Владивостокский государственный университет экономики и сервиса
Институт информатики, инноваций и бизнес систем
Кафедра информационных систем и компьютерных технологий

Предмет: «Телекоммуникационные технологии»

Руководитель: Сачко Максим Анатольевич, ст. преподаватель

ВГУЭС

Тема 9

Проблемы безопасности протоколов TCP/IP

Содержание:

1) Методы и инструменты
2) Перехват данных
3) Имперсонация
4) Несанкционированное подключение к сети и обмен данными
5) Принуждение к ускоренной передаче данных
6) Отказ в обслуживании
7) Обсуждение

1. Проблемы безопасности протоколов TCP/IP

- перехват данных, передаваемых через сеть от одного узла другому;
- имперсонация (spoofing) (узел злоумышленника выдает себя за другой узел);
- несанкционированное подключение к сети;
- несанкционированная передача данных (обход правил фильтрации IP-трафика в сетях, защищенных брандмауэрами);
- принуждение узла к передаче данных на завышенной скорости;
- приведение узла в состояние, когда он не может нормально функционировать, передавать и принимать данные (DoS — denial of service, отказ в обслуживании).

Методы и инструменты

Для достижения своих целей злоумышленник использует прослушивание *(sniffing),* сканирование сети и генерацию пакетов. Под генерацией пакетов понимается создание и отправка специально сконструированных датаграмм или кадров, позволяющих злоумышленнику выполнить ту или иную атаку. Особо выделим здесь фальсификацию пакетов, то есть создание IP-датаграмм или кадров уровня доступа к сети, направленных якобы от другого узла *(spoofing).*

Прослушивание сети

Прослушивание сети Ethernet (а подавляющее большинство локальных сетей используют именно эту технологию) является тривиальной задачей: для этого нужно просто перевести интерфейс в режим прослушивания *(promiscuous mode)*. Легко доступны программы, не только записывающие весь трафик в сегменте Ethernet, но и выполняющие его отбор по установленным критериям

AntiSniff

Злоумышленник, прослушивающий сеть, может быть обнаружен с помощью утилиты **AntiSniff**, которая выявляет в сети узлы, чьи интерфейсы переведены в режим прослушивания.

Первый тест основан на особенностях обработки разными операционными системами кадров Ethernet, содержащих IP-датаграммы, направленные в адрес тестируемого узла.

Второй тест основан на предположении, что программа прослушивания на хосте злоумышленника выполняет обратные DNS-преобразования для IP-адресов подслушанных датаграмм. AntiSniff фабрикует датаграммы с фиктивными IP-адресами, после чего прослушивает сеть на предмет DNS-запросов о доменных именах для этих фиктивных адресов. Узлы, отправившие такие запросы, находятся в режиме прослушивания.

Тесты третьей группы, наиболее универсальные. Тесты основаны на том, что в режиме прослушивания обработка всех кадров ложится на программное обеспечение злоумышленника, то есть, в конечном счете, на операционную систему. AntiSniff производит пробное тестирование узлов сети на предмет времени отклика на сообщения ICMP Echo, после чего порождает в сегменте шквал кадров, направленных на несуществующие MAC-адреса, при этом продолжая измерение времени отклика.

Сканирование сети

Сканирование сети имеет своей целью выявление подключенных к сети компьютеров и определение работающих на них сетевых сервисов (открытых портов TCP или UDP). Первая задача выполняется посылкой ICMP-сообщений Echo с помощью программы ping с последовательным перебором адресов узлов в сети. Стоит попробовать отправить Echo-сообщение по широковещательному адресу — на него ответят все компьютеры, поддерживающие обработку таких сообщений.

