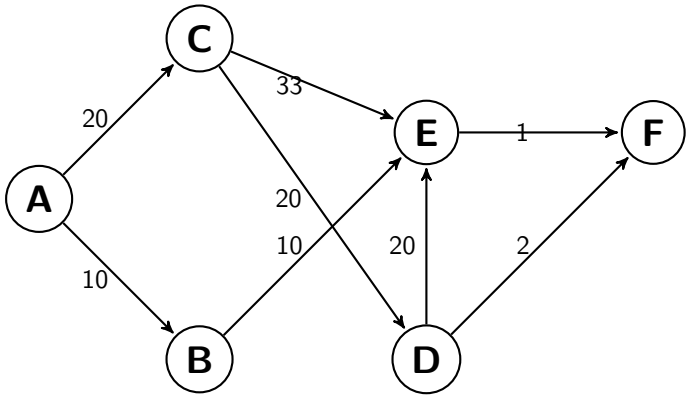
Übungsblatt 4 – Routing, ICMP, IP & ARP

Aufgabe A – Routing-Algorithmen

1. In der Vorlesung haben sie zwei Routing-Algorithmen kennen gelernt. Dies sind das Distanz-Vektor- und Link-State-Routing. Beide ermöglichen es den kürzesten Weg durch einen Graphen zu finden (Shortest-Path-Problem).
   Für gewöhnlich wird für das Distanz-Vektor-Routing der Bellman-Ford-Algorithmus verwandt, das Link-State-Routing nutzt den Dijkstra-Algorithmus. [**Kurose2012**]
   a) Erläutern sie das Link-State-Routing unter Nutzung des Dijkstra-Algorithmus [**Kurose2012**].
   b) Erläutern sie das Distanz-Vektor-Routing unter Nutzung des Bellman-Ford-Algorithmus [**Kurose2012**].
   c) In welchen Protokollen finden diese beiden Protokollen Verwendung? Ist diesen Protokollen etwas gemein?
   d) Erläutern sie die fundamentalen Unterschiede beider Lösungsansätze. Was unterscheidet Bellman-Ford und Dijkstra? **Hinweis:** Wie betrachtet der Algorithmus den Graph?
   e) Das Exterior-Gateway-Protokoll nutzt keines der beiden obigen Algorithmen, sondern ein Pfad-Vektor-Protokoll. Können sie Gründe nennen, warum weder Bellman-Ford noch Dijkstra genutzt wird?
   f) Diskutieren sie, ob der Bellman-Ford-Algorithmus für das Link-State-Routing und der Dijkstra-Algorithmus für das Distanz-Vektor-Routing genutzt werden könnte.

2. Gegeben sei folgender Graph:



   Finden sie den kürzesten Weg vom Knoten A zum Knoten F!
   a) Nutzen sie zunächst den Dijkstra-Algorithmus.

b) Nutzen sie den Bellman-Ford-Algorithmus.

3. Das *Border Gateway Protocol* wendet den sogenannte „Best Path Algorithm“ an. Erläutern sie wie ein BGP Router die Route wählt, falls mehrere Pfade (Path/-Teilrouten) verfügbar sind. [1]

4. Im gewöhnlichen BGP-Routing werden die Policies als „Valley Free“ bezeichnet. Erläutern sie warum „Valley Free Routing“ eine gute Policy-Entscheidung ist.[2]

Aufgabe B – Traceroute

1. Lesen sie die folgenden Artikel:
   https://www.freebsd.org/cgi/man.cgi?query=traceroute
   https://docs.freebsd.org/de_DE.ISO8859-1/books/handbook/network-routing.html Abschnitt 31.2.3. Problembehandlung Beantworten sie anschließend folgende Fragen:
   a) Wofür wird Traceroute genutzt?
   b) Wie wird Traceroute umgesetzt, d.h. wie läuft eine Routen-Verfolgung ab?
   c) Welche ICMP-Messages werden für die Realisierung genutzt?
   d) Welche Limitationen ergeben sich aus dieser Umsetzung?
   e) Dokumentieren sie die Syntax, sowie die Bedeutung von Traceroute beispielhaft.

Aufgabe C – Address Resolution Protocol (ARP) & Neighbor Discovery Protocol (NDP)

Es sollte ihnen aufgefallen sein, dass in der zweiten Übung (Geswitchte Netze) ihr Netzwerk in der Planung zwar IP-Adressen nutzt, aber kein Router Verwendung fand. Im Labor würde ein Switch zum Einsatz kommen. Switches sind OSI-Layer 2 Geräte und kommen ohne IP-Adressen zurecht. Ihre VMs verlangen jedoch zwingend eine IP-Adresse von Ihnen.

