**Уроки по Cisco с сайта** <http://alexsplanet.blogspot.com/>

**Что такое CISCO?**



Привет всем! В наши дни очень сложно представить свою жизнь без интернета. Он помогает нам общаться, делится своими фотографиями с друзьями, выкладывать видео файлы и находить необходимую нам информацию. Поэтому сетевые технологии в наши дни приобретают все большую популярность. И одним из лидеров в разработке сетевого оборудования на сегодняшний день является компания CISCO.

В 1984 году Сэндли Лернер и Лен Бозак объединили усилия для решения задачи совместимости компьютеров школы бизнеса и инженерного факультета Стенфордского университета. Таким образом они создали свои первые маршрутизаторы. Благодаря этому студенты школы бизнеса получили возможность обмениваться информацией. Естественно через некоторое время в двери Лернера и Бозака начали стучаться другие владельцы компьютеров, нуждавшиеся в коммуникационном оборудовании.

Так что такое CISCO сегодня? Сегодня CISCO - это компания, которая является лидером в области разработки и продажи сетевого оборудования. Около 80% всех маршрутизаторов, которые являются основой интернета, представлены маршрутизаторами CISCO. В настоящий момент CISCO поставляет сетевое оборудование для предприятий, провайдеров, небольших предприятий и для дома. Ниже приведен список оборудования и программного обеспечения.

Список оборудования:

* Datacenter products: Nexus Switches (1000v, 2000, 4000, 5000, 7000), MDS, Unified Computing System (UCS)
* Cisco SPA500 Series IP Phones
* Linksys SPA900 Series IP Phones
* Cisco Unified IP Phones (7945, 7965, 7942, 8900 series, 9900 series, 6900 series)
* Cisco Application Control Engine (ACE): Application Delivery Controller
* Routers, including: 837, 1000 Series, 2500 Series, 7600, 12000, 3600 Series, ASR Series and CRS-1 and CRS-3
* Cisco Security Manager
* Security appliances: ASA 5500, PIX 500 series
* Unified Computing: Cisco Unified Computing System (UCS) virtual server platform: with VMWare virtualization system run servers on Cisco hardware[40]
* Catalyst switches: Cisco Catalyst 2900 Series, Cisco Catalyst 3000 Series, Catalyst 4500, Cisco Catalyst 6500 Series
* Collaboration systems such as Cisco TelePresence, Cisco Manufacturing Mobile Video Collaboration with Librestream, Cisco acquired Tandberg, the world leader in Telepresence systems[41]
* VOIP: Wireless IP Phone 7920
* CLEO: Low Earth Orbit router
* Cisco Wireless LAN
* Cisco Cius: a new Android-based collaboration tablet
* Cisco Wide Area Application Services (WAAS)
* Set Top Boxes (High Definition PVRs)- Cable/IP

Список программного обеспечения:

* Internetwork Operating System (IOS)
* NX-OS
* IOS-XR
* Cisco Active Network Abstraction
* Cisco Fabric Manager
* Cisco AnyConnect Secure Mobility Client
* Cisco Systems VPN Client
* CiscoView
* Data Center Management and Automation – Cisco Intelligent Automation
* Cisco Tidal Enterprise Scheduler
* CiscoWorks Network Management software
* Clean Access Agent, Cisco NAC Appliance
* Cisco Eos
* Packet Tracer, didactic network simulator
* Cisco Network Magic Pro
* Cisco Unified Communications Manager
* Cisco Unified Operations Manager (CUOM) – is a NMS for voice. It features real-time monitoring of all system elements, and performs automatic discovery for the entire system and provides contextual diagnostics for troubleshooting.
* Cisco IP Communicator
* Cisco Quad
* Cisco Security Manager
* WebEx Collaboration Tools

Так же компания CISCO обладает достаточно разветвленной системой сертификации. Существует 5 сертификационных уровней: Entry, Associate, Professional, Expert, and recently Architect, так же как и 8 специализаций: Routing & Switching, Design, Network Security, Service Provider, и недавно появившиеся Service Provider Operations, Storage Networking, Voice, and Wireless. Не секрет, что системные инженеры CISCO сегодня пользуются большим спросом на рынке труда и их труд хорошо оплачивается. В настоящий момент существует большое количество курсов, посвященных сетевым технологиям и конфигурированию сетевых устройств CISCO. Все эти курсы довольно дорогостоящие, поэтому я решил создать данный видео-блог и поделится с вами своими знаниями в области конфигурированияустройств CISCO.

