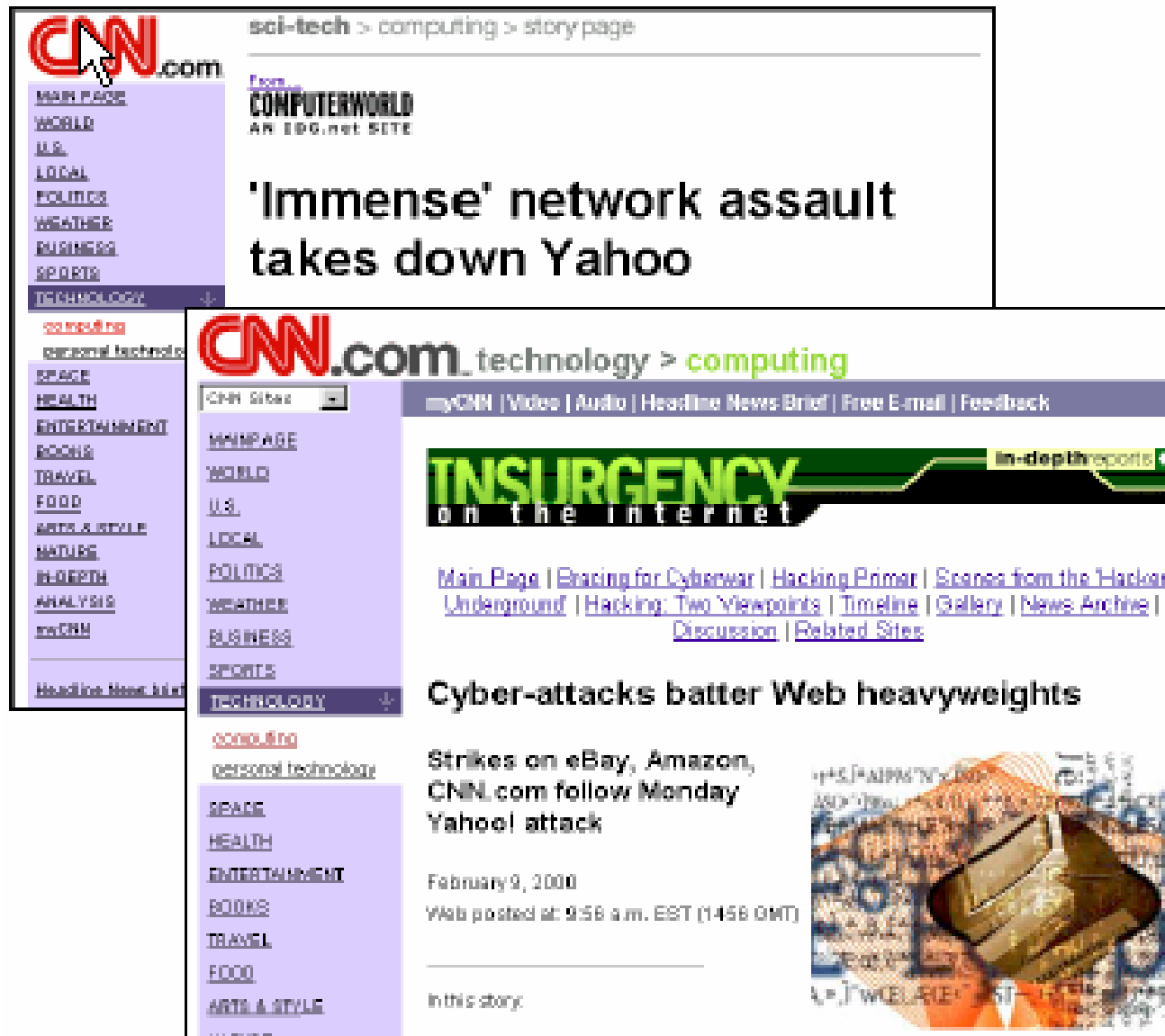


Обнаружение и реагирование на инциденты в области безопасности

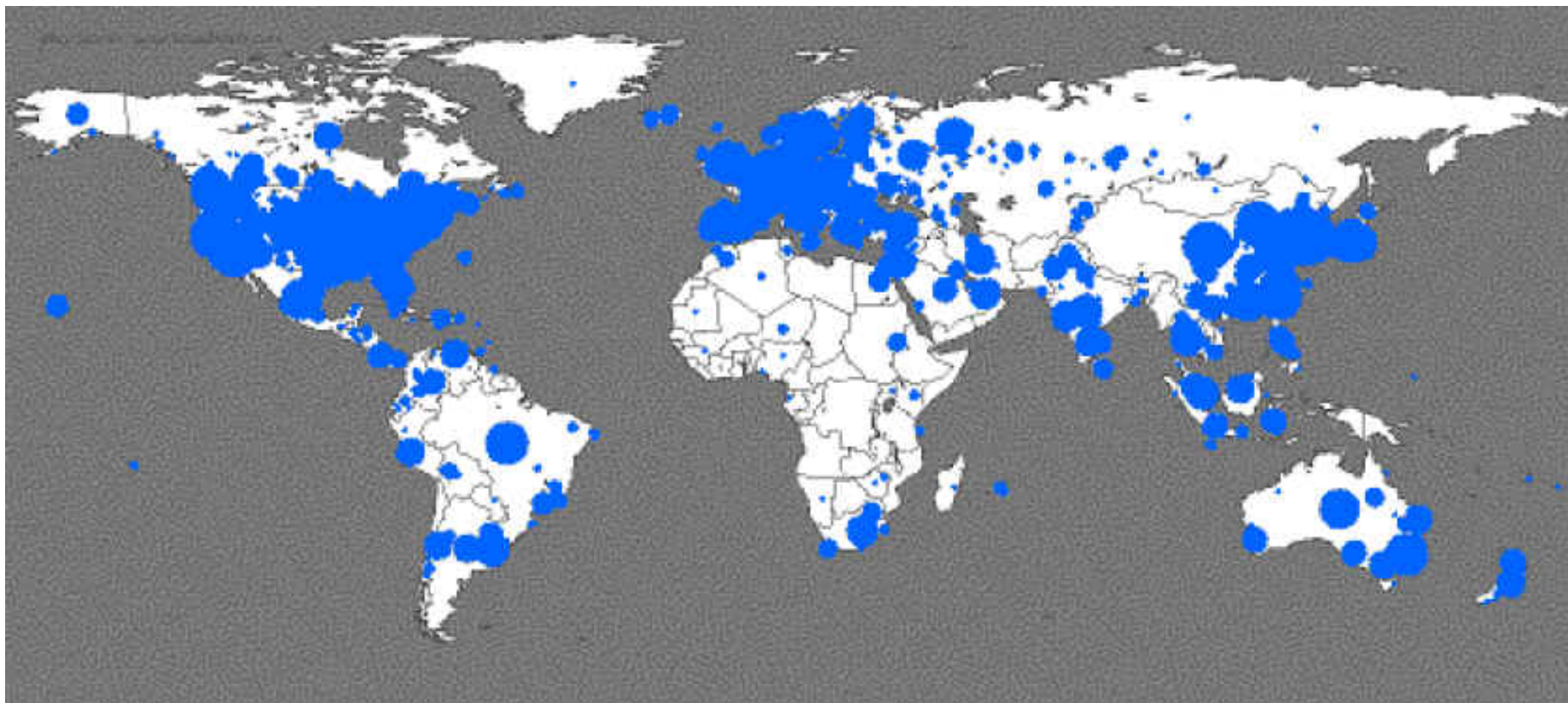
Владислав Кушка
Системный инженер
Ukrainian Mobile Communication

vkushka@umc.com.ua

Точка отсчета – 9 Февраля 2000



Январь 2003: The SQL Slammer Worm



- Количество инфицированных удваивалось каждые 8.5 секунд (!)
- Скорость распространения в 100 больше чем у Code Red
- В пике сканировалось 55 000 000 хостов в секунду.
- Через 5 минут 27 000 000 человек остались без мобильной связи
- Убытки уже через 5 минут стали исчисляться миллионами долларов

Атаки становятся бизнесом

DDOS услуги. (GPI forum; job) Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://www.gpi.ru/boards/job/messages/644.html Go

[Ответы](#) [Послать ответ](#) [GPI forum; job](#)

DDOS услуги

Автор DDOS 11 октября 2003 в 21:14:17

Выполняем качественно и быстро DDOS на любой сайт, быстро,
и на любой срок.

Простенький сайт - цена ~80-90\$. Серьезнее, дороже.

icq: 215714

р.з. По желанию, сделаем демо.

Ответы

Послать ответ

Имя:

E-Mail:

Тема:

Ссылка (URL):

Текст ссылки:

Картинка (URL):

Усложняется профиль атак

Distribution	Management	# Attackers (Bandwidth)	Type of attack	Protection
<ul style="list-style-type: none"> –Email attach –Download from questionable site –via "chat" –ICQ, AIM, IRC –Worms 	Via botnets	~X00,000 attackers (X-X0 Gbps)	<ul style="list-style-type: none"> •Legitimate requests •Infrastructure elements (DNS, SMTP, HTTP...) 	<ul style="list-style-type: none"> •Blackhole (?) •ACL (?) •DDoS solutions •Anycast (?)
<ul style="list-style-type: none"> –Email attach –via "chat" ICQ, AIM, IRC... 	Manually	~X00-X,000 Attackers (X00 Mbps)	<ul style="list-style-type: none"> •All type of applicatios (HTTP, DNS, SMTP) •Spoofed SYN 	<ul style="list-style-type: none"> •ISP/IDC •Blackhole •ACL •DDoS solutions
Manually (hack to servers)	Manually	X0-X00 attackers (X0 Mbps)	Spoofed SYN Non critical Protocols (eg ICMP)	<ul style="list-style-type: none"> •Enterprise level •Firewall/ •ACL access router

Положение дел на сегодняшний момент

- Атаки становятся сложнее, приобретают изменяющийся профиль
- Атаки становятся быстрее
- Появилось множество утилит, упрощающих управление и планирование атак
- Атаки стали приносить реальную выгоду. Это стало бизнесом !

К чему это приводит:

- Сложность реагирования
- Увеличивается вероятность атак. За один август 2003:
 - ❑ W32/Mimail@MM
 - ❑ W32.Blaster.worm
 - ❑ Nachi, Blaster-D, Welchia
 - ❑ W32.Sobig.A and Variants

Все это требует от администраторов:

- Постоянной готовности
- Быстрого реагирования
- Наличие методологической базы и мощных средств ее реализации.

А ты готов к этому ?????

News -January 22,2002

Провайдер Cloud-Nine прекращает свою деятельность!

By: mark.j Comments 10:44:AM - (35) -SendNews / PrintNews:

... Точно в 10:16 Эмерик Мисзти и Джон Пар – главы ISP C9 сообщили о том, что скорее всего это – их последнее объявление в форумах. C9 на сегодняшний первый из сервис провайдеров кто прекратил свою деятельность в связи с участвовавшими атаками...

