

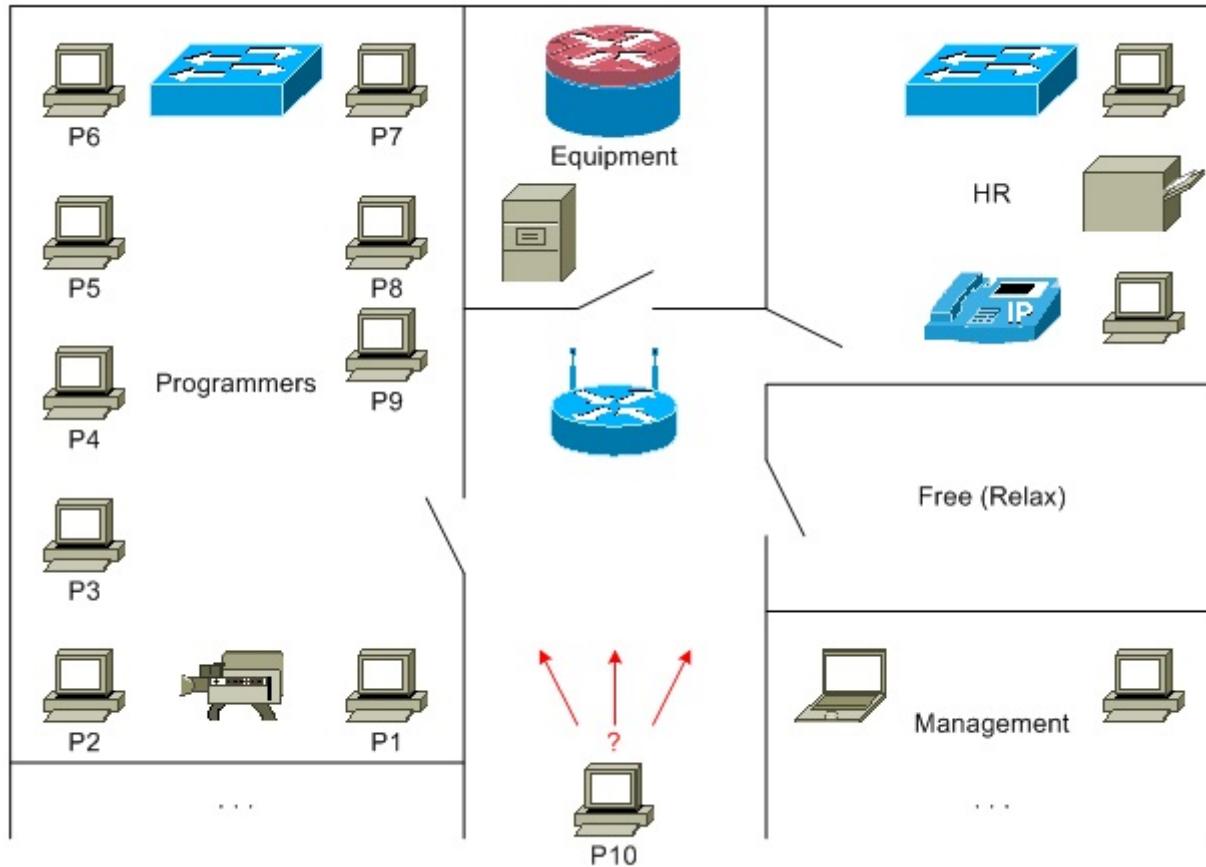
ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ АКТИВНОГО СЕТЕВОГО ОБОРУДОВАНИЯ

4.1

ВИЛАНЫ

Версия 2.4

4.1.1.1



У компании возникла необходимость разместить еще одного программиста. Что можно сделать?

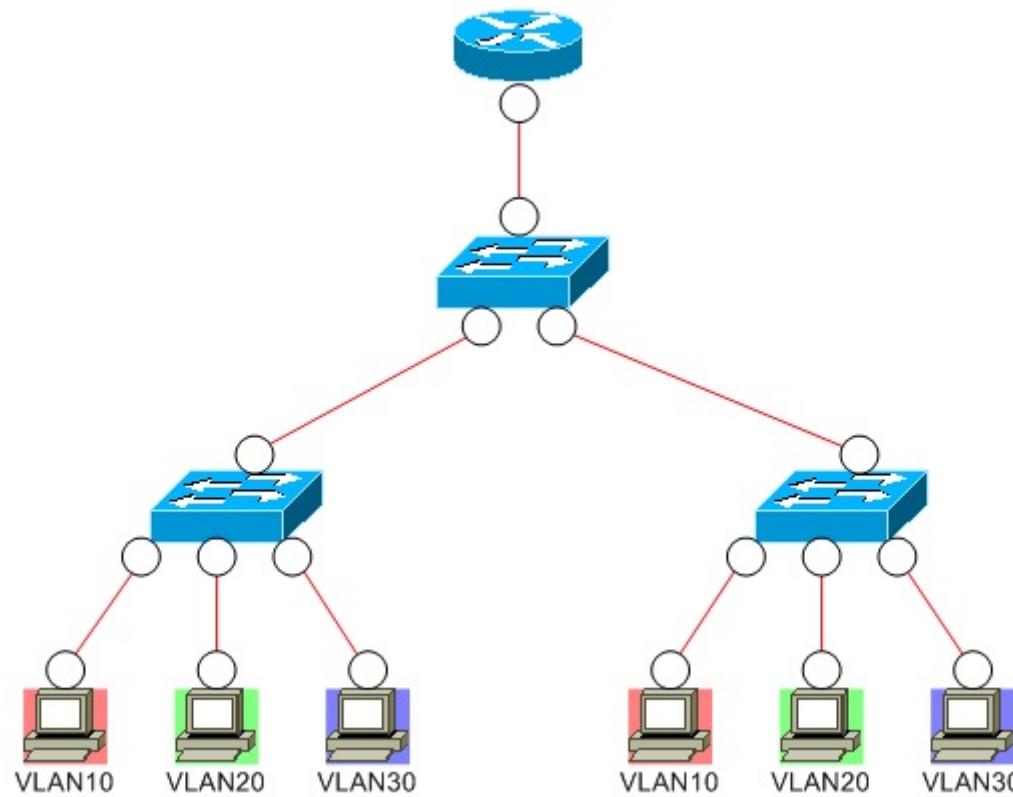
4.1.1.2

Виртуальные ЛКС -- Virtual LANs (VLANs), называемые также виланами, представляют собой множество реализаций находящей все большее применение концепции виртуальных машин.

Виланы позволяют строить на базе одной физической сети некоторое количество логических, причем логические сети будут существовать независимо друг от друга, то есть переданный в одной сети пакет никогда не будет принят в другой (если дополнительно об этом не позаботиться).

Применительно к подавляющему числу практических случаев, встречающееся в предыдущем предложении слово «сеть» следует заменить словом «сегмент».

4.1.1.3



Пример организации виланов

4.1.1.4

Основные достоинства виленов:

1. Использование виленов помогает контролировать трафик, в первую очередь широковещательный.
2. С помощью виленов обеспечивают дополнительную защиту информации.
3. Вилены лучше адаптированы к изменениям в составе сетевого оборудования.

Основные недостатки виленов:

1. Необходимость наличия значительно более дорогостоящего сетевого оборудования (например, сетевые адAPTERЫ типа **Server** и коммутаторы не ниже уровня L2+).
2. Применение виленов приводит к увеличению вычислительной нагрузки по причине вносимых количественных и качественных дополнений.

4.1.1.5

Виланы связаны, в первую очередь, с технологиями коммутации пакетов, то есть с коммутаторами.

Место виланов -- это «граница» СПД, то есть часть СПД, которая примыкает к пользовательским станциям (хотя она может быть организована достаточно сложно).

4.1.2.1

При рассмотрении виленов выделяют три группы понятий:

1. *Физические порты* (physical ports), то есть точки подключения сетевого оборудования (сетевых адаптеров, коммутаторов и другого).
2. *Физические соединения (каналы)* (links) между физическими портами.
3. *Виртуальные сетевые интерфейсы и подинтерфейсы* (subinterfaces) сетевого оборудования. (Не путать с логическими сетевыми интерфейсами при IP aliasing.)

