Route Injection and the Backtrackability of Cyber Misbehavior

Fall 2006 Internet2 Member Meeting

Chicago, Illinois, Dec 5th, 2006
4:30-5:30PM, CC10D

Joe St Sauver, Ph.D. (joe@uoregon.edu)
University of Oregon Computing Center
http://www.uoregon.edu/~joe/fall2006mm

A Note About The Format of This Talk and A Disclaimer

- I've prepared this talk in some detail so that it can be followed by those not present when the talk was originally given, and to minimize the need for the audience to jot down notes; doing so also help keep me on track.

- **Disclaimer: all opinions expressed in this document are strictly my own.**

- **Independently verify any/all data presented.**

- Portions of this presentation have previously been shared at closed meetings for non-higher ed audiences.

I. IP Addresses, Routing, and the Connections You See

"Where Did *THAT* Traffic Come From?"

- A fundamental tasks performed in most every cybersecurity investigation is attributing network traffic to a responsible party. That's not always easy.
- Miscreants obviously want to hide and avoid attribution, and have been known to employ a variety of strategies and techniques in an effort to hinder backtracking.
- For example, it is well known that open proxies or spam zombies may be used in an effort to keep an investigator from successfully "working back upstream" to the ultimate source of spam traffic, and similarly everyone has seen forged headers or other misleading data that may be provided as part of a spam message's headers, just to mention a couple of approaches.
- In general, however, most investigators **DO** "rely on" the IP address of a system that directly connects to a trusted host.

For Example…

- Assume you saw a connection on your server from 128.223.142.13…
- If you checked the DNS for that address on a Unix box, or if you checked whois, you'd associate that address with UO:

```
% host 128.223.142.13
13.142.223.128.in-addr.arpa domain name pointer darkwing.uoregon.edu.
% host darkwing.uoregon.edu
darkwing.uoregon.edu has address 128.223.142.13

% whois -h whois.arin.net 128.223.142.13
OrgName:        University of Oregon
OrgID:          UNIVER-193
Address:        1225 Kincaid St
City:           Eugene
StateProv:      OR
PostalCode:     97403-1212
[etc]
```

In Reality, However…

- **Just because some IP addresses are shown as having been assigned or allocated to someone doesn't mean that they're the ones actually USING those addresses.**
- For example, a miscreant may be able to arrange to have a third party ISP announce ("route") a range of IP addresses which they don't legitimately control. That announcement can be persistent, or temporary (e.g., brought up just long enough to be abused and then withdrawn), a processes commonly known as "address space hijacking."
- **Address space hijacking may have important implications for cybercrime investigations which rely on the backtracking of observed connections.**
- **If you've not verifying the routing of the TCP connections at the time IP addresses of interest were used, you may end up going after the wrong party.**

The Feds Are Also Focused on IP Usage and Attribution Information

- The belief that if you "know" an IP (and a timestamp/time zone) you "should" be able to tell who's associated with that address is also reflected in **ISP customer record retention requirements** mentioned as part of…
  -- The Attorney General's remarks at the NCMEC:
  `www.usdoj.gov/ag/speeches/2006/ag_speech_060420.html`
  -- Congresswoman Diana DeGettes's ISP data retention requirement amendment:
  `energycommerce.house.gov/108/Markups/04262006/degette_001_XML.PDF`
  -- EU/International data retention programs
  `www.epic.org/privacy/intl/data_retention.html`
- **It is probably important that policy makers understand that apparent Internet traffic sources should not be taken at face value; route hijacking must also be considered.**

II. A "Hand Waving" Introduction To Routing

What Do You Mean by "Routing?"

- A "route" can (informally) be thought of as the **path** that network traffic takes as it proceeds from its source to its destination. Anyone who's used the **traceroute** command has seen examples of network paths. For example, lets trace to 128.223.142.13 from a "looking glass" server in Seattle (for a list of looking glass sites see http://www.traceroute.org):

```
Tracing the route to darkwing.uoregon.edu (128.223.142.13)
1 so-3-0-0.gar1.Seattle1.Level3.net (209.0.227.133) 0 ms 4 ms 0 ms
2 ge-11-1.hsa2.Seattle1.Level3.net (4.68.105.103) [AS 3356] 0 ms
  ge-10-2.hsa2.Seattle1.Level3.net (4.68.105.135) [AS 3356] 0 ms
  ge-11-1.hsa2.Seattle1.Level3.net (4.68.105.103) [AS 3356] 0 ms
3 nero-gw.Level3.net (63.211.200.246) [AS 3356] 12 ms 4 ms 4 ms
4 ptck-core2-gw.nero.net (207.98.64.138) [AS 3701] 4 ms 4 ms 4 ms
5 eugn-core2-gw.nero.net (207.98.64.1) [AS 3701] 8 ms 4 ms 8 ms
6 eugn-car1-gw.nero.net (207.98.64.165) [AS 3701] 8 ms 8 ms 8 ms
7 uonet8-gw.nero.net (207.98.64.66) [AS 3701] 4 ms 8 ms 4 ms
8 ge-5-1.uonet2-gw.uoregon.edu (128.223.2.2) [AS 3582] 8 ms 8 ms 8 ms
9 darkwing.uoregon.edu (128.223.142.13) [AS 3582] 8 ms 4 ms 8 ms
```

Looking At That Traceroute…

- That traceroute shows the hop-by-hop path that traffic took going from a host in Seattle to 128.223.142.13. Because that traceroute was done from a "looking glass" running on a router, besides showing us "normal" traceroute stuff (such as IP addresses and host names for each router hop in the path), it **also** shows us some **additional** numbers, e.g.: "**AS 3356," "AS 3701,"** and **"AS 3582."**
- Those numbers represent the "autonomous systems" through which network traffic might pass when going from our source host to our destination host. **AS3356** represents Level3, **AS3701** represents NERO (Oregon's higher education network), and **AS3582** represents the U of O. That is a perfectly reasonable path for traffic to take in this case.
- Traffic from a different destination will likely take a different path. For example, what about traffic from Switzerland?

Traceroute From a Site in Switzerland

```
Tracing the route to darkwing.uoregon.edu (128.223.142.13)
1 switch.rt1.gen.ch.geant2.net (62.40.124.21) [AS 20965] 4 ms 0 ms 0 ms
2 so-7-2-0.rt1.fra.de.geant2.net (62.40.112.22) [AS 20965] 8 ms 8 ms 16 ms
3 abilene-wash-gw.rt1.fra.de.geant2.net (62.40.125.18) [AS 20965] 128 ms 124 ms
   112 ms
4 nycmng-washng.abilene.ucaid.edu (198.32.8.84) [AS 11537] 112 ms 108 ms 108 ms
5 chinng-nycmng.abilene.ucaid.edu (198.32.8.82) [AS 11537] 132 ms 132 ms 128 ms
6 iplsng-chinng.abilene.ucaid.edu (198.32.8.77) [AS 11537] 144 ms 132 ms 136 ms
7 kscyng-iplsng.abilene.ucaid.edu (198.32.8.81) [AS 11537] 152 ms 160 ms 140 ms
8 dnvrng-kscyng.abilene.ucaid.edu (198.32.8.13) [AS 11537] 164 ms 156 ms 152 ms
9 snvang-dnvrng.abilene.ucaid.edu (198.32.8.1) [AS 11537] 184 ms 176 ms 176 ms
10 pos-1-0.core0.eug.oregon-gigapop.net (198.32.163.17) [AS 4600] 192 ms 188 ms
   192 ms
11 uo-0.eug.oregon-gigapop.net (198.32.163.147) [AS 4600] 192 ms 200 ms 212 ms
12 ge-5-1.uonet1-gw.uoregon.edu (128.223.2.1) [AS 3582] 192 ms 188 ms
   ge-5-1.uonet2-gw.uoregon.edu (128.223.2.2) [AS 3582] 192 ms
13 darkwing.uoregon.edu (128.223.142.13) [AS 3582] 192 ms 188 ms 192 ms
```

- Now the path we see is **AS20965** (Geant), to **AS11537** (I2) to **AS4600** (the Oregon Gigapop) to **AS3582** (UO). If we checked other sites, we'd see still other paths, but in each case we could use the ASNs we see to compactly represent the path.

What Is An ASN?

- An Autonomous System Number is a number assigned to a group of network addresses managed by a particular network operator which share a common routing policy.
- Most ISPs, large corporations, and university networks have an ASN. For example, Google uses AS15169, Sprint uses AS1239, Intel uses AS4983, and so on. Some large networks with particularly complex routing policies may have multiple ASNs; others, with simple routing policies and only a single upstream network provider, may have none (their network blocks get announced using their upstream provider's ASN).
- You may want to think of an ASN as a number that "maps to" or represents a particular provider or network. ASNs are nice to work with because in most cases a given entity will only have one, no matter how many IP addresses or netblocks or customers they may have.

ASNs are New to Me. How Do I Translate the ASNs I See to Names?

- You can look ASNs up in the ARIN, RIPE, APNIC, LACNIC, AFRINIC, JPNIC, TWNIC (etc.) whois databases, just like IP addresses, either checking with a whois client or via the web whois interface provided by each of those registrars.
- If you don't find an ASN in the ARIN whois (for example), you may be redirected appropriately, or you may just need to try the other regions (e.g., check RIPE, check APNIC, check LACNIC, etc., etc.), until you finally get a match.
- Usually you'll preface the actual number with AS when looking it up, e.g., AS3582, but if you have difficulty getting a match with the AS included as a literal part of the query, try querying on just the actual AS number itself (this can help when the ASN you're trying to translate is part of a range of ASNs documented via a single entry in the database).

Example of Looking Up an ASN

- Assume, for example, we want to know who owns AS20965:

```
% whois -h whois.ripe.net AS20965
[snip]
aut-num:     AS20965
as-name:     GEANT
descr:       The GEANT IP Service
[snip]
role:        DANTE Operations
address:     City House, 126-130 Hills Road
address:     Cambridge CB2 1PQ, UK
phone:       +44 1223 371300
fax-no:      +44 1223 371371
[snip]
```

The Origin AS; Detecting Hijacking

- Coming back to the traceroutes we did from Seattle and Switzerland, in each case the **last AS** in the path was the same: **AS3582**. That's the "origin AS."
- In our case, 128.223.142.13 belonged to UO and AS3582 also belonged to UO, so we can feel fairly comfortable that the 128.223.142.13 address was being used by an appropriate party. If bad traffic was seen from 128.223.142.13, UO should indeed be the ones to hear about it.
- But what if we'd seen some other AS other than 3582? **If/when a network address block gets hijacked, the ASN we'd normally expect to see ends up getting replaced with a different ASN, the ASN of the network that's injecting an unauthorized route for the hijacked netblock.**
- **Are YOU checking the ASNs that are associated with the IPs connecting to YOUR servers?**

Doing IP==>ASN Checks *En Masse*

- While doing a traceroute from a looking glass is a handy way of illustrating the concept of network paths and ASNs, it won't scale as a solution for checking thousands (much less millions!) of IP addresses per hour.
- Fortunately, a more scalable option is available – you can simply query the $REVIP.asn.routeviews.org zone via DNS for txt records, either with dig or with host, or via equivalent programmatic calls. For example, to check to see what ASN is associated with 128.223.142.13, you'd say:

```
% host -t txt 13.142.223.128.asn.routeviews.org
13.142.223.128.asn.routeviews.org text "3582" "128.223.0.0" "16"
```

  (Non-routed IPs return a magic "AS" value of 4294967295)
- For those who want to run that ASN zone from a local DNS server, you can retrieve a copy of the routeviews ASN zone: ftp://archive.routeviews.org/dnszones/originas.zone (bzip2 compressed copies are also available in that same directory)

What's that "128.223.0.0" & "16"?

