МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ (МИИТ)

Институт управления и информационных технологий

Кафедра «Вычислительные системы и сети»

Я.М. Голдовский

ПРОЕКТИРОВАНИЕ КАМПУСНЫХ СЕТЕЙ

Рекомендовано редакционно-издательским советом университета в качестве учебного пособия

для студентов, обучающихся по направлению «Информатика и вычислительная техника»

Москва – 2009

УДК 681.3
Г-60

Голдовский Я.М. Проектирование кампусных сетей: Учебное пособие.- М.: МИИТ, 2009. – 130 с.

В учебном пособии рассматриваются основные принципы проектирования кампусных сетей на примере компьютерных сетей, построенных на основе сетевого оборудования «Cisco». Рассмотрены назначение и структура кампусной сети предприятия, методы резервирования оборудования и кабельных линий, методы балансирования нагрузки в сетях Cisco. Приведены примеры современных технологий, обеспечивающих устойчивую работу сети. Учебное пособие предназначено для студентов, обучающихся по направлению «Информатика и вычислительная техника».

Рецензенты:

Профессор кафедры «Проектирование ВК» РГТУ им. Циолковского, к.т.н., В.В.Шилов

Профессор кафедры «Управление и информатика в технических системах» МИИТа, д.т.н. В.Г.Сидоренко

Содержание

1. Сетевая архитектура Cisco

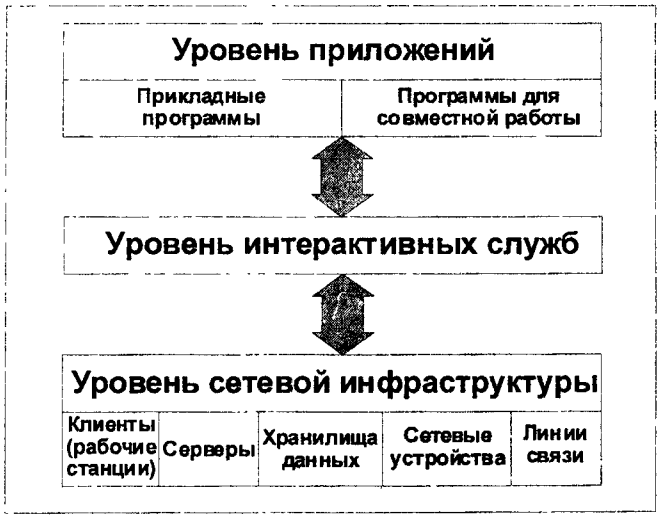
1.1. Типовая структура модульной сети предприятия

Построение сети предприятия – сложная задача. А всякую сложную задачу хочется разбить на несколько простых. В наибольшей степени этому желанию отвечает архитектура сети, состоящая из отдельных модулей, которые могут разрабатываться, до некоторой степени, независимо друг от друга. Кроме того, что каждый модуль проще, чем всю сеть целиком, модульная структура обладает еще несколькими важными достоинствами. Такая сеть сравнительно легко масштабируется добавлением еще одного модуля, а модернизация или переход на другое оборудование облегчается тем, что изменение одного модуля не затрагивает остальные.

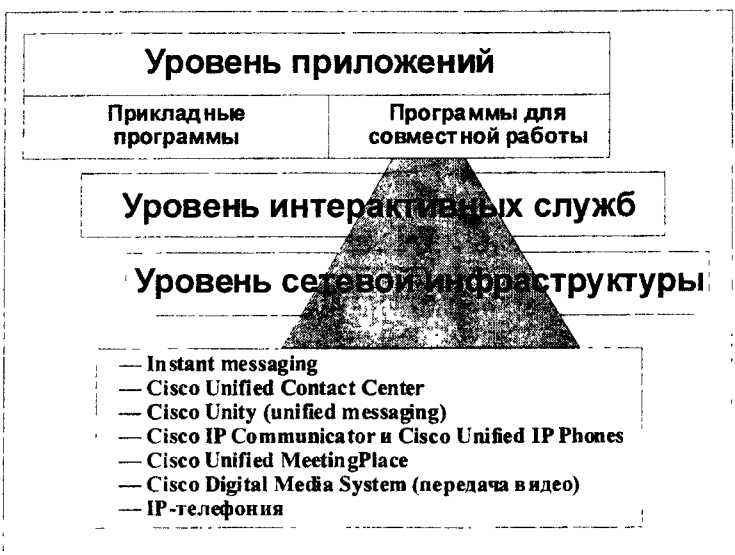
Типовая структура модульной сети предприятия предложена компанией Cisco systems и называется Cisco Service-Oriented Network Architecture (SONA).

В самом общем виде архитектура SONA состоит из трех уровней:

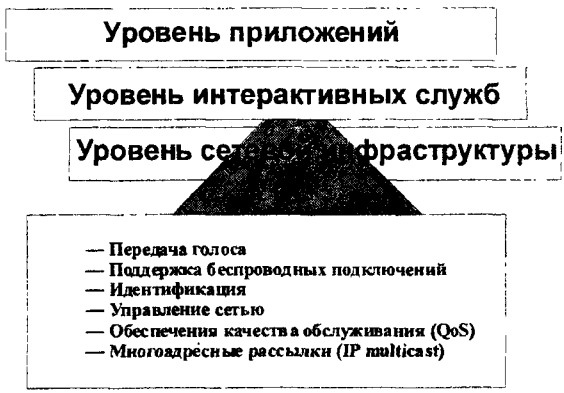
- Уровень приложений
- Уровень интерактивных служб
- Уровень сетевой инфраструктуры



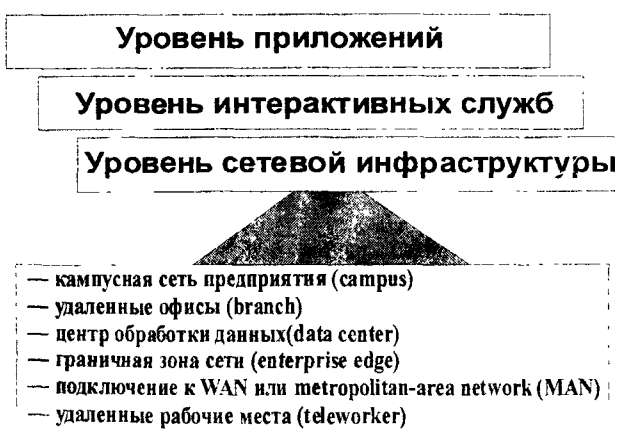
Уровень приложений (*Application layer*) состоит из прикладных программ (*business applications*) и программ, обеспечивающих совместную работу сотрудников (*collaboration applications*).



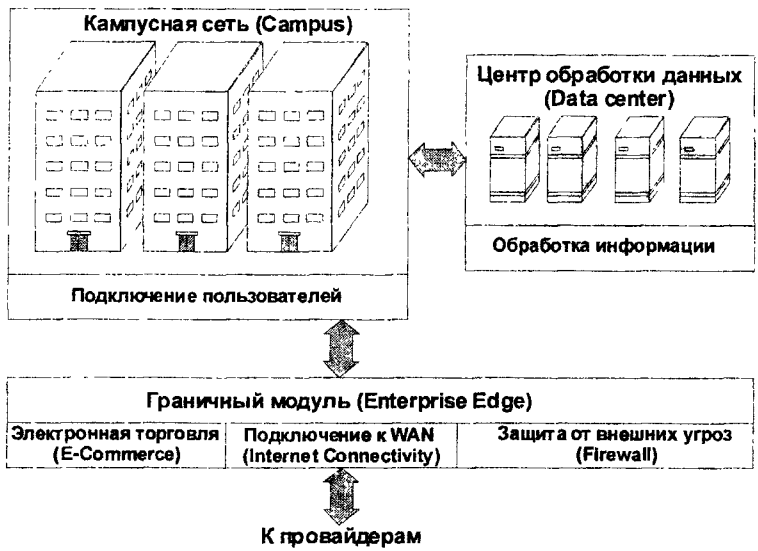
Уровень интерактивных служб (*Interactive Services layer*) служит связующим звеном между двумя другими. Его задача: обеспечить выполнение функций прикладного уровня на том оборудовании, которое составляет уровень сетевой инфраструктуры.



Уровень сетевой инфраструктуры (*Networked Infrastructure layer*) является основанием всей архитектуры SONA. Он с помощью линий связи и сетевых устройств соединяет в единую сеть все информационные ресурсы: серверы и рабочие станции. В общем случае, уровень сетевой инфраструктуры состоит из шести модулей:

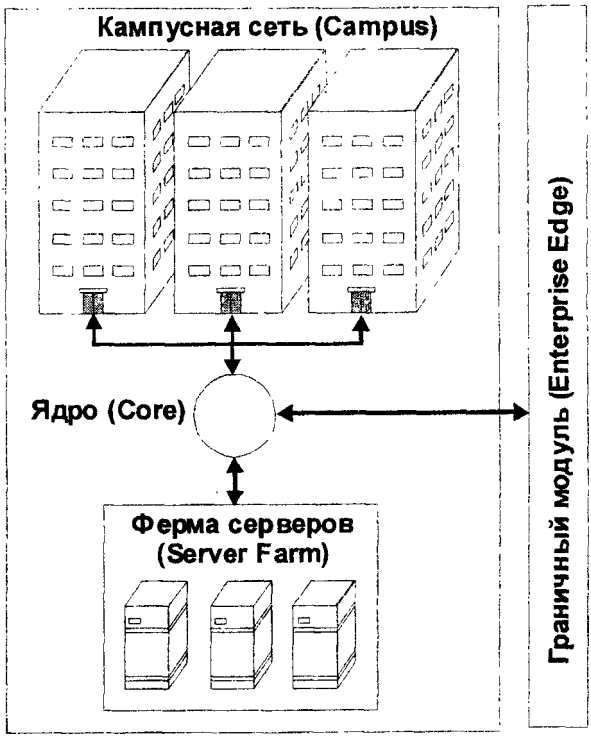


Каждый из модулей уровня сетевой инфраструктуры выполняет свою задачу, обеспечивая подключение рабочих станций, хранение и обработку данных, и подключение внешних связей через глобальные (WAN) или городские (MAN) сети.



Модульная архитектура позволяет гибко варьировать количество и состав модулей. Так, все модули, отвечающие за подключение к WAN, могут объединяться в один модуль Enterprise Edge.

Центр обработки данных может входить в состав кампусной сети в виде особого модуля – серверной фермы (server farm).



Как разделить сеть на модули?

Необходимо четко разграничить модули сети. При этом следует руководствоваться следующими простыми правилами:

Основные вычислительные ресурсы сети – серверы, обслуживающие всю компанию – объединяют в Центр обработки данных (Data center).

Все устройства, нужные для связи с удаленными офисами и другими абонентами за пределами основной территории, относят к граничному модулю (Enterprise Edge).

В кампусную сеть (Campus) включают все сетевые устройства на основной территории предприятия, кроме тех, которые входят в другие модули.

1.2. Функции и организация основных модулей

Рассмотрим подробнее функции и организацию каждого модуля.

Кампусная сеть

Архитектура модуля Cisco Enterprise Campus должна сочетать большое количество точек доступа, при умеренной их цене, высокопроизводительные технологии многоуровневой коммутации и большую пропускную способность, надежность и обеспечение целого ряда функций:

- резервирование оборудования и линий связи;
- автоматическое восстановление связи при сбое;
- поддержка многоадресных рассылок;
- обеспечение качества обслуживания (QoS), гарантирующего своевременную доставку пакетов, относящихся к передаче видео, аудио и других видов данных, чувствительных к задержке передачи и вариации времени задержки;
- защита от несанкционированного доступа, в том числе на уровне портов коммутатора.

Кампусная сеть, как правило, является основным, центральным модулем в сети предприятия, поэтому ее

организация подробнее рассматривается в следующей главе данного пособия.

Граничный модуль

Архитектура модуля Enterprise Edge должна обеспечивать подключение к службам передачи данных, голоса и видео, находящимся за пределами предприятия.

Для этого модуля первостепенное значение имеют защита от несанкционированного доступа и обеспечение качества обслуживания.

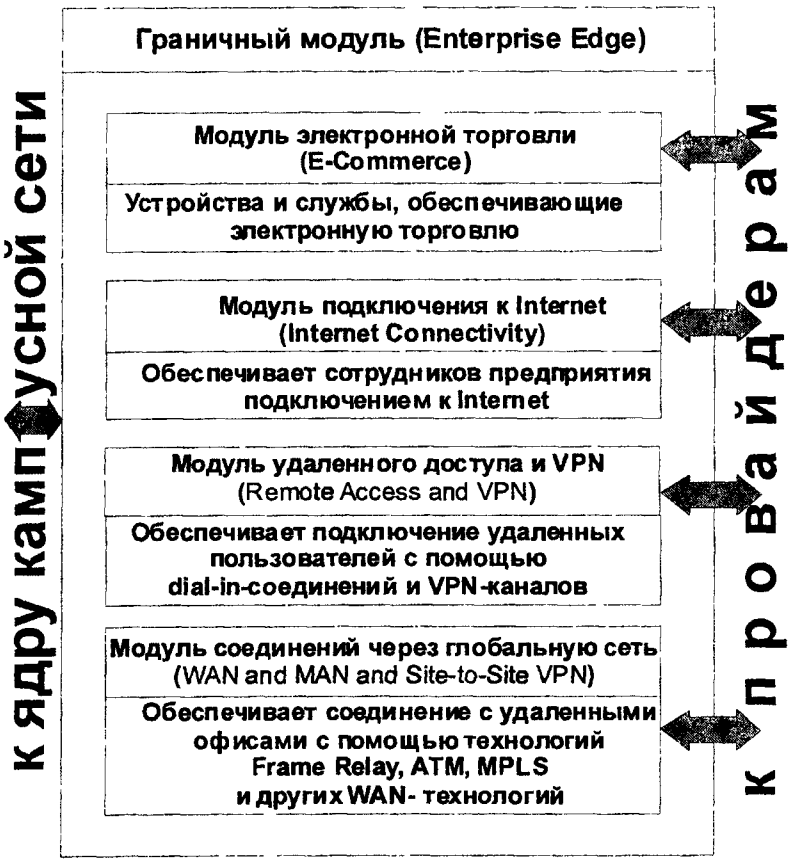
Задача модуля Enterprise Edge при обработке входящего трафика:

- собрать данные из Internet, каналов VPN, от филиалов предприятия, удаленных рабочих мест и многочисленных клиентов;
- проверить, не угрожают ли эти данные безопасности сети;
- направить этот трафик в кампусную сеть.

При обработке исходящего трафика модуль Enterprise Edge обеспечивает соединение абонента с соответствующей сетевой службой, скрывая при этом структуру сети от взгляда извне.

Некоторые виды трафика, такие как электронная торговля или доступ к web-серверу предприятия целесообразно обрабатывать непосредственно в граничном модуле, не пропуская этот трафик вглубь сети.

В общем случае, граничный модуль состоит из четырех модулей:



E-commerce Module

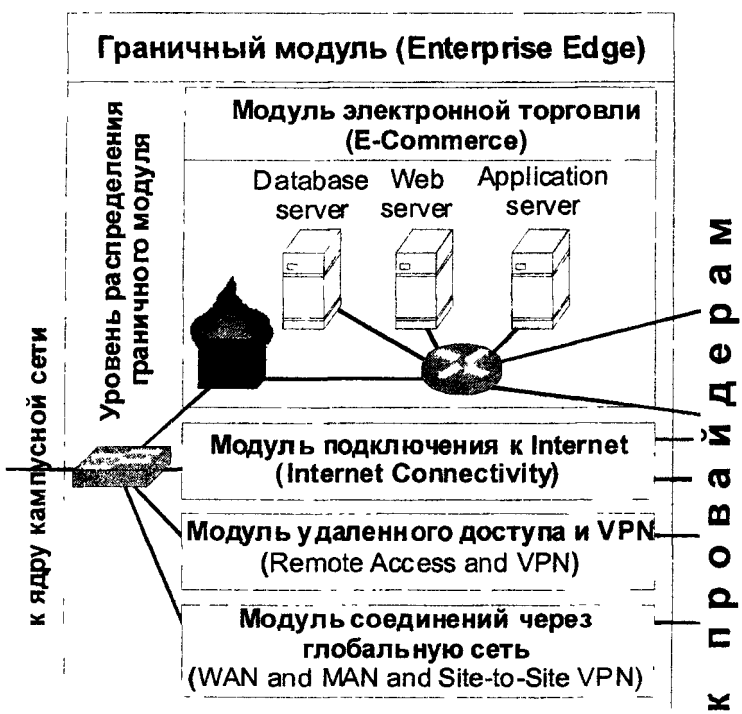
Назначение модуля электронной торговли понятно из названия. Для этого модуля характерно, что большая часть обращений к нему происходит извне сети предприятия.

Этим и объясняется расположение этого модуля внутри Enterprise Edge.

Для большей надежности, модуль электронной торговли подключен к Internet через нескольких провайдеров.

С «внутренней» стороны модуль электронной торговли подключается к коммутаторам уровня распределения модуля Enterprise Edge.

Типичный набор устройств модуля электронной торговли приведен на рисунке:



Internet Connectivity Module

Модуль подключения к Internet обеспечивает быстрый и безопасный доступ сотрудников предприятия к таким службам глобальной сети Internet, как HTTP, FTP, Simple Mail Transfer Protocol (SMTP), и DNS.

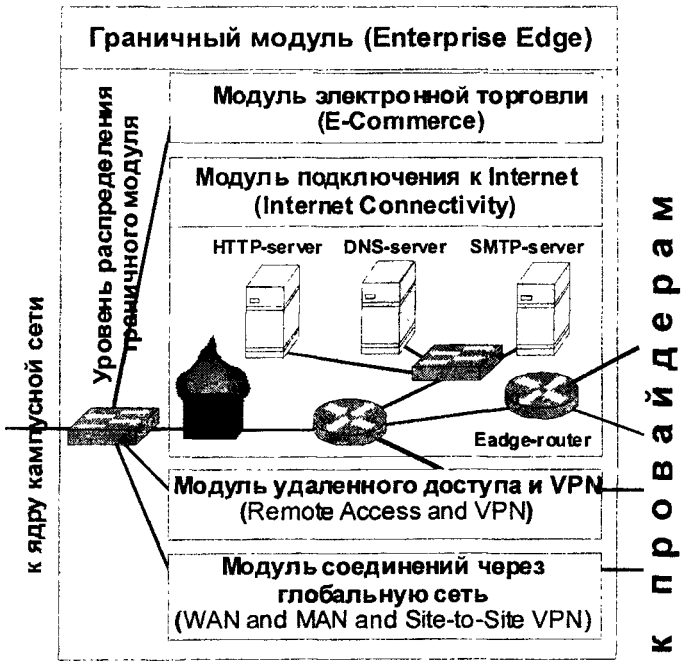
С другой стороны, для клиентов предприятия и других пользователей Internet этот модуль обеспечивает доступ к ресурсам предприятия, предназначенным для публичного доступа. Соответственно, в состав модуля подключения к Internet могут входить HTTP and FTP серверы.

Для модуля подключения к Internet характерно, что сеанс связи, как правило, инициируется изнутри корпорации.

Кроме того, этот же модуль принимает извне трафик от удаленных пользователей и передает его модулю удаленного доступа и VPN.

Для большей надежности, модуль Internet Connectivity Module подключен к Internet через нескольких провайдеров. С «внутренней» стороны модуль подключается к коммутаторам уровня распределения модуля Enterprise Edge.

Общая схема граничного модуля приведена на следующей странице.



Remote Access and VPN Module

Модуль удаленного доступа и VPN требуется если сеть предприятия предполагает использование VPN-каналов или dial-in-соединения для доступа в сеть предприятия извне.

Этот модуль служит для подключения входящего VPN-трафика и трафика dial-in-соединений, который поступает от модуля подключения к Internet.

Разумеется, пользователи не должны получать доступ к сети без аутентификации и авторизации. Поэтому

организация этого модуля должна быть тесно увязана с общей политикой безопасности.

WAN and MAN and Site-to-Site VPN Module

К этому модулю следует отнести все устройства, необходимые для поддержания постоянного соединения с удаленными офисами. Здесь же размещаются все устройства, необходимые для подключения по протоколам Frame Relay, ATM, MPLS и т.д.

Постоянные соединения с удаленными офисами обычно предполагают передачу смешанного содержимого: данных, голоса и видео. Соответственно, все используемое в этом модуле оборудование должно поддерживать технологии QoS.

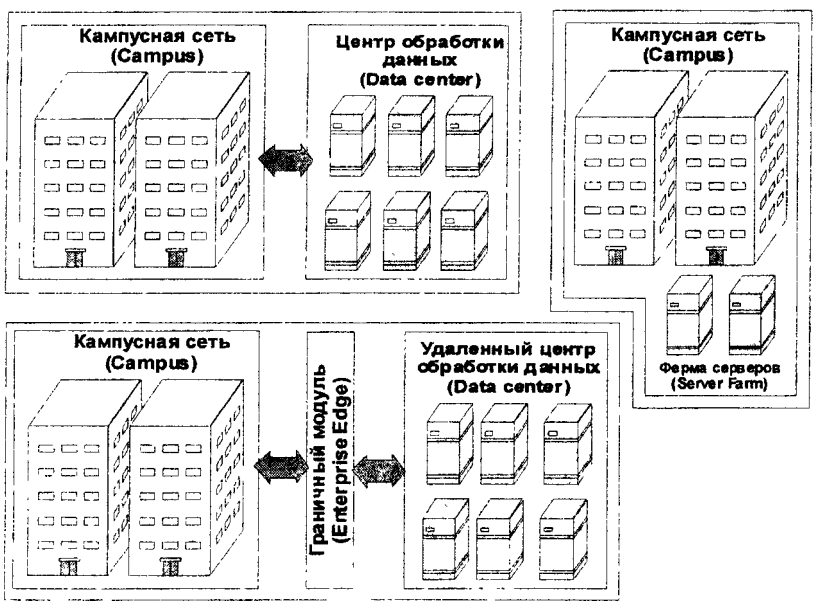
Центр обработки данных

Модуль обработки данных должен обеспечивать очень высокую скорость обслуживания клиентов и, в то же время, высокую надежность. С точки зрения организации сети, это обеспечивается избыточностью линий связи и сетевого оборудования, при этом обязательно надо использовать балансирование нагрузки. Тогда при нормальной работе избыточность и балансирование нагрузки обеспечивают высокую пропускную способность, а при сбоях – автоматическое восстановление соединения.

Центр обработки данных обычно содержит серверы внутренней электронной почты, Domain Name System (DNS), печати, приложений, файл-серверы и т.д..

Желательно подключать все серверы сразу к двум коммутаторам, а также иметь несколько подключений к ядру кампусной сети.

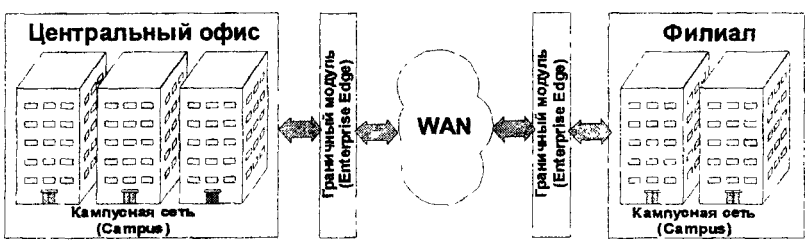
Конкретная организация центра обработки данных сильно зависит от его масштабов и расположения, и может принимать самые разные формы.



