Peering Security

IX Forum 13
Sao Paulo 2019

Walt Wollny, Director Interconnection Strategy
Hurricane Electric AS6939
Who is Walt Wollny?

- **Hurricane Electric AS6939 – 4 years**
  - Director Interconnection Strategy – supporting the network to reach to over 44 counties and over 223 Internet Exchanges. Focus on Global connectivity.

- **Amazon AS16509 – 4 years**
  - Developed IP Transit and Peering on five continents.
  - Primary focus on Japan, Singapore, Hong Kong, India, Taiwan, Philippines, Australia.
  - Over 62 new CDN sites.

- **Microsoft AS8075 – 13 years**
  - Developed IP Transit and Peering on four continents.
  - Primary focus on US, EU and South America.
Hurricane Electric Backbone

Contact us today at: +1 510-580-4190 or sales@he.net
The Most Peering Exchanges

IX Participation Count

<table>
<thead>
<tr>
<th>ASN</th>
<th>Name</th>
<th>IXes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS13335</td>
<td>Cloudflare, Inc.</td>
<td>227</td>
</tr>
<tr>
<td>AS6939</td>
<td>Hurricane Electric LLC</td>
<td>223</td>
</tr>
<tr>
<td>AS42</td>
<td>WoodyNet</td>
<td>178</td>
</tr>
<tr>
<td>AS3856</td>
<td>Packet Clearing House</td>
<td>170</td>
</tr>
<tr>
<td>AS20940</td>
<td>Akamai International B.V.</td>
<td>165</td>
</tr>
<tr>
<td>AS15169</td>
<td>Google LLC</td>
<td>163</td>
</tr>
<tr>
<td>AS8075</td>
<td>Microsoft Corporation</td>
<td>155</td>
</tr>
<tr>
<td>AS32934</td>
<td>Facebook, Inc.</td>
<td>113</td>
</tr>
<tr>
<td>AS16509</td>
<td>Amazon.com, Inc.</td>
<td>113</td>
</tr>
<tr>
<td>AS2906</td>
<td>Netflix Streaming Services Inc.</td>
<td>97</td>
</tr>
</tbody>
</table>
Why So Many Peering Exchanges?
Why So Many Peering Exchanges?

IPv4 Adjacencies

<table>
<thead>
<tr>
<th>ASN</th>
<th>Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS6939</td>
<td>Hurricane Electric LLC</td>
<td>7,809</td>
</tr>
<tr>
<td>AS174</td>
<td>Cogent Communications</td>
<td>5,989</td>
</tr>
<tr>
<td>AS3356</td>
<td>Level 3 Parent, LLC</td>
<td>5,417</td>
</tr>
<tr>
<td>AS36236</td>
<td>NetActuate, Inc</td>
<td>4,648</td>
</tr>
<tr>
<td>AS57463</td>
<td>NetIX Communications Ltd.</td>
<td>3,886</td>
</tr>
<tr>
<td>AS24482</td>
<td>SG.GS</td>
<td>3,859</td>
</tr>
<tr>
<td>AS267613</td>
<td>ELETRONET S.A.</td>
<td>3,679</td>
</tr>
<tr>
<td>AS263009</td>
<td>FORTE TELECOM LTDTA.</td>
<td>3,369</td>
</tr>
<tr>
<td>AS37468</td>
<td>Angola Cables</td>
<td>3,078</td>
</tr>
<tr>
<td>AS51185</td>
<td>Onecom Global Communications LTD</td>
<td>3,059</td>
</tr>
</tbody>
</table>

AS IPv4 Adjacency Count Chart

Hurricane Electric - Massive Peering!
Before we start…..

We all live in glass houses
So we shouldn't throw stones

Offer to help and drop that rock…..
What does security have to do with Peering?

A lot. Now.

