

## СОДЕРЖАНИЕ

<b><i>Введение в сетевые технологии.....</i></b>	<b><i>5</i></b>
Локальные сети.....	5
Глобальные сети.....	6
Архитектура сети .....	7
<b><i>1. Иерархические топологии .....</i></b>	<b><i>10</i></b>
1.1. Преимущества иерархической топологии .....	10
1.2. Трехуровневая иерархическая модель .....	12
<b><i>2. Обеспечение безопасности сети.....</i></b>	<b><i>16</i></b>
2.1. Чем вызвана необходимость обеспечения безопасности сетей.....	16
2.2. Основные определения безопасности сетей.....	16
2.3. Категории угроз безопасности сетей .....	19
2.4. Как нарушается безопасность сетей .....	20
2.5. Исследование сети.....	20
2.5. Взлом системы доступа.....	20
2.6. DoS-взломы.....	22
<b><i>3. Политика безопасности сетей и ее обеспечение.....</i></b>	<b><i>23</i></b>
<b><i>4. Списки управления доступом.....</i></b>	<b><i>26</i></b>
4.1.Чем вызвана необходимость обеспечения безопасности сетей.....	26
4.2. Принцип работы списков управления доступом.....	27
4.3. Конфигурирование списков управления доступом.....	29
4.4. Стандартные списки ACL .....	31
4.5. Расширенные списки управления доступом.....	33
<b><i>5. Преобразование сетевых адресов (NAT) и адресов портов (PAT).....</i></b>	<b><i>35</i></b>
5.1. Терминология NAT .....	35
5.2. Принцип работы NAT .....	36
5.3. Преимущества NAT.....	37
5.4. Недостатки NAT .....	37
5.5. Функции NAT .....	38
5.6. Настройка статического преобразования сетевых адресов .....	43
5.7. Настройка динамической трансляции NAT, совмещения внутренних глобальных адресов и распределения нагрузки TCP .....	44
5.8. Протокол PAT.....	45
5.8. Недостатки PAT.....	46
5.10. Настройка PAT.....	46
<b><i>6. Сегментация локальных сетей.....</i></b>	<b><i>48</i></b>
6.1. Сегментация локальных сетей с помощью повторителей .....	49
6.2. Сегментация локальных сетей с помощью мостов .....	53
6.3. Сегментация локальных сетей с помощью маршрутизаторов.....	58
6.4. Сравнение применения мостов с коммутацией в локальной сети.....	59

6.5. Три функции коммутации уровня 2 .....	59
6.6. Типы переключателей локальных сетей .....	61
<b>7. Виртуальные локальные сети .....</b>	<b>63</b>
7.1. Виртуальные сети и физические границы .....	63
7.2. Доказательство необходимости применения сетей VLAN .....	64
7.3. Статические сети VLAN .....	71
7.4. Динамические сети VLAN .....	72
7.5. Идентификация сетей VLAN .....	72
7.6. Маркировка кадров .....	73
7.7. Методы идентификации VLAN .....	73
7.8. Достоинства виртуальных сетей .....	74
7.9. Добавление новых пользователей в виртуальную локальную сеть .....	74
7.10. Управление широковещанием .....	75
7.11. Обеспечение безопасности сети .....	76
7.12. Конфигурирование сетей VLAN в коммутаторах Catalyst .....	77
<b>8. Основы протокола распределенного связующего дерева .....</b>	<b>84</b>
8.1. STP-процесс .....	86
8.2. Схема разрешения конфликтов в STP .....	86
8.3. Состояния портов в STP .....	86
8.4. Изменения STP-топологии .....	87
8.5. Усиление стабильности протокола STP .....	88
8.6. Пример функционирования протокола STP .....	89
8.7. Конфигурирование протокола STP .....	90
<b>9. Протокол магистральных каналов виртуальных локальных сетей .....</b>	<b>95</b>
9.1. Режимы протокола VTP .....	98
9.2. Принцип действия протокола VTP .....	104
9.3. Настройка протокола VTP .....	105

## 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 производить 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:

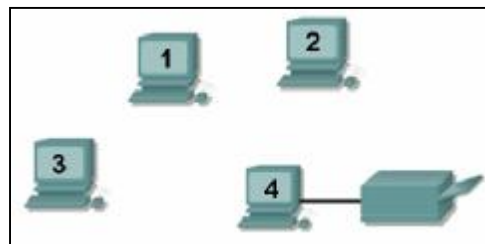


Рис 1. Пример сети, в которой к одному компьютеру подключен принтер

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

Было найдено два решения, выполняющих поставленные условия. И это были 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

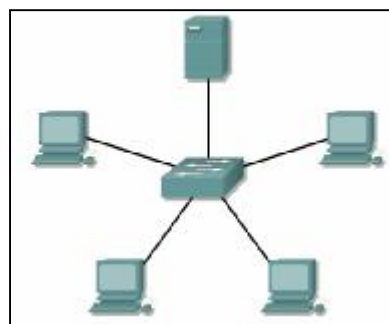


Рис 2. Локальная сеть

Характерными особенностями локальной сети являются:

- ограниченные географические пределы;
- обеспечение многим пользователям доступа к среде с высокой пропускной способностью;
- постоянное подключение к локальным сервисам;
- физическое соединение рядом стоящих устройств.

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 широковещанием

Наиболее распространенными технологиями ЛВС являются

- Ethernet,
- Fiber Distributed Data Interface (FDDI)
- Token Ring

### ***Глобальные сети***

Быстрое распространение компьютеров привело к увеличению числа локальных сетей. Каждая локальная сеть представляла отдельный электронный «остров», не имеющий связи с другими локальными сетями. Требовалось найти способ передачи информации от одной локальной сети к другой. Решить эту задачу помогло 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.
- Мосты (Bridge) передают сообщения на основе записей в таблице пересылки.
  - 
    - Возможность фильтрации сетевого трафика;
    - сохраняет информацию о всех узлах;
    - соединяет идентичные или разные сети (например, Ethernet и Token Ring).
- Маршрутизаторы (Router) обеспечивают выбор маршрута обмена данными между узлами сети.
  - 
    - Принимает решение о выборе "лучшего пути";
    - Дистанция обычно оценивается в интервалах (hop) - промежутках между двумя соседними маршрутизаторами на пути от отправителя к получателю

### ***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:

#### **Общая шина.**

При использовании шинной топологии компьютеры соединяются в одну линию, по концам, которой устанавливают терминаторы. Когда источник

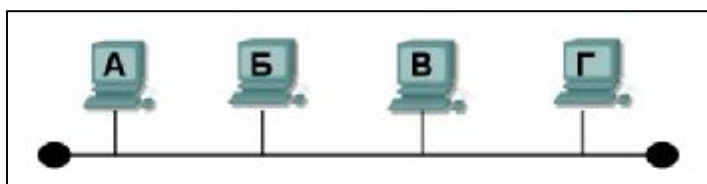


Рис 3. Топология общая шина

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.

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.

### **Звезда.**

При использовании топологии "звезда", каждый компьютер подключается к специальному концентратору (хабу). Связь между устройством и центральным каналом или концентратором осуществляется посредством двухточечных линий. Когда источник передает сигналы в сетевую среду, данные посылаются центральному сетевому устройству (концентратору), затем концентратор переправляет их устройству в соответствии с адресом, содержащимся в данных.

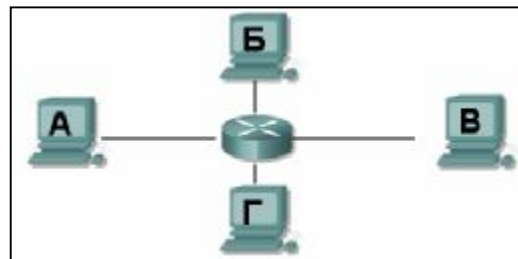


Рис 4. Топология звезда

Преимуществом топологии звезда:

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

### **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.

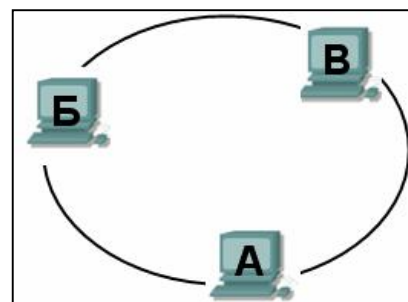


Рис 5. Топология кольцо

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.

# 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.

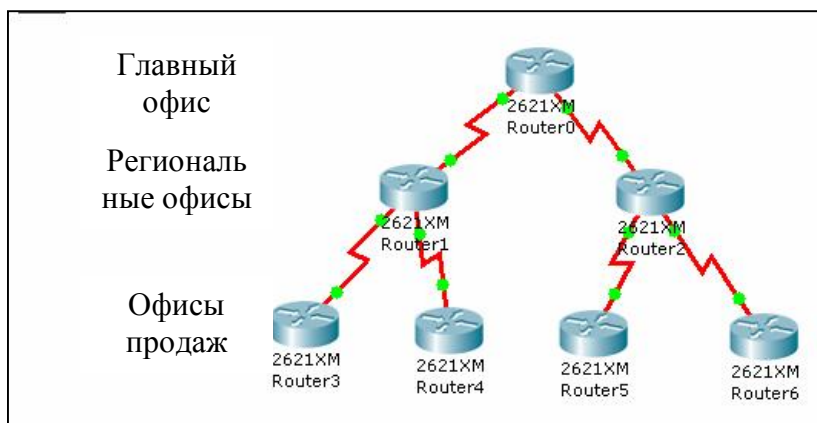


Рис 6. Пример иерархической сети

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

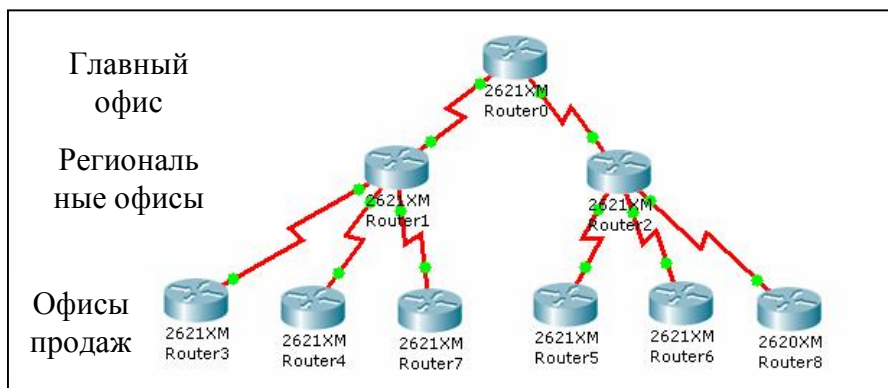


Рис 7. Пример иерархической сети после расширения

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.

### **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 10BaseT 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

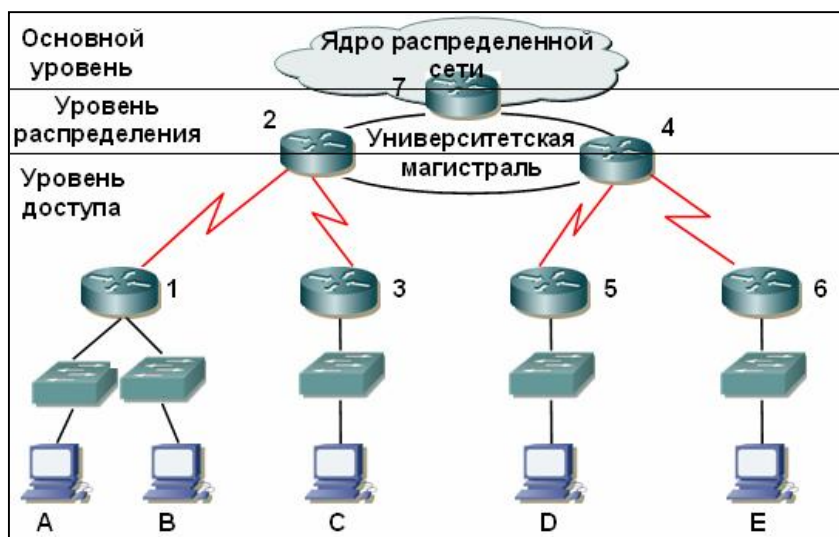


Рис 8. Иерархическая модель Cisco

комплексы. Модель Cisco описывает три уровня иерархии, как показано на рисунке 8. Вот эти три уровня:

- **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 рассылки.

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 коллизийных 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. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СЕТИ**

Компьютеры, сети, Internet стали неотъемлемой частью нашей повседневной жизни. Наш быстроразвивающийся, 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.

### ***2.1. Чем вызвана необходимость обеспечения безопасности сетей***

В настоящее время огромное количество сетей объединено посредством Internet. Поэтому очевидно, что 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.

### ***2.2. 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.

Обычно в брандмауэрах предусмотрены, по меньшей мере, три интерфейса, хотя в более ранних реализациях использовались два. По этой причине, в силу привычки, 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. 9 показана общая

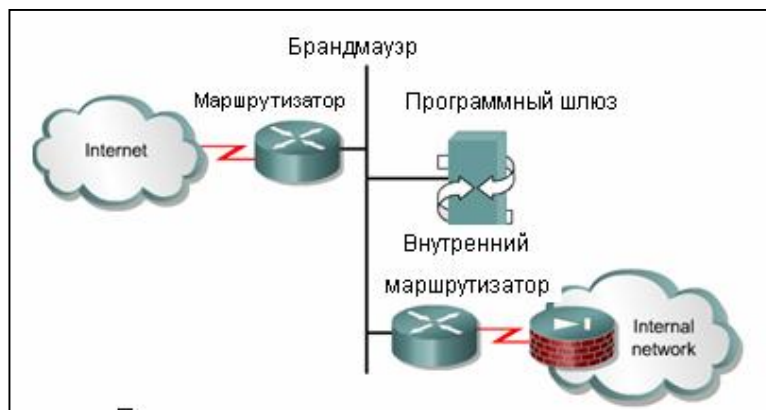


Рис 9. Общая структура сети при использовании брандмауэра

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.



### **2.3. 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. Конечно же, 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. Обычно 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. Обычно они получают доступ к сети компании через Internet или сервер удаленного доступа.
- **Внутренние угрозы.** Обычно 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.

## **2.4. 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.

## **2.5. 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 отправляет 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.

## **2.5. 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.

### **2.5.1. 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.

### **2.5.2. 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.

### **2.5.3. 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.

## **2.6. 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.

### 3. 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 10 изображены четыре этапа цикла обеспечения безопасности.

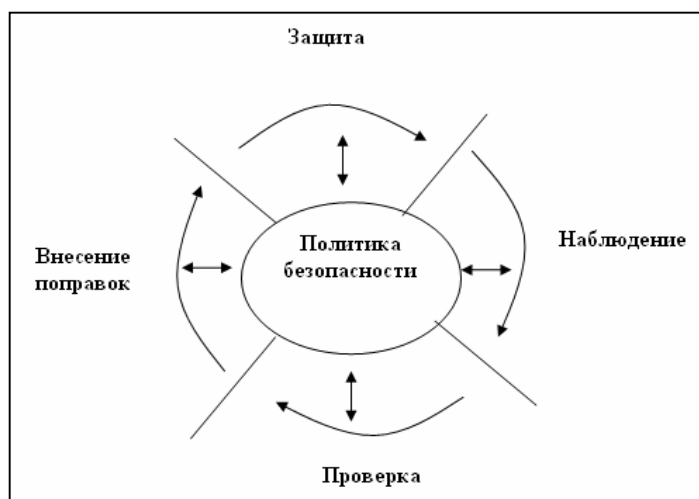


Рис 10. Цикл обеспечения безопасности компьютерной сети

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 неправомерный 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 SecurID.

(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 Intrusion 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.

## 4. СПИСКИ УПРАВЛЕНИЯ ДОСТУПОМ

Сетевой администратор должен уметь запрещать несанкционированный доступ к сети и в то же время обязан обеспечить доступ к сети авторизованных 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.

### ***4.1. Чем вызвана необходимость обеспечения безопасности сетей***

В настоящее время огромное количество сетей объединено посредством Internet. Поэтому очевидно, что 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.



- 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 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

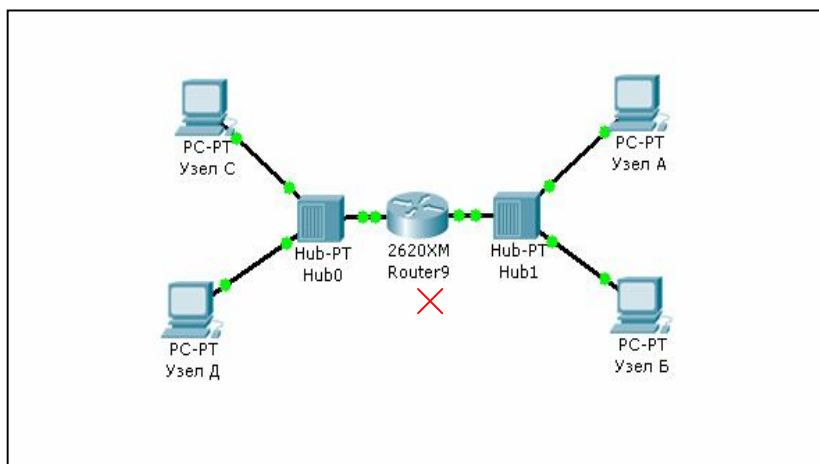


Рис 11. Пример ограниченного сетевого трафика

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 11 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.

