Влияние сетевых аномалий на доступность ресурсов

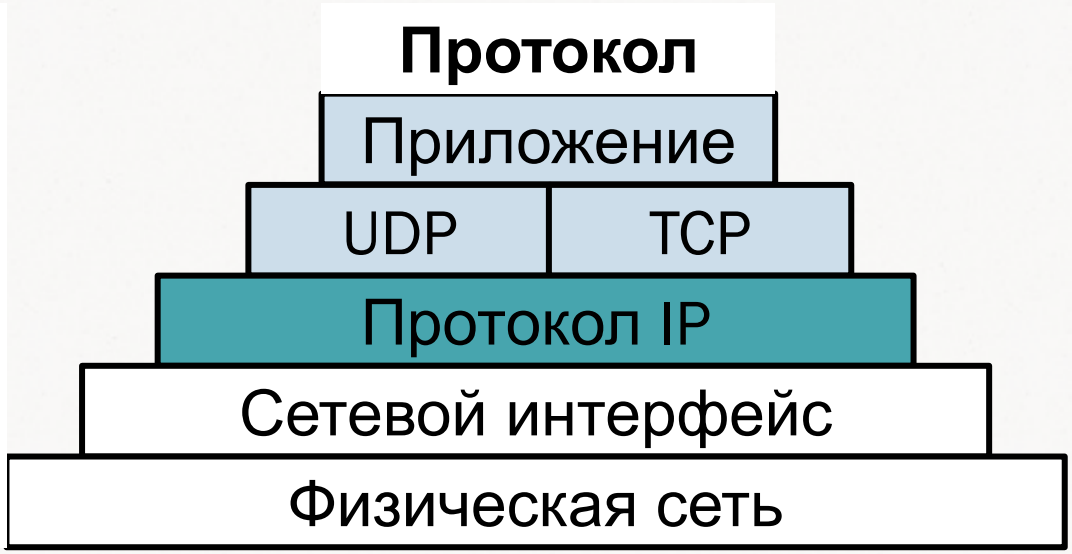
Alexander Azimov
<aa@highloadlab.com>
Highload Lab

Уровни протокола TCP/IP

Уровень
Прикладной
Транспортный
Сетевой
Канальный
Физический

Уровни протокола TCP/IP

Уровень
Прикладной
Транспортный
Сетевой
Канальный
Физический



Сетевые аномалии

1. Ошибки в настройке маршрутизаторов;
2. Циклы маршрутизации BGP;
3. Проблемы на уровне СПД.

Default route

- 14078 уязвимых префиксов;
- Может быть использовано для увеличения плеча DoS атаки (* TTL)
  - Атака на исчерпание канала;
  - А за трафик еще и платить ;)

Усилители DDoS атак

- 744 уязвимых префиксов;
- AC может быть использована в качестве усилителя DoS атаки
  - Атака нескольких AC одновременно;

Циклы маршрутизации BGP

Встроенная защита от статических циклов

Динамические циклы!

BGP Циклы

- 2347 уязвимых префиксов;
- Результат:
  - Частичная/полная недоступность целевой сети;
  - Шум сообщений BGP.

У них проблемы…

AS174	AS3356	AS7018	AS6939	AS701
AS3549	AS209	AS4323	AS1239	AS12389
AS2848	AS3257	AS6461	AS2914	AS8468
AS23148	AS8447	AS20485	AS6830	AS8220
AS8928	AS3303	AS4589	AS42708	AS6453
AS6730	AS31130	AS3491	AS3320	AS8218
AS286	AS702	AS3561	AS20764	AS31323
AS20632	AS4766	AS680	AS29686	AS5089
AS10026	AS12350	AS2516	AS3786	AS12741
AS7575	AS1916	AS2273	AS9498	AS1785

И более чем 5к других АС!

