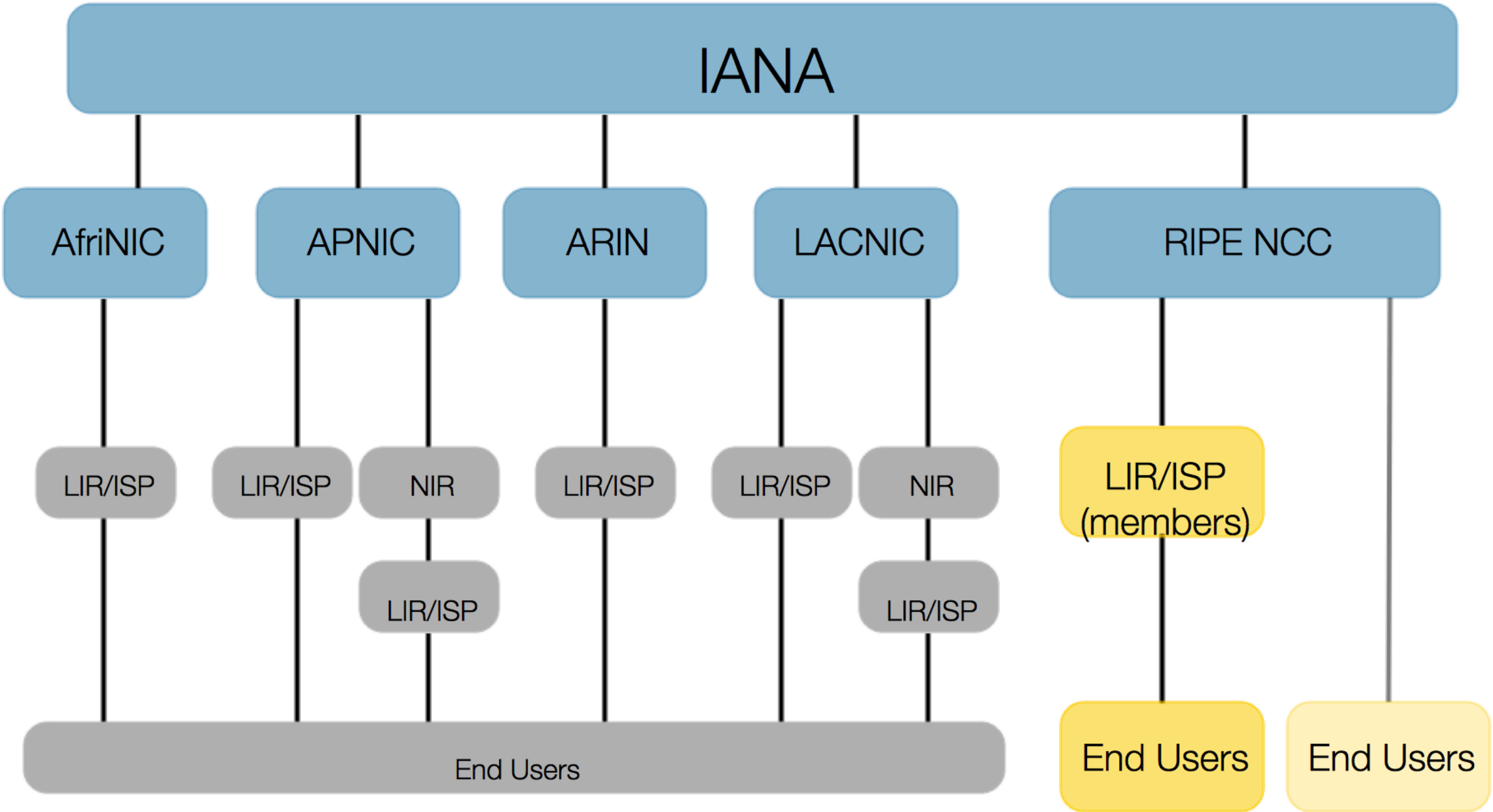
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Безопасная маршрутизация и где она обитает

Alex Semenyaka | 07-12-2018 | UADOM Kyiv

RIPE NCC

Internet Registry System



Regional Internet Registries

RIPE vs RIPE NCC

community

Decides on policy

- Valid reasons for getting resources
- Amount of resources
- RIPE Database features

membership

Decides on business

- Charging scheme
- Activity plan
- Additional Services
  - Atlas
  - RIPEstat

RIPE Working Groups

- Address Policy
- Anti-Abuse
- Connect
- Cooperation
- Database
- DNS
- Internet of Things
- IPv6
- MAT
- Open Source
- RIPE NCC services
- **Routing**

