Конфигурация изолированных частных VLAN на коммутаторах

Содержание

Введение

В некоторых случаях необходимо предотвратить соединение уровня 2 (L2) между устройствами на коммутаторе, не поместив устройства в разные подсети IP. С помощью данной установки можно предотвратить потерю IP-адресов. Частные сети VLAN (PVLAN) изолируют устройства уровня 2 в одной подсети IP. Можно направить порты на коммутаторе только на конкретные порты с шлюзом по умолчанию, резервным сервером или подключенным Cisco LocalDirector.

В данном документе описана процедура настройки изолированных сетей PVLAN на коммутаторах Cisco Catalyst с ПО Catalyst OS (CatOS) или Cisco IOS®.

Предварительные условия

Требования

В данном документе предполагается, что сеть уже существует, и с ее помощью можно установить соединение между различными портами в добавление к PVLAN. Если в наличии

есть несколько коммутаторов, убедитесь, магистраль между ними функционирует правильно и позволяет работать сетям PVLAN на магистрали.

Не все коммутаторы и версии программного обеспечения поддерживают частные виртуальные локальные сети. Чтобы определить, поддерживает ли платформа или версия ПО сети PVLAN перед началом конфигурации, см. раздел Матрица поддержки коммутаторов Catalyst на частных сетях VLAN.

Примечание: Некоторые коммутаторы (как задано в Матрице поддержки частной VLAN коммутатором Catalyst) в настоящее время поддерживают только функцию ГРАНИЦЫ PVLAN. Термин "защищенные порты" также относится в данной функции. На портах Edge сетей PVLAN есть ограничение, которое предотвращает связь с другими защищенными портами на одном коммутаторе. Однако защищенные порты на отдельных коммутаторах могут взаимодействовать друг с другом. Следует различать данную функцию с конфигурацией обычной PVLAN, которая отображена в данном документе. *Дополнительные сведения о защищенных портах см. в разделе Конфигурация безопасности порта документа Конфигурация контроля трафика на уровне порта.*

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Коммутатор Catalyst 4003 с модулем управления 2, который использует CatOS версии 6.3(5)
- Коммутатор Catalyst 4006 с модулем управления 3, который использует ПО Cisco IOS версии 12.1(12c)EW1

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Теоретические сведения

PVLAN – это VLAN с конфигурацией для изоляции уровня 2 от других портов с таким же доменом широковещательной рассылки или подсетью. Можно назначить особый набор портов в PVLAN и таким образом контролировать доступ к портам на уровне 2. А также можно настроить сети PVLAN и обычные VLAN на одном коммутаторе.

Существует три типа портов PVLAN: случайный, изолированный и общий.

- Случайный порт взаимодействует с другими портами PVLAN. Изолированный порт – это порт, который используют для взаимодействия с внешними маршрутизаторами, LocalDirectors, устройствами управления сетью, резервными серверами, административными рабочими станциями и другими устройствами. На других

коммутаторах порт для модуля маршрутизатора (например плата многоуровневой коммутации [MSFC]) должен быть случайным.
- На изолированном порте есть полное разделение уровня 2 от других портов с такой же PVLAN. Данное разделение содержит широковещательные рассылки. Исключением является только случайный порт. Разрешение конфиденциальности на уровне 2 присутствует в блоке исходящего трафика ко всем изолированным портам. Трафик, приходящий из изолированного порта, направляется только на все изолированные порты.
- Общие порты могут взаимодействовать друг с другом и со случайными портами. У данных портов есть изоляция уровня 2 от других портов в других сообществах или от изолированных портов в сети PVLAN. Рассылки распространяются только между связанными портами сообщества и разнородными портами.**Примечание:** Этот документ не покрывает конфигурацию VLAN сообщества.

Дополнительные сведения о сетях PVLAN см. в разделе Конфигурация частных сетей VLAN документа Общие сведения и конфигурация сетей VLAN.