**Введение в CISCO IOS**

Cisco IOS - операционная система, на которой работают маршрутизаторы CISCO. Для начала я опишу основные команды командной строки:

enable - вход в привилегированный режим.

show running-config - показывает текущую настройку роутера.

ping - проверяет связь с заданным сетевым устройством.

configure terminal - вход в режим конфигурирования.

show version - показывает версию операционной системы и различные системные ресурсы.

? - показывает все доступные команды в текущем режиме.

write mem - записать текущую конфигурацию в стартовую.Cisco IOS - операционная система, на которой работают маршрутизаторы CISCO. Для начала я опишу основные команды командной строки:

1. enable - вход в привилегированный режим.

2. show running-config - показывает текущую настройку роутера.

3. ping - проверяет связь с заданным сетевым устройством.

4. configure terminal - вход в режим конфигурирования.

5. show version - показывает версию операционной системы и различные системные ресурсы.

6. ? - показывает все доступные команды в текущем режиме.

7. write mem - записать текущую конфигурацию в стартовую.

**Установка пароля.**

Подключаемся к нашему роутеру с помощью HyperTerminal(Start-> Programs-> Accessories->Communications->HyperTerminal). Перед нами появляется командная строка. Далее путем нижеприведенных команд мы установим пароль на вход по терминальным и виртуальным линиям (с консольного порта и по telnet соответственно):

Router>enable

Router#configure terminal

Router(config)#service password-encryption

Router(config)#line con 0

Router(config-line)#password alexs

Router(config-line)#login

Router(config-line)#exit

Router(config)#line vty 0 4

Router(config-line)#password planet

Router(config-line)#login

Router(config-line)#exit

Router(config)#enable secret alexsplanet

Примечание:

1. Пароль alexs - вход с консольного порта.
2. Пароль planet - вход по telnet.
3. Пароль alexsplanet - вход в привелигированный режим.

**Конфигурирование интерфейса**

Если внимательно посмотреть на сетевое оборудование с тыльной стороны, то можно заметить, что каждый порт обазначен( например fa0/0, serial0/1 ). Сейчас я вам покажу как на порт fa0/0 повесить IP адрес:

Router>enable

Router#configure terminal

Router(config)#interface fa0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

**Настройка DHCP**

Каждое устройство в сети должно иметь свой IP адрес. Системный администраторы дают статические адреса маршрутизаторам, серверам, принтерам и другим сетевым устройствам адрес которых должен быть постоянным. Так же можно и всем пользовательским компьютерам назначить статические IP адреса, но если пользователи постоянно перемещаются, то вам придется постоянно менять их адреса. Чтобы автоматизировать процесс выдачи IP адресов был придумал протокол DHCP, который динамически назначает IP адрес устройства. Сейчас я расскажу как на маршрутизаторе CISCO настроить DHCP сервер:

1. Исключаем все статические адреса(адреса маршрутизатов и серверов).
2. Конфигурируем DHCP пул.
3. Конфигурируем особенности DHCP пула(указываем имя домена, шлюз по умолчанию).

Вот конфигурация:

R1>enable

R1#configure terminal

R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9

R1(config)#ip dhcp excluded-address 192.168.10.254

R1(config)#ip dhcp pool LAN-POOL-1

R1(dhcp-config)#network 192.168.10.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.10.1

R1(dhcp-config)#domain-name alexsplanet.com

R1(dhcp-config)#end

Примечание:

1. Исключенные адреса - 192.168.10.1 - 192.168.10.9, 192.168.10.254
2. Имя пула - LAN-POOL-1
3. Сеть - 192.168.10.0 255.255.255.0
4. Шлюз по умолчанию - 192.168.10.1
5. Домен - alexsplanet.com

**Конфигурирование статической маршрутизации**

Основной функцией маршрутизаторов является маршрутизация информации из одной сети в другую. В маршрутизаторах есть таблица маршрутизации, соответственно которой маршрутизируются данные устройством. В настоящее время существует два способа задания данной маршрутизации:

1. Протоколы маршрутизации.
2. Статическая маршрутизация.

