NVS

Laborprotokoll – 06 –Wireshark & TCP/IP

Alexander Brenner

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.

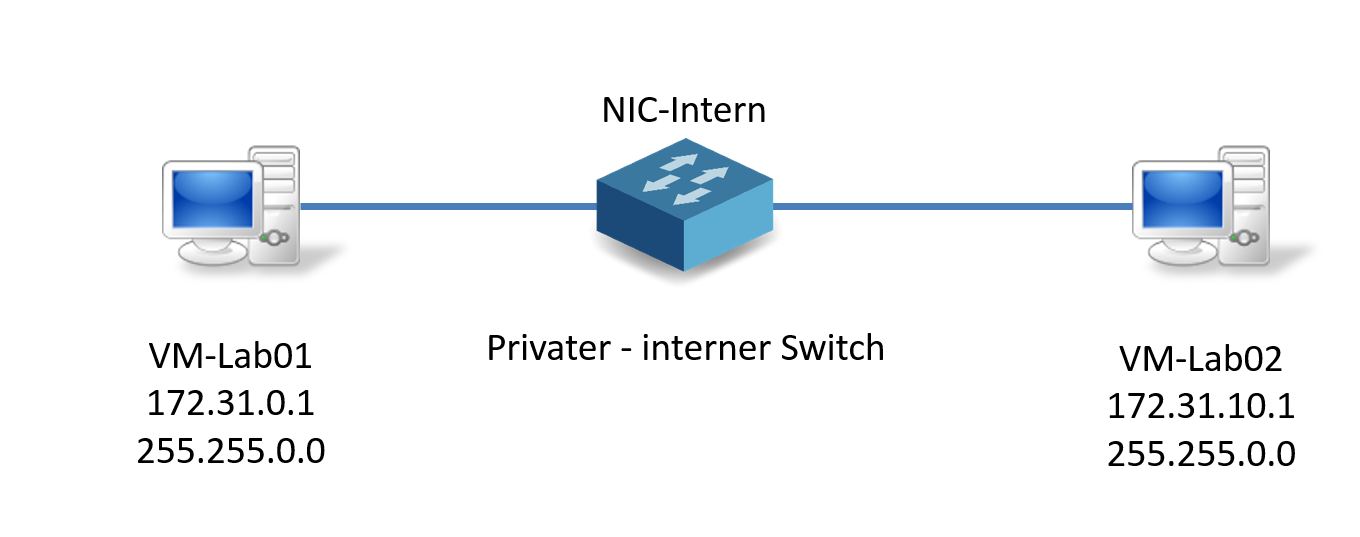


Abbildung: PCs und IP-Adressen für das Labor 06

# 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:

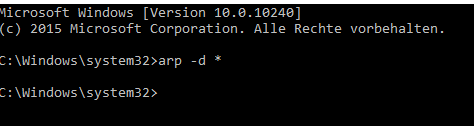
* Funktionsweise von ARP
* Kommunikation bei ICMPv4
* Kommunikation bei Verwendung von ICMPv6
* Drei Wege Handshake beim Aufbau einer TCP-Sitzung

# Durchführung des Labors

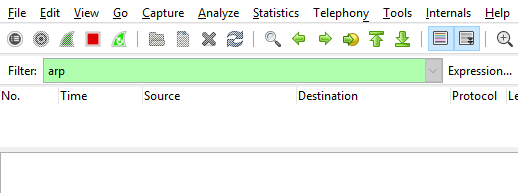
## Funktionsweise von ARP

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

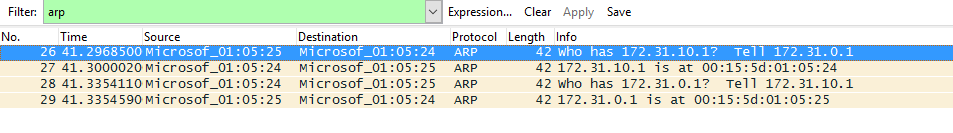
* Anmeldung auf VM-LAB01
* Lösche den Arp-Cache von VM-LAB01 

*Abb.1: Löschen des ARP-Caches*

* Starte Wireshark
* Erstelle einen Caputre-Filter der nur das ARP-Protokoll aufzeichnet

*Abb.2: ARP-Mitschnittsfilter links-oben*

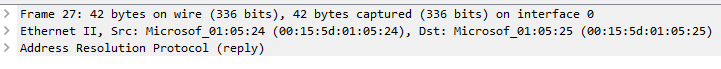
* Starte die Aufzeichnung
* Führe nun einen Ping auf 172.31.10.1 aus (damit muss eine ARP-Auflösung erfolgen des Zielrechners erfolgen - nicht den Name VM-LAB02 verwenden)
* Beende die Aufzeichnung



*Abb.3: Mitschnitt in Wireshark*

* 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.  
   

