



Глобальный сбой в работе Facebook* 4 октября 2021 года

* признана экстремистской организацией, ее деятельность на территории России запрещена.

Что произошло?

4 октября 2021 года в 15:40 UTC произошел один из самых крупных сбоев огромной социальной сети (около 2 млрд активных пользователей!)

“Facebook can't be down, can it?”, we thought, for a second. -- инженеры онлайн-сервиса Cloudflare*

Первые догадки

- Вердикт "SERVFAIL" спустя 10 минут с момента сбоя
- Сначала инженеры Cloudflare подумали, что причина сбоя на их стороне
- Инженеры подтвердили что Facebook*, а также принадлежащие ему сервисы Instagram* и Whatsapp, действительно упали, DNS-имена перестал работать, IP-адреса стали недоступны
- Как итог: проблема случилась из-за неполадки в ходе планового обслуживания дата-центров. Что произошло, и как это повлияло -- разберемся дальше

* признана экстремистской организацией, ее деятельность на территории России запрещена.

Встречайте BGP

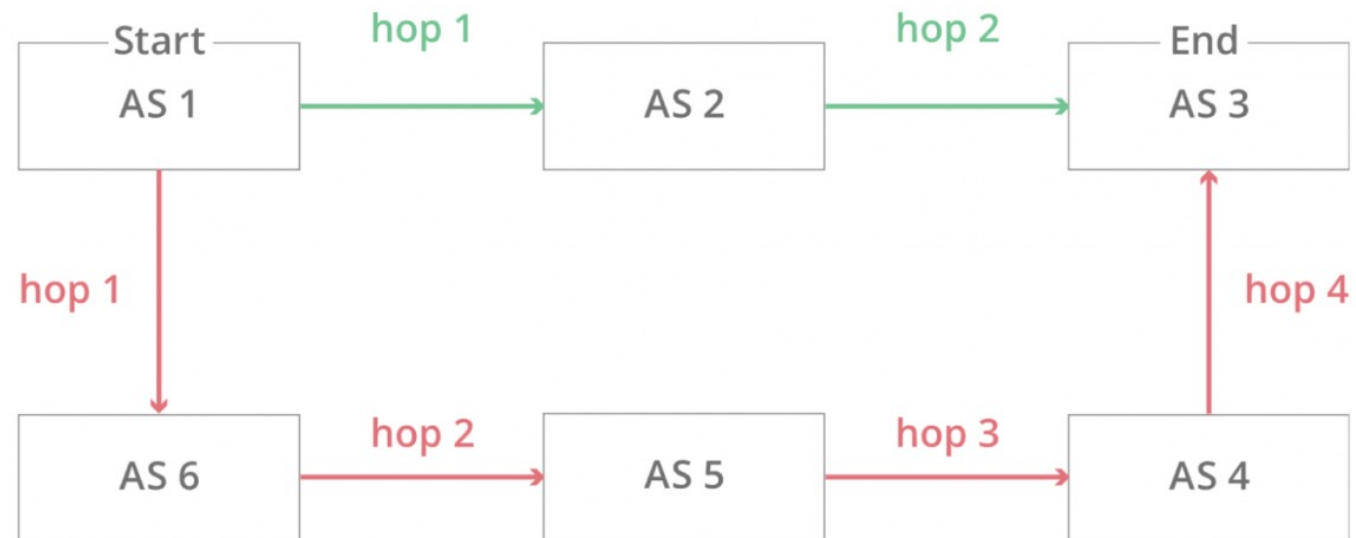
BGP — это «протокол граничного шлюза» (*Border Gateway Protocol*). Это механизм для обмена информацией о маршрутизации между автономными системами (AS) в интернете. У больших роутеров, благодаря которым работает интернет, есть постоянно обновляемые списки возможных маршрутов, используемых для доставки каждого сетевого пакета до мест их назначения. Без BGP интернет-роутеры не знают, что делать, и интернет просто не будет работать.

Автономные системы

Option 1:



Option 2:



И что же дальше?

«В 16:58 UTC мы заметили, что Facebook* перестал анонсировать маршруты для своих DNS-префиксов. Это означало, что по меньшей мере DNS-серверы Facebook* были недоступны», -- со слов инженеров Cloudflare

По этой причине DNS-ресолвер Cloudflare (уже упомянутый 1.1.1.1) не мог отвечать на запросы, требующие выдать IP-адрес для домена facebook.com* или instagram.com*.