1.3. Функции кампусной сети предприятия

Центральным модулем в архитектуре сети предприятия является кампусная сеть. Этот модуль обеспечивает подключение к сети всех сотрудников на основной территории предприятия и может охватывать несколько близко расположенных зданий.

Если предприятие располагается на нескольких удаленных территориях, сети удаленных офисов строятся по тому же принципу, что и кампусная сеть.



Сетевые приложения, для обслуживания которых и строится кампусная сеть, можно разделить на четыре группы:

- Точка - точка (Peer-peer)
- Рабочая станция – Сервер рабочей группы (Client–local server)
- Рабочая станция – Корпоративный сервер (Client–Server Farm)
- Рабочая станция – Сервер граничного модуля (Client–Enterprise Edge server)

Каждая из этих групп имеет характерные особенности сетевого трафика и предъявляет особые требования к организации сети.

Приложения, требующие соединения точка-точка

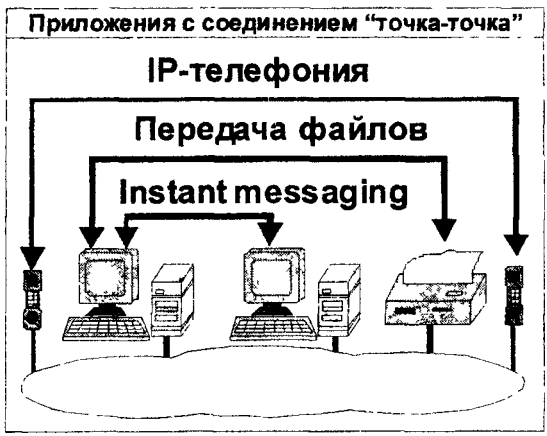
Это приложения, предполагающие соединение между двумя рабочими станциями. К ним, в частности, относятся следующие приложения:

- **Служба сообщений Instant messaging**: Соединение между рабочими станциями устанавливается при помощи соответствующего сервера, но затем обмен сообщениями можно считать процессом «точка-точка».
- **Соединение с помощью IP-телефонии**: Само соединение, опять же, устанавливается с помощью соответствующих серверов и служб, но разговор пользователей по IP-телефону можно считать процессом «точка-точка».
- **Передача файлов**: Хотя общие файлы обычно размещают на соответствующих серверах, некоторые приложения требуют передачи файла с одной рабочей станции на другую.

К этой же группе можно добавить и передачу данных при проведении **видеоконференций**. После настройки соединения с помощью соответствующих служб, дальнейшая передача данных от источника к

получателю может рассматриваться как процесс «точка-точка».

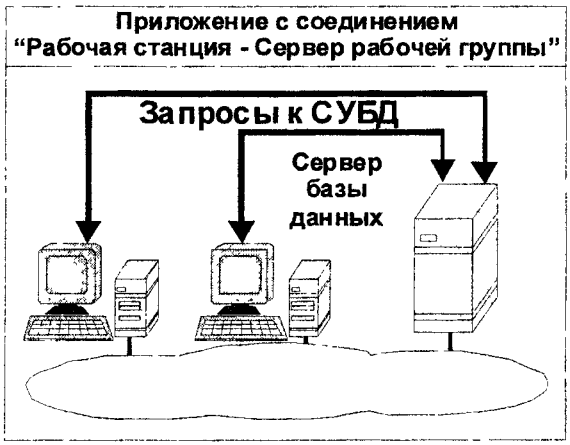
Отметим необходимость использования QoS для таких приложений как IP-телефония и видеоконференций.



Приложения, требующие соединения «Рабочая станция – Сервер рабочей группы» (Client–local server)

Это приложения, предполагающие соединение «клиент-сервер» в пределах одной рабочей группы (отдела).

Еще совсем недавно считалось, что в сетевом трафике такие соединения преобладают. Существовало даже «Правило 80/20», гласившее, что большая часть сетевого трафика (порядка 80%) составляют соединения в пределах рабочей группы.



Ориентация на подобные соединения предполагает максимальное упрощение связи именно в пределах рабочей группы, что обычно реализуется включением всех рабочих станций и серверов рабочей группы в одну виртуальную сеть (VLAN). А так как количество и расположение сотрудников одного отдела может быть весьма переменчиво, разумным решением представлялась такая организация сети, при которой в любой точке предприятия можно подключиться к любому VLAN.

В то же время, нагрузка на сетевые устройства и линии связи, соединяющие рабочие группы между собой и корпоративными серверами считалась не очень большой (порядка 20%), ну а в Internet, как считалось, серьезному

человеку обращаться надо раз в день – проверить почту и посмотреть курсы валют.

Приложения, требующие соединения «Рабочая станция – Корпоративный сервер» (Client– Server Farm)

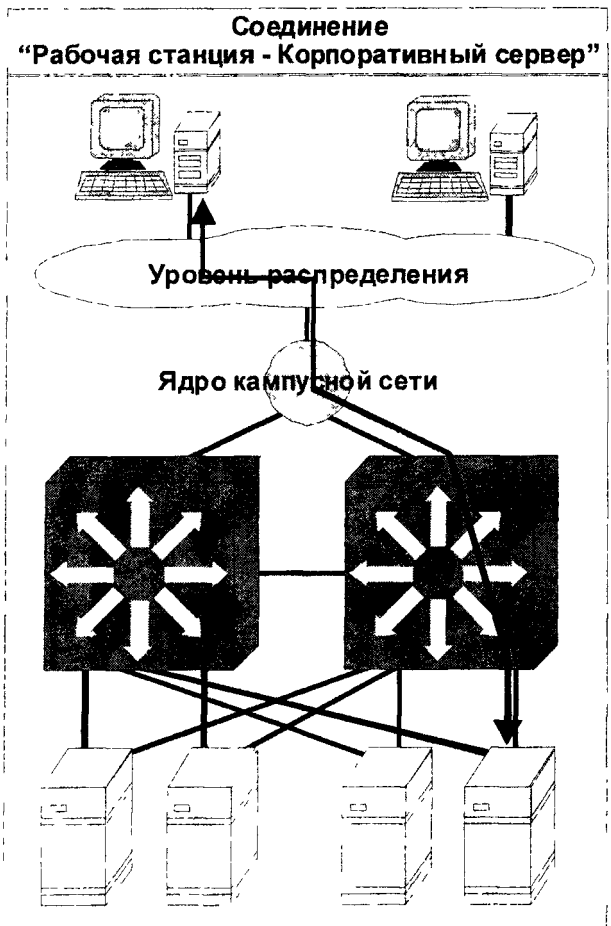
Совершенствование сетевых технологий привело к тому, что в настоящее время выгоднее не рассредоточивать многочисленные серверы по отделам, а собрать несколько мощных корпоративных серверов в одном месте – серверной ферме, где им обеспечено квалифицированное обслуживание, оперативное управление и быстрая связь с любым отделом предприятия.

Возникло даже новое «Правило 20/80», согласно которому лишь небольшая часть трафика (около 20%) приходится на соединения внутри отдела, тогда как большая часть запросов (около 80%) выходит за его пределы.

Примером приложений, требующих соединения «Рабочая станция – Корпоративный сервер», являются:

- корпоративный внутренний почтовый сервер;
- корпоративный файл-сервер;
- корпоративный сервер базы данных;
- Intranet-сервер.

Подобная концентрация вычислительной мощи предприятия в одном месте требует самого пристального внимания к вопросам безопасности и пропускной способности.

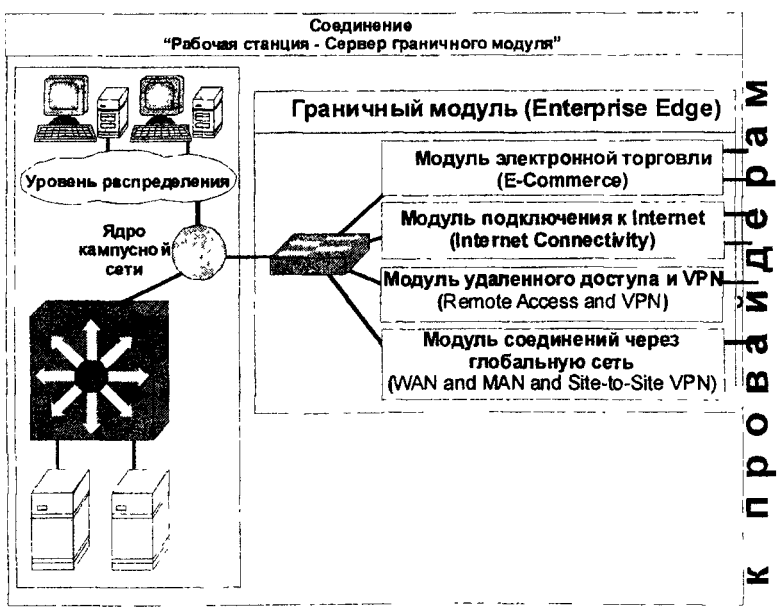


Как правило, серверы в серверной ферме подключается к ядру кампусной сети через несколько многоуровневых коммутаторов, при этом, серверы

подключаются, по возможности, сразу к двум коммутаторам линиями Gigabit Ethernet.

Приложения, требующие соединения «Рабочая станция – Сервер граничного модуля» (Client–Enterprise Edge server)

Практически каждое предприятие использует приложения, предусматривающие обмен данными с внешней средой – Internet, или другими глобальными сетями.



В качестве примера можно привести приложения, предназначенные для:

- электронной торговли;
- электронной почты;
- доступа к публичным web-серверам в Internet;
- связи с филиалами по VPN

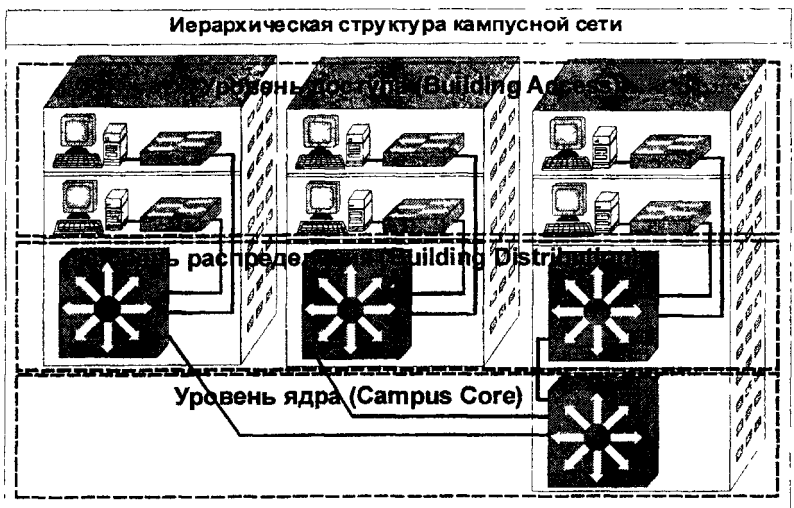
Растущая полезность доступа сотрудников предприятия к публичным web-серверам в Internet – характерная черта нашего времени. Возможность быстрого поиска нужной информации, консультации с коллегами, получение готовых форм документов и т.д. – значительно упрощает работу программиста, инженера или менеджера, повышая производительность их труда.

Традиционным требованием к подобным приложениям является защита от несанкционированного доступа.

Особенности организации кампусной сети предприятия

Иерархическая структура кампусной сети

Как правило, кампусную сеть можно разделить на три уровня:



Уровень доступа. Коммутаторы уровня доступа обеспечивают подключение конечных пользователей к сети.

Уровень распределения. Устройства уровня распределения соединяют коммутаторы уровня доступа в пределах здания с ядром сети

Уровень ядра. Ядро кампусной сети объединяет сети зданий в единую сеть и обеспечивает связь с серверной фермой и граничным модулем.

При разработке каждого уровня учитываются следующие параметры:

- Количество рабочих станций
- Использование ресурсоемких приложений – многоадресных трансляций, IP-телефонии, видеоконференций; необходимость поддержки QoS.
- Время восстановления после сбоя (Convergence time)
- Стоимость

Время восстановления после сбоя

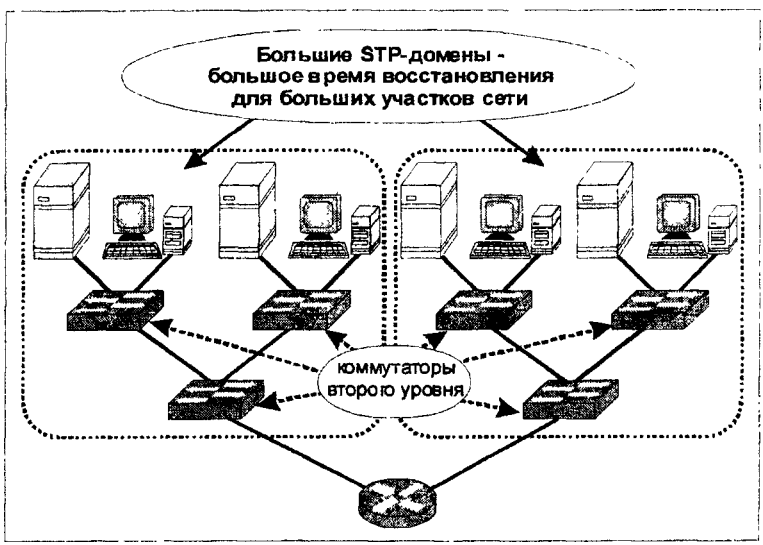
(Convergence time)

После сбоя в подаче электропитания, обрыве линии связи или отказе оборудования, сети, даже при наличии резервных линий связи и избыточности оборудования, требуется некоторой время, чтобы обнаружить отказ и перейти на резервные пути передачи данных.

Сети, использующие коммутацию второго (канального) уровня, для использования резервных линий связи нуждаются в специальном протоколе, предохраняющем от образования петель. Самым известным подобным протоколом является STP (Spanning Tree Protocol).

Время восстановления связи после сбоя для протокола STP определяется временем схождения (Convergence time) и составляет 30 – 50 секунд в

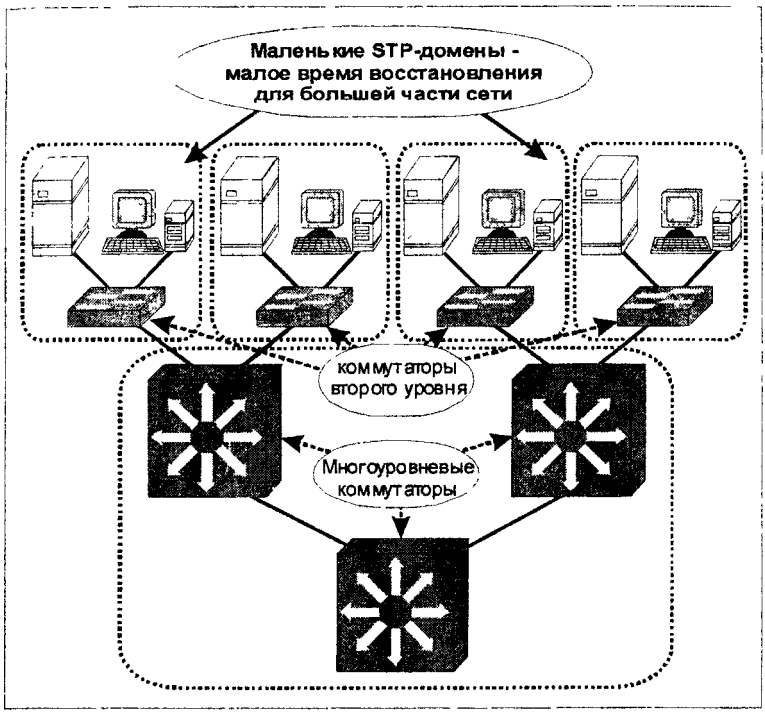
зависимости от размеров STP-домена. Потеря работоспособности всей сети на минуту считается нежелательной. В то же время, современные протоколы маршрутизации, работающие на третьем (сетевом) уровне, обеспечивают переход на резервный маршрут в течение нескольких секунд.



К тому же, современные протоколы маршрутизации, такие как Enhanced Interior Gateway Routing Protocol (EIGRP) или Open Shortest Path First (OSPF), не только быстро переходят на резервный маршрут, но и эффективно балансируют нагрузку по нескольким маршрутам, повышая пропускную способность сети.

Чтобы уменьшить время восстановления для большей части сети, а заодно ограничить

широковещательный трафик, желательно использовать, по возможности, коммутацию третьего уровня.



Рассмотрим подробнее уровни кампусной сети.

Уровень доступа

(Building Access Layer)

Основная задача уровня доступа – предоставлять пользователям доступ ко всем ресурсам сети. Необходимая при этом аутентификация пользователей

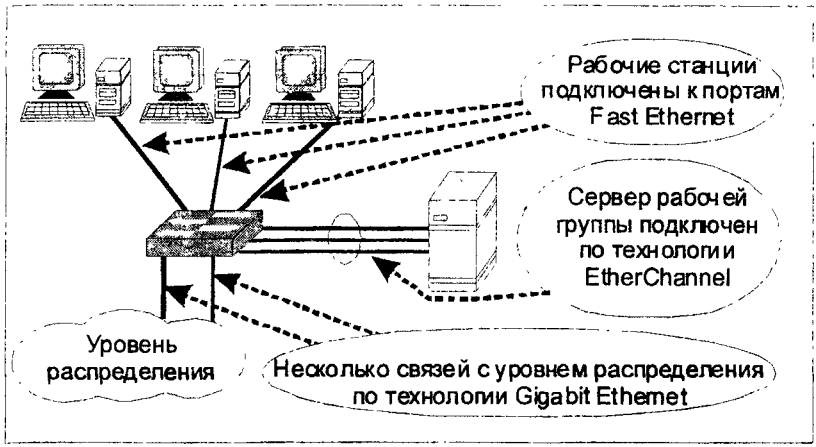
может обеспечиваться путем проверки соответствия их логических или физических адресов. Если в качестве сетевых устройств уровня доступа используются коммутаторы второго уровня, проверка физических адресов может быть организована настройкой portsecurity.

Сейчас, когда концентраторы уже почти не рассматриваются как современные сетевые устройства, уровень доступа кампусной сети строится из коммутаторов 2-го уровня или многоуровневых коммутаторов.

Большинство современных коммутаторов Cisco имеют несколько десятков портов Ethernet/Fast Ethernet для подключения рабочих станций и несколько (обычно 1-2) портов Gigabit Ethernet для связи с уровнем распределения. Последнее желательно как для резервирования, так и для балансирования нагрузки.

Расчет пропускной способности обычно проводится достаточно приближенно: считается, что если рабочие станции подключены к коммутатору по технологии Fast Ethernet (100 Мбит/с), то связь с коммутатором уровня распределения должна осуществляться по технологии Gigabit Ethernet (100 Мбит/с).

Если для подключаемого устройства предполагается интенсивный трафик, несколько линий Fast Ethernet могут объединяться в EtherChannel.



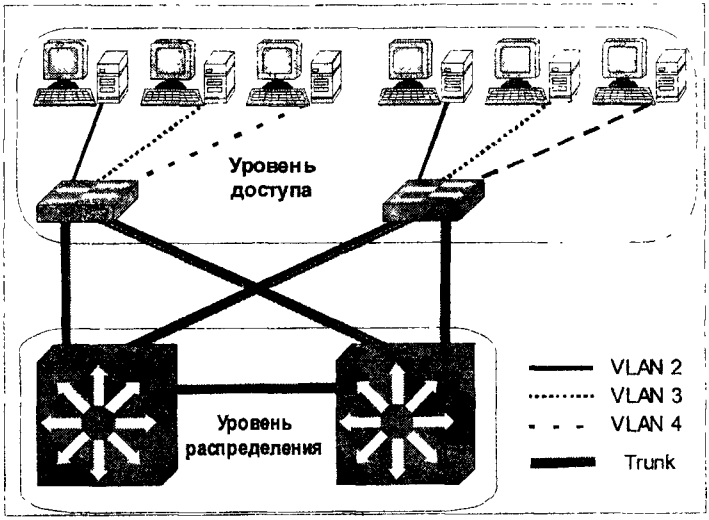
Если предполагается использование IP-телефонии, видеоконференций и других ресурсоемких сервисов, необходимо выбирать модель коммутатора, обеспечивающую QoS.

Использование коммутаторов второго уровня

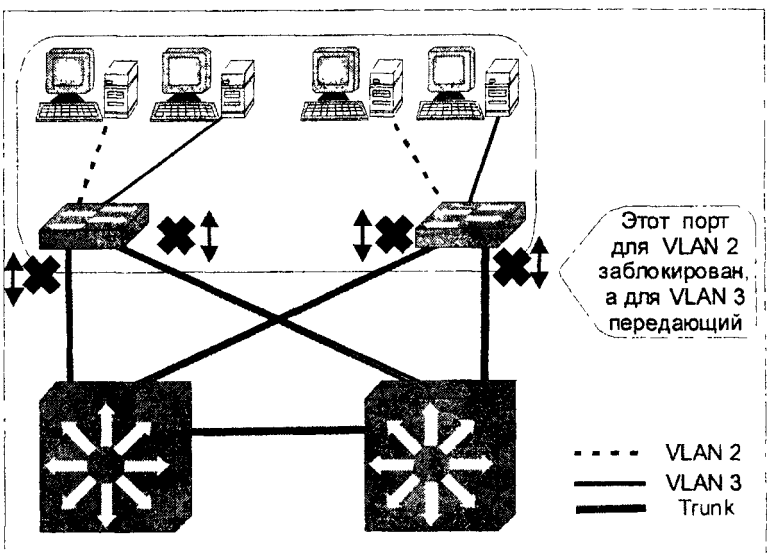
Любой современный коммутатор Cisco позволяет организовать несколько виртуальных сетей – VLAN.

Изображенная сеть позволяет подключиться к любому VLAN в любой точке здания. Каждый VLAN является отдельным STP доменом.

Наличие у каждого коммутатора нескольких связей с уровнем распределения весьма желательно для повышения отказоустойчивости, но делает необходимым

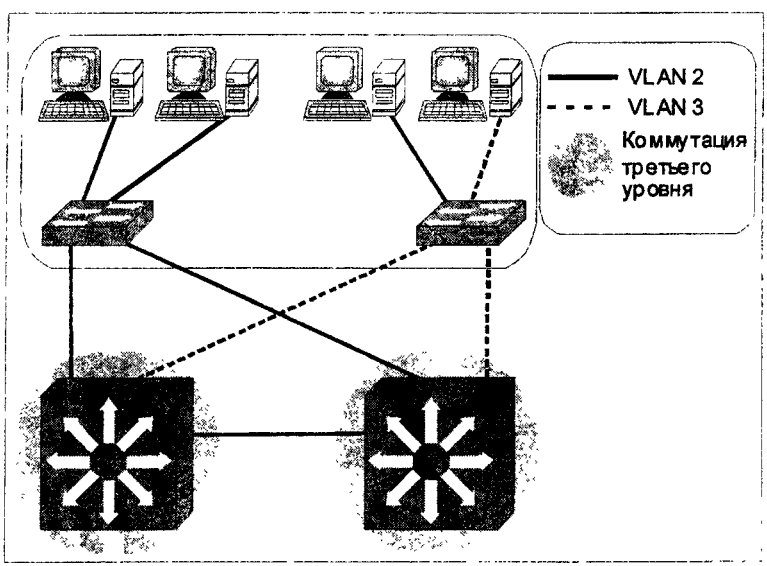


использование протокола STP для предотвращения образования петель путем блокирования резервных связей.