**Nach 2 Datenpaketen konnte die MAC-Adresse herausgefunden werden. Einzelheiten im Screenshot.**

1. Welches Protokoll wurde verwendet?

**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

**00:15:5d:01:05:24**

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

**Request (1)**

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

**2. Data-Link-Layer**

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

**3.Network-Layer**

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

**Internet-Layer**

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

**Host-To-Host (Transport-Layer)**

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

**Network-Layer, Internet-Layer**

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

**Wenn das Datenpaket an eine andere Netzwerkkarte gesendet wird.**

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.

**ARP-Spoofing**

### 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?

**Wenn der ARP Cache nicht gelöscht wurde dann nicht da die Adressen bereits aufgelöst wurden.**

1. Wozu wird RARP verwendet?

**RARP (Reverse Access Resolution Protocol) ist zur Zuordnung bzw. Verknüpfung von einer MAC und IP Adresse zuständig.**

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

**Nein es gibt keines, weil RARP nicht dynamisch ist und von 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.

**Layer-2: Frames**

**Layer-3: Packets**

**Layer-4: Segments**

**Layer-5: Data**

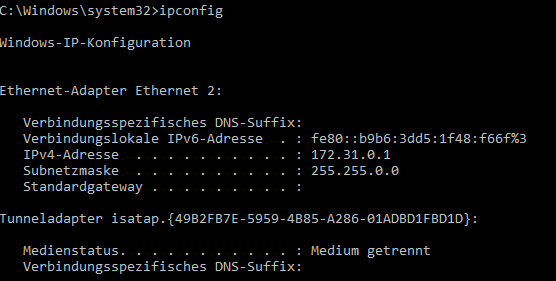
**Layer-6: Data**

**Layer-7: Data**

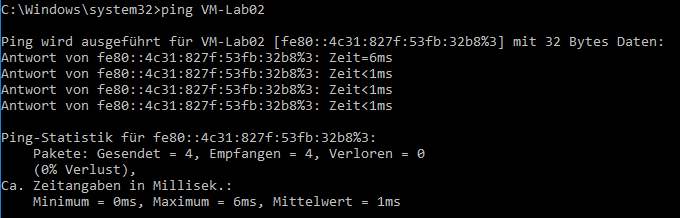
## Kommunikation bei ICMPv4

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

### Laborvorgangsweise für 3.2

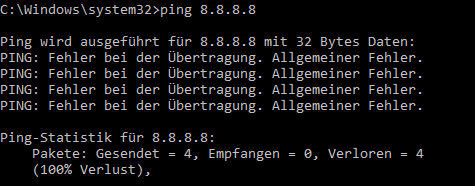
1. Überprüfen Sie anschließend die dem Adapter zugewiesenen IPv4-Adressen  
   **