Маршрутизация в Интернете

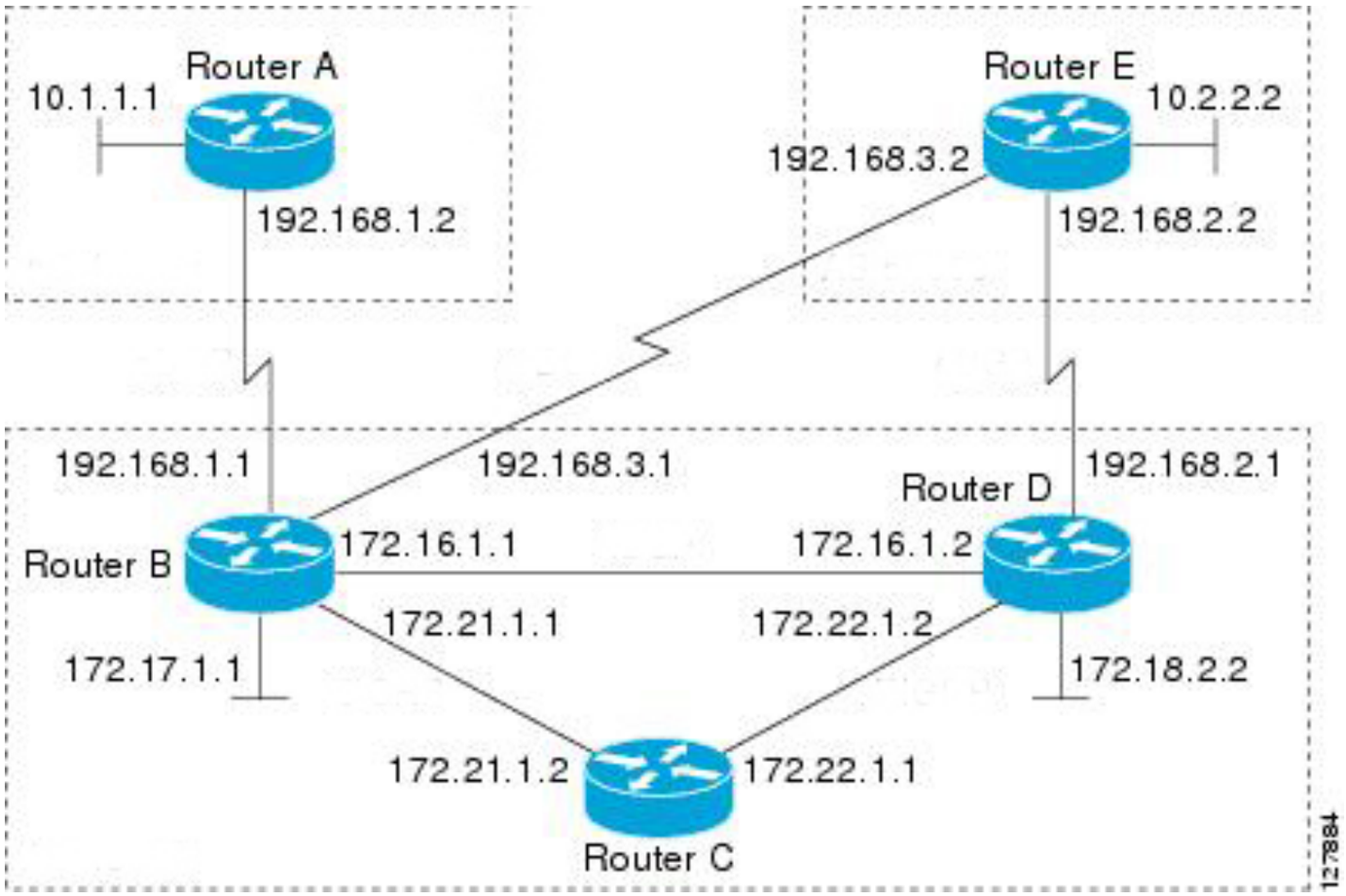
IP-адрес

- Двойная роль:
  - Identificator (что?)
  - Locator (где?)
- Блоки IP-адресов
  - Например 10.0.0.0/8 или fe80::/16
  - Блоки делятся на под-блоки
    - ✓ 10.0.0.0/8 =
      10.0.0.0/10 +
      10.64.0.0/10 +
      10.128.0.0/10 +
      10.192.0.0/10

IP-маршрутизация (“роутинг”)

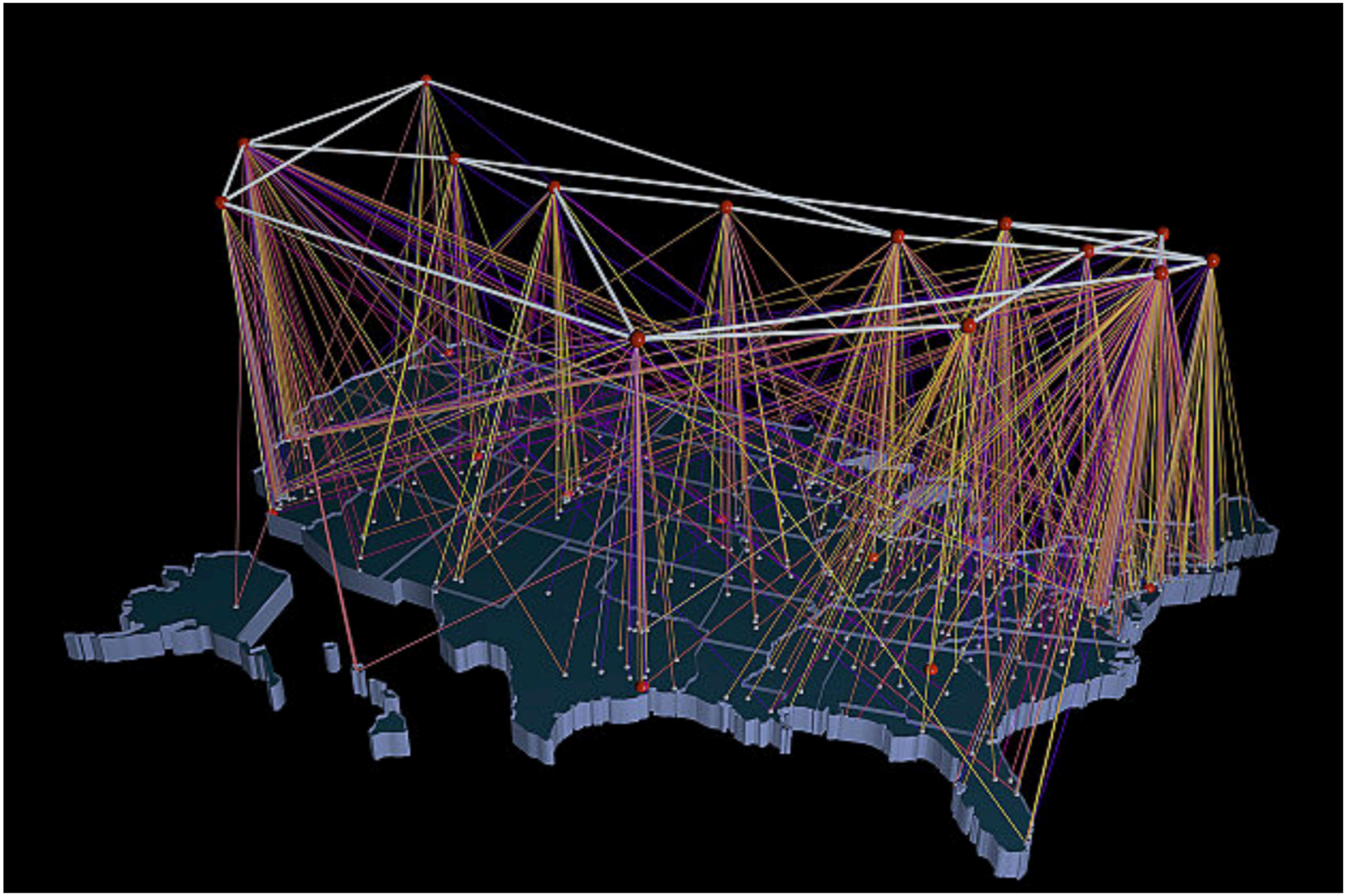
- IP-префикс
  - ≡ любой блок, используемый для маршрутизации
  - Является “единицей” процесса маршрутизации
- Протоколы маршрутизации автоматически строят “карту сети”
  - “Место рождения” префикса
  - Состояние каналов связи
  - Внешние факторы: технические, коммерческие, организационные