Чтобы обеспечить балансирование нагрузки необходимо так настроить STP, чтобы основная линия связи одних VLAN, была бы резервной для других.

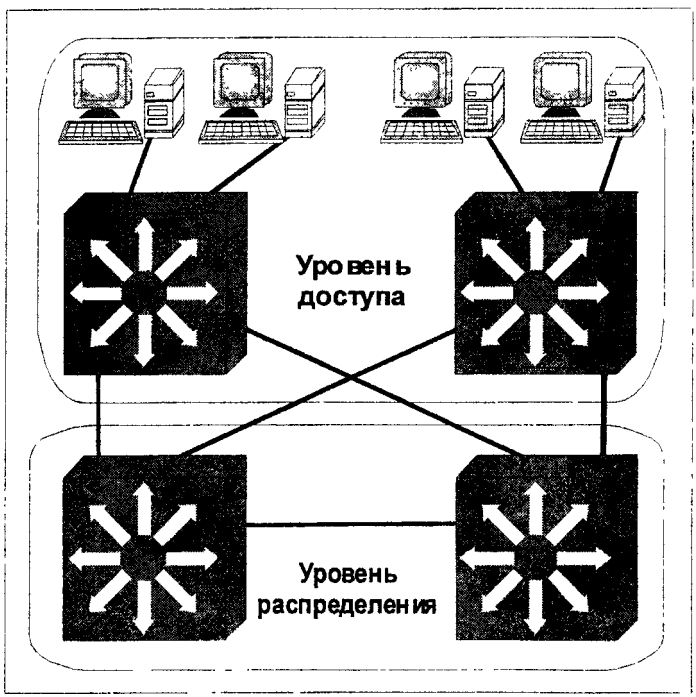
Показанные выше примеры обладают одним недостатком – необходимостью использования протокола STP для связей между уровнями доступа и распределения. Как уже говорилось, это нежелательно. Чтобы улучшить балансировку нагрузки и уменьшить время схождения, рекомендуется, по возможности, придерживаться правила «Один коммутатор – Один VLAN».



Такой подход может потребовать несколько большего количества коммутаторов уровня доступа, зато позволяет использовать вместо STP протоколы маршрутизации, улучшая время схождения и балансирование нагрузки.

Использование многоуровневых коммутаторов

Хотя самым распространенным решением, на сегодняшний день, является использование на уровне доступа кампусной сети коммутаторов второго уровня, при проектировании сети желательно рассмотреть и возможность построения уровня доступа на основе многоуровневых коммутаторов.



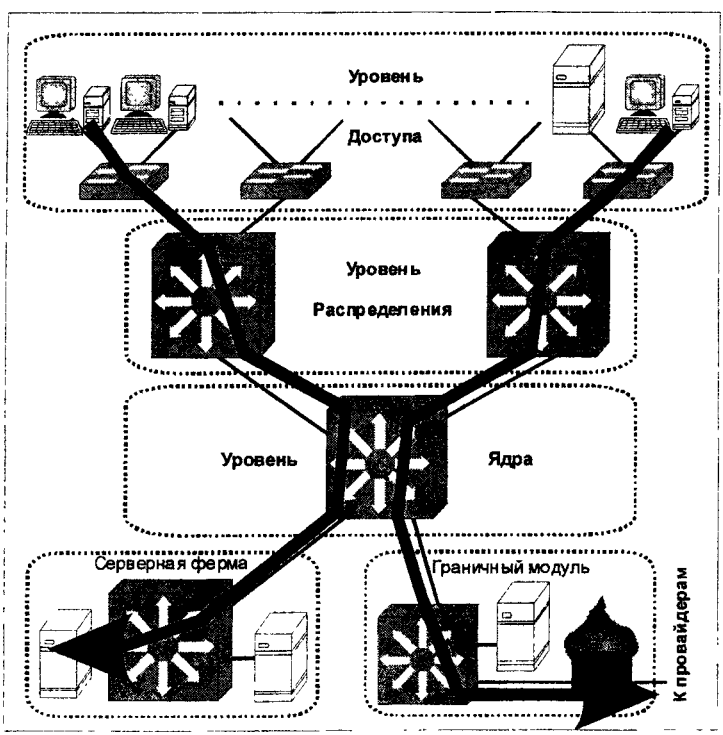
Это обеспечивает локализацию широковещательного трафика и использование на уровне доступа эффективных методов аутентификации пользователей и фильтрации пакетов, а также мощных средств маршрутизации и

обеспечения QoS, характерных для многоуровневых коммутаторов.

Уровень распределения
(Building Distribution Layer)

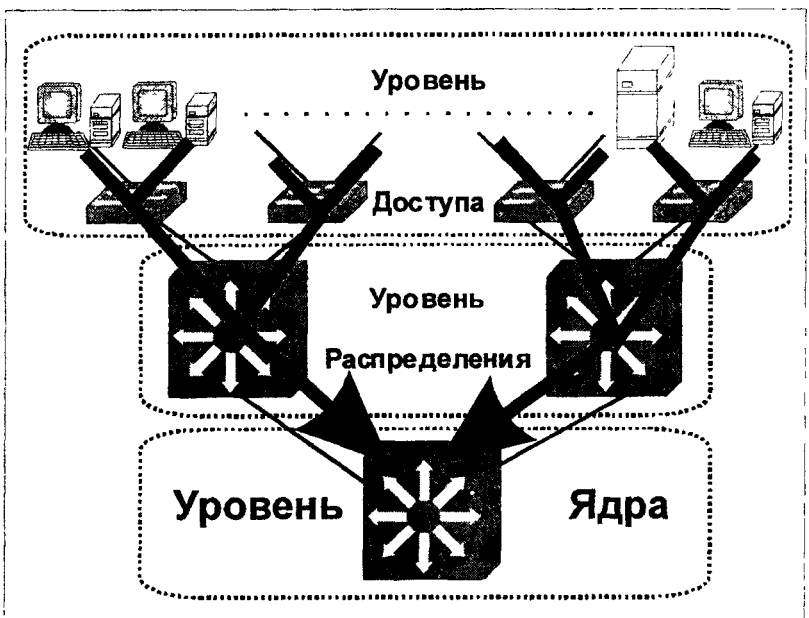
Находясь между уровнем доступа и ядром, уровень распределения кампусной сети осуществляет связь между ними, обеспечивая требуемую пропускную способность и принятую администратором политику.

Рассмотрим характерные особенности уровня распределения:



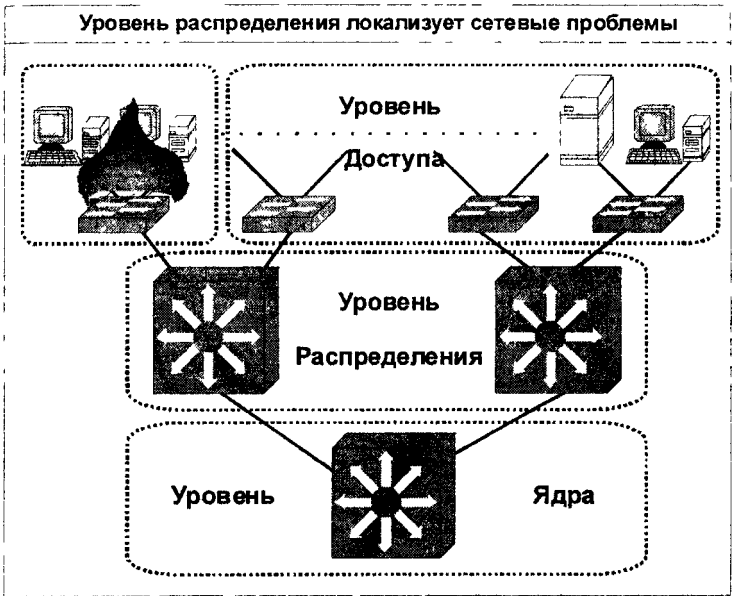
Так как уровень распределения обеспечивает доступ пользователей к ресурсам, подключенным к ядру сети, он не должен быть «узким местом».

Уровень распределения суммирует трафик от многочисленных устройств уровня доступа и передает его на высокоскоростные линии уровня ядра.

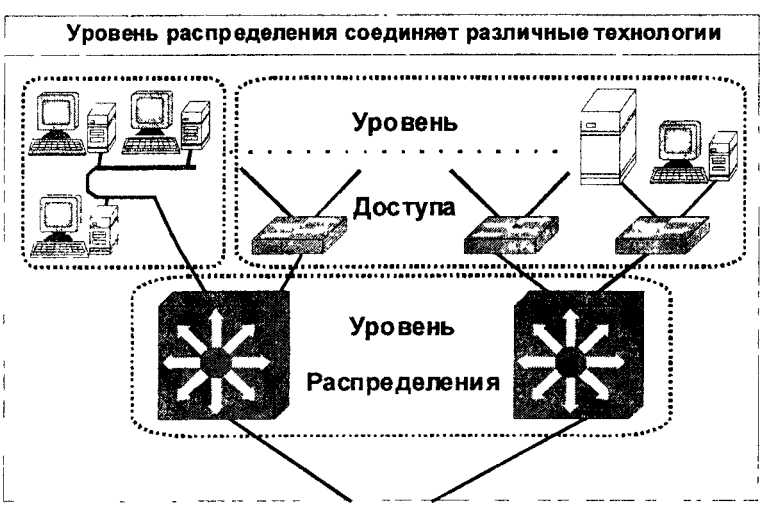


Это требует использовать для связи «Уровень распределения – Уровень ядра» более скоростных линий, чем для связи «Уровень распределения – Уровень доступа».

Уровень распределения локализует возникающие в сети проблемы, такие как, например, broadcast storm, не позволяя им захватить всю сеть.

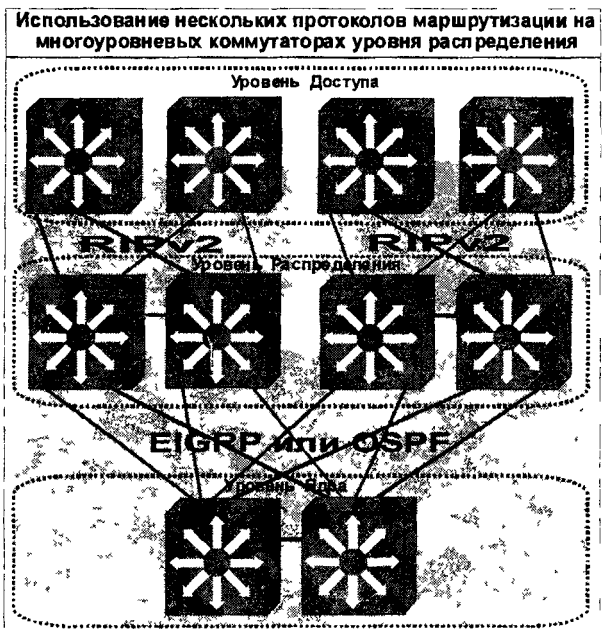


Если уровень доступа представлен различными технологиями, стыковка между ними выполняется на уровне распределения.



При необходимости обеспечения в сети QoS, коммутаторы уровня распределения должны поддерживать этот сервис.

Если уровень доступа соединяется с уровнем распределения транковыми линиями, на устройства уровня распределения ложится задача маршрутизации между VLAN.



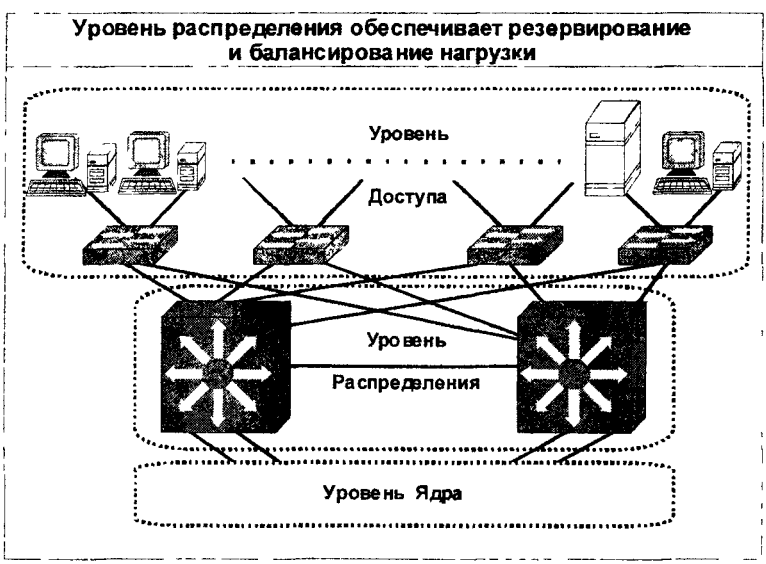
Если уровень доступа подключен к уровню распределения не транковыми, а маршрутизируемыми линиями, то в качестве протокола маршрутизации часто используют RIPv2, так как он не требователен к аппаратным ресурсам и не отвлекает их от более

напряженной работы на стыке с уровнем ядра, где применяются более мощные и ресурсоемкие протоколы.

Иногда, в этой ситуации, вместо RIP используют статические маршруты.

На уровне распределения используются, как правило, многоуровневые коммутаторы, обеспечивающие функции коммутации третьего уровня.

Соответственно, на уровне распределения выполняются все функции обработки пакетов – маршрутизация и фильтрация. Устройства уровня распределения могут эффективно суммировать маршруты от ядра к уровню доступа.



Уровень распределения обеспечивает резервирование соединений как с уровнем доступа, так и с

уровнем ядра. Наличие резервных связей обеспечивает, также, балансирование нагрузки.

Обеспечение сетевой политики

Как уже говорилось выше, одной из важнейших функций уровня распределения является обеспечение сетевой политики, проводимой администратором сети. Исходя из интересов защиты сети от несанкционированного доступа и обеспечения высокой пропускной способности для высокоприоритетных приложений, администратор сети определяет возможность определенных пользователей и приложений получать доступ к тем или иным участкам сети.

На уровне распределения основными инструментами обеспечения сетевой политики являются:

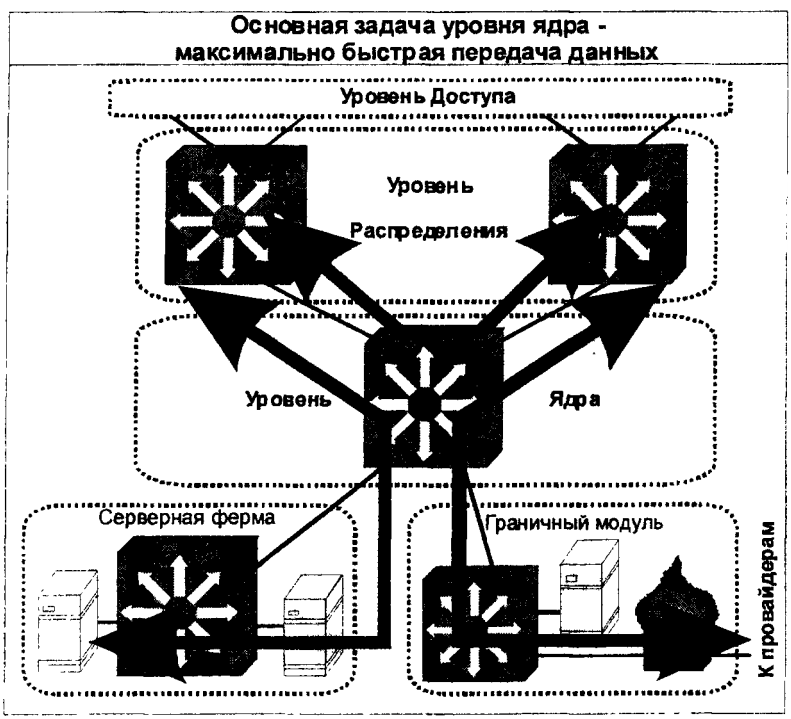
- Списки доступа (ACL) – позволяют фильтровать трафик на основе IP-адресов и номеров портов. Позволяют ограничить не только доступ к определенным ресурсам, но и использование определенных протоколов, например, для сокрытия структуры сети.
- Использование статических маршрутов и маршрутов по умолчанию – это позволяет избежать передачи по сети маршрутной информации и, следовательно, способствует сокрытию структуры сети.
- Настройка сервиса Quality of Service (QoS) –

определяет приоритетные приложения, обеспечивая их бесперебойную работу.

Уровень Ядра

(Core Layer)

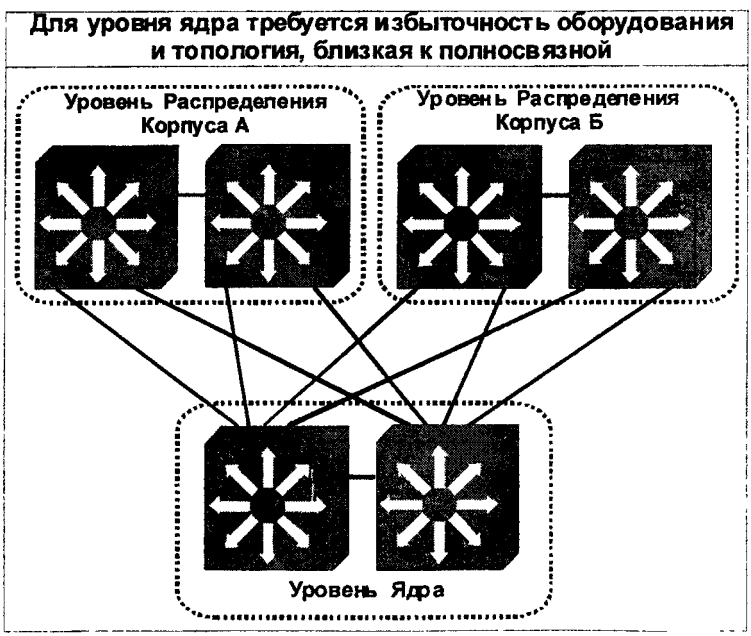
Основная задача уровня ядра – передавать пакеты между узлами уровня распределения и предоставлять доступ к серверной ферме и граничному модулю.



Ядро аккумулирует значительную часть трафика (порядка 80%) сети и, следовательно, должно обладать высокой пропускной способностью.

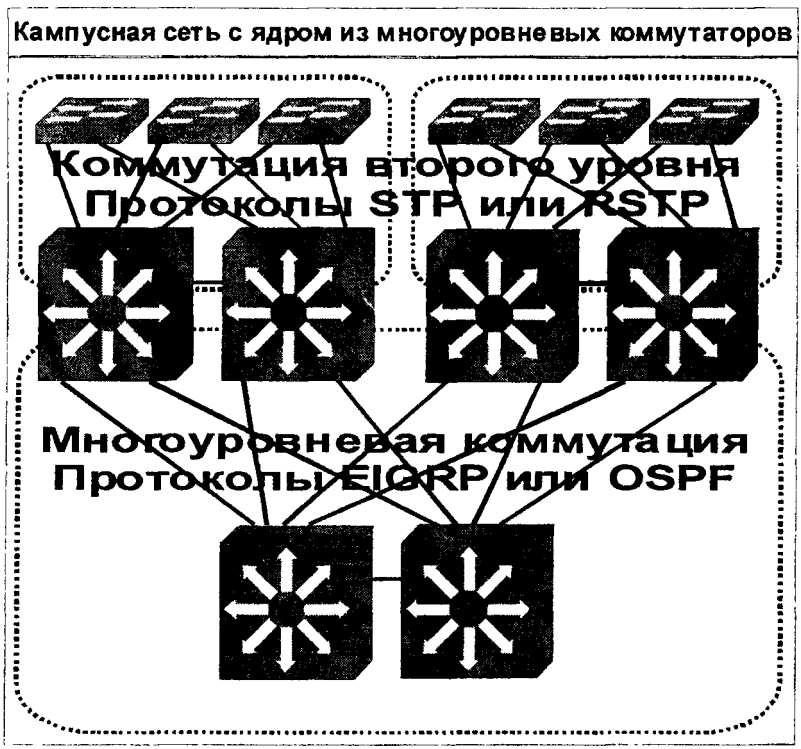
Выход из строя ядра кампусной приведет к потере большей части функциональных возможностей сети. Поэтому при построении уровня ядра важнейшими правилами являются:

- Избыточность сетевого оборудования.
- Полносвязная топология или близкая к ней.
- Использование современных протоколов маршрутизации – EIGRP или OSPF, обеспечивающих эффективное балансирование нагрузки и быстрое переключение на запасной маршрут.



В качестве сетевых устройств уровня ядра рекомендуется применять многоуровневые коммутаторы с высокоскоростными портами – Gigabit Ethernet или 10

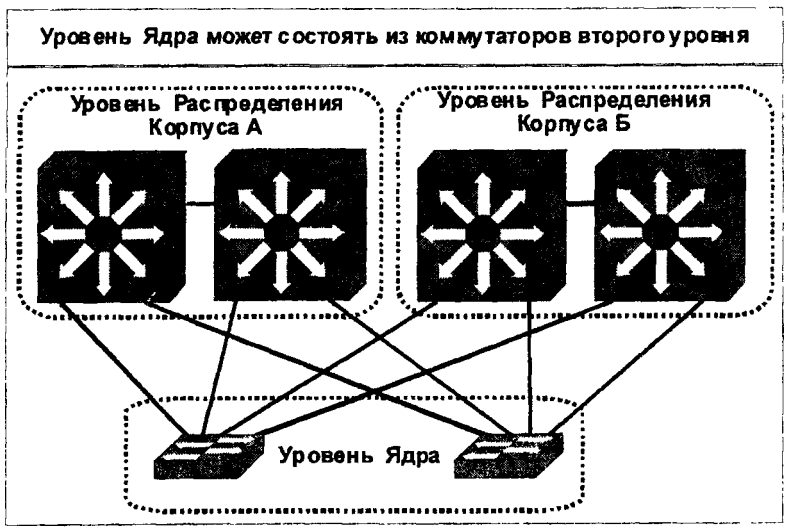
Gigabit Ethernet, обеспечивающие функции коммутации второго и третьего уровня и поддерживающие современные протоколы маршрутизации, и механизмы обеспечения QoS.



Обработка пакетов на уровне ядра должна, по возможности, сводится к их коммутации. Длительные операции, связанные с использованием списков доступа и т.д., должны выполняться на уровне распределения.

Так как большая часть операций, связанных с обеспечением политики безопасности сети реализуются на

уровне распределения, на уровне ядра кампусной сети допустимо применение более дешевых коммутаторов второго уровня.

