

Мониторинг BGP

Для мониторинга BGP в сети существует несколько сервисов. Об одном из таких я хотел бы рассказать. BGPmon.net — это сервис для мониторинга и анализа мировой маршрутной таблицы протокола BGP. Он может следить за изменениями в таблице маршрутизации относительно ваших анонсов и сообщать об этом. Изменения в aspath, origin AS, transit AS или любая комбинация из этих признаков протоколируются и классифицируется сервисом.

Особое внимание мониторингу мировой таблицы BGP стало уделяться после того, как Pakistan Telecom в феврале 2008 года «угнал» сети Youtube путем анонсирования более специфичных маршрутов через свою AS. Направляя трафик предназначенный для серверов Youtube в blackhole, вывел из строя(сети) весь сервис на несколько часов. Более подробно об этом инциденте можно почитать на сайте RIPE. В случае с Youtube трафик был направлен в blackhole, но что если бы он был перехвачен, проанализирован и затем отправлен к своему месту назначения. Подобные атаки могут быть классифицированы как BGP Man In The Middle Attack (MITM) что и было продемонстрировано на DEFCON в 2008 году(видео). Помимо этого случая было множество подобных мелких и крупных, один из таких описан в заметке «К чему приводит неправильная настройка BGP»

Сервис будет полезен все администраторам которые имеют дело с настройкой и обслуживанием BGP на маршрутизаторах глобальной сети. По словам автора сервис был разработан за полтора года для собственных нужд, но с ростом интереса к этой теме со стал общедоступным. Отличительной и приятной особенностью BGPmon являются простота и доступность, а также бесплатность

В своей статье я хотел бы предложить вольный перевод [последней статьи с сайта BGPmon.net](#) о diff отчетах с помощью [Rancid](#).

DIFF отчеты о маршрутизации. Rancid для BGP.

Как и многие из вас, я использую [RANCID](#) для резервного копирования и отслеживания изменений в конфигурациях маршрутизаторов и коммутаторов. На этой неделе BGPmon.net анонсировал новый функционал — 'Routing report', как можно догадаться, это RANCID для вашей таблицы BGP. Каждый день BGPmon сравнивает анонсы от вышей автономной системы со вчерашними. Информация о каждом изменении в анонсах и доступности высылается вам на email.

Я использую эту функцию несколько недель и нахожу ее довольно полезной. Этот сервис будет присылать отчеты об изменениях в анонсируемых префиксах, включая разбивку по доступности префиксов через конкретные апстримы(upstream) и соседние AS (peer AS). Это поможет обнаружить, что префикс более недоступен через каких либо AS peers или upstreams.

Routing report также содержит информацию по апстримам и даунстримам вашей автономной системы. В конце статьи вы найдете пример отчета. Пожалуйста, обратите внимание, каждый отчет содержит краткую информацию о вашей автономной системе в соответствии с CIDR.

Функция 'Routing report' может быть включена/выключена на странице 'my ASn'

Уведомление 'Новый префикс' (code 60)

Если вы недавно стали анонсировать новый префикс, то вскоре вы получите email уведомление «Новый префикс» (code 60). Это уведомление придет как только вы начнете оригиналировать новый префикс.

Уведомление этого типа может быть глобально включено/выключено через меню настроек. Если вы используете BGPmon.net для нескольких своих автономных систем Вам возможно понадобится включить эту функцию только на некоторых из AS. В ближайшем будущем это можно будет сделать.

Добавление вашей AS в 'My ASn'.

Все ваши номера AS (ASns), которые мониторятся, добавляются на страницу 'My ASn' автоматически. Если вы добавляете новый префикс и ASn в 'my prefixes', не забудьте добавить свою AS на страницу 'My ASn'. В противном случае 'routing report' и 'New Prefix alert' (code 60) не будут работать, пока вы не сделаете это вручную.

