Нижегородский государственный университет им. Н.И. Лобачевского

Национальный исследовательский университет

Программа повышение конкурентоспособности ННГУ им. Н.И. Лобачевского

Стратегическая инициатива 7 «Достижение лидирующих позиций в области суперкомпьютерных технологий и высокопроизводительных вычислений»

Основная образовательная программа

010300 Фундаментальная информатика и информационные технологии

Учебно-методическая разработка по дисциплине

Компьютерные сети

Гергель А.В.

СЕТИ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ВЫСОКОПРОИЗВОДТЕЛЬНЫХ СИСТЕМ

Нижний Новгород
2014 год

УДК 681.3.06
ББК 22.20

Гергель А.В. Сети передачи данных для высокопроизводительных систем: Учебное пособие. – Нижний Новгород: Нижегородский госуниверситет, 2014. – 92 с.

Высокопроизводительные вычислительные системы используют компьютерные сети для решения различных задач, например распределение вычислительной нагрузки между узлами системы. Важность и класс решаемых задач высокопроизводительными системами предъявляют определенные требования к используемой сети. Такими требования являются надежность работы сети, скорость передачи данных, безопасность передаваемых данных, возможность передачи трафика любого типа и т.п. Обеспечение всех требований осуществляется путем дополнительных настроек сетевых устройства, понимание сетевых протоколов, сервисов, и сетевых инструментов.

В предлагаемом пособии рассматриваются принципы построения компьютерных сетей, основные технологии локальных сетей, средства межсетевого взаимодействия, функционирование и основные характеристики коммутаторов и маршрутизаторов.

Рассматриваются семиуровневая модель и модель TCP/IP, прикладной и транспортный уровень, физический уровень модели. Канальный уровень представлен двумя подуровнями и соответствующими технологиями локальных сетей. Маршрутизаторы представляют средства межсетевого взаимодействия, которое базируется на IP-адресах. Принципы маршрутизации базируются на сетевых протоколах и протоколах маршрутизации. Приведены основные сведения о протоколах вектора расстояния и состояния канала связи. Излагаются основы и примеры конфигурирования наиболее широко используемого маршрутизирующего протокола OSPF. Рассмотрены принцип действия и конфигурирование сетевых фильтров. Приведены примеры конфигурирования коммутаторов, принципы и основы конфигурирования виртуальных локальных сетей.

Учебное пособие предназначено для широкой аудитории: студентов, аспирантов высших учебных заведений, преподавателей и научных сотрудников, изучающих параллельные технологии.

УДК 681.3.06
ББК 22.20

Содержание

Введение в сетевые технологии

Первые компьютеры были автономными устройствами. Каждый компьютер работал отдельно, независимо от других. При таком подходе возникало много проблем. Например, есть сеть, в которой к одному компьютеру подключен принтер. В этом случае, использовать принтер мог человек, работавший за этим компьютером, другие сотрудники не имели возможности распечатывать свои документы. Так же возникали трудности при работе над одним документом нескольких сотрудниками. При изменении файла требовалось каждый раз производит обновление у всех остальных сотрудников. При таком подходе была очень низкая эффективность работы. Необходимо было найти решение, которое бы удовлетворяло трем перечисленным ниже требованиям, а именно:

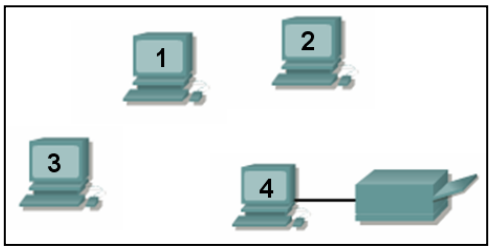


Рис 1. Пример сети, в которой к одному компьютеру подключен принтер

- устраняло дублирование оборудования и ресурсов;
- обеспечивало эффективный обмен данными между устройствами;
- снимало проблему управления сетью.

Было найдено два решения, выполняющих поставленные условия - локальные и глобальные сети.

Локальные сети

Локальные вычислительные сети (ЛВС) — это высокоскоростные сети с малым количеством ошибок, которые охватывают небольшие географические пространства (до нескольких тысяч метров). ЛВС объединяют рабочие станции, терминалы и периферийные устройства в одном здании или другой пространственно ограниченной области. Локальные сети обеспечивают множеству подключенных настольных устройств доступ к среде передачи данных с высокой пропускной способностью

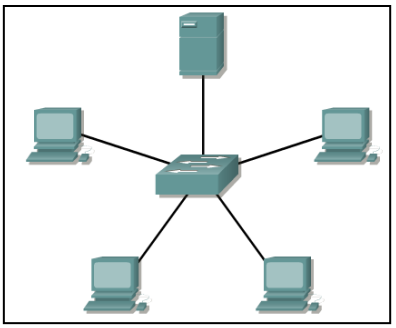


Рис 2. Локальная сеть

Характерными особенностями локальной сети являются:

- ограниченные географические пределы;
- обеспечение пользователей доступа к среде передачи данных с высокой пропускной способностью;
- постоянное подключение к локальным сервисам;
- физическое или беспроводное подключение к локальной сети.

К устройствам локальной сети относятся следующие устройства

- Мосты - подключают сегменты локальной сети и помогают фильтровать трафик
- Концентраторы - концентрируют соединения локальной сети и позволяют использовать в качестве среды передачи данных витую пару
- Коммутаторы Ethernet - обеспечивают сегментам и настольным системам полнодуплексную связь и выделенную полосу пропускания
- Маршрутизаторы - обеспечивают большое количество сервисов, включая организацию взаимодействия сетей и управление широковещательной рассылкой.

Глобальные сети

Быстрое распространение компьютеров привело к увеличению числа локальных сетей. Появилась потребность передачи данных от одной локальной сети до другой. Пешение данной задачи - создание глобальных сетей. Глобальные сети служат для объединения локальных сетей и обеспечивают связь между компьютерами, находящимися в локальных сетях. Глобальные сети охватывают значительные географические пространства и дают возможность связать устройства, расположенные на большом удалении друг от друга.

При подключении компьютеров, принтеров и других устройств к глобальной сети возникает возможность совместного использования информации и ресурсов, а также доступа к Internet.

Распределенные сети состоят из трех основных компонент:

- Локальные сети, как узлы распределенной сети
- Каналы, соединяющие ЛВС.
- Оборудование и программы, обеспечивающие локальным сетям доступ к каналам связи.

Для объединения локальных сетей требуется специальное оборудование независимо от того, находятся ли эти ЛВС в одном здании или связаны через распределенную сеть.

- Повторители (Repeater) - усиливают полученный из кабельного сегмента сигнал и передают его в другой сегмент.

  - объединяют идентичные ЛВС;
  - простое усиление сигналов.
- Коммутаторы передают сообщения на основе записей в таблице коммутации.

  - Возможность фильтрации сетевого трафика на основе MAC адресов;
  - сохраняет информацию о всех узлах;
- Маршрутизаторы (Router) обеспечивают выбор маршрута от сети в которой располагается отправитель до сети в которой располагается получатель.

- Принимает решение о выборе "лучшего пути" из множества маршрутов до сети получателя;
- Маршрутизатор поддерживает работу различных сервисов, например DHCP, NAT
- Маршрутизатор обеспечивает безопасность передаваемых данных
- и многое другое

Архитектура сети

Сетевая архитектура сродни архитектуре строений. Архитектура здания отражает стиль конструкций и материалы, используемые для постройки. Архитектура сети описывает не только физическое расположение сетевых устройств, но и тип используемых адаптеров и кабелей. Кроме того, сетевая архитектура определяет методы передачи данных по кабелю.

Топология сети описывает схему физического соединения компьютеров. Существуют 3 основных типа сетевой топологии:

Топология: Общая шина.

При использовании шинной топологии компьютеры соединяются в одну линию, по концам, которой устанавливают терминаторы. Когда источник передает сигналы в сетевую среду, они движутся в обоих направлениях от источника. Эти сигналы доступны всем устройствам в ЛВС. Каждое устройство проверяет проходящие данные. Если MAC- или IP-адрес пункта назначения, содержащийся в пакете данных, не совпадает с соответствующим адресом этого устройства, данные игнорируются.

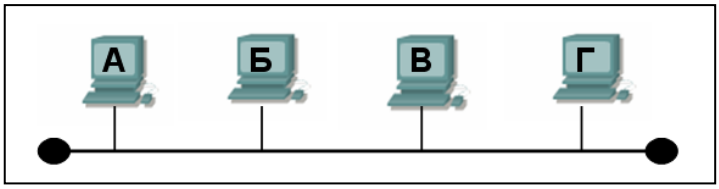


Рис 3. Топология общая шина

Преимущества шинной топологии заключаются в простоте организации сети и низкой стоимости. Недостатком является низкая устойчивость к повреждениям - при любом обрыве кабеля вся сеть перестает работать, а поиск повреждения весьма затруднителен.

Топология: *Звезда.*

При использовании топологии "звезда", каждый компьютер подключается к коммутатору. Связь между устройством и центральным каналом или коммутатором осуществляется посредством двухточечных линий. Когда источник передает сигналы в сетевую среду, данные посылаются центральному сетевому устройству (коммутатору),

затем коммутатору переправляет их устройству в соответствии с адресом, содержащимся в данных.

Преимуществом топологии звезда:

- простота обслуживания: единственной областью концентрации является центр сети.
- топология позволяет легко диагностировать проблемы и изменять схему прокладки.

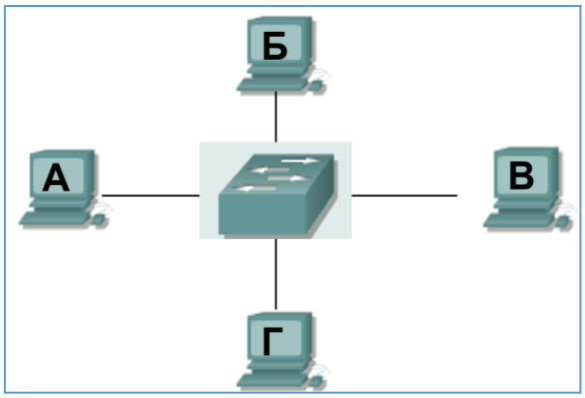


Рис 4. Топология звезда

- к сети, использующей звездообразная топология легко добавлять рабочие станции.
- если выходит из строя один из участков, то теряет связь только устройство, подключенное к этой точке, остальная часть сети будет функционировать нормально.
- звездообразная топология считается надежной.

Главным недостатком такой топологии является выход из строя центрального сетевого устройства, в этом случае сеть становится не работоспособной.

Топология: *Кольцо*.

При такой топологии узлы сети образуют виртуальное кольцо (концы кабеля соединены друг с другом). Каждый узел сети соединен с двумя соседними. Кольцевая топология - кадр управления (supervisory frame) называемый также маркером (token) последовательно передается от станции к соседней. Станция, которая хочет получить доступ к среде передачи, должна ждать получения кадра, и только после этого может начать передачу данных). Преимуществом кольцевой топологии является ее высокая надежность (за счет избыточности), однако стоимость такой сети достаточно высока за счет расходов на адаптеры, кабели и дополнительные приспособления

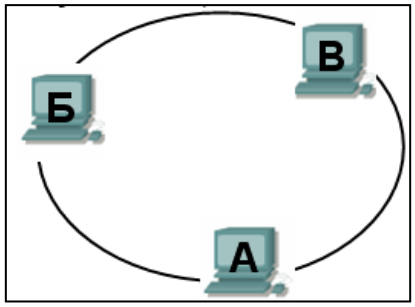


Рис 5. Топология кольцо

1. Иерархические топологии

Иерархия помогает нам осознавать взаимосвязь различных вещей, их функции и структуру. Это приносит упорядоченность и стройность в сложные модели мира. При разработке сетей иерархия способствует получению многих из тех преимуществ, которые

она позволяет получать в других областях жизни. Правильно использованная в процессе разработки сети, она делает сеть более предсказуемой. Она помогает определять и предвидеть, на каких уровнях иерархии следует выполнять определенные функции.

1.1. Преимущества иерархической топологии

Иерархия может быть применена к топологии сети многими способами. Среди прочих преимуществ иерархической топологии следует отметить улучшение следующих характеристик сетей:

- **Масштабируемости**
- **Управляемости**
- **Производительности**
- **Стоимости**

Рассмотрим каждую из этих характеристик более подробно.

1.1.1. Масштабируемость

Иерархические сети, состоят из множества отдельных модулей, каждый из которых занимает определенное место внутри иерархии. Поскольку такие сети имеют модульную структуру, их расширение обычно сводится к простому добавлению новых модулей в общий сетевой комплекс.

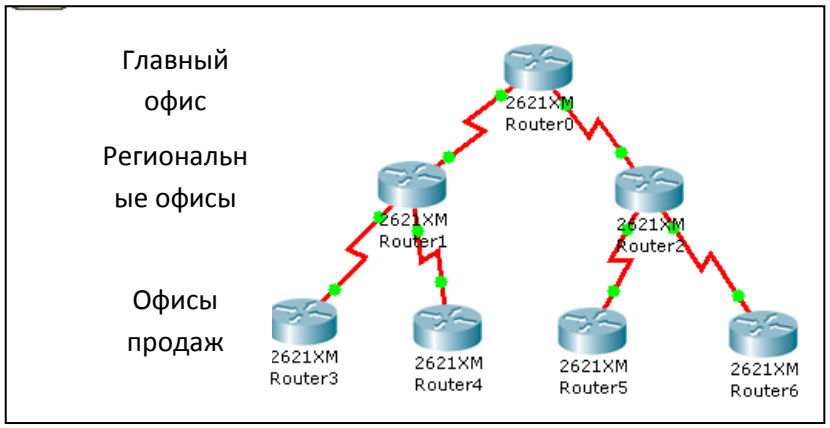


Рис 6. Пример иерархической сети

Рассмотрим сеть, изображенную на рисунке 6. Этот пример состоит из одного главного офиса, двух региональных офисов и четырех офисов продаж. Обратите внимание, что эта структура является иерархической. В данной сети два офиса продаж и вышестоящий региональный офис образуют единую иерархическую сеть.

Предположим теперь, что эта компания расширяется до размеров, соответствующих сети, изображенной на рисунке 7. В ней добавлены один региональный офис и пять офисов продаж. Обратите внимание, что мы почти удвоили размер сети, не внося существенных изменений в ее топологию. Поскольку иерархия по своей природе имеет модульную структуру, мы просто добавили несколько дополнительных модулей (маршрутизаторов) к существующей иерархии вполне предсказуемым образом. В этом случае нет необходимости перестраивать всю сеть, а ее расширение оказывается управляемым и эффективным, а не тягостным и мучительным процессом.

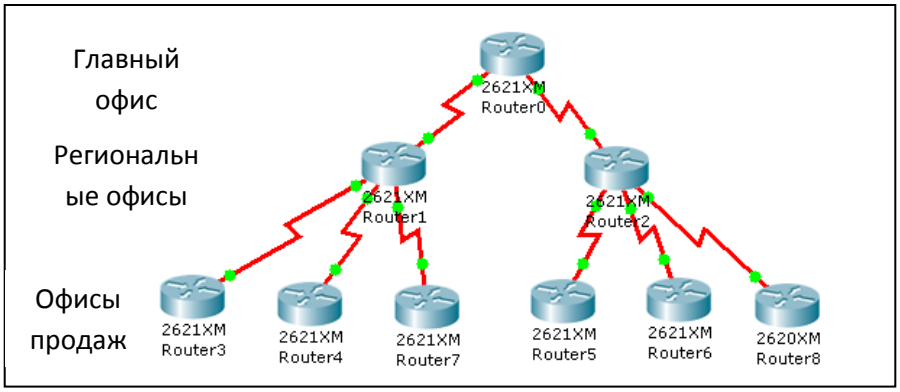


Рис 7. Пример иерархической сети после расширения

1.1.2. Управляемость

Иерархическими сетями проще управлять, нежели сетями других типов, поскольку в них легче находить и устранять неисправности. С чего следует начать поиск неисправностей, если сеть прекратила работу (предположим, что у вас отсутствуют мощные диагностические инструменты),- настоящая загадка. Конечно, для прокладки сети l0BaseT вам потребуется большее количество кабеля, однако дополнительные затраты почти всегда окупятся, поскольку поиск неисправностей в сети с топологией звезды оказывается намного проще, чем в сети с шинной топологией. Иерархические сети имеют аналогичные преимущества при поиске неисправностей. В иерархической структуре гораздо проще локализовать проблему, нежели в других моделях, таких, например, как сети с резервными соединениями. Рассмотрим пример, изображенный на рисунке 7. Когда какое-либо соединение в глобальной сети оказывается неисправным, местонахождение неисправности легко определяется с помощью нескольких эхо-запросов (пакетов Ping). Проблемы перегрузки тоже проще локализовывать и разрешать при такой структуре, нежели при какой-либо другой.

1.1.3. Производительность

Увеличение производительности — одно из достоинств иерархической структуры. Сети, имеющие иерархическую структуру, обладают тем преимуществом, что в них могут

использоваться наиболее современные способы маршрутизации, такие, например, как объединение маршрутов, в результате чего в больших сетях уменьшается размер таблиц маршрутизации и ускоряется оповещение. У сетей с резервными соединениями больше размеры таблиц маршрутизации и большее время оповещения по причине наличия большего количества возможных маршрутов.

1.1.4. Стоимость

Определяющим мотивом при построении сетей являются финансовые затраты. Иерархическим сетям обычно требуются меньшие трудозатраты администратора на сопровождение, и они позволяют более полно использовать возможности аппаратных и других ресурсов. В таких сетях проще, чем в неиерархических, предвидеть будущие требования к аппаратному обеспечению (этот вопрос мы более детально рассмотрим в следующем разделе). Кроме всего прочего, появляется возможность приобретать пропускную способность глобальной сети, точно соответствующую потребностям, и оптимально распределять ее между уровнями иерархии.

1.2. Трехуровневая иерархическая модель

В тот самый момент, когда казалось уместным создать окончательный вариант новой модели компьютерного образования, поскольку, наконец, все выучили эталонную модель OSI (Open Systems Interconnection - взаимодействие открытых систем), компания Cisco создала свою собственную иерархическую модель, которую придется изучать с самого начала. Эта модель предназначена для того, чтобы помочь разработчику создавать масштабируемые, надежные, экономичные иерархические сетевые комплексы. Модель Cisco описывает три уровня иерархии, как показано на рисунке 8. Вот эти три уровня:

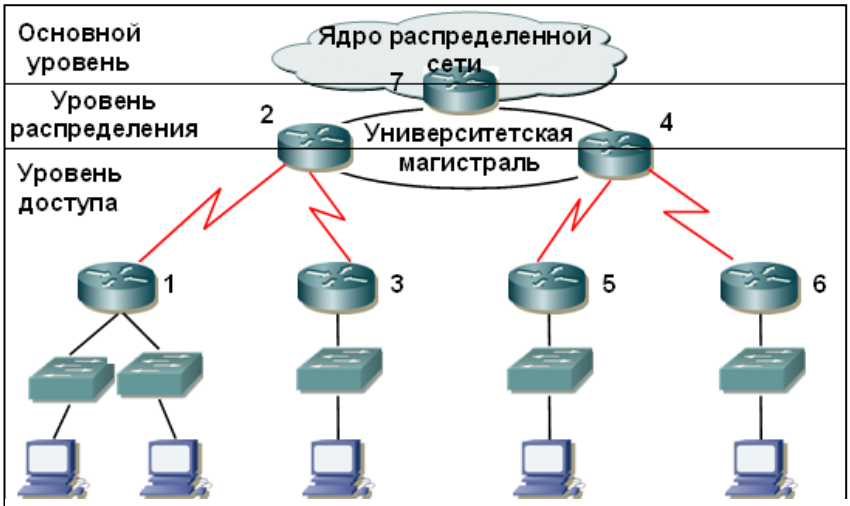


Рис 8. Иерархическая модель Cisco

- **Ядро**
- **Распределение**
- **Доступ**

Каждый уровень отвечает за выполнение своих конкретных задач. Это — логические уровни, и совсем необязательно они реализованы на физическом уровне. Три уровня не означают обязательного наличия трех отдельных устройств. В другой логической иерархии - модели OSI — семь уровней описывают выполняемые функции. Иногда протокол соответствует сразу нескольким уровням модели OSI, а иногда внутри одного уровня взаимодействуют несколько протоколов. Точно так же, когда мы создаем физические реализации иерархических сетей, у нас может оказаться несколько устройств на одном уровне, но с тем же успехом одно устройство может выполнять функции сразу на двух уровнях. Определение уровней - это логическое, а не физическое определение.

1.2.1. Уровень ядра

Уровень ядра в буквальном смысле является сердцем всей сети. Располагаясь на самой вершине иерархии, уровень ядра отвечает за быструю и надежную передачу больших объемов трафика. Единственной задачей уровня ядра является максимально быстрая передача трафика. Трафик, передаваемый через ядро, является общедоступным для большинства пользователей. Однако необходимо запомнить, что данные пользователей обрабатываются на уровне распределения, а уровень распределения отправляет запросы ядру только по мере необходимости.

Любой отказ на уровне ядра может отразиться на всех без исключения пользователях. Из этого следует, что проблема отказоустойчивости для этого уровня является очень важной. Через ядро, будут проходить большие объемы трафика, поэтому скорость и величина задержки являются определяющими. Поняв функции ядра, мы можем теперь рассмотреть некоторые особенности его создания. На уровне ядра нежелательно реализовывать:

- Не следует делать ничего такого, что замедляло бы обработку трафика. Сюда входит использование списков доступа, маршрутизация между виртуальными локальными сетями (VLAN) и фильтрация пакетов.
- На этом уровне не следует поддерживать доступ для рабочих групп.
- Следует избегать расширения ядра при увеличении размера сети (например, добавляя новые маршрутизаторы). Если производительность ядра начинает становиться проблемой, имеет смысл установить более мощные компоненты, не увеличивая их количество.

Теперь перечислим обязательные требования при разработке ядра (т.е. то, что необходимо делать всегда):

- Ядро должно обеспечивать максимально высокий уровень надежности. Следует выбирать технологии канального уровня, ориентированные на высокую скорость при наличии резервных каналов — как, например, FDDI, Fast Ethernet (с резервными соединениями) или даже ATM.
- При разработке не забывать о скорости. У ядра должна быть минимально возможная задержка.
- Следует выбирать протоколы с малым временем оповещения. Наличие быстрых соединений на канальном уровне и резервирование соединений ничем не поможет, если таблицы маршрутизации давно устарели.

1.2.2. Уровень распределения

Уровень распределения, который иногда называют уровнем рабочих групп,- это уровень, обеспечивающий взаимодействие между уровнем доступа и уровнем ядра. Первостепенными функциями уровня распределения является обеспечение маршрутизации, фильтрации и доступа к глобальной сети, а также определение того, каким образом пакет может получить доступ к ядру при возникновении такой необходимости. Уровень распределения должен определять наиболее быстрый маршрут для пользовательских запросов, например, маршрут, который должен использоваться пакетом запроса файла при его отправке на сервер. После того как уровень распределения выберет наилучший маршрут, он отправляет запрос на уровень ядра. Теперь уже уровень ядра ответственен за быструю пересылку запроса соответствующей службе.

Уровень распределения — это место, где должны применяться сетевые политики. Именно здесь имеется возможность использовать значительную гибкость при определении работы сети. На уровне распределения как правило реализовывается:

- Реализация инструментов, таких, как списки доступа, фильтрация пакетов и организация очередей.
- Обеспечение безопасности и реализация правил работы сети, включая преобразование адресов и межсетевые экраны (брандмауэры).
- Рассылка таблиц протоколов маршрутизации, включая статическую маршрутизацию.
- Выполнение маршрутизации между виртуальными локальными сетями и другие функции поддержки рабочих групп.
- Определение областей групповой и широковещательной рассылок.

Единственное, чего следует избегать на уровне распределения,- это выполнения функций, которые должны быть присущи исключительно одному из двух других уровней.

1.2.3. Уровень доступа

Уровень доступа осуществляет контроль за доступом пользователей и рабочих групп к сетевому комплексу. Уровень доступа иногда называется уровнем настольных систем. Сетевые ресурсы, которые требуются большинству пользователей, могут быть выделены локально. Любые обращения к удаленным службам осуществляются на уровне распределения. Функции, которые должны быть представлены на этом уровне, включают в себя:

- Сохранение преемственности (от уровня распределения) управления доступом и политик
- Создание отдельных коллизионных доменов (сегментация)
- Обеспечение взаимодействия рабочих групп с уровнем распределения

На уровне доступа могут использоваться такие технологии, как коммутация DDR (Dial-on-Demand Routing - маршрутизация с вызовом по мере необходимости) и Ethernet (хотя DDR обычно относится к уровню распределения). Статическая маршрутизация (заменяющая протоколы динамической маршрутизации) также располагается именно на этом уровне.

