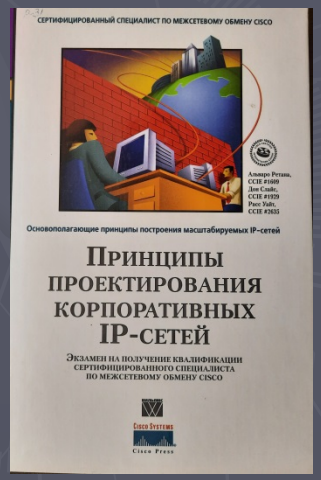
Принципы проектирования корпоративных IP-сетей



По материалам книги:

Ретана Альваро, Слайс Дон, Уайт Расс. Принципы проектирования корпоративных IP-сетей. : Пер. с англ. М.: Издательский дом «Вильямс», 2002. – 368 с. ISBN 5-8459-0248-7 (рус)

Содержание книги “Ретана Альваро и др”

Материал, представленный в книге (стр.15)

- Книга «Принципы проектирования корпоративных IP-сетей» предназначена для профессионалов в области проектирования компьютерных сетей; предполагается, что читатель уже знаком с маршрутизацией и протоколами маршрутизации
- Ниже приведен список вопросов, не рассматриваемых в данной книге
  - ✓ Все, что не касается маршрутизаторов компании Cisco
  - ✓ Настройка маршрутизатора
  - ✓ Принцип работы протоколов маршрутизации
  - ✓ Выбор протокола маршрутизации
  - ✓ Протоколы RIP и IGRP
  - ✓ Определение пропускной способности маршрутизатора, выбор маршрутизатора для заданного объема трафика и т..
  - ✓ Выбор среды передачи информации для сетей LAN или WAN, определение скорости передачи данных канала связи и другие требования физического уровня.

Глава 1. Принципы иерархического проектирования сетей

- L3 OSI RM аспекты проектирования сетей наиболее важные

Введение

Неумолимый закон компьютерных сетей гласит:

- Все, что было маленьким, станет большим; все, что было большим, станет огромным; все, что было огромным, превратится в транснациональную сеть
- Необходимо знать правила "хорошего тона" при проектировании сетей
- Стабильность работы сети не может быть достигнута
  - ✓ за счет установки новых коммутаторов уровня 2 или супербыстрых маршрутизаторов
  - ✓ переходом с одного сложного протокола маршрутизации на другой
  - ✓ запретом кому-либо прикасаться к работающим маршрутизаторам
    - хотя иногда это все же помогает
- Удачно выбранная структура сети, разработанная с учетом аргументированных принципов, проверенных опытом и временем,
  - ✓ залог хорошего сна сетевого инженера
- L3 OSI RM аспекты проектирования сетей наиболее важные

С чего начать ?

- С физической среды передачи информации, к которой относятся
  - ✓ биты и байты
  - ✓ оптимальный выбор пропускных способностей линий связи
  - ✓ используемые среды передачи информации
  - ✓ сигнальный метод передачи
  - ✓ извлечение данных из канала
- Стабильность каналов связи во многом определяется стабильность передачи трафика по сети
  - ✓ Часто возникающие неполадки физического уровня приводят к сетевым изменениям, вызывающим необходимость обновления таблиц маршрутизации.
- Однако *топология* (структура) сети имеет несравнимо большее влияние на ее стабильность, нежели выбор между технологиями ATM или Frame Relay для прокладки удаленных сетевых соединений
  - ✓ Удачно выбранная топология является базисом всех стабильно функционирующих сетей

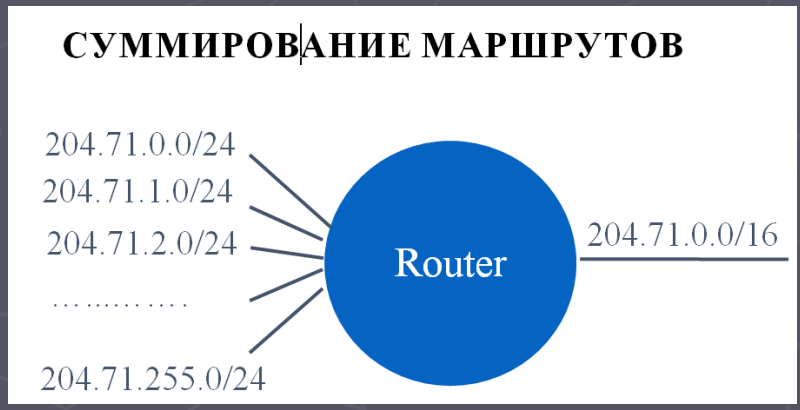
Почему сети зависают ?

Почему сети зависают?

- Простой ответ:
  - ✓ сходимость протокола маршрутизации невозможна
    - все протоколы маршрутизации в процессе сходимости порождают петли, очень важно как можно быстрее завершить процесс сходимости после возникновения непредвиденных изменений в сети
- Время, необходимое протоколу маршрутизации для завершения процесса сходимости, зависит от двух факторов:
  - ✓ количества маршрутизаторов, принимающих участие в процессе сходимости;
  - ✓ объема обрабатываемой маршрутизаторами информации
    - размера таблицы маршрутизации

Суммирование уменьшает обрабатываемую роутером информацию

- Количество маршрутизаторов, принимающих участие в процессе сходимости, зависит от размеров участка сети, на который влияет изменение топологии
  - ✓ Суммирование позволяет скрыть часть информации о маршрутах от маршрутизаторов
  - ✓ Следствие суммирования - уменьшение обрабатываемой маршрутизаторами информации,
    - поскольку маршрутизаторы, не обладающие информацией о заданном пункте назначения, не должны вносить изменения в таблицы маршрутизации при изменении маршрута к этому пункту назначения или при повреждении канала связи, которое привело к его недоступности
- Объем обрабатываемой маршрутизаторами информации при определении наилучшего маршрута к пункту назначения зависит от общего числа таких маршрутов
  - ✓ Опять же, суммирование позволяет уменьшить объем обрабатываемой маршрутизаторами информации при изменении топологии сети

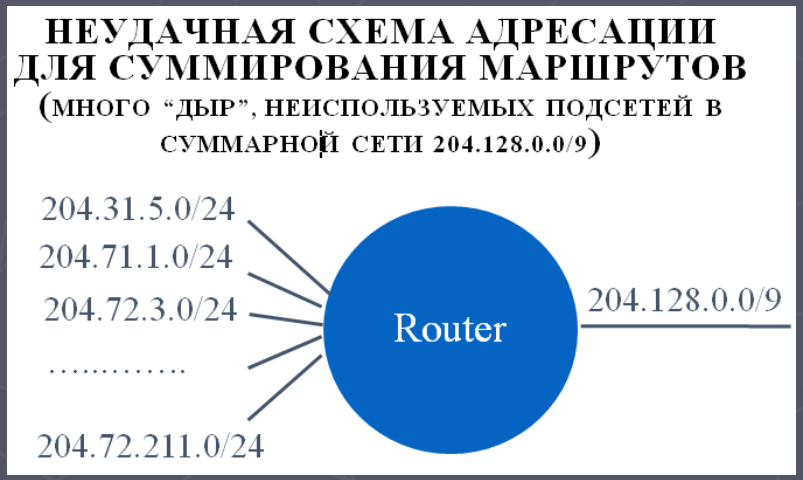


Удачная схема адресации повышает эффективность суммирования маршрутов

- Итак, суммирование позволяет уменьшить число участвующих в процессе сходимости маршрутизаторов и объем обрабатываемой ими информации
- Однако возможность выполнения суммирования зависит от удачного выбора схемы адресации, которая всегда базируется на тщательно продуманной топологии, лежащей в основе сети

Решить сетевые проблемы, вызванные неудачным выбором топологии и схемы адресации, с помощью более производительных маршрутизаторов, всевозможных доработок адресной схемы или улучшенных протоколов маршрутизации, НЕВОЗМОЖНО

Практика показывает: ничто не может заменить удачно выбранную и хорошо продуманную топологию



Уровневый / иерархический подход

- С любой проблемой легче справиться, если она разбита на несколько более мелких подзадач
- Крупная сеть может быть разделена на несколько сравнительно небольших участков, каждый из которых можно рассматривать отдельно от других
- Большинство удачно спроектированных крупных сетей являются иерархическими, т.е. разбитыми на несколько *уровней*
- Каждый уровень представляет собой отдельную проблемную область, в рамках которой структура уровня разрабатывается с учетом одной или нескольких четко обозначенных целей
- Концепция иерархических сетей очень напоминает концепцию OSI RM
  - ✓ взаимодействия между компьютерами разбивается на несколько функциональных уровней, выполняющих определенный круг задач
  - ✓ Уровни иерархической модели должны как можно более точно соответствовать поставленным перед ними целям
  - ✓ Попытка делегирования какому-нибудь определенному уровню слишком большого числа функциональных задач приводит, как правило, к неразберихе, что усложняет документирование и поддержку

Иерархическая модель сети

В большинстве случаев подразумевается три уровня

- *Ядро (core)* отвечает за высокоскоростную передачу сетевого трафика; мясорубка коммутации пакетов
- На *Уровне распределения (distribution layer)* происходит суммирование маршрутов и агрегация трафика
- *Уровень доступа (access layer)* отвечает за формирование сетевого трафика, выполняет контроль точек входа в сеть и предоставляет другие службы пограничных устройств

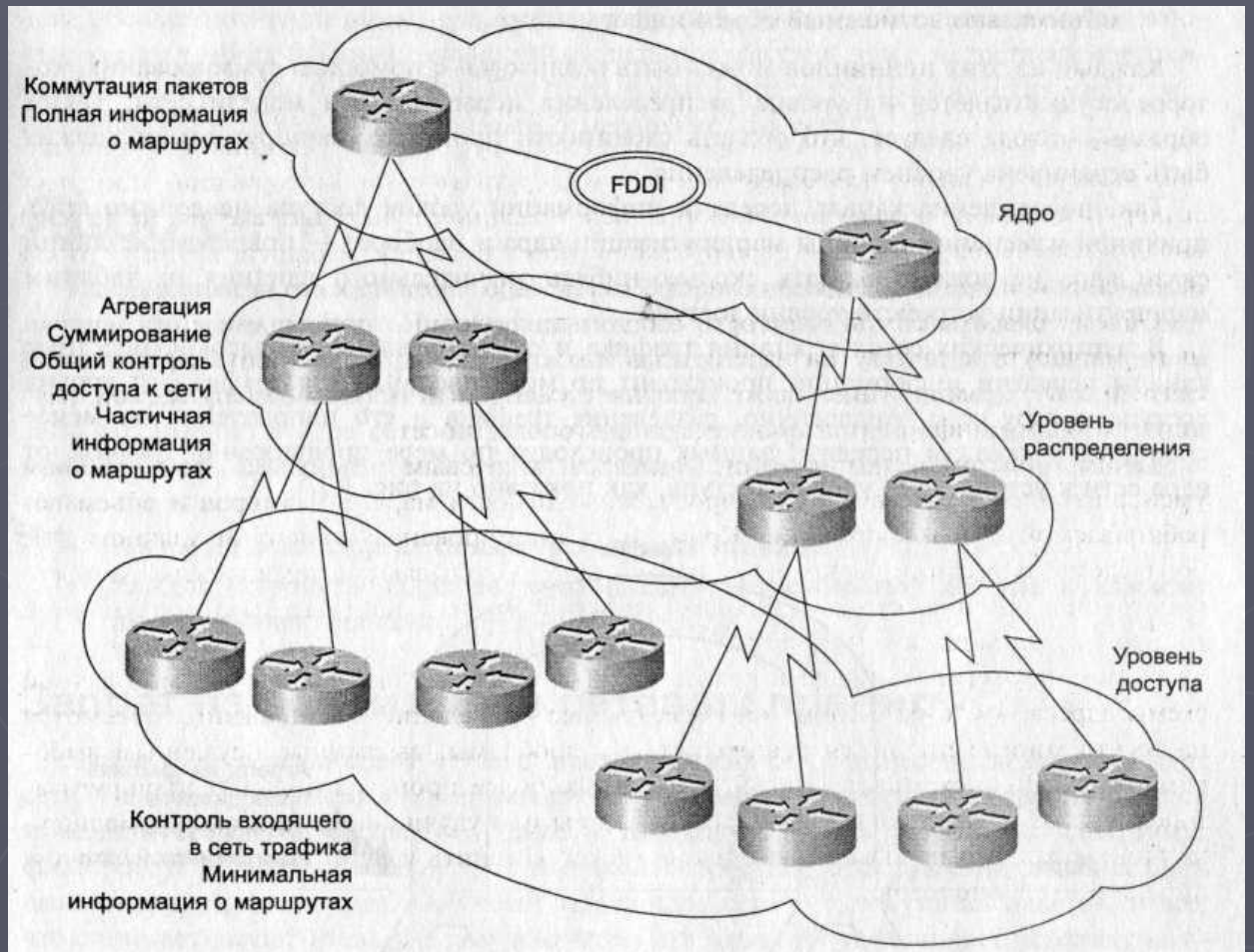


Рис. 1.1. Структура иерархической сети

Принципы разработки иерархической сети

- Итак, два основных принципа разработки иерархической структуры сети
  - ✓ Размеры участка сети, на который влияет изменение топологии, должны быть строго ограничены; при этом желательно, чтобы данный участок сети был как можно меньшим.
  - ✓ Маршрутизаторы (а также другие сетевые устройства) должны обрабатывать минимально возможный объем информации
- Каждый из этих принципов может быть реализован с помощью суммирования, которое осуществляется на уровне распределения иерархической модели сети
  - ✓ область сходимости протокола маршрутизации должна быть ограничена уровнем распределения
- Повреждение канала передачи информации на уровне доступа не должно стать причиной изменения таблицы маршрутизации ядра и наоборот — повреждение линии связи ядра не должно оказать сколько-нибудь значительного влияния на таблицы маршрутизации устройств уровня доступа