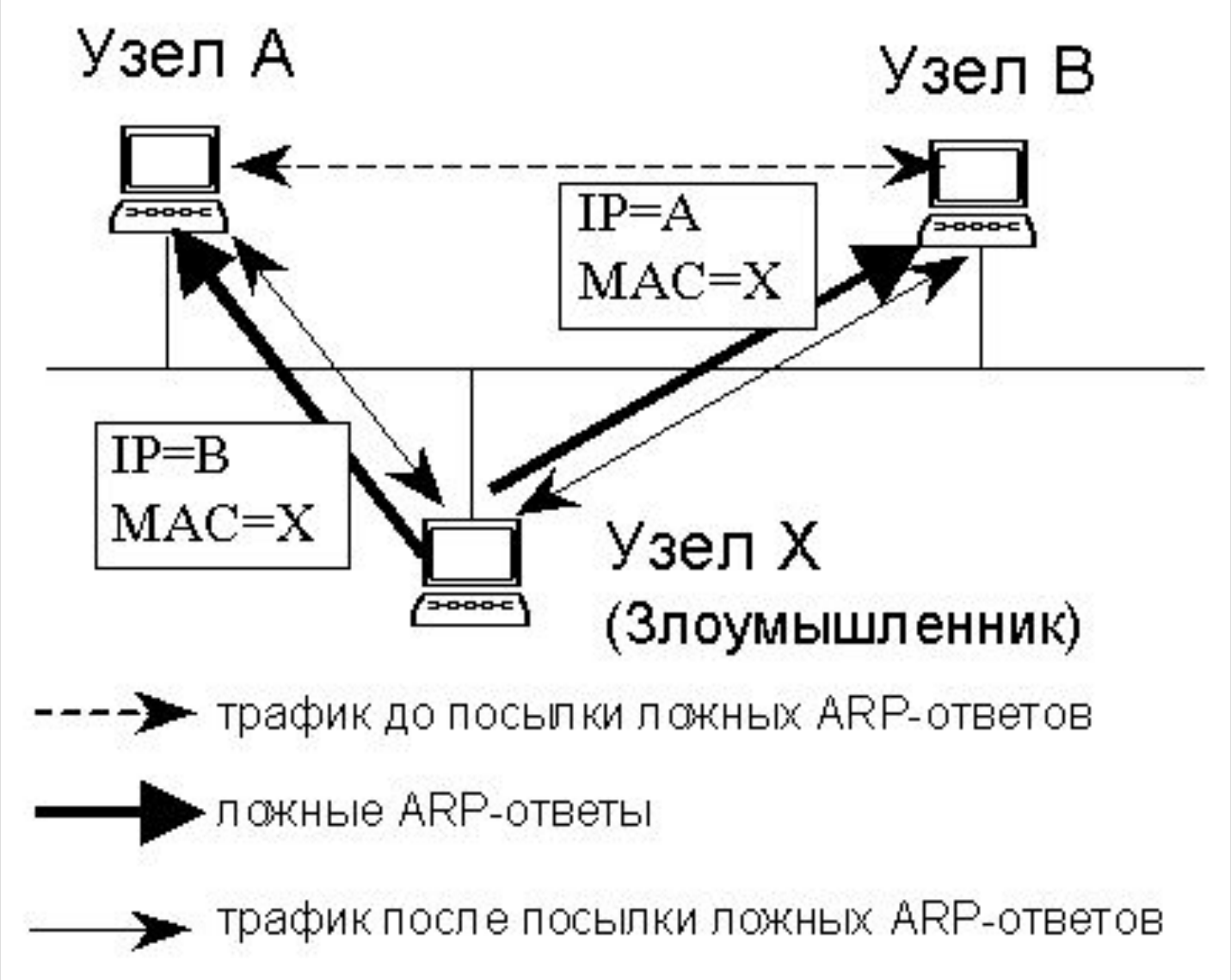
Генерация пакетов

Генерация датаграмм или кадров произвольного формата и содержания производится не менее просто, чем прослушивание сети Ethernet. Библиотека **libnet** обеспечит программиста всем необходимым для решения этой задачи. Библиотека **libpcap** предоставляет инструментарий для обратного действия - извлечения пакетов из сети и их анализа.