Протоколы маршрутизации позволяют маршрутизаторам динамически узнавать информацию о путях из одной сети в другую. Вот некоторые из них - RIP, EIGRP, BGP, OSPF, IS-IS.

Во время статической маршрутизации администратор вручную прописывает пути из одной сети в другую. Именно о статической маршрутизации рассказывается в данном уроке.

И так для того, чтобы вручную прописать маршрут из одной сети в другую в маршрутизаторах CISCO есть команда "ip route". Синтаксис этой команды следующий:

ip route (destination ip network address) (mask) (interface/next hop ip address).

В случае, если маршрутизатор не может найти в своей таблице маршрутизации необходимой записи и не знает ничего о сети в которую необходимо направить данные, то тогда роутер отправляет данные на шлюз по умолчанию. Для того, чтобы задать шлюз по умолчанию используется следующая команда:

 ip route 0.0.0.0 0.0.0.0 (interface/ next hop ip address).

Для того, чтобы посмотреть таблицу маршрутизации, в CISCO используется команда "show ip route".

Ниже приведена конфигурация маршрутизатора, в котором задана статическая маршрутизация:

Router>enable

Router#configure terminal

Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2

Router(config)#ip route 192.168.3.0 255.255.255.0 fa0/0

Примечание:

* 192.168.1.2 - является шлюзом по умолчанию для нашего маршрутизатора.

**Настройка RIP**

RIP - один из самых первых протоколов маршрутизации, но он до сих пор используется в небольших сетях. В настоящий момент существуют две версии данного протокола. В качестве метрики используется количество переходов до нужной сети(максимальное количество переходов-15). По умолчанию маршруты обновляются каждые 30 секунд. Обновления таблицы маршрутизации отправляются только соседним маршрутизаторам. Протокол RIP версии 1 поддерживает только сети со стандартной маской сети, то есть сети класса A, B, C. RIP версии 2 в свою очередь поддерживает сети в которых используются не стандартные маски. Так же RIP версии 2 поддерживает аутентификацию.

И так, для того чтобы войти в режим конфигурирования RIP необходимо набрать команду "router rip". Далее с помощью команды "version (1|2)" можно указать какую версию протокола вы настраиваете для данного маршрутизатора(я советую всегда использовать RIP v2, так как он включает функции и RIP v1). Затем с помощью команд "network (адрес сети)" задаются те напрямую подключенные к маршрутизаторы сети, которые маршрутизатор должен объявлять для других маршрутизаторов в вашей сети.

Основные команды:

* router rip - вход в режим конфигурирования rip;
* version(1|2) - версия протокола;
* network (ip address) - адрес сети;
* show ip route - отображение таблицы маршрутизации;
* debug ip rip - включение режима отладки работы протокола RIP.

Пример конфигурации:

Router(config)#router rip

Router(config-router)#network 192.168.3.0

Router(config-router)#network 192.168.5.0

Router(config-router)#network 192.168.1.0

**Настройка EIGRP**

В первые годы существования компьютерных сетей, RIP был королем протоколов маршрутизации. Но по мере роста сетей, сети, достигнувшие предела в 15 переходов установленного RIP, требовали отмены этого ограничения. Поэтому стали разрабатывать другие протоколы маршрутизации. И в данном уроке мы с вами поговорим о протоколе маршрутизации EIGRP.

В отличие от RIP, который использует в качестве мертрики количество переходов, протокол маршрутизации EIGRP использует следующие параметры:

1. Межсетевая задержка
2. Пропускная способность
3. Нагрузка
4. Надежность

На основании данных параметров вычисляется метрика маршрута.