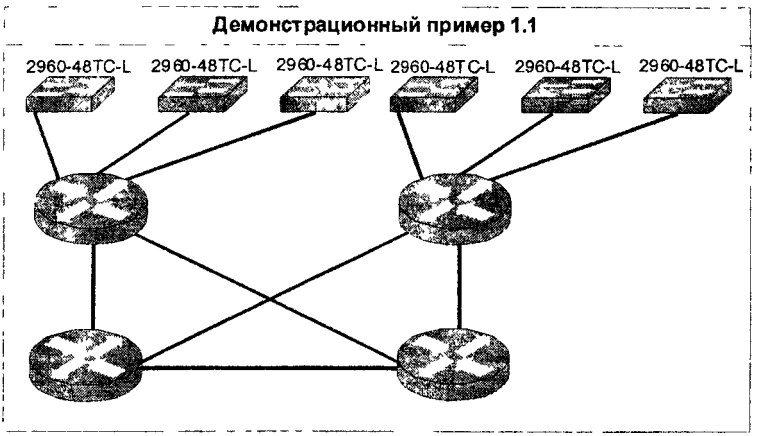


1.5. Примеры и упражнения

Пример 1.1

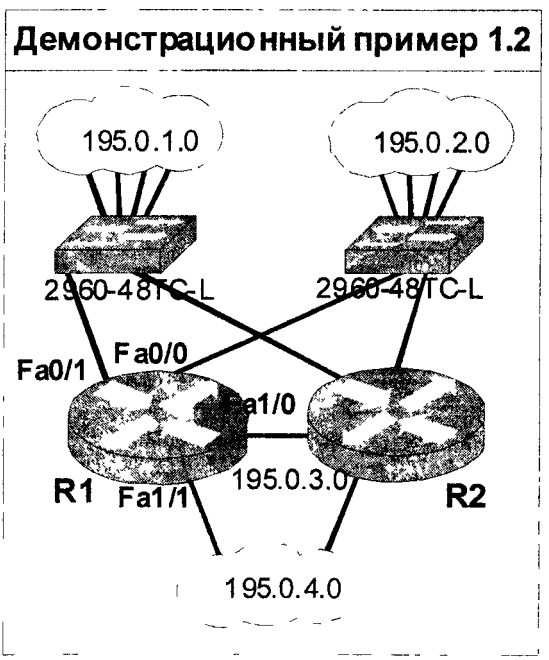
Использование маршрутизаторов при построении кампусной сети

Из примера (рис. на следующей странице) , сетевое оборудование Cisco позволяет построить кампусную сеть и с использованием традиционных маршрутизаторов. В качестве недостатка подобного подхода отметим характернсе для маршрутизаторов небольшое количество портов.



Пример 1.2

Настройка статического маршрута на уровне распределения



```
R1>en
R1#conf t
R1(config)#ip route 195.0.1.0 255.255.255.0 fa0/1
R1(config)#ip route 195.0.2.0 255.255.255.0 fa0/0
R1(config)#ip route 195.0.3.0 255.255.255.0 fa1/0
R1(config)#ip route 195.0.2.0 255.255.255.0 fa0/1
R1(config)#exit
```

Задания

Задание 1.1.

Напишите, зачем, на Ваш взгляд, нужен уровень распределения кампусной сети?

Задание 1.2.

В некоторой кампусной сети можно в любом месте любого здания подключиться к любому VLAN. Перечислите достоинства и недостатки такого решения.

2. Проектирование сети предприятия

2.1. Составление требований к сети и проектирование уровня доступа

Требования, предъявляемые к сети предприятия

Нет двух одинаковых предприятий, по этому каждая организация предъявляет свои требования к проектируемой сети. Тем не менее, можно представить себе некоторый набор обязательных требований, обычно предъявляемых к сети предприятия:

- Возможность подключения к сети по технологии Ethernet на каждом рабочем месте.
- Поддержка стека протоколов TCP/IP, и, частности, протокола сетевого уровня IP.
- Подключение к глобальным сетям и сетям, в т.ч. Internet.
- Возможность подключения локальных сетей, реализующих различные технологии.
- Возможность подключения корпоративных серверов, обеспечивающих обработку электронной почты, доступ к web-ресурсам и трансляцию мультимедийной информации по протоколам многоадресной рассылки.
- Добавление и перемещение рабочих станций по принципу «plug-and-play».
- Отсутствие единичных точек сбоя.

- Увеличение, при необходимости, пропускной способности отдельных участков сети без замены сетевого оборудования.
- Обеспечение расширяемости и масштабируемости сети.

При проектировании конкретной сети внимательно рассмотрите каждый пункт этого примерного списка. Изменяйте и добавляйте пункты под Ваши требования!

Для удобства разобьем большую задачу проектирования сети предприятия на несколько менее сложных. Для этого последовательно рассмотрим три иерархических уровня сети предприятия: уровень доступа, уровень распределения и уровень ядра системы.

Проектирование уровня доступа

Уровень доступа, в полном соответствии с названием, обеспечивает доступ пользователей к сети и включает набор коммутаторов, к которым непосредственно подключаются рабочие станции и горизонтальную кабельную систему, с помощью которой это подключение выполняется.

Проектируя уровень доступа, разработчик должен ответить на вопросы:

1. Сколько рабочих станций надо подключить и как они

распределяются по помещениям?

2. Как обеспечить физическое подключение рабочих станций соответствующей кабельной системой?
3. Как разбить сеть на подсети?
4. Какие модели коммутаторов использовать в качестве коммутаторов уровня доступа?

Сколько рабочих станций надо подключить?

Количество рабочих станций должно обеспечивать доступ к сети всем сотрудникам предприятия, кому это необходимо. Но это еще не все! На многих предприятиях существуют учебные классы и конференц-залы, а некоторые рабочие места должны оборудоваться несколькими точками доступа к сети. Кроме того, необходимо создать запас «на вырост», обеспечивая расширяемость сети.

Для конференц-залов часто удобно использовать беспроводные технологии: 1-2 точки доступа Wi-Fi обеспечат приемлемое качество подключения к сети участникам конференции при их свободном расположении в зале и вокруг него. Для учебных классов более удобным представляется подключение по технологии Ethernet.

На этом этапе разработчику нужно составить список всех рабочих мест с размещением их по помещениям предприятия и рассмотреть перспективы увеличения их числа.

Не существует четких ответов, сколько точек доступа надо взять «про запас». В каждом конкретном случае этот вопрос необходимо решать при участии руководства предприятия и его сотрудников, отвечающих за эксплуатацию компьютерной сети.

Как обеспечить физическое подключение рабочих станций соответствующей кабельной системой?

В настоящее время, при строительстве и ремонте офисных зданий, как правило, решается и вопрос прокладки кабельных линий в соответствии со стандартами структурированных кабельных систем (СКС), позволяющее подключать любое современное сетевое оборудование, в том числе и рассматриваемое нами оборудование фирмы Cisco. Поэтому, если предприятие расположено в современном или недавно отремонтированном здании, вынесенный в заголовок вопрос решается легко – кабельная система уже есть. Тем не менее, очень коротко рассмотрим некоторые аспекты современных СКС.

Создание СКС требует значительных первоначальных затрат и предполагает большую степень избыточности, тем не менее, нужно убедить себя (и, что еще труднее, руководство), что построение СКС необходимо. При проектировании сети предприятия, насчитывающей, как правило, не одну тысячу точек доступа, совершенно недопустима разводка кабеля случайным образом, с

хаотическим переплетением проводов и установкой оборудования по принципу «куда дотянется». Единственным современным и грамотным решением следует признать организацию полноценной структурированной кабельной сети (СКС) предприятия, удовлетворяющей принятым стандартам.

Россия, являясь членом Международной организации стандартизации (ISO), руководствуется требованиями международного стандарта ISO/IEC 11801.

Стандарт ISO/IEC 11801 подразделяет структурированную кабельную систему на три подсистемы:

- магистральную подсистему комплекса зданий;
- магистральную подсистему здания;
- горизонтальную подсистему.

Рекомендуемые стандартами рамки СКС составляют 50 – 50000 пользователей, 1000000 $м^2$ офисной площади. При необходимости, СКС может быть построена на одном этаже или в части здания, занимаемой отдельным арендатором.

Положения стандартов подробно изложены в соответствующих документах и легко доступны, в том числе, через глобальную сеть Internet, например, по адресу http://www.ecolan.ru/imp_info/standarts/review/iso/

Стандарт выделяет восемь функциональных элементов СКС:

- Распределительный пункт комплекса (зданий) (РП комплекса)
- Магистраль комплекса (МК)
- Распределительный пункт здания (РП здания)
- Магистраль здания (МЗ)
- Распределительный пункт этажа (РП этажа)
- Горизонтальные кабели (ГК)
- Точка перехода (ТП)
- Телекоммуникационный разъем (ТР)

СКС, построенная по стандарту ISO/IEC 11801 обладает следующими свойствами:

- СКС обеспечивает работу нескольких поколений компьютерных сетей;
- интерфейсы СКС позволяют подключать любое оборудование локальных сетей и речевых приложений;
- СКС реализует большой диапазон скорости передачи данных от 100 Кбит/сек речевых приложений до 10 Гбит/сек информационных приложений;
- администрирование СКС сокращает трудозатраты обслуживания локальной сети благодаря простоте эксплуатации;
- компьютерная сеть допускает одновременное

использование разнотипных сетевых протоколов;

- стандартизация плюс конкуренция рынка СКС обеспечивают снижение цен комплектующих.

Какие модели коммутаторов использовать в качестве коммутаторов уровня доступа?

В принципе, любой коммутатор можно использовать в качестве коммутатора уровня доступа. Тем не менее, существует множество нюансов, делающих ту или иную модель наиболее предпочтительной для этой роли.

В настоящее время, Cisco Systems рекомендует использовать в качестве коммутаторов уровня доступа (wiring closet) для сети предприятия несколько семейств коммутаторов.

- Cisco Catalyst 2960
- Cisco Catalyst 3560 и3560-E
- Cisco Catalyst 3750 и 3750-E
- Cisco Catalyst 4500 и 4500-E
- Cisco Catalyst 6500 и 6500-E

Рассмотрим эти семейства коммутаторов подробнее.

Данное пособие содержит лишь краткий обзор и не является подробным справочником по сетевому оборудованию Cisco Systems. С полными перечнями моделей оборудования и их описания можно ознакомиться на сайте www.cisco.com.

Cisco Catalyst 2960 Series Switches

Серия коммутаторов, имеющих 8, 24 или 48 портов Ethernet/Fast Ethernet, для подключения рабочих станций и 1, 2 или 4 порта Ethernet/Fast Ethernet/Gigabit Ethernet для связи с уровнем распределения. Часть портов, а в некоторых моделях и все, могут поддерживать технологию PoE.

Например, коммутатор **Cisco Catalyst 2960PD-8TT-L** имеет 8 портов Ethernet/Fast Ethernet и один порт Ethernet/Fast Ethernet/Gigabit Ethernet, способный получать электропитание по технологии PoE.

Коммутатор **Cisco Catalyst 2960-24PC-L** имеет 24 портов Ethernet/Fast Ethernet и 2 порта Ethernet/Fast Ethernet/Gigabit Ethernet, при этом все порты поддерживают передачу электропитания по технологии PoE.

Коммутатор **Cisco Catalyst 2960-48TC-L** имеет 48 портов Ethernet/Fast Ethernet и 2 порта Ethernet/Fast Ethernet/Gigabit Ethernet.

Cisco Catalyst 3560 Series Switches

Серия коммутаторов, имеющих 8, 24 или 48 портов Ethernet/Fast Ethernet, для подключения рабочих станций. Соединение с уровнем распределения обеспечивается 1, 2 или 4 восходящими связями, в качестве которых используются порты Ethernet/Fast

Ethernet/Gigabit Ethernet или порты SFP для подключения оптоволоконной линии по протоколам 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX. Часть портов, а в некоторых моделях и все, могут поддерживать технологию PoE. Коммутаторы этой серии поддерживают некоторые функции сетевого уровня – фильтрация пакетов с помощью ACL и маршрутизация по протоколу RIP.

Например, коммутатор **Cisco Catalyst 3560-8PC** имеет 8 портов Ethernet/Fast Ethernet поддерживающих технологию PoE и порт Ethernet/Fast Ethernet/Gigabit Ethernet/SFP.

Коммутатор **Cisco Catalyst 3560-24PC** имеет 24 порта Ethernet/Fast Ethernet, поддерживающих технологию PoE и 4 SFP-порта Gigabit Ethernet для связи с уровнем распределения.

Cisco Catalyst 3560-E Series Switches

Серия коммутаторов для высокопроизводительных сетей. Коммутаторы имеют для подключения рабочих станций 24 или 48 портов Ethernet/Fast Ethernet/Gigabit Ethernet, или 12 SFP-портов Gigabit Ethernet. Соединение с уровнем распределения обеспечивают 2 X2-порта 10 Gigabit Ethernet.

Например, коммутатор **Cisco Catalyst 3560E-24TD** имеет 24 порта Ethernet/Fast Ethernet/Gigabit Ethernet и 2 X2-порта 10 Gigabit Ethernet.

Коммутатор **Cisco Catalyst 3560E-48TD** имеет 48 портов Ethernet/Fast Ethernet/Gigabit Ethernet и 2 X2-порта 10 Gigabit Ethernet для связи с уровнем распределения.

Коммутатор **Cisco Catalyst 3560E-12SD** имеет 12 SFP-портов Gigabit Ethernet и 2 X2-порта 10 Gigabit Ethernet для связи с уровнем распределения.

Особо выделим коммутатор **Cisco Catalyst 3560E-12D** имеющий 12 X2-портов 10 Gigabit Ethernet.

Cisco Catalyst 3750 Series Switches

Серия стековых коммутаторов, поддерживающих технологию **StackWise**, позволяющую объединять до 9 коммутаторов Cisco Catalyst 3750 в единый блок. Коммутаторы имеют для подключения рабочих станций 24 или 48 портов Ethernet/Fast Ethernet/Gigabit Ethernet, или 12 SFP-портов Gigabit Ethernet. Соединение с уровнем распределения для большинства моделей обеспечивают 2 – 4 SFP-порта Gigabit Ethernet.

Например, коммутатор **Cisco Catalyst 3750-24TS** имеет 24 порта Ethernet/Fast Ethernet и 2 SFP-порта Gigabit Ethernet.

Коммутатор **Cisco Catalyst 3750-48PS** имеет 48 портов Ethernet/Fast Ethernet, поддерживающих технологию PoE и 4 SFP-порта Gigabit Ethernet.

Коммутатор **Cisco Catalyst 3750G-24PS** имеет 24 порта Ethernet/Fast Ethernet/Gigabit Ethernet,

поддерживающих технологию PoE и 4 SFP-порта Gigabit Ethernet.

Особо выделим коммутатор **Cisco Catalyst 3750G-12S** имеющий 12 SFP-портов Gigabit Ethernet.

Cisco Catalyst 3750-E Series Switches

Серия новых стековых коммутаторов, поддерживающих технологию **StackWise Plus**, позволяющую объединять до 9 коммутаторов Cisco Catalyst 3750 в единый блок. Коммутаторы имеют для подключения рабочих станций 24 или 48 портов Ethernet/Fast Ethernet/Gigabit Ethernet, соединение с уровнем распределения для большинства моделей обеспечивает модуль TwinGig, обеспечивающий подключение SFP-порта Gigabit Ethernet или X2-порта 10 Gigabit Ethernet.

Например, коммутатор **Cisco Catalyst 3750E-24TS** имеет 24 порта Ethernet/Fast Ethernet/Gigabit Ethernet и 2 X2-порта 10 Gigabit Ethernet.

Коммутатор **Cisco Catalyst 3750E-48TD** имеет 48 портов Ethernet/Fast Ethernet/Gigabit Ethernet, и 2 X2-порта 10 Gigabit Ethernet.

Коммутатор **Cisco Catalyst 3750E-48PD** имеет 48 порта Ethernet/Fast Ethernet/Gigabit Ethernet, поддерживающих технологию PoE и 2 X2-порта 10 Gigabit Ethernet.

Cisco Catalyst 4500 Series Switches

Серия модульных коммутаторов, шасси которых содержит 2-8 слотов для модулей коммутации, 1-2 слота для модулей управления и 2 отсека для блоков питания.

Например, коммутатор **Cisco Catalyst 4510R** имеет 10 слотов, в том числе 8 слотов для модулей коммутации и 2 слота для модулей управления, в качестве которых могут использоваться модули Supervisor Engine V, V-10GE или 6-E.

Например, коммутатор **Cisco Catalyst 4506R** имеет 6 слотов, в том числе 5 слотов для модулей коммутации и слот для модуля управления, в качестве которого могут использоваться модули Supervisor Engine II-Plus, II-Plus-10GE , IV, V, V-10GE или 6-E.

Например, коммутатор **Cisco Catalyst 4503R** имеет 3 слота, в том числе 2 слотов для модулей коммутации и слот для модуля управления, в качестве которого могут использоваться модули Supervisor Engine II-Plus, II-Plus-TS, II-Plus-10GE , IV, V, V-10GE или 6-E.

Cisco Catalyst 6500 Series Switches

Серия модульных коммутаторов **Catalyst 6500** занимает верхнюю строчку в линейке коммутаторов Cisco. Шасси содержит 2-13 слотов для модулей коммутации и управления, 2 отсека для блоков питания и поддержку функций 3-го уровня.

Модули содержат:

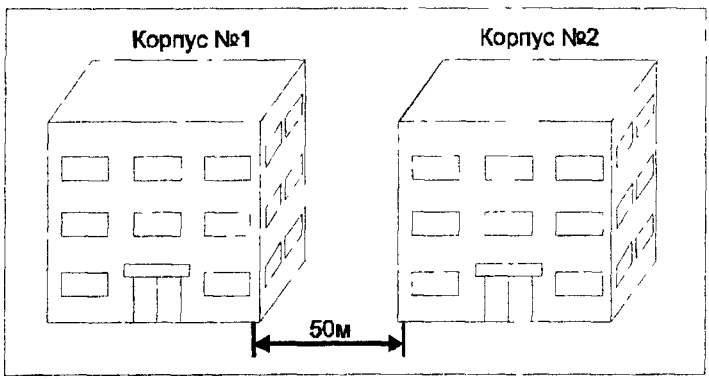
- порты Fast Ethernet, поддерживающие технологии PoE;
- порты Gigabit Ethernet, поддерживающие технологии PoE;
- порты 10 Gigabit Ethernet;
- WAN-модули;
- сервисные модули, реализующие функции VPN, SSL и т.д.

Например, коммутатор **Cisco Catalyst 6503-E** имеет габариты 178мм x 441мм x 552мм, 3 слота и может использовать модули управления Supervisor 32 или Supervisor 720.

Коммутатор **Cisco Catalyst 6509-E** имеет габариты 245мм x 175мм x 182мм, 9 слотов и может использовать модули управления Supervisor 2, Supervisor 32 или Supervisor 720.

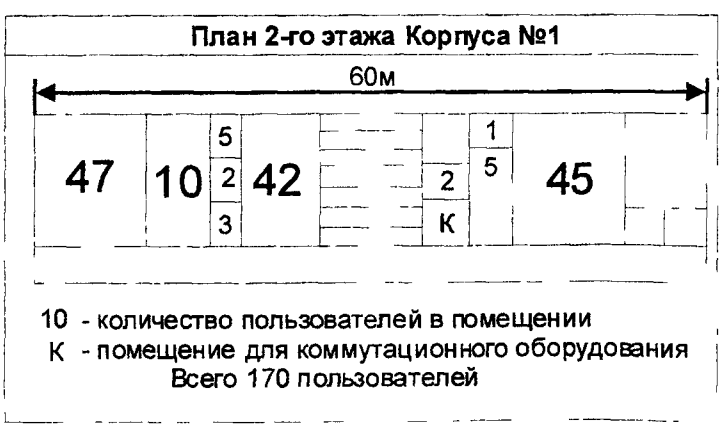
Необходимо отметить, что, хотя коммутаторы серии **Catalyst 6500**, позиционируются и для уровня доступа, более целесообразным представляется их использование на уровне распределения и ядра.

Конкретизируем задание: пусть наше предприятие занимает два трехэтажных здания, находящиеся в 50м друг от друга.



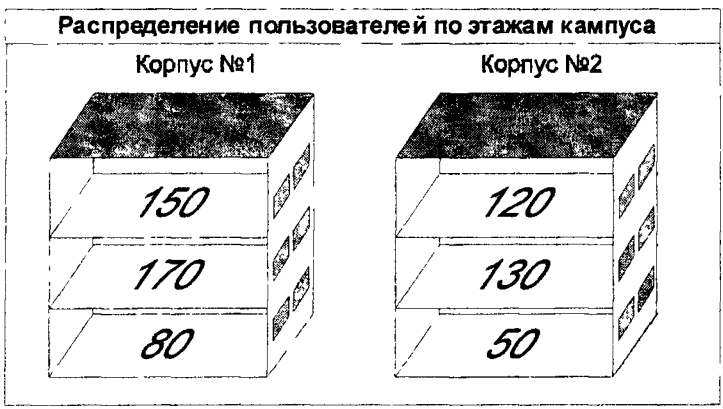
В первом корпусе требуется обеспечить подключение 400 пользователей, во втором – 300 пользователей. Будем считать, что при постройке/ремонте здания соблюдались стандарты СКС.

Далее, составим для каждого здания поэтажный план с указанием помещений для коммутационного оборудования.



Размеры здания и площади помещений допускают использование одного помещения для коммутационного оборудования на этаж.

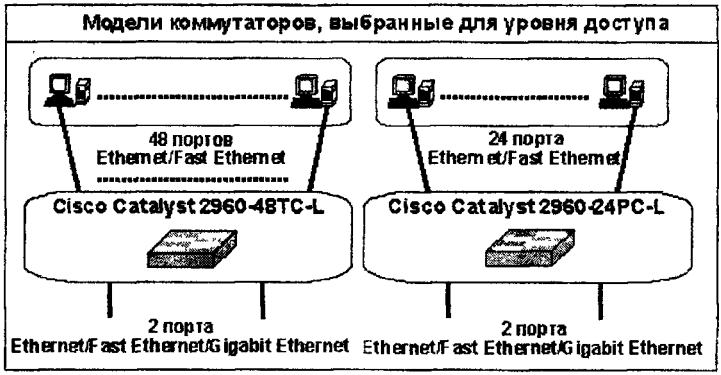
Проанализировав поэтажные планы, получим следующее распределение пользователей по этажам:



Оборудование уровня распределения разместим на первых этажах корпусов, оборудование уровня ядра – на первом этаже первого корпуса

Выберем в качестве коммутаторов уровня доступа устройства серии 2960. Используем , в зависимости от размеров подсети коммутаторы двух моделей: Cisco Catalyst 2960-24PC-L и Cisco Catalyst 2960-48TC-L.

Эти модели имеют, соответственно, 24 и 48 Ethernet/Fast Ethernet, для подключения рабочих станций и по 2 порта Ethernet/Fast Ethernet/Gigabit Ethernet для связи с уровнем распределения.



Как разбить сеть на подсети?

Этот вопрос распадается на два:

- По какому принципу делить сеть на подсети?
- Как составить адресный план сети?

Существует несколько способов разбиения сети на подсети:

- по отделам по отделам предприятия;
- по помещениям: каждая комната – отдельная подсеть;
- по служебным обязанностям пользователей;

В большинстве случаев разбиение на подсети по отделам предприятия представляется наиболее логичным.

Выделение подсетей по служебным обязанностям пользователей имеет смысл, если разным пользователям одного отдела требуются принципиально

разные ресурсы сети, предоставление которых влияет на ее структуру.

Например, одному сотруднику часто надо выполнять многоадресные трансляции по сети Ethernet и иметь постоянный доступ к корпоративным серверам, а его соседу – сеть Token Ring и доступ только к серверу отдела и в Internet.

Деление на подсети по помещениям, точнее, по географическому расположению, разумно, если сотрудники одних и тех же отделов находятся очень далеко друг от друга, и их не желательно выделять в самостоятельные подразделения. Отметим, что здесь идет речь не об удаленном доступе по глобальным каналам связи, а о разных подсетях большой, но, все-таки, локальной сети.

Удобнее всего реализовывать подсети с помощью механизма виртуальных локальных сетей - VLAN.