4.1.2.2

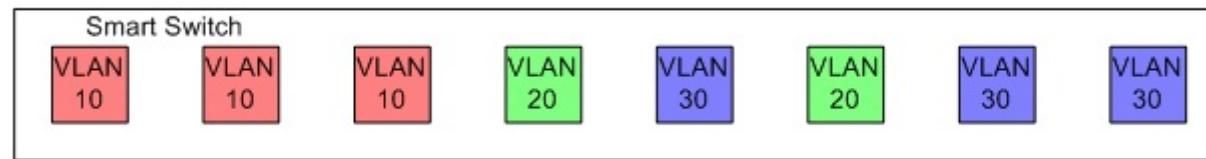
Критерии классификации виланов:

1. Порт-, интерфейс- либо канал-ориентированность: port-based, interface-based, link-based.
2. Наличие тегировки пакетов: tagged, untagged.
3. Наличие протокол-ориентированности (адрес-ориентированности): protocol-based.
4. Уровень модели OSI: L2, L3 и другие.
5. Наличие аутентификации: authentication-based.
6. Постоянство членства: static, dynamic.

4.1.2.3а

Основные практические примеры виланов:

- Собственно Port-based -- членство в вилане определяется в соответствии с портами активного сетевого оборудования.



- 802.1Q -- в кадр Ethernet вставляется специальный тег.
- Cisco ISL (Inter-Switch Link) -- проприетарный протокол, аналогичный 802.1Q.
- 3Com VLT (Virtual LAN Trunk) -- еще один проприетарный протокол, аналогичный 802.1Q.
- Cisco VTP (VLAN Trunking Protocol) -- проприетарный протокол, позволяющий частично автоматизировать настройку виланов.

4.1.2.3b

Из исторически менее значимых и относительно новых реализаций можно упомянуть еще:

802.1v -> 802.1Q (protocol-based),
Cisco VQP (VLAN Query Protocol) (аналог 802.1X),
D-Link ISM (IGMP Snooping Multicast) VLAN,
GVRP (GARP VLAN Registration Protocol) (открытый аналог VTP),
MAC-based VLANs от различных производителей, auto voice VLAN (связь с QoS),
auto surveillance VLAN.

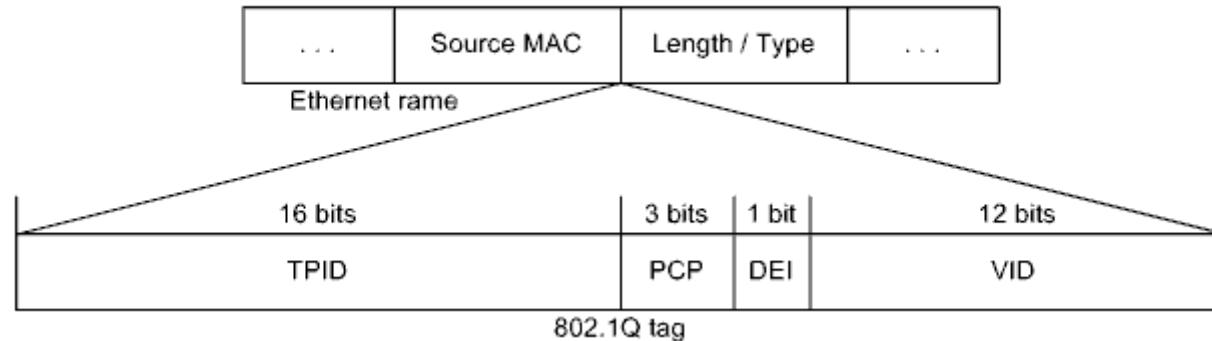
4.2

802.1Q

Версия 2.6

4.2.1.1

Рассмотрим более подробно реализации 802.1Q.



Поля:

1. TPID (Tag Protocol IDentifier) -- идентификатор протокола тегировки (является и признаком наличия тега, для 802.1Q равно 8100h).
2. PCP (Priority Code Point) либо (до 802.1Q-2005) User_Priority -- код приоритета либо приоритет пользователя.
3. Drop Eligible Indicator (DEI) либо (до 802.1Q-2011) CFI (Canonical Format Indicator) -- индикатор разрешения отбрасывания кадра либо индикатор канонического формата MAC-адреса (в обычном кадре Ethernet равно нулю).
4. VID (VLAN IDentifier) -- идентификатор вилана (собственно значение тега).

Тег 802.1Q в кадре Ethernet

4.2.2.1a

Здесь уместна еще одна классификация виланов на основе тегов:

1. Data VLAN -- «рабочий» вилан -- предназначен для передачи пользовательского трафика (может быть назначен любой незарезервированный VID).
2. Default VLAN -- вилан по умолчанию -- в данный вилан включаются все порты коммутатора по умолчанию (не может быть ни изменен, ни удален; зарезервирован VID = 1).
3. Management VLAN -- административный вилан -- предназначен для администрирования (выделяют исходя из соображений безопасности; от пользовательских виланов отличается только назначением).
4. Native VLAN -- вилан для оригинального трафика -- предназначен для передачи нетегированного трафика (по умолчанию это вилан с VID = 1; может быть назначен любой незарезервированный VID).
5. Private VLAN -- приватный вилан -- предназначен для частичного запрета трафика в рамках вилана (позволяет масштабировать виланы).
6. Reserved VLAN -- зарезервированный вилан -- предназначен для передачи специфического трафика (например, голосового; VID может быть как из зарезервированного, так и с незарезервированного диапазона; в Cisco IOS зарезервированы VIDs: 0, 1, 1002 – 1005, 1006 – 1024, 4095).

4.2.2.1b

Кадры с VID = 0 приравниваются к нетегированным, что позволяет подвергать нетегированный трафик приоритизации (QoS).

Кадры с VID = 4095 безусловно отбрасываются (в некоторых системах виртуализации, передаются во все определенные виланы).

4.2.2.2

Какие устройства администрируют с помощью административного видана?

4.2.3.1

Возникает несколько основных вопросов, связанных с внесением и удалением тегов:

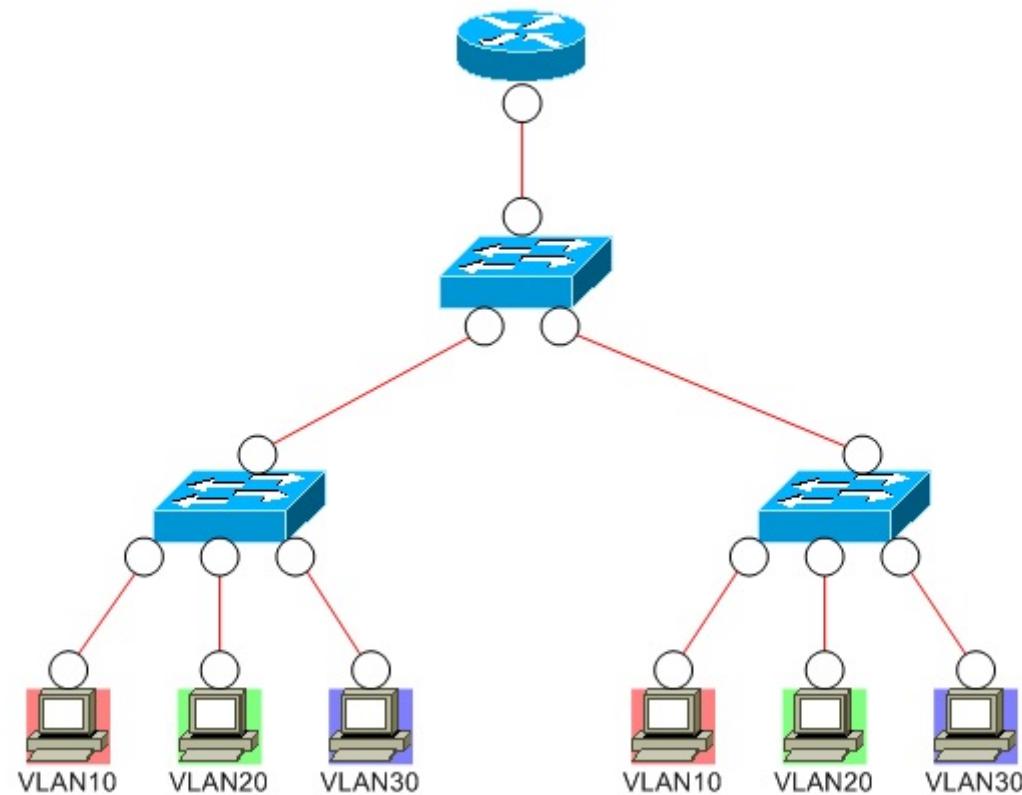
1. Где вносятся и удаляются теги?
2. Могут ли сосуществовать тегированный и нетегированный трафики?
3. Возможна ли многократная **тегировка**?

Эти вопросы «выливаются» во множество более мелких, что требует более подробного пояснения.

Отдельно взятый вилан представляет собой определенную независимую сущность на коммутаторе. Поэтому для использования вилан нужно привязать к портам.

Все виланы пронумерованы. Номера не только позволяют коммутаторам разграничивать трафик, а и позволяют связать воедино виланы на соседних коммутаторах.