... C9 с прискорбием объявляет о том, что в 7:45 сегодняшнего утра приняло решение о выключении всех своих соединений в срочном порядке.

... Мы старались всю ночь восстановить работоспособность наших серверов, но наблюдали непрекращающиеся атаки типа отказа в обслуживании, нацеленные на наши ключевые сервера, включая e-mail и DNS. Природа атак была необычайно разнообразна и широка.

[http://www.ispreview.co.uk/cgi-bin/ispnews/printnews.cgi?newsid1011696274,91619,](http://www.ispreview.co.uk/cgi-bin/ispnews/printnews.cgi?newsid1011696274,91619)

Этапы реагирования на инциденты.

- После DDOS февраля 2000 было проведено несколько workshop-ов и выработан подход, включающий в себя шесть основных моментов, влияющих на эффективность обнаружения и реагирования на инциденты, связанные с безопасностью.

Шесть этапов реагирования

- Подготовка
- Идентификация
- Классификация
- Отслеживание
- Реагирование
- Анализ случившегося

Подготовка

- Методология
- Патчи
- Контактная информация
- Механизм защищенных подключений
- Инструментарий для незамедлительного реагирования
- Полигон
- План реагирования
- Постоянный тренинг

Идентификация

- Мониторинг внутреннего и «темного пространства»
- Построить шаблоны нормального трафика для определения отклонений от нормального поведения
- Утилизировать приложения для корреляции данных получаемых на разных участках сети (CPU, маршруты? netFlow, пр.)
- Не ждите, пока Ваши пользователи (клиенты) уведомят вас.

Способы идентификации

- Звонки клиентов (пользователей, service desk)
- Отслеживание аномальных изменений в работе сети
 - ❑ SNMP: Line/CPU overload, drops
 - ❑ NetFlow
 - ❑ Arbor'sPeakflowDoS
- Списки доступа с включенным журналированием
- Backscatter
- Sniffers
- IDS

Классификация

Классификация – определение типа атаки и какие последствия могут быть

- Определите вид атаки и то, какой ущерб она наносит
- Нам необходимо знать чем нас атакуют
- Как это можно сделать не нарушив работы нашего маршрутизатора, а также продуктивных серверов

Классификация. Цели

- На этапе классификации происходит сбор данных для последующей оценки риска следующих стадий
 - ❑ Какой IP-адрес и порт цели атаки
 - ❑ Тип протокола
 - ❑ Насколько серьезна и масштабна атака
 - ❑ Какой источник атаки (?)
- Данная информация – ключ к принятию решения о способах реагирования/мерах пресечения.

Классификация

- Классы инцидентов:
 - ❑ Разрушение активов
 - ❑ Несанкционированное раскрытие конфиденциальной информации, интеллектуальной собственности
 - ❑ Несанкционированный доступ
 - ❑ Отказ в обслуживании
 - ❑ Другие

Отслеживание

- Откуда исходит атака ?

Отслеживание

- Сообщите об атаке вашему провайдеру
- Определите область действия атаки: кол-во устройств, данных и других поврежденных ресурсов – обратите внимание на происходящее за пределами изначально установленной цели.
- Оцените последствия атаки: каковы последствия атаки для организации
- По результатам анализа определите способ защиты от атаки

Реагирование

- Сделайте наконец что-нибудь !
- Важно восстановить функционирование всех устройств и сервисов
- Реакция всегда должна быть быстрой и гибкой
- Не всегда важно найти нападающего

«разбор полетов»

- Анализ случившегося
 - Проведите глубокий анализ случившегося, на основе которого определите что можно сделать что бы противостоять атаке, когда она повторится.
 - Представляла ли атака, с которой вы столкнулись реальную угрозу для вас? Или же это просто было ширмой для чего-то другого, что может быть только что произошло?
 - Учитесь на собственном опыте: что можно сделать для того, чтоб в будущем справится с подобным инцидентом быстрее, с меньшими затратами и минимальным ущербом.
 - Возможно, для того чтоб завершить анализ, вам будет необходимо полностью восстановить функционирование серверов и устройств сети
 - Если вы не устраните все известные вам уязвимости, вероятнее всего, хакер повторит атаку на незащищенную уязвимость
 - Возможно вам придется восстанавливать систему не один раз
-
- **Не забывайте об этом этапе защиты, именно его обычно предпочитают не замечать!**

Инструменты и методы защиты

Средства идентификации

- SNMP –строить базовую линию и отслеживать отклонения от нее. Наблюдать также за специально установленными семафорами (или триггерами - triggers) (в первую очередь - CPU и фолты буферов, дропы пакетов)
- SYSLOG – Отслеживаем отклонения от базовой линии. Приветствуется установка триггеров (SNMP Authentication Failure). Наблюдение за журналами ACL.
- Netflow –Anomaly Detection Tools. Установить триггера на переполнение таблиц потоков (flow tables).

Применение CAR для ограничения полосы пропускания атаки

```
interface Serial 0
```

```
rate-limit output access-group 102 64000 2000 2000
```

```
conform-action transmit exceed-action drop
```

```
!
```

```
access-list 102 permit icmp any any echo
```

```
access-list 102 permit icmp any any echo-reply
```

Особенности:

- Необходимо знать характеристики нормального трафика
- Более эффективно на пограничных маршрутизаторах

Распознавание приложений на базе сети NBAR

Network -Based Application Recognition (NBAR)

- Классифицирует трафик по прикладным протоколам
- Позволяет определять пользовательский протоколы
- Однажды классифицировав, позволяет определять QoS для расстановки приоритетов трафика
- Может быть настроен для распознавания определенных строк в частях данных пакета
- После распознавания входящие и исходящие пакеты могут сбрасываться, не достигая цели.

Проверка наличия обратного пути (uRPF)

- Предназначен для решения проблем, вызванных неправильными или недействительными исходными IP-адресами, которые проходят через маршрутизатор.
 - Неправильные или недействительные адреса источника могут означать атаки отказа в обслуживании, основанные на подстановке адресов источника.
-

Blackholing, Sinkholing

- Данный маршрутизатор создается для анонсирования адресов, которые еще не зарегистрированы организацией IANA
- Поглощающий маршрутизатор анонсирует эти сети только локально, а любые попытки найти их передаются маршрутизатору
- Когда червь или какой-либо другой вредоносный код попадает в вашу сеть и начинает генерировать трафик на выборочные адреса, некоторые из этих адресов будут принадлежать к категории незарегистрированных
- При получении такого вредоносного трафика он будет зарегистрирован но не принят. В результате из подобных записей будет создан список инфицированных хостов.

Отслеживание фиктивных IPv4 адресов

- Откуда Вы были атакованы: изнутри или снаружи?
- Как только Вы имеете точное понимание типа атаки (адрес источника, тип протокола) вам необходимо отследить атаку до точки входа вашу сеть
- Две основных техники:
 - Хоп за хопом
 - Скачек непосредственно на точку входа

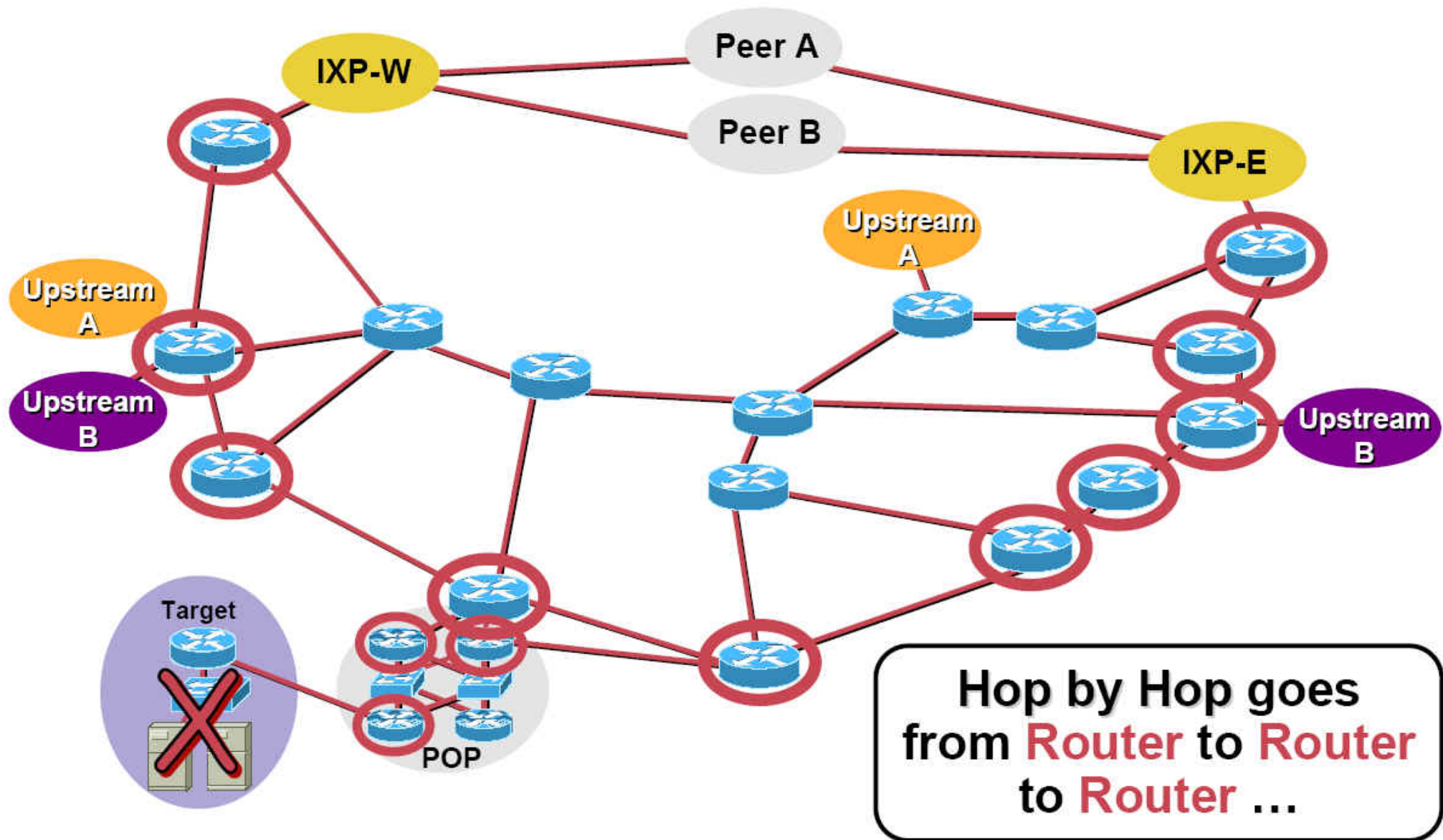
Техника отслеживания

«ХОП за ХОПОМ»

- Отслеживание занимает время
- Начинаем от места обнаружения атаки и отслеживаем до источника проблемы
- Использует поочередно все маршрутизаторы
- Часто требует разделения – отслеживание двумя отдельными путями
- Скорость – основное ограничение техники

