Частный VLAN и конфигурация UCS Cisco с VMware DVS или Cisco Nexus 1000v

Содержание

Введение

Этот документ описывает частный VLAN (PVLAN) поддержка в системе Cisco UCS (UCS) в выпуске 2.2. (2C) и позже

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- UCS
- Cisco Nexus 1000 V (N1K) или VMware DVS
- VMware
- Уровень 2 (L2) коммутация

Используемые компоненты

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.

Общие сведения

Теория

Частной VLAN является VLAN, настроенная для изоляции L2 от других портов в частном VLAN том же. Порты, которые принадлежат PVLAN, привязаны к единому набору VLAN поддержки, которые используются для создания структуры PVLAN.

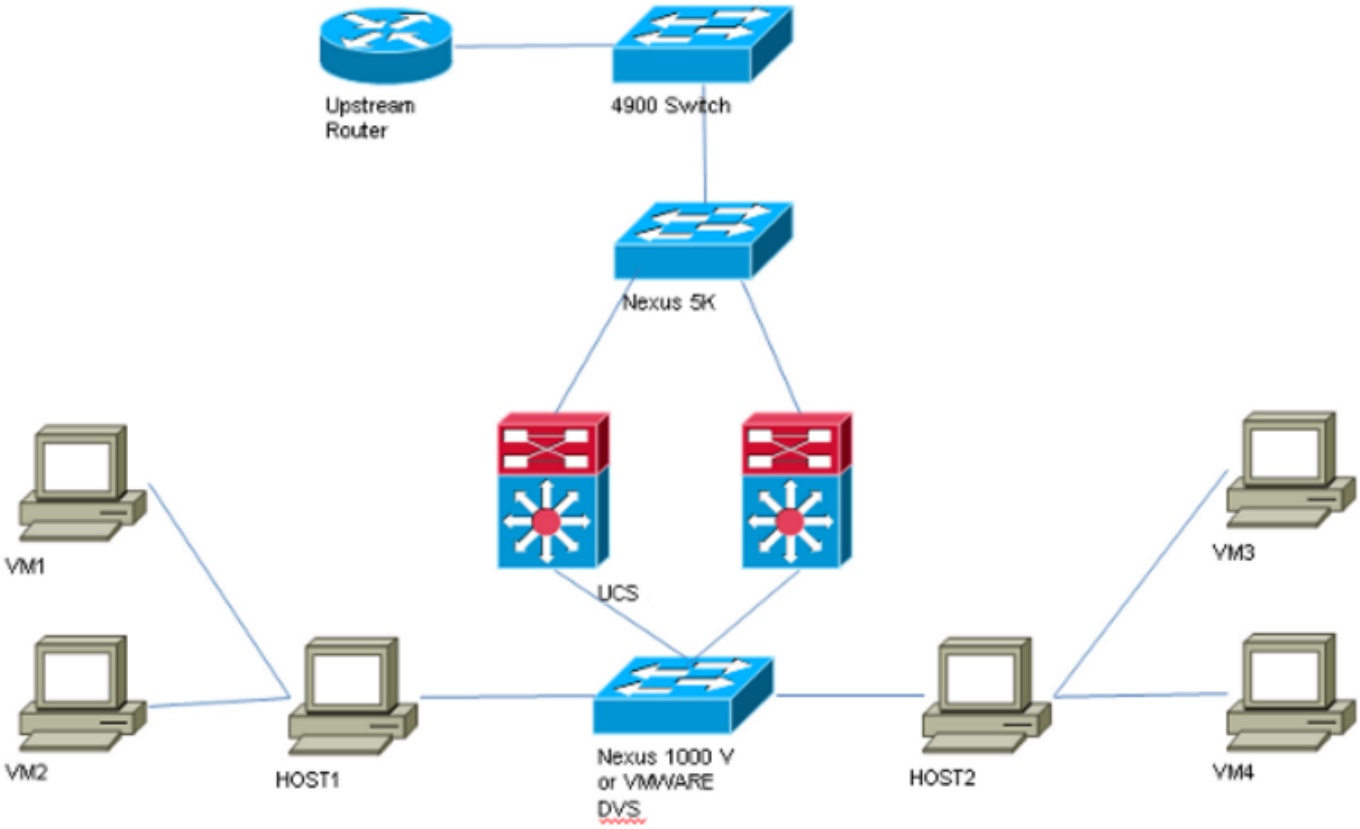
Существует три типа портов PVLAN:

- **Случайный порт** связывается со всеми другими портами PVLAN и является портом, используемым для передачи с устройствами за пределами PVLAN.
- **Изолированный порт** имеет завершенное разделение L2 (включая широковещательные сообщения) от других портов в том же PVLAN за исключением случайного порта.
- **Общий порт** может связаться с другими портами в том же PVLAN, а также случайном порту. Общие порты изолированы в L2 от портов в других сообществах или отдельных портов PVLAN. Широковещательные сообщения только распространяются к другим портам в сообществе и случайном порту.