Правила и ограничения

В данном разделе представлены правила и ограничения, которым необходимо следовать перед внедрением сетей PVLAN. *Более полный список см. в разделе Рекомендации по конфигурации частных сетей VLAN документа Конфигурация сетей VLAN.*

- PVLAN не могут включать в себя сети VLAN 1 или 1002-1005.
- `VTP transparent.`
- Можно только задать одну изолированную виртуальную локальную сеть для основной виртуальной локальной сети.
- Можно только назначить VLAN в качестве PVLAN, если у данной VLAN есть назначения текущих портов доступа. Удалите порты в данной сети VLAN перед преобразованием VLAN в PVLAN.
- Не настраивайте порты PVLAN как EtherChannels.
- Из-за ограничений аппаратного обеспечения модули коммутаторов Catalyst 6500/6000 Fast Ethernet ограничивают конфигурацию изолированного или общего порта VLAN, если порт в специализированной интегральной схеме одного COIL (ASIC) представляет собой следующее:МагистральНазначение анализатора коммутируемого порта (SPAN)Случайный порт PVLANB следующей таблице отображен диапазон портов, которые относятся к одной ASIC на модулях Catalyst 6500/6000 FastEthernet:**С помощью команды show pvlan capability (CatOS) также отображается возможность преобразования порта в порт PVLAN.** В ПО Cisco IOS нет эквивалентной команды.
- Если удалить VLAN, которая используется в конфигурации PVLAN, порты, связанные с VLAN станут неактивными.
- Настройте интерфейсы VLAN уровня 3 (L3) только для первичных VLAN. Интерфейсы VLAN для изолированных и общих VLAN являются неактивными, если в сети VLAN проходит процесс конфигурации изолированных или общих VLAN. Подробнее см. раздел "Конфигурирование частных виртуальных сетей".
- Можно расширить сети PVLAN среди коммутаторов с помощью магистралей. Порты магистрали направляют трафик из обычных VLAN, а также из первичных, изолированных и общих VLAN. Cisco рекомендует использование стандартных магистральных портов, если оба коммутатора, которые подвергаются PVLAN поддержки

транкинга.**Примечание:** Необходимо вручную ввести ту же Конфигурацию PVLAN в каждый коммутатор с участием, потому что VTP в не распространяется эту информацию.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:

В данном сценарии в устройствах в изолированной VLAN (101) есть ограничения от взаимодействия на уровне 2 друг с другом. Однако устройства не могут подключаться к Интернету. Кроме того, у порта Gig 3/26 на 4006 случайное назначение. Данная дополнительная конфигурация позволяет устройству на порте GigabitEthernet 3/26 соединиться с устройствами в изолированной VLAN. С помощью данной конфигурации также можно, например, делать резервную копию данных от всех устройств хостов PVLAN до рабочей станции администрирования. Другое использование случайных портов подразумевает соединение с внешним маршрутизатором, LocalDirector, устройством управления сетью и другими устройствами.

Конфигурация первичных и изолированных сетей VLAN

Чтобы создать первичные и вторичные сети VLAN, а также связать различные порты с данными VLAN, выполните следующие действия. В данных действиях описаны примеры ПО CatOS и Cisco IOS. Выполните соответствующий набор команд для установки OS.