IP-маршрутизация



(Схема была взята из учебника Cisco Systems,
и потом покоцана автором презентации)

Интернет - это сложно



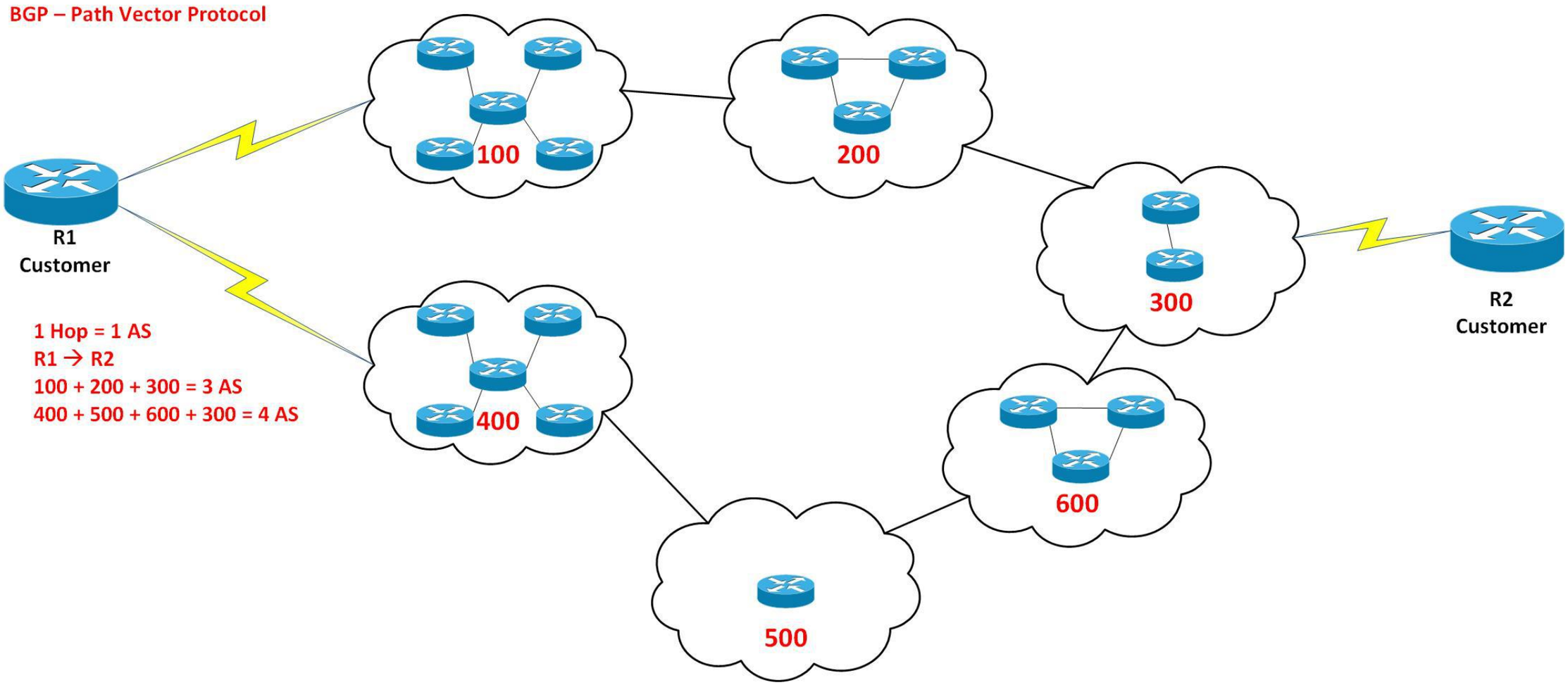
Автономные системы

- Определение
  - Автономная система - совокупность IP-префиксов и маршрутизаторов, находящаяся под единым управлением, и имеющая единую политику маршрутизации
  - Простым языком: автономная система “снаружи” ведет себя как один большой маршрутизатор
- Идентификатор автономной системы
  - Число: Autonomous System Number (ASN)
  - Старая (16bit ASN): 0-65536
  - Новая (32bit ASN): 0-4294967296

Процесс BGP-маршрутизации

- Анонсы
  - Анонс - информация о доступности IP-префикса
  - Каждая автономная система принимает и рассылает анонсы по каждому префиксу в Интернете
- Принятие решение о выборе среди анонсов
  - Критериев много!
  - Самые важные для нас сейчас:
    - Размер префикса: чем меньше адресов, тем выше приоритет маршрутной информации
    - Количество автономных систем по дороге: чем меньше, тем выше приоритет маршрутной информации