Примеры

AC174

- Увеличение плеча DDoS в 17 раз
- Default route: 25 уязвимых префиксов

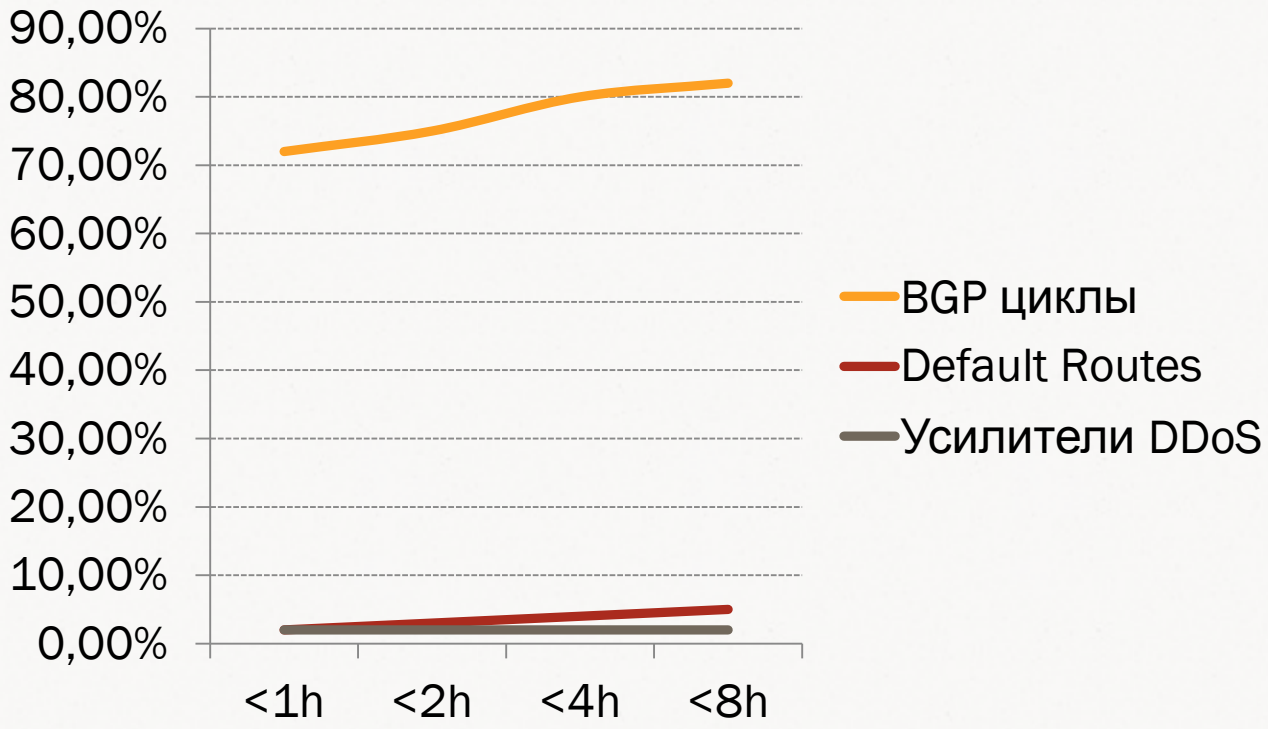
AC3356-AC3549

- Увеличение плеча DDoS в 8 раз
- BGP циклы: 12 prefixes affected
- Default route: 86 уязвимых префиксов