Не следует добавлять новые маршрутизаторы ниже уровня доступа. Такие действия приводят к увеличению диаметра сети, что нарушит предсказуемость топологии. Если возникает необходимость в подключении новых маршрутизаторов для обеспечения работы дополнительных рабочих групп,

2. Сегментация локальных сетей

Разработчики локальных сетей часто сталкиваются лицом к лицу с необходимостью увеличения протяженности сети, количества пользователей или пропускной способности, доступной для потребителей. С корпоративной точки зрения все перечисленные выше изменения являются необходимыми, т.к. указывают на рост и развитие корпорации.

Если на текущий момент пользователи подключены к сети, основанной на устаревшей технологии со скоростью передачи 10 Мбит/с, то можно использовать технологию Fast Ethernet и сразу же получить десятикратное улучшение пропускной способности. Изменение сетевой инфраструктуры в данном случае состоит в замене плат сетевых адаптеров рабочих станций на новые, которые поддерживают скорость обмена 100 Мбит/с. Такая модернизация повлечет за собой замену концентраторов, к которым подключены рабочие станции. Новые концентраторы также должны поддерживать сети с новой пропускной способностью. Однако, даже в таком минимальном объеме полная модернизация может стоить чрезмерно много.

Сегментация локальной сети — еще один подход к обеспечению пользователей дополнительной пропускной способностью без полной замены всего телекоммуникационного оборудования. Выполняя сегментацию, администратор разбивает сеть на более мелкие части и соединяет их с помощью оборудования для межсетевого обмена. На рис. 9 показаны варианты сети до и после сегментации.

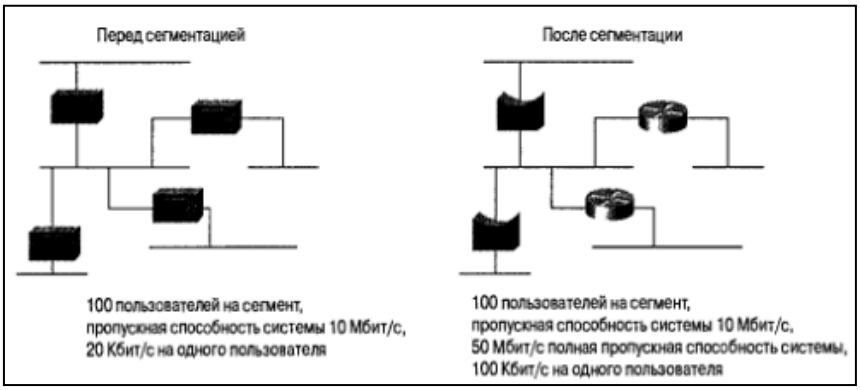


Рис 9. Сеть до и после сегментации

До проведения сегментации все 500 пользователей совместно использовали сеть с пропускной способностью 10 Мбит/с, поскольку сегменты были соединены с помощью повторителей. После сегментации сети повторители были заменены на мосты и маршрутизаторы, которые позволяют изолировать разные части друг от друга и обеспечить пользователей большей пропускной способностью. Коммутаторы и маршрутизаторы позволяют получить дополнительную пропускную способность благодаря ограничению доменов коллизий и широковещательных доменов, как показано в табл.1.

Устройство	Количество доменов коллизий	Количество широковещательных доменов
Маршрутизатор	Много	Много
Коммутатор	много	Может быть сконфигурировано

Каждый сегмент, в свою очередь, может быть разделен на более мелкие части с помощью мостов, маршрутизаторов и коммутаторов, и тем самым может быть получена большая пропускная способность для каждого отдельного пользователя. Уменьшение числа пользователей в каждом сегменте приводит к увеличению полезной пропускной способности для одного пользователя. В крайнем случае, когда в сегменте находится всего один пользователь, он получает полную пропускную способность среды передачи. Именно такой вариант соответствует ситуации, когда администратор использует только коммутаторы для построения сети.

Однако, остается нерешенным вопрос: "Что необходимо использовать для сегментации сети: маршрутизатор или сетевой коммутатор?" В следующих разделах приводится описание различных вариантов сетей.

2.1. Сегментация локальных сетей с помощью коммутаторов

Технологии Ethernet ограничивают максимальную длину сегмента и количество станций, подключенных к одному сегменту кабеля. Что же делать, если нужно получить большую длину сегмента или добавить больше устройств в сегмент? Необходимое решение может быть реализовано на основе коммутаторов. В коммутаторах используется фильтрация для того, чтобы определить, следует или не следует отправлять фрейм в другие интерфейсы.

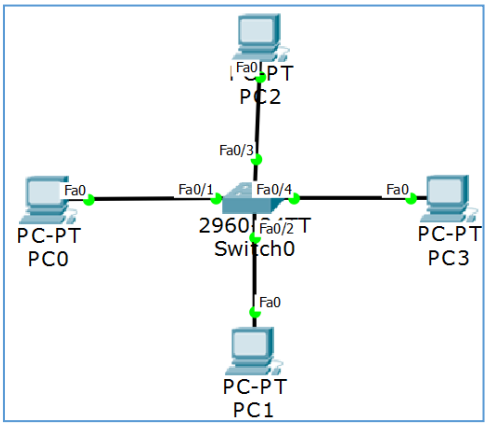


Рис 10. Объединение сегментов с помощью коммутатора

Коммутатор работает на уровне 2 модели OSI — канальном. Работа на данном уровне означает, что мост имеет доступ к заголовку фрейма, который содержит информацию о MAC-адресах. Таким образом, сетевые устройства принимают решение о пересылке фреймов по информации, которая находится в заголовках фреймов, содержащих MAC-адреса.

Коммутаторы фильтруют фреймы, отправитель и получатель которых находятся в одном сегменте. Исключением являются широковещательные фреймы и фреймы групповой рассылки. При получении широковещательного сообщения коммутатор передает фрейм во все интерфейсы. Рассмотрим для примера запросы протокола ARP, как и для сетей с повторителями. Станция-отправитель обменивается сообщениями с другой станцией, работающей по протоколу IP и находящейся в той же сети, посылает широковещательный ARP-запрос. Запрос передается в широковещательном фрейме и, следовательно, передается через все коммутаторы и все интерфейсы. Все сегменты, подключенные к коммутатору, принадлежат к одному широковещательному домену. Т.к. все станции принадлежат одному широковещательному домену, то, следовательно, они должны также принадлежать одной IP-подсети.

2.2. Сегментация локальных сетей с помощью маршрутизаторов

Маршрутизаторы работают на третьем уровне модели OSI, дают возможность расширить сеть и позволяют создавать домены коллизий и широковещательные домены. Маршрутизаторы предотвращают распространение широковещательных сообщений в сети. Подобная изоляция широковещательных запросов создает отдельные широковещательные домены, чего нельзя осуществить с помощью коммутаторов. Блокировка распространения широковещательных сообщений маршрутизаторами определяет границы широковещательного домена — области, за пределы которой не выходят широковещательные сообщения, которые распространяются в сети. На рисунке 11 показана сеть, построенная на основе маршрутизаторов, и показаны границы доменов коллизий и широковещательных доменов.

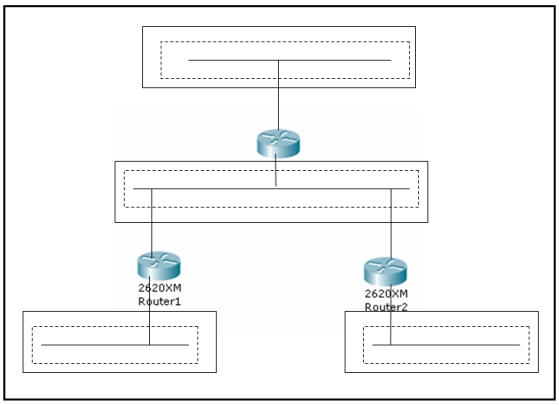


Рис 11. Домены коллизий и широковещательные домены в сети с маршрутизаторами

2.3. Три функции коммутации уровня 2

Во время переключения на уровне 2 выполняются три основные функции коммутации:

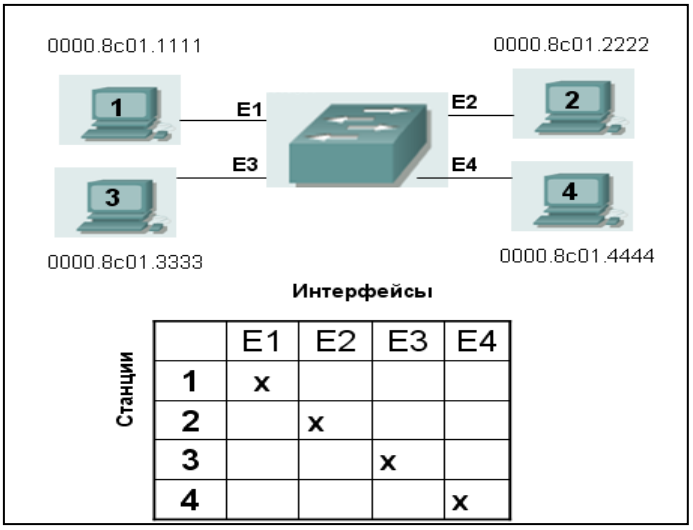
- Изучение адресов коммутаторы уровня 2 и мосты запоминают аппаратный адрес источника из каждого полученного интерфейсом кадра и хранят эту информацию в своей базе данных MAC-адресов.

- Решение о пересылке или фильтрации. Когда интерфейс получает кадр, коммутатор анализирует аппаратный адрес назначения и ищет в своей базе данных MAC-адресов нужный интерфейс.
- Исключение зацикливания. Если между коммутаторами для избыточности создано несколько путей, то могут появиться зацикленные пути передачи информации. Протокол STP позволяет исключить зацикливание пакетов в сети при сохранении избыточности.

2.4.1. Изучение адресов

После включения питания коммутаторя его таблица фильтрации MAC-адресов пуста. Когда устройство передает, а интерфейс получает кадр, переключатель помещает адрес источника в таблицу фильтрации MAC-адресов вместе с интерфейсом устройства. Коммутатор не делает самостоятельных решений о перенаправлении кадров, поскольку не знает о местонахождении устройства назначения.

Если устройство отвечает и посылает кадр обратно, то коммутатор извлекает адрес источника из возвращенного кадра и помещает MAC-адрес в свою базу данных, причем связывает этот адрес с интерфейсом, получившим кадр. Теперь коммутатор имеет в таблице фильтрации два MAC-адреса и может установить соединение "точка-точка", а кадры будут перемещаться только между двумя известными коммутатору устройствами. Именно поэтому коммутатор на уровне 2 работает эффективнее концентратора.



	E1	E2	E3	E4
1	x			
2		x		
3			x	
4				x

Рис 12. Изучение адресов

На рисунке показаны четыре подключенные к коммутатору хоста.

После включения питания коммутатора, его таблица MAC-адресов пуста.

1. Хост 1 посылает кадр хосту 3. MAC-адрес первого хоста равен 0000.8c01.1111, а MAC-адрес третьего хоста равен 0000.8c01.2222.

2. коммутатора принимает кадр в интерфейсе EO/1 и помещает в таблицу MAC-адресов адрес источника.

3. В базе данных MAC-адресов еще нет адреса назначения, поэтому кадр передается во все интерфейсы.

4. Хост 3 получает кадр и откликается на вызов хоста 1. Коммутатор принимает этот ответный кадр в интерфейсе E2 и помещает аппаратный адрес источника второго кадра в базу данных MAC-адресов.

5. Хосты 1 и 3 могут установить соединение "точка-точка", причем кадры будут пересылаться только между этими двумя устройствами. Хосты 2 и 4 не будут "видеть" подобные кадры.

Если в течение определенного времени два устройства не будут откликаться во время передачи кадров через переключатель, то переключатель очистит соответствующие записи в своей базе данных, чтобы поддержать корректность таблицы адресов.

2.4.2. Решение о фильтрации

Когда кадр попадает в интерфейс коммутатора, аппаратный адрес назначения сравнивается с базой данных перенаправления/фильтрации MAC-адресов. Если аппаратный адрес назначения известен и присутствует в базе данных, то кадр направляется только в один выходной интерфейс, предписанный в таблице базы данных. Коммутатор не транслирует кадр во все остальные интерфейсы, за исключением интерфейса, ведущего к точке назначения. Это сохраняет полосу пропускания в других сетевых сегментах, а сам процесс называется фшътрацией кадров (frame filtering).

Если же аппаратный адрес назначения не указан в базе данных MAC-адресов, то кадр отсылается в широковещательной рассылке по всем активным интерфейсам, за исключением интерфейса, в котором этот кадр был получен. Если одно из устройств откликается на широковещательную рассылку, происходит обновление базы данных MAC-адресов за счет добавления местоположения устройства (интерфейса).

3. Виртуальные локальные сети

В коммутируемых сетях уровня 2 сеть представляется "плоской". Любой широковещательный пакет пересылается всем устройствам, вне зависимости от того, нужно ли устройству принимать эти данные.

Поскольку коммутация на уровне 2 формирует отдельные домены конфликтов для каждого подключенного к переключателю устройства, снижаются ограничения на длину сегмента Ethernet, т.е. можно строить более крупные сети. Увеличение количества пользователей и устройств приводит к увеличению количества широковещательных рассылок и пакетов, обрабатываемых каждым устройством.

Еще одной проблемой "плоской" коммутации уровня 2 является безопасность сети. Нельзя отменить широковещательные рассылки в устройстве и ответы пользователей на эти рассылки. Увеличить уровень безопасности позволяет защита паролями серверов и других устройств. Создание виртуальной локальной сети VLAN помогает решить многие проблемы коммутации уровня 2, что и будет показано ниже.

Виртуальная локальная сеть представляет собой логическое объединение устройств или пользователей Объединение их в группу может производиться по выполняемым функциям, используемым приложениям, по отделам и т.д., независимо от их физического расположения в сегментах (segment). Конфигурирование виртуальной сети производится на коммутаторе программным путем. Виртуальные сети не стандартизированы и требуют использования программного обеспечения от производителя коммутатора.

3.1. Виртуальные сети и физические границы

В локальных сетях, содержащих коммутирующие устройства, использование технологии виртуальных сетей представляет собой эффективный и экономически выгодный способ объединения пользователей сети в рабочие группы независимо от их физического расположения. Сегментация в виртуальной сети и в обычной локальной сети различаются по следующим параметрам:

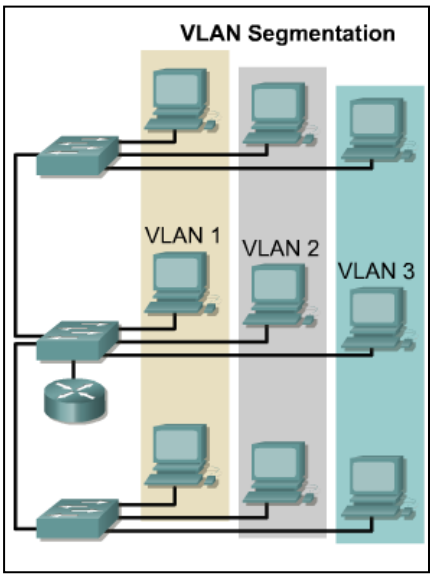


Рис 13. Виртуальные сети и физические границы

- Виртуальные сети работают на 2-м и 3-м уровнях эталонной модели OSI.
- □ Обмен информацией между виртуальными сетями

обеспечивается маршрутизацией 3-го уровня.

- Виртуальная сеть предоставляет средство управления широковещанием.
- Включение пользователей в виртуальную сеть производится сетевым администратором.
- VLAN позволяет повысить степень защиты сети путем задания сетевых узлов, которым разрешено обмениваться информацией друг с другом.

Использование технологии виртуальных сетей позволяет сгруппировать порты коммутатора и подсоединенные к ним компьютеры в логически определенные рабочие группы следующих типов.

- Сотрудники одного отдела.
- Группа сотрудников с пересекающимися функциями.
- Различные группы пользователей, совместно использующих приложения или программное обеспечение.

Можно сгруппировать порты и пользователей в рабочую группу на одном коммутаторе или на нескольких соединенных между собой коммутаторах. Группируя порты и пользователей вокруг нескольких коммутаторов, можно создать инфраструктуру сети в одном здании, в нескольких соединенных между собой зданиях или даже сеть большой области, как показано на рис.

3.2. Доказательство необходимости применения сетей VLAN

В обычных сетях сетевые администраторы подключали пользователей к сети по географическому принципу. Администратор подключал рабочую станцию пользователя с помощью ближайшего к ней сетевого кабеля. Если пользователь является сотрудником технического отдела и при этом его рабочее место находится рядом с кем-либо, кто работает в бухгалтерии, то они оба будут подключены к одной локальной сети, т.к. они подключаются с помощью одного кабеля. Такой подход создает некоторые интересные сетевые проблемы. Четкое понимание возникающих при такой структуре сети проблем и подчеркивает причины использования сетей VLAN.

3.2.1. Проблема 1: безопасность в сети

Первая причина напрямую связана с тем, что сети старого типа по своей природе рассчитаны на физическую среду общего доступа. Когда станция, находящаяся в сети устаревшего типа с совместно используемой физической средой передачи, как, например, сеть технологии l0BaseT, работающая в полудуплексном режиме, передает данные, то все станции, подключенные к сегменту, получают копию фрейма, даже если он адресован не

им. Такая ситуация, конечно, не мешает функционированию сети, однако, позволяет использовать множество программных пакетов для мониторинга сетевого трафика, которые широко доступны и работают на различных типах рабочих станций. Каждый, у кого есть подобное программное обеспечение, может перехватывать пароли, секретные (или обидные) сообщения электронной почты и любой другой тип сетевого трафика.

Если пользователи, подключенные к сети, являются сотрудниками одного отдела, то крупных катастроф, скорее всего, не случится, однако, если к общему сегменту имеют доступ, пользователи из различных отделов, то могут возникать нежелательные перехваты информации. Если кто-либо из персонала начнет отправлять секретные данные, такие, как информация о зарплатах, фондах, о состоянии здоровья по сети общего доступа, то кто угодно, имея программное обеспечение для мониторинга сети, сможет получить указанную информацию.

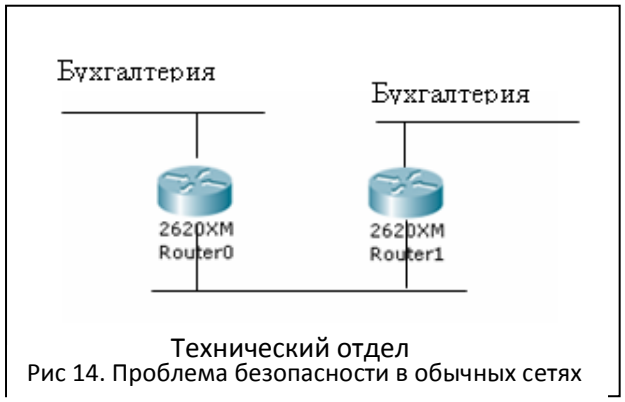


Рис 14. Проблема безопасности в обычных сетях

Возможность выполнить описанные выше действия не ограничивается одним сегментом сети. Такие же проблемы могут возникать и в сетях, где множество сегментов объединяются с помощью маршрутизаторов. В сети, показанной на рисунке 14, бухгалтерский отдел подключен к двум изолированным сегментам. Для того, чтобы пользователи из одного сегмента могли передавать данные пользователям на другом сегменте, фреймы должны пройти через сеть технического отдела. При прохождении фреймов через сегмент сети технического отдела они могут быть перехвачены, а информация использована в корыстных целях.

Один из методов организации сети, который позволяет избежать данной проблемы, — это переместить всех пользователей бухгалтерского отдела в один сегмент. Такой подход не всегда возможен, поскольку могут существовать пространственные ограничения, которые не позволяют разместить весь бухгалтерский отдел в одном здании. Еще одна причина может быть вызвана ограничением на географическое расположение различных частей бухгалтерского отдела. Пользователи одной части сегмента сети могут находиться на значительном расстоянии от пользователей другой части сегмента. Перемещение пользователей в одно и то же место может означать переезд офиса из одного города в другой.

Еще один путь — это заменить бухгалтерию маркетинговым отделом. Действительно, кому интересно перехватывать данные маркетингового отдела, кроме ситуации, когда

хочется хорошо посмеяться? Бухгалтерия же не имеет права распространять информацию о платежных чеках или данных, которые касаются торговли и других попыток заработать деньги. Ясно, что такое решение не является приемлемым.

Третий подход связан с применением виртуальных локальных сетей. Сети VLAN позволяют поместить всех пользователей, объединенных по определенному роду деятельности, в один широковещательный домен, и изолировать их от пользователей других широковещательных доменов. Всех пользователей, работающих в бухгалтерии, можно объединить в одну сеть VLAN, независимо от их местонахождения в здании. При этом больше нет необходимости подключать пользователей к сетям в соответствии с их местоположением. Пользователи могут входить в сети VLAN в соответствии с их функциональными обязанностями. Таким образом, пользователей бухгалтерского отдела можно включить в одну сеть VLAN, пользователей маркетингового отдела — в другую сеть VLAN, а пользователей технического отдела — в третью.

При создании сетей VLAN с помощью коммутирующего сетевого устройства создается еще один дополнительный уровень защиты. Коммутаторы передают сетевой трафик так же, как это делают мосты, только в пределах одной сети VLAN. Когда сетевая станция передает данные, то фреймы определяются к необходимому получателю. Если фреймы являются одноадресными фреймами, порты назначения которых известны, то коммутаторы не распространяют их всем пользователям, подключенным к сети VLAN (см. рис. 15).

Станция А, показанная на рисунке 15, передает фрейм станции Б, которая подключена к другому коммутатору Catalyst. Хотя фрейм проходит через несколько коммутаторов Catalyst, только станция-получатель получает копию фрейма. Коммутатор выполняет фильтрацию фреймов, которые передаются от других станций в зависимости от того, принадлежат ли они одной сети VLAN или различным сетям VLAN. Такая функция

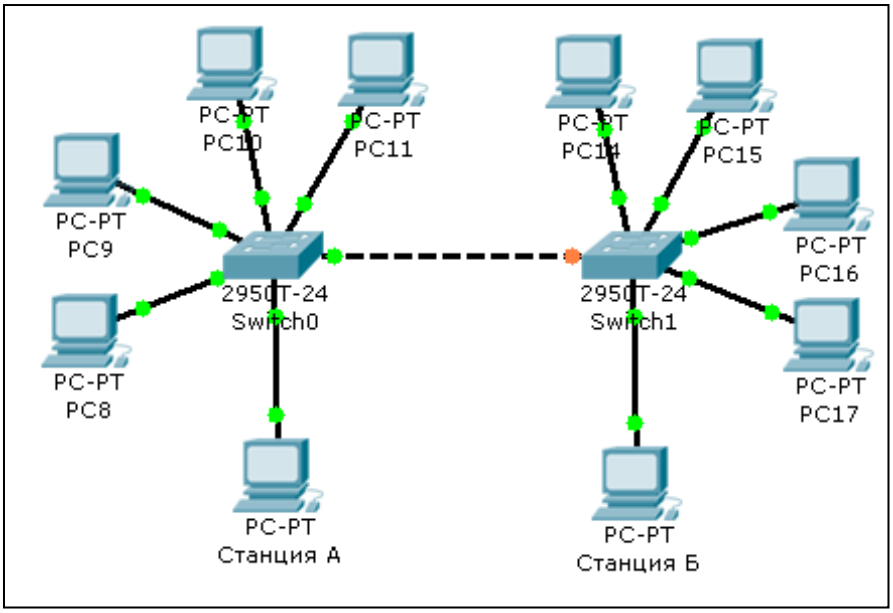


Рис 15. Распространение известных одноадресатных фреймов в коммутируемой сети

коммутатора ограничивает возможность беспорядочно захватывать трафик, повышая тем самым эффективность защиты сетей. Какой трафик все еще можно будет захватывать? Любой, который распространяется в сети VLAN с помощью процесса лавинной передачи. Трафик, который передается с помощью метода лавинной передачи, включает широковещательные сообщения, многоадресатные (multicast) сообщения и неизвестные одноадресатные фреймы.