Автономные системы и протокол BGP

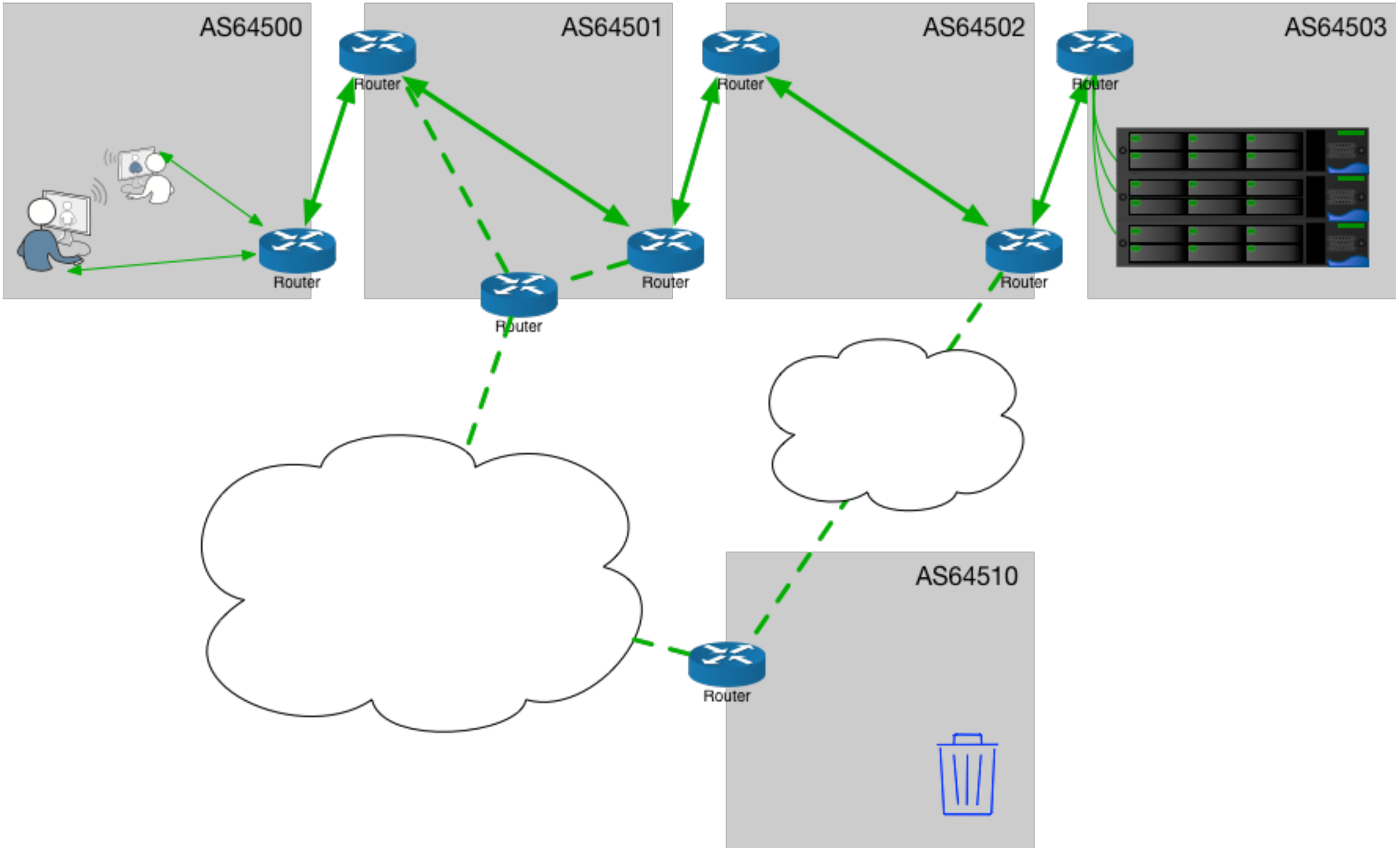


Route leaks
&
prefix hijacking

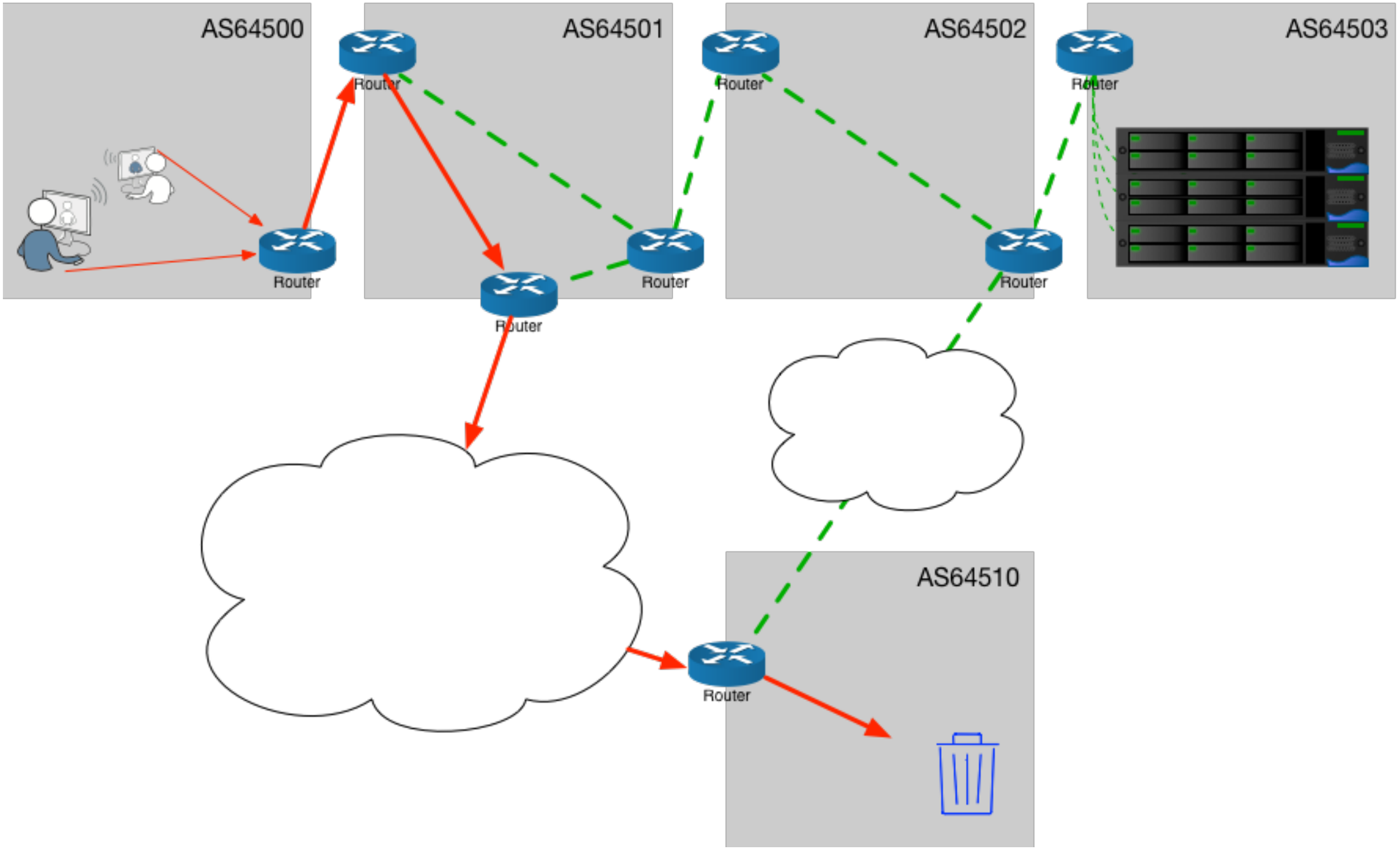
Что бы такого сделать плохого?

