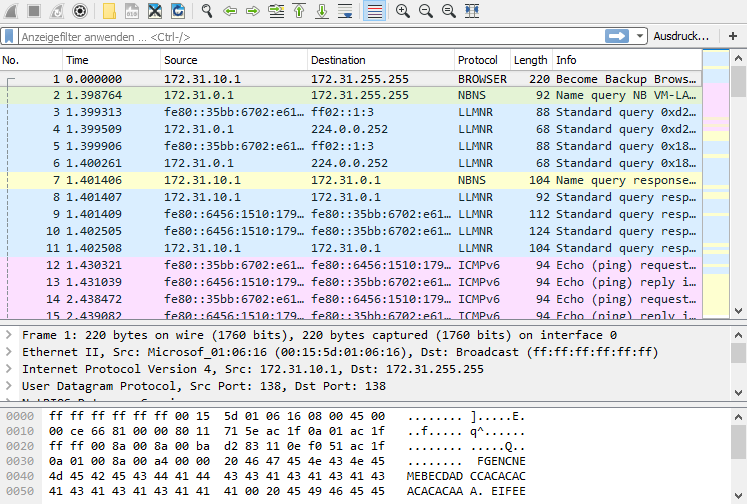
Für diesen Teil der Übung sind die am Anfang des Protokolls definierten IPv4 Adressen nötig

### Laborvorgangsweise für 3.2

1. Überprüfen Sie anschließend die dem Adapter zugewiesenen IPv4-Adressen  
   Abb: Adapter Einstellungen
2. Starten Sie Wireshark
3. Pingen Sie den PC VM-LAB02 mit Namen an**  
   *Abb: Ping VM-Lab02*
4. Pingen Sie den PC mit der IP-Adresse 8.8.8.8 anC:\Users\Peter\AppData\Local\Microsoft\Windows\INetCache\Content.Word\7.png

*Abb: Ping 8.8.8.8*

1. Beenden Sie Wireshark

  
*Abb: 06-LAB-02.pcapng*

1. Speichern Sie den Mitschnitt unter **06-LAB-02.pcapng** ab

### Analyse und Fragen zu 3.2

### Recherchen zu 3.2

1. Wofür steht ICMP und wofür wird dieses Protokoll verwendet

- ICMP steht für Internet Control Message Protocol und dient in Netzwerken zum Austausch diverser Informations- und Fehlermeldungen über IPv4. Für IPv6 gibt es ICMPv6.

1. ICMP verwendet unterschiedliche Code-Felder. Suchen Sie auf der Website – [www.iana.org](http://www.iana.org) – nach einer Seite die die Informationen über ICMP Parameter enthält – RFC 792.
   1. Welcher Bezeichner wird für Type 0 verwendet?

- Für Typ 0 wird der Bezeichner „Echo Reply“ verwendet.

* 1. Welcher Bezeichner wird für Type 3 verwendet?

- Für Typ 3 wird der Bezeichner „Destination Unreachable“ verwendet.

1. Wann erhält man die Echo-Antwort - Erklärung
   1. Destination unreachable?

- Der Frame konnte sein Ziel nicht erreichen.

* 1. Time to live exceeded?

- Die Daten haben zu lange gebraucht, um an ihr Ziel zu kommen und wurden verworfen.

## Kommunikation bei Verwendung von ICMPv6 – Neighbor Discovery Protokoll

Um ICMPv6 mit Wireshark mitschneiden zu können muss IPv6 aktiviert werden. Unter IPv6 kann ein PC mehrere IPv6 Adressen haben, aber nur eine einzige IPv4 Adresse. Wenn beide IP-Adressarten verwendet werden, dann benutzt Windows zuerst IPv6 und wenn diese nicht möglich ist, dann IPv4