1. Recherchieren sie mithilfe der Literatur was *ARP* ist [**Kurose2012**]

2. Wie adressiert ein Switch die Frames zwischen den Endknoten (also den VMs)? **Hinweis:** Wie oben bereits erwähnt geschieht dies nicht mittels IP-Adressen.

[1] In der echten Welt ist dies durchaus komplexer, s. https://www.ietf.org/rfc/rfc4271.txt.
[2] Dieser Blog-Eintrag könnte hilfreich sein: https://blog.ipspace.net/2018/09/valley-free-routing.html

3. Erläutern sie das *MAC*-Adressschema. Kann dieses Adressschema auch zu Problemen führen?

4. Unter *IPv6* gibt es kein *ARP*, wie wird dies dort gehandhabt? Bzw. wie funktioniert *NDP*?

5. Recherchieren sie wozu die Werkzeuge *arp* und *ip neigh* in unixoiden Betriebssystemen genutzt werden können.

6. Recherchieren sie die grundlegende Syntax und Semantik von *arp* sowie *ip neigh*.

Aufgabe D – IP

Im Moodle-Kurs liegt eine Zip-Datei `network_packets.zip`. Diese enthält verschiedene Dateien die sie auf verschiedene Arten in Wireshark öffnen können. Sie sollen diese Pakete analysieren. Teilweise sind in diesen Paketen Passwörter und Zugangsdaten zu finden, in einigen Fällen können ganze Nachrichten oder Geräteinformationen gefunden werden.

1. Öffnen sie aus dem Zip-Archiv die Datei `ch1.pcap` mit Wireshark. Stellen sie den Filter auf *IP*. Suchen sie sich ein IP-Paket heraus. Wo finden sie folgenden Informationen?
   - Welche Adressen sind im Paket enthalten? Wie viele sind dies?
   - Ethernet hat eine Prüfsumme, TCP ebenfalls. Hat IP eine Prüfsumme?
   - Ist IP ein verbindungsorientiertes Protokoll? Begründen sie ihre Antwort anhand der eben vorgenommen Analyse. Welche Information des Pakets legt ihren Schluss dar.
   - Ein IP-Paket besteht aus Header und Payload. Wo und wie wird die Trennung festgelegt?
   - Wo ist die Information der nächst höheren Protokollebene zu finden?

Aufgabe E – ICMP

Da die Befehle *ping* und *traceroute ICMP* nutzen, sollen Sie mit Wireshark solche Request mitverfolgen.

1. Setzen sie alle notwendigen Parameter um Wireshark mitlaufen zu lassen, sodass sie die ICMP-Nachrichten mitverfolgen können.

2. Nutzen sie Traceroute um einen Rechner mit seinen DNS-Namen zu erreichen (bspw.: `mi.fu-berlin.de`).

3. Ping auf die IP-Adresse ihres Routers.
   Hinweis: Sie können diese durch *netstat* in Erfahrung bringen.

```
#or.
netstat −nr
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 XXX.XXX.XXX.1 0.0.0.0 UG 0 0 0 pf−bridge
XXX.XXX.128.0 0.0.0.0 255.255.255.0 U 0 0 0 igb0
XXX.XXX.0.0 0.0.0.0 255.255.255.128 U 0 0 0 igb1
...
XXX.XXX.32.128 0.0.0.0 255.255.255.248 U 0 0 0 igb3
...
```

4. Nehmen sie nun eine ihrer Ping-Anfragen und analysieren sie diese mithilfe Wiresharks genauer.
   a) Auf welcher Ebene des OSI-Modells ist das ICMP-Protokoll einzuordnen? Begründen sie ihre Antwort!
   b) Analysieren sie mithilfe Wiresharks den Aufbau eines ICMP-Pakets. Wie ist der generische Aufbau? Skizzieren sie den Aufbau mithilfe der in Abb. **??**.

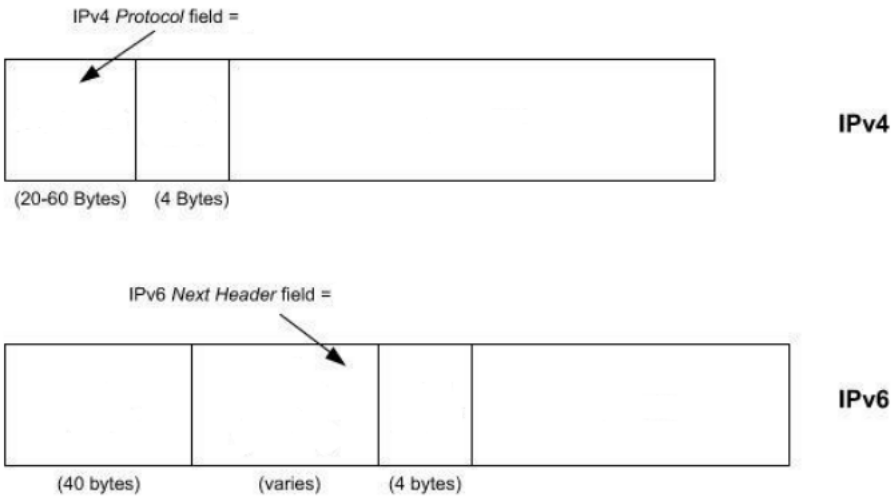


Abbildung 1: Generischer Aufbau eines ICMP-Pakets für IPv4 und IPv6.

