OTUS

Администратор Linux

Сетевые пакеты. VLAN’ы. LACP.

otus.ru

Проверить, идет ли запись

Меня хорошо видно && слышно?

Ставим “+”, если все хорошо
“-”, если есть проблемы

Тема вебинара

Сетевые пакеты. VLAN’ы. LACP.

Федоров Иван Романович

Технический директор ГК “Инотех”

Опыт:

Более 10 лет в IT-сфере

Аспирант университета ИТМО по направлению “Информационная безопасность”

Многократный победитель различных конкурсов и хакатонов (команда IBI Solutions)

Эл. почта: ifedorov.devops@gmail.com

Правила вебинара

Активно
участвуем

Off-topic обсуждаем
в группе Telegram
OTUS-Linux-2022-12

Задаем вопрос
в чат или голосом

Вопросы вижу в чате,
могу ответить не сразу

Маршрут вебинара

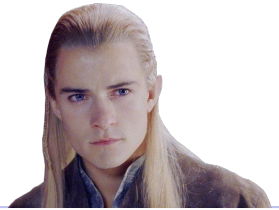
- Знакомство
- VLAN
- LACP
- Teaming/Bonding
- Практика
- Рефлексия

Цели вебинара

К концу занятия вы сможете

1. Понять как работает VLAN

2. Понять как работает агрегирование каналов



3. Настраивать teaming

Смысл

Зачем вам это уметь

1. Для более глубоких знаний сетевого стека
2. Чтобы эффективно строить сетевую инфраструктуру с максимальной стабильностью и безопасностью
3. Чтобы обеспечивать балансировку и отказоустойчивость трафика

Вспоминаем…

Коммутатор

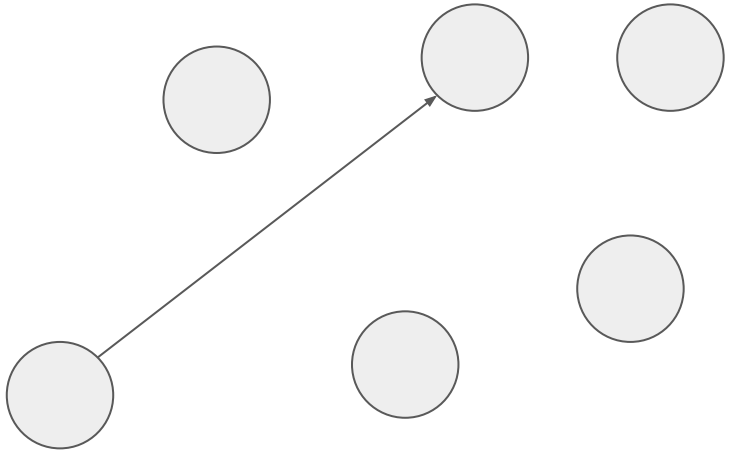
- Работает на втором уровне модели OSI
- При неизвестном адресе получателя начинается “flood” (broadcast во все порты)
- Не разграничивает широковещательные домены

Маршрутизатор

- Работает на третьем уровне модели OSI
- При неизвестном адресе получателя пакет отбрасывается
- Ограничивает широковещательные домены