Агрегация трафика

- Агрегация трафика и его направление в высокоскоростные каналы происходит по мере продвижения от уровня доступа к ядру сети
- Разделение трафика и его направление по менее скоростным каналам происходит по мере продвижения трафика от ядра сети к устройствам уровня доступа, как показано на рис. 1.2.
- Агрегация трафика подразумевает
  - ✓ не только возможность выбора в качестве маршрутизаторов уровня доступа менее производительных устройств,
  - ✓ но и то, что эти устройства не будут слишком отягощены коммутацией пакетов. Следовательно, освободившиеся вычислительные ресурсы маршрутизаторов уровня доступа могут быть использованы для реализации сетевых правил

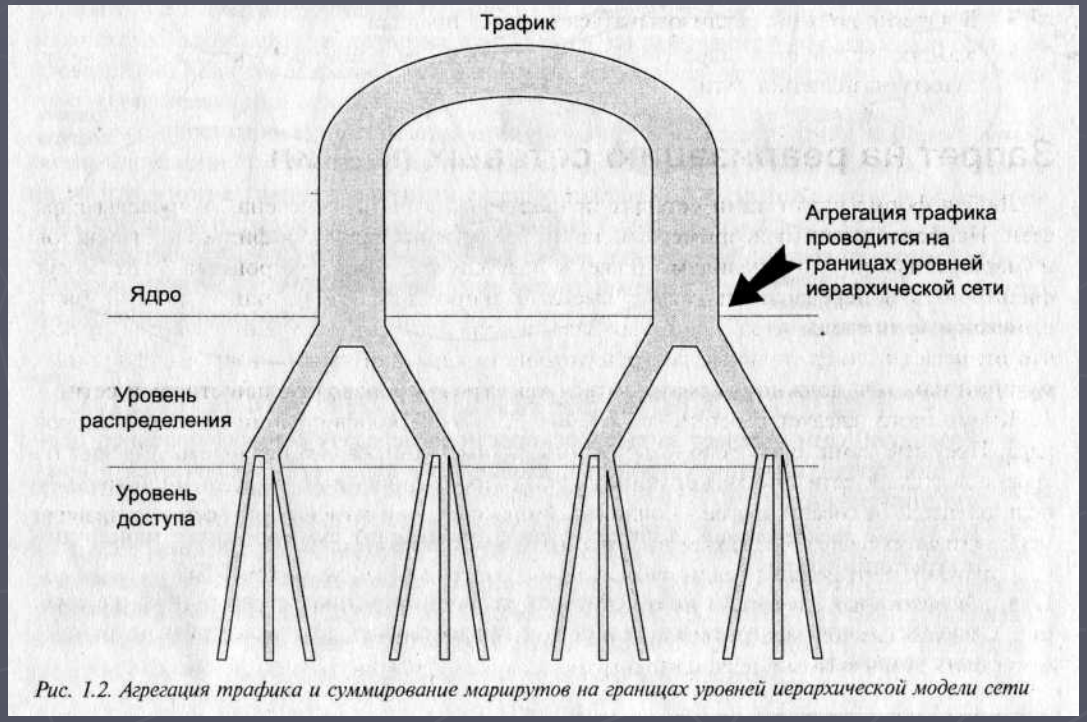


Рис. 1.2. Агрегация трафика и суммирование маршрутов на границах уровней иерархической модели сети

Одиночные точки отказа

- Одним из наиболее серьезных недостатков иерархической структуры –
  - ✓ потенциальная возможность появления одиночных точек отказа на физическом уровне
- При этом:
  - ✓ чем строже иерархия сети, тем выше вероятность того, что повреждение одного устройства или канала передачи информации вызовет крупные неполадки в ее работе
- Если серьезный сбой в работе сети абсолютно неприемлем, следует
  - ✓ позаботиться о мерах обеспечения избыточности, которая могла бы значительно уменьшить последствия этого недостатка иерархической модели сети
- Более подробно тема избыточности в иерархических сетях рассматривается в главе 3, "Избыточность в иерархических сетях".

Ядро сети: задачи и стратегии

- Задача ядра — *коммутация пакетов (switching packets)*
  - ✓ в ядре сосредоточена вся вычислительная мощность сети
  - ✓ устройства ядра не должны испытывать ни малейшего недостатка в производительности в случае максимальной нагрузки
  - ✓ все, что отнимает вычислительные ресурсы устройств ядра или увеличивает задержку коммутации пакетов, должно рассматриваться как угроза производительности всей сети
- Две основные стратегии достижения максимальной производительности ядра сети:
  - ✓ в ядре не должны реализовываться сетевые правила
    - Например, фильтрация пакетов и маршрутизация по правилам
  - ✓ каждое устройство ядра должно обладать возможностью доступа к каждому пункту назначения сети
- Ремарка. Следует избегать увеличения сложности конфигурации маршрутизаторов ядра
  - ✓ одно дело — ошибка на уровне доступа к сети, потеря соединения с определенной группой пользователей
  - ✓ совсем другое — ошибиться при внесении изменений в сетевые правила маршрутизаторов ядра, что может вызвать выход из строя всей сети

Ядро сети: запрет на реализацию сетевых правил

- Политики доступа / стратегия сети должны реализовываться
  - ✓ в ее пограничных устройствах на уровне доступа
  - ✓ в некоторых случаях — на границе между уровнем доступа и уровнем распределения в иерархической модели сети
  - ✓ в самых крайних случаях в ядре или на границе между ядром и уровнем распределения

Практический пример: маршрутизация по правилам

- Как правило, решение о передаче трафика, основываясь только на адресе конечного пункта назначения
- Тем не менее бывают ситуации, в которых маршрутизатор должен принять решение о передаче пакета на основании адреса источника, типа трафика или какого-нибудь другого критерия.
- Принятие решения о передаче пакета, базирующееся на некотором критерии или установленном системным администратором правиле, называется *маршрутизацией по правилам (policy-based routing).*
- Маршрутизатор может принять решение о передаче пакета, основываясь на приведенных ниже критериях.
  - ✓ Адрес источника
  - ✓ Адрес источника/адрес пункта назначения.
  - ✓ Адрес пункта назначения.
  - ✓ Тип IP-пакета (TCP, UDP, ICMP и т.д.).
  - ✓ Тип службы (Telnet, FTP, SMTP).
  - ✓ Последовательность бит в заголовке IP-пакета.
- Три этапа настройки маршрутизации по правилам
  - ✓ Создание фильтра для отделения трафика, нуждающегося в особой обработке, от остального трафика
  - ✓ Создание правила
  - ✓ Реализация правила

Пример: маршрутизация по правилам

Реализация решения о передаче трафика Telnet по медленному каналу Frame Relay, а остального трафика — по сравнительно быстрому спутниковому каналу

1. Создаем фильтр для разделения трафика
   access-list 150 permit tcp any eq telnet any → блокирует источник Telnet-трафика
   access-list 150 permit tcp any any eq telnet → блокирует пункты назначения Telnet-трафика

2. Создаем правило
   route-map telnetthroughframe permit 10
   match ip address 150
   set ip next-hop 192.168.10.x

карта маршрута идентифицирует все пакеты, выделенные на предыдущем шаге (порт TCP Telnet в качестве источника или пункта назначения), и передает их на IP-адрес маршрутизатора на другом конце канала FR

3. Применим созданное правило
   interface ethernet 0
   ip policy route-map telnetthroughframe

4. Укажем маршрутизатору на необходимость применения только что созданного правила для всех пакетов, полученных на интерфейс Ethernet 0

Пакеты, передаваемые по правилам, обрабатываются в соответствии с коммутацией типа *process switching* (в CiscoIOS) оказывают, как правило, крайне негативное влияние на маршрутизатор.

Каждый пакет, который должен быть обработан в соответствии с коммутацией типа *process switching,* необходимо заранее подать на коммутацию вместо того, чтобы переслать по одному из оптимизированных маршрутов коммутации

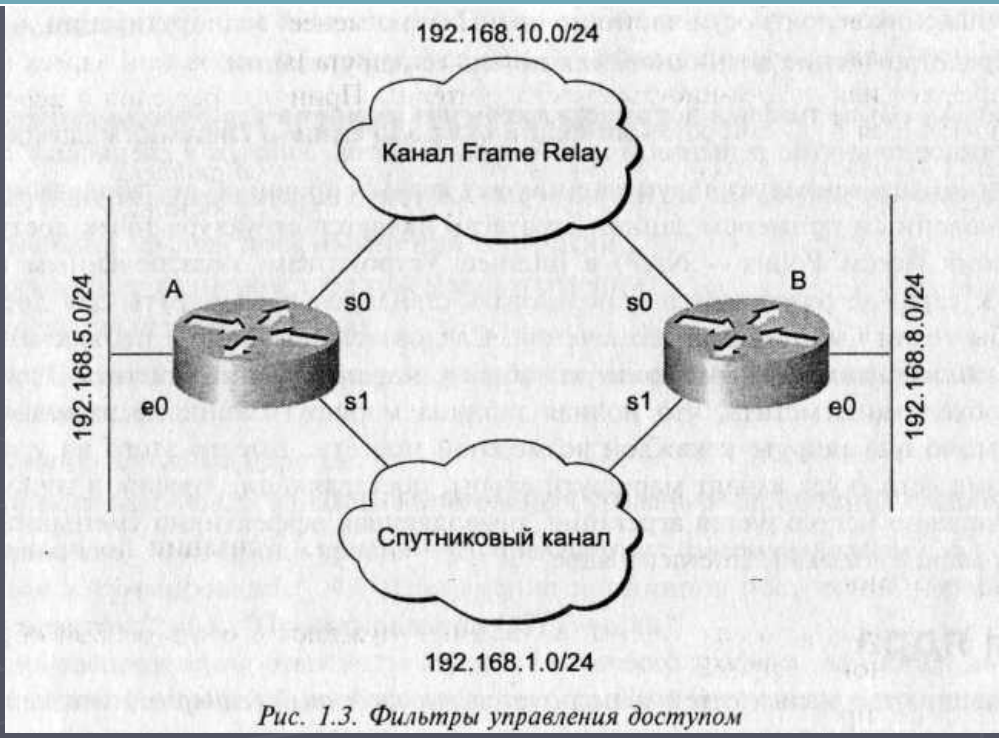


Рис. 1.3. Фильтры управления доступом

Полная достижимость каждого пункта назначения

- Устройства ядра должны обладать достаточной информацией о маршрутах для проведения интеллектуальной коммутации пакета, предназначенного для любого конечного устройства сети;
- маршрутизаторы ядра не должны использовать маршруты по умолчанию для достижения внутренних пунктов назначения
  - ✓ Это не означает, что маршрутизатор ядра должен обладать сведениями о маршруте к каждой отдельной подсети. Для уменьшения размеров таблицы маршрутизации ядра могут и должны использоваться суммарные маршруты.
- Маршруты по умолчанию следует использовать для достижения внешних пунктов назначения, например, узлы в Internet.
- Существует три основные причины для отказа от стратегии маршрутов по умолчанию:
  - ✓ Облегчение задачи обеспечения избыточности ядра
  - ✓ Снижение вероятности частично оптимизированной маршрутизации
  - ✓ Предотвращение возникновения петель маршрутизации.

Полная достижимость каждого пункта назначения

- Поскольку объем трафика достигает максимума именно в ядре, здесь необходимо учитывать каждое принятие решения о коммутации пакетов. Учитывая специфику ядра, частично оптимизированная маршрутизация может явиться причиной дестабилизации сети.
- Великолепным примером данной стратегии является структура точек доступа к сети (Network Access Points — NAP) в Internet
  - ✓ Устройствам, подключенным к NAP, не разрешается использовать маршруты по умолчанию для достижения какого бы то ни было пункта назначения
  - ✓ Следовательно, каждое подключенное устройство *должно* поддерживать полную таблицу маршрутизации Internet (full-BGP)
  - ✓ Здесь опять-таки необходимо отметить, что полная таблица маршрутизации не включает в себя информацию о маршруте к каждой возможной подсети. Вместо этого на уровне распределения сети (куда входят маршрутизаторы, поставляющие трафик в точку доступа к сети) активно используется агрегация, позволяющая эффективно уменьшить размер таблицы маршрутизации Internet в ядре

Типы ядра

- В большинстве малых сетей используется *вырожденный (collapsed)* тип ядра
  - ✓ В ядре один маршрутизатор, соединенный со всеми остальными маршрутизаторами уровня распределения
    - В совсем мелких сетях маршрутизатор вырожденного ядра может быть подключен непосредственно к маршрутизаторам уровня доступа (отсутствует уровень распределения)
  - ✓ Вырожденные ядра легко поддаются обслуживанию, однако достаточно негативно влияют на возможность масштабирования сети
    - необходимость прохождения каждого пакета сети через центральный маршрутизатор, что в конечном итоге может вызвать перегрузку даже самых больших и быстрых маршрутизаторов.
  - ✓ К сожалению, существует тесна связь понятия вырожденного ядра с понятием одиночной точки отказа
    - закон Мерфи: "Вышедший из строя маршрутизатор сети обязательно окажется маршрутизатором вырожденного ядра"
- В большинстве корпоративных сетей для ядра сети используется группа маршрутизаторов, соединенных между собой LAN, или высокоскоростными каналами глобальных сетей WAN
  - ✓ позволяет предусмотреть избыточность еще на этапе проектирования и сохраняет возможность масштабирования сети путем добавления в ядро новых маршрутизаторов и каналов передачи информации
  - ✓ более устойчива по отношению к различным неисправностям и гораздо лучше масштабируется, чем ядро, состоящее из одного маршрутизатора

Уровень распределения

Три четко сформулированные задачи

1. Изоляция последствий изменения топологии
2. Управление размером таблицы маршрутизации
3. Агрегация сетевого трафика

Две основные стратегии достижения этих целей

1. Суммирование маршрутов
2. Минимизация числа каналов, соединяющих уровень распределения с ядром сети

Уровень распределения отвечает за агрегацию сетевого трафика

- ✓ Агрегация достигается за счет объединения трафика,
  - поступающего по большому числу низкоскоростных каналов передачи информации, связывающих уровень распределения с устройствами уровня доступа, в несколько широкополосных каналов, связывающих уровень распределения с ядром сети

Уровень доступа

Три основные задачи

1. Формирование сетевого трафика
   - ✓ сформированный трафик не должен перегружать канал доступа к уровню распределения
     - как правило, эта задача решается на этапе определения пропускной способности
   - ✓ Зависит от расположения пары "сервер—служба" и фильтрации пакетов
     - Трафик, не предназначенный для узла за пределами локальной сети, не должен передаваться устройством уровня доступа
   - ✓ Не должно быть транзита на уровне доступа между двумя маршрутизаторами уровня распределения
     - такая ситуация свойственна сетям с высокой степенью избыточности
2. Контроль доступа к сети
   - ✓ Уровень доступа хорошее место злоумышленника для незаконного проникновения в сеть
   - ✓ Поэтому надо использовать фильтрацию пакетов для блокирования подозрительного трафика
     - Особенно предотвратить атаки, в основе которых лежит подмена (или *спуфинг (spoofing)*) адресов источников
     - Защитить хосты сегмента сети от атак извне (или даже изнутри) вашей сети
3. Выполнение других функций (сервисов) пограничных устройств.