- Route leak (утечка маршрута)
  - Прохождение транзитного трафика через автономную систему, не предназначенную для его пропускания
    - Например, трафик от одного оператора к другому проходит через автономную систем конечного клиента
  - **Обычно** является результатом ошибки инженера (“синдром толстых пальцев”)
- Prefix hijacking (воровство префикса)
  - Анонсирование чужих префиксов
  - **Практически всегда** - результат злого умысла

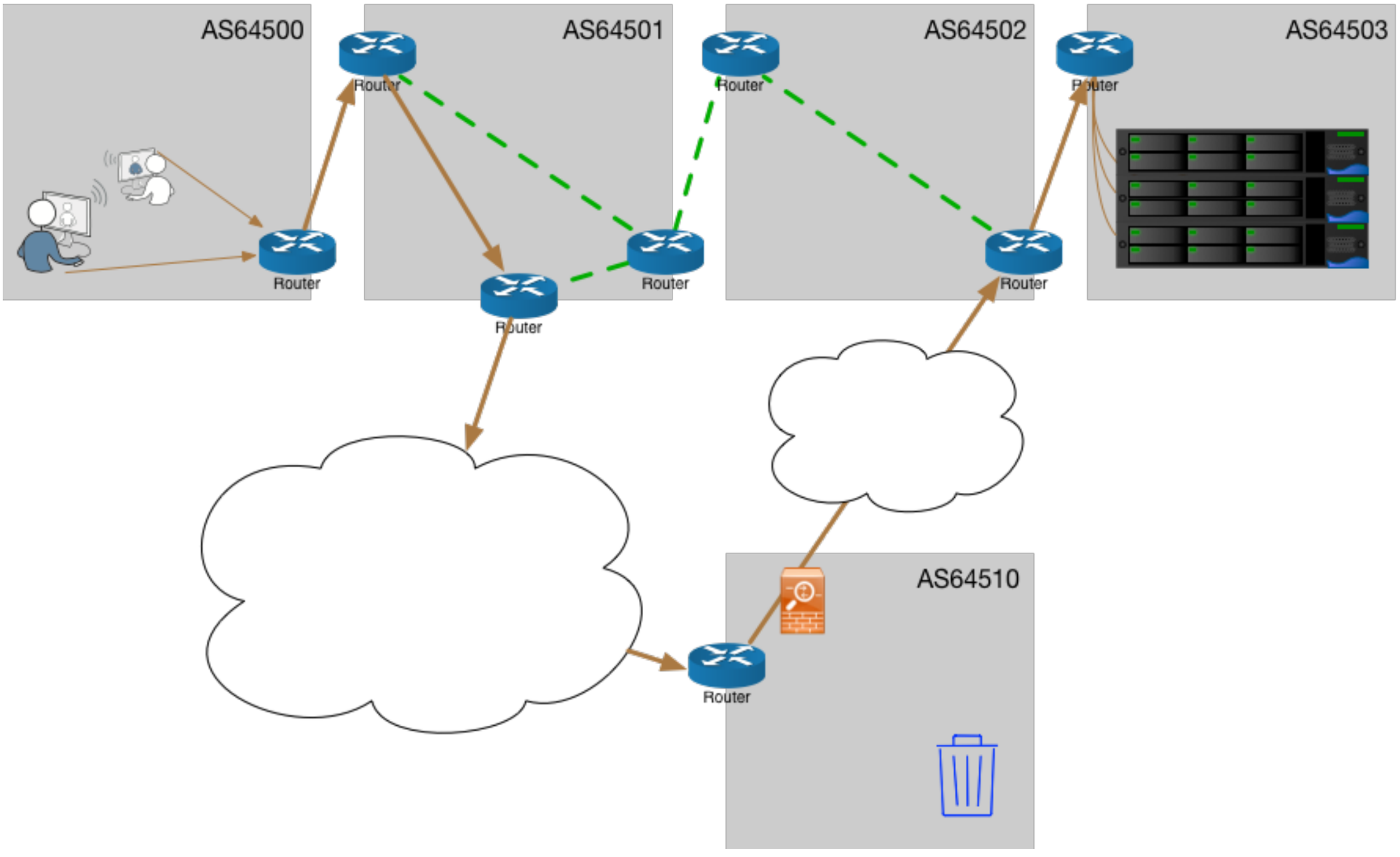
Нормальное прохождение трафика



Воровство префикса



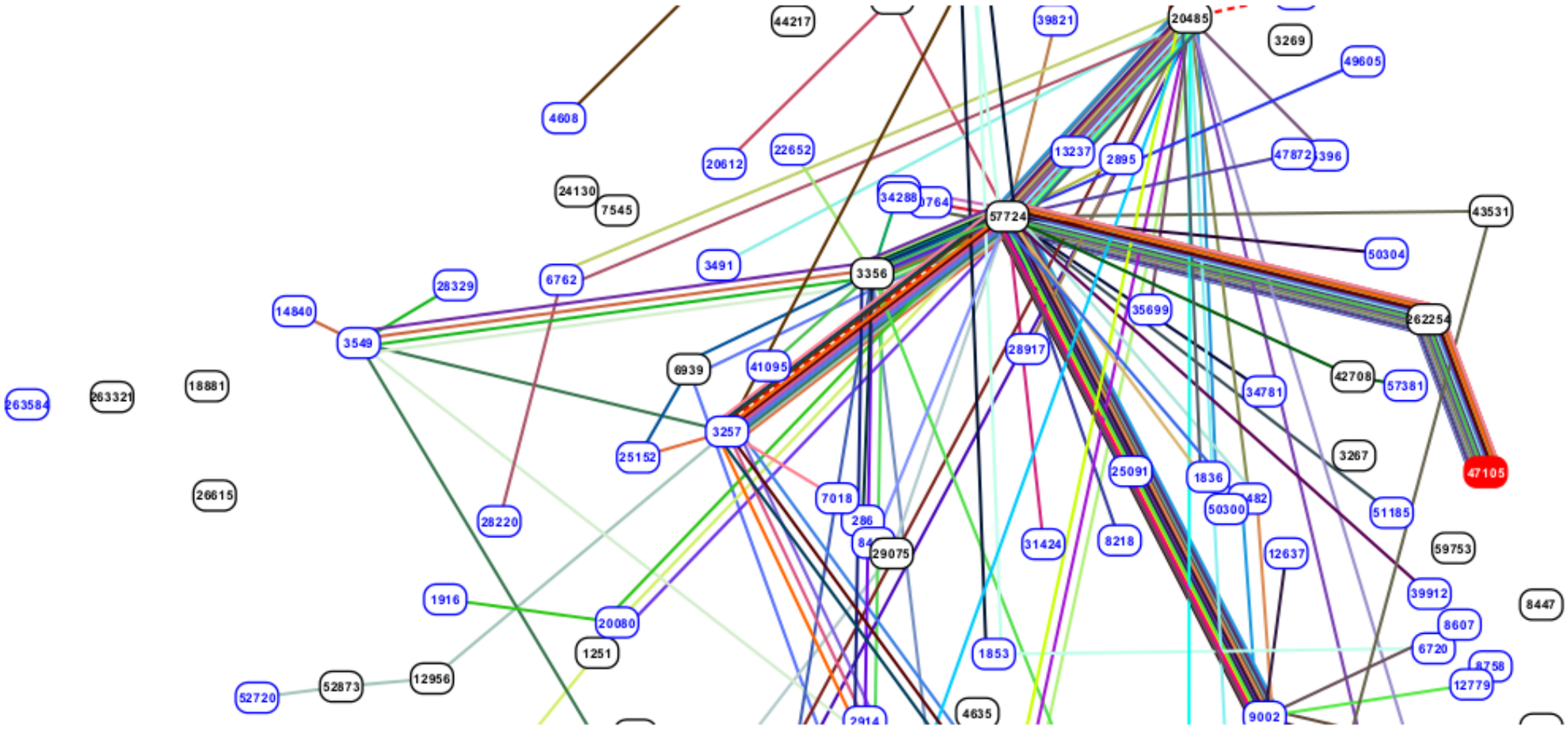
Утечка маршрута



Воровство префиксов