3.2.2. Проблема 2: распространение широковещательных сообщений

К сожалению, многие (если не все) протоколы создают трафик широковещательных сообщений. Одни протоколы создают больше широковещательного трафика, другие — меньше. Широковещательные сообщения доставляются всем устройствам сети и должны обрабатываться всеми принимающими устройствами. Другие протоколы также вносят свою долю в служебные потоки данных. Например, протокол NetBEUI создает много широковещательных фреймов даже в случае малой активности рабочих станций. Станции, работающие по протоколу TCP/IP, используют широковещательные сообщения для обновлений таблиц маршрутизации, сообщений протокола ARP и других целей.

В дополнение к сказанному многие мультимедийные приложения также создают широковещательные и многоадресатные фреймы, которые распространяются в пределах широковещательного домена.

Чем же плохи широковещательные сообщения? Они служат для выполнения основных функций различных протоколов и поэтому их необходимо отнести к накладным расходам. Широковещательные сообщения редко используются для передачи данных пользователей (исключением являются мультимедийные приложения). Они не переносят данные пользователей, однако занимают пропускную способность сети, что, соответственно, сокращает доступную пропускную способность для передачи полезных данных.

Широковещательные сообщения влияют на производительность рабочих станций. Любые широковещательные сообщения принимаются рабочими станциями, при этом происходит прерывание работы процессоров, в результате чего выполнение пользовательских приложений приостанавливается. При увеличении числа широковещательных фреймов, проходящих через интерфейс в течение одной секунды, эффективность использования процессора (CPU) уменьшается. Практически уровень потери эффективности зависит от приложений, выполняющихся на рабочих станциях, от типа сетевой платы и версий драйверов, от типа операционной системы и аппаратной платформы рабочих станций.

Если проблемой сети является большое количество широковещательных сообщений, то ее можно ослабить путем создания более мелких широковещательных доменов. При использовании сетей VLAN необходимо создание большего количества сетей VLAN и уменьшение количества устройств, подключенных к каждой виртуальной локальной сети. Эффективность такой процедуры зависит от природы широковещательных сообщений. Если широковещательные запросы приходят только от одного сервера, то, возможно, достаточно просто изолировать сервер в другом широковещательном домене. Если широковещательные запросы приходят от различных станций, то создание нескольких доменов может привести к сокращению числа широковещательных фреймов в каждом из них.

3.2.3. Проблема 3: использование пропускной способности

Когда пользователи подключены к одному сегменту, они совместно используют пропускную способность такого сегмента. Чем больше пользователей подключено к сегменту кабеля общего доступа, тем меньше среднее значение пропускной способности, отведенное каждому пользователю. Если степень совместного использования сети становится очень большой, то пользовательские приложения начинают "голодать". Администраторам тоже приходится несладко, потому что пользователи начинают надоедать относительно пропускной способности. Сети VLAN, которые могут быть созданы с помощью коммутирующего коммуникационного оборудования, позволяют выделять пользователям большую пропускную способность, чем это возможно в сетях устаревших типов с совместным доступом к физической среде передачи.

Каждый порт коммутатора Catalyst работает так же, как и порт обычного моста. Мосты фильтруют трафик, если нет необходимости отправлять его в сегменты, отличные от сегмента, к которому подключен отправитель.

В большинстве обычных ситуаций каждая станция принимает трафик, предназначенный только ей. Коммутатор фильтрует большую часть остального фонового трафика в сети. Такая ситуация позволяет каждой станции получать полную выделенную пропускную способность для приема и передачи интересующих

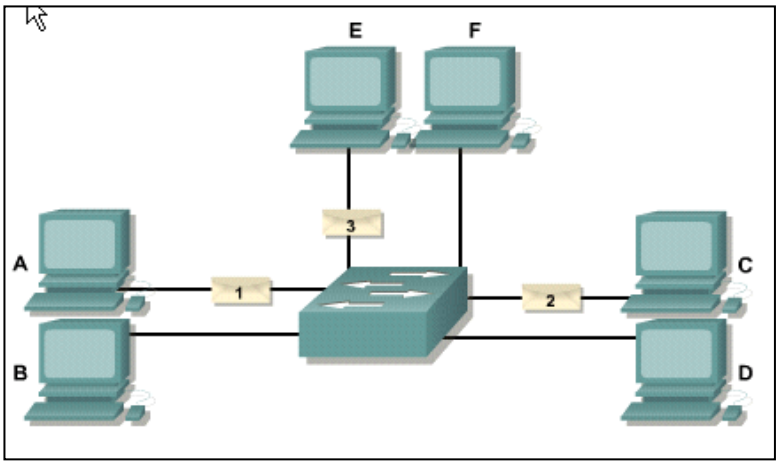


Рис 16. Параллельная передача данных коммутатором Catalyst

пользователя фреймов. В отличие от сети с концентратором разделяемого доступа, в которой только одна станция может передавать в любой момент времени, в коммутируемой сети, показанной на рисунке 16, разрешается выполнение параллельных сеансов передачи данных в пределах одного широковещательного домена, которые происходят без влияния одной станции на другую, как в случае принадлежности станций разным широковещательным доменам, так и в случае принадлежности одному широковещательному домену. Пары станций A/F, C/B и D/E могут обмениваться друг с другом информацией без какого-либо побочного воздействия на другие взаимодействующие станции.

3.2.4. Проблема 4: задержки при передаче данных через маршрутизаторы

В сетях старого типа, как показано на рисунке 14, пользователи бухгалтерского отдела вынуждены передавать данные друг другу через сегмент технического отдела. При этом фреймы должны пройти через маршрутизаторы. Старые маршрутизаторы, которые осуществляли маршрутизацию с помощью программного обеспечения, обычно были более медленными, чем другие типы коммуникационного оборудования, как, например, коммутаторы и мосты второго уровня. При прохождении фрейма через маршрутизатор он вносит некоторую задержку — время, которое необходимо затратить на передачу фрейма из входного (ingress) порта в выходной (egress) порт. Каждый маршрутизатор, через который проходит фрейм, увеличивает суммарную задержку передачи. Кроме того, каждый перегруженный сетевой сегмент, по которому должен пройти фрейм, также увеличивает задержку передачи. Перемещение пользователей бухгалтерского отдела в одну сеть VLAN устраняет необходимость прохода пакетов через несколько сегментов и маршрутизаторов. Сокращение времени задержки описанным способом позволяет увеличить производительность системы для пользователей, особенно, если они используют протоколы с отправкой подтверждений (send-acknowlegde). Протоколы с отправкой подтверждений не отправляют больших порций данных до того времени, пока не будет получено подтверждение о приеме предыдущей порции данных. Задержки передачи существенно снижают пропускную способность канала при использовании таких протоколов. Если есть возможность исключить прохождение пользовательского трафика через маршрутизаторы путем подключения пользователей к одной сети VLAN, то таким образом можно исключить общую задержку передачи данных через маршрутизаторы. Если фреймы должны передаваться через маршрутизаторы, то использование коммутации третьего уровня также позволяет сократить задержку за счет использования маршрутизаторов.

Использование сетей VLAN позволяет уменьшить задержку передачи путем уменьшения загрузки сегмента. Следует ожидать значительного улучшения работы в случае, когда рабочие станции первоначально были подключены к перегруженному сегменту с разделяемой средой передачи данных, а затем каждая рабочая станция оказалась подключенной к выделенному порту коммутатора.

3.3. Статические сети VLAN

Статические сети VLAN являются типичным способом формирования таких сетей и отличаются высокой безопасностью. Присвоенные сети VLAN порты переключателей всегда сохраняют свое действие, пока администратор не выполнит новое присваивание портов. Этот тип VLAN легко конфигурировать и отслеживать, причем статические VLAN хорошо подходят для сетей, где контролируется перемещение пользователей.

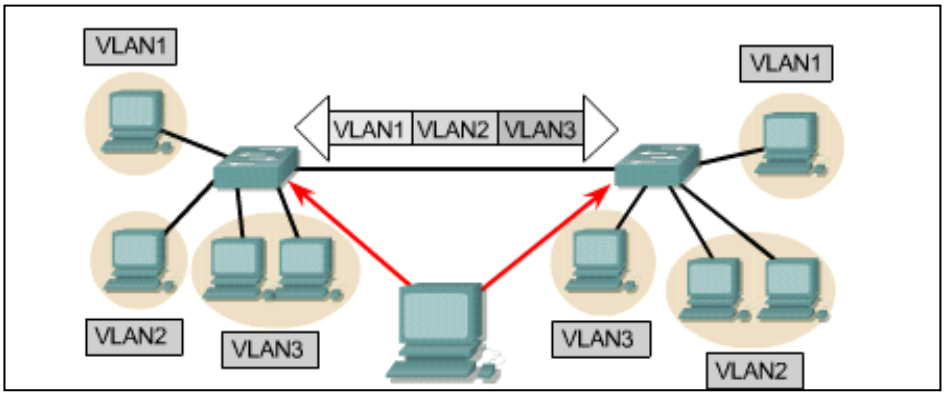


Рис 17. Статические сети VLAN

3.4. Идентификация сетей VLAN

Сеть VLAN может распространяться на несколько соединенных переключателей. Устройства в такой коммутационной фабрике отслеживает как сами кадры, так и их принадлежность определенной сети VLAN. Для этого выполняется маркирование кадров (frame tagging). Переключатели смогут направлять кадры в соответствующие порты. В такой среде коммутации существуют два разных типа связей:

- Связи доступа (Access link) Связи, принадлежащие только одной сети VLAN и считающиеся основной связью отдельного порта переключателя. Любое устройство, подключенное к связи доступа, не подозревает о своем членстве в сети VLAN. Это устройство считает себя частью широковещательного домена, но не подозревает о реальном членстве в физической сети. Переключатели удаляют всю информацию о VLAN еще до передачи кадра в связь доступа. Устройства на связях доступа не могут взаимодействовать с устройствами вне своей сети VLAN, если только пакеты не проходят через маршрутизатор.

- Магистральные связи (Trunk link) Магистральные линии способны обслуживать несколько сетей VLAN. В компьютерных сетях магистральные линии служат для связи переключателей с переключателями, маршрутизаторами и даже с серверами. В магистральных связях поддерживаются только протоколы Fast Ethernet или Gigabit Ethernet. Для идентификации в кадре принадлежности к определенной сети VLAN, построенной на технологии Ethernet, переключатель Cisco поддерживает две разные схемы идентификации: ISL и 802. lq. Магистральные связи служат для транспорта VLAN между устройствами и могут настраиваться на поддержку всех или только нескольких сетей VLAN. Магистральные связи сохраняют принадлежность к "родной" VLAN (т.е. виртуальной локальной сети по умолчанию), которая используется при отказе магистральной линии.

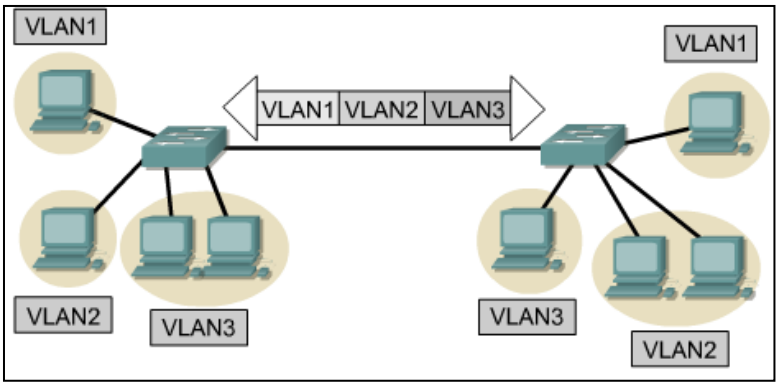


Рис 18. Маркировка кадров

3.5. Маркировка кадров

Коммутатору объединенной сети необходимо отслеживать пользователей и кадры, которые проходят через коммутационную фабрику и сеть VLAN. Коммутационной фабрикой называют группу коммутаторов, совместно использующих одинаковую информацию о сети VLAN. Идентификация (маркировка) кадров предполагает присваивание кадрам уникального идентификатора, определенного пользователем. Часто это называют присваиванием VLAN ID или присваиванием цвета. Компания Cisco разработала метод маркировки кадров, используемый для передачи кадров Ethernet по магистральным связям. Маркер (тег) сети VLAN удаляется перед выходом кадра из магистральной связи.

Любой получивший кадр коммутатор обязан идентифицировать VLAN ID, чтобы определить дальнейшие действия с кадром на основе таблицы фильтрации. Если кадр попадает в коммутатор, подключенный к другой магистральной связи, кадр направляется в порт этой магистральной линии. Когда кадр попадает в конец магистральной связи и

должен поступить в связь доступа, коммутатор удаляет идентификатор VLAN. Оконечное устройство получит кадр без какой-либо информации о сети VLAN.

3.6. Методы идентификации VLAN

Для отслеживания кадров, перемещающихся через коммутационную фабрику, используется идентификатор VLAN. Он отмечает принадлежность кадров определенной сети VLAN . Существует несколько методов отслеживания кадров в магистральных связях:

- Протокол ISL Протокол ISL (Inter-Switch Link — связи между переключателями) лицензирован для переключателей компании Cisco и используется только в линиях сетей FastEthernet и Gigabit Ethernet. Протокол может применяться к порту переключателя, интерфейсу маршрутизатора или интерфейсу сетевого адаптера на сервере, который является магистральным. Такой магистральный сервер пригоден для создания сетей VLAN, не нарушающих правила "80/20". Магистральный сервер одновременно является членом всех сетей VLAN (доменов широковещательных рассылок). Пользователям не нужно пересекать устройство уровня 3 для доступа к серверу, совместно используемому в организации.
- IEEE 802.1q Протокол создан институтом IEEE в качестве стандартного метода маркирования кадров. Протокол предполагает вставку в кадр дополнительного поля для идентификации VLAN. Для создания магистральной связи между коммутируемыми линиями Cisco и переключателем другого производителя придется использовать протокол 802.lq, который обеспечит работу магистральной связи. LANE

3.7. Достоинства виртуальных сетей

В качестве достоинств виртуальных сетей можно выделить следующие их особенности.

- Использование виртуальных сетей позволяет значительно экономить средства, затрачиваемые на решение вопросов, связанных с переездом в другое место, с появлением новых пользователей и с внесением изменений в структуру сети
- Виртуальные сети позволяют обеспечить контроль над широковещанием.
- Они позволяют обеспечить защиту информации в рабочих группах и во всей сети.
- Виртуальная сеть позволяет сэкономить средства за счет использования уже существующих концентраторов.

3.8. Добавление новых пользователей в виртуальную локальную сеть

Виртуальные сети представляют собой эффективный механизм управления этими изменениями и уменьшения расходов, связанных с установкой новой конфигурации концентраторов и маршрутизаторов Пользователи виртуальной локальной сети могут совместно использовать одно и то же сетевое адресное пространство (т е. IP-подсеть) независимо от их физического расположения. Если пользователь виртуальной сети переезжает из одного места в другое, оставаясь внутри той же самой виртуальной сети и оставаясь подключенным к тому же самому порту коммутатора, то его сетевой адрес не изменяется. Изменение положения пользователя требует всего лишь подключения его компьютера к одному из портов коммутатора и включения этого.

Конфигурация маршрутизаторов остается при этом неизменной; сам по себе переезд пользователя из одного места в другое, если пользователь остается в той же самой виртуальной сети, не требует изменения конфигурации маршрутизатора.

3.9. Управление широковещанием

Потоки широковещательных сообщений циркулируют в каждой сети. Частота появления широковещательных сообщений зависит от типа приложения, типа серверов, количества логических сегментов и характера их использования. Хотя многие приложения за последние годы были модифицированы таким образом, чтобы уменьшить число посылаемых ими широковещательных сообщений, разрабатываемые в настоящее время новые мультимедийные приложения интенсивно используют широковещание и множественную (групповую) адресацию (multicast).

Для предотвращения проблем, связанных с широковещанием, необходимо принимать превентивные меры. Одной из наиболее эффективных мер является сегментирование сети с помощью брандмауэров для того, чтобы в максимальной степени уменьшить влияние проблем, возникших в одном сегменте, на другие части сети. В этом случае, несмотря на наличие проблем широковещания в одном из сегментов, остальная часть сети оказывается защищенной брандмауэром, в качестве которого обычно используется маршрутизатор. Сегментация с помощью брандмауэров обеспечивает надежность и минимизирует поток широковещательных служебных сообщений, обеспечивая тем самым большую пропускную способность для потоков данных приложений.

Если между коммутаторами нет маршрутизаторов, то широковещательные сообщения (передачи 2-го уровня) передаются на все коммутируемые порты. Такую конфигурацию обычно называют плоской сетью (flat network); при этом вся сеть представляет собой один широковещательный домен. Преимущества плоской сети заключаются в небольшом времени ожидания и высокой производительности, а также в легкости администрирования. Недостатком такой сети является ее повышенная чувствительность к широковещательному потоку через коммутаторы, порты и магистральные каналы.

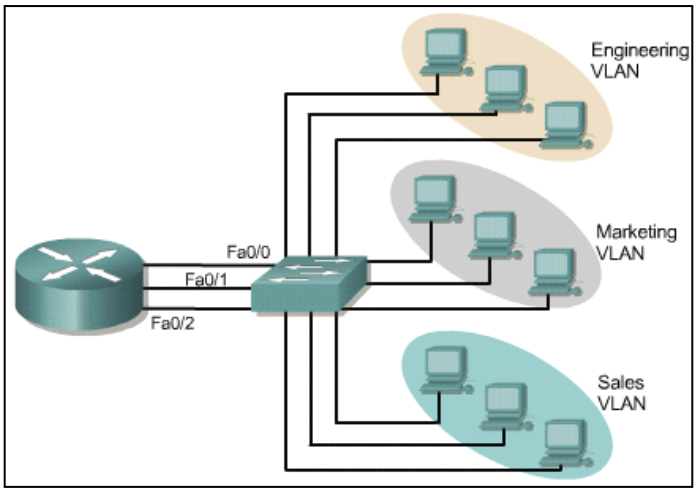


Рис 19. Управление широковещанием

Виртуальные сети представляют собой эффективный механизм расширения сферы действия брандмауэров (маршрутизаторов) на среду коммутации и защиты сети от потенциально опасных проблем широковещания. Кроме того, виртуальные сети сохраняют все преимущества, предоставляемые коммутацией.

Брандмауэры создаются путем логического объединения портов или пользователей в отдельные группы виртуальной сети как на отдельных коммутаторах, так и в группе соединенных коммутаторов. Широковещательные сообщения одной виртуальной сети не передаются за ее пределы и, наоборот, на прилегающие порты не поступают широковещательные сообщения от других виртуальных сетей. Такой тип конфигурации существенно уменьшает общий широковещательный поток, освобождает полосу пропускания для потока данных пользователей и снижает общую чувствительность сети к широковещательной лавине (broadcast storm).

Чем меньше группа виртуальной сети, тем меньше количество пользователей, которые получают широковещательные сообщения, распространяемые внутри какой-либо группы. Группировка пользователей виртуальной сети может также выполняться на основе типа используемых приложений или типа широковещательных сообщений, поступающих от приложений. Можно поместить пользователей, совместно использующих приложения с высокой широковещательной активностью, в одну группу и распределить приложение по всей сети предприятия.

3.10. Обеспечение безопасности сети

По сетям часто передаются конфиденциальные данные. Защита конфиденциальной информации требует ограничения доступа к сети. Проблема, вызванная совместным использованием локальных сетей, состоит в том, что в такую сеть можно относительно легко проникнуть. Подключившись к активному порту, вторгшийся без разрешения в сеть пользователь получает доступ ко всем данным, передаваемым по сегменту. При этом чем больше группа, тем больше потенциальная угроза несанкционированного доступа.

Одним из эффективных в финансовом отношении и легко административно реализуемых методов повышения безопасности является сегментация сети на большое количество широковещательных групп. Это позволяет сетевому администратору:

- ограничить количество пользователей в группе виртуальной сети;
- запретить другим пользователям подсоединение без предварительного получения разрешения от приложения, управляющего виртуальной сетью;
- установить конфигурацию всех неиспользуемых портов в принимаемое по умолчанию состояние низкой активности VLAN. Реализовать сегментацию такого типа относительно просто. Порты коммутатора группируются на основе типа приложений и приоритетов доступа.

Приложения и ресурсы, доступ к которым ограничен, обычно размещаются в защищенной группе виртуальной сети. Маршрутизатор ограничивает доступ в эту группу в соответствии с конфигурацией коммутаторов и маршрутизаторов.

3.11. Конфигурирование сетей VLAN в коммутаторах Catalyst

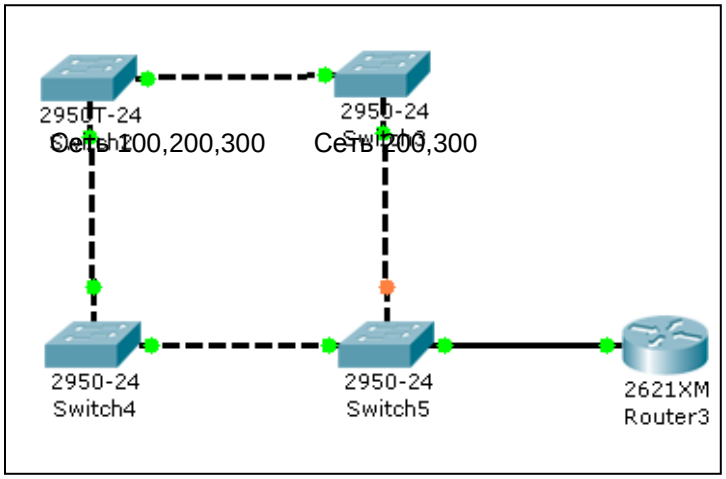
Некоторые устройства назначают принадлежность станций к сетям VLAN в соответствии со значениями их MAC-адресов. В коммутаторах Catalyst используется другой подход, а именно: назначение портов в принадлежность к сетям VLAN. Любое устройство, подключенное к порту коммутатора Catalyst, принадлежит сети VLAN в соответствии с описанием, которое осуществляется с помощью интерфейса командной сроки коммутатора. Даже если к порту подключен концентратор разделяемого доступа, то все равно все станции, подключенные к концентратору, принадлежат одной сети VLAN. Данный подход к организации сетей VLAN называется построением виртуальных локальных сетей на портовой основе (port-centric). Для конфигурации сетей VLAN в коммутаторах Catalyst вначале необходимо составить план принадлежности станций к сетям VLAN и правильно привязать порты к ним. Планирование принадлежности узлов к определенным виртуальным сетям включает знание того, какие сети третьего уровня должны принадлежать сети VLAN, какой необходим тип соединений между сетями VLAN

и где сети VLAN должны подключаться к уровню распределения. Необходимо ли при реализации структуры использовать сквозные сети VLAN или использовать подход третьего уровня? После завершения всех стадий планирования остается только создать сами сети VLAN.

3.11.1. Планирование сетей VLAN

Перед тем, как активизировать новую конфигурацию сетей VLAN, необходимо четко себе представлять, что именно необходимо сделать и как новые действия скажутся на других сетях VLAN или рабочих станциях, которые уже существуют в системе. На данной стадии планирование, в основном, должно концентрироваться вокруг факторов третьего уровня. Какие типы сетей должны поддерживаться в системе VLAN? Необходимо ли в сети VLAN использовать более одного протокола? Поскольку каждая сеть VLAN соответствует широковещательному домену, то существует возможность поддержки нескольких протоколов в сети VLAN. Однако каждому протоколу может соответствовать только одна сеть в системе VLAN.

Рис 20. Планирование сетей VLAN



Система, состоящая из нескольких коммутаторов, как в случае, показанном на рисунке. 20, может содержать несколько сетей VLAN.

Каждая сеть VLAN, показанная на рисунке. 20, поддерживает несколько протоколов. Для связи сетей друг с другом информация должна передаваться через маршрутизатор. Маршрутизатор, показанный на ответвлении сети, используется для соединения сетей друге другом. Ниже представлен конфигурационный файл такого маршрутизатора.

