WireShark Aufgabe

# Aufgabe 1

* Einleitung

# Aufgabe 2

*1. Welche Pakete werden gesendet, wenn der Ping-Befehl ausgeführt wird? Kopieren Sie die entsprechenden Pakete aus WireShark. Führen Sie den Ping-Befehl gegebenenfalls für mehrere IP Adressen aus, um diese Pakete zu identifizieren.*

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

*2. Welche Protokolle werden zur Übertragung dieser Pakete genutzt?*

Bei nsa.gov wird das Protokoll ICMPv6 genutzt (auch sichtbar an der IPv6 Adresse)

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Bei der Stadtwerke Konstanz dagegen ICMP (sichtbar an den IPv4 Adressen)

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

*3. Welche Ergebnisse liefert der Ping-Befehl? Wie können Sie diese Ergebnisse aus den in WireShark aufgezeichneten Paketen bestimmen?*

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

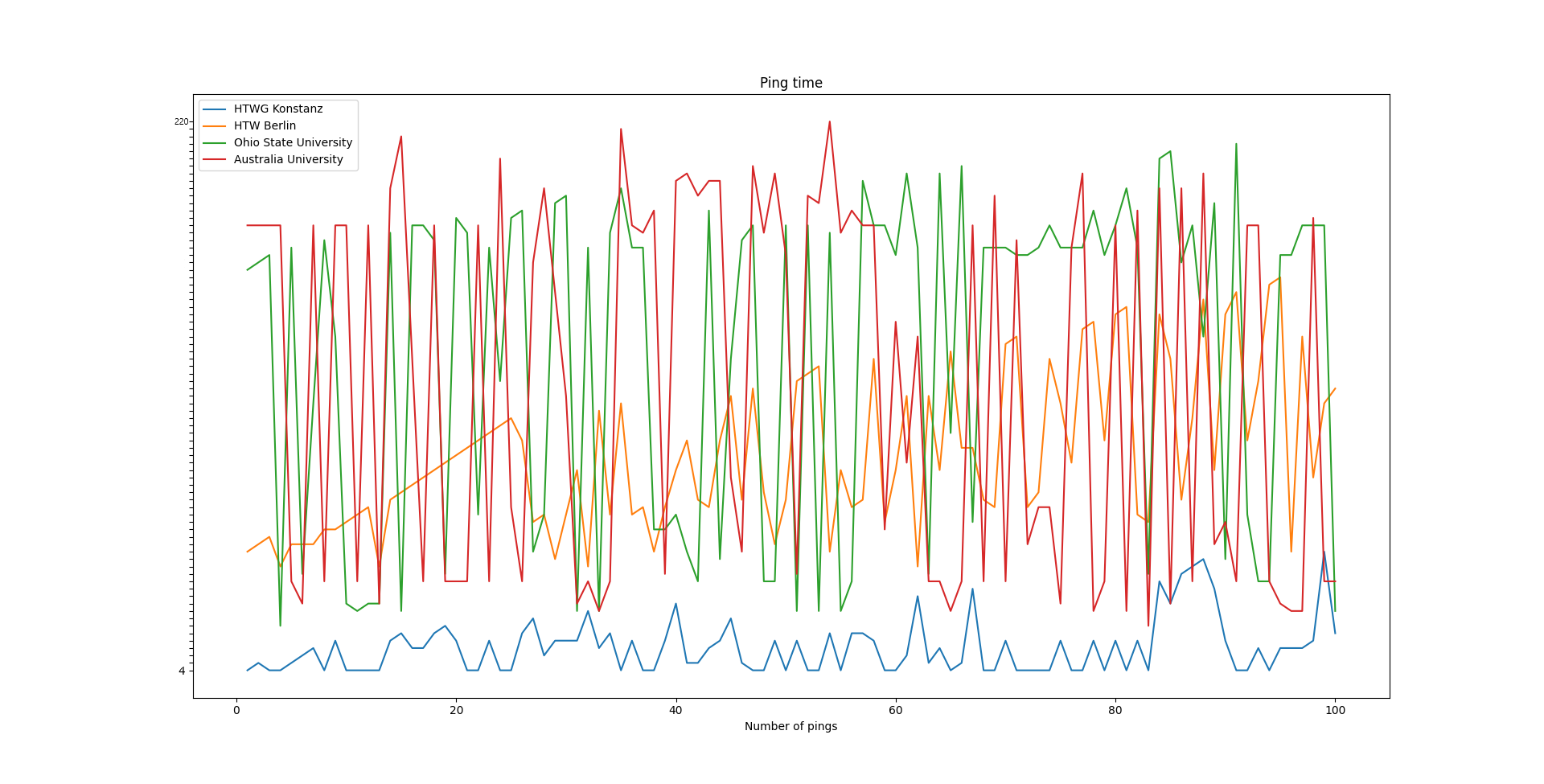
Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