1. Создайте первичную PVLAN.**CatOS**
```
Switch_CatOS> (enable) set vlan primary_vlan_id pvlan-type primary name primary_vlan
!--- Note: Thise command should be on one line.

VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 100 configuration successful
```
ПО Cisco IOS)
```
Switch_IOS(config)#vlan primary_vlan_id
Switch_IOS(config-vlan)#private-vlan primary
Switch_IOS(config-vlan)#name primary-vlan
Switch_IOS(config-vlan)#exit
```
2. Создайте одну или несколько изолированных сетей VLAN.**CatOS**
```
Switch_CatOS> (enable) set vlan secondary_vlan_id pvlan-type isolated name isolated_pvlan
!--- Note: This command should be on one line.

VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 101 configuration successful
```
ПО Cisco IOS)
```
Switch_IOS(config)#vlan secondary_vlan_id
Switch_IOS(config-vlan)#private-vlan isolated
Switch_IOS(config-vlan)#name isolated_pvlan
Switch_IOS(config-vlan)#exit
```
3. Свяжите изолированную(ые) сеть(и) VLAN с первичной VLAN.**CatOS**
```
Switch_CatOS>
```

```
(enable) set pvlan primary_vlan_id secondary_vlan_id
Vlan 101 configuration successful
Successfully set association between 100 and 101.ПО Cisco IOS)Switch_IOS(config)#vlan
primary_vlan_id
Switch_IOS(config-vlan)#private-vlan association secondary_vlan_id
Switch_IOS(config-vlan)#exit
```

4. Проверьте конфигурацию частной VLAN.CatOS
```
Switch_CatOS> (enable) show pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
100     101       isolated
```
ПО Cisco IOS)
```
Switch_IOS#show vlan private-vlan
Primary  Secondary  Type              Ports
------- --------- ----------------- -------
100     101       isolated
```

Назначение портов для сетей PVLAN

Совет: Прежде чем вы внедрите эту процедуру, выполните команду *show pvlan capability mod/port* (для CatOS), чтобы определить, может ли порт стать портом PVLAN.

Примечание: Прежде чем вы выполните Шаг 1 этой процедуры, выполните **команду switchport** в режиме конфигурации интерфейса для настройки порта как коммутируемого интерфейса Уровня 2.

1. Настройте порты хоста на всех соответствующих коммутаторах.CatOS
```
Switch_CatOS> (enable)set pvlan primary_vlan_id secondary_vlan_id mod/port
!--- Note: This command should be on one line.

Successfully set the following ports to Private Vlan 100,101: 2/20ПО Cisco
IOS)Switch_IOS(config)#interface gigabitEthernet mod/port
Switch_IOS(config-if)#switchport private-vlan host
primary_vlan_id secondary_vlan_id
!--- Note: This command should be on one line.

Switch_IOS(config-if)#switchport mode private-vlan host
Switch_IOS(config-if)#exit
```
2. Настройте случайный порт на одном из коммутаторов.CatOS
```
Switch_CatOS> (enable) set pvlan mapping primary_vlan_id secondary_vlan_id mod/port
!--- Note: This command should be on one line.

Successfully set mapping between 100 and 101 on 3/26
```
Примечание: Для Catalyst 6500/6000, когда CatOS выполнений Supervisor Engine как системное программное обеспечение, порт MSFC на Supervisor Engine (15/1 или 16/1) должен быть разнородным, если вы желаете к Коммутатору 3 уровня между VLAN.ПО Cisco IOS)
```
Switch_IOS(config)#interface
interface_type mod/port
Switch_IOS(config-if)#switchport private-vlan
mapping primary_vlan_id secondary_vlan_id
!--- Note: This command should be on one line.

Switch_IOS(config-if)#switchport mode private-vlan promiscuous
Switch_IOS(config-if)#end
```

Конфигурация уровня 3

В дополнительном разделе описаны шаги конфигурации, чтобы разрешить маршрутизатор входящего трафика PVLAN. Если необходимо только активировать соединение уровня 2, данный этап можно опустить.