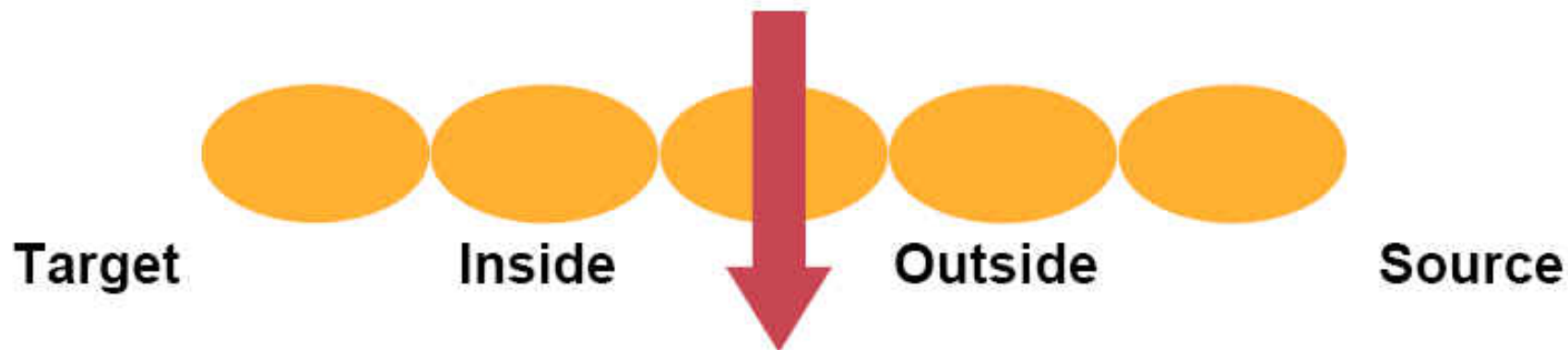


Техника «хоп за хопом»

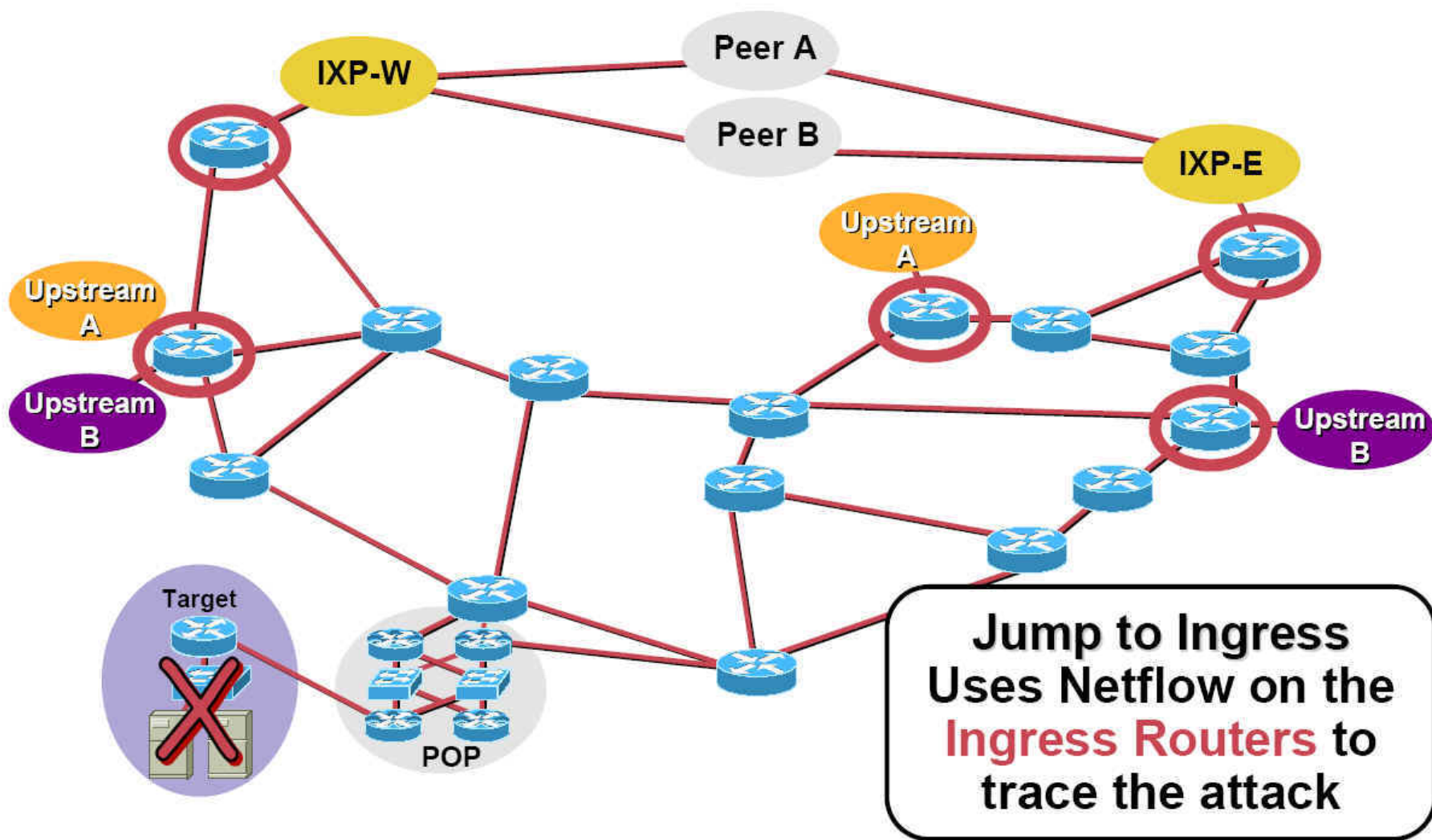


Отслеживание посредством прыжка непосредственно к точке входа в сеть

- Прыжок к точке входа уменьшает проблемы на половину
 - ❑ Организована ли атака внутри сети или же снаружи?
 - ❑ Необходимо перейти на точки входа, чтобы определить, входит ли атака снаружи или изнутри
 - ❑ Преимущество – скорость.



Техника прыжка к входной точке в сети



Отслеживание фиктивных IPv4 адресов

■ Техники отслеживания:

- ❑ Введение временных списков доступа с опцией журналирования и последующая проверка результатов (аналогично методу классификации)
 - ❑ Опрос таблицы потоков Netflow
 - *show ip cache-flow* (Netflow должен быть включен)
 - ❑ Использование функции IP Source Tracker (в случае с маршрутизаторами Cisco)
 - ❑ Техника отслеживания Backscatter Отслеживание с использованием телеметрии Netflow
-

Отслеживание с использованием списков доступа (ACL)

- Достаточно оригинальная техника отслеживания
- Риск — внесение изменений в сеть, которая находится под воздействием атаки
- Риск — обычно опция журналирования требует придерживать пакет для того, чтобы сгенерировать сообщение

Отслеживание с использованием списков доступа

```
access-list 170 permit icmp any any echo
access-list 170 permit icmp any any echo-reply log-input
access-list 170 permit udp any any eq echo
access-list 170 permit udp any eq echo any
access-list 170 permit tcp any any established
access-list 170 permit tcp any any
access-list 170 permit ip any any
interface serial 0
ip access-group 170 out
! Wait a short time
no ip access-group 170 out
```

Отслеживание с использованием списков доступа. Вывод

Удостоверьтесь в том, что счетчики увеличились

show access-list 170

Затем просмотрите журнал входящего интерфейса:

show logging

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.212.72
(Serial0 *HDLC*) -> 198.133.219.25 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 172.16.132.154
(Serial0 *HDLC*) -> 198.133.219.25 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.45.15
(Serial0 *HDLC*) -> 198.133.219.25 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 192.168.45.142
(Serial0 *HDLC*) -> 198.133.219.25 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 170 permit icmp 172.16.132.47
(Serial0 *HDLC*) -> 198.133.219.25 (0/0), 1 packet

Отслеживание с использованием Netflow

■ Основные способы использования Netflow:

```
show ip cache <addr> <mask> verbose flow
```

```
show ip cache flow | include <addr>
```

■ Дальновидный подход – генерация скрипта

```
ssh -x -t -c [des|3des] -l <username> <IPAddr> "show  
ip cache <addr> <mask> verbose flow"
```

Отслеживание с использованием Netflow.

Анализ данных

- **Анализируем вывод команд:**

```
router1#sh ip cache flow | include <destination>  
Se1 <source> Et0 <destination> 11 0013 0007 159
```

...

...

```
Se1 <source> Et0 <destination> 11 0013 0007 159
```

- **Берем имя серийного интерфейса (Se1). Затем ищем путь, откуда пришел поток:**

```
router1#sh ip cef se1  
Prefix Next Hop Interface  
0.0.0.0/0 10.10.10.2 Serial1  
10.10.10.0/30 attached Serial1
```

- **Следовательно, продолжаем на маршрутизаторе 10.10.10.2**

Отслеживание с использованием Netflow.

Основные преимущества

Основные преимущества Netflow:

- Не надо производить никаких изменений конфигурации маршрутизатора во время атаки; мониторинг пассивный
- Может использоваться для отслеживания «хоп за хопом»; данный процесс может быть автоматизирован при помощи скрипта
- Системы обнаружения вторжений третьих фирм могут работать с Netflow

Основной нюанс: все должно быть готово заранее

Netflow. Пример. Отслеживание хостов, инфицированных W32.Blaster

Хосты, инфицированные W32.Blaster пытаются реплицироваться на случайные хосты по порту 135 (0x0087)

```
Router>show ip cache flow | include 0087
```

:

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Fa2/0	XX.XX.XX.242	Fa1/0	XX.XX.XX.119	06	0B88	0087	1
Fa2/0	XX.XX.XX.242	Fa1/0	XX.XX.XX.169	06	0BF8	0087	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.63	06	0E80	0087	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.111	06	0CB0	0087	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.95	06	0CA0	0087	1
Fa2/0	XX.XX.XX.204	Fa1/0	XX.XX.XX.79	06	0C90	0087	1