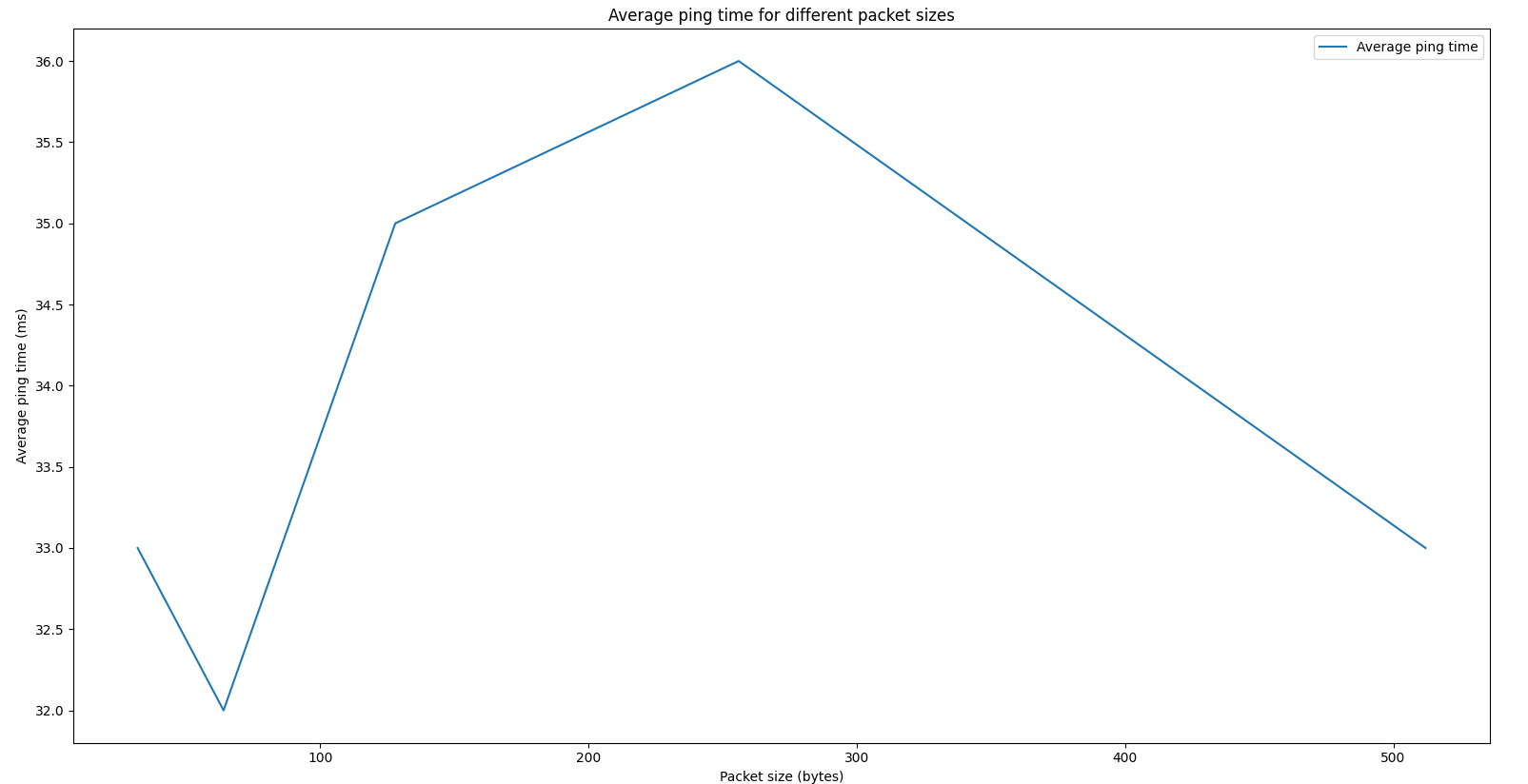
*4. Erstellen Sie einen Filter für diese beiden Protokolle (zusätzlich zu dem Filter auf ihre IP-Adresse), um nur diese beiden Protokolle zu filtern. Testen Sie den Filter, indem Sie weitere Adressen pingen.*