Security was an afterthought, but it has become **critically** important with the increase of BGP hijacks

Some of the basics...
Best defenses for your network?
- Logical Port Security
- IXP Subnet Security
- Routing Security
- Peering tools
Logical Port Security

- Many IXPs will post their recommended port configuration (HKIX, AMS-IX, etc).
- Don’t just connect an interface with a default configuration to an IX Port!
- Services like Proxy-ARP will disrupt the IX as well as degrade your own network.
- Most IXs allow only unicast traffic. (IPv6 multicast neighbor discovery packets are an exception.)
Logical Port Security

- Apply ACL’s to your interfaces—don’t forget to configure both IPv4 and IPv6 ACLs!
- The SIX (Seattle Internet Exchange) has a great example [here](#).
- Your IX port is an exposed piece of your network.
- Hundreds of other networks are directly connected.
- Remove this security risk!
Logical Port Security

- Why do we care?
Ticket: 341134
Subject: Instability on AMS-IX
Status: closed
Opened: 2017-06-20 16:04:56 +0200
Type: unscheduled
Scope: AMS-IX NL
Start: 2017-06-20 15:20:00 +0200
CLOSED 2017-06-21 16:54:10 +0200:

Total impact time – 1 hour 34 mins

Root cause human error

The instability was caused due to a hardware issue on the customer's NIC and due to proxy-arp being enabled after the port passed the testing phase and was moved to production.
BBIX Tokyo

Occurred time: 2018/5/16 17:28 JST
Corresponded time: 2018/5/16 17:48 JST
Recovered time: 2018/5/16 18:10 JST
Affected area: BBIX Tokyo IX service

Total impact time - 39 mins

Root cause human error

Arp proxy response (= proxy arp) became effective when we changed the subnet mask on our monitoring router
Your IX Port is a target for DDoS Attacks!

Applying the best security practices will help limit the exposure.
IXP Subnet

- The IXP is responsible for protecting the infrastructure.
- The IX LAN is not your IP space and should not be routed.
- Checking this...
# IXP Subnet

## Public Peering Exchange Points

<table>
<thead>
<tr>
<th>Exchange</th>
<th>IPv4</th>
<th>IPv6</th>
<th>Speed</th>
<th>RS Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPNAP Osaka</td>
<td>210.173.178.70</td>
<td>2001:7fa:7:2::6939:1</td>
<td>10G</td>
<td></td>
</tr>
<tr>
<td>6939</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JPNAP Tokyo</td>
<td><strong>210.173.176.106</strong></td>
<td><strong>2001:7fa:7:1::6939:1</strong></td>
<td>10G</td>
<td></td>
</tr>
<tr>
<td>6939</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IXP Subnet

Hurricane Electric - Massive Peering!

210.173.176.106

Announced By

<table>
<thead>
<tr>
<th>Origin AS</th>
<th>Announcement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS7521</td>
<td>210.173.160.0/19</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>AS7521</td>
<td>210.173.176.0/20</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>AS18403</td>
<td>210.173.176.0/24</td>
<td>✓ ✓</td>
</tr>
</tbody>
</table>

Address has 0 hosts associated with it.
IXP Subnet

Quick Links
- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel

IP Info | Whois | DNS | RBL
---|---|---|---
210.173.176.106 (gigabitethernet2-8.core1.tyo1.he.net)

Announced By

<table>
<thead>
<tr>
<th>Origin AS</th>
<th>Announcement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS7521</td>
<td>210.173.160.0/19</td>
<td></td>
</tr>
<tr>
<td>AS7521</td>
<td>210.173.176.0/20</td>
<td></td>
</tr>
<tr>
<td>AS18403</td>
<td>210.173.176.0/24</td>
<td></td>
</tr>
</tbody>
</table>

Address has 0 hosts associated with it.

Hurricane Electric - Massive Peering!
IXP Subnet

Hurricane Electric - Massive Peering!

210.173.176.106

210.173.176.106 (gigabitethernet2-8.core1.tyo1.he.net)

<table>
<thead>
<tr>
<th>Origin AS</th>
<th>Announcement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS7521</td>
<td>210.173.176.0/19</td>
<td></td>
</tr>
<tr>
<td>AS7521</td>
<td>210.173.176.0/20</td>
<td></td>
</tr>
<tr>
<td>AS18403</td>
<td>210.173.176.0/24</td>
<td></td>
</tr>
</tbody>
</table>

Address has 0 hosts associated with it.
The IX LAN is not your IP space and should not be routed.

