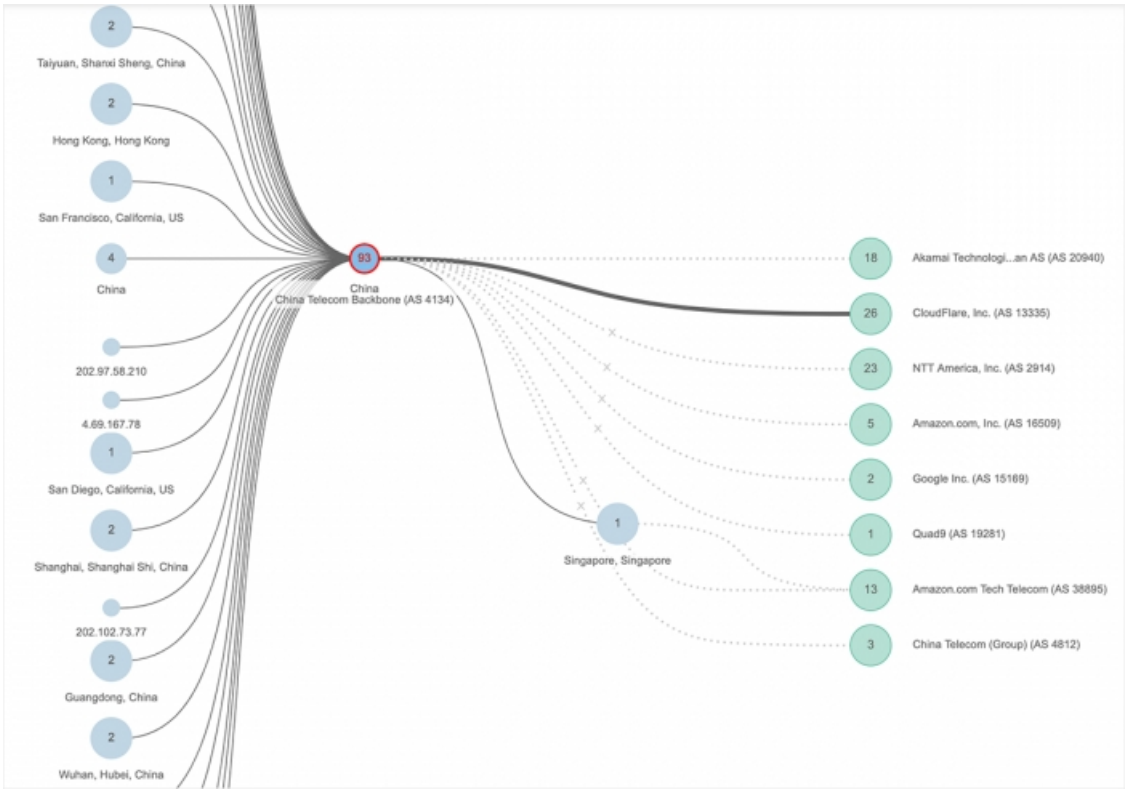
Чем запомнился 2019 год: крупнейшие сбои в работе интернета

В 2019 году сервис ThousandEyes, специализирующийся на мониторинге Глобальной сети, неоднократно регистрировал крупные сбои в работе интернета, последствия которых ощущали организации и потребители по всему миру. Специалисты недавно подвели итоги года и рассказали о самых серьезных перебоях. Большинство из них пришлись на лето и в какой-то мере затронули практически все ведущие технологические компании.



13 мая 2019 года - China Telecom

Хотя отказ сети China Telecom в середине мая - не самый масштабный в прошлом году, он запомнился своими глобальными отголосками и показал, что сфера влияния одного из ведущих китайский провайдеров простирается далеко за пределы КНР.