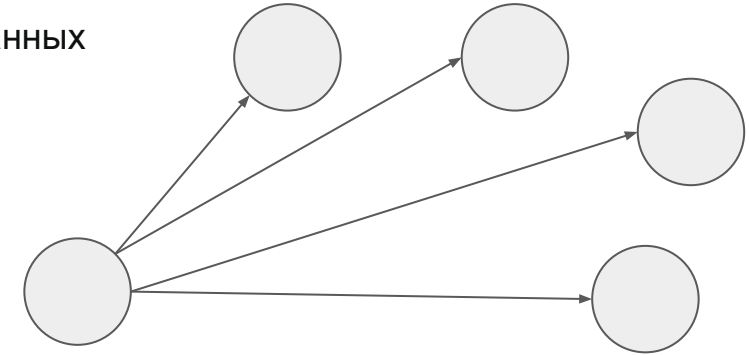
Unicast

- Один адресат данных



Broadcast

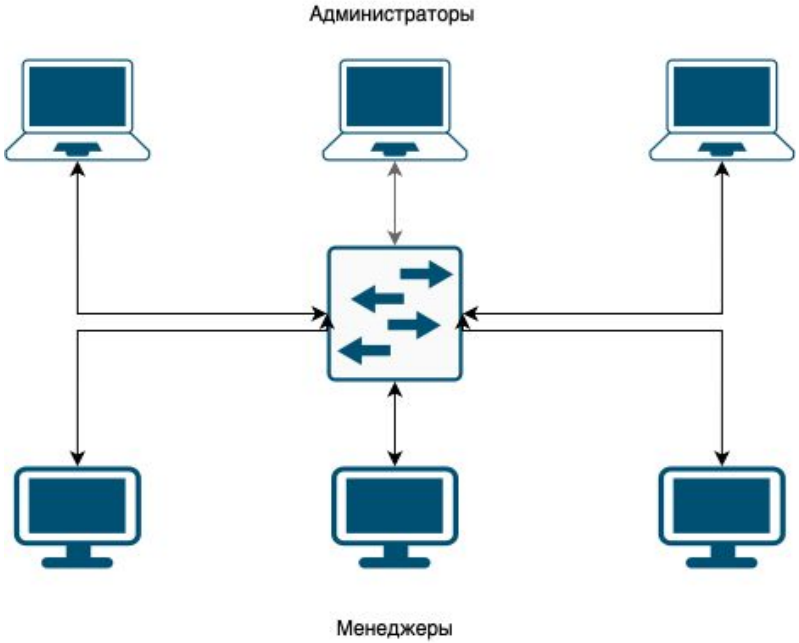
- Широковещательная адресация данных



VLAN

Проблема

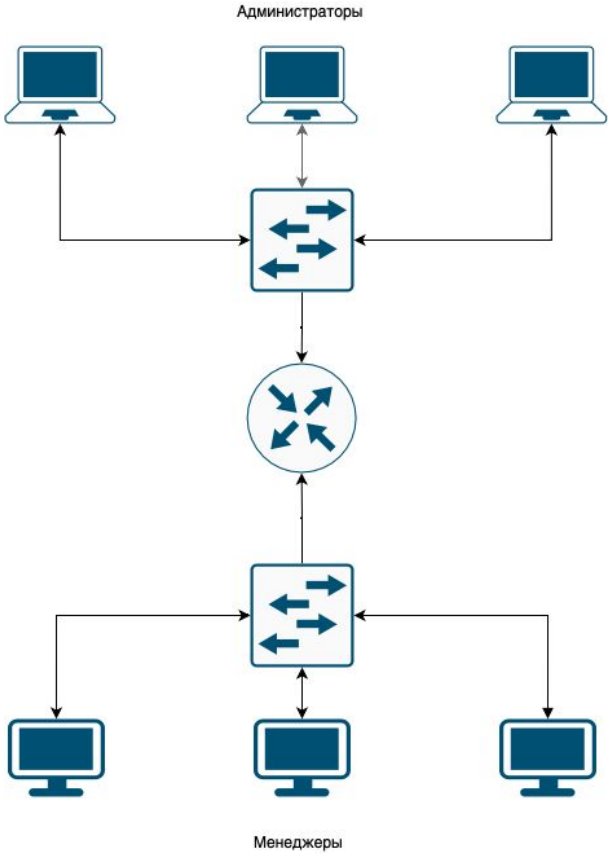
Один широковещательный домен



Вариант решения

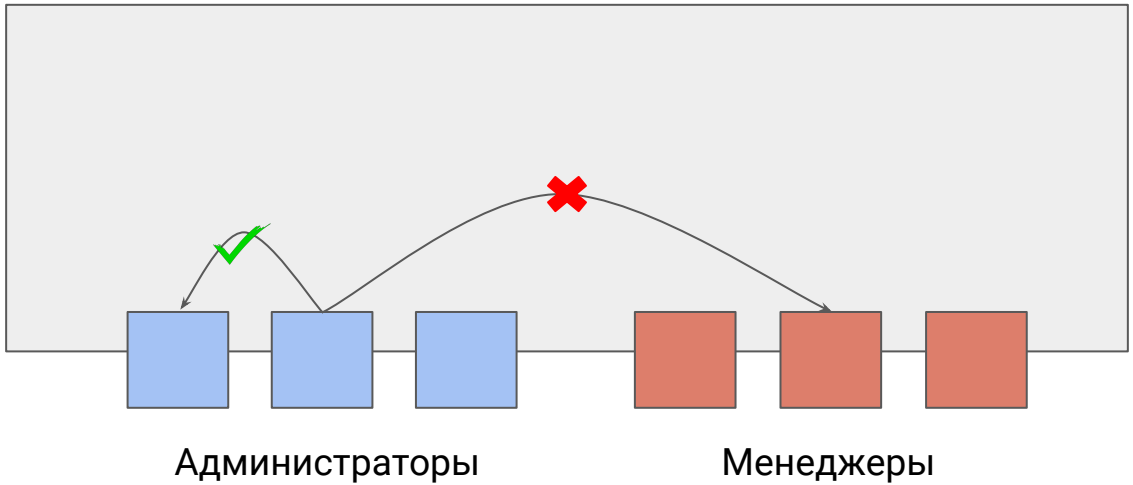
Добавить роутер ?