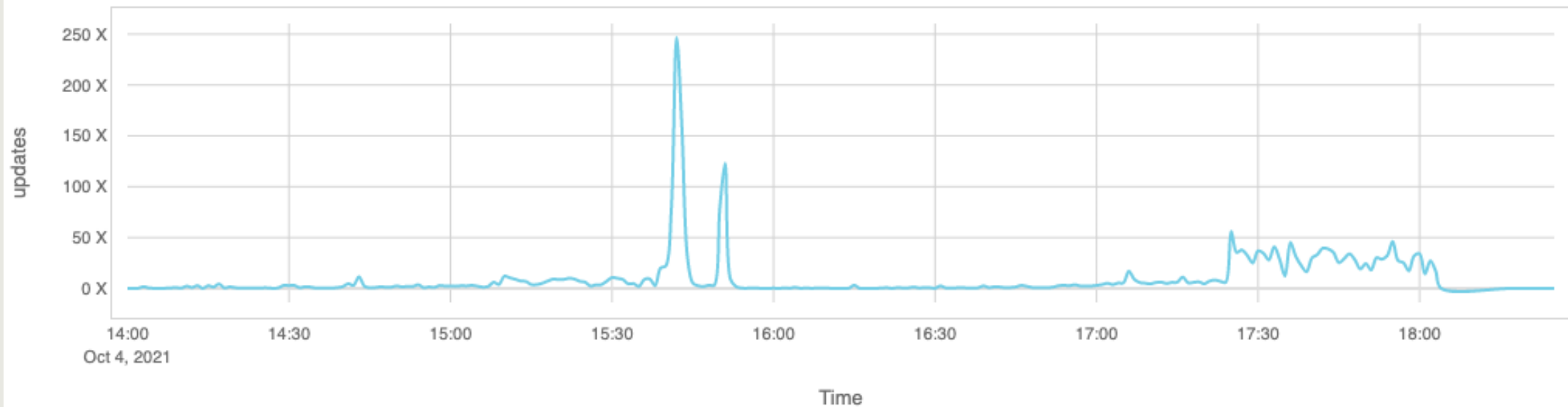
```
route-views>show ip bgp 185.89.218.0/23
% Network not in table
route-views>
```

```
route-views>show ip bgp 129.134.30.0/23
% Network not in table
route-views>
```

* признана экстремистской организацией, ее деятельность на территории России запрещена.

И что же дальше?

BGP updates Facebook*



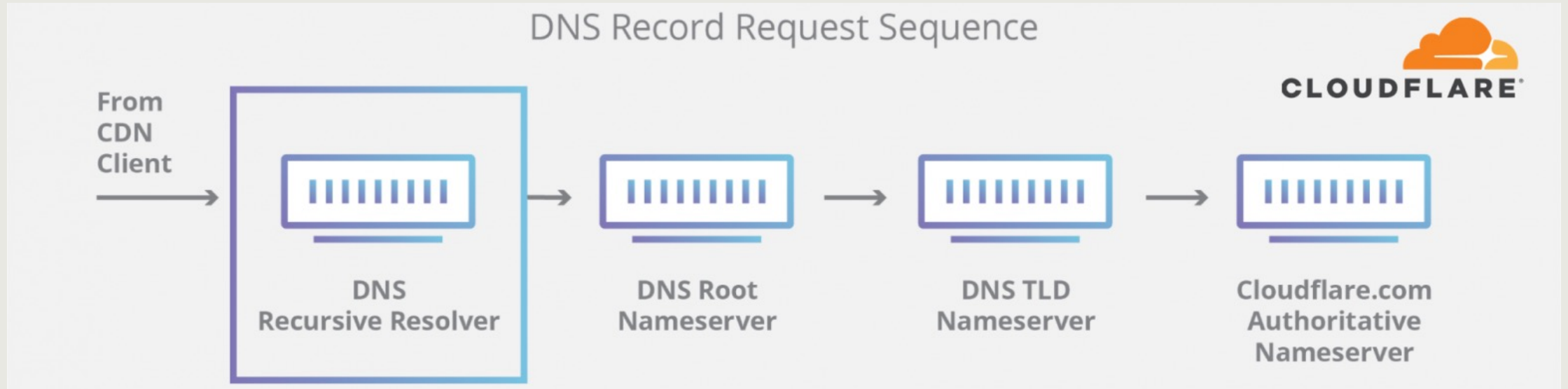
* признана экстремистской организацией, ее деятельность на территории России запрещена.