(icmpv6 || icmp) && (ip.src==local IPv4 || ipv6.src==local IPv6)

*1. Pingen Sie die Adressen jeweils 100mal und speichern Sie das Ergebnis in einer Datei. Stellen Sie die Ping-Zeit mit einem Tool ihrer Wahl (Excel, Matlab, etc.) grafisch dar.*

**

*2. Wählen Sie die Adresse mit den längsten Ping-Zeiten und stellen Sie den Einfluss der Paketgröße grafisch dar.*

**

# Aufgabe 3

*1. Führen Sie den traceroute-Befehl für den Web-Server der Hochschule und für ihre eigene IP-Adresse aus. Welche Ergebnisse erhalten Sie?*

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

*2. Bestimmen Sie, in welchem Netz sich der Rechner befindet, von dem der traceroute Befehl gestartet wird. Bestimmen Sie außerdem, durch welche Netze die Pakete geroutet werden. Sie können bestimmen, zu welchem Netz ein Router gehört, in dem Sie die ASN (Autonomous System Number) des Routers bestimmen, die Netze eindeutig kennzeichnet. Nutzen Sie dazu beispielsweise* das Online Tool <https://www.ultratools.com/tools/asnInfo>.

1. 2001:16b8:a5fe:1500:7eff:4dff:fea1:21d9 :

Der Rechner von welchem der Befehl ausgeführt wird befindet sich im lokalen LAN (Fritz-Box Router). Dies ist auch dem unteren Bild zu entnehmen.

1. 2001:1438::62:214:63:147

**AS:** 8881 **AS Name**: VERSATEL, DE

1. 2001:1438:0:1::15:21

**AS:** 8881 **AS Name**: VERSATEL, DE

1. fra020isp005.versatel.de [2001:7f8::22b1:193:80]

**AS:** None **AS Name:** Not found

1. kar-rz-a99-hu0-2-0-0.belwue.net [2001:7c0:2:10c8::]

**AS:** 553 **AS Name**: BELWUE BelWue-Koordination, DE

1. stu-nwz-a99-hu0-1-0-0.belwue.net [2001:7c0:2:10c1::]

**AS:** 553 **AS Name**: BELWUE BelWue-Koordination, DE

1. stu-al30-1-hu0-0-1-0.belwue.net [2001:7c0:2:1104::1]

**AS:** 553 **AS Name**: BELWUE BelWue-Koordination, DE

1. tue-wae-1-te0-0-0-15.belwue.net [2001:7c0:2:1064::1]

**AS:** 553 **AS Name**: BELWUE BelWue-Koordination, DE

1. kon-bib-1-te0-0-0-11.belwue.net [2001:7c0:2:104a::1]

**AS:** 553 **AS Name**: BELWUE BelWue-Koordination, DE

1. cmssrv6.htwg-konstanz.de [2001:7c0:5f0:f020::20:17]

**AS:** 553 **AS Name**: BELWUE BelWue-Koordination, DE

Zu sehen ist, dass die Route über VERSATEL (Internet-Provider) läuft und in Karlsruhe in das Landeshochschulnetz "**B**aden-**Wü**rttembergs **e**xtended **L**AN" geht von wo es über das Hochschulnetz nach Konstanz geleitet wird. Cool? Cool!