Маршрутизаторы EIGRP, как и RIP-маршрутизаторы, периодически посылают обновления своих таблиц маршрутизации непосредственно связанным с ними соседями, но расписание отправки существенно отличается. Обновления посылаются каждые 90 секунд, в отличие от 30 секунд в RIP. Если обновление не пришло в течение 270 секунд, то маршрут помечается как неактивный. Если обновление не пришло после 630 секунд, то маршрут удаляется из таблицы. Так же можно поменять таймеры обновлений с помощью команды "timers basic".

И так для того, чтобы войти в режим конфигурирования eigrp, необходимо набрать команду "router eigrp {номер автономной системы(АС)}". АС можно рассматривать как набор сетей или сред с общим элементов маршрутизации. К автономным системам можно обращаться как к самостоятельным объектам, адресуя данные целой сети. На данном этапе вам возможно не совсем будет понятно назначение автоновных сетей, но позже, когда мы перейдем к протоколам маршрутизации внешнего шлюза, например BGP, то вам все сразу станет понятно.

Далее с помощью команды network {ip address} {EIGRP wild card bits} задается сеть, которая непосредственно подключена к маршрутизатору и о существовании которой наш маршрутизатор будет сообщать своим соседям. EIGRP wild card bits = 255.255.255.255-(маска сети). Так же с помощью команды "passive-interface" можно указать порт, в который маршрутизатор не должен отправлять обновленную таблицу маршрутизации.

Пример конфигурации:

Router(config)#router eigrp 200

Router(config-router)#network 192.168.1.0 0.0.0.255

Router(config-router)#network 192.168.2.0 0.0.0.3

**Сертификация CISCO**

Было бы упущением не упомянуть тему сертификации CISCO. Поэтому я решил коротко написать какие сертификации существуют у CISCO.

Экзамены принимаются центром тестирования Pearson VUE.

Существует 4 уровня сертификации:

1)Entry.

2)Associate.

3)Professional.

4)Expert.

Сертификация уровня Assosiate

Cisco Certified Network Associate (CCNA)

Кандидат на статус CCNA должен сдать два экзамена (ICND1 640—822 и ICND2 640—816), или один тест CCNA 640—802.

Сертификат действителен в течение трёх лет. Для сохранения сертификата CCNA по истечении 3х лет обладатель сертификата CCNA должен выполнить одно из 3х условий:

1)пересдать CCNA или ICND

2)сдать экзамен на один из профессиональных сертификатов (Professional Level) (в том числе CCNP)

3)сдать письменный экзамен CCIE.

В рамках сетевой академии Cisco, учебные курсы CCNA и CCNP проводятся в более чем 150 странах мира в рамках традиционных учебных заведений.Студенты Сетевой Академии Cisco могут получить ваучер, дающий право сдачи экзамена со скидкой в 80 %. Стоимость экзамена 250$ за CCNA или по 125$ за ICND1 и ICND2.

Cisco Certified Design Associate (CCDA)

Обладатели статуса CCDA способны разрабатывать дизайн коммутируемой или маршрутизируемой сети, состоящей из LAN'ов, WAN'ов и различных сервисов. Cертификат CCNA не обязателен для получения статуса CCDA (экзамен 640—863 DESGN), но Cisco рекомендует обладать знаниями в рамках курса CCNA. Также рекомендованы знания BCMSN и BSCI.

Cisco IOS Network Security (CCNA Security)

CCNA Security Certification соответствует потребностям IT специалистов, ответственных за сетевую безопасность. Данная сертификация проверяет навыки, включающие установку, устранение ошибок и мониторинг системных устройств для поддержки целостности, конфиденциальности и доступности данных и устройств и вырабатывает компетентность в технологиях, используемых Cisco в структурах безопасности.

Cisco IOS Unified Communications (CCNA Voice)

Сертификация проверяет навыки в технологиях VoIP, таких как IP PBX, IP телефония, handset, контроль вызовов и решения в области голосовой почты. Кандидаты также посвящены в архитектуру Cisco Unified Communications и дизайн, объединяющий мобильность, presence и TelePresence приложения.