Меры безопасности на уровне доступа

- Большая часть мер безопасности реализуется на участке доступа в Internet
- Однако фильтрация на уровне доступа позволяет регулировать входящий трафик и может значительно повысить безопасность всей сети
- Пример элементарных мер безопасности на уровне доступа (рис. 1.4.)
  - ✓ Запрет спуфинга (разрешить передачу маршрутизатором только тех пакетов, источником которых являются узлы сети 10.1.4.0/24)
  - ✓ Запрет источника с широковещательным адресом (Широковещательный адрес 255.255.255.255 и широковещательный адрес сегмента 10.1.4.255 не являются допустимыми адресами источника и должны отфильтровываться уровнем доступа)
  - ✓ Запрет направленного широковещания (*directed broadcast)*

Адрес назначения *directed broadcast* пакета - широковещательный адрес сегмента

Маршрутизаторы, не подключенные к сегменту, которому предназначается направленное широковещание, будут передавать такой пакет с уникальным Next-hop MAC-адресом назначения

Маршрутизаторы, подключенные к указанному сегменту, преобразуют направленное широковещание в обычное, предназначенное всем хостам сегмента (широковещательный MAC-адрес)

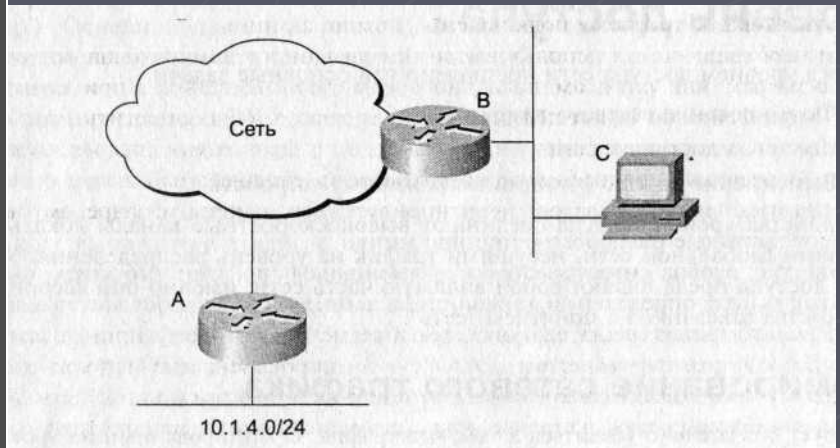


Рис. 1.4. Элементарные меры безопасности, реализуемые на уровне доступа

Меры безопасности на уровне доступа

Пример: Хост С посылает пакет с адресом назначения 10.1.4.255

- ✓ Роутеры сети передадут этот пакет роутеру А
- ✓ Роутер А заменит IP-адрес назначения и MAC-адрес назначения на 255.255.255.255 и FF:FF:FF:FF:FF соответственно и передаст в локальный сегмент Ethernet

Directed broadcast часто используется сетевыми ОС для установки соединений типа клиент/сервер

Directed broadcast может быть сгенерировано путем применения *вспомогательного IP-адреса (IP helper address)* на интерфейсе маршрутизатора, к которому подключены рабочие станции (надо разобраться)

Если нет необходимости в *directed broadcast* необходимо применить команду на интерфейсе роутера **no ip directed broadcast**

Тогда маршрутизатор (какой?) проигнорирует все пакеты с адресом назначения 10.1.4.255, принятые от любого источника сети

Один из способов снижения частоты применения *directed broadcast* — использовать при определении вспомогательных IP-адресов действительный IP-адрес сервера вместо широковещательного адреса сегмента, которому принадлежит данный сервер (надо разобраться)

И даже в случае *directed broadcast* для обращения к устройствам непосредственно подключенного локального сегмента, вы все еще можете блокировать направленное широковещание с неизвестных источников или с источников, находящихся вне вашей сети

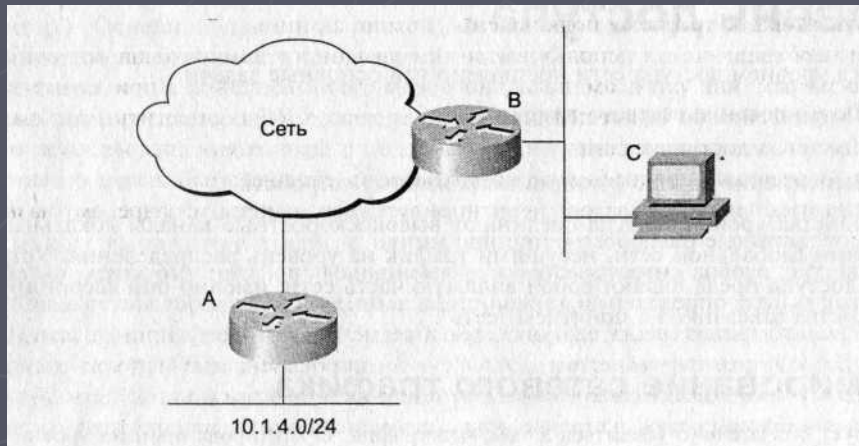


Рис. 1.4. Элементарные меры безопасности, реализуемые на уровне доступа

Другие сервисы пограничных устройств

Некоторые сервисы рекомендуется реализовать еще до того, как пакеты будут переданы какому-либо другому роутеру, так как именно в этом случае удается достичь максимального эффекта от их использования

Примеры наиболее распространенные сервисов, получивших название *сервисы пограничных устройств (edge services).*

- **Маркировка пакетов для маршрутизации, осуществляемой в соответствии с критерием качества обслуживания (Quality of Service — QoS).**
  - случай применения технологии передачи голосовой информации по сетям IP и видеоконференции
  - понятно, что нужна соответствующая настройка маршрутизаторов
- **Уничтожение туннеля.** Как правило, туннели используются для передачи широковещательного трафика, протоколов, не коммутируемых ядром, а также защищенного трафика (виртуальные частные каналы)
- **Измерения объема и учет трафика.** Эти службы включают в себя службы маршрутизаторов Cisco NetFlow.
- **Маршрутизация по правилам.** Более подробно маршрутизация по правилам описана выше в этой главе, в разделе "Практический пример: маршрутизация по правилам"

Подключение к сервисам общего назначения

- Сервисом общего назначения считается любой сервис, к которой регулярно обращается большое число пользователей сети (каких ?)
  - ✓ Примеры: кластер серверов, соединение с внешним маршрутным доменом (например, сеть партнеров или Internet) либо мэйнфрейм.
- Существует два наиболее распространенных метода подключения ресурсов этого типа к сети
  1. Подключение непосредственно к ядру сети
  2. Подключение через демилитаризованную зону (DeMilitarized Zone — DMZ).
- Выбор способа подключения ресурсов к сети зависит от особенностей ее топологии
  - ✓ адресная схема и избыточность
  - ✓ поток трафика и архитектура
- Как правило, в случае подключения внешнего маршрутного домена (DNS ?) рекомендуется создать буферную зону между внешним доменом и ядром сети. Другие службы общего назначения, такие, как мэйнфреймы и кластеры серверов, чаще всего подключаются непосредственно к ядру.
- На рис. 1.5 изображен один из способов подключения сети к сервисам общего назначения.

Подключение к сервисам общего назначения

- Все внешние маршрутные домены подключены через одну демилитаризованную зону (DMZ) в то время, как высокоскоростные устройства, доступ к которым необходим большому числу пользователей сети, подключены к общему высокоскоростному сегменту за пределами ядра.

- Одна из наиболее веских причин организации демилитаризованной зоны — необходимость буферизации трафика (это касается физического уровня сети)
- Достаточно распространенной проблемой маршрутизации является необходимость передачи трафика с радикально различающейся скоростью, например несколько каналов FDDI, соединенных с ядром сети, формируют трафик для передачи по каналу T1 в Internet.

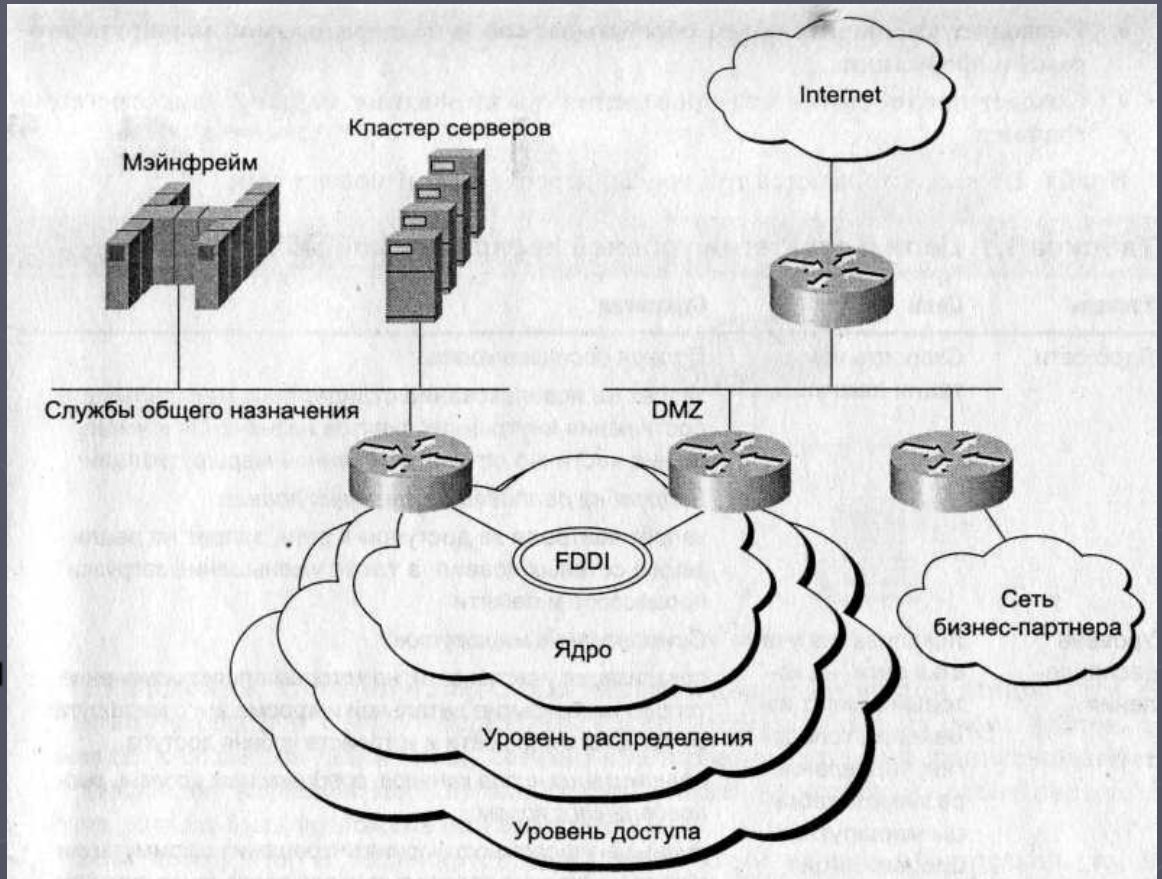


Рис. 1.5. Подключение сети к службам общего назначения

Резюме

Иерархическая маршрутизация - наиболее эффективный способ проектирования крупномасштабной сети благодаря таким ниже перечисленным преимуществам:

- ✓ Иерархия подразумевает разделение одной большой проблемы на несколько более мелких, каждая из которых может быть решена отдельно от других
- ✓ Позволяет эффективно уменьшить размер участка сети, на который влияет изменение топологии
- ✓ Позволяет уменьшить объем обрабатываемой и поддерживаемой маршрутизаторами информации
- ✓ Создает предпосылки для проведения суммирования маршрутов и агрегации трафика

Очень важно реализовать иерархическую структуру в самом начале жизненного цикла сети

- ✓ когда сеть еще не достигла крупного размера, поскольку чем масштабнее будет становиться сеть, тем сложнее будет провести изменение ее структуры