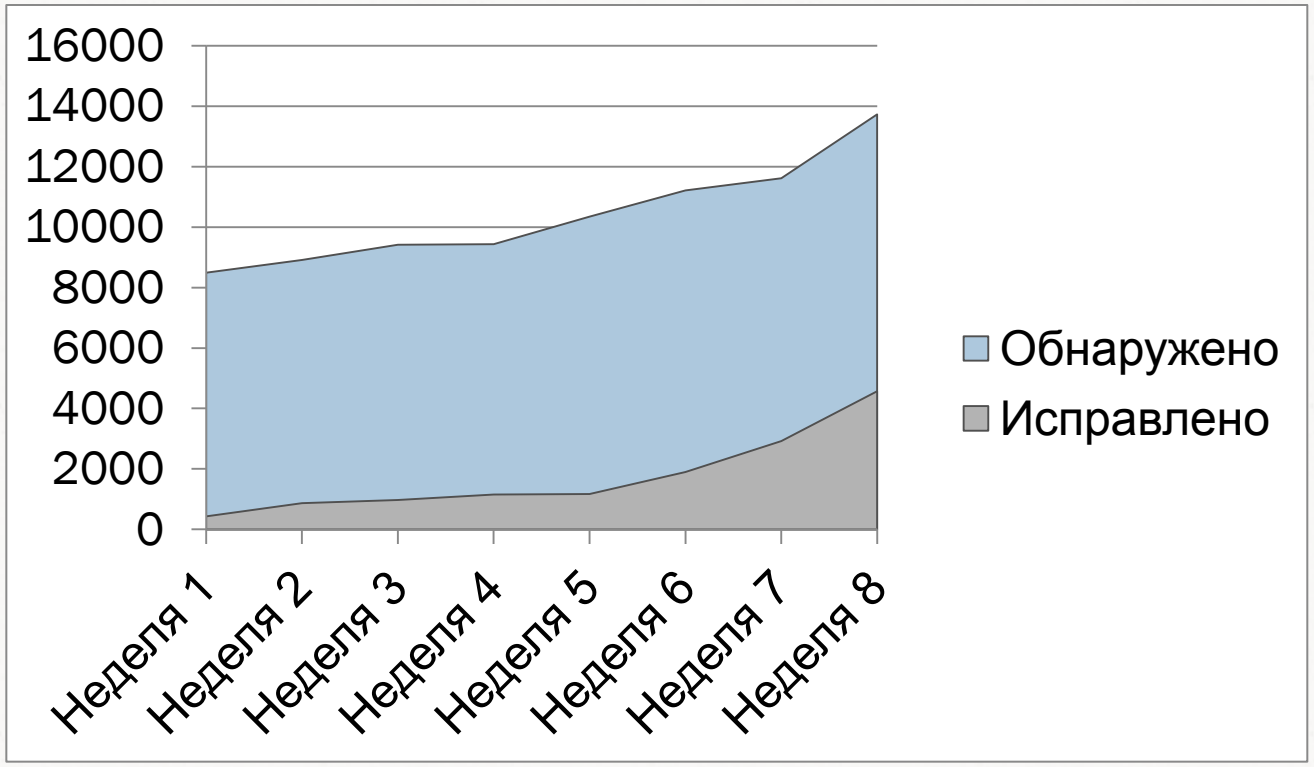
ENOG

- Default route 2204;
- BGP циклы 213;
- Усилители DDoS атак 22
  максимально в 11 раз.

Продолжительность



Тренд


16000
14000
12000
10000
8000
6000
4000
2000
0
Неделя 1
Неделя 2
Неделя 3
Неделя 4
Неделя 5
Неделя 6
Неделя 7
Неделя 8
Обнаружено
Исправлено

Робин Гуд

Hello.

During our research project we have detected IP address "*.*.*.*" in AS***, which multiplies ICMP packets. 11 times is a mean value.

It is dangerous vulnerability because this IP could be used by attackers to N-times increase DoS attack.

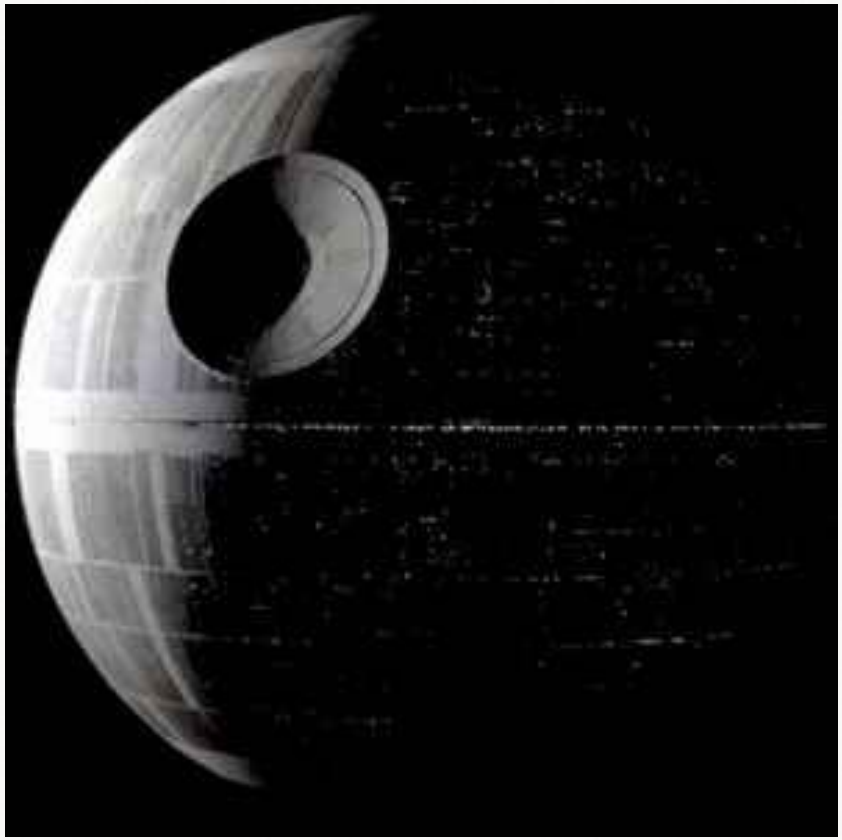
This could be harmful for your own network infrastructure and also break down attacked network.

