Netzwerk-Labor 1
Internet-Protocol IP
Internet-Control-Massage-Protocol ICMP

Übersicht:

In dieser Übung untersuchen wir das Internet Protocol IP. RFC 791 beschreibt die Details des IP. IP dient zum Adressieren von Hosts und Netzen und ist für das Durchleiten der IP-Pakete durch Netzwerke zuständig.

Benötigte Ausstattung:

Computer: x86 PCs
Netzwerk: Ethernet mit Internetzugang
Betriebssystem: Linux (oder Windows)
Hilfsmittel: Wireshark Netzwerk-Analyse-Werkzeug, Shutter (oder snapit o.ä.) um Bildschirmfotos zu erstellen

Aufgabenstellung

1. IP-Pakete eines einfachen „ping“ untersuchen
2. Fragementierung von großen IP-Paketen untersuchen
3. IP-Pakete eines „trace“-Aufrufs untersuchen
4. ICMP Pakete untersuchen

Der *ping* -Befehl schickt ein Datenpaket an die angegebene Adresse. Der angesprochene Rechner schickt dieses wieder zurück. Die Zeit vom Absenden des Paketes bis zum Eintreffen des Antwortpaketes ist die Rundlaufzeit, Round Trip Time RTT.

traceroute schickt IP-Pakete an die angegebene Adresse. Dabei wird bei schrittweise die „Lebensdauer“ TTL der Pakete beginnend von 1 erhöht. Jeder Router auf dem Weg zum Zielrechner dekrementiert den TTL-Wert um 1. Wird dabei TTL auf null gezählt, wird eine Fehlermeldung (ICMP Message Type 11, TTL exceeded) zurückgeschickt. So entsteht nach und nach eine komplette Liste der Router zwischen Quell-Rechner und Ziel-Rechner.
Traceroute ist auf allen gängigen netzwerkfähigen Rechnern verfügbar. Der Name des Programms kann allerdings systemabhängig variieren. Bei Ubuntu heißt dieses Tool *tracepath*.

Aktion 1 PING:

1. Wireshark starten, IP Reassembly ausschalten, damit IP-Fragmente nicht von Wireshark wieder zusammengesetzt werden. Menü *Edit → Preferences*, dort unter *Protocols* zu IPv4 scrollen, anklicken und im rechten Fenster Haken bei *Reassemble fragmented IP Datagram* entfernen.
2. Capture starten
3. An der Linux-Konsole einen ping auf ein externes Ziel (z. B.: google.de) starten (~>ping

google.de).

4. Stoppen Sie die Aufzeichnung und schauen Sie sich die aufgezeichneten Pakete an.
   Sie sollten nun eine Serie von ICMP-Paketen sehen. Bei Windows und Linux-Rechnern sehen die Ergebnisse leicht unterschiedlich aus.

Wenn Sie Die folgenden Fragen beantworten, dann fügen Sie jeweils Screenshots Ihrer Analyse bei, um Ihre Aussagen zu belegen.

1. Wie lautet die IP-Adresse Ihres Rechners?

2. Wie ist der Wert des Feldes im IP-Protokollkopf, welches das im IP-Paket transportierten Protokolls angibt?

3. Wie viele Bytes sind im IP-Header? Wie viele Bytes sind in der IP Nutzlast?

4. Wie lange ist die RTT?

5. Wie lauten die Identifikationsnummern der Pakete?

6. Wurde das IP-Paket fragmentiert? Erklären Sie, wann ein Paket fragmentiert wird und wann nicht. Zeigen Sie mit Hilfe von Screenshots, wie ein großes Paket in kleinere fragmentiert wird.

Aktion 2 FRAGMENTIERUNG:

1. Wiederholen Sie Schritt 1 bis 4 aus der Aktion 1 mit folgender Änderung:
   Schicken Sie den Ping ab mit 2000 Byte Nutzdaten und ein weiteres Mal mit 3500 Byte Nutzdaten.

Wenn Sie Die folgenden Fragen beantworten, dann fügen Sie jeweils Screenshots Ihrer Analyse bei, um Ihre Aussagen zu belegen.

1. Wurde das IP-Paket fragmentiert?

2. Wie verändert sich die Identifikationsnummer der IP-Pakete?

3. Wie verändert sich die RTT bei steigender Datenmenge?

4. Erklären Sie, wann ein Paket fragmentiert wird und wann nicht. Zeigen Sie mit Hilfe von Screenshots, wie ein großes Paket in kleinere fragmentiert wird.

Aktion 3 TRACEROUTE:

1. Wireshark starten, IP Reassembly ausschalten, damit IP-Fragmente nicht von Wireshark wieder zusammengesetzt werden. Menü *Edit → Preferences*, dort unter *Protocols* zu IPv4 scrollen, anklicken und im rechten Fenster Haken bei *Reassemble fragmented IP Datagram* entfernen.
2. Capture starten

3. An der Linux-Konsole einen Traceroute (oder tracepath) auf ein externes Ziel starten (z. B.: google.de).
   Machen Sie diesen Schritt zunächst ohne zusätzliche Parameter und wiederholen Sie ihn dann mit entsprechendem Parameter um 2000 Bytes und ein weiteres Mal 3500 Byte Nutzdaten zu verschicken.
   (Sollte an Ihrem System kein Trace-Befehl vorhanden sein, bei dem sich die Größe des Datenpaketes einstellen lässt, dann verwenden Sie an dieser Stelle den ping-Befehl mit dem entsprechenden Parameter).
4. Stoppen Sie die Aufzeichnung und schauen Sie sich die aufgezeichneten Pakete an.
   Sie sollten nun Serien von UDP- und ICMP-Paketen sehen. Bei Windows und Linux-Rechnern sehen die Ergebnisse leicht unterschiedlich aus.

Wenn Sie Die folgenden Fragen beantworten, dann fügen Sie jeweils Screenshots Ihrer Analyse bei, um Ihre Aussagen zu belegen.

1. Wie verändert sich der Wert des TTL-Feldes?

2. Welches Protokoll wird benutzt um die Anfrage zu verschicken?

3. Welches Protokoll transportiert die Antwort?

4. Wie sind die IP-Adressen der ersten beiden Router auf dem Weg ins Internet?

Aktion 4 ICMP:

1. Öffnen Sie ein beliebiges ICMP-Paket aus dem vorherigen Mitschnitt. Analysieren Sie den Inhalt dieses Paketes. Untersuchen Sie noch mehrere solcher Pakete.

Beantworten Sie folgende Fragen und belegen Sie die Antworten mit Screenshots.

1. Welche „Nutzdaten“ werden von einer ICMP-Fehlermeldung transportiert?

2. Wodurch kann der Empfänger einer Fehlermeldung per ICMP ermitteln, welches Paket den Fehler verursacht hat?

3. Recherchieren Sie im Internet, welche Typen von ICMP-Messages es gibt.