1. Настройте интерфейс VLAN также, как и при настройке для обычной маршрутизации уровня 3.В данную конфигурацию входит:Конфигурация IP-адреса**Активация интерфейса с помощью команды no shutdown**Проверка существования сети VLAN в базе данных VLAN[Примеры конфигурации см. в разделе Техническая поддержка сетей VLAN/протокола VTP.]
2. Сопоставьте вторичные сети VLAN, которые необходимо маршрутизировать, первичной VLAN.`Switch_IOS(config)#`**`interface vlan`** *`primary_vlan_id`*
   `Switch_IOS(config-if)#`**`private-vlan mapping`** *`secondary_vlan_list`*
   `Switch_IOS(config-if)#`**`end`**
   Примечание: Настройте интерфейсы виртуальной локальной сети (VLAN) Уровня 3 только для основных VLAN (виртуальная локальная сеть). Интерфейсы VLAN для изолированных и общих VLAN являются неактивными с помощью конфигурации изолированных или общих VLAN.
3. **Выполните команду show interfaces private-vlan mapping (ПО Cisco IOS) или show pvlan mapping (CatOS), чтобы проверить сопоставление.**
4. **Если необходимо изменить список вторичных VLAN после конфигурации сопоставления, используйте ключевое слово add или remove.**`Switch_IOS(config-if)#`**`private-vlan mapping add`** *`secondary_vlan_list`*
   or
   `Switch_IOS(config-if)#`**`private-vlan mapping remove`** *`secondary_vlan_list`*

[Дополнительные сведения см. в разделе Сопоставление вторичных сетей VLAN интерфейсу VLAN уровня 3 первичной VLAN раздела Конфигурация частных сетей VLAN.]

Примечание: Для коммутаторов Catalyst 6500/6000 с MSFC гарантируйте, что порт от Supervisor Engine до ядра маршрутизации (например, порт 15/1 или 16/1) являются разнородными.

```
cat6000> (enable) set pvlan mapping primary_vlan secondary_vlan 15/1
Successfully set mapping between 100 and 101 on 15/1
```

Выполните команду show pvlan mapping, чтобы проверить сопоставление.

```
cat6000> (enable) show pvlan mapping
Port Primary Secondary
---- ------- ---------
15/1  100      101
```

Конфигурации

Эти конфигурации используются в данном документе:

- Access_Layer (Коммутатор Catalyst 4003: CatOS)
- Ядро (Коммутатор Catalyst 4006: ПО Cisco IOS)

Access_Layer (Коммутатор Catalyst 4003: CatOS)

```
Access_Layer> (enable) show config
 This command shows non-default configurations only.
 Use 'show config all' to show both default and non-
default configurations.
 ..............

 !--- Output suppressed. #system set system name
Access_Layer ! #frame distribution method set port
channel all distribution mac both ! #vtp set vtp domain
Cisco set vtp mode transparent set vlan 1 name default
type ethernet mtu 1500 said 100001 state active set vlan
```

```
100 name primary_for_101 type ethernet pvlan-type
primary mtu 1500 said 100100 state active !--- This is
the primary VLAN 100. !--- Note: This command should be
on one line.

 set vlan 101 name isolated_under_100 type ethernet
pvlan-type isolated mtu
 1500 said 100101 state active
!--- This is the isolated VLAN 101. !--- Note: This
command should be on one line.

 set vlan 1002 name fddi-default type fddi mtu 1500 said
101002 state active

!--- Output suppressed. #module 1 : 0-port Switching
Supervisor ! #module 2 : 24-port 10/100/1000 Ethernet
set pvlan 100 101 2/20
!--- Port 2/20 is the PVLAN host port in primary VLAN
100, isolated !--- VLAN 101. set trunk 2/3 desirable
dot1q 1-1005 set trunk 2/4 desirable dot1q 1-1005 set
trunk 2/20 off dot1q 1-1005 !--- Trunking is
automatically disabled on PVLAN host ports.

 set spantree portfast    2/20 enable
!--- PortFast is automatically enabled on PVLAN host
ports.

 set spantree portvlancost 2/1  cost 3

!--- Output suppressed. set spantree portvlancost 2/24
cost 3 set port channel 2/20 mode off !--- Port
channeling is automatically disabled on PVLAN !--- host
ports.

 set port channel 2/3-4 mode desirable silent
 !
 #module 3 : 34-port 10/100/1000 Ethernet
 end
```

