

Cisco — Urbanculture

Интернет Техника



Cisco Systems — широко известный в Интернете и за его пределами производитель сетевого оборудования по шокирующим неподготовленного человека ценам. По пути от сервера к тебе составляющие эту статью байты наверняка прошли через хотя бы одну железку их производства. В массовом админском сознании Циска практически стала синонимом маршрутизатора, но в последнее время ситуация в этом вопросе сильно меняется.

Правильное прочтение названия — «сиско». В жаргоне русскоязычных админов более распространены варианты «циска», «киска», «кошка» и даже «сиська».

История

Утверждается, что основана семьей научных работников, которые сильно хотели общаться друг с другом, но сети их подразделений использовали разные протоколы. Для этой цели они и придумали первый многопротокольный маршрутизатор. От многих других компаний отличается наличием продукции для всех связанных с сетями задач: коммутаторов, маршрутизаторов, WiFi-точек, IP-телефонов, межсетевых экранов^[1], серверов, софта и многих других вещей. Вплоть до планшетов с Android'ом в последнее время.

Название

Название происходит от города Сан-Франциско, в котором она изначально располагалась, «San-Francisco Systems». По легенде кто-то случайно порвал документ так, что от первоначального названия осталось только «cisco Systems», да так и прижилось. Такое написание до сих пор можно встретить внутри софта, но в официальных документах и на сайте давно уже пишется с заглавной буквы. А штаб-квартира теперь находится в Сан-Хосе. Логотип исторически изображал мост «Золотые Ворота» (который в Сан-Франциско и находится), но после ребрендинга пилоны моста проросли вниз и он стал похож на непонятно что.

Значение

Вторую половину восьмидесятых и все девяностые Cisco была безусловным лидером в корпоративных сетях и очень серьезным участником в магистральных. Она оказывала большое влияние на их развитие, как техническое, так и методологическое. Число стандартов Интернета (RFC), в авторах которых есть люди из Cisco огромно. В конце двухтысячных стали сильно сдавать позиции и прибыль пошла вниз. Не самые приятные цены (см. ниже), появление более дешевых или более продвинутых решений у конкурентов, да и слабая поддержка и разработка новых тенденций (в частности, виртуализации)^[2] сделали свое дело. Но большое значение для Интернета трудно отрицать, и Cisco навеки останется в админских сердцах.

Интерфейс

Широко известной фицей всей продукции является интерфейс командной строки. Конкретные команды в разных железках могут отличаться, но общая суть одна:

- Команды состоят из нескольких слов (ip tcp adjust-mss 1412).
- Действие команды можно отменить, поставив перед ней слово «no» (ip cef/no ip cef).
- Команды можно сокращать до потери двусмысленности («sh ip ro» вместо «show ip route»).
- Можно ввести часть команды и нажать Tab для ее



Допускается естественный осадок IP-пакетов



Теперь без шуток



А это уже совсем серьезно

автодополнения, либо увидеть возможные продолжения по нажатию «?». Если нажать «?» без части команды, можно увидеть список всех команд текущего режима с краткими описаниями.

- Каждая строка файла настроек соответствует команде (можно копипастить и вставлять в консоль, опционально приписав «по» к ненужным).

У интерфейса есть три режима: непривилегированный (можно только немного посмотреть), привилегированный (можно смотреть все параметры и выполнять поддержку, устроить пользователю разрыв сессии, например), конфигурационный (можно менять настройки). Команду привилегированного режима можно выполнить прямо из режима настройки, поставив перед ней слово «do». Эти же идеи были скопированы очень многими другими производителями, включая HP, Foundry, да почти всех. Радикально отличный интерфейс разве что у Juniper и Allied Telesis (а также у взявших их идеи).

Недокументированные команды

В интерфейсе есть много недокументированных команд, которые не отображаются в справке и автодополнении. В основном это оставленные авторами софта отладочные операции (вплоть до «test crash», которая позволяет воспроизвести отказ железки по выбранной оператором причине и получить отчет об этом). Иногда встречаются недокументированные полезные функции (например, в 1700 так можно было включить PPTP-клиент), а иногда и просто пасхальные яйца.

Графический интерфейс

Не то, чтобы его там нет, но его никто не использует. Хотя бы потому, что там есть далеко не все, что на самом деле можно настроить. Да и неудобен он для таких целей. Есть внешние средства, например CiscoWorks, но они больше ориентированы на массовое управление сетью и дорого стоят.