См. RFC 5517, Частные VLAN Cisco Systems: Масштабируемая Безопасность в Мультиклиентской среде для понимания теории, операции и понятий PVLAN.

Настройка

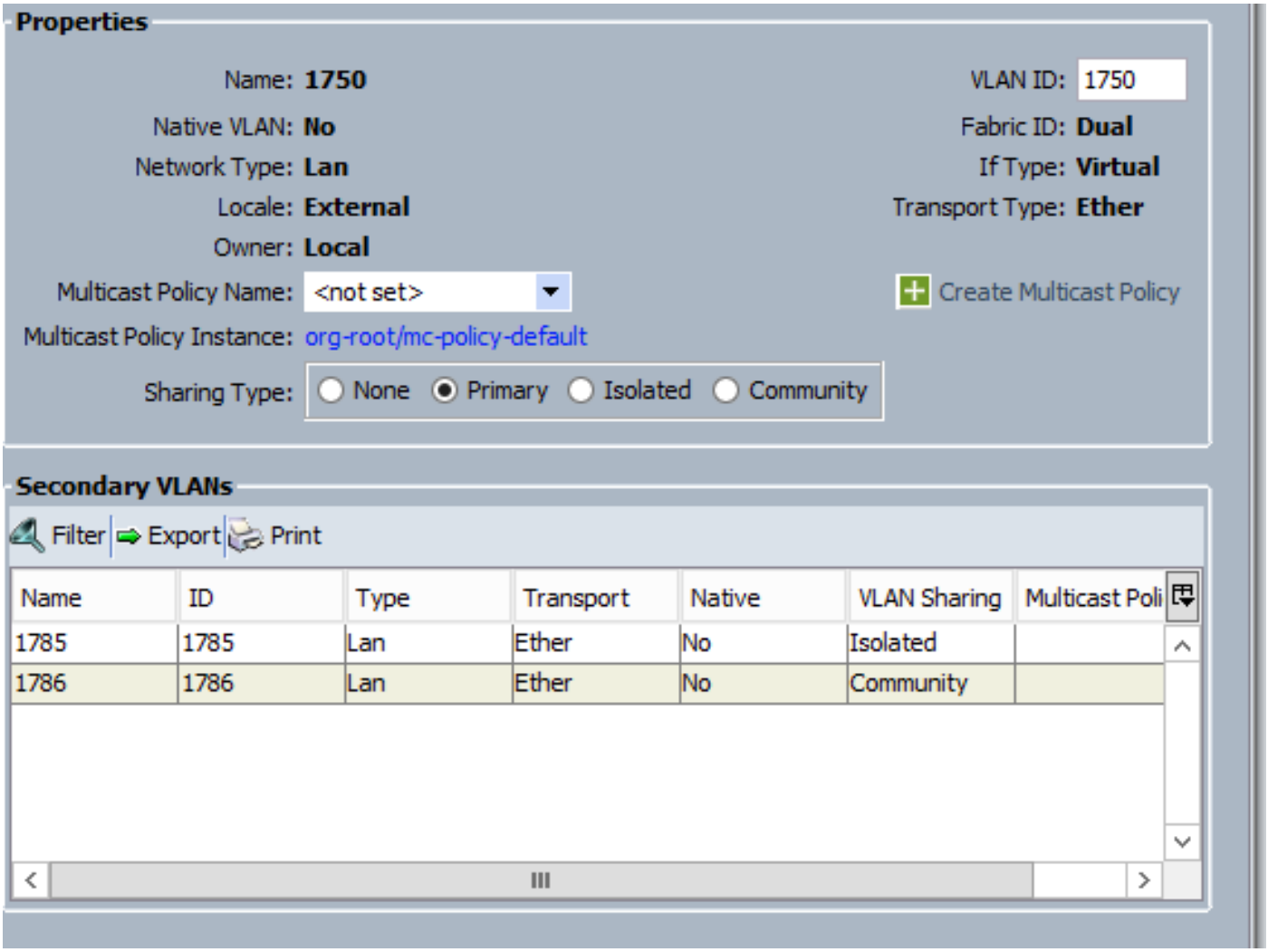