Тщательное проектирование сети сегодня поможет избежать огромных затрат времени на устранение сетевых неполадок в будущем

Цели и стратегии уровней иерархической модели сети

Уровень	Цели	Стратегии
Ядро сети	Скорость коммутации пакетов	Полная достижимость: запрет на использование стандартных маршрутов для достижения внутренних пунктов назначения и уменьшение частично оптимизированной маршрутизации Запрет на реализацию сетевых правил: запрет контроля за доступом к сети, запрет на реализацию сетевых правил, а также уменьшение загрузки процессора и памяти
Уровень распределения	Локализация участка сети, на который влияет изменение топологии, управление размером таблицы маршрутиза	*Суммирование маршрутов*: локализация участка сети, на который влияет изменение топологии, сокрытие детальной информации о маршрутах от устройств ядра сети и устройств уровня доступа, Минимизация числа каналов, соединяющих уровень распределения с ядром: -уменьшение сложности принятия решения о коммутации пакета и создание предпосылок для проведения суммирования маршрутов и агрегации трафика
Уровень доступа	Формирование сетевого трафика; контроль	Предотвращение транзитного трафика. Фильтрация пакетов. В число других служб пограничных устройств входит маркировка пакетов для маршрутизации, осуществляемой в соответствии с критерием качества

Вопросы и упражнения

1. Почему топология сети имеет такое большое значение? Являются ли топология сети и логическая структура сети взаимозаменяемыми понятиями?
2. Почему иерархические сети состоят из нескольких "уровней"?
3. Назовите уровень сети, на котором должны выполняться приведенные ниже функции/службы. Обоснуйте свой ответ.
   - ✓ Суммирование набора сетей назначения для снижения объема информа ции, обрабатываемой маршрутизаторами.
   - ✓ Маркировка пакетов для проведения маршрутизации, осуществляемой в соответствии с критерием качества обслуживания.
   - ✓ Снижение загрузки маршрутизаторов и каналов передачи информации в целях проведения максимально быстрой коммутации пакетов.
   - ✓ Измерение объема трафика.
   - ✓ Использование стандартного маршрута для достижения внутренних пунк-тов назначения.
   - ✓ Контроль поступающего в сеть трафика с помощью фильтрации пакетов
   - ✓ Агрегация нескольких каналов с невысокой пропускной способностью в один высокоскоростной канал.
   - ✓ Уничтожение туннеля

Вопросы и упражнения

4. Назовите два фактора, от которых зависит время, необходимое протоколу маршрутизации для завершения процесса сходимости
5. Какие типы контроля должны быть реализованы в маршрутизаторе уровня доступа для блокировки атак, исходящих из сети?
6. Назовите основные преимущества и недостатки вырожденного ядра, состояего из одного маршрутизатора.
7. Укажите отличие маршрутизации по правилам от обычной маршрутизации.
8. Допустима ли в обычной ситуации передача направленного широковещания в локальный сегмент сети?
9. Какими основными факторами определяется число маршрутизаторов, участвующих в процессе сходимости?
10. Должно ли повреждение сети назначения на уровне доступа инициировать процесс обновления таблиц маршрутизации в маршрутизаторах ядра?
11. Какова первичная цель ядра сети? Какие стратегии используются для достижения этой цели?
12. Обоснуйте исключительную важность оптимальной маршрутизации в ядре сети.
13. Назовите первичные цели уровня распределения сети.
14. Какие стратегии используются на уровне распределения сети для достижения первичных целей этого уровня?
15. Назовите первичные цели уровня доступа сети

Глава 2. Адресация и суммирование

Пример позитива “Суммирование”

IP-адрес v4 - ТЕОРИЯ

Classless Interdomain Routing — CIDR

Правило суммирования

Пример суммирования

Стратегии адресации

Адресация и суммирование

- Выбор способа распределения IP-адресов - один из наиболее тщательно планируемых этапов проектирования сети
- *Необходимо учитывать две основные Цели адресации*
  - ✓ Управление размером таблицы маршрутизации
  - ✓ Управление расстоянием, на которое может распространиться информация об изменении топологии сети (аналогично управлению объемом вычислений, проводимых роутерами в ответ на изменение топологии)
- Наиболее эффективные средства достижения обеих целей - суммирование
- Суммирование позволяет скрыть подробную информацию о топологии, сужая тем самым участок сети, подверженный изменениям, и уменьшая число маршрутизаторов, участвующих в процессе сходимости

Рис. 2.1. Стабильность сети зависит от топологии, адресации и суммирования

Пример позитива “Суммирование”

- Если каналы к 10.1.4.0/24 или 10.1.7.0/24 повреждается, то H потребуется учесть изменение топологии и принять участие в процессе сходимости
- Вопрос: как "спрятать" информацию об изменении топологии от H
- Ответ — выполнить суммирование маршрутов 10.1.4.0/24, 10.1.5.0/24, 10.1.6.0/24 и 10.1.7.0/24 в один маршрут 10.1.4.0/22 на уровне G и предоставить информацию об этом единственном маршруте H

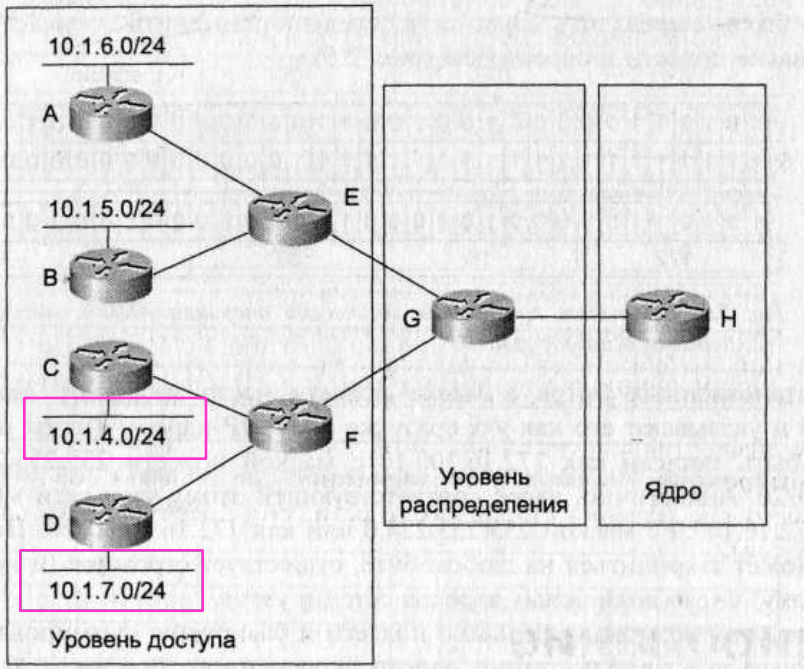


Рис. 2.2. Сокрытие подробной информации о топологии сети от маршрутизатора

- Какие цели достигаются?
  - ✓ Убирается из таблицы маршрутизации H подробная информацию о подсетях
    - поэтому не надо пересчитывать заново свою таблицу маршрутизации
  - ✓ Уменьшается общее число маршрутов, с которыми приходится работать H
    - Снижается требования к памяти и ЦП роутера H
    - Уменьшается время сходимости при изменении топологии, затрагивающем роутер H

IP-адрес v4 - ТЕОРИЯ

- IP-адрес состоит из четырех байт, каждый байт состоит из восьми бит. В каждом байте может быть десятичное число в диапазоне от 0 до 255
- Для поддержки иерархии IP-адрес из четырех байт делится на две части: адрес сети и адрес узла.
- Разделение IP-адреса на адрес сети и адрес узла осуществляется с помощью так называемой маски (или маски подсети).
  - ✓ Каждый бит IP-адреса, которому соответствует бит маски, установленный в 1, относится к адресу сети.
  - ✓ Каждый бит IP-адреса, которому соответствует бит маски, установленный в 0, относится к адресу узла.
- На рис. 2.3 изображено двоичное представление IP-адреса 172.16.100.10.

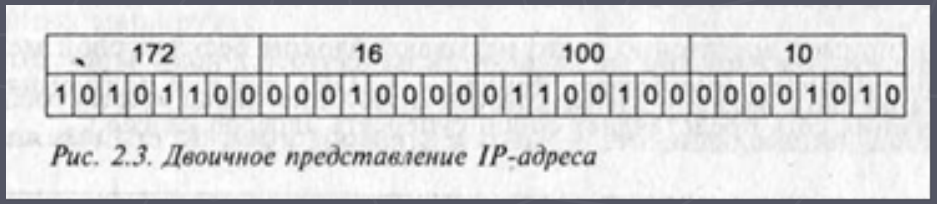


Рис. 2.3. Двоичное представление IP-адреса

IP-адрес v4 - ТЕОРИЯ

- Предположим, что маска подсети, соответствующая данному **IP-адресу, равна** 255.255.240.0; двоичное представление маски подсети показано на рис. 2.4.

255								255								240								0							
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0

Рис. 2.4. Двоичное представление маски подсети

- Для того чтобы определить адрес сети, следует применить логическую операцию AND (И) «маска подсети» AND «адрес узла» (рис. 2.5).

	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	1	0	1	0
&	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
	172								16								92								0							

Рис. 2.5. Результат применения логической операции AND к маске подсети и адресу узла

IP-адрес v4 - ТЕОРИЯ

Рис. 2.5. Результат применения логической операции AND к маске подсети и адресу узла

- Число установленных битов в маске подсети часто называют *длиной префикса (prefix length)* и указывают его как */xx* сразу же после IP-адреса.
- Таким образом, адрес узла может быть записан как 172.16.100.10 с маской подсети 255.255.240.0 или как 172.16.100.10/20.
- Поскольку маска подсети может закончиться на любом бите, существует огромное (и несколько сбивающее с толку) число возможных адресов сетей и узлов.
- Именно на этой возможности маски подсети и базируется суммирование, цель которого заключается в использовании одного укороченного префикса для представления нескольких сетей назначения с более длинным префиксом.

IP-адрес v4 - ТЕОРИЯ

В качестве примера рассмотрим четыре сети IP (рис. 2.6) с длиной префикса 20 бит (маска подсети 255.255.224.0)

Отметим, что все рассматриваемые сети отличаются всего лишь третьим и четвертым битом третьего байта. Если бы удалось каким-то образом отнести эти два бита на адрес узла вместо адреса сети, мы смогли бы представить все четыре сети с помощью одного адреса

Суммирование позволяет легко решить эту задачу путем сокращения длины префикса. В данном случае длину префикса необходимо сократить на два бита (до 18 бит) и представить все четыре сети одной сетью с адресом 172.16.0.0/18. На рис. 2.7 показан пример подобного сокращения длины префикса.

.

172	16	0	0
10101100	00010000	00000000	00000000
11111111	11111111	11100000	00000000
255	255	240	0

172	16	32	0
10101100	00010000	00100000	00000000
11111111	11111111	11100000	00000000
255	255	240	0

172	16	64	0
10101100	00010000	01000000	00000000
11111111	11111111	11100000	00000000
255	255	240	0

172	16	96	0
10101100	00010000	01100000	00000000
11111111	11111111	11100000	00000000
255	255	240	0

Рис. 2.6. Сети IP, представляющие собой идеальный объект для суммирования

172	16	0	0
10101100	00010000	00000000	00000000
11111111	11111111	11000000	00000000
255	255	192	0

Рис. 2.7. Сеть, получившаяся в результате суммирования четырех сетей

IP-адрес v4 - ТЕОРИЯ

- Суммирование может быть проведено на любой границе бита, подтверждением чему служат приведенные ниже примеры.

  10.100.12.0/25 и 10.100.12.128/25 = 10.100.12.0/24

  10.20.0.0/16 и 10.21.0.0/16 = 10.20.0.0/15

  172.16.24.0/27 до 172.16.24.96/27 = 172.16.24.0/25

  192.168.32.0/24 до 192.168.63.0/24 = 192.168.32.0/19

- Последний пример достаточно часто называют блоком бесклассовой междоменной маршрутизации (Classless Interdomain Routing — CIDR), так как полученная в результате суммирования сеть представляет собой суперсеть адресов класса C

Выбор участка сети, на котором должно быть проведено суммирование

- Эмпирическое правило: *предоставляйте полную информацию о топологии только на тех участках сети, где это действительно необходимо*
- ядру не обязательно знать о подсетях доступа
  - ✓ уровень распределения должен
    - суммировать подсети назначения уровня доступа путем укорачивания префикса
    - предоставить ядру информацию о суммированных маршрутах
- уровень доступа:
  - ✓ не должен знать все маршруты, надо знать только маршруты к “своим подсетям”, остальные маршруты “по умолчанию”
  - ✓ уметь принимать решения о пересылке трафика на один или несколько (чаще всего два) подключенных к данному сегменту маршрутизаторов уровня распределения
- уровень распределения представляет собой наиболее оптимальный участок для проведения суммирования в иерархической сети

Пример суммирования уровнем распределения для уровня ядра

Роутер А уровня распределения получает объявления маршрутов от следующих подсетей: 10.1.1.0/26; 10.1.1.64/26; 10.1.1.128/26; 10.1.1.192/26

Роутер А суммирует эти маршруты 10.1.1.0/24 и предоставляет ядру

Поскольку все четыре сети с более длинными префиксами — 10.1.1.0/26, 10.1.1.64/26, 10.1.1.128/26 и 10.1.1.192/26 — "спрятаны" от роутеров ядра в сети 10.1.1.0/24, повреждение любой из этих сетей не повлияет на ядро (другими словами, ни один из роутеров ядра не должен будет обновлять свою таблицу маршрутизации).

Рис. 2.8. Суммирование маршрутной информации, поступающей с уровня распределения в ядро сети

Сокрытие подробной информации о топологии сети от устройств уровня ядра позволяет существенно сузить участок, на который влияет изменение топологии.