Ядро (Коммутатор Catalyst 4006: ПО Cisco IOS)

```
Core#show running-config
 Building configuration...

 !--- Output suppressed. ! hostname Core ! vtp domain
Cisco vtp mode transparent !--- VTP mode is transparent,
as PVLANs require. ip subnet-zero ! vlan 2-4,6,10-11,20-
22,26,28 ! vlan 100 name primary_for_101 private-vlan
primary private-vlan association 101 ! vlan 101 name
isolated_under_100 private-vlan isolated ! interface
Port-channel1 !--- This is the port channel for
interface GigabitEthernet3/1 !--- and interface
GigabitEthernet3/2. switchport switchport trunk
encapsulation dot1q switchport mode dynamic desirable !
interface GigabitEthernet1/1 ! interface
GigabitEthernet1/2 ! interface GigabitEthernet3/1 !---
This is the trunk to the Access_Layer switch. switchport
trunk encapsulation dot1q switchport mode dynamic
desirable channel-group 1 mode desirable ! interface
GigabitEthernet3/2 !--- This is the trunk to the
Access_Layer switch. switchport trunk encapsulation
dot1q switchport mode dynamic desirable channel-group 1
mode desirable ! interface GigabitEthernet3/3 ! !---
There is an omission of the interface configuration !---
that you do not use. ! interface GigabitEthernet3/26
```

```
  switchport private-vlan mapping 100 101
  switchport mode private-vlan promiscuous
!--- Designate the port as promiscuous for PVLAN 101. !
!--- There is an omission of the interface configuration
!--- that you do not use. ! !--- Output suppressed.
interface Vlan25 !--- This is the connection to the
Internet. ip address 10.25.1.1 255.255.255.0 ! interface
Vlan100 !--- This is the Layer 3 interface for the
primary VLAN. ip address 10.1.1.1 255.255.255.0 private-
vlan mapping 101 !--- Map VLAN 101 to the VLAN interface
of the primary VLAN (100). !--- Ingress traffic for
devices in isolated VLAN 101 routes !--- via interface
VLAN 100.
```

Частные сети VLAN в нескольких коммутаторах

Частные сети VLAN можно использовать в нескольких коммутаторах двумя способами. В этом разделе описаны данные способы:

- Обычные магистрали
- Магистрали частных сетей VLAN

Обычные магистрали

С помощью обычных VLAN сети PVLAN могут взаимодействовать с несколькими коммутаторами. Порт магистрали переносит первичную и вторичные VLAN на соседний коммутатор. Порт магистрали взаимодействует с частной VLAN также, как и с другими сетями VLAN. Функция сетей PVLAN в нескольких коммутаторах состоит в том, чтобы трафик изолированного порта на одном коммутаторе не достигал изолированного порта на другом коммутаторе.

Настройте сети PVLAN на всех промежуточных устройствах, в которых находятся устройства без портов PVLAN, чтобы поддержать безопасность конфигурации PVLAN и избежать другого использования сетей VLAN, настроенных в качестве сетей PVLAN.

Порты магистрали направляют трафик из обычных VLAN, а также из первичных, изолированных и общих VLAN.

Совет: Cisco рекомендует использование стандартных магистральных портов, если оба коммутатора, которые подвергаются PVLAN поддержки транкинга.

Так как протокол VTP не поддерживает сети PVLAN, необходимо настроить их вручную на всех коммутаторах в сети уровня 2. Если не настроить объединение первичной и вторичных сетей VLAN в некоторых коммутаторах в сети, базы данных уровня 2 в данных коммутаторах не объединятся. Это может привести к лавинной маршрутизации трафика PVLAN на данных коммутаторах.

Магистрали частных сетей VLAN

Порт магистрали PVLAN может вмещать несколько вторичных сетей PVLAN, а также сети, отличные от сетей PVLAN. Пакеты получают и передают с помощью тегов вторичных или обычных VLAN на портах магистрали PVLAN.

