TECHNISCHE UNIVERSITÄT BERLIN

Fakultät IV – Elektrotechnik und Informatik
Fachgebiet Intelligente Netze und Management verteilter Systeme
Prof. Anja Feldmann, Ph.D.
Gregor Maier, Jörg Wallerich, Andi Wundsam

8th Work Sheet Praktikum Protokolldesign WS 07/08

Question 1: (100 points) *BGP-Analysis*

The directory `/afs/net.t-labs.tu-berlin.de/home/praktikum/daten/8.uebung/` contains two files:

- `table.gz` contains the initial routing tables of several routers.
- `updates.gz` is a tracefile with the BPG update messages of these routers.

Both files are from a BGP collector station and have the following format:

`Protocol|Time|Type|PeerIP|PeerAS|Prefix`

For announcement messages in `updates.gz` and for the complete file `table.gz` the following fields are appended to each line:

`|ASPath|Origin|NextHop|LocalPref|MED|Community|Aggregation|Aggregator`

The ASes in the `ASPath` field are separated by spaces. The fields `Origin`, `NextHop`, `LocalPref`, `MED`, `Community`, `Aggregation`, and `Aggregator` are irrelevant for most of this exercise.

A BGP peer is uniquely defined by the tuple `(PeerIP,PeerAS)`.

(a) (20 points) Write a script that is able to find pairs of consecutive[1] updates (for the same prefix, from the same peer) that extend the AS-path. What could be the reason for such an update?

Deliverables:

- An ASCII text, ps, pdf, or HTML file (no office files!) with the two consecutive updates, and your explanation.
- Your (Shell-)script

(b) (30 points) Now you are to analyse pairs of consecutive prefix updates: Look at consective pairs of prefix updates having the `same` prefix-peer-combination. Each such pair belongs to one of five categories: AW, WA, WW, AADup, AADiff. A *A* stands for an announcement and a *W* stands for a withraw.

AW announcement followed by a witdraw

WA withdraw followed by an announcement

WW withdraw followed by a withdraw

AADup a duplicated Announcement. I.e., both announenements contain exactly the same information in **all** field (including the ‘uninteresting’ fields `Origin`, `NextHop`, etc.)

AADiff all other cases with two consecutive announcements

Example: An announcement for prefix *p* from peer *a*, followed by a withdraw for prefix *p* from peer *a* belongs to category *AW*

Deliverables:

- An ASCII text, ps, pdf, or HTML file (no office files!) with percantage values.
- Your script

[1] Consecutive does **not** imply, that the updates are beneath each other in the file!

(c) (50 points) An ‘Update-Burst’ is a group of prefix updates for the same prefix from the same peer, where the time interval between two updates is short. In this case ‘short interval’ is defined here as the time between two consecutive updates being shorter than 15 minutes.

Group the updates into such burst and find the 10 longest bursts[2]. Try to explain the possible causes for such bursts.

Deliverables:

- an ASCII text, ps, pdf, or HTML file (no office files!) with the 10 longest burst in the same format as the input file
- Your script

Submission details: look at the FAQ (on `http://www.net.t-labs.tu-berlin.de/teaching/ws0708/PD_labcourse/`**)**
Due Date: Tuesday, December 18., 2007 11:59 h s. t.

[2] the bursts with the longest total duration, not with the most updates