Следует отметить, что для проведения суммирования диапазона адресов условие использования всех адресов диапазона не является обязательным (МГФ- справедливый факт);

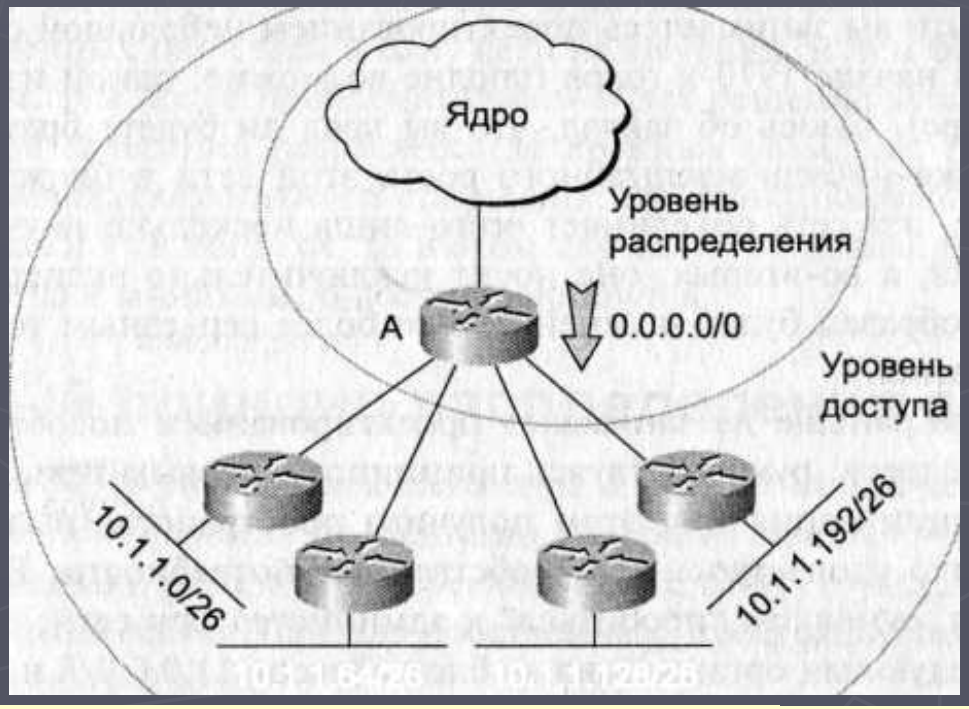
Поэтому единственный негативный момент состоит в том, что нераспределенные адреса суммируемого диапазона не могут быть использованы в дальнейшем (могут - МГФ)

Так, маршруты 10.1.1.0/24, 10.1.2.0/24 и 10.1.3.0/24 могут быть суммированы в единственный маршрут 10.1.0.0/16, при этом адреса с 10.1.4.0 по 10.1.255.255 будут недоступны для дальнейшего использования (МГФ -будут доступны согласно правили длиннейшего префикса).

Пример суммирования уровнем распределения для уровня доступа

- Вся таблица маршрутизации роутера А была суммирована в один пункт назначения 0.0.0.0/0, который известен также как *маршрут по умолчанию (default route)*
- Поскольку ***маршрут по умолчанию*** является единственным маршрутом , объявленным роутерам уровня доступа, то повреждение канала, ведущего к какому-либо пункту назначения в другой части сети, не должно спровоцировать обновление маршрутизаторами уровня доступа своих таблиц маршрутизации. Другими словами, эти маршрутизаторы не будут участвовать в процессе сходимости.

Единственный недостаток при объявлении маршрутизаторам уровня доступа только одного стандартного маршрута связан с возможностью возникновения ***частично оптимизированной маршрутизации***.



Стратегии адресации

- **"Первым пришел — первым обслужен»**
  - ✓ Необходимо достаточное количество адресов и выделять их по мере необходимости.
- **Структурная схема адресации**
  - ✓ Заблаговременное распределение доступного адресного пространства между различными подразделениями организации так, чтобы каждое подразделение обладало собственным пространством выделяемых адресов.
- **Географическая схема адресации**
  - ✓ Заблаговременное распределение адресного пространства между различными региональными офисами организации так, чтобы каждый офис обладал собственным пространством выделяемых адресов.
- **Топологическая схема адресации**
  - ✓ Зависит от точки подключения к сети
  - ✓ (Может совпадать с географической схемой адресации в некоторых сетях)

«Первым пришел - первым обслужен»

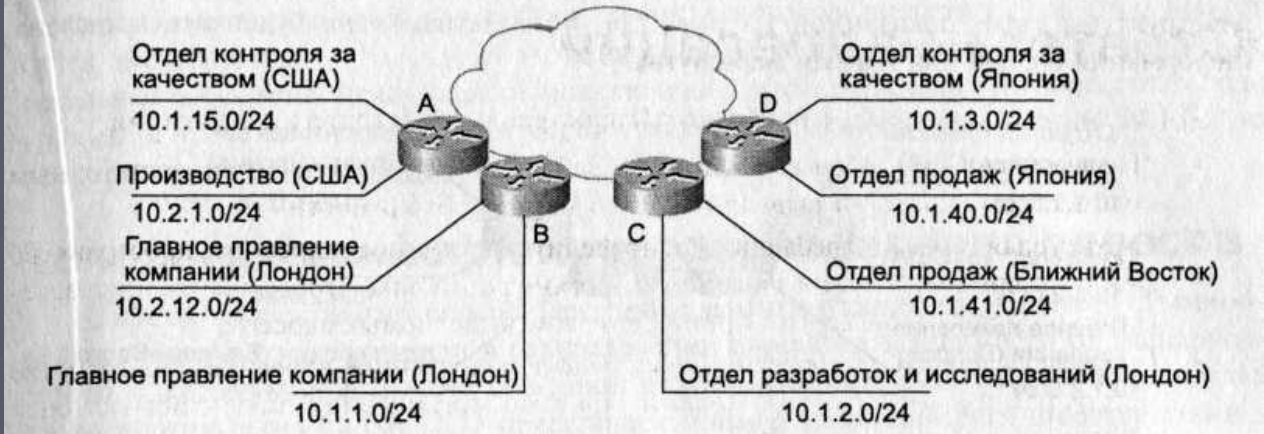


Рис. 2.10. Стратегия распределения адресов по принципу "первым пришел — первым обслужен"

- Маршрутизатор A соединен с двумя сетями: 10.1.15.0/24 и 10.2.1.0/24.
- Маршрутизатор B соединен с двумя сетями: 10.2.12.0/24 и 10.1.1.0/24.
- Маршрутизатор C соединен с двумя сетями: 10.1.2.0/24 и 10.1.41.0/24.
- Маршрутизатор D соединен с двумя сетями: 10.1.40.0/24 и 10.1.3.0/24.

- «Многовековая» традиция проектирования сетей
- Недостатки проявляются при значительном увеличении масштабов сети, поскольку
  - ✓ не существует возможности суммирования
  - ✓ если сеть разрастется до крупных размеров, то будут проблемы, связанные со стабильностью функционирования

Структурный принцип распределения

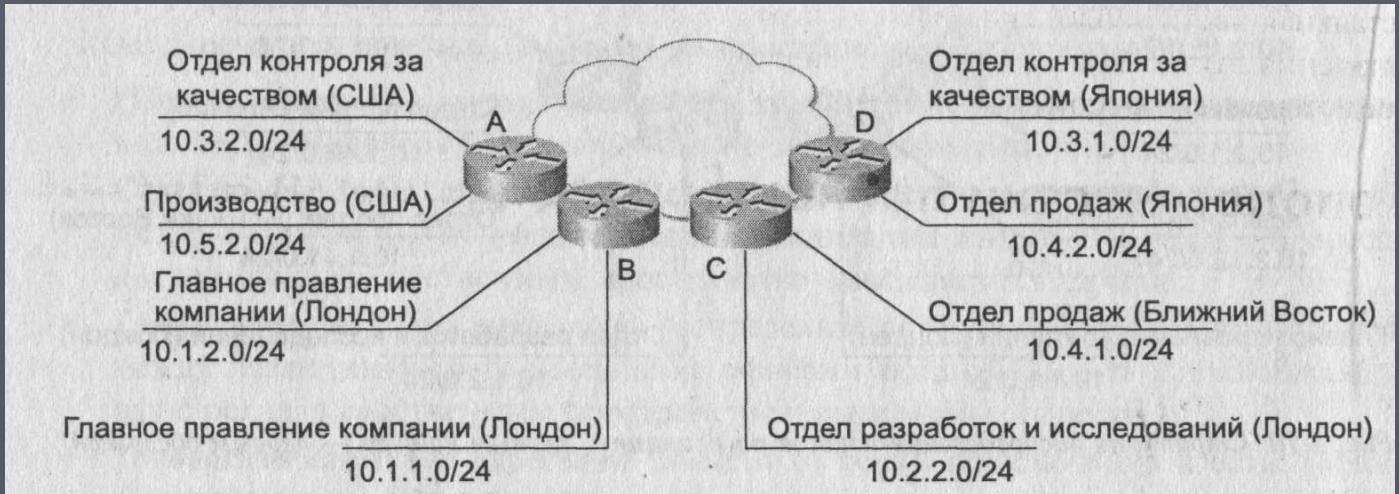


Рис. 2.11. Стратегия распределения адресов в соответствии со структурой организации

- Каждому подразделению выделяем собственное пространство адресов:
  - ✓ Главное правление компании: 10.1.0.0/16.
  - ✓ Отдел исследований: 10.2.0.0/16.
  - ✓ Отдел контроля за качеством: 10.3.0.0/16.
  - ✓ Отдел продаж: 10.4.0.0/16.
  - ✓ Производство: 10.5.0.0/16
- Существуют шансы для проведения суммирования
- По большому счету приводит к такому же результату, что и схема "первым пришел — первым обслужен"

Географический принцип распределения

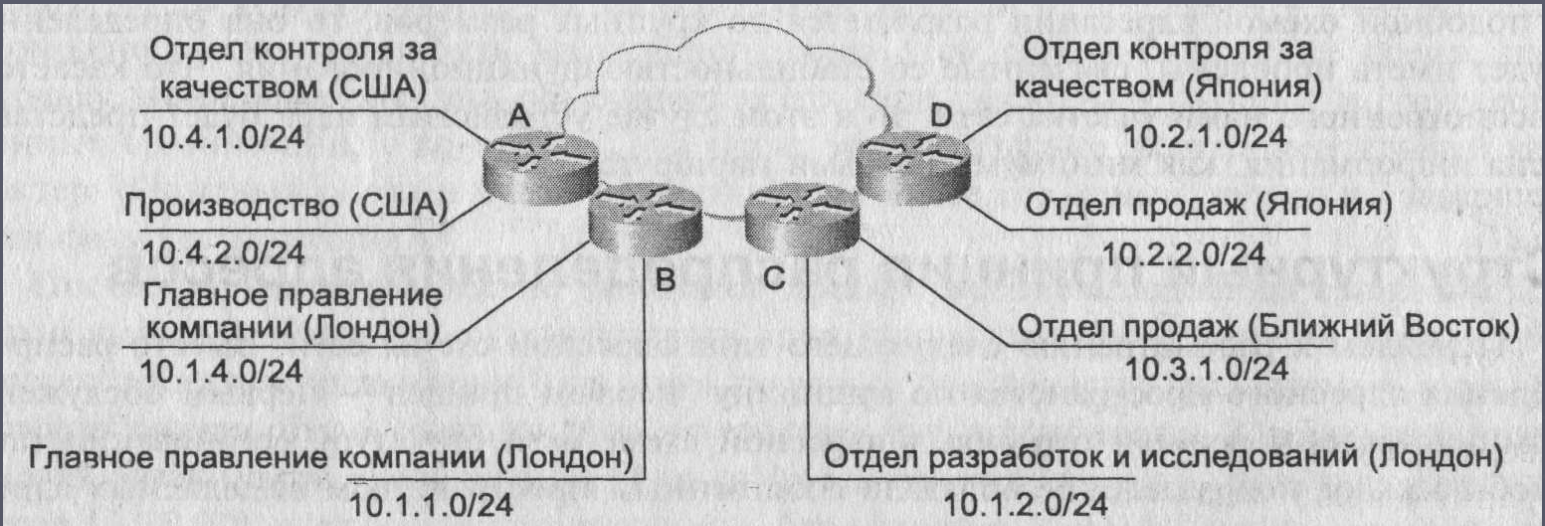


Рис. 2.12. Стратегия распределения адресов в соответствии с географическим расположением сегментов сети

- Гораздо лучше, однако
- Сети Лондона представляют некоторую проблему
  - ✓ Лондонский отдел исследований — 10.1.2.0/24 — подключен к роутеру C
  - ✓ Остальная часть лондонских офисов подключена к роутеру B.
  - ✓ Подключения этих сетей к различным роутерам не позволяет суммирование адресов 10.1.x.x