Поддерживается только инкапсуляция IEEE 802.1q. С помощью изолированных портов магистрали можно объединять трафик всех вторичных портов на магистрали. С помощью случайных портов магистрали можно объединять несколько случайных портов, необходимых в данной топологии, в один порт магистрали, который вмещает несколько первичных сетей VLAN.

Используйте изолированные порты магистрали частных сетей VLAN при предупреждении использования Частных VLAN отдельных портов хоста для переноса несколько интерфейсов VLAN, или обычные VLAN или для множественных Частных VLAN доменов. Это делает его полезным для соединения нисходящего коммутатора, который не поддерживает Частные VLAN.

Частные VLAN Разнородные Транки используются в ситуациях, где Частный VLAN разнородный порт хоста обычно используется, но где необходимо нести несколько интерфейсов VLAN, или обычный vlans или для множественных Частных VLAN доменов. Это делает его полезным для соединения вышестоящего маршрутизатора, который не поддерживает Частные VLAN.

Дополнительные сведения см. в разделе Магистрали частных сетей VLAN.

Чтобы настроить интерфейс в качестве порта магистрали PVLAN, см. раздел Конфигурация интерфейса уровня 2 в качестве порта магистрали PVLAN.

Чтобы настроить интерфейс в качестве случайного порта магистрали, см. раздел Конфигурация интерфейса уровня 2 в качестве случайного порта магистрали.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

CatOS

- **show pvlan - Отображает конфигурацию PVLAN.** Проверьте связь изолированных и первичных сетей VLAN друг с другом. А также проверьте отображение портов хоста.
- **show pvlan mapping — отображает сопоставление PVLAN с конфигурацией на случайных портах.**

ПО Cisco IOS)

- **show vlan private-vlan — отображает сведения о PVLAN со связанными портами.**
- *show interface mod/port switchport — отображает сведения об интерфейсах.* Проверьте правильность работы рабочего режима, а также рабочие параметры PVLAN.
- **show interfaces private-vlan mapping — отображает настроенное сопоставление сетей PVLAN.**

Процедура проверки

Выполните следующие действия:

1. Проверьте конфигурацию PVLAN на коммутаторах.Проверьте связь/сопоставление первичных и вторичных сетей PVLAN друг с другом. А также проверьте включение необходимых портов.Access_Layer> (enable) **show pvlan**

```
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
 100     101       isolated         2/20

Core#show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- -----------
100     101       isolated          Gi3/26
```

2. Проверьте правильность конфигурации случайного порта. , – **promiscuous, VLAN – 100 101**.Core#**show interface gigabitEthernet 3/26 switchport**

```
Name: Gi3/26
Switchport: Enabled
Administrative Mode: private-Vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative Private VLAN Host Association: none
Administrative Private VLAN Promiscuous Mapping: 100
(primary_for_101) 101 (isolated_under_100)
Private VLAN Trunk Native VLAN: none
Administrative Private VLAN Trunk Encapsulation: dot1q
Administrative Private VLAN Trunk Normal VLANs: none
Administrative Private VLAN Trunk Private VLANs: none
Operational Private VLANs:
100 (primary_for_101) 101 (isolated_under_100)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

3. Запустите пакет запроса ICMP-эхо из порта хоста на случайный порт.Помните, что так как оба устройства находятся в первичной VLAN, они могут быть в одной сети.host_port#**show arp**

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.100              -   0008.a390.fc80  ARPA   FastEthernet0/24
!--- The Address Resolution Protocol (ARP) table on the client indicates !--- that no MAC
addresses other than the client addresses are known. host_port#ping 10.1.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
!--- The ping is successful. The first ping fails while the !--- device attempts to map via
ARP for the peer MAC address. host_port#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.100              -   0008.a390.fc80  ARPA   FastEthernet0/24
Internet  10.1.1.254              0   0060.834f.66f0  ARPA   FastEthernet0/24
!--- There is now a new MAC address entry for the peer.
```