4.2.3.2



Как вы думаете, где нужно вносить теги? А где удалять?

4.2.3.3

В рядовом случае, полученный от оконечной пользовательской станции кадр тегируется ближайшим коммутатором с поддержкой 802.1Q.

При этом физические порты, обращенные к оконечным пользовательским станциям (в общем случае, к домену, «не заботящемуся» о видах) принято называть *портами доступа* (access ports) (согласно терминологии некоторых компаний, в первую очередь Cisco) или, по-другому, *нетегирующими портами* (untagged ports).

Конечно, теги может вносить и сама станция, например, серверная, но для этого требуется поддержка 802.1Q со стороны сетевого адаптера. Возлагать задачу внесения тегов на рядовую клиентскую станцию некорректно.

4.2.3.4

Особенности порта доступа заключаются в следующем.

Порт доступа предназначен для внесения кадров в конкретный вилан и изъятия кадров оттуда. Именно поэтому порт доступа должен быть ассоциирован только с одним виланом (иначе в виланах нет смысла).

Для **привязки** порта к вилану (равно как и вилана к порту) используется параметр PVID (Port VID).

В нормальной ситуации коммутатор принимает через порт доступа только нетегированные кадры.

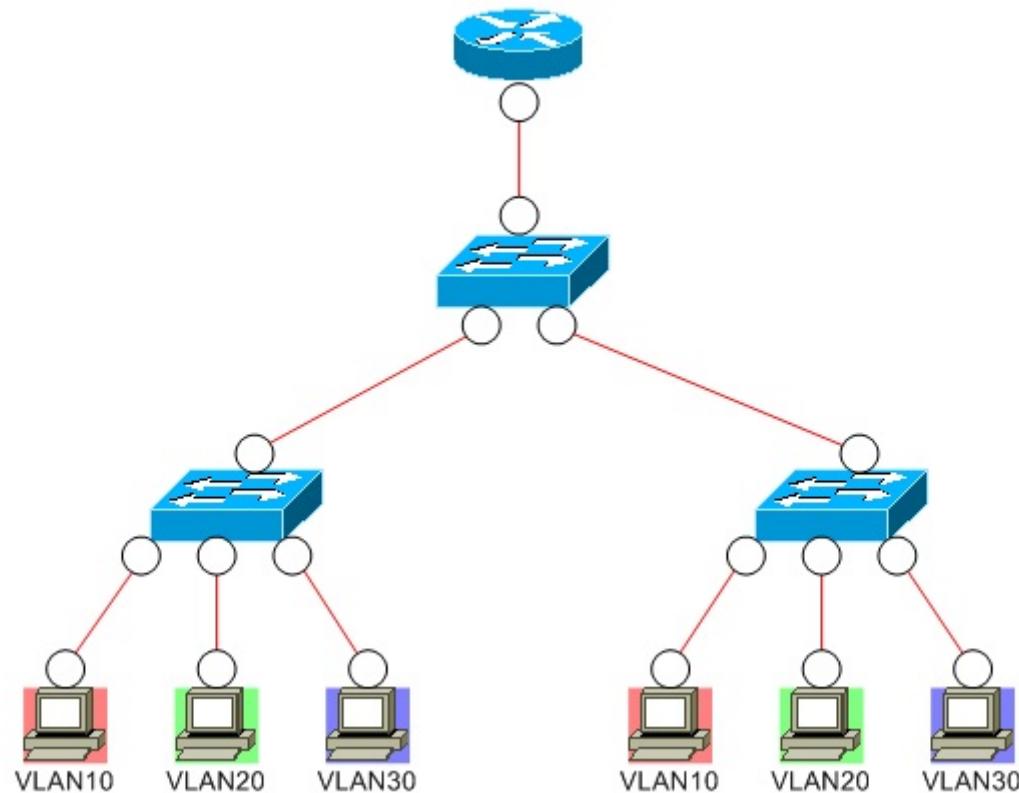
Реально же тег вносится в кадр при ретрансляции.

По умолчанию порт является портом доступа в вилан с VID = 1.

Если коммутатор все-таки принимает через порт доступа уже тегированный кадр, то просто «глотает» этот кадр (игнорируя тег), на чем основаны некоторые атаки (например, VLAN Hopping).

Благодаря описанному подходу, порт-ориентированные виланы на современных коммутаторах реализуют как подмножество 802.1Q.

4.2.3.5



Могут ли по одним и тем же каналам передаваться кадры с разными тегами? Если да, то по скольким?

4.2.3.6

Один и тот же физический канал может быть связан с передачей тегированных кадров, относящихся к различным виленам.

В рядовом случае, таковыми являются физические каналы между коммутаторами. Эти каналы называют *транками* (trunks) (согласно терминологии Cisco), а примыкающие к ним порты (в общем случае обращенные к домену, «заботящемуся» о виленах) называют *транковыми портами* (trunk ports) или, по-другому, *тегирующими портами* (tagged ports).

4.2.3.7

Транковый порт **привязан** ко всем имеющимся виленам либо к списку разрешенных.

PVIDs при этом не нужны и не используются.

4.2.3.8

Транковый порт по своей сути предназначен для работы с тегированными кадрами, но, с учетом широко распространенной практики использования, должен «понимать» и нетегированные.

Согласно общеиндустриальному представлению проблему сосуществования нетегированного и тегированного трафика решают просто -- один и тот же соответствующий порт рассматривают как тегирующий, так и нетегирующий одновременно (часто в реализациях каждый порт в отношении каждого вилана является тегирующим, либо нетегирующим, либо вообще не относящимся к данному вилану).

Cisco решает проблему с помощью **вилана для оригинального трафика**.

Таким образом, на коммутаторе с поддержкой 802.1Q отдельно взятый порт может быть либо портом доступа, либо транковым, либо, если предусмотрено, сочетать эти два режима (поддержка 802.1Q не отключается).

4.2.3.9

Замечание о Cisco native VLAN.

Понятие native VLAN применимо только к транковому порту.

Это вилан, в который коммутатор помещает все принимаемые через данный транковый порт нетегированные кадры, и, попутно, вилан, все кадры из которого передаются через данный транковый порт нетегированными.

По умолчанию native VLAN является вилан с VID = 1, в результате весь трафик по умолчанию передается нетегированным.

На разных концах одного физического канала могут быть разные native VLANs, но это противоречит правилам хорошего тона и порождает скрытые проблемы. Более того, на одном коммутаторе на разных транковых портах могут быть назначены разные native VLANs.

Старшие серии коммутаторов опционально поддерживают native VLAN tagging. После включения этой опции native VLAN становится неотличимым от «обычного» вилана (номер в кадре равен номеру native VLAN, может быть равен и единице), но коммутатор начинает отбрасывать все принимаемые через данный транковый порт нетегированные кадры.

4.2.3.10

Замечание о вилане по умолчанию.

Вилан по умолчанию отличается от других виланов лишь тем, что к нему привязываются все порты по умолчанию («**отвязывают**» -- по мере надобности) и он на коммутаторе существует всегда.

Виланом по умолчанию является вилан с VID = 1.

4.2.3.11

Концепция 802.1Q допускает многократную **тегировку** кадров (QinQ), но нужно помнить что каждый тег увеличивает кадр, а значит длина кадра может превысить значение MTU.

Сетевое оборудование обрабатывает теги, находящиеся «на вершине» (наиболее близкие к началу кадра).

4.2.3.12

Некоторые реализации поддерживают **множественные** (multi) или, по-другому, **ассиметричные** (asymmetric) виланы, что несколько отходит от «стержня» концепции 802.1Q.

Таковые механизмы позволяют «срастить» некоторые из виланов без задействования маршрутизаторов (на втором уровне), что обычно востребовано при предоставлении ресурсов в совместный доступ (например, два вилана должны быть, как и положено, изолированы друг от друга, но каждый из них должен иметь совместный трафик с третьим виланом).

Это достигают путем разрешения присваивать отдельно взятому **нетегирующему** порту более одного PVID либо путем дополнительного указания какие виланы с какими должны быть объединены (на каких портах «пересекаются»).

Аналогичное решение от Cisco -- **приватные виланы**.

4.2.3.13а

Замечание о Cisco private VLAN (RFC 5517).

Private VLAN -- это вилан, в границах которого можно выделить подвиланы. При этом сам вилан становится первичным (primary), а подвиланы -- вторичными (secondary). Бо'льшая степень вложенности не допускается.

Все вторичные виланы связаны с первичным, но изолированы друг от друга.