с Nexus 1000v или VMware DVS



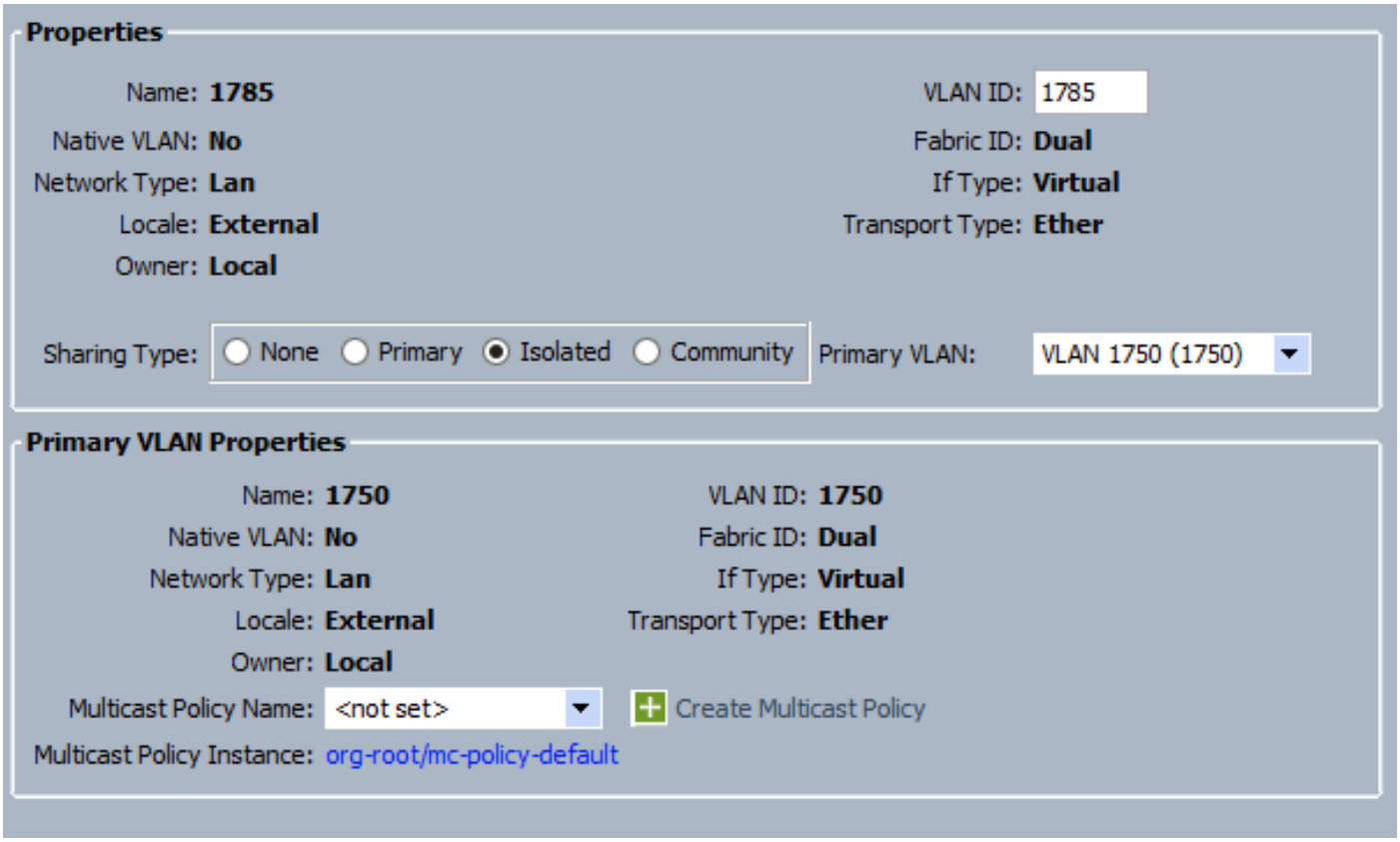
Примечание: Данный пример использует vlan 1750 в качестве основного , 1785 столь же отдельный и 1786 года как vlan сообщества