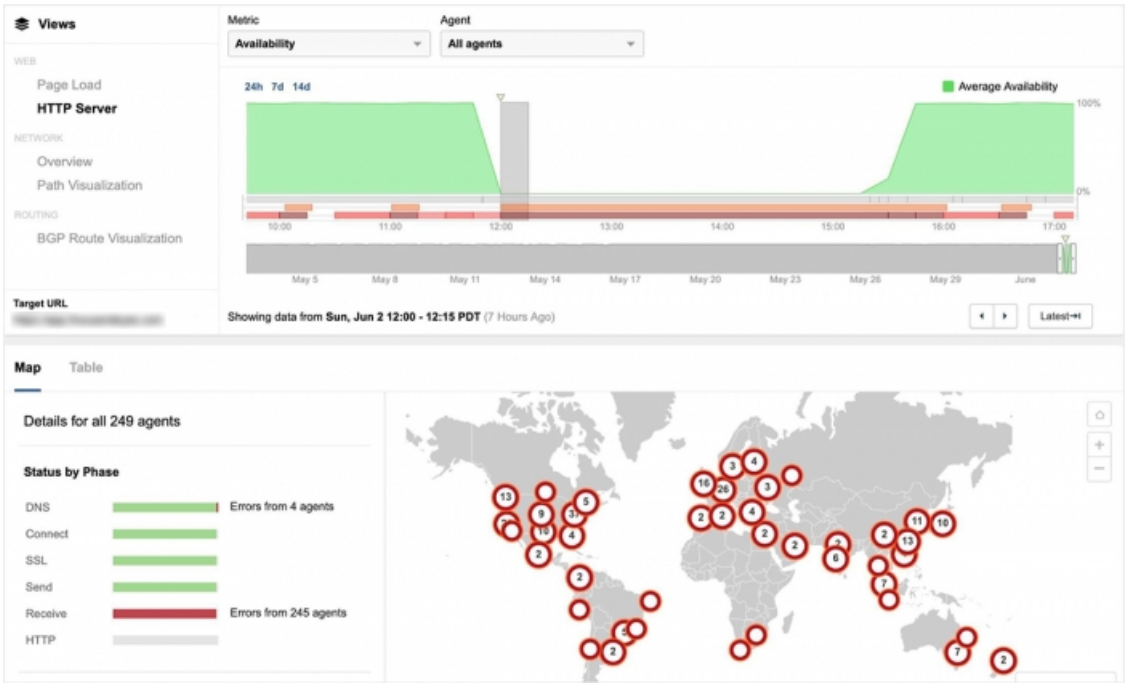
13 мая на протяжении почти пяти часов в магистральной сети China Telecom наблюдались значительные потери пакетов. Пострадала, в основном, инфраструктура оператора в материковом Китае, но последствия сбоя коснулись также сингапурской сети China Telecom и нескольких точек в США, в том числе в Лос-Анджелесе. В целом была нарушена работа более ста сервисов. Перебои отмечали пользователи Apple, Amazon, Microsoft, Slack, Workday и SAP.

Инцидент наглядно проиллюстрировал, как действующая в отношении китайских пользователей политика цензурирования может выходить за границы Поднебесной и затрагивать страны с совершенно с другим отношением к интернету и принципами его использования.

2 июня 2019 года - Google Cloud

Череда летних сбоев началась 2 июня 2019 года. В этот день облачная платформа Google Cloud Platform (GCP) пережила серьезный отказ сети, который отразился на работе сервисов, размещенных на узлах в несколько GCP-регионах или зонах - us-west, us-east и us-central. Сбой продолжался больше четырех часов и затронул собственные приложения Google, такие как GSuite и YouTube.

Спустя несколько дней Google разместила у себя на сайте отчет об инциденте, но специалисты ThousandEyes опубликовали информацию о сбое и его масштабах раньше, поскольку успели отследить происходившее в режиме реального времени.