#### **4.2. 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. 12).

Когда пакет поступает на интерфейс, маршрутизатор определяет, куда его направить — на маршрутизатор или на мост (т.е. являются ли пакеты маршрутизируемыми или коммутируемыми). Если пакет по какой-либо причине не может быть обработан маршрутизатором

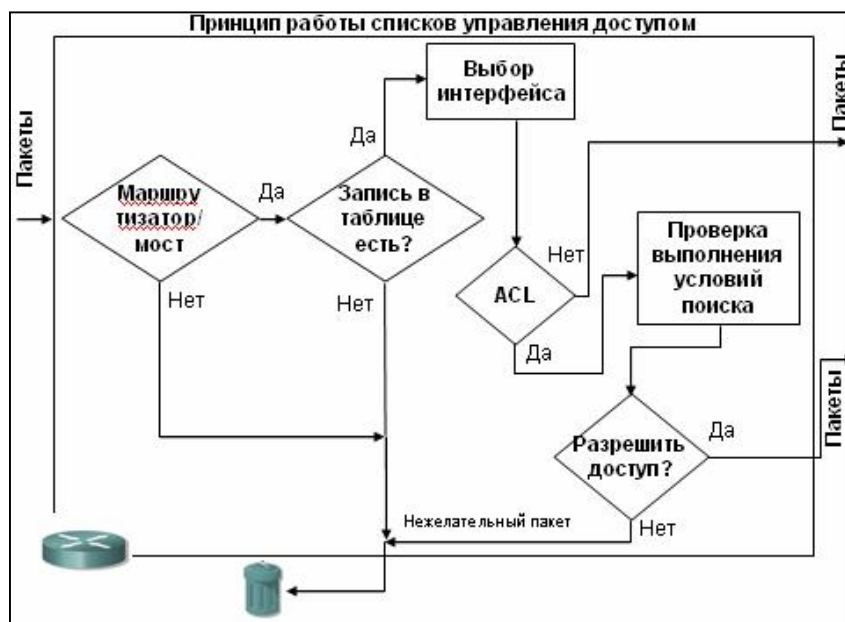


Рис 12. Принцип работы списков управления доступом

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 ЕО, 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.

### 4.3. 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

```
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

interface ethernet 0
ip address 1.1.1.1 255.0.0.0
ip access-group 1 in
ip access-group 2 out
```

списка, он по- Рис 13. Пример конфигурирования списков управления доступом следовательно вводит директивы списка ACL, начиная с ключевого слова **access-list** и заканчивая правильными параметрами, как показано на рисунке 13. Создание списка управления доступом — это только половина дела. Вторая, и не менее важная часть процесса, — это привязка списка к интерфейсу.

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 13). 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.

#### 4.4. Стандартные списки ACL

Стандартный список управления доступом позволяет проверять и сравнивать адреса отправителей пакетов с директивами, как показано на рисунке 14.

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

Например, для пакетов, поступивших на интерфейс E0

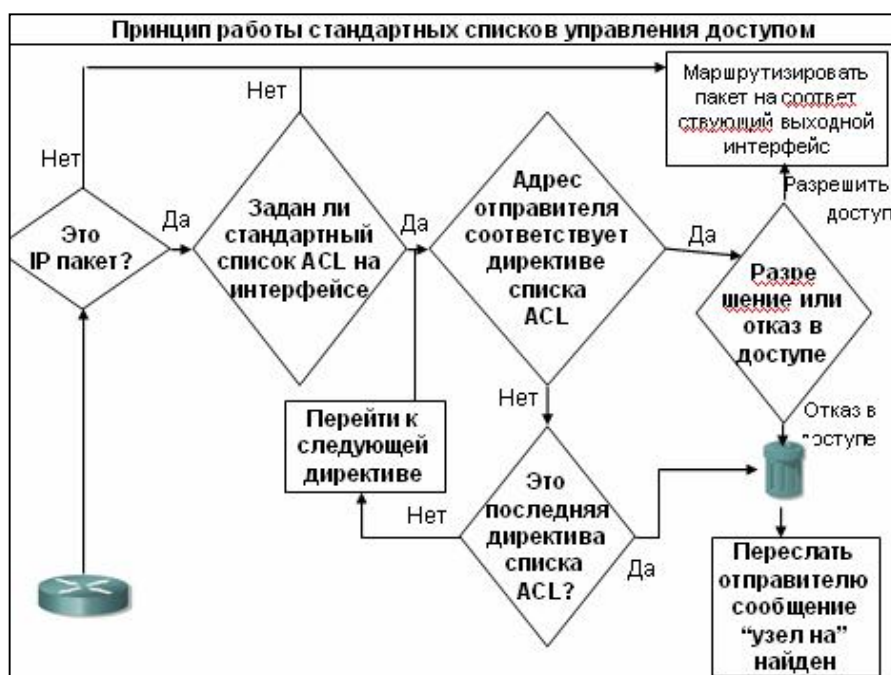


Рис 14. Принцип работы стандартных списков управления доступом

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, с первого взгляда 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 15 показан стандартный список доступа, который

```
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  
access-list 2 permit 10.0.0.0 0.255.255.255
```

Рис 15. Принцип конфигурирования стандартных списков управления доступом

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).

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 следующий формат:

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

#### 4.5. 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. 16.



Рис 16. Принцип работы расширенного списка управления доступом

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.

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-wildcard destination destination-wildcard] [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

<pre>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 access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data</pre>
---

показано на Рис 17. Пример конфигурирования расширенного списка управления

рисунке 17. 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 17 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.

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.



## 5. 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.

### 5.1. 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 комплексов 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.

## 5.2. 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. 18). Обратите внимание,

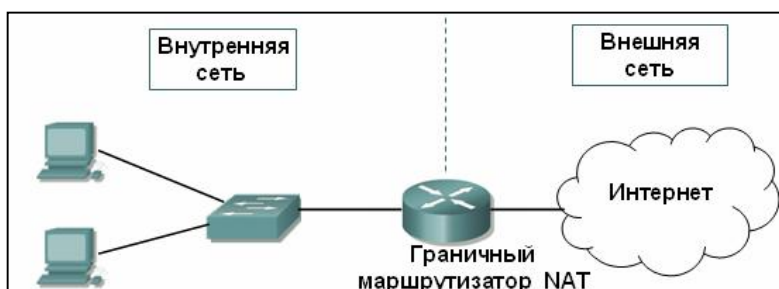


Рис 18. Маршрутизатор NAT на границе внутренней и внешней сетей

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.

Протокол NAT учитывает, что немногие люди пользуются внешней сетью в определенный момент времени. Применяется коммутация 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.

### 5.3. 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.

### 5.4. 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.

## 5.5. 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

### 5.5.1. 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. 19). Рассмотрим этапы процесса, показанного на рис. 19.

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.

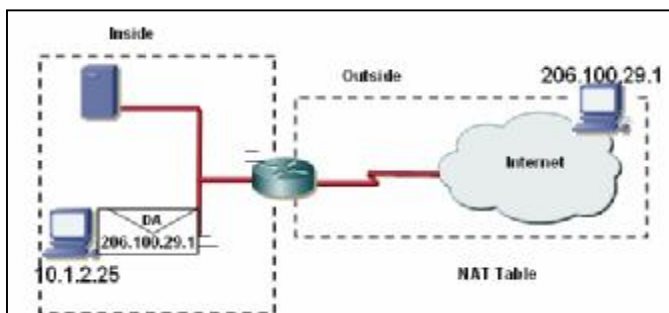


Рис 19. Преобразование внутренних локальных адресов

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.

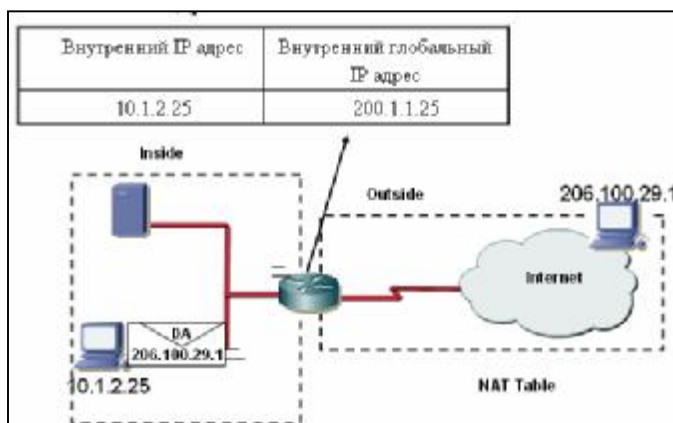


Рис 20. Преобразование внутреннего локального адреса в внутренний глобальный адрес

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.

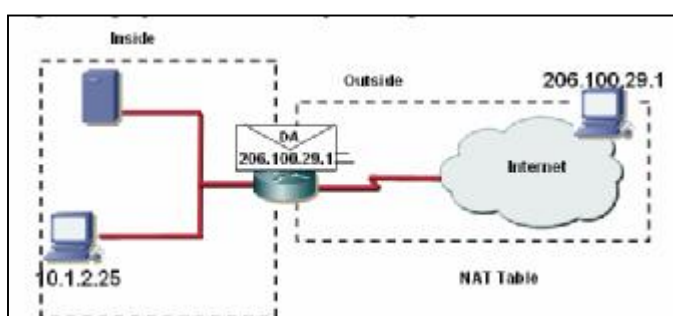


Рис 21. При получении пакета от 206.100.29.1 выполняется обратное преобразование

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.

### **5.5.2. 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 22 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.

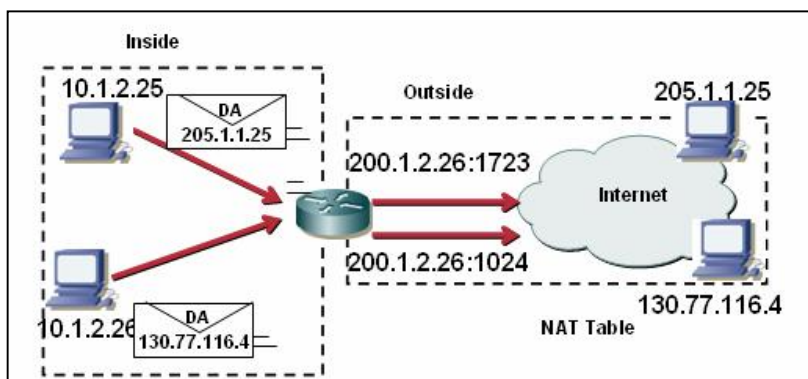


Рис 22. Совмещение внутренних глобальных адресов

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.

### **5.5.3. 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 23 показано распределение нагрузки TCP.

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

1. На рис. 23 ПК с глобальным IP-адресом 200.1.1.25 начинает соединение TCP с виртуальным

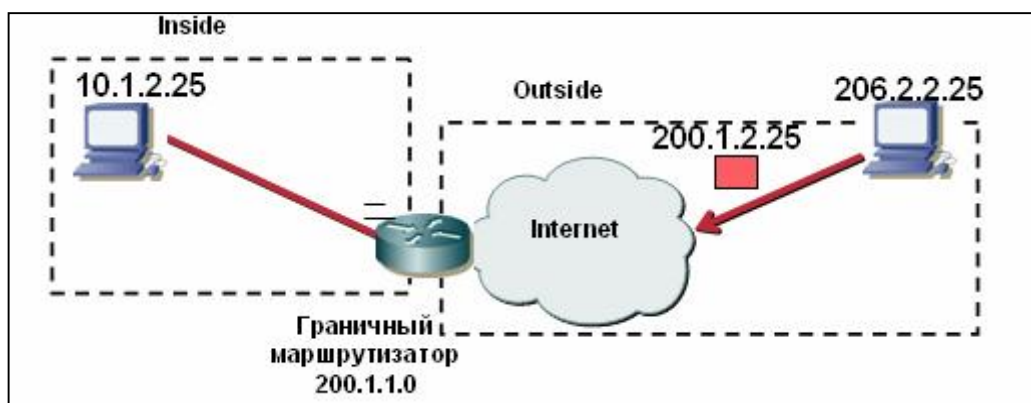


Рис 23. Применение распределения нагрузки TCP

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.

#### **5.5.4. Перекрывание 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 перекрыванием.

Вы узнаете, как переводить IP-адреса, не допустимые для использования во внешней сети, например в 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.