Недостатки

- Конфиг почти не структурирован, поэтому большие ACL'ы или списки соседей BGP превращаются в сплошную стену текста, порой непростую для восприятия. Частично решается с помощью пайпов « | include нужный_текст», « | exclude ненужный_текст» и « | section нужный_кусочек». Но до удобства просмотра только нужных частей в Juniper-подобных интерфейсах сильно не дотягивает.
- Активное применение десятичных масок подсетей вместо длины префикса, впрочем, скорее дело вкуса. Но /27 все равно быстрее набрать, чем 255.255.255.224. Для IPv6 все таки сделали длину префикса, потому как проще повеситься, чем его 128-битные маски набирать.
- Конфиг не имеет состояний, что делает неудобным его версионирование и откат изменений (автоматически сохранять ревизии конфига можно, но только через некоторые периоды времени, а не по факту внесения изменений). Тот же факт требует аккуратности в порядке ввода команд: если прописать соседу BGP автономную систему до применения к нему route-map, можно слить ему полную таблицу и нарваться на ресет сессии до прихода админа.
- Нет возможности копировать и переименовывать элементы конфига (смягчается возможностью легко копипастить в текстовый редактор, менять нужное и вставлять обратно). Также нельзя оставить комментарий в любом месте или закоментировать кусок конфига, не удаляя его.

Цисководы

Админы цискок пользуются в ИТшной среде известным уважением. Отчасти из-за некоторой таинственности для не работавшего с ними человека, отчасти из-за того, что циски часто используются в больших и серьезных сетях.

Сертификации

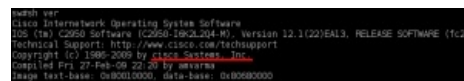
Формальным показателем крутизны цисковеда является сертификат. Система сертификатов состоит из нескольких веток с разной специализацией. Все сертификаты присваиваются по результатам экзаменов, экзамены платные, чем круче сертификат, тем дороже попытка сдачи. Цена попытки от \$300 за CCNA до нескольких тысяч долларов за CCIE. Все письменные экзамены проводятся в форме автоматизированного



Новый логотип



Старый логотип



Пруффик старого написания



Пасхальное яйцо

теста, и все на английском языке.

Низшим уровнем является CCENT (Cisco Certified Entry Networking Technician) — сертифицированный нуб. В основном содержит вопросы по основам сетей, от цисок там не много.

Дальнейший путь обычно выглядит так:

1. CCNA (Cisco Certified Network Associate) — может самостоятельно построить небольшую сеть или помогать админу большой.
2. CCNP (Network Professional) — может сам строить достаточно большие сети.
3. CCIE (Internetwork Expert) — сетевой гуру.

В конце двухтысячных еще ввели Certified Architect — так сказать, цисковод 80-го уровня.

Все N-экзамены бывают с разной тематикой: маршрутизация и коммутация (обычно именуется R&S — routing and switching), голос, безопасность. Еще есть ветка Design с такой же иерархией.

Для CCENT и CCNA нужно сдать только письменный экзамен. CCNP с какого-то момента стал включать лабораторную работу на симуляторе, а CCIE всегда включал также построение действующего макета сети на реальном железе. Первые две ступени обычно можно сдать в любом крупном городе, CCNP только в некоторых сертифицированных центрах, а CCIE в СНГ не принимают вообще, ближайший центр находится в Бельгии.

Принято считать, что сертификаты нравятся работодателям. До начала двухтысячных это было безусловно так, потом в Интернете распространились дампы (готовые ответы к тестам) и их ценность сильно снизилась, поскольку сдать их мог каждый, вызубривший несколько десятков страниц ответов. В порядке борьбы с дампами стали чаще менять вопросы и ввели лабораторную в CCNP.

Но и сейчас сертификат, особенно CCNP и выше может стать серьезным преимуществом при устройстве на работу. В том числе потому, что компаниям с сертифицированными сотрудниками Циска предоставляет скидки на покупку железа и прочие бонусы. По этой причине, кстати, крупные компании и интеграторы часто отправляют сотрудников на сертификацию за счет заведения. Естественно, не нужно думать, что за сам факт наличия сертификата тебя сразу захотят все работодатели. Отношение к «бумажным» сертификатам без соответствующего опыта зачастую не самое лучшее.