- *The routeviews data shown in the example on the previous page provided an ASN, but it also returned two other values: "128.223.0.0" & "16" – what are those all about?*
- Those values show the **origin address** and the **CIDR length** associated with that IP addresses "most specific encompassing prefix." Decoding that just a bit…
- Routing rules in the global routing table normally don't specify routes on a host-by-host basis, they normally work with larger chunks. Those chunks are normally referred to as "prefixes."
- In our example, the most specific route encompassing 128.223.142.13 was 128.223.0.0/16, or the range of addresses beginning at 128.223.0.0 and going through 128.223.255.255 (65,536 addresses in all).
- Note: just checking 128.223.142.13 won't detect any more specific routes for IPs other in the 128.223.0.0/16 block.

Table of Common CIDR Prefix Lengths

- /8 ==> 16,777,216 addresses
  /9 ==> 8,388,608
  /10 ==> 4,194,304
  /11 ==> 2,097,152
  /12 ==> 1,048,576
  /13 ==> 524,288
  /14 ==> 262,144
  /15 ==> 131,072
  /16 ==> 65,536
  /17 ==> 32,768
  /18 ==> 16,384
  /19 ==> 8,192
  /20 ==> 4,096
  /21 ==> 2,048
  /22 ==> 1,024

/23 ==> 512
/24 ==> 256
/25 ==> 128
/26 ==> 64
/27 ==> 32
/28 ==> 16
/29 ==> 8
/30 ==> 4
/31 ==> 2
/32 ==> 1

Where Does The IP To ASN Zone Data Come From?

- The IP to ASN zone is produced by Routeviews, a project that Dave Meyer has here at the University of Oregon. See http://www.routeviews.org/
- A publicly available command line interface is also available:

```
% telnet route-views.routeviews.org
Username: rviews
route-views.oregon-ix.net> show ip bgp 128.223.142.13
BGP routing table entry for 128.223.0.0/16, version 68025
Paths: (45 available, best #44, table Default-IP-Routing-Table)
  6395 3356 3701 3582
    216.140.2.59 (inaccessible) from 216.140.2.59 (216.140.2.59)
      Origin IGP, metric 20, localpref 100, valid, external
      Community: 6395:200
  16150 3549 3356 3701 3582
    217.75.96.60 from 217.75.96.60 (217.75.96.60)
    Origin IGP, metric 0, localpref 100, valid, external
    Community: 3549:2681 3549:31528 16150:63392 16150:65321
    16150:65326 [etc]
```

Interpreting Routeviews CLI Output

- Routeviews shows network paths from 45 different points on the Internet (just like our two sample traceroutes, which differed when run from Seattle and from Switzerland)
- Just like our sample traceroutes, the **LAST (rightmost) ASN** shown is the one that will usually be the one of interest
- Sometimes we do care about who's **UPSTREAM** of the last ASN; using the command language interface makes it easy to see that, too. See also the Routeviews **aspath** zone:

```
% host -t txt 13.142.223.128.aspath.routeviews.org
13.142.223.128.aspath.routeviews.org text "22388 11537 4600 3582"
"128.223.0.0" "16"
```

- Other CLI queries are also possible via routeviews, e.g.:

```
route-views.oregon-ix.net> show ip bgp regex _3582$
```

will show a list of all prefixes originated by AS3582

Why Does Routeviews Bother Showing Routing Data from 45 Sites?

- Hosts on the Internet may be multihomed (multihoming is the practice of connecting to the Internet via multiple service providers). For example, a large corporation may purchase connectivity from Level3, from Sprint, and from Cogent in an effort to get provider diversity and redundancy. When you do a traceroute from the one site to the other site, you'll only see ONE such path into a site.
- The Routeviews CLI shows you the paths into a site from 45 different locations, thereby maximizing the chance that you'll see multiple (all? most?) different routes into a site of interest, thereby giving you a better sense of how that site is connected to the Internet at large. Instead of saying, "That site connects to the Internet via Level3," you may learn that it connects via Level3, AND Sprint AND Cogent, for example.

ICMP, BGP and TCP/UDP Traffic

- Occasionally folks may find a situation where the path shown by traceroute (an ICMP-based tool) differs radically from the path shown in routeviews BGP data, or in other cases, actual TCP or UDP application traffic follows a radically different path than the path implied by BGP data. There may be multiple reasons for this, including (just to mention a few)
  -- BGP reports the *signaling* path associated with routing update messages, which will usually be the same as the traffic *forwarding* path (but sometimes may not be)
  -- Traffic may be selectively filtered, tunneled or otherwise handled in ways which can easily obfuscate or mislead
  -- there are a number of other possible causes of anomalies.
- Nice discussion of this can be found in Mao et. al.'s "Towards an Accurate AS-Level Traceroute Tool,"
  http://www.acm.org/sigs/sigcomm/sigcomm2003/papers/p365-mao.pdf

One Last Note for This Section: ASN-tag IPs As You See Them

- Routing information is time sensitive/dynamic. If you wait to check the routing associated with an IP address, during that interval the routing may have changed, and you may tag an IP with the wrong ASN. For example, you may want to add ASN tags to mail at the time the email is received. If it turns out you don't need the ASN info, it is just one more header you've added to the mail (which you can ignore); if you do need or want the ASN data, you'll be dang glad it's there.
- Note: the ASN zone updates/reloads at 11:45 and 23:45 UTC; the plans is to increase that frequency in the future...
- Karsten Self has released procmail code he uses to tag his incoming mail at delivery time with a X-ASN: header at `http://linuxmafia.com/~karsten/Download/procmail-asn-header` Similar things can be done for other applications.

III. Miscreant Motivations for Doing Address Space Hijackings

Why Would a Miscreant Not Just Get Their Own Legitimate Address Space?

- Bad guys and bad gals have several problems when it comes to getting and using legitimate address space…
  -- as quickly as they get new address space and begin to use it for evil purposes, that space gets blocked/filtered (at which point the usability of that space drops dramatically)
  -- if miscreants get address space legitimately, there's an administrative trail leading right back at 'em; very handy for law suits and criminal prosecutions!
  -- requests for more address space need to be justified, and ***"I've heavily abused all the network address space I've currently got, and now that space is all heavily filtered damaged goods I can no longer use,"*** doesn't "cut it"
  -- miscreants want to "fly under the radar" if they can, and concentrated abuse from one's own IP space stands out

So What's a Miscreant, Such As A Spammer, To Do?

- Well, we know that spammers will try to send their spam via spam zombies, but that's not working as well for them as it used to.
- Is there anything **else** they could do? Well, if you're a spammer and not particularly worried about doing bad things, the "expedient" thing to do might be to just **take some IP addresses that don't belong to you** (if you're accustomed to hijacking PCs and using them as spam zombies, hijacking network address blocks probably won't feel particularly daring).
- Heck, stealing otherwise unused address space may be **LESS** legally risky than hijacking PCs and turning them into zombies…

Taking That Which Doesn't Belong to You *Is* Stealing, Right?

- Hijacking a netblock is clearly "wrong" and "bad," but a non-rhetorical, non-flip, truly serious question…

  ***Is** hijacking a not-otherwise-in-use netblock a **crime**? If so, is it a felony or misdemeanor? What **statute** is being violated? **How many** netblock hijackers have been successfully prosecuted to-date?*

- Would there be the willpower to actually prosecute a netblock hijacker (or would this be just yet another technical violation that never actually gets charged)?
- Will this require some really grotesque routing-based denial of service incident to motivate official attention and new law?
- And what about netblock hijackings ***overseas***?

CAN-SPAM And Hijacked IP Addresses

- 18 USC Sec. 1037. Fraud and related activity in connection with electronic mail

  (a) IN GENERAL- Whoever, in or affecting interstate or foreign commerce, knowingly--

  * * *

  (5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses, or conspires to do so, shall be punished as provided in subsection (b).

  (b) PENALTIES- The punishment for an offense under subsection (a) is--

  (1) a fine under this title, imprisonment for not more than 5 years, or both, if--

  (A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

  (B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

Zero Prosecutions…

- To the best of my knowledge, that's a section of the United States criminal code that's never been the basis of any federal prosecution.
- Happy to hear about examples I may have missed in this area…

Well, Even If Hijacking A Netblock Isn't Something That's Routinely Prosecuted...

- Wouldn't someone at least **notice/care** if a miscreant hijacked a prefix?
- Maybe yes, maybe no. It depends in part on what prefixes the miscreant announces, and how they use/announce it.

Announcing an Already-Used Prefix

- If a miscreant announces an **already-used** prefix, this **will** typically end up being noticed because at least some legitimate traffic will be diverted from its intended destination, and connectivity to the normal hosts using that prefix will break.[1] Of course, one could imagine a miscreant **intentionally** announcing an already-used prefix as part of a denial of service attack, or as part of an effort to obtain traffic to sniff, etc. (see RFC4272 at 1-2) but for the purpose of this spam-oriented discussion, we'll disregard those possibilities.
- Given that the miscreant wants to "fly below the radar," his/her quest becomes one of finding an address block, or at least part of an address block, that's **not** currently in use.

---

1. How much traffic will be diverted depends on whether the unauthorized user announces a prefix that is of the same specificity or granularity as the real user or one or more more-specific prefixes, as well as a variety of other factors.

Unallocated/Reserved Space?

- Some folks may assume that when we talk about address space that's "not currently in use" we're talking about IP address space that's reserved or which has yet-to-be-allocated by IANA ("bogon space").
- See http://www.iana.org/assignments/ipv4-address-space and http://www.cymru.com/Documents/bogon-list.html
- Unallocated/reserved space would not work well for stealthy spammer use because unallocated/reserved space is well documented, widely filtered, and any use of that space will typically be quickly noticed and publicized (see the next slide for examples where unallocated/reserved space is reportedly in use, generally/presumably with no malicious intent).

http://thyme.apnic.net/ap-data/2006/12/03/0400/mail-global

Advertised Unallocated Addresses

Network	Origin AS	Description
132.0.0.0/10	721	DLA Systems Automation Center
137.0.0.0/13	721	DLA Systems Automation Center
158.0.0.0/13	721	DLA Systems Automation Center
172.33.1.0/24	7018	AT&T WorldNet Services
176.16.0.0/16	7908	Comsat Argentina S.A.
192.44.0.0/24	5501	Fraunhofer Gesellschaft
192.44.0.0/19	702	UUNET - Commercial IP service
192.70.164.0/24	25689	National Research Council of
192.172.0.0/19	721	DLA Systems Automation Center

Forgotten/Ignored Prefixes

- Most persistent hijackings are associated with forgotten/ignored "zombie" network prefixes which bad guys notice, "resurrect," and then begin to use as their own.
- Forgotten/ignored prefixes are often the result of legacy address allocation provided to a now-out-of-business company. When that company folded or was acquired, if its address space was no longer required, it should have been returned to ARIN/RIPE/APNIC/etc. (e.g., see http://www.arin.net/policy/nrpm.html at 8.1) but often the employees of a company in "freefall" have other, more personal, priorities.
- Since the now-out-of-business company doesn't exist any more, and thus has no networking staff, and thus no one to notice/complain that its IP address space is being used w/o authorization, the hijackers have the addresses they want.