Cisco Unified Wireless Networking Essentials (CCNA Wireless)

CCNA Wireless (Сертифицированный специалист Cisco по беспроводным сетям) проверяет навыки, необходимые для специалистов, осуществляющих поддержку беспроводных сетей, в том числе системных администраторов — associate, Специалистов по поддержке беспроводных сетей и управляющих проектами WLAN.

Сертификация уровня Professional

Cisco Certified Network Professional (CCNP)

Сертификация CCNP подтверждает профессионализм обладателя и способность работать с сетью средних размеров (100—500 хостов) с использованием таких технологий, как QoS, Broadband, VPNs, а также поддерживать ее безопасность. Для получения сертификата CCNP соискатель должен обладать сертификатом CCNA и сдать 3-4 экзамена (количество по выбору). 4 теста:

-642-901 BSCI: Построение масштабируемых интегрированных сетей Cisco Internetworks (BSCI)

-642-812 BCMSN: Построение многоуровневых коммутируемых сетей Cisco (BCMSN)

-642-825 ISCW: Implementing Secure Converged Wide Area Networks (ISCW)

-642-845 ONT: Optimizing Converged Cisco Networks (ONT)[6] QoS и VoIP.

3 теста:

-642-892 Composite — Тесты BSCI и BCMSN могут быть сданы в виде одного единого экзамена 642-892 Composite объединяющего в себе программы экзаменаций BSCI и BCMSN.

-642-825 ISCW: Implementing Secure Converged Wide Area Networks (ISCW)

-642-845 ONT: Optimizing Converged Cisco Networks (ONT)[6] QoS и VoIP.

Cisco Certified Design Professional (CCDP)

Сертификация CCDP — профессиональная сертификация в области дизайна компьютерных сетей Cisco Systems. Для получения сертификата нужен сертификат CCDA. Для сертификаций CCNP and CCDP два экзамена (642—901 BSCI и 642—812 BCMSN) одинаковы, так что обладатель статуса CCNP может получить сертификат CCDP путем сдачи всего одного экзамена 642—873 ARCH.

Экзамены:

-642-901 BSCI: Building Scalable Cisco Internetworks (BSCI)

-642-812 BCMSN: Building Cisco Multilayer Switched Networks (BCMSN)[

-642-873 ARCH: Designing Cisco Network Service Architectures (ARCH)

или

-642-892 Composite: Объединенный экзамен BSCI и BCMSN

-642-873 ARCH: Designing Cisco Network Service Architectures (ARCH)

Cisco Certified Internetwork Professional (CCIP)

CCIP — это профессиональная сертификация в области end-to-end протоколов, используемых в сетях большого масштаба.

Для получения этого сертификата должны быть сданы тесты:

-642-901 BSCI: Building Scalable Cisco Internetworks либо 642-892 Composite

-642-642 QOS: Implementing Cisco Quality of Service

-642-661 BGP: Configuring BGP on Cisco Routers

-642-611 MPLS: Implementing Cisco MPLS

или

-642-901 BSCI: Building Scalable Cisco Internetworks либо 642-892 Composite

-642-642 QOS — Implementing Cisco Quality of Service

-642-691 BGP+MPLS — Configuring BGP on Cisco Routers и Implementing Cisco MPLS

Cisco Certified Security Professional (CCSP)

CCSP — продвинутая сертификация в области сетевой безопасности. Претенденты на сертификат должны продемонстрировать глубокие знания по безопасности различных продуктов корпорации Cisco. Для получения статуса CCSP требуется актуальный статус CCNA или выше (например, CCNP или CCIP).

Сертификация уровня Expert

Cisco Certified Internetwork Expert — высший уровень сертификата. Существует 5 программ для CCIE (Routing and Switching, Service Provider, Security, Wireless, Storage, Voice). Обладатель данного сертификата как правильно имеет очень высокооплачиваемую работу. Порядка 20000 человек в мире имеют статус CCIE.

Топология сертификации CISCO:



**Настройка NAT**

В середине 90-х годов протокол NAT стал популярен из-за проблемы нехватки IPv4 адресов. Большинство систем, которые используют NAT имеют несколько сетевых устройств в сети с частными IP адресами и для выхода в интернет используют публичные IP адреса.

В обычной конфигурации, сетевым устройствам локальной сети радаются IP адреса из пула выделенных частных IP адресов:

1) 192.168.х.х

2) 172.16.х.х - 172.31.х.х

3) 10.х.х.х

Частные IP адреса не маршрутизируются в интернете, поэтому маршрутизатору, который выходит в интернет напрямую, на интерфейс во внутренней сети назначается так же частный IP адрес, а на внешний сетевой интерфейс назначается один или несколько публичных IP адресов. Затем, при помощи протокола NAT происходить преобразование частных IP адресов во внешние.

Существуют несколько разновидностей протокола NAT:

1) Статический NAT - частный IP адрес преобразуется во внешний IP адрес один к одному. Часто применятся, когда сетевое устройство должно быть доступно из интернета или снаружи сетки.

2) PAT (Port address translation) - отображает несколько внутренний адресов в один внешний адрес, использую порты. Например, у вас есть три внутренних адреса 172.1.1.1, 172.1.1.2, 172.1.1.3, и один внешний адрес 192.1.1.1. При использование PAT адреса будут преобазованны следующим образом:

172.1.1.1 - 192.1.1.1:6001

172.1.1.2 - 192.1.1.1:6002

172.1.1.3 - 192.1.1.1:6003

Основные функции NAT:

1) Позволяет сэкономить IP-адреса.

2) Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу.

3) Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов.

Пример настройки NAT:

//Настройка IP адреса для Ethernet 0 и использование в качестве внутреннего NAT интерфейса//

interface ethernet 0

ip address 10.10.10.1 255.255.255.0

ip nat inside

//Настройка IP адреса для Ethernet 1 и использование в качестве внутреннего NAT интерфейса//

interface ethernet 1

ip address 10.10.20.1 255.255.255.0

ip nat inside

//Настройка IP адреса для serial 0 и использование в качестве внешнего NAT интерфейса//

interface serial 0

ip address 172.16.10.64 255.255.255.0

ip nat outside

//Конфигурирование именованного пула NAT с рядом адресов 172.16.10.1 - 172.16.10.63//

ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 24

//Указание какие пакеты могут "проходить" через внутренний интерфейс разрешение следующим acl - access-list 7 транслирование исходного адреса "наружу" NAT pool "no-overload"//

ip nat inside source list 7 pool no-overload

//Access-list 7 разрешает пакеты от следующих сетей 10.10.10.0/24 и 10.10.20.0/24 //

access-list 7 permit 10.10.10.0 0.0.0.255

access-list 7 permit 10.10.20.0 0.0.0.255

Пример настройки PAT:

//Настройка IP адреса для Ethernet 0 и использование в качестве внутреннего NAT интерфейса//

interface ethernet 0

ip address 10.10.10.1 255.255.255.0

ip nat inside

//Настройка IP адреса для Ethernet 1 и использование в качестве внутреннего NAT интерфейса//

interface ethernet 1

ip address 10.10.20.1 255.255.255.0

ip nat inside

//Настройка IP адреса для serial 0 и использование в качестве внешнего NAT интерфейса//

interface serial 0

ip address 172.16.10.64 255.255.255.0

ip nat outside

//Конфигурирование именованного пула с адресом 172.16.10.1//

ip nat pool patpool 172.16.10.1 172.16.10.1 prefix 24

//Указание какие пакеты могут "проходить" через внутренний интерфейс разрешение следующим acl - access-list 7 транслирование исходного адреса "наружу" NAT pool "patpool"//

ip nat inside source list 7 pool patpool overload

//Access-list 7 разрешает пакеты от следующих сетей 10.10.10.0/24 и 10.10.20.0/24 //

access-list 7 permit 10.10.10.0 0.0.0.255

access-list 7 permit 10.10.20.0 0.0.0.255

**Настройка VLAN**

VLAN (Virtual Local Area Network) — группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN'ах, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях.