DNS тоже в деле

Прямым последствием этого события стала невозможность для DNS-ресолверов со всего мира получать IP для связанных с проектами доменных имён:

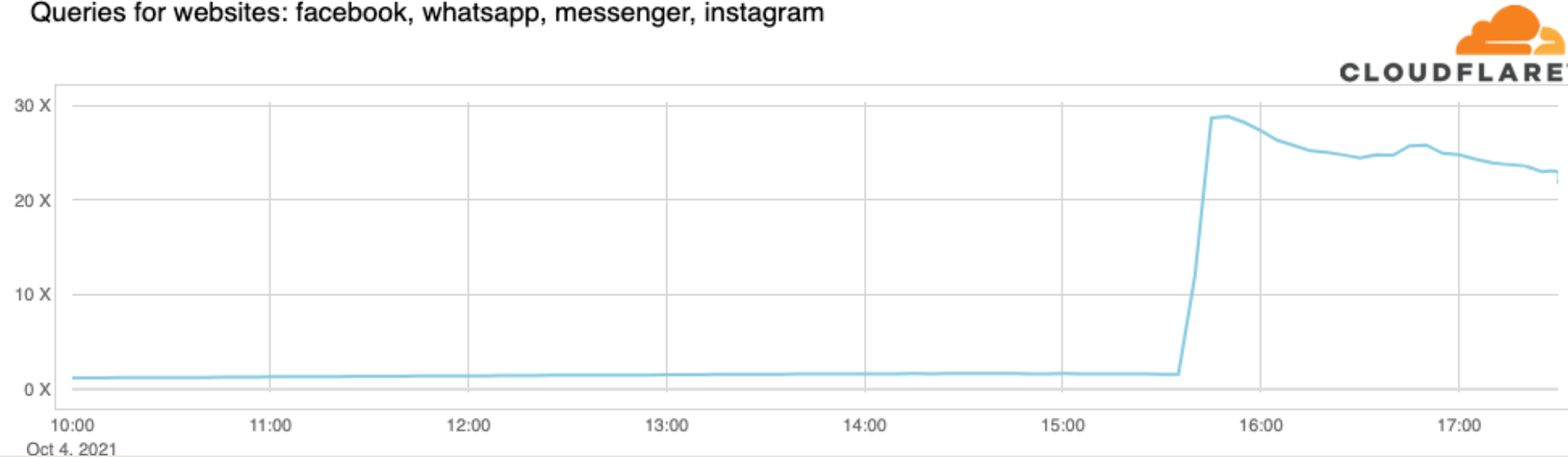
```
→ ~ dig @1.1.1.1 facebook.com *
;; ->HEADER<<- opcode: QUERY, status: SERVFAIL, id: 31322
;facebook.com.          IN  A
→ ~ dig @1.1.1.1 whatsapp.com
;; ->HEADER<<- opcode: QUERY, status: SERVFAIL, id: 31322
;whatsapp.com.          IN  A
→ ~ dig @8.8.8.8 facebook.com *
;; ->HEADER<<- opcode: QUERY, status: SERVFAIL, id: 31322
;facebook.com.          IN  A
→ ~ dig @8.8.8.8 whatsapp.com
;; ->HEADER<<- opcode: QUERY, status: SERVFAIL, id: 31322
;whatsapp.com.          IN  A
```


DNS тоже в деле



И человеческий фактор

Queries for websites: facebook, whatsapp, messenger, instagram



Тогда почему так долго?

Встает закономерный вопрос: почему восстановление проходило 7 часов, если проблему удалось выявить значительно быстрее?

Потому что. . .

Все дело заключалось в том, что «неаккуратное» одновременное включение большого количество дата-центров могло негативно сказаться на тех самых серверах из-за скачка энергопотребления.

Но инженеры подготовились

«К счастью, к этому событию мы хорошо подготовились благодаря «шторм-тестам», которые мы проводим уже долгое время. В ходе таких учений мы имитируем серьезный системный сбой, переводя службу, центр обработки данных или весь регион в автономный режим, проводя стресс-тестирование всей задействованной инфраструктуры и программного обеспечения. Опыт этих учений придал нам уверенности и опыта, чтобы вернуть все в рабочее состояние и тщательно управлять растущими нагрузками. В конце концов, наши сервисы восстановились относительно быстро без каких-либо дальнейших общесистемных сбоев»

Спасибо за внимание!