4. Выполните запрос ICMP-эхо между портами хоста. host_port_2 (10.1.1.99) ICMP-

host_port (10.1.1.100). Этот эхо-запрос не удался. Однако выполнение запроса ICMP-эхо из другого порта хоста на случайный порт прошло успешно.

```
host_port_2#ping 10.1.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
!--- The ping between host ports fails, which is desirable. host_port_2#ping 10.1.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!--- The ping to the promiscuous port still succeeds. host_port_2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.99               -   0005.7428.1c40  ARPA   Vlan1
Internet  10.1.1.254              2   0060.834f.66f0  ARPA   Vlan1
!--- The ARP table includes only an entry for this port and !--- the promiscuous port.
```

Устранение неполадок

Поиск и устранение неполадок в сетях PVLAN

В данном разделе описаны некоторые основные проблемы, которые возникают во время конфигурации PVLAN.

Проблема 1

Отображается следующее сообщение об ошибке: `%PM-SP-3-ERR_INCOMP_PORT: <mod/port> is set to inactive because <mod/port> is a trunk port`

Это сообщение об ошибках может быть отображено по множественным причинам, как обсуждено здесь.

Пояснение - 1: Из-за ограничений аппаратного обеспечения модули коммутаторов Catalyst 6500/6000 10/100-Mbps ограничивают конфигурацию изолированного или общего порта VLAN, если порт в специализированной интегральной схеме одного COIL является магистралью, назначением SPAN или случайным портом PVLAN. (Специализированная интегральная схема COIL контролирует 12 портов на большинстве модулей и 48 портов на модуле Catalyst 6548.). В таблице раздела Правила и ограничения данного документа представлены сведения об ограничении портов на модулях коммутаторов Catalyst 6500/6000 10/100-Mbps.

Процедура разрешения - 1: Если нет поддержки на порте PVLAN, выберите порт в другой ASIC на данном или на другом модуле. **Чтобы возобновить деятельность портов, удалите конфигурацию изолированного или общего порта VLAN и выполните команды shutdown и no shutdown.**

Пояснение - 2: Если порты настроены вручную или по умолчанию к *выбираемому динамическому* или режим *динамического автоматического режима*.

Процедура разрешения - 2: Настройте порты как режим доступа с командой **switchport mode access**. Для повторной активации портов выполните **команду shutdown** и **команду no**

shutdown.

Примечание: В программном обеспечении Cisco IOS версии 12.2(17a)SX и более поздних версиях, 12 ограничений порта не применяются к WS-X6548-RJ-45, WS-X6548-RJ-21 и Модулям коммутации Ethernet WS-X6524-100FX-MM. Дополнительные сведения об ограничениях конфигураций сетей PVLAN с помощью других функций см. в разделе Ограничения и другие функции документа Конфигурация частных сетей VLAN.

Проблема 2

В процессе конфигурации PVLAN может отобразится одно из следующих сообщений:

- host_port_2#**ping 10.1.1.100**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
!--- The ping between host ports fails, which is desirable. host_port_2#ping 10.1.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!--- The ping to the promiscuous port still succeeds. host_port_2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.99               -   0005.7428.1c40  ARPA   Vlan1
Internet  10.1.1.254              2   0060.834f.66f0  ARPA   Vlan1
!--- The ARP table includes only an entry for this port and !--- the promiscuous port.
```

- host_port_2#**ping 10.1.1.100**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.100, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
!--- The ping between host ports fails, which is desirable. host_port_2#ping 10.1.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.254, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
!--- The ping to the promiscuous port still succeeds. host_port_2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.99               -   0005.7428.1c40  ARPA   Vlan1
Internet  10.1.1.254              2   0060.834f.66f0  ARPA   Vlan1
!--- The ARP table includes only an entry for this port and !--- the promiscuous port.
```

Пояснение: Из-за ограничений аппаратного обеспечения модули коммутаторов Catalyst 6500/6000 10/100-Mbps ограничивают конфигурацию изолированного или общего порта VLAN, если порт в специализированной интегральной схеме одного COIL является магистралью, назначением SPAN или случайным портом PVLAN. (Специализированная интегральная схема COIL контролирует 12 портов на большинстве модулей и 48 портов на модуле Catalyst 6548.). В таблице раздела Правила и ограничения данного документа представлены сведения об ограничении портов на модулях коммутаторов Catalyst 6500/6000 10/100-Mbps.