*Abb.4: IP der VM-01*

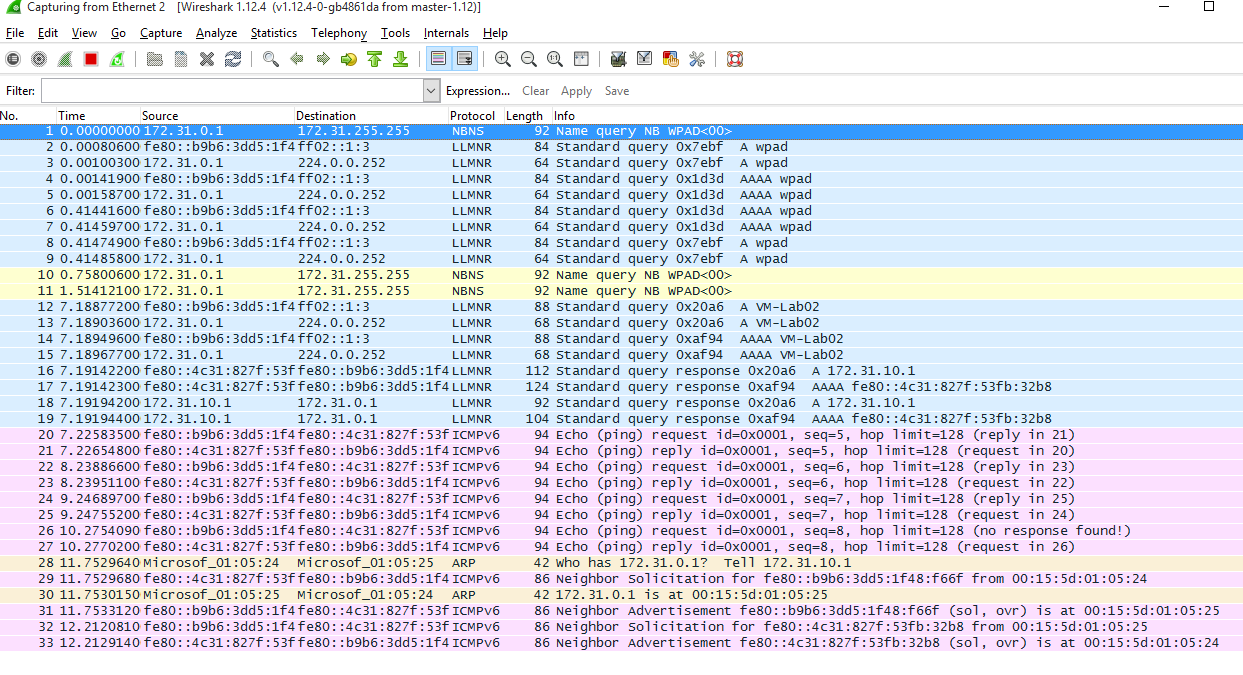
1. Starten Sie Wireshark
2. Pingen Sie den PC VM-LAB02 mit Namen an  
   **

*Abb.5: Ping durch den VM-Namen*

1. Pingen Sie den PC mit der IP-Adresse 8.8.8.8 an

**

*Abb.6: Ping durch 8.8.8.8*

1. Beenden Sie Wireshark  
   **

*Abb.7: Mitschnitt in Wireshark*

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

**Internet Control Message Protocol wird für die Übertragung von Statusinformationen und Fehlermeldungen verwendet.**

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?

**„Echo Reply“**

* 1. Welcher Bezeichner wird für Type 3 verwendet?

**„Destination Unreachable“**

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

**Man erhält diese wenn die Ziel-Adresse nicht vorhanden ist oder nicht erreichbar ist.**

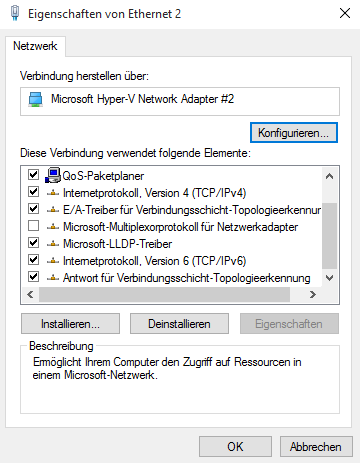
* 1. Time to live exceeded?

**Diese Antwort erscheint wenn die Datenübertragung zu lange gedauert hat bzw. wenn die Daten zu lange gebraucht haben um an ihr Ziel zu kommen.**