### Laborvorgangsweise für 3.3

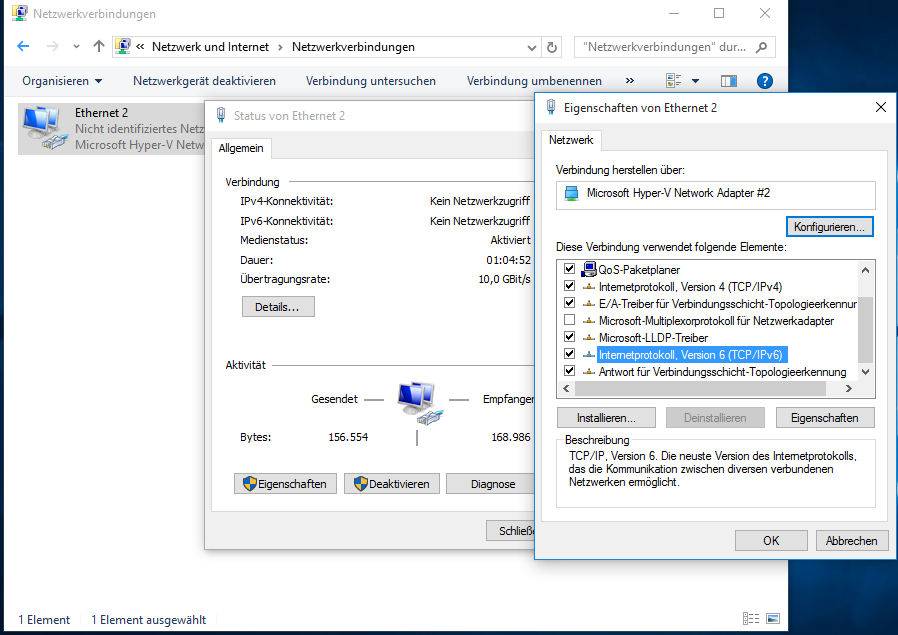
1. Öffnen Sie den „**Netzwerk und Freigabe Center**“. Klicken Sie anschließend auf „**Adapter Einstellungen ändern**“ um ein Fenster zu öffnen. Öffnen Sie im Anschluss die Eigenschaften der Netzwerkkarte und aktivieren Sie das IPv6 Protokoll. 

Abb: Netzwerkkarte mit aktiviertem IPv6

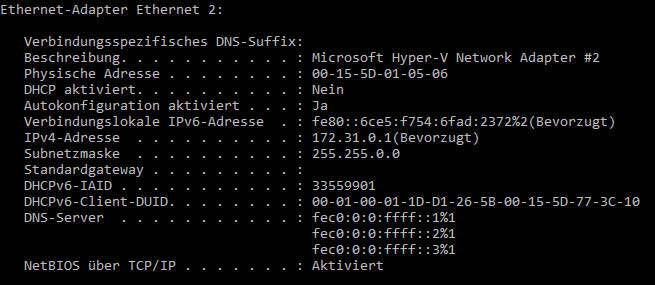
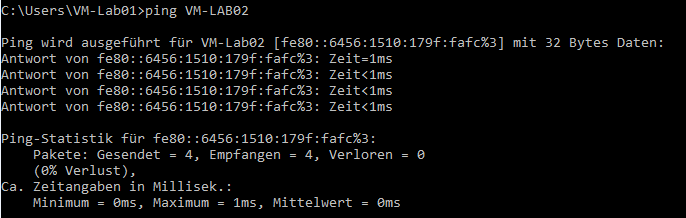
1. Überprüfen Sie anschließend die dem Adapter zugewiesenen IP-Adressen  
   *Abb: Adapter Konfiguration*
2. Starten Sie Wireshark
3. Pingen Sie den PC VM-LAB02 mit Namen an