Техника отслеживания Backscatter

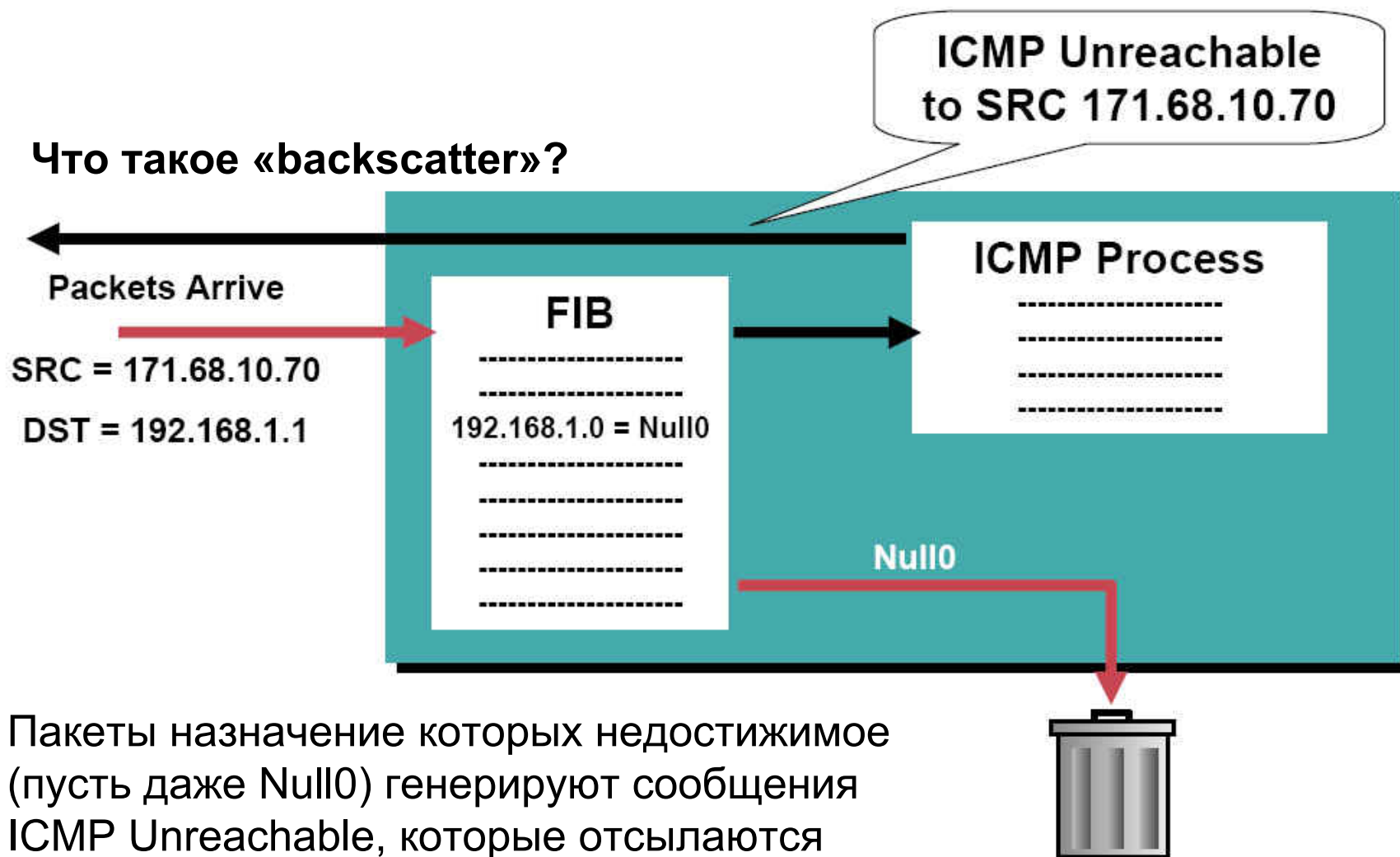
Три основных преимущества:

- Уменьшает риск работы сети в процессе отслеживания
- Достаточно быстрое отслеживание
- Существует возможность передачи от одного провайдера к другому, т.е. потенциально можно отследить до самого источника атаки.

Дополнительная информация:

<http://www.secsup.org/Tracking/>

Техника отслеживания Backscatter



Пакеты назначение которых недостижимое (пусть даже Null0) генерируют сообщения ICMP Unreachable, которые отсылаются обратно. Данное «отражение» определяется термином **Backscatter**

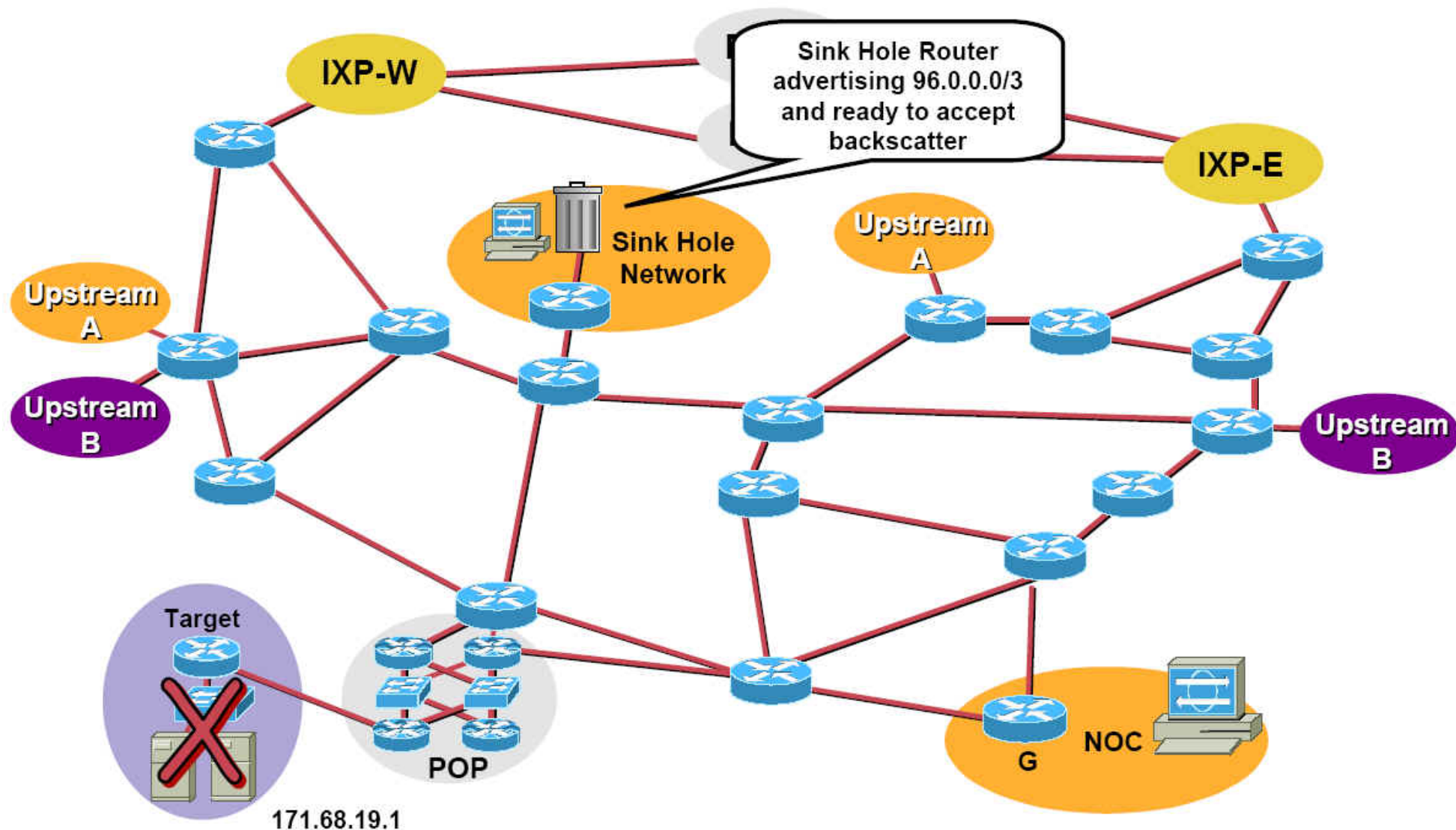
Backscatter. Приготовление.

Шаг 1 – «Sink Hole»

- «Sink-Hole» маршрутизатор объявляет большой блок незанятых адресов при помощи BGP *no-export*, а также исходящие фильтры BGP для того, чтоб оставить блок внутри. Допустим этот блок 96.0.0.0/3.
 - Это могут быть не зарезервированные блоки IANA, или ваши незанятые блоки.
www.iana.org/assignments/ipv4-address-space
 - Исходящий фильтр BGP должен не давать данному объявлению покинуть внутреннюю сеть.
 - Для того, чтоб убедиться в том, что объявление не покидает сеть, используйте опцию *no-export*.

Backscatter. Приготовление.

Шаг 1 – «Sink Hole»



Backscatter. Приготовление.

Шаг 2 – статический маршрут на Null0

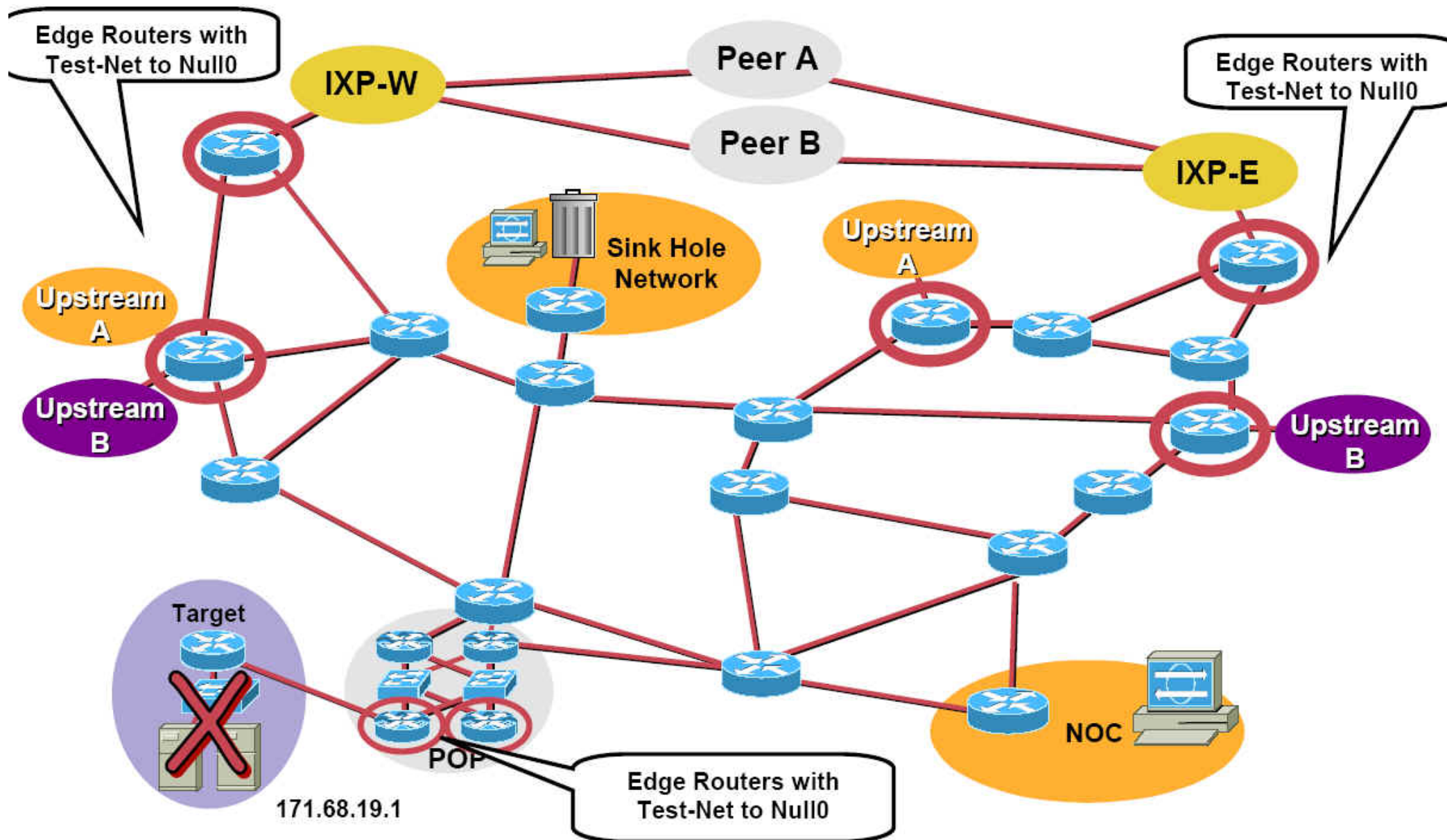
- На всех пограничных устройствах (маршрутизаторы, NAS, IXP маршрутизаторы, пр.) добавляется статический маршрут на Null0
- Заводится тестовая сеть – никем не используемый диапазон адресов (пусть это будет например 192.0.2.0/24)

`ip route 192.0.2.1 255.255.255.255 Null0`

- На маршрутизаторах должны быть разрешены пакеты ICMP Unreachables (команда *ip unreachable* на Cisco)
- В случае озабоченности возможным уровнем ICMP Unreachable Можно ограничить прохождение данных пакетов (команда *ip icmp rate-limit unreachable* на Cisco).