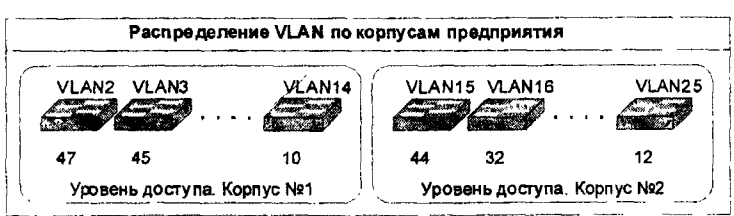
Как уже говорилось в первом разделе, сеть можно спроектировать так, что VLAN будут распространяться по всему зданию или даже кампусу, а можно ограничить распространение VLAN уровнем доступа и даже, одним коммутатором, причем последнее лучше, так как позволяет уменьшить время схождения и улучшить балансирование нагрузки.

Основная рекомендация – если это возможно – один VLAN на один коммутатор.

Если следовать этому правилу невозможно, то, по крайней мере не используйте протокол STP, так как его время схождения очень велико – порядка минуты. Вместо STP (IEEE 802.1d) для устранения петель используйте RSTP (Rapid STP, IEEE 802.1w). Одновременно желательно использовать разработанные Cisco протоколы PVST или PVST+, улучшающие балансирование нагрузки.

Мы будем следовать принципу «Один коммутатор – Один VLAN». Совсем мелкие отделы (1-5 компьютеров) постараемся, если возможно, объединить в один VLAN. Очень крупные отделы можно, наоборот, представить несколькими VLAN.

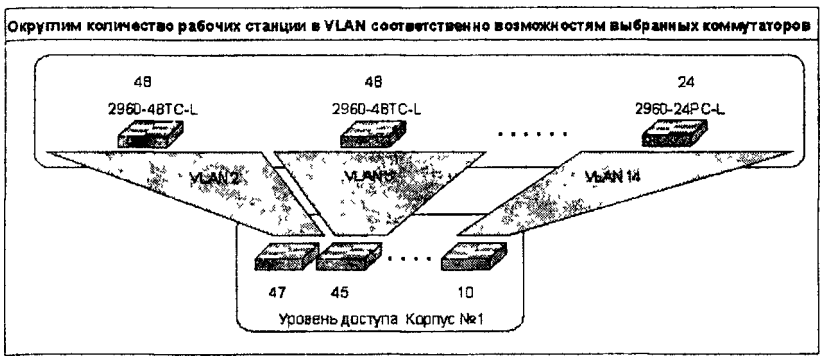
Пусть полученное распределение VLAN по корпусам предприятия соответствует изображенному на рисунке:



Не так важно совпадение границ VLAN, как надежное и удобное подключение пользователей к сети предприятия.

Исходя из характеристик выбранных коммутаторов, округлим количество рабочих станций в каждой подсети в большую сторону:

- до 24, если их было меньше чем 24;
- до 48, если их было больше чем 24.



Составим примерный адресный план нашей сети. Для этого, в первую очередь, выпишем в таблицу все подсети в порядке убывания числа компьютеров в них:

Таблица 2.1.

Подсети	Число рабочих станций в VLAN	Корпус
VLAN2	48	1
VLAN3	48	1
VLAN22	48	2
.....	...	
VLAN14	24	1

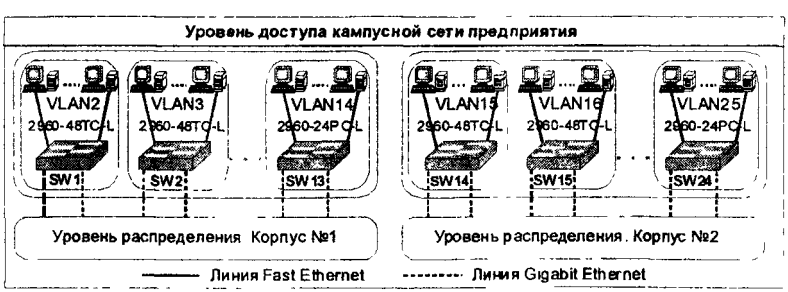
Возьмем для сети адрес из пространства частных (privat) IP-адресов, например, 10.0.0.0

Определим адреса и маски подсетей для каждого VLAN. При этом будем, по возможности экономить адресное пространство для будущих подсетей.

Таблица 2.2.

Подсети	Число рабочих станций в VLAN	Адрес подсети	Маска подсети
VLAN2	48	10.0.0.0	255.255.255.192
VLAN3	48	10.0.0.64	255.255.255.192
VLAN15	48	10.0.0.128	255.255.255.192
.....	...	.....	.....
VLAN14	24	10.0.0.208	255.255.255.240

Итак, наш уровень доступа составят 24 коммутатора Cisco Catalyst 2960-24PC-L и Cisco Catalyst 2960-48TC-L, 13 в первом корпусе и 11 во втором. Рабочие станции подключаются к портам Fast Ethernet.



Каждый коммутатор уровня доступа подключен к уровню распределения двумя линиями Gigabit Ethernet, все связи с уровнем распределения – не транковые, а маршрутизируемые линии, что улучшает балансировку нагрузки и уменьшает время восстановления после сбоя.

2.2. Проектирование уровня распределения

Проектирование уровня распределения.

При проектировании уровня распределения сети решаются задачи обеспечения коммутации между уровнем доступа и ядром. При этом часто приходится рассматривать проблемы изменения среды передачи данных, объединения множества низкоскоростных каналов в высокоскоростные магистральные каналы. Кроме того, на уровне распределения в значительной степени решается задача отказоустойчивости – соединение ядра с уровнем доступа обязательно должно резервироваться.

Проектируя уровень распределения, разработчик должен ответить на вопросы:

1. Сколько коммутаторов уровня доступа должен обслуживать уровень распределения в каждом здании?
2. Как обеспечить резервирование маршрутов ?

3. Как обеспечить равномерное распределение нагрузки?
4. Какие модели коммутаторов использовать в качестве коммутаторов уровня распределения?

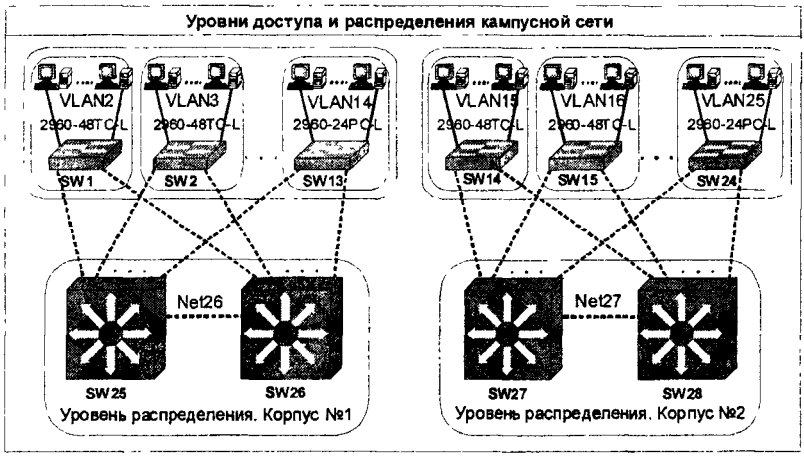
Определение структуры уровня распределения

Итоги проектирования уровня доступа показывают, что уровень распределения первого корпуса должен обслуживать 13 коммутаторов уровня доступа, а уровень распределения второго корпуса – 11 коммутаторов уровня доступа. Резервирование, как показано выше, достигается за счет наличия у каждого коммутатора уровня доступа двух портов Gigabit Ethernet, что дает возможность соединить каждый коммутатор уровня доступа с двумя коммутаторами уровня распределения.

Таким образом, уровень распределения каждого корпуса будет представлен двумя, связанными друг с другом, многоуровневыми коммутаторами. Обозначим их SW25 – SW28.

Так как все связи спроектированного нами уровня доступа с уровнем распределения являются не транковыми, а маршрутизируемыми линиями, то на уровне распределения мы можем ограничиться коммутацией третьего уровня и возложить задачи балансировку нагрузки

и поиска резервных маршрутов на протоколы маршрутизации.



Важным достоинством подобного решения, как уже говорилось выше, является то, что современные протоколы маршрутизации справляются с этими задачами лучше, чем протокол STP, использование которого было бы необходимо, если бы мы использовали на уровне распределения коммутацию второго уровня.

Современные протоколы маршрутизации по сравнению с самыми современными вариантами STP обеспечивают лучшую балансировку нагрузки и меньшее время восстановления после сбоя.

Выбор модели коммутатора уровня распределения

Cisco Systems рекомендует использовать на уровне распределения кампусной сети многоуровневые коммутаторы серий Cisco Catalyst 4500 и 4500-E, Cisco

Catalyst 6500 и 6500-E, а также Cisco Catalyst 6500 Virtual switching system 1440.

Характеристики этих устройств легко узнать на сайте www.cisco.com, выбрав закладку Products&Services и пункт Switches.

В качестве коммутатора уровня распределения используем модульный коммутатор Cisco Catalyst 4506. Он имеет 6 слотов, в том числе 5 слотов для модулей коммутации (Line card) и слот для модуля управления (Supervisor Engine), в качестве которого могут использоваться модули Supervisor Engine II-Plus, II-Plus-10GE , IV, V, V-10GE или 6-E.

Для модульного коммутатора необходимо выбрать модули управления и коммутации.

Выбор модуля коммутации (line card)

Для модульных коммутаторов Cisco выпускаются весьма разнообразные модули коммутации (line card). Учитывая особенности спроектированной нами схемы (11-13 линий витой пары Gigabit Ethernet на каждый коммутатор), желательность использования оптоволоконного кабеля между зданиями и необходимость оставить запас для масштабирования.

Выберем модуль WS-X4506-GB-T, содержащий 6 портов Gigabit Ethernet. Таким образом, для коммутаторов SW25 и SW26 потребуется по 3 модуля WS-X4506-GB-T, а

для коммутаторов SW27 и SW27 потребуется по 2 модуля WS-X4506-GB-T.

Особенности модуля коммутации WS-X4506-GB-T

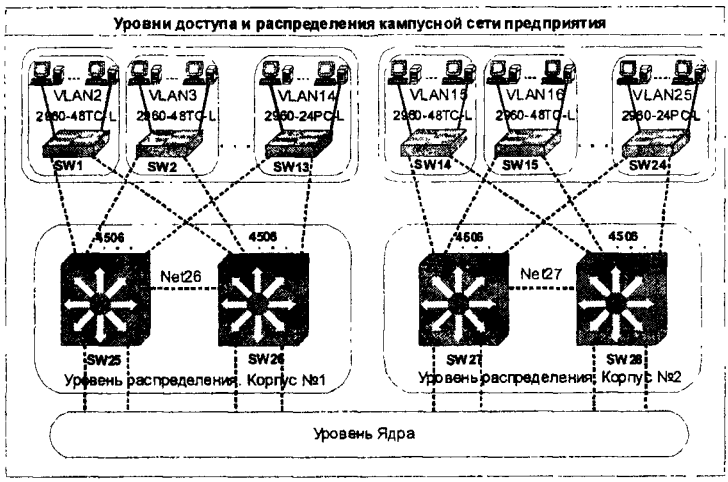
Модуль коммутации WS-X4506-GB-T имеет 6 портов Ethernet/Fast Ethernet/ Gigabit Ethernet, поддерживающих технологию PoE и 6 оптоволоконных портов SFP. При этом, одновременно могут использоваться любые 6 из этих 12 портов, т.е. один модуль позволяет иметь 6 подключений Gigabit Ethernet с помощью витой пары или оптоволокна.

Выбор модуля управления

При выборе модуля управления исходим из того, что он должен поддерживать современные протоколы маршрутизации и работать совместно с выбранным шасси (Cisco Catalyst 4506) и модулем коммутации WS-X4506-GB-T.

Исходя из этих критериев, выбираем модуль Cisco Catalyst 4500 Series Supervisor Engine IV, поддерживающий, помимо прочего, протоколы маршрутизации IGRP, EIGRP, OSPF и RIP, в том числе RIPv2.

Получившийся в результате уровень распределения представлен на следующем рисунке.



Каждый коммутатор уровня распределения подключен к уровню ядра двумя линиями Gigabit Ethernet, что обеспечивает высокую пропускную способность, возможность балансирования нагрузки и резервирование на случай сбоя.

2.3. Проектирование уровня ядра и серверной фермы

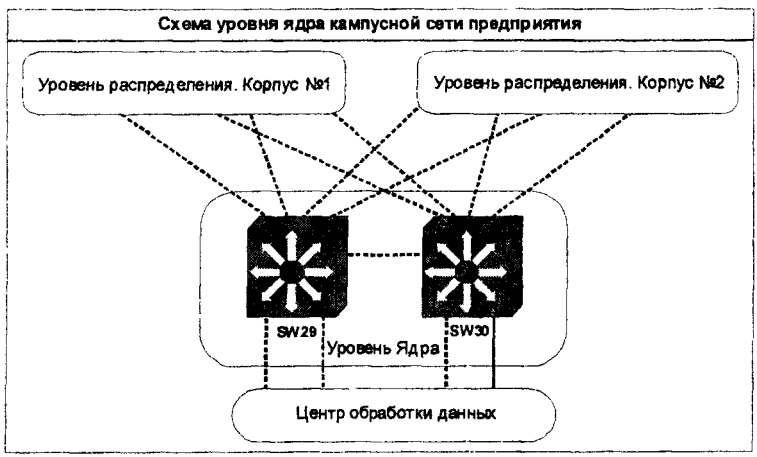
Проектирование уровня ядра и серверной фермы.

При проектировании уровня ядра надо учесть, что главная функция ядра – быстро и надежно передавать данные между модулями сети – уровнями распределения корпусов, серверной фермой и граничным модулем.

Быструю и надежную коммутацию пакетов обеспечивают многоуровневые коммутаторы при использовании современных протоколов маршрутизации.

Необходимость резервировать оборудование требует использования на уровне ядра двух коммутаторов.

Таким образом, уровень ядра нашей сети будет состоять из двух многоуровневых коммутаторов SW29 и SW30.



Коммутаторы уровня ядра связаны линиями Gigabit Ethernet, с уровнем распределения и центром обработки данных по топологии, близкой к полносвязной, что обеспечивает высокую пропускную способность, возможность балансирования нагрузки и резервирование на случай сбоя.

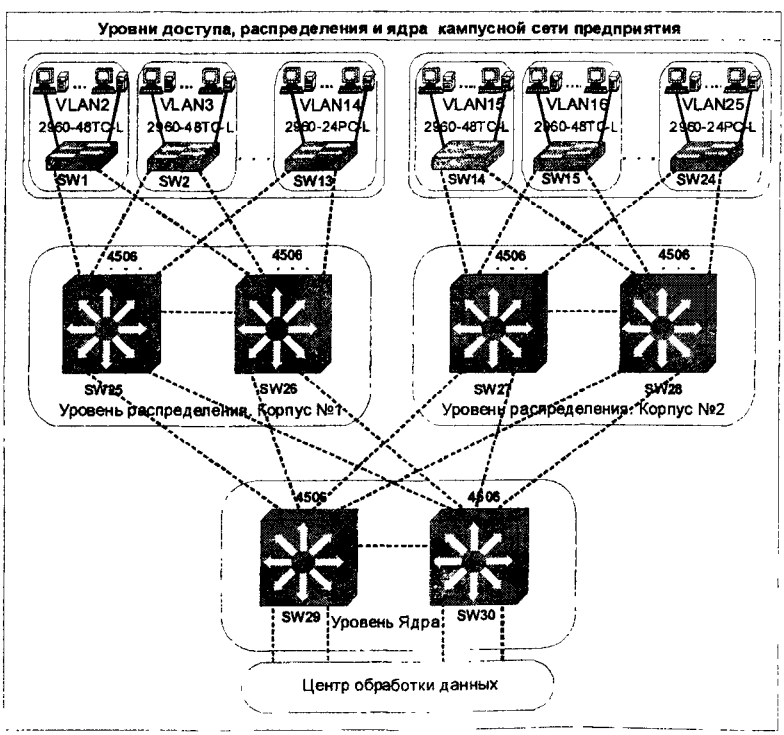
Выбор модели коммутатора уровня ядра

Cisco Systems рекомендует использовать на уровне ядра кампусной сети, в основном, те же модели, что и для уровня распределения. Это уже знакомые нам многоуровневые коммутаторы серий Cisco Catalyst 4500 и

4500-E, Cisco Catalyst 6500 и 6500-E, а также Cisco Catalyst 6500 Virtual switching system 1440.

Оборудование, выбранное нами для уровня распределения, подходит и для ядра нашей сети. Поэтому, воспользовавшись возможностью не увеличивать число типов сетевых устройств, выберем два многоуровневых коммутатора Cisco Catalyst 4506, каждый из которых должен иметь два модуля WS-X4506-GB-T и модуль управления Cisco Catalyst 4500 Series Supervisor Engine IV.

Получившийся в результате уровень ядра представлен на рисунке:



Подключение серверной фермы к уровню ядра

Так как значительная часть запросов в сети будет адресована к корпоративным серверам, пропускная способность подключения серверной фермы будет, в значительной степени, определять скорость работы всей сети.

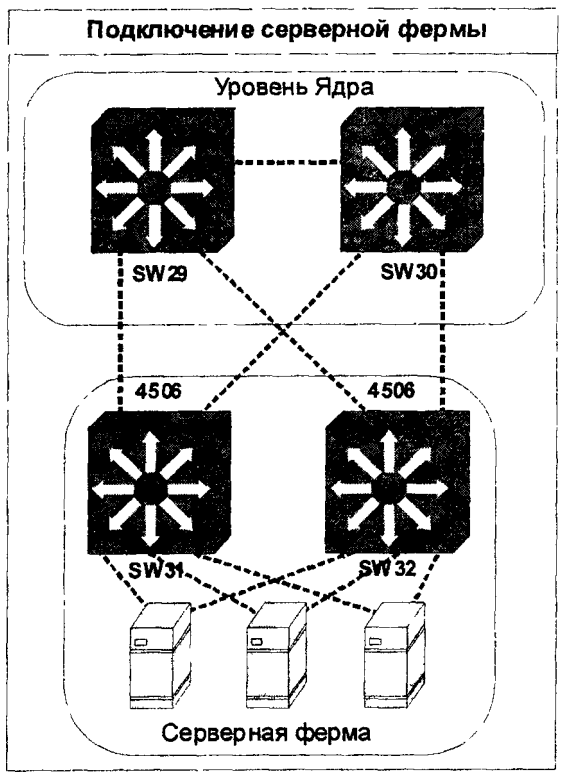
Если уровень доступа представлен технологией Fast Ethernet, а уровень распределения подключен к ядру кампусной сети несколькими линиями Gigabit Ethernet, то для подключения серверной фермы к ядру рекомендуется использовать технологию 10 Gigabit Ethernet или несколько линий Gigabit Ethernet.

Для надежности, каждый сервер должен снабжаться двумя сетевыми адаптерами (Network Interface Card - NIC) или многопортовым сетевым адаптером (Multipoint NIC) и подключаться к двум разным коммутаторам.

Каждый сервер можно представить в виде отдельной подсети – VLAN. Это позволяет использовать для каждого сервера свою политику доступа.

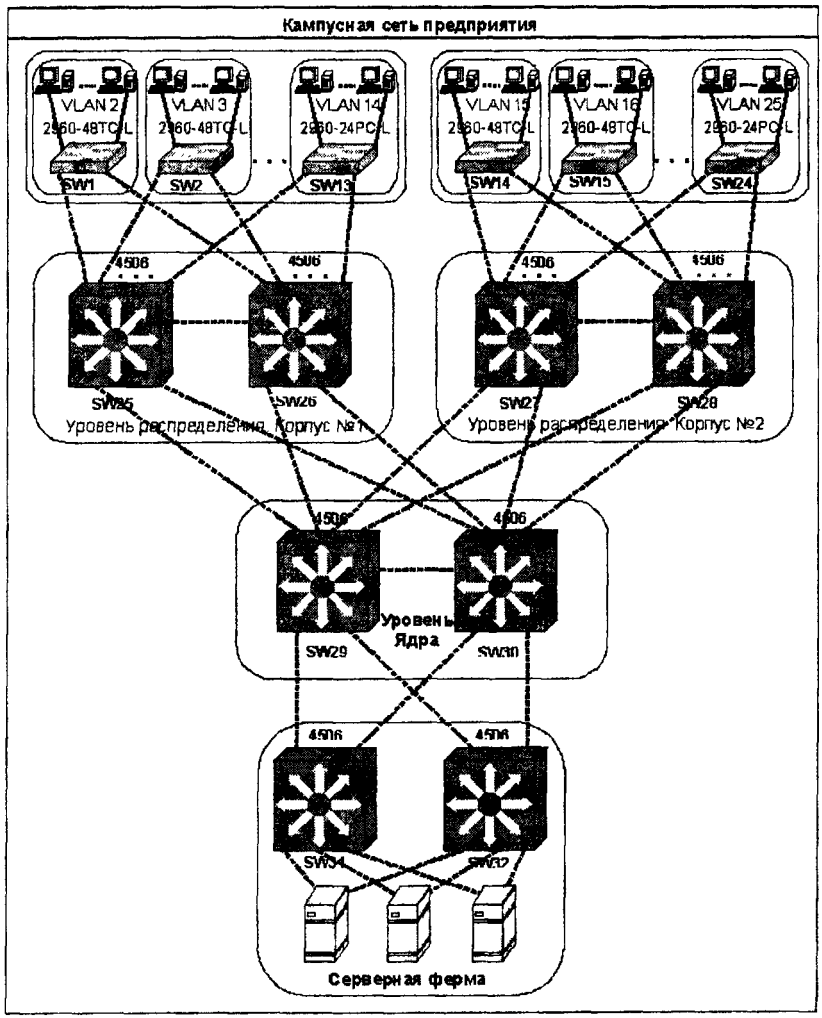
Коммутаторы серверной фермы связаны несколькими линиями Gigabit Ethernet с коммутаторами уровня ядра и серверами по топологии, близкой к полносвязной, что обеспечивает высокую пропускную способность, возможность балансирования нагрузки и резервирование на случай сбоя.

Подключение серверной фермы к уровню ядра представлено на рисунке:



В качестве коммутаторов серверной фермы SW31 и SW32 используем два многоуровневых коммутатора Cisco Catalyst 4506, каждый из которых должен иметь модуль WS-X4506-GB-T и модуль управления Cisco Catalyst 4500 Series Supervisor Engine IV.

И вот, наконец, можно взглянуть на результат – кампусную сеть предприятия:



Сетевое оборудование спроектированной нами сети состоит из:

Коммутаторов второго уровня Cisco Catalyst 2960 – 24 шт.

Многоуровневых коммутаторов Cisco Catalyst 4506 – 8 шт.

Коммутационных модулей WS-X4506-GB-T – 16 шт.

Модулей управления Cisco Catalyst 4500 Series Supervisor Engine IV – 8 шт.

Кроме этого, каждый компьютер в сети должен снабжаться сетевым адаптером Ethernet или Fast Ethernet, а каждый сервер – двумя сетевыми адаптерами Fast Ethernet.

На всех многоуровневых коммутаторах следует настроить протокол маршрутизации EIGRP.

2.4. Примеры и упражнения

Пример 2.1.