Пример отчета.

```
From: BGPmon Alert <info@bgpmon.net>
To: you@gmail.com
Subject: BGPmon Routing report
Date: Sun, 10 Jan 2010 02:53:27 +0100 (CET)
```

Your routing table report for AS271 (BCNET-AS — BCnet)

===== Changes:

=====

RIB file used:

RRC01 — LINX, London
RRC03 — AMS-IX / NL-IX / GN-IX, Amsterdam
RRC11 — NYIIX, New York
RRC12 — DE-CIX, Frankfurt
RRC13 — MSK-IX, Moscow
RRC15 — PTTMetro, Sao Paulo

----- AS Adjacency report -----

New Downstream / Customer AS:

+ AS25689 (NRCNET-AS — National Research Council of Canada)

----- Prefixes report -----

Lost prefixes for AS271

— 207.23.245.0/24 (Sky Research Inc.)
— 209.87.17.0/24 (UBC Commercial Client)

----- Prefixes reachable via peers report -----

+ 134.87.113.0/24 via AS6939 (BCNET IPv6 awareness day) now reachable via HURRICANE — Hurricane Electric, Inc.
+ 2607:f8f0:690::/48 via AS6939 (No valid route object!) now reachable via HURRICANE — Hurricane Electric, Inc.

— 209.87.17.0/24 via AS6509 (UBC Commercial Client) no longer reachable via CANARIE-NTN — Canarie Inc
— 207.23.245.0/24 via AS6509 (Sky Research Inc.) no longer reachable via CANARIE-NTN — Canarie Inc
— 209.87.17.0/24 via AS6939 (UBC Commercial Client) no longer reachable via HURRICANE — Hurricane Electric, Inc.
— 207.23.245.0/24 via AS6939 (Sky Research Inc.) no longer reachable via HURRICANE — Hurricane Electric, Inc.

===== AS271 Summary report 01/09/10 23:59:58: =====

Upstream Adjacent AS list:

*AS852 ASN852 — Telus Advanced Communications)
*AS6327 SHAW — Shaw Communications Inc.)
*AS6509 CANARIE-NTN — Canarie Inc)
*AS6939 HURRICANE — Hurricane Electric, Inc.)
*AS13768 PEER1 — Peer 1 Network Inc.)

Downstream Adjacent AS list:

*AS3633 BC-SYSTEMS — Province of British Columbia)
*AS11105 SFU-AS — Simon Fraser University)
*AS16462 UVIC-AS — University of Victoria)
*AS25689 NRCNET-AS — National Research Council of Canada)
*AS25722 GATEWAY-OPERATIONS — Payment Processing Inc.)
*AS32956 ZED-RADIO3 — Canadian Broadcasting Corporation)
*AS36000 NHA-ASN1 — Northern Health Authority)
*AS36391 TRIUMF — TRIUMF (Tri-University Meson Facility))
*AS25689 NRCNET-AS — National Research Council of Canada

Announced IPv6 prefixes:

*2607:f8f0:670::/48 (No valid route object!)
*2607:f8f0:680::/48 (No valid route object!)
*2607:f8f0:690::/48 (No valid route object!)
*2607:f8f0::/32 (No valid route object!)

Announced IPv4 prefixes:

*128.189.0.0/16 (BCNet Class B network)
*128.189.0.0/17 (BCNet network)
*128.189.128.0/18 (UBC RESnet network)
*128.189.192.0/18 (UBC wireless network)
*128.189.4.0/24 (No valid route object!)
*128.189.64.0/19 (No valid route object!)
*128.189.96.0/19 (No valid route object!)
*134.87.0.0/16 (BCNET-2)
*134.87.112.0/24 (BCnet gigapop servers — News,DNS)
*134.87.113.0/24 (BCNET IPv6 awareness day)
*134.87.114.0/23 (BCNET conference 2009 (DUAL stack))
*134.87.2.0/24 (BCnet gigapop C3 interconnect links)

