BGP protokolliga seotud ohud ja nende minimeerimine

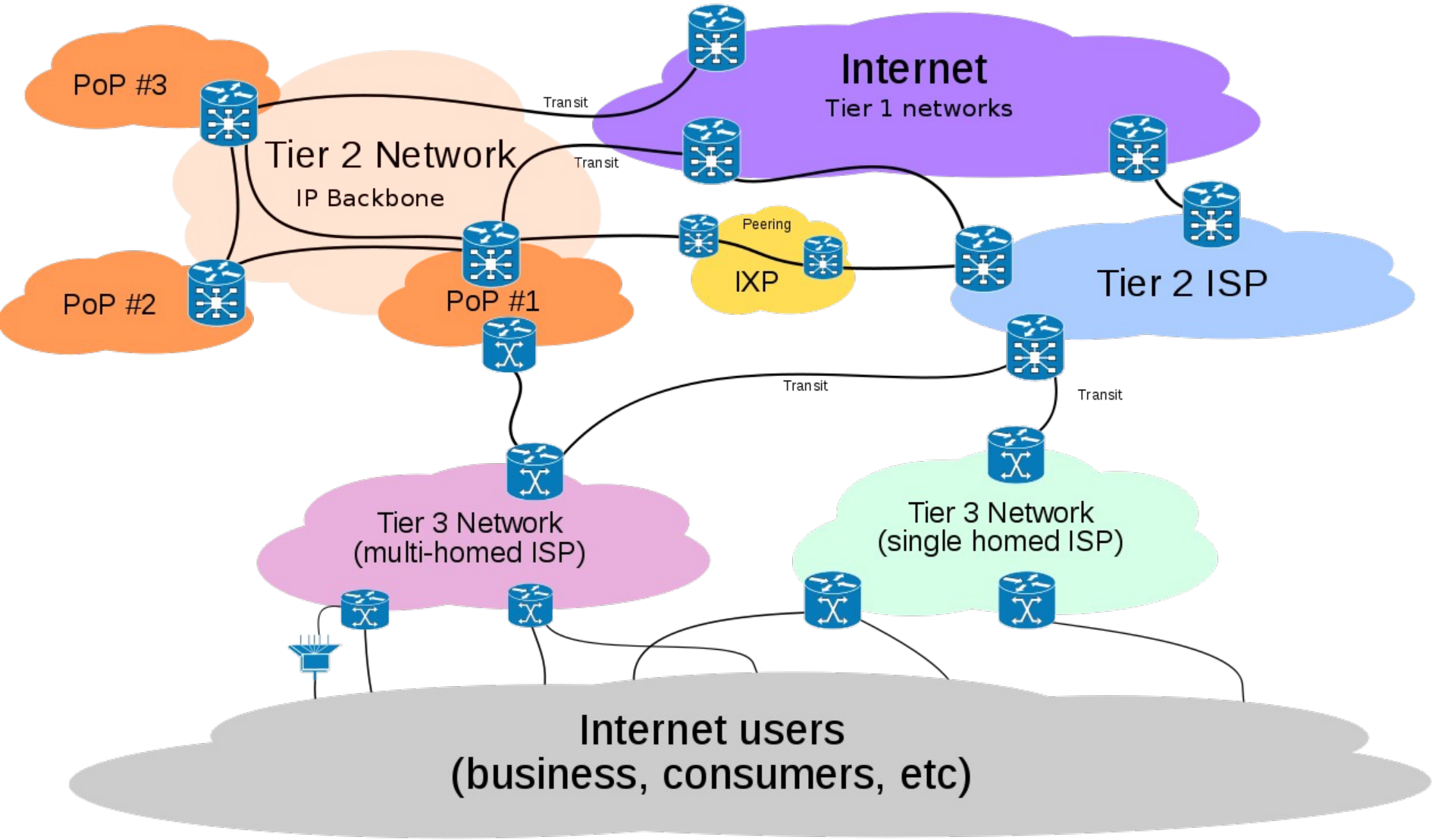
Autor: Siim Adamson

ELUG 2011

Mida räägin?

- Interneti ülesehitus. Näited
- Marsruutimine? Näited!
- BGP milleks vajalik on? Näited!
- BGP rünnatavus? Näited!
- BGP rünnatavuse leevendamine Näited!