Abb: ping auf VM-LAB02 mit IPv6

1. Beenden Sie Wireshark

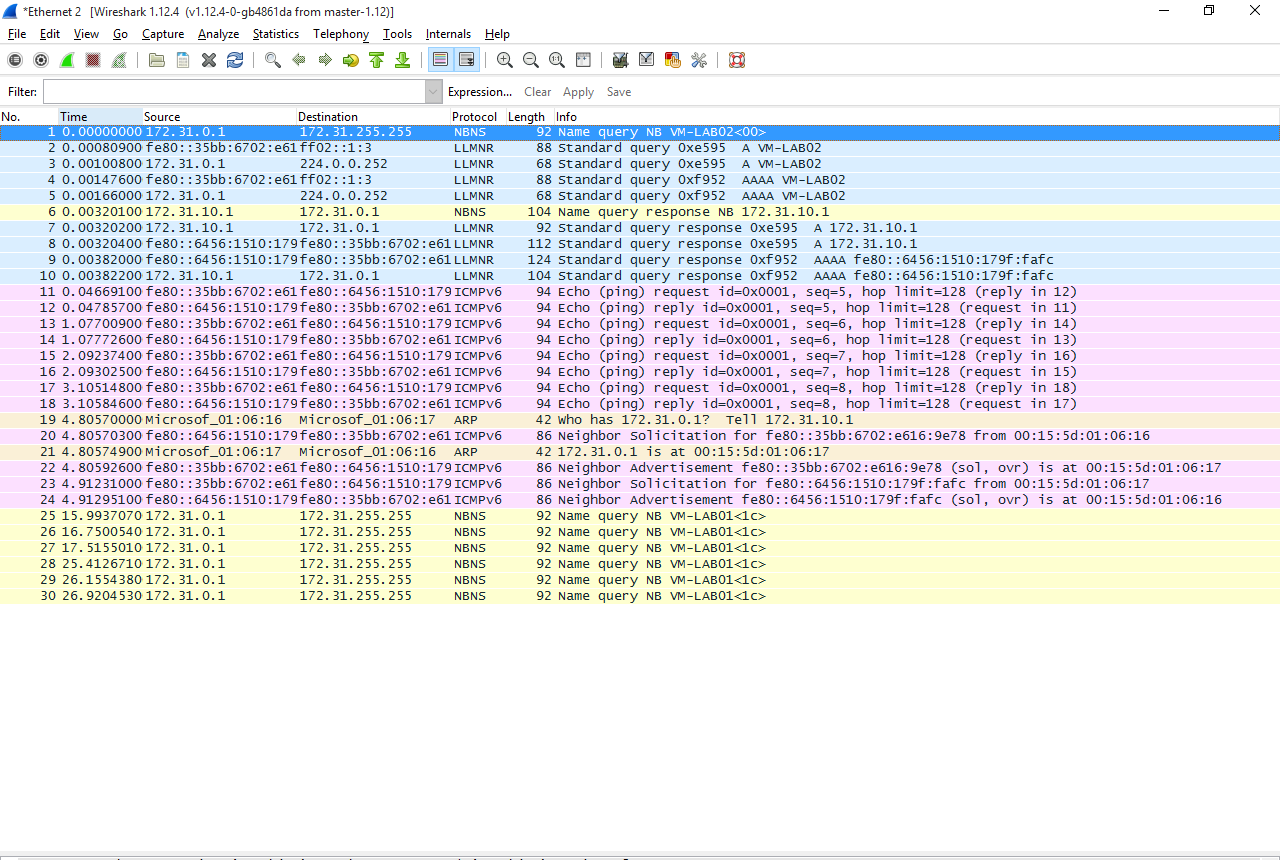


Abb: 06-LAB-03.pcapng  
Speichern Sie den Mitschnitt unter **06-LAB-03.pcapng** ab

### Analyse und Fragen zu 3.3

1. Wie viele Datenpakete waren notwendig um den PC VM-Lab02 unter IPv6 anzupingen?

- Es waren 8 Datenpakete nötig, um VM-Lab02 unter IPv6 anzupingen.

1. Welches Transportschichtenprotokoll, welcher Port wurde verwendet? Begründen Sie Ihre Antwort

- Es wurde das Protokoll LLMNR verwendet und vom Port 51799 an den Port 5355 gesendet.

1. An welche Ziel-MAC-Adresse wurde das erste Paket von 172.31.0.1 geschickt? Öffne dazu den Paket-Detail Bereich und analysiere den Mitschnitt des OSI Layer 2

- Die Ziel-MAC-Adresse lautet 00:15:5d:01:06:17

### Recherchen zu 3.3

1. Welche drei Arten von IPv6 Adressen kennen Sie?

- Es gibt sog. Link-Local Adressen, Site-Local Unicast und Unique-Local Unicast

1. Wie nennt man unter IPv6 eine Adresse die mit „fe80“ beginnt?

- Diese sind sog. Link-Local Adressen. Sie werden nicht geroutet und sind nur innerhalb eines Netzes gültig. Sie sind aus dem Internet aus nicht erreichbar.

1. Was bedeutet der Ausdruck „%10“ am Ende einer IPv6 Adresse mit dem Präfix „fe80“?

- Die Zahl hinter dem % ist die Scope-ID. Sie bestimmt, über welche Link-Local Adresse einen für einen Befehl verwendet wird. Sind zum Beispiel 2 Netzwerkkarten in einem PC und man führt den ping-Befehl aus, bestimmt die Scope-ID, welche Link-Local Adresse als Source-IP verwendet wird.