Another Possibility: Underutilized Prefixes

- Underutilized prefixes arise when an entity has access to more address space than it currently needs. When that's the case, a miscreant may "borrow" a chunk of that address space that's not currently being actively used, and begin to advertise that space via a more specific route for the hijacker's own nefarious purposes.
- So what's the role of universities, gigapops, regional optical networks and Internet2 when it comes to preventing the announcement of unauthorized prefixes?

IV. Hijacked Blocks, Universities, Gigapops, Regional Optical Networks and Internet2

"I've Got A New Prefix I'd Like to Route"

- Most edu's connecting to I2 take great care to only announce their own IP address space, or portable address space legitimately controlled by their partners, filtering all other prefixes which may be seen from a downstream source. [Most commercial ISPs are also quite careful with their prefixes, too.]

- Internet2 helps double check that process by reviewing all prefixes which a connector asks to announce. Prefixes are specified via the PDF form that's at: http://abilene.internet2.edu/AbilenePrefix2.pdf

- Prefixes seen via networks with which I2 peers with are **NOT** filtered.

Whois and Hijacked Blocks

- Because all conscientious providers check whois details when asked to route a new prefix, some IP address hijackers create **new** entities with names that "look like" the name of a company that originally received a prefix they want to use. They then attempt to **socially engineer** the registrar into "updating" the whois data that's associated with the targeted prefix to use the look-alike company's contact information.
- Bad guys have historically also attempted to **mechanically update** whois data when that data is only secured by MAIL-FROM authentication, but this is now less commonly possible. See: http://www.ripe.net/db/news/mailfrom.html http://www.apnic.net/meetings/14/sigs/db/minutes.html http://www.arin.net/CA/ca_faq.html
- Nice historical discussion of mntner object security at www.trustmatta.com/downloads/Matta_NIC_Security.pdf

Routing Registries

- ISPs sometimes require all customer prefixes to be registered in a routing registry ("RR"), either one run by the ISP itself, or in a community RR serving a wider constituency.
- A list of routing registries is available online at http://www.irr.net/docs/list.html
- You can query the RADB at http://www.radb.net/
- RR's usually use "RPSL" to express objects in the database; see RFC2622 and RFC2650 for information about RPSL.
- Among other data, routing registries list routes (or route-sets) and the ASNs that should be originating those routes.
- When use of a RR is required, and that data is kept accurate and current, ISPs can use that data to mechanically build prefix filters (e.g., using tools from the IRRToolSet) and thus avoid accidentally accepting unauthorized/typo'd prefixes
- Unfortunately, use of RRs is not universally compulsory.

Routing Registries and Internet2

- *Once upon a time…* there used to be an active I2 Routing Working Group, and one of the good projects which that group worked on was an I2 routing registry. See

  http://routing.internet2.edu/wg-meetings/20010130-I2rwg-slides/sld004.htm

  Unfortunately the service referred to is no longer in operation:

  % whois -h whois.internet2.edu AS25
  [Querying whois.internet2.edu]
  [whois.internet2.edu: Name or service not known]
  [Unable to connect to remote host]

  You *could* use an alternative routing registry, however! :-)

Detecting Route-Related Anomalies

- Routing registries can make it easy to detect routing anomalies, but we can detect some unusual things even with incomplete routing registry usage.
- For example, let us consider a brief digression: singly-homed ASN usage.

ASNs and Multihoming

- ASNs have historically been scarce resources, and as a matter of policy, ASNs are **only** supposed to be allocated to **multihomed entities** (e.g., sites with two or more upstream service providers). See, for example:

  http://www.ripe.net/docs/asn-assignment.html which states:

  > "Current guidelines require a network to be multi-homed for an AS Number to be assigned."

So Are There ASNs Which Aren't Multihomed?

- **You bet.** Go to http://www.cidr-report.org/bgp-originas.html and scroll down to the bottom. Now "drill down" (click on) some of those toward-the-bottom-of-the-list ASNs. Notice how many of them have only a single upstream provider? Unless they have additional upstream connectivity which isn't externally discernable, those apparently single-homed sites should not have their own ASN.
- You may ask, "Heck, who cares if they get an ASN or not? What's it to you?" Well, 16 bit traditional ASNs are scarce (there are only 64510 available) and unfortunately we've been blowing through them at a very high rate of speed.
- Think about ASNs consumed by those single homed sites when you can no longer just do 16 bit ASNs, and you need to begin upgrading gear to deal with 32 bit ASNs…

For Those Not Following 32 Bit ASNs:

- Fwd: The IESG Approved the Expansion of the AS Number Registry (Mon, 27 Nov 2006)
  http://www1.ietf.org/mail-archive/web/ietf/current/msg44519.html

- BGP Support for Four-octet AS Number Space
  http://www.ietf.org/internet-drafts/draft-ietf-idr-as4bytes-12.txt

32 Bit Timeline…

5.1 16-bit and 32-bit AS Numbers

- Commencing 1 January 2007, ARIN will process applications that specifically request 32-bit only AS Numbers and assign such AS numbers as requested by the applicant. In the absence of any specific request for a 32-bit only AS Number, a 16-bit only AS Number will be assigned.

- Commencing 1 January 2009, ARIN will process applications that specifically request 16-bit only AS Numbers and assign such AS Numbers as requested by the applicant. In the absence of any specific request for a 16-bit only AS Number, a 32-bit only AS Number will be assigned.

- Commencing 1 January 2010, ARIN will cease to make any distinction between 16-bit only AS Numbers and 32-bit only AS Numbers, and will operate AS number assignments from an undifferentiated 32-bit AS Number pool.

- Terminology

  "16-bit only AS Numbers" refers to AS numbers in the range 0 - 65535

  "32-bit only AS Numbers" refers to AS Numbers in the range 65,536 - 4,294,967,295

  "32-bit AS Numbers" refers to AS Numbers in the range 0 - 4,294,967,295

Source: http://www.arin.net/policy/nrpm.html#five1

"Defensively Deaggregated" Announcements

- One last thing that should be mentioned in the context of ISPs and route hijacking is what might be called "defensive deaggregation" of routes in an effort to prevent hijackers from announcing more specific routes.
- Recall that the most specific match in the routing table will be used to route bits. Thus, if you announce a nicely aggregated /19, but a hijacker announces two /20's, his more specific routes will "win" and traffic will flow toward his network rather than toward yours. To proactively discourage this, some providers intentionally deaggregate their own prefixes and announce "more specifics" (e.g., often a whole pile of /24's).
- Obviously, this is **NOT desirable** when it comes to containing routing table bloat, but a (perception) of private benefits may once again outweigh public costs.

Route Filtering Policies

- If an ISP announces a pile of /24's, you might wonder what would keep a miscreant from simply announcing a larger pile of more specific /25's, etc. ISP **route filtering policies** normally kick in to help limit overly specific routes. Example: http://www.ip-plus.net/technical/route_filtering_policy.en.html
- Many providers ignore routes more specific than a /24
- It is also common for providers to reserve the right to aggregate (where feasible) more specific announcements they see from customers.
- Nonetheless, you should not be surprised to see LOTS of deaggregated prefixes announced, e.g., check out the CIDR Report: http://www.cidr-report.org/ For example, on 3 Dec 2006, AS4134 could have announced 282 routes, but gave the Internet 1206 less-aggregated routes instead…

[Stipulated: There are/can be legitimate technical reasons for announcing more specifics]

Route Filtering on Abilene

- Prefix Length Routing Policy
  http://www.abilene.iu.edu/abilene/documentation/
  policy-statements/prefix-length-routing-policy.html

  The following was sent to the Abilene operations list on 17 January 2003.

  Abilene encourages its connectors to aggregate advertised prefixes as an internet best practice. Therefore, we will accept approved IPv4 prefixes up through /27. However, we realize that in unusual special cases, prefixes more specific than /27 must be advertised, so if there is an important reason a prefix more specific than /27 must be advertised, explain your need and we will try to accomodate you.

  Since connectors are the only ones from whom specific prefixes are accepted, this policy applies so far only to Abilene connectors (i.e. not to peer networks).

"Accidental" Classful Summarization

- Feedback from a person who looked at an earlier version of this talk included the comment that the reason they intentionally deaggregate is to protect against problems with people who ended up "accidentally" doing bgp auto-summary with disastrous results.
- Grease pencil on a match book version: downstream customer ended up with two different widely separated /24's, router was set to do BGP auto-summary, and customer ended up announcing a rather overlarge classful prefix.
- Nice discussion about auto-summary from Cisco at "How does BGP behave differently with auto-summary enabled or disabled?" www.cisco.com/warp/public/459/bgpfaq_5816.shtml#five
- Fortunately auto-summary is now disabled by default! :-)

Is Anyone Watching For Hijackings?

- It would be great if ARIN/RIPE/APNIC/LACNIC or some other technical body was watching the entire Internet's address space for hijackings, but in general they are neither charged nor equipped to generally do so (RIPE does deserve credit for running an ASN-by-ASN opt-in route monitoring service called myASN, however)
- To the best of my knowledge, the federal government also doesn't monitor the Internet routing table looking for hijackings, or if they do do so, they don't do so in any general/publicly advertised way.
- Just as in many things spam- or network security-related, private parties carry the load…:-)

CompleteWhois, Spamhaus DROP, Etc

- For example, the **CompleteWhois** folks have a list of over 125 known or suspected netblock hijacks documented at http://www.completewhois.com/hijacked/index.htm ; see also the **Spamhaus DROP** (Do not Route Or Peer) Advisory Null List (http://www.spamhaus.org/drop/) and the **UNM Internet Alert Registry** (http://cs.unm.edu/~karlinjf/IAR/index.php)
- Two other route monitoring resources are **RIPE's myASN** service (http://www.ris.ripe.net/myasn.html), and the Colorado State's **Prefix Hijack Alert System (PHAS)** http://netsec.cs.colostate.edu/phas/
- There are even commercial projects such as **Renesys' Routing Intelligence Service**, see http://www.renesys.com/products_services/routing_intelligence.shtml

Who Has Announced Hijacked Netblocks Flagged by CompleteWhois?

- In order for a hijacked netblock to be useful, it needs to be announced by an ISP, at which point it becomes associated with that ISP's Autonomous System Number. The next slide shows ASNs that were listed by CompleteWhois as having announced one or more potentially hijacked netblocks.
- Couple of things to note:
  -- some of those ASNs are familiar and unquestionably "white hat;" others may be comparatively unknown or may have less uniformly favorable reputations.
  -- ASNs were mapped to entity names this Summer; it is possible that some ASNs have changed to an unrelated 3rd party since the time that they were listed (although most will have a stable assignment and usage history)

ASNs from CompleteWhois' List

3491:	BTNA (VA)
5042:	Discnet (CT)
6216:	Turfway Park (KY)
7438:	Telefonica Data Mexico
7474:	SingTel Optus Pty Ltd (NSW Aus)
8001:	NAC (NJ)
8121:	TCH Network Svcs. (CA)
8129:	CAI Wireless (VA)
8143:	Publicom Corp. (FL)
8167:	TELESC (BR)
9723:	ISEEK Ltd. (Qld. Aus)
9826:	iLink.net Ltd (HK)
9929:	China Netcom Corp. (CN)
10741:	Wam Net Entr. Inc. (FL)
10912:	Internap (GA)
13419:	2Access.net, Inc (OH)
13768:	Peer1 (NY)
13953:	Bisco Industries Inc. (CA)
14492:	DataPipe (NJ)
15188:	Diali Internet (FL)
16631:	Cogent (DC)
18747:	IFX Comm (FL)
19151:	WV Fiber LLC (TN)
20290:	Lynch Intl. (GA)
20473:	NetTransactions (NJ)
21844:	The Planet (TX)
22653:	Global Compass (GA)
22938:	BigCity Networks (TX)
23131:	Starlan Comm. (NY)
23184:	Persona Comm. (Nfld. Can.)
23401:	NAC (NJ)
23352:	Server Central Network (IL)
25847:	ServInt Corp (VA)
26522:	Netwave Tech. Inc. (NY)
26797:	SIMRAD (Norway)

[continued next slide]

ASNs from CompleteWhois' List

26857: Web Design House (NY)
26891: INGS (IN)
26978: Sterling Network Svcs (AZ)
27255: VMX, Inc. (NY)
27526: Endai Corp. (NY)
27595: InterCage, Inc. (CA)
28706: Stream TC (Ukraine)
29698: INVESTools Inc. (TX)
29713: ITV Direct Inc. (MA)
29761: OC3 Networks (CA)
29893: Bombay Co. (TX)
29994: Iskimaro (CA)
30080: Arnold Mag. Tech. (NY)

See the individual Completewhois listings
for details associated with each ASN.

