Internet Routing Behavior on 9/11
and in the following weeks

Andy Ogielski and Jim Cowie
Renesys Corporation

[ato, cowie]@renesys.com

5-6 March 2002
National Research Council, Workshop on The Internet Under Crisis Conditions
Outline

High resolution spatio-temporal analysis based on multiple timeseries of BGP messages from 162 peers in 115 ASes in USA, Europe, Japan, and Australia (RIPE RIS).

1. **Reachability**
   
   track all network prefixes reachable vs time, per peer

2. **Outages**
   
   track all prefix outages in Sept 2001

3. **Drill-down**
   
   analyze outages after WTC 2 collapse, and during power failures in NYC telco hotels
Background

Internet routing is very dynamic.

• Precise routing analysis: explore timeseries of BGP messages from a large number of BGP routers, at diverse locations.

• When a BGP router’s preferred route to a given network prefix has changed, or no route is available, it sends out a BGP update message to each connected peer router.

• Analysis of logged BGP message traffic provides a great deal of quantitative information about the way the routers “see” the changing routing topology, about the dynamics of route changes, about reachability of networks over a wide range of time scales, and about the events that caused the routing changes.
Data source: RIPE RIS  EBGP peers
10+ large providers and 100+ regionals.
Partial list of default-free peers

<table>
<thead>
<tr>
<th>peering AS</th>
<th>router location</th>
</tr>
</thead>
<tbody>
<tr>
<td>13129</td>
<td>Global Access</td>
</tr>
<tr>
<td></td>
<td>Germany</td>
</tr>
<tr>
<td>1103</td>
<td>SURFnet</td>
</tr>
<tr>
<td></td>
<td>Netherlands</td>
</tr>
<tr>
<td>513</td>
<td>CERN</td>
</tr>
<tr>
<td></td>
<td>Switzerland</td>
</tr>
<tr>
<td>3333</td>
<td>RIPE NCC</td>
</tr>
<tr>
<td></td>
<td>Netherlands</td>
</tr>
<tr>
<td>286</td>
<td>KPN Qwest (multiple)</td>
</tr>
<tr>
<td></td>
<td>UK, Netherlands</td>
</tr>
<tr>
<td>4777</td>
<td>APNIC Tokyo</td>
</tr>
<tr>
<td></td>
<td>Japan</td>
</tr>
<tr>
<td>9177</td>
<td>Nextra</td>
</tr>
<tr>
<td></td>
<td>Switzerland</td>
</tr>
<tr>
<td>4608</td>
<td>Telstra</td>
</tr>
<tr>
<td></td>
<td>Australia</td>
</tr>
<tr>
<td>6893</td>
<td>Cable &amp; Wireless Global</td>
</tr>
<tr>
<td></td>
<td>Switzerland</td>
</tr>
<tr>
<td>3257</td>
<td>Tiscali</td>
</tr>
<tr>
<td></td>
<td>Netherlands</td>
</tr>
<tr>
<td>3549</td>
<td>Global Crossing (multiple)</td>
</tr>
<tr>
<td></td>
<td>UK, USA</td>
</tr>
<tr>
<td>6762</td>
<td>Telecom Italia</td>
</tr>
<tr>
<td></td>
<td>Netherlands</td>
</tr>
<tr>
<td>2914</td>
<td>Verio (multiple)</td>
</tr>
<tr>
<td></td>
<td>USA, UK</td>
</tr>
<tr>
<td>7018</td>
<td>AT&amp;T Internet4</td>
</tr>
<tr>
<td></td>
<td>USA</td>
</tr>
</tbody>
</table>
9/11 in context

Number of prefix announcements in 30 sec intervals

1 June – September 30, 2002

Amsterdam (rrc00) all peers aggregate

Code red II 9/11 Nimda
9/11 in context: zoom-in

Number of prefix announcements in 30 sec intervals

Sept 11:
only one distinguishable feature at this scale – fewer router maintenance resets

Sept 18 (Nimda worm):
20-fold instability growth.
Reachability analysis
Background

Several locations in downtown Manhattan of special interest in the BGP routing analysis.

• World Trade Center 1 & 2: Below-ground-level fiber from the Telehouse to 60 Hudson St, and to transatlantic cables.

• 60 Hudson St: A large carrier hotel, termination of multiple transatlantic cables, with many PoPs at 25 Broadway.

• NYIIX at 25 Broadway Telehouse: A peering site serving about 40 Internet providers from NYC area, Europe, South America, and South Africa. Claims about 70% of Europe to US traffic.
Number of reachable prefixes Sept 2001

BGP updates from 10 selected peers Europe, USA, Japan

9/11 WTC 2 down
9/13 25 Bway out
9/15 25 Bway back
9/18 Nimda worm attack
Reachable prefixes 10 – 16 Sept zoom

BGP updates from 10 selected peers Europe, USA, Japan

- 9/11 WTC 2 down
- 9/13 25 Bway power out
- 9/15 25 Bway power is back
- 9/15 25 Bway power out again
Reachable prefixes 13-14 Sept zoom

BGP updates from 10 selected peers Europe, USA, Japan

9/13 25 Broadway power generator out, many NYC area, South Africa, South America networks become globally unreachable
Outage analysis
Outage start - duration correlations

x-axis: outage start time, September 1 – 30, 2001
y-axis: outage duration in seconds (log scale 1e0 – 1e7 sec)

Note MRAI timer and full table load resonances

9/11 WTC collapse
9/18 Nimda worm attack massive transient outages
Prefix outages Sept 11 12:00 – 24:00 GMT

Each blue row = outage-starts w/common origin AS.
Back wall in red = total number of outage-starts.
Outages of any duration, 60 sec resolution.