See on Internet



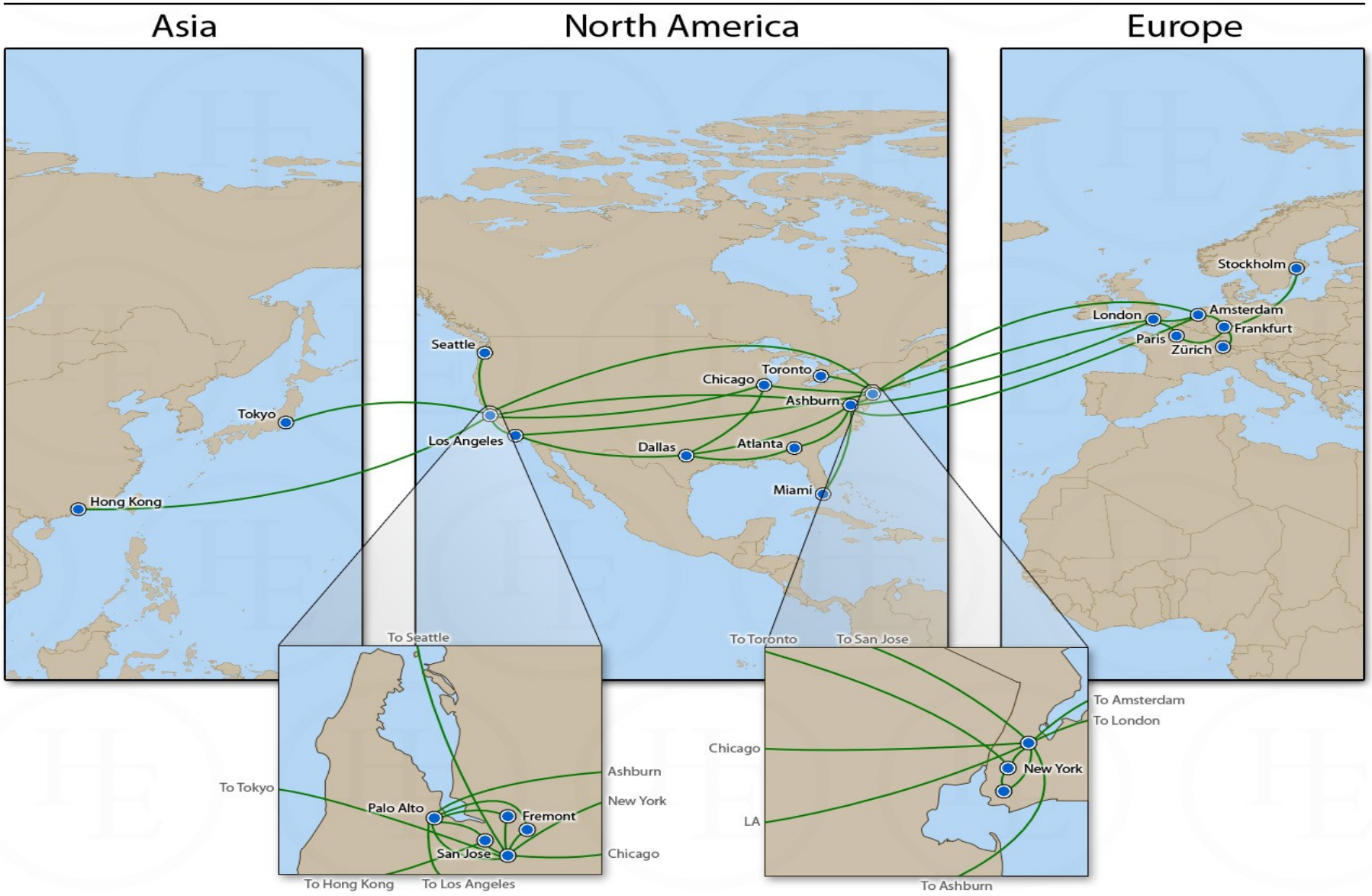
ISP

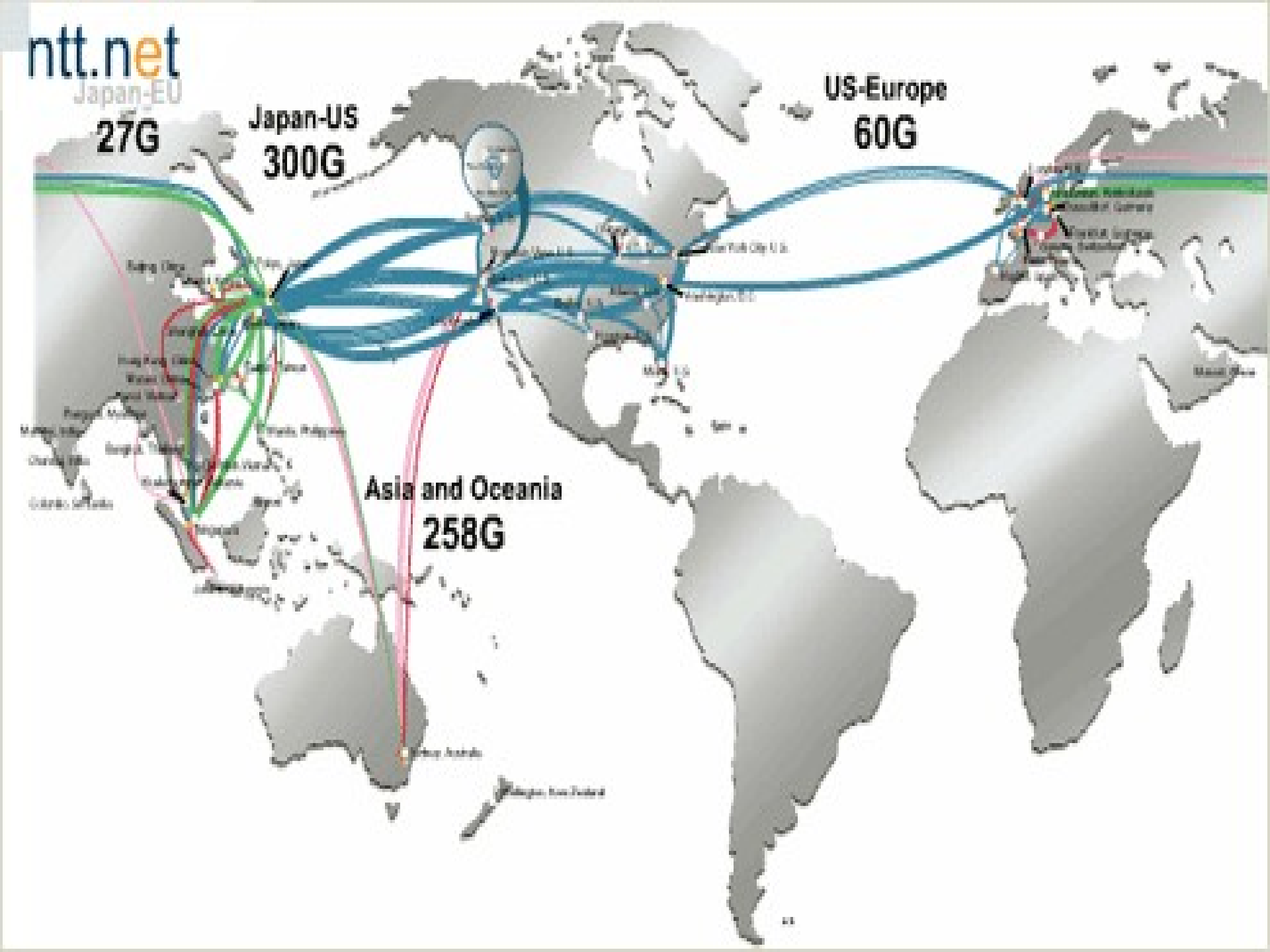
- ICANN (IANA)->reg AS („riigi“ tase)
- ICANN (IANA)->RIR(RIPE)
- ->LIR(ISP) reg IP subnet (whois DB)
- 1 või enam transiit ühendusi (upstream)
- 1 või enam peeringuid (local shortcut)
- 1 või enam downstream BGP kliente
- Tier 1 ISP - pole transiit ühendusi
- (no default route)
- kogu tabel ~338000 kirjet