Вторичные виланы могут быть двух видов:

1. Community -- сообщества -- содержат устройства, трафик между которыми разрешен.

2. Isolated -- с изоляцией -- содержат устройства, трафик между которыми запрещен.

4.2.3.13b

При реализации private VLANs понятие порта доступа было расширено. Предусмотрено три вида таких портов:

1. Community -- подключают станции, которым разрешено взаимодействовать друг с другом (соответствуют вторичным виланам -- сообществам).
2. Isolated -- подключают станции, которым запрещено взаимодействовать друг с другом (соответствуют вторичным виланам с изоляцией).
3. Promiscuous -- подключают станции, которым разрешено взаимодействовать с любыми другими станциями (соответствуют первичному вилану).

4.2.3.14

Если коммутатор не поддерживает 802.1Q и принимает тегированный кадр, то он «не видит» тег.

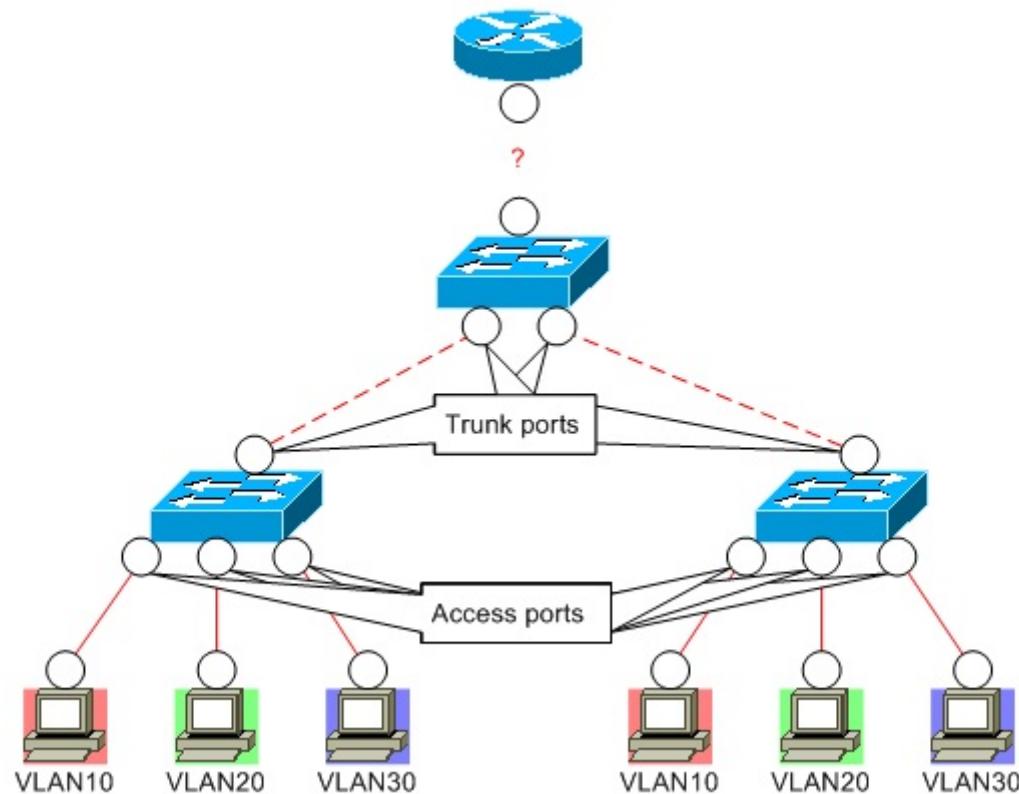
Трафик циркулирует, но теги теряются.

4.2.3.15

Новое условное графическое обозначение (в нотации Cisco).

----- -- LAN-транк

4.2.3.16



Access & trunk ports

4.2.4.1

С точки зрения IP-адресации каждый вилан 802.1Q является виртуальным аналогом физического сегмента (в большинстве случаев оконечного) и соответствует IP-подсети -- со всеми вытекающими последствиями.

Для обеспечения возможности передачи пакетов из одного вилана в другие необходима маршрутизация между виланами (inter-VLAN routing).

4.2.4.2

Маршрутизация между виленами может выполняться:

1. L3-коммутатором с виртуальными сетевыми интерфейсами в разных IP-подсетях.
2. Маршрутизатором с относящимися к разным IP-подсетям виртуальными подинтерфейсами одного реального сетевого интерфейса (иногда называют *router-on-stick*).
3. Маршрутизатором с относящимися к разным IP-подсетям сетевыми интерфейсами (иногда называют классической маршрутизацией между виленами).

4.2.4.3

Новое условное графическое обозначение.



-- L3-коммутатор

Разработчики Cisco долгое время предпочитали название многоуровневый коммутатор (multilayer switch).

4.2.4.4

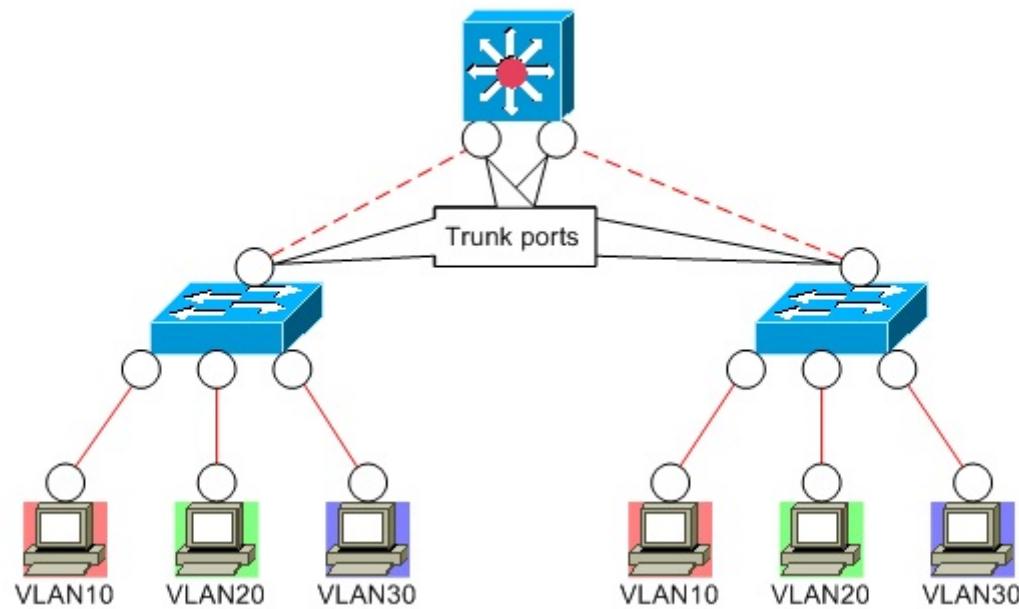
Типичный L3-коммутатор отличается от маршрутизатора большим числом физических портов и отсутствием «физически выраженных» сетевых интерфейсов (можно сказать, что L3-коммутатор -- это один «большой» сетевой интерфейс с большим числом точек подключения).

4.2.4.5



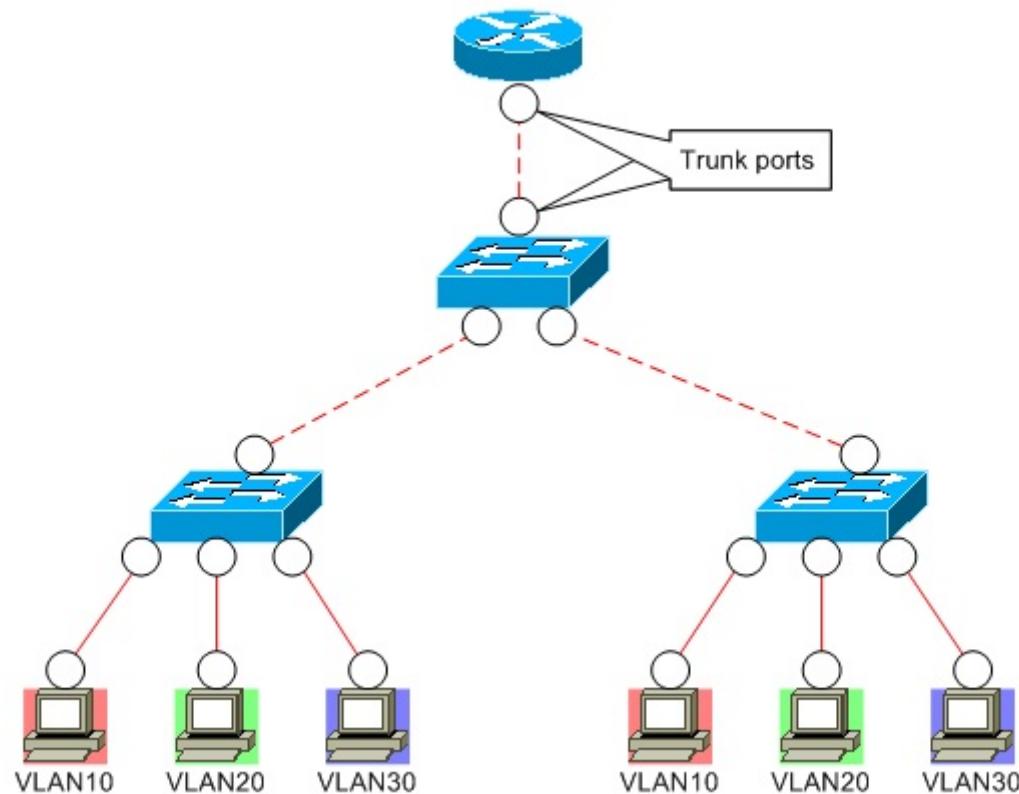
D-Link DGS-3627G [D-Link]