Файл конфигурации маршрутизатора, показанного на рисунке. 20

```
interface fastethernet 2/0
encapsulation isl 100
ip address 172.16.10.1 255.255.255.0
interface fastethernet 2/0.2
encapsulation isl 200
ip address 172.16.20.1 255.255.255.0
```

interface fastethernet 2/0.3

ip address 172.16.30.1 255.255.255.0

encapsulation isl 300

В примере показано, что между коммутатором и маршрутизатором установлено магистральное соединение (trunk). Магистральные соединения и инкапсуляция протокола межкоммутаторного канала (Inter-Switch Link — ISL). Магистральные соединения позволяют осуществлять передачу трафика более чем одной сети VLAN по одному физическому соединению. Команда **encapsulation isl**, показанная в примере, указывает маршрутизатору на необходимость использовать протокол ISL для того, чтобы осуществлять взаимодействие между широковещательными доменами, в которые входит каждый отдельный подынтерфейс. Следует заметить, что в конфигурации маршрутизатора используются логические подынтерфейсы. Обычно на маршрутизаторе каждому интерфейсу назначается один адрес для каждого протокола. Однако, если необходимо, чтобы один интерфейс виделся для протоколов маршрутизации как несколько интерфейсов, то в таких случаях можно использовать несколько подынтерфейсов, например, когда необходимо создать магистральное соединение между коммутатором Catalyst и маршрутизатором, как это показано в примере. Маршрутизатору необходимо идентифицировать различные широковещательные домены, соответствующие различным сетям VLAN, данные которых передаются по магистрали.

В маршрутизаторах Cisco для построения магистрали используется подход на основе подынтерфейсов, чтобы заставить маршрутизатор использовать один физический интерфейс как несколько физических интерфейсов. Каждый подынтерфейс определяет новый широковещательный домен, соответствующий одному физическому интерфейсу, который может принадлежать к своей сети протокола IP, даже в случае, когда все подынтерфейсы принадлежат одному главному (major) интерфейсу. В конфигурации, приведенной в примере, используются три подынтерфейса, т.е. один физический интерфейс (главный интерфейс) interface fastethernet 2/0 в действительности представляет собой три физических интерфейса и соответствует трем широковещательным доменам. Каждый из них входит в различную сеть IP. Для маршрутизаторов Cisco подынтерфейсы легко определяются, поскольку в описании главного интерфейса для них используется запись в виде /x. Например, подынтерфейс 3 в примере определяется как **int fastethernet 2/0.3**, где .3 задает подынтерфейс, соответствующий главному интерфейсу.

3.11.2. Создание сетей VLAN

Создание сети VLAN включает в себя этапы, которые приведены ниже.

Этап 1. Создать сеть VLAN.

Этап 2. Связать порты с сетью VLAN.

1. Для создание VLAN на коммутаторе Cisco используется команда
   Switch(config)#vlan *number_vlan*

2. При назначении портов следует помнить, что блок портов может быть указан с помощью знаков разделения: запятая и дефис. Не следует использовать символы пробелов между названиями портов в командной строке. В противном случае коммутатор Catalyst обрабатывает командную строку до первого символа пробела, и при этом только часть портов оказываются назначенными в принадлежность сети VLAN.

В большинстве ситуаций в сетях, где администраторы устанавливают коммутаторы Catalyst, еще существуют концентраторы старых типов. При этом могут существовать участки сетей, в которых станциям нет необходимости использовать полную пропускную способность выделенного порта коммутатора, а вполне достаточно пропускной способности, которая совместно используется несколькими устройствами. Для обеспечения большего значения пропускной способности можно подключить к концентратору меньшее количество устройств, чем было подключено ранее, а затем подключить концентратор к интерфейсу коммутатора Catalyst. При этом необходимо помнить, что все устройства, подключенные к концентратору, могут принадлежать только одной сети VLAN второго уровня, т.к. они в конечном счете подключены к одному порту коммутатора Catalyst.

3.11.3. Удаление сетей VLAN

Для удаления сети VLAN используется команда: Switch(config)#no vlan *number_vlan*, при этом стоит отметить все порты коммутаторы принадлежащие данному VLAN будут переведены в неактивное (disabled) состояние. Если к сети VLAN подключены 50 устройств, то при удалении такой сети все 50 станций окажутся изолированными, потому что порт коммутатора Catalyst, к которому подключена каждая станция, оказывается неактивным. При создании этой же сети VLAN все порты снова переходят в активное состояние, поскольку коммутатор Catalyst хранит информацию о том, какой сети VLAN порты принадлежали ранее.

Контрольные вопросы:

1. Укажите область применения виртуальных сетей?
2. Пользователь работающий за компьютером знает о том к какой виртуальной сети подключен его компьютер?

3. Один порт коммутатора может одноврменно находится в двух виртульаных сетях?
4. Что произойдет с портом находящийся в виртуальной сети номер 10 в случае удаления последней?
5. Укажите максимальное количество виртуальных сетей, которые можно сконфигурировать в локальной сети?
6. Технология виртуальных сетей применяется, поддерживается в глобальных сетях?
7. Каким образом обеспечивается безопасность передаваемых данных при использовании виртуальных локальных сетей?
8. Укажите преимущества использования виртуальных локальных сетей?

4.Сетевой уровень и маршрутизация

Каким путем должен пойти трафик через сети Этот выбор пути происходит на сетевом уровне. Функция выбора пути позволяет маршрутизатору оценивать имеющиеся пути до пункта назначения и устанавливать наилучший в этом плане метод обработки пакетов.

Оценивая возможные пути, протоколы маршрутизации используют информацию о топологии сетей. Эта информация может конфигурироваться сетевым администратором или собираться посредством динамических процессов, исполняемых в сети.

Сетевой уровень для сетей играет роль интерфейсов и обеспечивает своему пользователю, транспортному уровню, сервис по наилучшей сквозной доставке пакетов. Сетевой уровень пересылает пакеты из сети-источника в сеть пункта назначения на основе таблицы IP-маршрутизации.

После того как маршрутизатор определит, какой путь использовать, он может переходить к коммутированию пакета: принимая пакет, полученный через один интерфейс, и перенаправляя его на другой интерфейс или порт, который соответствует наилучшему пути к пункту назначения пакета.

Чтобы иметь практическую ценность, сеть должна непротиворечивым образом показывать пути, имеющиеся между маршрутизаторами. Как показано на рисунке, каждая связь между маршрутизаторами имеет номер, который маршрутизаторы используют в качестве адреса. Эти адреса должны нести в себе информацию, которая может быть использована в процессе маршрутизации. Это означает, что адрес должен содержать информацию о пути соединений сред передачи данных, которую процесс маршрутизации будет использовать для пересылки пакетов от отправителя в конечный пункт назначения.

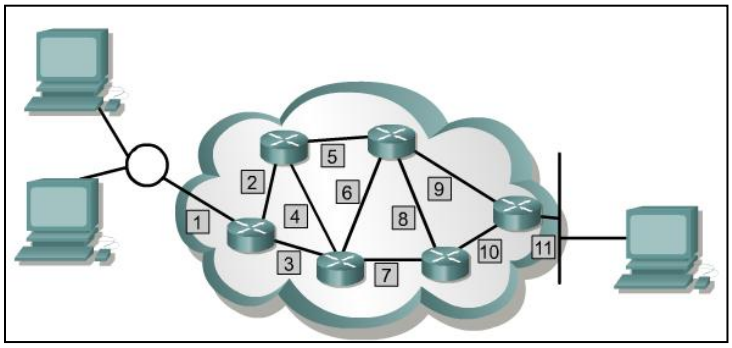


Рис 21. Определение маршрута между удаленными сетями

Используя эти адреса, сетевой уровень может обеспечить организацию релейного соединения, которое будет связывать независимые сети. Непротиворечивость адресов уровня 3 во всем многосетевом комплексе также улучшает использование полосы пропускания, исключая необходимость в широковещательных рассылках. Широковещательные рассылки приводят к накладным расходам в виде ненужных

процессов и напрасно расходуют мощности устройств или каналов связи, которым вовсе не надо принимать эти широковещательные рассылки.

Благодаря использованию непротиворечивой сквозной адресации для представления пути соединений сред передачи данных сетевой уровень может находить путь до пункта назначения без ненужной загрузки устройств или каналов связи многосетевого комплекса широковещательными рассылками.

4.1.Адресация: сеть и хост-машина

Сетевой адрес состоит из сетевой части и части хост-машины, которые используются маршрутизатором в "облаке" сети. Обе они нужны для доставки пакетов от отправителя получателю. Сетевой адрес используется маршрутизатором для идентификации сети отправителя или получателя пакета внутри сетевого комплекса.

Для некоторых протоколов сетевого уровня эти отношения задаются администратором сети, который назначает сетевые адреса в соответствии с планом адресации сетевого комплекса. Для других же протоколов сетевого уровня назначение адресов является частично или полностью динамическим. Большинство схем адресации в сетевых протоколах использует некоторую форму адреса хост-машины или узла.

4.2.Маршрутизация с использованием сетевых адресов

В общем случае маршрутизаторы передают пакет по эстафете из одного канала связи: другой. Чтобы осуществить такую эстафетную передачу, маршрутизаторы используют, основные функции: функцию определения пути и функцию коммутации.

На рисунке показано, как маршрутизаторы используют адресацию для реализации своих функций маршрутизации и коммутации. Сетевая часть адреса используется для осуществления выбора пути, а узловая часть адреса говорит о порте маршрутизатора" по пути следования.

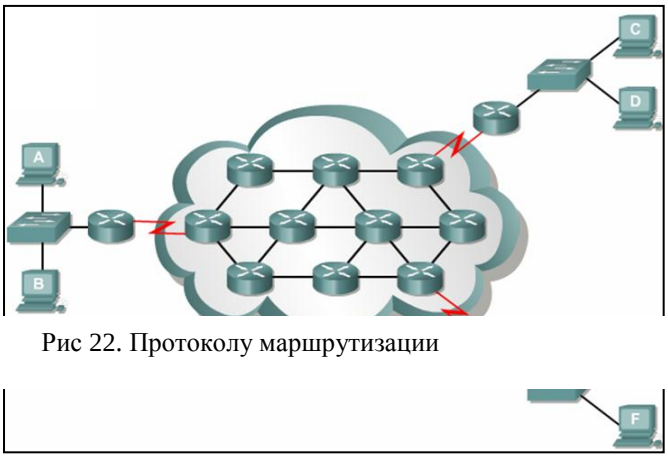


Рис 22. Протоколу маршрутизации

Маршрутизатор отвечает за передачу пакета в следующую сеть по пути следования. Сетевая часть адреса используется маршрутизатором для выбора пути. Функция коммутирования позволяет маршрутизатору принимать пакет на один интерфейс и переправлять его на другой. Функция определения пути позволяет маршрутизатору выбрать наиболее подходящий интерфейс для

переадресации пакета. Узловая часть адреса говорит о конкретном порте маршрутизатора, который имеет выход на соседний маршрутизатор в выбранном направлении.

4.3. Протоколы маршрутизации и маршрутизируемые протоколы

- Маршрутизируемый протокол — любой сетевой протокол, который обеспечивает в адресе сетевого уровня достаточно информации, чтобы позволить передать пакет от одной хост-машины к другой на основе принятой схемы адресации. Маршрутизируемый протокол определяет формат и назначение полей внутри пакета. В общем случае пакеты переносятся от одной конечной системы к другой. Примером маршрутизируемого протокола является межсетевой протокол IP.
- Протокол маршрутизации — поддерживает маршрутизируемый протокол за счет предоставления механизмов коллективного использования маршрутной информации. Сообщения протокола маршрутизации циркулируют между маршрутизаторами. Протокол маршрутизации позволяет маршрутизаторам обмениваться информацией с другими маршрутизаторами с целью актуализации и ведения таблиц. Примерами протоколов маршрутизации являются протокол маршрутной информации (RIP), протокол внутренней маршрутизации между шлюзами (IGRP), усовершенствованный протокол внутренней маршрутизации между шлюзами (EIGRP) и протокол маршрутизации с выбором кратчайшего пути (OSPF).

4.4.Статические и динамические маршруты

Статическая информация администрируется вручную. Сетевой администратор вводит ее в конфигурацию маршрутизатора. Если изменение в топологии сети требует актуализации статической информации, то администратор сети должен вручную обновить соответствующую запись о статическом маршруте.

Динамическая информация работает по-другому. После ввода администратором сети команд, запускающих функцию динамической маршрутизации, сведения о маршрутах обновляются процессом маршрутизации автоматически сразу после поступления из сети новой информации. Изменения в динамически получаемой информации распространяются между маршутизаторами как часть процесса актуализации данных.

Статическая маршрутизация имеет несколько полезных применений, которые связаны с привлечением специальных знаний администратора сети о сетевой топологии. Одним из таких применений является защита в сети. Динамическая маршрутизация раскрывает все, что известно о сети. Однако по причинам безопасности может понадобиться скрыть

некоторые части сети. Статическая маршрутизация позволяет администратору сетевого комплекса задавать те сведения, которые могут сообщаться о закрытых частях сети.

Статический маршрут к сети также достаточен в том случае, если сеть доступна только по одному пути. Такой тип участка сетевого комплекса называется тупиковой сетью.

Конфигурирование статического маршрута к тупиковой сети исключает накладные расходы, связанные с динамической маршрутизацией.

Маршрут по умолчанию— записи в таблице маршрутизации, которая используется для направления кадров, которые не имеют в таблице маршрутизации явно указанного следующего перехода. Маршруты по умолчанию могут устанавливаться как результат статического конфигурирования, выполняемого администратором, но ничего не знают о других сетях.

4.5.Адаптация к изменениям топологии

Показанная на рисунке сеть по-разному адаптируется к изменениям в топологии, в зависимости от того, используется статическая или динамическая информация.

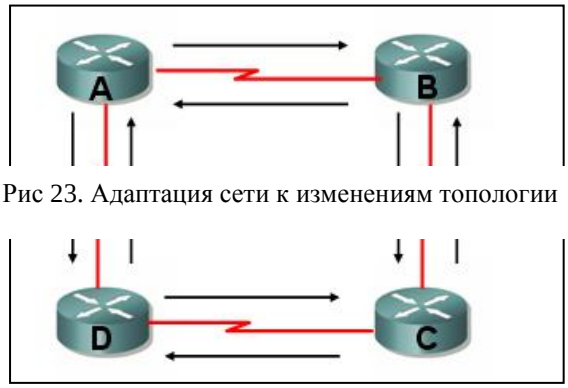


Рис 23. Адаптация сети к изменениям топологии

Статическая маршрутизация позволяет маршрутизаторам правильно направлять пакет от сети к сети. Маршрутизатор просматривает свою таблицу маршрутизации и, следуя содержащимся там статическим данным, ретранслирует пакет маршрутизатору D. Маршрутизатор D делает то же самое и ретранслирует пакет маршрутизатору C. Маршрутизатор C доставляет пакет хост-машине получателя.

Но что произойдет, если путь между маршрутизаторами A и D становится непроходимым? Ясно, что маршрутизатор A не сможет ретранслировать пакет маршрутизатору D по статическому маршруту. Связь с сетью пункта назначения будет невозможна до тех пор, пока маршрутизатор A не будет реконфигурирован на ретрансляцию пакетов маршрутизатору B. Динамическая маршрутизация обеспечивает более гибкое и автоматическое поведение. В соответствии с таблицей маршрутизации, генерируемой маршрутизатором A, пакет может достичь своего пункта назначения по предпочтительному маршруту через маршрутизатор D. Однако к пункту назначения возможен и другой путь через маршрутизатор B. Когда маршрутизатор A узнает, что канал на маршрутизатор D нарушен, он перестраивает свою таблицу маршрутизации, делая предпочтительным путь к пункту назначения через маршрутизатор B, а

маршрутизаторы продолжают слать пакеты по этому каналу связи. Когда путь между маршрутизаторами A и D восстанавливается, маршрутизатор A может снова изменить свою таблицу маршрутизации и указать предпочтительным путь к сети пункта назначения против часовой стрелки через маршрутизаторы D и C.

Протоколы динамической маршрутизации могут также перенаправлять трафик между различными путями в сети.

Успех динамической маршрутизации зависит от двух основных функций маршрутизатора.

- Ведение таблицы маршрутизации.
- Своевременное распространение информации — в виде пакетов актуализации — среди других маршрутизаторов.

В обеспечении коллективного пользования информацией о маршрутах динамическая маршрутизация полагается на протокол маршрутизации.

. Протокол маршрутизации определяет набор правил, используемых маршрутизатором при его общении с соседними маршрутизаторами.

Например, протокол маршрутизации описывает следующее:

- как посылаются пакеты актуализации;
- какие сведения содержатся в таких пакетах актуализации;
- когда следует посылать эту информацию;
- как определять получателей этих пакетов актуализации.

4.6. Представление расстояния с помощью метрики

Когда алгоритм маршрутизации обновляет таблицу маршрутизации, его главной целью является определение наилучшей информации для включения в таблицу. Каждый алгоритм маршрутизации интерпретирует понятие наилучшая по-своему. Для каждого пути в сети алгоритм генерирует число, называемое метрикой. Как правило, чем меньше величина этого числа, тем лучше путь.

Метрики могут рассчитываться на основе одной характеристики пути. Объединяя несколько характеристик, можно рассчитывать и более сложные метрики.

Наиболее общеупотребительными метриками, используемыми маршрутизаторами, являются следующие:

- Количество переходов - количество маршрутизаторов, которые должен пройти пакет, чтобы дойти до получателя. Чем меньше количество переходов, тем лучше путь. Для обозначения суммы переходов до пункта назначения используется термин длина пути.

- Полоса пропускания - пропускная способность канала передачи данных. Например, для арендуемой линии 64 Кбит/с обычно предпочтительным является канал типа T1 с полосой пропускания 1,544 Мбит/с.
- Задержка - продолжительность времени, требующегося для перемещения пакета от отправителя получателю.
- Нагрузка - объем действий, выполняемый сетевым ресурсом, например маршрутизатором или каналом.
- Надежность - темп возникновения ошибок в каждом сетевом канале.
- Тики - задержка в канале передачи данных, определяемая в машинных тактах IBM-подобного ПК (приблизительно 55 миллисекунд).
- Стоимость - произвольное значение, обычно основанное на величине полосы пропускания, денежной стоимости или результате других измерений, которое назначается сетевым администратором.

4.7.Протоколы маршрутизации

Большинство алгоритмов маршрутизации можно свести к трем основным алгоритмам.

- Подход на основе маршрутизации по вектору расстояния, в соответствии с которым определяются направление (вектор) и расстояние до каждого канала в сети.
- Подход на основе оценки состояния канала (также называемый выбором наикратчайшего пути), при котором воссоздается точная топология всей сети (или по крайней мере той части, где размещается маршрутизатор).

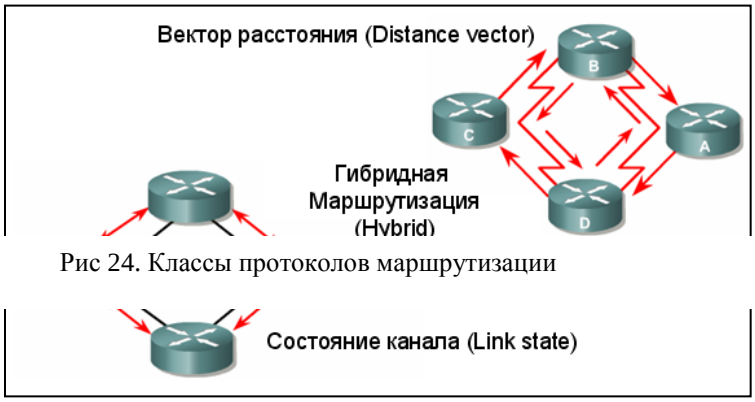


Рис 24. Классы протоколов маршрутизации

Алгоритм маршрутизации является основой динамической маршрутизации. Как только вследствие роста, реконфигурирования или отказа изменяется топология сети, база знаний о сети должна изменяться тоже; это прерывает маршрутизацию, топологии. В том случае, когда все маршрутизаторы используют непротиворечивое представление топологии сети, имеет место сходимость. Говорят, что сетевой комплекс сошелся, когда все имеющиеся в нем маршрутизаторы работают с одной и той же информацией. Процесс и время, требующиеся для возобновления сходимости маршрутизаторов, меняются в зависимости

от протокола маршрутизации. Для сети желательно обладать свойством быстрой сходимости, поскольку это уменьшает время, когда маршрутизаторы используют для принятия решений о выборе маршрута устаревшие знания, и эти решения могут быть неправильными, расточительными по времени или и теми и другими одновременно.

4.7.1. Алгоритмы маршрутизации по вектору расстояния

Алгоритмы маршрутизации на основе вектора расстояния (также известные под названием алгоритмы Беллмана—Форда (Bellman-Ford algorithms)) предусматривают периодическую передачу копий таблицы маршрутизации от одного маршрутизатора другому. Регулярно посылаемые между маршрутизаторами пакеты актуализации сообщают обо всех изменениях топологии.

Каждый маршрутизатор получает таблицу маршрутизации от своего соседа. Например, на маршрутизатор B получает информацию от маршрутизатора A. Маршрутизатор B добавляет величину, отражающую вектор расстояния (скажем, количество переходов), которая увеличивает вектор расстояния, и затем передает таблицу маршрутизации своему соседу - маршрутизатору C. Такой же процесс пошагово выполняется между соседними маршрутизаторами во всех направлениях. Подобным образом алгоритм аккумулирует сетевые расстояния и поэтому способен поддерживать базу данных информации о топологии сети. Однако алгоритмы на основе вектора расстояния не позволяют маршрутизатору знать точную топологию всего сетевого комплекса Алгоритм маршрутизации по вектору расстояния и исследование сети. Каждый маршрутизатор, использующий алгоритм маршрутизации по вектору расстояния, начинает с идентификации или исследования своих соседей.

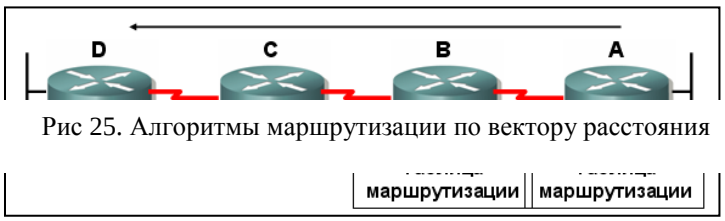


Рис 25. Алгоритмы маршрутизации по вектору расстояния

Продолжая процесс исследования векторов расстояния в сети, маршрутизаторы как бы открывают наилучший путь до сети пункта назначения на основе информации от каждого соседа. Например, маршрутизатор A узнает о других сетях, основываясь на информации, которую он получает от маршрутизатора B. Каждая запись в таблице маршрутизации об этих других сетях имеет кумулятивное значение вектора расстояния, показывающее, насколько далеко эта сеть находится в данном направлении.

4.7.1.1. Алгоритм маршрутизации по вектору расстояния и изменения топологии

При изменении топологии сети, использующей протокол на основе вектора расстояния, таблицы маршрутизации должны быть обновлены Аналогично процессу исследования сети, обновление содержания таблиц маршрутизации из-за изменения топологии происходит шаг за шагом от одного маршрутизатора к другому.

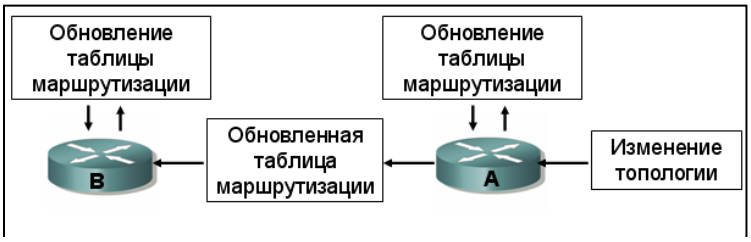


Рис 26. Алгоритмы маршрутизации по вектору расстояния при изменении топологии

Алгоритмы с вектором расстояния заставляют каждый маршрутизатор отсылать всю таблицу маршрутизации каждому своему непосредственному соседу. Таблицы маршрутизации, генерируемые в рамках метода вектора расстояния, содержат информацию об общей стоимости пути (определяемой его метрикой) и логический адрес первого маршрутизатора, стоящего на пути к каждой известной ему сети.

4.8. Алгоритмы маршрутизации с учетом состояния канала связи

Вторым основным алгоритмом, используемым для маршрутизации, является алгоритм с учетом состояния канала связи. Алгоритмы маршрутизации с учетом состояния канала связи, также известные под названием алгоритмов выбора первого кратчайшего пути (shortest path first (SPF) algorithms), поддерживают сложную базу данных топологической информации. И если алгоритмы с маршрутизацией по вектору расстояния работают с неконкретной информацией о дальних сетях, то алгоритмы маршрутизации с учетом состояния канала собирают полные данные о дальних маршрутизаторах и о том, как они соединены друг с другом. Для выполнения маршрутизации с учетом состояния канала связи используются сообщения объявлений о состоянии канала (link-state advertisements, LSA), база данных топологии, SPF- алгоритм, результирующее SPS-дерево и таблица маршрутизации, содержащая пути и порты к каждой сети.