Investigating a Prefix (Beyond Just Finding What ASN Is Announcing It)

- Unfortunately, it can be quite difficult to investigate a potentially hijacked prefix beyond finding the ASN that's announcing it:
  -- whois data may be inaccurate/questionable
  -- the announcing ISP may be less than cooperative if the hijacked block is associated with a lucrative/bad customer
  -- just as netblocks can be hijacked, ASNs can also be hijacked/used without authorization
  -- if you get "too close" the hijacked prefix may get replaced with a new one; rinse, lather, repeat
  -- working route hijacking issues will likely require the involvement of your corporation's network engineers, and may be time consuming

The Network Engineer Perspective vs. The Anti-Spam Perspective

- I've come to understand that network engineers view route hijacking risks differently than anti-spammers.
- Routing geeks generally worry about someone hijacking their own prefixes, or a customer trying to slide a hijacked prefix past the local NOC's staff.
- Anti-spammers, on the other hand, care about ANY hijacked netblock that may be used to emit spam, provide spammer DNS service, host spamvertised web sites, etc.
- Some antihijacking/route-monitoring projects focus on the routing geek perspective, others follow the anti-spam perspective.
- I suggest taking each project on its own merits, because each can be valuable in different ways.

V. Transient Routing of Large Prefixes

What About Possible Short-Lived Hijackings of Large Prefixes?

- See "Short-Lived Prefix Hijacking on the Internet," by Peter Boothe, et. al. (Peter's with the UO CIS Department), http://www.nanog.org/mtg-0602/pdf/boothe.pdf which states that there were between **26 and 96 successful prefix hijackings in December 2005** (95% confidence level)
- Do spammers use those sort of short-lived prefix hijackings? Well, seee "Understanding the Network Level Behavior of Spammers," A. Ramachandran and Nick Feamster, Georgia Tech, http://www.nanog.org/mtg-0606/pdf/nick-feamster.pdf :

  "Common short lived prefixes and ASes
  61.0.0.0/8 4678
  66.0.0.0/8 21562
  82.0.0.0/8 8717"

How Would Announcing x/8 Work?

- Any traffic addressed to parts of x/8 which are NOT covered by some other route would go to a general route covering x/8.
- Because that's a very large announcement, any more specific announcement will be preferred over it; if you're someone who's legitimately announcing some smaller chunk of x/8 you'll never notice the larger covering announcement.
- Spammers announcing the large covering x/8 WILL have the ability to use onesie-twosie addresses scattered throughout all the otherwise unrouted parts of "their" large prefix… no need to cluster all their spam traffic in a single, compact, easily-identified and easily-filtered range.
- "Nice" side effect: complaints will also often end up being directed to inappropriate parties, or just fall on the floor.
- This is obviously potentially very, very, evil.

"Problems" of Advertising Large Blocks

- There's only a small number of /8's that can potentially be announced.
- If you know to look for those announcements, it is awfully easy to spot them.
- Once you know they exist, you can work on getting them filtered or otherwise eliminated at a technical level.
- Other bad guys can "take" "your" /8 by advertising more specific covering routes, such as /9's (or /10's, or /11's, etc.)
- There's one other issue that sometimes is raised when the possibility of doing transient announcement of large blocks comes up… damping.

What Do We Currently (12/2/06) See For 61/8?

```
% telnet route-views.oregon-ix.net
Username: rviews
route-views.oregon-ix.net>show ip bgp 61.0.0.0/8
BGP routing table entry for 61.0.0.0/8, version 531810282
Paths: (3 available, no best path)
  Not advertised to any peer
  3303 15412 4678 (history entry)
    164.128.32.11 from 164.128.32.11 (164.128.32.11)
      Origin IGP, localpref 100, external
      Community: 3303:3008 15412:603 15412:621 15412:803 15412:1301
      Dampinfo: penalty 928, flapped 1 times in 00:01:43
  7500 2518 4678 (history entry)
    202.249.2.86 from 202.249.2.86 (203.178.133.115)
      Origin IGP, localpref 100, external
      Dampinfo: penalty 1964, flapped 3 times in 00:15:32
  2497 4678 (history entry)
    202.232.0.2 from 202.232.0.2 (202.232.0.2)
      Origin IGP, localpref 100, external
      Dampinfo: penalty 488, flapped 1 times in 00:15:36
```

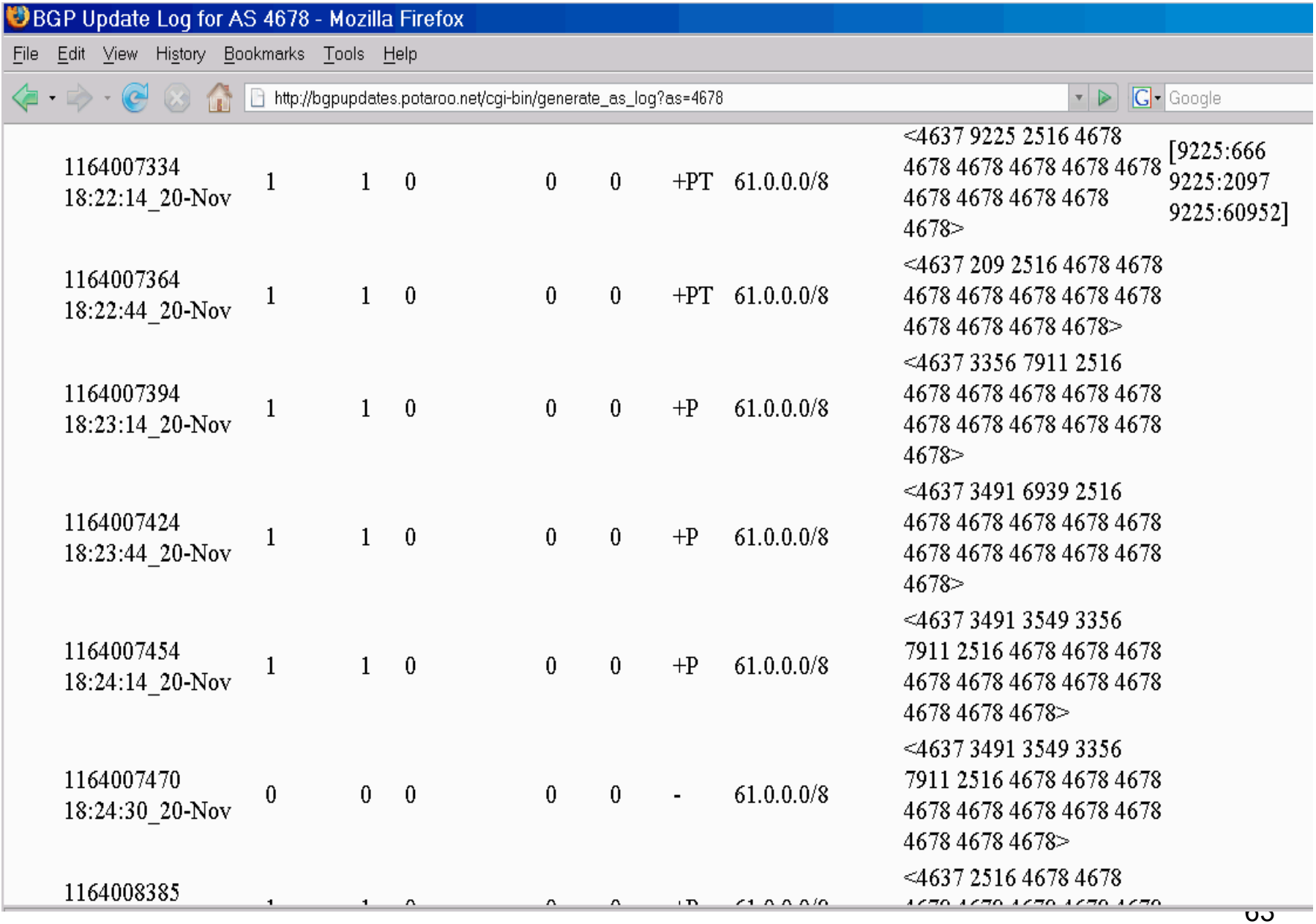
What Do We Know About The Introduction and Withdrawal of These Routes Over Time?

- If an announcement is put up just long enough for a brief spam run, only to be torn down immediately thereafter, and that behavior gets repeated, as hypothesized by some, we should see those changes show up in a BGP updates log, such as the web-based one that's offered by Potaroo…

- For example, see the update report for AS4678 on the following slide…

  `http://bgpupdates.potaroo.net/cgi-bin/generate_as_log?as=4678`

  Sure enough, interesting announcement and withdrawal activity is seen for that ASN (although we have no way of knowing if that activity is associated with spam)



1164007334 18:22:14_20-Nov	1	1	0	0	0	+PT	61.0.0.0/8	<4637 9225 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678>	[9225:666 9225:2097 9225:60952]
1164007364 18:22:44_20-Nov	1	1	0	0	0	+PT	61.0.0.0/8	<4637 209 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678>	
1164007394 18:23:14_20-Nov	1	1	0	0	0	+P	61.0.0.0/8	<4637 3356 7911 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678>	
1164007424 18:23:44_20-Nov	1	1	0	0	0	+P	61.0.0.0/8	<4637 3491 6939 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678>	
1164007454 18:24:14_20-Nov	1	1	0	0	0	+P	61.0.0.0/8	<4637 3491 3549 3356 7911 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678>	
1164007470 18:24:30_20-Nov	0	0	0	0	0	-	61.0.0.0/8	<4637 3491 3549 3356 7911 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678>	
1164008385								<4637 2516 4678 4678	

Route Flap Damping

- Something to ponder: if the bad guys inject a route for a short period of time and then withdraw it, and then re-advertise it repeatedly, they may trigger **route-flap damping.** Damping holds down, or suppresses, an oscillating route for a period of time. See RFC2439, November 1998.
- Route-flap damping was introduced to improve the stability of the Internet core's routing table and to control the CPU load placed on core routers, and has been widely deployed.
- If spammers are rapidly introducing and withdrawing routes, per Feamster's talk, wouldn't they get damped? Maybe, maybe not. For example, the RIPE Routing Working Group has now recommended that ISPs NOT do damping (see http://www.ripe.net/ripe/docs/ripe-378.html). See also http://www.nanog.org/mtg-0210/ppt/flap.pdf
- Obviously, at least in the 61/8 case, we **do** see damping.

What To Make of Those Route Flaps?

