Понимание версий APS на интерфейсах POS

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Обзор PGP
Версии PGP
Таймеры приветствия и удержания
Authentication
Обращение в Центр технической поддержки Cisco
Дополнительные сведения

Введение

Этот документ описывает Протокол Protect Group (PGP), который является ключевой частью Автоматического переключения на резерв (APS) Передачи пакета по сети SONET (POS) на маршрутизаторах Cisco и коммутаторах Enterprise.

Предварительные условия

Требования

Этот документ не имеет никаких определенных требований.

Используемые компоненты

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

Условные обозначения

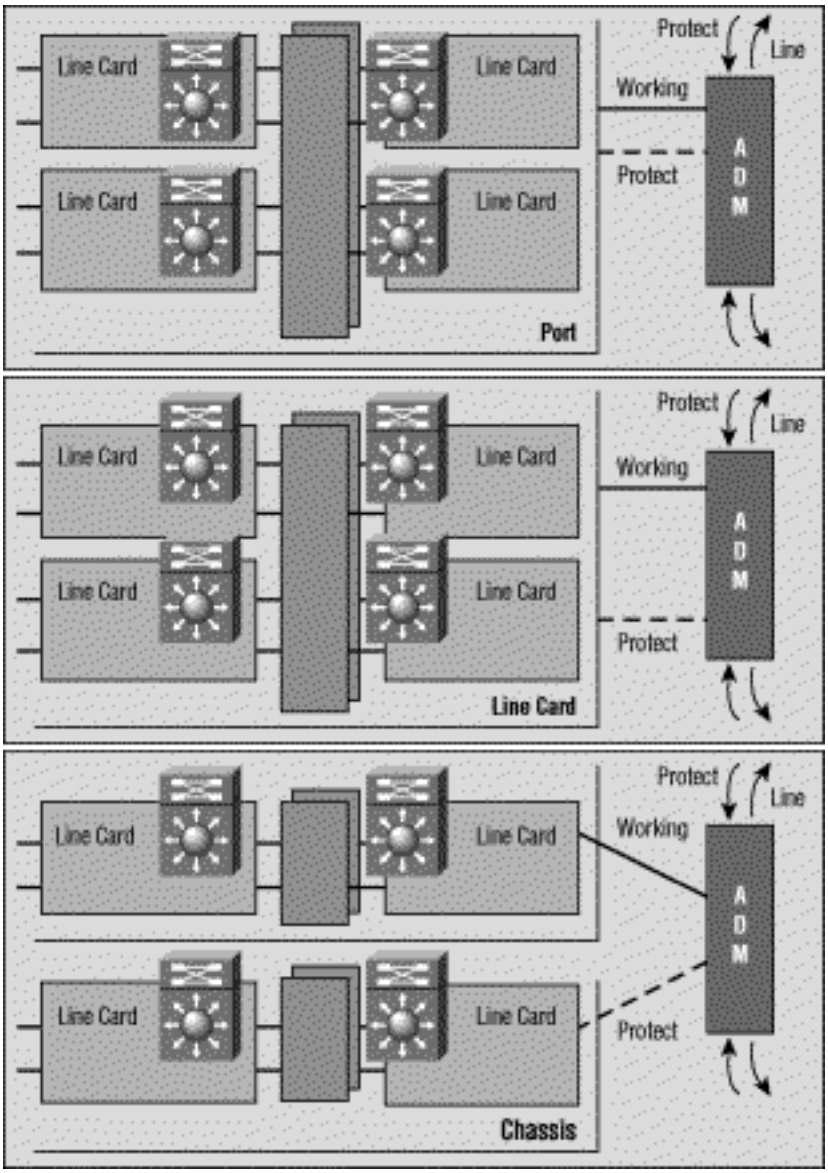
Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Обзор PGP

Bellcore (теперь Telcordia) публикация TR-TSY-000253, Системы Передачи по протоколу SONET; Общие Общие критерии, Раздел 5.3, определяют Автоматическое переключение на

резерв (APS). Механизм защиты, используемый для этой функции, имеет 1+1, архитектура, в которой резервная пара линий состоит из рабочей линии и защищенной линии.

Этот рисунок показывает возможные Конфигурации защиты SONET. Можно установить Cisco POS схема защиты для ситуаций, где защищают, и рабочие интерфейсы являются другими портами. Эти порты могут быть на том же маршрутизатор или на той же линейной карте в том же маршрутизатор. Эти сценарии, однако, обеспечивают защиту для интерфейса маршрутизатора или отказ соединения. Большинство развертываний на производстве имеет работу и защищает интерфейсы на других маршрутизаторах. В такой конфигурации APS с двумя маршрутизаторами требуется протокол как PGP. PGP определяет протокол между работой, и защитите маршрутизаторы.



Версии PGP

С релиза 12.0 программного обеспечения Cisco IOS (10) S, две версии PGP доступны. Работа и защищает маршрутизаторы, должен использовать ту же версию PGP и обменные сообщения согласования с помощью внеполосного коммуникационного канала. Во время согласования защищать маршрутизатор передает сообщения в несколько версьих PGP, самых высоких сначала. Рабочий маршрутизатор игнорирует hellos с номерами версий выше, чем его собственное и отвечает на другие. Как только рабочий маршрутизатор отвечает на приветственное сообщение, он принимает тот номер версии и использует его

во всех последующих ответах.

В текущих Cisco IOS Release, работе и защищают маршрутизаторы, не должны выполнять тот же IOS Release. Работа и защищает маршрутизаторы, может поэтому быть обновлен независимо.

Если программное обеспечение Cisco IOS обнаруживает несоответствие версии, оно распечатывает сообщения журнала, подобные этому:

```
Sep 10 06:34:25.305 cdt: %SONET-3-MISVER: POS4/0: APS version mismatch.
WARNING: Loss of Working-Protect link can deselect both
protect and working interfaces. Protect router requires
software upgrade for full protection.
Sep 10 06:34:25.305 cdt: %SONET-3-APSCOMMEST: POS4/0:
Link to protect channel established - protocol version 0
Sep 10 06:34:33.257 cdt: %SONET-3-APSCOMMEST: POS4/0:
Link to protect channel established - protocol version 1
```

Если эта ссылка испытывает ухудшенную производительность и высокую потерю пакета, согласование версий APS между работой, и защитите сбои маршрутизаторов. В результате оба маршрутизатора принимают версии PGP "down-rev". Проблема следует из поврежденных сообщений согласования. Если потеря пакета высокоскоростного канала связи PGP, рабочий маршрутизатор может отсутствовать привет передаваемый защищать маршрутизатором с объявленным номером версии. Если это происходит, это могло бы только видеть, что последующий down-rev обменивался сообщениями. Этот сценарий вызывает обоих работа, и защитите маршрутизаторы для блокировки на номер более ранней версии. Cisco IOS релиз 12.0 Sofware (21) S избегает этой проблемы путем выполнения непрерывного пересмотра как требуется.

При использовании выпуск до IOS релиз 12.0 Sofware (21) S и испытываете эту проблему, используйте этот обходной путь для восстановления стандартной версии PGP. Сделайте это, как только вы установили надежный канал между этими двумя маршрутизаторами:

1. Гарантируйте, что выбран рабочий интерфейс. Можно использовать **команду aps force 0**, чтобы сделать это.
2. Закройте защищать интерфейс. Снижайте его достаточно долго так, чтобы рабочий объявил, что это потеряло связь с защищать интерфейсом.
3. Используйте **команду no shutdown** на защищать интерфейсе для перезапуска согласований протокола.

Сбои связи PGP могут произойти из-за любой из этих проблем:

- Сбой рабочего маршрутизатора
- Защитите ошибку маршрутизатора
- Отказ канала PGP

Отказ канала PGP может произойти из-за любой из этих проблем:

- Перегрузка канала связи трафиком
- Отказ интерфейса из-за сигналов тревоги
- Сбой интерфейсного оборудования

Можно предоставить интерфейсы более высокой пропускной способности для PGP, чтобы минимизировать перегрузку и избежать некоторых отказов канала PGP. Рабочий маршрутизатор ожидает получать *hellos* от защищать маршрутизатора каждый hello-interval. Если рабочий маршрутизатор не получает hellos какое-то время интервал, заданный

держать-интервалом, рабочий маршрутизатор принимает сбой PGP, и APS приостановлен. Точно так же, если защищать маршрутизатор не получает привет подтверждения от рабочего маршрутизатора, прежде чем держать-таймер-интервала истечет, это объявляет сбой PGP, и переключатель может произойти.

Таймеры приветствия и удержания

POS APS отличается от "строгих" ТОЧЕК ДОСТУПА К СЕТИ SONET. POS APS поддерживает команды дополнительной настройки, используемые для настройки параметров PGP.

Можно использовать **команду aps timers** для изменения таймера приветствия и таймера ожидания. Таймер приветствия определяет время между пакетами приветствия. Таймер ожидания устанавливает время, прежде чем защищать интерфейсный процесс объявит, что маршрутизатор рабочего интерфейса не работает. По умолчанию время удержания больше, чем или равно три раза времени приветствия.

Следующий пример задает время приветствия двух секунд и времени удержания шести секунд на канале 1 на Интерфейсе пакетной передачи POS (по сети Sonet) 5/0/0:

```
router#configure terminal router(config)#interface pos 5/0/0 router(config-if)#aps working 1
router(config-if)#aps timers 2 6 router(config-if)#end
```

Как показано выше, мы настроили **команду aps timers** только на защищать интерфейсах.

Можно настроить работу и защитить интерфейсы с уникальное приветствие и держать времена. Когда работа находится в контакте с защищать интерфейсом, это использует значения таймера, заданные для защищать интерфейса. Когда работа не находится в контакте с защищать интерфейсом, это использует привет и таймеры ожидания, заданные для рабочего интерфейса.

Authentication

Другая команда, поддерживаемая только APS POS, является **командой проверки подлинности**, которая включает аутентификацию между процессами, управляющими работой, и защитите интерфейсы. Используйте эту команду для определения строки, которая должна присутствовать для принятия любого пакета на защищении или рабочем интерфейсе. Приняты до восьми алфавитно-цифровых знаков.

Обращение в Центр технической поддержки Cisco

При необходимости в помощи устранить неполадки APS свяжитесь с Центром технической поддержки Cisco (TAC). Соберите выходные данные из следующих **команд показа** на маршрутизаторах с защищением и рабочими интерфейсами:

- **show version-** Отображает конфигурацию системного оборудования и версии программного обеспечения. Эта команда также отображает названия и файлы источников конфигурации и образы загрузки.
- **show controller pos** Отображает информацию о Контроллерах POS.
- **show aps-** Отображает информацию о текущей функции автоматической резервной

коммутации.

Дополнительные сведения

- Страницы поддержки оптических технологий
- Техническая поддержка - Cisco Systems