

10. Übung zur VL Betriebs- und Kommunikationssysteme

Tutor: Thomas Tegethoff

Bearbeiter: Etienne Jentzsch, Carola Bothe

Aufgabe 1: Internetworking

- Address Resolution Protocol (ARP):

Das ARP ist ein Netzwerkprotokoll und arbeitet auf der Schicht 2, der Sicherungsschicht, des OSI-Schichtenmodells und setzt IP-Adressen in Hardware- und MAC-Adressen um (also in physikalische Adressen). Damit ein IP-Paket innerhalb eines lokalen Netzwerks zugestellt werden kann, muss die Hardware-Adresse des Ziels bekannt sein, dies geschieht durch die Adressauflösung. Dazu sendet der Host einen ARP-Request mit einer MAC-Adresse und diese Meldung wird von jedem Netzwerk-Interface entgegengenommen und ausgewertet, wenn sich dabei ein Host angesprochen fühlt mit dieser IP-Adresse, dann schickt er ein ARP-Reply an den Sender zurück und hinterlegt die Zuordnung in so genannten ARP-Tabellen des Rechners.

Quelle: (<https://www.elektronik-kompodium.de/sites/net/0901061.htm> # https://de.wikipedia.org/wiki/Address_Resolution_Protocol # VL. Folien 10.32 + Mitschrift)

- Internet Protocol (IP):

Das IP ist das am weitesten verbreitete Netzwerkprotokoll und stellt damit die Basis des Internets dar. Das IP ist die Implementierung der Internetschicht (bildet also die erste Schicht der Internetprotokollfamilie) des TCP/IP-Modells bzw. der Vermittlungsschicht (der Network Layer) des OSI-Modells. IP ist ein verbindungsloses, paketorientiertes und nicht garantierendes Protokoll, d.h. die Einhaltung der Reihenfolge der Datenpakete wird weder beim Sender noch beim Empfänger garantiert und identische Datenpakete werden als voneinander unabhängige transportiert.

Quelle: (VL. Folien 10.25 & 10.36 + Mitschrift # https://de.wikipedia.org/wiki/Internet_Protocol)

- Transmission Control Protocol (TCP):

Das Übertragungssteuerungsprotokoll ist auch ein Netzwerkprotokoll, welches die Definition festlegt auf welche Art und Weise die Daten zwischen Netzwerkkomponenten ausgetauscht werden sollen. Das Protokoll ist ein zuverlässiges, verbindungsorientiertes, paketvermitteltes Transportprotokoll! TCP stellt also eine Verbindung zwischen zwei Endpunkten einer Netzverbindung her (mit unseren geliebten Sockets), dadurch können die Daten in beide Richtungen übertragen werden, zudem werden Datenverluste erkannt und behoben, und eine Netzwerküberlastung kann verhindert werden.

Quelle: (VL. Folien 10.23 + Mitschrift # https://de.wikipedia.org/wiki/Transmission_Control_Protocol)

- Internet Control Message Protocol (ICMP):

Das ICMP ist Bestandteil des Internet Protokolls (IP), ist aber ein eigenständiges Protokoll, welches zur Übermittlung von Informations- und Fehlermeldungen über IP dient. Die Hauptaufgabe von ICMP ist die Übertragung dieser Meldungen von den Protokollen IP, TCP und UDP. Die ICMP-Meldungen werden benutzt, um sich gegenseitig Probleme mit Datenpaketen mitzuteilen, hierbei ist das Ziel, die Übertragungsqualität zu verbessern.

Quelle: (VL Folien 10.23 & 10.36 + Mitschrift # <https://www.elektronik-kompendium.de/sites/net/0901011.htm>)

- **Open Shortest Path First (OSPF):**

OSPF ist das am häufigsten verwendete Interior Gateway Protocol (IGP), also ein Link-State-Routing-Protokoll, welches innerhalb von einem autonomen System genutzt wird. Es kann verschiedene Verkehrsarten unterstützen, sodass bspw. Administrative Daten anders gehandhabt werden (höhere Priorität bekommen) und wählt den kürzesten Weg zwischen den Routern im System als ein dynamischer Algorithmus. OSPF bietet eine Hierarchie durch Areas(Bereiche) an bei denen OSPF-Router zugeordnet werden können, dies vereinfacht die Kommunikation und Wartung innerhalb des Systems.

Quelle: (VL. Folien 10.17)

Notiz: Bei dem Link-State-Routing geht es grundsätzlich darum eine Karte von dem autonomen System zu erstellen. Also wie ist wer miteinander verbunden, um z.B. bei ausfällen einen anderen Weg der Kommunikation zu finden.