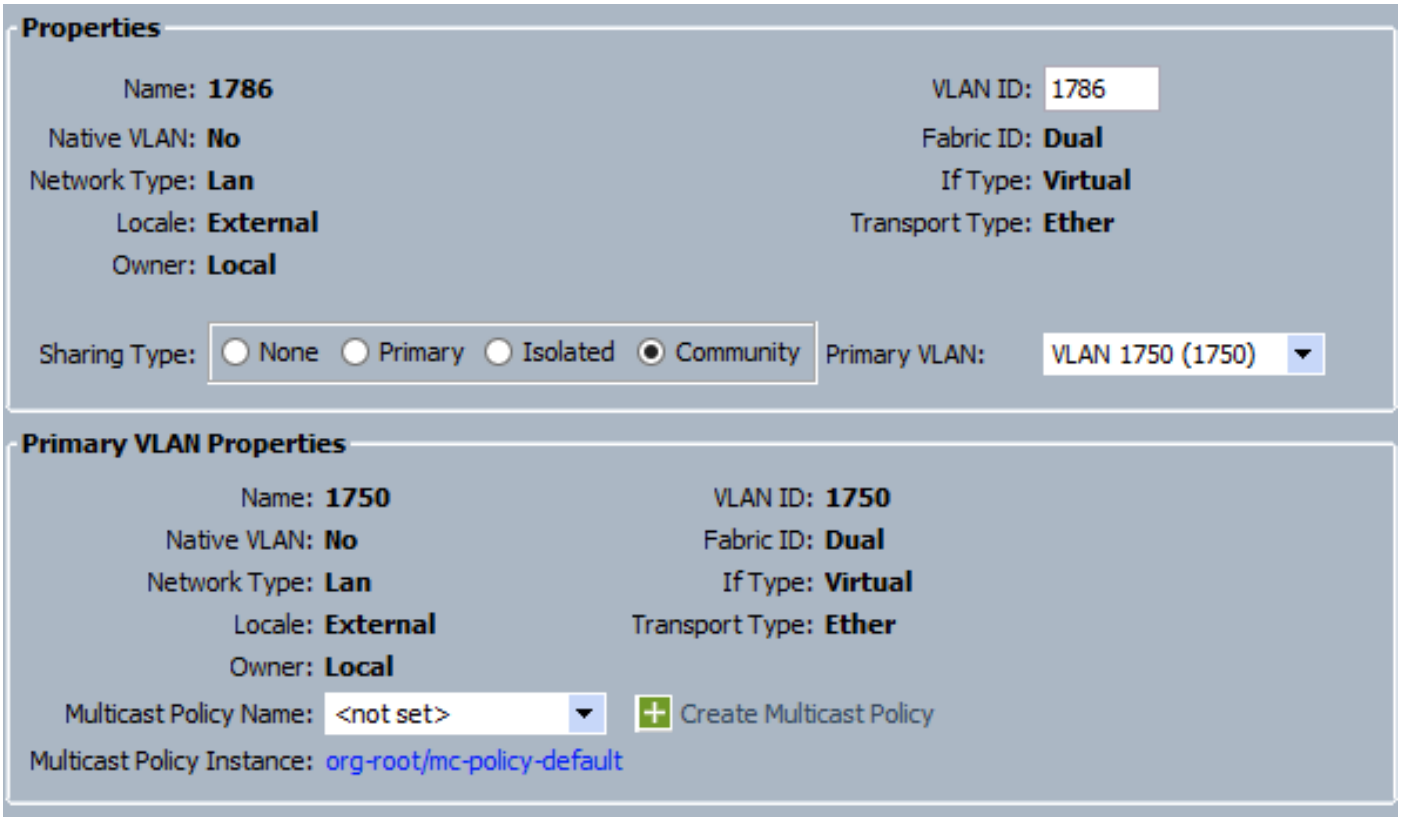
Конфигурация UCS с VMware DVS

1. Для создания основного VLAN (виртуальная локальная сеть) нажмите **Primary** как Совместное использование Типа и введите **ИДЕНТИФИКАТОР VLAN** 1750:

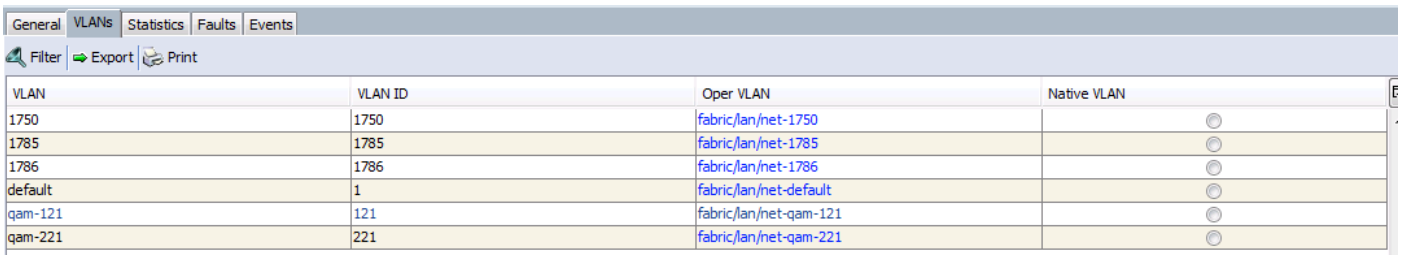


2. Создайте Отдельный и Vlans Сообщества соответственно как ниже. Ни один из них не должен быть Исходной виртуальной локальной сетью (VLAN)





3. vnic на профиле сервиса несет обычный vlans, а также pvlans



4.

Port-channel канала от абонента к оператору на UCS несет обычный vlans, а также pvlans