4.2.4.6



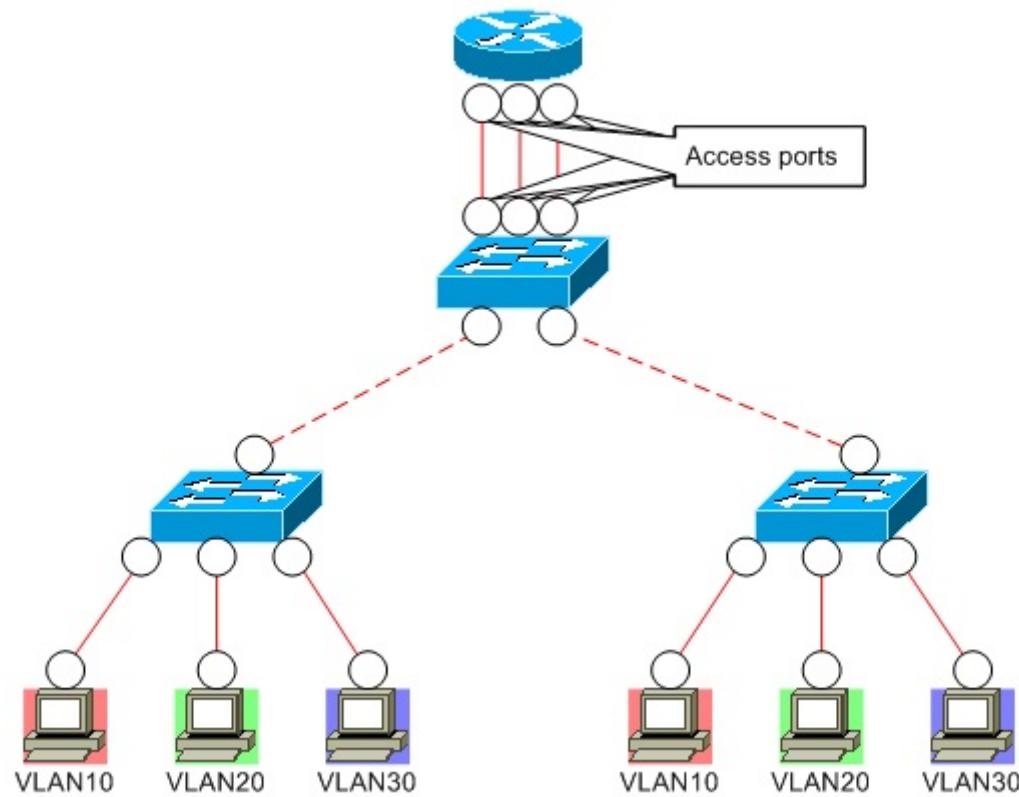
IVR via L3 Switch

4.2.4.7



IVR via Router-on-stick

4.2.4.8



Classic IVR

4.2.4.9

При IVR, как изолировать административный вилан?

4.2.5.1

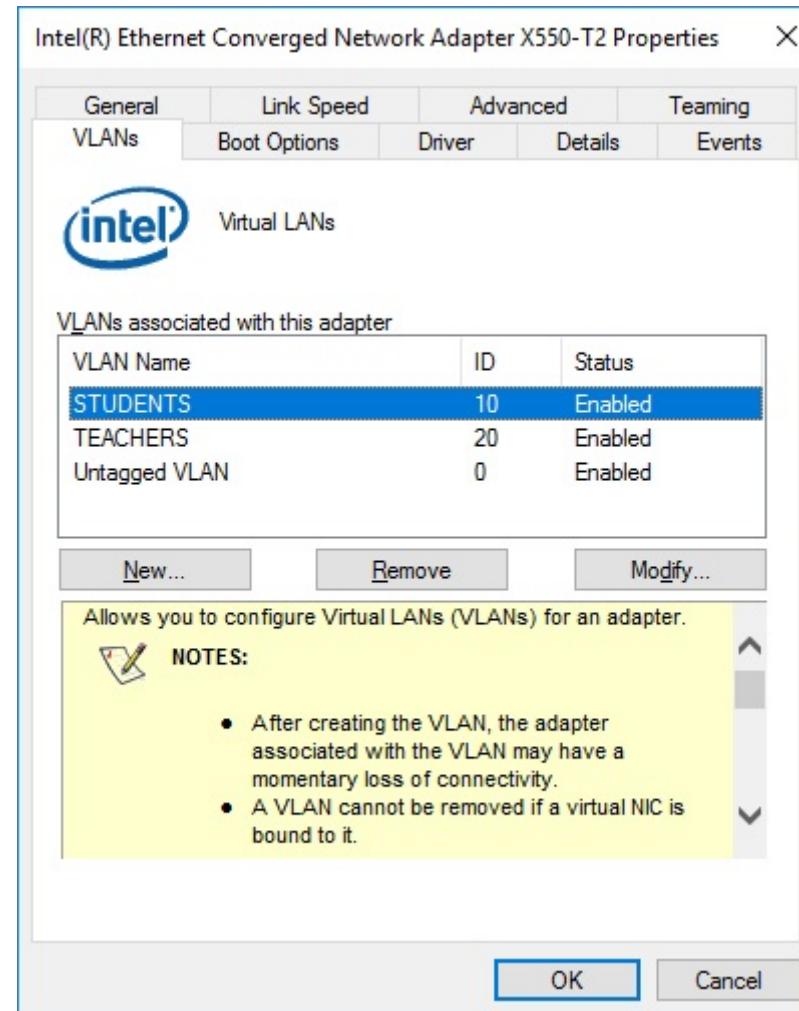
В Windows, исключая Server 2012 – Server 2019, виланы поддерживаются только на уровне драйверов сетевых адаптеров (например, Intel).

При этом необходимо конфигурационное ПО (например, утилиты) от производителей.

Подинтерфейсы как таковые не поддерживаются.