14:05 GMT WTC south tower collapse
Prefix outages Sept 11  13:30 – 14:40 GMT

Each blue row = outage-starts w/common origin AS.
Back wall in red = total number of outage-starts.
Outages of any duration, 1 sec resolution.

WTC south tower collapse
14:03 – 14:08 GMT
Outage drilldown: WTC collapse 5 minutes
Outages lasting over 4 hours, starting 14:03 – 14:08 GMT

All times are GMT, at a European peering router, including multi-hop peers.

14:03 - three UUNET-originated downtown NYC prefixes (WTC),
Many networks originated by AS 1785 (ASN-APPLIED): City of NY, Bank of NY, multiple SUNY campuses, PACE Univ., Fashion Inst. Tech.,..., seven other NYC, Westchester and Ulster county prefixes,
16 Romanian /19 - /24 networks via origin AS 11227 Long Island

14:06 - Swiss SWITCH AS 559 and CERN AS 513 see massive outages to all US National Labs, Yucca Mtn., other nuclear research facilities, and Universities: Rochester, Princeton, Binghamton,...

-One /24 DoD, /24 UUNET Internet Africa, NET-QWEST-3BLKS,...

→ Cause: fiber from 25 Bway to 60 Hudson lost under WTC
Outages lasting over 4 hours, starting 14:03 – 14:08 GMT

Other suspected WTC collapse-related transatlantic outages:

- **Ninety two** /16 - /24 networks CNUCE Pisa Italy, outage seen from US and Tokyo.

- **Twenty three** /16 - /24 Bogota Colombia via Global One, outage seen from Europe.

Unrelated outages?

- thirteen /24s in India, /23 Savvis Florida, /22 in Argentina

- eight /23 - /24 Rhythms NetConnections CO,

....There is always a constant background of outages worldwide.

Correlation analysis of BGP updates can localize network outages well.
Outage drilldown continued

Outages triggered by generator power loss at the Telehouse, 25 Broadway NYC
9/13 about 21:30 GMT

Generator replaced, power back
9/15 about  04:00  GMT
Outage at the Telehouse: no traffic on 9/14

Inbound/outbound MRTG traffic plots:

NYIIX

PSINET
Prefix outages 9/13 19:00 – 9/14 01:00 GMT

Each blue row = outage-starts w/common origin AS.
Back wall in red = total number of outage-starts.
Outages longer than 4 hours.

Telehouse generator failure
about 21:30 GMT
Prefix outages 9/13 19:00 – 9/14 01:00 GMT

Each blue row = outage-starts w/common origin AS.
Back wall in red = total number of outage-starts.
Outages longer than 24 hours.

Telehouse generator failure
about 21:30 GMT
Outages starting in the time window 21:20 – 22:30 GMT

Outages lasting over 4 hours:
- 1157 network prefixes.

Outages lasting over 24 hours:
- 175 network prefixes

Majority of these outages can be traced to Telehouse power failure:
- many lower Manhattan and NYC area institutions, esp. Internet providers and financial institutions,
- many South African networks (incl. some in Zimbabwe)
- some outages last until 9/16 (Federal Reserve Bank NY) or longer

Some outages are unrelated - part of normal "background noise".
portable generator next to Telehouse, 9/15

Photo: Anthony Townsend, Taub Urban Research Center, New York University
Conclusions 1

- The collapse of WTC 2 caused immediately a multi-hour loss of reachability to fewer than 1,000 network prefixes – below 1% of all globally announced prefixes. The loss of power at the Telehouse at 25 Broadway on September 13/14 caused a comparable loss. *Reachability was lost either on one, or on both sides of the Atlantic.* Damage to network access, and power losses in downtown Manhattan were the immediate root causes.

- The 9/11 attack-related reachability losses did not create any routing instabilities (in contrast to the Nimda worm attack on 9/18).

- Apart from these reachability losses, the global Internet routing continued to operate normally.
Conclusions 2

- The attacks on WTC and subsequent loss of the Telehouse were localized events, although magnified by a loss of a number of peering sessions across the transatlantic cables.

- There has been a sufficiently high peering redundancy, and so far single localized events such as the 9/11 attacks, or the 7/18 Baltimore tunnel fire, do not cause widespread global routing problems. Lack of redundancy is fatal: cf. South Africa.

- However, geographic concentration of peering facilities and of certain transatlantic and transcontinental cable routes implies that a moderate number of carefully targeted localized events will likely cause a significant loss of global routing capabilities, and a fragmentation of the global Internet into disconnected components.
Appendix: Nimda worm attack

prefix announcements by peer in 15-min intervals
RIPE rrc00 peering point,
10 – 22 september

18 September 2001:
Long-tail wave of routing instabilities in BGP message streams from major Internet providers due to large numbers of transiently failing BGP routers. This is a true global routing instability, also analyzed at Renesys.