1. Wie lautet das IPv6 Gegenstück zu 127.0.0.1?

- Das IPv6-Gegenstück lautet ::1

## Drei Wege Handshake beim Aufbau einer TCP-Sitzung mit einem Web-Server

Auf VM-Lab02 muss für die nachfolgende Übung ein Web Server installiert sein. Bitte überprüfen Sie dies. Falls dies nicht der Fall ist, dann installieren Sie einen Web-Server – Internet Informationsdienste - über Programme und Features.

Der Verbindungsaufbau mit einem Web-Server erfolgt unter TCP, wobei eine Session eingerichtet wird. In der nachfolgenden Übung soll dieser Verbindungsaufbau – auch drei Wege Handshake – näher untersucht werden.

### Laborvorgangsweise für 3.4

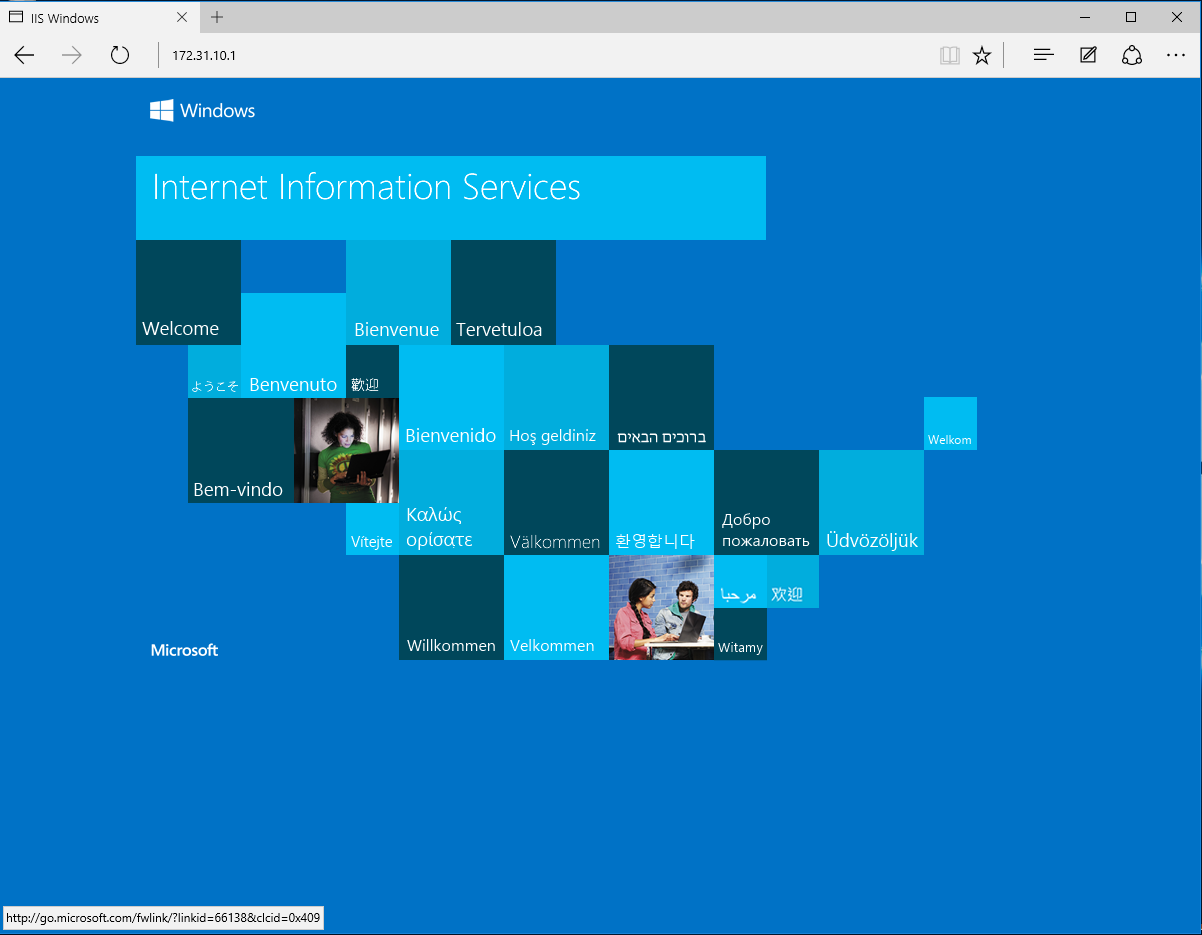
1. Überprüfen Sie, ob auf VM-Lab02 ein Webserver eingerichtet wurde. Öffnen Sie zur Kontrolle die Website 172.31.10.1
2. Leeren Sie den ARP-Cache auf VM-LAB01 und VM-LAB02
3. Leeren Sie den Cache des Browsers und schließen Sie diesen anschließend
4. Starten Sie Wireshark
5. Öffnen Sie den Browser und rufen Sie die Website 172.31.10.1 auf**