Backscatter. Приготовление.

Шаг 2 – статический маршрут на Null0



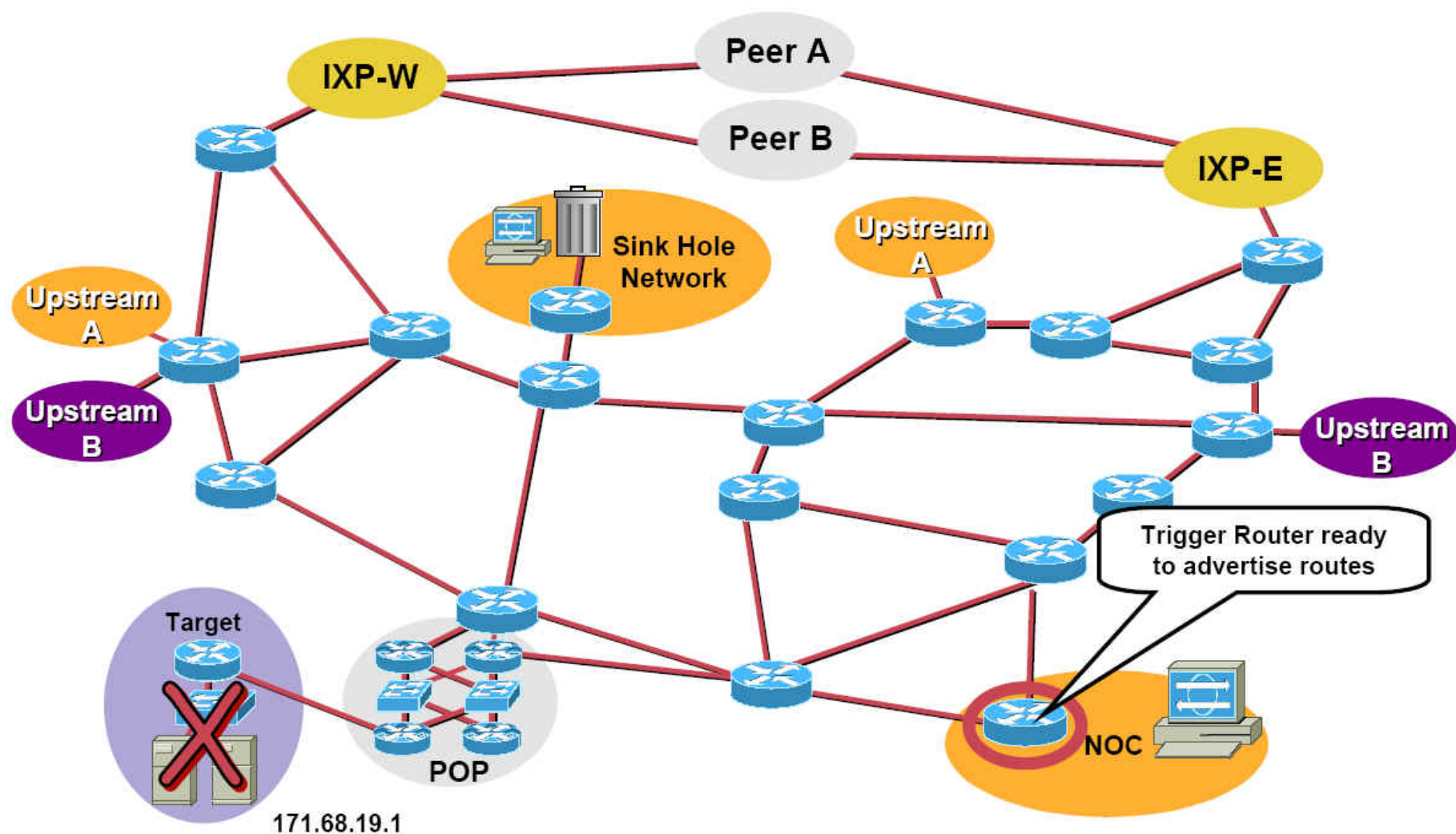
Backscatter. Приготовление.

Шаг 3 –Trigger-маршрутизатор

- **Trigger-маршрутизатор – устройство, которое должно посылать iBGP анонсы во внутреннюю сеть.**
- **Может быть продуктивный маршрутизатор (данный подход не рекомендуется)**
- **В случае выделенного маршрутизатора – что-то маленькое, например 2600 (ему не надо получать BGP маршруты, только посылать их)**

Backscatter. Приготовление.

Шаг 3 – Trigger-маршрутизатор



Backscatter. Приготовление.

Шаг 3 –Trigger-маршрутизатор. Конфигурация

```
router bgp XXX
```

```
!
```

```
! Redistribute Static with a route-map
```

```
redistribute static route-map static-to-bgp
```

```
!
```

```
route-map static-to-bgp permit 5
```

```
! Match Static Route Tag
```

```
match tag 666
```

```
! Set Next-Hop to the Trigger
```

```
set ip next-hop 192.0.2.1
```

```
set local-preference 50
```

```
set community additive no-export
```

```
set origin igp
```

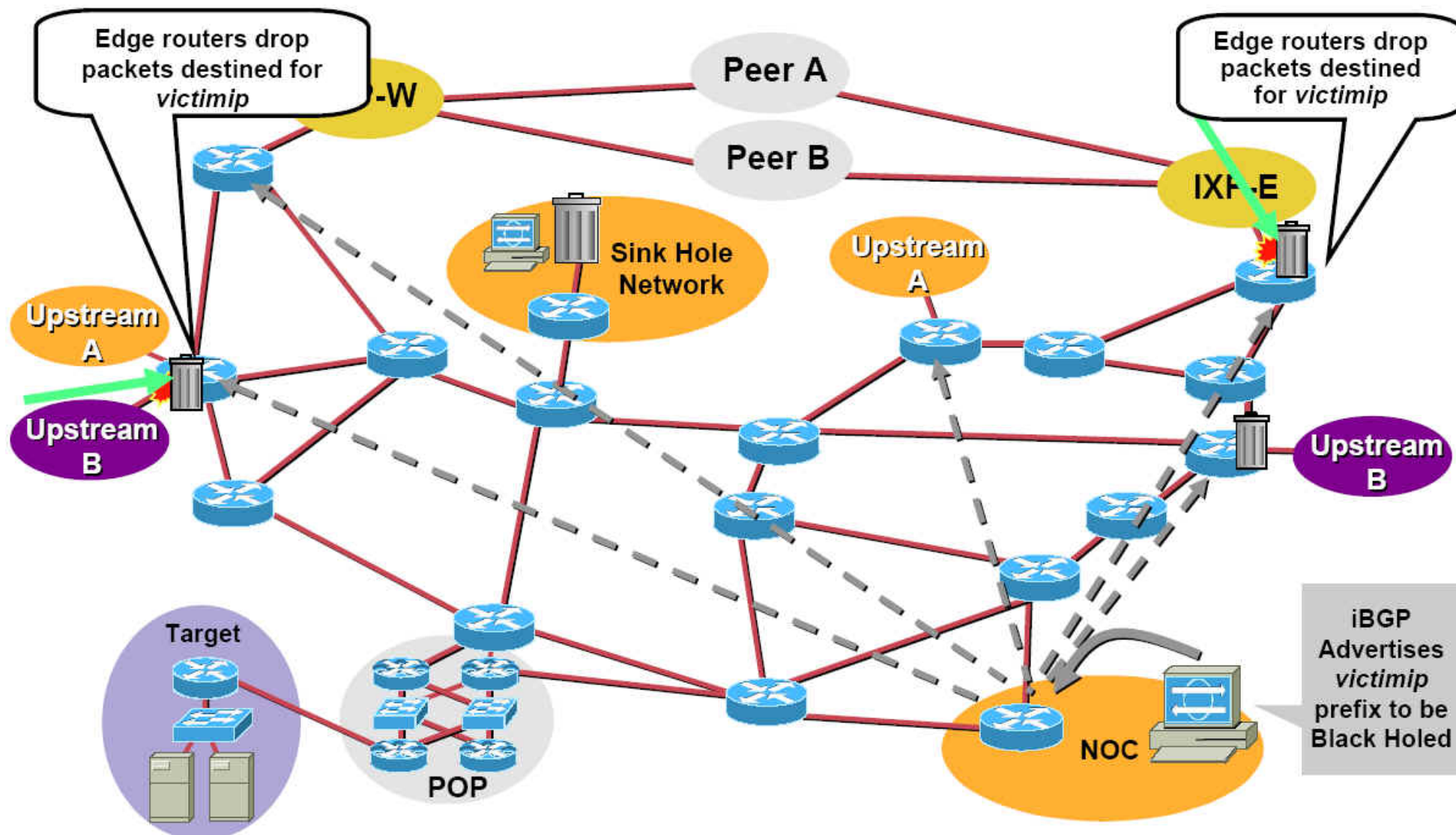
Backscatter. Активация

- Активация происходит в случае идентификации атаки
- Должна быть проведена простейшая классификация, чтобы понять, сработает ли данная техника:
 - Может быть придется поменять анонсируемый блок адресов
 - Согласно статистике, в большинстве атак использовался весь адресный блок Интернет

Backscatter. Активация

- Trigger-маршрутизатор в случае атаки анонсирует /32 по iBGP.
 - Конфигурируем статический маршрут с меткой “666”:
 - `ip route victimip 255.255.255.255 Null0 tag 666`
 - Метка в route-map совпадает с меткой маршрута и маршрутизатор начинает анонсировать префикс у которого next-hop указывает на 192.0.2.1. В свою очередь, на каждом из маршрутизаторе данный маршрут ассоциирован с Null0 (no-export)
 - Таким образом, посредством BGP включается «Black Hole» фильтрация
- Пакеты, предназначенные жертве, тихо уничтожаются.