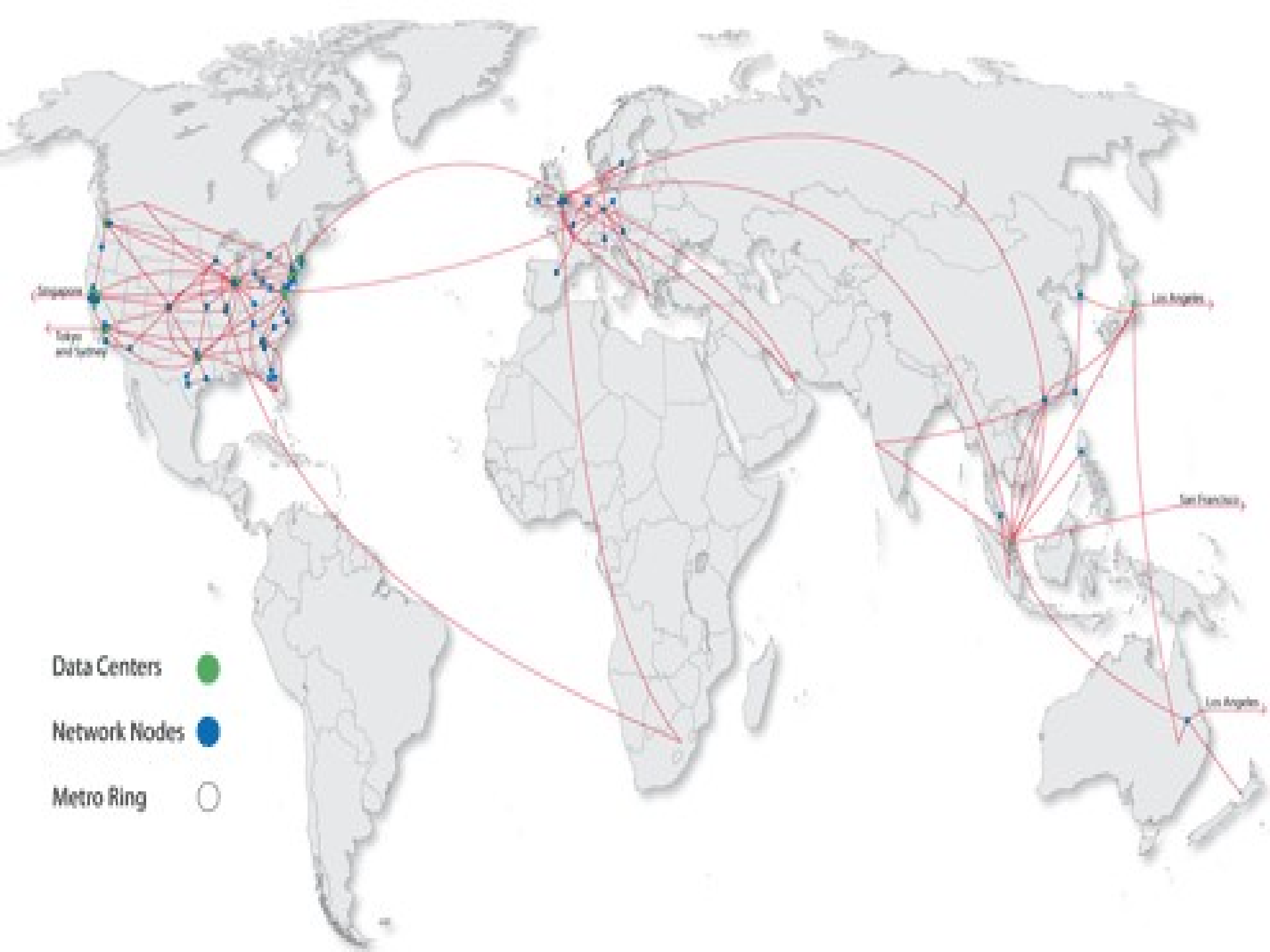
Level (3)

- http://maps.level3.com/default/
- http://en.wikipedia.org/wiki/Tier_1_network
- http://www.robtex.com/as/as3249.html?tab=bgp
- http://www.robtex.com/as/as3332.html?tab=graph

HURRICANE ELECTRIC
INTERNET SERVICES



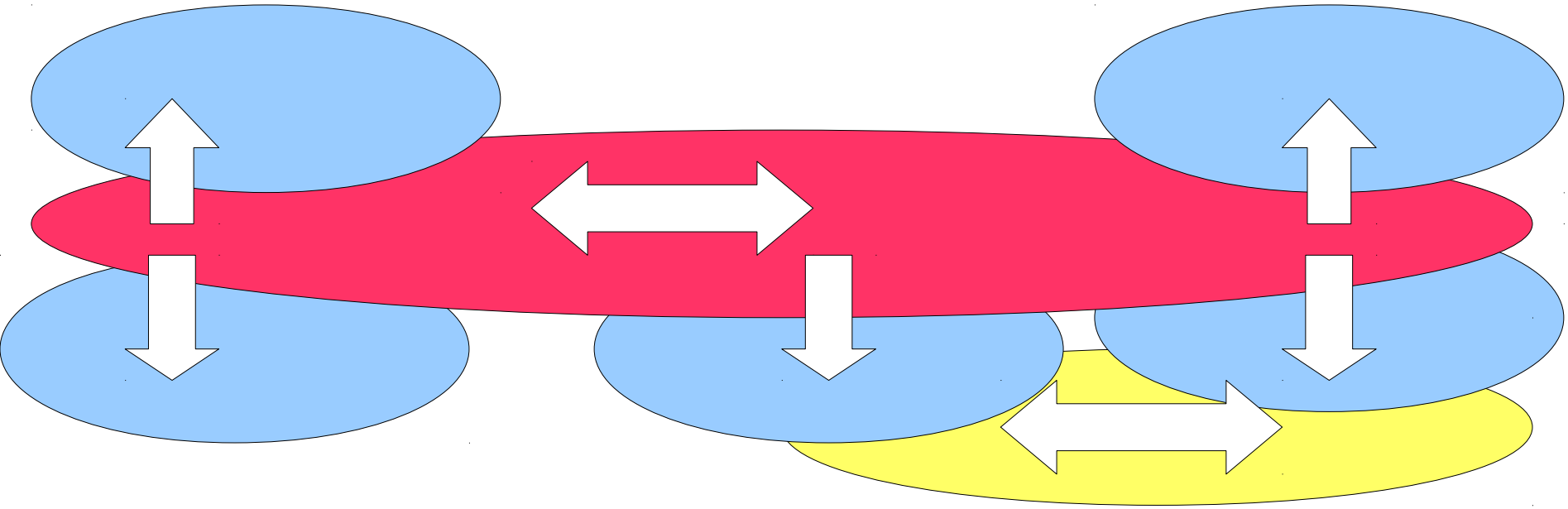

ntt.net
Japan-EU
27G
Japan-US
300G
US-Europe
60G
Asia and Oceania
258G


Singapore
Tokyo and Sydney
Los Angeles
San Francisco
Los Angeles
Data Centers
Network Nodes
Metro Ring

linxtelecom
Crossing Borders

Network Route Map

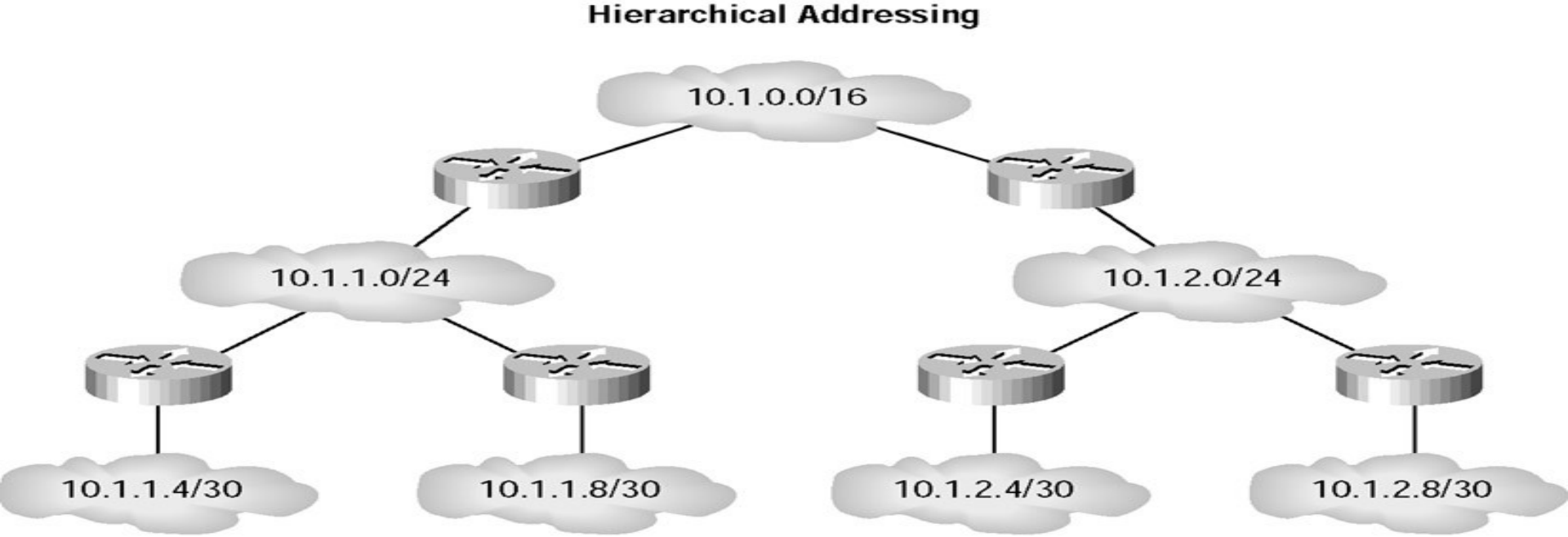
ISP'de AS'd kohakuti = 3D võrgu struktuur