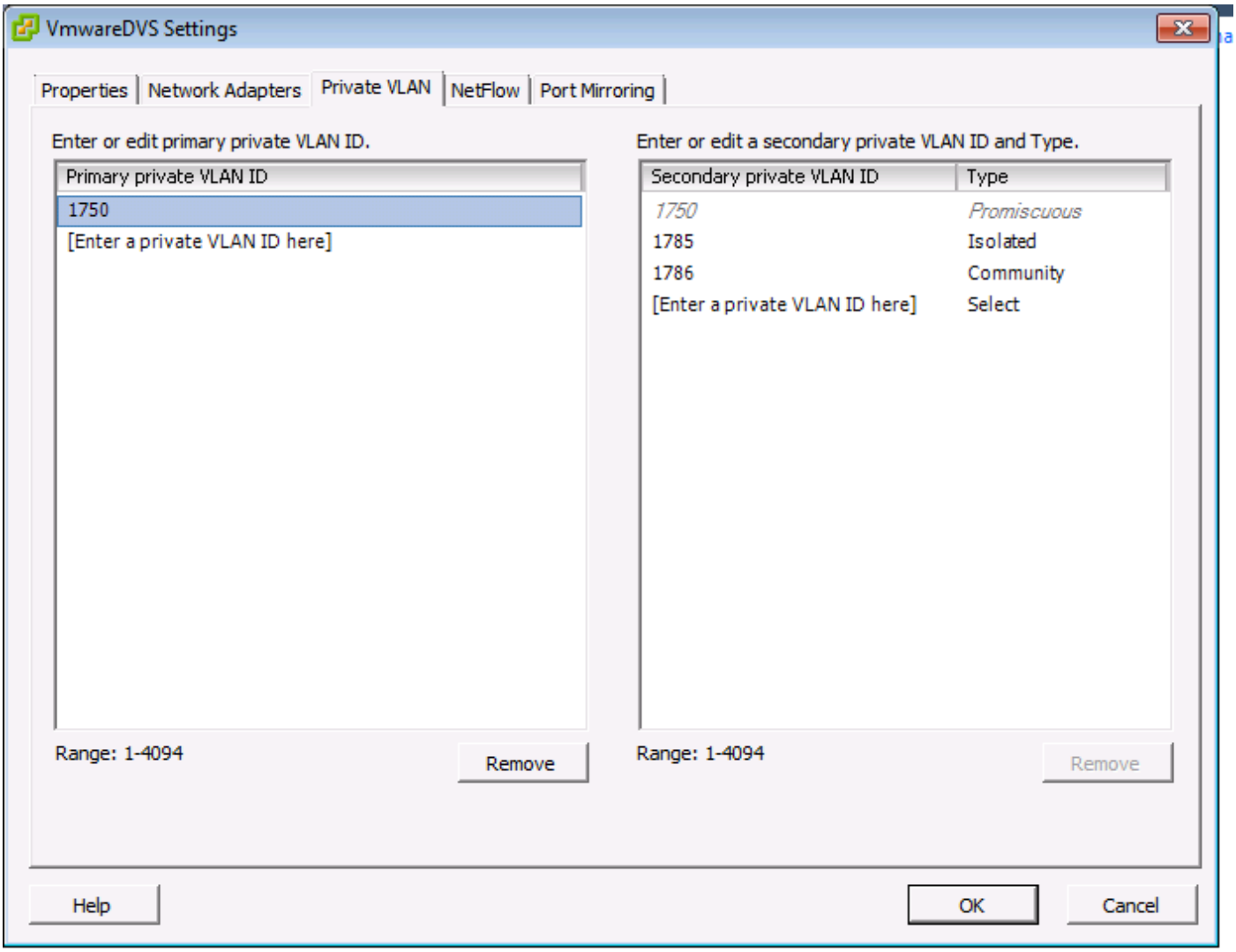
интерфейсный порт-канал1
описание U: Канал от абонента к оператору
!-- switchport mode trunk
прикрепление границы
switchport trunk allowed vlan 1,121,221,321,1750,1785-1786
скорость 10000