### ***5.6. 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
```

### ***5.7. 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 "InternetIPPool". 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)#ip nat pool InternetIPPool 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 InternetIPPool, заданным в пункте 2. Для этого используется такая команда:

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

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)#**

## ***5.8. 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, предназначенном 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.

### **5.8. Недостатки PAT**

Применение PAT имеет недостатки, потому что этот протокол устраняет прямую, двустороннюю 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.

### **5.10. 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.

## 6. 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. 24 показаны варианты сети 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

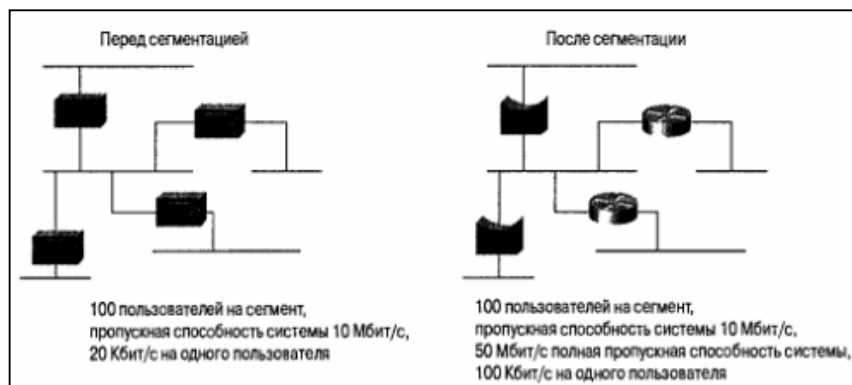


Рис 24. Сеть до и после сегментации

сегментации сети повторители были заменены на мосты и маршрутизаторы, которые позволяют изолировать разные части друг от друга и обеспечить пользователей большей пропускной способностью. Мосты 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
Повторитель	один	Один
Мост	много	Один
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: повторитель, мост, маршрутизатор или сетевой коммутатор?" Повторители, на самом деле, не позволяют осуществить сегментацию сети и, соответственно, не позволяют получить большую пропускную способность. Они лишь предоставляют возможность в некоторой степени увеличить протяженность сети. Мосты, маршрутизаторы и коммутаторы больше подходят для сегментации локальных сетей. В следующих разделах приводится описание различных вариантов сетей.

### **6.1. Сегментация локальных сетей с помощью повторителей**

В случае необходимости увеличения размеров сети можно использовать устройство для объединения сетей, например, повторитель. Повторители работают на первом уровне модели OSI (Open System Interconnection — модель взаимодействия открытых систем) и выполняют роль расширителей кабельных

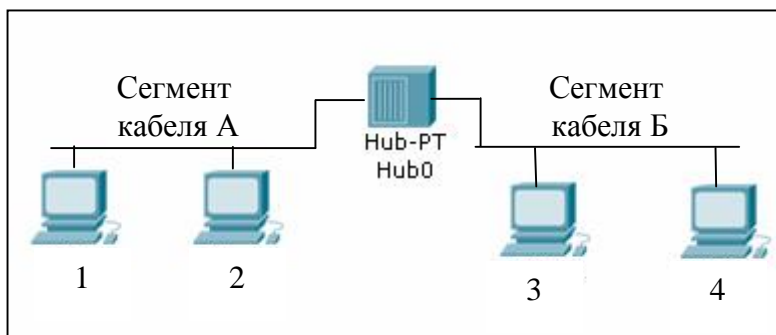


Рис 25. Соединение сегментов локальной сети с помощью повторителей

сегментов. Рабочие станции не ощущают наличия повторителя, который является абсолютно прозрачным для подключенных к нему устройств. Повторитель соединяет кабельные сегменты, как показано на рисунке 25.

Повторители регенерируют сигнал при передаче из одного сегмента кабеля в другой. Когда станция 1 передает информацию станции 2, фрейм также передается в сегмент кабеля Б, даже если устройства отправителя и получателя подключены к сегменту кабеля А. Повторители не являются интеллектуальными устройствами и не вникают в содержание передаваемых данных. Они слепо выполняют свои обязанности по передаче сигналов из одного сегмента кабеля во все остальные. Если фрейм содержит ошибочные данные, то повторитель также будет их передавать. Если размер фрейма превышает максимальный или меньше минимального размера фрейма в сети Ethernet, то повторитель все равно будет передавать такие фреймы. Если коллизия произойдет на сегменте кабеля А, то устройства, подключенные к сегменту Б, также обнаружат коллизию. Повторители действительно работают только как удлинитель кабеля.

На рисунке 25 показано соединение двух сегментов, но повторители могут иметь несколько портов для подключения нескольких сегментов, как показано на рисунке 26.

Сеть 10BaseT включает в себя концентраторы и кабели витой пары, которые используются для соединения рабочих станций. Концентраторы являются многопортовыми повторителями, они передают сигналы от одного интерфейса ко всем остальным. Тот факт, что станции, подключенные к концентратору, как показано на рисунке 25 и на рисунке 26, получают весь трафик, имеет как положительные, так и отрицательные стороны.

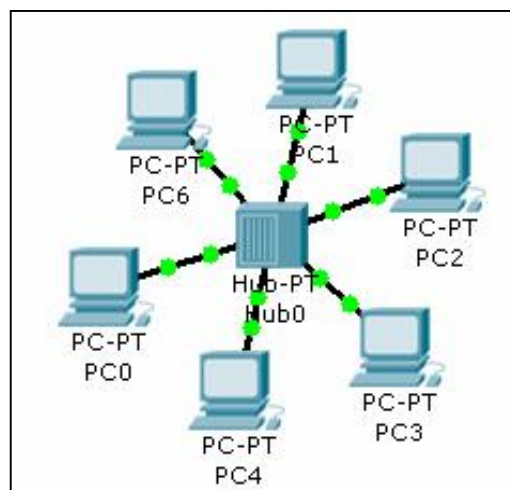


Рис 26. Многопортовый повторитель

Повторители выполняют несколько задач, связанных с распространением сигнала. Например, повторители регенерируют сигнал и вводят новые стартовые биты. Стартовые биты следуют перед MAC-адресом станции-получателя и помогают приемному устройству сетевого адаптера синхронизироваться. Размер блока стартовых бит равен 8 байтам. Он содержит чередующуюся комбинацию бит, которая в бинарном виде содержит последовательность 1010. Последний байт стартового блока отличается от всех предыдущих и имеет двоичное значение 10101011. Он называется разделителем фрейма (start frame delimiter — SFD). Два последних бита указывают приемнику на то, что далее



следуют данные. Повторители убирают все 8 байт стартового блока приходящего фрейма, а затем генерируют новый блок перед тем, как передавать фрейм через выходной интерфейс.

Повторитель также гарантирует, что сигнал оповещения о коллизии будет передан на все порты. Если произошла коллизия между станциями 1 и 2 сегмента А на рисунке 25, то коллизия принудительно передается повторителем на все порты, и все станции сегмента Б также обнаруживают наличие коллизии. Станции сегмента Б должны подождать устранения коллизии, и лишь затем начинать передачу. Если станции 3 и 4 не будут знать о коллизии, они могут начать передачу во время коллизии между станциями 1 и 2, и таким образом, также станут ее участниками.

Для сетей с повторителями существуют ограничения, перечисленные ниже, которые вытекают из различных причин и с которыми необходимо считаться при расширении сети с помощью повторителей.

- Все устройства совместно используют пропускную способность сети.
- Существуют ограничения на количество станций в одном сегменте.
- Существует ограничение максимального расстояния между дальними концами сети.

#### **6.1.1. Совместное использование пропускной способности**

При использовании повторителя происходит не только увеличение протяженности сети, но расширяется также и домен коллизий. Коллизии, которые происходят в одном сегменте, подключенном к повторителю, также оказывают влияние на рабочие станции, находящиеся в сегменте, подключенном к другому порту повторителя. Коллизия "распространяется" через повторитель и при этом, соответственно, используется пропускная способность всех объединенных сегментов. Другим побочным эффектом общего домена коллизий является распространение фреймов в сети. Если используется технология с общим доступом, то все рабочие станции совместно используют пропускную способность сети. Данный факт имеет место в случае передачи одноадресных, широковещательных и групповых фреймов. Все рабочие станции получают все фреймы. Добавление новых сетевых станций потенциально еще больше дробит пропускную способность. Старые Ethernet-системы обеспечивают общую пропускную способность сети 10 Мбит/с. Станции по очереди используют эту общую пропускную способность. С увеличением числа передающих станций доступная для каждого узла пропускная способность уменьшается.

Сетевой администратор должен определить требования пользовательских приложений к пропускной способности и сравнить их с теоретическим и реальным значениями доступной пропускной способности сети. Для измерения средней и пиковой пропускной способности сети необходимо использовать сетевой анализатор. Учет приведенных выше факторов позволяет определить, насколько необходимо увеличить пропускную способность сети для поддержки пользовательских приложений.

### **6.1.2.Количество станций в одном сегменте**

В технологии Ethernet оговорены ограничения на количество станций, которые могут быть подключены к одному кабелю. Ограничения связаны с электротехническими характеристиками системы. С увеличением количества трансиверов, подключенных к кабелю, изменяется полное сопротивление (импеданс) кабеля, что вызывает появление отраженных сигналов. При чрезмерном изменении импеданса механизм обнаружения коллизий прекращает корректно работать. Для устаревших вариантов технологии Ethernet максимальное количество устройств, подключенных к сегменту, не должно превышать 100 при использовании стандарта 10Base5. В системе, где используется стандарт 10Base2, число станций не должно превышать 30. Использование повторителей не может увеличить число станций, подключенных к одному сегменту. Данные ограничения связаны с топологией сети — шина, которая используется в сетях стандартов 10Base2 и 10Base5.

### **6.1.3. Расстояние между дальними концами сети**

Еще одно ограничение на расширение сети с помощью повторителей связано с протяженностью сети. Длина соединения в сети Ethernet может быть увеличена до тех пор, пока значение канального интервала не противоречит стандарту Ethernet. Канальный интервал зависит от пропускной способности сети. Для сетей с пропускной способностью 10 Мбит/с, такой, как

стандарта 10BaseT, значение канального интервала равно 51,2 мкс. Для сети с пропускной способностью 100 Мбит/с значение канального интервала

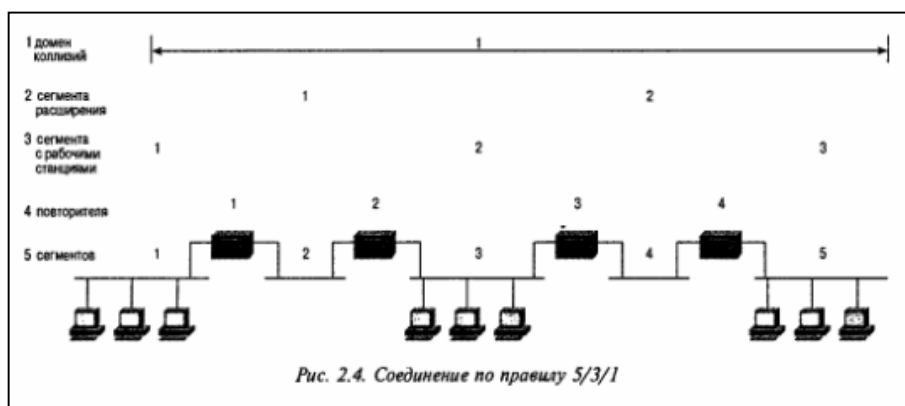


Рис 27. Соединение по правилу 5/3/1

в 10 раз меньше, чем для сети стандарта 10BaseT. Для расчета протяженности сети необходимо принять во внимание величину канального интервала, задержку, связанную со средой передачи, такой, как медный кабель или оптическое волокно, а также количество повторителей в сети. Для сети Ethernet с пропускной способностью 10 Мбит/с количество повторителей в сети должно соответствовать так называемому правилу 5/3/1, которое иллюстрируется на рисунке 27. Это правило гласит, что с помощью повторителей может быть соединено до пяти сегментов, но только к трем из них могут быть подключены сетевые устройства. Два других сегмента служат для объединения, и к их концам могут быть подключены только повторители. Следуя правилу 5/3/1, администратор создает один домен коллизий. Сигнал коллизии распространяется через все повторители по всем сегментам.

При правильном использовании повторители позволяют расширить домен коллизий за счет объединения нескольких сегментов на первом уровне модели OSI. Любая передача данных в домене коллизий распространяется ко всем станциям домена. Однако, администратор также должен принимать во внимание правило 5/3/1. Если сеть должна быть расширена до размеров больших, чем установлено правилом 5/3/1, то необходимо использовать другой тип коммуникационного оборудования. Например, администратор может использовать мост или маршрутизатор.

Повторители увеличивают размеры доменов коллизий и широковещательных доменов до размеров, которые допускаются правилами для повторителей. Максимальные географические размеры ограничиваются значением канального интервала для выбранной среды передачи и определяют величину домена коллизий. При увеличении размера сети до значений больших, чем предельно допустимые для используемой среды передачи, сеть будет работать некорректно. В случае использования технологии Ethernet могут возникать запоздалые коллизии (late collisions), если протяженность сети будет очень большой. Запоздалые коллизии возникают тогда, когда станция определяет наличие коллизии за пределами канального интервала, равного 51,2 мкс.

## ***6.2. Сегментация локальных сетей с помощью мостов***

Как было описано в предыдущем разделе, правила 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 мостов. Объединение сетей на основе метода, показанного на рисунке 28, существенно отличается от объединения сетей с помощью повторителя. Например, если в сети с повторителем станции находятся в одном сегменте и передают информацию друг другу,

то переданные фреймы появляются на всех остальных сегментах рассматриваемой сети. В случае сетей, объединенных с помощью моста, такого обычно не происходит. В мостах используется фильтрация для

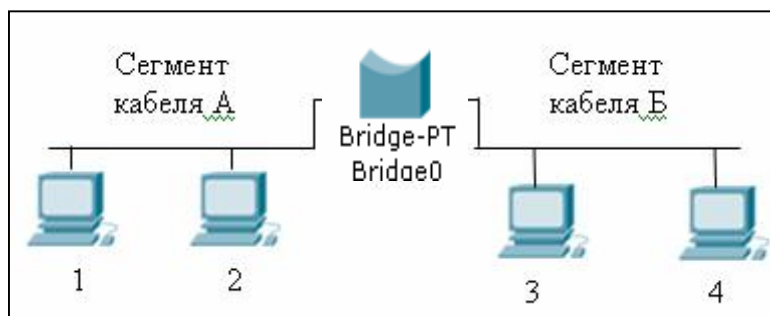


Рис 28. Объединение сегментов с помощью моста

того, чтобы определить, следует или не следует отправлять фрейм в другие интерфейсы.

Для технологий, которые используют различные методы доступа к среде передачи, как, например, Ethernet и Token Ring, методы фильтрации также различны. Например, в технологии Ethernet используется метод, называемый прозрачным мостовым соединением (transparent bridging), который состоит в том, что проверяется MAC-адрес получателя фрейма и по результатам определяется, должен ли фрейм передаваться, быть отфильтрованным, или передаваться на все порты (flood). Мост 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. В технологии Token Ring также может использоваться метод исходного маршрута (source route bridging), в котором применяется принцип перенаправления потока фреймов, отличный от метода прозрачного мостового соединения.

Наиболее важным свойством мостов является то, что они позволяют соединять домены коллизий так, что объединенные домены коллизий являются независимыми, т.е. коллизии не распространяются между соединенными сегментами. На рисунке 29 показана сеть, сегменты в данном случае объединены с помощью

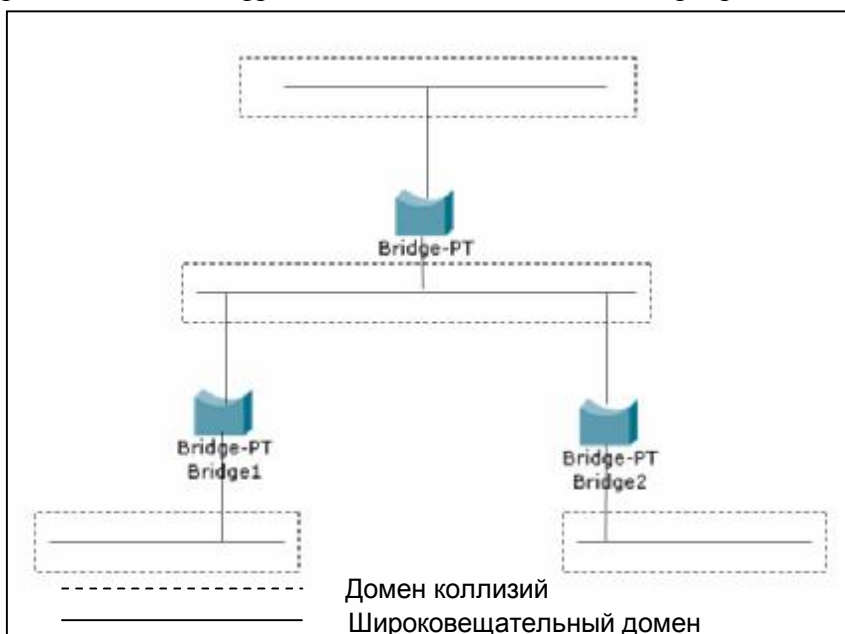


Рис 29. Объединение сегментов с помощью моста позволяет создать несколько доменов коллизий и один широковещательный домен

мостов. В сети с повторителями все сегменты принадлежат одному домену коллизий, а пропускная способность сети делится между четырьмя сегментами. В сети, показанной на рисунке 29, каждый сегмент принадлежит отдельному домену коллизий. В сети с пропускной способностью 10 Мбит/с каждый сегмент в таком случае обеспечивает собственную пропускную способность 10 Мбит/с, общая пропускная способность при этом составляет 40 Мбит/с.

Существенное увеличение пропускной способности объясняет, почему сегментация локальной сети с помощью мостов позволяет получить преимущество для пользователей. При одинаковом количестве рабочих станций пользователям сети, показанной на рисунке 29, доступна большая пропускная способность. Хотя технологии коммутации обсуждаются ниже в данной главе, сейчас необходимо заметить, что крайний случай распределения пропускной способности имеет место при выделении каждому пользователю отдельного интерфейса моста. В таком случае, каждому пользователю доступна полная пропускная способность его локального сегмента; только одна станция и один порт моста принадлежат к домену коллизий. Именно такая структура характерна для сети с использованием технологий коммутации.

Еще одно преимущество использования мостов вытекает из того, что они работают на втором уровне. В сети с повторителями ограничение на максимальную протяженность сети приводит к невозможности расширения размеров структуры до бесконечности. Использование мостов позволяет использовать для каждого сегмента максимально возможную длину. Каждый сегмент имеет свое значение канального интервала. Мосты не передают коллизий между сегментами, т.е. они позволяют изолировать отдельные участки сети и восстанавливать значения канального интервала. В теории с помощью мостов можно расширять сеть до бесконечности. Практические соображения, однако, не позволяют использовать такую возможность.

Мосты фильтруют фреймы, отправитель и получатель которых находятся в одном сегменте. Исключением являются широковещательные фреймы и фреймы групповой рассылки. При получении широковещательного сообщения мост передает фрейм во все интерфейсы. Рассмотрим для примера запросы протокола ARP, как и для сетей с повторителями. Станция-отправитель, которая находится в сети с повторителями и 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 мосты и все интерфейсы. Все сегменты, подключенные к мосту, принадлежат к одному широковещательному домену. Т.к. все станции принадлежат одному

широковещательному домену, то, следовательно, они должны также принадлежать одной IP-подсети.

Сеть, объединенная с помощью мостов, очень легко может быть "переполнена" трафиком широковещательных и групповых сообщений, если приложения генерируют такой вид данных. Например, мультимедийные приложения, такие, как приложения для видеоконференций по протоколу IP, создают трафик групповых сообщений.

Фреймы, посланные всеми участниками конференции, распространяются по всем сегментам. И сеть, в сущности, становится одной гигантской сетью с общим доступом. Пропускная способность также становится разделяемой.

В большинстве сетей фреймы преимущественно не являются широковещательными. Некоторые протоколы генерируют подобный трафик больше, чем остальные приложения, но число широковещательных фреймов, генерируемых разными протоколами, составляет лишь небольшой процент от того объема, который сеть способна эффективно передать.

В каких случаях необходимо использовать мосты? Каковы преимущества в использовании мостов по сравнению с повторителями? Что происходит в случае, когда станции обмениваются одноадресными фреймами? Как мосты обрабатывают такой вид трафика?

В случае, когда устройство-отправитель и устройство-получатель подключены к одному интерфейсу, мост фильтрует соответствующие фреймы и не передает трафик на остальные интерфейсы (если фрейм не является широковещательным или фреймом групповой пересылки). Если отправитель и получатель подключены к различным портам моста, то мост перенаправляет фрейм в соответствующий интерфейс, чтобы он мог быть доставлен получателю. Процесс фильтрации и селективного перенаправления позволяет сохранить пропускную способность на других сегментах, что является существенным преимуществом мостов по сравнению с повторителями, которые не имеют функции дифференциации фреймов.

Когда мост осуществляет перенаправление трафика, он не меняет содержимого фреймов. Так же, как и в случае повторителя, мост не проводит никакой обработки фрейма, кроме "очистки" сигнала перед его отправкой через другой порт. При прохождении фрейма через мост адреса второго и третьего уровней остаются без изменений. В отличие от мостов маршрутизаторы изменяют адреса второго уровня.

Существует эмпирическое правило "80/20", которое необходимо учитывать при проектировании сетей с использованием мостов. Согласно данному правилу использование мостов наиболее эффективно, если 80 процентов трафика сосредоточены в локальном сегменте, а 20 процентов трафика перенаправляются мостом в другие сегменты. В основе рассматриваемого правила лежит традиционный способ построения

сетей, когда серверные ресурсы находятся в том же сегменте, что и клиентские устройства, которые ими обслуживаются.

Клиентским устройствам не часто приходится обращаться к станциям, подключенным к другим портам моста. Сети с использованием мостов считаются правильно спроектированными, если соблюдается правило 80/20. В случае поддержания рассмотренного выше баланса трафика каждый сегмент сети обеспечивает полную пропускную способность. Если же баланс нарушается и большая часть трафика проходит через мост, вместо того, чтобы фильтроваться, то сеть начинает работать так, как если бы все сегменты принадлежали сети с разделяемой пропускной способностью. В рассмотренном случае мост позволяет образовать цепь доменов коллизий и увеличить протяженность сети, но без каких-либо улучшений пропускной способности.