+ Сегментирование сети
- Финансовые издержки
- Возможно неэффективное использование оборудования



Как бы хотелось решить задачу

Отделить трафик в рамках коммутатора



VLAN (определение)

VLAN (аббр. от англ. Virtual Local Area Network) — топологическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения

Более простой вариант определения:

VLAN — механизм для создания логической топологии сети, не зависящей от ее физической топологии

VLAN (особенности)

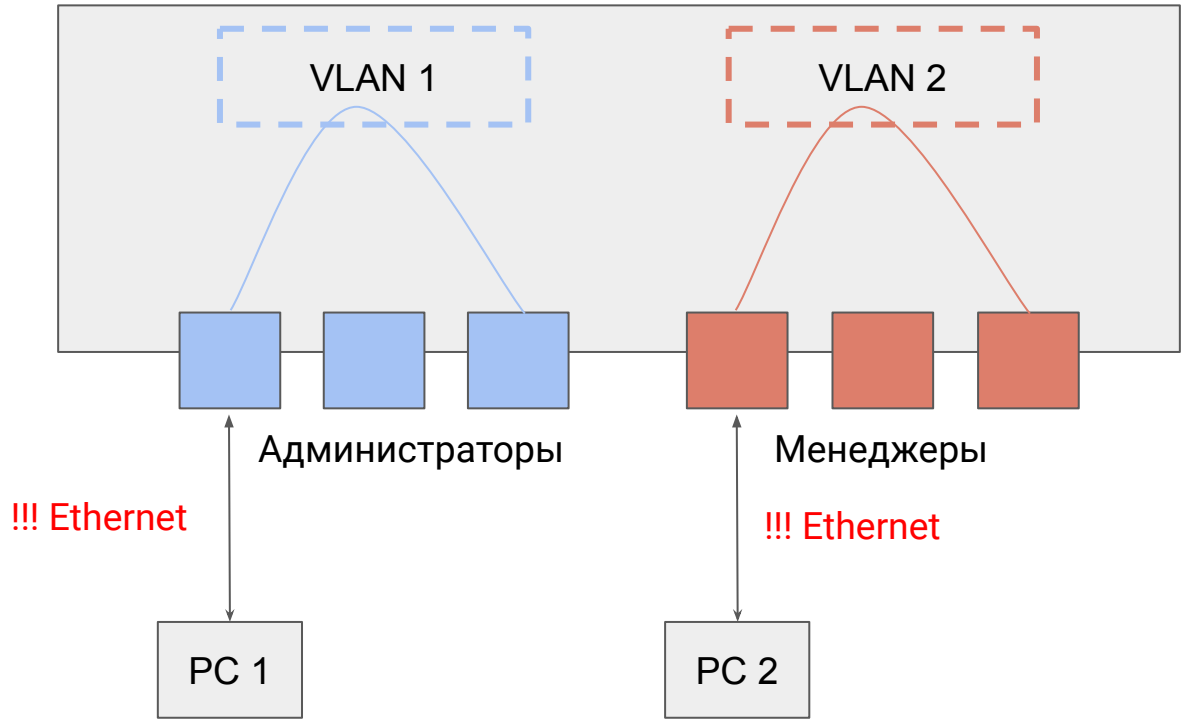
Необходимость применения VLAN:

- изоляция сегментов сети
- гибкое разделение хостов на группы
- сокращение широковещательного трафика
- увеличение безопасности и управляемости сети

Особенности:

- не требуется физическое перемещение устройств
- требуется использование коммутаторов с поддержкой VLAN