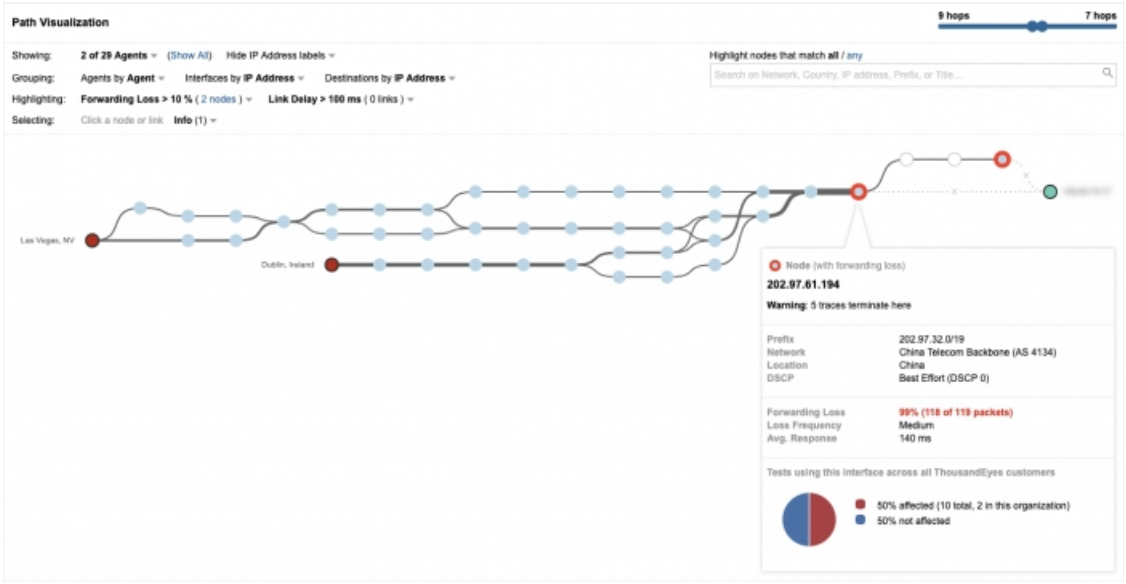
Начиная примерно с 9 часов утра по Североамериканскому восточному времени, наблюдалась 100-процентная потеря пакетов при попытках подключиться к сервисам, размещенным в GCP-зоне us-west2-a (Лос-Анджелес, Калифорния, США). Аналогичные потери происходили и при обращении к сайтам на серверах в отдельных частях зоны us-east, включая us-east4-c (Эшберн, Северная Вирджиния, США).

Как установили в ThousandEyes, к полной недоступности отдельных частей сети Google привело случайное отключение системы управления сетью Google (Google’s network control plane). В корпорации позднее пояснили, что во время сбоя доступность или недоступность сервисов определяли автоматические политики доступа через незатронутые участки сети.

6 июня 2019 года - WhatsApp

В этот день множество пользователей WhatsApp по всему миру испытали затруднения с подключением к сервису. Анализ ThousandEyes сразу же показал, что недоступность вызвана 100-процентной потерей пакетов.

В дальнейшем выяснилось, что основной причиной потерь стала крупная утечка трафика в сеть китайской China Telecom, которая блокирует трафик, имеющий отношение к Facebook и любыми связанным с американской соцсетью сервисами.



Виновницей инцидента стала швейцарская колокейшн-компания Safe Host, которая анонсировала лучший BGP-маршрут к WhatsApp и тысячам ее IP-префиксов через свою автономную систему AS21217. Анонсированные Safe Host маршруты были приняты China Telecom (AS4134) и далее распространены другим интернет-провайдерам, таким как Cogent. Пользователям, чей трафик был перенаправлен через Cogent к China Telecom, сервисы Facebook стали полностью недоступны.

24 июня 2019 года - Cloudflare

Всего через пару недель после масштабной утечки BGP-маршрутов, затронувшей пользователей WhatsApp, произошел еще один похожий, только гораздо более серьезный инцидент.

24 июня 2019 года из-за ошибочного BGP-анонса у CDN-провайдера CloudFlare, услугами которого пользуются миллионы сайтов, на протяжении почти двух часов был недоступен ряд крупных сервисов, в том числе сайт Reddit, стриминговая платформа Twitch, мессенджер Discord, Amazon Web Services (AWS) и другие.

Анализ ThousandEyes показал, что крупная утечка маршрутов затронула многочисленные IP-префиксы. Первоисточником сбоя в маршрутизации трафика стал транзитный провайдер DQE Communications, использовавший в своей сети BGP Optimizer - инструмент, который разбивает блоки IP-адресов на более мелкие, конкретизируя маршрутизацию внутри сети. Если проводить аналогию с географией, вместо области или штата он указывает на конкретный город в области или штате. Более "конкретные" маршруты всегда имеют более высокий приоритет, чем "общие".