Топологический принцип распределения

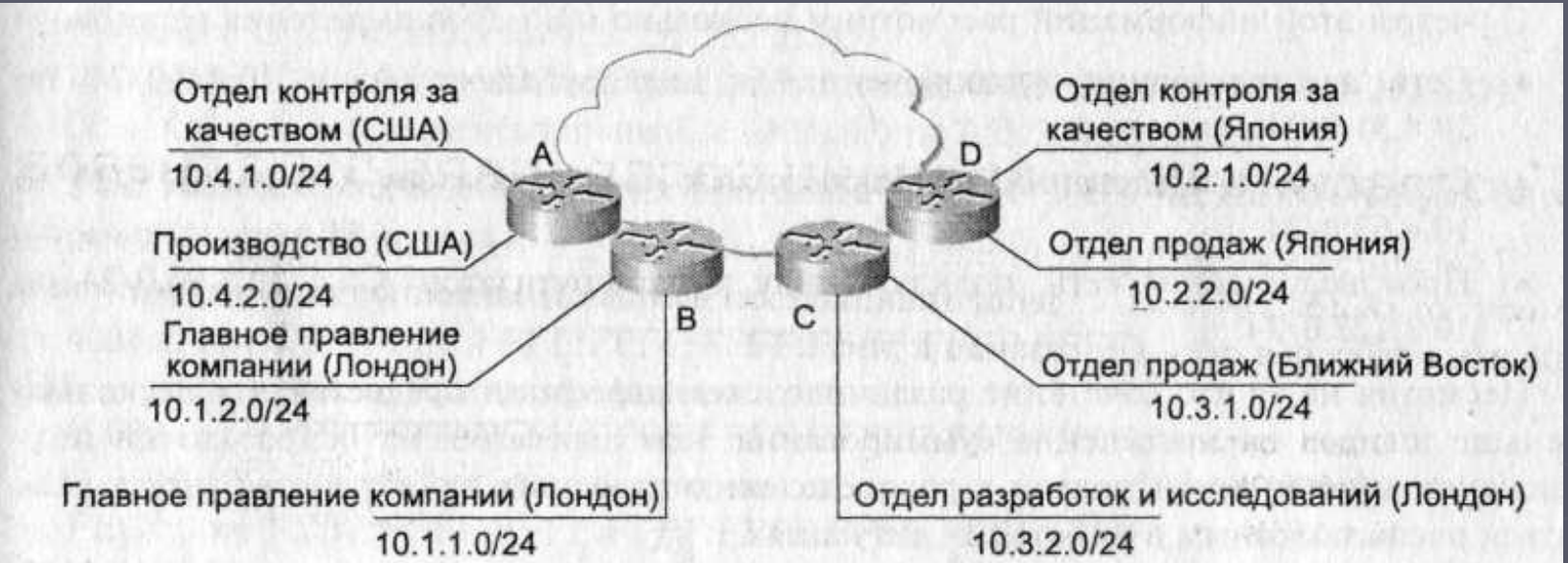


Рис. 2.13. Стратегия распределения адресов, основанная на топологии сети

- Наиболее эффективный способ адресации
  - ✓ гарантирующий возможность суммирования маршрутов
  - ✓ заключается в распределении адресов в зависимости от точки подключения к роутеру

Сочетание различных схем распределения

- Недостаток топологического принципа - затруднен способ определения какого-либо контекста без предварительного знания структуры или базы данных, например подразделения компании, к которому относится определенная сеть
- Минимизация недостатка – сочетание топологического принципа с другими принципами
- Предположим следующие назначения адресов
  - ✓ Администрация: 0 - 31
  - ✓ Отдел исследований: 32 - 63
  - ✓ Отдел продаж: 64 - 95
  - ✓ Производство: 96 - 127
- Нумерация точек **подключения к роутерам**
  - ✓ Маршрутизатор A: 4.
  - ✓ Маршрутизатор B: 1.
  - ✓ Маршрутизатор C: 3.
  - ✓ Маршрутизатор D: 2.
- С учетом этой информации рассмотрим несколько примеров выделения адресов.
  - ✓ Сеть администрации, подключена к роутеру A: с 10.4.0.0/24 по 10.4.31.0 /24
  - ✓ Сеть отдела исследований, подключена к роутеру A: с 10.4.32.0/24 по 10.4.63.0 /24
  - ✓ Производственная сеть, подключенная к роутеру C: с 10.3.96.0/24 по 10.3.127.0/24
- Сочетание различных схем адресации предоставляет несколько меньше шансов на проведение суммирования
  - ✓ такой подход к распределению адресного пространства может оказаться очень полезным в некоторых ситуациях

Система адресации протокола IPv6

- Главное различие между IPv4 (32-битовый адрес) и IPv6 (128-битовый адрес) заключается в намного большем адресном пространстве IPv6
- IPv6-адрес представляется в виде восьми 16-битовых частей
  - ✓ FE81:2345:6789:ABCD:EF12:3456:789A:BCDE /96)
  - ✓ / xx в конце адреса IPv6 по-прежнему определяет число битов в маске подсети
- Любая единственная серия из нулей (0) в адресе IPv6 может быть заменена символом двоеточия
  - ✓ Пример эквивалентных записей
    - FE80:0000:0000:0000:1111:2222:3333:4444
    - FE80::1111:2222:3333:4444.
      - символом двоеточия может быть заменена только одна серия нулей
  - ✓ последние 32 бита адреса IPv6 могут быть записаны как адрес IPv4:
    - FE80::172.16.10.4

Система адресации протокола IPv6

- Другие отличия в способах адресации протоколов IPv4 и IPv6
  - ✓ В IPv4 класс адреса определяется по нескольким первым битам.
    - 0 - класс A (с 0.0.0.0 по 126.255.255.255)
    - 10 - класс B (с 128.0.0.0 по 191.255.255.255).
    - 11O - класс C (с 192.0.0.0 по 223.255.255.255)
    - 1110 - класс D (групповой с 224.0.0.0 по 239.255.255.255).
    - 1111 — класс E (экспериментальный, с 240.0.0.0 по 255.255.255.255).
  - ✓ В IPv6 несколько первых битов определяют *тип* IP-адреса
    - 010 — выделяемые уникальные адреса поставщиков услуг
      - с 4000::0 по 5FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
    - 100 — уникальные адреса географических зон
      - с 8000::0 по 9FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
    - 1111 1110 10 — адреса локальных каналов
      - с FE80::0 по FEBF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
    - 1111 1110 11 — адреса локальных узлов
      - с FEC0::0 по FEFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF)
    - 1111 1111 — адреса групповой передачи данных
      - с FF00::0 по FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF)

Система адресации протокола IPv6

- Специальные адреса IPv6
  - ✓ 0::0 — неопределенный адрес
  - ✓ С 0::1.1.1.1 по 0::255.255.255.255 - адреса IPv4
  - ✓ 0::0001 — адрес обратной связи
- В IPv6 отсутствует широковещательный адрес
  - ✓ Вместо него используется адрес групповой передачи данных всем узлам сети

Между адресами IPv4 и IPv6 существует огромное число различий — начиная от формата пакета и заканчивая способом определения узлом своего адреса.

Общие принципы адресации

- Необходимость “суммирования и обеспечения стабильности” приводит к потере некоторой части адресного пространства
- Принципы “суммирования и стабильности” диаметрально противоположны принципам полного использования адресного пространства
- Решение проблемы нехватки адресов
  - ✓ Использование изначально *очень* большого по объему адресного пространства (большего чем понадобиться)
    - использование блока частных адресов и применении *трансляции сетевых адресов (Network Address Translation — NAT) для* преобразования частных адресов вашей сети при подключении к внешним пунктам назначения
  - ✓ Частные адреса IPv4, определенные группой IETF:
    - С 10.0.0.0 по 10.255.255.255 - одна сеть класса A
    - С 172.16.0.0 по 172.31.255.255 - 16 сетей класса B
    - С 192.168.0.0 по 192.168.255.255 - 256 сетей класса C
  - ✓ Недостатки использования NAT:
    - некоторые приложения функционируют не самым лучшим образом
    - дополнительная сложность, связанной с настройкой NAT

Резюме

- Первичные цели стратегий адресации и суммирования управление размером таблицы маршрутизации (уменьшение) и ограничении участка сети, через который должна распространиться информация об изменении топологии
- Размер таблиц маршрутизации во всей сети должен быть примерно одинаковым, за исключением удаленных устройств, использующих стандартный маршрут для пересылки всего трафика. Данный принцип наглядно представлен на рис. 2.14.
- Для обеспечения большей наглядности принципы и стратегии суммиро¬вания представлены в табл. 2.1.

Таблица 2.1. Места проведения и стратегии суммирования

Место проведения суммирования	Стратегия суммирования
Участок "уровень распределения — ядро"	Суммирование большого числа точек назначения уровня доступа в несколько маршрутов, объявляемых устройствам ядра. Сокрытие подробной информации о топологии уровня доступа и уровня распределения от устройств ядра
Участок "уровень распределения — уровень доступа"	Суммирование топологии всей сети в очень ограниченный набор объявлений маршрутов, предостав-ляемых устройствам уровня доступа (по возможности использование стандартного маршрута). Объявление маршрута к ближайшему роутеру уровня распределения, имеющему доступ к устройствам ядра Сокрытие информации о топологии ядра и уровня распределения от устройств уровня доступа

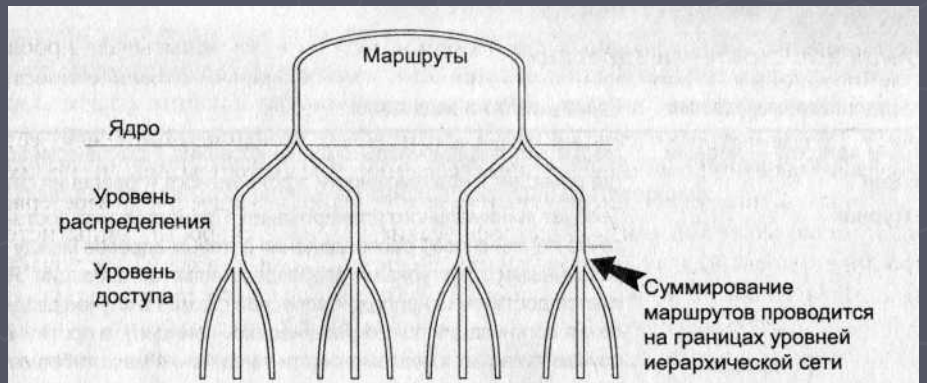


Рис. 2.14. Размер таблиц маршрутизации по всей сети должен быть примерно одинаковым

Таблица 2.2. Стратегии адресации

Схема распределения адресов	Преимущества и недостатки
Первым пришел — первым обслужен	Не требует предварительного планирования. Практически всегда приводит к невозможности эффективного управления сетью
Структурная	Требует минимального планирования. Предоставляет достаточно легкий способ распределения сетевых адресов между различными структурными подразделениями организации. Является достаточно неплохой адресной схемой в случае разделения организации по географическому принципу; в противном случае приводит к невозможности увеличения масштабов сети
Географическая	Требует предварительного планирования. Создает некоторые предпосылки для проведения суммирования
Топологическая	Требует предварительного планирования. Создает предпосылки для проведения суммирования, которое выражается в существенном уменьшении размера таблиц маршрутизации устройств ядра в крупномасштабных сетях. Позволяет проводить эффективное увеличение масштабов сети. Как правило, поддается достаточно легкой настройке и уменьшает число проблем, связанных с поддержкой сети

Пример: default-route к интерфейсам

- При настройке роутеров определяется default-route, указывающий на интерфейс выходного трафика по умолчанию
- Иногда использование default-route к интерфейсу может привести к весьма плачевным последствиям
- Проблемы, связаны, как правило, с типом канала передачи данных
  - ✓ протоколом ARP
  - ✓ и так называемым прокси-ARP

Пример, когда плохо прокси ARP

Пусть имеем конфигурацию

- default-route исходящего трафика роутера A (рис. 2.15) интерфейс Ethernet0
  - ✓ ip route 0.0.0.0 0.0.0.0 Ethernet 0
- default-route исходящего трафика роутера B интерфейс Serial0
  - ✓ ip route 0.0.0.0 0.0.0.0 serial 0

Негативная сторона конфигурации - высокая степень использования ЦП и памяти роутера A

Пример:

- Если пакет идет от ws2 в хост в Internet
  - ✓ ws2 посылает пакет на свой default-route, роутер B;
  - ✓ роутер B пересылает пакет по default-route на serial 0 (двухточечный интерфейс, нет вариантов)
- Если пакет идет от ws1 в хост Internet
  - ✓ ws1 перешлет пакет на default-route (роутер A).
  - ✓ роутер A хочет переслать пакет по default-route через Ethernet0, но не знает MAC-адреса next-hop

поэтому

1. Роутер A выставляет ARP-запрос
2. Роутер B в ARP-ответе показывает свой маршрут default-route
3. Роутер A установит в кэше ARP соответствие:
   - ✓ MAC-адрес роутера B - IP-адрес пункта назначения в Internet
     - ✓ Ответ на ARP-запрос роутера B называется *прокси-ARP (proxy ARP)*
     - ✓ поскольку роутер B, по сути, подменяет своим адресом каждую точку назначения в Internet

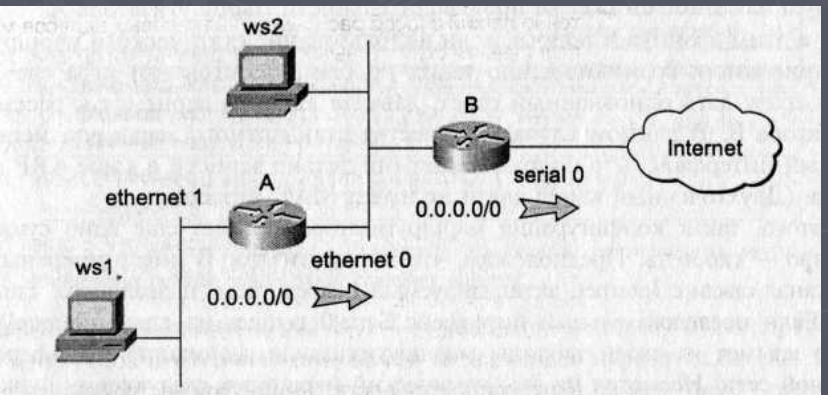


Рис. 2.15. Стандартный маршрут к широковещательному интерфейсу

Пример, когда плохо прокси ARP

- Существенный недостаток: роутер A поддерживает информацию о каждом пункте назначения, к которому обращается рабочая станция ws1, в своем кэше ARP-запросов
  - ✓ Расходование памяти и ресурсов процессора
  - ✓ Трата времени на освобождение места в кэше ARP для размещения результатов новых запросов
    - снижению эффективности использования кэша ARP
    - снижение производительности роутера A
- Вопрос: если статический default-route к интерфейсу приводит к проблемам, то зачем это надо?
- Еще раз о роутере B
  - ✓ в качестве default-route используется двухточечный интерфейс, что подразумевает отсутствие записей в кэше ARP для этого интерфейса. (Двухточечный канал связи не имеет MAC-адресов)
  - ✓ такая конфигурация роутера B имеет еще одно существенное преимущество — скорость. Предположим, что роутер B имеет резервный коммутируемый канал связи с Internet, активизируемый посредством "плавающего" статического маршрута. Если последовательный интерфейс Serial0 выйдет из строя, роутер B немедленно изымет из своей таблицы маршрутизации информацию о непосредственно подключенной сети
  - ✓ Несмотря на это, статический маршрут к следующему пункту назначения будет присутствовать в таблице маршрутизации примерно еще одну секунду, поскольку роутеру B потребуется некоторое время для того, чтобы убедиться в повреждении рекурсивного маршрута к следующему пункту назначения
- Использование статического маршрута, указывающего непосредственно на интерфейс, способно уменьшить количество времени, требующееся маршрутизатору для активизации резервного канала связи (например, канала ISDN).