Рассмотрим наихудший случай, когда трафик в сети с мостом распределен как 0/100, т.е. локальный трафик отсутствует и все устройства-отправители передают информацию на другие сегменты. В случае использования двухпортового моста вся система обеспечивает только разделяемую пропускную способность и совсем не обеспечивает изоляцию пропускной способности отдельных сегментов. Использование моста позволяет только лишь расширить географические размеры сети, но не обеспечивает рост пропускной способности. К сожалению, во многих внутренних сетях организаций преобладает именно такой вид трафика с типичным соотношением 20/80, а не 80/20. Такая ситуация возникает потому, что многие пользователи пытаются получать информацию из сети Internet или обмениваться информацией через Internet. Большинство трафика передается из локальных сегментов через соединения с распределенными сетями (WAN) и таким образом пересекает границу широковещательного домена.

Другим преимуществом использования мостов является то, что они не передают в другие сегменты фреймы, содержащие ошибки. Если мост определяет, что фрейм содержит ошибку или допустимые для используемого метода доступа к физической среде передачи размеры нарушены, то мост отбрасывает такой фрейм. Данная функция защищает сегмент получателя от поврежденных фреймов, т.к. они требуют затрат пропускной способности, а устройство-получатель в любом случае отбросит фрейм, содержащий ошибки при его обработке. Наличие коллизий в сетях, которые работают на основе старых технологий с общим доступом к среде передачи, часто приводит к появлению в сети отдельных фрагментов фреймов, которые иногда называют карликовыми (runt) фреймами. Для таких фреймов нарушено правило минимально допустимого размера, для технологии Ethernet составляющего 64 байта. Повторитель

перенаправляет карликовые фреймы во все сегменты, в то время как мост препятствует их распространению.

### 6.3. Сегментация локальных сетей с помощью маршрутизаторов

Уровень 3, на котором работают мосты, на один выше, чем уровень работы повторителей, что позволяет получить новые функции для инфраструктур, в которых используются мосты, по сравнению с сетями, в которых используются повторители. Мосты выполняют все функции повторителей, и кроме того, позволяют создавать новые домены коллизий. Точно так же маршрутизаторы, которые работают на третьем уровне модели OSI, позволяют получить больше функций по сравнению с мостами. Маршрутизаторы, подобно мостам, 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

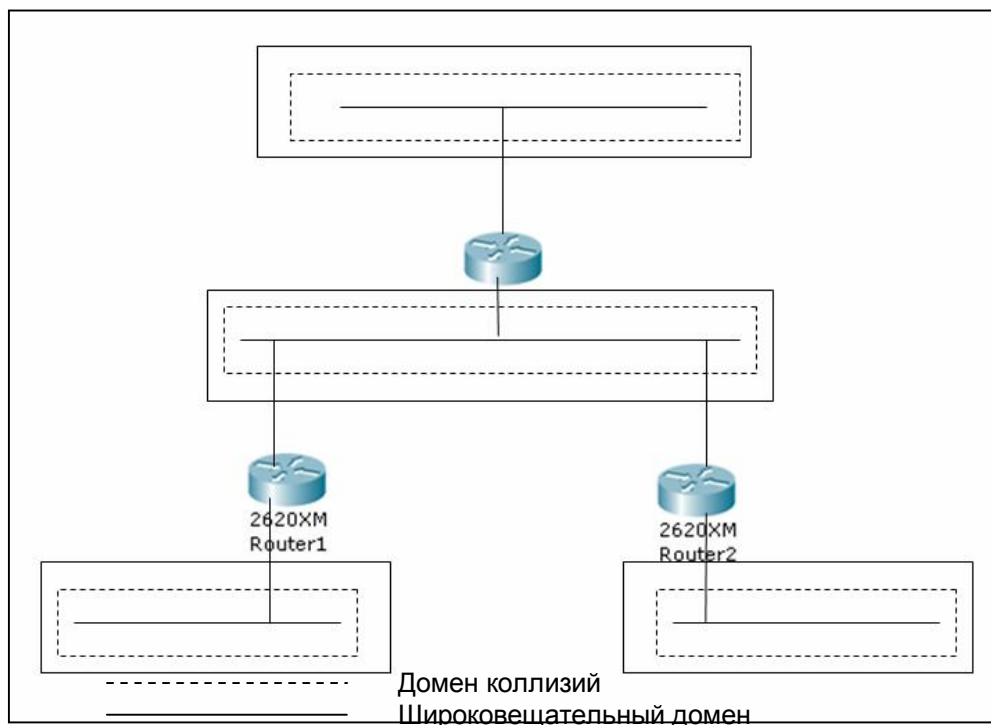


Рис 30. Домены коллизий и широковещательные домены в сети с маршрутизаторами

осуществить с помощью мостов. Блокировка распространения широковещательных сообщений маршрутизаторами определяет границы широковещательного домена — области, за пределы которой не выходят широковещательные сообщения, которые распространяются в сети. На рисунке 30 показана сеть, построенная на основе маршрутизаторов, и показаны границы доменов коллизий и широковещательных доменов.



#### ***6.4. Сравнение применения мостов с коммутацией в локальной сети***

Переключатели уровня 2 являются мостами с большим числом портов. Однако между ними есть несколько важных отличий:

- Мосты реализованы программно, а переключатели — аппаратно, поскольку переключатели могут использовать микросхемы ASIC во время принятия решений о фильтрации данных.
- Мосты способны обслужить только один экземпляр покрывающего дерева на устройство, а переключатели — несколько покрывающих деревьев.
- Мосты содержат не более 16 портов, а переключатели могут иметь сотни портов.

#### ***6.5. Три функции коммутации уровня 2***

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

- Изучение адресов. Переключатели 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, переключатель анализирует аппаратный адрес назначения и ищет в своей базе данных MAC-адресов нужный интерфейс.
- Исключение заикливания. Если между переключателями для избыточности создано несколько путей, то могут появиться заикленные пути передачи информации. Протокол STP (Spanning-Tree Protocol — протокол покрывающего дерева) позволяет исключить заикливание пакетов в сети при сохранении избыточности.

##### **6.5.1. Изучение адресов**

После включения питания переключателя 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. Переключатель не делает самостоятельных решений о перенаправлении кадров, поскольку не знает о местонахождении устройства назначения.

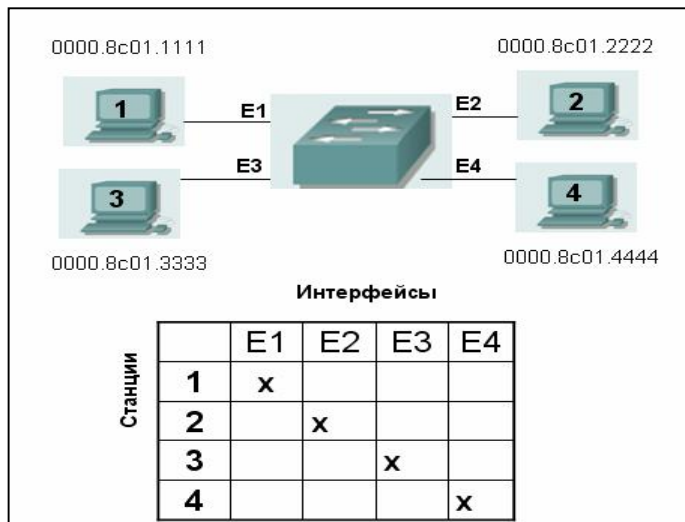
Если устройство отвечает и посылает кадр обратно, то переключатель извлекает адрес источника из возвращенного кадра и помещает MAC-адрес в свою базу данных, причем связывает этот адрес с интерфейсом, получившим кадр. Теперь переключатель имеет в таблице фильтрации два MAC-адреса и может установить соединение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

концентратора. В сетях с концентраторами кадры перенаправляются во все выходные порты устройства.

На рисунке показаны четыре подключенные к переключателю хоста.

После включения питания переключателя, 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. Переключатель принимает кадр в интерфейсе E0/1 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.

Рис 31. Изучение адресов

Переключатель 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.

### **6.5.2. Решение о фильтрации**

Когда кадр попадает в интерфейс переключателя, 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. Переключатель 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 фшльтрацией 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).

## **6.6. Типы переключателей локальных сетей**

Задержка коммутации пакетов в переключателе зависит от выбранного режима работы. Существуют три режима работы переключателей:

- Store and forward (сохранить и передать) В буфер переключателя записывается весь кадр данных, проверяется CRC, а затем в таблице фильтрации MAC-адресов выбирается адрес назначения для полученного кадра.
- Cut-through (сквозной) Переключатель только ожидает получения аппаратного адреса назначения, а затем производит по нему поиск в таблице фильтрации MAC-адресов.
- FragmentFree (без фрагментации) Режим называют модифицированным сквозным режимом (modified cut-through). Производится проверка первых 64 байтов кадра для фрагментации (из-за возможных конфликтов в сегменте) перед перенаправлением кадра.

### **6.6.1. Режим сохранить и передать**

Переключатель в режиме "сохранить и передать" является одним из трех основных типов переключателей локальных сетей. В таком режиме переключатель локальной сети полностью копирует кадр в собственный встроенный буфер и проверяет контрольную сумму CRC. Поскольку копируется весь кадр, задержка

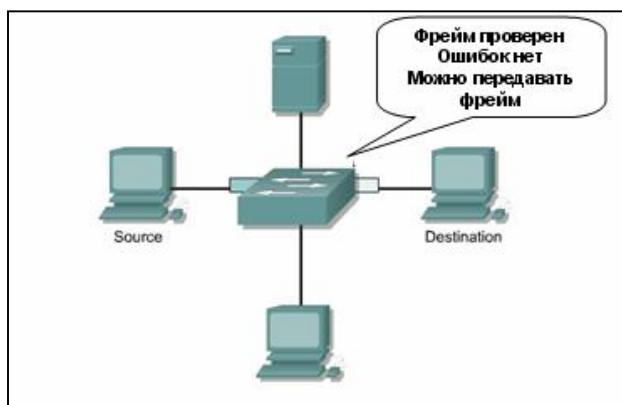


Рис 32. Режим сохранить и передать

коммутации переключателя зависит от длины кадра.

При ошибке CRC кадр отбрасывается, а также отбрасываются слишком короткие (менее 64 байтов, включая CRC) или слишком длинные (более 1518 байтов, включая CRC) кадры. Если в кадре не обнаружено ошибок, переключатель локальной сети выполняет поиск по аппаратному адресу назначения в своей таблице коммутации или перенаправления и выявляет выходной интерфейс для кадра. Затем кадр отправляется через выбранный интерфейс в точку назначения.

### **6.6.2. Сквозной режим**

Еще одним основным типом переключателей в локальных сетях являются устройства, работающие в сквозном режиме. В этом режиме переключатель копирует в собственный встроенный буфер только адрес назначения (первые шесть байтов после преамбулы). Затем ищется аппаратный адрес

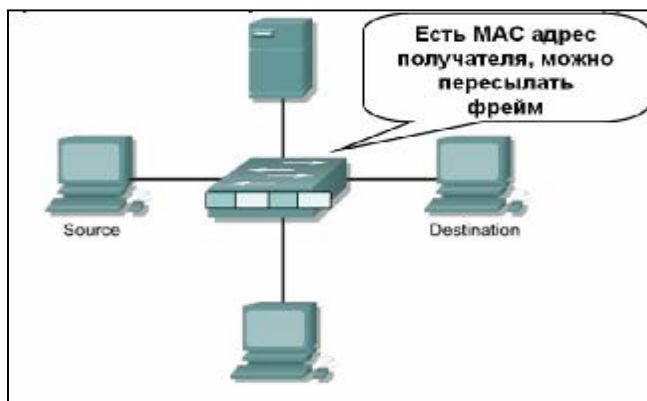


Рис 33. Сквозной режим

назначения в MAC-таблице переключателя, чтобы определить выходной интерфейс и направить в него кадр. Сквозные переключатели обеспечивают низкую задержку, поскольку начинают пересылку кадра сразу после чтения адреса назначения и выявления выходного интерфейса.

Некоторые переключатели могут настраиваться на сквозной режим для каждого отдельного порта. Причем этот режим действует до превышения установленной пользователем границы ошибок. Затем устройство автоматически переходит в режим "сохранить и передать", чтобы предотвратить дальнейшее распространение ошибок. Если же уровень ошибок для порта возвращается в установленные пределы, переключатель автоматически возвращается в сквозной режим.

### **6.6.3. Бесфрагментный режим**

Режим FragmentFree является модифицированной версией сквозного режима, причем переключатель. Ожидает заполнения окна конфликтов (64 байта) до выполнения перенаправления. Если обнаруживается ошибка в принятом пакете, то она всегда проявляется в первых 64 байтах. Бесфрагментный режим обеспечивает лучшую проверку на ошибки по сравнению со сквозным режимом (в частности, за счет того, что не происходит увеличения задержки на длинных кадрах).

## 7. 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.

### 7.1. 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:

- Виртуальные сети работают на 2-м и 3-м уровнях эталонной модели OSI.
- Обмен информацией между виртуальными сетями обеспечивается маршрутизацией 3-го уровня.

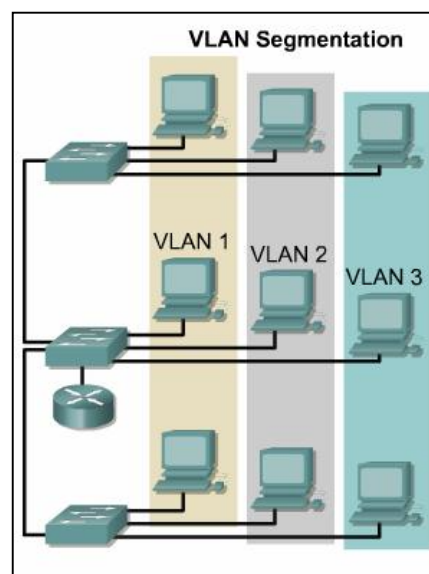


Рис 34. Виртуальные сети и физические границы

- 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.

## ***7.2. 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. В следующих разделах описаны пять причин, которые приводят к необходимости реализации виртуальных локальных сетей.

### **7.2.1. 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 ЮBaseT, 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 35. 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 35, 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 по пользователям, подключенным к сети VLAN (см. рис. 36).

Станция А, показанная на рисунке 36, 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, коммутируемой сети

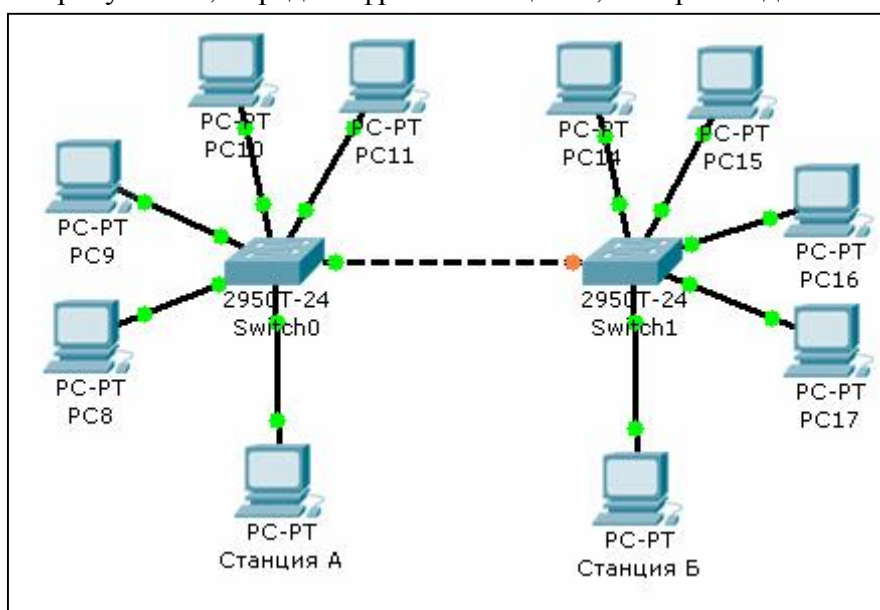


Рис 36. Распространение известных одноадресных фреймов в

принадлежат ли они одной сети VLAN или различным сетям VLAN. Такая функция



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. Следует заметить, что такая функция, как протокол управления группами корпорации Cisco (Cisco Group Management Protocol — CGMP), при активизации позволяет ограничивать передачу многоадресатных сообщений.

### **7.2.2. Проблема 2: распространение широковещательных сообщений**

К сожалению, многие (если не все) протоколы создают трафик широковещательных сообщений. Одни протоколы создают больше широковещательного трафика, другие — меньше. Многим нравятся персональные компьютеры Macintosh. Однако сетевые администраторы ненавидят их в связи с тем, что они генерируют большой объем трафика широковещательных сообщений. Каждые 10 с маршрутизаторы, работающие по протоколу AppleTalk, отправляют широковещательные сообщения с обновлениями таблиц маршрутизации. 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. Протокол IPX генерирует широковещательные фреймы для передачи фреймов протоколов SAP и GNS.

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.

### **7.2.3. 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. Если фрейму необходимо пройти через мост, то мост перенаправляет фрейм в один необходимый интерфейс, а не в какие-либо другие интерфейсы. Если мост (коммутатор) не имеет информации о том, к какому порту

подключено устройство-получатель, то фрейм перенаправляется на все порты, входящие в широковещательный домен (локальную сеть).

Хотя каждый порт коммутатора Catalyst работает так же, как и порт моста, тем не менее, существуют исключения. Коммутаторы семейства Catalyst могут работать с групповыми коммутирующими модулями (group switch module), в которых все порты работают как порты концентратора с разделяемым доступом. Когда устройства подключаются к портам таких модулей, они совместно используют пропускную способность, как и в случае сети старого типа. Данный модуль необходимо использовать в случае, когда предъявляются высокие требования к плотности разъемов подключения, и при низких требованиях к пропускной способности сети и необходимости подключения к сети VLAN.

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 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 37, 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.

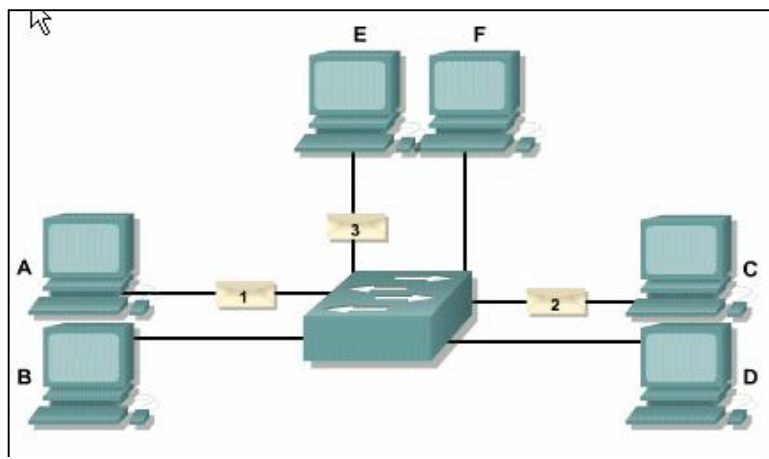


Рис 37. Параллельная передача данных коммутатором

Пары станций A/F, C/B и D/E Catalyst

могут обмениваться друг с другом информацией без какого-либо побочного воздействия на другие взаимодействующие станции.

#### **7.2.4. Проблема 4: задержки при передаче данных через маршрутизаторы**

В сетях старого типа, как показано на рисунке 35, 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-acknowledge). 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.

#### **7.2.5. Проблема 5: сложные списки контроля доступа**

Маршрутизаторы Cisco позволяют пользователям применять различные политики контроля трафика в сети. Списки контроля доступа (access list) позволяют контролировать прохождение трафика в сети с различными уровнями детализации политики управления. С помощью списков контроля доступа можно запретить отдельному пользователю обмениваться данными с другим пользователем, а также запретить пользователям целой сети обмениваться данными с пользователями другой сети или с отдельным пользователем какой-либо сети. Такие возможности могут быть использованы с целью

обеспечения безопасности или с целью предотвращения прохождения трафика через определенный сегмент для обеспечения большей пропускной способности такого сегмента.

В любом случае работа со списками контроля доступа достаточно обременительна. Списки контроля доступа должны соответствовать правилам, разработанным корпорацией, для того, чтобы фильтрация трафика происходила корректно.

В сети, показанной на рисунке 35, фильтры на маршрутизаторах могут быть установлены таким образом, чтобы трафик проходил через сегмент технического отдела, однако при этом на обмен информацией с любым устройством технического отдела наложен запрет. Однако, такой вариант не позволяет избежать того, чтобы служащие технического отдела не могли осуществлять мониторинг трафика, а только лишь предотвращает возможность прямого обмена трафиком между устройствами технического отдела и бухгалтерии. Пользователи бухгалтерского отдела никогда не смогут перехватывать трафик технического отдела, однако техническому отделу доступен весь проходящий трафик бухгалтерии.

Сети VLAN позволяют решить существующую проблему путем помещения всех пользователей бухгалтерского отдела в одну сеть VLAN. Таким образом, не будет необходимости передавать трафик через маршрутизаторы для того, чтобы пользователи, подключенные к одной сети VLAN, могли обмениваться информацией. Такое решение также позволяет упростить разработку списков контроля доступа, т.к. сети теперь можно считать группами пользователей с одинаковыми правами.

### 7.3. 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.

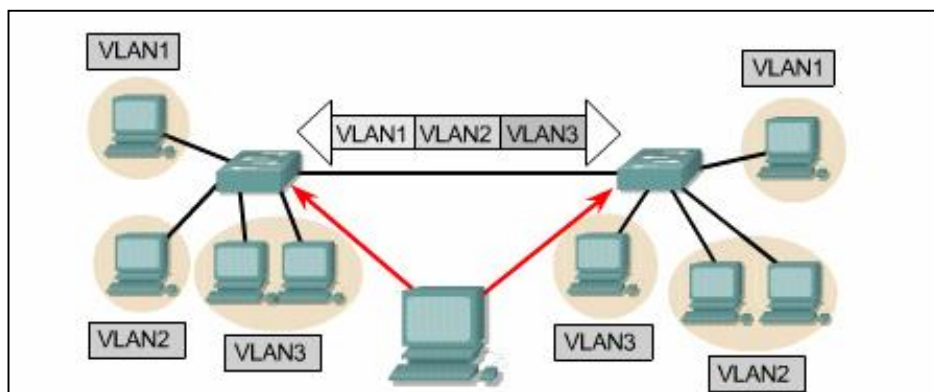


Рис 38. Статические сети VLAN

#### **7.4. Динамические сети VLAN**

Динамические сети VLAN автоматически отслеживают присваивание узлов. Использование интеллектуального программного обеспечения сетевого управления допускает формирование динамических VLAN на основе аппаратных адресов (MAC), протоколов и даже приложений. Предположим, MAC-адрес был введен в приложение централизованного управления VLAN. Если порт будет затем подключен к неприсвоенному порту переключателя, база данных управления VLAN найдет аппаратный адрес, присвоит его и сконфигурирует порт переключателя для нужной сети VLAN. Это упрощает административные задачи по управлению и настройке. Если пользователь перемещается в другое место сети, порт переключателя будет автоматически присвоен снова в нужную сеть VLAN. Однако для первоначального наполнения базы данных администратору придется поработать.

#### **7.5. Идентификация сетей VLAN**

Сеть VLAN может распространяться на несколько соединенных переключателей. Устройства в такой коммутационной фабрике отслеживают 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 802.1q. 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 приотказе магистральной линии.

### 7.6. Маркировка кадров

Переключателю объединенной сети необходимо отслеживать пользователей и кадры, которые проходят через коммутационную фабрику и сеть VLAN. Коммутационной фабрикой называют группу переключателей, 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

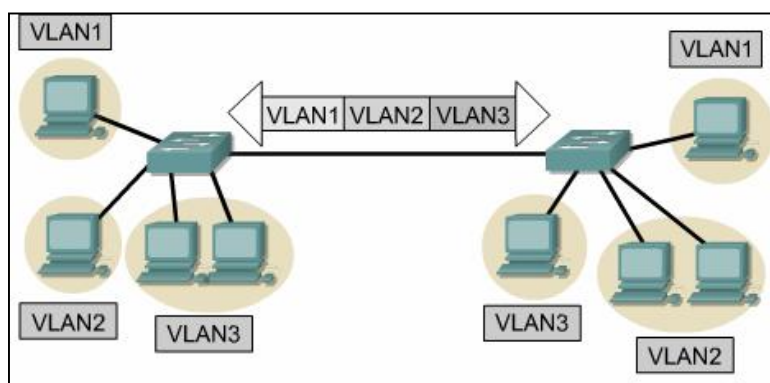


Рис 39. Маркировка кадров

метод маркировки кадров, используемый для передачи

кадров Ethernet по магистральным связям. Маркер (tag) сети VLAN удаляется перед выходом кадра из магистральной связи.

Любой получивший кадр переключатель обязан идентифицировать VLAN ID, чтобы определить дальнейшие действия с кадром на основе таблицы фильтрации. Если кадр попадает в переключатель, 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, переключатель удаляет идентификатор VLAN. Оконечное устройство получит кадр без какой-либо информации о сети VLAN.

### 7.7. 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 802.1q, который обеспечит работу магистральной связи. LANE

### ***7.8. 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 экономить средства за счет использования уже существующих концентраторов.

### ***7.9. 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.

Виртуальные сети обладают значительными преимуществами перед обычными локальными сетями, поскольку они требуют меньших изменений при прокладке кабелей, при установке конфигурации сети и уменьшают время, требуемое для отладки.



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.

### 7.10. 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.

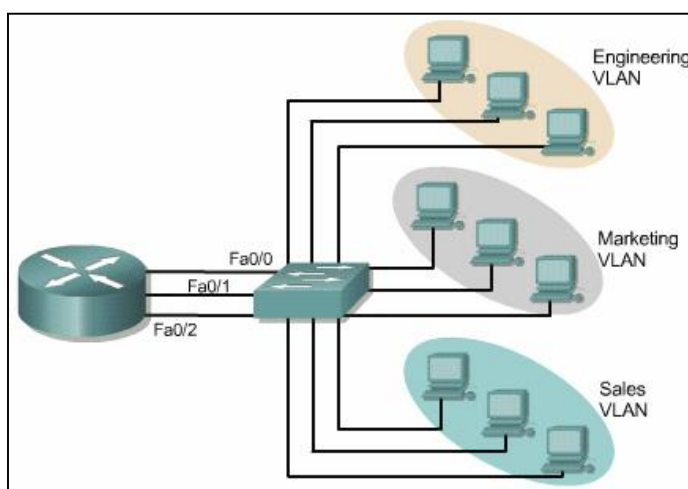


Рис 40. Управление широковещанием

Недостатком такой сети является ее повышенная чувствительность к широковещательному потоку

через коммутаторы, порты и магистральные каналы.

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.

### ***7.11. 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. Ограничения доступа могут основываться на адресах станций, типах приложений или типах протоколов.

### ***7.12. 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 строки 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.

#### **7.12.1. 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.

Система, состоящая из нескольких коммутаторов, как в случае, показанном на рисунке. 41, может содержать несколько сетей VLAN.

Каждая сеть VLAN, показанная на рисунке. 41, поддерживает несколько протоколов. Для связи

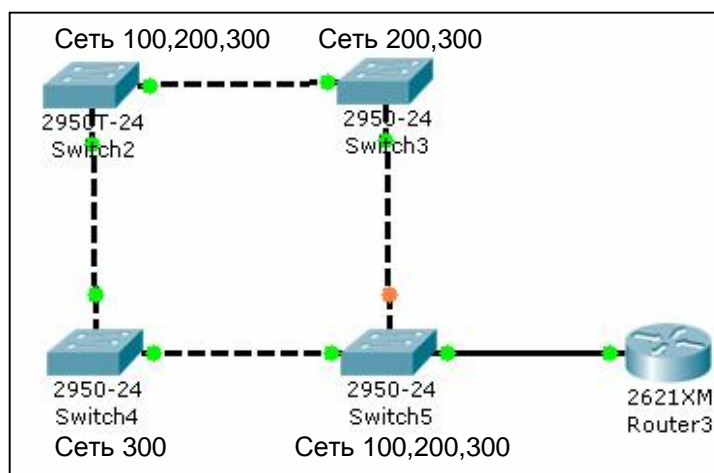


Рис 41. Планирование сетей VLAN

сетей друг с другом информация должна передаваться через

маршрутизатор. Маршрутизатор, показанный на ответвлении сети, используется для соединения сетей друг с другом. Ниже представлен конфигурационный файл такого маршрутизатора.

Файл конфигурации маршрутизатора, показанного на рисунке. 41