- Глобальное
  - Префикс разбивается на более мелкие
  - Для каждого из них создается свой анонс
  - Анонсы с более мелкими префиксами имеют приоритет
  - Результат виден на всех маршрутизаторах в Интернете
- Локальное
  - Создаем ложный анонс с исходным префиксом
  - Результат виден на той части маршрутизаторов, которые “недалеко” от точки создания поддельного анонса

Найдите, что не так

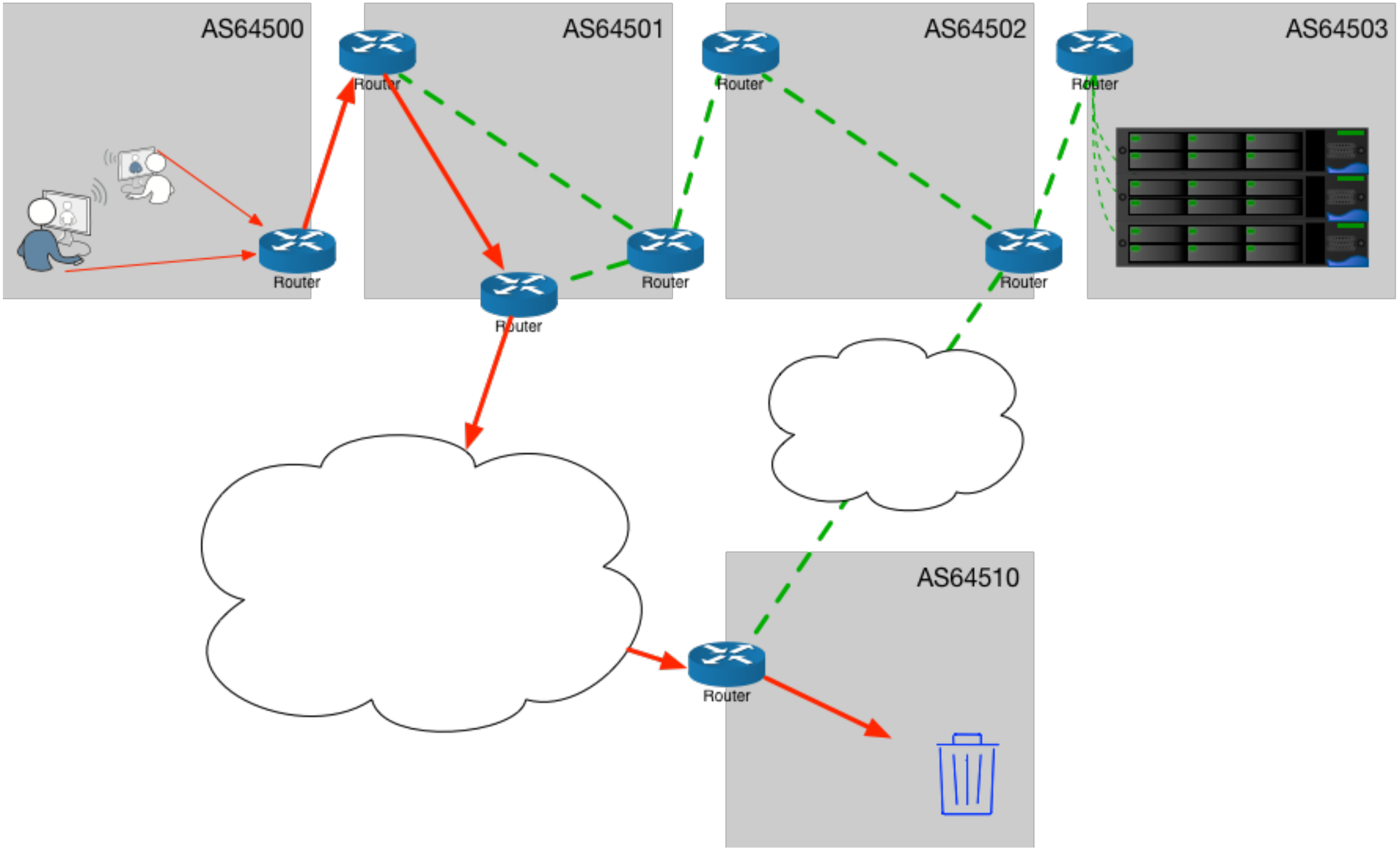


Практические последствия

DoS

- Denial of Service, отказ в обслуживании
- **Полная или частичная потеря доступности ресурса «извне»** без нарушения его внутренней структуры («взлома»).