Процедура устранения неполадок: Выполните команду show pvlan capability (CatOS), которая указывает преобразование порта в порт PVLAN. Если нет поддержки для PVLAN на определенном порте, выберите порт в другой ASIC на данном или на другом модуле.

Примечание: В программном обеспечении Cisco IOS версии 12.2(17a)SX и более поздних версиях, 12 ограничений порта не применяются к WS-X6548-RJ-45, WS-X6548-RJ-21 и Модулям коммутации Ethernet WS-X6524-100FX-MM. Дополнительные сведения об ограничениях конфигураций сетей PVLAN с помощью других функций см. в разделе Ограничения и другие функции документа Конфигурация частных сетей VLAN.

Проблема 3

Не удается настроить PVLAN на некоторых платформах.

Разрешение: Проверьте, чтобы платформа поддерживала сети PVLAN. Чтобы определить, поддерживает ли платформа или версия ПО сети PVLAN перед началом конфигурации, см. раздел Матрица поддержки коммутаторов Catalyst на частных сетях VLAN.

Проблема 4

На MSFC коммутатора Catalyst 6500/6000 невозможно выполнить запрос ICMP-эхо на устройство, которое соединено с изолированным портом на данном коммутаторе.

Разрешение: На модуле управления проверьте, чтобы данный порт на MSFC (15/1 или 16/1) является случайным.

```
cat6000> (enable) set pvlan mapping primary_vlan secondary_vlan 15/1
Successfully set mapping between 100 and 101 on 15/1
```

Также настройте интерфейс VLAN на MSFC, как указано в разделе Конфигурация уровня 3 данного документа.

Проблема 5

С помощью команды no shutdown невозможно активировать интерфейс VLAN для изолированных или общих сетей VLAN.

Разрешение: Из-за особенностей сетей PVLAN активировать интерфейс VLAN для изолированной VLAN или VLAN сообщества невозможно. Можно активировать только тот интерфейс VLAN, который относится к первичной VLAN.

Проблема 6

На устройствах Catalyst 6500/6000 с MSFC/MSFC2 записи ARP, полученные на интерфейсах PVLAN уровня 3 не устаревают.

Разрешение: Записи ARP, полученные на интерфейсах частных VLAN уровня 3, являются фиксированными и не устаревают. С помощью подключения нового оборудования с помощью IP-адреса создается сообщение. Запись ARP не создается. Таким образом, необходимо удалить ARP-записи порта PVLAN при изменении MAC-адреса. Чтобы добавить или удалить ARP-записи PVLAN вручную, выполните следующие команды:

```
Router(config)#no arp 11.1.3.30
IP ARP:Deleting Sticky ARP entry 11.1.3.30
Router(config)#arp 11.1.3.30 0000.5403.2356 arpa
IP ARP:Overwriting Sticky ARP entry 11.1.3.30, hw:00d0.bb09.266e by
hw:0000.5403.2356
```

Второй способ – выполнить команду no ip sticky-arp в ПО Cisco IOS версии 12.1(11b)E и более поздних.

Дополнительные сведения

- Матрица поддержки частной VLAN коммутатором Catalyst
- Обеспечение безопасности сетей с использованием частных виртуальных локальных сетей (VLAN) и списков контроля доступа
- Конфигурирование частной виртуальной локальной сети VLAN
- Поддержка продуктов для ЛВС
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация