Функции PPP виртуального доступа в Cisco IOS

Содержание

Введение

Этот документ описывает общую архитектуру приложений для виртуального доступа PPP в Cisco IOS®. Для получения дополнительной информации по конкретным функциям см. список документов после глоссария.

Перед началом работы

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с

конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Глоссарий

Далее приведены термины, используемые в этом документе.

- **Сервер доступа:** Платформы Cisco Access Server, включая интерфейсы ISDN и асинхронные интерфейсы для обеспечения удаленного доступа.
- **L2F:** Протокол передачи 2-го уровня (экспериментальный проект RFC). Это базовая технология канального уровня как для Multichassis MP, так и для виртуальных частных сетей (VPN).
- **Соединение:** Точка подключения, предоставляемая системой. Это может быть выделенный аппаратный интерфейс (например, асинхронный интерфейс) или канал на мультиканальном аппаратном интерфейсе (например, PRI или BRI).
- **MP:** Многоканальный протокол PPP (см. RFC 1717).
- **Многокорпусный MP:** MP + SGBP + L2F + Vtemplate.
- **PPP:** Протокол "точка-точка" (см. RFC 1331).
- **Чередующаяся группа:** Группа физических интерфейсов, выделенных для исходящих и входящих вызовов. Эта группа служит пулом, любой канал которого можно использовать, чтобы подключиться к внешней сети или принять вызов.
- **SGBP:** Протокол приглашения группы стека (SGBP)
- **Группа стеков:** Сбор двух или более систем, которые будут конфигурированы для работы как группа и поддержки MP пакетов с каналами на разных системах.
- **VPDN:** Виртуальные частные коммутируемые сети. Перенаправление каналов PPP от интернет-провайдера (ISP) к домашнему шлюзу.
- **Vtemplate:** Интерфейс виртуального шаблона.

Примечание: Для получения информации о RFC, на который ссылается этот документ, см. документ Поддержка RFC в Cisco IOS Release 11.2, информационный листок продукта; или см. документ Получение RFC и других стандартных документов, содержащих ссылку непосредственно на InterNIC.

Обзор интерфейса виртуального доступа

В Cisco IOS Release 11.2F среда Cisco поддерживает функции доступа удаленного подключения: VPDN, протокол объединения серверов доступа в стек, VP, трансляция протокола с помощью виртуального доступа и PPP/ATM. Эти возможности используют виртуальные интерфейсы для передачи PPP на конечные компьютеры.

Интерфейс виртуального доступа — это интерфейс Cisco IOS, такой же, как и физические интерфейсы, например последовательный интерфейс. Настройка последовательного интерфейса хранится в конфигурации последовательного интерфейса.

```
#config int s0 ip unnumbered e0 encap ppp :
```

Для физических интерфейсов предусмотрены статические фиксированные настройки. Однако интерфейсы виртуального доступа созданы динамически по требованию (в следующем разделе настоящего документа рассматриваются различные использования). Они также свободны, если больше не нужны. **Таким образом, источник конфигурации интерфейсов виртуального доступа должен быть закреплен другим способом.**

Различные методы, по которым виртуальный доступ получает конфигурацию, проводятся через интерфейс виртуального шаблона и/или записи RADIUS и TACAC+, которые постоянно хранятся на сервере аутентификации. *Последний метод называется виртуальными профилями пользователей.* Поскольку интерфейсы виртуального доступа можно настраивать с помощью глобального виртуального шаблона, интерфейсы виртуального доступа для разных пользователей могут наследовать одинаковые конфигурации из одного интерфейса виртуального шаблона. Например, администратор сети может принять решение задать общий метод проверки подлинности PPP (CHAP) для всех пользователей виртуального доступа к системе. **Для специальных конфигураций для конкретного пользователя администратор сети может задать конфигурации интерфейса – такие, как аутентификация PAP – заданная для пользователя в виртуальном профиле.** Короче говоря, схема настройки от общего к конкретному, доступная для интерфейсов виртуального доступа, позволяет администратору сети разрабатывать конфигурации интерфейса общие для всех пользователей или отдельно для пользователя.

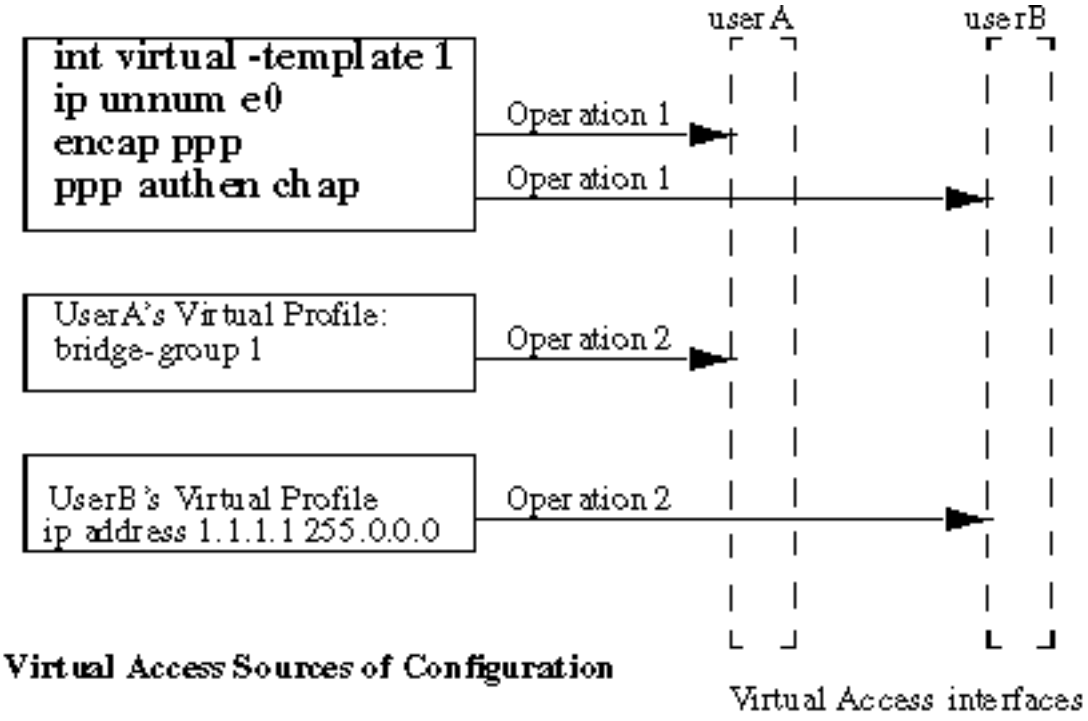

Figure 1. Virtual Access Sources of Configuration

Рисунок 1 выше иллюстрирует два из интерфейсов виртуального доступа для userA и userB. **Операция 1 обозначает применение конфигурации интерфейса от интерфейса глобального виртуального шаблона к этим двух интерфейсам виртуального доступа. Операция 2 обозначает применение конфигураций интерфейса для каждого пользователя от других виртуальных профилей к этим двум интерфейсам виртуального доступа.**

Приложения интерфейсов виртуального доступа

В этом разделе описаны различные способы использования интерфейсов виртуального доступа в Cisco IOS.

Вы заметите повторяющуюся тему каждого приложения – они обеспечивают использование общего виртуального шаблона для конкретного приложения (операция 1). Виртуальные профили затем применяются к каждому пользователю (операция 2)

Multilink PPP

Многоканальная система PPP использует интерфейс виртуального доступа как пакетный интерфейс для повторной сборки пакетов, полученных по отдельным каналам, а также для фрагментации пакетов, посылаемых по отдельным каналам. Групповой интерфейс получает свою конфигурацию от виртуального шаблона, заданного для многоканального PPP. Если сетевой администратор принимает решение о включении виртуальных профилей, конфигурация интерфейса виртуального профиля для каждого пользователя применяется к групповому интерфейсу пользователя.