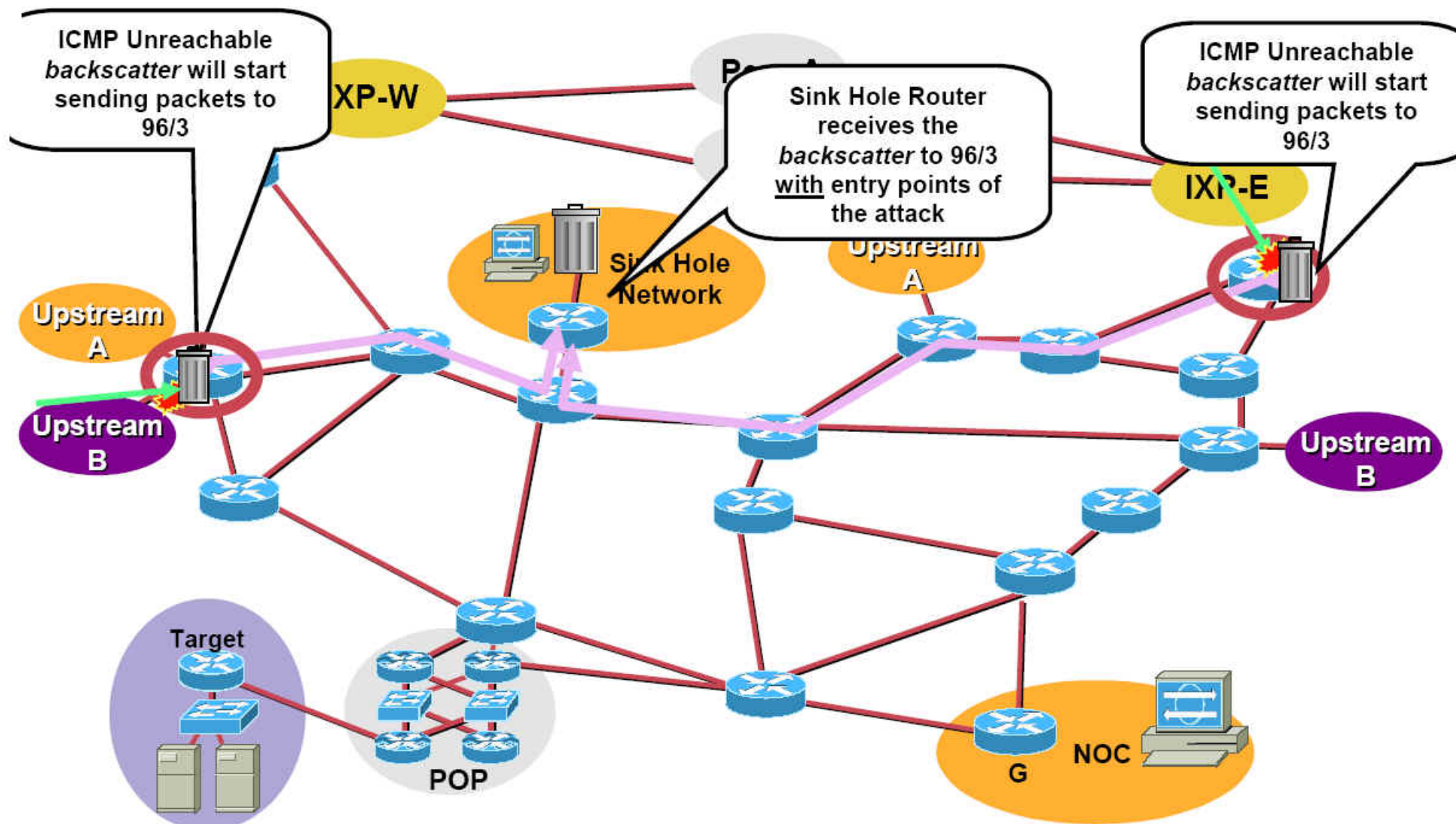
Backscatter. Активация



Backscatter. Активация

- Пакеты предназначенные *victimip* уничтожаются.
- ICMP Unreachable от пограничных маршрутизаторов начинают поступать на «Sink-Hole» (согласно анонсу 96.0.0.0/3)
- Для нахождения того, который из маршрутизаторов посылает пакеты достаточно использовать списки доступа на маршрутизаторе «SinkHole»:
 - ❑ access-list 101 permit icmp any any unreachable log
 - ❑ access-list 101 permit ip any any

Backscatter. Активация



Backscatter. Активация

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18

-> 96.47.251.104 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18

-> 96.70.92.28 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18

-> 96.222.127.7 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18

-> 96.96.223.54 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18

-> 96.14.21.8 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18

-> 96.105.33.126 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18

-> 96.77.198.85 (3/1), 1 packet

SLOT 5:3w1d: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 171.68.66.18

-> 96.50.106.45 (3/1), 1 packet

Отслеживание при помощи телеметрии Netflow

- Пограничные маршрутизаторы могут экспортировать данные Netflow, содержащие детальную информацию о сетевых потоках.
 - Данная телеметрия может быть обработана целью обнаружения аномалий, а также с целью отслеживания атак до их источника.
 - Существует много открытых и коммерческих проектов, занимающихся данным вопросом (напр. Arbor PeakFlow)
-

Отслеживание. Заключение

- Отслеживание «От хопа к хопу» занимает много времени. Полезно знать, но старайтесь применять более подходящую методологию.
- Отслеживание «Backscatter» работает с большим диапазоном атак. Является техникой приемлемой для отслеживания от провайдера к провайдеру.
- На рынке появились продукты, способные использовать описанные методики для быстрого отслеживания инцидентов

Реагирование на атаки. Принципы

- Необходимо попытаться сделать что-то, для уменьшения влияния атаки или для ее прекращения
 - Варианты разные: от ничего-не-деланья (иногда действия рожают проблемы) до отключения от источника атак (кибер-войны между странами)
- Большинство провайдеров стараются помочь своим клиентам
 - Необходимо отвести атаку от клиента
 - Сведите влияние атаки к безопасному посредством ограничения трафика (rate-limit)
 - Уничтожайте пакеты на основе списка адресов источника
 - Реагирование должно быть быстрым и гибким

Реагирование на атаки. Техника

- **Существуют различные техники уничтожения пакетов или урезания канала для данного вида трафика:**
 - ❑ **ACLs – ручная или автоматическая загрузка**
 - ❑ **Black Hole – включение посредством BGP**
 - ❑ **uRPF – включение посредством BGP**
 - ❑ **CAR – ручная загрузка или включение посредством BGP**
 - ❑ **Sink Holes – перенаправления трафика посредством BGP**

Реагирование на атаки. ACL.

- Традиционный способ прерывания атаки
- Возникают некоторые трудности при масштабировании:
 - ❑ Попробуйте обновить вручную списки на многих-многих маршрутизаторах
 - ❑ Дополнительные списки при сложных атаках (множество адресов) – тоже не подарок
 - ❑ Постоянная борьба за здоровый баланс между производительностью и кол-вом строк в списках

Реагирование на атаки. ACL.

Выводы

- Списки доступа широко используются как первичный и наиболее простой способ сдерживания атак
- Предварительные требования : Идентификация и классификация – необходимо знать что блокировать
- Старайтесь использовать как можно более конкретные списки доступа
- Списки доступа более подходят для статических атак, не для атак с часто меняющимся профилем.
- Необходимо понимать ограничения списков доступа перед тем как их использовать

Удаленно включаемая фильтрация «BlackHole» основанная на знании адреса назначения

Destination Based Remote Triggered Black Hole Filtering

- Для реагирования на инцидент на уровне всей сети используйте BGP.
- Простой статический маршрут на Null0, а также протокол BGP позволит реагировать на атаку настолько быстро, насколько быстро iBGP сможет обновить таблицы по сети.
- Данная техника дает возможность провайдеру реагировать на инциденты, или же может использоваться вместе с техникой Backscatter для отслеживания распространения атак типа DDOS.

Удаленно включаемая фильтрация «BlackHole» основанная на знании адреса назначения. Принцип

- На пограничных маршрутизаторах заготавливается маршрут на вымышленную сеть, указывающий в Null0
- Trigger-маршрутизатор настраивается таким образом, чтоб быть готовым посылать iBGP анонсы во внутреннюю сеть.
- Оператор добавляет статический(е) маршрут(ы) для адреса(ов) назначения, которые должны быть «сокрыты». Маршрут добавляется с особой меткой (tag 666) для обособления данного маршрута от остальных статических маршрутов на маршрутизаторе.

ip route 171.68.1.0 255.255.255.0 Null0 Tag 666

- Согласно метке, карта маршрутов устанавливает no-export community
- iBGP анонсы посылаются на все понимающие BGP маршрутизаторы, соседствующие с данным.
- Пограничные маршрутизаторы принимают анонс, поднимают статический маршрут, устанавливая next-hop в null0, тем самым включая фильтрацию по адресу назначения.

«Black Hole». Активация

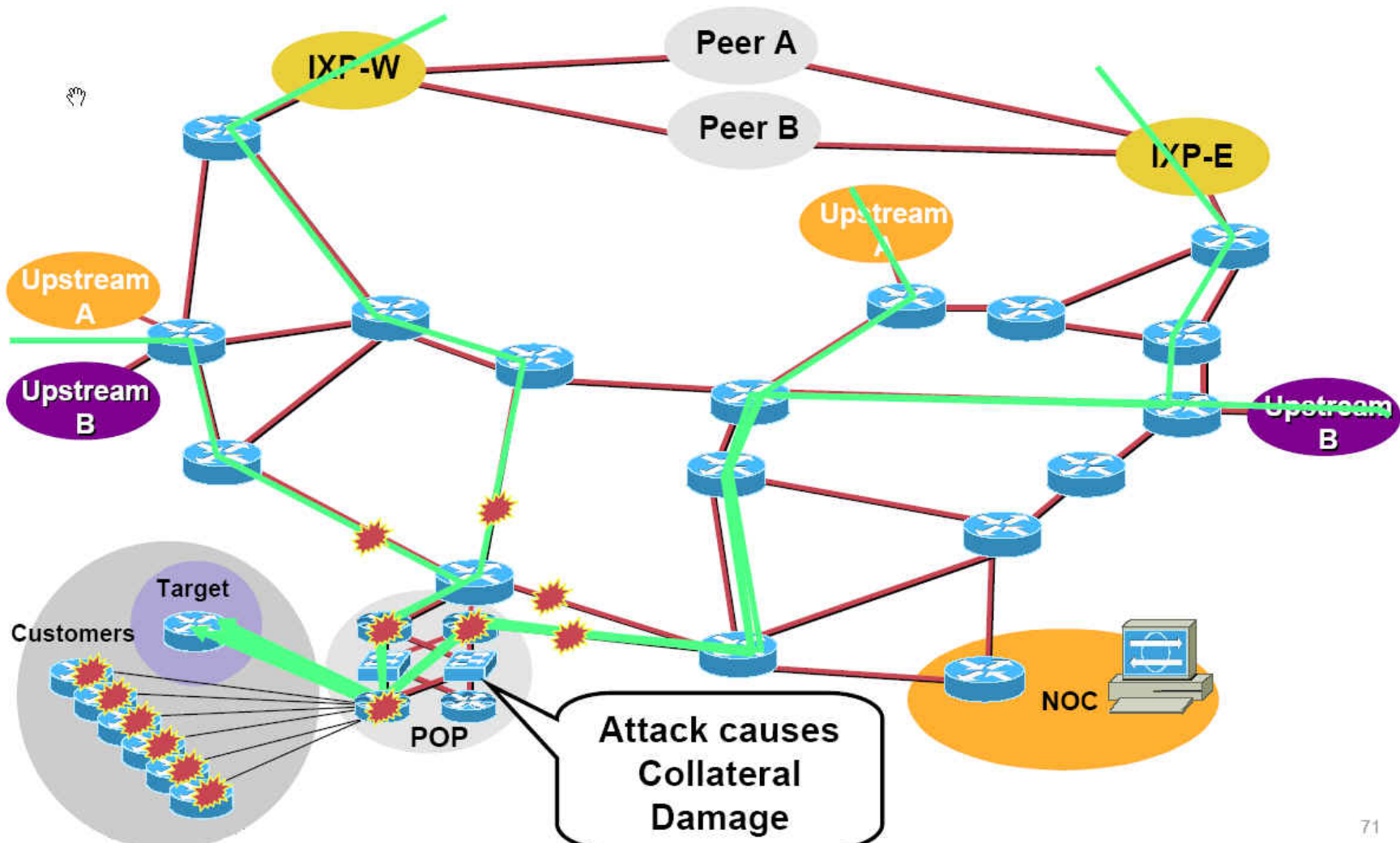
BGP Sent – 171.68.1.0/24 Next-Hop = 192.0.2.1