- If you advertise a route for whatever's not more specifically routed within a large prefix, you may want to make sure you have a **LOT** of bandwidth available to absorb random packets that will likely end up coming your way… failure to do so might conceivably result in starvation of the control plane (but see "BGP Vulnerability Testing: Separating Fact from FUD," http://www.nanog.org/mtg-0306/pdf/franz.pdf at pp.16).
- Then again, this flapping might be caused by something else entirely (see, for example, "A Study of BGP Origin AS Changes and Partial Connectivity," by Ratul Mahajan, et. al., http://www.cs.washington.edu/homes/ratul/bgp/nanog.pdf)
- Widespread route-flap damping, however, should limit the practical usefulness of some short-lived announcements.
- Just interested in route-flap damping data? See http://archive.routeviews.org/oix-route-views-damp/

VI. Historical Routing Data

Historical Routing Data

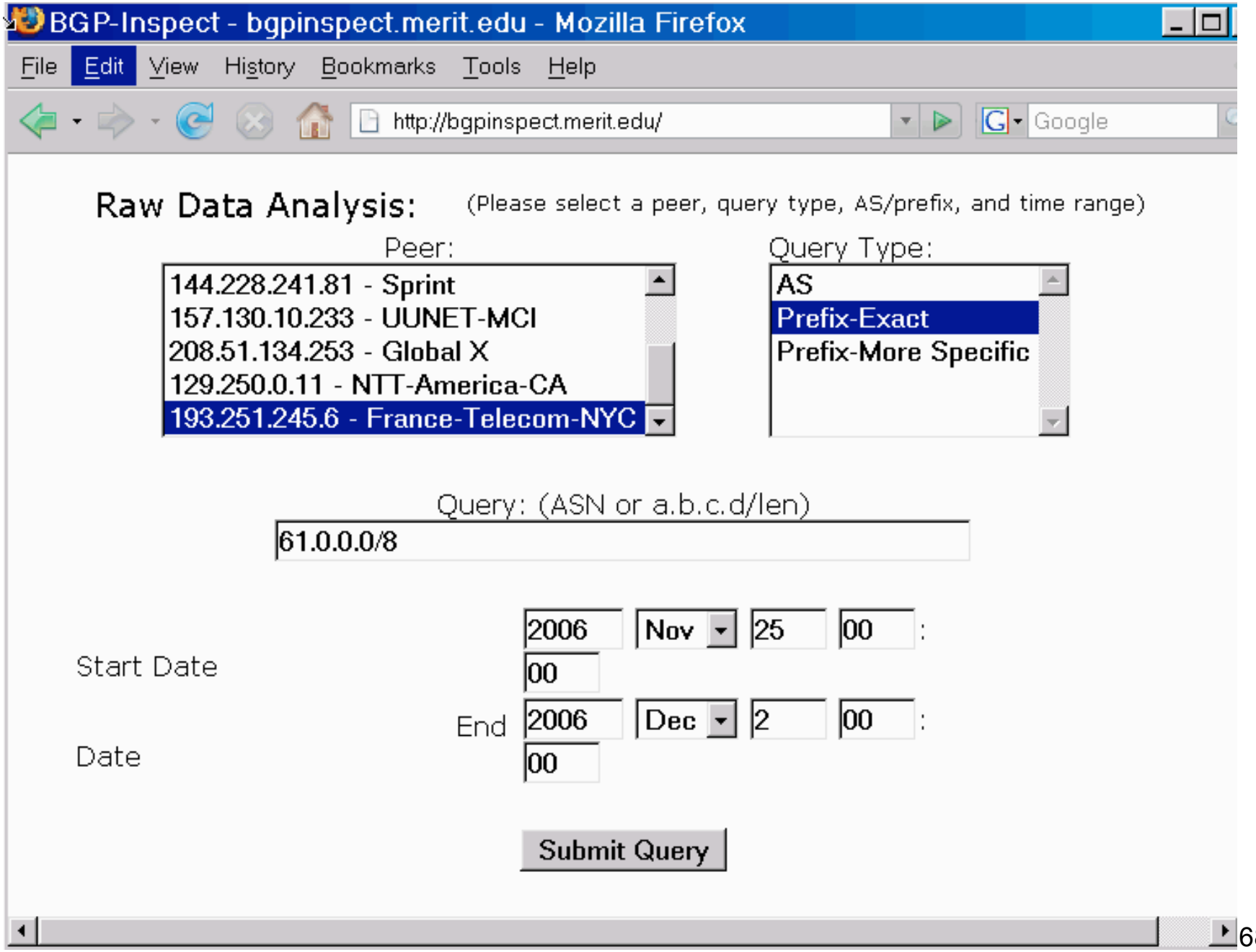
- More about Route-Views data… Route-views has both:

  -- CLI format data (similar to what you'd see if you telnet'd to route-views) routing data archived back to November 1997 (see http://archive.routeviews.org/oix-route-views/) and

  -- MRT format routing data that goes back to October 2001.

- The easiest way to access at least a limited subset of that data is via Merit's web-based BGP-Inspect-Routeviews, see **http://bgpinspect.merit.edu/**

- Sample BGP-Inspect query form, and resulting output excerpts can be seen on the following slides…


BGP-Inspect - bgpinspect.merit.edu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://bgpinspect.merit.edu/
Google
Raw Data Analysis:
(Please select a peer, query type, AS/prefix, and time range)
Peer:
144.228.241.81 - Sprint
157.130.10.233 - UUNET-MCI
208.51.134.253 - Global X
129.250.0.11 - NTT-America-CA
193.251.245.6 - France-Telecom-NYC
Query Type:
AS
Prefix-Exact
Prefix-More Specific
Query: (ASN or a.b.c.d/len)
61.0.0.0/8
Start Date
2006 Nov 25 00 : 00
End Date
2006 Dec 2 00 : 00
Submit Query

BGP-Inspect - bgpinspect.merit.edu - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://bgpinspect.merit.edu/query.php

Google

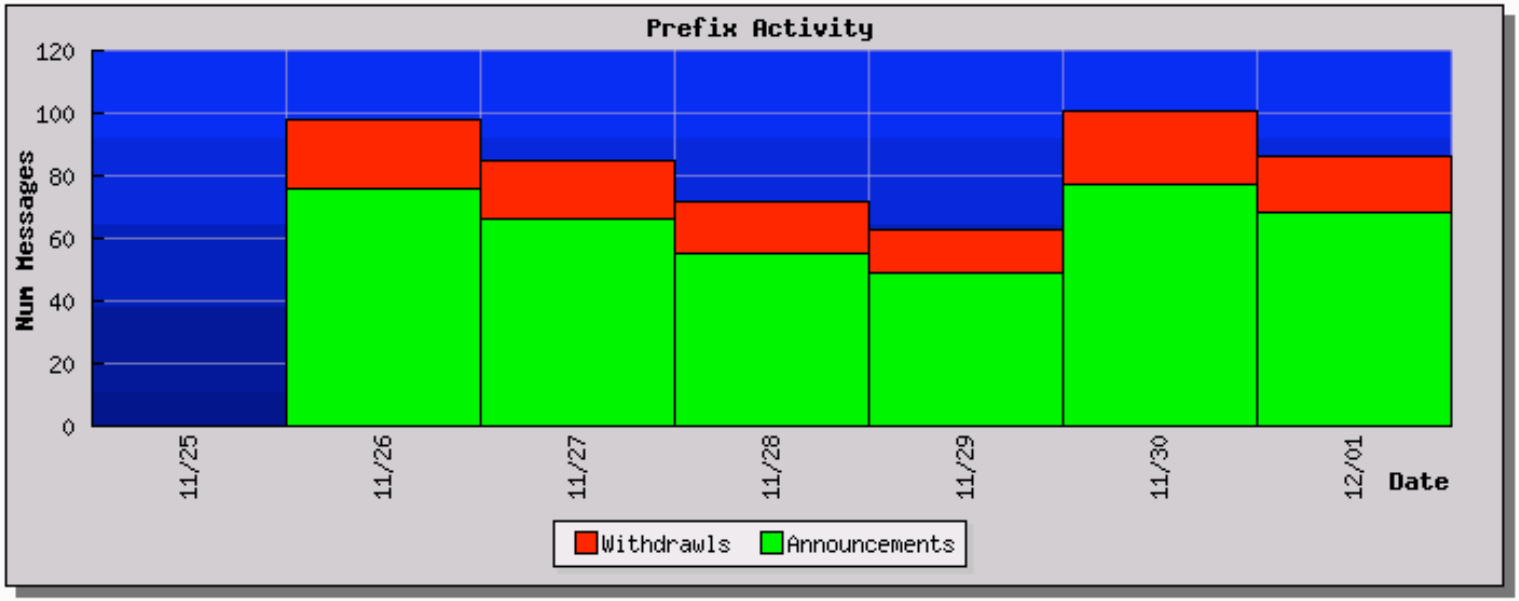
BGP-Inspect-Routeviews

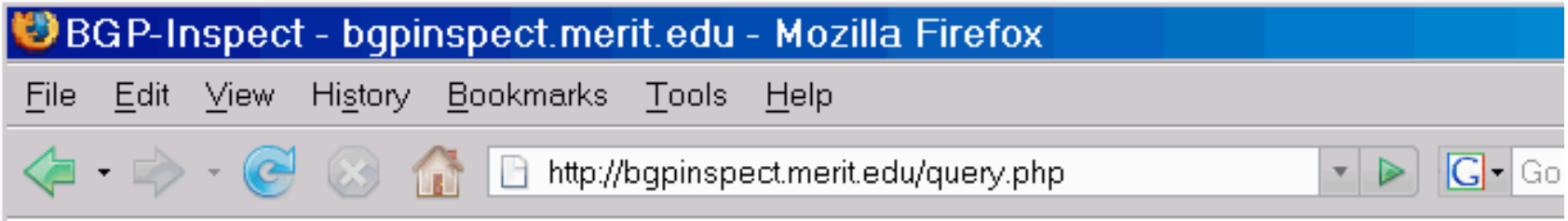
First DB Update: Aug 1, 2005,12:01 am +0000
Last DB Update: December 2, 2006, 12:14 am +0000