Трансляция сетевых адресов (NAT)

- Network Address Translation (NAT) позволяет преобразовать один набор IP-адресов в другой
  - ✓ например, частный IP-адрес в зарегистрированный адрес
- NAT может быть использована также для
  - ✓ равномерного выравнивания нагрузки между серверами
  - ✓ обеспечения избыточности на уровне серверов
  - ✓ объединения компаний, использующих одинаковое адресное пространство

Пример:

- Узел с частным IP-адресом 10.1.4.1 пытается обратиться к серверу в Internet с IP-адресом 109.10.1.4
- частный IP-адрес 10.1.4.1 не может быть в качестве адреса источника при маршрутизации пакетов в Internet
- Роутер А может преобразовать пакеты от 10.1.4.1, таким образом, чтобы они выглядели как пакеты, полученные от источника, принадлежащего сети обратной связи

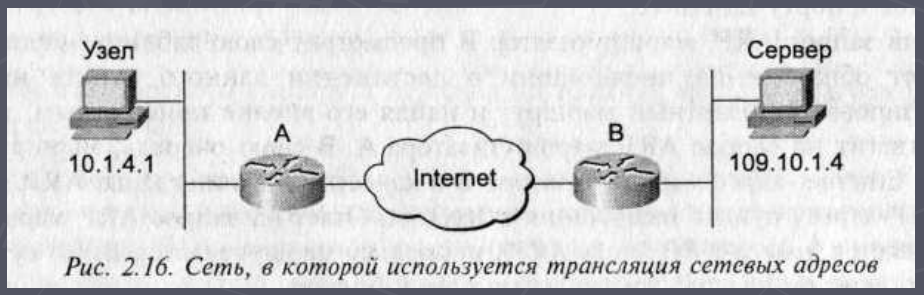


Рис. 2.16. Сеть, в которой используется трансляция сетевых адресов

	До трансляции		После трансляции	
Направление	Отправитель	Получатель	Отправитель	Получатель
От узла к серверу	10.1.4.1	109.10.1.4	127.10.1.10	109.10.1.4
От сервера к узлу	109.10.1.4	127.10.1.10	109.10.1.4	10.1.4.1

Рис. 2.17. Адреса источника и пункта назначения, полученные в результате применения трансляции сетевых адресов

Пример NAT

В результате трансляции адрес 10.1.4.1 (внутренний адрес) будет преобразован в Internet-адрес 127.10.1.10 (внешний адрес)

- Терминология Cisco
  - ✓ адрес 10.1.4.1 - *внутренний локальный адрес (inside local address)*
  - ✓ адрес 127.10.1.10 - *внутренний глобальный адрес (inside global address)*
  - ✓ адрес 109.10.1.4 - *внешний глобальный адрес (outside global address)*

Пример настройки роутера А

- ✓ ip nat pool tothenet 127.10.1.10 127.10.1.10 prefix-length 24
- ✓ ip nat inside source list 1 pool tothenet
- ✓ !
- ✓ interface Ethernet 0
  - ➢ ip nat inside
- ✓ !
- ✓ interface Serial 0
  - ➢ ip nat outside
- ✓ !
- ✓ access-list 1 permit 10.0.0.0 0.255.255.255

- NAT полезна за исключением случаев, когда огромному числу узлов внутренней локальной сети соответствует всего лишь несколько внешних адресов

Пример PAT

Направление	До трансляции		После трансляции	
	Отправитель	Получатель	Отправитель	Получатель
От узла к серверу	10.1.4.1 порт 5312	109.10.1 порт 80	127.10.1.10 порт 1254	109.10.1.4 порт 80
От сервера к узлу	109.10.1.4 порт 80	127.10.1.10 порт 1254	109.10.1.4 порт 80	10.1.4.1 порт 5312

Рис. 2.18. Трансляция адреса с использованием портов

- Большинство реализаций NAT проводят "тонкое" присвоение адреса
  - ✓ известное как трансляция адресов с использованием портов
    - Port Address Translation — PAT или *перегрузка (overloading)* адреса
- Трансляция адресов с использованием портов (PAT) подразумевает
  - ✓ присвоение *номера порта (port number)* внутреннему глобальному (транслированному) адресу для каждого инициированного соединения
  - ✓ использование одного внутреннего глобального адреса позволяет организовать ~32 тыс (2^{16}) одновременных соединений внутренних хостов с внешними хостами в Инет
- Если предусмотреть для каждого внутреннего хоста 10 одновременных соединений с внешними узлами, получим следующее
  - ✓ один внешний адрес может обеспечить возможность доступа к внешнему миру почти 3000 внутренних узлов

Настройки роутера A

```
ip nat pool tothenet 127.10.1.10 127.10.1.10 prefix-length 30
ip nat inside source list 1 pool tothenet overload
!
interface Ethernet 0
    ip nat inside
!
interface Serial 0
    ip nat outside
!
access-list 1 permit 10.0.0.0 0.255.255.255
```

- Роутеры Cisco назначают порт на внутреннем глобальном адресе согласно группы диапазонов, при проведении PAT трансляции адресов:
  - ✓ 1-511
  - ✓ 512-1023
  - ✓ 1024-4999
  - ✓ 5000-65535
- Т.е. если внутренний узел использует порт источника 500, то при проведении трансляции адресов типа PAT в качестве порта источника маршрутизатор выберет порт из диапазона 1—511

Вопросы и упражнения

1. Чем обусловлена исключительная сложность изменения способа распределения сетевых адресов?
2. Почему способ распределения сетевых адресов тесно связан со стабильностью функционирования всей сети?
3. Назовите первичные цели, о которых необходимо помнить при выборе способа распределения сетевых адресов.
4. Что обозначает фраза "Суммирование позволяет скрыть подробную информацию о топологии"?
5. Каким образом сокрытие подробной информации о топологии позволяет улучшить стабильность функционирования сети?
6. На каких участках сети следует проводить суммирование?
7. Назовите единственный случай, в котором устройствам уровня доступа следует предоставить более чем один стандартный маршрут. Почему?
8. На какие две части может быть разделен IP-адрес?
9. Что представляет собой длина префикса сети?

Вопросы и упражнения

10. Определите наибольшую длину суммарного префикса для приведенных ниже адресов.
    - ✓ Набор A: 172.16.1.1/30, 172.16.1.5/30, 172.16.1.9/30, 172.16.1.14/30
    - ✓ Набор B: 10.100.40.14/24, 10.100.34.56/24, 10.100.59.81/24
    - ✓ Набор C: 172.18.10.10/23, 172.31.40.8/24, 172.24.8.1/22, 172.30.200.1/24
    - ✓ Набор D: 192.168.8.10/27, 192.168.60.14/27, 192.168.74.90/27, 192.168.101.48/27
11. Опишите эффект, возникающий вследствие использования в качестве стандартного маршрута широковещательного сетевого интерфейса.
12. Что обозначает пара двоеточий в адресе IPv6? Сколько раз можно использовать данный символ в записи адреса?
13. Объясните различие между трансляцией сетевых адресов (Network Address Translation — NAT) и трансляцией адресов с использованием портов (Port Address Translation — PAT).

Вопросы и упражнения

14. Выполните адресацию сети, схематически изображенной на рис. 2.19, в соответствии со структурным (организационным), географическим и топологическим принципом распределения сетевых адресов

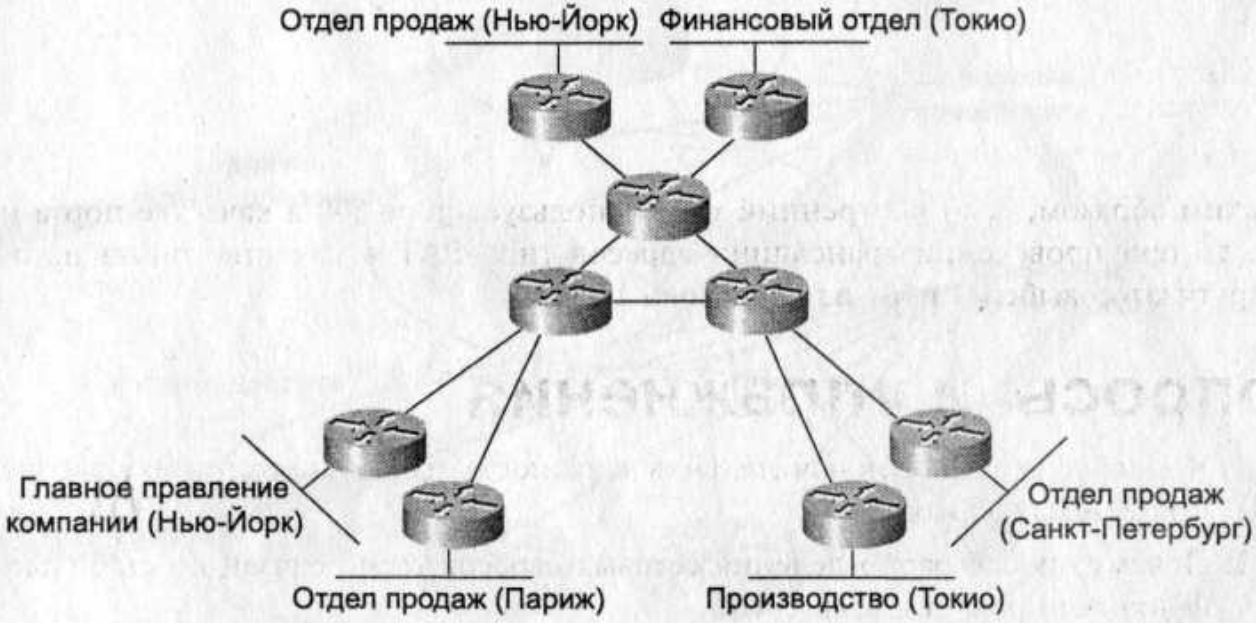


Рис. 2.19. Проведите адресацию сети в соответствии с различными принципами распределения сетевых адресов

Глава 3. Избыточность в иерархических сетях

Одиночная точка отказа и избыточность

Цели и стратегии избыточности

Избыточность на уровне распределения

Избыточность на уровне доступа

Одиночная точка отказа и избыточность

- Одиночная точка отказа — это любое устройство, интерфейс устройства или канал передачи информации, который, будучи поврежденным, приводит к изоляции пользователей от необходимых им в повседневной работе служб
- Для сетей, спроектированных в соответствии со строгой иерархической моделью, характерно наличие достаточно большого числа одиночных точек отказа,
  - ✓ Это связано с их ориентацией на проведение суммирования и четкой разграниченностью между различными уровнями сети.

- Надежность может быть существенно повышена за счет использования коммутируемых резервных каналов
- Избыточность предполагает наличие альтернативных каналов
- Однако неумело спланированная и реализованная избыточность может нанести вред, заметно превосходящий все ее потенциальные достоинства
- Каждый избыточный канал и каждая избыточная точка подключения ослабляют иерархию и приводят к снижению стабильности сети

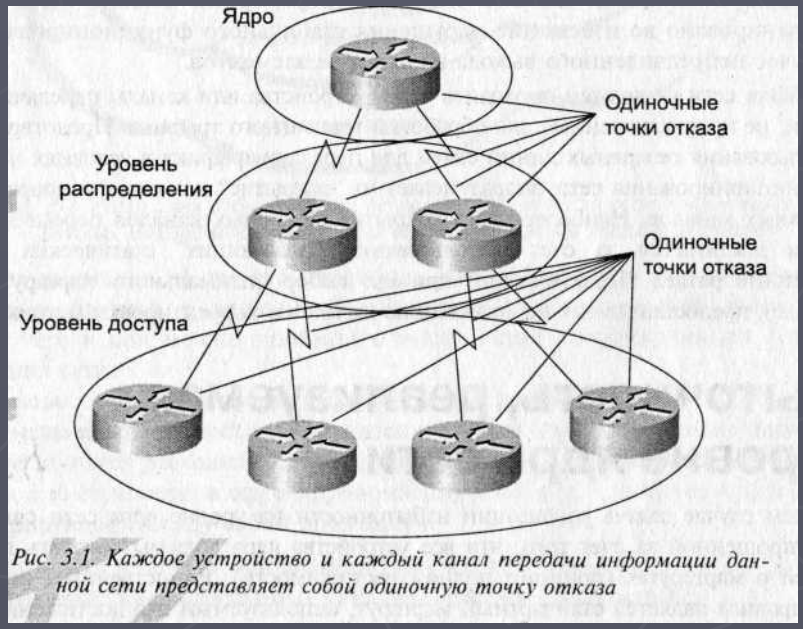


Рис. 3.1. Каждое устройство и каждый канал передачи информации данной сети представляет собой одиночную точку отказа

Цели и стратегии избыточности

- Избыточные каналы передачи информации должны использоваться только в случае повреждения основных каналов
  - ✓ единственное исключение - для выравнивания потока трафика в сети
- Трафик сети не должен проходить через устройства или каналы, не предназначенные для обработки транзитного трафика.
- Предотвращение использования резервных линий связи для передачи трафика в условиях нормального функционирования сети подразумевает их "сокрытие" до момента повреждения основных каналов.
- Наиболее часто сокрытие резервных каналов передачи информации достигается за счет использования "плавающих" статических маршрутов
  - ✓ (читайте раздел "Практический пример: выбор оптимального маршрута" далее в главе), предоставляемых по требованию каналов и корректировки метрики.