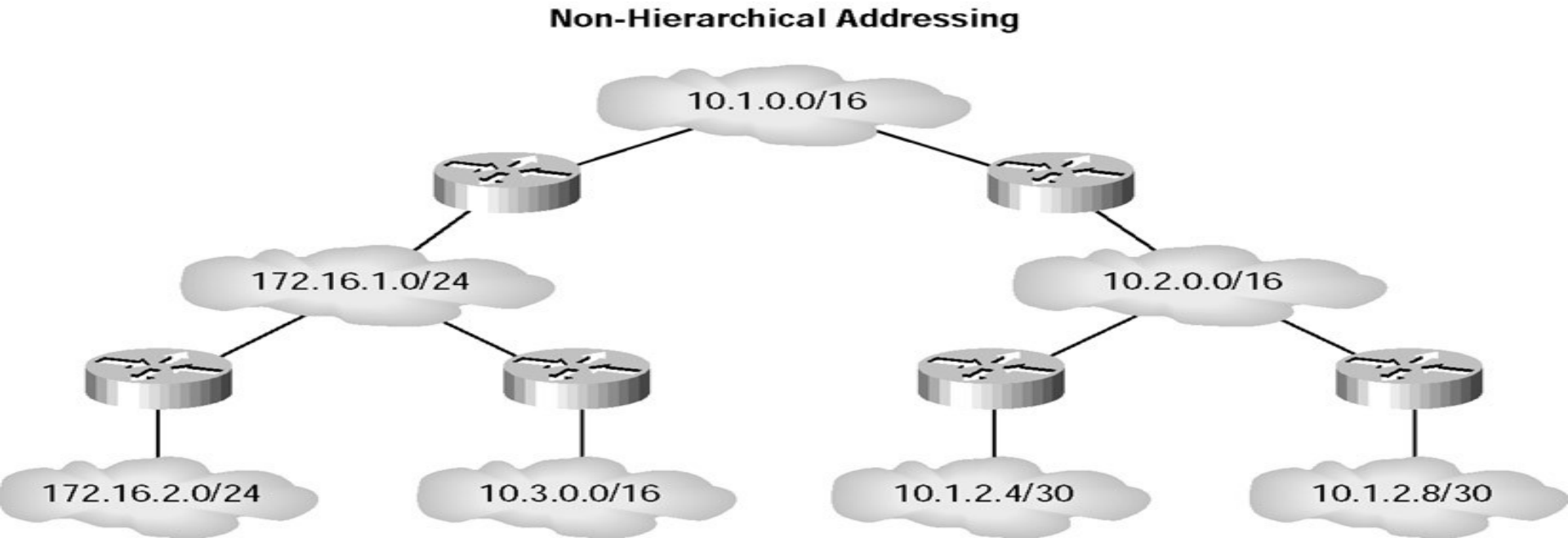


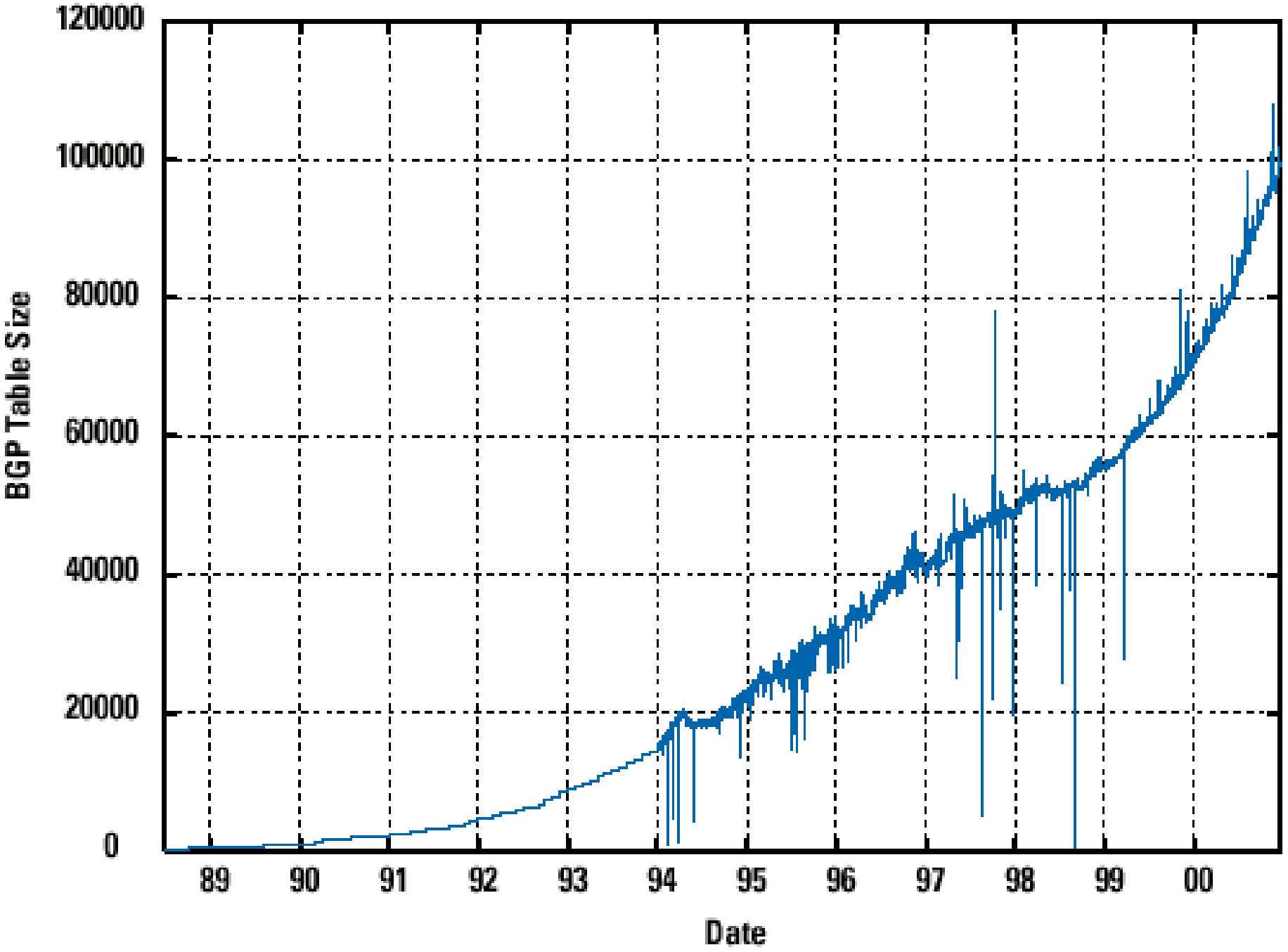
New York

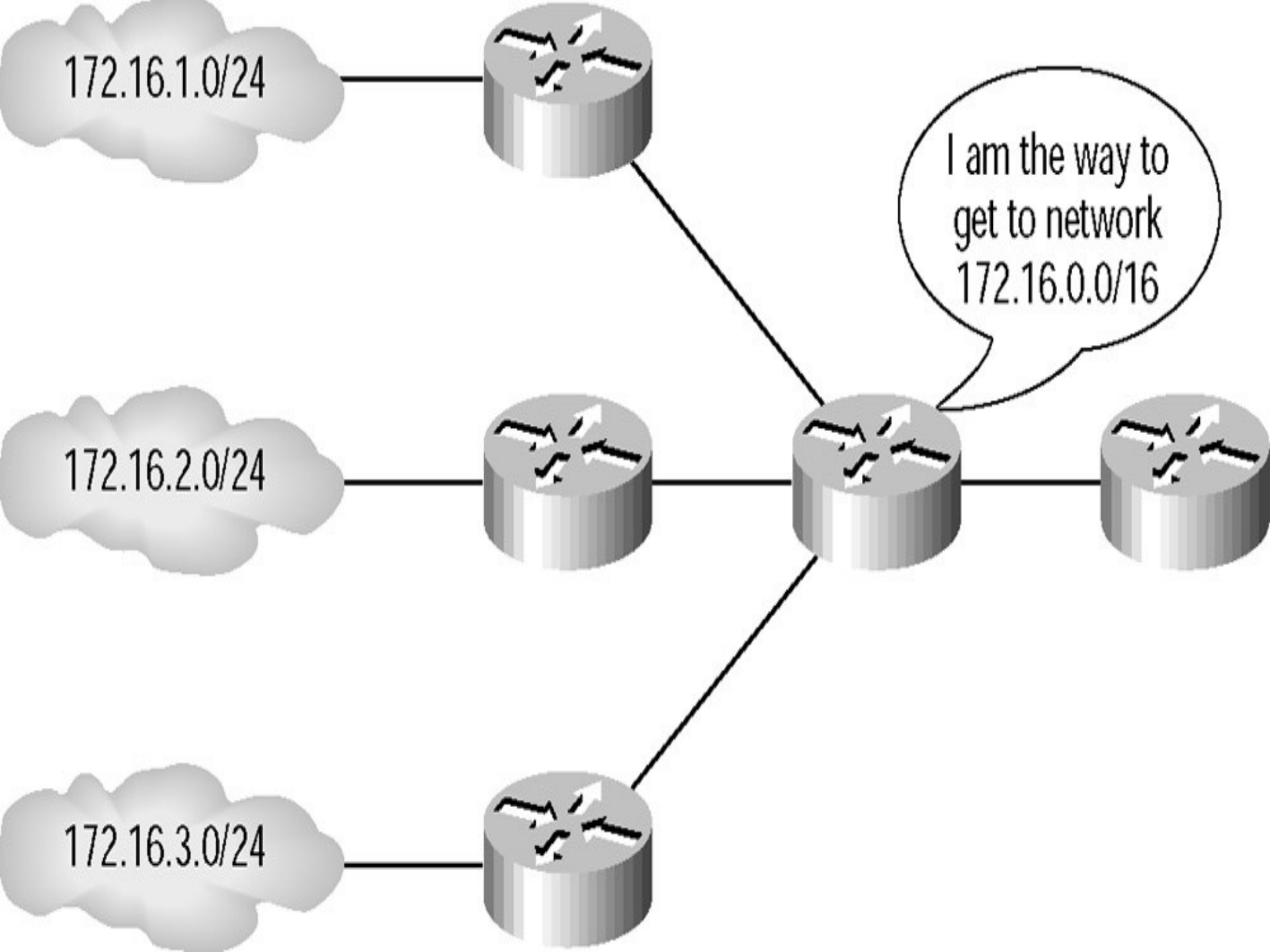
Pariis

Tokyo


Hierarchical Addressing
10.1.0.0/16
10.1.1.0/24
10.1.2.0/24
10.1.1.4/30
10.1.1.8/30
10.1.2.4/30
10.1.2.8/30