Home | Reports | Documentation | FAQ | About

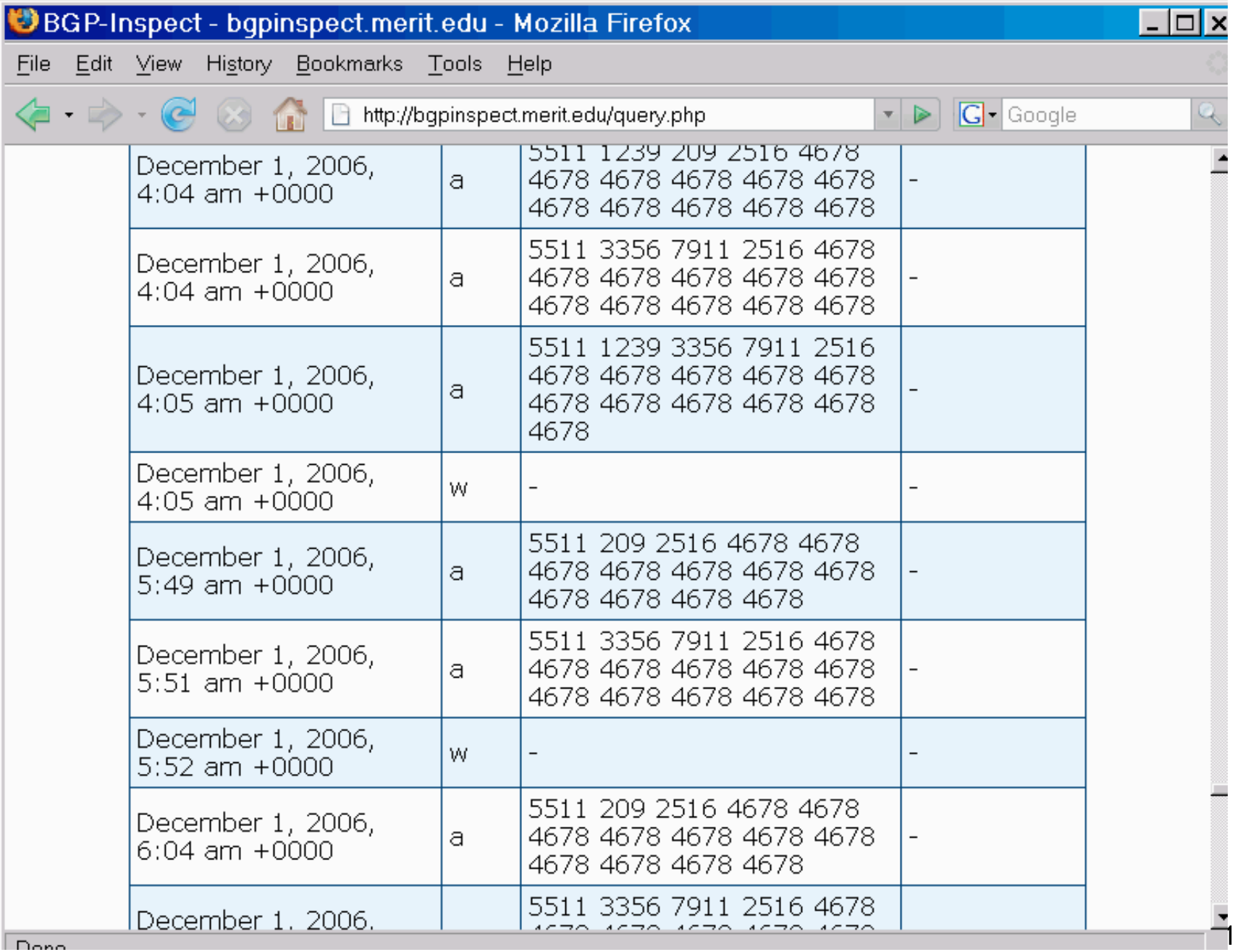
Peer: 193.251.245.6

Prefix: 61.0.0.0/8





Query Summary Statistics	
Attribute	**Value**
Query Time Range Start	November 25, 2006, 12:00 am +0000
Query Time Range End	December 2, 2006, 12:00 am +0000
Total Update Messages	505
Total Announce Messages	391
Total Withdraw Messages	114
Maximum AS Path Length	16
Minimum AS Path Length	14
Average AS Path Length	14.700769
Origin AS Changes	0
Number of Unique ASes	1
Origin ASes List	4678
Time to run query	1.729 seconds



December 1, 2006, 4:04 am +0000	a	5511 1239 209 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678	-
December 1, 2006, 4:04 am +0000	a	5511 3356 7911 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678	-
December 1, 2006, 4:05 am +0000	a	5511 1239 3356 7911 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678	-
December 1, 2006, 4:05 am +0000	w	-	-
December 1, 2006, 5:49 am +0000	a	5511 209 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678	-
December 1, 2006, 5:51 am +0000	a	5511 3356 7911 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678	-
December 1, 2006, 5:52 am +0000	w	-	-
December 1, 2006, 6:04 am +0000	a	5511 209 2516 4678 4678 4678 4678 4678 4678 4678 4678 4678 4678	-
December 1, 2006,		5511 3356 7911 2516 4678	

Some Notes About That Output

- The announcements you're seeing in that report are awfully brief (and thus most likely are not spam-related).
- Some ASNs are repeated in the reported routes; that's called "AS path prepending" and is generally done in an effort to force traffic AWAY from that route (for two equally specific routes, the one with the shorter path will usually get used)
- The last column (with dashes in it) is for community strings. Community strings are "tags" that get applied to routes by ISPs. The tags may signal the source of routes, or be used to control where routes get advertised, for example. Each ISP may use its own unique community string naming conventions. These conventions may be described on a public web page, in whois information for their ASN, or be company proprietary/undisclosed. See, for example: http://www.cenic.net/operations/documentation/BGPCommunities.shtml

Working Directly With The Routeviews Zebra Format MRT Data

- While Merit's BGP-Inspect interface is convenient for casually looking at a month's worth of data at a time, sometimes you may want to look at historical routing data over a longer time span, or as part of a script.
- Thus, you should also know that in addition to collecting data in Cisco "show ip" CLI format, Route-Views also collects data in Zebra MRT format (for example, Route-Views collects data in that format via the Equinix Route-Views box).
- Marco d'Itri's Zebra Dump Parser tools can be convenient for working with MRT format data. For a copy of his tools, see: http://www.linux.it/~md/software/zebra-dump-parser.tgz

For Example, Who's Announcing /8's?

- Assume you'd like to know who's announcing /8 network blocks. Install Marco d'Itri's Zebra Dump Parser tools if you've not already done so.
- Retrieve a sample mrt format dataset (mind the wrap!):
  % wget ftp://archive.routeviews.org/route-views.eqix/bgpdata/2006.12/RIBS/rib.20061202.2348.bz2 <== large!
- Uncompress the dataset, run it through the parser, and show any slash eight's seen:

  % bzcat rib.20061202.2348.bz2 | ./zebra-dump-parser.pl | sort | uniq | grep "\/8" <== that's "backslash slash eight"!
- The output on the next page has been annotated for ease of interpretation.
- Each /8 represents 16,777,216 IP addresses

Prefix	ASN	ASN Name
3.0.0.0/8	80	General Electric's block and ASN
4.0.0.0/8	3356	Level3's block and ASN
8.0.0.0/8	3356	ditto
10.0.0.0/8	**16559**	**RFC1918 space, RealConnect, Washington DC**
12.0.0.0/8	7018	AT&T Worldnet's block and ASN
15.0.0.0/8	71	Hewlett-Packard's block and ASN
16.0.0.0/8	71	ditto
17.0.0.0/8	714	Apple's block and ASN
18.0.0.0/8	3	MIT's block and ASN
32.0.0.0/8	2686	AT&T Global Network Services block and ASN
33.0.0.0/8	721	DOD's block and ASN
35.0.0.0/8	237	Michnet/Merit Network's block and ASN
38.0.0.0/8	174	Cogent/PSI Network's block and ASN
44.0.0.0/8	7377	Amateur Radio block, UCSD ASN (consistent POC)
45.0.0.0/8	2381	Interop Show Network block, U Wisc-Madison ASN
53.0.0.0/8	31399	Cap Debis CCS, c/o Mercedes Benz, Stuttgart block; Daimler Chrysler ASN
55.0.0.0/8	721	DOD's Block and ASN
57.0.0.0/8	**2647**	**SITA (FR)'s block, EQUANT (FR)'s ASN**
126.0.0.0/8	17676	BB Technology Japan's Block and ASN
214.0.0.0/8	721	DISA CONUS

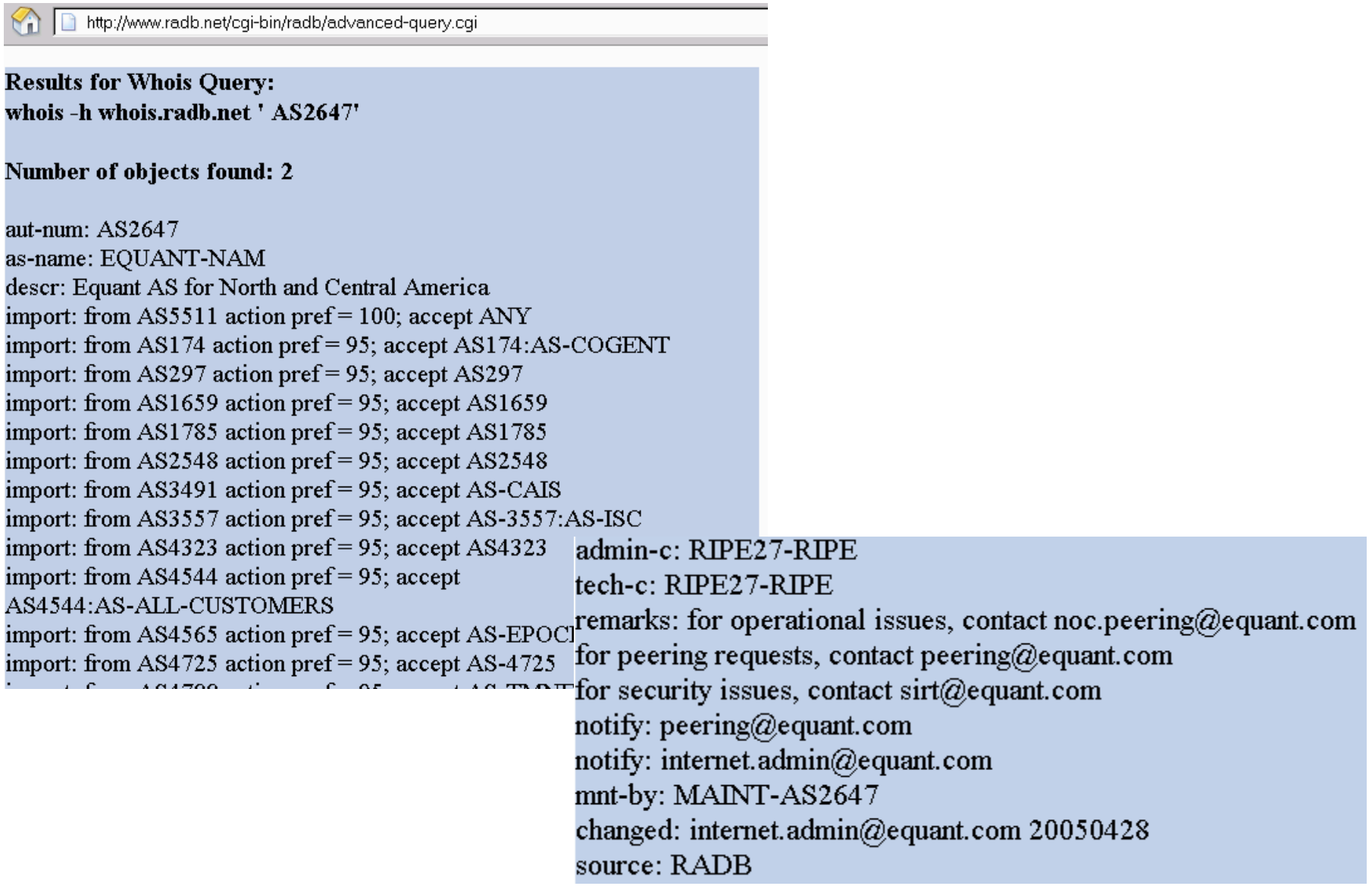
VII. A Brief Exercise
If We Have Time

[whois.arin.net]