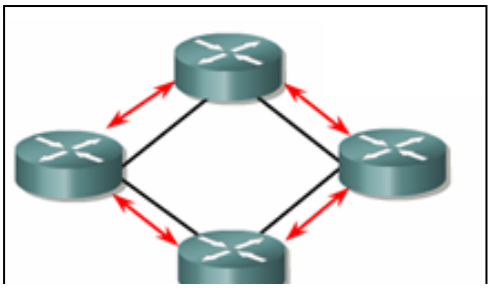


Рис 27. Алгоритмы маршрутизации с учетом состояния канала связи

Инженерами концепция учета состояния канала была реализована в виде OSPF-маршрутизации.

4.8.1.Режим исследования сети в алгоритмах с учетом состояния канала

Для создания общей картины всей сети используются механизмы исследования сети с учетом состояния канала связи. После этого все маршрутизаторы, которые работают с алгоритмом учета состояния канала, коллективно используют это представление сети. Все это подобно существованию нескольких идентичных карт города. На рисунке четыре сети (W, X, Y и Z) соединены тремя маршрутизаторами, выполняющими маршрутизацию с учетом состояния канала связи.

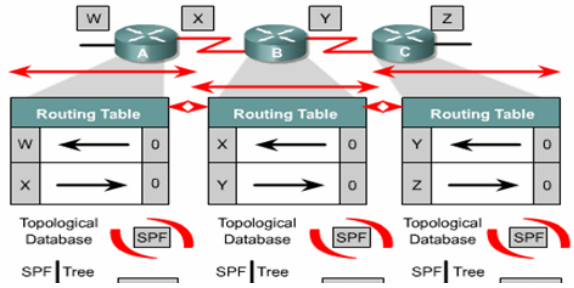


Рис 28. Режим исследования сети в алгоритмах с учетом состояния канала связи

В режиме исследования сети при маршрутизации с учетом состояния канала связи выполняются следующие процессы.

1. Маршрутизаторы обмениваются друг с другом LSA-сообщениями. Каждый маршрутизатор начинает с непосредственно подключенных сетей, о которых у него есть прямая информация.

2. Маршрутизаторы параллельно друг с другом создают топологическую базу данных, содержащую все LSA-сообщения, сгенерированные в сетевом комплексе.

3. SPF-алгоритм вычисляет достижимость сетей, определяя кратчайший путь до каждой сети сетевого комплекса, где применяется протокол маршрутизации с учетом состояния канала связи. Маршрутизатор создает эту логическую топологию кратчайших путей в виде SPF- дерева, помещая себя в корень. Это дерево отображает пути от маршрутизатора до всех пунктов назначения.

4. Наилучшие пути и порты, имеющие выход на эти сети назначения, сводятся маршрутизатором в таблице маршрутизации. Он также формирует и другие базы данных с топологическими элементами и подробностями о статусе.

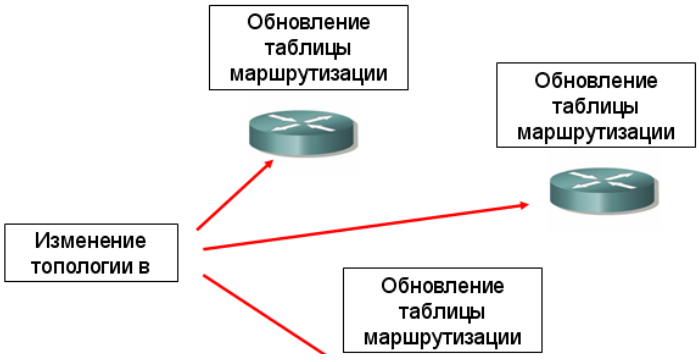


Рис 29. Распространение информации о изменении топологии в протоколах маршрутизации с учетом состояния канала связи

Алгоритмы учета состояния канала связи полагаются на маршрутизаторы, имеющие общее

представление о сети. Как показано на рисунке, при изменении топологии в сетевом комплексе, использующем маршрутизацию с учетом состояния канала связи, маршрутизаторы, которые первыми узнают об изменении, посылают информацию другим маршрутизаторам или специально назначенному маршрутизатору, который затем могут использовать все другие маршрутизаторы для обновления своей топологической информации. Это влечет за собой отсылку общей маршрутной информации всем маршрутизаторам, стоящим в сети. Для достижения сходимости каждый маршрутизатор выполняет следующие действия.

- Отслеживает своих соседей: его имя, его рабочее состояние и стоимость линии связи с ним.
- Создает LSA-пакет, в котором приводится перечень имен соседних маршрутизаторов и стоимость линий связи. Сюда же включаются данные о новых соседях, об изменениях в стоимости линий связи и о связях с соседями, которые стали нерабочими.
- Посылает LSA-пакет, так что все другие маршрутизаторы получают его.
- Получая LSA-пакет, записывает его в свою базу данных, так что он может хранить самые последние LSA-пакеты, сгенерированные каждым другим маршрутизатором.
- Используя накопленные данные LSA-пакетов для создания полной карты топологии сети, маршрутизатор, стартуя с этой общей точки, запускает на исполнение SPF- алгоритм и рассчитывает маршруты до каждой сети назначения.

Каждый раз, когда LSA-пакет вызывает изменение в базе данных состояний каналов, алгоритм учета состояния каналов связи пересчитывает лучшие пути и обновляет таблицу маршрутизации. Затем каждый маршрутизатор принимает к сведению изменение топологии и определяет кратчайшие пути для использования при коммутировании пакетов.

Сравнивать маршрутизацию по вектору расстояния и маршрутизацию с учетом стояния канала связи можно в нескольких ключевых областях.

- Процесс маршрутизации по вектору расстояния получает все топологические данные из информации, содержащейся в таблицах маршрутизации соседей. Процесс маршрутизации с учетом состояния канала связи получает широко представление обо всей топологии сетевого комплекса, собирая данные из всех необходимых LSA-пакетов.

- Процесс маршрутизации по вектору расстояния определяет лучший путь с помощью сложения получаемых метрик по мере того, как таблица движется от одного маршрутизатора к другому. При использовании маршрутизации с учетом состояния канала каждый маршрутизатор работает отдельно, вычисляя свой собственный кратчайший путь к пункту назначения.
- В большинстве протоколов маршрутизации по вектору расстояния пакеты актуализации, содержащие сведения об изменениях топологии, являются периодически посылаемыми пакетами актуализации таблиц маршрутизации. Эти таблицы передаются от одного маршрутизатора к другому, что обычно приводит к более медленной сходимости.
- В протоколах маршрутизации с учетом состояния канала связи пакеты актуализации обычно генерируются и рассылаются по факту возникновения изменения топологии. Относительно небольшие LSA-пакеты передаются всем другим маршрутизаторам, что, как правило, приводит к более быстрой сходимости при любом изменении топологии сетевого комплекса.

Контрольные вопросы:

1. Укажите область применения протоколов маршрутизации?
2. Конечные устройства, например компьютеры поддерживают протоколы маршрутизации?
3. Укажите характерные черты протоколов маршрутизации на основе вектора расстояния?
4. Укажите причины возникновения петель маршрутизации?
5. Укажите протоколы маршрутизации реализующие классы протоколов маршрутизации на основе вектора расстония и с учетом состояния канала?
6. Какие задачи решают протоколы маршрутизации?
7. Что происходит при изменении топологии, например обрывается канал между двумя маршрутизаторами при настроенном протоколе маршрутизации?
8. Какой критерий используется для выбора лучшего маршрута при использовании протоколов маршрутизации?
9. Какие математические алгоритмы используются для выбора лучшего маршрута в протоколах маршрутизации?
10. Укажите максимальные размер сети в которой может использоваться протокол маршрутизации?
11. Что такое статическая маршрутизация?

12. Укажите преимущества и недостатки статической и динамической маршрутизации?
13. Укажите открытые протоколы маршрутизации?

5. КОнфигурирование протокола маршрутизации OSPF. Проверка и поиск неисправностей

Протокол OSPF (Open Shortest Path First), описанный в стандарте RFC 2328, — это внутренний шлюзовый протокол, используемый для распространения данных маршрутизации внутри одной автономной системы.

OSPF — это открытый протокол маршрутизации, базирующийся на алгоритме поиска наикратчайшего пути.

5.1.Общие сведения

Протокол OSPF был разработан в 1991 году. Протокол OSPF основан на технологии отслеживания состояния канала, которая является отступлением от векторных алгоритмов Беллмана-Форда, используемых в традиционных протоколах маршрутизации Интернета, таких как RIP.

Преимущества использования протокола маршрутизации OSPF:

- Протокол маршрутизации OSPF применим только в сетях IP
- Высокая скорость сходимости, по сравнению с протоколами маршрутизации на основе вектора расстояния
- Отсутствие петель маршрутизации
- Поддержка сетевых масок переменной длины (VLSM)
- Применим с сетях любого размера
- Оптимальное использование пропускной способности с построением дерева кратчайших путей;
- Поддержка балансировки между маршрутами имеющие одинаковое значение метрики
- Поддержка аутентификации маршрутизации с использованием различных методов аутентификации на основе пароля
- Поддержка механизма агрегирования маршрутов и сокращение ненужного распространения данных подсети.
- Поддержка иерархической структуры разделения сетей, что позволяет ограничить распространение обновлений по сети

5.2. Принцип работы протокола маршрутизации

Протокол маршрутизации OSPF использует алгоритм состояния канала для формирования и расчета кратчайшего пути ко всем известным местам назначения. Понимание принципа работы протокола маршрутизации OSPF позволяет выполнить его общую настройку, обеспечивая высокую эффективность его работы, например уменьшения времени конвергенции сети при изменении топологии, использование оптимизированной маршрутизации. Стоит отметить представленный далее материал не обеспечивает полноту рассказа принципа работы протокола маршрутизации OSPF и его настройки, для более детального изучения необходимо изучение дополнительной литературы и выполнения усложненных лабораторных работ. Общий принцип работы протокола маршрутизации представлен ниже:

1. На сетевом оборудовании включается протокол маршрутизации OSPF.
2. Маршрутизаторы обмениваются hello-пакетами через все интерфейсы, на которых настроен OSPF.

   Стоит отметить рассылка специализированных сообщений hello используется для решения нескольких задач, например установки смежных отношений и отслеживание смежности. Под сменными отношениями понимается непосредственное подключение двух маршрутизаторов между собой и обмена маршрутизирующей информацией по протоколу OSPF. Маршрутизаторы, разделяющие общий канал передачи данных, становятся соседями, когда они приходят к договоренности об определённых параметрах, указанных в их hello-пакетах.

   Условия установки смежных отношений варьируются от типа используемой сети в рамках протокола маршрутизации OSPF. В общем виде для установления смежных отношений необходимо выполнение следующих условий:

   - Совпадение номера области, сконфигурированной на этих маршрутизаторах
   - Совпадение времени рассылки hello сообщений
   - Совпадение паролей безопасности настроенных для обеспечения безопасности работы протокола OSPF
   - Совпадение размера mtu
   - Совпадение типа сети OSPF
   - Идентификаторы маршрутизаторов не должны совпадать между собой

3. Каждый маршрутизатор посылает объявления о состоянии канала маршрутизаторам, с которыми он находится в состоянии смежности.

   Информация о состоянии канала содержит - список сетей подключенных непосредственно к данному маршрутизатору, стоимость каналов непосредственно подключенных сетей.

   Стоимость (метрика) интерфейса OSPF характеризует издержки на отправку пакетов через тот или иной интерфейс. Формула для расчета стоимости:

   стоимость = 10000 0000/пропускная способность в бит/с

4. Каждый маршрутизатор, получивший объявление от смежного маршрутизатора, записывает полученную информацию в свою топологическую таблицу и рассылает копию данного объявления всем другим смежным с ним маршрутизаторам.

   Таким образом рассылка объявления о состоянии канала осуществляется всем маршрутизаторам одной OSPF-зоны, тем самым обеспечивает идентичность топологической информации между всеми маршрутизаторами области.

5. На основе топологической таблицы, каждый маршрутизатор используя алгоритм «Shortest Path First» вычисляет граф без петель, который будет описывать кратчайший путь к каждому известному пункту назначения. В качестве корня построенного дерева кратчайших путей является маршрутизатор, который его строит.
6. На основе дерева кратчайших путей каждый маршрутизатор осуществляет поиск кратчайшего пути до удаленных сетей и лучший маршрут записывает в свою таблицу маршрутизации.

5.3.Области OSPF

В протоколах маршрутизации на основе состояния канала, все маршрутизаторы должны иметь одинаковую таблицу топологии. При увеличении количества маршрутизаторов увеличивается размер топологической таблицы. С одной стороны знание обо всех маршрутах можно отнести к преимуществу, но данный подход не применим к большим сетям. В протоколе маршрутизации OSPF используется понятие областей, на основе которых формируется двух уровневая иерархическая структура топологии сети. В основе данной структуры находится область с номером – 0. Данная область называется магистральная зона. Все оставшиеся области должны непосредственно подключаться к магистральной зоне, как показано на рисунке.

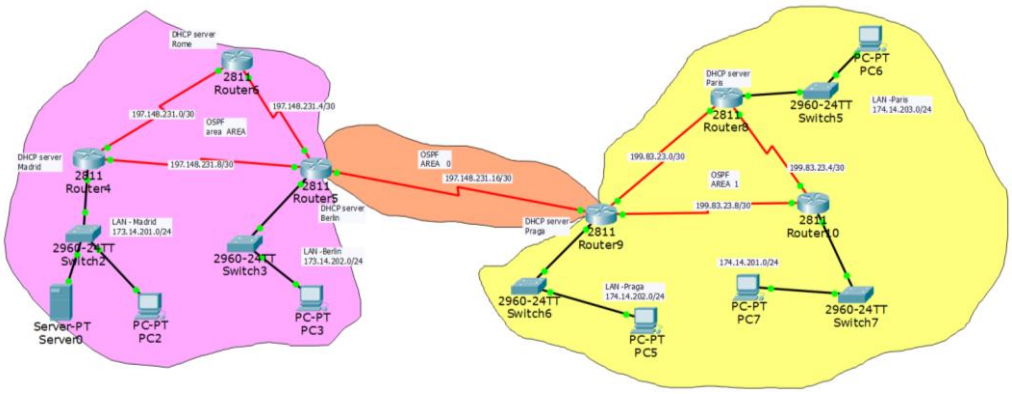


Рис 30. Иерархическая структура областей OSPF

Маршрутизаторы внутри зоны содержат детальную информацию обо всех каналах и маршрутизаторах этой зоны.

Данный иерархический подход позволяет при выходе из строя канала в одной области, осуществлять рассылку информации о данном изменении всем соседям в пределах этой зоны. Маршрутизаторы других областей не получают эту информацию.

Рекомендации позволяющие не перегружать маршрутизаторы расчётами OSPF:

- Область должна содержать не более 50 маршрутизаторов.
- Маршрутизатор должен быть не более чем в 3 областях.

5.4.Конфигурирование протокола маршрутизации OSPF для одной области

Для повышения наглядности представляемого материала в дальнейшем будет использоваться топология представленная на рисунке 31.

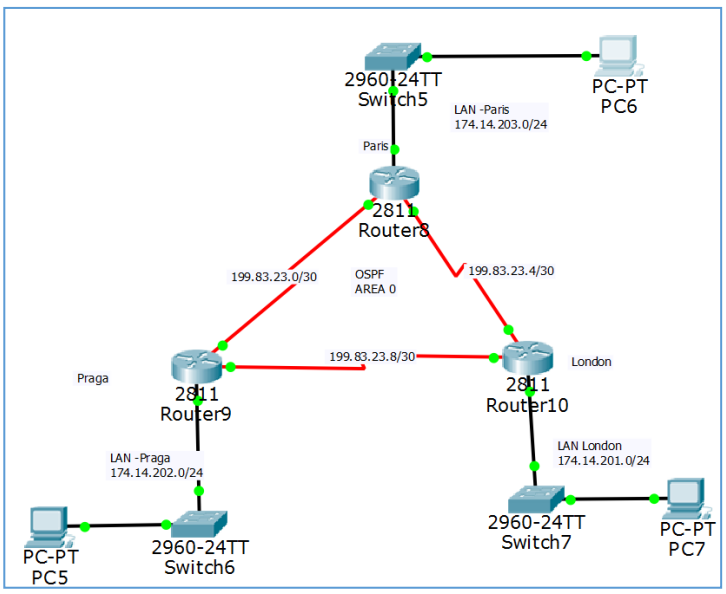


Рис 31. Пример сети для настройки OSPF в одной области

5.4.1.Выбор идентификатора маршрутизатора (Router ID)

На первом шаге для каждого маршрутизатора необходимо сконфигурировать идентификатор - Router ID, данный параметр можно назначить административно выполнив команду:

R1(config-router)#**router-id** <ip-address>

Если идентификатор маршрутизатор не был назначен административно, то он выбирается автоматически, в зависимости от настроек маршрутизатора, согласно следующим правилам:

- В качестве идентификатора маршрутизатора выбирается наибольший IP-адрес присвоенный любому из loopback-интерфейсов.

Loopback-интерфейс – является логическим интерфейсом настраиваемом на маршрутизаторе, для решения различных задач.

Чтобы назначить IP адрес loopback-интерфейсу используется следующая последовательность команд:

R1(config)#**interface loopback** <номер интерфейса>

R1(config-if)#**ip address** <ip-address> <маска подсети>

- Если не используются вышеперечисленные способы, то в качестве идентификатора маршрутизатора выбирается наибольший IP-адрес из всех активных интерфейсов сетевого устройства.

Важно отметить при изменении идентификатора маршрутизатора необходимо выполнить дополнительные действия, чтобы данные изменения вступили в силу. Возможны два варианта для применения изменения настроек протокола маршрутизации OSPF: первый – перегрузить сетевое устройство, второй вариант - использовать команду перезапуска процесс OSPF:

R1(config)#**clear ip ospf process**

5.4.2.Включение OSPF

На втором этапе конфигурирования протокола маршрутизации OSPF осуществляется его включение на соответствующих интерфейсах. Для настройки протокола маршрутизации OSPF используются следующие команды:

R1(config)# router ospf <process-id>

R1 (config-router)# network <network> <wildcard mask> area <area-id>

Параметры команды network:

<network> — непосредственно присоединенная сеть к маршрутизатору.

<wildcard mask> — шаблонная маска, которая указывает с помощью 0 какая часть из указанной сети должна совпадать, а с помощью 1 какая часть сети может быть произвольной.

<area-id> — идентификатор области, в которой будет работать интерфейс маршрутизатора. Интерфейс попадет в эту область при условии, что его IP-адрес совпадает с сетью указанной с помощью network и wildcard mask.

Для небольших сетей этот параметр можно указывать равным 0, но для больших сетей необходимо соблюдать иерархический дизайн областей в OSPF. Все обновления OSPF, которые передаются между различными областями, должны проходить через область 0.

Команда network делает следующее:

- включает OSPF на интерфейсе, IP-адрес которого совпадает с указанной сетью и маской,
- анонсирует сеть этого интерфейса через другие интерфейсы, на которых включен OSPF.

5.4.2.Проверка работы OSPF. Поиск и устранение неисправностей при конфигурировании OSPF

Сетевой специалист выполняя настройку протокола маршрутизации OSPF должен уметь проверять правильность работы OSPF. Ниже представлен краткий обзор команд, используемых для проверки работы OSPF.

- **show ip ospf neighbor—** команда используется для того, чтобы убедиться, что маршрутизатор сформировал отношения смежности с соседними маршрутизаторами.

  Отображает идентификатор соседнего маршрутизатора, приоритет, состояние OSPF, таймер простоя (dead), IP-адрес интерфейса соседнего устройства, интерфейс, через который доступно это соседнее устройство.

Если идентификатор соседнего маршрутизатора не отображается или не показывает состояние FULL или 2WAY, это значит, что оба маршрутизатора не создали отношения смежности OSPF.

- **show ip protocols**— эта команда обеспечивает быструю проверку критически важных данных конфигурации OSPF: идентификатор маршрутизатора; сети анонсируемые маршрутизатором, соседние устройства, от которых маршрутизатор принимает обновления,
- **show ip ospf**— эта команда используется для отображения идентификатора процесса OSPF и идентификатора маршрутизатора, а также сведений об OSPF SPF и об области OSPF.
- **show ip ospf interface**— эта команда предоставляет подробный список интерфейсов, где работает протокол OSPF, с ее помощью можно определить, правильно ли были составлены выражения **network.**
- **show ip route ospf** — используется только для отображения полученных маршрутов OSPF в таблице маршрутизации, как показано на рисунке.

```
R1# show ip route ospf
Codes:L - local,C - connected,S - static,R - RIP,M - mobile,B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS,su - IS-IS summary,L1 - IS-IS level-1,L2-IS-IS level-2
      ia - IS-IS inter area,*-candidate default,U-per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:33:17, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.16.2.0/24 [110/65] via 172.16.3.2, 00:33:17,Serial0/0/0
O
O

R1#
```

Рис 32. Таблица маршрутизации маршрутизатора

Обозначения маршрутов OSPF в таблице маршрутизации:

- O — OSPF intra-area (router LSA) и network LSA — сети в зоне маршрутизатора.
- O IA — OSPF interarea (summary LSA) — сети вне зоны маршрутизатора, но в той же автономной системе.
- O E1 — Type 1 external routes — сети вне автономной системы маршрутизатора. К метрике внешнего маршрута добавляется cost всех линков по которым передавался

маршрут. Используется когда несколько маршрутизаторов анонсируют внешнюю сеть.

- O E2 — Type 2 external routes (по умолчанию) — сети вне автономной системы маршрутизатора. Используется только cost внешнего маршрута.

Контрольные вопросы:

1. Укажите способы задания идентификатора маршрутизатора?
2. Идентификатор маршрутизатора – где используется данный параметр?
3. Какие команды используютс для настройки протокола маршрутизации OSPF?
4. Какие команды используются для проверки работы протокола маршрутизации OSPF?
5. Назовите условия, которые должны выполнятся при установлении смежных отношений?
6. Назовите все обозначения, которые используются для отображения маршрутов в таблице маршрутизации полученных с помощью протокола маршрутизации OSPF
7. Укажите преимущества иерархической структуры областей в OSPF?
8. Какой критерий используется в OSPF для выбора лучшего маршрута до удаленной сети?
9. Какие три таблицы используется протокола маршрутизации в OSPF для своей работы?
10. Укажите действия, выполняемые протоколом маршрутизации OSPF в случае изменения топологии?

6.Обеспечение безопасности сети

Компьютеры, сети, Internet стали неотъемлемой частью нашей повседневной жизни. Наш быстро развивающийся, насыщенный технологиями мир с каждым днем все больше становится зависимым от компьютерных технологий и сетей. И достаточно долгое время специалисты в области компьютерных технологий не уделяли внимания безопасности компьютерных сетей.

6.1.Чем вызвана необходимость обеспечения безопасности сетей

В настоящее время огромное количество сетей объединено посредством Internet. Для безопасной работы такой огромной системы необходимо принимать определенные меры безопасности, поскольку практически с любого компьютера можно получить доступ к любой сети любой организации, причем опасность значительно возрастает по той причине, что для взлома компьютера к нему вовсе не требуется физического доступа.

Согласно данным, полученным Институтом компьютерной безопасности (Computer Security Institute) в результате недавно проведенного исследования, у 70% организаций были взломаны системы сетевой защиты, кроме того, 60% выявленных попыток изломов исходили из внутренних сетей организаций.

Учитывая эти факты, можно с уверенностью сказать, что проблема безопасности сетей остается неразрешенной и на сегодняшний день, поскольку у подавляющего большинства компаний не решены вопросы обеспечения безопасности, в результате чего они несут финансовые убытки.

6.2.Основные определения безопасности сетей

Под термином объединенная сеть (internetwork) понимают множество подключенных друг к другу сетей. В объединенной сети создаются специальные области, каждая из которых предназначена для обработки и хранения определенной информации. Для разделения этих областей с целью обеспечения их безопасности используются специальные устройства, называемые брандмауэрами (firewall), или межсетевыми экранами. Бытует мнение о том, что брандмауэры предназначены для разделения закрытых сетей и сетей общего пользования, однако это не всегда так. Довольно часто брандмауэры используют и для разграничения сегментов закрытой сети.