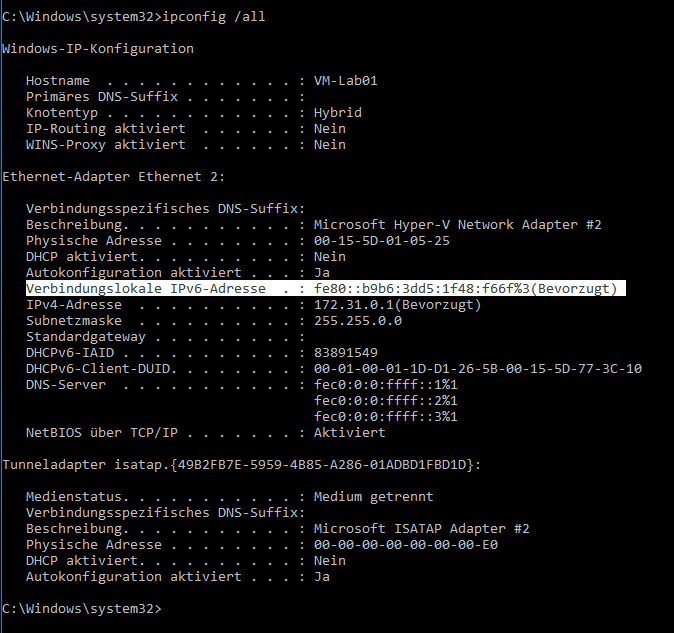
## Kommunikation bei Verwendung von ICMPv6 – Neighbor Discovery Protokoll

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

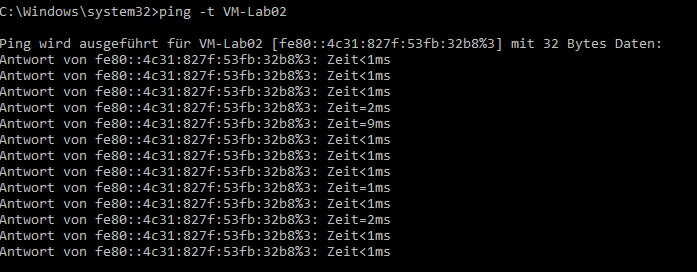
### Laborvorgangsweise für 3.3

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.   
   **

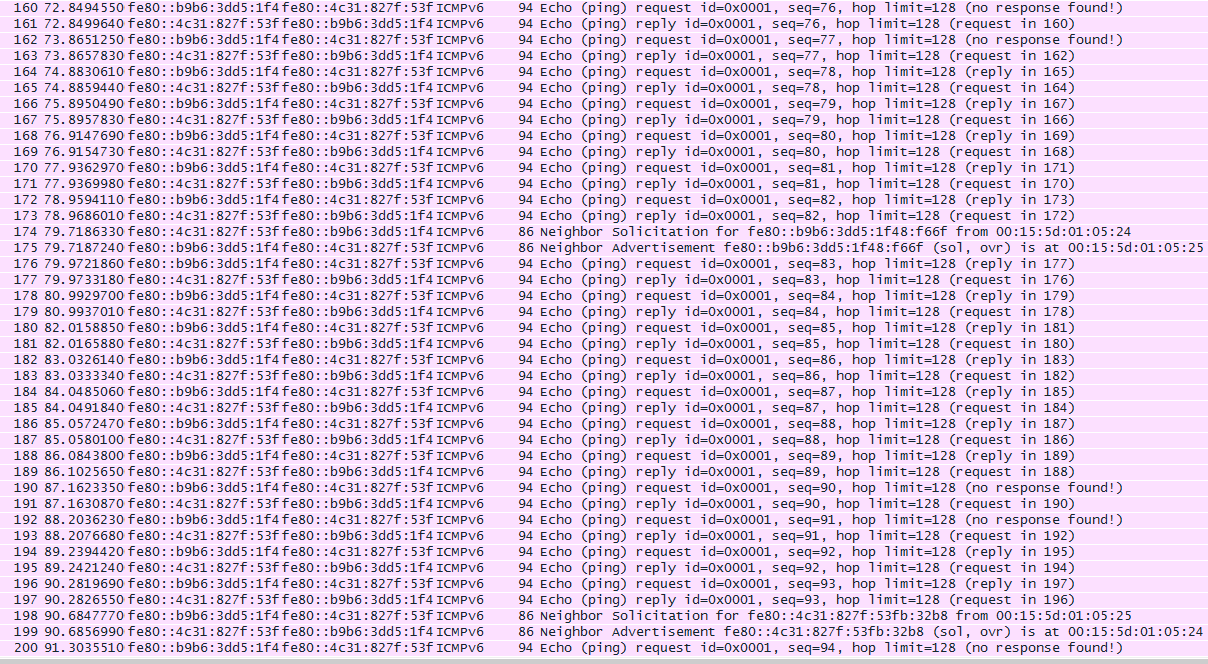
*Abb.8: IPv6 Konfiguration*

1. Überprüfen Sie anschließend die dem Adapter zugewiesenen IP-Adressen  
   **

*Abb.9: IPv6*

1. Starten Sie Wireshark
2. Pingen Sie den PC VM-LAB02 mit Namen an  
   **

*Abb.10: Dauerping an VM-Lab02*

1. Beenden Sie Wireshark  
   **

*Abb.11: Mitschnitt in Wireshark*

1. 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 wurden 8 Datenpakete benötigt.**