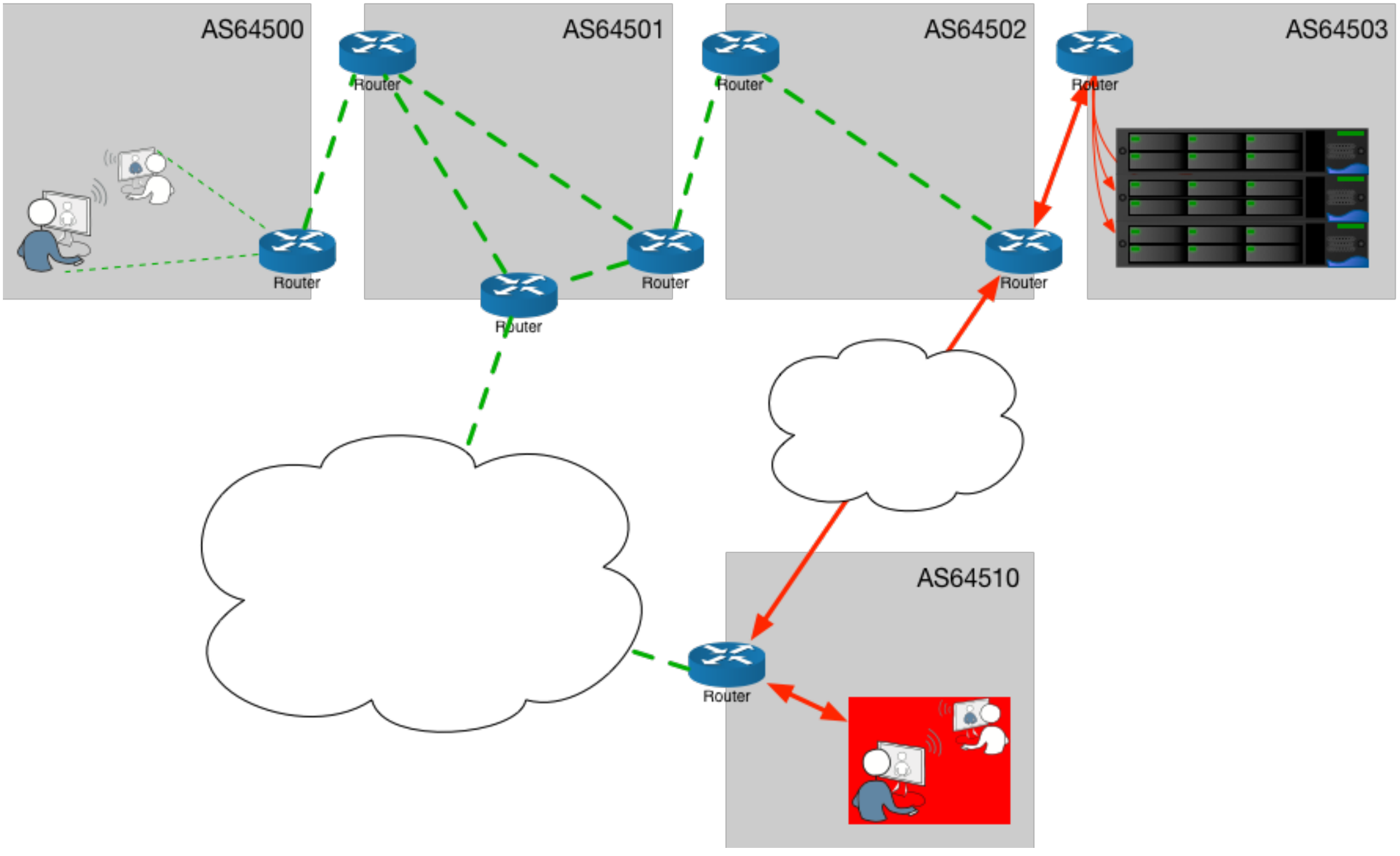
Воровство префикса как DoS



А теперь наоборот

- Что если красть префикс не сервиса, а клиента?

