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

8. Blatt Praktikum Protokolldesign WS 07/08

Aufgabe 1: (100 Punkte) *BGP-Verkehrsanalyse*

Das Verzeichnis `/afs/net.t-labs.tu-berlin.de/home/praktikum/daten/8.uebung/` enthält zwei Dateien:

- `table.gz` enthält die initialen Routingtabellen von mehreren Routern,
- `updates.gz` ist ein Tracefile mit BGP Announcement-Nachrichten aller dieser Router.

Beide Dateien stammen von einer BGP-Sammelstelle und haben folgendes Format:

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

Sowohl bei Announcement-Nachrichten in `updates.gz` als auch bei der kompletten Datei `table.gz` sind am Ende einer Zeile noch folgende Felder angehängt:

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

Die einzelnen ASes im Feld `ASPath` sind dabei durch Leerzeichen getrennt. (Die Felder `Origin`, `NextHop`, `LocalPref`, `MED`, `Community`, `Aggregation` und `Aggregator` sind für den größten Teil dieser Aufgabe irrelevant.)

Ein bestimmter BGP-Peer wird eindeutig durch das Tupel `(PeerIP,PeerAS)` bestimmt.

(a) (20 Punkte) Schreibe ein Skript, dass je zwei aufeinanderfolgende[1] Updates für denselben Prefix vom selben Peer findet, die den AS-Pfad verlängern. Was könnte eine mögliche Erklärung für die Änderung sein?
Abzugeben sind:

- eine ASCII text, ps, pdf oder HTML Datei (keine Officedateien !) mit den beiden aufeinanderfolgenden Updates und deiner Erklärung.
- Dein (Shell-)Skript

(b) (30 Punkte) Nun sollen aufeinanderfolgende Prefix-Updates untersucht werden: Betrachte wieder Paare aufeinanderfolgender Prefix-Updates, die die **gleiche** Prefix-Peer-Kombination betreffen. Diese Paare können in 5 verschiedene Kategorien eingeteilt werden: AW, WA, WW, AADup und AADiff.

AW Announcement gefolgt von einem Witdraw

WA Withdraw gefolgt von einem Announcement

WW Withdraw gefolgt von einem Withdraw

AADup duplizierte Announcements. D.h. beide Announcements haben **exakt** dieselben Informationen in allen Feldern (auch in den „uninteressanten“ Feldern `Origin`, `NextHop` etc.).

AADiff Alle anderen Fällen, in denen zwei Announcements aufeinander folgend

Beispielsweise würde ein Announcement für den Prefix p, dem ein Withdraw vom gleichen Peer für das gleiche Prefix p folgt, in die Klasse AW eingeordnet.

Schreibe ein Skript, dass die Updates im Tracefile klassifiziert und ihre prozentuale Verteilung berechnet.

Abzugeben sind:

[1] Aufeinanderfolgend bedeutet **nicht**, dass die Updates im File direkt untereinander stehen.

- eine ASCII text, ps, pdf oder HTML Datei (keine Officedateien !) mit den Prozentzahlen der Verteilung
- Dein Skript

(c) (50 Punkte) Ein „Update-Burst“ ist eine Gruppe von Prefix-Updates für den gleichen Prefix vom gleichen Peer, wobei die Updates in kurzen Zeitintervallen aufeinander folgen. „In kurzen Zeitintervallen“ bedeutet hier, dass jedes Zeitintervall zwischen zwei aufeinander folgenden Updates desselben Bursts kleiner als 15 Minuten ist.

Gruppiere nun die Updates in solche Bursts. Suche die 10 längsten Bursts[2]. Versuche, mögliche Erklärungen für die beobachteten Phänomene zu finden.

Abzugeben sind:

- eine ASCII text, ps, pdf oder HTML Datei (keine Officedateien !) mit den 10 längsten Update-Bursts (gleiches Format wie die Eingabedateien)
- ein ASCII text, ps, pdf oder HTML Datei (keine Officedateien !) mit Deinen Spekulationen über diese Bursts
- Dein Skript

Details zur Abgabe der Aufgaben: siehe FAQ (unterhalb `http://www.net.t-labs.tu-berlin.de/teaching/ws0708/PD_labcourse/`**)**
Abgabe bis: Dienstag, 18.12.2007, 11:59 h s. t.

[2] die zeitlich längsten, nicht die von der Anzahl der Updates größten Bursts