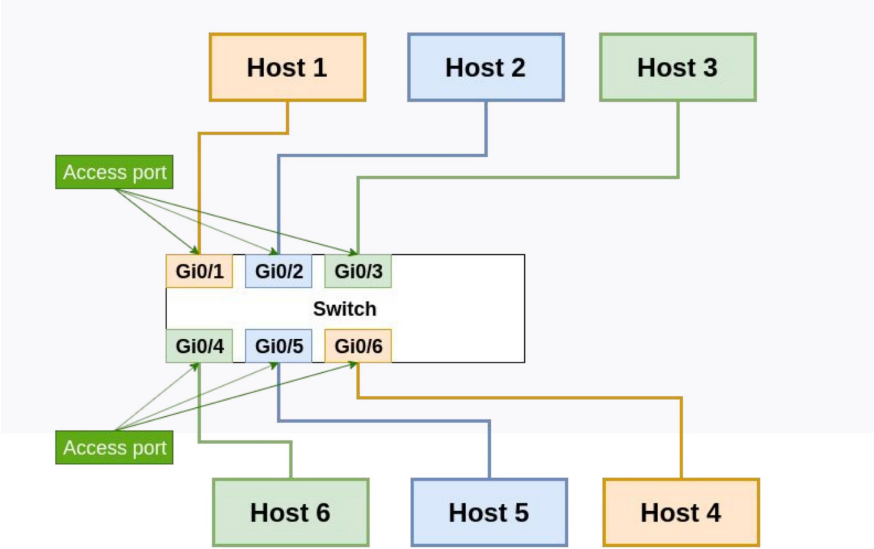
Пример работы



Access port

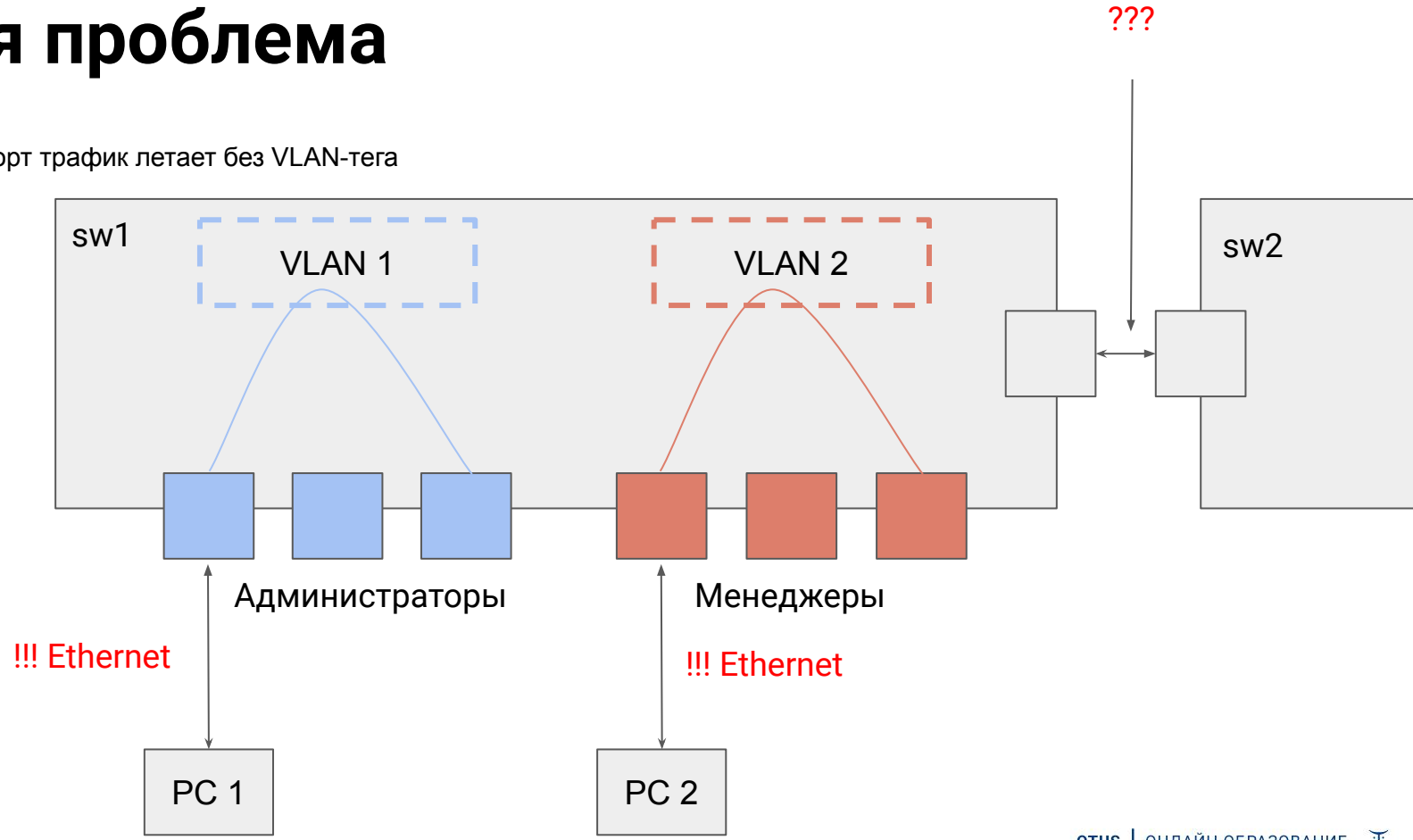
Access port (порт доступа) — порт, находящийся в определенном VLAN и передающий не тегированные кадры.