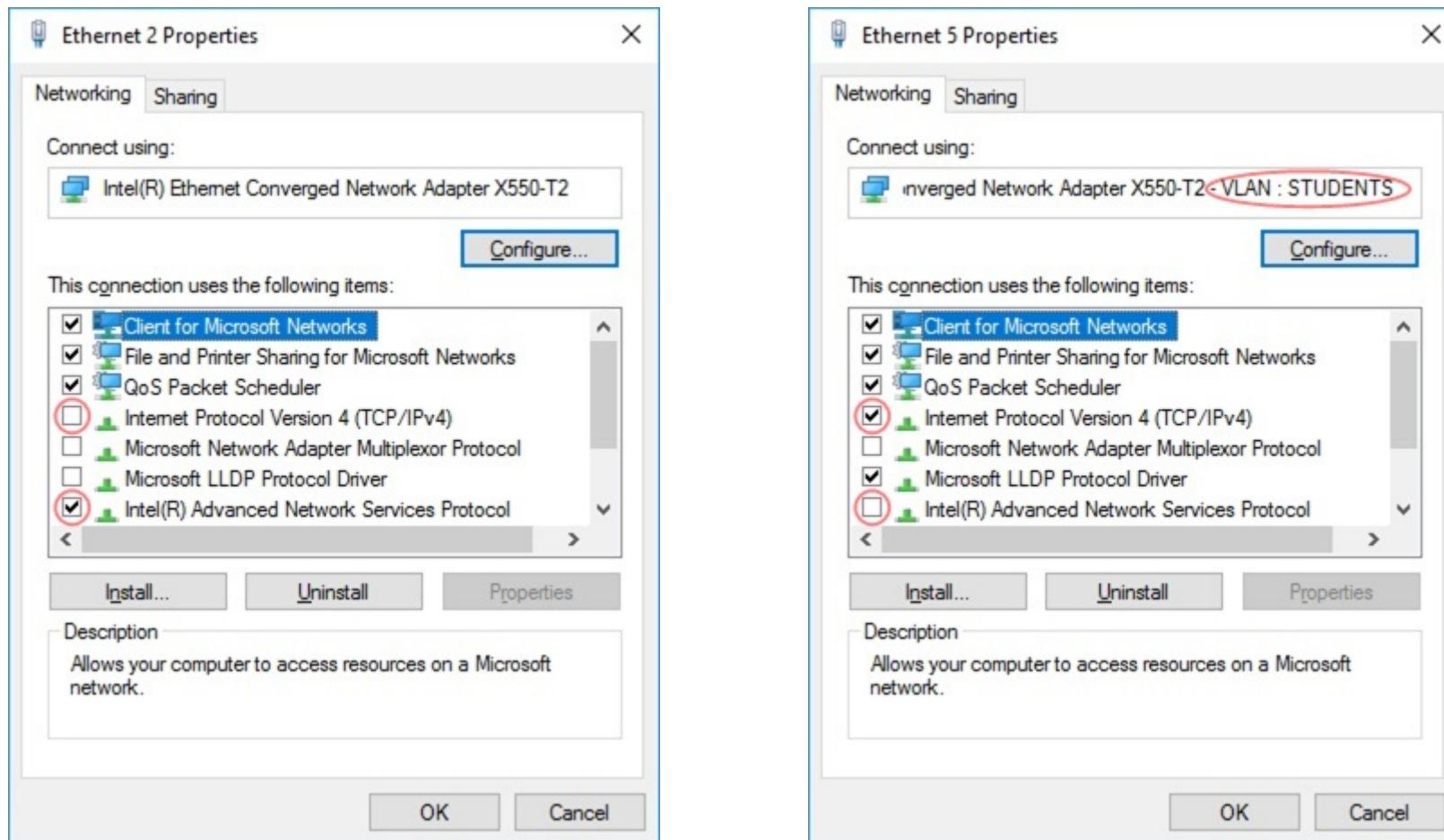
Виланы представлены виртуальными мультиплексируемыми сетевыми интерфейсами (тегированный и нетегированный трафик).

4.2.5.2a



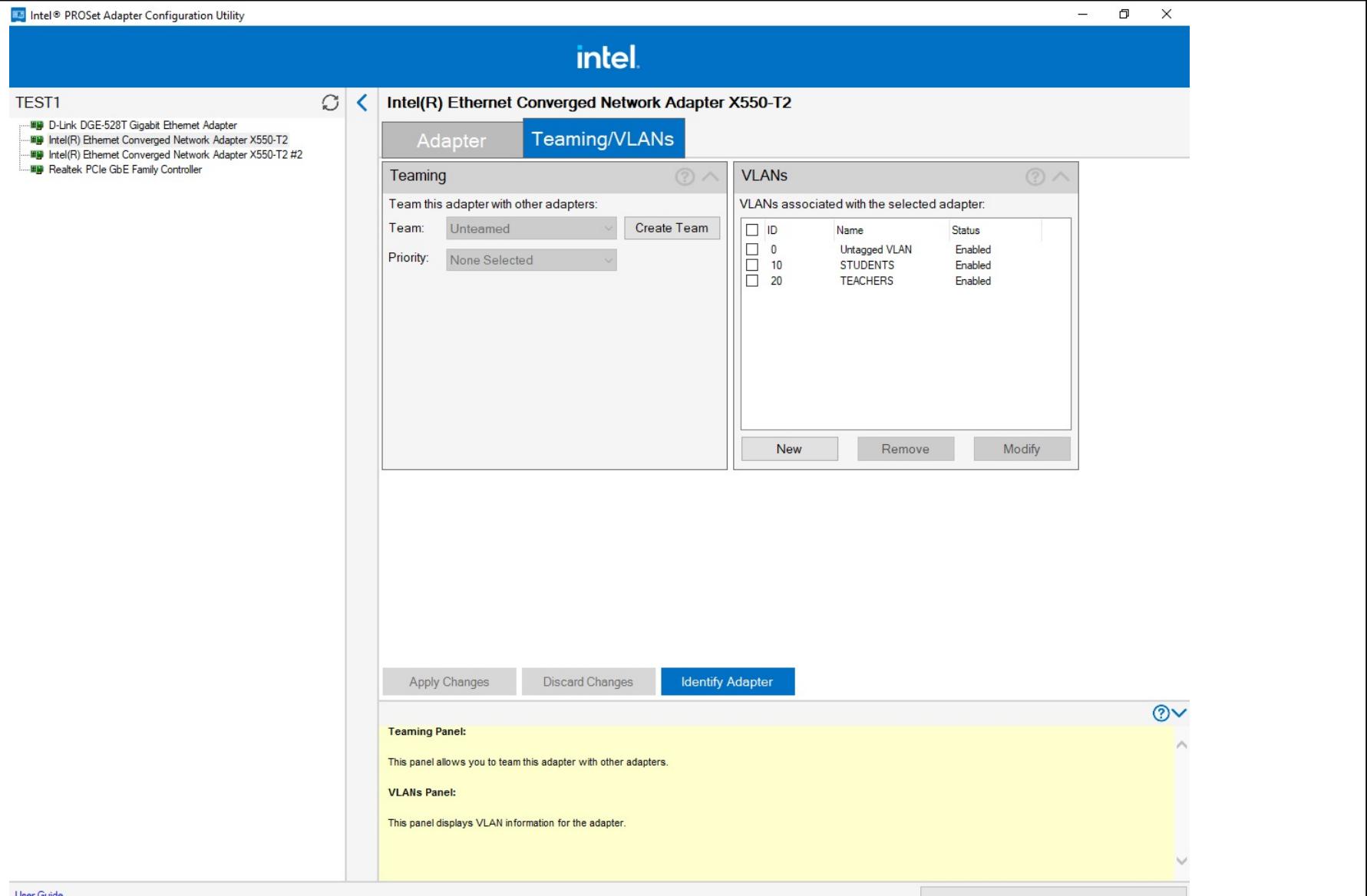
Пример виленов в Windows 10 1607 (Intel Advanced Network Services)

4.2.5.2b



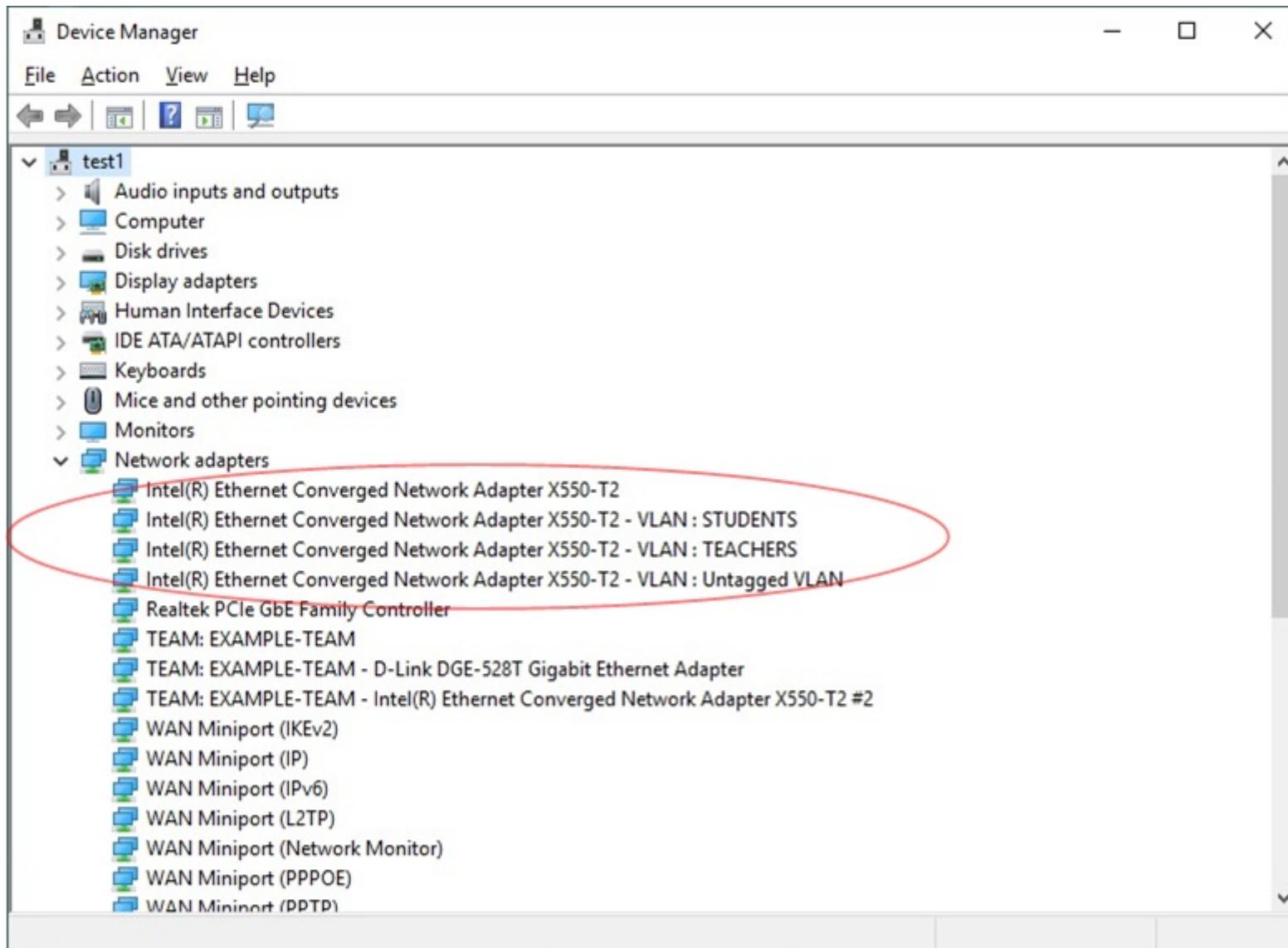
Пример вилянов в Windows 10 1607 (Intel Advanced Network Services)

