

Protokoll zum Laborversuch Modul Networking+Services



Technikumstrasse 21, CH-6048 Horw
T +41 41 349 33 11, F +41 41 349 39 60
www.hslu.ch

Nicola Lardieri
Assistent

T direkt +41 41 349 33 39
nicola.lardieri@hslu.ch

Horw, 17. März 2009
Seite 1/4

Teilnehmer

Versuch: D6 – Protokollanalyse TCP, ARP, ICMP

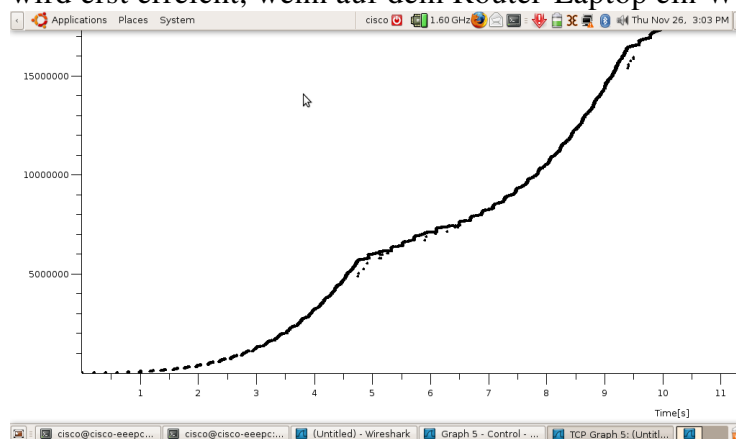
Gruppe/Gr.Nr: Team 7

Studierende: Daniel Hauswirth
Thomas Galliker

Datum: Donnerstag, 26. November 2009

Versuchsablauf

- Schreiben Sie auf, welche Erfahrungen und Erkenntnisse aus den einzelnen Versuchen gewonnen wurden und geben Sie mindestens 5 „AHA-Erlebnisse“ dazu an. Unter „AHA-Erlebnisse“ verstehen wir Erkenntnisse eines Ingenieurs und erwarten Ingenieur Aussagen.
Versuchen Sie die Fragen im Versuchsdokument zu beantworten, falls vorhanden.
- Geben sie bei jeder Protokollaussage das relative Kapitel im Versuchsdokument an.
- Haben Sie in diesem Bereich noch offene Fragen? Fragen Sie das Laborpersonal.
Falls Fragen nicht unmittelbar beantwortet werden können, formulieren Sie die Frage in diesem Dokument.
- Sind Ihnen Fehler in der Versuchsbeschreibung / Konfiguration aufgefallen? Seien Sie bitte präzise beim Angeben des betroffenen Kapitels.
- Wireshark: Ein Display Filter ermöglicht das Filtern aller gesniffen Pakete, während der Capture Filter herausgefilterte Pakete schon gar nicht erst aufzeichnet.
- Die Begründung, warum in einer Zero Window Situation ein Deadlock entstehen kann: *„When a receiver advertises a window size of 0, the sender stops sending data and starts the persist timer. The persist timer is used to protect TCP from a deadlock situation that could arise if the window size update from the receiver is lost and the sender has no more data to send while the receiver is waiting for the new window size update. When the persist timer expires, the TCP sender sends a small packet so that the receiver sends an acknowledgement with the new window size.”* (http://en.wikipedia.org/wiki/Transmission_Control_Protocol).
- Die maximale Grösse des Empfangsfensters ist auf 65535 Bytes (16bit Adressraum) limitiert. Dank einer Erweiterung namens „Window Scale Option“ (RFC1323, <http://tools.ietf.org/html/rfc1323>) kann dieser Adressraum auf 32bit erweitert werden. So wird in einer offenen Verbindung weniger Netzwerk Overhead entstehen. Siehe auch http://en.wikipedia.org/wiki/TCP_tuning
- Die „Slow Start Sequence“ aus Aufgabe 4.4.6 konnten wir im Time-Sequence Graph leider zuerst nicht sehen, da das LAN einfach zu schnell ist und innerhalb kurzer Zeit sehr viele TCP Segmente übertragen wurden. Das kostete viel Zeit, da wir dachten, wir hätten etwas falsches gesnifft/gefiltet. Der angestrebte Effekt wird erst erreicht, wenn auf dem Router-Laptop ein WAN simuliert wird:



- Beim Trace Routing ist zu vermeiden, dass die Software für jede IP Adresse eine Namensauflösung macht --- das schlägt nämlich in diesem Laborbeispiel sowiso fehl und verursacht unnötigen Verkehr auf dem Sniffer. (Filter „icmp“ muss zwingend aktiviert werden).

Offene Fragen

- Keine

Verbesserungsvorschläge

- Seite 9 enthält Rechtschreibfehler
- Seite 17 befindet sich ein komischer Satz: „TCP löst das folgendermassen: Das Endsystem A muss auch bei einem Sendefenster = 0 Dateneinheiten der Grösse 1 Byte, die vom Endsystem B quittiert werden müssen. Somit kann B den aktualisierten Empfangspuffer bekannt geben“.
- Software „SRIP“ in kompilierter Form beilegen. Der C-Code alleine bringt uns nicht viel.

Versuchsbewertung

Aufgabe erledigt bis Kapitel 5

Ist der Umfang angemessen für die vorgesehene Zeit?

- Umfang zu gross / Zuwenig Zeit
- ... Gerade richtig
- ... Umfang zu klein / Zuviel Zeit

Hat der Versuch den angestrebten Lerneffekt erreicht?

- ... vollkommen
- ... gerade richtig
- teilweise

Ist das Thema genügend tief behandelt worden?

- ... zu tief, zu viel spezifisches Fachwissen vermittelt
- Gerade richtig
- ... zu oberflächlich

Empfehlen Sie diesen Versuch anderen Studierenden weiter?

- ... ja
- vielleicht
- ... nein

Unterschriften

Name / Vorname: D.Hauswirth

Name / Vorname: T.Galliker