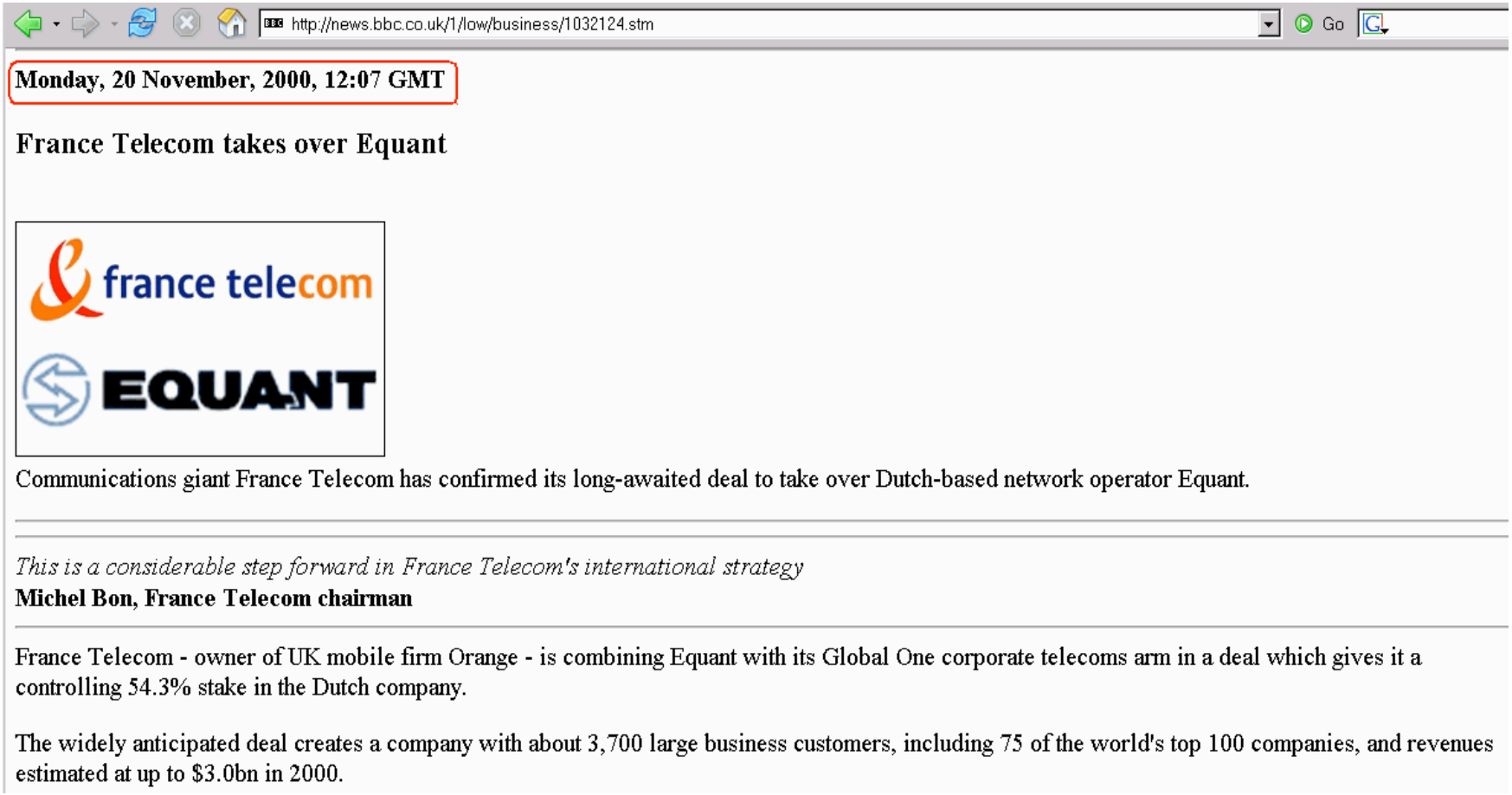
OrgName:	**SITA-Societe Internationale de Telecommunications Aeronautiques**
OrgID:	SIDTA
Address:	112 Avenue Charles de Gaulle
Address:	Neuilly, 92522 Cedex
Country:	FR
NetRange:	57.0.0.0 - 57.255.255.255
CIDR:	**57.0.0.0/8**
NetName:	SITA-A
NetHandle:	NET-57-0-0-0-1
NetType:	Direct Assignment
NameServer:	NS1.**EQUANT.NET**
NameServer:	NS2.**EQUANT.NET**
NameServer:	NS3.**EQUANT.NET**
RegDate:	**1993-06-21**
Updated:	**2000-02-02**
RTechHandle:	SITA-NOC-ARIN
RTechName:	**SITA EQUANT** Network Operations Center
RTechPhone:	+33 4 92 96 63 66
RTechEmail:	**noc@sita.net**

```
% Information related to 'AS2647'

aut-num:        AS2647
as-name:        SITA
descr:          SITA
                112 Avenue Charles de Gaulle
                Neuilly sur Seine, 92522
                FR
admin-c:        SEN01-RIPE
tech-c:         SEN01-RIPE
admin-c:        JC927-RIPE
tech-c:         JC927-RIPE
mnt-by:         ERX-AS2647-MNT
changed:        hostmaster@arin.net 19930519
changed:        hostmaster@arin.net 19990625
changed:        er-transfer@ripe.net 20020821
source:         RIPE

person:         Jimmy Chang
address:        Wisecom, Inc.
                2011 N Capital Avenue
                San Jose
                CA
                95132
                US
phone:          +1 408 935 0888
nic-hdl:        JC927-RIPE
mnt-by:         RIPE-ERX-MNT
changed:        hostmaster@arin.net 19980310
changed:        er-transfer@ripe.net 20020821
source:         RIPE

person:         SITA EQUANT Network Operations Center
address:        SITA EQUANT Network Operations Center
                Batiment Heraklion - 1041 Route des
                Dolines
                Valbonne - Sophia Antipolis, 06560
                FR
phone:          +33 4 92 96 63 66
e-mail:         noc@sita.net
nic-hdl:        SEN01-RIPE
mnt-by:         RIPE-ERX-MNT
changed:        hostmaster@arin.net 20000503
changed:        er-transfer@ripe.net 20020821
source:         RIPE
```

What Does the RADB Show Beyond the AS2647 whois data?



France Telecom Buys Equant…



Or SITA Buys Equant Application Services?

SITA announces purchase of Equant Application Services division

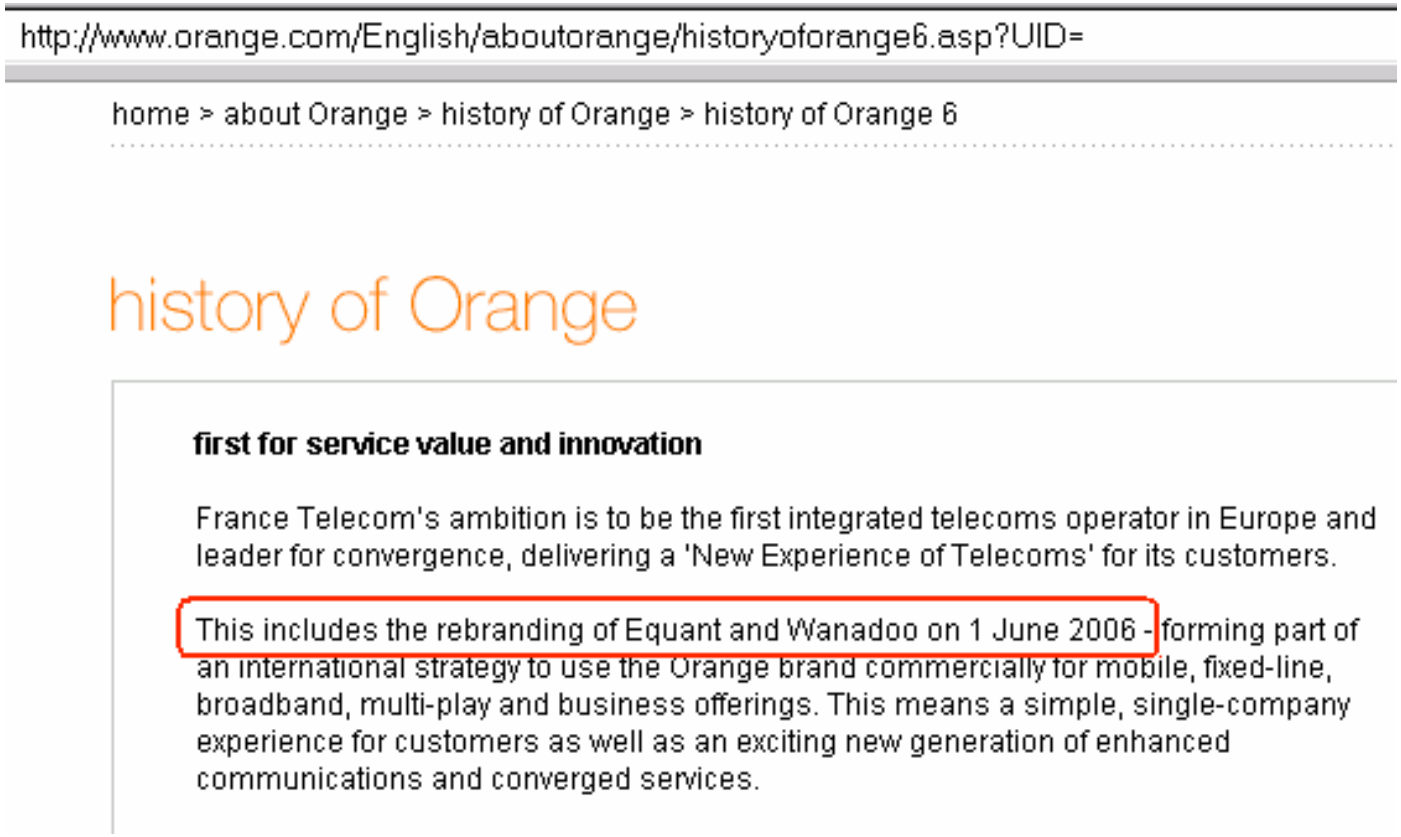
Amsterdam, The Netherlands - 1st October 2001

Acquisition enhances SITA capabilities as e-commerce integrator for the travel and transport sectors

SITA has acquired the Equant Applications Services (EAS) business unit from Equant (NYSE: ENT) (Euronext Paris: EQU). The division has 150 employees and had revenues of more than US$26 million in 2000. Financial terms of the transaction were not disclosed.

The unit will now operate as SITA Advanced Travel Solutions - a subsidiary of SITA Information Networking Computing (SITA INC) - and will continue to provide web-based applications and e-commerce integration services for the travel and transport sectors. Its focus will remain on leveraging Internet technologies to help customers reduce distribution costs and improve operational effectiveness, while ensuring the highest levels of security are maintained. The business unit has a customer base that includes companies such as Air France, British Airways, Canada 3000, Carlson Wagonlit Travel, Eurostar(UK) and Priceline.com, among many others.