Some of the smaller guys
## IXP Subnet

### Europe

<table>
<thead>
<tr>
<th>CC Exchange</th>
<th>Speed</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIX</td>
<td>2x10GE</td>
<td>193.203.0.185</td>
<td>2001:7f8:30:0:2:1:0:6939</td>
</tr>
<tr>
<td>BNIX</td>
<td>2x10GE</td>
<td>194.53.172.33</td>
<td>2001:7f8:26::a500:6939:1</td>
</tr>
<tr>
<td>B-IX Balkans</td>
<td>10GE</td>
<td>217.174.157.31</td>
<td>2001:7f8:8e::31</td>
</tr>
<tr>
<td>BIX.BG</td>
<td>2x10GE</td>
<td>193.169.198.70</td>
<td>2001:7f8:58::1b1b:0:1</td>
</tr>
<tr>
<td>NetIX</td>
<td>10GE</td>
<td>193.218.0.89</td>
<td>2001:67c:29f0::6939:1</td>
</tr>
<tr>
<td>MegaIX Sofia</td>
<td>10GE</td>
<td>91.212.235.55</td>
<td>2001:7f8:9f::a6939:1</td>
</tr>
<tr>
<td>T-CIX Bulgaria</td>
<td>10GE</td>
<td>185.1.40.26</td>
<td>2001:7f8:98::26</td>
</tr>
<tr>
<td>CIXP</td>
<td>10GE</td>
<td>192.65.185.143</td>
<td>2001:7f8:1c:24a::1b1b:1</td>
</tr>
</tbody>
</table>
I XP Subnet

- Some of the big ones.....
## IXP Subnet

<table>
<thead>
<tr>
<th>CC Exchange</th>
<th>Speed</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE-CIX Frankfurt</td>
<td>2x100GE</td>
<td>80.81.192.172</td>
<td>2001:7f8::1b1b:0:1</td>
</tr>
<tr>
<td>France-IX Paris</td>
<td>2x10GE</td>
<td>37.49.236.10</td>
<td>2001:7f8:54::10</td>
</tr>
<tr>
<td>AMS-IX 2x100GE</td>
<td></td>
<td>80.249.209.150</td>
<td>2001:7f8:1::a500:6939:1</td>
</tr>
<tr>
<td>LINX 100GE</td>
<td></td>
<td>195.66.224.21</td>
<td>2001:7f8:4:0::1b1b:1</td>
</tr>
<tr>
<td>NL-IX 3x10GE</td>
<td></td>
<td>193.239.116.14</td>
<td>2001:7f8:13::a500:6939:1</td>
</tr>
</tbody>
</table>
Our Basic plan enables you to monitor up to 5 prefixes for free. Our premium plan allows you to monitor more than 5 prefixes, provides full alert details plus it comes with a number of other features such as access to our web services API, our popular daily routing report software which informs you of any routing changes for your network. Other extras include an additional email address for alerts as well as SMS formatted emails.

This product is now end of life in March 2020
Basics - Routing Security

Hurricane Electric - Massive Peering!

---

Possible Prefix Hijack (Code: 10)
---

Your prefix: 206.81.80.0/22:
Update time: 2019-01-29 21:55 (UTC)
Detected by #peers: 1
Detected prefix: 206.81.80.0/23
Announced by: AS10310 (YAHOO-1 - Yahoo!, US)
Upstream AS: AS29467 (LUXNETWORK Network Service Provider in Luxembourg, LU)
ASpath: 60983 29467 10310
Alert details: https://portal.bgpmon.net/alerts.php?details&alert_id=86973730
Mark as false alert: https://portal.bgpmon.net/fp.php?aid=86973730

---

*for questions regarding the change code or other question, please see:
https://portal.bgpmon.net/faq.php

---

Latest BGPmon news: http://bgpmon.net/blog/
* Popular Destinations rerouted to Russia
* Todayâ€™s BGP leak in Brazil
* BGP leak causing Internet outages in Japan and beyond.
BGPMON Replacement


Thanks to Job & Massimo @NTT Ltd
IXP Subnet

Why do we care?
The DDoS That Almost Broke the Internet

Cloudflare March 2013  ~120Gbps attack on LINX
Basics - Routing Security

You must filter your peers.