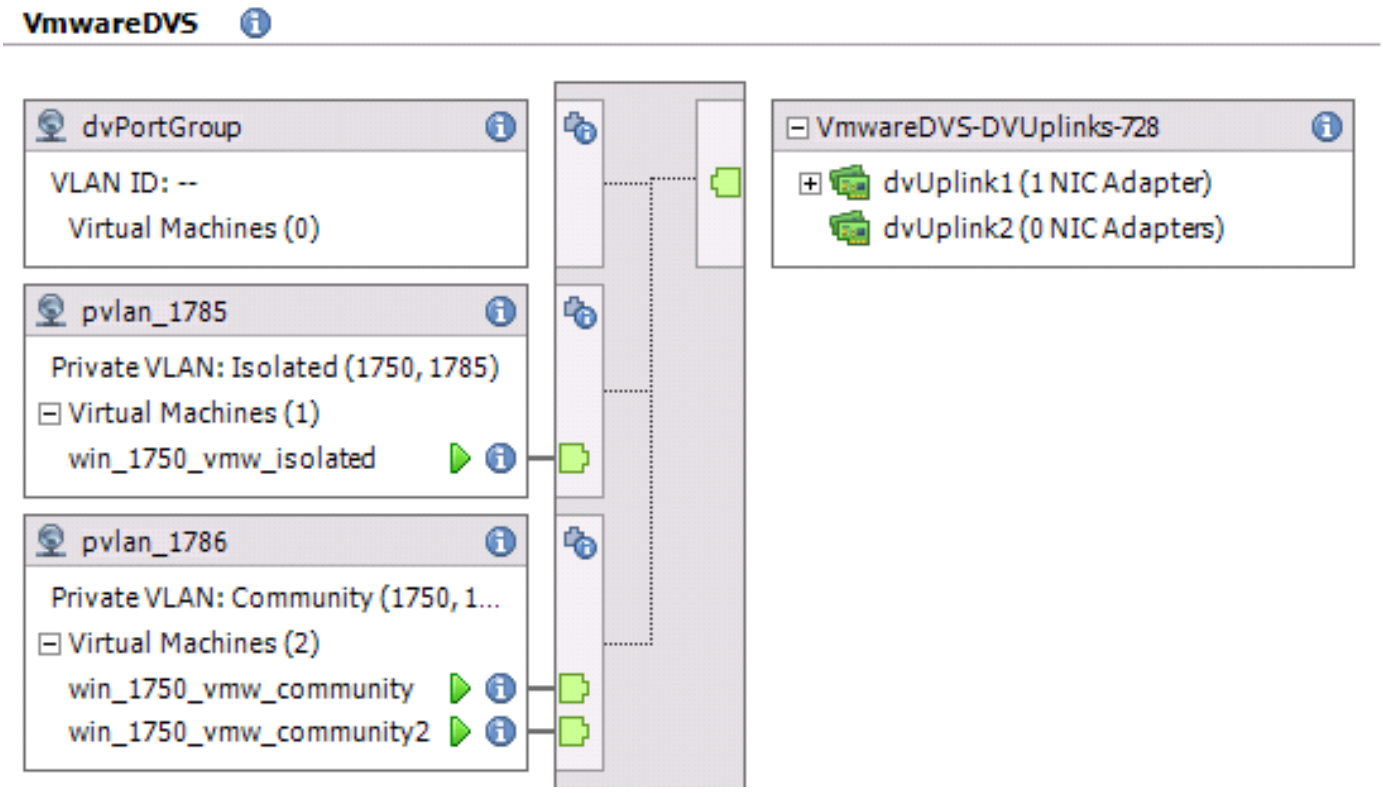
F240-01-09-UCS4-A (nxos) #

F240-01-09-UCS4-A (nxos) # show vlan private-vlan
Основные вторичные порты типа
------- --------- --------------- --

1750 1785 изолирован
Сообщество 1786 года 1750 года

Конфигурация на VMware DVS





Конфигурация восходящего коммутатора N5k

feature private-vlan

vlan 1750
основной private-vlan
private-vlan association 1785-1786

vlan 1785
private-vlan изолирован

vlan 1786
сообщество private-vlan

интерфейсный Vlan1750

IP-адрес 10.10.175.252/24
сопоставление "частной виртуальной локальной сети" 1785-1786

no shutdown

интерфейсный-порт-channel114

Описание к UCS
!-- switchport mode trunk
switchport trunk allowed vlan 1,121,154,169,221,269,321,369,1750,1785-1786
spanning-tree port type edge
spanning-tree bpduguard enable
spanning-tree bpdufilter включает
vpc 114 <===, если существует 5k пара в конфигурации vPC только тогда, добавляет эту линию к обоим N5k

Конфигурация восходящего потока 4900 коммутаторов

На этих 4900 коммутаторах сделайте эти шаги и установите случайный порт. PVLAN заканчивается в случайном порту.

1. Включите Характеристику PVLAN при необходимости.
2. Создайте и привяжите VLAN, как сделано на Nexus 5K.
3. Создайте случайный порт на выходном порте этих 4900 коммутаторов. С этого момента пакеты от VLAN 1785 и 1786 замечены на VLAN 1750 в этом случае.

```
Switch(config-if)#switchport mode trunk
switchport private-vlan mapping 1785-1786
switchport mode private-vlan promiscuous
```

На вышестоящем маршрутизаторе создайте подинтерфейс для VLAN 1750 только. На этом уровне требования зависят от конфигурации сети, которую вы используете:

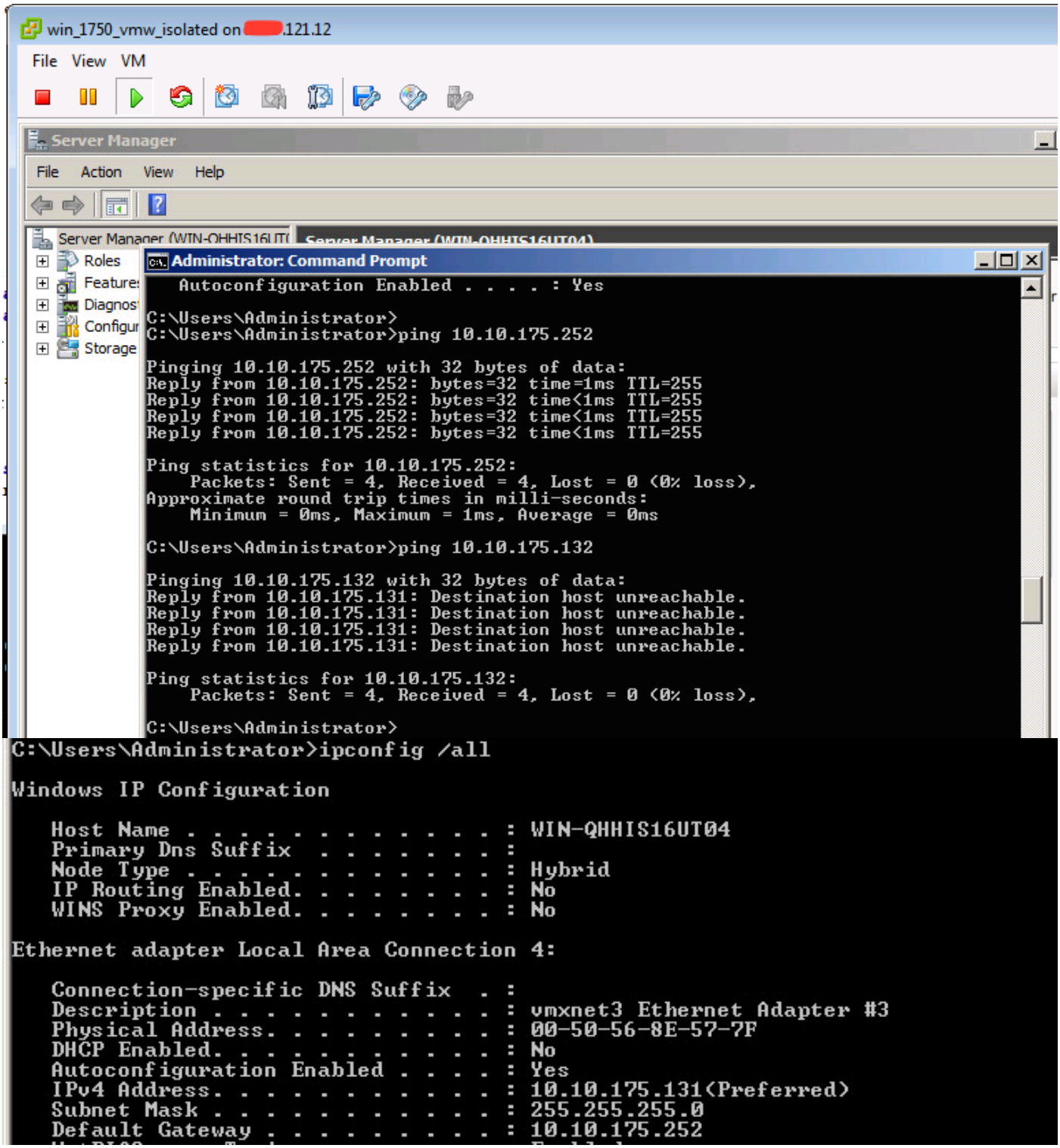
1. интерфейсный GigabitEthernet0/1.1
2. encapsulation dot1Q 1750