В брандмауэрах предусмотрены, по меньшей мере, три интерфейса, хотя в более ранних реализациях использовались два. По этой причине, в настоящее время в брандмауэрах в основном используют всего два интерфейса из трех. В том случае, когда

используется брандмауэр с тремя установленными интерфейсами, имеется возможность создания трех разделенных сетевых зон. Ниже коротко описана каждая из этих зон.

- Внутренняя (inside) зона объединенной сети является доверительной зоной и предназначена для работы устройств закрытой сети. Эти устройства подчиняются определенной политике безопасности при работе с внешней сетью (например, Internet). Однако на практике довольно часто брандмауэр используется для разделения сегментов частей в доверительной зоне. Например, брандмауэром можно воспользоваться для отделения сети какого-то подразделения предприятия от общей сети.
- Внешняя (outside) зона объединенной сети является зоной с пониженным доверием. Основной функцией брандмауэра является защита устройств внутренней и демилитаризованной зон от устройств, находящихся во внешней зоне. Кроме того, при необходимости брандмауэр может быть настроен для безопасного выборочного доступа из внешней зоны к устройствам, находящимся в демилитаризованной зоне. В случае крайней необходимости брандмауэр может быть настроен для обеспечения доступа из внешней зоны во внутреннюю зону. Однако к этим действиям необходимо прибегать в исключительных случаях, поскольку доступ к внутренней зоне из внешней зоны таит гораздо больше угроз, чем доступ к изолированной демилитаризованной зоне.
- Демилитаризованная зона (Demilitarized zone — DMZ) — это изолированная сеть (или сети), которая обычно доступна пользователям из внешней сети. Брандмауэр должен быть сконфигурирован таким образом, чтобы обеспечивать доступ из внешней зоны во внутреннюю или демилитаризованную зону. Создание разрешений для доступа в демилитаризованную зону позволяет компании организовать безопасный доступ внешних пользователей к предоставляемой компанией информации и службам. Таким образом, эта зона позволяет работать с внешними пользователями без допуска их в безопасную внутреннюю зону.

Узлы, или серверы, которые входят в демилитаризованную зону, обычно называются бастионными узлами (bastion host). Здесь под бастионными понимаются узлы, на которых работают новые версии операционных систем и установлены все модули обновления. Использование бастионных узлов делает систему более устойчивой к взломам, поскольку производитель имеет возможность устранить ошибки и установить дополнения в приложении. Кроме того, бастионный узел отличается тем, что на нем выполняются лишь те службы, которые необходимы для работы приложения. Ненужные (и в некоторых случаях более опасные) службы отключаются или вообще удаляются с узла. На рисунке. 33 показана общая структура сети при использовании брандмауэра.

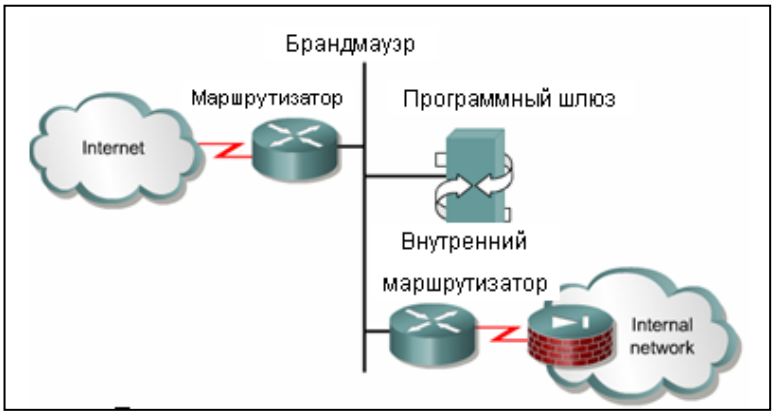


Рис 33. Общая структура сети при использовании брандмауэра

Брандмауэр должен обеспечивать следующие основные функции.

- Запрет доступа из внешней зоны во внутреннюю.
- Ограничение доступа из внешней зоны в демилитаризованную.
- Полный доступ из внутренней зоны во внешнюю.
- Ограничение доступа из внутренней зоны в демилитаризованную.

Однако в некоторых проектах сетей могут быть исключены отдельные или все пункты приведенного списка функций брандмауэра. Предположим, например, что нам необходимо обеспечить доставку SMTP-сообщений из внешней зоны во внутреннюю. Если в демилитаризованной зоне нет SMTP-сервера или средств для передачи SMTP-сообщений, необходимо обеспечить отправку SMTP-пакетов непосредственно на SMTP-сервер, который физически находится во внутренней зоне. В результате реализации подобного подхода безопасность работы в данной зоне значительно снизится.

Другим исключением может быть запрещение всего потока данных из внутренней зоны во внешнюю. Ограничения в использовании определенного приложения (порта) могут устанавливаться на уровне отдельных IP-адресов, подсетей или всей внутренней сети. Еще одним способом контролирования потока данных из внутренней сети во внешнюю является фильтрация по URL-адресам. Использование HTTP-фильтров, таких как WebSense, и другие исключения будут рассмотрены в следующих главах.

6.3. Категории угроз безопасности сетей

Существуют четыре категории угрозы безопасности сетей.

- **Бесструктурные угрозы**. Угрозы такого типа исходят в основном от отдельных лиц, использующих для взлома готовые инструменты, которые можно легко найти в Internet. Некоторые из них имеют злонамеренные цели, однако большинство являются обычными скриптоманами (script kiddies), которые производят взломы из чистого любопытства. Скриптоманы представляют серьезную угрозу для безопасности сетей. Очень часто они активизируют действия различных вирусов или "троянских коней", не подозревая обо всех разрушительных действиях, которые способны совершить эти программы. Иногда разрушительное действие вируса принимает всемирный размах, и убыток, принесенный этой программой, исчисляется миллионами долларов. Кроме того, в некоторых случаях автор вируса сам может стать его жертвой. Большинство бесструктурных угроз осуществляется только с целью проверки и испытания мастерства и опыта скриптоманов, однако из-за этих действий компании зачастую несут серьезные убытки. Например, при взломе внешнего Web-узла компании под угрозу попадают все направления ее деятельности. Даже если внешний Web-узел отделен от внутренней информационной структуры компании специальным брандмауэром, пользователи, которые захотят получить доступ к информации о компании, не смогут сделать этого. И поскольку все эти пользователи увидели, что Web-узел компании был взломан, то, скорее всего, они решат, что эта компания не является безопасным партнером по бизнесу.
- **Структурированные угрозы.** Такие угрозы представляют взломщики, которые имеют более серьезные намерения и более компетентны в области компьютерных технологий. Эти люди понимают принципы работы сетевых систем и хорошо разбираются в их изъянах. Они способны самостоятельно писать сценарии, предназначенные для взлома заранее определенных Web-узлов или сетей компаний. Как правило, подобным взломам подвергаются различные юридические учреждения с целью мошенничества или воровства.
- **Внешние угрозы**. Эти угрозы исходят от сторонних лиц или организаций, не имеющих официального доступа к компьютерным системам или сетям компании. Они получают доступ к сети компании через Internet или сервер удаленного доступа.

- **Внутренние угрозы**. эти угрозы представляют лица, имеющие доступ к внутренней сети компании (имеют учетную запись на сервере или физический доступ к компьютерной сети). Внутренние угрозы могут исходить от обиженного бывшего или работающего в компании постоянного или временного служащего. Во многих учебниках по сетевой безопасности отмечено, что большинство инцидентов нарушения безопасности в компании связано именно с внутренними угрозами.

6.4. Как нарушается безопасность сетей

Существуют три типа нарушений безопасности сетей.

- **Исследование сети** — попытка исследовать сеть и получить схему ее систем, служб и изъянов.
- **Взлом системы доступа** — взлом компьютерных сетей или систем с целью получения данных, доступа или персональных привилегий в системе.
- **Отказ в обслуживании** — взлом системы таким образом, чтобы авторизованные пользователи не смогли получить доступ к сети, системе или службам.

6.4.1.Исследование сети

Под исследованием сети подразумевается попытка определения неавторизованным пользователем ее структуры, служб, работающих в этой системе, и выявления возможных изъянов, с помощью технологии ping-прослушивания (ping sweep). Эти действия также иногда называют процессом сбора информации (information gathering), и в большинстве случаев этот процесс предшествует нарушению доступности системы, или DoS-взломам (Denial of Service attack — отказ в обслуживании).

Первым делом взломщик проверяет интересующую его сеть, чтобы выявить в ней активные IP-адреса. Получив эти данные, он может определить, какие службы работают на узлах с выявленными IP-адресами и какие порты они используют. Затем взломщик отсылает запросы на определенные порты для выяснения типа работающих приложений на активных IP-адресах. В результате он получает информацию о типе приложения и, может быть, даже информацию о типе и версии операционной системы.

Исследование сети похоже на сбор информации грабителем, который осматривает окрестные дома и выясняет, где отсутствуют хозяева и легко ли открываются двери и окна. И точно так же как грабитель, компьютерный взломщик может не воспользоваться обнаруженной брешью в системе защиты и взломать сеть позже, когда вероятность его обнаружения будет меньше.

6.4.2.Взлом системы доступа

Термин доступ (access) имеет довольно много значений и обычно обозначает свойство определенного источника (это может быть пользователь компьютера, соединенного с сетью, которая подсоединена к Internet) подсоединяться к определенному объекту (компьютер, который соединен с сетью, которая в свою очередь подсоединена к Internet). После того как определен объект взлома, взломщик пытается проникнуть в него с помощью специального программного обеспечения. Если взлом выполнен успешно, взломщик получает возможность без авторизации запрашивать данные и манипулировать ими, обращаться к системе или расширять свои полномочия. Взлом доступа может быть также использован для получения контроля над системой, что дает возможность установки и дальнейшей маскировки программного обеспечения, которое впоследствии может быть использовано для взлома.

6.4.3.Неавторизованное получение данных

Неавторизованное получение данных (unauthorized data retrieval) — это обычные операции чтения, записи, копирования или перемещения файлов, которые являются недоступными для неавторизованных пользователей. Достаточно часто встречаются общедоступные папки в системах Windows 9x или NT или NFS-экспортируемые каталоги в UNIX-системах с правом чтения или чтения и записи для любых пользователей. Неавторизованные пользователи могут без труда получить доступ к таким файлам, и достаточно часто оказывается, что легкодоступная информация является конфиденциальной, не предназначенной для посторонних глаз.

Неавторизованный доступ к системе

Взлом системы доступа позволяет пользователю получить доступ к системе без авторизации. Неавторизованный пользователь может получить доступ к системе несколькими путями. Так, некоторые системы могут не требовать при входе пароль, предоставляя тем самым анонимному пользователю простой доступ к системе. Для получения доступа к системам, в которых используются некоторые средства защиты, взломщик может воспользоваться изъянами в сценариях или программном обеспечении, которые выполняются в системе.

Кроме того, для получения неавторизованным пользователем доступа к системе он может воспользоваться уязвимыми местами в самой операционной системе. (Некоторые операционные системы были разработаны без учета требований к безопасности.) Эти изъяны, конечно же, могут быть исправлены в последующих версиях операционных

систем, но до тех пор, пока в системе не установлено обновление, ими может воспользоваться любой взломщик.

Неавторизованное расширение полномочий

К взломам подобного типа прибегают пользователи, имеющие ограниченный уровень доступа в системе. Неавторизованные пользователи, получившие непривилегированный доступ к системе, также могут воспользоваться подобными взломами. Целью данных взломов является получение информации или выполнение процедур, которые запрещены при данном уровне доступа. В большинстве случаев эти взломы позволяют получить права суперпользователя системы (root), установить программу, которая анализирует весь поток данных и обнаруживает учетные записи пользователей и соответствующие им пароли.

В некоторых случаях анонимные пользователи занимаются подобным взломом не для похищения информации, а для проверки своих интеллектуальных способностей, из-за любопытства или по незнанию того, что такие действия являются незаконными.

DoS-взломы

DoS-взломы предназначены для блокировки или повреждения функций компьютерной сети с целью воспрепятствовать ей в обслуживании внешних пользователей. Обычно подобные взломы приводят к крушению системы или замедлению ее работы до уровня, при котором дальнейшее обслуживание пользователей становится невозможным. При этом DoS-взлом может заключаться в уничтожении или повреждении жизненно важной информации, необходимой для работы компании. В большинстве случаев проведение такого взлома сводится к выполнению специальной программы или сценария, при этом злоумышленнику даже не требуется наличие доступа к взламываемой системе, достаточно знать лишь путь к ней. Получение этого пути может привести к серьезному DoS-взлому. Поскольку такие типы взломов реализуются достаточно просто и их легко осуществлять, оставаясь анонимным, они являются самыми распространенными в сети Internet.

Под понятием распределенного взлома, приводящего к отказу в обслуживании (Distributed Denial of Service — DDoS), понимают множество DoS-взломов, осуществляемых одновременно с многих компьютеров, что делает практически невозможным обнаружение и блокирование источников взлома.

Контрольные вопросы:

1. Укажите категории угроз безопасности?
2. Что такое демилитизированная зона?

3. Укажите примеры сетевых атак?
4. Какие инструменты используются в сети для обеспечения безопасности?
5. Какие задачи решает брандмауэр?
6. В случае обнаружения нарушения безопасности сети предприятия, укажите дальнейшие действия выполнямые для устранения угрозы?
7. Каким образом проверяется работа защиты сети предприятия

7. Политика безопасности сетей и ее обеспечение

Обеспечение безопасности компьютерных сетей является непрерывным процессом, обусловленным постоянным развитием и внедрением новых компьютерных технологий.

Поэтому любая политика безопасности в компьютерных системах должна строиться с учетом всех потенциальных угроз, существующих в области безопасности сетей.

В документе RFC 2196 Site Security Handbook сказано: "Политика безопасности — это набор строго определенных правил и формулировок, которые должны соблюдать лица, имеющие доступ к технологиям организации и информационным данным".

Политика безопасности должна решать следующие задачи.

- Идентификация защищаемых объектов организации. Определите, что вам необходимо защитить и как вы можете осуществить это. Выявление слабых мест в компьютерной сети и понимание того, как их могут использовать для взлома, поможет повысить уровень безопасности при работе в данной сети.
- Организация строгого учета защищаемых ресурсов. Изучите функционирование системы в нормальном режиме, какие устройства используются, какие потоки данных проходят в сети.
- Определение структуры сети с ее текущими схемами и устройствами. Продумайте безопасность сети и средства для ее обеспечения. Физический доступ пользователя к устройству может дать ему контроль над этим устройством.

Наиболее эффективной является непрерывно обновляющаяся политика безопасности, поскольку она обеспечивает постоянную проверку безопасности системы и обновляющиеся методы защиты. Последовательность процессов обеспечения безопасности можно представить в виде цикла обеспечения безопасности (Security Wheel). На рисунке 34 изображены четыре этапа цикла обеспечения безопасности.

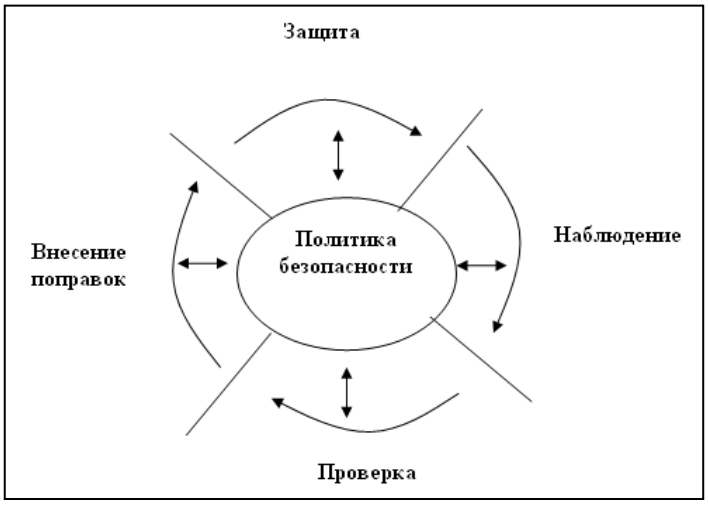


Рис 34. Цикл обеспечения безопасности компьютерной сети

Политика безопасности должна строиться на основе четырех этапов, из которых состоит цикл обеспечения безопасности.

Этап 1. Защита системы. Используйте следующие устройства и (или) системы, предотвращающие неправомочный доступ к сетевым системам.

(а) Системы идентификации и аутентификации (Identification Authentication System), такие как One-Time Password (OTP), обеспечивают средства аутентификации и авторизации пользователей. Примерами таких систем являются Cisco Secure Control Server (CSACS), Windows Dial-up Networking, S/Key, CryptoCard и SecurlD.

(б) Шифрование позволяет предотвратить перехват информации из потока данных неавторизованными пользователями. Стандартным протоколом шифрования при работе в Internet является IP Security (IPSec). Стандарт IPSec определен документом RFC 2401.

(в) Брандмауэры позволяют пропускать или блокировать поток данных, отфильтровывая только определенные типы потока данных.

(г) Устранение изъянов, существующих в системе, необходимо для предотвращения взломов, основанных на их использовании. Этот процесс подразумевает отключение на всех системах ненужных служб; чем меньше служб выполняется, тем тяжелее взломщикам получить доступ к системе.

(д) Физическая безопасность является очень важным элементом обеспечения безопасности компьютерных сетей, хотя довольно часто ей уделяют слишком мало внимания. Если злоумышленник имеет возможность физического похищения аппаратных средств, обеспечивающих работу сети, то решение всех остальных вопросов обеспечения безопасности становится просто бесполезным. Также необходимо запретить несанкционированную установку в сети различных устройств, которые могут быть использованы для похищения важных данных.

Этап 2. Анализ состояния потоков данных в сети на предмет нарушений и взломов, направленных против корпоративной политики безопасности. Источники нарушения безопасности могут находиться как внутри сети (например, обиженные служащие), так и за ее пределами (например, хакеры). Для предотвращения подобных нарушений политики безопасности сети используются специальные системы обнаружения вторжений, такие как Cisco Secure Instruction Detection System (CSIDS), которые позволяют обнаружить и предотвратить различные типы взломов. Кроме того, с помощью системы CSIDS можно проверить корректность настроек устройств, обеспечивающих безопасность, которые упоминались при описании первого этапа цикла обеспечения безопасности. Важной составляющей анализа состояния потоков данных в сети является протоколирование всех событий, произошедших в системе. Ведение протокола потока данных, который проходит в сети, поможет обнаружить действия злоумышленника на этапе сбора информации о сети и предотвратить взлом, который может блокировать всю работу сети.

Этап 3. Проверка эффективности средств обеспечения безопасности. У вас может быть очень сложная и дорогая система обеспечения безопасности сети, но если ее средства не

будут правильно настроены или будут работать некорректно, ваша сеть может быть легко взломана. Для проверки состояния безопасности сети может использоваться инструмент Cisco Secure Scanner.

Этап 4. Непрерывное совершенствование корпоративной политики безопасности. Собирайте и анализируйте всю информацию, полученную в результате анализа состояния потоков данных в сети, с целью повышения общего уровня безопасности.

Не следует забывать, что ежедневно обнаруживаются новые изъяны и угрозы безопасности сетей. Для того чтобы уровень безопасности вашей сети был максимально высоким, необходимо выполнить все четыре этапа — защита сети, анализ состояния потоков данных, тестирование и совершенствование политики безопасности. Все эти этапы должны постоянно сменять друг друга, а каждый новый цикл должен вносить качественные изменения в корпоративную политику безопасности.

8. Списки управления доступом

Сетевой администратор должен уметь запрещать несанкционированный доступ к сети и в то же время обязан обеспечить доступ к сети авторизированных пользователей. Несмотря на то, что средства безопасности, такие, как пароли, средства установления обратного вызова и физические устройства безопасности, достаточно полезны, им часто не хватает гибкости при фильтрации потока данных и специализированных управляющих средств, которые чаще всего предпочитают администраторы. Например, бывают ситуации, когда сетевой администратор готов предоставить пользователям локальной сети выход в сеть Internet, но при этом не хочет разрешать пользователям сети Internet, находящимся вне такой локальной сети, входить в сеть предприятия средствами протокола telnet.

Маршрутизаторы предоставляют администраторам основные возможности фильтрации, такие, как блокирование потока данных из сети Internet с использованием списков управления доступом (Access Control List— ACL). Список управления доступом представляет собой последовательный набор разрешающих или запрещающих директив, которые относятся к адресам или протоколам верхнего уровня.

Для создания списков управления доступом существует множество причин; некоторые из них перечислены ниже.

- Списки ACL можно использовать для ограничения потока данных в сети и повышения ее производительности. В частности, списки могут быть использованы для того, чтобы некоторые пакеты какого-либо протокола обрабатывались маршрутизатором ранее других. Такая функция называется установкой очередности (queuing) и используется для того, чтобы маршрутизатор не обрабатывал пакеты, которые в данный момент не являются жизненно

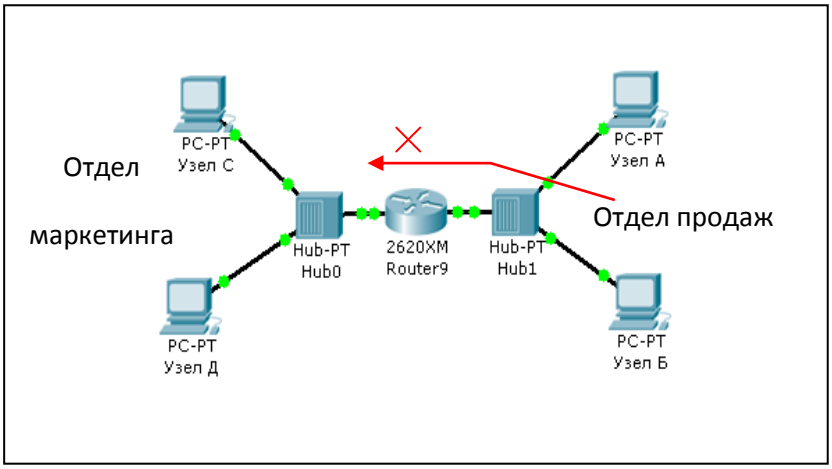


Рис 35.Пример ограниченного сетевого трафика

необходимыми. Установка пакетов в очередь ограничивает поток данных в сети и уменьшает вероятность перегрузки.

- Списки ACL можно использовать для управления потоком данных. Например, с помощью списков можно ограничить или уменьшить количество сообщений об изменениях в сети.

  Такие ограничения используются для предотвращения распространения информации об отдельных сетях на всю сеть. Списки ACL можно использовать для обеспечения базового уровня защиты от несанкционированного доступа. Например, списки доступа позволяют разрешить одному узлу доступ к некоторому сегменту сети, а другому закрыть доступ к этой же области. На рисунке 35 показано, что узлу А разрешен доступ к сети пользователей, а узлу Б такой доступ запрещен. Если на маршрутизаторе не установлен список управления доступом, то все пакеты, проходящие через него, поступают во все сегменты сети.

- Списки ACL можно использовать для указания данных, которые будут направляться далее или блокироваться на интерфейсе маршрутизатора. Например, можно разрешить маршрутизацию трафика электронной почты и в то же время заблокировать весь поток данных протокола telnet.

8.1. Принцип работы списков управления доступом

Список управления доступом представляет собой набор директив, которые определяют то, как пакеты

- поступают на входной интерфейс маршрутизатора,
- доставляются внутри маршрутизатора,
- пересылаются далее через выходной интерфейс маршрутизатора.

Начальная стадия процесса установления связи не зависит от того, используются ли списки управления доступом или нет (рис. 36). Когда пакет поступает на интерфейс, маршрутизатор определяет, куда его направить — на

Рис 36. Принцип работы списков управления доступом

маршрутизатор или на мост (т.е. являются ли пакеты маршрутизируемыми или коммутируемыми). Если пакет по какой-либо причине не может быть обработан маршрутизатором или мостом, он отбрасывается. Далее операционная система проверяет, связан ли со входным интерфейсом какой-либо список доступа. Если список есть, то операционная система сверяет параметры пакета с записями такого списка ACL. Если пакет соответствует разрешающему правилу и подвергается маршрутизации, то в таблице маршрутизации выполняется поиск сети-получателя, определяется метрика маршрута или состояние и интерфейс, через который следует отправить пакет. Список управления доступом не фильтрует пакеты, которые возникают внутри маршрутизатора, но фильтрует пакеты из иных источников.