4.2.5.2c



Пример виланов в Windows 10 1809 (Intel Advanced Network Services)

4.2.5.2d



Пример виланов в Windows 10 1809 (Intel Advanced Network Services)

4.2.5.2e

The screenshot shows the NIC Teaming configuration interface in Windows Server 2019. It includes three main sections:

- SERVERS:** Displays one server named TEST1, which is in a Fault status. The table columns are Name, Status, Server Type, Operating System Version, and Teams.
- TEAMS:** Displays two teams: EXAMPLE-MULTIPLE-VLANS and EXAMPLE-TEAM. The table columns are Team, Status, Teaming Mode, Load Balancing, and Adapters.
- ADAPTERS AND INTERFACES:** Displays network adapters and team interfaces. The table columns are Network Adapters, Team Interfaces, Primary, VLAN, State, and Team. It lists three team interfaces under EXAMPLE-MULTIPLE-VLANS and one under EXAMPLE-TEAM.

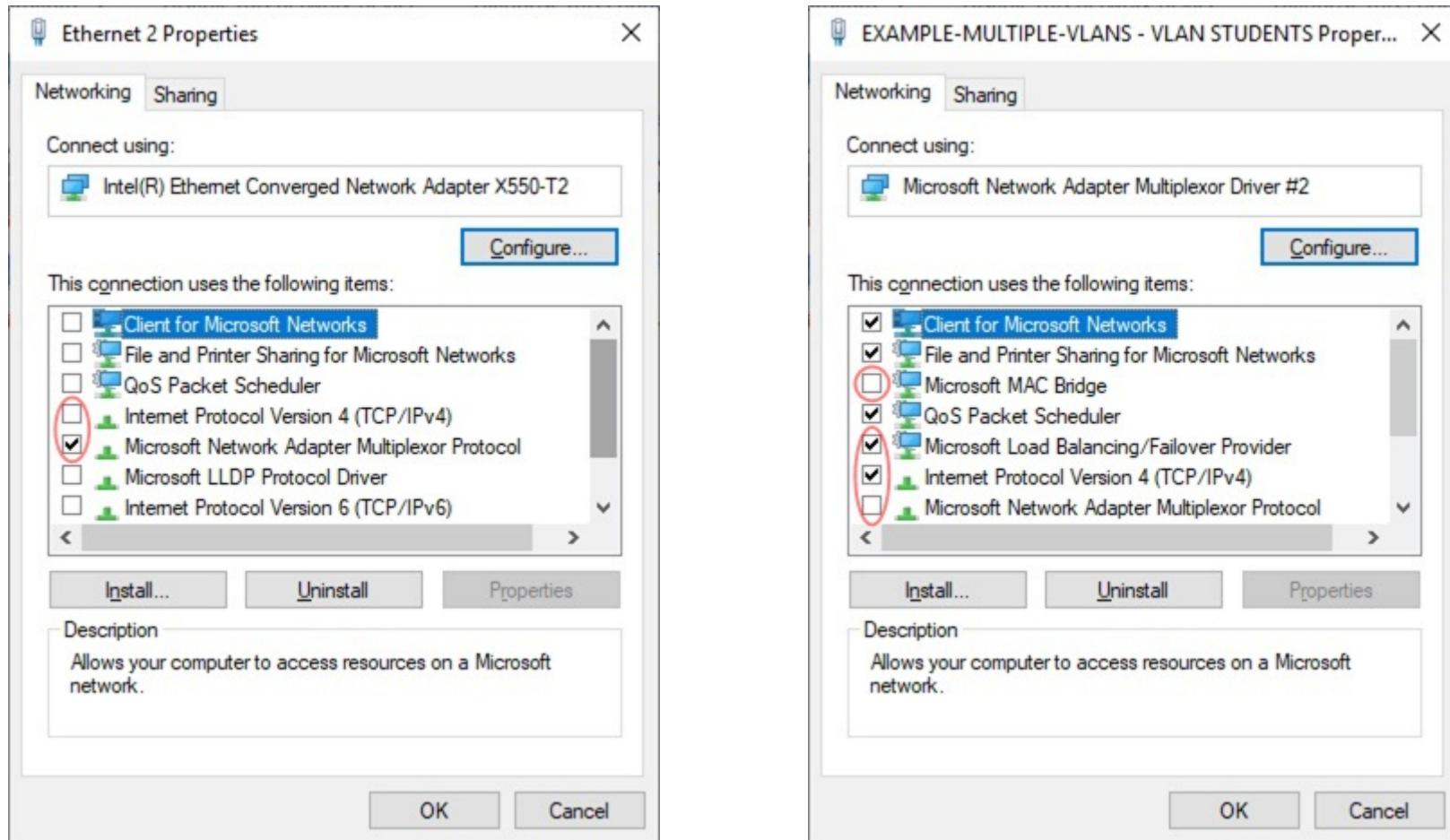
Name	Status	Server Type	Operating System Version	Teams
TEST1	Fault	Physical	Microsoft Windows Server 2019 Standard	2

Team	Status	Teaming Mode	Load Balancing	Adapters
EXAMPLE-MULTIPLE-VLANS	Fault	Switch Independent	Dynamic	1
EXAMPLE-TEAM	Warning	Static Teaming	Dynamic	2

Name	Primary	VLAN	State	Team
EXAMPLE-MULTIPLE-VLANS	Yes	Default	Disconnected	EXAMPLE-MULTIPLE-VLANS (3)
EXAMPLE-MULTIPLE-VLANS - VLAN STUDENTS	No	10	Disconnected	EXAMPLE-MULTIPLE-VLANS (3)
EXAMPLE-MULTIPLE-VLANS - VLAN TEACHERS	No	20	Disconnected	EXAMPLE-MULTIPLE-VLANS (3)
EXAMPLE-TEAM	Yes	Default	Connected	EXAMPLE-TEAM (1)