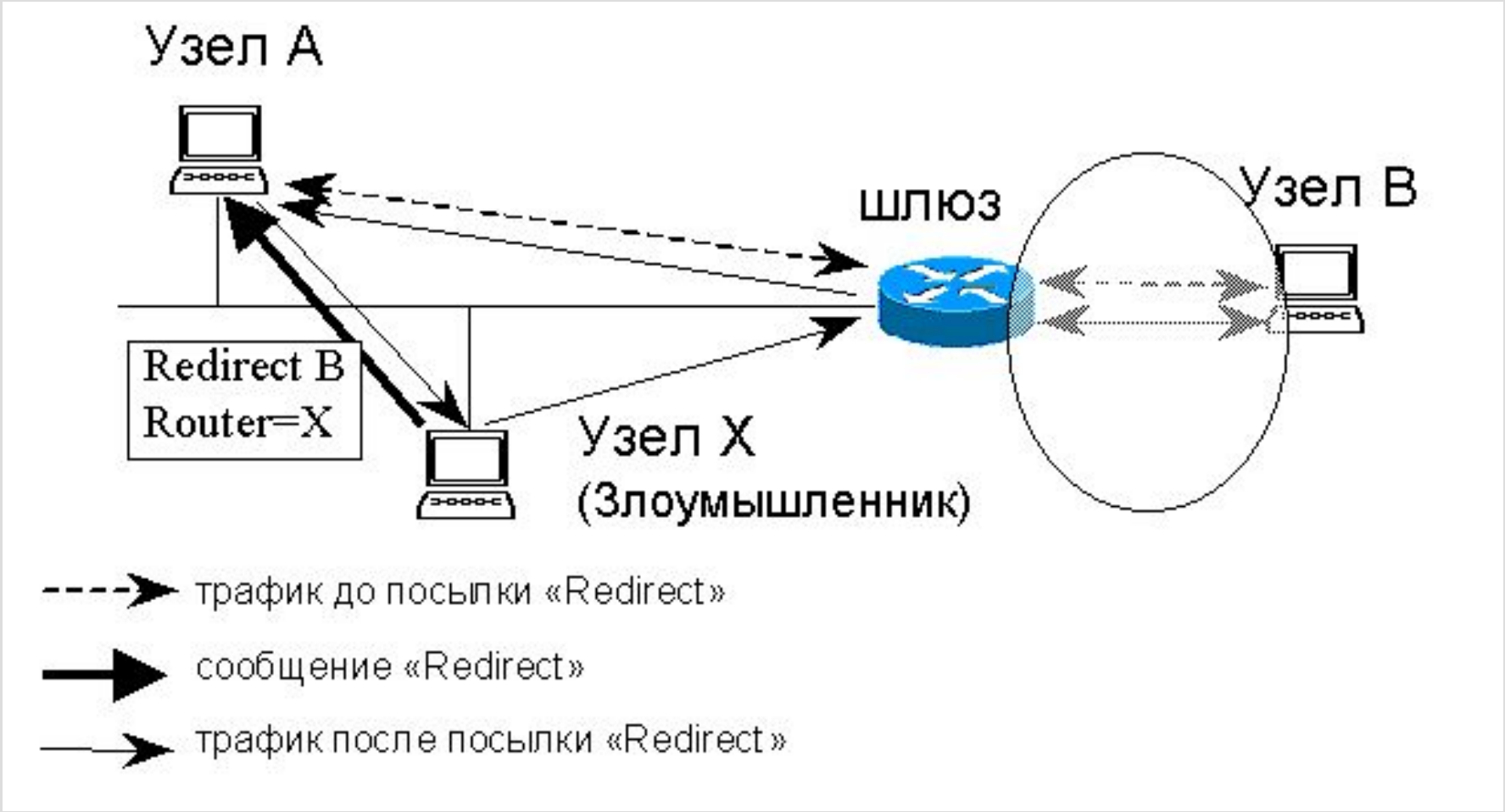
2. Перехват данных

Простейшей формой перехвата данных является прослушивание сети. В этом случае злоумышленник может получить массу полезной информации: имена пользователей и пароли (многие приложения передают их в открытом виде), адреса компьютеров в сети, в том числе адреса серверов и запущенные на них приложения, адрес маршрутизатора, собственно передаваемые данные, которые могут быть конфиденциальными (например, тексты электронных писем) и т. п.