Abb: Browser

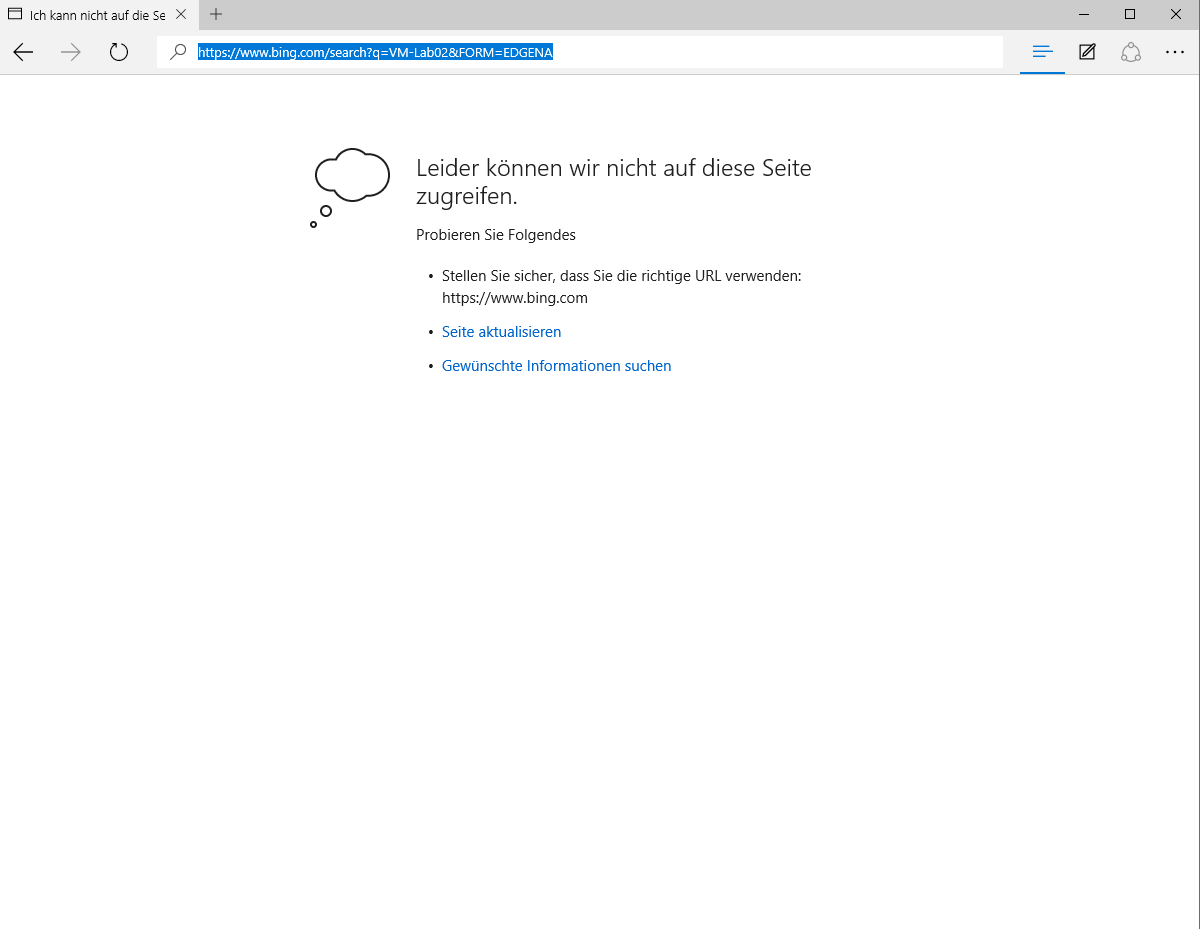
1. Leeren Sie den Browsercache Browser und rufen Sie die Website über den Namen VM-Lab02 auf

Abb: Browser nach leeren des Caches.