Настройка VLAN на коммутаторах уровня доступа

Настроим на коммутаторе VLAN3 и включим в него порт fa0/3

1. Войдем в привилегированный режим

*Switch>**enable***

2. Создадим на коммутаторе VLAN3

*Switch#**vlan database***

*Switch(vlan)#**vlan 3***

VLAN 2 added:

Name: VLAN0002

*Switch(vlan)#**^Z***

%SYS-5-CONFIG_I: Configured from console by console

Switch#

3. Включим порт fa0/3 в VLAN3

*Switch#**configure terminal***

*Switch(config)#**int fastEthernet 0/3***

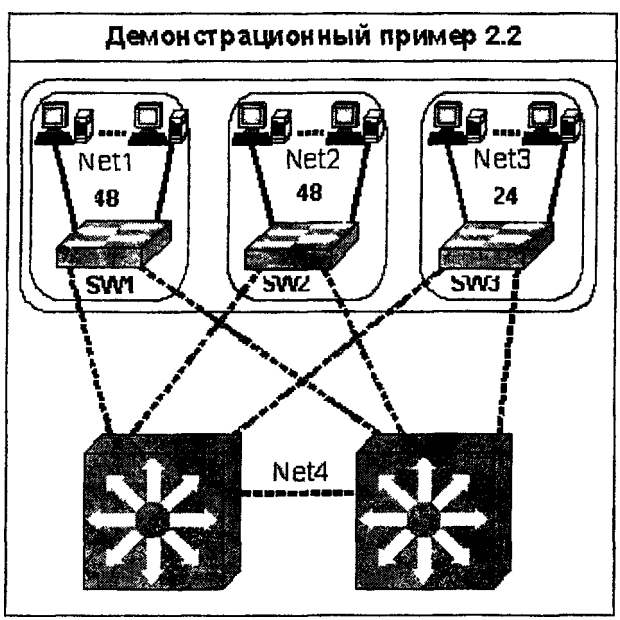
*Switch(config-if)#**switchport access vlan 3***

*Switch(config-if)#**exit***

Switch(config)#

Пример 2.2.

Расчет адресного плана сети



На рисунке представлена небольшая сеть. Составим адресный план для нее.

Выпишем подсети в порядке убывания компьютеров в них:

Подсеть	Число рабочих станций
Net1	48
Net2	48
Net3	24
Net4	2

Пусть для адресации всей сети дан IP-адрес 197.10.1.0. Это адрес класса С, следовательно, по умолчанию маска подсети 255.255.255.0 – три байта на адрес сети и один байт на адрес подсети и адрес хоста.

Рассмотрим сеть Net1. Для адресации 48 хостов с учетом адреса подсети и адреса широковещания нужно 50 адресов – 6 двоичных разрядов.

Маска подсети 255.255.255.192.

Значит хостовая часть адреса 6 бит, на номер подсети остается 2 бита. Назначим эти два бита для подсети Net1 равными 00, а для Net2 – 01. Сочетания 10 и 11 остаются пока свободными.

Сеть Net3 имеет не более 24 хостов и требует 24+2=26 адресов. Для их адресации требуется 5 бит, а номер подсети будет из трех бит, например, 100.

Сеть Net4 имеет не более 2-х хостов и требует 2+2=4 адреса. Для их адресации требуется 2 бита, а номер подсети будет из 6 бит, например, 101000.

Результат приведен в следующей таблице:

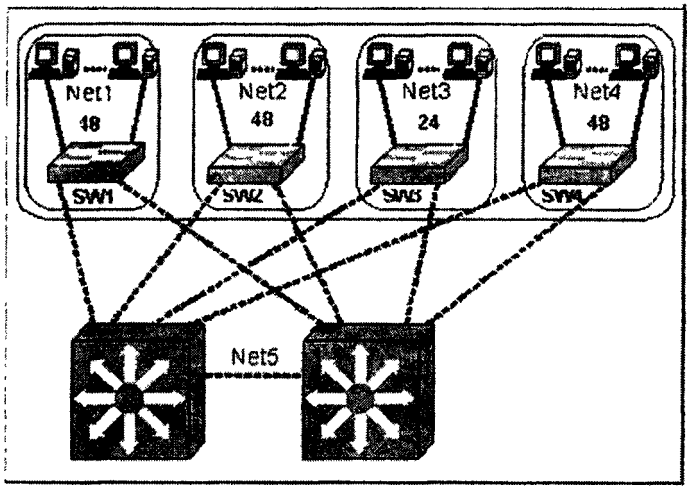
Подсеть	Адрес подсети	Маска подсети
Net1	197.10.1.0	255.255.255.192
Net2	197.10.1.64	255.255.255.192
Net3	197.10.1.128	255.255.255.224
Net4	197.10.1.160	255.255.255.250

Таким образом, с помощью одного IP-адреса класса С и технологии VLSM (маска подсети переменной длины) удалось не только снабдить адресами 4 сети, но и оставить солидный запас адресов на будущее.

Задания

Задание 2.1.

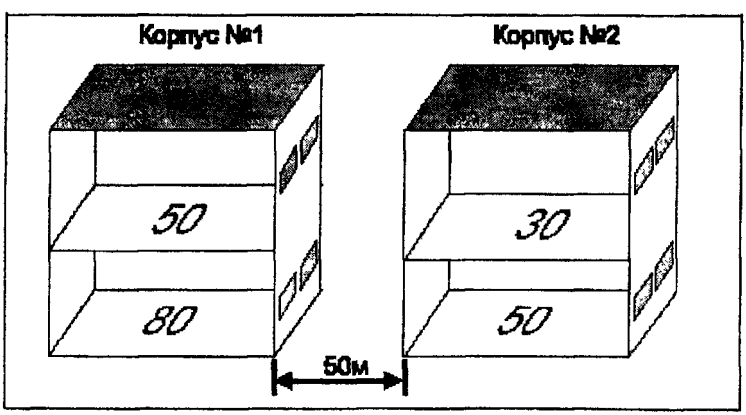
Рассчитать адресный план сети, изображенной на рисунке.



Использовать адрес 194.5.8.0.

Задание 2.2.

Спроектировать кампусную сеть для предприятия, изображенного на рисунке:



- для каждого уровня кампусной сети указать модель и количество сетевых устройств;
- описать связи между устройствами;
- описать распределение VLAN;

- перечислить основные протоколы, используемые в спроектированной Вами сети для балансирования нагрузки, предотвращения петель и повышения отказоустойчивости.

3. Современные технологии обеспечения устойчивости сети

3.1. Особенности использования STP в сетях Cisco

Особенности использования протокола STP в сетях Cisco

Во втором разделе уже отмечалось, что устойчивость работы сети во многом определяется наличием избыточных, резервных маршрутов. Если на уровне доступа выполняется правило «один коммутатор – один VLAN», задачи выбора основного и резервного маршрутов, обнаружения сбоя и предотвращения петель решается протоколами маршрутизации, причем, решаются за считанные секунды.

При поддержании нескольких подсетей на одном коммутаторе, эти задачи решаются протоколом STP или его многочисленными вариантами. Такой способ имеет ряд недостатков, главные из которых: большое время схождения STP и невысокие возможности балансировки нагрузки. Тем важнее знать о некоторых вариантах

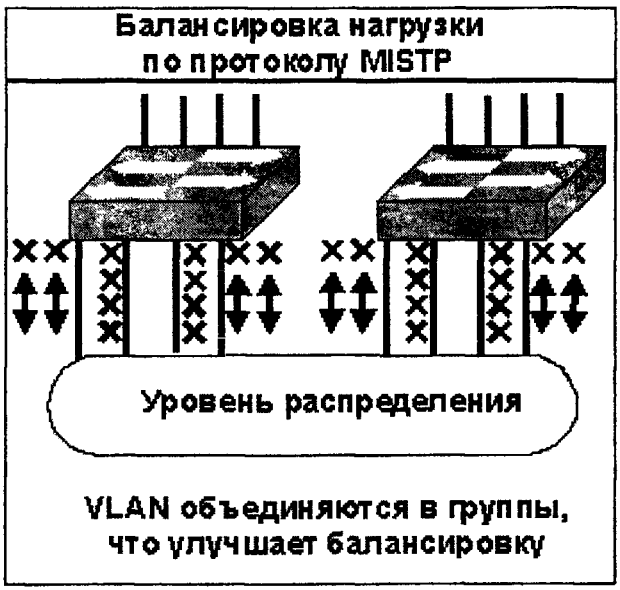
использования подобных протоколов в сетях Cisco, значительно сглаживающих эти недостатки.

Multiple Instance STP

Прежде всего надо помнить, что помимо всем известного протокола STP (IEEE 802.d) существует и более совершенный протокол RSTP (Rapid STP – IEEE 802.w). Эти два протокола давно стали общепризнанным стандартом, но есть и другие, так же стандартные, но менее известные протоколы.

Одним из них является протокол MISTP (Multiple Instance STP – IEEE 802.s, во многих источниках называется MSTP). По своему функционированию он аналогичен RSTP, но позволяет объединять подсети (VLAN) в группы. Для каждой такой группы VLAN выполняется отдельный процесс RSTP. Таким образом, один и тот же порт коммутатора может быть передающим

для одного процесса и блокированным для другого. Это позволяет несколько лучше балансировать нагрузку, чем в RSTP.



Несколько соединенных между собой коммутаторов с одинаковой конфигурацией протокола MSTP составляют регион. Балансировка нагрузки выполняется в пределах одного региона. В каждом регионе поддерживается до 65 STP-процессов, которые идентифицируются номерами 0..4096. Номера STP-процессов должны быть уникальными в пределах региона.

Протокол MSTP поддерживает два типа STP-деревьев:

- **Internal Spanning Tree (IST)** – существует в пределах региона. Дереву IST соответствует STP-процесс

с номером 0. Этот процесс – единственный в регионе рассылает BPDU, обеспечивая обмен STP-информацией между коммутаторами. Сообщение BPDU содержит данные обо всех STP-процессах в регионе. Остальные STP-процессы в регионе (т.е. все, кроме нулевого) никаких сообщений не рассылают, а черпают нужную им информацию из сообщений BPDU, рассылаемых IST, т.е. STP-процессом с номером 0.

- **Common and internal spanning tree (CIST)** – общее STP-дерево в сети из нескольких регионов и отдельных STP-деревьев. CIST объединяет деревья IST во всех регионах и отдельные STP-деревья в единый STP-процесс.

Как и в случае обычного STP, коммутатор с наименьшим значением ID, становится корневым: CIST root. В каждом регионе выбирается свой корневой коммутатор - CIST regional root - с наименьшими значениями ID и стоимости пути (path cost) до CIST root.

Конфигурация протокола MSTP

Рассмотрим конфигурацию протокола MSTP на примере коммутатора серии Cisco Catalist 2960.

1) Войти в режим конфигурации MSTP с помощью команды глобальной конфигурации

spanning-tree mst configuration

2) Следующий шаг – установить параметры региона. Для этого надо задать номер региона, номер ревизии и карту соответствия, показывающую какой VLAN к какому STP-процессу относится. Все эти параметры должны быть одинаковы для всех коммутаторов региона.

Карта соответствия задается командой:

instance *номер STP-процесса* **vlan** *перечень VLAN*

Параметр *номер STP-процесса* указывает на один из STP-процессов данного региона и может иметь значения от 0 до 4096.

Параметр *перечень VLAN* может задаваться как в виде списка номеров VLAN: *5,7,15* , так и в виде диапазона: *5-15.*

Имя региона задается командой:

name *имя региона,*

где *имя региона* – строка длинной до 32 символов.

Номер ревизии задается командой:

revision *номер ревизии,*

где *номер ревизии* – значение от 0 до 65535.

3) Собственно, конфигурация на этом закончена. Осталось выйти из режима конфигурации протокола MSTP командой

exit.

4) По умолчанию протокол MSTP отключен. Поэтому его надо включить командой глобальной конфигурации:

spanning-tree mode mst

При этом автоматически будут включены и функции протокола RSTP.

5) Важно не забыть сохранить сделанные изменения командой

copy running-config startup-config

и не забыть настроить аналогичным образом остальные коммутаторы сети.

Чтобы сделать данный коммутатор корневым для определенного STP-процесса надо воспользоваться командой глобальной конфигурации

spanning-tree mst *номер процесса* **root primary**

Указать значение приоритета для конкретного порта можно командой конфигурации интерфейса:

spanning-tree mst *номер процесса* **port-priority** *приоритет*

где параметр *приоритет* может принимать значения: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. По умолчанию порт имеет значение приоритета 128.

Указать значение *cost* для конкретного порта можно командой конфигурации интерфейса:

spanning-tree mst *номер процесса* **cost** *cost*

где параметр *cost* может принимать значение от 1 до 200000000

Просмотреть настройки протокола MSTP можно, например, командами

show spanning-tree mst *номер процесса*

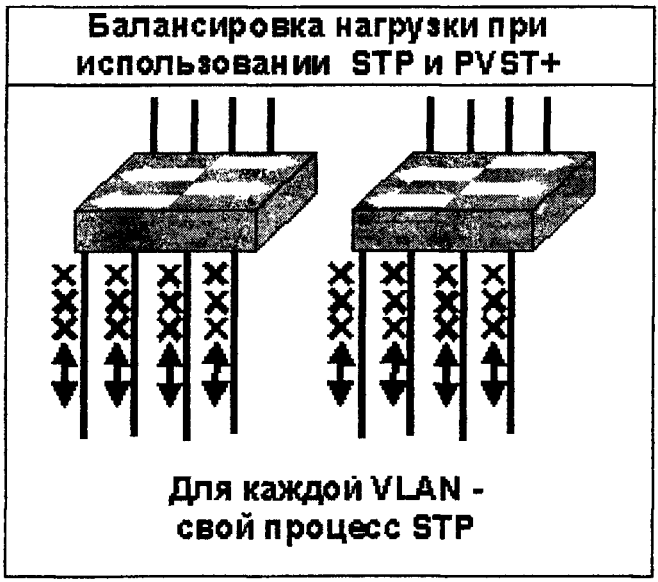
или

show spanning-tree mst interface *номер интерфейса*

Per-VLAN Spanning Tree Plus

Кроме протоколов, являющихся международными стандартами, существуют и протоколы, разработанные отдельными производителями и используемые, наряду со стандартными, на их оборудовании. Ряд подобных протоколов разработан компанией Cisco Systems. Рассмотрим их подробнее.

Для протокола STP компанией Cisco Systems разработано расширение Per-VLAN Spanning Tree Plus (PVST+). Использование протоколов STP и PVST+ позволяет иметь по отдельному процессу на каждую подсеть (VLAN). Одновременно поддерживается до 128 STP-процессов.



На рисунке показано, что один и тот же порт открыт для одной подсети (VLAN) и блокирован для других. Предыдущая версия – PVST, отличалась только тем, что работала только на транковых линиях использующих протокол ISL. PVST+ позволяет использовать и транковые линии, использующие протокол 802.1q.

При использовании протокола PVST+ для каждого VLAN создается свой STP-процесс, который поддерживает свое STP-дерево и рассылает свои сообщения BPDU. По сравнению с протоколом MSTP это несколько увеличивает сетевой трафик.

Протокол PVST+ обеспечивает балансировку нагрузки, распределяя ее, по возможности, между всеми имеющимися линиями.

Протокол PVST+ решает проблему балансирования нагрузки настолько, насколько это возможно на втором (канальном) уровне. В то же время возможности протокола PVST+ ограничены использованием для создания STP-процессов старого протокола STP (802.1d), имеющего большое время схождения.

Использование протокола PVST+ на коммутаторах Cisco, в частности, на коммутаторах серии Cisco Catalyst 2960, включено по умолчанию.

Протокол Rapid PVST+

Если протокол PVST+ был призван дополнить возможности старого протокола STP (802.1d), то для более нового протокола RSTP (802.1w), разработан протокол **Rapid PVST+.**

Протокол Rapid PVST+ создает для каждой подсети STP-процесс по протоколу RSTP (802.1w), имеющему меньшее время схождения, чем STP (802.1d).

Если PVST+, узнав об изменении топологии, выжидает некоторое время (aging time), прежде чем учесть эти изменения, то протокол Rapid PVST+, получив обновление, сразу применяет его.

Как и PVST+, протокол Rapid PVST+ поддерживает до 128 STP-процессов.

Если на коммутаторе существует более 128 VLAN, STP-процессы будут созданы только для 128. В этом

случае администратор может отключить STP-процесс для одного VLAN, для которого он, по мнению администратора не нужен, командой глобальной конфигурации

no spanning-tree vlan *номер VLAN*

а затем создать STP-процесс для нужного VLAN командой глобальной конфигурации

spanning-tree vlan *номер VLAN*

так что общее число STP-процессов не превысит 128.

Другой способ решить эту проблему - перейти на протокол MSTP, обеспечивающей STP-процессы для 65 групп VLAN с практически неограниченным числом VLAN в группе.

Современные коммутаторы Cisco обеспечивают работу протоколов MSTP, PVST+, или Rapid PVST+. Выбор одного из них выполняется в режиме глобальной конфигурации.

Протокол PVST+ включен по умолчанию, но если он был отключен, его можно включить снова следующей командой:

spanning-tree mode pvst

Протокол Rapid PVST+ можно включить следующей командой:

spanning-tree mode rapid-pvst

Настройка протокола MSTP показана выше.

Узнать настройки STP на коммутаторе можно командой

show spanning-tree vlan

а настройки STP для конкретного VLAN – следующей командой:

show spanning-tree vlan *номер VLAN*

3.2. Использование Cisco STP Toolkit

Использование Cisco STP Toolkit

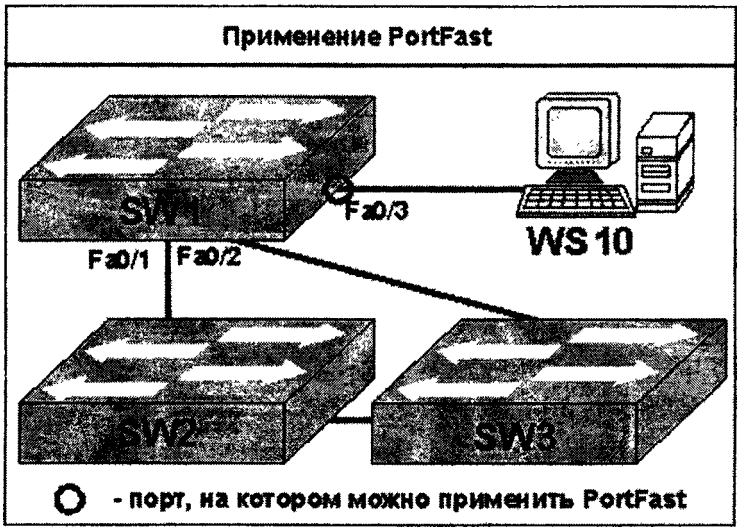
Для рассмотренных выше STP-протоколов компания Cisco Systems разработала набор дополнительных компонентов, известный как **Cisco STP Toolkit** или **Optional Spanning-Tree Features**:

- Port Fast
- BPDU Guard
- BPDU Filtering
- UplinkFast
- BackboneFast
- EtherChannel Guard
- Root Guard
- Loop Guard

Port Fast

Рассмотрим ситуацию, изображенную на рисунке ниже. Коммутаторы SW1, SW2 и SW3 связаны несколькими линиями и нуждаются в STP-протоколе для предотвращения петель и балансирования нагрузки. Но порт Fa0/3 коммутатора SW1 не нуждается в STP-

протоколе так как он никогда не вызовет образования петли.



Если к порту коммутатора подключена рабочая станция или иное оконечное оборудование, то этот порт, разумеется, никогда не получит сообщения BPDU от другого коммутатора. Но STP-процесс, не зная об этом, все равно заставит этот порт выполнить все положенные по протоколу STP процедуры.

Но если на этом порте включена опция **Port Fast**, то он немедленно перейдет в передающий режим (forwarding), позволяя сразу включить рабочую станцию в сеть.

Опция Port Fast может использоваться совместно с протоколами STP (IEEE 802.1d) и PVST+.

Настройка Port Fast

По умолчанию опция Port Fast на коммутаторах Cisco отключена.

Если заранее известно, что к какому-то порту коммутатора будет подключен только компьютер, надо зайти в режим настройки этого интерфейса и выполнить команду:

spanning-tree portfast

Если это известно обо всех портах коммутатора, можно воспользоваться командой глобальной конфигурации:

spanning-tree portfast default

Если к порту коммутатора может быть подключен другой коммутатор, использовать Port Fast нежелательно – это оставит сеть без наблюдения за петлями коммутации. На транковых портах опция Port Fast включается следующей командой:

spanning-tree portfast trunk

BPDU Guard

В большой и разветвленной сети нельзя полностью исключить, что к интерфейсу, на котором включен режим Port Fast, будет случайно подключен коммутатор, что может привести к образованию петель коммутации. Застраховаться от этого позволяет опция **BPDU Guard**,

переводящая порты, на которых включен режим Port Fast в режим ErrDisable, если на этот порт придет сигнал BPDU.

Опция BPDU Guard может использоваться совместно с протоколами STP (IEEE 802.1d) и PVST+.

Настройка опции BPDU Guard

По умолчанию опция BPDU Guard на коммутаторах Cisco отключена.

Для включения опции BPDU Guard на коммутаторе надо войти в режим глобальной конфигурации и использовать команду:

spanning-tree portfast bpduguard default

При необходимости можно включить опцию BPDU Guard на отдельном порте коммутатора с помощью команды конфигурации интерфейса

spanning-tree bpduguard enable

в последнем случае порт при появлении сигнала BPDU будет отключен, даже если на этом порте режим Port Fast отключен.

BPDU Filtering

Порт коммутатора, даже находящийся в режиме Port Fast, может продолжать передавать сигналы BPDU. Чтобы избежать этого, можно использовать функцию BPDU Filtering.

Если на коммутаторе включена опция BPDU Filtering, то все порты, находящиеся в режиме Port Fast, не передают сигналы BPDU, которые и не нужны подключенным к ним рабочим станциям. Если такой порт получит сигнал BPDU, а это значит, что к нему подключили коммутатор, то этот порт выходит из режима Port Fast и отключает BPDU Filtering.

Если опция BPDU Filtering настроена не на коммутаторе в целом, а на конкретном интерфейсе, то соответствующий порт не передает сигналы BPDU даже если на нем не включен режим Port Fast. Подключение к такому порту другого коммутатора может, при наличии в сети избыточных линий, вызвать петлю коммутации.

Настройка опции BPDU Filtering

Опция BPDU Filtering может использоваться совместно с протоколами STP (IEEE 802.1d) и PVST+.

По умолчанию опция BPDU Filtering на коммутаторах Cisco отключена.

Для включения опции BPDU Filtering на коммутаторе надо войти в режим глобальной конфигурации и использовать следующую команду:

spanning-tree portfast bpdufilter default

При необходимости можно включить опцию BPDU Filtering на отдельном порте коммутатора с помощью следующей команды конфигурации интерфейса:

spanning-tree bpdufilter enable

UplinkFast

Если коммутатор связан с остальной сетью двумя или более линиями, то, согласно принципам STP, одна из этих линий будет работать, а остальные, резервные, блокируются. При отказе основной линии, одна из остальных будет разблокирована после длительной процедуры. Опция **UplinkFast** позволяет значительно сократить эту процедуру – при обнаружении отказа основной линии, резервная сразу, минуя состояния listening и learning, переходит в состояние forwarding.

Переключение с основной линии на резервную происходит за 1-5 секунд.

Опция UplinkFast срабатывает только при отказе линии, непосредственно подключенной к маршрутизатору.

Опция UplinkFast может использоваться совместно с протоколами STP (IEEE 802.1d) и PVST+.

