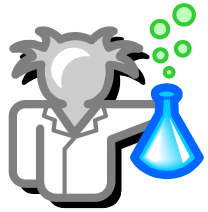
Securing the Internet's Foundations: Addresses and Routing

AUSCERT 2011

Geoff Huston

Chief Scientist, APNIC



On the Internet…

…there are many ways to be bad!

An Ascending Scale of Badness

- Port Scan for known exploits

  General annoyance

- Spew spam

  Yes, there are still gullible folk out there!

- Mount a fake web site attack

  And lure victims

- Enlist a bot army and mount multi-gigabit DOS attacks

  Extortion leverage and general mayhem

- Mount a routing attack

  And bring down an entire region / country / global network!

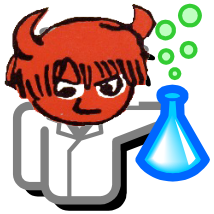
If I were bad (and greedy)…

I'd attack routing.

If I were bad (and greedy)…

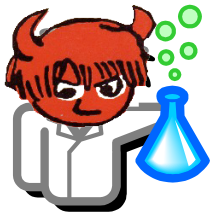
- Through **routing** I'd attack the **DNS**
- Through the DNS I'd lure traffic through an **interceptor web server**
- And be able to quietly collect users' details quietly, selectively and (if I am careful) undetectably

Welcome to today's online fraud industry



If I were <u>really</u> bad (and evil)…

I'd still attack routing.



If I were really bad (and evil)…

- Through routing I'd attack:
  - the route registry server system
  - the DNS root system
  - trust anchors for TLS and browser certificates
  - isolate critical public servers and resources
  - overwhelm the routing system with spurious information

And bring selected parts of the network to a complete chaotic halt!

c|net NEWS.com

Search:

Today on CNET | Reviews | News | Downloads | Tips & Tricks | CNET TV | Compare Prices

Business Tech | Cutting Edge | Green Tech | Wireless | Security | Media | Markets | Personal

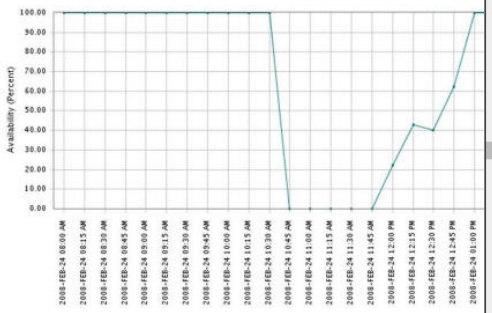
News Blog

Recent posts on technology, trends, and

February 25, 2008 2:30 PM PST

How Pakistan knocked YouTube offline (and how to make s happens again)

Posted by Declan McCullagh



This graph that network-monitoring firm Keynote Systems provided to us availability of YouTube.com dropping dramatically from 100 percent to 0 hour. It didn't recover completely until two hours had elapsed.

(Credit: Keynote Systems)

A high-profile incident this weekend in which Pakistan's state-owned telecommunications company man global Web highlights a long-standing security weakness in the way the Internet is managed.

After receiving a censorship order from the telecommunications ministry directing that YouTube.com b went even further. By accident or design, the company broadcast instructions worldwide claiming to be anyone trying to reach YouTube's range of Internet addresses.

The security weakness lies in why those false instructions, which took YouTube offline for two hours o routers around the globe. That's because Hong Kong-based PCCW, which provides the Internet link to the misleading broadcast--which is what most large providers in the United States and Europe do.

This is not a new problem. A network provider in Turkey once pretended to be the entire Internet, snarli Web sites unreachable. Con Edison accidentally hijacked the Internet addresses for Panix customers Omnimedia and the *New York Daily News*. Problems with errant broadcasts go back as far as 1997.

It's also not an infrequent problem. An automatically-updated list of suspicious broadcasts created by New Mexico shows apparent mischief--in the form of dubious claims to be the true destination for certs

bbc.co.uk

Home | TV | Radio | Talk | Where I Live | A-Z Index | Search

UK version | International version | About the versions | Low graphics | Accessibility help

BBC NEWS

BBC News 24

News services
Your news when you want it

News Front Page
World
UK
England
Northern Ireland
Scotland
Wales
Business
Politics
Health
Education
Science/Nature
Technology
Entertainment
Also in the news

Video and Audio

Have Your Say
Magazine
In Pictures
Country Profiles
Special Reports

RELATED BBC SITES
SPORT
WEATHER
CBBC NEWSROUND
ON THIS DAY
EDITORS' BLOG

Last Updated: Tuesday, 26 February 2008, 13:43 GMT

E-mail this to a friend | Printable version

Pakistan lifts the ban on YouTube

Pakistan's telecoms regulator has lifted the restrictions it imposed on video-sharing website YouTube.

The Pakistan Telecommunications Authority has told internet service providers (ISPs) to restore access to the site, according to a spokeswoman.

Turkey and Thailand have in the past also banned access to the site

Google, the owner of YouTube, confirmed service had been restored in Pakistan.

The attempt to block the site, reportedly because of a "blasphemous" video clip, caused a near global blackout of the site on Sunday.

A spokesman for YouTube told the BBC News website: "We are pleased to confirm that YouTube is again accessible in Pakistan."

It is reported that a trailer for a forthcoming film by Dutch lawmaker Geert Wilders, which portrays Islam in a negative light, was behind the restrictions.

The ban wa
Pakistan on
the BBC Ne
technology
Waters, sai
citizens fror
it was belie
"hijacked" t
address of
site.

Those detai
on to the cc
Pakistan at
a different

But the det
internet by
YouTube wa

The block o
lifted once
of the issue
engineers.

VIDEO AND AUDIO NEWS
How the YouTube block caused waves around the world
WATCH

SEE ALSO
- Pakistan blocks YouTube website
  24 Feb 08 | South Asia
- Should governments block websites?
  25 Feb 08 | Middle East
- Thai ban on YouTube website ends
  31 Aug 07 | Asia-Pacific
- YouTube site 'blocked' in Morocco
  29 May 07 | Africa
- Turkish court bans YouTube access
  07 Mar 07 | Europe

RELATED INTERNET LINKS
- YouTube

The BBC is not responsible for the content of external internet sites

TOP TECHNOLOGY STORIES
- Wiki boss 'edited for donation'

The block on the servers was lifted once PCCW had been told of the issue by YouTube engineers.

A statement from Google said that the problems lasted for "about two hours".

"Traffic to YouTube was routed according to erroneous internet protocols, and many users around the world could not access our site," it said.

A leading net professional told BBC News: "This was probably a simple mistake by an engineer at Pakistan Telecom. There's nothing to suggest this was malicious."

IP hijacking [illegible] unique address by corrupting the internet's routing tables, which direct the flow of data around the world.

"The fact YouTube is back in action makes me revise my thoughts on the clash between governments and freedom of speech"

Rory Cellan-Jones

Read Rory's blog

Some recent cases …

208.65.153.0/24 originated by AS17557

Advertisement of a more specific route by Pakistan Telecom that managed to take YouTube off the air in February 2008

61.0.0.0/8 originated by AS4678

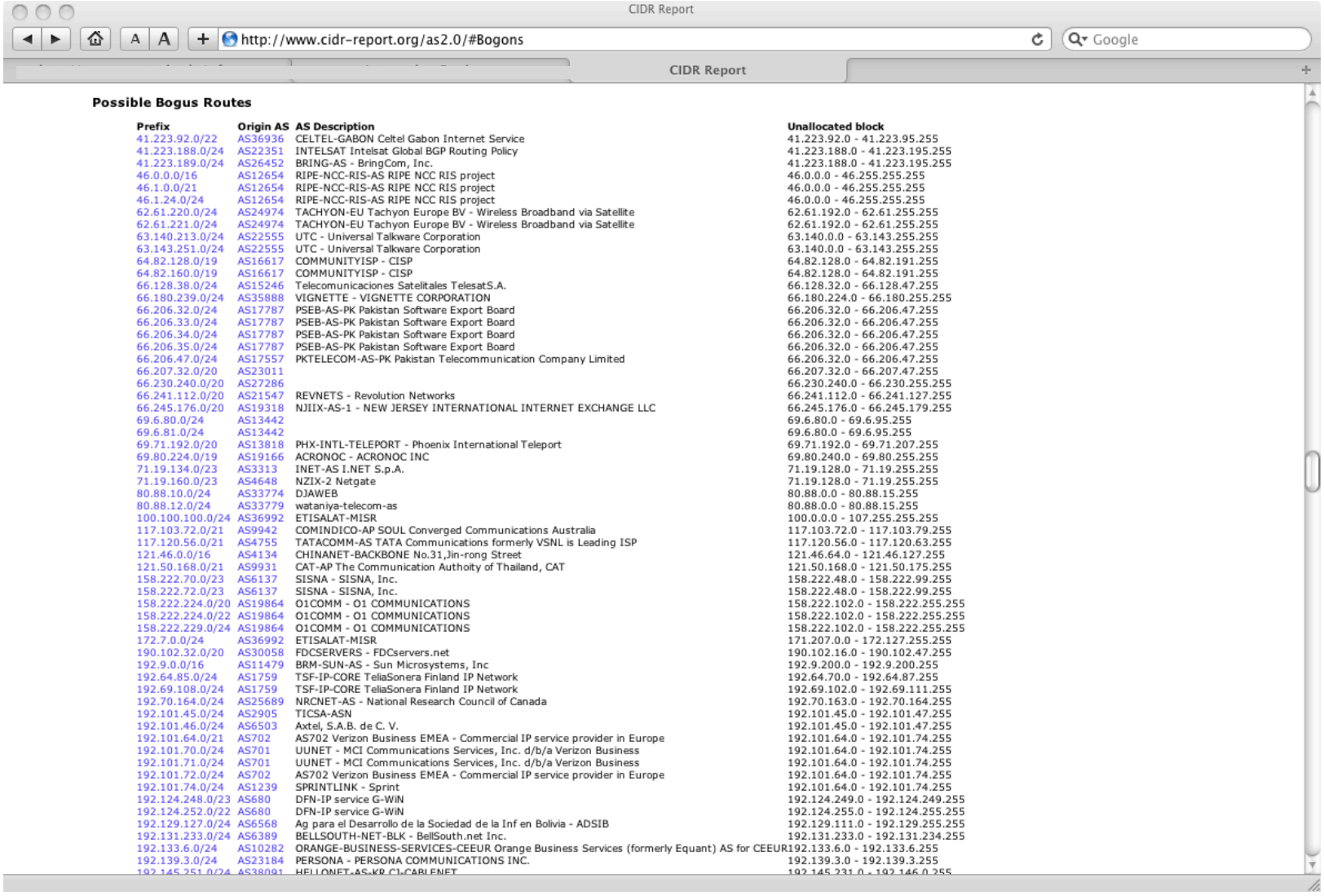
Advertisement of a more general route by a spammer in order to conceal their identity by using an anonymous source ip address, occurring intermittently 2004 – 2007

d000::/8 originated by AS28716

Advertisement of a massive bogon more general route in IPV6 from 13 Nov 2009 until 15 Jan 2010 – and noone noticed for 2 months!

How many advertisements in today's BGP are "lies"?

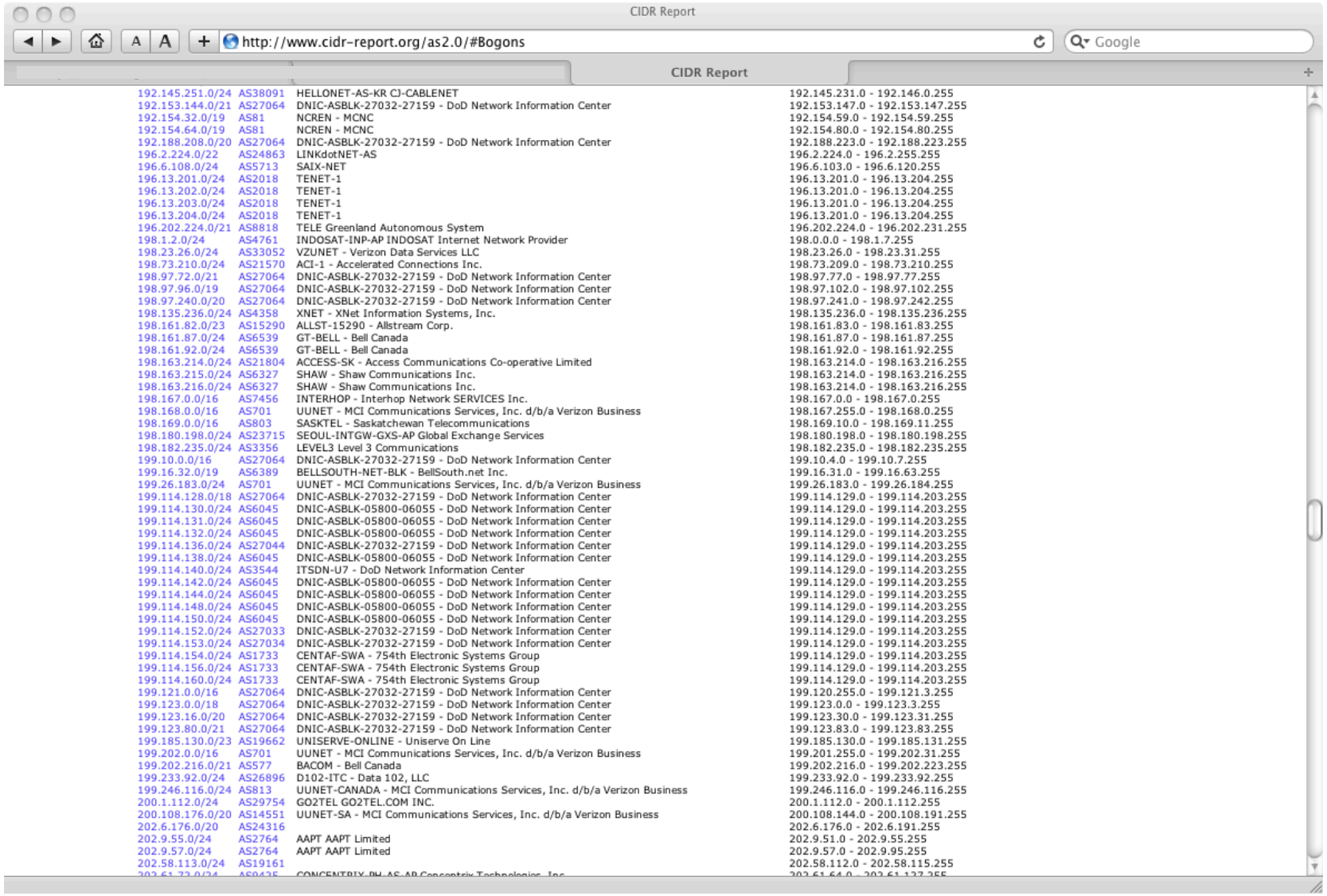
www.cidr-report.org



Possible Bogus Routes

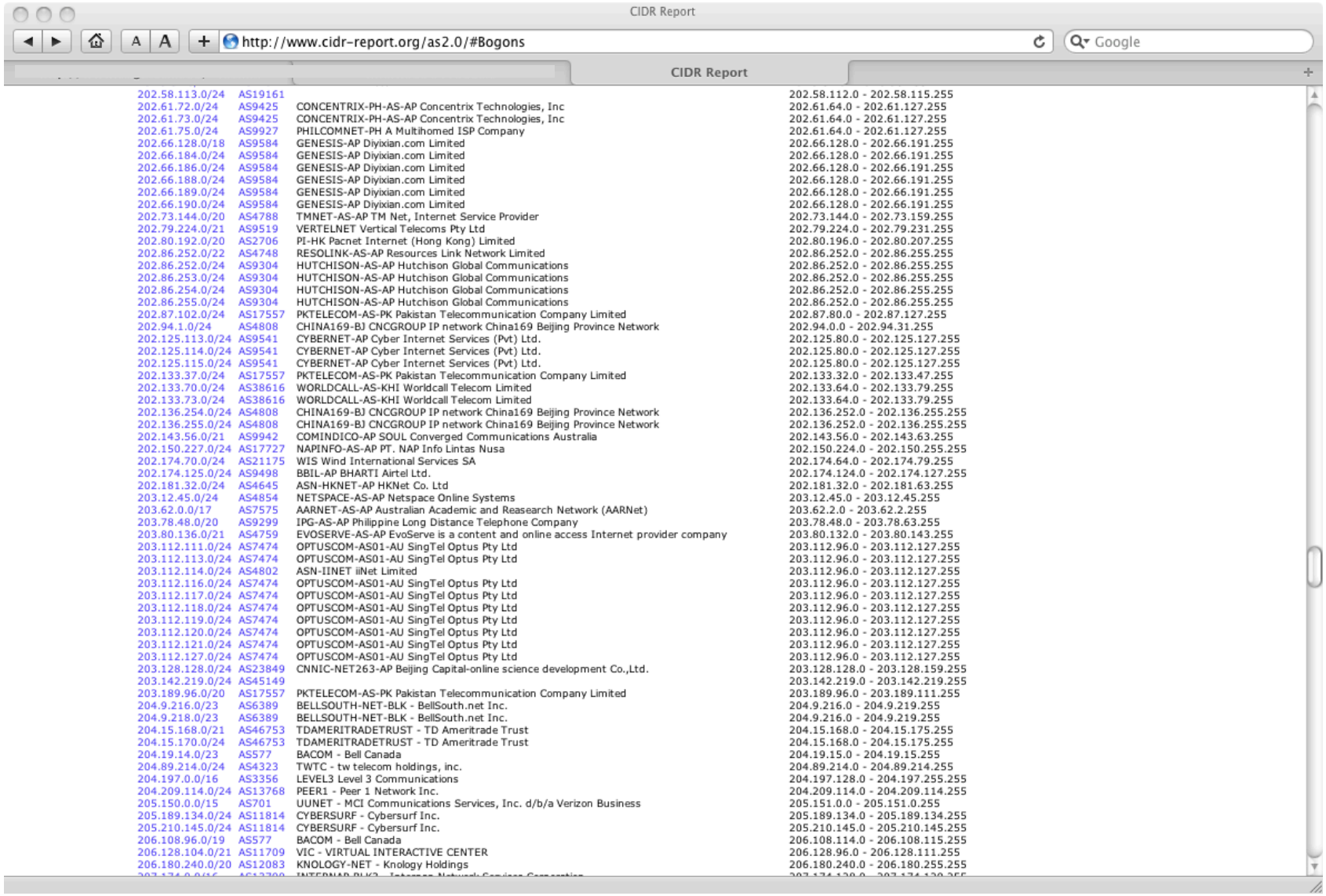
Prefix	Origin AS	AS Description	Unallocated block
41.223.92.0/22	AS36936	CELTEL-GABON Celtel Gabon Internet Service	41.223.92.0 - 41.223.95.255
41.223.188.0/24	AS22351	INTELSAT Intelsat Global BGP Routing Policy	41.223.188.0 - 41.223.195.255
41.223.189.0/24	AS26452	BRING-AS - BringCom, Inc.	41.223.188.0 - 41.223.195.255
46.0.0.0/16	AS12654	RIPE-NCC-RIS-AS RIPE NCC RIS project	46.0.0.0 - 46.255.255.255
46.1.0.0/21	AS12654	RIPE-NCC-RIS-AS RIPE NCC RIS project	46.0.0.0 - 46.255.255.255
46.1.24.0/24	AS12654	RIPE-NCC-RIS-AS RIPE NCC RIS project	46.0.0.0 - 46.255.255.255
62.61.220.0/24	AS24974	TACHYON-EU Tachyon Europe BV - Wireless Broadband via Satellite	62.61.192.0 - 62.61.255.255
62.61.221.0/24	AS24974	TACHYON-EU Tachyon Europe BV - Wireless Broadband via Satellite	62.61.192.0 - 62.61.255.255
63.140.213.0/24	AS22555	UTC - Universal Talkware Corporation	63.140.0.0 - 63.143.255.255
63.143.251.0/24	AS22555	UTC - Universal Talkware Corporation	63.140.0.0 - 63.143.255.255
64.82.128.0/19	AS16617	COMMUNITYISP - CISP	64.82.128.0 - 64.82.191.255
64.82.160.0/19	AS16617	COMMUNITYISP - CISP	64.82.128.0 - 64.82.191.255
66.128.38.0/24	AS15246	Telecomunicaciones Satelitales TelesatS.A.	66.128.32.0 - 66.128.47.255
66.180.239.0/24	AS35888	VIGNETTE - VIGNETTE CORPORATION	66.180.224.0 - 66.180.255.255
66.206.32.0/24	AS17787	PSEB-AS-PK Pakistan Software Export Board	66.206.32.0 - 66.206.47.255
66.206.33.0/24	AS17787	PSEB-AS-PK Pakistan Software Export Board	66.206.32.0 - 66.206.47.255
66.206.34.0/24	AS17787	PSEB-AS-PK Pakistan Software Export Board	66.206.32.0 - 66.206.47.255
66.206.35.0/24	AS17787	PSEB-AS-PK Pakistan Software Export Board	66.206.32.0 - 66.206.47.255
66.206.47.0/24	AS17557	PKTELECOM-AS-PK Pakistan Telecommunication Company Limited	66.206.32.0 - 66.206.47.255
66.207.32.0/20	AS23011		66.207.32.0 - 66.207.47.255
66.230.240.0/20	AS27286		66.230.240.0 - 66.230.255.255
66.241.112.0/20	AS21547	REVNETS - Revolution Networks	66.241.112.0 - 66.241.127.255
66.245.176.0/20	AS19318	NJIIX-AS-1 - NEW JERSEY INTERNATIONAL INTERNET EXCHANGE LLC	66.245.176.0 - 66.245.179.255
69.6.80.0/24	AS13442		69.6.80.0 - 69.6.95.255
69.6.81.0/24	AS13442		69.6.80.0 - 69.6.95.255
69.71.192.0/20	AS13818	PHX-INTL-TELEPORT - Phoenix International Teleport	69.71.192.0 - 69.71.207.255
69.80.224.0/19	AS19166	ACRONOC - ACRONOC INC	69.80.240.0 - 69.80.255.255
71.19.134.0/23	AS3313	INET-AS I.NET S.p.A.	71.19.128.0 - 71.19.255.255
71.19.160.0/23	AS4648	NZIX-2 Netgate	71.19.128.0 - 71.19.255.255
80.88.10.0/24	AS33774	DJAWEB	80.88.0.0 - 80.88.15.255
80.88.12.0/24	AS33779	wataniya-telecom-as	80.88.0.0 - 80.88.15.255
100.100.100.0/24	AS36992	ETISALAT-MISR	100.0.0.0 - 107.255.255.255
117.103.72.0/21	AS9942	COMINDICO-AP SOUL Converged Communications Australia	117.103.72.0 - 117.103.79.255
117.120.56.0/21	AS4755	TATACOMM-AS TATA Communications formerly VSNL is Leading ISP	117.120.56.0 - 117.120.63.255
121.46.0.0/16	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	121.46.64.0 - 121.46.127.255
121.50.168.0/21	AS9931	CAT-AP The Communication Authoity of Thailand, CAT	121.50.168.0 - 121.50.175.255
158.222.70.0/23	AS6137	SISNA - SISNA, Inc.	158.222.48.0 - 158.222.99.255
158.222.72.0/23	AS6137	SISNA - SISNA, Inc.	158.222.48.0 - 158.222.99.255
158.222.224.0/20	AS19864	O1COMM - O1 COMMUNICATIONS	158.222.102.0 - 158.222.255.255
158.222.224.0/22	AS19864	O1COMM - O1 COMMUNICATIONS	158.222.102.0 - 158.222.255.255
158.222.229.0/24	AS19864	O1COMM - O1 COMMUNICATIONS	158.222.102.0 - 158.222.255.255
172.7.0.0/24	AS36992	ETISALAT-MISR	171.207.0.0 - 172.127.255.255
190.102.32.0/20	AS30058	FDCSERVERS - FDCservers.net	190.102.16.0 - 190.102.47.255
192.9.0.0/16	AS11479	BRM-SUN-AS - Sun Microsystems, Inc	192.9.200.0 - 192.9.200.255
192.64.85.0/24	AS1759	TSF-IP-CORE TeliaSonera Finland IP Network	192.64.70.0 - 192.64.87.255
192.69.108.0/24	AS1759	TSF-IP-CORE TeliaSonera Finland IP Network	192.69.102.0 - 192.69.111.255
192.70.164.0/24	AS25689	NRCNET-AS - National Research Council of Canada	192.70.163.0 - 192.70.164.255
192.101.45.0/24	AS2905	TICSA-ASN	192.101.45.0 - 192.101.47.255
192.101.46.0/24	AS6503	Axtel, S.A.B. de C. V.	192.101.45.0 - 192.101.47.255
192.101.64.0/21	AS702	AS702 Verizon Business EMEA - Commercial IP service provider in Europe	192.101.64.0 - 192.101.74.255
192.101.70.0/24	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business	192.101.64.0 - 192.101.74.255
192.101.71.0/24	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business	192.101.64.0 - 192.101.74.255
192.101.72.0/24	AS702	AS702 Verizon Business EMEA - Commercial IP service provider in Europe	192.101.64.0 - 192.101.74.255
192.101.74.0/24	AS1239	SPRINTLINK - Sprint	192.101.64.0 - 192.101.74.255
192.124.248.0/23	AS680	DFN-IP service G-WiN	192.124.249.0 - 192.124.249.255
192.124.252.0/22	AS680	DFN-IP service G-WiN	192.124.255.0 - 192.124.255.255
192.129.127.0/24	AS6568	Ag para el Desarrollo de la Sociedad de la Inf en Bolivia - ADSIB	192.129.111.0 - 192.129.255.255
192.131.233.0/24	AS6389	BELLSOUTH-NET-BLK - BellSouth.net Inc.	192.131.233.0 - 192.131.234.255
192.133.6.0/24	AS10282	ORANGE-BUSINESS-SERVICES-CEEUR Orange Business Services (formerly Equant) AS for CEEUR	192.133.6.0 - 192.133.6.255
192.139.3.0/24	AS23184	PERSONA - PERSONA COMMUNICATIONS INC.	192.139.3.0 - 192.139.3.255
192.145.251.0/24	AS38091	HELLONET-AS-KR C\-CABLENET	192.145.231.0 - 192.146.0.255

and…



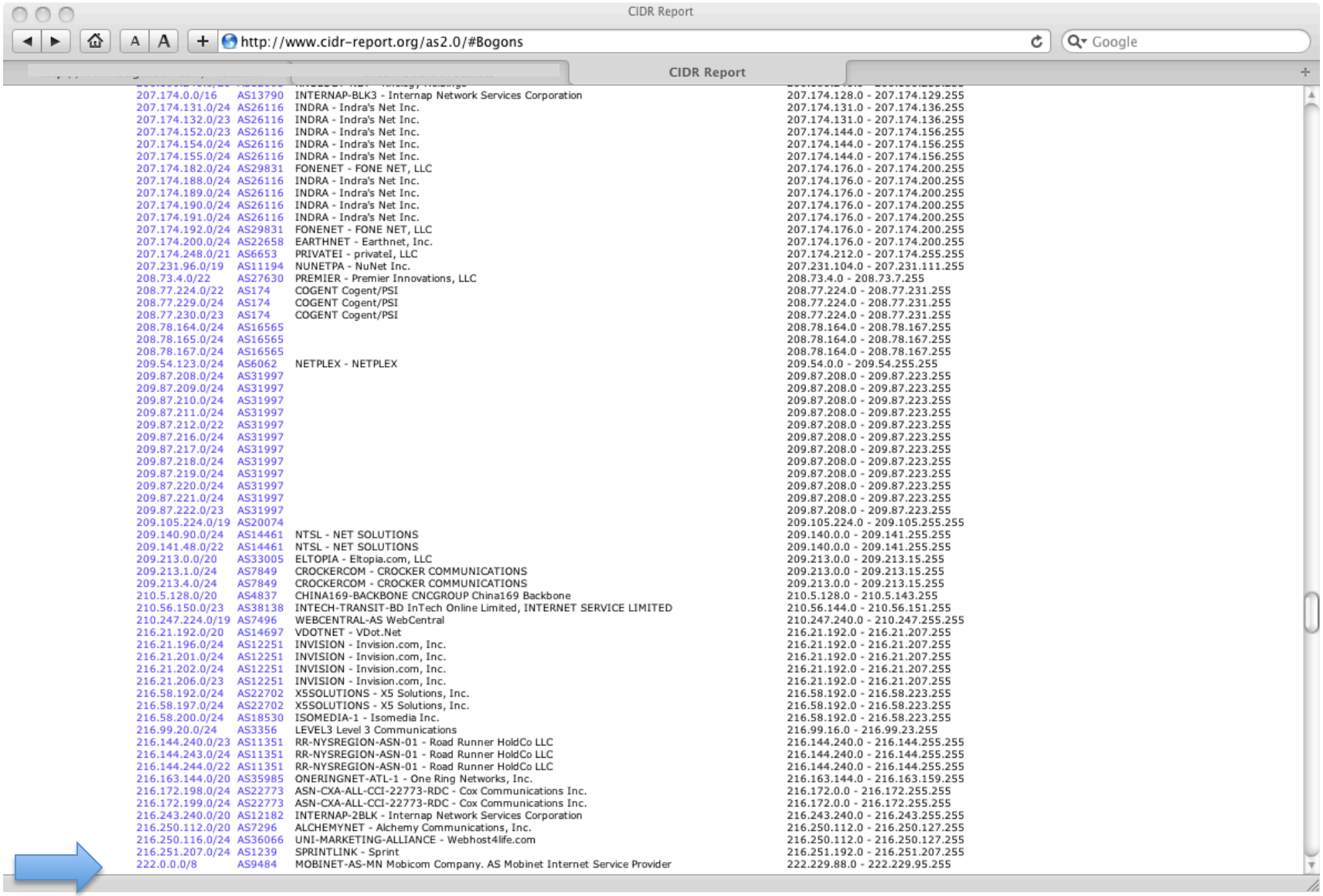
192.145.251.0/24	AS38091	HELLONET-AS-KR CJ-CABLENET	192.145.231.0 - 192.146.0.255
192.153.144.0/21	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	192.153.147.0 - 192.153.147.255
192.154.32.0/19	AS81	NCREN - MCNC	192.154.59.0 - 192.154.59.255
192.154.64.0/19	AS81	NCREN - MCNC	192.154.80.0 - 192.154.80.255
192.188.208.0/20	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	192.188.223.0 - 192.188.223.255
196.2.224.0/22	AS24863	LINKdotNET-AS	196.2.224.0 - 196.2.255.255
196.6.108.0/24	AS5713	SAIX-NET	196.6.103.0 - 196.6.120.255
196.13.201.0/24	AS2018	TENET-1	196.13.201.0 - 196.13.204.255
196.13.202.0/24	AS2018	TENET-1	196.13.201.0 - 196.13.204.255
196.13.203.0/24	AS2018	TENET-1	196.13.201.0 - 196.13.204.255
196.13.204.0/24	AS2018	TENET-1	196.13.201.0 - 196.13.204.255
196.202.224.0/21	AS8818	TELE Greenland Autonomous System	196.202.224.0 - 196.202.231.255
198.1.2.0/24	AS4761	INDOSAT-INP-AP INDOSAT Internet Network Provider	198.0.0.0 - 198.1.7.255
198.23.26.0/24	AS33052	VZUNET - Verizon Data Services LLC	198.23.26.0 - 198.23.31.255
198.73.210.0/24	AS21570	ACI-1 - Accelerated Connections Inc.	198.73.209.0 - 198.73.210.255
198.97.72.0/21	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	198.97.77.0 - 198.97.77.255
198.97.96.0/19	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	198.97.102.0 - 198.97.102.255
198.97.240.0/20	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	198.97.241.0 - 198.97.242.255
198.135.236.0/24	AS4358	XNET - XNet Information Systems, Inc.	198.135.236.0 - 198.135.236.255
198.161.82.0/23	AS15290	ALLST-15290 - Allstream Corp.	198.161.83.0 - 198.161.83.255
198.161.87.0/24	AS6539	GT-BELL - Bell Canada	198.161.87.0 - 198.161.87.255
198.161.92.0/24	AS6539	GT-BELL - Bell Canada	198.161.92.0 - 198.161.92.255
198.163.214.0/24	AS21804	ACCESS-SK - Access Communications Co-operative Limited	198.163.214.0 - 198.163.216.255
198.163.215.0/24	AS6327	SHAW - Shaw Communications Inc.	198.163.214.0 - 198.163.216.255
198.163.216.0/24	AS6327	SHAW - Shaw Communications Inc.	198.163.214.0 - 198.163.216.255
198.167.0.0/16	AS7456	INTERHOP - Interhop Network SERVICES Inc.	198.167.0.0 - 198.167.0.255
198.168.0.0/16	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business	198.167.255.0 - 198.168.0.255
198.169.0.0/16	AS803	SASKTEL - Saskatchewan Telecommunications	198.169.10.0 - 198.169.11.255
198.180.198.0/24	AS23715	SEOUL-INTGW-GXS-AP Global Exchange Services	198.180.198.0 - 198.180.198.255
198.182.235.0/24	AS3356	LEVEL3 Level 3 Communications	198.182.235.0 - 198.182.235.255
199.10.0.0/16	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	199.10.4.0 - 199.10.7.255
199.16.32.0/19	AS6389	BELLSOUTH-NET-BLK - BellSouth.net Inc.	199.16.31.0 - 199.16.63.255
199.26.183.0/24	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business	199.26.183.0 - 199.26.184.255
199.114.128.0/18	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.130.0/24	AS6045	DNIC-ASBLK-05800-06055 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.131.0/24	AS6045	DNIC-ASBLK-05800-06055 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.132.0/24	AS6045	DNIC-ASBLK-05800-06055 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.136.0/24	AS27044	DNIC-ASBLK-27032-27159 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.138.0/24	AS6045	DNIC-ASBLK-05800-06055 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.140.0/24	AS3544	ITSDN-U7 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.142.0/24	AS6045	DNIC-ASBLK-05800-06055 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.144.0/24	AS6045	DNIC-ASBLK-05800-06055 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.148.0/24	AS6045	DNIC-ASBLK-05800-06055 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.150.0/24	AS6045	DNIC-ASBLK-05800-06055 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.152.0/24	AS27033	DNIC-ASBLK-27032-27159 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.153.0/24	AS27034	DNIC-ASBLK-27032-27159 - DoD Network Information Center	199.114.129.0 - 199.114.203.255
199.114.154.0/24	AS1733	CENTAF-SWA - 754th Electronic Systems Group	199.114.129.0 - 199.114.203.255
199.114.156.0/24	AS1733	CENTAF-SWA - 754th Electronic Systems Group	199.114.129.0 - 199.114.203.255
199.114.160.0/24	AS1733	CENTAF-SWA - 754th Electronic Systems Group	199.114.129.0 - 199.114.203.255
199.121.0.0/16	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	199.120.255.0 - 199.121.3.255
199.123.0.0/18	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	199.123.0.0 - 199.123.3.255
199.123.16.0/20	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	199.123.30.0 - 199.123.31.255
199.123.80.0/21	AS27064	DNIC-ASBLK-27032-27159 - DoD Network Information Center	199.123.83.0 - 199.123.83.255
199.185.130.0/23	AS19662	UNISERVE-ONLINE - Uniserve On Line	199.185.130.0 - 199.185.131.255
199.202.0.0/16	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business	199.201.255.0 - 199.202.31.255
199.202.216.0/21	AS577	BACOM - Bell Canada	199.202.216.0 - 199.202.223.255
199.233.92.0/24	AS26896	D102-ITC - Data 102, LLC	199.233.92.0 - 199.233.92.255
199.246.116.0/24	AS813	UUNET-CANADA - MCI Communications Services, Inc. d/b/a Verizon Business	199.246.116.0 - 199.246.116.255
200.1.112.0/24	AS29754	GO2TEL GO2TEL.COM INC.	200.1.112.0 - 200.1.112.255
200.108.176.0/20	AS14551	UUNET-SA - MCI Communications Services, Inc. d/b/a Verizon Business	200.108.144.0 - 200.108.191.255
202.6.176.0/20	AS24316		202.6.176.0 - 202.6.191.255
202.9.55.0/24	AS2764	AAPT AAPT Limited	202.9.51.0 - 202.9.55.255
202.9.57.0/24	AS2764	AAPT AAPT Limited	202.9.57.0 - 202.9.95.255
202.58.113.0/24	AS19161		202.58.112.0 - 202.58.115.255
202.61.72.0/24	AS9425	CONCENTRIX-PH-AS-AP Concentrix Technologies, Inc.	202.61.64.0 - 202.61.127.255

plus…



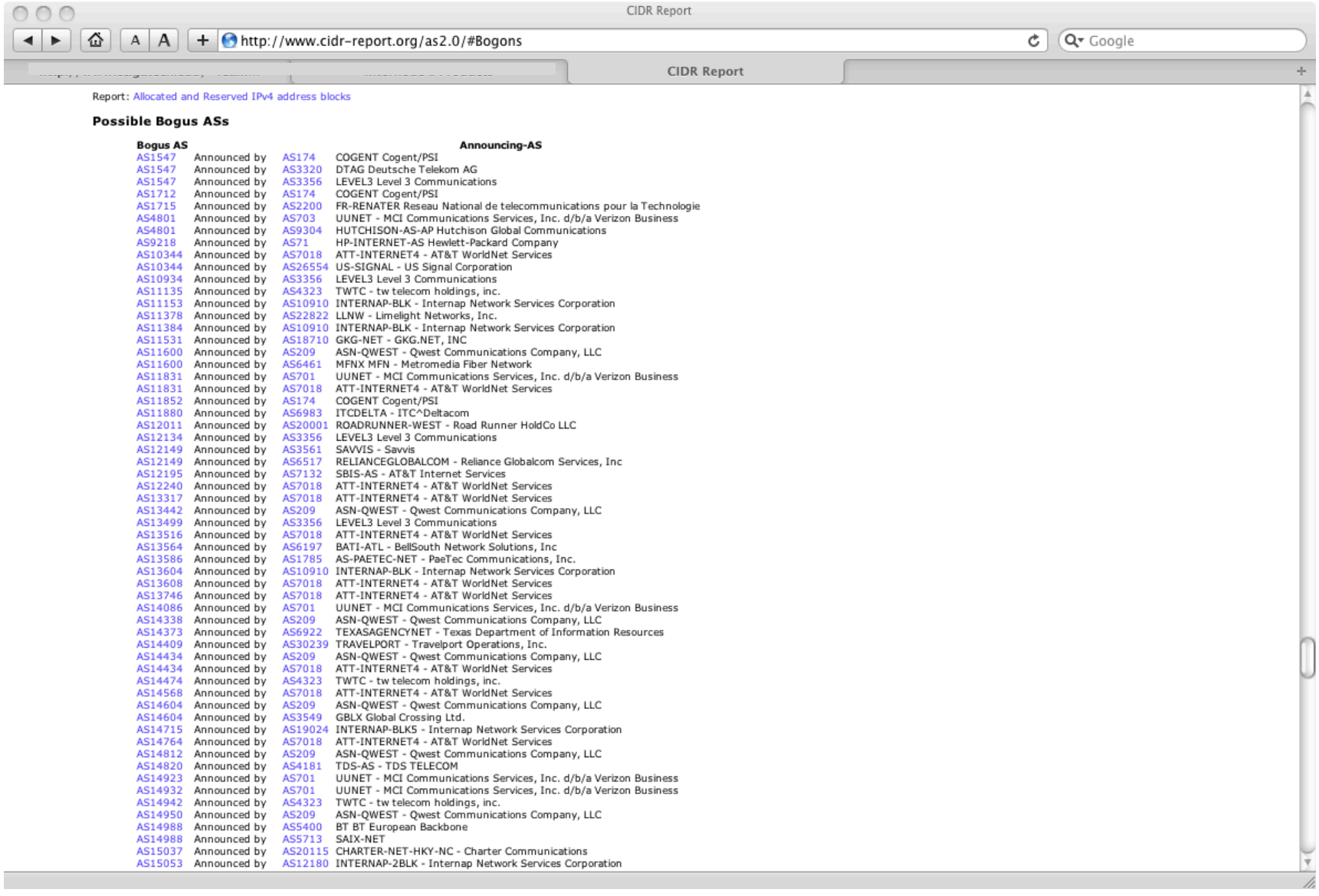
202.58.113.0/24	AS19161		202.58.112.0 - 202.58.115.255
202.61.72.0/24	AS9425	CONCENTRIX-PH-AS-AP Concentrix Technologies, Inc	202.61.64.0 - 202.61.127.255
202.61.73.0/24	AS9425	CONCENTRIX-PH-AS-AP Concentrix Technologies, Inc	202.61.64.0 - 202.61.127.255
202.61.75.0/24	AS9927	PHILCOMNET-PH A Multihomed ISP Company	202.61.64.0 - 202.61.127.255
202.66.128.0/18	AS9584	GENESIS-AP Diyixian.com Limited	202.66.128.0 - 202.66.191.255
202.66.184.0/24	AS9584	GENESIS-AP Diyixian.com Limited	202.66.128.0 - 202.66.191.255
202.66.186.0/24	AS9584	GENESIS-AP Diyixian.com Limited	202.66.128.0 - 202.66.191.255
202.66.188.0/24	AS9584	GENESIS-AP Diyixian.com Limited	202.66.128.0 - 202.66.191.255
202.66.189.0/24	AS9584	GENESIS-AP Diyixian.com Limited	202.66.128.0 - 202.66.191.255
202.66.190.0/24	AS9584	GENESIS-AP Diyixian.com Limited	202.66.128.0 - 202.66.191.255
202.73.144.0/20	AS4788	TMNET-AS-AP TM Net, Internet Service Provider	202.73.144.0 - 202.73.159.255
202.79.224.0/21	AS9519	VERTELNET Vertical Telecoms Pty Ltd	202.79.224.0 - 202.79.231.255
202.80.192.0/20	AS2706	PI-HK Pacnet Internet (Hong Kong) Limited	202.80.196.0 - 202.80.207.255
202.86.252.0/22	AS4748	RESOLINK-AS-AP Resources Link Network Limited	202.86.252.0 - 202.86.255.255
202.86.252.0/24	AS9304	HUTCHISON-AS-AP Hutchison Global Communications	202.86.252.0 - 202.86.255.255
202.86.253.0/24	AS9304	HUTCHISON-AS-AP Hutchison Global Communications	202.86.252.0 - 202.86.255.255
202.86.254.0/24	AS9304	HUTCHISON-AS-AP Hutchison Global Communications	202.86.252.0 - 202.86.255.255
202.86.255.0/24	AS9304	HUTCHISON-AS-AP Hutchison Global Communications	202.86.252.0 - 202.86.255.255
202.87.102.0/24	AS17557	PKTELECOM-AS-PK Pakistan Telecommunication Company Limited	202.87.80.0 - 202.87.127.255
202.94.1.0/24	AS4808	CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network	202.94.0.0 - 202.94.31.255
202.125.113.0/24	AS9541	CYBERNET-AP Cyber Internet Services (Pvt) Ltd.	202.125.80.0 - 202.125.127.255
202.125.114.0/24	AS9541	CYBERNET-AP Cyber Internet Services (Pvt) Ltd.	202.125.80.0 - 202.125.127.255
202.125.115.0/24	AS9541	CYBERNET-AP Cyber Internet Services (Pvt) Ltd.	202.125.80.0 - 202.125.127.255
202.133.37.0/24	AS17557	PKTELECOM-AS-PK Pakistan Telecommunication Company Limited	202.133.32.0 - 202.133.47.255
202.133.70.0/24	AS38616	WORLDCALL-AS-KHI Worldcall Telecom Limited	202.133.64.0 - 202.133.79.255
202.133.73.0/24	AS38616	WORLDCALL-AS-KHI Worldcall Telecom Limited	202.133.64.0 - 202.133.79.255
202.136.254.0/24	AS4808	CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network	202.136.252.0 - 202.136.255.255
202.136.255.0/24	AS4808	CHINA169-BJ CNCGROUP IP network China169 Beijing Province Network	202.136.252.0 - 202.136.255.255
202.143.56.0/21	AS9942	COMINDICO-AP SOUL Converged Communications Australia	202.143.56.0 - 202.143.63.255
202.150.227.0/24	AS17727	NAPINFO-AS-AP PT. NAP Info Lintas Nusa	202.150.224.0 - 202.150.255.255
202.174.70.0/24	AS21175	WIS Wind International Services SA	202.174.64.0 - 202.174.79.255
202.174.125.0/24	AS9498	BBIL-AP BHARTI Airtel Ltd.	202.174.124.0 - 202.174.127.255
202.181.32.0/24	AS4645	ASN-HKNET-AP HKNet Co. Ltd	202.181.32.0 - 202.181.63.255
203.12.45.0/24	AS4854	NETSPACE-AS-AP Netspace Online Systems	203.12.45.0 - 203.12.45.255
203.62.0.0/17	AS7575	AARNET-AS-AP Australian Academic and Reasearch Network (AARNet)	203.62.2.0 - 203.62.2.255
203.78.48.0/20	AS9299	IPG-AS-AP Philippine Long Distance Telephone Company	203.78.48.0 - 203.78.63.255
203.80.136.0/21	AS4759	EVOSERVE-AS-AP EvoServe is a content and online access Internet provider company	203.80.132.0 - 203.80.143.255
203.112.111.0/24	AS7474	OPTUSCOM-AS01-AU SingTel Optus Pty Ltd	203.112.96.0 - 203.112.127.255
203.112.113.0/24	AS7474	OPTUSCOM-AS01-AU SingTel Optus Pty Ltd	203.112.96.0 - 203.112.127.255
203.112.114.0/24	AS4802	ASN-IINET iiNet Limited	203.112.96.0 - 203.112.127.255
203.112.116.0/24	AS7474	OPTUSCOM-AS01-AU SingTel Optus Pty Ltd	203.112.96.0 - 203.112.127.255
203.112.117.0/24	AS7474	OPTUSCOM-AS01-AU SingTel Optus Pty Ltd	203.112.96.0 - 203.112.127.255
203.112.118.0/24	AS7474	OPTUSCOM-AS01-AU SingTel Optus Pty Ltd	203.112.96.0 - 203.112.127.255
203.112.119.0/24	AS7474	OPTUSCOM-AS01-AU SingTel Optus Pty Ltd	203.112.96.0 - 203.112.127.255
203.112.120.0/24	AS7474	OPTUSCOM-AS01-AU SingTel Optus Pty Ltd	203.112.96.0 - 203.112.127.255
203.112.121.0/24	AS7474	OPTUSCOM-AS01-AU SingTel Optus Pty Ltd	203.112.96.0 - 203.112.127.255
203.112.127.0/24	AS7474	OPTUSCOM-AS01-AU SingTel Optus Pty Ltd	203.112.96.0 - 203.112.127.255
203.128.128.0/24	AS23849	CNNIC-NET263-AP Beijing Capital-online science development Co.,Ltd.	203.128.128.0 - 203.128.159.255
203.142.219.0/24	AS45149		203.142.219.0 - 203.142.219.255
203.189.96.0/20	AS17557	PKTELECOM-AS-PK Pakistan Telecommunication Company Limited	203.189.96.0 - 203.189.111.255
204.9.216.0/23	AS6389	BELLSOUTH-NET-BLK - BellSouth.net Inc.	204.9.216.0 - 204.9.219.255
204.9.218.0/23	AS6389	BELLSOUTH-NET-BLK - BellSouth.net Inc.	204.9.216.0 - 204.9.219.255
204.15.168.0/21	AS46753	TDAMERITRADETRUST - TD Ameritrade Trust	204.15.168.0 - 204.15.175.255
204.15.170.0/24	AS46753	TDAMERITRADETRUST - TD Ameritrade Trust	204.15.168.0 - 204.15.175.255
204.19.14.0/23	AS577	BACOM - Bell Canada	204.19.15.0 - 204.19.15.255
204.89.214.0/24	AS4323	TWTC - tw telecom holdings, inc.	204.89.214.0 - 204.89.214.255
204.197.0.0/16	AS3356	LEVEL3 Level 3 Communications	204.197.128.0 - 204.197.255.255
204.209.114.0/24	AS13768	PEER1 - Peer 1 Network Inc.	204.209.114.0 - 204.209.114.255
205.150.0.0/15	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business	205.151.0.0 - 205.151.0.255
205.189.134.0/24	AS11814	CYBERSURF - Cybersurf Inc.	205.189.134.0 - 205.189.134.255
205.210.145.0/24	AS11814	CYBERSURF - Cybersurf Inc.	205.210.145.0 - 205.210.145.255
206.108.96.0/19	AS577	BACOM - Bell Canada	206.108.114.0 - 206.108.115.255
206.128.104.0/21	AS11709	VIC - VIRTUAL INTERACTIVE CENTER	206.128.96.0 - 206.128.111.255
206.180.240.0/20	AS12083	KNOLOGY-NET - Knology Holdings	206.180.240.0 - 206.180.255.255

yes, there's more



207.174.0.0/16	AS13790	INTERNAP-BLK3 - Internap Network Services Corporation	207.174.128.0 - 207.174.129.255
207.174.131.0/24	AS26116	INDRA - Indra's Net Inc.	207.174.131.0 - 207.174.136.255
207.174.132.0/23	AS26116	INDRA - Indra's Net Inc.	207.174.131.0 - 207.174.136.255
207.174.152.0/23	AS26116	INDRA - Indra's Net Inc.	207.174.144.0 - 207.174.156.255
207.174.154.0/24	AS26116	INDRA - Indra's Net Inc.	207.174.144.0 - 207.174.156.255
207.174.155.0/24	AS26116	INDRA - Indra's Net Inc.	207.174.144.0 - 207.174.156.255
207.174.182.0/24	AS29831	FONENET - FONE NET, LLC	207.174.176.0 - 207.174.200.255
207.174.188.0/24	AS26116	INDRA - Indra's Net Inc.	207.174.176.0 - 207.174.200.255
207.174.189.0/24	AS26116	INDRA - Indra's Net Inc.	207.174.176.0 - 207.174.200.255
207.174.190.0/24	AS26116	INDRA - Indra's Net Inc.	207.174.176.0 - 207.174.200.255
207.174.191.0/24	AS26116	INDRA - Indra's Net Inc.	207.174.176.0 - 207.174.200.255
207.174.192.0/24	AS29831	FONENET - FONE NET, LLC	207.174.176.0 - 207.174.200.255
207.174.200.0/24	AS22658	EARTHNET - Earthnet, Inc.	207.174.176.0 - 207.174.200.255
207.174.248.0/21	AS6653	PRIVATEI - privateI, LLC	207.174.212.0 - 207.174.255.255
207.231.96.0/19	AS11194	NUNETPA - NuNet Inc.	207.231.104.0 - 207.231.111.255
208.73.4.0/22	AS27630	PREMIER - Premier Innovations, LLC	208.73.4.0 - 208.73.7.255
208.77.224.0/22	AS174	COGENT Cogent/PSI	208.77.224.0 - 208.77.231.255
208.77.229.0/24	AS174	COGENT Cogent/PSI	208.77.224.0 - 208.77.231.255
208.77.230.0/23	AS174	COGENT Cogent/PSI	208.77.224.0 - 208.77.231.255
208.78.164.0/24	AS16565		208.78.164.0 - 208.78.167.255
208.78.165.0/24	AS16565		208.78.164.0 - 208.78.167.255
208.78.167.0/24	AS16565		208.78.164.0 - 208.78.167.255
209.54.123.0/24	AS6062	NETPLEX - NETPLEX	209.54.0.0 - 209.54.255.255
209.87.208.0/24	AS31997		209.87.208.0 - 209.87.223.255
209.87.209.0/24	AS31997		209.87.208.0 - 209.87.223.255
209.87.210.0/24	AS31997		209.87.208.0 - 209.87.223.255
209.87.211.0/24	AS31997		209.87.208.0 - 209.87.223.255
209.87.212.0/22	AS31997		209.87.208.0 - 209.87.223.255
209.87.216.0/24	AS31997		209.87.208.0 - 209.87.223.255
209.87.217.0/24	AS31997		209.87.208.0 - 209.87.223.255
209.87.218.0/24	AS31997		209.87.208.0 - 209.87.223.255
209.87.219.0/24	AS31997		209.87.208.0 - 209.87.223.255
209.87.220.0/24	AS31997		209.87.208.0 - 209.87.223.255
209.87.221.0/24	AS31997		209.87.208.0 - 209.87.223.255
209.87.222.0/23	AS31997		209.87.208.0 - 209.87.223.255
209.105.224.0/19	AS20074		209.105.224.0 - 209.105.255.255
209.140.90.0/24	AS14461	NTSL - NET SOLUTIONS	209.140.0.0 - 209.141.255.255
209.141.48.0/22	AS14461	NTSL - NET SOLUTIONS	209.140.0.0 - 209.141.255.255
209.213.0.0/20	AS33005	ELTOPIA - Eltopia.com, LLC	209.213.0.0 - 209.213.15.255
209.213.1.0/24	AS7849	CROCKERCOM - CROCKER COMMUNICATIONS	209.213.0.0 - 209.213.15.255
209.213.4.0/24	AS7849	CROCKERCOM - CROCKER COMMUNICATIONS	209.213.0.0 - 209.213.15.255
210.5.128.0/20	AS4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	210.5.128.0 - 210.5.143.255
210.56.150.0/23	AS38138	INTECH-TRANSIT-BD InTech Online Limited, INTERNET SERVICE LIMITED	210.56.144.0 - 210.56.151.255
210.247.224.0/19	AS7496	WEBCENTRAL-AS WebCentral	210.247.240.0 - 210.247.255.255
216.21.192.0/20	AS14697	VDOTNET - VDot.Net	216.21.192.0 - 216.21.207.255
216.21.196.0/24	AS12251	INVISION - Invision.com, Inc.	216.21.192.0 - 216.21.207.255
216.21.201.0/24	AS12251	INVISION - Invision.com, Inc.	216.21.192.0 - 216.21.207.255
216.21.202.0/24	AS12251	INVISION - Invision.com, Inc.	216.21.192.0 - 216.21.207.255
216.21.206.0/23	AS12251	INVISION - Invision.com, Inc.	216.21.192.0 - 216.21.207.255
216.58.192.0/24	AS22702	X5SOLUTIONS - X5 Solutions, Inc.	216.58.192.0 - 216.58.223.255
216.58.197.0/24	AS22702	X5SOLUTIONS - X5 Solutions, Inc.	216.58.192.0 - 216.58.223.255
216.58.200.0/24	AS18530	ISOMEDIA-1 - Isomedia Inc.	216.58.192.0 - 216.58.223.255
216.99.20.0/24	AS3356	LEVEL3 Level 3 Communications	216.99.16.0 - 216.99.23.255
216.144.240.0/23	AS11351	RR-NYSREGION-ASN-01 - Road Runner HoldCo LLC	216.144.240.0 - 216.144.255.255
216.144.243.0/24	AS11351	RR-NYSREGION-ASN-01 - Road Runner HoldCo LLC	216.144.240.0 - 216.144.255.255
216.144.244.0/22	AS11351	RR-NYSREGION-ASN-01 - Road Runner HoldCo LLC	216.144.240.0 - 216.144.255.255
216.163.144.0/20	AS35985	ONERINGNET-ATL-1 - One Ring Networks, Inc.	216.163.144.0 - 216.163.159.255
216.172.198.0/24	AS22773	ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc.	216.172.0.0 - 216.172.255.255
216.172.199.0/24	AS22773	ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc.	216.172.0.0 - 216.172.255.255
216.243.240.0/20	AS12182	INTERNAP-2BLK - Internap Network Services Corporation	216.243.240.0 - 216.243.255.255
216.250.112.0/20	AS7296	ALCHEMYNET - Alchemy Communications, Inc.	216.250.112.0 - 216.250.127.255
216.250.116.0/24	AS36066	UNI-MARKETING-ALLIANCE - Webhost4life.com	216.250.112.0 - 216.250.127.255
216.251.207.0/24	AS1239	SPRINTLINK - Sprint	216.251.192.0 - 216.251.207.255
222.0.0.0/8	AS9484	MOBINET-AS-MN Mobicom Company. AS Mobinet Internet Service Provider	222.229.88.0 - 222.229.95.255

getting the point yet?

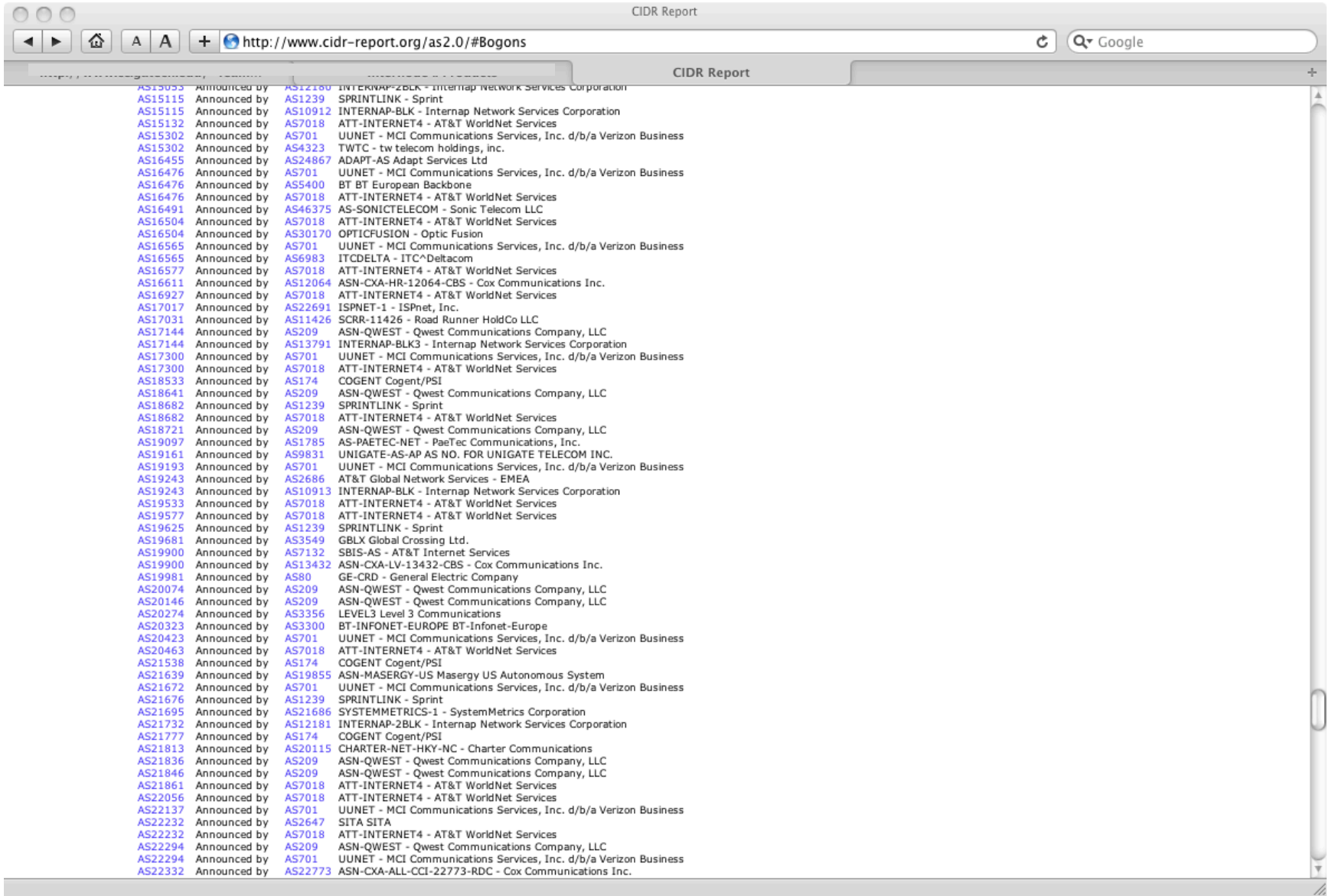


Report: Allocated and Reserved IPv4 address blocks

Possible Bogus ASs

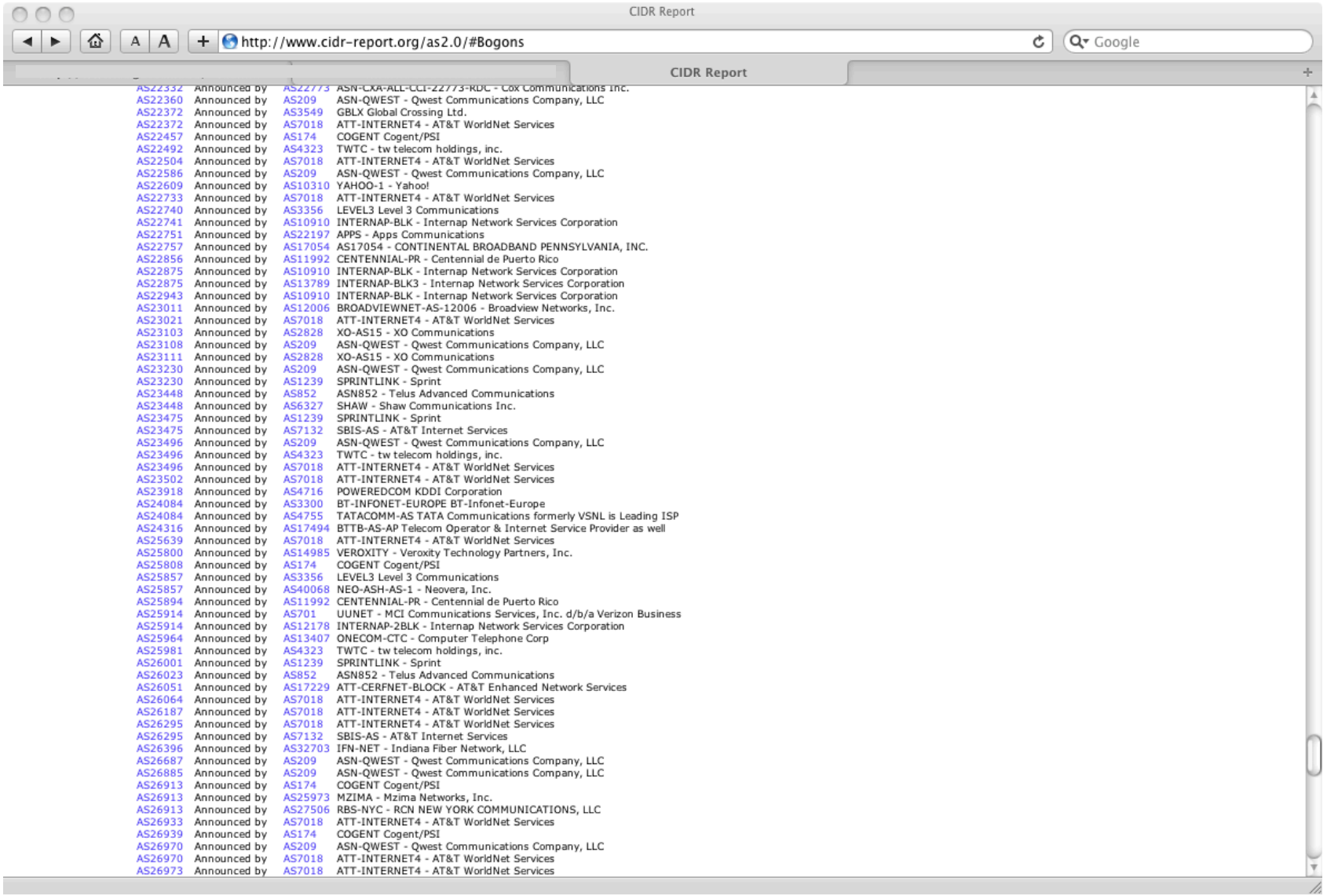
Bogus AS		Announcing-AS	
AS1547	Announced by	AS174	COGENT Cogent/PSI
AS1547	Announced by	AS3320	DTAG Deutsche Telekom AG
AS1547	Announced by	AS3356	LEVEL3 Level 3 Communications
AS1712	Announced by	AS174	COGENT Cogent/PSI
AS1715	Announced by	AS2200	FR-RENATER Reseau National de telecommunications pour la Technologie
AS4801	Announced by	AS703	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS4801	Announced by	AS9304	HUTCHISON-AS-AP Hutchison Global Communications
AS9218	Announced by	AS71	HP-INTERNET-AS Hewlett-Packard Company
AS10344	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS10344	Announced by	AS26554	US-SIGNAL - US Signal Corporation
AS10934	Announced by	AS3356	LEVEL3 Level 3 Communications
AS11135	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS11153	Announced by	AS10910	INTERNAP-BLK - Internap Network Services Corporation
AS11378	Announced by	AS22822	LLNW - Limelight Networks, Inc.
AS11384	Announced by	AS10910	INTERNAP-BLK - Internap Network Services Corporation
AS11531	Announced by	AS18710	GKG-NET - GKG.NET, INC
AS11600	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS11600	Announced by	AS6461	MFNX MFN - Metromedia Fiber Network
AS11831	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS11831	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS11852	Announced by	AS174	COGENT Cogent/PSI
AS11880	Announced by	AS6983	ITCDELTA - ITC^Deltacom
AS12011	Announced by	AS20001	ROADRUNNER-WEST - Road Runner HoldCo LLC
AS12134	Announced by	AS3356	LEVEL3 Level 3 Communications
AS12149	Announced by	AS3561	SAVVIS - Savvis
AS12149	Announced by	AS6517	RELIANCEGLOBALCOM - Reliance Globalcom Services, Inc
AS12195	Announced by	AS7132	SBIS-AS - AT&T Internet Services
AS12240	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS13317	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS13442	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS13499	Announced by	AS3356	LEVEL3 Level 3 Communications
AS13516	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS13564	Announced by	AS6197	BATI-ATL - BellSouth Network Solutions, Inc
AS13586	Announced by	AS1785	AS-PAETEC-NET - PaeTec Communications, Inc.
AS13604	Announced by	AS10910	INTERNAP-BLK - Internap Network Services Corporation
AS13608	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS13746	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS14086	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS14338	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS14373	Announced by	AS6922	TEXASAGENCYNET - Texas Department of Information Resources
AS14409	Announced by	AS30239	TRAVELPORT - Travelport Operations, Inc.
AS14434	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS14434	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS14474	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS14568	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS14604	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS14604	Announced by	AS3549	GBLX Global Crossing Ltd.
AS14715	Announced by	AS19024	INTERNAP-BLK5 - Internap Network Services Corporation
AS14764	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS14812	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS14820	Announced by	AS4181	TDS-AS - TDS TELECOM
AS14923	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS14932	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS14942	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS14950	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS14988	Announced by	AS5400	BT BT European Backbone
AS14988	Announced by	AS5713	SAIX-NET
AS15037	Announced by	AS20115	CHARTER-NET-HKY-NC - Charter Communications
AS15053	Announced by	AS12180	INTERNAP-2BLK - Internap Network Services Corporation

still more!



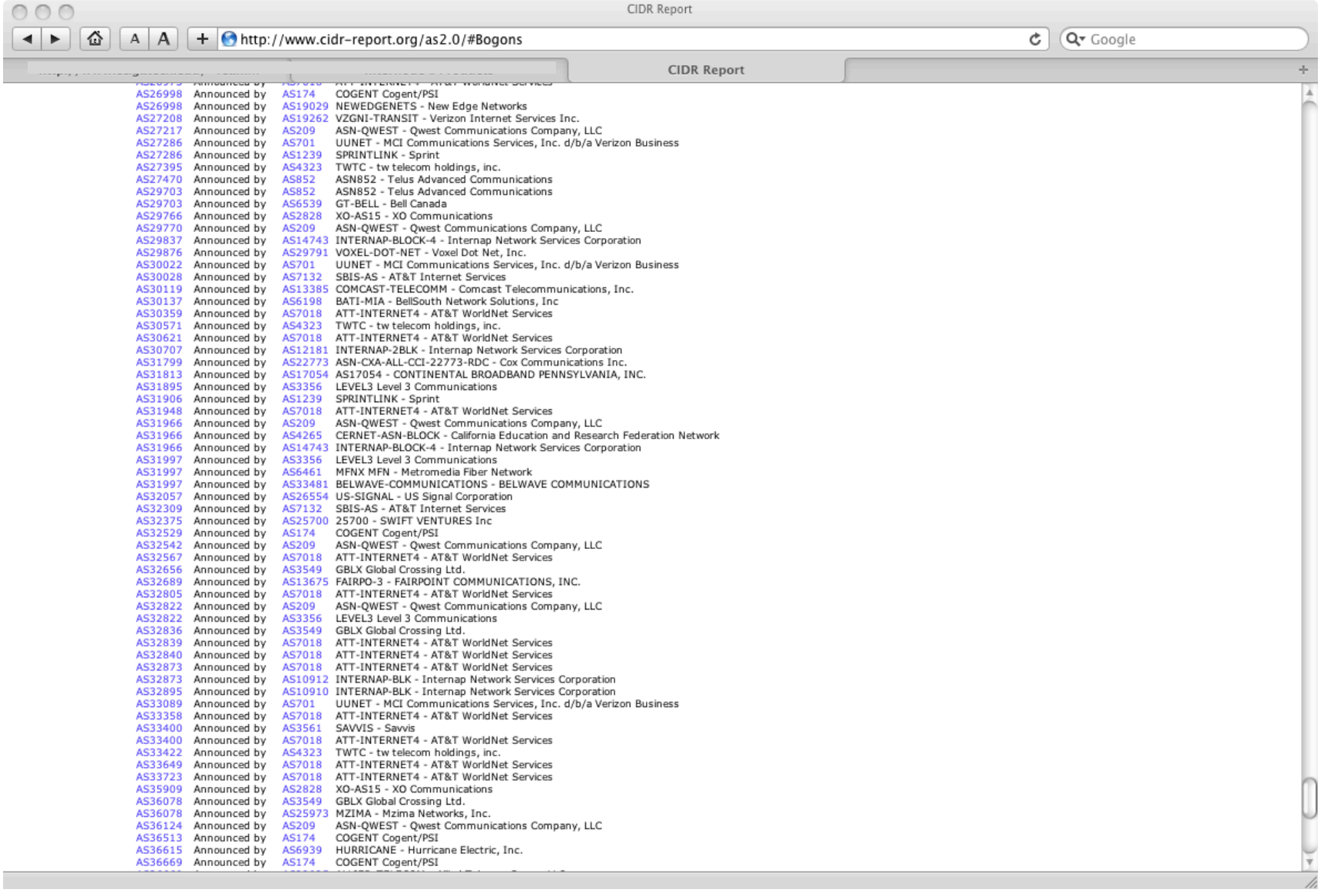
AS15115	Announced by	AS1239	SPRINTLINK - Sprint
AS15115	Announced by	AS10912	INTERNAP-BLK - Internap Network Services Corporation
AS15132	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS15302	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS15302	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS16455	Announced by	AS24867	ADAPT-AS Adapt Services Ltd
AS16476	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS16476	Announced by	AS5400	BT BT European Backbone
AS16476	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS16491	Announced by	AS46375	AS-SONICTELECOM - Sonic Telecom LLC
AS16504	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS16504	Announced by	AS30170	OPTICFUSION - Optic Fusion
AS16565	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS16565	Announced by	AS6983	ITCDELTA - ITC^Deltacom
AS16577	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS16611	Announced by	AS12064	ASN-CXA-HR-12064-CBS - Cox Communications Inc.
AS16927	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS17017	Announced by	AS22691	ISPNET-1 - ISPnet, Inc.
AS17031	Announced by	AS11426	SCRR-11426 - Road Runner HoldCo LLC
AS17144	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS17144	Announced by	AS13791	INTERNAP-BLK3 - Internap Network Services Corporation
AS17300	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS17300	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS18533	Announced by	AS174	COGENT Cogent/PSI
AS18641	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS18682	Announced by	AS1239	SPRINTLINK - Sprint
AS18682	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS18721	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS19097	Announced by	AS1785	AS-PAETEC-NET - PaeTec Communications, Inc.
AS19161	Announced by	AS9831	UNIGATE-AS-AP AS NO. FOR UNIGATE TELECOM INC.
AS19193	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS19243	Announced by	AS2686	AT&T Global Network Services - EMEA
AS19243	Announced by	AS10913	INTERNAP-BLK - Internap Network Services Corporation
AS19533	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS19577	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS19625	Announced by	AS1239	SPRINTLINK - Sprint
AS19681	Announced by	AS3549	GBLX Global Crossing Ltd.
AS19900	Announced by	AS7132	SBIS-AS - AT&T Internet Services
AS19900	Announced by	AS13432	ASN-CXA-LV-13432-CBS - Cox Communications Inc.
AS19981	Announced by	AS80	GE-CRD - General Electric Company
AS20074	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS20146	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS20274	Announced by	AS3356	LEVEL3 Level 3 Communications
AS20323	Announced by	AS3300	BT-INFONET-EUROPE BT-Infonet-Europe
AS20423	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS20463	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS21538	Announced by	AS174	COGENT Cogent/PSI
AS21639	Announced by	AS19855	ASN-MASERGY-US Masergy US Autonomous System
AS21672	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS21676	Announced by	AS1239	SPRINTLINK - Sprint
AS21695	Announced by	AS21686	SYSTEMMETRICS-1 - SystemMetrics Corporation
AS21732	Announced by	AS12181	INTERNAP-2BLK - Internap Network Services Corporation
AS21777	Announced by	AS174	COGENT Cogent/PSI
AS21813	Announced by	AS20115	CHARTER-NET-HKY-NC - Charter Communications
AS21836	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS21846	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS21861	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS22056	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS22137	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS22232	Announced by	AS2647	SITA SITA
AS22232	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS22294	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS22294	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS22332	Announced by	AS22773	ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc.

wake me up when we're done



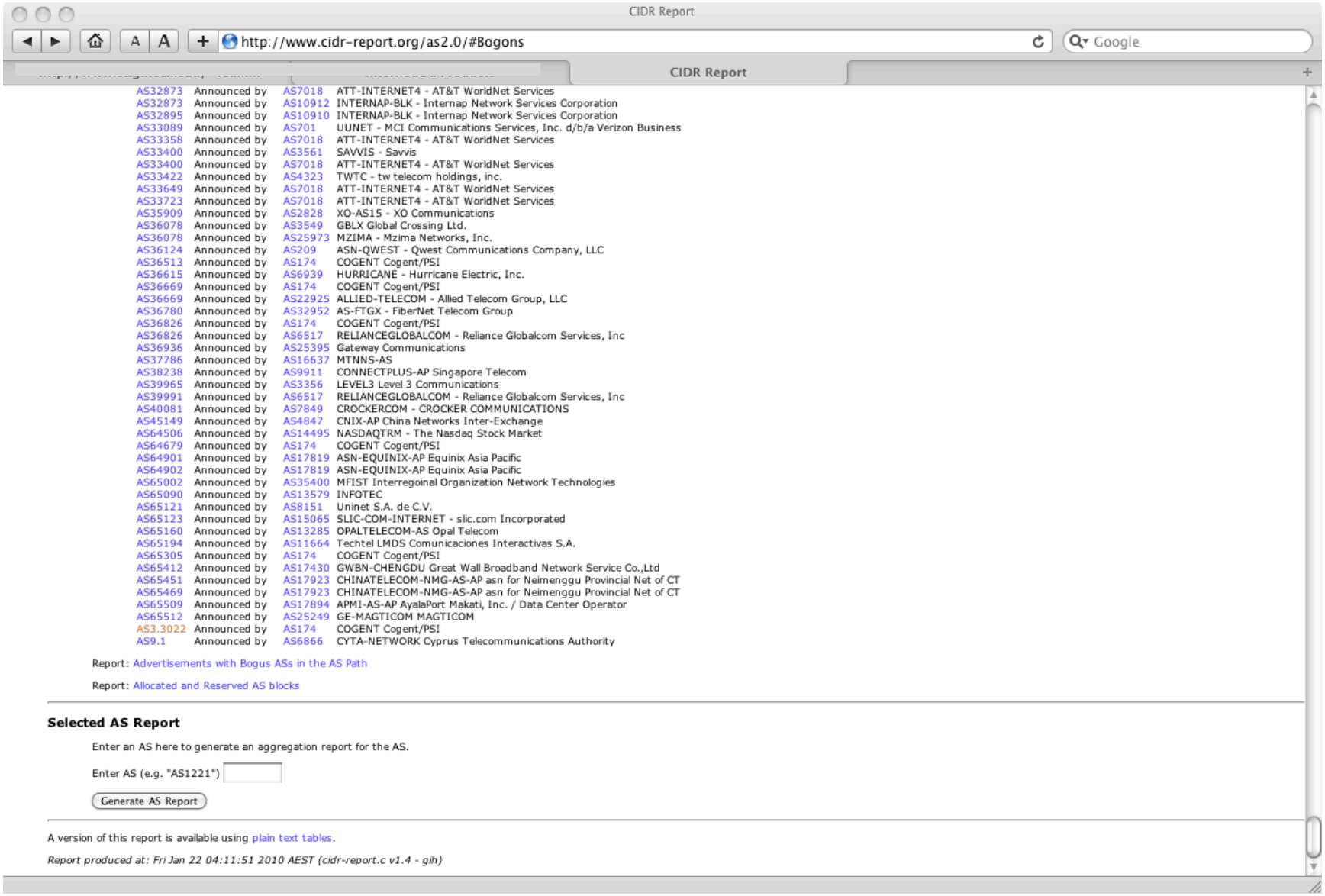
AS22332	Announced by	AS22773	ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc.
AS22360	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS22372	Announced by	AS3549	GBLX Global Crossing Ltd.
AS22372	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS22457	Announced by	AS174	COGENT Cogent/PSI
AS22492	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS22504	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS22586	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS22609	Announced by	AS10310	YAHOO-1 - Yahoo!
AS22733	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS22740	Announced by	AS3356	LEVEL3 Level 3 Communications
AS22741	Announced by	AS10910	INTERNAP-BLK - Internap Network Services Corporation
AS22751	Announced by	AS22197	APPS - Apps Communications
AS22757	Announced by	AS17054	AS17054 - CONTINENTAL BROADBAND PENNSYLVANIA, INC.
AS22856	Announced by	AS11992	CENTENNIAL-PR - Centennial de Puerto Rico
AS22875	Announced by	AS10910	INTERNAP-BLK - Internap Network Services Corporation
AS22875	Announced by	AS13789	INTERNAP-BLK3 - Internap Network Services Corporation
AS22943	Announced by	AS10910	INTERNAP-BLK - Internap Network Services Corporation
AS23011	Announced by	AS12006	BROADVIEWNET-AS-12006 - Broadview Networks, Inc.
AS23021	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS23103	Announced by	AS2828	XO-AS15 - XO Communications
AS23108	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS23111	Announced by	AS2828	XO-AS15 - XO Communications
AS23230	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS23230	Announced by	AS1239	SPRINTLINK - Sprint
AS23448	Announced by	AS852	ASN852 - Telus Advanced Communications
AS23448	Announced by	AS6327	SHAW - Shaw Communications Inc.
AS23475	Announced by	AS1239	SPRINTLINK - Sprint
AS23475	Announced by	AS7132	SBIS-AS - AT&T Internet Services
AS23496	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS23496	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS23496	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS23502	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS23918	Announced by	AS4716	POWEREDCOM KDDI Corporation
AS24084	Announced by	AS3300	BT-INFONET-EUROPE BT-Infonet-Europe
AS24084	Announced by	AS4755	TATACOMM-AS TATA Communications formerly VSNL is Leading ISP
AS24316	Announced by	AS17494	BTTB-AS-AP Telecom Operator & Internet Service Provider as well
AS25639	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS25800	Announced by	AS14985	VEROXITY - Veroxity Technology Partners, Inc.
AS25808	Announced by	AS174	COGENT Cogent/PSI
AS25857	Announced by	AS3356	LEVEL3 Level 3 Communications
AS25857	Announced by	AS40068	NEO-ASH-AS-1 - Neovera, Inc.
AS25894	Announced by	AS11992	CENTENNIAL-PR - Centennial de Puerto Rico
AS25914	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS25914	Announced by	AS12178	INTERNAP-2BLK - Internap Network Services Corporation
AS25964	Announced by	AS13407	ONECOM-CTC - Computer Telephone Corp
AS25981	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS26001	Announced by	AS1239	SPRINTLINK - Sprint
AS26023	Announced by	AS852	ASN852 - Telus Advanced Communications
AS26051	Announced by	AS17229	ATT-CERFNET-BLOCK - AT&T Enhanced Network Services
AS26064	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS26187	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS26295	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS26295	Announced by	AS7132	SBIS-AS - AT&T Internet Services
AS26396	Announced by	AS32703	IFN-NET - Indiana Fiber Network, LLC
AS26687	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS26885	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS26913	Announced by	AS174	COGENT Cogent/PSI
AS26913	Announced by	AS25973	MZIMA - Mzima Networks, Inc.
AS26913	Announced by	AS27506	RBS-NYC - RCN NEW YORK COMMUNICATIONS, LLC
AS26933	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS26939	Announced by	AS174	COGENT Cogent/PSI
AS26970	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS26970	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS26973	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services

ZZZZZZZ



AS26998	Announced by	AS174	COGENT Cogent/PSI
AS26998	Announced by	AS19029	NEWEDGENETS - New Edge Networks
AS27208	Announced by	AS19262	VZGNI-TRANSIT - Verizon Internet Services Inc.
AS27217	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS27286	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS27286	Announced by	AS1239	SPRINTLINK - Sprint
AS27395	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS27470	Announced by	AS852	ASN852 - Telus Advanced Communications
AS29703	Announced by	AS852	ASN852 - Telus Advanced Communications
AS29703	Announced by	AS6539	GT-BELL - Bell Canada
AS29766	Announced by	AS2828	XO-AS15 - XO Communications
AS29770	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS29837	Announced by	AS14743	INTERNAP-BLOCK-4 - Internap Network Services Corporation
AS29876	Announced by	AS29791	VOXEL-DOT-NET - Voxel Dot Net, Inc.
AS30022	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS30028	Announced by	AS7132	SBIS-AS - AT&T Internet Services
AS30119	Announced by	AS13385	COMCAST-TELECOMM - Comcast Telecommunications, Inc.
AS30137	Announced by	AS6198	BATI-MIA - BellSouth Network Solutions, Inc
AS30359	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS30571	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS30621	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS30707	Announced by	AS12181	INTERNAP-2BLK - Internap Network Services Corporation
AS31799	Announced by	AS22773	ASN-CXA-ALL-CCI-22773-RDC - Cox Communications Inc.
AS31813	Announced by	AS17054	AS17054 - CONTINENTAL BROADBAND PENNSYLVANIA, INC.
AS31895	Announced by	AS3356	LEVEL3 Level 3 Communications
AS31906	Announced by	AS1239	SPRINTLINK - Sprint
AS31948	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS31966	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS31966	Announced by	AS4265	CERNET-ASN-BLOCK - California Education and Research Federation Network
AS31966	Announced by	AS14743	INTERNAP-BLOCK-4 - Internap Network Services Corporation
AS31997	Announced by	AS3356	LEVEL3 Level 3 Communications
AS31997	Announced by	AS6461	MFNX MFN - Metromedia Fiber Network
AS31997	Announced by	AS33481	BELWAVE-COMMUNICATIONS - BELWAVE COMMUNICATIONS
AS32057	Announced by	AS26554	US-SIGNAL - US Signal Corporation
AS32309	Announced by	AS7132	SBIS-AS - AT&T Internet Services
AS32375	Announced by	AS25700	25700 - SWIFT VENTURES Inc
AS32529	Announced by	AS174	COGENT Cogent/PSI
AS32542	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS32567	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS32656	Announced by	AS3549	GBLX Global Crossing Ltd.
AS32689	Announced by	AS13675	FAIRPO-3 - FAIRPOINT COMMUNICATIONS, INC.
AS32805	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS32822	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS32822	Announced by	AS3356	LEVEL3 Level 3 Communications
AS32836	Announced by	AS3549	GBLX Global Crossing Ltd.
AS32839	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS32840	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS32873	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS32873	Announced by	AS10912	INTERNAP-BLK - Internap Network Services Corporation
AS32895	Announced by	AS10910	INTERNAP-BLK - Internap Network Services Corporation
AS33089	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS33358	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS33400	Announced by	AS3561	SAVVIS - Savvis
AS33400	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS33422	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS33649	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS33723	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS35909	Announced by	AS2828	XO-AS15 - XO Communications
AS36078	Announced by	AS3549	GBLX Global Crossing Ltd.
AS36078	Announced by	AS25973	MZIMA - Mzima Networks, Inc.
AS36124	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS36513	Announced by	AS174	COGENT Cogent/PSI
AS36615	Announced by	AS6939	HURRICANE - Hurricane Electric, Inc.
AS36669	Announced by	AS174	COGENT Cogent/PSI

almost done…



AS32873	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS32873	Announced by	AS10912	INTERNAP-BLK - Internap Network Services Corporation
AS32895	Announced by	AS10910	INTERNAP-BLK - Internap Network Services Corporation
AS33089	Announced by	AS701	UUNET - MCI Communications Services, Inc. d/b/a Verizon Business
AS33358	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS33400	Announced by	AS3561	SAVVIS - Savvis
AS33400	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS33422	Announced by	AS4323	TWTC - tw telecom holdings, inc.
AS33649	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS33723	Announced by	AS7018	ATT-INTERNET4 - AT&T WorldNet Services
AS35909	Announced by	AS2828	XO-AS15 - XO Communications
AS36078	Announced by	AS3549	GBLX Global Crossing Ltd.
AS36078	Announced by	AS25973	MZIMA - Mzima Networks, Inc.
AS36124	Announced by	AS209	ASN-QWEST - Qwest Communications Company, LLC
AS36513	Announced by	AS174	COGENT Cogent/PSI
AS36615	Announced by	AS6939	HURRICANE - Hurricane Electric, Inc.
AS36669	Announced by	AS174	COGENT Cogent/PSI
AS36669	Announced by	AS22925	ALLIED-TELECOM - Allied Telecom Group, LLC
AS36780	Announced by	AS32952	AS-FTGX - FiberNet Telecom Group
AS36826	Announced by	AS174	COGENT Cogent/PSI
AS36826	Announced by	AS6517	RELIANCEGLOBALCOM - Reliance Globalcom Services, Inc
AS36936	Announced by	AS25395	Gateway Communications
AS37786	Announced by	AS16637	MTNNS-AS
AS38238	Announced by	AS9911	CONNECTPLUS-AP Singapore Telecom
AS39965	Announced by	AS3356	LEVEL3 Level 3 Communications
AS39991	Announced by	AS6517	RELIANCEGLOBALCOM - Reliance Globalcom Services, Inc
AS40081	Announced by	AS7849	CROCKERCOM - CROCKER COMMUNICATIONS
AS45149	Announced by	AS4847	CNIX-AP China Networks Inter-Exchange
AS64506	Announced by	AS14495	NASDAQTRM - The Nasdaq Stock Market
AS64679	Announced by	AS174	COGENT Cogent/PSI
AS64901	Announced by	AS17819	ASN-EQUINIX-AP Equinix Asia Pacific
AS64902	Announced by	AS17819	ASN-EQUINIX-AP Equinix Asia Pacific
AS65002	Announced by	AS35400	MFIST Interregoinal Organization Network Technologies
AS65090	Announced by	AS13579	INFOTEC
AS65121	Announced by	AS8151	Uninet S.A. de C.V.
AS65123	Announced by	AS15065	SLIC-COM-INTERNET - slic.com Incorporated
AS65160	Announced by	AS13285	OPALTELECOM-AS Opal Telecom
AS65194	Announced by	AS11664	Techtel LMDS Comunicaciones Interactivas S.A.
AS65305	Announced by	AS174	COGENT Cogent/PSI
AS65412	Announced by	AS17430	GWBN-CHENGDU Great Wall Broadband Network Service Co.,Ltd
AS65451	Announced by	AS17923	CHINATELECOM-NMG-AS-AP asn for Neimenggu Provincial Net of CT
AS65469	Announced by	AS17923	CHINATELECOM-NMG-AS-AP asn for Neimenggu Provincial Net of CT
AS65509	Announced by	AS17894	APMI-AS-AP AyalaPort Makati, Inc. / Data Center Operator
AS65512	Announced by	AS25249	GE-MAGTICOM MAGTICOM
AS3.3022	Announced by	AS174	COGENT Cogent/PSI
AS9.1	Announced by	AS6866	CYTA-NETWORK Cyprus Telecommunications Authority

Report: Advertisements with Bogus ASs in the AS Path

Report: Allocated and Reserved AS blocks

Selected AS Report

Enter an AS here to generate an aggregation report for the AS.

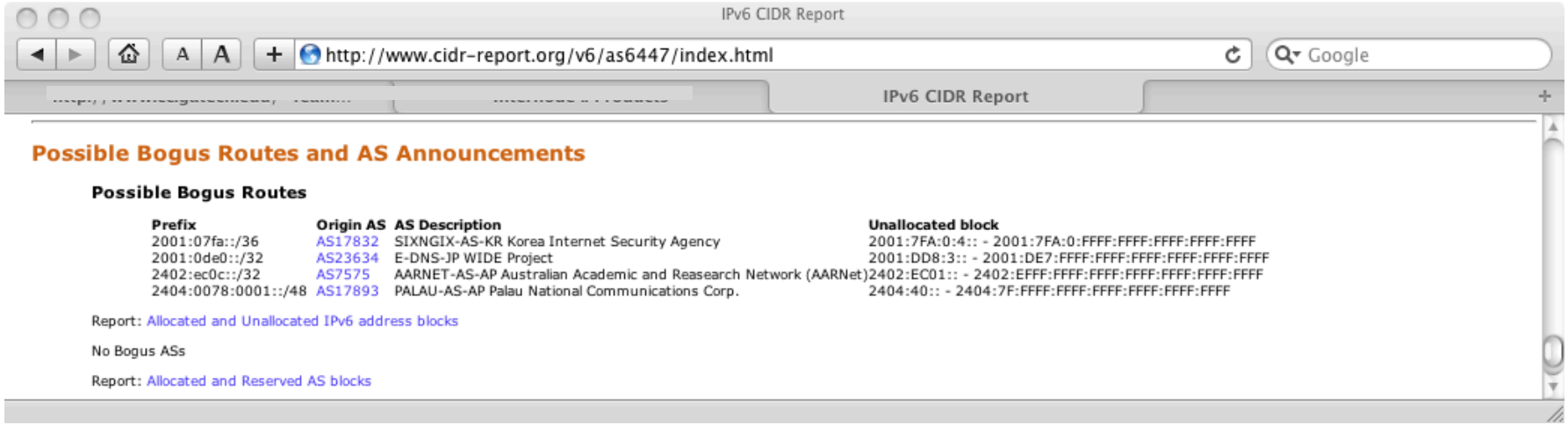
Enter AS (e.g. "AS1221")

Generate AS Report

A version of this report is available using plain text tables.

Report produced at: Fri Jan 22 04:11:51 2010 AEST (cidr-report.c v1.4 - gih)

phew!


IPv6 CIDR Report
http://www.cidr-report.org/v6/as6447/index.html
Google
IPv6 CIDR Report
Possible Bogus Routes and AS Announcements
Possible Bogus Routes
Prefix Origin AS AS Description Unallocated block
2001:07fa::/36 AS17832 SIXNGIX-AS-KR Korea Internet Security Agency 2001:7FA:0:4:: - 2001:7FA:0:FFFF:FFFF:FFFF:FFFF:FFFF
2001:0de0::/32 AS23634 E-DNS-JP WIDE Project 2001:DD8:3:: - 2001:DE7:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
2402:ec0c::/32 AS7575 AARNET-AS-AP Australian Academic and Reasearch Network (AARNet) 2402:EC01:: - 2402:EFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
2404:0078:0001::/48 AS17893 PALAU-AS-AP Palau National Communications Corp. 2404:40:: - 2404:7F:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Report: Allocated and Unallocated IPv6 address blocks
No Bogus ASs
Report: Allocated and Reserved AS blocks

What's the base problem here?

Addresses and Routing are insecure

- Routing is built on sloppy mutual trust models
- Routing auditing is a low value activity that noone performs with any level of thoroughness
- We have grown used to lousy solutions and institutionalized lying in the routing system
- And because instances of abuse are supposedly relatively infrequent we are prepared to tolerate the risk of having a completely insecure routing system

What's the base problem here?

Noone seems to want to care enough about the integrity of the network to address routing integrity!

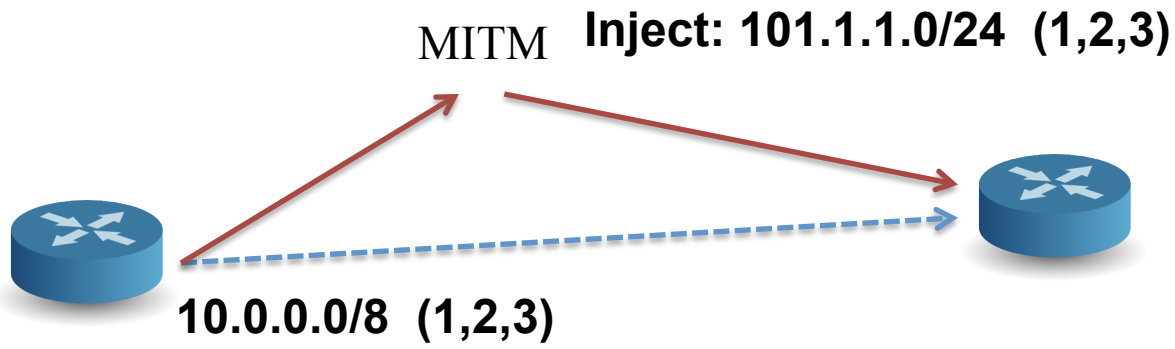
Routing Security is a shared problem

It's a tragedy of the commons situation

- Nobody can single-handedly apply rigorous tests on the routing system
- And the lowest common denominator approach is to apply no integrity tests at all
- It's all trust and absolutely no defence

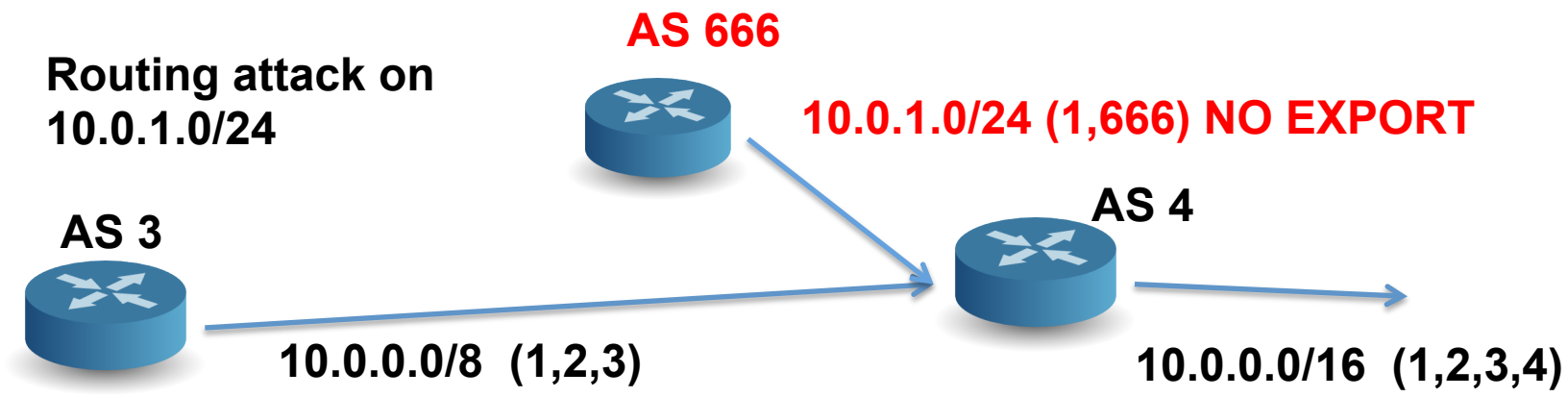
Routing Security

1. Protecting **routing protocols** and their operation
   - Threat model:
     - Disrupt the operation of the routing protocol by a "man-in-the-middle" attack
     - Compromise the topology discovery / reachability operation of the routing protocol by injection of false routing information
   - Response:
     - Current operational best practice uses TCP-MD5 and avoids eBGP-multihop



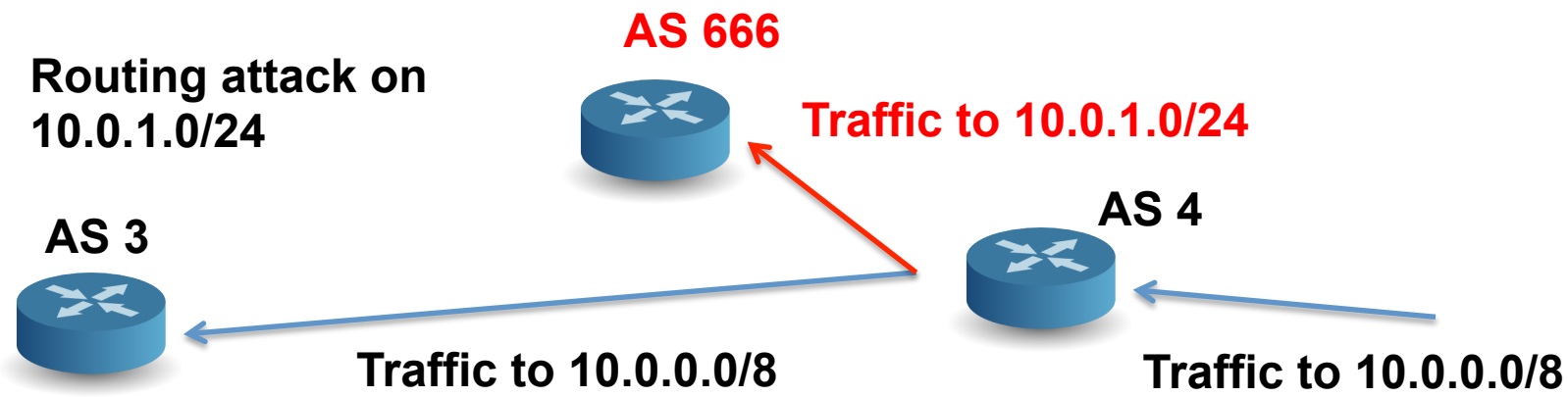
Routing Integrity

2. Protecting the **routing protocol payload**
   - Threat model:
     - Compromised router or compromised Routing Entity (AS)
     - Insert corrupted address information into your network's routing tables
     - Insert corrupt reachability information into your network's forwarding tables
     - Allow the routing protocol to disseminate the corrupted information across the entire internet



Threats

- Corrupting the routers' forwarding tables can result in:
  - Misdirecting traffic (subversion, denial of service, third party inspection, passing off)
  - Dropping traffic (denial of service)
  - Adding false addresses into the routing system (anon attacks)
  - Isolating or removing the router from the network



Can we "tweak" BGP so that it can detect the difference between good and evil, and only advertise and propagate the "good" routes?

Routing Security

- The basic routing payload security questions that need to be answered are:
  - **Who** injected this address prefix into the network?
  - Did they have the necessary **credentials** to inject this address prefix? Is this a valid address prefix?
  - Is the forwarding path to reach this address prefix **trustable**?
- And can these questions be answered by any BGP speaker quickly and cheaply?

A (random) BGP Update

2010/01/26 00:03:35 rcvd UPDATE w/ attr:

nexthop 203.119.76.3, origin i, path 4608 1221 4637 3561 3356 4657 4773

124.197.64.0/19

BGP Update Validation

2010/01/26 00:03:35 rcvd UPDATE w/ attr:

nexthop 203.119.76.3, origin i, path 4608 1221 4637 3561 3356 4657 4773

124.197.64.0/19

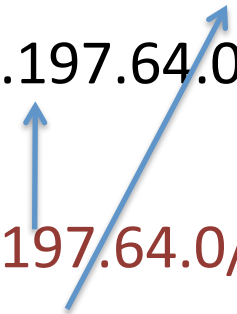
Is 124.197.64.0/19 a “valid” prefix?

BGP Update Validation

2010/01/26 00:03:35 rcvd UPDATE w/ attr:

nexthop 203.119.76.3, origin i, path 4608 1221 4637 3561 3356 4657 4773

124.197.64.0/19



Is 124.197.64.0/19 a “valid” prefix?

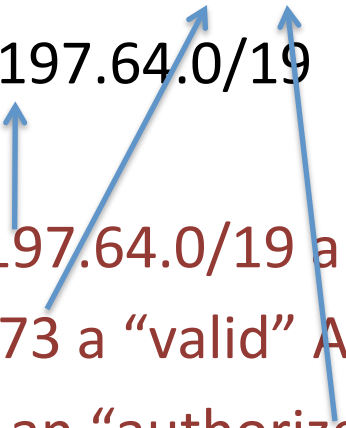
Is AS4773 a “valid” ASN?

BGP Update Validation

2010/01/26 00:03:35 rcvd UPDATE w/ attr:

nexthop 203.119.76.3, origin i, path 4608 1221 4637 3561 3356 4657 4773

124.197.64.0/19



Is 124.197.64.0/19 a “valid” prefix?

Is AS4773 a “valid” ASN?

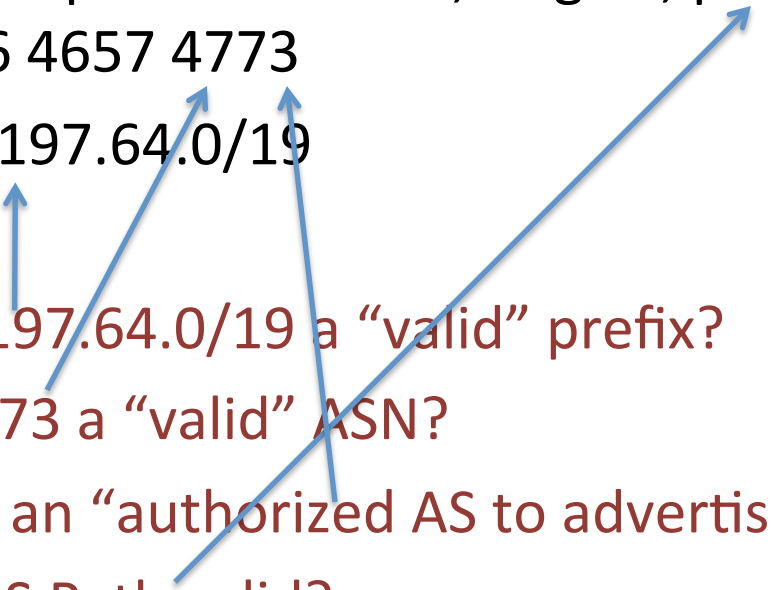
Is 4773 an “authorized AS to advertise a route to this prefix?

BGP Update Validation

2010/01/26 00:03:35 rcvd UPDATE w/ attr:

nexthop 203.119.76.3, origin i, path 4608 1221 4637 3561 3356 4657 4773

124.197.64.0/19



Is 124.197.64.0/19 a "valid" prefix?

Is AS4773 a "valid" ASN?

Is 4773 an "authorized AS to advertise a route to this prefix?

Is the AS Path valid?

- Is AS 4657 a valid AS, and did AS 4773 advertise this route to AS 4657?
- Is AS 3356 a valid AS, and did AS 4657 advertise this route to AS 3356?
- etc

A Foundation for Routing Security

- The use of authenticatable attestations to allow automated validation of:
  - the authenticity of the route object being advertised
  - authenticity of the origin AS
  - the binding of the origin AS to the route object
- Such attestations used to provide a cost effective method of validating routing requests
  - as compared to the today's state of the art based on techniques of vague trust and random whois data mining

A Foundation for Routing Security

Adoption of some basic security functions into the Internet's routing domain:

- Injection of reliable trustable data

  A ***Resource PKI*** as the base of validation of network data

- Explicit verifiable mechanisms for integrity of data distribution

  Adoption of some form of certified authorization mechanism to support validation of credentials associated with address and routing information

A Starting Point

- How can you certify who what which address?
  - follow the allocation trail
  - Certification of the "Right-of-Use" of IP Addresses and AS numbers as a linked attribute of the Internet's number resource allocation and distribution framework

For example:

APNIC (the "Issuer") certifies that:

the certificate's "Subject"

whose public key is contained in the certificate

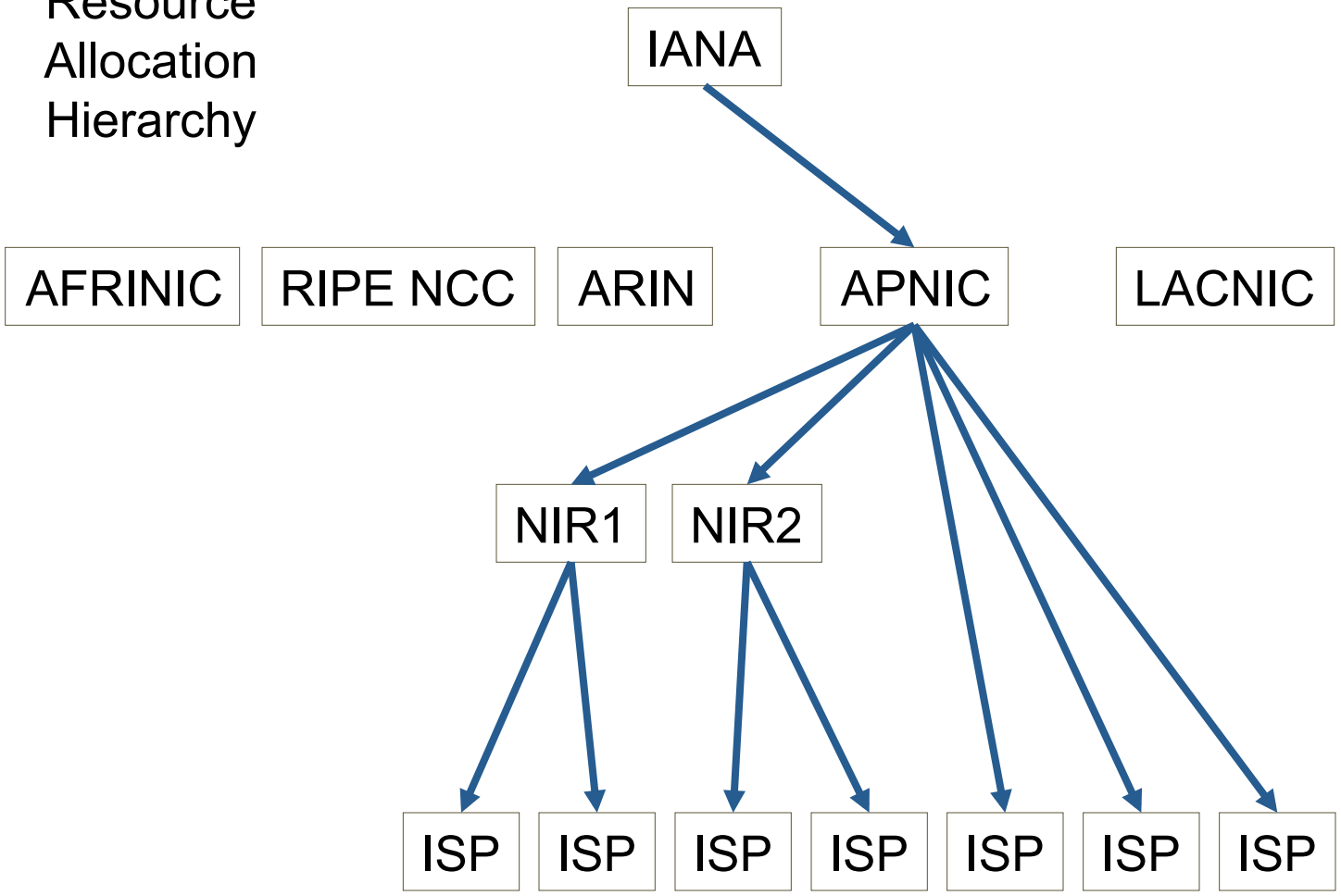
is the current holder of a set of IP address and AS resources

that are listed in the certificate extension

APNIC does NOT certify the identity of the subject, nor their good (or evil) intentions!

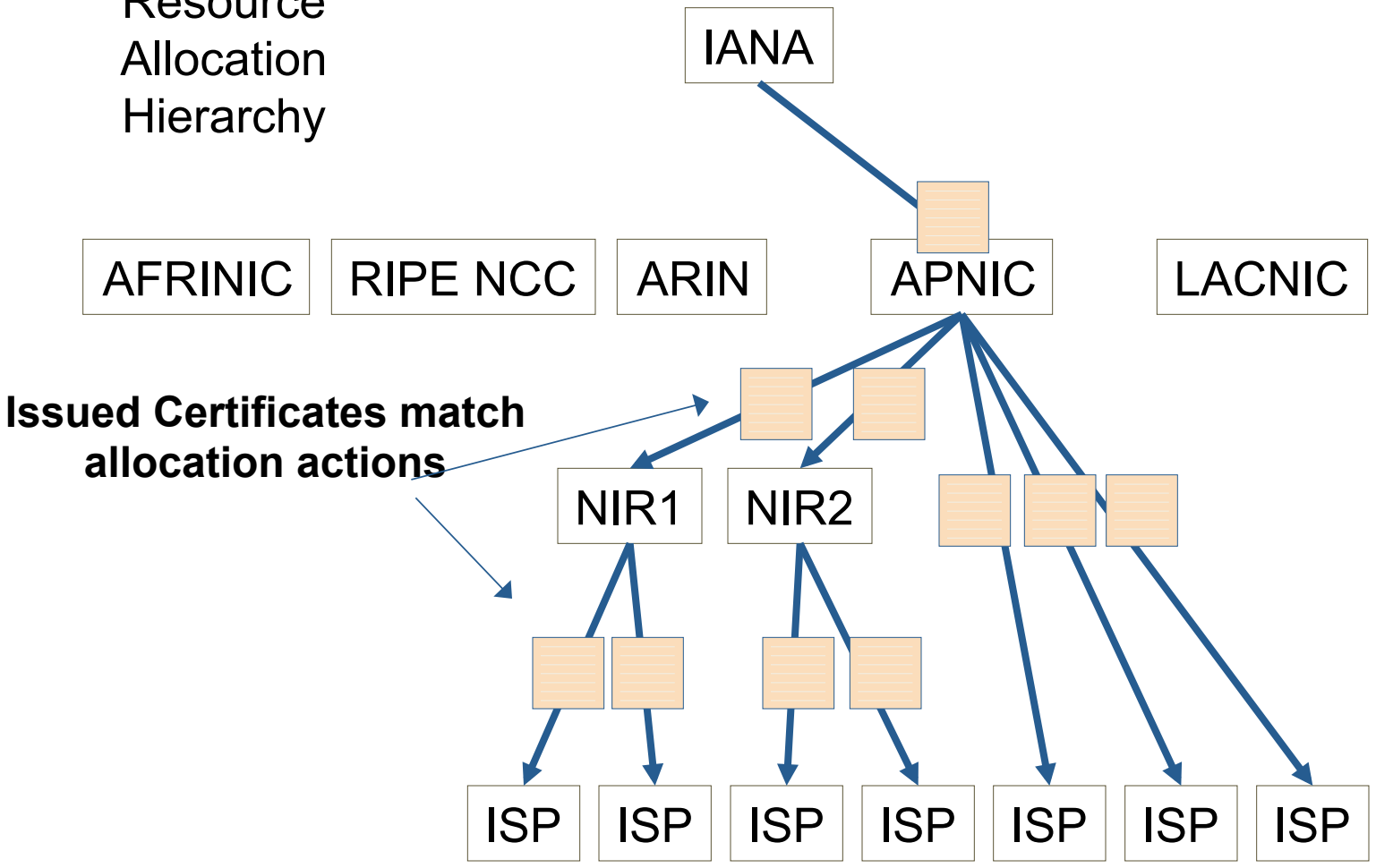
Resource Certificates

Resource
Allocation
Hierarchy

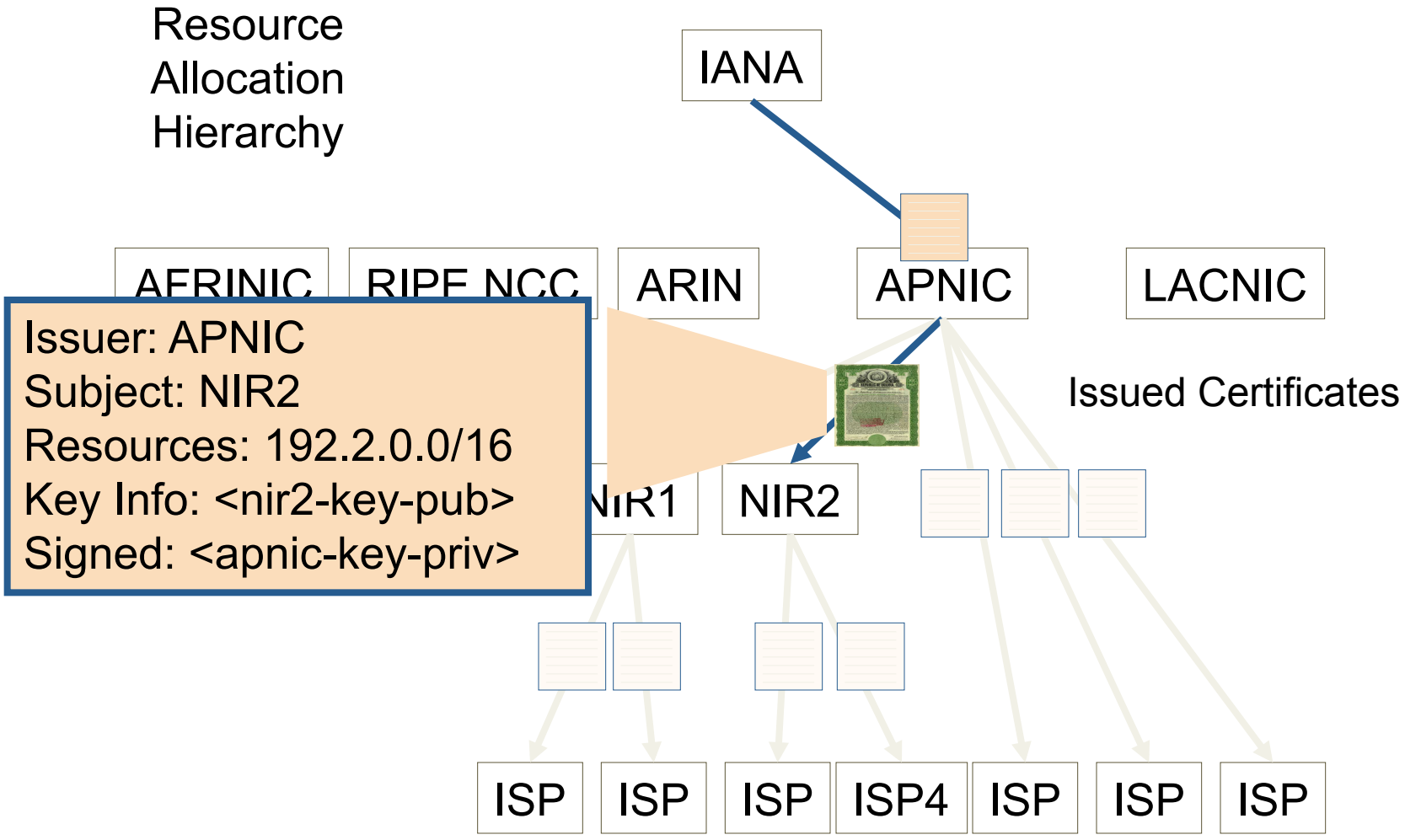


Resource Certificates

Resource Allocation Hierarchy

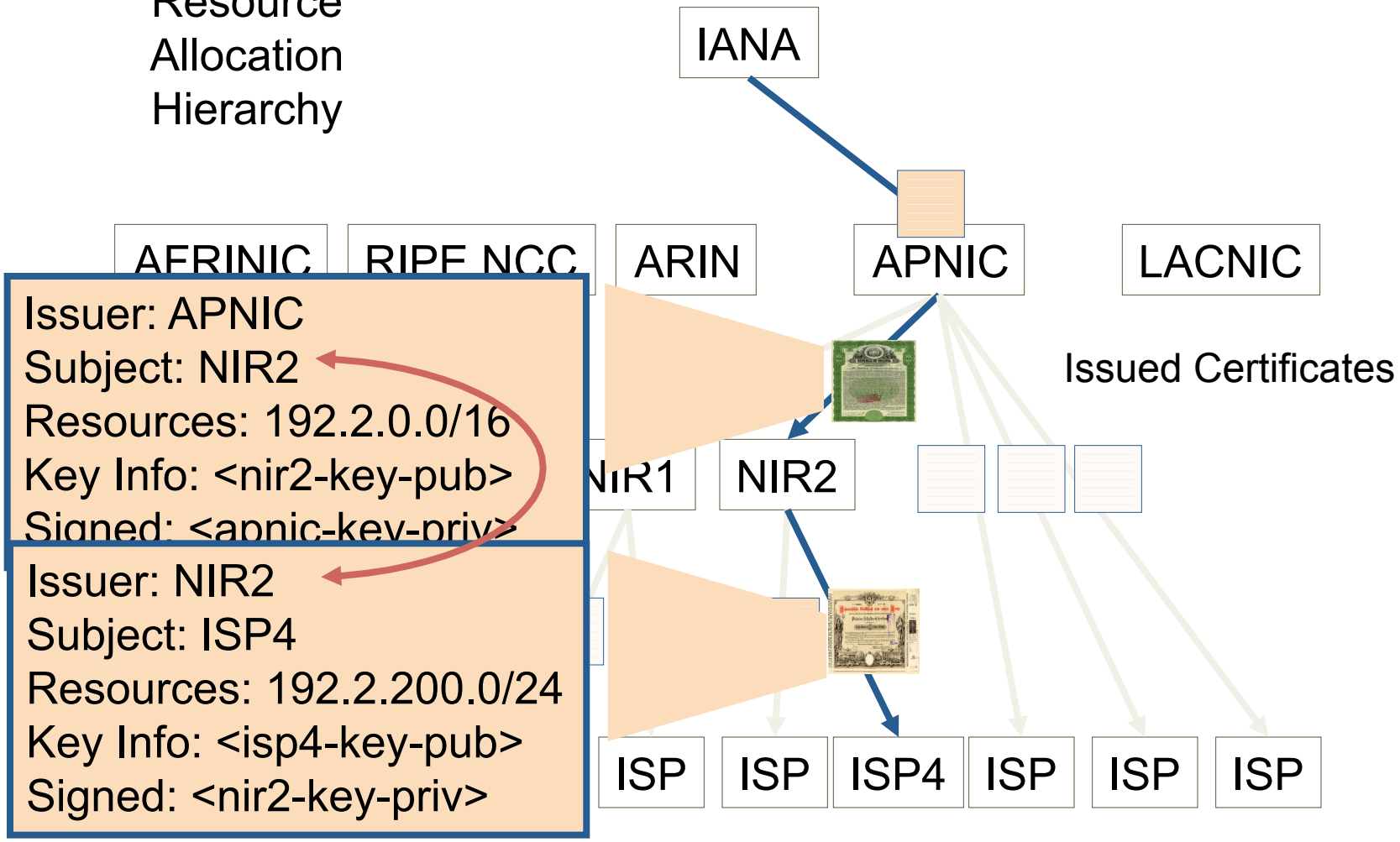


Resource Certificates



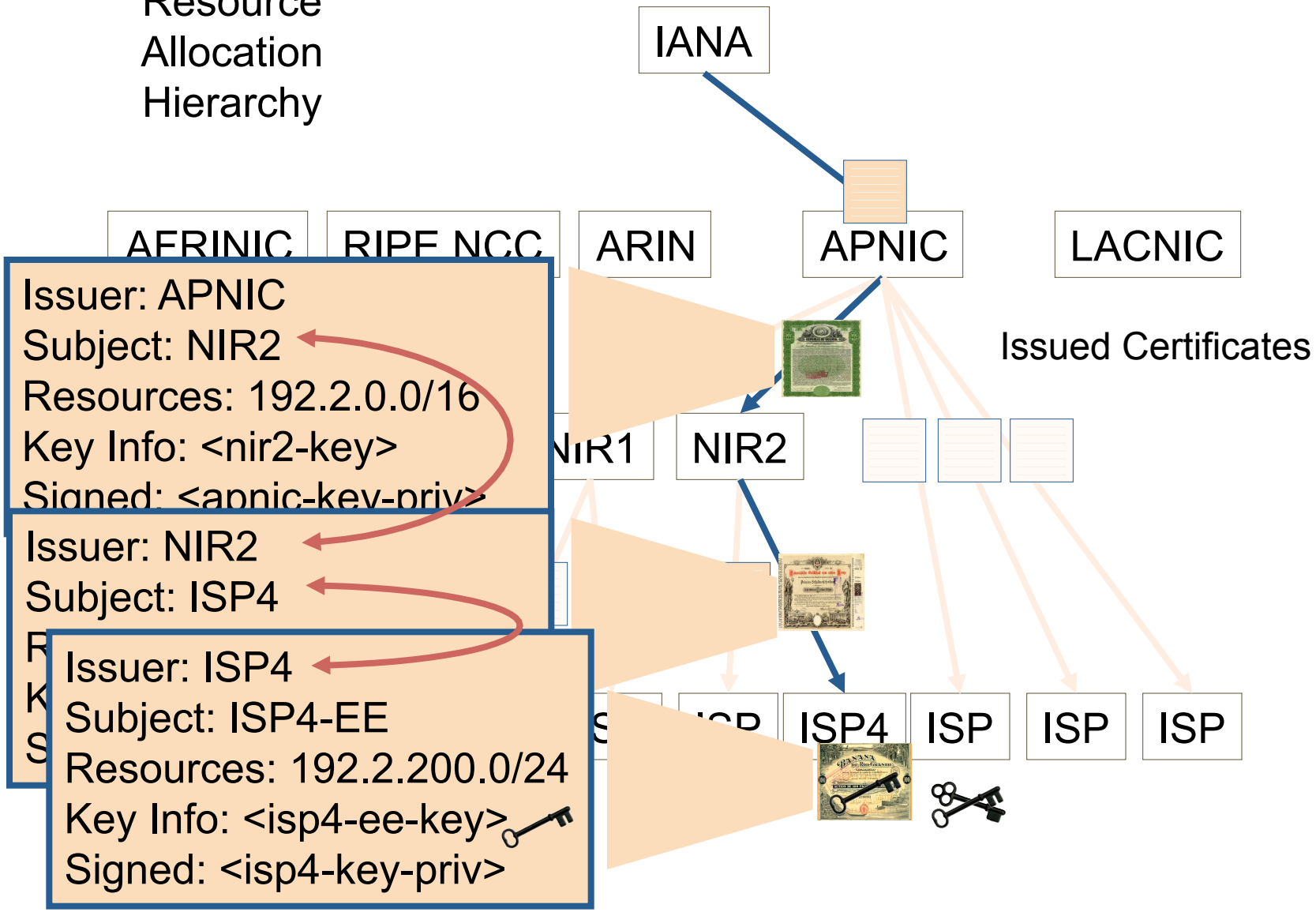
Resource Certificates

Resource
Allocation
Hierarchy



Resource Certificates

Resource
Allocation
Hierarchy

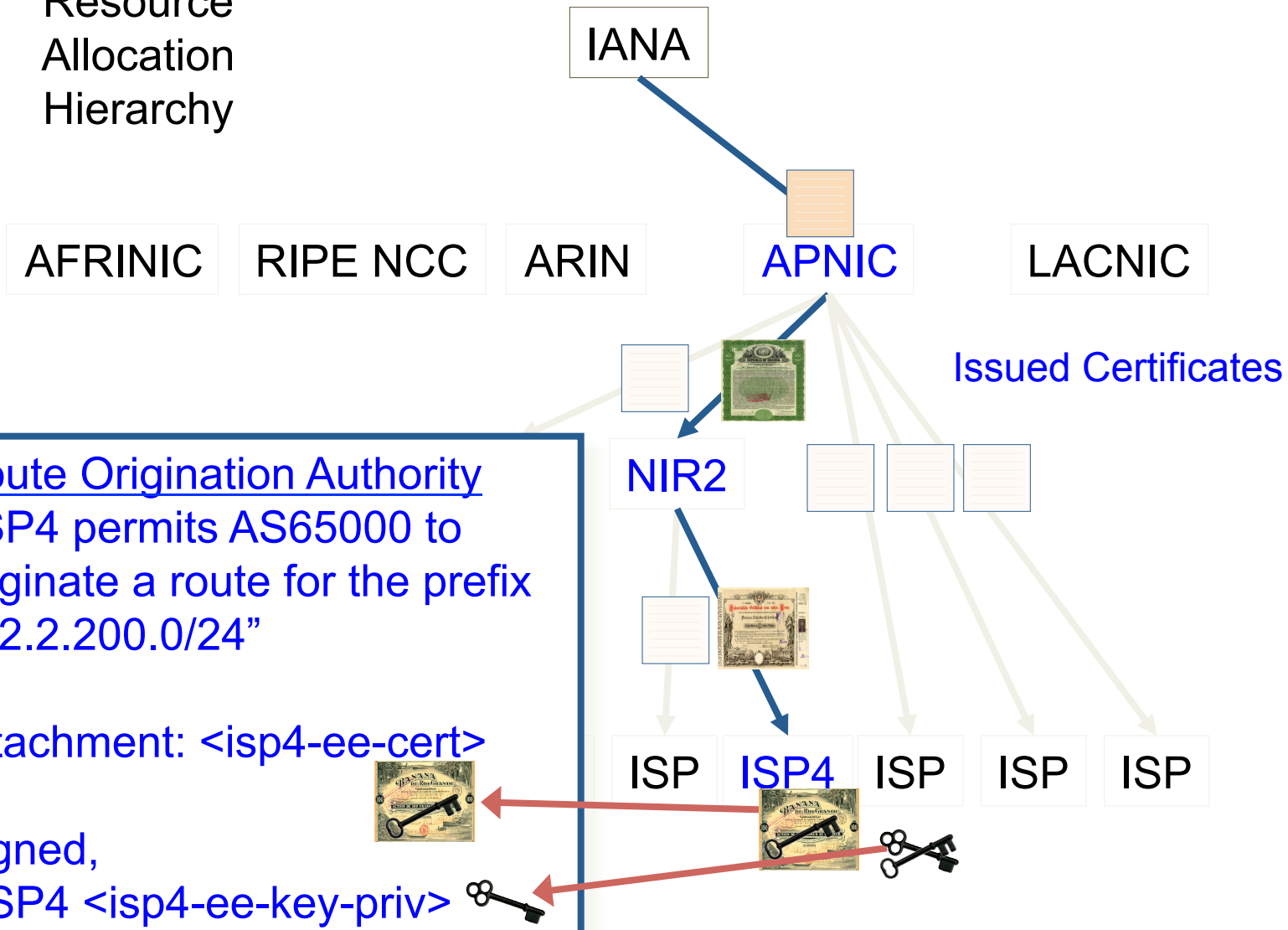


What could you do with Resource Certificates?

- You could sign "routing authorities" with your private key, providing an authority for an AS to originate a route for the named prefix. Any Relying Party could validate this authority in the RPKI
- You could use the private key to sign routing information in an Internet Route Registry
- You could attach a digital signature to a protocol element in a routing protocol
- You could issue signed derivative certificates for any sub-allocations of resources

Signed Objects

Resource Allocation Hierarchy



Route Origination Authority

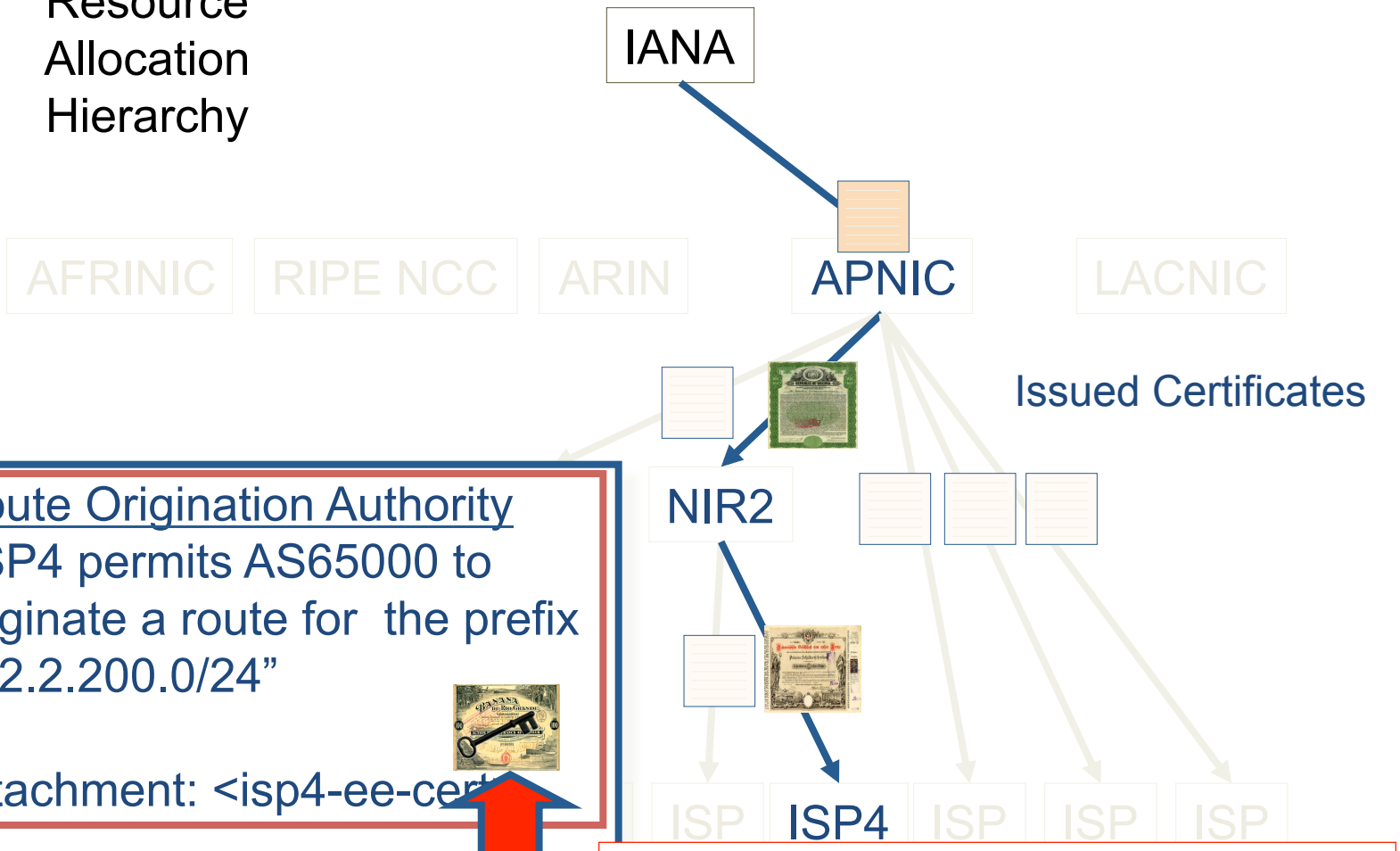
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>

Signed Object Validation

Resource Allocation Hierarchy



Route Origination Authority

"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

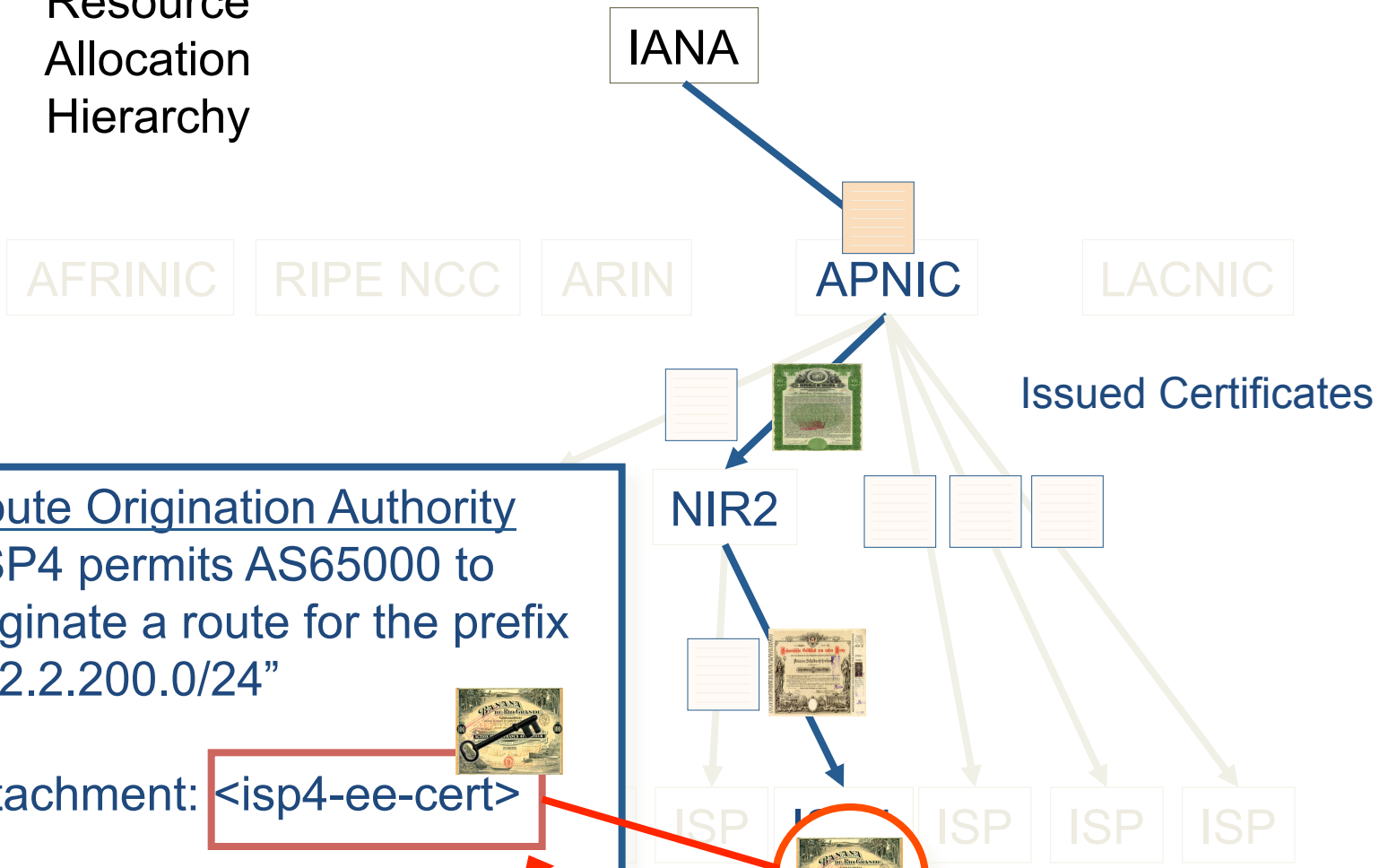
Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>