3. IP address10.10.175.254/24

Устранение неисправностей

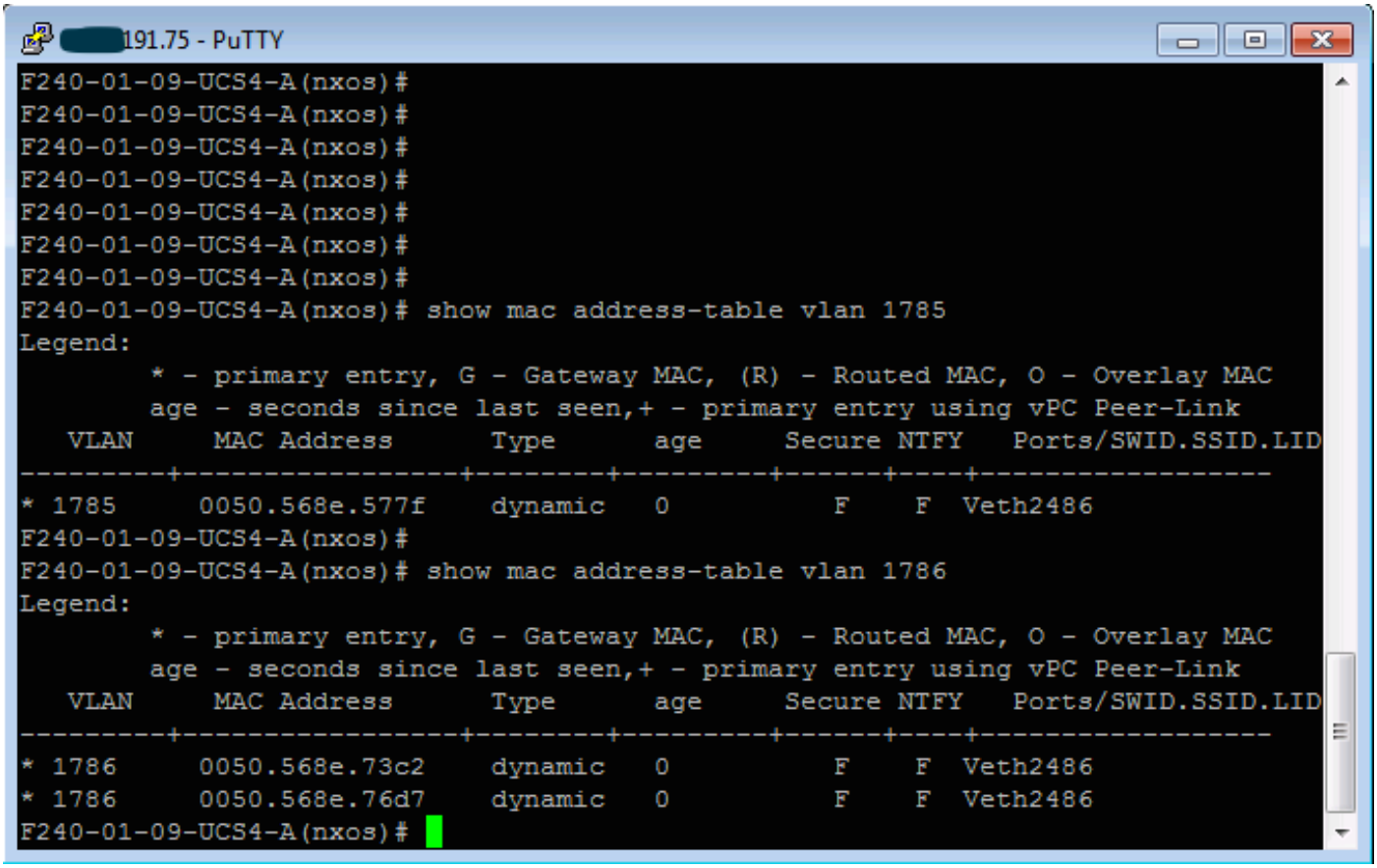
Эта процедура описывает, как протестировать конфигурацию на VMware dvs использующий pvlan.

1. Выполните эхо-запросы к другим системам, настроенным в группе портов, а также маршрутизаторе или другом устройстве в случайном порту. Эхо-запросы к устройству мимо случайного порта должны работать, в то время как те к другим устройствам в выделенном VLAN должны отказать.



Проверьте таблицы MAC-адресов для наблюдения, где изучается MAC. На всех коммутаторах MAC должен быть в выделенном VLAN за исключением коммутатора со случайным портом. На разнородном коммутаторе MAC должен быть в основном VLAN (виртуальная локальная сеть).

2. UCS



3. проверьте восходящий n5k для того же Mac, выходные данные, подобные вышеупомянутым выходным данным, должны присутствовать на n5k

```
f241-01-08-5596-a# show mac address-table | inc 577f
* 1785      0050.568e.577f    dynamic   170         F    F  Po114
f241-01-08-5596-a#
f241-01-08-5596-a# show mac address-table | inc 73c2
* 1786      0050.568e.73c2    dynamic   10          F    F  Po114
f241-01-08-5596-a# show mac address-table | inc 76d7
* 1786      0050.568e.76d7    dynamic   30          F    F  Po114
f241-01-08-5596-a#
```

Использование конфигурации Nexus 1000v с портом Promiscous на восходящем N5k

Конфигурация UCS

Конфигурация UCS (inclusing профиль сервиса vnic config) останется то же согласно вышеупомянутому примеру с VMware DVS

Конфигурация N1k

feature private-vlan

vlan 1750
основной private-vlan
private-vlan association 1785-1786

vlan 1785
private-vlan изолирован

vlan 1786
сообщество private-vlan

тот же профиль порта каскадного соединения используется для обычного vlans и pvlans. В данном примере vlan 121 и 221 обычный vlans, но можно изменить их соответственно

ethernet типа профиля порта pvlan-uplink-no-prom
!-- switchport mode trunk
mtu 9000
switchport trunk allowed vlan 121,221,1750,1785-1786
автоматический режим channel-group на прикреплении Mac

система vlan 121
no shutdown
состояние включено
группа портов VMware

тип профиля порта vethernet pvlan_1785
switchport mode private-vlan host
1750 switchport private-vlan host-association 1785
switchport access vlan 1785
no shutdown
состояние включено
группа портов VMware

тип профиля порта vethernet pvlan_1786
switchport mode private-vlan host
switchport access vlan 1786
1750 switchport private-vlan host-association 1786
no shutdown
состояние включено
группа портов VMware

Устранение неисправностей

Эта процедура описывает, как протестировать конфигурацию.

1. Выполните эхо-запросы к другим системам, настроенным в группе портов, а также маршрутизаторе или другом устройстве в случайном порту. Эхо-запросы к устройству мимо случайного порта должны работать, в то время как те к другим устройствам в выделенном

VLAN должны отказать, как показано в предыдущем разделе