DQE передал эти маршруты своему клиенту, Allegheny Technologies, у которого также было настроено подключение к транзитному провайдеру Verizon. Приоритетные маршруты перетекли к нему, и Verizon стал транслировать их на весь интернет, усугубляя последствия.

В результате около 15 процентов глобального трафика Cloudflare пошло через Verizon к DQE, и те не справились с такой нагрузкой на свои сети.

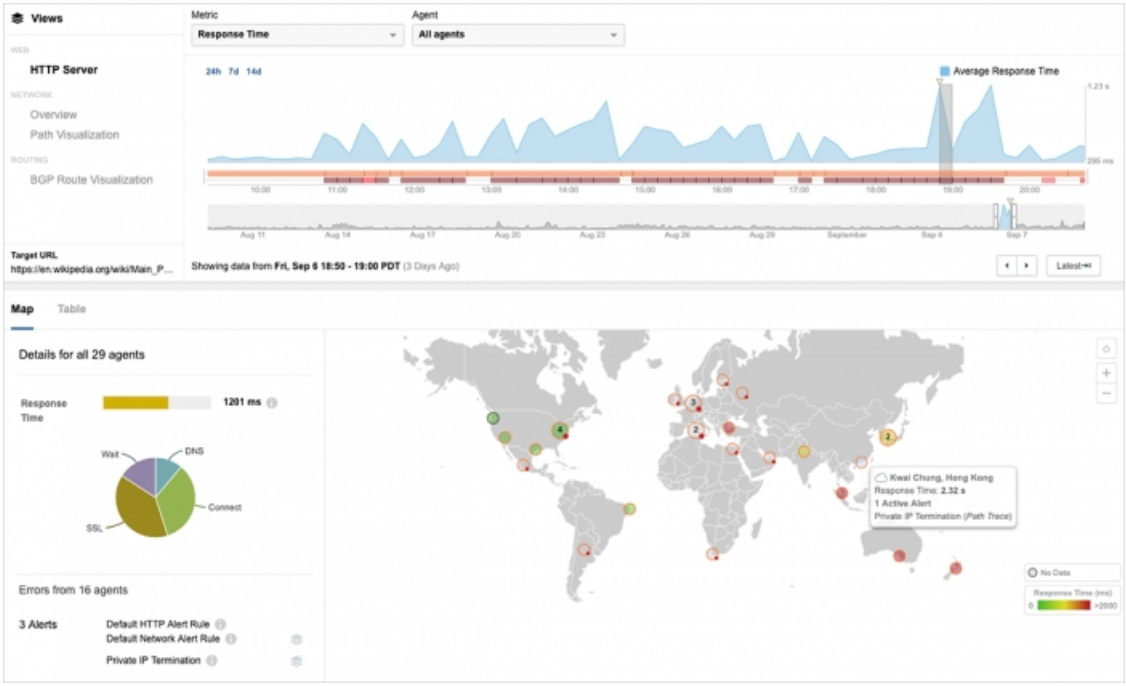
4 июля 2019 года - сервисы Apple

В этот день, начиная примерно в 9 утра по тихоокеанскому времени, доступ к сайту Apple и некоторым ее сервисам был затруднен в связи со значительной потерей пакетов длившейся более

полутора часов. Специалисты ThousandEyes установили, что потери спровоцировала череда быстрых перестроений маршрутов BGP (BGP route flap). Хотя сервисами Apple пользуются достаточно много людей, сбой не вызвал большого числа жалоб из-за того, что произошел утром выходного дня (4 июля - День независимости США).

6 сентября 2019 года - DDoS-атака на Wikipedia

В этот день Wikipedia ушла в офлайн и была недоступна в целом ряде стран из-за мощной и продолжительной атаки, длившейся почти девять часов.



Как известно, DDoS-атаки могут перегружать веб-инфраструктуру атакуемого объекта и сетей поставщиков услуг, что ведет к потере пакетов. Именно это и случилось с онлайн-энциклопедией. Во время сбоя специалисты ThousandEyes регистрировали существенные проблемы с доступом к HTTP-серверам Wikipedia по всему миру, а также резкое увеличение времени ответа HTTP. Также отмечалась потеря до 60% пакетов, что также препятствовало доступу к популярному ресурсу.