```
interface fastethernet 2/0.1
ip address 172.16.10.1 255.255.255.0
ipx network 100
encapsulation isl 100 interface fastethernet 2/0.2
ip address 172.16.20.1 255.255.255.0
ipx network 200
encapsulation isl 200 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 ширококестельные 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 ширококестельный 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 ширококестельным 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 `/х`. Например, подынтерфейс 3 в примере определяется как **`int fastethernet 2/0.3`**, где `.3` задает подынтерфейс, соответствующий главному интерфейсу.

Какие из сетей, показанных в примере, являются изолированными друг от друга? Сеть протокола IPX с номером 300 является изолированной, поскольку в конфигурации маршрутизатора данная сеть не определена для других интерфейсов.

Иногда физическая конфигурация сети может сбивать с толку. Вопрос: "Можно ли это сделать с помощью сетей VLAN?". Часто ответ может быть найден путем представления логической конфигурации сетей VLAN. На рисунке 41 показана физическая топология сети. На рисунке каждая сеть VLAN заменена линией, которая маркируется номерами сетей, связанных с каждой сетью VLAN. Такое более традиционное представление помогает при проектировании и использовании сетей VLAN, поскольку сети и их компоненты показаны вместе с их логическими взаимоотношениями.

### **7.12.2. Создание сетей VLAN**

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

Этап 1. Назначить принадлежность коммутатора Catalyst домену VTP.

Этап 2. Создать сеть VLAN.

Этап 3. Связать порты с сетью VLAN.

Для упрощения процесса создания, удаления и работы с сетями VLAN в коммутаторах Catalyst корпорация Cisco разработала протокол, называемый магистральным протоколом

сетей VLAN (VLAN Trunking Protocol — VTP). Сеть с коммутаторами Catalyst может быть разбита на домены, управляемые по протоколу VTP (VTP management domain) для того, чтобы облегчить некоторые задачи конфигурации и управления.

Домены, управляемые по протоколу VTP, являются грубой аналогией автономных систем в маршрутизируемых сетях, когда группа устройств совместно использует некоторые атрибуты. Коммутаторы Catalyst, принадлежащие одному домену VTP, совместно используют информацию о сетях VLAN. Для того, чтобы получить возможность создавать сети VLAN, необходимо, чтобы коммутатор Catalyst принадлежал какому-либо домену VTP. Для создания сетей VLAN коммутатор Catalyst должен быть сконфигурирован в режиме сервера (server mode) или в прозрачном режиме (transparent mode). Стандартно коммутатор Catalyst работает в режиме сервера.

Конфигурация принадлежности коммутатора Catalyst домену VTP может быть установлена с помощью команды **set vtp domain domain\_name**. Каждый домен должен иметь уникальный идентификатор в виде текстовой строки. Заметим, что имя домена является чувствительным к регистру символов. Таким образом, имя домена Cisco не является совпадающим с именем cisco.

При создании или удалении сети VLAN коммутаторы Catalyst передают с помощью протокола VTP информацию об изменении состояния сети VLAN другим коммутаторам Catalyst, которые входят в общий домен VTP. В том случае, когда какой-либо коммутатор Catalyst, который входит в домен VTP и сконфигурирован как сервер или как клиент, получает данную информацию, он автоматически модифицирует свой список сетей VLAN. Такой метод работы спасает от необходимости повторять команды по созданию одной и той же сети VLAN на всех коммутаторах Catalyst, входящих в один домен. Стоит создать сеть VLAN на одном коммутаторе Catalyst, и все коммутаторы Catalyst, принадлежащие одному домену, автоматически "узнают" о том, что создана новая сеть VLAN. Исключением из правила являются те коммутаторы, которые работают в прозрачном режиме: они игнорируют сообщения протокола VTP.

Коммутаторы Catalyst, работающие в прозрачном режиме, могут использовать только информацию из своей локальной конфигурации.

После того, как коммутатор Catalyst становится членом указанного домена VTP, можно создавать сети VLAN. Для создания сети VLAN в коммутаторе Catalyst необходимо воспользоваться командой **set vlan**.

Следует заметить, что информация по использованию команды указывает на то, что минимальное количество вводимых параметров, необходимых для создания сети VLAN, включает всего один параметр — номер сети VLAN. Могут быть также указаны

необязательные сведения: имя сети VLAN, ее тип и другие параметры. Существует множество дополнительных параметров, необходимых для конфигурации поддержки коммутаторами Catalyst сетей VLAN для работы в рамках технологий Token Ring или FDDI. Если имя сети VLAN не указано, то коммутатор Catalyst назначает ей стандартное имя VLAN#. Если не указан тип сети VLAN, коммутатор использует для конфигурации тип Ethernet-сеть VLAN. Назначение имени сети VLAN не влияет на производительность коммутатора Catalyst или сети VLAN. При правильном использовании имя позволяет документировать сети VLAN и позволяет администратору вспомнить, для чего сеть VLAN была создана. Для документирования сетей VLAN необходимо использовать имена, имеющие смысл. Такой подход очень помогает при поиске и устранении неисправностей при конфигурировании новых сетей.

После создания сети VLAN необходимо назначить порты в принадлежность заданной сети VLAN. Для назначения портов сети VLAN используется та же команда, что и для создания сети VLAN. В примере ниже показано, как необходимо назначать набор портов в принадлежность сети VLAN с номером 2. К сожалению, в первый раз команда в примере была введена неправильно. Что в же этой команде было не так? При первом вводе команда **set vlan** не выполнялась из-за того, что в указанном диапазоне портов присутствовал несуществующий интерфейс модуля Supervisor. Запись 1/8 означает восьмой порт модуля Supervisor.

Пример. Назначение портов в принадлежность сети VLAN

```
Console> (enable) set vlan 2 2/1-1/8
```

```
Usage: set vlan <vlan num> <mod/ports...>
```

```
(An example of "mod/ports is 1/1,2/1-12,3/1-2,4/1-12)
```

```
Console> (enable) set vlan 2 2/1-2/8
```

```
VLAN 2 modified.
```

```
VLAN 1 modified.
```

После того, как параметры команды назначения принадлежности портов указаны корректно, коммутатор Catalyst переназначает блок портов в принадлежность сети 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.

### **7.12.3. Удаление сетей VLAN**

Сети VLAN из обслуживаемого домена могут быть удалены с помощью команды **clear vlan VLAN\_number**. Например, если необходимо удалить сеть VLAN с номером 5 из домена, управляемого по протоколу VTP, следует воспользоваться командой **clear vlan 5** на коммутаторе, который сконфигурирован в качестве сервера, обслуживающего домен VTP. На коммутаторе, сконфигурированном в качестве клиента, работающего по протоколу VTP, сети VLAN удалять нельзя. Если коммутатор Catalyst сконфигурирован для работы в прозрачном режиме, то сеть VLAN также может быть удалена. Однако в таком случае сеть VLAN удаляется только на одном коммутаторе Catalyst и не удаляется на всех остальных коммутаторах управляемого домена. Все процедуры удаления и добавления сетей VLAN на коммутаторе Catalyst, работающем в прозрачном режиме, осуществляются локально для данного коммутатора.

При попытке удалить сеть VLAN коммутатор Catalyst выдает предупреждение, что все порты домена VTP, принадлежащие удаляемой сети 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. Если сеть VLAN существует, то порты становятся активными, если же сеть VLAN не существует, порты становятся неактивными. Если вдруг будет удалена сеть VLAN, к которой подключены активные пользователи, то такое действие может привести к катастрофическим последствиям.

Следует также понимать, что если в домене, управляемом по протоколу VTP, большинство коммутаторов Catalyst сконфигурированы как клиенты или серверы про-



токола VTP и небольшое количество коммутаторов Catalyst сконфигурировано для работы в прозрачном режиме, то по недосмотру может произойти другая ситуация, когда сеть VLAN удаляется на коммутаторе Catalyst, работающем в прозрачном режиме, и при этом в домене, управляемом по протоколу VTP, существует сеть VLAN с таким же номером. Например, предположим, что в сети установлены три последовательно подключенных коммутатора Catalyst, коммутатор Catalyst-A сконфигурирован в режиме сервера, коммутатор Catalyst-B — в прозрачном режиме, а коммутатор Catalyst-C — в режиме клиента или сервера. Каждый из коммутаторов обслуживает устройства, которые подключены к сети VLAN с номером 10. Таким образом, вся сеть VLAN должна быть создана на коммутаторе Catalyst-B и на коммутаторе Catalyst-A (коммутатор Catalyst-C получает информацию о создаваемой сети из настроек коммутатора Catalyst-A в результате работы протокола VTP). С точки зрения протокола распределенного связующего дерева в такой системе существует один домен распределенного связующего дерева и соответственно — один корневой мост распределенного связующего дерева. Предположим теперь, что администратор решил, что на коммутаторе Catalyst-B больше нет необходимости в сети VLAN 10, поскольку ни одно устройство из подключенных к данному коммутатору больше не принадлежит сети VLAN 10. Таким образом, сеть VLAN 10 на коммутаторе Catalyst-B удаляется с помощью команды `clear vlan 10`. С точки зрения технологии сетей VLAN такие действия вполне допустимы. Однако, с точки зрения протокола распределенного связующего дерева такие действия приводят к появлению двух доменов распределенного связующего дерева. Поскольку коммутатор Catalyst-B больше не участвует в обслуживании сети VLAN, он больше не участвует в работе протокола распределенного связующего дерева для данной сети VLAN. Поэтому каждый из коммутаторов Catalyst-A и Catalyst-C становится корневым мостом для сети VLAN 10, причем каждый в своем домене распределенного связующего дерева.

## 8. ОСНОВЫ ПРОТОКОЛА РАСПРЕДЕЛЕННОГО СВЯЗУЮЩЕГО ДЕРЕВА

С появлением новых технологий и стандартов в индустрии компьютерных сетей в начале 90-х годов появились маршрутизаторы, и протокол STP отошел на второй план как менее важный протокол, который "просто работает". Тем не менее, технологии коммутации продолжали развиваться, и использование протокола STP стало одним из основных факторов, влияющих на производительность сети в целом.

Использование протокола STP в два раза уменьшает количество проблем, связанных с конфигурацией, поиском неисправностей и поддержкой реальных сетей. Профессионалы, хорошо разбирающиеся в устройствах и протоколах третьего уровня модели OSI, приступая к изучению технологии коммутации, обычно задаются вопросом о сложности протокола STP. Протокол STP достаточно сложен для понимания, и найти какую-либо информацию о современных его реализациях достаточно трудно.

Протокол STP позволяет мостам (или коммутаторам) общаться между собой для предотвращения проблем, связанных с физическими петлями в топологии сети. Используемый мостами алгоритм создает беспетельную логическую топологию сети или, другими словами, протокол STP создает структуру в виде дерева с листьями и ветвями, полностью покрывающими инфраструктуру сети на втором уровне модели OSI. Большая часть главы будет посвящена обсуждению механизмов взаимодействия мостов и процессам протокола STP.