Избыточность на уровне ядра сети

- Несколько упрощена реализация избыточности - поскольку все устройства ядра должны обладать полной информацией о маршрутах (Исключение – маршрут по умолчанию, используемый для достижения внешних маршрутных доменов, таких, как Internet или сеть партнера)
  - ✓ И поэтому шанс возникновения петли маршрутизации внутри ядра в условиях нормального функционирования сети крайне невелик
    - использование в ядре нескольких внутренних протоколов маршрутизации *не считается* условием нормального функционирования сети
  - ✓ Вполне *возможно,* что пакеты будут передаваться по частично оптимизированным маршрутам, однако петля маршрутизации при наличии полной информации о маршрутах является событием из ряда вон выходящим

Структура ядра с резервными связями

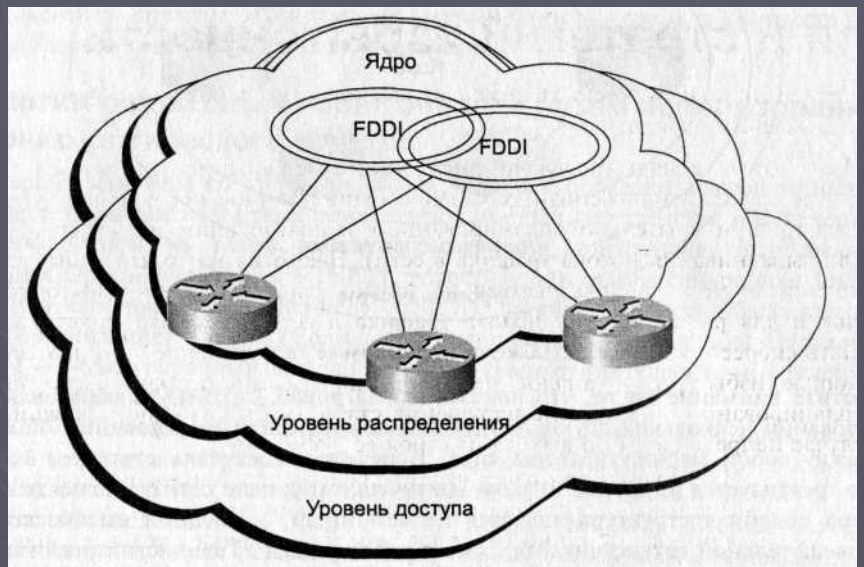


Рис. 3.2. Реализация избыточности на уровне ядра сети за счет подключения базовых маршрутизаторов к двум высокоскоростным локальным сетям

- Если вся базовая сеть сосредоточена в одном здании, избыточность может быть достигнута за счет подключения каждого маршрутизатора к двум высокоскоростным локальным сетям (LAN), таким, как Ethernet или волоконно-оптическое кольцо
- Логически данная структура ядра является топологией с полным объединением, вследствие чего к ней можно применить аналогичные соображения по поводу масштабирования сети.

Избыточность на уровне распределения сети

- Существует два наиболее распространённых метода реализации избыточности на уровне распределения сети:
  - ✓ двойное подключение устройств (Рис. 3.8) и
  - ✓ использование резервных каналов передачи информации для соединения маршрутизаторов уровня распределения (Рис.3.9)

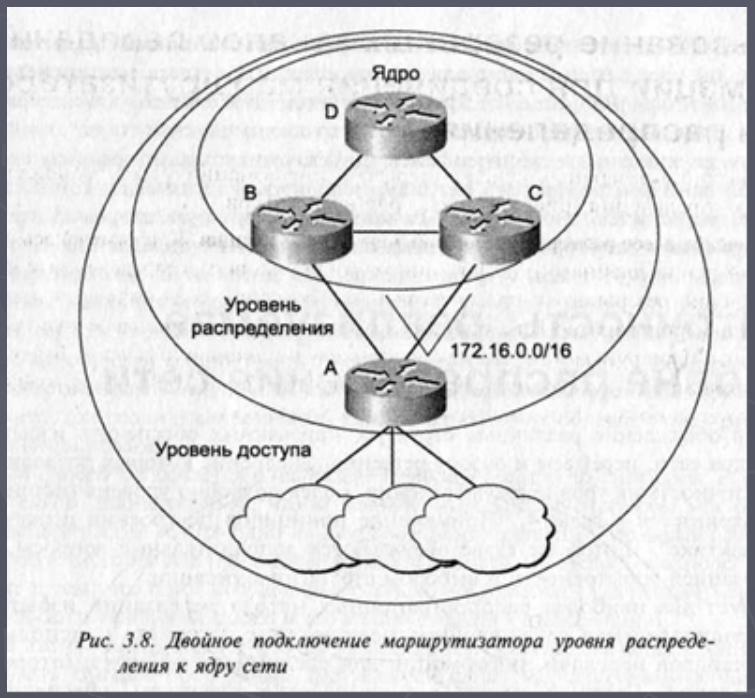


Рис. 3.8. Двойное подключение маршрутизатора уровня распределения к ядру сети

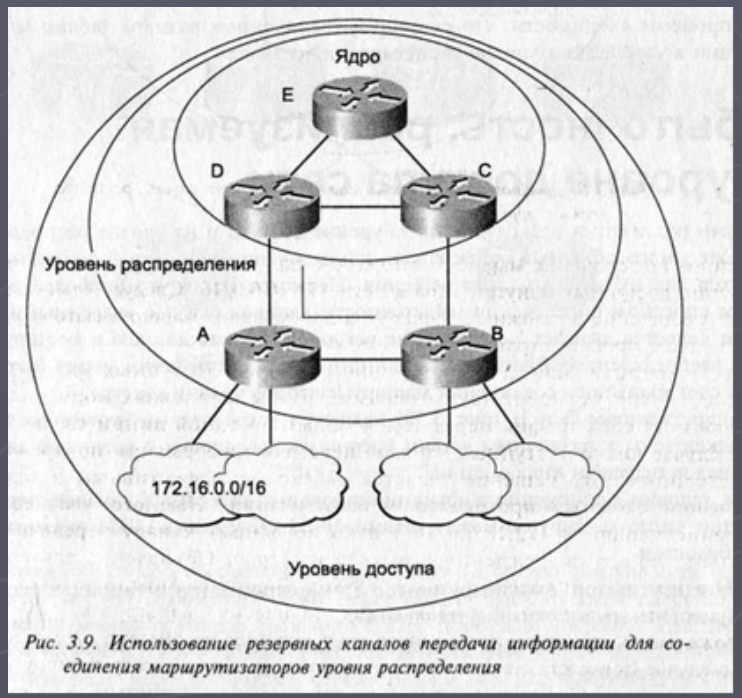


Рис. 3.9. Использование резервных каналов передачи информации для соединения маршрутизаторов уровня распределения

Избыточность на уровне доступа

- двойное подключение устройств уровня доступа к маршрутизаторам уровня распределения (рис 3.10)
- взаимное соединение маршрутизаторов уровня доступа (Рис. 3.11).

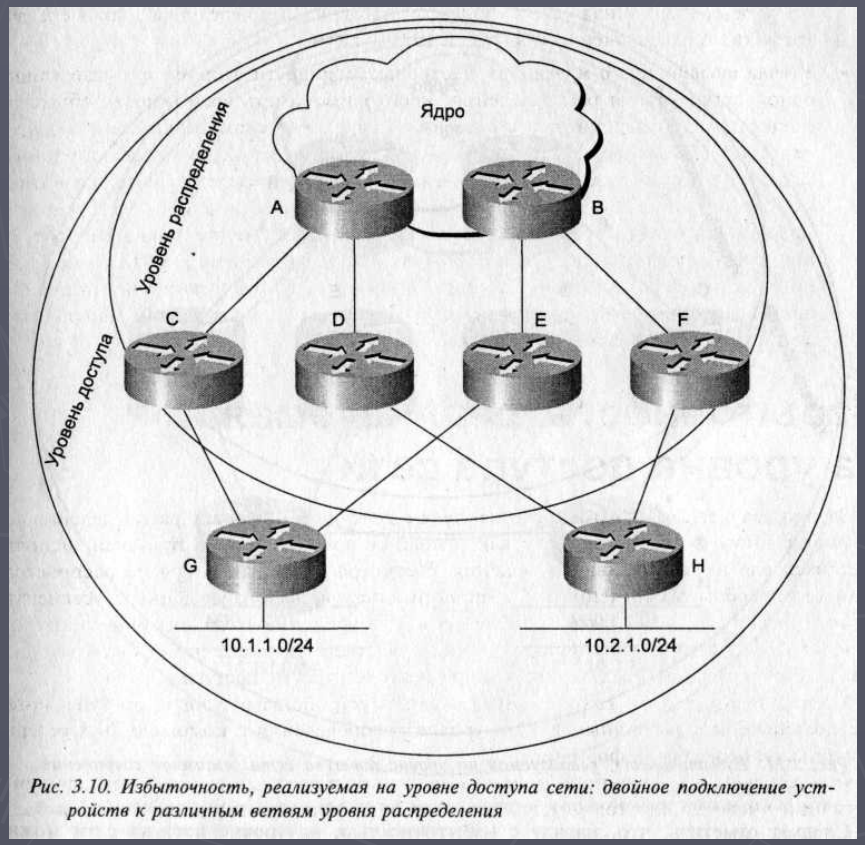


Рис. 3.10. Избыточность, реализуемая на уровне доступа сети: двойное подключение устройств к различным ветвям уровня распределения

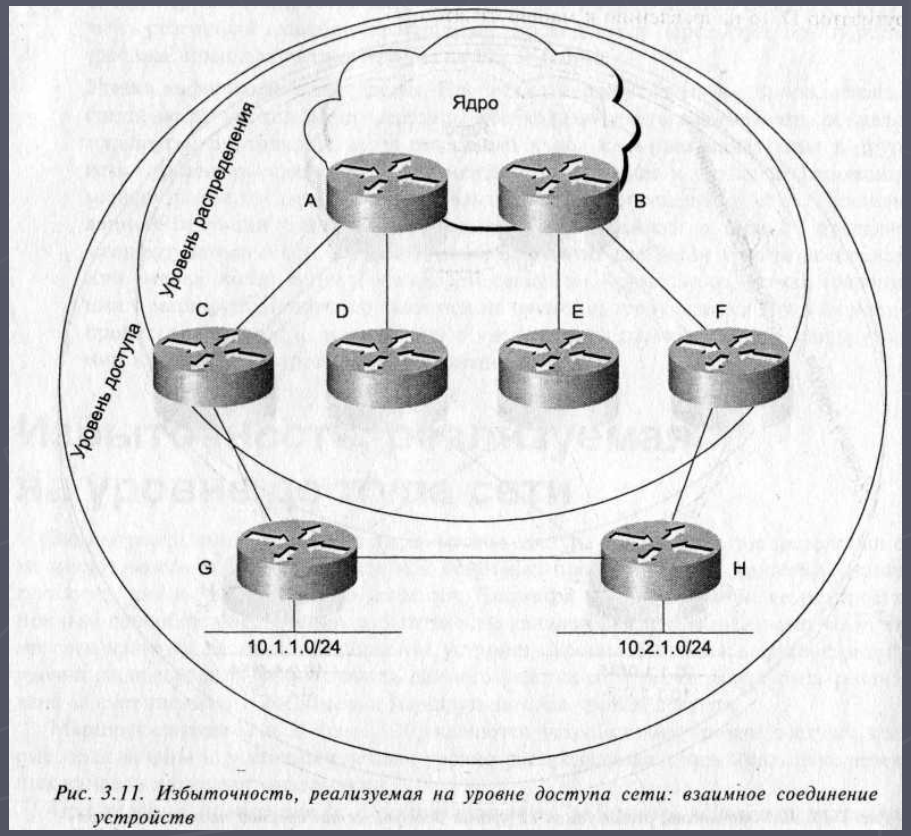


Рис. 3.11. Избыточность, реализуемая на уровне доступа сети: взаимное соединение устройств

Избыточность на уровне доступа сети

Глава 4. Применение принципов построения иерархических сетей на практике

Выполнять в рамках НИРС, дипломных, курсовых и лабораторных работ

Темы:

- Проектирование OSPF-сетей
- Проектирование IS-IS-сетей
- Проектирование EIGRP-сетей

'Проектирование OSPF-сетей

Литература

1. Ретана Альваро, Слайс Дон, Уайт Расс. Принципы проектирования корпоративных IP-сетей. : Пер. с англ. М.: Издательский дом «Вильямс», 2002. – 368 с. ISBN 5-8459-0248-7 (рус)