   c) Welche Nachrichtentypen werden für den Ping-Messages genutzt? Wo sind die Nachrichtentypen zu finden?
   d) Skizzieren sie mithilfe von Abb.**??** die ICMP-Nachricht und welche Informationen Wireshark ihnen liefert.

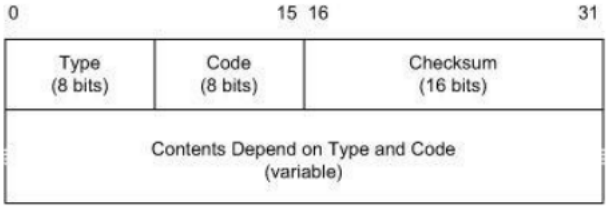


Abbildung 2: Nutzlast eines ICMP-Pakets.

5. Starten sie eine Routen-Verfolgung via *traceroute* auf eine beliebige Adresse. Verfolgen sie dabei die Ausgabe auf der Konsole und Wireshark (Filtern sie in Wireshark entsprechend). Spiegeln sich die Einträge in Wireshark mit denen auf der Kommandozeile?
6. Welche ICMP-Nachrichten wurden hier verwendet?
7. Erläutern sie die genaue Routen-Verfolgung mithilfe der ICMP-Nachrichten. Welches Feld wird hier genutzt um jeden Hop „verfolgen“ zu können?
8. Überlegen sie sich zunächst anhand Ihrer Recherche was *traceroute* in etwa ausgeben müsste, wenn sie auf der VM eine Route von einem Rechner A zu einem Rechner B verfolgen würden. Wobei beide Rechner zu unterschiedlichen LANs gehören.
9. Nutzen Sie anschließend *traceroute* um sich die Router zwischen zwei VMs anzeigen zu lassen. Stimmen Ihre theoretische Überlegungen mit denen von *traceroute* überein? Falls nicht, sollten Sie analysieren woran dies liegen könnte.

Aufgabe F - Bestimmung des physischen Rechners zu einer IP-Adresse – ARP

Sie haben bereits theoretisch recherchiert, wie die Zuordnung von physischer Adresse zu einer IP-Adresse vonstatten geht. Im Folgenden sollen sie herausfinden, ob die Auflösung von IP-Adresse auf physische Adresse wirklich analog zu ihren theoretischen Recherchen abläuft.

1. Um einen ARP-Request auszulösen können sie das Werkzeug *arp* nutzen. Lesen sie in der *man*-Page:
   - Wie können sie sich ihre MAC-Adresse und Interface anzeigen lassen?
   - Wie können sie sich den ARP-Table ausgeben lassen?
   - Wie leeren sie den ARP-Cache?
2. Finden sie mithilfe Wiresharks heraus, wie die Adressauflösung funktioniert.

a) Starten sie Wireshark und stellen sie das korrekte Interface ein.

b) Leeren sie zunächst den ARP-Cache.

c) Pingen sie nun einen Rechner an, den sie vorhin noch nicht „angepingt“ haben. Die dafür ausgetauschten Pakete werden nun „gesnifft“.

d) Beenden sie das Mitschneiden des Netzwerksverkehrs und setzen sie als Filtern die MAC-Adresse ihres Adapters.

e) Versuchen sie über den Mitschnitt herauszufinden, wie die Bestimmung des zugehörigen Netzadapters und die MAC-Adresse erfolgt.

3. Damit ihr Rechner nicht jedes mal eine Auflösung veranlassen muss, werden die ARP-Informationen lokal in einem Cache zwischengespeichert („cached“).

   a) Lassen sie sich Ihren aktuellen ARP-Cache anzeigen. Welche Informationen können sie diesem entnehmen?

   b) Schauen sie kurz nach, wie lange der ARP-Cache Einträge vorhält.

   c) Lassen sie zwei VMs die IP-Adressen tauschen. Dies sollte möglichst schnell umgesetzt werden!

   d) Versuchen sie nun durch eine dritte VM eine „alte“ IP-Adresse zu erreichen. Werden die Daten an den richtigen Knoten übermittelt?

   e) Verfolgen sie die Datenübermittlung per Wireshark mit.