Static Route in Edge Router – 192.0.2.1 = Null0

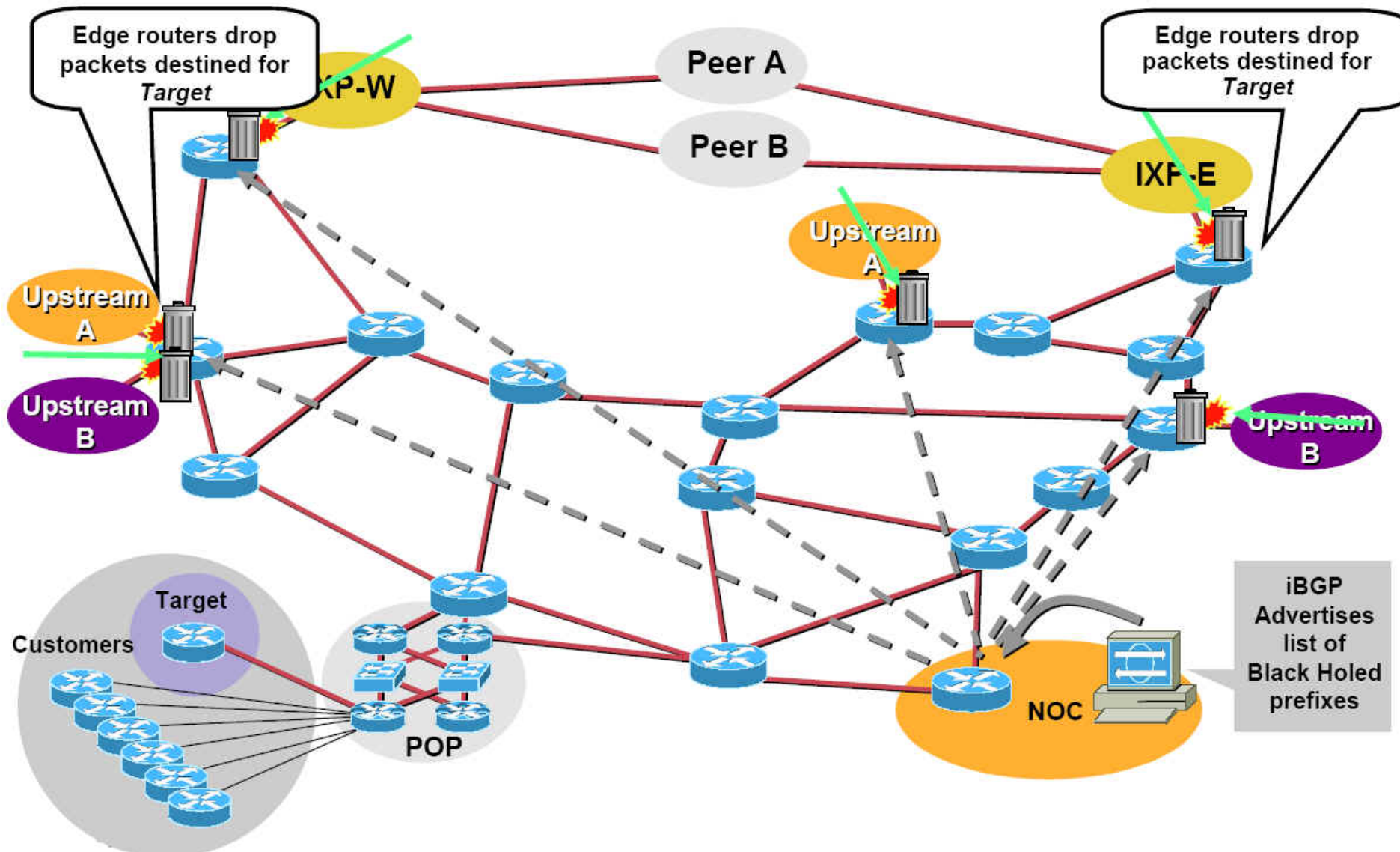
171.68.1.0/24 = 192.0.2.1 = Null0

Next hop of 171.68.1.0/24 is now equal to Null0

Атака. Перед внедрением метода



Атака. После внедрения метода



Remote Triggered Black Hole Filtering. ВЫВОДЫ

- Remote Triggered Black Hole Filtering – определение для целого семейства техник и методик отслеживания и реагирования на атаки (преимущ. DDOS)
- Приготовления не влияют на работоспособность или на производительность вашей сети
- Данная методика достаточно мощная, масштабируемая, не требующая изменений в конфигурации сети в масштабе реального времени.

Feb'00 Distributed Denial of Service (DDoS)

В результате пришли к следующему заключению:

“Нам необходимо средство фильтрации пакетов на основе адреса источника, которое может быть установлено на более чем 60-ти маршрутизаторах за время менее 60-ти секунд, при этом насчитывать не менее тысячи строк, иметь возможность быть редактированным «на лету» и работать на всех наших платформах без потери производительности”.

И задумались ;(

Удаленно включаемая «BlackHole» фильтрация пакетов на основе адреса **источника**

(Source Based Remote Triggered Black Hole Filtering)

... И придумали!

Black Hole Filtering – фильтруем все пакеты, чьи адреса **назначения** равны Null0

Remote Triggered – включаем префикс равным Null0 на маршрутизаторах со скоростью iBGP.

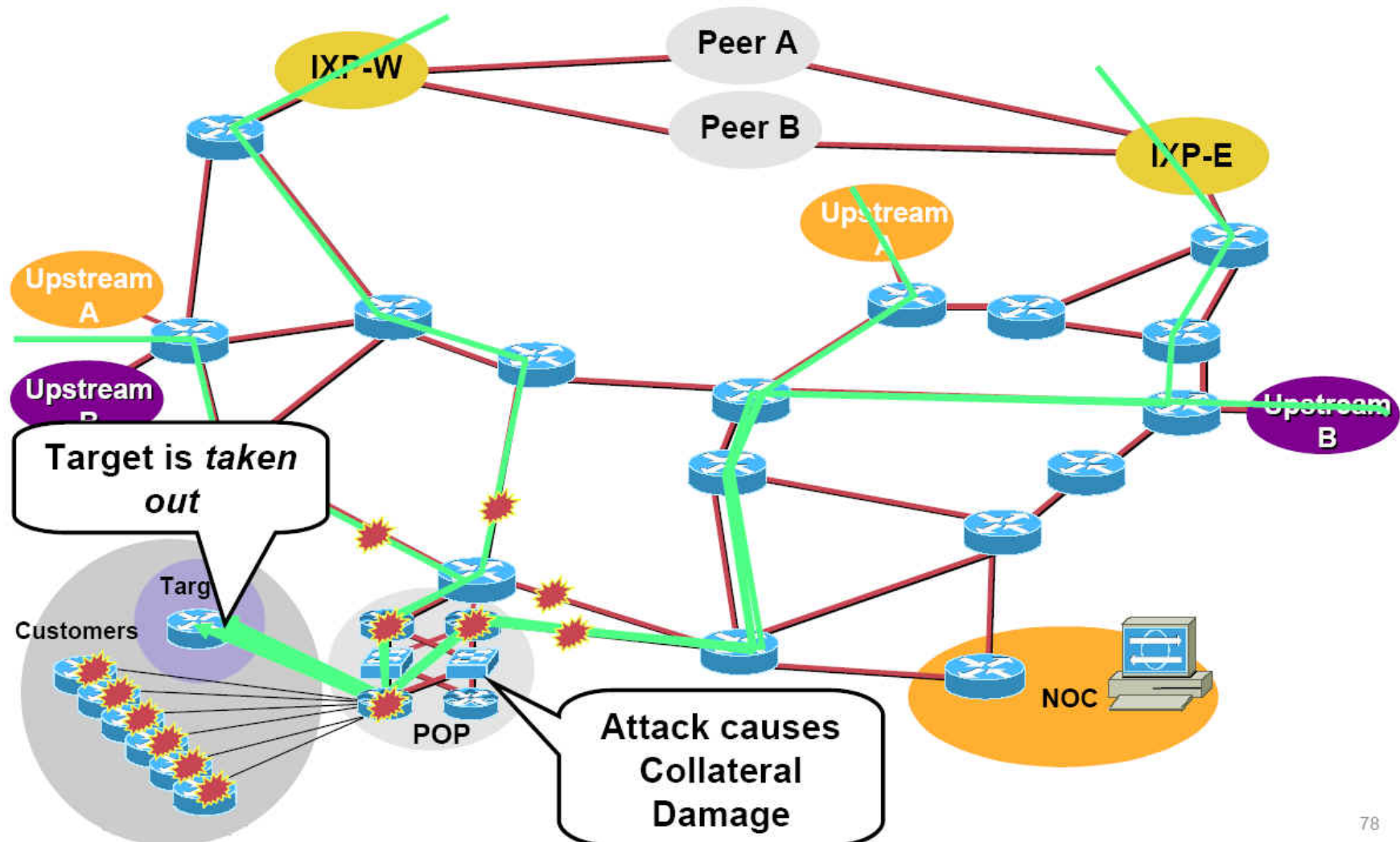
uRPF Loose Check – фильтруем также пакеты с адресом **источника** равным Null0

Решение: Соединяем все воедино и получаем средство фильтрации любых пакетов, чей адрес назначения или источника равен Null0!