Обычно опцию UplinkFast используют на коммутаторах уровня доступа для резервирования связи с уровнем распределения.

Настройка UplinkFast

Опция UplinkFast настраивается на коммутаторе в целом – в режиме глобальной конфигурации - и, соответственно, действует на все VLAN, существующие на этом коммутаторе:

spanning-tree uplinkfast [max-update-rate *пакетов_в_секунду*]

где необязательный параметр **max-update-rate** указывает скорость рассылки многоадресных пакетов в рамках процедуры выбора корневого коммутатора; по умолчанию max-update-rate равен 150 пакетов в секунду, но может быть задан в пределах 0..32000. Увеличение этого параметра способствует ускорению схождения STP, но увеличивает трафик.

BackboneFast

Если опция UplinkFast срабатывает при отказе линии, непосредственно подключенной к данному коммутатору, то опция BackboneFast ускоряет переход на резервную линию при разрыве линии, непосредственно к данному коммутатору не подключенной.

Коммутатор с включенной опцией BackboneFast анализирует сигналы BPDU и отслеживает ситуацию, когда другой коммутатор, подключенный к его блокированному порту, теряет связь с корневым. Тогда первый коммутатор, сохранивший связь с корневым, разблокирует свой порт, не дожидаясь истечения Aging Time.

Переключение с основной линии на резервную происходит примерно за 30 секунд.

Настройка BackboneFast

Опция BackboneFast может использоваться совместно с протоколами STP (IEEE 802.1d) и PVST+.

Опция BackboneFast включается в режиме глобальной конфигурации следующей командой:

spanning-tree backbonefast

EtherChannel Guard

Для увеличения пропускной способности сети несколько линий Ethernet иногда объединяют в EtherChannel. Опция EtherChannel Guard обнаруживает ошибки в конфигурации EtherChannel. Если на одном конце канала EtherChannel коммутатор настроен как EtherChannel, а на другом нет, или если параметры EtherChannel на концах канала различны, то опция EtherChannel Guard переводит соответствующие порты коммутатора в состояние ErrDisabled.

Чтобы включить опцию EtherChannel Guard надо войти в режим глобальной конфигурации и ввести команду

spanning-tree etherchannel guard misconfig

Опция EtherChannel Guard может использоваться совместно с протоколами STP (IEEE 802.1d), RSTP, MSTP, PVST+ и Rapid PVST+.

Root Guard

Опция Root Guard может быть полезна на стыке сетей, принадлежащих разным владельцам. Чаще всего ее используют в сетях провайдеров. Если наша сеть имеет связь с чужими коммутаторами, желательно, чтобы чужой коммутатор не стал в нашей сети корневым, так как на

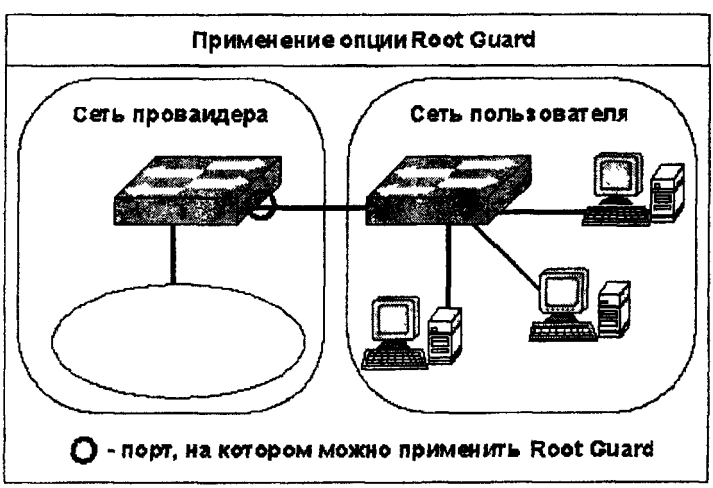
использование и настройки чужого коммутатора мы не можем повлиять и не можем отвечать за его надежность.

Опция Root Guard, настроенная на интерфейсах коммутатора, граничащих с чужой сетью, не дает чужому коммутатору стать корневым или даже быть частью пути к корневому коммутатору для нашей сети.

Опция Root Guard может использоваться совместно с протоколами STP (IEEE 802.1d), RSTP, MSTP, PVST+ и Rapid PVST+, но несовместима с опцией Loop Guard.

Чтобы включить опцию Root Guard надо войти в режим конфигурации соответствующего интерфейса и ввести команду

spanning-tree guard root



Loop Guard

Возможна ситуация, когда при нормально работающих интерфейсах сигналы BPDU не доходят до получателя

своевременно, например, из-за большого трафика в сети. В этом случае коммутатор, не получив вовремя на свой корневой порт сигнал BPDU, может решить, что связь с корневым коммутатором разорвана и, соответственно, разблокирует заблокированные до этого порты. Это может вызвать образование петли коммутации.

Опция Loop Guard обнаруживает эту ситуацию и не дает коммутатору включить резервные, заблокированные порты.

Настройка Loop Guard

Опция Loop Guard может использоваться совместно с протоколами STP (IEEE 802.1d), RSTP, MSTP, PVST+ и Rapid PVST+, но несовместима с опцией Root Guard.

Чтобы включить опцию Loop Guard надо войти в глобальной конфигурации и ввести команду

spanning-tree loopguard default

Опция Loop Guard наиболее эффективна, если настроена не на одном коммутаторе, а в коммутируемой сети в целом.

Общие рекомендации по использованию STP

Как уже говорилось в предыдущих разделах, лучше всего последовать правилу «один коммутатор – один VLAN» и возложить задачи резервирования, предотвращения петель и балансирования нагрузки на протоколы маршрутизации.

Если, по какой-то причине, это невозможно, а число VLAN на коммутаторе не превышает 128, следует использовать протокол Rapid PVST+.

Если число VLAN на коммутаторе очень велико, целесообразно использовать протокол MSTP.

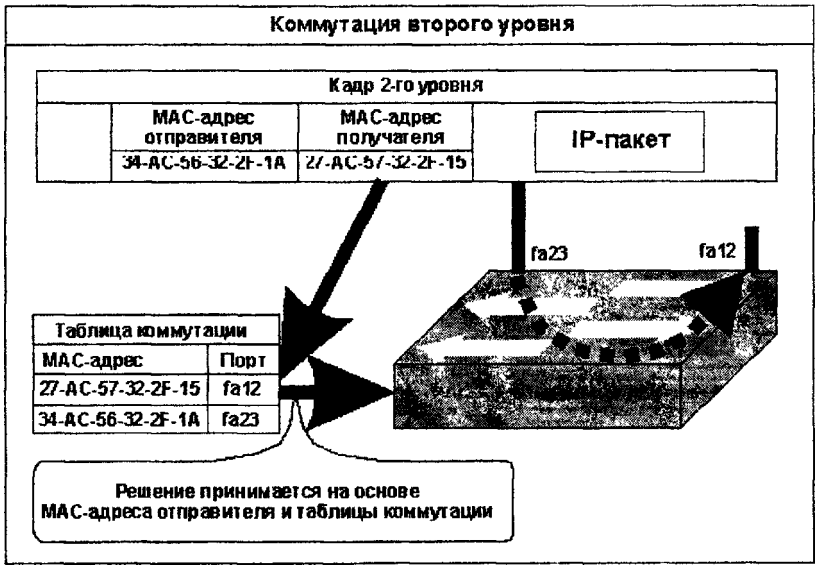
Если использование протоколов Rapid PVST+ или MSTP невозможно, следует использовать PVST+ - он включен по умолчанию – и настроить STP Toolkit.

3.3. Многоуровневая коммутация

Многоуровневая коммутация

Традиционно считается, что коммутация выполняется на втором – канальном – уровне модели OSI. При этом коммутатор анализирует заголовок кадра, содержащий MAC-адреса отправителя и получателя. По MAC-адресам отправителей формируется таблица коммутации, по таблице коммутации и MAC-адресу получателя принимается решение о передаче кадра на тот или иной порт коммутатора.

Достоинства такого подхода, прежде всего простота и дешевизна, способствуют его популярности и по сей день. Как показано в предыдущих разделах, коммутация второго уровня может применяться в кампусной сети предприятия, например, на уровне доступа.



В то же время, коммутации второго уровня присущи некоторые недостатки:

- При наличии избыточных связей необходимо использовать STP или RSTP, которые, несмотря на все усовершенствования, все же имеют большое время схождения.
- При коммутации не используется обширная информация, содержащаяся в заголовках сетевого и транспортного уровней.

Эти недостатки устраняются при использовании многоуровневой коммутации, поддерживаемой многими современными сетевыми устройствами.

При многоуровневой коммутации решение о передаче кадра на тот или иной порт принимается на основании

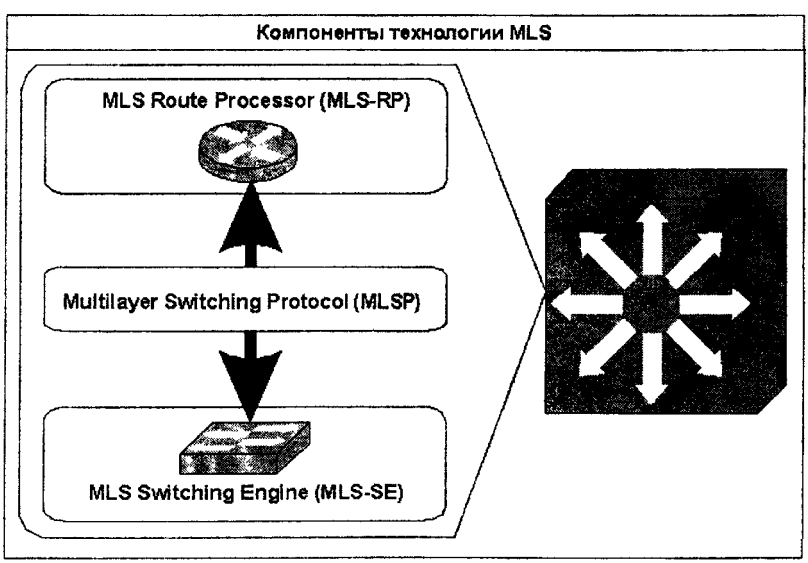
информации не только второго (канального) уровня, но также и на основе информации третьего (сетевого), а иногда и четвертого (транспортного) уровней.

В многоуровневых коммутаторах Cisco многоуровневая коммутация реализована в виде двух технологий:

- Multilayer switching (MLS);
- Cisco Express Forwarding.

Технология Multilayer switching (MLS)

Технология Multilayer switching впервые была использована на модульных коммутаторах Cisco Catalyst 5500 где реализовывалась в модуле RSM (Route Switch Module).



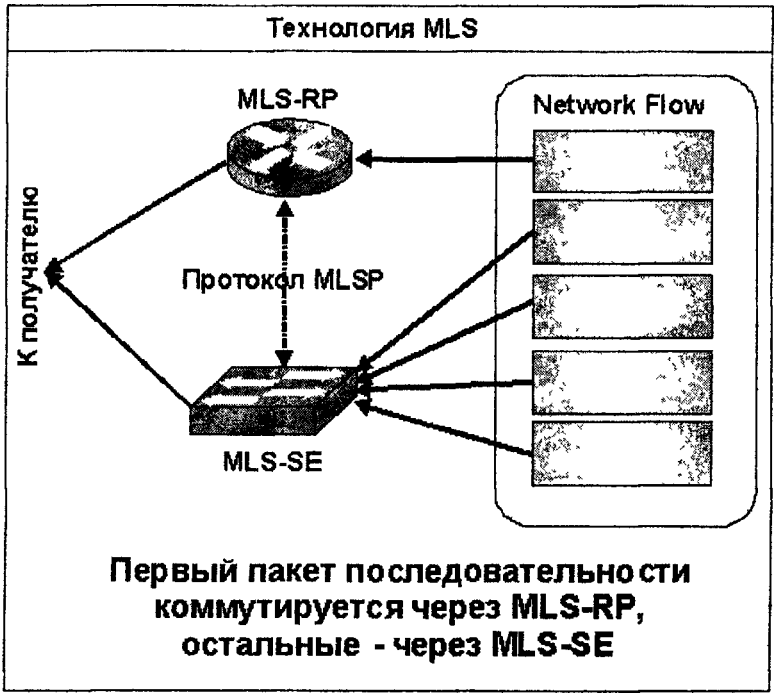
Перечислим основные компоненты технологии MLS.

- MLS Route Processor (MLS-RP) – маршрутизатор, обеспечивающий маршрутизацию между сетями на основании информации третьего, а иногда и четвертого уровня.
- MLS Switching Engine (MLS-SE): Коммутатор, задача которого – разгрузить MLS-RP.
- Multilayer Switching Protocol (MLSP): протокол для связи между MLS-RP и MLS-SE.

Технология MLS работает так: среди передаваемой информации MLS Route Processor выделяет последовательность пакетов (network flow), пересылаемых между источником и получателем. MLS-RP анализирует первый пакет этой последовательности и, на основании информации третьего, а иногда и четвертого уровня, определяет маршрут, который сообщает MLS-SE.

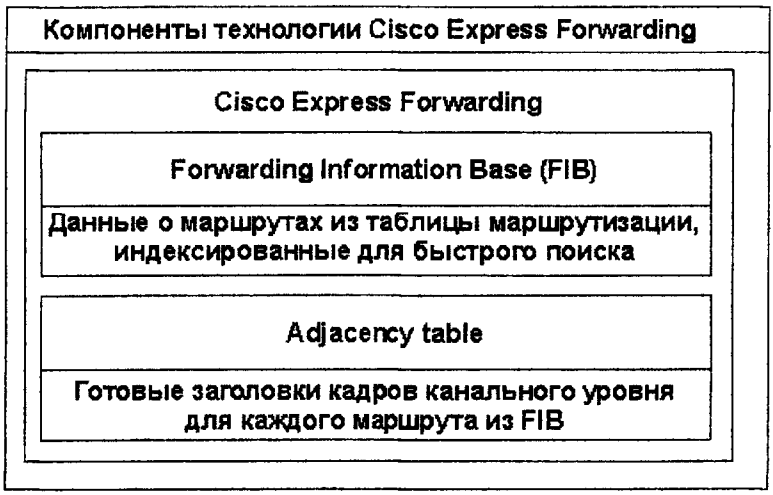
Последующие пакеты из этой последовательности коммутируются MLS-SE минуя MLS-RP.

Схематически функционирование технологии Multilayer Switching изображено на рисунке:

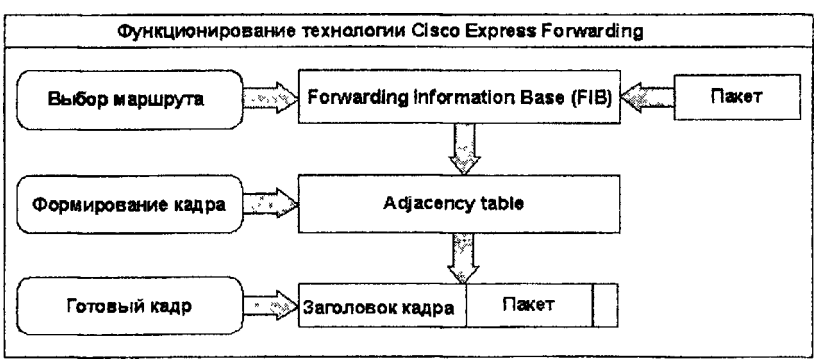


Технология Cisco Express Forwarding

Наиболее современной технологией многоуровневой коммутации является технология Cisco Express Forwarding, предусматривающая использование двух основных компонент: Forwarding Information Base (FIB) и Adjacency table.



Маршрут для коммутируемого пакета выбирается по данным FIB, это происходит быстро, благодаря индексации FIB. Затем из Adjacency table выбирается готовый заголовок кадра с MAC-адресом следующего скачка и формируется новый кадр, инкапсулирующий исходный пакет.

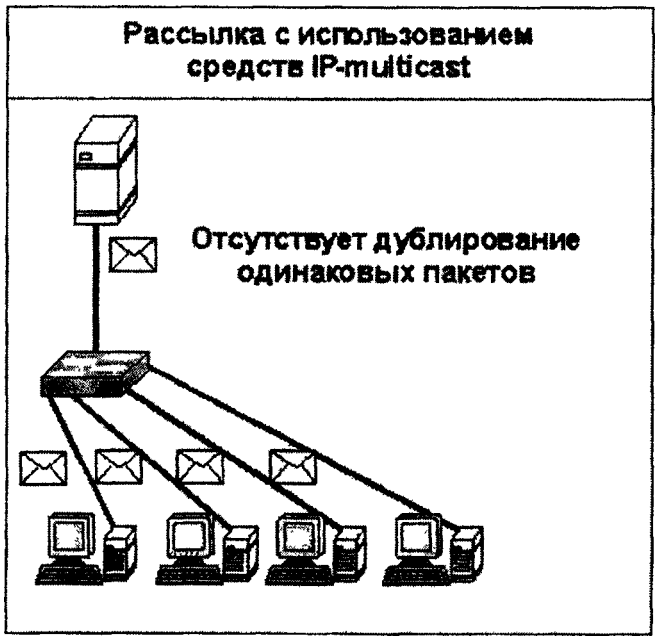


3.4. Средства обеспечения многоадресных рассылок

Средства обеспечения многоадресных рассылок

Необходимость в специальных средствах обеспечения многоадресных рассылок возникает, если необходимо доставить одну и ту же информацию нескольким получателям.

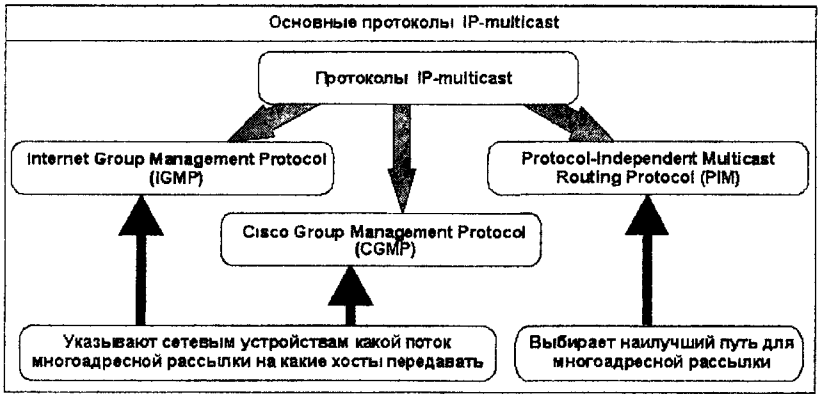
Технология IP multicast позволяет передавать многоадресную рассылку одним потоком по наиболее выгодному маршруту, дублируя пакеты лишь в точках разветвления маршрутов к разным получателям.



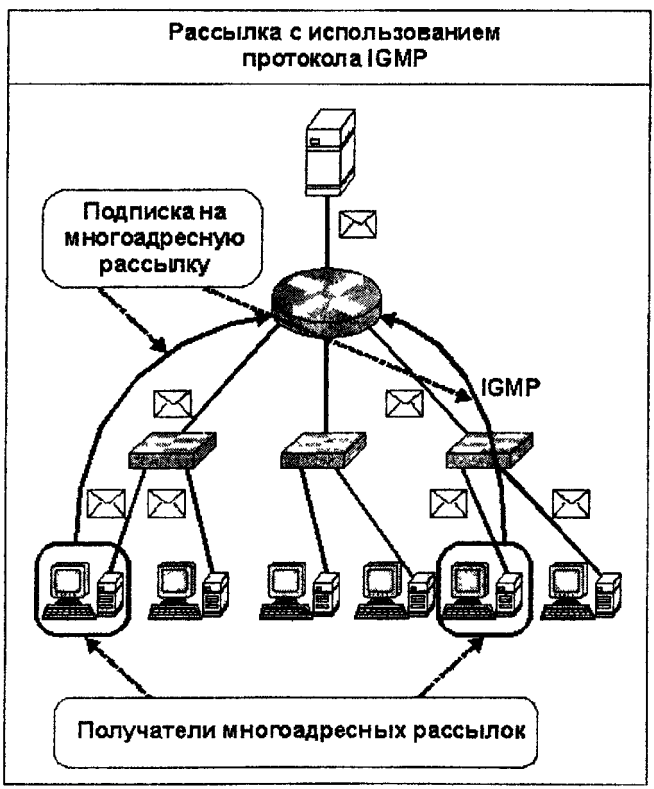
Получатели многоадресных рассылок объединяются в группы, идентифицируемые IP-адресом класса D (224.0.0.0 ... 239.255.255.255).

Технология IP multicast использует три основных протокола:

- Internet Group Management Protocol (IGMP)
- Cisco Group Management Protocol (CGMP)
- Protocol-Independent Multicast Routing Protocol (PIM)



Internet Group Management Protocol (IGMP)



Internet Group Management Protocol (IGMP) – протокол сетевого уровня, с помощью которого хост сообщает ближайшему маршрутизатору на какие многоадресные рассылки он подписан.

Теперь маршрутизатор знает, на какие интерфейсы рассылать многоадресные рассылки.

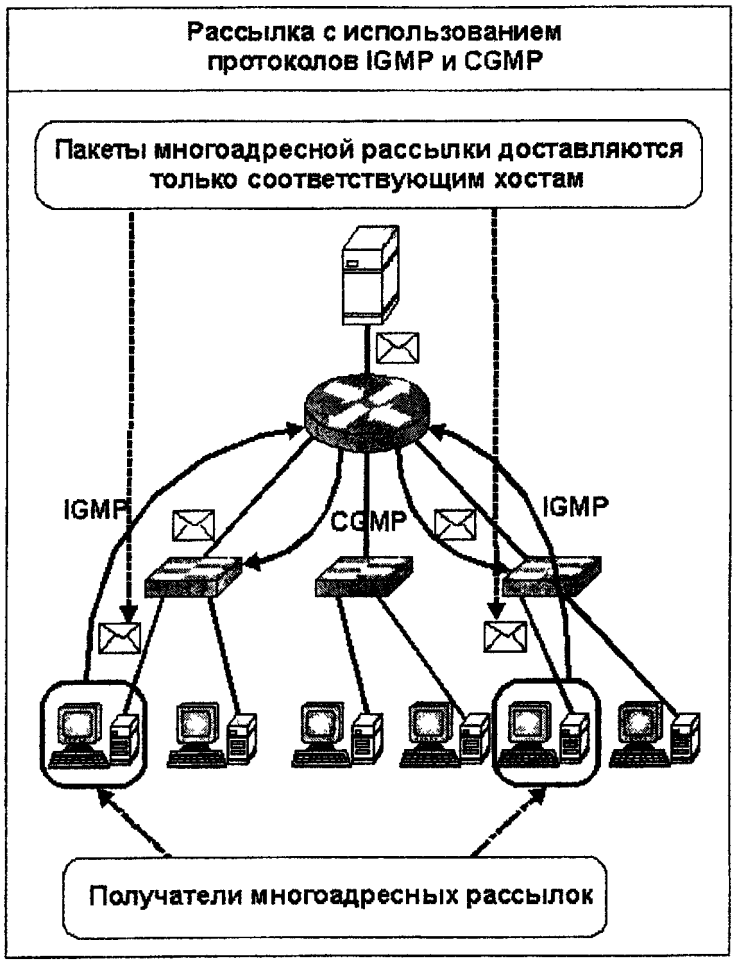
Cisco Group Management Protocol (CGMP)

На предыдущем рисунке показано, что коммутаторы разошлют пакеты многоадресной рассылки и тем хостам, которые на нее не подписаны. Этот недостаток исправляется протоколом CGMP (Cisco Group Management Protocol), с помощью которого маршрутизатор сообщает непосредственно подключенному к нему коммутатору о хостах, подписавшихся по протоколу IGMP на многоадресные рассылки.