В современных сетях VLAN — главный механизм для создания логической топологии сети, не зависящей от её физической топологии. VLAN'ы используются для сокращения широковещательного трафика в сети. Имеют большое значение с точки зрения безопасности, в частности как средство борьбы с ARP-spoofing'ом.

Как правило, одному VLAN соответствует одна подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения.

Каждый VLAN — это отдельный широковещательный домен. Например, коммутатор — это устройство 2 уровня модели OSI. Все порты на коммутаторе, где нет VLANов, находятся в одном широковещательном домене. Создание VLAN на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов. Если один и тот же VLAN есть на разных коммутаторах, то порты разных коммутаторов будут образовывать один широковещательный домен.

Когда сеть разбита на VLAN, упрощается задача применения политик и правил безопасности. С VLAN политики можно применять к целым подсетям, а не к отдельному устройству. Кроме того, переход из одного VLAN в другой предполагает прохождение через устройство 3 уровня, на котором, как правило, применяются политики разрешающие или запрещающие доступ из VLAN в VLAN.

Компьютер при отправке трафика в сеть даже не догадывается, в каком VLAN'е он размещён. Об этом думает коммутатор. Коммутатор знает, что компьютер, который подключен к определённому порту, находится в соответствующем VLAN'e. Трафик, приходящий на порт определённого VLAN'а, ничем особенным не отличается от трафика другого VLAN'а. Другими словами, никакой информации о принадлежности трафика определённому VLAN'у в нём нет.

Однако, если через порт может прийти трафик разных VLAN'ов, коммутатор должен его как-то различать. Для этого каждый кадр (frame) трафика должен быть помечен каким-то особым образом. Пометка должна говорить о том, какому VLAN'у трафик принадлежит.

Наиболее распространённый сейчас способ ставить такую пометку описан в открытом стандарте IEEE 802.1Q.

Порты коммутатора, поддерживающие VLAN'ы, (с некоторыми допущениями) можно разделить на два множества:

-Тегированные порты (или транковые порты, trunk-порты в терминологии Cisco).

-Нетегированные порты (или порты доступа, access-порты в терминологии Cisco);

Тегированные порты нужны для того, чтобы через один порт была возможность передать несколько VLAN'ов и, соответственно, получать трафик нескольких VLAN'ов на один порт. Информация о принадлежности трафика VLAN'у, как было сказано выше, указывается в специальном теге. Без тега коммутатор не сможет различить трафик различных VLAN'ов.

Если порт нетегированный в каком-то VLAN'е, то трафик этого VLAN передается без тега.

Порядок конфигурирования vlan:

1)access-port:

switch1(config)# interface fa0/1 - входим в конфигурирование необходимого порта

switch1(config-if)# switchport mode access - задаем режим access

switch1(config-if)# switchport access vlan 2 - назначаем какому vlan соответствует данный порт

2)trunk-port:

switch1(config)# interface fa0/2 - входим в конфигурирование необходимого порта

switch1(config-if)# switchport mode trunk - задаем режим работы trunk

switch1(config-if)# switchport trunk allowed vlan all - указываем какие vlan будет пропускать данный порт

**InterVLAN routing**

В данном уроке мы рассмотрим как настраивается InterVLAN routing (маршрутизация между VLAN) на маршрутизаторах cisco.

Если вы настраиваете VLAN на коммутаторе третьего уровня, то для маршрутизации между VLAN необходимо просто ввести команду ip routing на коммутаторе.

**Списки доступа (Access list)**

Списки доступа (access list) используются для управления входящими и исходящими данными. В данном уроке мы рассмотрим 2 типа списков доступа (access list) (стандартные и расширенные).

Настраиваются списки доступа на маршрутизаторах Cisco в два этапа. Сначала создается сам список доступа (access list), то есть задаются правила, определяющие действия маршрутизатора с определенными пакетами. Затем список доступа связывается с необходимым интерфейсом. Таким образом разные списки доступа могут быть связаны с разными интерфейсами.