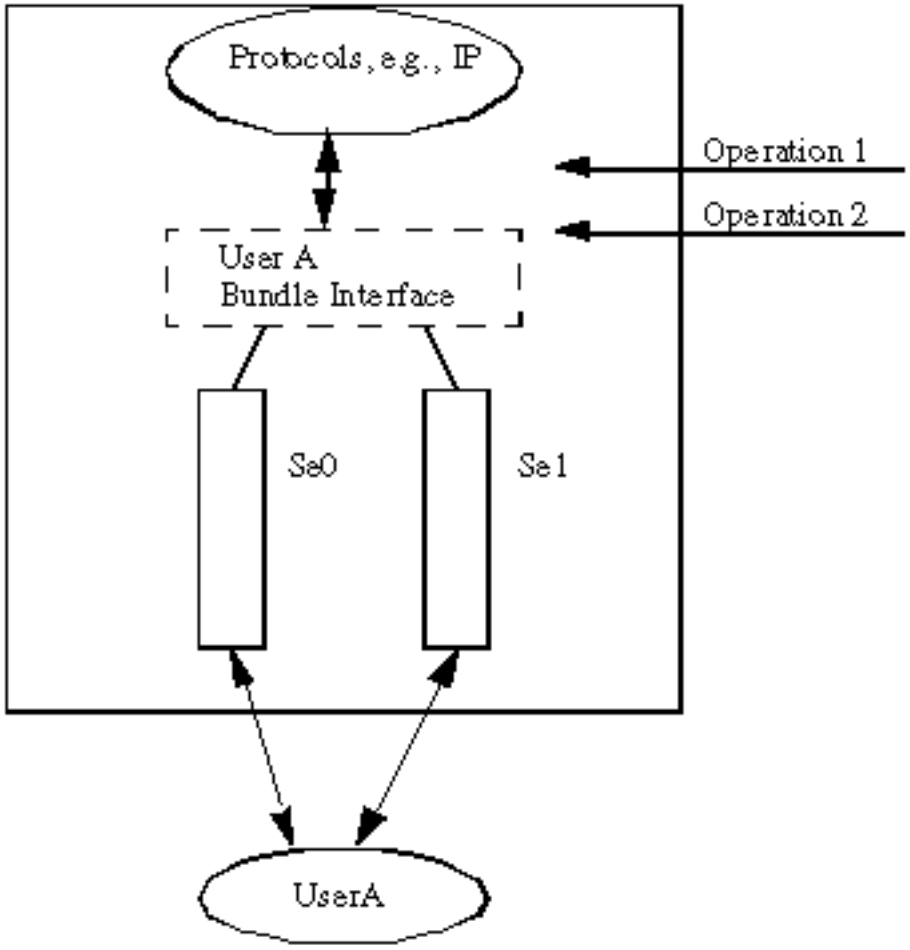

Figure 2. Multilink PPP Bundle Interface

На рис. 2 изображено использование многоканального PPP последовательны интерфейсов. Поскольку интерфейс номеронабирателя отсутствует, интерфейс виртуального шаблона определяется следующим:

```
multilink virtual-template 1

  int virtual-template 1
  ip unnum e0
  encap ppp
  ppp chap authen
```

Затем к групповому интерфейсу применяется необязательная конфигурация виртуальных профилей для имени пользователя. Когда интерфейс номеронабирателя включен, групповой интерфейс является пассивным интерфейсом – интерфейс виртуального шаблона не требуется.

Например, на рис. 3 изображена настройка PRI se0:23 для поддержки Multilink PPP.