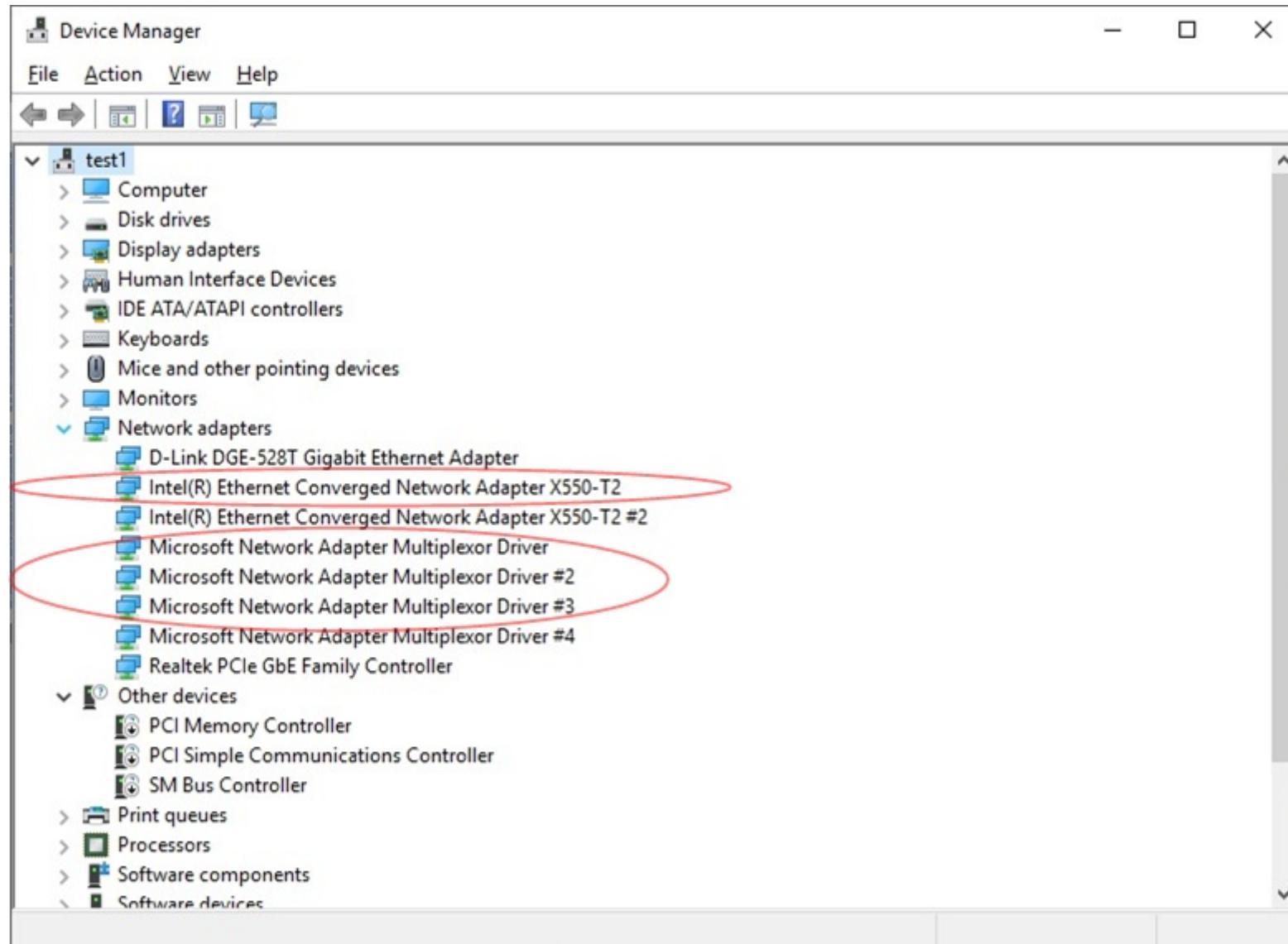
Пример виленов в Windows Server 2019 (в рамках NIC Teaming)

4.2.5.2f



Пример виленов в Windows Server 2019 (в рамках NIC Teaming)

4.2.5.2g



Пример виланов в Windows Server 2019 (в рамках NIC Teaming)

4.2.6.1

В Linux поддержка виленов выражена в подинтерфейсах.

На примере eth0 -- это eth0.1, eth0.2, eth0.3 и так далее.

Номер подинтерфейса соответствует VID в кадре (тегированный трафик),
eth0 соответствует native VLAN (нетегированный трафик).

Подинтерфейсы eth0 могут сосуществовать с eth0.

4.2.6.2

/etc/sysconfig/network-scripts/ifcfg-eth1.10 (ветви Red Hat и SUSE):

```
DEVICE=eth1.10
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.10.1
NETMASK=255.255.255.0
```

/etc/network/interfaces (ветвь Debian):

```
auto eth1.10
iface eth1.10 inet static
    address 192.168.10.1
    netmask 255.255.255.0
    vlan_raw_device eth1
```

4.2.7.1a

Типичные последовательности команд при настройке коммутатора Cisco с целью поддержки виланов.

Пример создания пользовательского вилана.

4.2.7.1b

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name STUDENTS
Switch(config-vlan)#end
Switch#
```

4.2.7.2a

Раньше то же самое можно было сделать по-другому -- создать вилан в специальном режиме конфигурирования базы данных виланов (VLAN database configuration mode).

4.2.7.2b

```
Switch#vlan database
Switch(vlan)#vlan 10 name STUDENTS
Switch(vlan)#exit
Switch#
```

4.2.7.3

Для сохранения информации о видах создается специальная база данных `vlan.dat` -- традиционный файл в корневом каталоге подсистемы памяти Flash.

4.2.7.4a

Пример назначения порта доступа.

4.2.7.4b

```
Switch(config)#interface fa0/11
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
```

4.2.7.5a

Пример назначения транкового порта.

Если кроме 802.1Q поддерживается ISL (как на 3560), то по умолчанию происходит автосогласование типа инкапсуляции. Рекомендуется использовать команду `switchport trunk encapsulation dot1q --` для явного указания.

4.2.7.5b

```
Switch(config)#interface fa0/12
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40
Switch(config-if)#switchport trunk native vlan 40
Switch(config-if)#exit
```

4.2.7.6

Кроме статического задания транка, существует возможность его динамического формирования с помощью сообщений протокола DTP (Dynamic Trunking Protocol).

В результате, порт может находиться в одном из следующих транковых режимов:

1. dynamic auto (по умолчанию).
2. dynamic desirable.
3. trunk.

Для задания транкового режима указанные названия вводят как аргументы команды `switchport mode`.

Формирование транка зависит от режима каждого из портов, образующих соответствующую пару, следующим образом.

	Access	Trunk	Dynamic auto	Dynamic desirable
Access	Access	Not Recommended	Access	Access
Trunk	Not Recommended	Trunk	Trunk	Trunk
Dynamic auto	Access	Trunk	Access	Trunk
Dynamic desirable	Access	Trunk	Trunk	Trunk

4.2.7.7a

Пример создания и конфигурирования SVI (Switch Virtual Interface) -- ассоциированного с виланом виртуального сетевого интерфейса (L3-интерфейса).

SVIs для администрирования доступны на всех управляемых коммутаторах Cisco, в том числе **на** 2960. «Рабочие» SVIs доступны на **L3-**коммутаторах, таких как 3560. Правда, начиная с IOS версии 12.2(55) даже на 2960 доступен специальный маршрутизирующий шаблон (один из SDM templates), но, в сравнении с 3560, с **сильными количественными ограничениями** (например, максимум 16 статических маршрутов).

Начиная с IOS версии 12.2, SVI необходимо административно включать (после создания, по аналогии с другими L3-интерфейсами).

4.2.7.7b

```
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.11.11 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

4.2.7.8a

Если IP-адрес нужен только в рамках административного видана, то для указания шлюза по умолчанию предназначена команда `ip default-gateway`.

Поскольку коммутатор Cisco по умолчанию является устройством второго уровня, IP-маршрутизация на нем по умолчанию выключена (в отличии от маршрутизатора -- устройства третьего уровня).

4.2.7.8b

```
Switch(config)#ip default-gateway 192.168.11.1
```

```
Switch(config)#ip routing
```

```
...
```

```
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.11.1
```

4.2.7.9

Зачем на коммутаторе нужно назначать шлюз по умолчанию?

4.2.7.10а

Пример создания и конфигурирования подинтерфейсов на маршрутизаторе (нумерацию можно начинать с нуля). При этом IP-адрес можно назначить только после включения инкапсуляции и IP-адрес подинтерфейса совместим с IP-адресом интерфейса (с проверкой уникальности подсетей).

4.2.7.10b

```
Router(config)#interface gi0/0.1
Router(config-subif)#encapsulation dot1q 40 native
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface gi0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
...
...
```

4.2.7.11

Для просмотра информации о видах в основном используют команду `show vlan` с опциональным указанием VID либо названия интересующего вида. Можно использовать и команду `show interfaces`.

Особенности вывода на экран команды `show vlan`:

- в столбце `Ports` перечисляются соответствующие порты доступа, причем вне зависимости от их состояния (`up` и `down`);
- транковые порты в состоянии `up` при выводе на экран выпадают;
- также выпадают SPAN-порты (будут рассмотрены позже);
- транковые порты в состоянии `down` показываются как порты доступа `default VLAN`, причем вне зависимости от VID native VLAN.

4.2.7.12

```
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2
2	ISP	active	Fa0/1
3	LAN	active	Fa0/3
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdmnet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
1002	fdmi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdmnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

```
Remote SPAN VLANs
```

Primary	Secondary	Type	Ports

4.2.7.13

Table Default Layer 2 Ethernet Interface VLAN Configuration

Feature	Default Setting
Interface mode	<code>switchport mode dynamic auto</code>
Trunk encapsulation	<code>switchport trunk encapsulation negotiate</code>
Allowed VLAN range	VLANs 1 to 4094
VLAN range eligible for pruning	VLANs 2 to 1001
Default VLAN (for access ports)	VLAN 1
Native VLAN (for IEEE 802.1Q trunks)	VLAN 1

Конфигурация порта коммутатора Cisco по умолчанию применительно к виланам [Cisco]