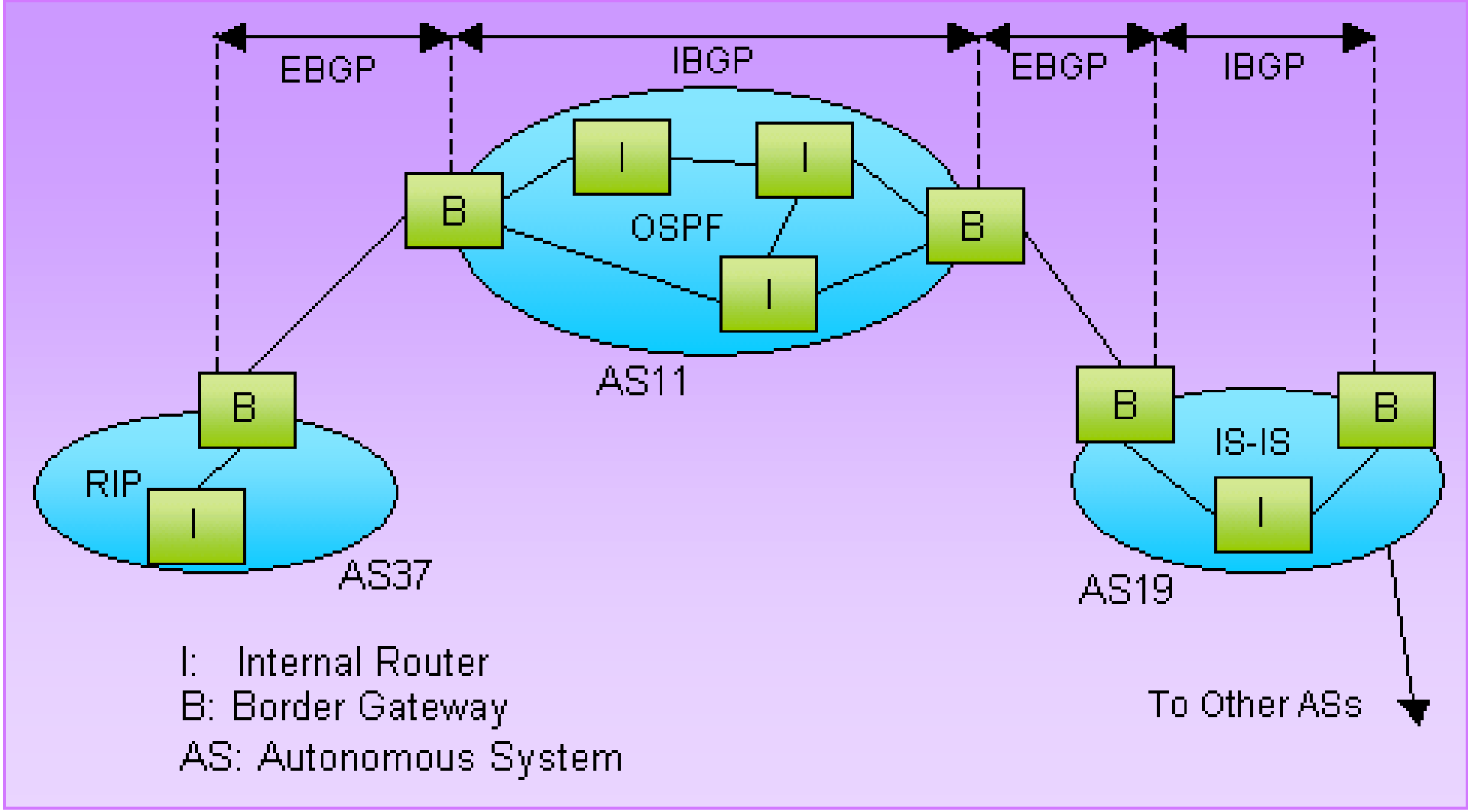

Non-Hierarchical Addressing
10.1.0.0/16
172.16.1.0/24
10.2.0.0/16
172.16.2.0/24
10.3.0.0/16
10.1.2.4/30
10.1.2.8/30


120000
100000
80000
60000
40000
20000
0
BGP Table Size
89
90
91
92
93
94
95
96
97
98
99
00
Date


172.16.1.0/24
172.16.2.0/24
172.16.3.0/24
I am the way to get to network 172.16.0.0/16

BGP

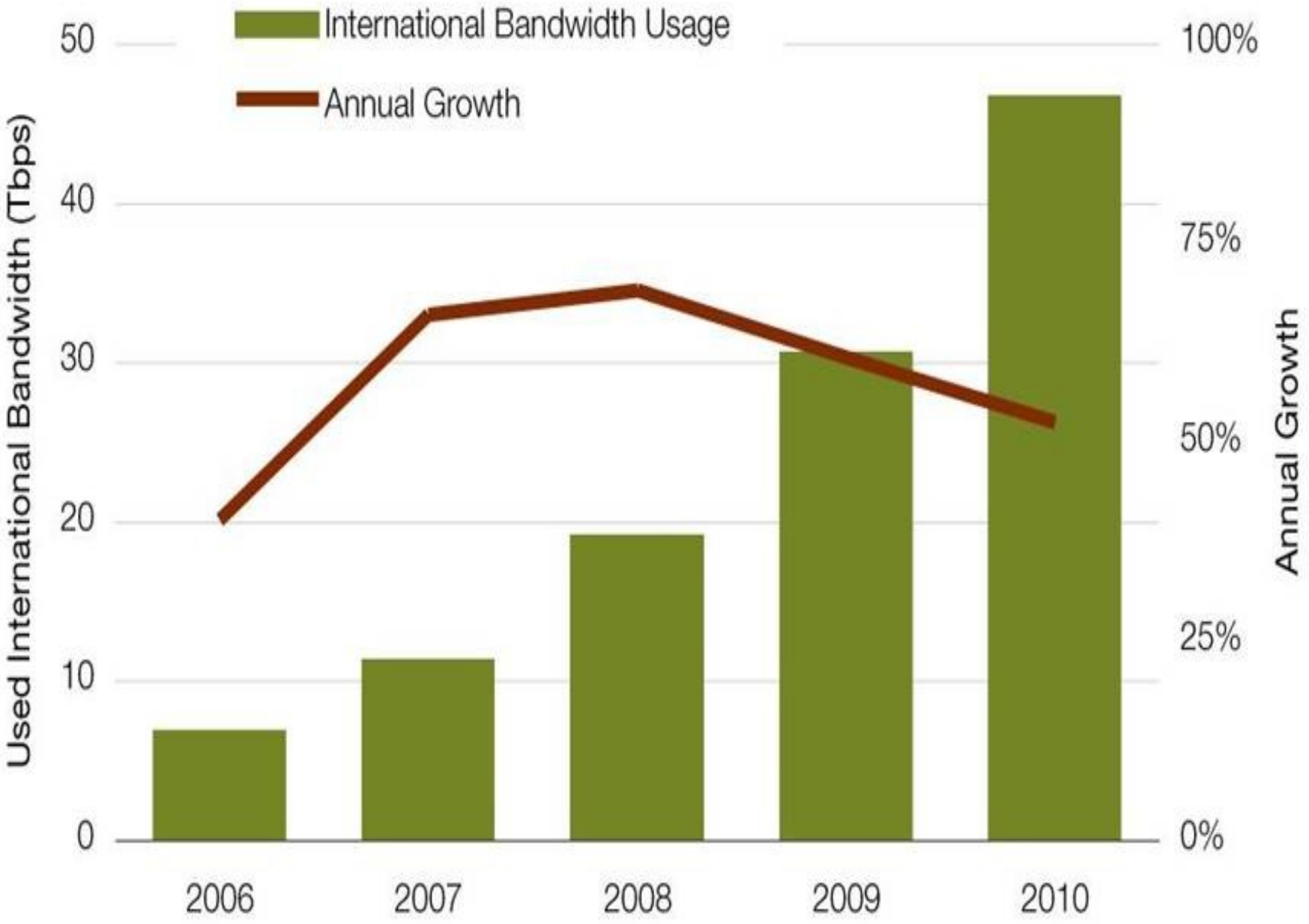
- BGP protokoll, mis edastab AS vahel võrkude kättesaadavuse infot.
- BGP baseerub TCP ühendusel
- BGP koostab võrgust AS to AS graafid (AS path)
- On **Policy based** routing protokoll
- AS'i sees RIP/EIGRP/OSPF/ISIS – kohalik keel, näiteks eesti keel
- AS'de vahel BGP – rahvusvaheline keel, näiteks inglise keel
- Jutu sisu IP-võrkude kohta info vahetus



- RIP/EIRGP/OSPF/ISIS redistributed into BGP
  - http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800943c5.shtml
  - http://www.one-net.eu/jsw/j_data/m_routing.html

Mida ISP kaitseb?

