

Практика 4. Протокол BGP: базы RIS'ов, утилита BGPlay, Looking glass, сервис whois и т. д.

Цель: на практике познакомиться с особенностями поведения трафика в Интернете и распространения BGP-маршрутной информации; научиться анализировать содержимое публичных баз данных от RIS'ов, в частности, использовать утилиту BGPlay и сервис whois.

Сохранить результаты работы (скриншоты) и показать их преподавателю практики (убедиться, что преподаватель отметил в ведомости или гуглдоке факт сдачи).

На вопросы **можно** отвечать письменно (можно в электронном виде) и пользоваться ими при беседе с преподавателем.

Задачи внутренней внешней маршрутизации принципиально отличаются.

Обсуждение со студентами: Разберем первую причину. Для протоколов IGP, работающих в локальных сетях, наибольшее значение имеет скорость сходимости, время реагирования на изменения. Маршрутизаторы при построении таблиц маршрутизации обычно ориентируются на пропускную способность линков. На что ориентируются BGP-маршрутизаторы при выборе между каналами двух (или более) провайдеров?

Задание 1. Разберем вторую причину. IGP-маршрутизаторы строят маршруты к подсетям, которых на предприятии десятки (в крупных – сотни). С точки зрения BGP Интернет выглядит как множество соединенных между собой автономных систем. Оцените количество IP-префиксов и автономных систем, с которыми работает BGP. <http://bgp.he.net/report/netstats>

Как число IP-v4 и IP-v6 префиксов и АС, которые их анонсируют, изменялось за последние три года? Построить графики. <http://bgp.he.net/report/prefixes>

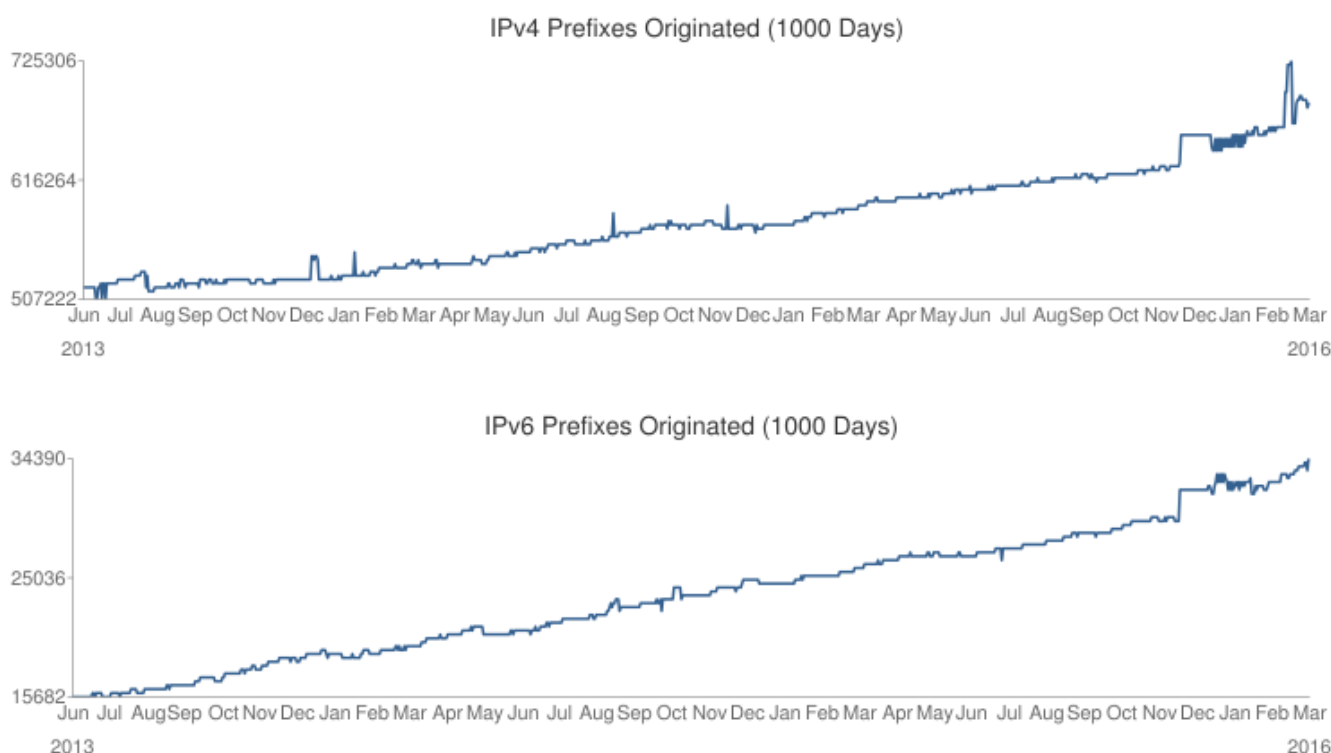


Рисунок 1. Динамика числа IP-префиксов анонсируемых в Интернете.

Согласно RFC-1918 некоторые диапазоны адресов не используются для маршрутизации в Интернете. Назовите их. А для чего они должны использоваться? Анонсируют ли «серые» адреса BGP-маршрутизаторы? <http://bgp.he.net/report/bogons>

Задание 2.

Шаг 1. Выяснить IP-адрес, под которым вас видят в Интернете. Можно ли для этого использовать утилиту командной строки `ipconfig`?

Можно снова использовать <http://bgp.he.net/>. Можно запрос в google «what is my ip».

