2. Praktikum: Technik und Technologie

Andreas Krohn Benjamin Vetter Benjamin Jochheim

11. Januar 2011

1 Kurzdokumentation

Dem Quellcode liegt ein Ant Buildfile bei. Die Parameter *Benutzername* und *Port* sind über das Buildfile festgelegt. Per `ant run` wird die SIP Applikation kompiliert und gestartet.

Abbildung 1 zeigt einen Screenshot der gestarteten Anwendung.

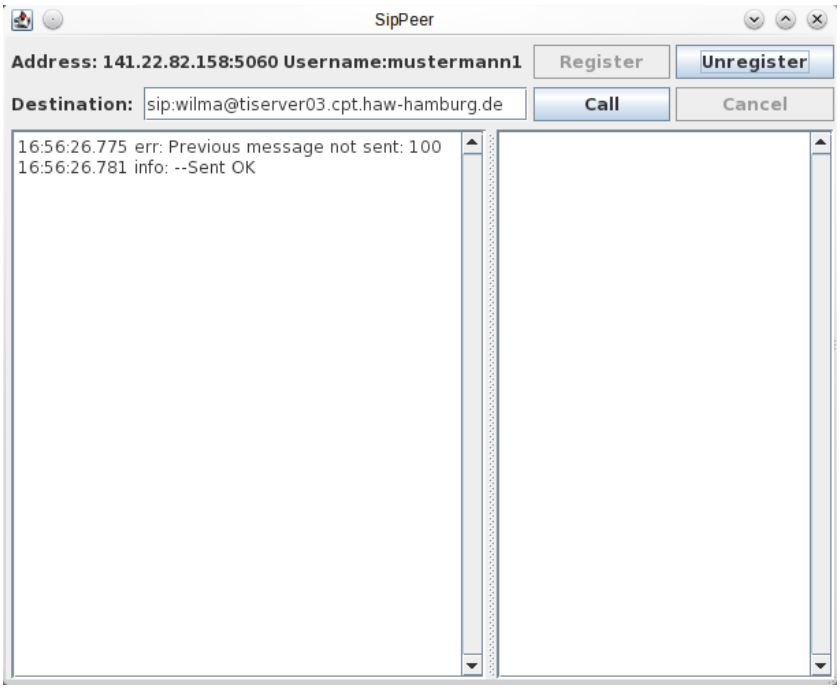

Abbildung 1: Screenshot der Anwendung

Beim Start der SIP Applikation registriert diese sich beim SIP Proxy Server. Über die Buttons „Unregister“ und „Register“ kann diese Registrierung manuell zurückgezogen bzw. wieder gesetzt werden.

Die SIP Applikation kann sowohl UAC als auch UAS sein.

Durch Betätigen des „Call“-Buttons wird eine Session zu dem im Textfeld angegebenen Teilnehmer aufgebaut. Damit übernimmt die Anwendung die UAC Rolle und setzt ein IGMP `join` an die Gruppe `239.238.237.17` ab. Eingehende Multicast Nachrichten werden in der Anwendung angezeigt. Der „Cancel“-Button beendet die Session und veranlasst das Verlassen der Multicast Gruppe.

Ruft ein anderer Teilnehmer die SIP Applikation an, übernimmt die Anwendung die UAS Rolle und beginnt kontinuierlich (1x pro Sekunde) Multicast Nachrichten zu senden bis die letzte Session beendet wird. Die Adressen der „Anrufer“ werden für die Dauer der Session in der Anwendung angezeigt.

2 Erklärung Ihrer Beobachtungen zur Multicast Paketverteilung

2.1 Wie erreichen die Multicast Daten Ihren Rechner auf der Ethernet Protokollebene?

Hierzu werden die Multicast IP Host Group Adressen auf Ethernet Multicast Adressen gemappt, indem die low-order 23 bit der IP-Adresse auf die low-order 23 bit der Ethernet Multicast Adressen gemappt werden (01-00-5E-00-00-00). Da viele Ethernet-Netzwerkkarten bzgl. der konfigurierbaren Adressen, für die sie zuständig sein sollen, eingeschränkt sind, muss ggf. der Adress-Filter der Karte ausser Kraft gesetzt werden. Hierdurch nimmt die Netzwerkkarte alle Pakete entgegen, auch wenn sie gar nicht für das Interface bestimmt sind (vgl. `http://tools.ietf.org/html/rfc1112` und Abbildung 2).