- *134.87.3.0/24 (UBC_TRU DR project)
- *134.87.4.0/24 (BC Genome Sequence Centre)
- *134.87.58.0/24 (BCnet gigapop C3 interconnect links)
- *137.82.0.0/16 (UBC)
- *142.103.0.0/16 (University of British Columbia (UBC1))
- *142.207.0.0/16 (NET-UNBC)
- *142.231.0.0/16 (BCNET3)
- *142.231.1.0/24 (BCnet gigapop C3 interconnect links)
- *142.231.110.0/24 (BCNET VANTX interconnects)
- *142.231.112.0/24 (BCnet gigapop servers — News,IRR)
- *142.231.113.0/24 (BCnet gigapop servers — RealServer, Video Server)
- *142.231.142.0/24 (BCnet gigapop connections)
- *142.231.2.0/24 (No valid route object!)
- *142.231.20.0/24 (UBC MedSchool AV Network)
- *142.231.3.0/24 (BCIT Internet Engineering Lab)
- *142.231.4.0/24 (UBC MedSchool AV Network)
- *142.231.5.0/24 (UBC MedSchool AV Network)
- *142.231.64.0/19 (University of British Columbia (UBC) Okanagan)
- *142.232.0.0/16 (BCITNET2)
- *142.90.0.0/16 (TRIUMF)
- *192.139.193.0/24 (DPIC)
- *192.146.156.0/24 (Thompson Rivers University)
- *192.219.32.0/19 (Open Learning Agency)
- *192.68.67.0/24 (British Columbia Institute of Technology (NET-192-68-67-0-2))
- *192.68.68.0/24 (British Columbia Institute of Technology (NET-192-68-68-0-1))
- *192.68.69.0/24 (British Columbia Institute of Technology (NET-192-68-69-0-1))
- *192.68.72.0/24 (British Columbia Institute of Technology (BCIT))
- *192.68.73.0/24 (BCIT Internet Engineering Lab)
- *192.73.5.0/24 (University of British Columbia (CDNnet))
- *198.162.20.0/22 (BCNET-AGG-13)
- *198.162.32.0/19 (University of British Columbia (UBC-CS))
- *198.162.67.0/24 (Forintek)
- *199.175.163.0/24 (SPINNAKER)
- *199.60.119.0/24 (Emily Carr Institute of Art and Design)
- *199.60.120.0/24 (Emily Carr Institute of Art and Design)
- *199.60.226.0/23 (Emily Carr Institute of Art and Design)
- *204.239.83.0/24 (NETBLK-UNBC-DMZ)
- *206.12.0.0/16 (NETBLK-BR-COL-6)
- *206.12.0.0/24 (BCNET ORAN interconnect links)
- *206.12.10.0/24 (Great Northen Way Digital Arts)
- *206.12.104.0/22 (University of British Columbia (UBC) Vancouver BCWARN BC Amateur Radio Network)
- *206.12.11.0/24 (E-Learning Conference)
- *206.12.12.0/24 (UBC Commercial Clients)
- *206.12.14.0/24 (CANFOR)
- *206.12.18.0/24 (UBC Commercial Clients)
- *206.12.19.0/24 (UBC Commercial Clients Debian Project)
- *206.12.2.0/24 (No valid route object!)
- *206.12.24.0/22 (WestGrid project)
- *206.12.24.0/24 (WestGrid)
- *206.12.28.0/24 (UBC Commercial)
- *206.12.52.0/22 (UBC eduroam wireless)
- *206.12.8.0/24 (WestGrid project inter-router links)
- *206.123.160.0/19 (Thompson Rivers University)
- *206.87.0.0/16 (BCNET (Non-portable address space))
- *206.87.0.0/18 (University of British Columbia (UBC) Okanagan)
- *206.87.128.0/19 (University of British Columbia (UBC) Vancouver wireless)
- *206.87.96.0/19 (University of British Columbia (UBC) Vancouver wireless)
- *207.23.0.0/16 (BR-COL-8)
- *207.23.128.0/19 (BC Childrens and Womens Hospital)
- *207.23.240.0/24 (BCnet gigapop interconnects (BCNET-4))
- *207.23.241.0/24 (BCNET VICTX interconnects)
- *207.23.242.0/24 (BCNET PGTX interconnects)
- *207.23.243.0/24 (BC Research — UBC Commercial Client)
- *207.23.249.0/24 (UBC Commercial Client)
- *207.23.252.0/24 (UBC Commercial Client)
- *207.23.254.0/24 (BCNET KELTX interconnects)
- *207.23.255.0/24 (BCNET KAMTX interconnects)
- *207.23.78.0/24 (UBC Research Enterprises Inc.)

*207.23.8.0/21 (University College of the Cariboo)
*207.23.94.0/24 (BCnet gigapop C3 interconnect links)
*207.23.95.0/24 (BCnet gigapop C3 interconnect links)
*207.23.96.0/20 (Royal Roads University (RRU))
*209.87.0.0/18 (BCNET-5)
*209.87.18.0/24 (Prince George Public Library)
*65.39.232.0/22 (Farleigh Dickinson University Vancouver campus)

* The upstream / downstream categorisation in this report is strictly a description relative topology, and should not be confused with provider / customer / peer inter-AS relationships.

Источник