Далее маршрутизатор проверяет, находится ли интерфейс получателя в группе списка управления доступом. Если его там нет, то пакет может быть направлен на интерфейс получателя непосредственно; например, при использовании интерфейса E0, который не связан со списками управления доступом, пакет отправляется непосредственно через такой интерфейс.

Директивы списка исполняются в последовательном логическом порядке. Если заголовок пакета соответствует директиве списка, то остальные директивы пропускаются. Если условие директивы выполнено, пакет передается далее или отбрасывается в соответствии с конфигурацией. Если заголовок пакета не соответствует ни одной директиве списка, то к нему применяется стандартное правило, размещенное в конце списка, которое запрещает передачу любых пакетов. Даже если такая директива не отображается в последней строке списка управления доступом, она стандартно там присутствует.

Списки ACL позволяют контролировать, каким пользователям разрешен доступ к конкретной сети. Условия в списке контроля доступа позволяют:

- просмотреть адреса определенных узлов для того, чтобы разрешить или заблокировать им доступ к некоторой части сети;
- разрешить или запретить доступ пользователям только к определенным видам приложений, таким, как службы FTP и HTTP.

8.2. Конфигурирование списков управления доступом

Списки ACL создаются в режиме глобальной конфигурации устройства. Существует великое множество разных типов списков управления доступом: стандартные, расширенные, списки протокола IPX, списки AppleTalk и многие другие. При создании списков ACL в маршрутизаторе каждому списку следует назначить уникальный номер.

Такой номер идентифицирует тип списка и не должен выходить за границы диапазона номеров, который выделен для определенной разновидности списков.

После того как администратор переводит режим командной строки в нужный и принято решение о том, из какого диапазона следует выбрать номер списка, он последовательно вводит директивы списка ACL, начиная с ключевого слова access-list и заканчивая правильными параметрами, как показано на рисунке 37. Создание списка управления доступом — это только половина дела. Вторая, и не менее важная часть процесса, — это привязка списка к интерфейсу.

```
access-list 1 permit 5.6.0.0 0.0.255.255
access-list 1 deny 7.9.0.0 0.0.255.255


access-list 2 permit 1.2.3.4

access-list 2 deny 1.2.0.0 0.0.255.255
```

Рис 37. Пример конфигурирования списков управления доступом

```
interface ethernet 0
```

Списки ACL могут быть привязаны к одному и более интерфейсам и могут фильтровать как входные, так и выходные потоки данных. Привязка списка к интерфейсу (интерфейсам) осуществляется посредством команды **access-group** (рисунок 37). Команда **access-group** вводится в режиме конфигурирования интерфейса. Список управления доступом привязывается к интерфейсу во входном или выходном направлении: для входящего или исходящего трафика. Чтобы определить, в каком направлении должен воздействовать список ACL на проходящие через интерфейс потоки данных, следует "взглянуть на интерфейс изнутри маршрутизатора", т.е. представить себе, что вы находитесь внутри устройства. Такой подход поможет разобраться в потоках трафика во многих ситуациях, когда необходимо понять, какие потоки данных в каком направлении передаются. С точки зрения "наблюдателя внутри маршрутизатора", трафик, который входит из внешнего мира внутрь устройства через интерфейс, может быть отфильтрован входным списком управления доступом; соответственно, поток данных, который направлен из устройства во внешнюю сеть через интерфейс, может быть отфильтрован выходным списком. После того как нумерованный список ACL создан, его следует привязать к нужному интерфейсу. Чтобы изменить порядок следования директив в нумерованном списке управления доступом, необходимо удалить весь список с помощью команды **no access-list** номер списка и создать его заново.

На практике команды списков управления доступом представляют собой длинные символьные строки. Основные задачи, решение которых описано в этом разделе, включают в себя следующие действия:

- необходимо сконфигурировать список управления доступом в режиме глобальной конфигурации маршрутизатора;
- следует назначить номер списку управления доступом в диапазоне от 1 до 99, если требуется создать стандартный список для протокола IP;
- следует назначить номер списку управления доступом в диапазоне от 100 до 199, если требуется создать расширенный список ACL для протокола IP;
- при создании списка ACL необходимо тщательно отбирать необходимые директивы и соблюдать их логическую последовательность. В списке должны быть указаны разрешенные IP-протоколы; все данные других протоколов должны быть запрещены;
- необходимо выбрать IP-протоколы, которые следует проверять; все остальные протоколы проверяться не будут. В дальнейшем для большей точности можно будет также указать порт получателя;
- после того как будет создан необходимый список контроля доступа, его следует привязать к определенному интерфейсу.

Несмотря на то, что каждый протокол выдвигает свои специфические требования и правила, выполнение которых необходимо для фильтрации трафика, в целом создание списков управления доступом требует выполнения всего двух основных действий, которые указаны ниже.

Этап 1. Создать список доступа ACL.

Этап 2. Применить список доступа на конкретном интерфейсе.

Списки управления доступом применяются к одному или нескольким интерфейсам и выполняют фильтрацию входящих или исходящих потоков данных, в зависимости от установленной конфигурации. Списки для исходящего трафика обычно более эффективны, поэтому предпочтительнее использовать именно их. Маршрутизатор, в котором сконфигурирован список ACL для входящего трафика, должен проверять каждый пакет на его соответствие условиям списка перед тем, как отправить пакет на выходной интерфейс.

8.3. Стандартные списки ACL

Стандартный список управления доступом позволяет проверять и сравнивать адреса отправителей пакетов с директивами, как показано на рисунке 38.

Стандартные списки управления доступом используются тогда, когда необходимо заблокировать или разрешить доступ всему набору протоколов на основании адреса сети, подсети или узла.

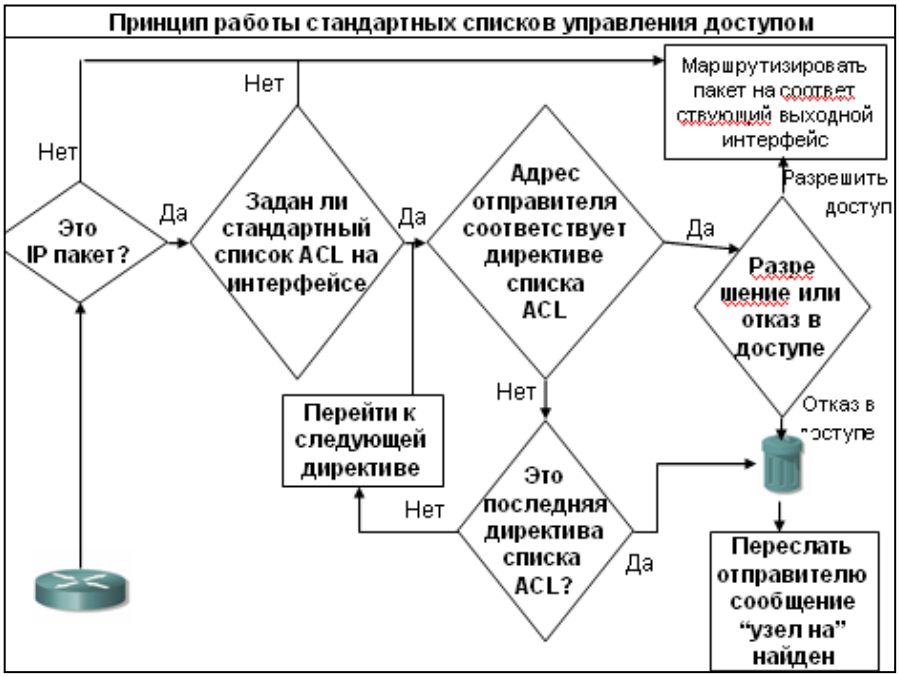


Рис 38. Принцип работы стандартных списков управления доступом

Например, для пакетов, поступивших на интерфейс E0 проверяются адреса отправителя и протоколы. Затем они сравниваются с директивами списка управления доступа. Если соответствие найдено, выполняется указанное действие (разрешение или запрет). Если пакеты соответствуют разрешающему правилу (permit), они перенаправляются через маршрутизатор к выходному интерфейсу, который логически связан со списком управления доступом. Если же пакеты соответствуют запрещающему правилу (deny), они отбрасываются.

Полный синтаксис директивы стандартного списка ACL имеет вид:

Router(config)#access-list *access-list-number {permit|deny|remark}* **source** *[source-wildcart] [***log***]*

Ключевое слово remark используется для внесения в список комментария, который впоследствии поможет разобраться в списке управления доступом. Длина такой строки-комментария не может превышать ста символов.

Например, тяжело сказать, для чего именно нужна такая запись:

access-list 1 permit 171.69.2.88

Если же в списке управления доступом присутствует комментарий, то разобраться, к чему именно относится определенная директива, будет значительно проще.

access-list 1 remark Permit only Howard workstation though ACL 1 171.69.2.88

access-list 1 permit 171.69.2.88

Для удаления стандартного списка управления доступом используется форма этой команды с ключевым словом no:

Router(config)# no access-list number

Стандартная версия команды **access-list** списка доступа в режиме глобальной конфигурации задает стандартный список управления доступом с номером в диапазоне от 1 до 99. В На рисунке 39 показан стандартный список доступа, который содержит 4 директивы; все директивы входят в список доступа с номером 2. Следует помнить, что даже если пакеты не отвечают ни одному из правил (т.е. записям или директивам) списка доступа, они попадают под неявное правило в конце списка доступа ACL, которое запрещает передачу всех пакетов (это правило не отображается в конфигурации).

```
access-list  2  deny  172.16.1.1
access-list  2  permit  192.168.1.0   0.0.0.255
access-list  2   deny  172.16.0.0   0.0.255.255
```

Рис 39. Принцип конфигурирования стандартных списков управления доступом

В первой строке списка управления доступом указано, что инвертированная маска не используется. В подобной ситуации, когда не указана маска, используется инвертированная маска со стандартным значением 0.0.0.0. Данная директива списка ACL запретит доступ с одного IP-адреса — 172.16.1.1.

Вторая строка разрешает доступ с адресов из сети 192.168.1.0, т.е. с любого адреса, который начинается с комбинации 192.168.1.

Третья строка-директива запрещает доступ из сети 172.16.0.0, а четвертая разрешает передавать пакеты с любого адреса, который начинается с 10., т.е. из сети 10.0.0.0.

Команда **ip access-group** используется для привязки созданного списка управления доступом к интерфейсу. Для каждого порта, протокола и направления допускается использовать только один список. Команда имеет следуюший формат:

Router (config) # ip access-group номер списка {in | out}

8.4. Расширенные списки управления доступом

Расширенные списки управления доступом (extended access control list— extended ACL) используются чаще, чем стандартные, поскольку они обеспечивают большие возможности контроля. Расширенный список управления доступом проверяет как адрес отправителя, так и адрес получателя. Список может также проверять конкретные протоколы, номера портов и другие параметры. Процесс обработки трафика маршрутизатором для проверки пакетов на соответствие правилам расширенных списков управления доступом проиллюстрирован на рисунке. 40.

Отправка пакета может быть разрешена или же может быть отказано в передаче в зависимости от того, откуда был переслан пакет и куда направлен, какой протокол, адрес порта и тип приложения при этом были использованы. Расширенные списки управления доступом, например, позволяют пересылать трафик электронной почты из интерфейса Fa0/0 в интерфейс S0/0 и в то же время могут запрещать передачу файлов и потоки данных от Web-сайтов. Когда маршрутизатор уничтожает пакеты, некоторые протоколы посылают эхо-сообщения отправителю, уведомляющие, что получатель недоступен.

Рис 40. Принцип работы расширенного списка управления доступом

Расширенные списки управления позволяют более точно контролировать и управлять пакетами, нежели стандартные. Стандартные списки управления доступом предназначены для того, чтобы запрещать весь набор или стек протоколов; расширенные списки позволяют точно указать, какой из протоколов необходимо разрешить или запретить. Например, с помощью такого списка ACL можно разрешить трафик HTTP, но запретить доступ к ресурсам по протоколу FTP.

Полный формат команды **access-list** для расширенного списка контроля доступа имеет следующий вид:

***Router(config-if)#*access-list** access-list-number **[dynamic** dynamic-name**]** **[timeout** minutes**]]** **{permit|deny}** protocol source **[**source-wildcart destination destination-wildcart**]** **[precedence** precedence **]** **[tos** tos**]** **[log|log-input]** **[time-range** time-range-name**]** **established** **[fragments]**

Ключевое слово no в начале команды используется для удаления расширенного списка управления доступом. Например, чтобы удалить список, следует ввести команду с параметром **no** в начале:

Router(config)# no access-list access-list-number

В одном списке управления доступом может быть указано несколько директив. Каждая из записей списка должна содержать один и тот же номер списка доступа, чтобы относиться к одному и тому же списку, как показано на рисунке 41. В одном списке управления доступом может быть указано столько директив, сколько требуется. Количество директив ограничено только доступной памятью маршрутизатора. Чем больше записей содержится в каждом списке управления доступом, тем сложнее будет поддерживать и управлять списками ACL в маршрутизаторе. На рисунке 41 используются три последовательные директивы, которые указывают, что telnet-, ftp-пакеты и пакеты данных протокола FTP разрешено передавать от любых узлов подсети 172.16.6.0 в любую сеть.

Рис 41. Пример конфигурирования расширенного списка управления

```
access-list  114  permit  tcp  172.16.6.0  0.0.0.255  any eq  telnet
access-list  114  permit  tcp  172.16.6.0  0.0.0.255  any eq  ftp
```

Расширенные списки управления доступом являются практически универсальным инструментом и, по существу, позволяют использовать практически любые опции и параметры, которые характерны для любого используемого протокола. Порядок следования записей в списке может быть различным и зависит от используемого протокола.

Контрольные вопросы:

1. Укажите типы списков контроля доступа?
2. Какие задачи позволяют решить списки контроля доступа?
3. Укажите принцип работы стандартного списка контроля доступа?
4. Укажите принцип работы расширенного списка контроля доступа?
5. Укажите принцип определения месторасположения и применения списков контроля доступа?
6. Списки контроля доступа позволяют анализировать данные передаваемые в пакетах?
7. На каких сетевых устройствах возможно использование списков контроля доступа?

8. Укажите максимальное количество списков контроля доступа, которые можно применить к одному интерфейсу
9. Какие действия нат трафиком могут осуществлять списки контроля доступа?
10. Каким образом редактируются списки контроля доступа при необходимости внесения изменения в них?

9. Преобразование сетевых адресов (NAT) и адресов портов (PAT)

NAT — это протокол, который допускает преобразование внутреннего IP-адреса, используемого в локальной сетевой среде, в адрес внешней сетевой среды, и наоборот. Есть много оснований для применения NAT в сетевой среде. Среди преимуществ NAT выделяются следующие:

- Возможность использования частной сетью незарегистрированных IP-адресов для доступа к внешней сети, например, Интернет.
- Возможность повторного применения выделенных IP-адресов, которые уже используются в Интернете.
- Обеспечение связи с Интернетом в сетях, где недостаточно зарегистрированных индивидуальных IP-адресов.
- Правильное преобразование адресов в двух объединенных интрасетях, например в сетях двух слившихся компаний.
- Перевод внутренних IP-адресов, выделенных старыми Интернет-провайдерами, в недавно выделенные адреса нового провайдера без ручной настройки локальных сетевых интерфейсов.

9.1. Терминология NAT

Внутренняя сеть (Inside network) Это набор сетевых адресов, которые будут преобразовываться. Используемые внутри сети IP-адреса недействительны во внешней сети, например в сети Интернет или в сети провайдера.

Часто IP- адреса, используемые внутри сети, являются устаревшими, или же подпадают под действие спецификации RFC 1918, которая резервирует определенные IP-адреса для особого применения.

Внешняя сеть (Outside network) Это сеть, не находящаяся в собственности организации, которой принадлежит внутренняя сеть, а также ее филиалов. Это может быть сеть другой компании, когда происходит слияние двух предприятий, но обычно это сеть Интернет-провайдера. Адреса, используемые в этой сети, являются законно зарегистрированными.

Слияние сетевых комппексов двух предприятий, что иногда происходит с корпоративными слияниями при использовании протокола NAT, называют "многоярусными NAT".

Внутренний локальный IP-адрес (Inside local IP address) IP-адрес, выделенный интерфейсу внутренней сети. Этот адрес не может использоваться в Интернете, или же он

сразу определен спецификацией RFC 1918 как неиспользуемый в Интернете. Данный адрес не подлежит глобальной маршрутизации. Если адрес глобально маршрутизируемый, он скорее всего выделен другой организацией и не может использоваться в Интернете.

Внутренний глобальный IP-адрес (Inside global IP address) IP-адрес внутреннего узла после его преобразования с помощью NAT, каким он представляется интерфейсам внешних сетей. Этот адрес можно использовать во внешней сети или в Интернете.

Простая запись преобразования (Simple translation entry) Запись в таблице NAT, в которой маршрутизатор NAT сопоставляет не имеющий законной силы внутренний IP-адрес с глобально направляемым IP-адресом, последний официально зарегистрирован для использования в Интернете.

Расширенная запись преобразования (Extended translation entry) Это запись в таблице NAT, которая сопоставляет пару из IP-адреса и порта с внутренним IP-адресом.

9.2. Принцип работы NAT

NAT настраивается на маршрутизаторе или маршрутном процессоре, ближайшем к границе ответвления, между внутренней сетью (локальной сетью) и внешней сетью (общедоступной сетью, например сетью Интернет-провайдера или Интернета). Внешней сетью может быть также сеть другой компании, например, при слиянии двух сетей после поглощения (см. рис. 42). Обратите внимание, что маршрутизатор разделяет внутреннюю и внешнюю сеть. NAT переводит внутренние, локальные адреса в глобально уникальные IP-адреса. Таким образом, данные могут переходить во внешнюю сеть.

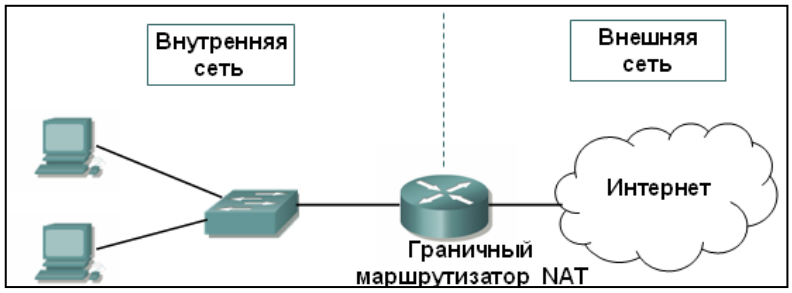


Рис 42. Маршрутизатор NAT на границе

Протокол NAT учитывает, что немногие люди пользуются внешней сетью в определенный момент времени. Применяется коммутации процессов для изменения адреса источника исходящих пакетов и направления их обратно соответствующему маршрутизатору. Потребляется меньше IP-адресов, чем узлов внутри сети. Перед применением протокола NAT на всех корпоративных маршрутизаторах Cisco, единственным способом реализации этих функций было использование сквозных шлюзов брандмауэров.

9.2.1. Преимущества NAT

Применение NAT имеет много плюсов. Если необходимо изменить внутренние адреса - из-за смены провайдера или слияния с другой компанией,- NAT позволяет переводить адреса из одной сети в другую.

- NAT позволяет наращивать или сокращать зарегистрированное адресное пространство IP, не изменяя узлы, коммутаторы или маршрутизаторы сети. (Исключение составляют граничные маршрутизаторы NAT, соединяющие внутренние и внешние сети.)
- NAT может применяться статически или динамически.
    - Статическое преобразование — это ввод IP-адресов в таблицу адресов вручную. Обозначенный адрес внутренней сети использует для доступа к внешней сети IP-адрес, вручную заданный администратором сети.
    - Динамические сопоставления позволяют администратору задавать один и более пулов зарегистрированных адресов на граничном маршрутизаторе NAT. Адреса пулов могут использоваться узлами внутренней сети для доступа к узлам внешней сети. Таким образом, несколько внутренних узлов могут пользоваться одним IP-адресом.
- NAT распределяет обработку пакетов между маршрутизаторами с помощью функции распределения нагрузки протокола TCP. Распределение нагрузки NAT может производиться посредством одного внешнего адреса, сопоставленного с внутренним адресом маршрутизатора. Этот циклический подход используется с несколькими маршрутизаторами. Между ними распределяются входящие соединения. Каждое отдельное соединение можно настроить так, чтобы оно использовало один отдельный маршрутизатор.

9.2.2. Недостатки NAT

Расскажем о недостатках применения NAT:

- NAT увеличивает сетевую задержку. Задержки происходят на маршрутах коммутации из-за большого количества трансляций каждого IP-адреса, содержащегося в заголовках пакетов. CPU маршрутизатора используется для обработки каждого пакета, чтобы определить, следует ли маршрутизатору переводить и изменять заголовок IP.
- NAT скрывает IP-адреса от точки к точке. В связи с этим нельзя использовать некоторые приложения. Данные приложений, которые требуют использования

физических адресов, а не полного домена имени, не дойдут до назначения, когда NAT транслирует IP- адреса через граничный маршрутизатор NAT.

- Так как NAT изменяет IP-адрес, происходит потеря трассируемости IP от точки к точке. Изменения адресов многочисленных пакетов приводят в замешательство отслеживающие программы IP. В то же время это является преимуществом с точки зрения безопасности: уменьшаются шансы хакеров определить источник пакета.

9.2.3. Функции NAT

Знание функционирования протокола NAT в той или иной конфигурации поможет принимать верные решения по настройке. В этом разделе рассматриваются действия NAT при его настройке для выполнения следующих задач:

- Преобразование внутренних локальных адресов
- Совмещение внутренних глобальных адресов
- Применение распределения нагрузки TCP
- Перекрытие сетей

9.3. Преобразование внутренних локальных адресов

NAT действует на маршрутизаторе и обычно соединяет две сети. Протокол NAT переводит локальные недопустимые для использования в Интернете IP-адреса в законные, зарегистрированные IP-адреса перед перемещением пакетов из локальной сети в Интернет или в другую внешнюю сеть. Для этого NAT осуществляет четырехступенчатый процесс (см. рис. 43). Рассмотрим этапы процесса, показанного на рис. 43.

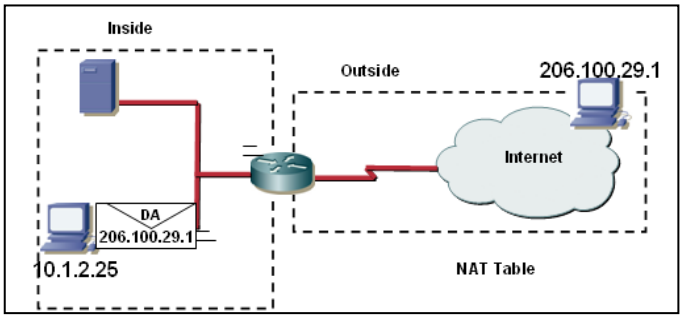


Рис 43. Преобразование внутренних локальных адресов

1. Пользователь 10.1.2.25 посылает пакет и пытается установить соединение с сетью 206.100.29.1

2. Когда на граничный маршрутизатор NAT приходит первый пакет, маршрутизатор проверяет, есть ли запись адреса источника, который совпадает с адресом в таблице.

3. Если в таблице NAT запись адреса источника совпадает с адресом в таблице, начинается этап 4. Если соответствие не находится, маршрутизатор NAT использует простую запись из своего пула зарегистрированных Интернет-адресов. Простая запись происходит тогда, когда маршрутизатор NAT сопоставляет незаконный внутренний IP-адрес с зарегистрированным законным, допустимым IP-адресом Интернета. В данном примере маршрутизатор NAT сопоставляет адрес 10.1.2.25 с адресом 200.1.1.25.