- Adekvaatne marsruut tabel
  - Õiged marsruutide uuendused
  - Võrgus on kättesaadavad
- Saadan välja õiget infot võrgu kohta
  - Ei tapa Internet!
  - Ei taha saada lisa liiklust oma võrku (maksab!)
  - Ei taha suunata liilust läbi kallima side kanali (maksab!)


International Bandwidth Usage
Annual Growth
Used International Bandwidth (Tbps)
Annual Growth
50
40
30
20
10
0
100%
75%
50%
25%
0%
2006
2007
2008
2009
2010

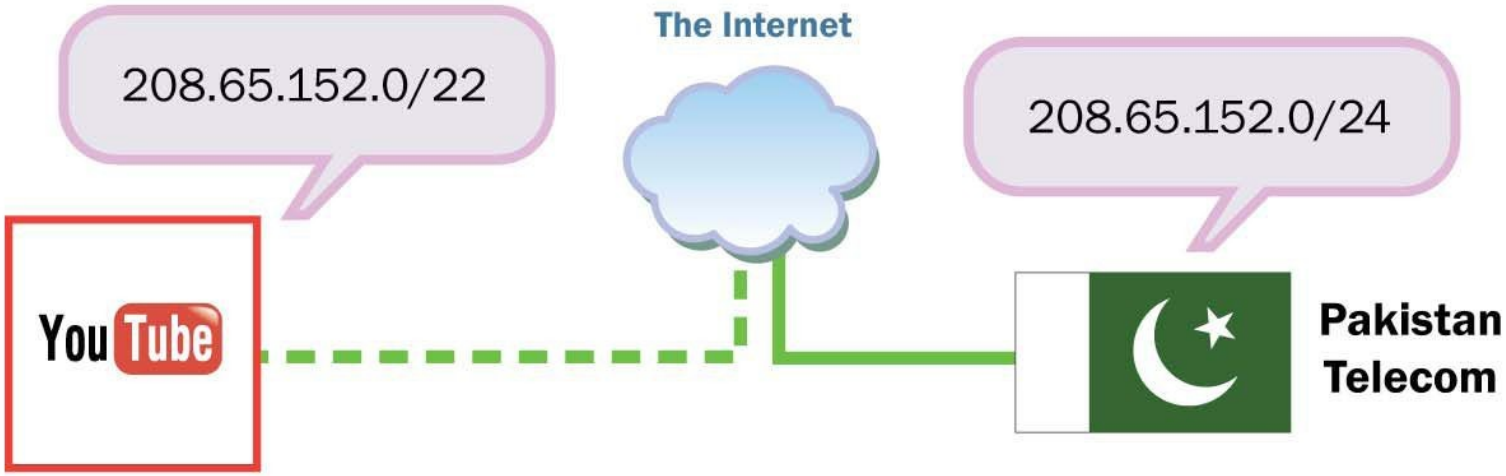
Router flood

- Mis juhtub? ressursid piiratud (CPU, mälu, lingi läbilase)
- Miks juhtub? Valesti seadistamine, tarkvara uuendused
- Leevendus? Piirangud routing tabelile, uuendustele
  - Deny prefixes > /28
  - Deny prefixes < /6
  - Signeeri BGP uuendused

Attack TCP session

- BGP on TCP rünnetele avatud
- TCP RST – BGP peering katkeb, võrgu kättesaadavus!
- Leevendus? Kasuta TCP md5 sessiooni autentimist (md5 :) palju pärand rauda võrgus!)
- TTL piirang – BGP ruuterid on otse ühendatud tavaliselt (samas võrgus)

Aadressruumi kaaberdamine



- Youtube case
- http://www.renesys.com/tech/presentations/
- Leevendus: PKI, Subnet DB,
- signeeritud BGP uuendused

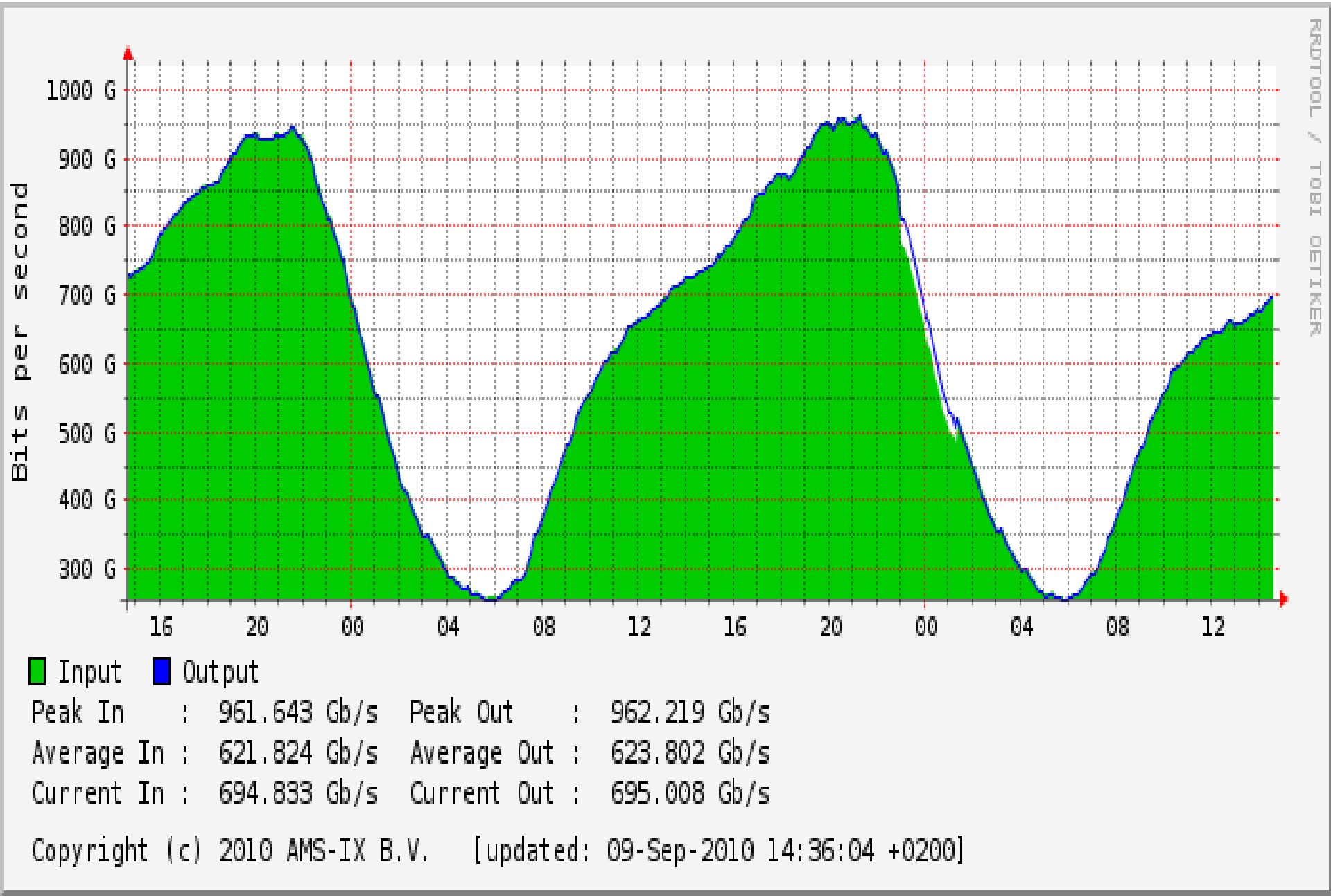
Kasutamata aadressiruumi hõivamine

- Kasutatakse, et:
  - Saata SPAMi
  - Jälitamatu ründe tegemiseks
  - Privaat alamvõrkudest ei jätku :|
- Näide **jaanuaris 2010 APNIC võttis kasutsele 1.0.0.0/8 võrgu ja sai 200 Mbps võrguliiklust selga (keegi juba kasutas 1.0.0.0/8 võrku :)**