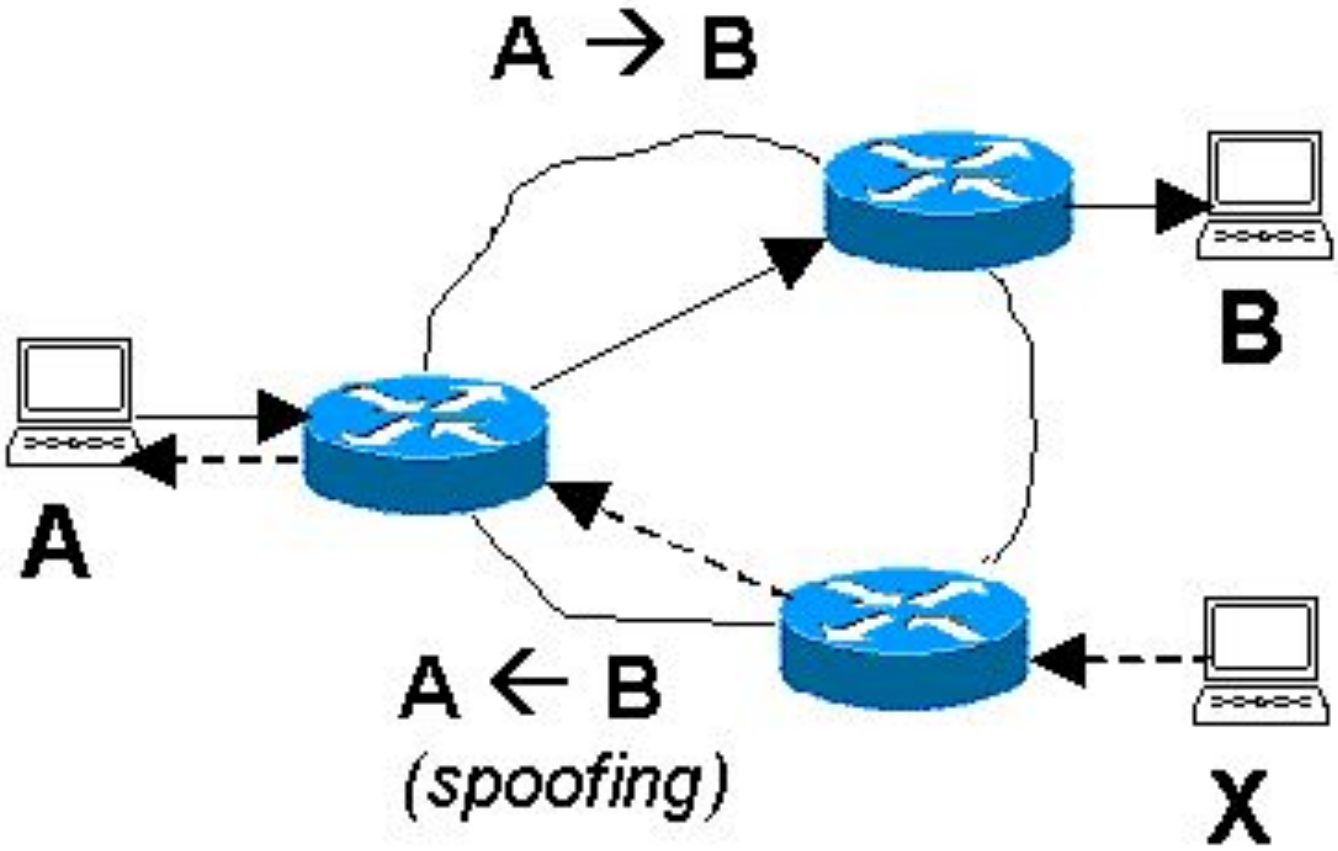
Схема ARP-атаки



Навязывание ложного маршрутизатора



Имперсонация



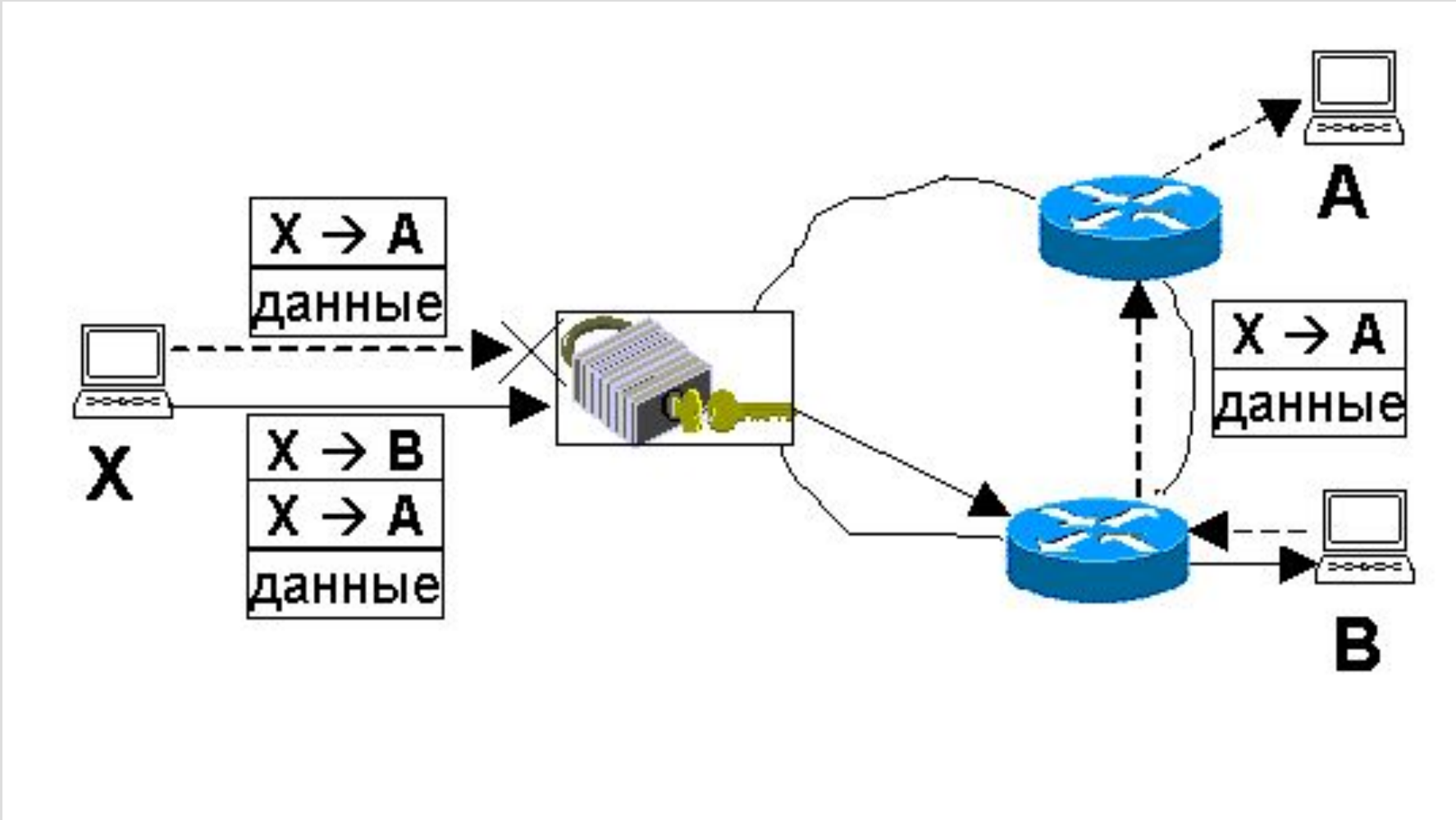
Несанкционированное подключение к сети

Для незаконного подключения к сети злоумышленник, разумеется, должен иметь физическую возможность такого подключения. В крупных корпоративных и особенно университетских сетях такая возможность часто имеется. Следующим шагом для злоумышленника является конфигурирование параметров стека TCP/IP его компьютера.

Несанкционированный обмен данными

С целью обеспечения безопасности внутренней (корпоративной) сети на шлюзе могут использоваться фильтры, препятствующие прохождению определенных типов датаграмм. Датаграммы могут фильтроваться по IP-адресам отправителя или получателя, по протоколу (поле Protocol IP-датаграммы), по номеру порта TCP или UDP, по другим параметрам, а также по комбинации этих параметров.