*3. Betrachten Sie nun mehrere Online-Tools, so dass Sie den Traceroute-Befehl von mindestens drei unterschiedlichen Netzen aus starten können. Führen Sie den Traceroute-Befehl nun nicht mehr nur für den Web-Server der Hochschule sondern zusätzlich für www.ntt.co.jp und www.google.com aus. Bestimmen Sie, welche Teile der Route für die unterschiedlichen Kombinationen aus Online-Tool und Zielrechner identisch sind.*

### HTWG Konstanz

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 1: <http://www.dnstools.ch/visual-traceroute.html>

Zu sehen ist, dass die Route erst über Internationale Knotenpunkte nach Frankfurt geleitet wird. Von dort wird es regional nach Stuttgart weitergeleitet, wo es dann wieder ins BelWue geleitet wird. Warum dies diesmal nicht in Karlsruhe ins Hochschulnetz geht, sondern in Stuttgart lässt sich nicht genau sagen. Zu sehen ist aber auch, dass der zweite Pfad (siehe Abbildung 2) in Stuttgart ins BelWue Netz geht. Sobald sich die Pakte im BelWue Netz befinden werden Sie immer auf dem gleichen Weg nach Konstanz geroutet.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 2: <https://traceroute-online.com/>

## Google

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text, Monitor, Screenshot, Fernsehen enthält.

Automatisch generierte Beschreibung

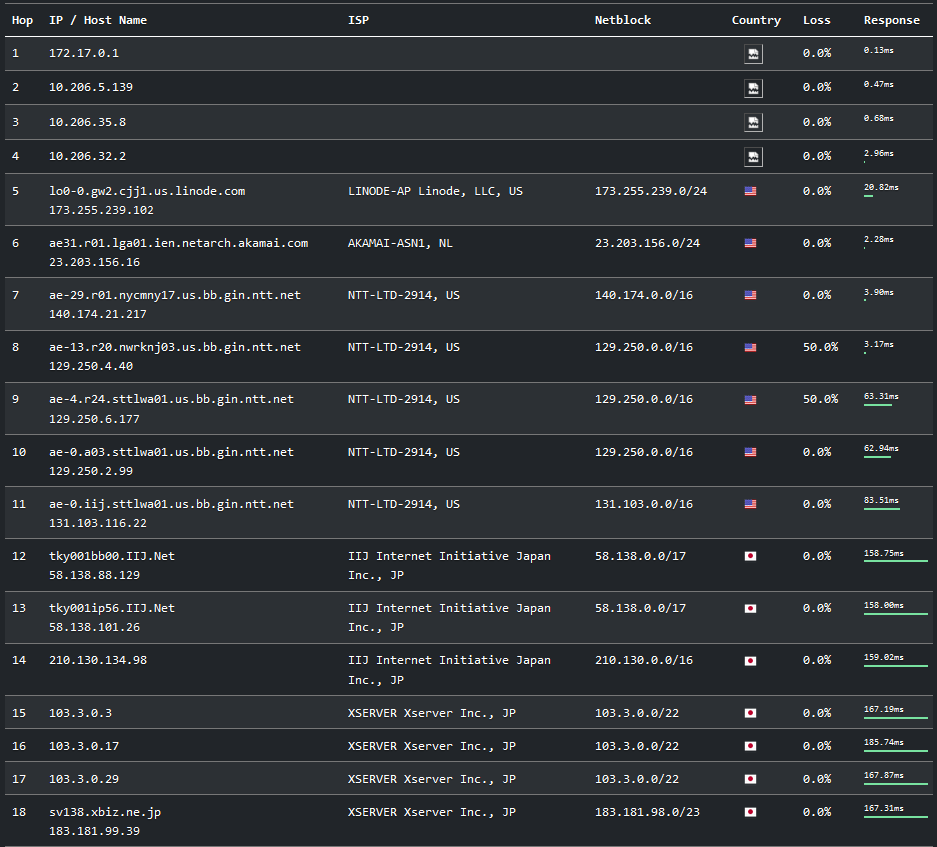
Bei Google lässt sich erkennen, dass nicht der gleiche Google Server als Ziel genutzt wird sondern wahrscheinlich immer der nächstmögliche. In dem Fall unterscheiden sich die Ziele zueinander. Laut ASN Lookup befinden sich jedoch alle Ziel-Server in der US & A.

# NTTグループ公式HP

## 

Ein Bild, das Text, Elektronik, Screenshot, Anzeige enthält.

Automatisch generierte Beschreibung



# Aufgabe 4

Ein Bild, das Karte enthält.