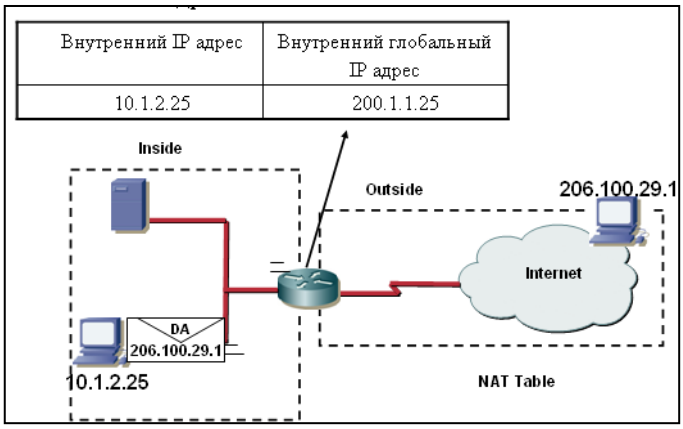


Рис 44. Преобразование внутреннего локального адреса в внутренний глобальный адрес

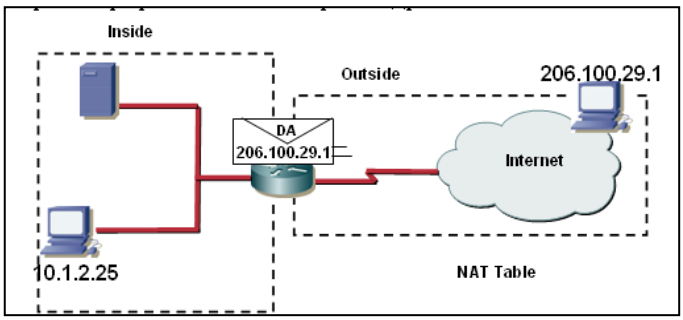


Рис 45. При получении пакета от 206.100.29.1 выполняется обратное преобразование

4. Граничный маршрутизатор NAT меняет локальный незаконный адрес 10.1.2.25 (записанный как исходный адрес пакета) на адрес 200.1.1.25. Для узла назначения IP-адрес отправляющего узла представляется как 200.1.1.25.

5. Когда в Интернете используется узел с IP-адресом 206.100.29.1, он приводит в качестве конечного адреса выделенный маршрутизатором NAT IP-адрес 200.1.1.25.

6. Когда граничный маршрутизатор NAT получает ответ от 206.100.29.1 с пакетом, предназначенным для 200.1.1.25, он снова проверяет свою таблицу NAT. Таблица показывает, что внутренний адрес 10.1.2.25 должен получить пакет, предназначенный для 200.1.1.25, и заменяет адрес назначения на IP-адрес внутреннего интерфейса.

Действия 2-6 повторяются для каждого пакета.

9.4. Совмещение внутренних глобальных адресов

Если разрешить маршрутизатору использовать один глобальный адрес для многих локальных адресов, можно сэкономить адреса пула внутренних глобальных адресов. Когда включено совмещение NAT, маршрутизатор поддерживает в таблице NAT сведения протокола высшего уровня для номеров портов TCP и UDP, чтобы переводить глобальный адрес обратно в нужный внутренний, локальный адрес. Когда несколько локальных адресов соответствуют одному глобальному адресу, NAT использует номер порта TCP

или UDP каждого внутреннего узла. Таким образом, создается уникальный адрес внутренней сети.

На рисунке 46 показана работа NAT, когда один внутренний глобальный адрес представляет несколько внутренних локальных адресов. Номер порта TCP - это часть сетевого адреса, которая отличает его от других адресов данной сети.

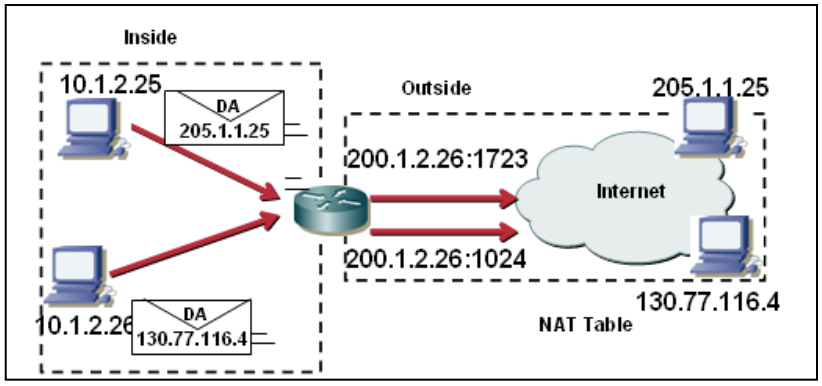


Рис 46. Совмещение внутренних глобальных адресов

Когда маршрутизатор обрабатывает несколько немаршрутизируемых внутренних IP-адресов в один глобально маршрутизируемый внешний IP-адрес, он производит следующие действия для совмещения внутренних глобальных адресов:

1. Пользователь с внутренним адресом 10.1.2.25 начинает соединение с узлом 205.1.1.25.

2. Первый пакет, который получает граничный маршрутизатор NAT от узла с адресом 10.1.2.25, заставляет маршрутизатор проверить свою таблицу NAT. Далее маршрутизатор определяет, что необходимо транслировать адрес 10.1.2.25, и настраивает перевод во внутренний глобальный адрес 200.1.2.25. Если совмещение включено и активно другое преобразование, маршрутизатор использует глобальный адрес этого преобразования и сохраняет необходимые сведения для обратного преобразования. Такая запись называется расширенной.

3. Маршрутизатор меняет внутренний локальный исходный адрес 10.1.2.25 на выбранный глобально маршрутизируемый адрес и уникальный номер порта и пересылает пакет. В данном примере исходный адрес в таблице NAT-200.1.2.26:1723.

4. Узел 205.1.1.25 получает пакет и отвечает узлу 10.1.2.25. Он использует внутренний глобальный IP-адрес в поле исходного адреса полученного пакета (200.1.2.26).

5. Граничный маршрутизатор NAT получает пакет от узла 205.1.1.25. Затем он просматривает таблицу NAT, используя протокол, внутренний глобальный адрес и порт, переводя внешний адрес порта в текущий адрес назначения 10.1.2.25. Затем граничный маршрутизатор NAT пересылает пакет узлу, используя IP-адрес 10.1.2.25 внутренней сети. Действия 2-5 продолжаются в ходе всей последующей связи до разрыва соединения.

Узлы с IP-адресом 205.1.1.25 и с 130.77.116.4 считают, что связываются с одним узлом по адресу 200.1.2.26. На самом деле они объединяются с разными узлами, где номер порта

позволяет их отличать граничному маршрутизатору NAT, чтобы пересылать пакеты нужному узлу. Схема адресации портов допускает одновременное использование одного внутреннего глобального IP- адреса примерно 4000 разными узлами, благодаря многочисленным имеющимся номерам портов TCP и UDP.

9.5. Применение распределения нагрузки TCP

Распределение нагрузки TCP - это динамический способ преобразования целевых IP-адресов. Его можно применить для сопоставления определенного трафика внешней сети с допустимым трафиком внутренней сети, предназначенным более чем для одного узла. После создания структуры сопоставления целевые IP-адреса, имеющие соответствия в списке доступа, меняются на адрес из вращательного пула по циклической схеме.

Когда создается новое соединение из внешней сети с внутренней сетью, весь не относящийся к TCP трафик проходит без преобразования, если только к интерфейсам не применен другой вид трансляции. На рисунке 47 показано распределение нагрузки TCP.

Рассмотрим, как NAT сопоставляет один виртуальный узел с несколькими настоящими узлами.

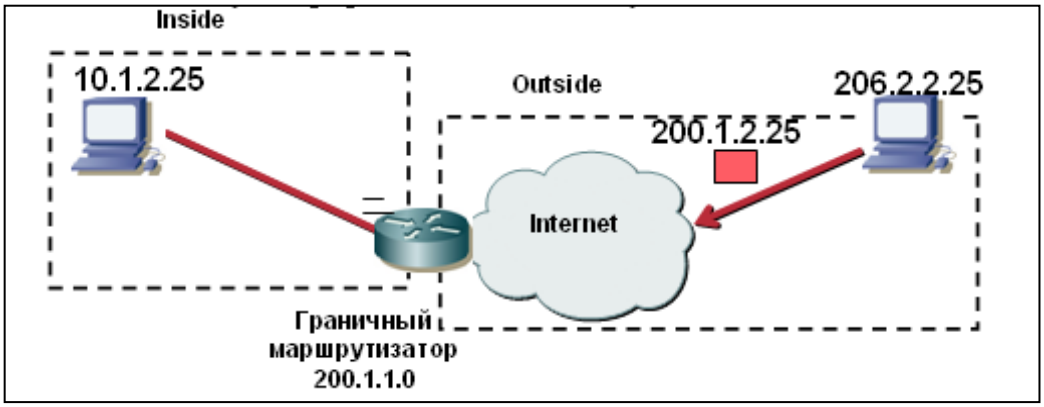


Рис 47. Применение распределения нагрузки TCP

1. На рис. 47 ПК с глобальным IP-адресом 200.1.1.25 начинает соединение TCP с виртуальным узлом по адресу 10.1.2.25.

2. Граничный маршрутизатор NAT получает запрос на новое соединение и создает новую трансляцию, отводя соседний настоящий узел 10.1.2.25 для внутреннего локального IP-адреса и добавляя эту информацию в таблицу NAT.

3. Граничный маршрутизатор NAT меняет адрес назначения на выбранный IP-адрес настоящего узла и пересылает пакет.

4. Настоящий узел по IP-адресу 10.1.2.25 получает пакет и отвечает граничному маршрутизатору NAT.

5. Граничный маршрутизатор NAT получает пакет и еще раз просматривает таблицу NAT, используя внутренний локальный IP-адрес и номер порта, а также внешний IP-адрес

и номер порта в качестве ключа. Граничный маршрутизатор NAT переводит адрес источника в адрес виртуального узла и пересылает пакет.

6. При следующем запросе на соединение граничный маршрутизатор отводит 10.1.2.26 для внутреннего локального адреса.

9.6. Перекрытие сетей

Предположим, сеть использует структуру адресации IP, которая является допустимой и может применяться глобально. Но допустим еще, что ее использует другая организация или что вы потеряли право ее использовать. Интернет-провайдер же считает, что вы никуда от него не денетесь, потому что он предоставляет вашу структуру адресации IP, и вдруг удваивает счета. Вместо того чтобы платить больше, вы переходите к другому провайдеру с другой областью адресов IP.

Вы нашли провайдер, который может предоставить отличную скорость доступа к Интернету. Кроме того, он в три раза дешевле бывшего провайдера. К сожалению, он предоставит вам и новую структуру IP-адресов, которую нужно применить к своей сети. Даже в сети среднего размера на изменение структуры IP-адресов уйдет несколько часов — такая задержка сильно затронет пользователей. Рекомендуем вам использовать преобразование адресов NAT с перекрытием.

Вы узнаете, как переводить IP-адреса, не допустимые для использования во внешней сети, например Интернете, и как переводить их в новые официально выделенные IP-адреса от провайдера. Здесь рассматриваются только действия NAT по преобразованию перекрывающихся адресов. Настройка перекрывающихся адресов описана далее в этой главе.

При преобразовании перекрывающихся адресов производятся следующие действия.

1. Узел внутренней сети инициирует соединение с узлом внешней сети с помощью полного доменного имени, запрашивая преобразование имя-адрес на сервере доменных имен Интернета DNS.

2. Граничный маршрутизатор NAT принимает ответ сервера DNS и начинает процесс преобразования с выданным адресом, если есть перекрывающийся адрес, используемый в сети неофициально.

3. Для перевода возвращенного адреса граничный маршрутизатор создает простую запись преобразования. Она сопоставляет перекрывающийся незаконный внутренний адрес с адресом из пула адресов, которые могут законно использоваться во внешней сети.

4. Граничный маршрутизатор NAT меняет адрес источника на новый внутренний глобальный адрес, а адрес назначения на внешний глобальный адрес и пересылает пакет.

5. Узел внешней сети получает пакет и продолжает диалог.

6. Для каждого пакета, полученного между внутренним и внешним узлами, маршрутизатор производит просмотр таблицы NAT, меняет адрес назначения на внутренний локальный адрес и исходный адрес на внешний локальный адрес.

9.7. Настройка статического преобразования сетевых адресов

Прежде, чем приступить к настройке NAT, на маршрутизаторе следует включить маршрутизацию IP и на каждом интерфейсе задать правильные IP-адреса и маски подсети. Начнем процесс в режиме глобальной настройки. Предположим, что у нас есть лишь один интерфейс на маршрутизаторе, подключенном к внутренней сети. В этом примере необходим доступ к данным Интернета компьютеру, использующему незаконный внутренний IP- адрес 10.1.2.25. Настроим граничный маршрутизатор NAT так, чтобы при получении пакета, выделенного внешней сетью от IP-адреса 10.1.2.25, он переводил адрес источника в допустимый адрес 200.1.1.25. Выполните такую команду:

Router (config)# ip nat inside source static 10.1.2.25 200.1.1.25

Чтобы включить NAT, сначала выберите интерфейс, соединяющий внутреннюю сеть с маршрутизатором или внешним маршрутным процессором. На маршрутизаторе находится один интерфейс, подключенный к внутренней сети, и один интерфейс, подключенный к внешней сети. Необходимо определить их и включить на обоих трансляцию NAT с помощью разных команд. В данном примере интерфейс маршрутизатора для внутренней сети — ethernet 0, а внешний интерфейс - последовательный интерфейс 0. Чтобы включить статическое преобразование NAT на ethernet 0, выполните такие действия в режиме глобальной настройки:

1. Войдите в режим настройки интерфейса, включите NAT и определите, что следует транслировать - внутренние или внешние адреса. В этом примере NAT переводит внутренние адреса во внешние.

Router (config)# interface e0

Router (config-if)#ip nat inside

Router (config-if)

2. Включите NAT на последовательном интерфейсе 0 и укажите, что этот интерфейс подключен к внешней сети. Задайте следующие команды из режима глобальной настройки:

Router (config)# interface s0

Router (config-if)#ip nat outside

Router (config-if)#

3. Должны появиться следующие данные при отображении настроек маршрутизатора. 10.1.2.254 и 200.1.1,1 - это IP-адреса, настроенные на физическом интерфейсе маршрутизатора,

interface Ethenet0

ip address 10.1.2.254 255.255.0.0 ip nat inside

interface Ethenet0

ip address 200.1.1.1 255.255.0.0 ip nat outside

9.8. Настройка динамической трансляции NAT, совмещения внутренних глобальных адресов и распределения нагрузки TCP

В этом разделе описывается настройка динамического преобразования NAT для сопоставления незаконного внутреннего IP-адреса с любым из законных, зарегистрированных глобальных IP-адресов из определенного пула адреса. Сначала рекомендуем вам на маршрутизаторе включить маршрутизацию IP и на каждом интерфейсе задать правильные IP-адреса и маски подсети.

Начнем работать в режиме глобальной настройки, предположив, что у нас есть лишь один интерфейс на маршрутизаторе, подключенном к внутренней сети. В данном примере необходим доступ к данным Интернета компьютеру, использующему незаконный внутренний IP-адрес 10.1.2.25. Настроим граничный маршрутизатор NAT так, чтобы при получении пакета, предназначенного внешней сети от IP-адреса 10.1.20.26, он выбирал доступный глобально маршрутизируемый IP-адрес из пула адресов и переводил адрес источника в допустимый адрес 200.10.1.25. Для этого выполните следующие действия:

1. Процессы преобразования NAT из внутренней сети во внешнюю происходят после маршрутизации. Поэтому все списки доступа или политики маршрутизации следует выполнять до преобразования. Можно создать список доступа и применить его к внутреннему списку для IP-адресов, которыми пользуются локальные устройства. В данном примере представлена сеть с серией IP-адресов 10.1.0.0, поэтому создадим стандартный список доступа IP со знаком подстановки вместо двух последних октетов. Используйте следующую команду:

Router(config)# access-list 2 permit 10.1.0.0 0.0.255.255

2. Вы знаете, что список доступа для пакетов, приходящих с адреса 10.1.2.25, будет определять политику маршрутизации. При применении укажите собственно пул адресов, допустимых для Интернета. Это будут законные IP-адреса, предоставленные провайдером. Мы можем получить лишь 100 адресов для 1000 ПК и серверов нашей сети, но так как в каждый момент времени не все наши ПК работают в Интернете, этого может

быть достаточно. Если недостаточно, необходимо другое решение, например настройка совмещения внутренних глобальных адресов. До настройки пула адресов придумайте имя. Назовем пул адресов "InternetlPPool". Для определения 100 IP-адресов, предоставленных поставщиком (от 200.1.1.1 до 200.1.1.100 с маской подсети 255.255.255.0), введем такую команду:

Router(config)#1pnat pool InternetlPPool 200.1.1.1 200.1.1.100 netmask 255.255.255.0

Команда ip nat pool имеет две другие опции. Вместо ключа netmask можно воспользоваться командой prefix-length, дополненной значением количества битов в маске. В данном случае маску подсети определяет число 24. Можно еще воспользоваться синтаксисом type rotary для распределения нагрузки TCP. Это означает, что IP-адреса пула представляют настоящие внутренние узлы, которые могут использоваться для распределения нагрузки TCP.

3. Сопоставьте список доступа 2, созданный в действии 1, с пулом NAT InternetlPPool, заданным в пункте 2. Для этого используется такая команда:

Router(config)#ip nat inside source list 2 pool InternetlPPool

4, Чтобы включить NAT, выберите интерфейс, соединяющий внутреннюю сеть с маршрутизатором или с внешним маршрутным процессором. Чтобы включить NAT на ethernet 0, выполните следующие команды в режиме глобальной настройки:

Router (config)# interface e0

Router (config-if)#ip nat inside

Router (config-if) #

5. Включите NAT на последовательном интерфейсе 0, подключенном к внешней сети. Задайте такие команды из режима глобальной настройки:

Router (config)# interface s0

Router (config-if)#ip nat outside

Router (config-if)#

9.9. Протокол PAT

PAT - это вариант NAT и единственная функция преобразования адресов на маршрутизаторах. PAT использует порты TCP. За счет этого вся сеть применяет лишь один глобально маршрутизируемый IP-адрес.

Локальные узлы внутренней сети связываются с внешней сетью IP, например с Интернетом. IP-адрес источника в трафике, предназначаемом для внешнего IP-адреса по другую сторону граничного маршрутизатора, транслируется перед пересылкой пакета

внешней сети. IP-адреса пакетов IP, возвращающиеся во внутреннюю сеть, переводятся в IP-адреса. Их же использует интерфейс назначения внутренней сети.

PAT позволяет сэкономить сетевые адреса. Кроме того, он приписывает один IP-адрес всей LAN. Весь трафик WAN сопоставляется с одним адресом. Это IP-адрес маршрутизатора со стороны сети ISDN. Внутренняя сеть становится невидимой для внешней сети или Интернета, поскольку во внешней сети создается впечатление, что весь трафик приходит от маршрутизатора.

Если пользователям нужен доступ к определенному удаленному серверу внешней сети, следует настроить статический адрес. PAT позволяет проходить пакетам с известным номером порта, например с протоколом передачи файлов FTP или Telnet.

9.9.1. Недостатки PAT

Применение PAT имеет недостатки, потому что этот протокол устраняет прямую, двухточечную трансляцию. Перечислим эти недостатки.

- Нельзя использовать программу Ping из внешнего узла до узла частной сети.
- Сигналы Telnet от внешнего узла до внутреннего узла не пересылаются, если только не настроен обработчик портов Telnet.
- Во внутренней сети поддерживается лишь один сервер FTP и один сервер Telnet.
- Пакеты, предназначенные для маршрутизатора, а не адреса внутренней сети (DHCP, SNMP, Ping или TFTP), не отклоняются и не фильтруются с помощью PAT.
- Если во внутренней сети одновременно пытаются загрузиться более 12 компьютеров, один или несколько из них могут получить сообщение об ошибке. Оно указывает на невозможность доступа к серверу.
- Компьютеры внутренней сети могут совместно использовать до 400 записей PAT. Если установлены соединения TCP и интервалы ожидания TCP настроены для поддержки работоспособности, то в определенный момент времени не более 400 машин могут получить доступ к внешней сети.
- Маршрутизатор, на котором используется PAT, не обрабатывает фрагментированные пакеты FTP.
- Для некоторых хорошо известных портов не определяются обработчики портов. А именно порты клиентов DHCP, используемые маршрутизатором для получения ответов сервера DHCP и порты WINS NetBIOS, используемые клиентами внутренней сети с Windows для получения данных протокола WINS.

9.9.2. Настройка PAT

Функция PAT позволяет локальным узлам с выделенными частными IP- адресами связываться с внешним миром. Маршрутизатор переводит адрес источника заголовка IP в глобальный, уникальный IP-адрес перед пересылкой пакета для внешней сети. Аналогичным образом на обратном пути пакеты IP преобразовываются в выделенные частные IP-адреса.

При включении PAT автоматически отключается передача пакетов. Таким образом предотвращается утечка информации о частных IP-адресах во внешнюю сеть.

Для включения PAT используются две команды.

set ip pat on Эта команда включает NAT и задается, чтобы можно было использовать команду set ip pat port

set ip pat porthandler Обработчик порта переводит общедоступный порт TCP или UDP в частный IP-адрес. Когда приходит пакет из внешней сети, PAT сравнивает номер порта с внутренне настроенным списком обработчика порта, который содержит до 15 записей. Если для порта определен специальный обработчик, пакет направляется к подходящему обработчику порта (IP-адресу).

Если задан стандартный обработчик портов, пакет направляется к нему. Возможны следующие ключи:

- **default** - Включает обработчик порта для основных обработчиков всех портов. Исключением является специальный обработчик.
- **telnet** - Включает обработчик порта для порта 23 протокола Telnet.
- **ftp** - Включает обработчик порта для протокола передачи файлов FTP и использует протокольный порт 21.
- **smtp** - Включает обработчик порта для простого протокола передачи почты SMTP и использует протокольный порт 25.
- **wins** - Включает обработчик порта для службы сеансов NetBIOS на порту 139.
- **http** - World Wide Web-HTTP и безопасный порт HTTP 80 или 443. off Отключает обработчик порта.

Контрольные вопросы:

1. Укажите преимущества и недостатки технологии NAT?
2. Укажите преимущества и недостатки технологии PAT?
3. Укажите общее и различия между технологиями NAT и PAT?
4. Укажите принцип работы NAT?
5. Укажите принцип работы PAT?

6. Укажите когда надо в сети использовать NAT, а когда PAT?
7. Какие настройки необходимо выполнить для конфигурирования NAT?
8. На интерфейсе маршрутизатора применены списки контроля доступа и NAT, какой инструмент будет выполняться первым?

10. Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы. 3-е изд. СПб: Издательство «Питер», 2008. 958 с.
2. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации. Спб.: Питер, 2002, 688 с.
3. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. М.:Техносфера, 2003. 512с.
4. Куин Лаем, Рассел Ричард. Fast Ethernet. К.: Издательская группа BHV,1998. 448 с.
5. Кулаков Ю.А., Луцкий Г.М. Компьютерные сети. К.: Юниор, 1998. 384 с.
6. Кульгин М.В. Коммутация и маршрутизация IP/IPX-трафика. М.: КомпьютерПресс, 1998. 320 с.
7. Кульгин М.В. Практика построения компьютерных сетей. Для профессионалов. СПб.: Питер, 2001. 320 с.
8. Кульгин М.В. Технологии корпоративных сетей. Энциклопедия. СПб: Изд-во "Питер", 1999. 704 с.
8. Мартин М. Введение в сетевые технологии. М.:Изд-во Лори,2002. 659 с.
9. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. СПб.: БХВ – Санкт-Петербург, 2000. 512 с.
10. Пятибратов А.П., Гудыно Л.П. Вычислительные системы, сети и телекоммуникации. М.: Финансы и статистика, 2001. 512 с.
11. Ретана А., Слайс Д., Уайт Р. Принципы проектирования корпоративных IP сетей / пер. с анг. – М.: Издательский дом «Вильяс», 2002. – 368 с.
12. Столлингс В., Компьютерные системы передачи данных: Изд. 6. М.: Вильямс 2002. 928 с.
13. Фейбел Вернер. Энциклопедия современных сетевых технологий. К.: Комиздат, 1998, 687 с.

Гергель Александр Викторович

СЕТИ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ВЫСОКОПРОИЗВОДТЕЛЬНЫХ СИСТЕМ

Учебно-методическое пособие

Федеральное государственное автономное образовательное учреждение
высшего образования
«Нижегородский государственный университет им. Н.И. Лобачевского».
603950, Нижний Новгород, пр. Гагарина, 23.

Подписано в печать . Формат 60 84 1/16.
Бумага офсетная. Печать офсетная. Гарнитура Таймс.
Усл. печ. л.____ . Уч-изд. л.____
Заказ № ____. Тираж ____ экз.

Отпечатано в типографии Нижегородского госуниверситета
им. Н.И. Лобачевского
603600, г. Нижний Новгород, ул. Большая Покровская, 37
Лицензия ПД № 18-0099 от 14.05.01