Protocol-Independent Multicast Routing Protocol (PIM)

Для маршрутизации пакетов многоадресных рассылок используется Protocol-Independent Multicast Routing Protocol (PIM). В отличие от обычных протоколов маршрутизации, таких как RIP или EIGRP, протокол PIM не получает

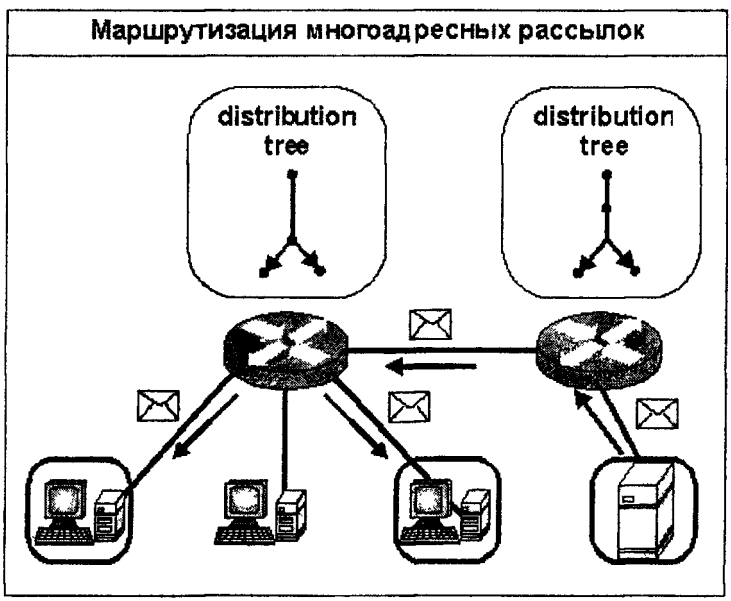
маршрутную информацию от соседей, а использует имеющуюся на маршрутизаторе таблицу маршрутизации.



Зная, какие многоадресные рассылки проходят через этот маршрутизатор, зная адреса их источников и получателей, протокол PIM, с помощью таблицы

маршрутизации, вычисляет «дерево распределения» (distribution tree) от источников многоадресных рассылок к их получателям и, благодаря этому, знает на какие интерфейсы передать очередной пакет многоадресной рассылки.

Использование протокола PIM схематически изображено на рисунке:



3.5. Средства обеспечения QoS

Качество обслуживания (Quolity of Service)

Устойчивая работа сети зависит не только от надежности оборудования и наличия резервных устройств

и маршрутов, но и возможности обеспечить обработку пользовательских данных в требуемом темпе, не превышая допустимого времени задержки, не допуская большой вариации задержки и предотвращая образования «пробок» в «узких» местах сети. Эта задача решается специальным механизмом QoS (Quolity of Service - Качество обслуживания).

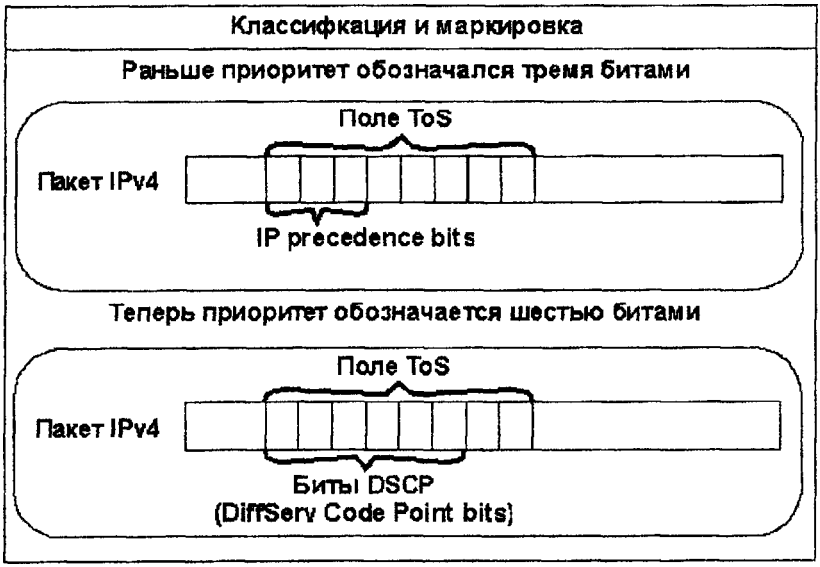
Основные компоненты QoS:

- Классификация и маркировка
- Регулирование заторов
- Уменьшение трафика за счет буферизации
- Уменьшение трафика за счет удаления фреймов

Классификация и маркировка (Classification and marking)

При использовании этого механизма каждому пакету присваивается определенный приоритет, например, пакет с очередным кадром видеотрансляции будет иметь более высокий приоритет, чем пакет с текстом.

Для маркировки обычно используют поле ToS (Type of Service – тип сервиса) в заголовке пакета протокола сетевого уровня IPv4.



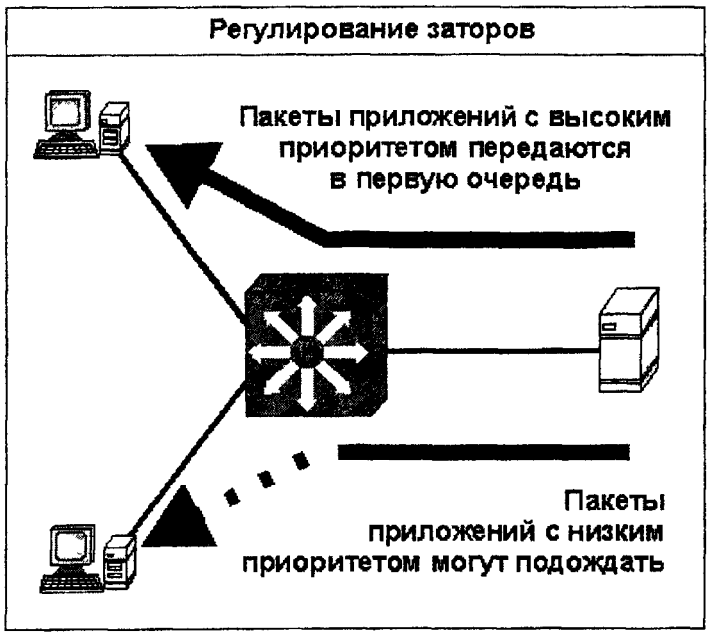
Регулирование заторов (Congestion management)

В случае возникновения затора, сетевое устройство определяет очередность передачи пакетов в соответствии с их приоритетом. Это позволяет даже в случае затора обеспечивать требуемое качество обслуживания для приложений, наиболее критичных к задержкам и вариации времени задержки.

Процесс регулирования заторов состоит из двух компонент:

Queuing – пакеты распределяются по нескольким буферам, в зависимости от уровня приоритета;

Scheduling – определяется очередность передачи из различных буферов.



Уменьшение трафика за счет буферизации и удаления пакетов (Traffic Policing and Shaping)

Возникновение затора, может быть предотвращено за счет использования механизмов удаления низкоприоритетных пакетов и использования буферизации:

- **Traffic Policing** – проверяет биты CoS и DSCP, или IP-precedence и, затем, или пропускает пакет, или удаляет его, или пропускает, но меняет в пакете значение приоритета согласно заданному критерию.

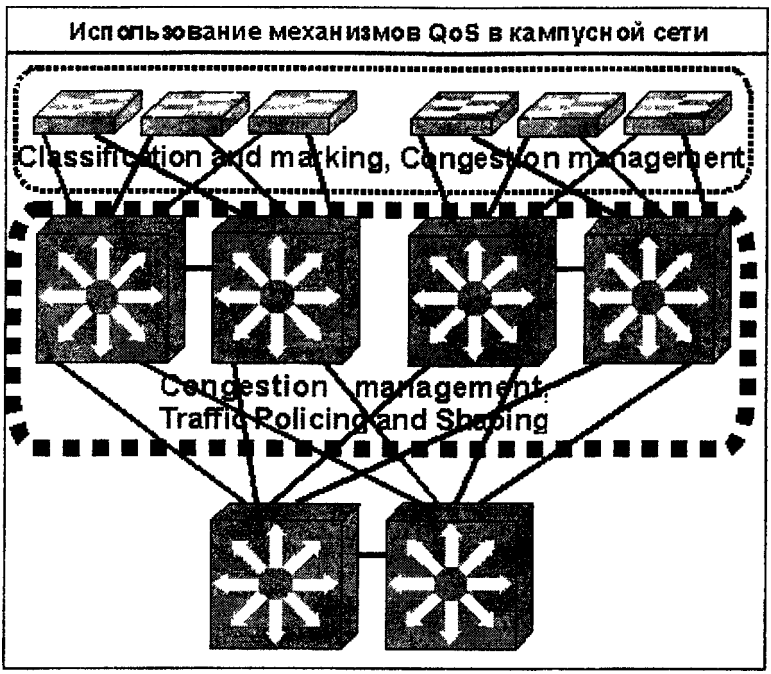
- **Traffic Shaping** – сглаживает пиковые нагрузки за счет временного помещения части пакетов в буфер.

В кампусной сети предприятия механизмы QoS обычно используют так:

На **уровне доступа**, там, где пакеты создаются, выполняется их классификация и маркировка. Здесь же используется механизм Congestion management, при этом коммутаторы второго уровня определяют приоритет только по заголовку кадра – информации второго уровня, например, номеру порта, тогда как многоуровневые коммутаторы могут использовать биты DSCP и другую информацию третьего уровня.

На **уровне распределения** применяются многоуровневые коммутаторы или маршрутизаторы, что позволяет полноценно использовать средства Congestion management. На этом же уровне применяются механизмы Traffic Policing и Traffic Shaping.

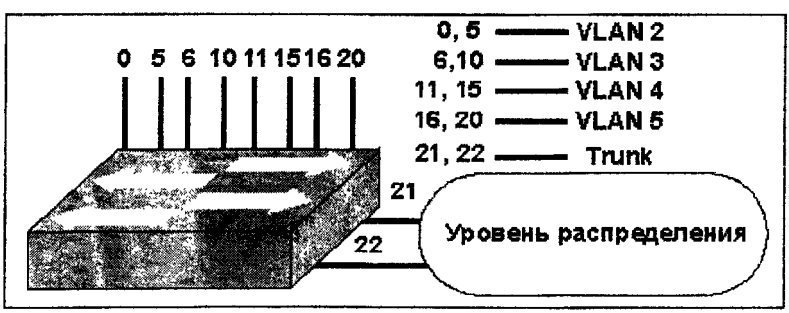
На **уровне ядра** кампусной сети выполнение любых операций, связанных с распаковкой пакета и анализом его содержимого, нежелательно, так как снижает скорость работы ядра и сети в целом.



3.6. Примеры и упражнения

Пример 3.1.

Настройка протокола MSTP



Задача

Настроить протокол MSTP на данном коммутаторе.

Установить следующие параметры:

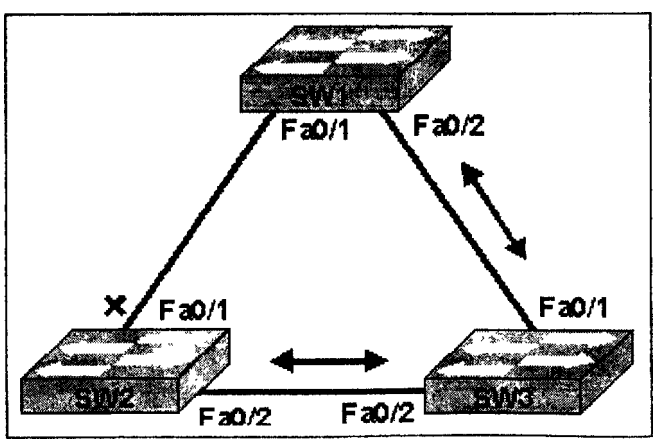
- Имя региона: region2
- Номер ревизии 1
- Обеспечить балансировку нагрузки, сделать этот коммутатор корневым для VLAN 2 и VLAN 3

Решение

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 2,3
Switch(config-mst)# instance 2 vlan 3,4
Switch(config-mst)# name region2
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Switch(config-mst)# exit
Switch(config)# spanning-tree mst 1 root primary
```

Пример 3.2.

Просмотр настроек STP на коммутаторе



Узнаем настройки STP на коммутаторе SW2:

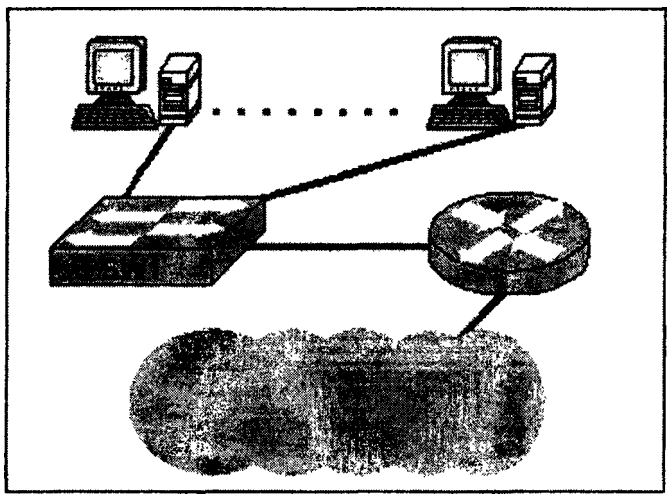
```
SW2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0004.9AB9.6399
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0060.3E1C.B202
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Altn BLK 19        128.3    Shr
Fa0/2            Root FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr

SW2#
```

Из листинга видно, что порт Fa0/1 блокирован как альтернативный маршрут (Altn BLK), порт Fa0/2 является корневым и находится в передающем режиме (Root FWD), а порт Fa0/3 – назначенный и, также, находится в передающем режиме (Desg FWD 19)

Пример 3.3.

Настройка режима Port Fast на коммутаторе

Рассмотрим сеть, изображенную на рисунке:



Отметим, что в данном случае почти ко всем портам коммутатора подключены компьютеры, а единственное соединение с маршрутизатором не оставляет места для образования петель коммутации.

Вывод: можно настроить режима Port Fast в качестве режима по умолчанию для всех портов коммутатора.

SW1> enable

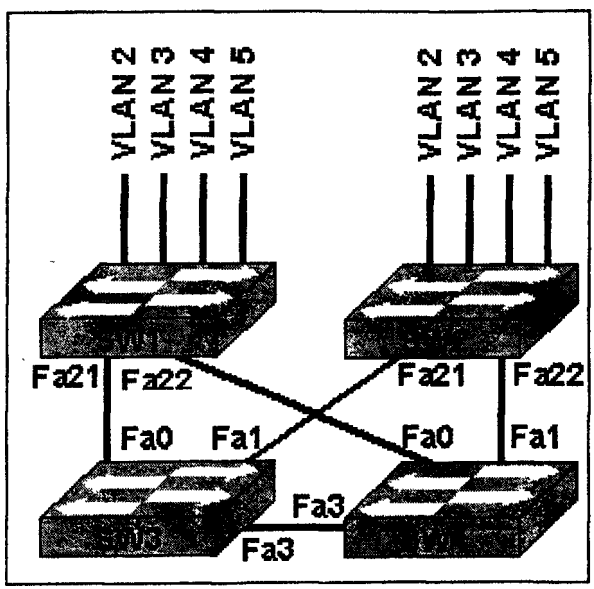
SW1# configure terminal

SW1(config)# spanning-tree portfast default

Задания

Задание 3.1.

В сети, изображенной на рисунке, настроить протокол MSTP. Сделать коммутатор SW3 корневым для VLAN 2,4, а коммутатор SW4 корневым для VLAN 3,5. Покажите листинг настройки преподавателю.



Задание 3.2.

Выполните следующие действия:

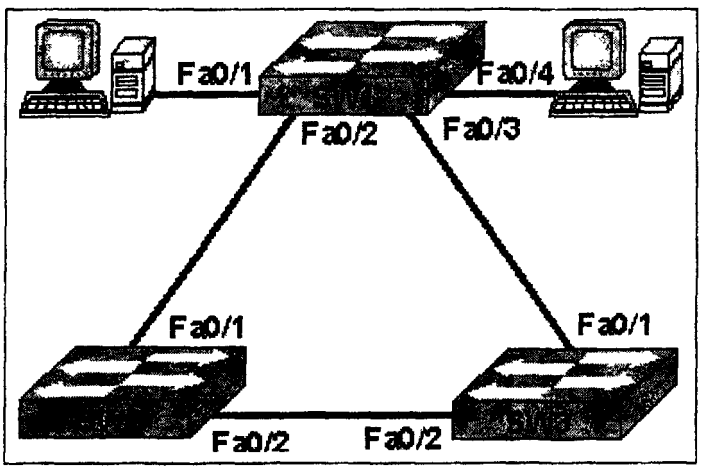
1) Отключить STP-процесс для VLAN 52,

2) Включить STP-процесс для VLAN 132.

Покажите преподавателю листинг настройки. Ответьте, для чего могут потребоваться такие действия, если на коммутаторе настроен протокол Rapid PVST+?

Задание 3.3.

Выполните следующие действия:



Настройте на коммутаторе SW-1опции Port Fast, UplinkFast и BackboneFast. Покажите преподавателю листинг настройки.

4. Глоссарий.

Campus – в данном случае, кампусная сеть – сеть, охватывающая одно или несколько близко расположенных зданий. Один из модулей Cisco SONA.

Data center - крупный центр обработки данных, соединенный с кампусной сетью предприятия через граничный модуль. Один из модулей Cisco SONA.

E-commerce – электронная торговля - обобщенное название торговых операций, проводимых с использованием компьютерных сетей. Модуль E-commerce - один из модулей Cisco SONA.

Enterprase Edge – граничный модуль - один из модулей Cisco SONA, контролирующий внешние связи.

Fast Ethernet – стандарт канального уровня на технологию локальных сетей, обеспечивающая передачу данных со скоростью до 100 Мб/сек.

EIGRP – современный протокол маршрутизации – относится к бесклассовым гибридным протоколам.

Frame Relay – стандарт канального уровня на технологию сетей с коммутацией пакетов.

Ethernet – группа стандартов канального и физического уровня, описывающих технологии LAN с доступом к среде передачи данных по принципам CSMA/CD. Собственно Ethernet обеспечивает передачу данных со скоростью до 10 Мб/сек.

Ethernet/Fast Ethernet/Gigabit Ethernet-порт – интерфейс сетевого устройства, например, коммутатора, снабженный разъемом RJ-45 и обеспечивающий подключение витой пары по технологии Ethernet или Fast Ethernet или Gigabit Ethernet.

FTP – File Transfer Protocol – протокол передачи файлов – одна из служб Internet.

Gigabit Ethernet – стандарт канального уровня на технологию локальных сетей, обеспечивающая передачу данных со скоростью до 1000 Мб/сек.

IGRP – протокол маршрутизации – относится к классовым дистанционно-векторным протоколам.

Internet Connectivity Module – элемент Enterprase Edge - модуль подключения к таким службам глобальной сети Internet, как HTTP, FTP, Simple Mail Transfer Protocol (SMTP), и DNS.

LAN – Local Area Network – локальные сети – сети, охватывающие офис или предприятие на ограниченной площади.

MAN – Metropoliten Area Network – городские сети – сети, охватывающие крупный мегаполис или регион и занимающие промежуточное положение между WAN и LAN.

OSPF - современный протокол маршрутизации – относится к бесклассовым протоколам состояния канала.

QoS – Qality of Service – комплекс протоколов, обеспечивающих доставку пакетов с заданным качеством.

PoE – Power over Ethernet – технология передачи электропитания вместе с данными по линиям Ethernet

RIP – протокол маршрутизации – относится к классовым дистанционно-векторным протоколам.

Route Table – таблица маршрутизации – хранится на маршрутизаторе и содержит маршруты до всех известных ему сетей.

Server farm – серверная ферма – небольшой центр обработки данных, входящий непосредственно в состав кампусной сети.

SONA - Cisco Service-Oriented Network Architecture, Cisco SONA - типовая структура модульной сети предприятия, предложенная компанией Cisco systems.

StackWise – технология, позволяющая объединить несколько стековых коммутаторов в один.

VLSM – variable lenth subnet mask – использование разных масок для разных подсетей.

VPN – Virtual Private Network – виртуальная частная сеть – группа протоколов, организовать передачу зашифрованных сообщений через Internet.

WAN – World Area Network – глобальные сети – сети, охватывающие большие территории, сопоставимые с размером государства или континента.

Бесклассовый протокол – протокол маршрутизации, при использовании которого каждый маршрутизатор сообщает соседям маски известных ему сетей. Это позволяет использовать разные маски для разных подсетей.

Гибридный протокол маршрутизации - протокол маршрутизации, сочетающий особенности дистанционно-векторных протоколов и протоколов состояния канала.

Дистанционно-векторный протокол - протокол маршрутизации, представляющий маршрут до заданной сети в виде дистанции (количество хопов, задержка и т.д.) и вектора (на какой интерфейс маршрутизатора передавать пакет в эту сеть).

Кампусная сеть – сеть, охватывающая одно или несколько близко расположенных зданий.

Коммутатор второго уровня – обычный коммутатор, выполняющий коммутацию на основании информации второго уровня модели OSI, содержащейся в заголовке кадра.

Классовый протокол – протокол маршрутизации, при использовании которого каждый маршрутизатор не сообщает соседям маски известных ему сетей. При этом маска подсети определяется по классу IP-адреса.

Многоуровневый коммутатор – коммутатор, выполняющий коммутацию на основании информации второго, третьего, а иногда и четвертого уровня модели OSI.

Модульный коммутатор – коммутатор, состоящий из шасси и нескольких модулей, обеспечивающих коммутацию, управление и электропитание.

Серверная ферма – небольшой центр обработки данных, входящий непосредственно в состав кампусной сети.

Статический маршрут – маршрут, записанный администратором вручную в таблицу маршрутизации маршрутизатора.

Стековый коммутатор – коммутатор, который можно соединить с другими стековыми коммутаторами в единый коммутатор.

Протокол состояния канала - протокол маршрутизации, при котором каждый маршрутизатор представляет себе структуру сети и вычисляет маршрут до заданной сети.

Литература

1 Я.М. Голдовский Введение в сетевые технологии Cisco. Электронное учебное пособие. МИИТ, 2005 г.

2 Б.В. Желенков Использование сетевого оборудования Cisco. Электронное учебное пособие. МИИТ, 2005 г.

3 В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы. 3_е издание. – СПб.: Питер, 2006.

4 Основы организации сетей Cisco, том1.: Пер. с англ. – М. Издательский дом «Вильямс», 2002.

5 Основы организации сетей Cisco, том2.: Пер. с англ. – М. Издательский дом «Вильямс», 2004.

6 Создание масштабируемых сетей Cisco.: Пер. с англ. – М. Издательский дом «Вильямс», 2004.

Св. план 2009 г., поз.71

Голдовский Яков Михайлович

ПРОЕКТИРОВАНИЕ КАМПУСНЫХ СЕТЕЙ

Учебное пособие

Подписано к печати 29.12.09. Формат 60 x 84 1/16

Тираж 100 экз. Заказ – 868.

Усл.-печ. л. – 8,25.

127994, Москва, ул. Образцова, 9, стр. 9
Типография МИИТа