Automatisch generierte Beschreibung

Eine detaillierte Aufzeichnung der Traceroute Knoten befindet sich auf der folgenden Seite. Es ist mittels der genannten Seite nicht möglich Pakete direkt zwischen drei Servern einmal um den Globus zu senden sondern lediglich von bis zu drei Servern zu einem Ziel. Hierbei wird in der Regel der kürzeste bzw. schnellste Pfad gewählt. Je nach Server und Ziel können Pakete auch noch über einen anderen Server am gleichen Standort gesendet werden. So gibt es z.B.: in London mehrere Server nach Johannesburg wobei einer direkt und ein anderer über Kappstadt läuft. Eine direkte Route von Marseille nach Tokyo war nicht möglich da Marseille als einziger Knotenpunkt nicht in der Liste geführt wurde.

1. Für ein Paket um den gesamten Globus wurde die kleinste Dauer einer Übertragung der unten aufgeführten Knotenpunkte addiert.
2. Daraus ergibt sich eine gesamte Zeit von:
3. Gesamte Strecke: 41.742 km

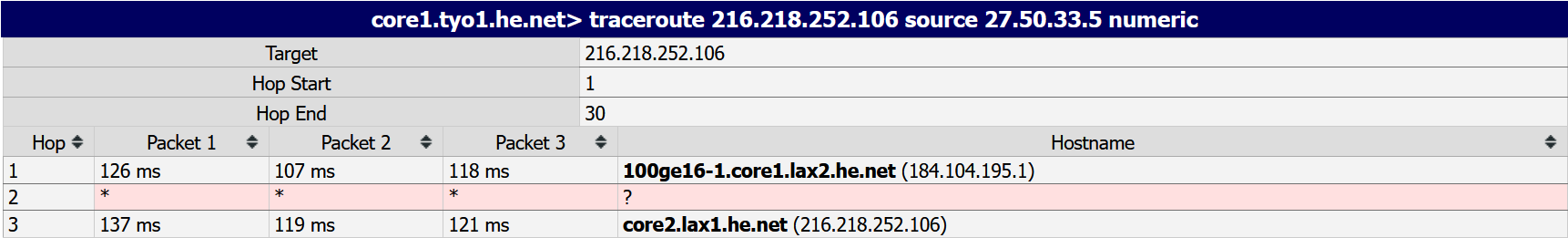
Ein Bild, das Karte enthält.

Automatisch generierte Beschreibung

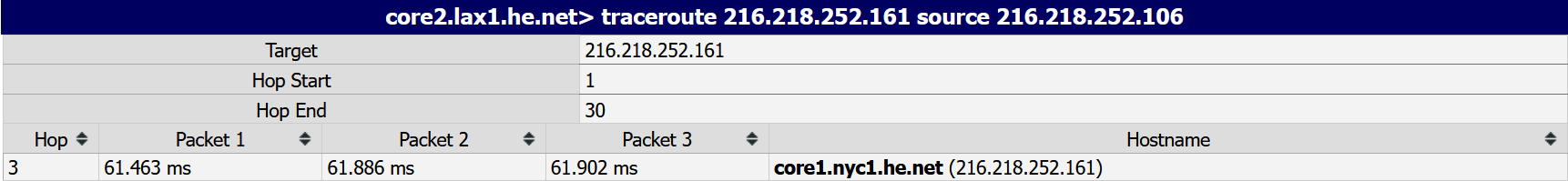
🡪 Die tatsächlich gemessene Zeit ist um ca. 574 ms länger. Dies liegt zum einen daran, dass die tatsächliche Übertragung nicht mit Lichtgeschwindigkeit erfolgt, die Kabel auch auf den Seestrecken nicht der Luftlinie nach verlaufen (siehe Routenbild) sowie aufgrund einer nicht bekannten Auslastung an den einzelnen Knotenpunkten (Paketpuffern).

**Die Gewählte Route verläuft über die folgenden Knotenpunkte**

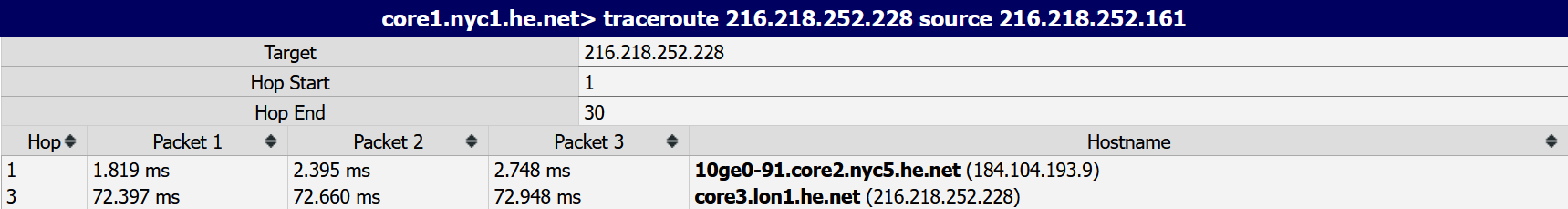
**Server Tokyo [JP]: core1.tyo1.he.net**



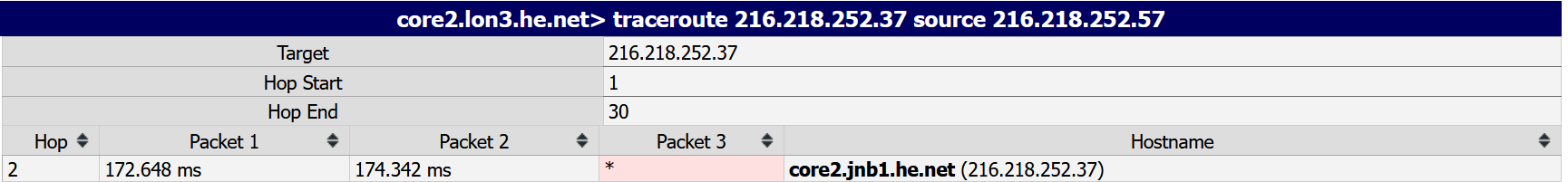
**Server LA [US]: core2.lax1.he.net**



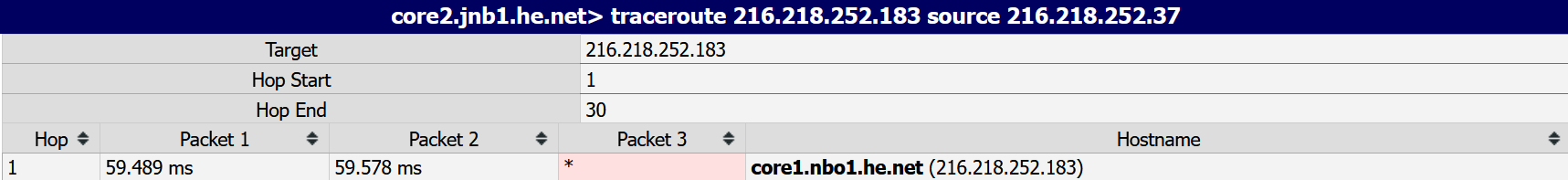
**Server New York [US]: core1.nyc1.he.net**



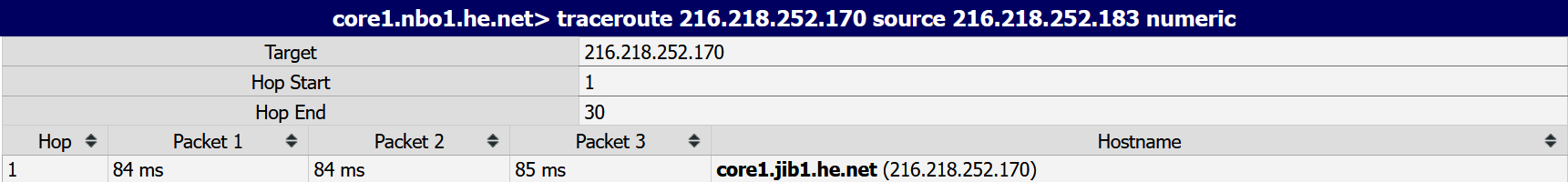
**Server London [UK]: core3.lon1.he.net**



**Server Johannesburg [ZA]: core2.jnb1.he.net**



**Server Nairobi [KE]: core1.nbo1.he.net**



**Server Djibouti [DJ]**  **core1.jib1.he.net**