- **Border Gateway Protocol (BGP):**

Das BGP(auch als Pfadvektorprotokoll bezeichnet) ist ein Exterior Routing Protocol (ERP), das die Routinginformationen zwischen autonomen Systemen überträgt und sie dadurch verbindet. Beim BGP informieren sich die Router untereinander über die verfügbaren Verbindungswege (Router kennen nur ganze Bereiche). Die Stärke des BGP-Protokolls liegt darin, verschiedene optionale Routing-Pfade in einer einzigen Routingtabelle(Pfad-Ermittlungen der Router) zu vereinen.

Quelle: (VL. Folien 10.19)

Aufgabe 2: Traceroute

- **Traceroute:**

Traceroute liefert zu einem gegebenen Server alle Router zurück, die ein IP Paket auf dem Weg zum Ziel passiert. Trace Route wird benutzt, um in einem IP-Netzwerk den Weg von Datenpaketen zu verfolgen und sichtbar zu machen. Man guckt also, welche Stationen ein Datenpaket bis zum Ziel nimmt, funktioniert damit ähnlich wie Ping. Man bekommt hierbei jedoch noch mehr Informationen über die Netzwerkverbindung zwischen der lokalen „Station“ und dem Ziel, was mit ihrer eigenen IP-Adresse angesprochen wird: traceroute <Ziel>. Bei der Ausführung des Befehls werden für uns mehrere ICMP-Befehle hintereinander verschickt an die Ziel-Adresse. Beim ersten ICMP-Befehl wird der TTL-Wert (im ff. erklärt) des IP-Pakets auf 1 gesetzt. Die „Station“(bzw. auch der Router), die die abgelaufene Lebenszeit des Datenpakets erkennt, verwirft das Paket und schickt eine ICMP-Meldung "Time Exceeded"(TTL-Wert 0) zurück. Nach der Ankunft dieser Meldung wird erneut ein ICMP-Befehl mit um eins erhöhten TTL-Wert verschickt. bis die Route zur Ziel-Adresse ermittelt wurde. Bsp.:

Sender→Router1(TTL 1)→Router2(TTL 2)→Router3(TTL 3)→Empfänger(TTL 4)

←-----←-----←-----←-----←

ICMP-Meldet jeweils von jedem Router ein „feedback“ an den Empfänger zurück.

Traceroute wird oft benutzt für:

- Eine Überprüfung, ob die Datenpakete die richtige Route zum Ziel wählen.
- Die Überprüfung, ob ein Router/Station ausgefallen ist.
- Die Vermeidung von Routingschleifen(tauchen Stationen/Router mehrfach vor) etc.

Quelle: (VL. Folien 10.36 # <https://www.elektronik-kompendium.de/sites/net/0901041.htm>)

• Time to live (TTL):

Der TTL-Wert gibt an, nach wie vielen Stationen die Lebenszeit eines IP-Pakets verfällt. Das TTL-Feld ist ein 1 Byte langes Zählerfeld im IP-Header und wird von jedem Netzknoten/Station/Router um den Wert 1 reduziert. Hat das IP-Paket beim Durchlauf den Wert 0 erreicht, wird es verworfen. Dies dient auch zur Entlastung des Netzes. Da es auch für längere Zeit in einem Router sein kann, wird der TTL-Wert sowohl durch den Hop, aber auch durch die Zeit(Sekunden) verringert. Die Anzahl an Hops sagt uns über wie viel Netzwerk-Abschnitte die Datenpakete bereits übertragen wurden. Wenn ein Paket bspw. für 3 Sekunden in einer Station ist, wird auch der TTL-Wert um 3 reduziert. Allgemein kann man sagen dass die Lebensdauer eines Pakets maximal 255 Sekunden beträgt oder sie entspricht der Zeit, die es für das Durchlaufen von 255 Stationen braucht. Quelle: (VL. Folien 10.26 #10.27# <http://www.itwissen.info/Hop-hop.html>)

• RAW-Socket:

Ein RAW-Socket ist ein Internet-Socket, der das direkte Senden und Empfangen von Internet-Protokollpaketen ohne projektspezifische Transportschicht-Formatierung ermöglicht.

In Standard-Sockeln wird die Nutzlast automatisch entsprechend dem gewählten Transportschichtprotokoll (z.B. TCP, UDP) eingekapselt, und der Socket-Benutzer ist sich der Existenz von Protokoll-Headern nicht bewusst, die mit der Nutzlast ausgestrahlt werden.

Beim Lesen aus einem RAW-Socket sind die Header in der Regel enthalten.

Eine mögliche Anwendung für RAW-Sockets sind Implementierungen neuer Transportschichtprotokolle im Benutzerraum. RAW-Sockets sind in der Regel in Netzwerkgeräten verfügbar und werden für Routing-Protokolle wie das Internet Group Management Protocol (IGMPv4) und OSPF und im ICMP genutzt.

sd = socket (AF_INET, SOCK_RAW, IPPROTO_RAW);

Quelle: (<http://www.pdbuchan.com/rawsock/rawsock.html> # http://sock-raw.org/papers/sock_raw)