Реагирование на атаку по методу Source Based Remote Triggered Black Hole

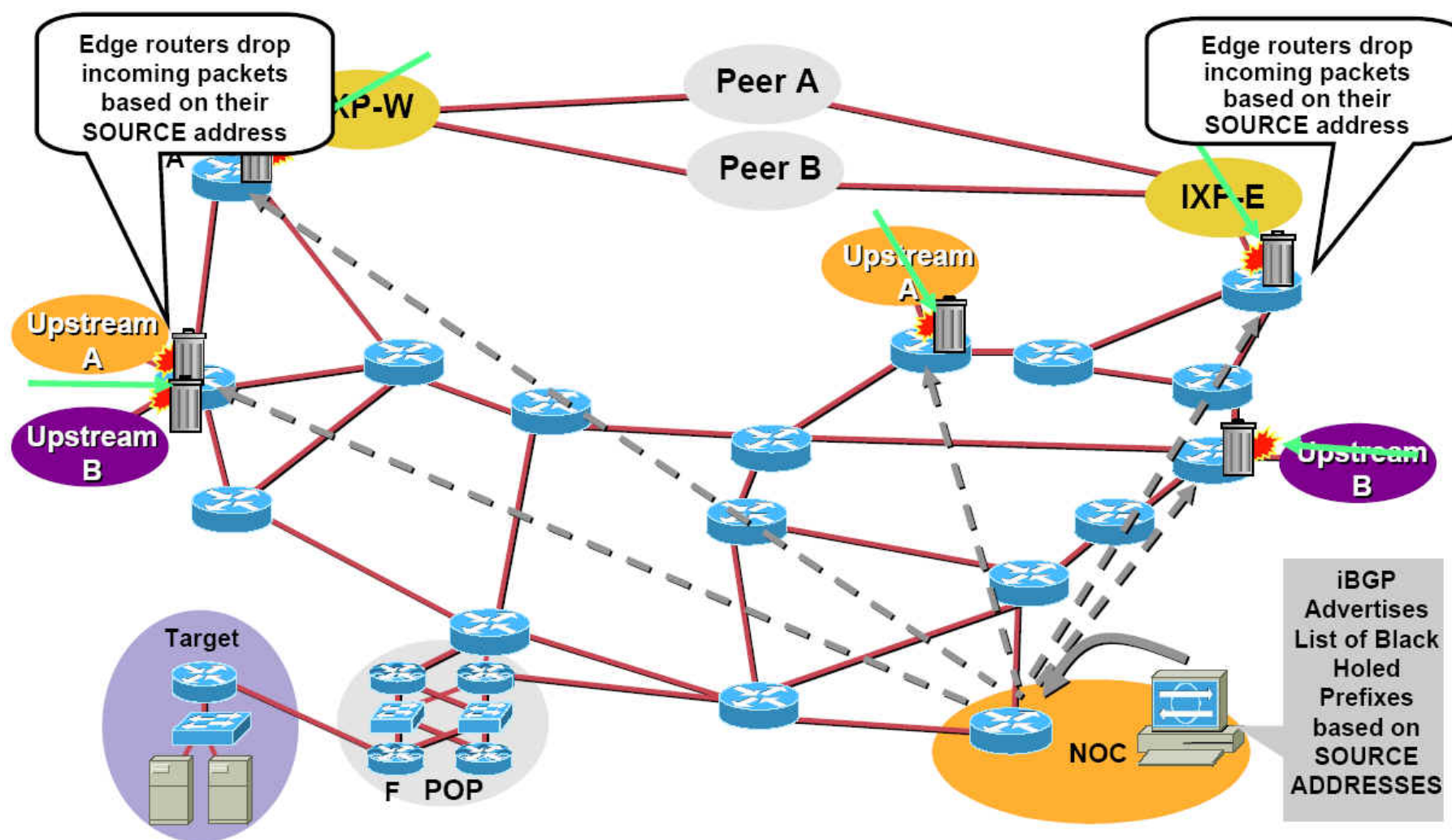
- Что для этого надо?
 - Приготовления:
 - uRPF loose check на всех пограничных маршрутизаторах
 - Статика в Null0 для адресов из **вымышленной_сети** на всех пограничных маршрутизаторах
 - Возможность анонсировать BGP объявления в сети при помощи community проассоциированного с Null0 (конечно необходимо вспомнить об опции no-export).
-

Customer Is DOSed – Before



Customer is DOSed – After

пакеты удаляются прямо на границе



Реагирование на атаки по методу Remote Triggered Black Hole

- Основные преимущества:
 - Нет необходимости обновлять ACL
 - Нет необходимости вносить изменения в настройки маршрутизаторов
 - Фильтрация происходит также по пути распространения (forwarding path)
 - Частые внесения изменений при быстроменяющемся профиле атаки (множественные атаки на множество клиентов)

Реагирование на атаки по методу Remote Triggered Black Hole

- Это уже сегодняшний день
 - Многие провайдеры используют данный метод на регулярной основе
 - Иногда это – единственный масштабируемый ответ на глобальные DDOS атаки.
 - Возможность делегировать право «порулить» самим клиентам.
-

Источник или назначение?

- Фильтрация по адресу назначения очень важна
 - Часто нам больше ничего и не надо
- Реагирование на основе адреса источника предлагает некоторые интересные возможности:
 - Препятствие атаке без «затемнения» реальных служб
 - Фильтрация командных и контрольных серверов
 - Изоляция инфицированных станций внутри сети
- Метод масштабируем:
 - Сама по себе **BGP triggered Black Hole** фильтрация базируется на адресе назначения
 - Стоит добавить **Loose-mode uRPF** – и появляется возможность фильтровать пакеты как с адресом назначения, так и с адресом источника

Списки доступа или uRPF фильтрация?

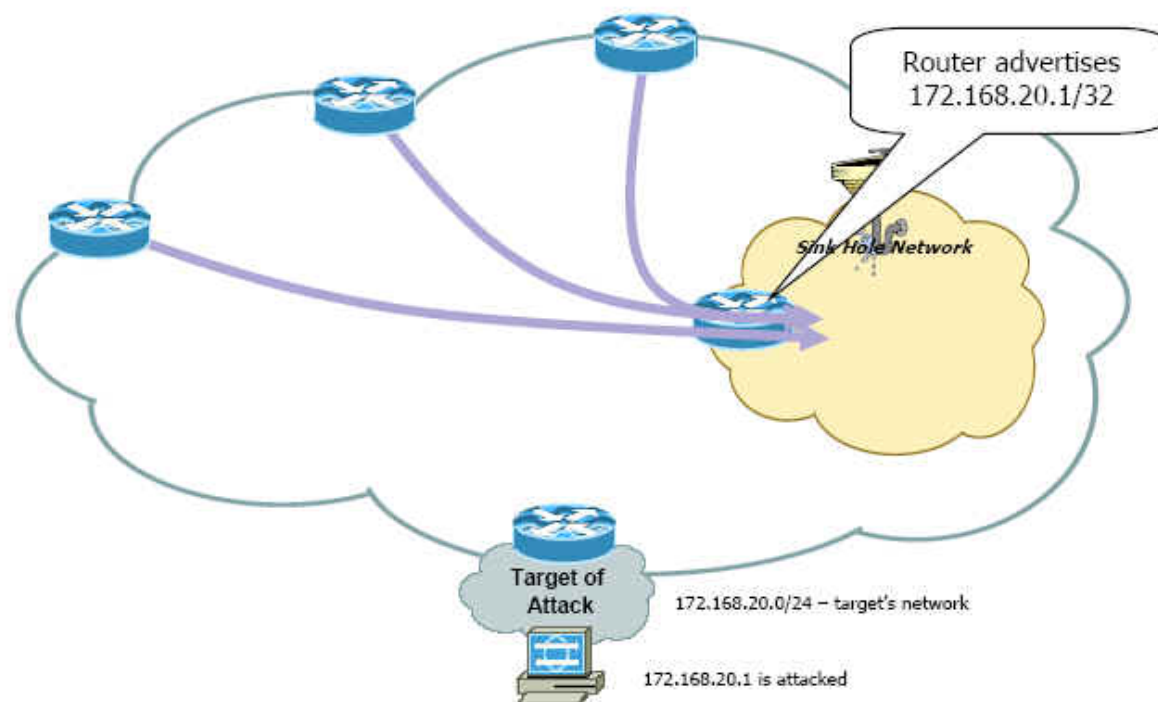
- Сильные стороны ACL:
 - Детальная фильтрация пакетов (порты, протоколы, фрагменты, пр.)
 - Относительно статическое фильтрующее окружение
 - Достаточно понятная и четкая политика фильтрации
- ACL испытывают трудности в случаях:
 - Атак с динамическими профилями (различные источники, различные точки входа, пр.)
 - Часто меняющиеся профили атак
 - Необходимость быстрого и одновременного внедрения на многих устройствах
- Комбинация ACL позволяет ACL охватывать вопросы статических политик, в то время как фильтрация uRPF Remote-Triggered Black Hole охватывает вопросы фильтрации пакетов с динамическими адресами источника.

Реагирование на атаки по методу «Sink Holes»

- «Sinkholes» - метод нацелен больше на анализ
- маршрутизатор или рабочая станция настраиваются таким образом, чтоб «всасывать» сетевой трафик для последующего его анализа (изначальное предназначение)
- Используется также для отведения атак от клиента
- Используется для мониторинга атак, процессов сканирования, фактов неправильной конфигурации, другой активности (посредством анонсирования дефолтовых или неиспользуемых адресных блоков)
- Трафик обычно отклоняется посредством объявлений BGP маршрутов

Sink Hole маршрутизаторы/сети

- Атака отводится от клиента или ваших продуктивных систем.
- Теперь можно спокойно производить классификацию списками доступа, анализ с использованием NetFlow, анализ дампа, отслеживание, пр.
- Основная задача – минимизировать влияние на сеть на стадии расследования инцидента.



Отслеживание и реагирование.

Выводы

- На данный момент насчитывает достаточное кол-во техник и методик отслеживания и реагирования на инциденты связанные с безопасностью в сети:
 - ACLs, CAR, Remote Triggered Blackhole Filtering (uRPF), Remote Triggered Rate Limiting (CAR+QPPB), Sink Holes, Black Hole Shunts with Scrubbing, etc..
- Ключ к успеху – совместная работа разных команд с целью обмена опытом и достижениями
- Большое значение – процессу подготовки. Не рекомендую внедрять новые технологии непосредственно в процессе реагирования на атаку
- Ситуация с инцидентами больше походить на сводку с поля боя: атаки происходят каждый день. В этом свете требуются быстрые и эффективные решения.

Советы

- НЕ ПАНИКОВАТЬ!!!!!!
- Большинство битв выигрывается еще до начала
- Быть готовым (теоретически)
- Политика безопасности
- Практика рождает мастерство

Обнаружение и реагирование на инциденты в области безопасности

Владислав Кушка
Системный инженер
Ukrainian Mobile Communication

vkushka@umc.com.ua