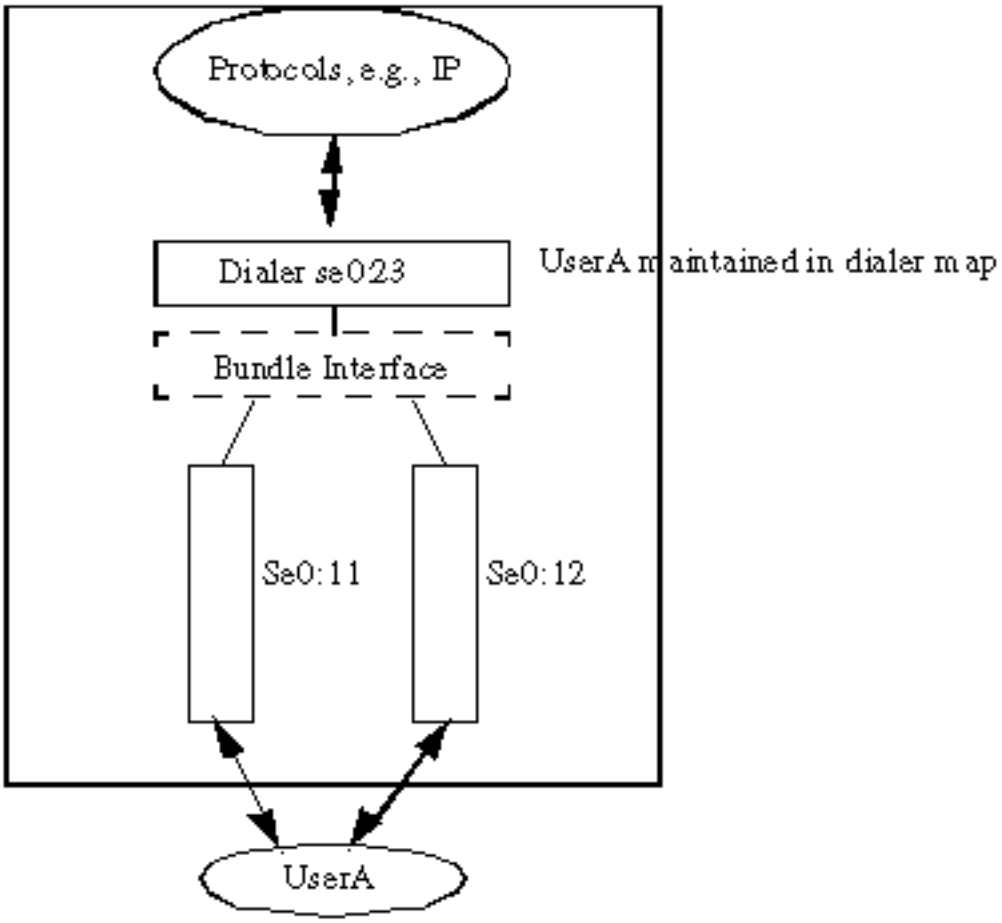

Figure 3. Multilink PPP Interface (Passive)

Обратите внимание, что виртуальный профиль выключен, схема возвращается к предшествующему состоянию, что показано на рис. 2. То есть, если входящий вызов получен на интерфейс номеронабирателя и виртуальный профиль выключен, источник конфигурации уже не является номеронабирателем. Вместо этого групповой интерфейс (см. Рис. 2) является активным интерфейсом, к которому обращаются протоколы при чтении или записи. Первый источник конфигурации — интерфейс виртуального шаблона, а затем — виртуальный профиль для индивидуального пользователя.

L2F

Пересылка уровня 2 на уровне канала связи или L2F позволяет завершить PPP на удаленном назначении. Обычно, без L2F, PPP устанавливается между вызываемым клиентом и NAS, который ответил на входящий вызов. При помощи L2F протокол PPP переносится на узел назначения. С точки зрения клиента ему кажется, что он подключен к узлу назначения через PPP. На самом деле NAS становится простым механизмом продвижения данных PPP кадров. **В терминологии L2F узел назначения называется домашним шлюзом.**

На домашнем шлюзе для окончания линии "точка-точка" используется виртуальный интерфейс доступа. И снова виртуальный шаблон используется как источник конфигурации. Если определен виртуальный профиль, к виртуальному интерфейсу доступа будет применяться конфигурация интерфейса для каждого пользователя.

Туннель L2F в данный момент распространяется через UDP/IP.

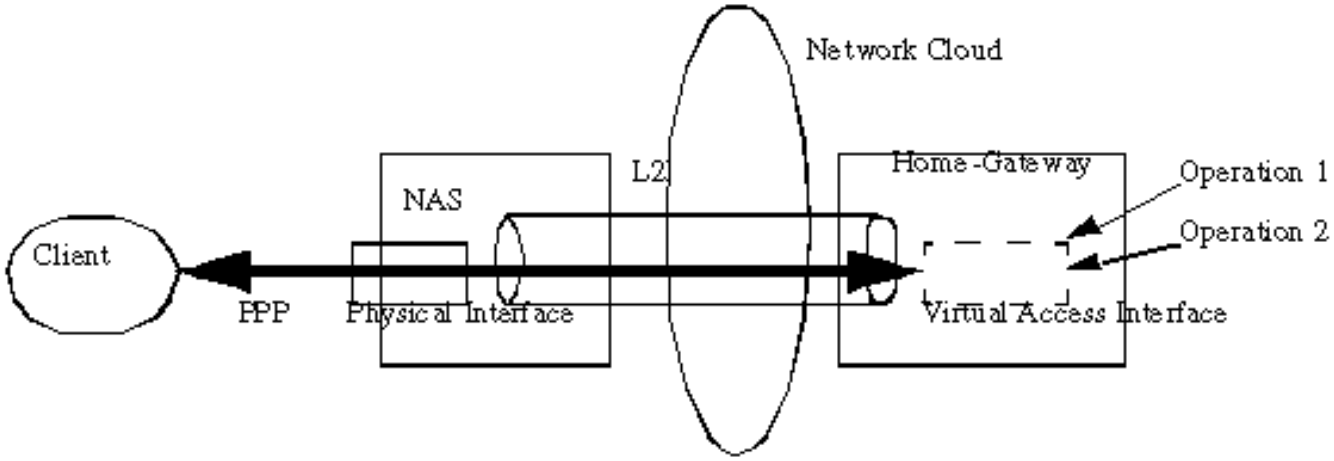

Figure 4. Client PPP to the Home-Gateway via a L2F Tunnel

Туннельная технология L2F сейчас используется в двух функциях Cisco IOS 11.2: **VPDN (виртуальная частная сеть удаленного доступа) и многоблочный многоканальный PPP (MMP).**

VPDN

VPDN позволяет частным сетям развертываться от клиента напрямую к выбранному домашнему шлюзу. Например, мобильные пользователи HP (например, в торговле) хотят иметь возможность постоянного подключения к домашнему шлюзу выбора HP везде и в любое время. HP договорится об использовании ISP, поддерживающих PDN. **Эти ISP должны быть настроены таким образом, что если jsmith@hp.com вызывает любой из номеров ISP, то сервер NAS выполняет автоматическую пересылку на домашний шлюз HP.** ISP, таким образом, освобождается от администрирования IP-адресов пользователей HP, маршрутизации и других функций, связанных с базой пользователя HP. Администрирование ISP HP сводится до проблем IP-подключения для домашнего шлюза HP.

NAS: isp

```
  vpdn outgoing hp.com isp ip 1.1.1.2
```

Домашний шлюз: hp-gateway

```
int virtual-template 1
  ip unnum e0
  encap ppp
  ppp chap authen

  vpdn incoming isp hp-gateway virtual-template 1
```

Multichassis

PPP Multilink предоставляет пользователям дополнительную полосу по требованию с возможностью разделения и перекомпоновки пакетов через логический канал (связку), формируемую несколькими соединениями. Это уменьшит задержку передачи через медленные WAN-каналы, а также предоставит метод увеличения максимального полученного блока. Multilink поддерживается в единой среде сервера доступа.

Для ISP, например, удобно задать один номер в группе телефонной связи нескольким PRI

на нескольких серверах доступа, что обеспечит масштабируемость и гибкость для бизнес-потребностей.

При использовании многоблочного мультиканального протокола несколько мультиканальных соединений от одного клиента могут завершаться на разных серверах доступа. В то время как отдельные каналы MP из одной группы могут фактически завершаться на разных серверах доступа, клиент MP всегда завершается на сервере одиночного доступа. После сравнения компонентов с компонентами VPDN комплексные шасси будут отличаться только дополнительным протоколом SGBP для обработки приглашений и устранения ошибок многоканальных связок. После определения IP-адреса назначения победителя стековой группы по протоколу SGBP, стек использует L2F для перехода с одного NAS на другой, который и является победителем стековой группы.

Например, в стеке групп вызывается команда stackq для двух NAS: nasa и nasb.

nasa:

```
  username stackq password hello
  multilink virtual-template 1

  int virtual-template 1
  ip unnum e0
  encap ppp
  ppp authen chap

  sgbp stack stackq
  sgbp member nasb 1.1.1.2
```

nasb:

```
username stackq password hello
  multilink virtual-template 1

  int virtual-template 1
  ip unnum e0
  encap ppp
  ppp authen chap

  sgbp stack stackq
  sgbp member nasb 1.1.1.2
```

Преобразование протокола

Преобразование протокола позволяет инкапсулированному трафику PPP через шлюз – такой, как X.25/TCP – завершаться как интерфейс виртуального доступа (преобразование в два этапа). Интерфейс виртуального доступа поддерживается также через одноступенчатое преобразование.

Пример преобразования протокола в два этапа:

```
  int virtual-template 1
  ip unnum e0
  encap ppp
  ppp authen chap

  vty-async virtual-template 1
```

Пример одноэтапного преобразования протокола:

```
int virtual-template 1
  ip unnum e0
  encap ppp
  ppp authen chap

  translate tcp 1.1.1.1 virtual-template 1
```

PPP через ATM

Когда данные форматируются согласно инкапсуляции пересылки кадров Cisco (StrataCom), , эта функция предоставляет поддержку для завершения нескольких PPP-подключений в интерфейсе ATM маршрутизатора. Соединение PPP завершается на маршрутизаторе по аналогии с завершением соединения со стандартным последовательным интерфейсом PPP. Каждое PPP-подключение будет инкапсулироваться в отдельном VC ATM. VCs, использующие другие методы инкапсуляции, могут быть также настроены на одном и том же интерфейсе.

```
interface Virtual-Template1
  ip unnumbered e0/0
  ppp authentication chap

  interface ATM2/0.2 point-to-point
  atm pvc 34 34 34 aal5ppp virtual-template 1
```

Виртуальные профили

Виртуальные профили представляют собой уникальное приложение PPP, которое определяет и применяет данные настройки каждого пользователя для пользователей, подключающихся к маршрутизатору. Виртуальные профили позволяют применять информацию о конфигурации для определенного пользователя независимо от среды, используемой для удаленного вызова. Информацию о конфигурации виртуальных профилей можно получить из шаблона виртуального интерфейса, данных о настройках пользователей, которые хранятся на сервере AAA, или же из обоих источников в зависимости от настроек маршрутизатора и сервера AAA. Виртуальные профили могут использоваться в среде с одним устройством, в домашнем шлюзе VPDN или многоблочной среде.

Чтобы определить виртуальный шаблон в качестве источника конфигурации для виртуального профиля:

```
virtual-profile virtual-template 1
  int virtual-template 1
  ip unnum e0
  encap ppp
  ppp authen chap
  :
```

Чтобы определить AAA как источник конфигурации для виртуального профиля:

```
virtual-profile aaa
```

В этом примере администратор решил отфильтровать маршруты, заявленный Джону, и применить списки доступа для подключений Рика к сети извне по телефонной линии. При входящем звонке от любого пользователя через интерфейс S1 или BRI 0 и его аутентификации создается виртуальный профиль: фильтры маршрута применяются к Джону, а списки доступа применяются к Рику.

Конфигурация AAA для пользователей Джон и Рик:

```
john Password = ``welcome''
       User-Service-Type = Framed-User,
       Framed-Protocol = PPP,
           cisco-avpair = ``ip:rte-fltr-out#0=router igrp 60'',
           cisco-avpair = ``ip:rte-fltr-out#3=deny 171.0.0.0 0.255.255.255'',
           cisco-avpair = ``ip:rte-fltr-out#4=deny 172.0.0.0 0.255.255.255'',
           cisco-avpair = ``ip:rte-fltr-out#5=permit any''
  rick Password = ``emoclew''
       User-Service-Type = Framed-User,
       Framed-Protocol = PPP,
           cisco-avpair = ``ip:inacl#3=permit ip any any precedence immediate'',
           cisco-avpair = ``ip:inacl#4=deny igrp 0.0.1.2 255.255.0.0 any'',
           cisco-avpair = ``ip:outacl#2=permit ip any any precedence immediate'',
           cisco-avpair = ``ip:outacl#3=deny igrp 0.0.9.10 255.255.0.0 any''
```

Вкратце, пары AAA cisco-avpairs содержат команды Cisco IOS для каждого интерфейса, чтобы применять их для определенного пользователя.

Дополнительные сведения

- Многоблочный PPP Multilink (MMP)
- Запросы RFC, поддерживаемые в Cisco IOS(tm) выпуска 11.2(1)
- Техническая поддержка - Cisco Systems