1. Beenden Sie den Mitschnitt und speichern Sie diesen unter 06-LAB-04.pcapng

### Analyse und Fragen zu 3.4

1. Sie wollen einen Anzeigefilter setzen um die Frames 1 bis 10 anzuzeigen. Was müssen Sie dabei im Anzeigefilter eingeben?

- Die Eingabe lautet: frame.number >= 1 && frame.number <= 10

1. Wie viele Frames waren notwendig, bis die http-Sitzung eingerichtet war

- Es waren insgesamt 3 Frames notwendig, bis ein Paket mit dem HTTP Protokoll gecaptured wurde.

1. Welche Ports auf Sender/Empfängerseite – aus Sicht von VM-LAB01 – wurden verwendet?

- Sender: 49421, Empfänger: 80

### Recherchen zu 3.4

1. Beschreibe den Verbindungsaufbau einer TCP-Verbindung mit dem Webserver.

- Der Rechner sendet ein TCP-Segment ohne Daten an den Webserver, wo die SYN (= Synchronization) Flag gesetzt ist und eine Sequence Number (eine beliebige Zahl) übertragen wird.

Sobald der Webserver das Segment empfangen hat, überprüft er, ob der angesprochene Port geöffnet ist. Ist dies nicht der Fall, wird der Verbindungsaufbau abgebrochen. Anderenfalls antwortet der Server mit einem TCP-Segment, welches eine eigene Sequence Number im TCP Header enthält. Außerdem sind auch die SYN- und die ACK- (= Acknowledgement) Flag gesetzt und die Sequence Number vom Anforder (dem Rechner) wird um eins erhöht und im ACK-Number Feld des TCP-Segments eingetragen.

Um den Erhalt des TCP-Segments vom Webserver zu bestätigen, erhöht der Rechner sowohl seine, als auch die Sequence Number vom Webserver um 1, wobei er die vom Webserver im Acknowledgment Number Feld des TCP-Segments und seine eigene im Sequence Number Feld des TCP-Segments einträgt. Zum Schluss wird die ACK-Flag gesetzt und das Segment wird zum Webserver geschickt. Die Verbindung ist nun aufgebaut.

1. Sie wollen die Verbindung zu ihrem Bank-Webserver schließen und loggen sich aus. Beschreibe den Verbindungsabbau einer TCP-Verbindung der dabei vorgeht.

- Der Rechner sendet ein FIN-Segment an der Webserver, welches zeigt, dass der Rechner keine Daten mehr senden will. Außer der gesetzten FIN-Flag sind noch die Sequence Number, sowie der Source- und der Destination- Port im TCP-Header angegeben.

Der Webserver bestätigt den Erhalt dieses Segments mit einem TCP-Segment, bei dem die ACK-Flag gesetzt, und die Sequence Number um eins erhöht wird. Diese erhöhte Sequence Number wird in das Acknowledgement Number Feld eingetragen.

Nachdem der Webserver alle anstehenden Daten an den Rechner gesendet hat, sendet er ebenfalls ein FIN-Segment, das genauso aufgebaut ist, wie das FIN-Segment vom Rechner.

Der Rechner bestätigt den Erhalt des FIN-Segments des Webservers mit einem ACK-Segment. Dieses ist wiederum genauso aufgebaut, wie das ACK-Segment des Webservers zur Bestätigung des Erhalts des FIN-Segments des Rechners, außer, dass die Sequence Number des FIN-Segments des Servers um eins erhöht wurde. Die Verbindung ist nun geschlossen.

1. Während einer TCP-Verbindung nimmt diese überschiedliche Stadien an. Welche Stadien einer TCP-Verbindung gibt es?

- SYN – Synchronisierung

- ACK – Anerkennung (Bestätigt den Erhalt von Daten.)

- PSH – Schieben (Sender signalisiert, dass der TCP Treiber die Daten zur Applikation hoch „schieben“ soll, wenn er fertig gesendet hat.)

- URG – Dringend (Weißt auf einen „Urgent-Pointer“ im TCP-Header hin. Dieser markiert eine bestimmte Byte-Position in der Nutzdatenmenge.)

- FIN – Final (Signalisiert, dass die Verbindung abgebaut werden kann.)

- RST – Zurücksetzen (Zum Abbrechen einer Sitzung oder zum Ablehnen einer SYN-Flag.)

1. Die Ports werden in drei Gruppen eingeteilt. Wie lauten diese Gruppen

- System Ports (0 – 1023)

- Registered Ports (1024 – 49151)

- Dynamic Ports (49152 – 65535)