Could you tell me for what purpose your router was configured by such way?

Hello

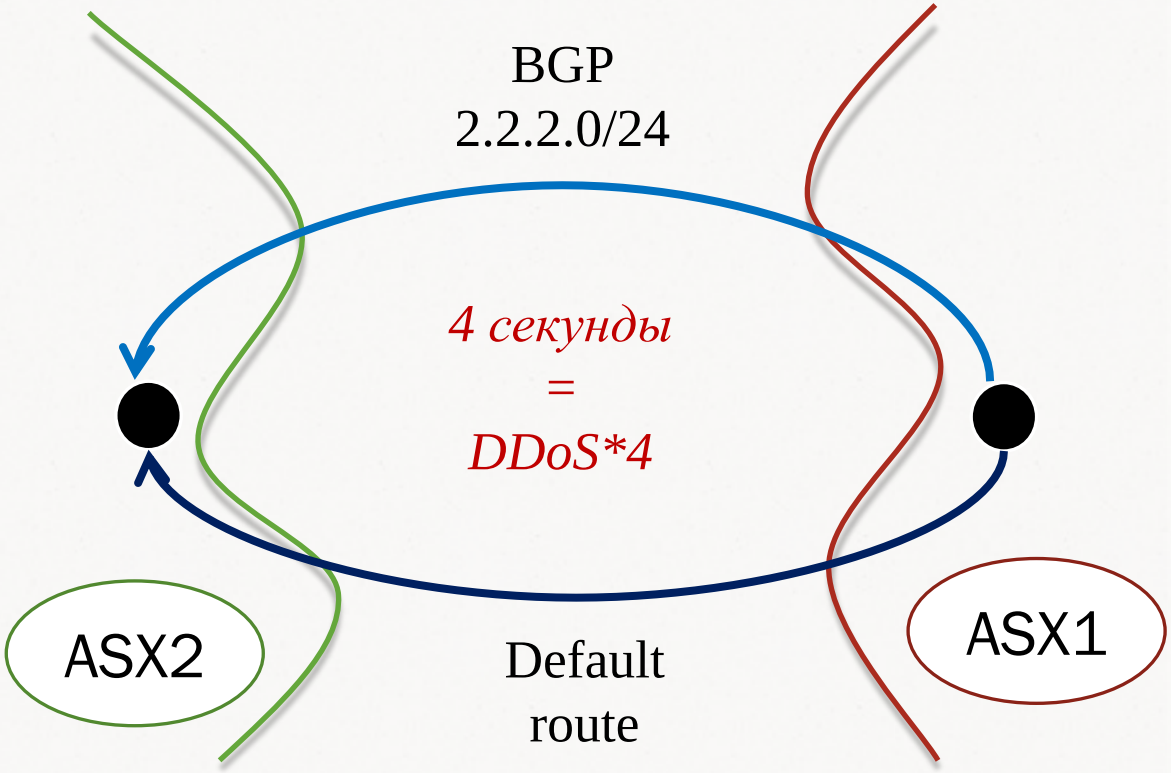
This is assigned to one of our customers. We cannot see how there equipment is configured. If you believe this is in violation of our Acceptable use policy you can email abuse@***.com to report that.