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

**ICMPv6, Port: 1, da Wireshark dies anzeigt.**

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

**00:15:5d:01:05:24**

### Recherchen zu 3.3

1. Welche drei Arten von IPv6 Adressen kennen Sie?

**Unicast-Adressen, Multicast-Adresse, Anycast-Adressen**

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

**Link-Local-Adresse**

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

**Die Zahl nach der IP ist die sogenannte Zone-ID. Mit Hilfe dieser wird bestimmt, wenn mehrere Netzwerkkarten in einem PC sind, welche Adresse als Source-IP verwendet wird.**

1. Wie lautet das IPv6 Gegenstück zu 127.0.0.1?

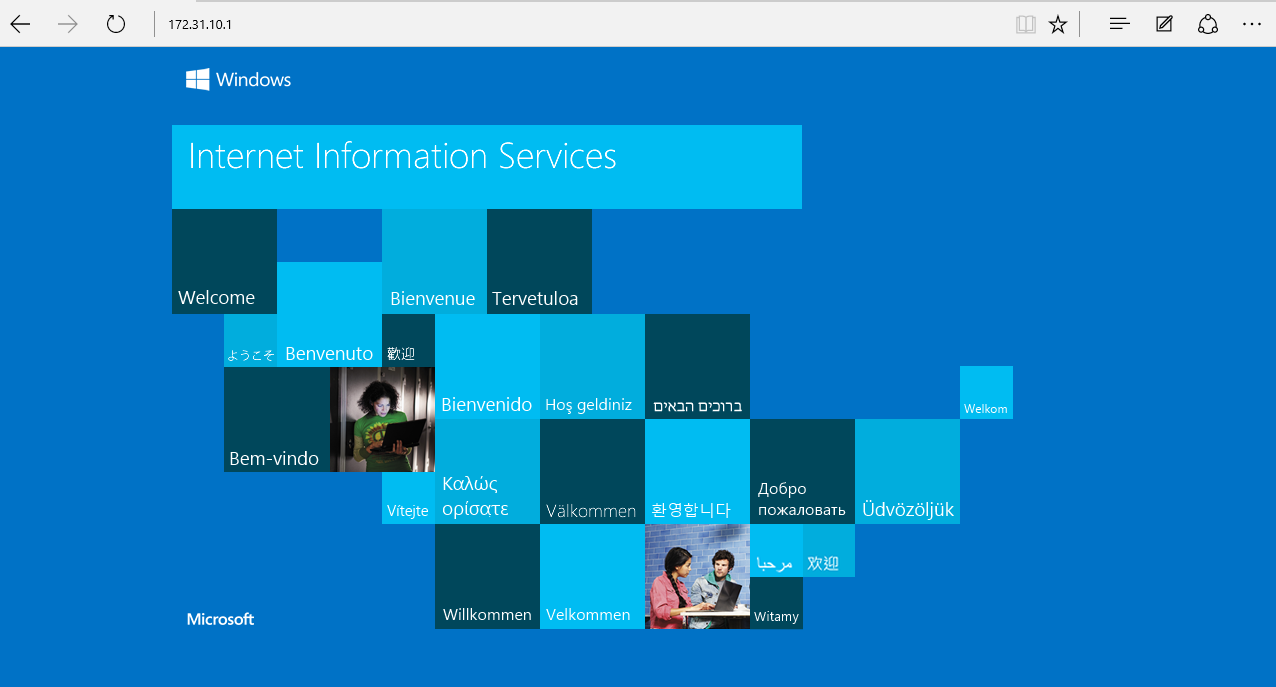
**0:0:0:0:0:ffff:7f00:1**

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

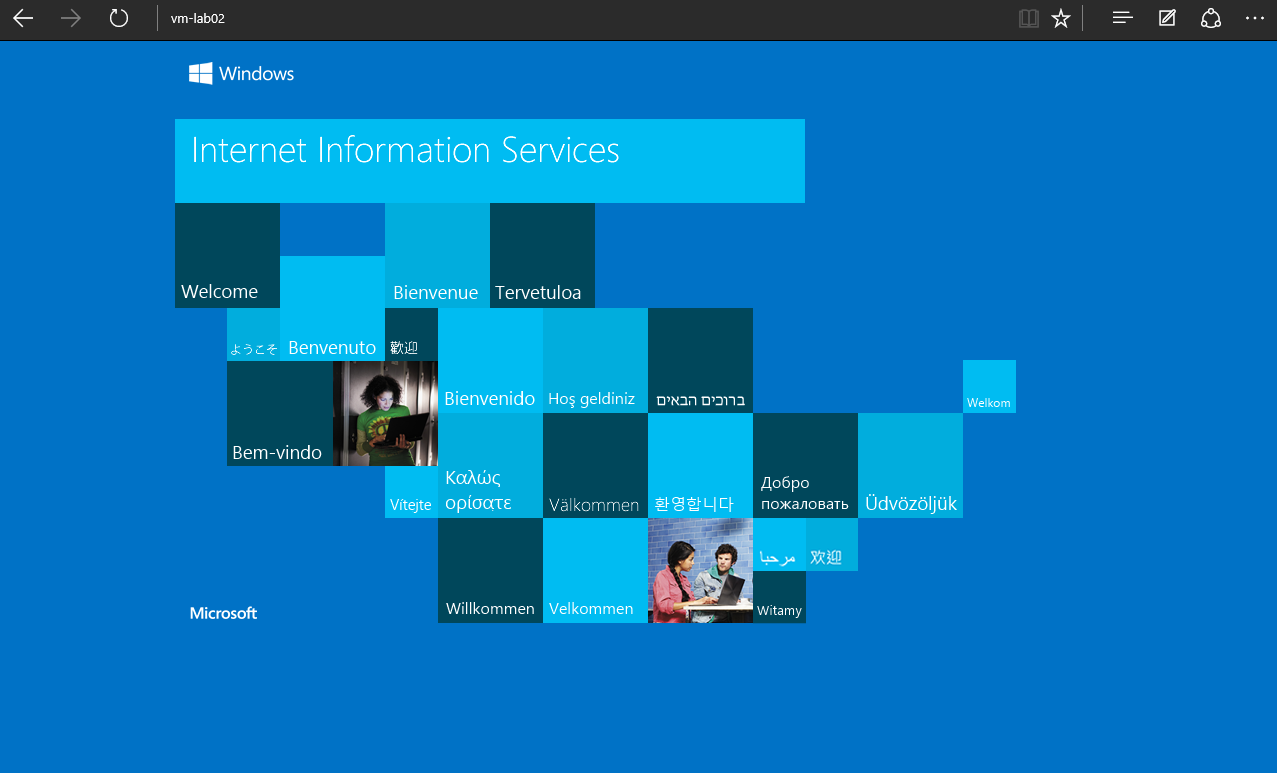
Auf VM-Lab02 muss für die nachfolgende Übung ein Web Server installiert sein. Bitte überprüfen Sie dies. Falls dies nicht der Fall ist, dann installieren Sie einen Web-Server – Internet Informationsdienste - über Programme und Features.

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.12: Aufruf des Webservers durch IP-Adresse*

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

*Abb.13: Aufruf des Webservers durch Name*

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?

**„frame.number >= 1 && frame.number <= 10“**

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

**Es waren 3 Frames notwendig.**

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

**Source Port: 49414 | Destination Port: 80**

### Recherchen zu 3.4

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

**Die VM-01 sendet eine http request und der der Webserver auf der VM-02 antwortet dann mit der Website.**

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

**Man sendet eine http request zu dem Webserver der Band und diese schließt dann die Sitzung und liefert die Bank-Website als Antwort zurück.**

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

**Listen, Syn-(Sent, Received), Established, Close-Wait, Close, Last-Ack, Fin-Wait-1, Fin-Wait-2, Closing, Time-Wait**

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

**Well-Known Ports, Registered Ports, Dynamically Allocated Ports**