- Most networks don’t filter their peers.
- This is negligent behavior.
Routing Security: Why it matters

On 28 December 2018 China Telecom hijacked a US Department of Energy prefix (192.208.19.0/24) and did not correct the problem for 6 days.
At 06:28 UTC earlier today (30-Jul), an Iranian state telecom network briefly leaked over 100 prefixes. Most were Iranian networks, but the leak also included 10 prefixes of popular messaging app @telegram (8 were more-specifics).
Every day there are several hijacks and leaks

<table>
<thead>
<tr>
<th>Type</th>
<th>Expected Origin AS:</th>
<th>Detected Origin AS:</th>
<th>Date</th>
<th>Time</th>
<th>More Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible</td>
<td>COMCAST-7922</td>
<td>LIVEPERSON-ASN, IL</td>
<td>2019-08-21</td>
<td>14:20:14</td>
<td></td>
</tr>
<tr>
<td>Hijack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td>ADAPT-AS, GB</td>
<td>LEVEL3 - Level 3 Parent, LLC, US</td>
<td>2019-08-21</td>
<td>14:20:14</td>
<td></td>
</tr>
<tr>
<td>Hijack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hijack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outage</td>
<td>Fundação Carlos Chagas Filho de Amparo a Pesquisa, BR</td>
<td>2019-08-21</td>
<td>12:42:00</td>
<td>2019-08-21</td>
<td>12:54:00</td>
</tr>
<tr>
<td>Outage</td>
<td>Assoc do Inst Nac de Matematica Pura e Aplicada, BR</td>
<td>2019-08-21</td>
<td>12:42:00</td>
<td>2019-08-21</td>
<td>12:54:00</td>
</tr>
<tr>
<td>Possible</td>
<td>LASVEGASNET-AS</td>
<td>LIQUID-AS, GB</td>
<td>2019-08-21</td>
<td>10:48:30</td>
<td></td>
</tr>
<tr>
<td>Hijack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td>LASVEGASNET-AS</td>
<td>LIQUID-AS, GB</td>
<td>2019-08-21</td>
<td>10:48:30</td>
<td></td>
</tr>
<tr>
<td>Hijack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Basics - Routing Security

I know we can do better
Basics - Routing Security

You must filter your peers!
Basics - Routing Security

• Routing security is important in two directions:
  • The routes you receive
  • The routes you announce

• Starting with the routes you receive...
Basics - Routing Security

- The routes you receive can be filtered in a few ways:
  - Prefix Count
  - AS-Path
  - Prefix list
  - RPKI
Basics - Routing Security

• Prefix Count

Consider tightening up the limits with bgp neighbor restart/graceful
Basics - Routing Security

AS-Path
BBIX peer 各位 (Dear BBIX peering partners,)

さくらインターネット(AS9371)の津田です。
いつもお世話になっております。

弊社から広報しておりますAS Pathに変更が御座います。
AS Pathでのフィルタ設定が御座います場合、設定変更をお願い致します。

AS name: SAKURA-C
AS set: AS-SAKURA
AS number: 9371

▼追加するAS Path(IPv4)
^((9371_)+(2519_)+(9354_)+(10001_))+$
^((9371_)+(9370_)+(2519_)+(9354_)+(10001_))+$
Basics - Routing Security

Prefix list per neighbor
ip prefix-list AS57660 permit 37.26.208.0/20
ip prefix-list AS57660 permit 185.67.16.0/22
ip prefix-list AS57660 permit 212.67.48.0/20
Basics - Routing Security

RPKI
Basics - Routing Security

Building filters does not have to be hard. You can script it yourself or use a tool like bgpq3. Here is an example using bgpq3 to generate a prefix list for a Juniper router:

```
walt@staff:~$ bgpq3 -J4l AS57660-IN AS57660
policy-options {
    replace:
    prefix-list AS57660-IN {
        37.26.208.0/20;
        185.67.16.0/22;
        212.67.48.0/20;
    }
}
walt@staff:~$  
```
IXPs using RPKI

- IX.BR
- AMS-IX
- DE-CIX
- France-IX
- LINX
- Over 58 IXP today and more coming!