Петли возникают в сети по нескольким причинам. Основной причиной является результат намеренной попытки повысить надежность сети за счет избыточных соединений — в случае, когда канал или коммутатор вышли из строя, то оставшиеся работоспособные каналы или коммутаторы принимают на себя функции поврежденного. Не исключается ситуация, что петли могут возникнуть в результате ошибок администратора (несомненно, именно с вами никогда такого не случается)

- Протокол STP обнаруживает и предотвращает формирование мостовых петель второго уровня. Параллельные маршруты могут существовать, но передача фреймов допускается только по одному из них.
- Протокол STP основан на стандарте мостового протокола IEEE 802.ID.
- Коммутаторы запускают по одному экземпляру STP на каждую VLAN-сеть с помощью алгоритма PVST (Per- VLAN Spanning Tree — отдельные экземпляры распределенного связующего дерева для разных сетей VLAN). PVST-алгоритм между коммутаторами требует использования ISL-транкинга.

- В магистральных каналах IEEE 802.1Q разрешено использование только одного экземпляра STP для всех сетей. Общее распределенное связующее дерево (Common Spanning Tree — CST) связывается посредством сети VLAN 1.
- Функция PVST+ является частным расширением, созданным корпорацией Cisco, которое позволяет коммутаторам взаимодействовать между CST и PVST. Блоки данных мостового протокола (Bridge Protocol Data Units — BPDU) режима PVST отправляются по туннелю через магистральный 802.1Q-канал. Коммутаторы Catalyst стандартно используют режим PVST+.
- Многоэкземплярный протокол распределенного связующего дерева (Multiple Instance Spanning Tree Protocol — MISTP) также является частным протоколом корпорации Cisco, который допускает использование одного экземпляра STP для одной или нескольких VLAN-сетей посредством функции отображения (mapping). Такой подход позволяет ускорить конвергенцию с меньшей нагрузкой на процессор и меньшим количеством блоков BPDU. Протокол MISTP отбрасывает BPDU-блоки PVST+.
- MISTP-PVST+ — гибридный STP-режим, который используется для перехода ; между режимами PVST+ и MISTP в сети. BPDU-блоки обоих режимов распознаются и не уничтожаются.
- Множественные распределенные связующие деревья (Multiple Spanning Tree — MSI), основанные на стандарте IEEE 802.1s, расширяют ускоренный протокол распределенного связующего дерева (802.1w Rapid Spanning Tree Protocol — RSTP) до нескольких экземпляров STP.
  - Режим MST обладает обратной совместимостью с STP-режимами 802.1D, 802.1w и PVST+.
  - Коммутаторы, сконфигурированные с общими VLAN-назначениями и экземпляром STP, формируют отдельную MST-область (region).
  - MST-структуры для обеспечения взаимодействия способны генерировать блоки BPDU PVST+.
  - Режим MST поддерживает до 16 экземпляров STP.
- Коммутаторы отправляют BPDU-блоки через все порты по одному разу в течение каждого интервала hello-таймера (стандартно — 2 секунды).
- Блоки BPDU не перенаправляются коммутатором, они применяются только для дальнейшего вычисления и генерирования BPDU.
- Коммутаторы отправляют два типа BPDU-блоков:
  - конфигурационные сообщения BPDU;

- о уведомления об изменении топологии (Topology Change Notification — TCN BPDU).

### **8.1. STP-процесс**

1. Выбор корневого моста (root bridge). Коммутатор с наименьшим идентификатором моста становится корневым узлом распределенного связующего дерева. Идентификатор моста (bridge ID) составляется из двухбайтового значения приоритета и шестибайтового MAC-адреса. Приоритет может варьироваться от 0 до 65535, стандартное значение — 32768.

2. Выбор корневого порта (root port). Каждый некорневой коммутатор путем определения порта с наименьшей стоимостью корневого маршрута выбирает корневой порт или порт, "ближайший" к корневому мосту. Значение стоимости транспортируется в составе блока BPDU. Каждый некорневой коммутатор маршрута добавляет стоимость своего локального порта, па котором принимается BPDU-блок. Стоимость корневого маршрута накапливается по мере создания новых BPDU-блоков.

3. Выбор назначенного порта (designated port). Один порт коммутатора в каждом сетевом сегменте выбирается для обработки трафика данного сегмента. Порт, объявивший наименьшую стоимость корневого маршрута в сегменте, становится назначенным.

4. Удаление мостовых петель. Порты коммутатора, не являющиеся ни корневыми, ни назначенным, переводятся в состояние блокировки. На этом этапе уничтожаются все возможные мостовые петли.

### **8.2. Схема разрешения конфликтов в STP**

Если какое-либо STP-решение имеет идентичные или совпадающие состояния, то окончательное решение базируется на описанной ниже последовательности условий.

1. Выбор наименьшего BID -идентификатора.
2. Выбор наименьшей стоимости корневого маршрута.
3. Выбор наименьшего BID-идентификатора отправителя.
4. Выбор наименьшего идентификатора порта.

### **8.3. Состояния портов в STP**

Каждый порт коммутатора последовательно проходит ряд состояний.

1. Отключен. Административно отключенные порты или порты, отключенные ввиду возникновения сбоя. В режиме MST такое состояние называется отбрасывающим (discarding).

2. Блокировка. Состояние, которое применяется после инициализации порта. Порт в состоянии блокировки не может принимать или передавать данные, добавлять MAC-

адреса в свою адресную таблицу, он может лишь принимать блоки BPDU. При обнаружении мостовой петли либо потери портом статуса корневого или назначенного порт возвращается в состояние блокировки. В режиме MST такое состояние называется отбрасывающим.

3. Прослушивание. Если порт может стать корневым или назначенным, он переводится в состояние прослушивания, при котором не может принимать или передавать данные, добавлять MAC-адреса в свою адресную таблицу, но может получать и отправлять BPDU-блоки. В режиме MST такое состояние называется отбрасывающим.

4. Состояние самообучения. По истечении таймера задержки передачи (стандартно — 15 секунд) порт входит в состояние самообучения (learning state). Он не может передавать данные, но может получать и отправлять BPDU-блоки. В этом состоянии порт может изучать MAC-адреса и добавлять их в адресную таблицу.

5. Состояние передачи. По истечении следующей задержки передачи (стандартно — 15 секунд) порт переходит в состояние передачи, при котором он может отправлять и принимать данные, изучать MAC-адреса, а также отправлять и принимать BPDU-блоки.

#### **8.4. Изменения STP-топологии**

- • Если порт переводится в состояние передачи (кроме случая, когда включена функция PortFast), отправляется уведомление об изменении топологии.
- • Если порт переводится из состояния самообучения или передачи в состояние блокировки, отправляется уведомление об изменении топологии.
- • Для объявления об изменении топологии коммутатор периодически (период равен hello-интервалу) отправляет в свой корневой порт TCN BPDU-блоки. Отправка BPDU происходит до тех пор, пока не будет получено TCN-подтверждение от соседа вышестоящего выделенного моста. Соседи продолжают ретранслировать TCN BPDU-блок на свои корневые порты до тех пор, пока он не будет получен корневым мостом.

Корневой мост информирует все распределенное связующее дерево об изменении топологии путем отправки конфигурационного BPDU-блока с установленным битом изменения топологии (Topology Change — TC). В результате все нижестоящие коммутаторы сокращают таймеры старения адресных таблиц на длительность задержки передачи (15 секунд) от стандартного значения (300 секунд). Неактивные MAC-адреса в таком случае удаляются из таблиц быстрее, чем обычно.

### 8.5. Усиление стабильности протокола STP

- Служба STP Root Guard (служба защиты корневого моста) может быть полезна при выборе местоположения корневого моста и при поддержании его уникальности в коммутируемой сети. Когда данная функция включена на каком-либо порту, при получении лучшего BPDU-блока порт отключается, что препятствует другим коммутаторам незапланированно становиться корневыми.
- Служба STP Root Guard должна быть включена на всех портах, где не следует обнаруживать корневой мост. Это позволяет сохранить текущий выбор основного и дополнительного корневых мостов.
- Обнаружение однонаправленной передачи в канале (Unidirectional Link Detection — UDLD) — способ обнаружения канала, в котором передача осуществляется только в одном направлении, что позволяет предотвратить возникновение мостовых петель и "черных дыр" для трафика, которые обычно не обнаруживаются и не предотвращаются протоколом STP.
- Механизм UDLD функционирует на втором уровне путем отправки пакетов, содержащих идентификаторы устройства и порта, соседям, подключенным к портам коммутатора. Также любые UDLD-пакеты, получаемые от соседнего устройства, отражаются для того, чтобы данное устройство получило подтверждение о том, что оно опознано. UDLD-сообщения отправляются в течение интервалов сообщений (message interval), стандартная длительность которых обычно равна 15 секундам.
- Механизм UDLD функционирует в двух режимах.
- Обычный режим. Однонаправленные каналы обнаруживаются и объявляются ошибочными, но никакие действия не предпринимаются.
- Агрессивный режим. Однонаправленные каналы обнаруживаются, объявляются ошибочными и отключаются после восьми попыток (по одной в секунду в течение восьми секунд) переустановки канала. Отключенные порты необходимо включать вручную.
- Функция STP Loop Guard обнаруживает отсутствие BPDU-блоков на корневом и альтернативном корневом портах. Неназначенные порты временно отключаются, что препятствует их переходу в назначенные порты и состояние передачи.
- Функцию STP Loop Guard необходимо включить на корневом и альтернативном корневом портах (оба неназначенные) для всех возможных вариантов активной STP-топологии.

## 8.6. Пример функционирования протокола STP

В качестве примера функционирования протокола STP рассмотрим сеть, состоящую из трех коммутаторов Catalyst, подключенных по схеме треугольника (рис. 42).

Корневые порты отмечаются литерами RP, назначенные порты — DP, метки F соответствуют портам в состоянии передачи, а X — портам, которые находятся в состоянии блокировки.

Рассмотрим выполнение алгоритма распределенного связующего дерева.

1. Выбор корневого моста. Все три коммутатора имеют равные значения приоритета моста (стандартный приоритет равен 32786). В то же время коммутатор Catalyst A имеет наименьший MAC-адрес (00-00-00-00-00-0a), поэтому он становится корневым мостом.

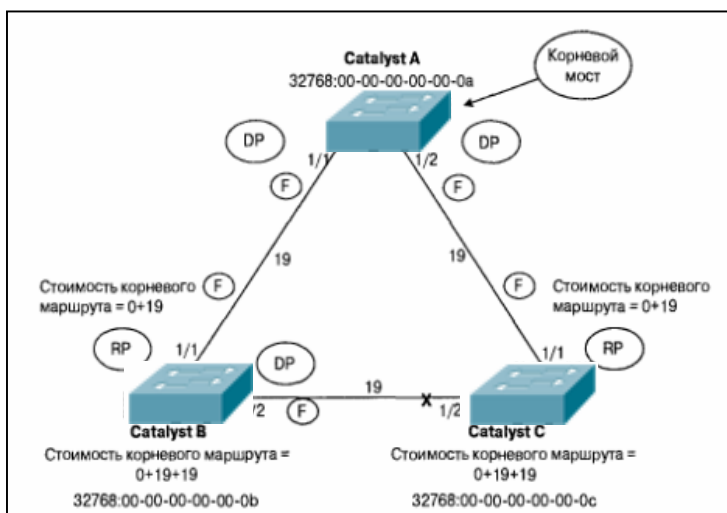


Рис 42. Структура сети для примера функционирования протокола STP

2. Выбор корневых портов. На каждом коммутаторе вычисляются

стоимости корневых маршрутов. На коммутаторе Catalyst B порт 1/1 имеет стоимость корневого маршрута  $0+19$ . Порт 1/1 коммутатора Catalyst C также имеет стоимость корневого маршрута, равную  $0+19$ .

3. Выбор назначенных портов. По определению все порты корневого моста становятся назначенными портами для своих сегментов. Следовательно, порты 1/1 и 1/2 коммутатора Catalyst A являются назначенными. Порт 1/2 коммутатора Catalyst B и порт 1/2 коммутатора Catalyst C совместно используют один сегмент. Требуется, чтобы один из указанных портов стал назначенным. Стоимость корневого маршрута для каждого из портов равна  $0+19+19$ , или 38, что делает невозможным выбор одного из них. Наименьший отправляемый идентификатор моста позволяет решить эту проблему, и порт 1/2 коммутатора Catalyst B (имеющего наименьший адрес из двух) становится назначенным.

4. Все порты, не являющиеся ни корневыми, ни назначенными, переводятся в состояние блокировки. Единственный порт, который не является ни корневым, ни назначенным, — это порт 1/2 коммутатора Catalyst C. Порт переводится в состояние блокировки (отмеченное на схеме литерой X).

## 8.7. Конфигурирование протокола STP

1. Включение или отключение протокола STP (необязательно).

Включение : **set spantree [enable | disable] [vlan]**

Отключение : **[no] spanning-tree [vlan vlan]**

Протокол STP стандартно включен в сети VLAN 1 и в любых недавно созданных VLAN-сетях. Если сеть VLAN не указана, то протокол STP включается или отключается во всех VLAN-сетях. Следует помнить о том, что при отключенном механизме STP мостовые петли не обнаруживаются, а их возникновение не предотвращается. Протокол STP следует включать всегда.

2. Для установки STP-режима для коммутатора необходимо использовать команду:

**set spantree mode {mistp | pvst+ | mistp-pvst+ | mst}**

При стандартных настройках для одного экземпляра STP в каждой VLAN-сети все коммутаторы Catalyst выполняют протокол STP в режиме PVST+. Для настройки других STP-режимов используются ключевые слова mistp (MISTP), mistp-pvst+ (взаимодействие MISTP-PVST+) и mst (MST).

3. Активизация MST-экземпляра.

- а) Идентификация MST-области.

**set spantree mst conf ig {name name} {revision number}**

MST-область идентифицируется по имени (name) (текстовая строка длиной до 32 символов). Если имя не задано, то имя области не используется. Чтобы указать количество изменений конфигурации области, можно использовать номер ревизии области (region revision number). Номер ревизии (number) (от 0 до 65535, стандартно 1) указывается явно и не увеличивается автоматически при изменениях области.

- б) Назначение одной или нескольких VLAN-сетей экземпляру.

**set spantree mst instance vlan vlan**

Номер VLAN-сети (vlan) (от 1 до 1005, от 1025 до 4094) сопоставляется с MST-экземпляром (instance) (от 0 до 15). Это назначение сохраняется в буфере MST-области до тех пор, пока не будут внесены изменения.

- в) Фиксация назначения области.

**set spantree met config commit**

Конфигурационные изменения MST-области помещаются в буфер редактора, который выделяется пользователю, осуществляющему эти изменения. Их необходимо зафиксировать до того, как они станут активными. При фиксации изменений также освобождается буфер редактора и появляется возможность инициировать новый сеанс редактирования,



г) Отмена последних изменений конфигурации области (необязательно).

**set spantree mat conf ig rollback [force]**

Если конфигурационные изменения для MST-области были сделаны ошибочно, их можно отменить при помощи ключевого слова `rollback`. Отмена возможна только для тех изменений, которые еще не были зафиксированы или введены в действие. В ситуации, когда какой-либо пользователь внес изменения и продолжает удерживать буфер редактора, можно при помощи ключевого слова `force` освободить буфер и удалить изменения.

#### 4. Указание корневого моста

Корневой мост (и вторичные корневые мосты) следует размещать вблизи от "центра" сети, для того чтобы вычислять оптимальную топологию распределенного связующего дерева. Как правило, корневой мост располагается на основном уровне или на уровне распределения сети. Если не конфигурировать размещение корневого моста вручную, то корневым становится коммутатор с наименьшим BID-идентификатором. В таком случае почти всегда создается неэффективная топология распределенного связующего дерева.

PVST+: **set spantree root [secondary] [vlans] [dia net-diameter] [hello hello-time]**

MISTP: **set spantree root [secondary] mistp-instance instance [dia net-diameter] [hello hello-time]**

MST: **set spantree root [secondary] met instance [dia net-diameter] [hello hello-time]**

Коммутатор вынужден стать основным корневым мостом для VLAN-сетей (сети с номерами от 1 до 1005 и с 1025 по 4094) или для указанных STP-экземпляров (с 1 по 16) (если VLAN-сеть не указывается, используется сеть VLAN 1). Значение приоритета моста модифицируется следующим образом: если приоритет превышает 8192, то значение устанавливается равным 8192; если значение приоритета меньше 8192, оно устанавливается меньшим приоритета текущего корневого моста. Можно использовать ключевое слово `secondary` для размещения дополнительного или резервного корневого моста тогда, когда основной корневой мост выйдет из строя. В данном случае приоритет моста устанавливается равным 16384. (Для MST приоритет корневого моста устанавливается равным 24576, а приоритет вторичного корневого моста — равным 28672.) Ключевое слово **dia** определяет диаметр либо максимальное количество мостов или коммутаторов между двумя конечными точками сети (от 1 до 7, стандартно 7). Также можно установить hello-интервал (стандартно 2 секунды). Установка диаметра сети приводит к тому, что другие STP-таймеры автоматически пересчитываются и изменяются.

С помощью других команд можно явно отрегулировать таймеры, но настройка диаметра сети позволяет избежать сложности расчета таймеров.

#### 5. Регулировка приоритета моста.

**PVST+: set spantree priority priority vlans**

**MISTP: set spantree priority priority mistp-instance instance-list**

**MST: set spantree priority priority met instance-list**

Кроме того, можно непосредственно модифицировать приоритет моста для достижения значений, отличных от автоматически определенных величин приоритета основного или дополнительного корневого моста. Приоритет можно устанавливать отдельно для каждой VLAN-сети и экземпляра. Экземпляры можно указывать в виде списка (instance-list) как один или несколько экземпляров, разделенных запятыми, или в виде диапазона номеров, заданного с помощью дефиса. Чтобы перевести коммутатор в режим корневого, необходимо выбрать приоритет так, чтобы приоритет корневого моста был ниже приоритета всех остальных коммутаторов в данной VLAN-сети или STP-экземпляре. Значения приоритета моста варьируются в диапазоне от 0 до 65535 (стандартный приоритет равен 23768) для PVST+, для MISTP-режима приоритет выбирается из списка значений: 0 (наивысший приоритет), 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 и 61440 (наименьший приоритет).