Все сертификаты выдаются сроком на три года, после этого нужно либо пересдавать, либо сдавать следующий. Для CCIE достаточно сдавать только письменную часть, причем из любого трека (то есть, любой тематики).

Хочешь стать цисководом?

Не самая плохая идея. Циска очень хорошо подходит для начала карьеры сетевого администратора. По ней много печатной (и отсканированной) литературы, статей в Интернете и прочей документации. Кроме того у нее весьма большое сообщество специалистов и развитый вторичный рынок железа.

Есть два способа. Первый — записаться на официальные курсы Cisco Networking Academy. Либо при каком-нибудь университете, либо в учебном центре^[3]. Там тебя обеспечат учебной литературой, доступом к железу для лабораторных и прочими удовольствиями. За пару тысяч долларов в неделю. Поэтому лучше всего на такие курсы ходить за счет работодателя. Зато слушателям курсов дают скидку на сдачу экзаменов.

Если работодатель тебя отправлять не спешит, а своих денег на такое жалко, можно экспериментировать самому. Тут опять же два варианта: реальное железо или эмулятор.

Реальное железо

Набор «юный сетевой инженер» начального уровня при желании можно собрать по цене в пределах килобакса. Пару маршрутизаторов типа 2600 и один коммутатор 292х/295х. Потом добавить еще коммутатор чтобы поиграться со spanning tree и прочим EtherChannel. Коммутаторы третьего уровня дороже, но на начальном этапе не особо нужны.

Не забудь обзавестись кабелем консоли и машиной с COM-портом (или переходником USB-RS232). Без доступа консолью не сможешь ни провести начальную настройку из дефолтного конфига, ни сбросить пароль, ни установить/восстановить софт если его на железке не было или ты его неосторожно прибил.

Если собираешься использовать в качестве домашнего маршрутизатора, а не только для нездоровых экспериментов, смотри на серию 8xx, которая с пассивным охлаждением. У всех стоечных моделей мощные и шумные вентиляторы, которые твои родственники едва ли одобряют.

Да, и еще. Маршрутизаторы и межсетевые экраны с 2010 года придется искать на внутреннем российском рынке, eбaу не прокатит. Из-за запрета на импорт продукции со строгим шифрованием их с большой вероятностью не пропустят через границу. Коммутаторы, скорее всего, пропустят.

Эмуляция

Если и на это жалко денег, можно воспользоваться эмулятором или симулятором. Симулятор называется «Packet Tracer» и используется на курсах, тыренные дистрибутивы есть в р2р. Есть и для винды, и для линукса. Умеет симулировать работу коммутаторов, есть файлы с готовыми топологиями и задачами. Но настроить в нем можно далеко не все, что есть в реальных устройствах. Для начала — самое оно.

Эмулятор маршрутизаторов называется dynamips. Поддерживает 2600, 3700, 7200 и еще несколько. Не поддерживает и никогда не будет поддерживать [123]800 и всю ISR G2, тем более 10000^[4].

Для эмуляции PIX есть форк QEMU под названием PIXEMU. Для ASA несвежих версий есть просто образы виртуальных машин.

Если нет желания возиться с dynamips и pixemu напрямую, можно поставить GNS. Там все в комплекте, легко объединяется в сеть, можно рисовать топологию перетаскиванием значков железок на поле — примерно как в Packet Tracer.

Все эмуляторы эмулируют только аппаратную платформу и для работы требуют образы ОС соответствующей железки. Найти их в Интернете не составит труда.

Последняя тенденция — утекшие в сеть образы IOU (IOS on UNIX). IOS, который запускается как приложение в UNIX.

Сеанс цисководства

Цены

Ссылки

- cisco.com

Примечания

1. ↑ Файрволлов, по простому.
2. ↑ То есть, поддержка как бы есть, но с упором на виртуализацию внутри их железа и с жесткой привязкой к VMWare, что довольно далеко от желаний многих операторов облачных сервисов.
3. ↑ Вот в [этом](#), например.
4. ↑ Они основаны на проприетарных чипсетах, поэтому их поддержка эмулятором потребовала бы обратной разработки, что незаконно. Старые модели делались на стандартных с открытыми спецификациями.