Vigase BGP sõnumi saatmine

- Halvemal juhul ruuter hangub (tarkavara viga) TUUMIKVÕRGU RIKE!
- Vigane kirje marsruuttabelis
  - 1 AS = 1 ISP
  - Mitu AS'i = Internet
- Ruuteri exploitimine!
- Leevendus oma tarkvara uuenuse protsessi ja väldi monokultuuri (kasutusel on ainult 1 tootja mudel X seadmed)

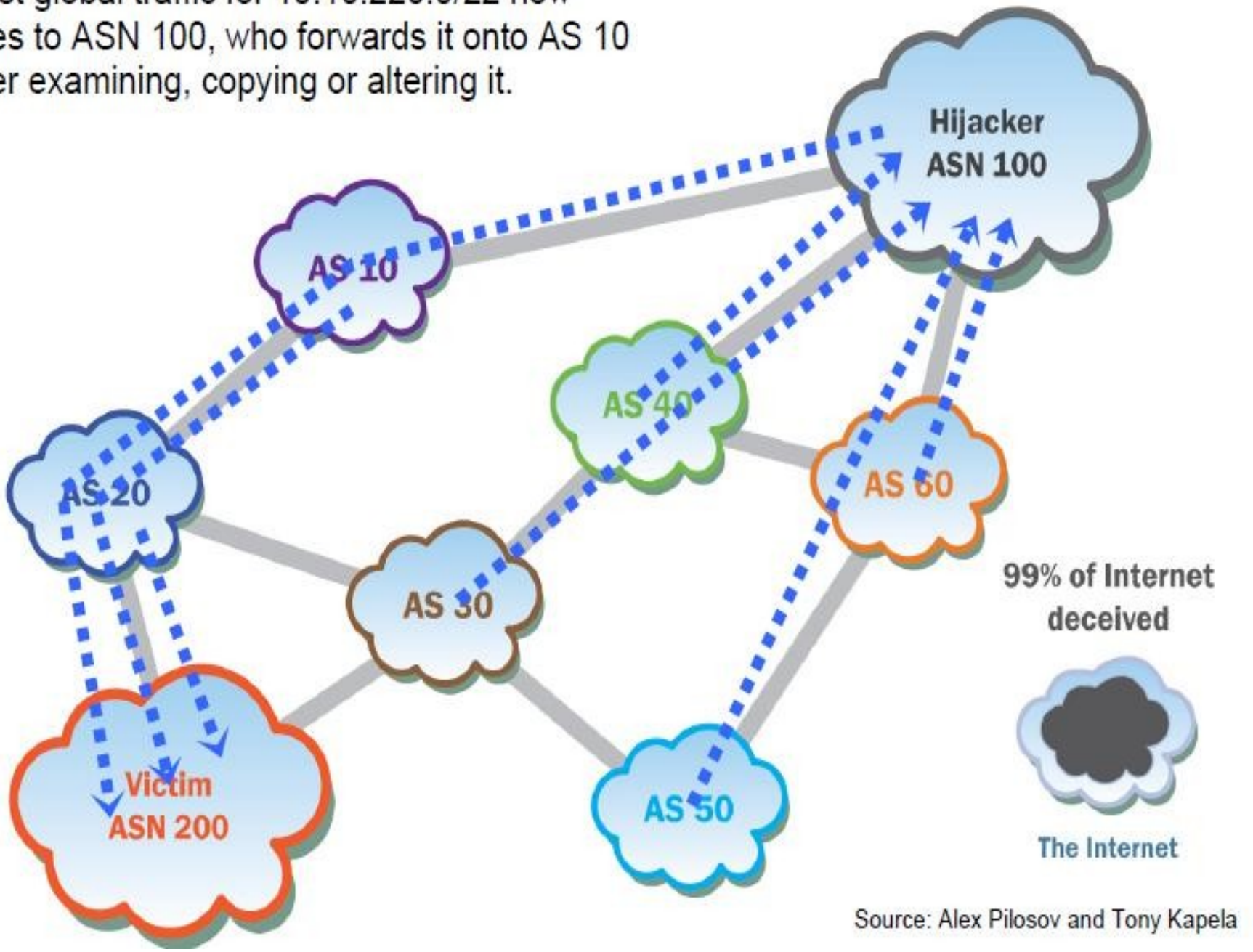
AMS-IX 1Tb/s


RRDTOOL / TOBI OETIKER
Bits per second
1000 G
900 G
800 G
700 G
600 G
500 G
400 G
300 G
16
20
00
04
08
12
16
20
00
04
08
12
Input
Output
Peak In : 961.643 Gb/s
Peak Out : 962.219 Gb/s
Average In : 621.824 Gb/s
Average Out : 623.802 Gb/s
Current In : 694.833 Gb/s
Current Out : 695.008 Gb/s
Copyright (c) 2010 AMS-IX B.V. [updated: 09-Sep-2010 14:36:04 +0200]

Miks rünnatakse?

- DoS rünne – eeldab kuulikindlat ISP'd
- Teenuse/IP vargus
  - SPAM, viiruste, pahavara levitamine,
  - Pealtkuulamine (Hiina vs USA 2011)
  - http://bgpmon.net/blog/?p=323
- MITM ründe näide
  - http://nanog.org/meetings/nanog44/presentat
- Õnneks 99% BGP probleemidest on ISP poolsed vead

Most global traffic for 10.10.220.0/22 now goes to ASN 100, who forwards it onto AS 10 after examining, copying or altering it.



Source: Alex Pilosov and Tony Kapela

Kokkuvõte

- Muudatused/uuendused aeglased
- Palju vana tarkvara ja riistvara võrgus
- ISP pole muudatuseks valmis (if IT work ain't fix IT)
- Oluline pole mida MA maailmast arvan, **oluline on mida MAAILM arvab minust**!
- IP (subnet) pole geograafilise asukohaga seotud! **Numbri liikuvus!**

TLLIX/TIX ülevaade

- BGP uuendused pole md5 signatuuridega
- Väike usalduse ring ~15 ISP'i
- http://tix.estpak.ee/ operates Elion, 13 members
- http://www.tllix.net/ operates Linxtelecom 17 members