#### 6. Предотвращение перехода других коммутаторов в режим корневого моста STP.

**set spantree guard {root | none} mod/port**

**spanning-tree guard {root | none}**

Служба STP Root Guard будет включена на порту или интерфейсе. Если другой мост, подключенный к данному порту, попытается стать корневым, порт будет переведен в STP-состояние root-inconsistent (прослушивание). Если на порту более не обнаруживаются BPDU-блоки, он переводится обратно в нормальное состояние.

#### 7. Настройка стоимости корневого маршрута.

##### а) Установка шкалы стоимости порта.

**set spantree defaultcostmode {short | long}**

**spanning-tree pathcost defaultcost-method {long | short}**

Стандартно коммутаторы в режиме PVST+ используют короткие, или сокращенные (short), 16-битовые значения стоимости порта. Если используются какие-либо порты с полосой пропускания 10 Гбит/с или более, то на каждом коммутаторе в сети следует установить шкалу стоимости порта для расширенных (long), 32-битовых значений. В MISTP, M1STP-PVST+ и MST стандартно используется расширенный режим.

б) Установка стоимости порта для всех VLAN-сетей или экземпляров.

**set spantree portcost mod/port cost [mst]**

Стоимость порта может быть установлена в значение cost (от 1 до 65535 — сокращенный, или MISTP-режим, от 1 до 2000000 — расширенный режим) для всех VLAN-сетей или STP-экземпляров. Ключевое слово mst обозначает порт, используемый в режиме MST.

в) Установка стоимости порта в отдельных VLAN-сетях или экземплярах.

PVST+: **set spantree portvlancost mod/port [cost cost] [vlan-list]**

MISTP: **set spantree portinstancecost mod/port [cost cost] [instances]**

MST: **set spantree portinstancecost mod/port [cost cost] mst [instances]**

Стоимость порта может быть установлена в значение cost (от 1 до 65535 — короткий режим, от 1 до 2000000 — длинный режим) для VLAN-сети vlan-id, списка VLAN-сетей vlan-list или STP-экземпляра (с 0 по 15).

8. Точная настройка приоритета порта.

а) Установка приоритета порта для всех VLAN-сетей или экземпляров.

**set spantree portpri mod/port priority [mst]**

Приоритет порта может устанавливаться в значение priority (от 0 до 63 — для COS или от 2 до 255 — для IOS). Чтобы указать, что порт используется для MST-режима, используется ключевое слово mst.

б) Установка приоритета порта для отдельных VLAN-сетей или экземпляров.

PVST+: **set spantree portvlanpri mod/port priority [vlans]**

MISTP: **set spantree portinstancepri mod/port priority [instances]**

MST: **set spantree portinstancepri mod/port priority met [instances]**

Приоритет порта может устанавливаться в значение priority (от 0 до 63 — для COS или от 2 до 255 — для IOS) для VLAN-сети vlan-id, списка сетей vlan-list или для STP-экземпляра (с 0 по 15).

9. Активизация MISTP-экземпляра (только для MISTP-режима).

а) Включение MISTP-экземпляра.

**set spantree enable mistp-instance {instance | all}**

MISTP-экземпляр 1 стандартно включен. Другие экземпляры можно включить, используя номер экземпляра (instance от 1 до 16) или ключевое слово all.

б) Назначение VLAN-сетей MISTP-экземпляру.

**set vlan vlan-list mistp-instance {instance \ none}**

Чтобы сопоставить одну или несколько VLAN-сетей с одним MISTP-экземпляром, можно задавать номера в виде списка vlan-list. Если случайно одна VLAN-сеть будет назначена нескольким экземплярам, то все ее порты будут переведены в

состояние STP-блокировки. Чтобы отменить назначение VLAN-сетей каким-либо экземплярам, можно использовать ключевое слово `pop`.

#### 10. Обнаружение однонаправленных соединений с помощью функции UDLD.

##### а) Включение функции UDLD на коммутаторе.

**set udld {enable | disable}** Стандартно функция UDLD отключена. Прежде чем использовать ее на определенных портах, ее необходимо включить. В операционной системе Supervisor IOS допускается использование ключевого слова `aggressive` для глобального включения агрессивного режима UDLD на всех волоконно-оптических Ethernet-интерфейсах.

##### б) Регулировка интервала UDLD-сообщений.

##### **set udld interval interval**

Интервал UDLD-сообщений может быть установлен равным значению параметра `interval` (от 7 до 90 секунд; стандартные значения равны 15 и 60 секунд для систем COS и Supervisor IOS соответственно).

##### в) Включение функции UDLD на определенных портах.

##### **set udld {enable | disable} mod/port**

После глобального включения на коммутаторе функции UDLD она стандартно включается также на всех волоконно-оптических Ethernet-портах. На всех Ethernet-портах для витой пары функция UDLD стандартно отключена.

##### г) Включение агрессивного режима UDLD на определенных портах.

##### **set udld aggressive-mode {enable | disable} mod/port**

После включения на каком-либо порту агрессивного режима порт отключается, если обнаружено однонаправленное соединение. После устранения проблемы порт необходимо включить вручную. В операционной системе Supervisor IOS для включения всех портов, отключенных функцией UDLD, используется команда `udld reset EXEC-режима`.

#### 11. Повышение стабильности протокола STP с помощью функции Loop Guard (защита от петель).

##### **set spantree guard loop mod/port**

Службу Loop Guard следует включать только на тех портах, о которых точно известно, что они корневые или альтернативные корневые. Например, внешние порты коммутатора уровня доступа всегда будут корневыми или альтернативными корневыми, поскольку находятся наиболее близко к корневому мосту. (При этом предполагается, что корневой мост расположен вблизи центра сети.)

## 9. ПРОТОКОЛ МАГИСТРАЛЬНЫХ КАНАЛОВ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

Протокол VTP является фирменным протоколом корпорации Cisco и представляет собой протокол многоадресатных сообщений второго уровня, который способен облегчить некоторые административные трудности, связанные с поддержкой виртуальных локальных сетей. Протокол VTP определяет соответствие сетей VLAN всем типам передающей среды (media types) и методам разметки виртуальных локальных сетей (VLAN tagging methods) между коммутаторами, а также осуществляет согласование конфигурации сети. Данный протокол способствует сокращению операций, которые необходимо выполнить вручную для настройки коммутаторов при добавлении новой сети VLAN, когда она расширяется к другим коммутаторам сети. Более того, протокол VTP минимизирует потенциальную возможность несоответствий конфигурации и управляет добавлением, удалением и переименованием виртуальных локальных сетей в более безопасном режиме, чем это возможно при ручном изменении настроек для каждого коммутатора.

Довольно часто пользователи путают различия между протоколами VTP, ISL, 802.1Q, DISL и DTP. Все перечисленные протоколы предполагают использование магистральных каналов (trunks), но имеют различное назначение.

Протоколы ISL и 802.1Q указывают, как инкапсулировать или маркировать (tag) данные, транспортируемые через магистральные порты. Методы инкапсуляции и маркировки пакетов идентифицируют виртуальную локальную сеть отправителя пакета. Такой подход позволяет коммутаторам мультиплексировать трафик от многочисленных сетей VLAN в общий магистральный канал (trunk link).

Протоколы DISL и DTP позволяют устройствам Catalyst автоматически согласовывать необходимость включения общего канала в качестве магистрального. Программное обеспечение коммутатора Catalyst включало в себя протокол DISL до тех пор, пока корпорация Cisco не внедрила поддержку стандарта 802.1Q. Когда протокол 802.1Q был реализован в программном обеспечении, возникла необходимость согласования протоколов при использовании ISL- или 802.1Q-инкапсуляции. По этой причине корпорация Cisco разработала второе поколение протоколов согласования магистральных каналов — DTP.

Протокол VTP описывает правила обмена данными между устройствами Catalyst через магистральные каналы. Данный протокол позволяет коммутаторам Catalyst совместно использовать информацию о виртуальных локальных сетях в VTP-домене управления. Он вступает в работу только после завершения согласования параметров магистрального

канала, осуществляемого посредством протоколов DISL/DTP, и функционирует в качестве полезной нагрузки (payload) для пакетов протоколов ISL/802.1Q. Кроме того, протокол VTP не способен работать на обычных (немагистральных) портах. Следовательно, с его помощью невозможно отправлять или принимать сообщения до тех пор, пока с помощью протоколов DISL или DTP канал не будет приведен в состояние магистрального. Работа описываемого протокола обособлена от протоколов ISL и 802.1Q: сообщения протокола VTP транспортируют конфигурационные данные, тогда как протоколы ISL и 802.1Q определяют методы инкапсуляции пакетов. Для наглядности можно воспользоваться анализатором протокола (protocol analyzer), способным декодировать указанные протоколы, сконфигурировав его для перехвата магистрального трафика. Сообщения протокола VTP в отчетах анализатора будут представлены инкапсулированными во фреймы протоколов ISL или 802.1Q данными.

Протокол VTP осуществляет первоначальное распространение VLAN-информации. Настраивать протокол необходимо до начала конфигурирования любой из виртуальных локальных сетей.

Ниже описаны три этапа, которые необходимы для создания сети VLAN:

**Этап 1.** Назначение устройства Catalyst VTP-домену (если коммутатор Catalyst не сконфигурирован в прозрачном режиме протокола VTP).

**Этап 2.** Создание виртуальной локальной сети.

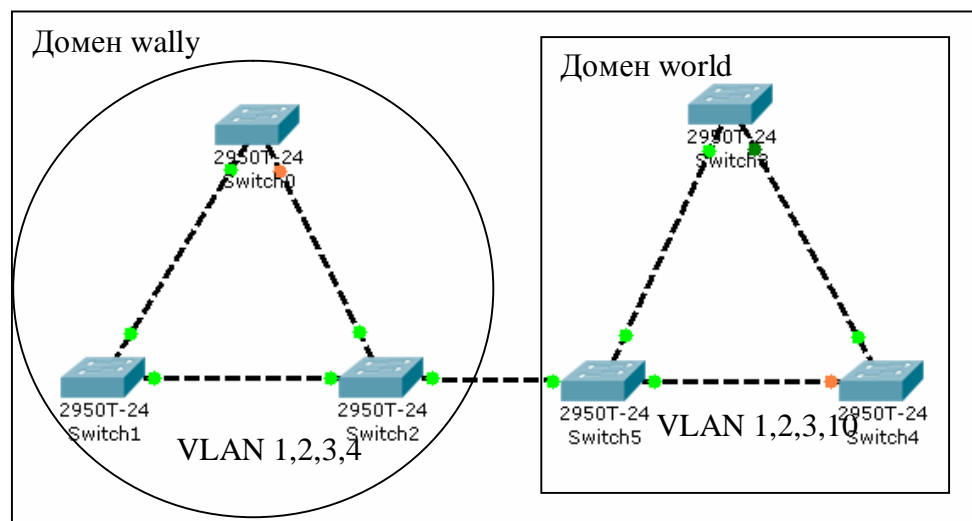
**Этап 3.** Назначение портов виртуальной локальной сети.

Домен протокола VTP связывает коммутаторы Catalyst, которые решают общие конфигурационные задачи. Устройства Catalyst внутри VTP-домена совместно используют всю VLAN-информацию. При удалении или создании сети VLAN администратором на каком-либо коммутаторе Catalyst изменения в списке виртуальных локальных сетей домена автоматически становятся известны всем остальным коммутаторам Catalyst. Подобное средство способствует административной согласованности между устройствами Catalyst. Например, без конфигурационного единообразия распределенное связующее дерево не сможет конвергировать в оптимальной для виртуальных локальных сетей топологии. Протокол VTP служит также для упрощения конфигурационных операций для администратора сети. Без него создавать и удалять виртуальные локальные сети необходимо вручную на каждом коммутаторе Catalyst. Вместе с тем, с помощью данного протокола сети VLAN автоматически распространяются по всем остальным устройствам Catalyst в VTP-домene управления. Такая возможность является принципиальным преимуществом протокола VTP. Для небольших сетей данное преимущество, вероятно, не

выглядит столь значительно. Однако в более крупных сетях оно становится исключительно полезным.

Наряду с преимуществами наличие домена управления ограничивает степень, до которой могут распространяться изменения. На рисунке 42 представлена система коммутаторов

Catalyst с двумя доменами управления wally и world. Домен wally содержит



сконфигурированные сети VLAN

Рис 43. Распределение сетей VLAN в сети коммутаторов

1, 2, 3 и 4, а домен world — сконфигурированные сети VLAN 1, 2, 3 и 10. Предположим, что не существует проблем на третьем уровне сети, и рабочие станции, принадлежащие одной и той же сети VLAN, могут обмениваться данными друг с другом, даже если они расположены в различных доменах управления. Станция сети VLAN 2 в домене wally относится к тому же широковещательному домену, что и станция сети VLAN 2 в домене world.

Допустим также, что администратор сети принял решение добавить в оба домена сеть VLAN 5. Если создать сеть VLAN 5 в домене wally, то с помощью протокола VTP она распространится по всему упомянутому домену. Когда VTP-уведомление достигнет граничного коммутатора Catalyst в домене world, коммутатор проигнорирует информацию из домена wally. Чтобы распространить виртуальную локальную сеть на остальные устройства, администратору необходимо также создать сеть VLAN 5 и в домене world.

Предположим, что администратор решил удалить сеть VLAN 3 из домена world. Администратор удаляет сеть VLAN 3 на коммутаторе Catalyst в домене world. Что в данном случае произойдет с сетью VLAN 3 в домене wally? Ничего. Когда граничный коммутатор Catalyst в домене world сгенерирует и отправит VTP-уведомление коммутатору Catalyst в домене wally, граничный коммутатор Catalyst в домене wally проигнорирует данное уведомление и сохранит сеть VLAN 3.

В случае, когда администратор удаляет сеть VLAN, протокол VTP распространяет информацию об удалении остальным коммутаторам Catalyst в домене управления. Любые узлы, подключенные к портам удаляемой сети, утрачивают связь с сетью, поскольку все порты коммутаторов Catalyst в домене, назначенном данной сети VLAN, отключаются.

Иногда администраторы сетей получают новое оборудование. Естественно, оборудование поставляется без заранее установленной конфигурации. Немедленно приступить к созданию виртуальных локальных сетей невозможно. Прежде всего, администратору необходимо определить VTP-домен. Если коммутатор Catalyst конфигурируется в стандартном режиме VTP-сервера (default server VTP mode) и ему не назначен VTP-домен, то коммутатор не позволит создать сеть VLAN, как это показано на примере. Необходимо отметить, что коммутатор Catalyst отправляет на консоль сообщение с уведомлением об отказе изменения состояния любой сети VLAN до тех пор, пока не будет задано доменное имя. Сообщение также отправляется VTP-серверу.

Пример создание сети VLAN бей сконфигурированного VTP-домена

**Console> (enable) set vlan 10 name willitwork**

**Cannot add/modify VLANs on a VTP server without a domain name.**

**Console> (enable)**

Рассмотрим компоненты, образующие VTP-домен. Для связывания коммутаторов Catalyst с общим VTP-доменом необходимо выполнение трех условий:

- коммутаторы Catalyst должны иметь одно и то же имя VTP-домена;
- устройства Catalyst должны быть смежными;
- между коммутаторами должно быть настроено магистральное соединение (trunking).

Первая предпосылка для вхождения в состав VTP-домена включает в себя имя домена управления. Коммутатор Catalyst определяет свое членство в домене управления протокола VTP посредством доменного имени. Всем коммутаторам Catalyst, которые должны входить в один домен, необходимо присвоить одно и то же имя домена управления. Первоначально коммутатор Catalyst может получить имя своего домена управления тремя способами: из командной строки, из конфигурационного файла или, если включены магистральные каналы, автоматически от соседнего коммутатора. Для включения коммутатора Catalyst в домен управления вручную необходимо использовать команду **set vtp domain name**.

### ***9.1. Режимы протокола VTP***

Обратимся к информации, полученной с помощью команды **set vtp ?**. В выводимой информации представлены параметры для конфигурирования режима протокола VTP.



Протокол VTP можно настроить для функционирования в трех режимах: режиме сервера (server mode), режиме клиента (client mode) или в прозрачном режиме (transparent mode). Отличия между указанными режимами сводятся к разным способам генерации VTP-сообщений и реакции на полученные уведомления.

### **9.1.1. Отправка VTP-сообщений**

Для того, чтобы впоследствии с помощью протокола VTP можно было автоматически распределить новую виртуальную локальную сеть по всем коммутаторам Catalyst, необходимо создавать ее на коммутаторе Catalyst, сконфигурированном в режиме VTP-сервера. После того, как сеть VLAN создана, VTP-сервер автоматически распространяет информацию о ней посредством VTP-сообщения, которое называется уведомлением подгруппы VTP (VTP subset advertisement). Сообщения такого типа более подробно рассматриваются в разделе "Уведомления подгруппы". С помощью такого сообщения остальные коммутаторы Catalyst в домене управления информируются о появлении новой виртуальной локальной сети. Коммутатор Catalyst, на котором настраивалась новая сеть VLAN, генерирует первоначальное уведомление подгруппы, которое рассылается через магистральный интерфейс коммутатора. Остальные серверы и клиенты продолжают распространение VLAN-информации на другие коммутаторы Catalyst в сети.

Коммутаторы Catalyst, сконфигурированные в прозрачном режиме, никогда не генерируют VTP-сообщения. При создании виртуальной локальной сети на коммутаторе, функционирующем в прозрачном режиме, VLAN-информация остается локальной и не предоставляется остальным устройствам, даже если существует магистральное соединение с другими коммутаторами Catalyst.

Только коммутаторы Catalyst, сконфигурированные в режиме сервера или клиента, учитывают информацию, содержащуюся в VTP-сообщениях. Каждый раз при получении многоадресного VTP-сообщения с адресом 01-00-0C-CC-CC-CC и значением SNAP-типа, равным 0x2003, принимающий коммутатор Catalyst отправляет фрейм модулю Supervisor (модулю управления), в котором происходит обработка данного фрейма. Если модуль Supervisor определяет, что информация, включенная в пакет обновления, отлична от имеющейся, он обновляет свою VLAN-информацию, создает сообщения обновления и рассылает их соседним коммутаторам Catalyst. Коммутатор Catalyst использует номер ревизии конфигурации протокола VTP (VTP configuration revision number) для определения актуальности имеющихся данных. Использование номера ревизии конфигурации описывается ниже в текущей главе.