Воровство префикса как подделка документов

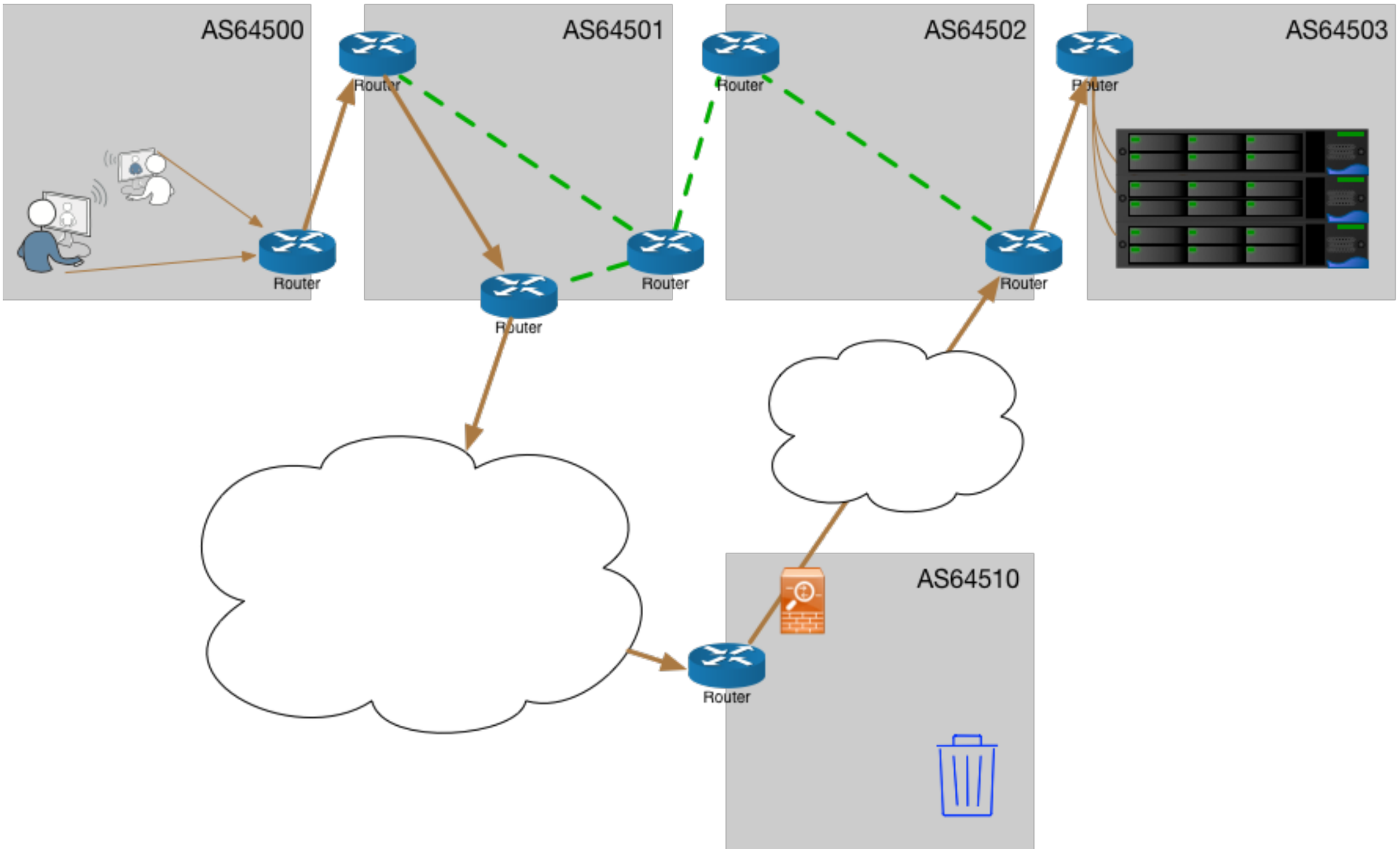


Сценарий MitM

- Получение чужого трафика = возможность выдавать себя за другого…
- …например, для получения сертификата безопасности у CA…
- …и создания поддельных сайтов **с формально правильным сертификатом**…
- …и последующим воровством всего трафика.

Роутинговый MitM сегодня = контентный MitM завтра

Утечка маршрута = анализ трафика



Что можно найти?

- Анализ и модификация незащищенных протоколов. Например:
  - DNS (всё ещё)
  - HTTP (всё ещё не менее четверти сайтов!)
  - SMTP, POP3, IMAP4
  - FTP (в том числе login/password)
  - VNC
  - SQL*Net
  - syslog

Что можно найти?

- Анализ мета-информации защищенных протоколов
  - Информация о совершаемых действиях (обращения к платежным шлюзам, например)
  - Поведенческий анализ
    - Отделение людей от ботов по поведенческому анализу зашифрованного трафика: точность около 95%
  - Идентификация пользователей
    - Построение временны́х корреляций: точность >95%

Роли

- Атакующая сторона
- Жертва
- **Невольный пособник**

Организация, у которой *“нет же ничего интересного”* легко может являться частью роутинговой атаки.

Примеры из истории

- 1997 год: “инцидент AS7007”, DoS на весь тогдашний Интернет
- 2015 год: перехват американского трафика белорусским оператором
- 2017 год: кража биткоинов из “майнингового кооператива” путем воровства маршрута
- 2018 год: роутинговый DoS на финансовые учреждения в Южной Америке
- Действия правительств
  - 2008 год. Пакистан заблокировал Youtube - но не “удержал” анонсы внутри страны
  - 2014 год. Турция заблокировала Google DNS себе и части глобального интернета
  - 2017 год. Украина заблокировала Яндекс. И Cloudflare для части мирового Интернета, нечаянно.

Что делать

Routing security

- Базовые меры
  - Явное анонсирование **важных** мелких префиксов
  - Использование встроенных механизмов защиты BGP (TCP MD5, TTL Protection)
- RPKI
- RIPE DB
- Системы слежения и анализа системы маршрутизации
- MANRS

Routing security: RPKI

- Криптографическая привязка префикса к ASN
- Цепочка доверия: ICANN → RIR → LIR
- Защита от “синдрома толстых пальцев”
  - Т.к. AS PATH не защищен!
- Две стороны администрирования:
  - Подпись своих ресурсов
    - ✓ 45 секунд на портале My RIPE (бывший LIR Portal)
  - Проверка подписи чужих ресурсов
    - ✓ Требуются сервер, софт на нём, и поддержка на сетевом оборудовании

Routing security: RIPE DB

- Часть, называемая IRR
  - Описания префиксов
  - Описания политик маршрутизации в роутинговых объектах
- Управляется LIRами
  - Поэтому не всегда точны
  - (это был намёк)
- Используется для построения фильтров
  - В наши дни - в основном на IXP

Routing security: monitoring

- Системы слежения и анализа системы маршрутизации
  - BGPlay и RIPEStat
    - JSON API
    - Наличие исторических данных
    - Визуализация исторических данных
  - Qrator/Radar
    - Наглядность и простота представления
  - BGPMon
- Можно (да и нужно) пользоваться всеми параллельно
- “Сырые данные” в RIS (dataset от RIPE)
  - Приглашаем присоединяться к проекту!

Routing security: MANRS

- Инициатива ISOC
  - https://www.manrs.org/
  - Состоит из нескольких частей
  - Одна из которых - BCP38
    - Не всегда легко реализуется, но подумать стоит!
- “Доска почёта” как дополнительный PR
  - https://www.manrs.org/isps/participants/
  - Ни одного участника из Украины 😟

Routing security: future

- A.R.T.E.MI.S. (Automatic and Real-Time dEtection and MItigation System)
  - Авторы: INSPIRE group, Greece (www.inspire.edu.gr); the Center for Applied Internet Data Analysis (CAIDA), USA (www.caida.org)
  - Поддержка: RIPE NCC Community Projects Fund
- BGPSEC
  - RFC8205, September 2017
  - Это будущее уже не случилось
- draft-azimov-sidrops-aspa-profile-00
  - “Продолжение” RPKI (наследует логику)
  - Уже есть в roadmap у вендоров

Эшелонированная защита

- Локализация сенситивных данных
  - Например, не писать в syslog даже неправильно введенные пароли
- Отказ от нешифрованных протоколов
  - Особенно на внешних каналах!
- Контроль доступа
  - Как осуществляется доступ в сеть?
  - На оборудование?
- Контроль активов
  - Какие есть выданные мне сертификаты?
- Etc
- Etc
- Etc
- Etc

Questions