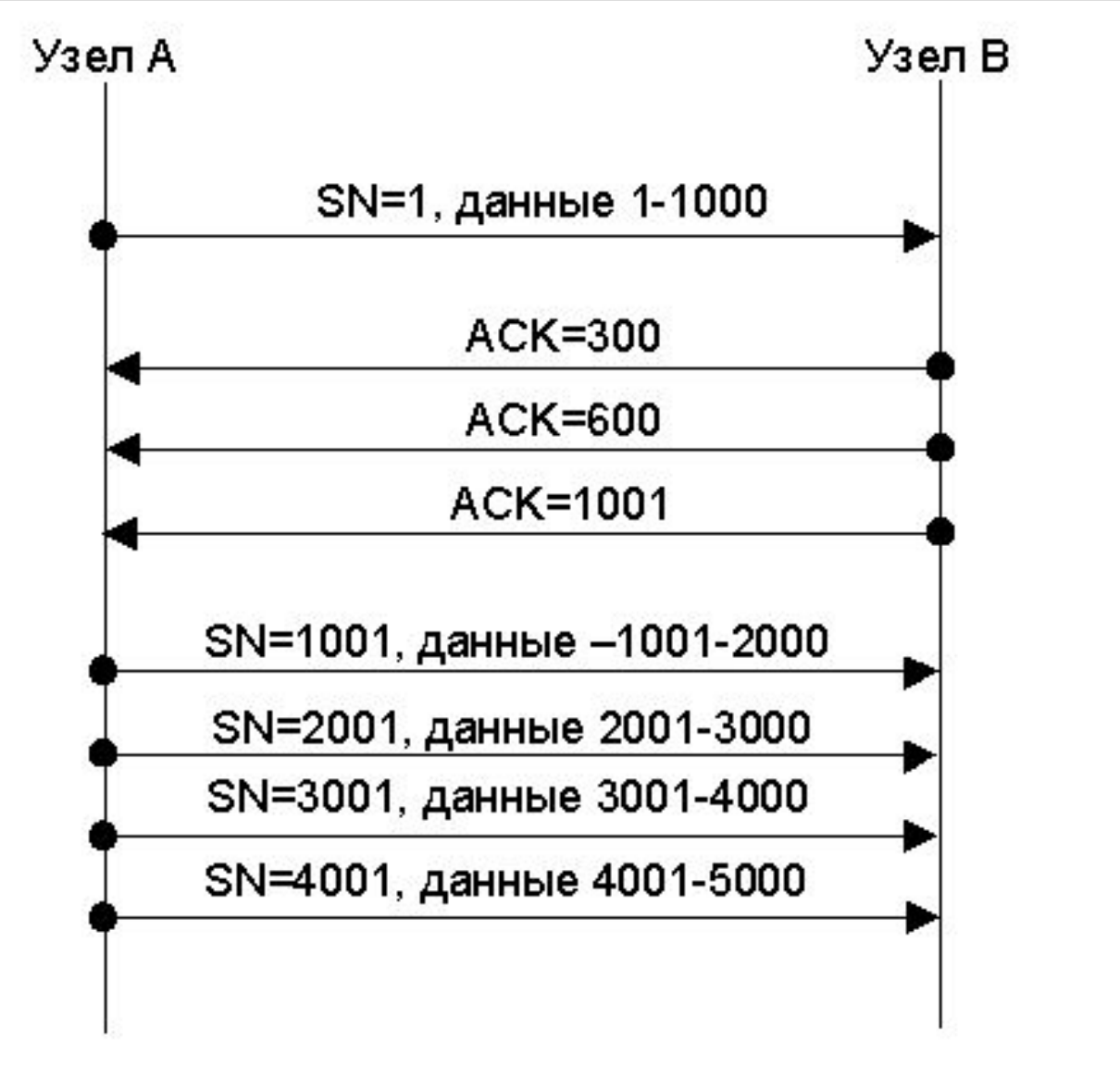
Туннелирование сквозь маршрутизатор



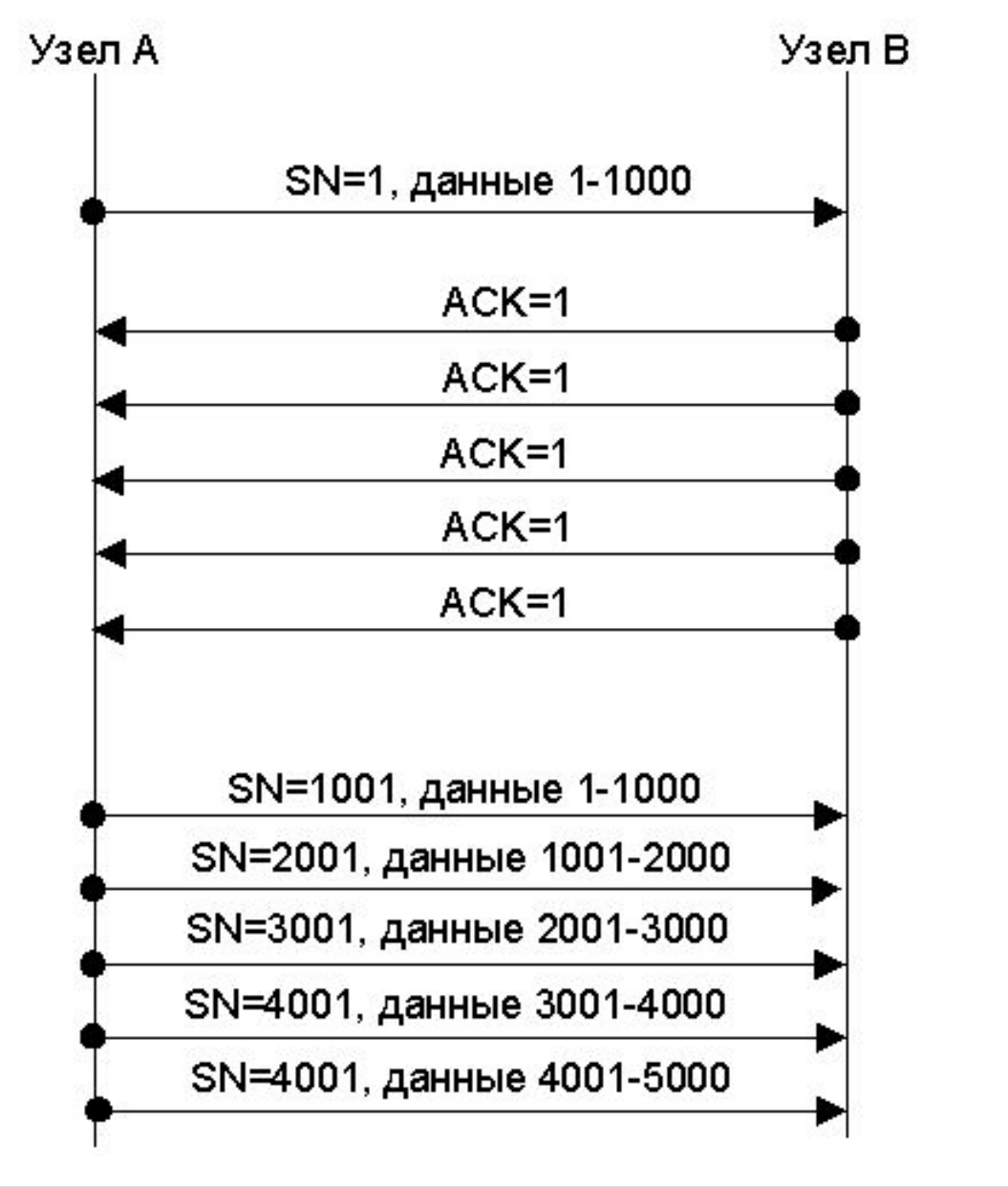
Принуждение к ускоренной передаче данных

Атаки выполняются путем специально организованной посылки злоумышленником подтверждений приема данных (ACK-сегментов). Эти атаки эксплуатируют следующее неявное допущение, заложенное в протокол TCP: один участник TCP-соединения полностью доверяет другому участнику в том, что тот действует в строгом соответствии с теми же спецификациями протокола, что и первый

Расщепление подтверждений



Ложные дубликаты подтверждений



Отказ в обслуживании

Атаки типа «отказ в обслуживании» (**DoS**, denial of service), по-видимому, являются наиболее распространенными и простыми в исполнении. Целью атаки является приведение атакуемого узла или сети в такое состояние, когда передача данных другому узлу (или передача данных вообще) становится невозможна или крайне затруднена. Вследствие этого пользователи сетевых приложений, работающих на атакуемом узле, не могут быть обслужены

Истощение ресурсов

Атака **smurf** состоит в генерации шквала ICMP Echo-ответов, направленных на атакуемый узел.

Атака **SYN flood** состоит в посылке злоумышленником SYN-сегментов TCP на атакуемый узел в количестве большем, чем тот может обработать одновременно.

Атака **UDP flood** состоит в затоплении атакуемой сети шквалом UDP-сообщений.

Ложные DHCP-клиенты - создании злоумышленником большого числа сфальсифицированных запросов от различных несуществующих DHCP-клиентов.

Фильтрация на маршрутизаторе

- Запретить пропуск датаграмм с широковещательным адресом.
- Запретить пропуск датаграмм, направленных из внутренней сети в Интернет, но имеющих внешний адрес отправителя.
- Запретить пропуск датаграмм, прибывающих из Интернета, но имеющих внутренний адрес отправителя.
- Запретить пропуск датаграмм с опцией «Source Route» и, если они не используются для групповой рассылки, инкапсулированных датаграмм.