Каждый список доступа (access list) идентифицируется номером. Стандартным спискам доступа назначается номер из диапазона от 1 до 99, расширенному - от 100 до 199. Стандартные списки доступа прекрасно подходят для небольших сред, они позволяют запрещать или разрешать весь трафик с определенного адреса. Расширенные списки доступа позволяют настраивать правила более гибко.

Настройка списка доступа:

1) Стандартный список доступа (standart access list). Используя команду

"access-list <номер (1-99)> <действие (deny|permit)> <адрес источника>"

в режиме конфигурирования создается список доступа. Затем, используя команду

"ip access-group <номер списка доступа> in|out"

в режиме конфигурирования интерфейса список доступа связывается с интерфейсом. Правило in или out определяет к каким пакетам будет применяться это правило (к входящим или исходящим).

Пример настройки:

Router#conf term

Router(config)#access-list 10 permit 192.168.1.1 (создаем список доступа)

Router(config)#interface fa0/0

Router(config-if)#ip access-group 10 in (связываем с интерфейсом)

2) Расширенный список доступа (extended access list). Используя команду

"access-list <номер (100-199)> <действие (permit|deny)> <протокол> <адрес источника> <адрес получателя> <порт>"

создаем расширенный список доступа (extended access list). Далее с помощью команды

"ip access-group <номер списка доступа> in|out"

связываем список доступа (access list) с интерфейсом.

Пример настройки:

Router#conf term

Router(config)#access-list 110 deny icmp 192.168.1.0 0.0.0.255 host 192.168.10.1 (создаем список доступа)

Router(config)#interface fa0/0

Router(config-if)#ip access-group 110 in (связываем с интерфейсом)

**Настройка GRE Tunnel**

Generic Routing Encapsulation (GRE) - протокол туннелирования сетевых пакетов, разработанный фирмой Cisco. Этот протокол используется для передачи пакетов одной сети, через другую сеть. GRE туннель представляет собой соединение точка - точка, его можно считать одной из разновидностей VPN туннеля, без шифрования. Основное достоинство GRE это возможность передавать широковещательный трафик, что позволяет пропускать через такой туннель протоколы маршрутизации использующие его, IPSec туннели в чистом виде этого не могут. Так что причин для организации GRE туннеля может быть множество от банальной необходимости пробросить свою сеть через чужое IP пространство до использования протоколов OSPF, RIPv2, EGRP совместно с IPSec.

В нашем примере есть два офиса. В каждом офисе настроена своя локальная сетка. Наша задача заключается в том, чтобы связать две локальные сетки путем конфигурирования GRE Tunnel.



Основные шаги настройки GRE tunnel.

Заходим в режим конфигурирования, используя команду configure terminal.

Создаем виртуальный интерфейс для туннеля, используя команду interface tunnel 0

Задаем ip address используя команду ip address {номер} {маска сети}

Указываем интерфейс, на котором будет открыт наш туннель, tunnel source {интерфейс}

Указываем ip address маршрутизатора, на котором находится другой конец туннеля tunnel destination {ip address}

Повторяем аналогичные действия на другом маршрутизаторе.

Настройка роутеров для нашего примера:

Маршрутизатор №1:

interface Tunnel0

ip address 10.20.20.1 255.255.255.252

tunnel source FastEthernet0/1

tunnel destination 216.4.4.2

!

interface FastEthernet0/0

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

!

interface FastEthernet0/1

ip address 216.4.4.1 255.255.255.252

duplex auto

speed auto

!

ip route 0.0.0.0 0.0.0.0 216.4.4.2

ip route 192.168.2.0 255.255.255.0 10.20.20.2

Маршрутизатор №2:

interface Tunnel0

ip address 10.20.20.2 255.255.255.252

tunnel source FastEthernet0/1

tunnel destination 216.4.4.1

!

!

interface FastEthernet0/0

ip address 192.168.2.1 255.255.255.0

duplex auto

speed auto

!

interface FastEthernet0/1

ip address 216.4.4.2 255.255.255.252

duplex auto

speed auto

!

ip route 0.0.0.0 0.0.0.0 216.4.4.1

ip route 192.168.1.0 255.255.255.0 10.20.20.1