Когда коммутатор Catalyst, сконфигурированный в прозрачном режиме, получает VTP-обновление, то не отправляет фрейм модулю Supervisor, а локально игнорирует данный фрейм. Однако, если коммутатор Catalyst имеет другие подключенные магистральные каналы, то он лавинно рассылает фрейм через магистральные порты. VTP-сообщение в данном случае не изменяет конфигурацию коммутатора, сконфигурированного в прозрачном режиме, как это происходит в случае, когда устройство работает в режиме сервера или клиента.

### **9.1.2. Создание сетей VLAN**

Для создания виртуальной локальной сети необходимо использовать коммутатор Catalyst, который сконфигурирован в режиме сервера или прозрачном режиме. Только устройства, работающие в указанных режимах, способны воспринимать команды `set vlan` и `clear vlan`. Однако, между ними существует различие, которое заключается в поведении устройства после создания сети VLAN. В режиме сервера коммутатор Catalyst рассылает VTP-уведомления соседним коммутаторам через все магистральные порты. Коммутатор Catalyst в прозрачном режиме после создания сети VLAN не генерирует VTP-уведомления. Новая сеть VLAN имеет только локальное значение. Для того, чтобы создать распределенную сеть на основе устройств Catalyst в прозрачном режиме, необходимо создавать новые сети VLAN на всех устройствах и для каждого коммутатора отдельно. Устройства Catalyst в прозрачном режиме, в сущности, не принимают участия в работе протокола VTP. С точки зрения таких устройств протокола VTP не существует вообще. Нет необходимости включать устройство Catalyst в прозрачном режиме в состав VTP-домена до того, как можно будет создать какие-либо локальные сети VLAN. Коммутаторы в прозрачном режиме протокола VTP не объявляют об изменениях или дополнениях, внесенных в конфигурацию сетей VLAN на локальном коммутаторе. Однако, они транзитом пропускают через себя дополнения или изменения, внесенные в сети VLAN где-либо еще.

Коммутаторы Catalyst в режиме клиента не имеют полномочий на создание сетей VLAN. При попытке связать клиентский порт с неизвестной ему сетью VLAN коммутатор генерирует сообщение, информирующее администратора о необходимости создания виртуальной локальной сети на сервере, перед тем, как он сможет логически присоединять порты к указанной сети VLAN. Если после назначения портов для сети VLAN запросить информацию о ее состоянии с помощью команды `show vlans`, то можно отметить, что порты принадлежат новой несуществующей виртуальной локальной сети. Кроме того, все порты находятся в неактивном состоянии, предотвращающем продвижение фреймов в

сети VLAN. После создания виртуальной локальной сети на сервере, принадлежащем тому же домену управления, что и клиент, последний в конечном итоге получает информацию о новой сети VLAN и интерпретирует полученную информацию как разрешение на активизацию портов в новой сети VLAN.

Также не существует возможности удалять виртуальные локальные сети с устройства, функционирующего в режиме клиента. Данную операцию можно осуществить только при помощи устройств в режиме сервера или прозрачном режиме. В отличие от режима сервера, удаление виртуальной локальной сети с коммутатора в прозрачном режиме влияет только на локальное устройство. Удаляя сеть VLAN с сервера, администратор получает предупреждение от коммутатора Catalyst о том, что такая операция переведет все порты, назначенные данной сети VLAN внутри домена управления, в приостановленное состояние, как это показано в примере

Пример удаление виртуальной локальной сети в домене управления

```
Console> (enable) clear vlan 10
```

```
This command will deactivate all ports on vlan 10  
in the entire management domain
```

```
Do you want to continue(y/n) [n]?y
```

```
Vlan 10 deleted
```

```
Console> (enable)
```

При удалении сети VLAN порты в домене управления не переназначаются стандартной сети VLAN 1. Коммутатор Catalyst оставляет порты назначенными несуществующей теперь сети VLAN, но переводит их в неактивное состояние. Для того, чтобы подключенные устройства снова могли обмениваться данными, необходимо связать порты с любой активной сетью VLAN.

### **9.1.3. Хранение VLAN-информации**

Всегда при создании, удалении или переводе сети VLAN в неактивное состояние при помощи коммутатора Catalyst в прозрачном или серверном режиме он сохраняет конфигурационную информацию в энергонезависимой памяти (NVRAM) и при включении питания может восстановить последнюю известную конфигурацию. Если при этом устройство работало в серверном режиме, то оно также передает конфигурационную информацию соседним устройствам Catalyst.

Вместе с тем, устройства-клиенты не сохраняют VLAN-информацию. При отключении питания в коммутаторе Catalyst, сконфигурированном в режиме клиента, информация обо всех виртуальных локальных сетях, известных ему, теряется. Однако, данные о

стандартной сети VLAN 1 сохраняются. При включении питания коммутатор в режиме клиента не может локально активизировать какую-либо виртуальную локальную сеть, кроме VLAN 1, до тех пор, пока не получит уведомление от VTP-сервера об авторизации группы сетей VLAN. Все порты, назначенные виртуальным локальным сетям, кроме портов сети VLAN 1, остаются в неактивном состоянии до получения VTP-уведомления от сервера. Когда клиент получает от сервера VTP-сообщение об обновлении, он может активизировать любые назначенные сетям VLAN порты, указанные в информационном пакете.

#### **9.1.4. Распространение сети VLAN с помощью протокола VTP**

В качестве иллюстрации различий между серверным (коммутатор Cat-A), клиентским (Cat-C) и прозрачным (Cat-B) видами конфигурации рассмотрим рисунок 43. Сервер и клиент объединены в линейный каскад с помощью расположенного посередине коммутатора, работающего в прозрачном режиме (Cat-B).

На начальной  
стадии  
конфигурации (этап  
1) всем  
коммутаторам  
Catalyst присвоено  
доменное имя. В  
действительности  
протокол VTP в  
устройстве Cat-B

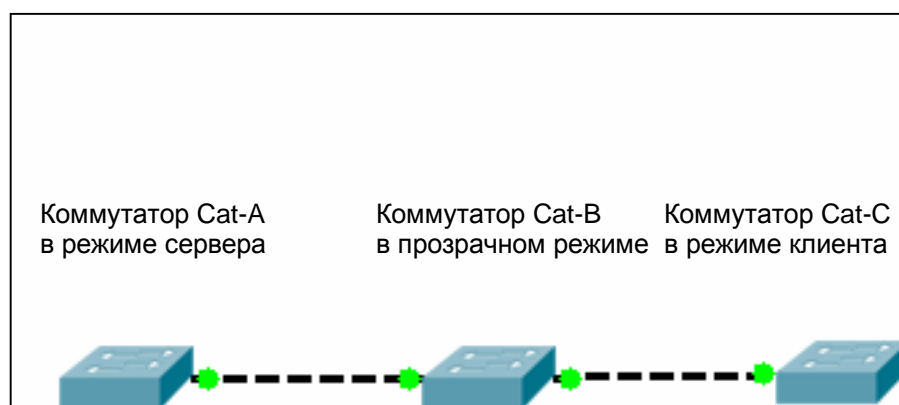


Рис 44. Распространение виртуальной локальной сети для схемы с устройствами в серверном, клиентском и прозрачном режимах протокола VTP

реально не участвует в обмене данными и может быть проигнорирован. Все три коммутатора Catalyst начинают работать после загрузки только со стандартной сетью VLAN 1. В процессе выполнения этапа 2 администратор, используя устройство в режиме клиента, пытается создать новую виртуальную локальную сеть. Поскольку коммутатор Cat-C является клиентом, он отвергает команду, отправляет на консоль сообщение об ошибке и не создает новую сеть VLAN. Как и ранее, существует только сеть VLAN 1. С помощью команды **set vlan** на этапе 3 администратор назначает порты сети VLAN 2. Даже если на данном этапе сеть VLAN 2 еще не существует, коммутатор Cat-C принимает назначения портов, привязывает определенные порты к VLAN 2 и переводит их в неактивное состояние. Однако, коммутатор Cat-C владеет информацией только о сети VLAN 1.

На четвертом этапе администратор переходит к коммутатору Cat-A, т.е. к серверу, и создает сеть VLAN 2, которая затем распространяется к соседнему коммутатору — Cat-B. Однако, коммутатор Cat-B сконфигурирован в прозрачном режиме и игнорирует VTP-уведомление. Он не добавляет сеть VLAN 2 к своему локальному списку сетей VLAN. Коммутатор Cat-B лавинно отправляет VTP-уведомления соседним коммутаторам Catalyst через все магистральные порты. В данном случае коммутатор Cat-C получает VTP-уведомление об обновлении, проверяет совпадение имени VTP-домена управления и добавляет сеть VLAN 2 к своему локальному списку. Коммутатор Cat-C затем активизирует все порты, назначенные сети VLAN 2. После чего любые устройства, подключенные к портам сети VLAN 2 на коммутаторе Cat-A, принадлежат тому же широковещательному домену, что и порты, назначенные сети VLAN 2 на коммутаторе Cat-C. В результате устройства могут обмениваться данными друг с другом, если такой обмен разрешен на сетевом уровне.

Затем на пятом этапе администратор переходит (или связывается по протоколу Telnet) к коммутатору Cat-B и создает новый широковещательный домен, сеть VLAN 10. Поскольку данное устройство сконфигурировано в прозрачном режиме, Cat-B авторизован для создания сети VLAN 10. Однако, коммутатор Cat-B не распространяет информацию о сети VLAN 10 среди остальных устройств. Данная сеть остается локальной для коммутатора Cat-B и не является общей виртуальной локальной сетью.

На этапе 6 происходит авария — отключается питание коммутаторов Cat-A и Cat-B. Однако в результате грамотных действий инженера при создании сети указанные устройства ранее были сконфигурированы в серверном и прозрачном режиме, что позволило им сохранить конфигурационную VLAN-информацию. Несмотря на то, что коммутаторы Cat-A и Cat-B отключены, устройство Cat-C продолжает функционировать, основываясь на последней известной VLAN-конфигурации. Все порты коммутатора Cat-C продолжают функционировать в назначенных им сетях VLAN. Когда включается электропитание коммутаторов Cat-A и Cat-B, оба устройства восстанавливают авторизованные сети VLAN и активизируют их. Кроме того, коммутатор Cat-A генерирует VTP-сообщения для соседних устройств. Однако, такие сообщения не влияют на работу коммутаторов Cat-B и Cat-C, т.к. они оба используют свою прежнюю конфигурацию.

Рассмотрим случай отключения питания устройств Cat-A и Cat-C, которое происходит на этапе 7. Причем питание коммутатора Cat-C восстанавливается раньше. Когда коммутатор Cat-C снова включается, он начинает работать с авторизованной стандартной сетью VLAN 1. Порты в любой другой сети VLAN отключены до тех пор, пока коммутатор Cat-C не получит VTP-сообщение от сервера. Если восстановление

работоспособности коммутатора Cat-A длится один час, то устройство Cat-C все время остается в описанном выше состоянии. Когда, наконец, происходит перезапуск коммутатора Cat-A (этап 8), он отправляет VTP-сообщения, с помощью которых устройство Cat-C получает разрешение на активизацию любых портов в виртуальных локальных сетях, включенных в VTP-уведомление.

В завершение, на этапе 9 администратор создает другую виртуальную локальную сеть (VLAN 20) для всего домена управления. Однако добавление сети требует конфигурирования остальных двух устройств. Администратор должен создать указанную сеть VLAN на устройствах Cat-A и Cat-B, после чего в домене появятся две общих VLAN-сети. Все устройства в сети VLAN 20 принадлежат одному широковещательному домену вне зависимости от того, к какому коммутатору Catalyst они подключены. Сеть VLAN 1 является другим общим широковещательным доменом. Любые устройства в сети VLAN 1 также могут общаться друг с другом. Однако устройства, входящие в нее, не имеют возможности обмениваться данными с устройствами сети VLAN 20, если в сети не присутствует маршрутизатор.

## **9.2. Принцип действия протокола VTP**

Протокол магистральных каналов виртуальных локальных сетей (VTP), разработанный корпорацией Cisco, функционирует в качестве протокола канального уровня для устройств семейства Catalyst. При передаче коммутатором Catalyst VTP-сообщений таким же устройствам в сети сообщение инкапсулируется во фрейм магистрального протокола, такого, как ISL или 802.1Q. Длина VTP-заголовка варьируется в зависимости от типа сообщения, однако в общем случае во всех VTP-сообщениях обязательно присутствуют четыре элемента:

- версия протокола VTP — 1 либо 2;
- тип VTP-сообщения — поле указывает на один из четырех типов;
- длина имени домена управления — в поле указана величина последующего доменного имени;
- имя домена управления — имя, заданное для домена управления.

Более подробно структура VTP-сообщений описывается в следующих разделах. VTP-сообщения всегда перемещаются по стандартной для среды передачи виртуальной локальной сети. Например, в Ethernet-магистральной VTP-сообщения транспортируются по сети VLAN 1; в FDDI-магистральной — по сети VLAN 1002; в ATM-магистральной для транспортировки VTP-сообщений стандартно используется эмулируемая локальная сеть (emulated LAN — ELAN). Поскольку удалить какую-либо стандартную сеть невозможно, VTP-сообщения всегда распространяются через магистральные порты такой локальной

сети. Однако, пакеты протокола VTP не всегда транспортируются именно по ATM-магистралям. Для того, чтобы осуществить подобную передачу, необходимо использовать стандартную (используемую по умолчанию) ELAN-сеть. Вместе с тем, такая сеть не создается автоматически. Если требуется настроить передачу VTP-сообщений по ATM-каналу, то необходимо явно задать эмулируемую локальную сеть. Несмотря на то, что маршрутизаторы Cisco поддерживают магистральные протоколы, такие, как ISL, LANE и 802.1Q, устройства такого типа в настоящее время не участвуют в распространении VTP-сообщений. Маршрутизаторы игнорируют VTP-сообщения и отбрасывают их при поступлении пакетов на интерфейсы. Следовательно, VTP-сообщения могут распространяться не далее интерфейса маршрутизатора или другого коммутатора Catalyst, который принадлежит иному домену управления.

### ***9.3. Настройка протокола VTP***

Перед настройкой домена VTP следует ознакомиться с возможными параметрами.

1. Обратите внимание на номер редакции протокола VTP, который вы собираетесь задействовать.
2. Определитесь, должен ли коммутатор быть участником имеющегося домена или же нужно создать новый домен. Чтобы добавить его в существующий домен, найдите имя домена и пароль, если они используются.
3. Выберите режим VTP для каждого коммутатора в сетевом комплексе.

#### **Настройка версии VTP**

На коммутаторах можно настраивать две разные версии протокола VTP. Версия 1 — это стандартная версия VTP на всех коммутаторах. Для работы этой стандартной версии 1 не требуется настройка версии VTP. Версии 1 и 2 несовместимы, так что для коммутаторов настройка может означать все или ничего: Но если все коммутаторы совместимы с версией 2 VTP, изменение одного коммутатора приводит к изменению всех коммутаторов. Будьте осторожны, если вы не уверены, что все коммутаторы совместимы с версией 2. Версия 2 задается по следующим причинам:

**Поддержка виртуальных LAN Token Ring** Для использования Token Ring необходим протокол VTP версии 2. Т.е. все коммутаторы должны быть рассчитаны на работу версии 2.

**Поддержка TLV** Поддержка неизвестных параметров type-length-value (TLV — тип-длина-значение). Получив уведомление VTP, имеющее неизвестные параметры тип-длина-значение, коммутаторы VTP версии 2 все равно распространяют изменения по своим магистральным каналам.

Прозрачный режим Коммутаторы могут работать в прозрачном режиме, они только пересылают сообщения и уведомления, не добавляя их в свою базу данных. В версии 1 коммутатор проверяет имя домена, а в версии 2 пересылает VTP-сообщения без проверки версии.

Проверка согласованности Проверка согласованности выполняется, когда администратор вводит в коммутатор новые данные, с помощью интерфейса командной строки или другого ПО для управления. Если данные получены из уведомления или считаны из энергонезависимого ОЗУ, проверка согласованности не производится. Коммутатор проверяет дайджест по сообщению. Если он правильный, проверка согласованности не производится.

Для настройки протокола VTP версии 2 на коммутаторе служит команда **set vtp v2 enable**.

```
Console> (enable) set vtp v2 enable
```

This command will enable the version 2 function in the entire management domain. All devices in the management domain should be version2-capable before enabling. Do you want to continue (y/n) [n]?y VTP domain modified

```
Console> (enable)
```

### **9.3.1. Настройка домена**

Установите имя домена VTP и пароль на первом коммутаторе. Имя VTP может содержать до 32 символов. На любом совместимом с VTP коммутаторе1 можно установить пароль домена VTP. Пароль может быть минимум 8 знаков и максимум 64 знака.

```
Console> (enable) set vtp domain ?
```

```
Usage: set vtp [domain <name>] [mode <mode>] [passwd <passwd>]
```

```
[pruning enable|disables] [v2 <enable|disable> (mode = client|server|transparent
```

```
Use passwd '0' to clear vtp password) Usage: set vtp pruneeligible <vlans> (vlans = 2..1000
```

```
An example of vlans is 2-10,1000)
```

```
Console> (enable) set vtp domain Globalnet VTP domain Globalnet modified
```

```
Console> (enable)
```

### **9.3.2. Настройка режима VTP**

Создайте первый коммутатор в серверном режиме, а затем подключенные коммутаторы в качестве клиентов. Можно назначить этим коммутаторам прозрачный или клиентский режим — в зависимости от ваших требований. Данные VTP можно настроить в одной строке, включая пароли, режимы и версии. На коммутаторе Catalyst:



Console> (enable) setvtp domain

Usage: setvtp [domain<name>] [mode<mode>] [passwd<passwd>] pruning <enable|disable>]  
[v2 <enable|disable>] (mode = client|server|transparent Use passwd '0' to clear vtp password)  
Usage: setvtp pruneenable<vtans> (vtans = 2..1000)

An example of vtans is 2-10,1000)

Console> (enable) set vtp domain Globlanet mode server VTP domain Globlanet modified

Проверить данные домена VTP можно с помощью команды **show vtp domain show vtp statistics**.

Команда show VTP domain отображает имя домена, режим и данные отсечения.