Фильтрация на маршрутизаторе

- Запретить пропуск датаграмм с ICMP-сообщениями между сетью организации и Интернетом, кроме необходимых.
- На сервере доступа клиентов по коммутируемой линии — разрешить пропуск датаграмм, направленных только с или на IP-адрес, назначенный клиенту.
- Запретить пропуск датаграмм с UDP-сообщениями, направленными с или на порты echo и chargen, либо на все порты, кроме используемых.

Фильтрация на маршрутизаторе

- Использование TCP Intercept для защиты от атак SYN flood.
- Фильтрация TCP-сегментов выполняется в соответствии с политикой безопасности: разрешаются все сервисы, кроме запрещенных, или запрещаются все сервисы, кроме разрешенных (описывая каждый прикладной сервис в главе 3, мы будем обсуждать вопросы фильтрации сегментов применительно к сервису).

Защита маршрутизатора

- Использовать аутентификацию сообщений протоколов маршрутизации с помощью алгоритма MD5.
- Осуществлять фильтрацию маршрутов, объявляемых сетями-клиентами, провайдером или другими автономными системами. Фильтрация выполняется в соответствии с маршрутной политикой организации; маршруты, не соответствующие политике, игнорируются.
- Использовать на маршрутизаторе, а также на коммутаторах статическую ARP-таблицу узлов сети организации.

Защита маршрутизатора

- Отключить на маршрутизаторе все ненужные сервисы.
- Ограничить доступ к маршрутизатору консолью или выделенной рабочей станцией администратора, использовать парольную защиту; не использовать telnet для доступа к маршрутизатору в сети, которая может быть прослушана.
- Использовать последние версии и обновления программного обеспечения, следить за бюллетенями по безопасности, выпускаемыми производителем.

Защита хоста

- Запретить обработку ICMP Echo-запросов, направленных на широковещательный адрес.
- Запретить обработку ICMP-сообщений Redirect, Address Mask Reply, Router Advertisement, Source Quench.
- Если хосты локальной сети конфигурируются динамически сервером DHCP, использовать на DHCP-сервере таблицу соответствия MAC- и IP-адресов и выдавать хостам заранее определенные IP-адреса.

Защита хоста

- Отключить все ненужные сервисы TCP и UDP.
- Если входящие соединения обслуживаются супердемоном inetd, то использовать оболочки TCP wrappers или заменить inetd на супердемон типа xinetd или tcpserver, позволяющий устанавливать максимальное число одновременных соединений, список разрешенных адресов клиентов, выполнять проверку легальности адреса через DNS и регистрировать соединения в лог-файле.

Защита хоста

- Использовать программу типа tcplogd, позволяющую отследить попытки скрытного сканирования.
- Использовать статическую ARP-таблицу узлов локальной сети.
- Применять средства безопасности используемых на хосте прикладных сервисов.
- Использовать последние версии и обновления программного обеспечения, следить за бюллетенями по безопасности, выпускаемыми производителем.

Вопросы для самопроверки:

1. Определите проблему качества обслуживания в сетях IP.
2. В чем отличие коммутации от маршрутизации? Какова выгода от использования технологий коммутации при передаче трафика в IP-сетях?
3. Какие преимущества имеет IP версии 6 над версией 4?
4. Какие меры защиты от атак необходимы маршрутизатору и хосту?
5. В чем отличие стандартный и расширенных листов доступа?
6. Какие методы перехвата данных вы знаете?

Рекомендуемая литература:

1. Мамаев М.А. Телекоммуникационные технологии (Сети TCP/IP). – Владивосток: Изд-во ВГУЭС, 2004.
2. Леинванд А., Пински Б. Конфигурирование маршрутизаторов Cisco. 3-е издание. – М.: "Вильямс", 2007.
3. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. – СПб: "Питер", 2005.
4. Вегешна Ш. Качество обслуживания в сетях IP - М.: "Вильямс", 2003.

- **Использование материалов презентации**

- Использование данной презентации, может осуществляться только при условии соблюдения требований законов РФ об авторском праве и интеллектуальной собственности, а также с учетом требований настоящего Заявления.

- Презентация является собственностью авторов. Разрешается распечатывать копию любой части презентации для личного некоммерческого использования, однако не допускается распечатывать какую-либо часть презентации с любой иной целью или по каким-либо причинам вносить изменения в любую часть презентации. Использование любой части презентации в другом произведении, как в печатной, электронной, так и иной форме, а также использование любой части презентации в другой презентации посредством ссылки или иным образом допускается только после получения письменного согласия авторов.