Атака на сетевом уровне

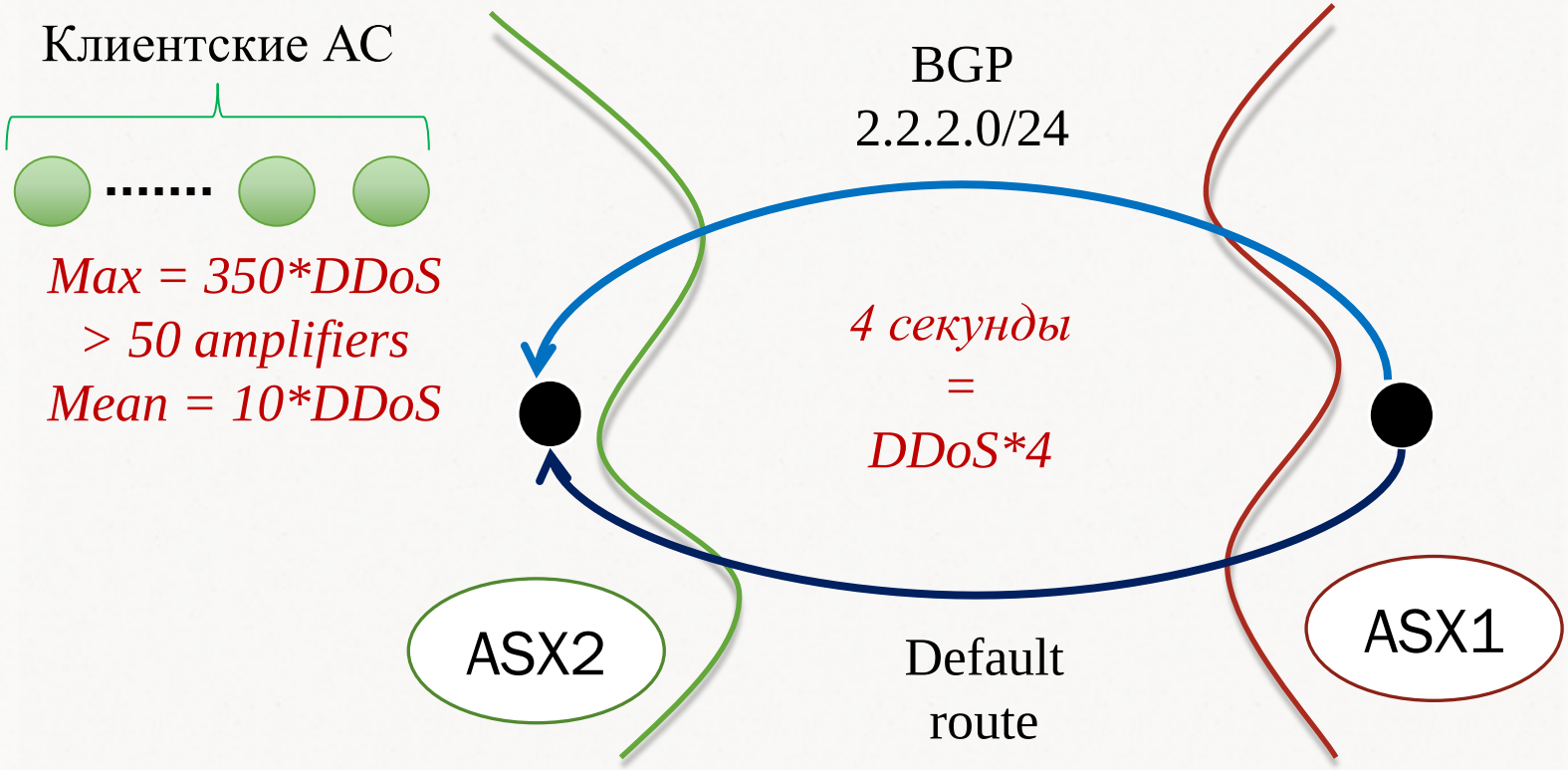


Атака на сетевом уровне

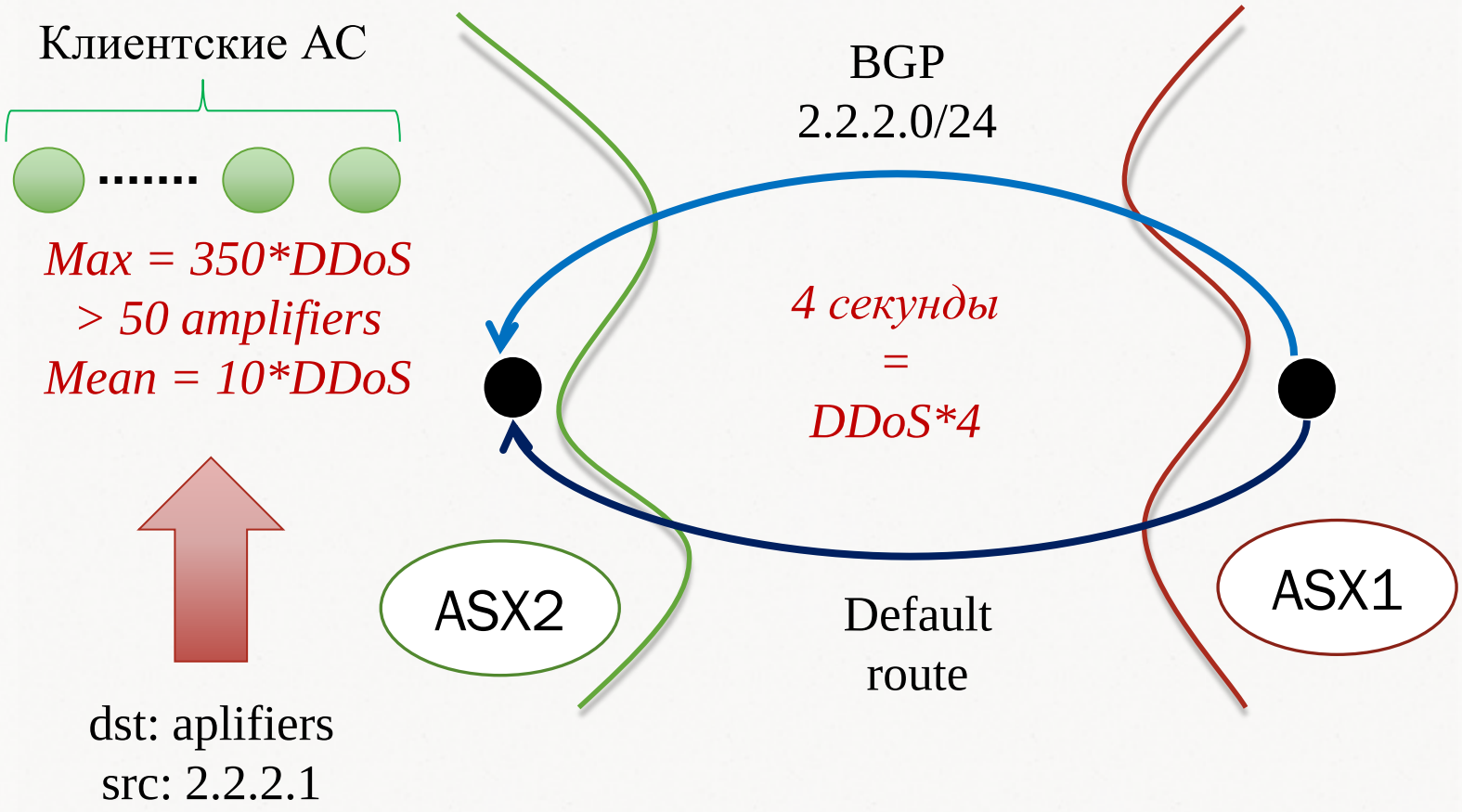
В «сердце» Интернета



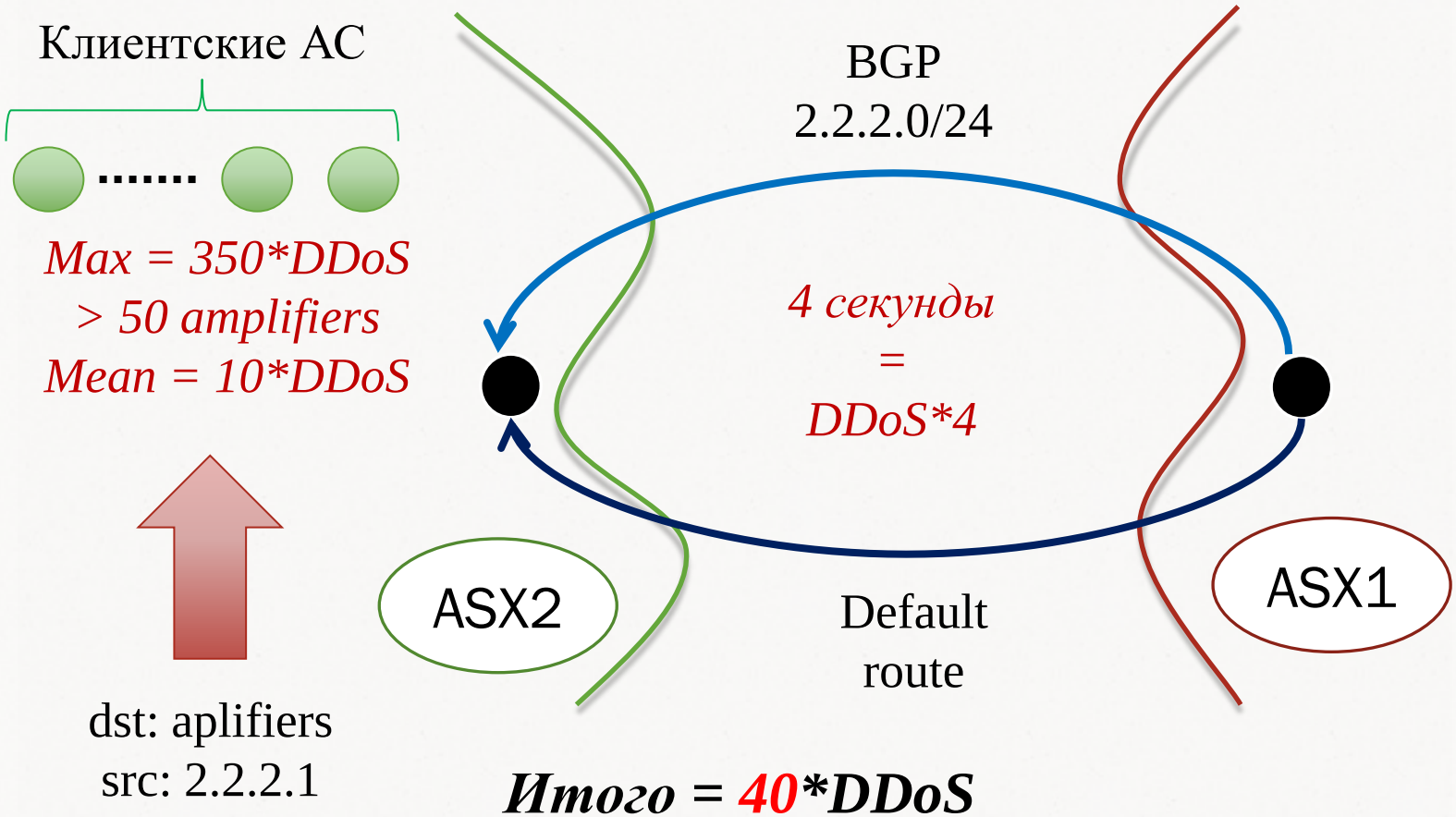
В «сердце» Интернета



В «сердце» Интернета



В «сердце» Интернета



Результаты

- Проблемы клиентской сети – это ваши проблемы;
- Проблемы сети поставщика – это тоже ваши проблемы;
- Нестабильность сети может быть невидима со стороны АС-источника.
- У нас есть система мониторинга. Мы готовы предоставить информацию бесплатно.

Проверяйте свою сеть. Дважды