1. Did the matching private key sign this text?

Signed Object Validation

Resource Allocation Hierarchy



Route Origination Authority

"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

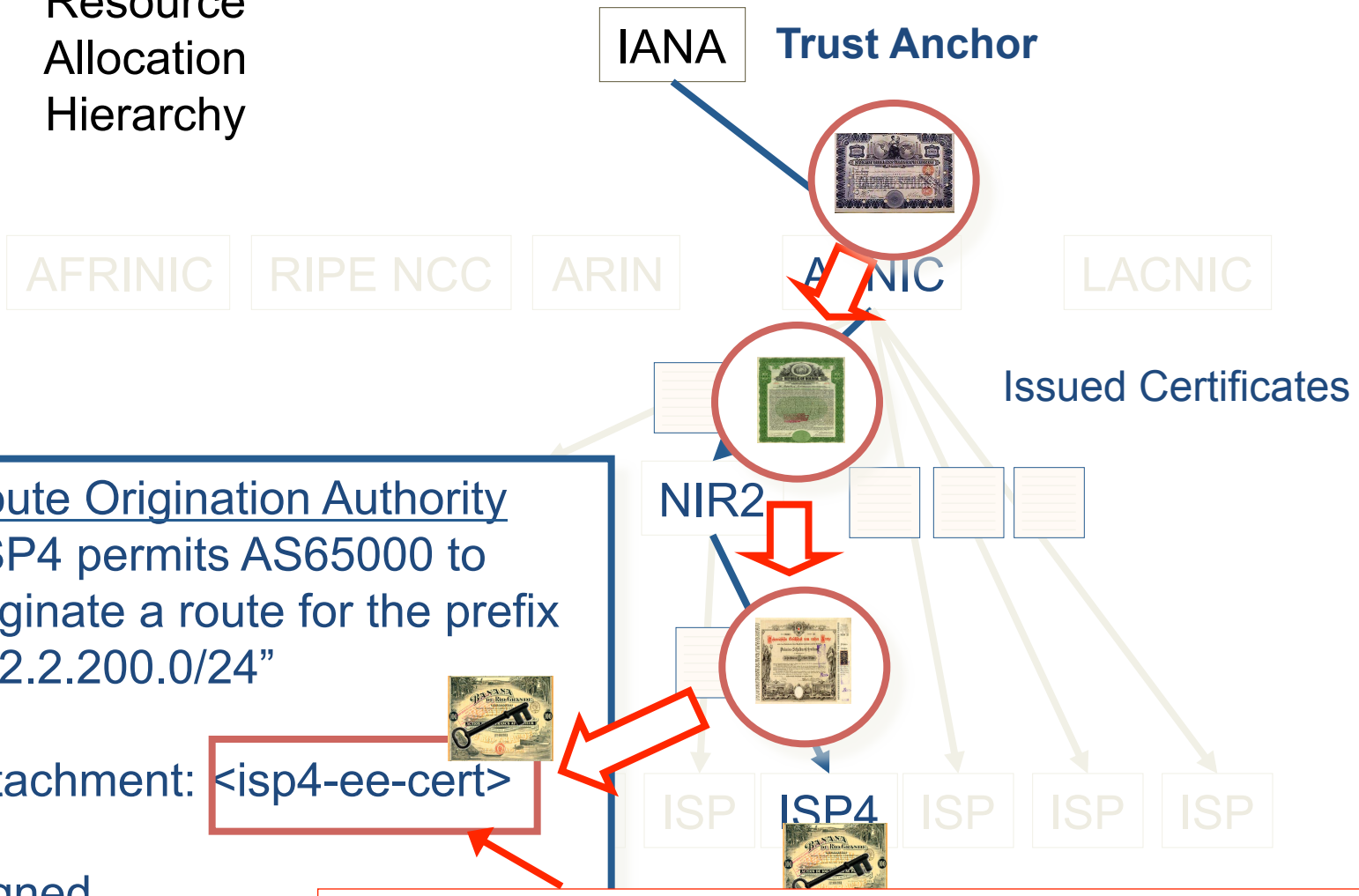
Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>

2. Is this certificate valid?

Signed Object Validation

Resource Allocation Hierarchy



Signed Object Validation

Resource
Allocation
Hierarchy

AFRINIC RIPE NCC A

Route Origination Authority
"ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24"

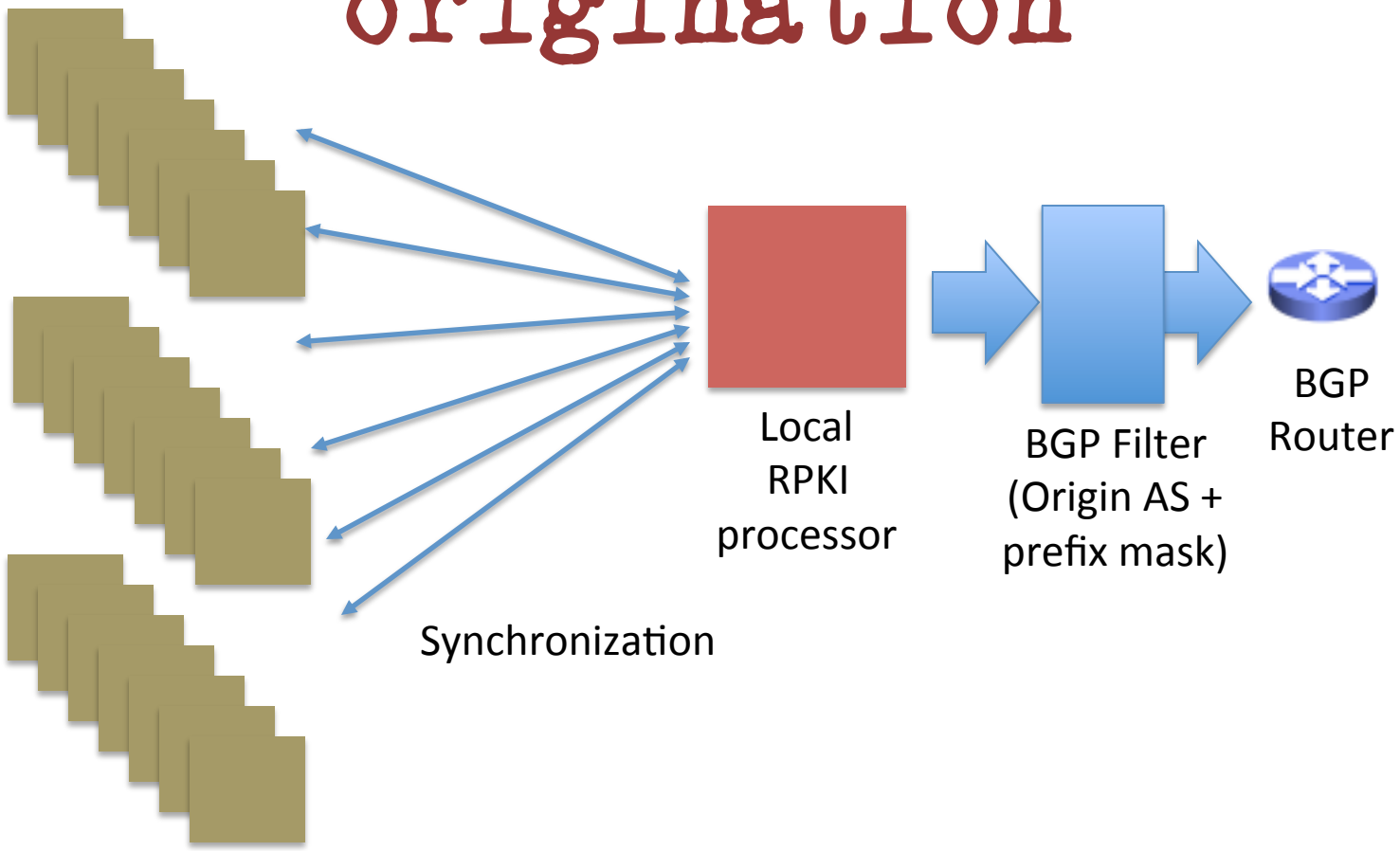
Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>

Validation Outcomes

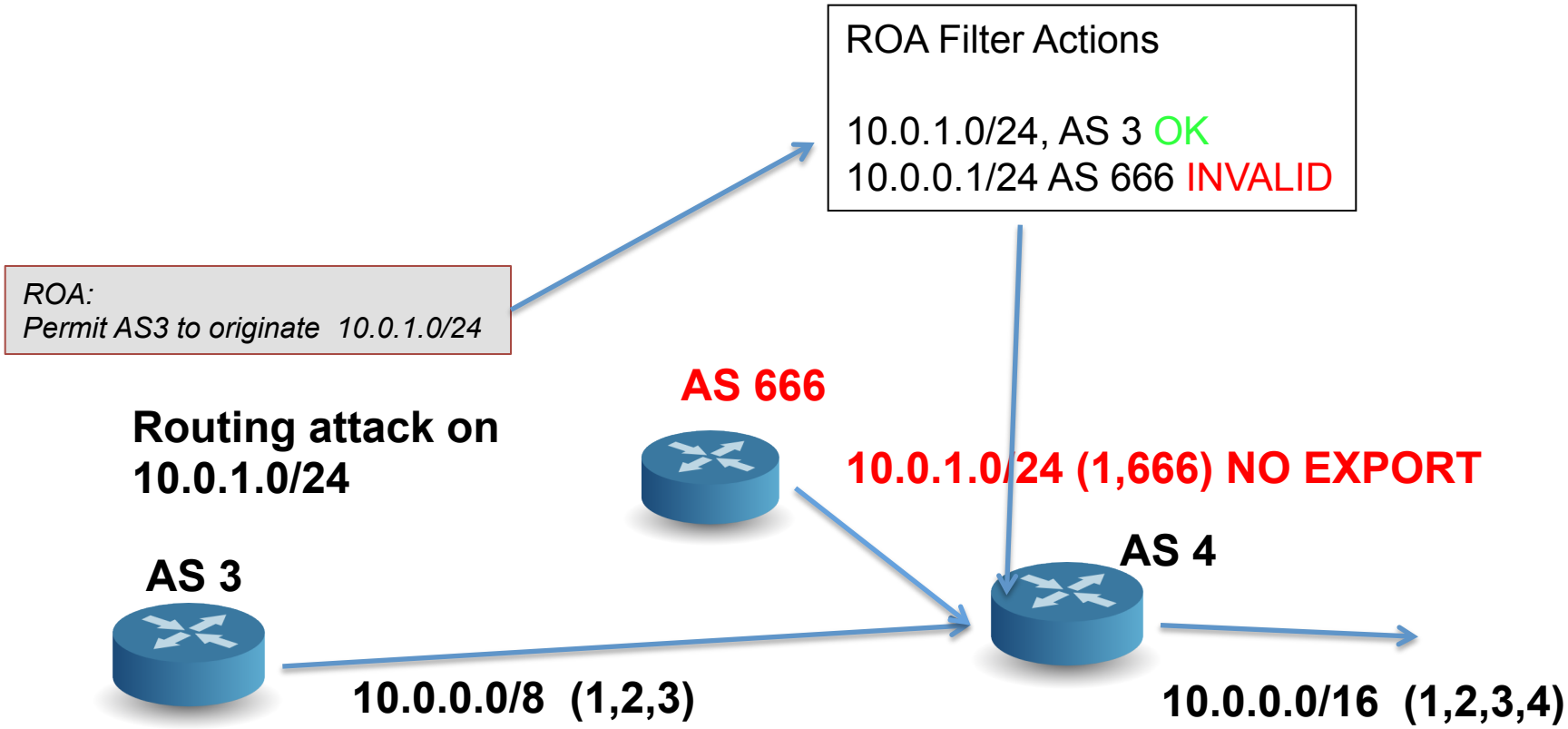
1. ISP4 authorized this Authority document
2. 192.2.200.0/24 is a **valid** address, derived from an APNIC allocation
3. ISP4 holds a current right-of-use of 192.2 200.0/24
4. A route object, where AS65000 originates an advertisement for the address prefix 192.2.200.0/24, has the explicit authority of ISP4, who is the current holder of this address prefix

A (partial) architecture for securing BGP origination



ROA-based Filtering

- If a ROA exists for (10.0.1.0.24, AS 3) then the AS666 attack is detectable and preventable at AS 4

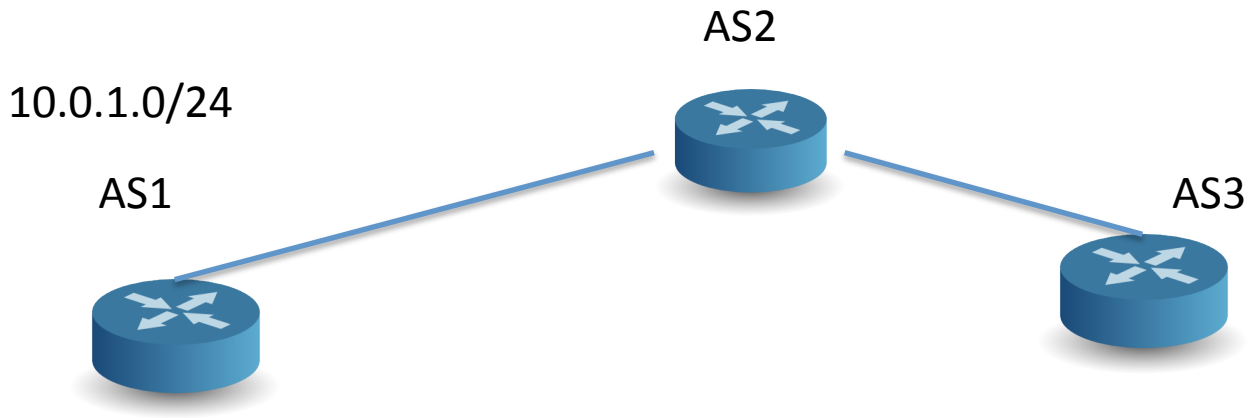


What about AS Path Validation?

Securing the AS PATH

We need two additional components:

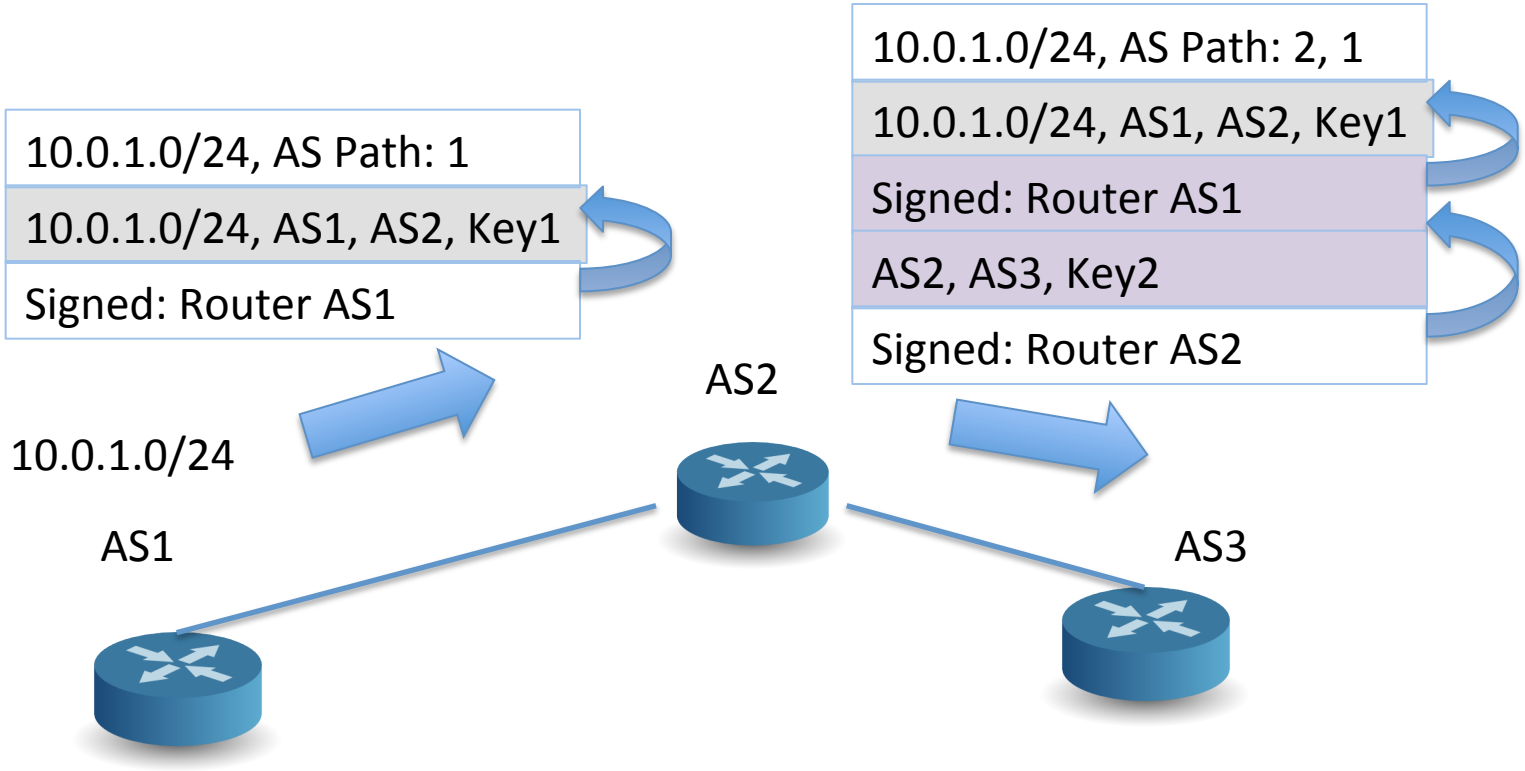
- An RPKI router certificate (AS and BGP router ID)
- a new BGP attribute
- Each eBGP Router “forward signs” the AS Path with its private key
- Each validating routing can validate the chain of signatures against the AS Path to match the path to the sig chain



Securing the AS PATH

We need two additional components:

- An RPKI router certificate (AS and BGP router ID)
- a new BGP attribute



Securing the AS Path

- Each router to sign across the triplet of: the signature of what was received, its own AS and the next hop AS
- BGPsec routers are required to unchain the signature set and match it to the AS Path in the update, using the local RPKI cache to validate the router signatures

Signing the AS Path

- The AS Path represents the inter-AS propagation path of the route from the origin to the BGP speaker
- Attempts to manipulate the AS Path by adding or removing AS's will invalidate this signature chain attribute of the update
- "validation" of an update allows the receiver to assure themselves that each AS propagated the route in the order shown in the AS Path

Securing the AS Path

BUT this does not all happen for free:

- It adds size and weight to the operation of BGP
- It's slow and cumbersome
- It cannot be deployed incrementally piecewise
- Partial deployment has limited benefits
- It's brittle
- It's not clear that gain > pain!

Concerns

A major issue here is that of ***partial use and deployment***

- This security mechanism has to cope with partial deployment in the routing system
  - The basic conventional approach of "what is not certified and proved as good must be bad" will not work in a partial deployment scenario
- In BGP we need to think about both origination and the AS Path of a route object in a partial deployed environment
  - AS path validation is challenging indeed in an environment of piecemeal use of secure credentials, as the mechanism cannot tunnel from one BGPsec "island" to the next "island"
- A partially secured environment may incur a combination of high incremental cost with only marginal net benefit to those deploying BGPsec

Concerns

Is a ***trust hierarchy*** the best approach to use?

- The concern here is concentration of vulnerability

  If validation of routing information is dependent on the availability and validity of a single root trust anchor then what happens when this single digital artifact is attacked?

- But is there a viable alternative approach?

  Can you successfully incorporate robust diversity of authentication of security credentials into a supposedly highly resilient secure trust framework?

  This is very challenging!

Concerns

Is certification the ***only way*** to achieve useful outcomes in securing routing?

- Is this form of augmentation to BGP to enforce "protocol payload correctness" over-engineered, and does it rely on impractical models of universal adoption?
- Can various forms of *routing anomaly detectors* adequately detect the most prevalent forms of typos and deliberate lies in routing with a far lower overhead, and allow for unilateral detection of routing anomalies?
- Or are such anomaly detectors yet another instance of "cheap security pantomime" that offer a thinly veiled placebo of apparent security that is easily circumvented or fooled by determined malicious attack?

Good, Fast, or Cheap? Pick one!

We can't make secure routing mechanisms cheaper, faster, more robust, and more effective than existing routing tools ...

- We can make it robust, but it won't be cheap!
- We can make it fast, but it won't be robust and it won't be cheap!
- We can make it cheap, but it won't be robust!

Thank You

Questions?