- Downside is that not all networks peer on route servers

- [http://peering.exposed/](http://peering.exposed/)
http://routing.he.net
# ROUTE FILTERING HOME ALGORITHM

## AS13335

<table>
<thead>
<tr>
<th>ASN</th>
<th>STATUS</th>
<th>PEERINGDB_I RR</th>
<th>EXTRACTED_V4</th>
<th>EXTRACTED_V6</th>
<th>OK_V4</th>
<th>OK_V6</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>13335</td>
<td>explicit</td>
<td>AS-CLOUDFLARE</td>
<td></td>
<td></td>
<td>AS-CLOUDFLARE</td>
<td>AS-CLOUDFLARE</td>
<td>peeringdb</td>
</tr>
</tbody>
</table>

### FILTERS

<table>
<thead>
<tr>
<th>AF</th>
<th>AS-SET NAME</th>
<th>IRR STATUS</th>
<th>IRR BUILT</th>
<th>IRR LINES</th>
<th>PREFIXES RECEIVED</th>
<th>FILTER BUILT</th>
<th>FILTER LINES</th>
<th>POLICY</th>
<th>REASONS</th>
<th>FILTER</th>
</tr>
</thead>
</table>

### PREFIX LISTS

<table>
<thead>
<tr>
<th>AF</th>
<th>ROUTER</th>
<th>NAME</th>
<th>STATUS</th>
<th>CHECKED</th>
<th>EXISTING_LINES</th>
<th>VERIFIED</th>
<th>EXISTING</th>
<th>DELTA</th>
<th>LOG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>Next Hop</td>
<td>MED</td>
<td>LocPrf</td>
<td>Weight</td>
<td>Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
<td>-----</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.0.0/24</td>
<td>185.1.32.22</td>
<td></td>
<td>100</td>
<td>0</td>
<td>ME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>AS_PATH: 13335</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.1.0/24</td>
<td>185.1.32.22</td>
<td></td>
<td>100</td>
<td>0</td>
<td>ME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>AS_PATH: 13335</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23.227.63.0/24</td>
<td>185.1.32.22</td>
<td></td>
<td>100</td>
<td>0</td>
<td>ME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>AS_PATH: 13335</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>64.68.192.0/24</td>
<td>185.1.32.22</td>
<td></td>
<td>100</td>
<td>0</td>
<td>ME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>AS_PATH: 13335</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66.235.200.0/24</td>
<td>185.1.32.22</td>
<td></td>
<td>100</td>
<td>0</td>
<td><strong>EF</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>AS_PATH: 13335</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>104.16.0.0/12</td>
<td>185.1.32.22</td>
<td></td>
<td>100</td>
<td>0</td>
<td>ME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>AS_PATH: 13335</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>104.16.0.0/20</td>
<td>185.1.32.22</td>
<td></td>
<td>100</td>
<td>0</td>
<td>ME</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
route: 66.235.200.0/24

descr: CMI (Customer Route)

origin: AS38082

mnt-by: MAINT-AS58453

changed: qas_support@cmi.chinamobile.com 20180906

source: RADB

route: 66.235.200.0/24

descr: CMI IP Transit

origin: AS38082

admin-c: MAINT-CMI-INT-HK

tech-c: MAINT-CMI-INT-HK

mnt-by: MAINT-CMI-INT-HK

changed: qas_support@cmi.chinamobile.com 20180906

source: NTTCOM
Hurricane Electric
Route Filtering Algorithm

- Read more here
  http://routing.he.net/algorith.html

- Example:
  - xx.7.224.0/24, rejected, does not strictly match IRR policy or RIR handles
  - xx.10.254.0/23, accepted, strictly matched IRR policy
  - xx.17.248.0/24, accepted, strictly matched IRR policy
  - xx.26.36.0/22, rejected, does not strictly match IRR policy or RIR handles
  - xx.26.39.0/24, rejected, does not strictly match IRR policy or RIR handles

Hurricane Electric - Massive Peering!
Resources

- https://www.seattleix.net/faq
- https://twitter.com/bgpstream/status/1078584924364595202?lang=en
- https://bgp.he.net
- https://routing.he.net
- https://github.com/snar/bgpq3
- https://bgpmon.net/
- https://bgpstream.com/
- https://bgpmon.net/
- http://peering.exposed/
Thanks!

Walt Wollny, Director Interconnection Strategy
Hurricane Electric  AS6939
walt@he.net