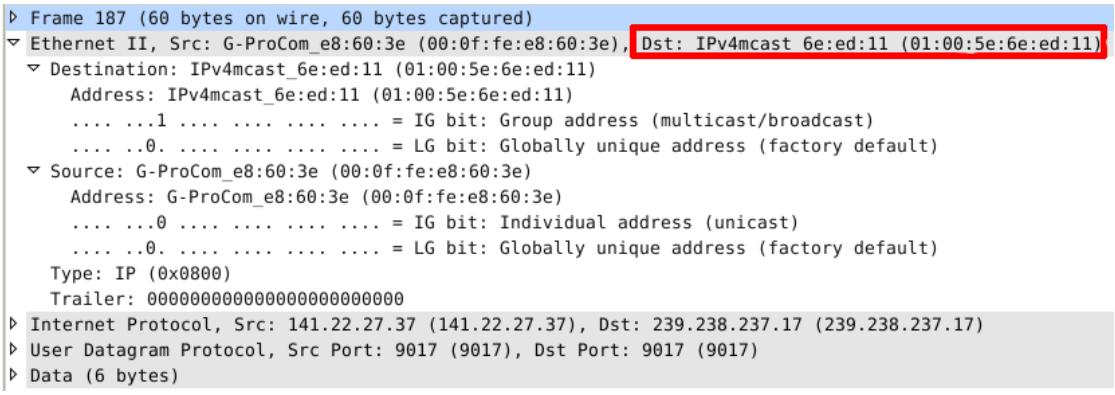

Abbildung 2: Multicast im Ethernet

2.2 Welchen Einfluss hat Ihr IGMP join?

Der IGMP Join selbst hat keinen Einfluss auf das Verhalten auf Ethernet-Ebene, da wir bspw. mithilfe des Sniffers beobachten konnten, dass auch nach einem IGMP Leave weiterhin die Multicast-Pakete den Host erreicht haben, wenngleich diese auch nicht bis zur Anwendungsebene hochgereicht wurden (vgl. Abbildung 3).

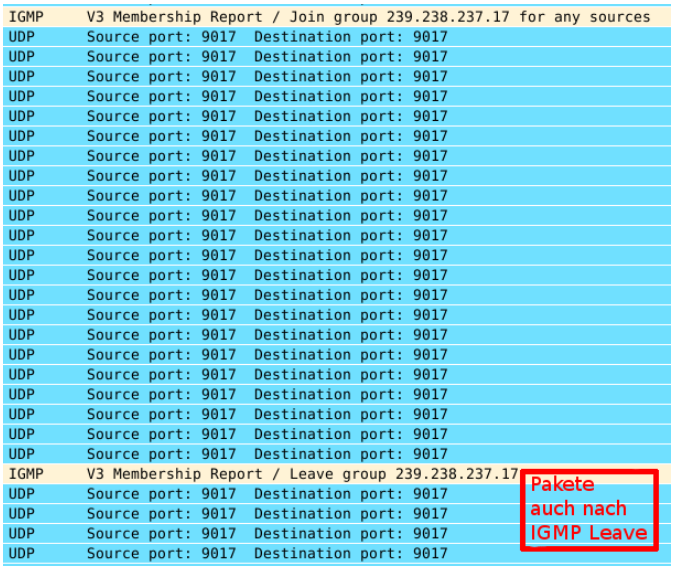

Abbildung 3: IGMP Join/Leave bzgl. Ethernet-Ebene

Insofern hat das IGMP Join nur Auswirkungen auf den Stack des Hosts, der die IGMP-Join Nachricht abgesetzt hat.

2.3 IGMP-Snooping

Zum Empfang einer Multicast-Gruppe sendet der Client ein Join (Membership Report) an die reservierte Multicast-Adresse 224.0.0.22. Das Paket wird mit gesetzter „Router Alert“ Option versandt, die Gruppenadresse wird dabei im „Group Record“ mitgeteilt. So erfahren die Router innerhalb derselben Broadcast-Domäne von der Multicast-Teilnahme des Hosts.

Der Router merkt sich die Multicast-Teilehmer und fragt diese in regelmäßigen Abständen ob sie weiterhin Teilnehmen möchten. Antwortet ein Host auf solch eine Anfrage nicht, so verläßt er Routerseitig automatisch die Multicast-Gruppe.

Auf der MAC-Schicht werden die unteren bits der MAC-Adresse 01-00-5e-00-00-00 verwendet um die Multicast-Adresse abzubilden. Ein Multicast-fähiger Switch sollte „IGMP-Snooping“ können um diese speziellen Pakete auch nur den Multicast-Teilnehmern zuzustellen.

Ein nicht IGMP-Snooping-fähiger Switch wird diese Pakete mit der speziellen MAC-Adresse ansonsten als Broadcast-Pakete verstehen und entsprechend an alle Ports weiterleiten.