Maybe Equant Is Now Orange?



http://www.orange.com/English/aboutorange/historyoforange6.asp?UID=

home > about Orange > history of Orange > history of Orange 6

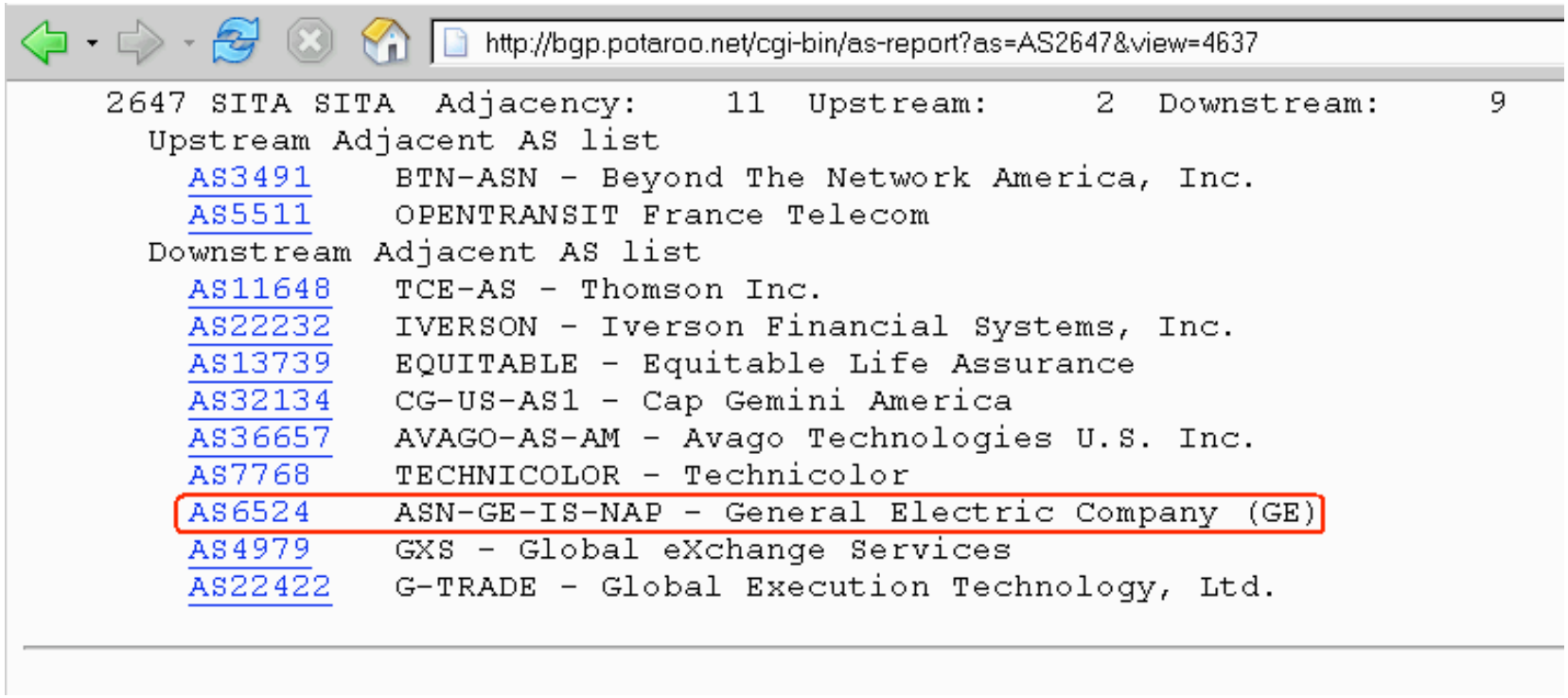
history of Orange

first for service value and innovation

France Telecom's ambition is to be the first integrated telecoms operator in Europe and leader for convergence, delivering a 'New Experience of Telecoms' for its customers.

This includes the rebranding of Equant and Wanadoo on 1 June 2006 - forming part of an international strategy to use the Orange brand commercially for mobile, fixed-line, broadband, multi-play and business offerings. This means a simple, single-company experience for customers as well as an exciting new generation of enhanced communications and converged services.

Sigh. So What ASNs Does Potaroo See Downstream of AS2647?



[whois.arin.net]

OrgName:	General Electric Company (GE)
OrgID:	GECG
Address:	Information Services (MC7D)
Address:	401 N. Washington St.
City:	Rockville
StateProv:	MD
PostalCode:	20850
Country:	US
ASNumber:	**6524**
ASName:	ASN-GE-IS-NAP
ASHandle:	AS6524
Comment:	
RegDate:	1996-05-15
Updated:	**1998-05-01**
RTechHandle:	BS3030-ARIN
RTechName:	Suskind, Barry
RTechPhone:	+1-301-340-4667
RTechEmail:	**alf_of_melmak@yahoo.com**

What Prefixes Does Potaroo See AS6524/"GE" Announce?

Rank	AS	AS Name	Current	Wthdw	Aggte	Annce	Redctn	%
6714	AS6524	ASN-GE-IS-NAP - General Electric Company	5	0	0	5	0	0.00%

AS 6524: ASN-GE-IS-NAP - General Electric Company (GE)

Prefix	(AS Path)	Aggregation Action
198.147.170.0/24	4637 5511 2647 6524	
204.90.130.0/24	4637 5511 2647 6524	
204.90.138.0/24	4637 5511 2647 6524	
204.90.187.0/24	4637 5511 2647 6524	
204.90.230.0/24	4637 5511 2647 6524	

Advertisements that are fragments of the original RIR allocation (more specifics) originated by this AS.

AS6524	5 More Specifics	5 Total Advertisements	ASN-GE-IS-NAP - General Electric Company (GE)
	198.147.170.0/24	(198.147.170.0/23)	
	204.90.130.0/24	(204.90.128.0/17)	
	204.90.138.0/24	(204.90.128.0/17)	
	204.90.187.0/24	(204.90.128.0/17)	
	204.90.230.0/24	(204.90.128.0/17)	

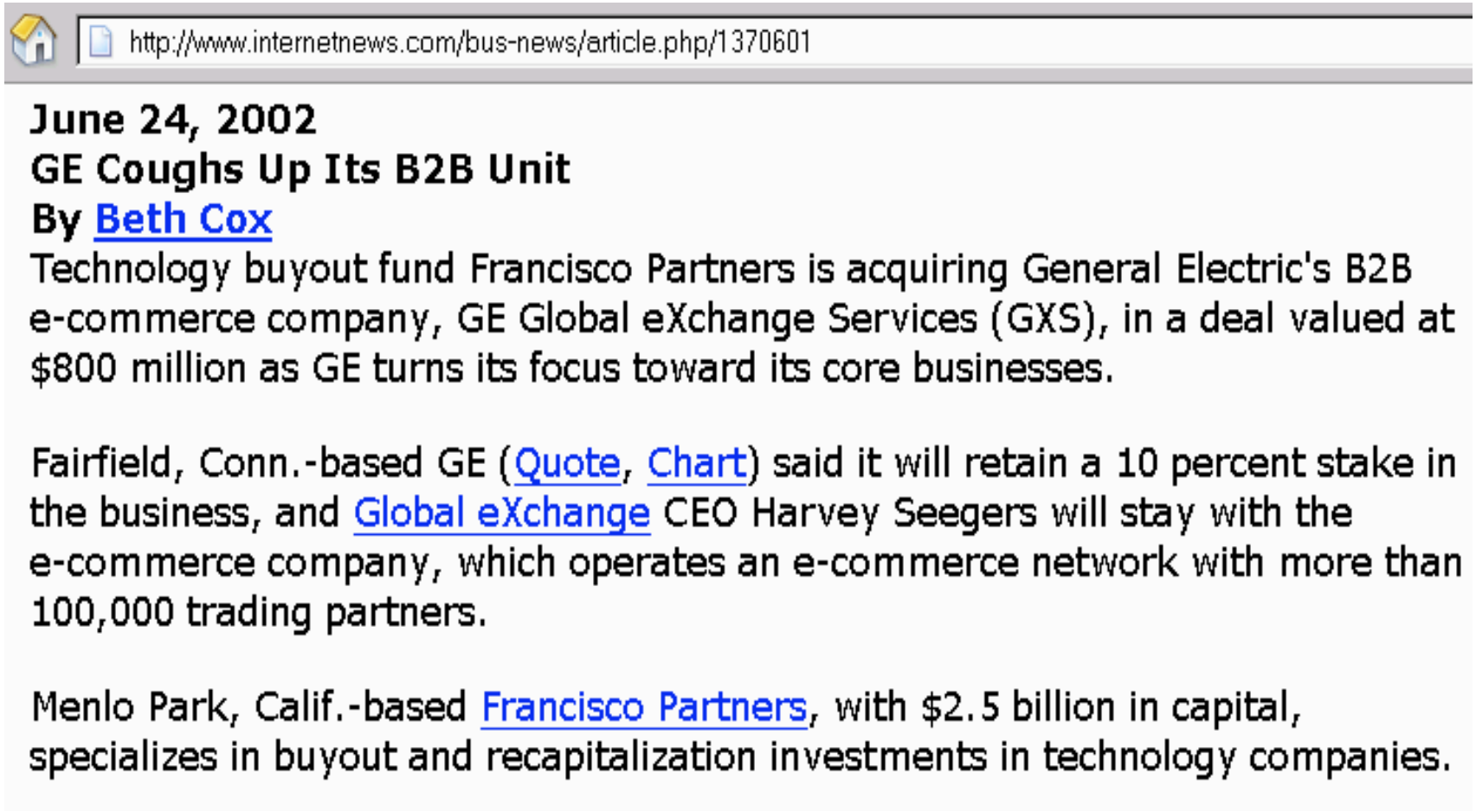
[whois.arin.net]

OrgName:	GE Information Services, Inc.
OrgID:	GEIS
Address:	100 edison park drive
City:	Gaithersburg
StateProv:	MD
PostalCode:	20878
Country:	US
NetRange:	198.147.170.0 - 198.147.174.255
CIDR:	**198.147.170.0/23, 198.147.172.0/23, 198.147.174.0/24**
NetName:	GEIS-198-BLK
NetHandle:	NET-198-147-170-0-1
Parent:	NET-198-0-0-0-0
NetType:	Direct Allocation
RegDate:	**1993-06-04**
Updated:	**2000-04-07**
RTechHandle:	ZG28-ARIN
RTechName:	GE Information Services
RTechPhone:	**+1-301-340-4000**
RTechEmail:	genictech@ge.com

[whois.arin.net]

OrgName:	Global eXchange Services
OrgID:	GES-54
Address:	100 Edison Park Drive
City:	Gaithersburg
StateProv:	MD
PostalCode:	20878
Country:	US
NetRange:	204.90.128.0 - 204.90.255.255
CIDR:	204.90.128.0/17
NetName:	GXS
NetHandle:	NET-204-90-128-0-1
Parent:	NET-204-0-0-0-0
NetType:	Direct Allocation
NameServer:	NS.**GXS.COM**
NameServer:	NS.GEIS.COM
RegDate:	**1994-09-12**
Updated:	**2005-06-06**
OrgTechHandle:	BVI3-ARIN
OrgTechName:	Vink, Ben
OrgTechPhone:	**+31-20-503-5591**
OrgTechEmail:	Ben.Vink@**gxs.com**

GXS Acquired…



http://www.internetnews.com/bus-news/article.php/1370601

June 24, 2002

GE Coughs Up Its B2B Unit

By Beth Cox

Technology buyout fund Francisco Partners is acquiring General Electric's B2B e-commerce company, GE Global eXchange Services (GXS), in a deal valued at $800 million as GE turns its focus toward its core businesses.

Fairfield, Conn.-based GE (Quote, Chart) said it will retain a 10 percent stake in the business, and Global eXchange CEO Harvey Seegers will stay with the e-commerce company, which operates an e-commerce network with more than 100,000 trading partners.

Menlo Park, Calif.-based Francisco Partners, with $2.5 billion in capital, specializes in buyout and recapitalization investments in technology companies.

So…

- 57/8: SITA? Equant? France Telecom? Orange? Someone else?
- AS2647: SITA? Equant? Wisecom? France Telecom? Orange? Someone else?
- AS6524: General Electric? Global Exchange Services? Francisco Partners? Someone else?

- **MY POINT: It can be *really* hard to figure out who is using a given address block, or who *should* be using a given address block, even for a block as large as a /8. Route injection/prefix hijacking is a real risk, but out-of-date/inaccurate whois data is also an important (if far less "cool") contributing issue.**

Thanks for the Chance to Talk Today!

- Are there any questions?