



## 10. Aufgabenblatt zum Internet-Praktikum

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

Das Verzeichnis `/home/inetprak/daten/10.uebung/` enthält zwei für diese Aufgabe benötigte Dateien:

- `table.gz` enthält die initialen Routingtabellen von 12 Routern,
- `updates.gz` ist ein Tracefile mit BGP-Update Nachrichten.

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 im Falle der kompletten Datei `table.gz` sind ans Ende jeder Zeile noch die folgenden Felder angehängt:

`|ASPath1|Origin|NextHop|LocalPref|MED|Community|Aggregation|Aggregator`

(Die Felder `Origin`, `MED`, `Aggregation` und `Aggregator` sind für den größten Teil dieser Aufgabe irrelevant.)

- (a) (10 Punkte) Finde 2 aufeinanderfolgende Updates (für denselben Prefix vom selben Peer), die den AS-Pfad verlängern. Was könnte eine mögliche Erklärung für die Änderung sein?

Abzugeben sind:

- eine Datei mit den beiden aufeinanderfolgenden Updates,
- Dein Skript/Dein Shell-,Einzeiler<sup>2</sup>, mit dem Du diese Information bekommen hast

- (b) (20 Punkte) Nun sollen aufeinanderfolgende Prefix-Updates untersucht werden: Betrachte 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. Hierbei bedeutet *A* ein Announcement und *W* ein Withdraw. *AADup* enthält duplizierte Announcement; *AADiff* enthält alle anderen (also diejenigen, die sich voneinander unterscheiden). *Dupliziert* sind Announcements genau dann, wenn sie genau den gleichen Inhalt in **allen** Feldern aufweisen (auch in den „uninteressanten“ Feldern `Origin`, `MED`, `Aggregation` und `Aggregator`).

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:

- ein ASCII-Plaintextfile mit den Prozentzahlen der Verteilung
- Dein Skript

---

<sup>1</sup>mit Leerzeichen getrennt

<sup>2</sup>Generell schließt der Begriff „Shell-Einzeiler“ auch den Fall eines einzelnen `less`-Kommandos nicht aus – aber in diesem Fall musst Du ganz genau erklären, wie Du „von Hand“ an die Information herangekommen bist ;-)

- (c) (30 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.

Gruppierere nun die Updates in solche Bursts. Suche die 10 längsten Bursts<sup>3</sup>. Versuche, mögliche Erklärungen für die beobachteten Phänomene zu finden.

Abzugeben sind:

- ein ASCII-Plaintextfile mit den 10 längsten Update-Bursts (gleiches Format wie oben)
  - ein ASCII-Plaintextfile mit Deinen Spekulationen über diese Bursts
  - Dein Skript
- (d) (40 Punkte) Ein lokaler Session-Reset ist ein Verbindungsabriß zwischen der Sammelstelle und dem Nachbarrouter.

Beschreibe eine Methode, wie man lokale Session-Resets finden kann. Schreibe ein Skript, mit dem man solche Resets im Tracefile finden kann. Gib ein Beispiel für einen lokalen Session-Reset.

Abzugeben sind:

- ein ASCII-Plaintextfile mit allen Updates, die an einem lokalen Session-Reset beteiligt sind (gleiches Format wie oben)
- ein ASCII-Plaintextfile mit der Erklärung Deiner Methode
- Dein Skript

**Details zur Abgabe der Aufgaben: siehe FAQ**

(unterhalb <http://www.net.in.tum.de/teaching/SS05/inetprak/>).

**Abgabe:** bis Dienstag, den 28. Juni 2005, 23:59h s. t.

---

<sup>3</sup>die zeitlich längsten, nicht die von der Anzahl der Updates größten Bursts