Перейдем по ссылке <https://www.nic.ru/whois/?query=urfu.ru>

Какой организации согласно данным из БД ru-центра принадлежит этот домен? Какую еще информацию можно извлечь? Находим строки

```
domain:          URFU.RU
nserver:         ns1.urfu.ru. 212.193.66.21
nserver:         ns2.urfu.ru. 212.193.82.21
nserver:         ns3.urfu.ru. 212.193.72.21
```

Снова делаем запрос к ru-центру:

<https://www.nic.ru/whois/?query=212.193.66.21>

<https://www.nic.ru/whois/?query=212.193.82.21>

Что видим в результате?! Можно ли в этом выводе найти свой номер АС?

Шаг 2. Используя открытые БД RIR'а RIPE, выяснить, кто анонсирует префиксы 212.193.80.0/20. См. рис 2. <https://stat.ripe.net/212.193.80.0%2F20>

Видим, что этот префикс является частью большего префикса. Какого? Как это интерпретировать? Объяснить содержимое виджетов (внизу каждого виджита есть кнопка «info»).

Шаг 3. Сделать зарос <https://stat.ripe.net/AS5468>. Объяснить результаты. Объяснить содержимое виджетов. Рассмотреть вкладки At a Glance и Routing. Остальные – для интересующихся.

Что такое Routing Information Service (RIS)? Кто такие RIS коллекторы? Для чего они нужны и как работают? Что такое «BGP Full view» или иными словами «BGP Full table»?

Шаг 4. Что такое Looking glass? Используя сервис <http://www.msk-ix.ru/network/lookingglass.html>, выяснить, как именно из других АС видят нашу АС, см. рис. 3. То же сделать с других серверов, расположенных по всему миру.

Шаг 5. На сервисе stat.ripe.net рассмотреть вкладку Routing, виджет «BGP Update Activity», отобразить обновления в динамике, используя BGPlay. Интерпретировать результаты. Научиться «читать» цвета и легенду, научиться управлять BGPlay'ем.

212.193.80.0/20 Search

permalink

At a Glance (4)

Routing (8)

DNS (2)

Anti Abuse (2)

Database (9)

Geographic (2)

Activity (4)

Suggestions (1)

+ MyView ?

Prefix Overview (212.193.80.0/20)

✓ Announced

This prefix is part of 212.193.64.0/19 announced by

AS5468

"URFU Yeltsin UrFU, Ural Federal University, RU"

RIR	Status	Registration	Country
RIPE NCC	ALLOCATED	1999-05-12	RU

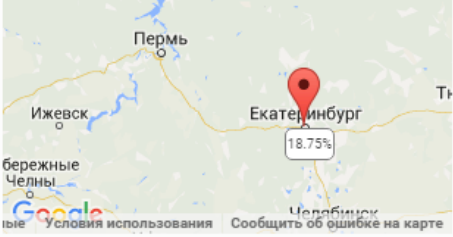
Show IANA Registry Information

Showing results for 212.193.64.0/19 as of 2016-03-06 08:00:00 UTC

⚠ Given resource is not announced but result has been aligned to first-level less-specific (212.193.64.0/19).

source data embed code permalink info

Geoloc (212.193.80.0/20)



▶ **Geoloc details**

ⓘ Data is based on MaxMind's GeoLite City data set and valid for the stated query time (see below)

Showing results for 212.193.80.0/20 as of 2016-03-01 00:00:00 UTC

source data embed code permalink info

Routing Status (212.193.80.0/20)

⚠ 212.193.80.0/20 was not globally visible as exact match in BGP by any of the RIS peers at observation time stated below

Рисунок 2. Результаты запроса к stat.ripe.net.

bgp summary
prefix info
neighbor info
rejected routes
community

msk-rs1.ripn.net
▼
212.193.80.0/20
➔

Роут-сервер
Префикс сети или IP-адрес

msk-rs1.ripn.net

```

> sh ip bgp 212.193.80.0/20
*** Note: the first route is the BEST ***
212.193.64.0/19 via 195.208.208.44 on ixp0 [R3267x1 2016-02-16 23:33:35] * (100) [AS5468i]
  Type: BGP unicast univ
  BGP.router_id: 193.232.80.3
  BGP.origin: IGP
  BGP.as_path: 3267 5468
  BGP.next_hop: 195.208.208.44
  BGP.med: 10
  BGP.local_pref: 100
  BGP.community: (0,2848) (0,2895) (0,3218) (0,5429) (0,5567) (0,5568) (0,6854) (0,15169)

```

Рисунок 3. Результаты запроса к Looking glass серверу, расположенному в Москве.

Задание 3.

Обсуждение со студентами: Что такое протокол whois? Для чего нужен? Тексториентированный или биториентированный? Формат ответа регламентирован или нет?

Используя утилиту telnet командной строки подключиться к сервису whois.ripe.net, TCP порт 43. Подать запрос: **212.193.82.21**. Указание: запрос надо отправлять быстро, лучше не набирать адрес, а вставлять из буфера. Отчего такой некрасивый вывод?

Можно использовать putty или ее аналог.

Задание 4. На любом разумном языке программирования написать утилиту для опроса RIR'a RIPE. По IP-адресу получать номер АС и страну. Протестировать на IP-адресах из ниже приведенных доменов, заполнить таблицу.

Доменное имя	IP-адрес	Номер АС
e1.ru		
www.nic.ru		
www.msk-ix.ru		
kontur.ru		

Будет ли работать эта утилита на адресах из Азии, Америки, Африки?