Как правило, это порт, смотрящий на пользовательское устройство.

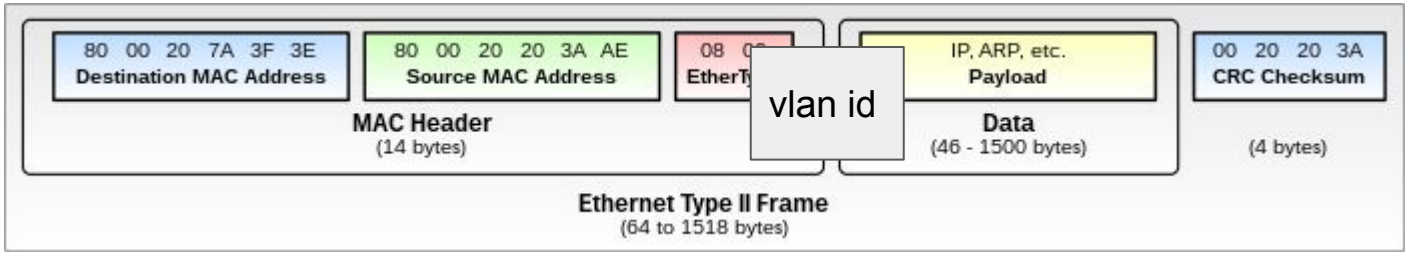


Новая проблема

Через access порт трафик летает без VLAN-тега



Ethernet


80 00 20 7A 3F 3E
Destination MAC Address
80 00 20 20 3A AE
Source MAC Address
08
EtherT
vlan id
IP, ARP, etc.
Payload
00 20 20 3A
CRC Checksum
MAC Header
(14 bytes)
Data
(46 - 1500 bytes)
(4 bytes)
Ethernet Type II Frame
(64 to 1518 bytes)

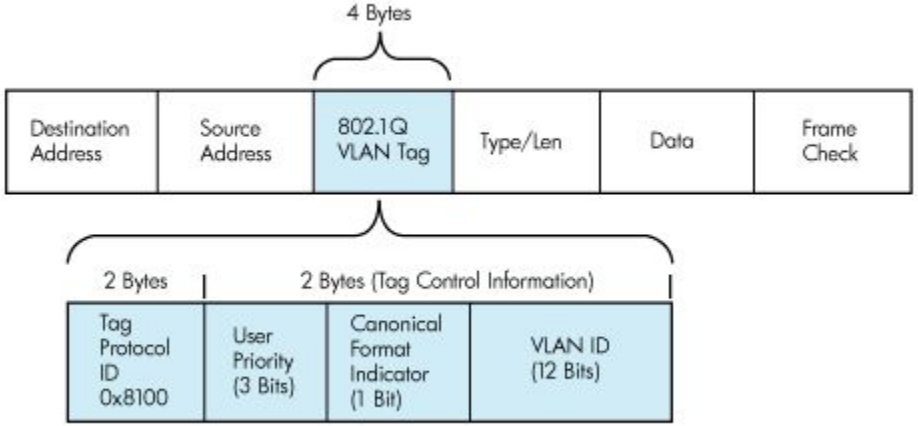
dot1q

IEEE 802.1Q — открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN по сетям стандарта IEEE 802.3 Ethernet

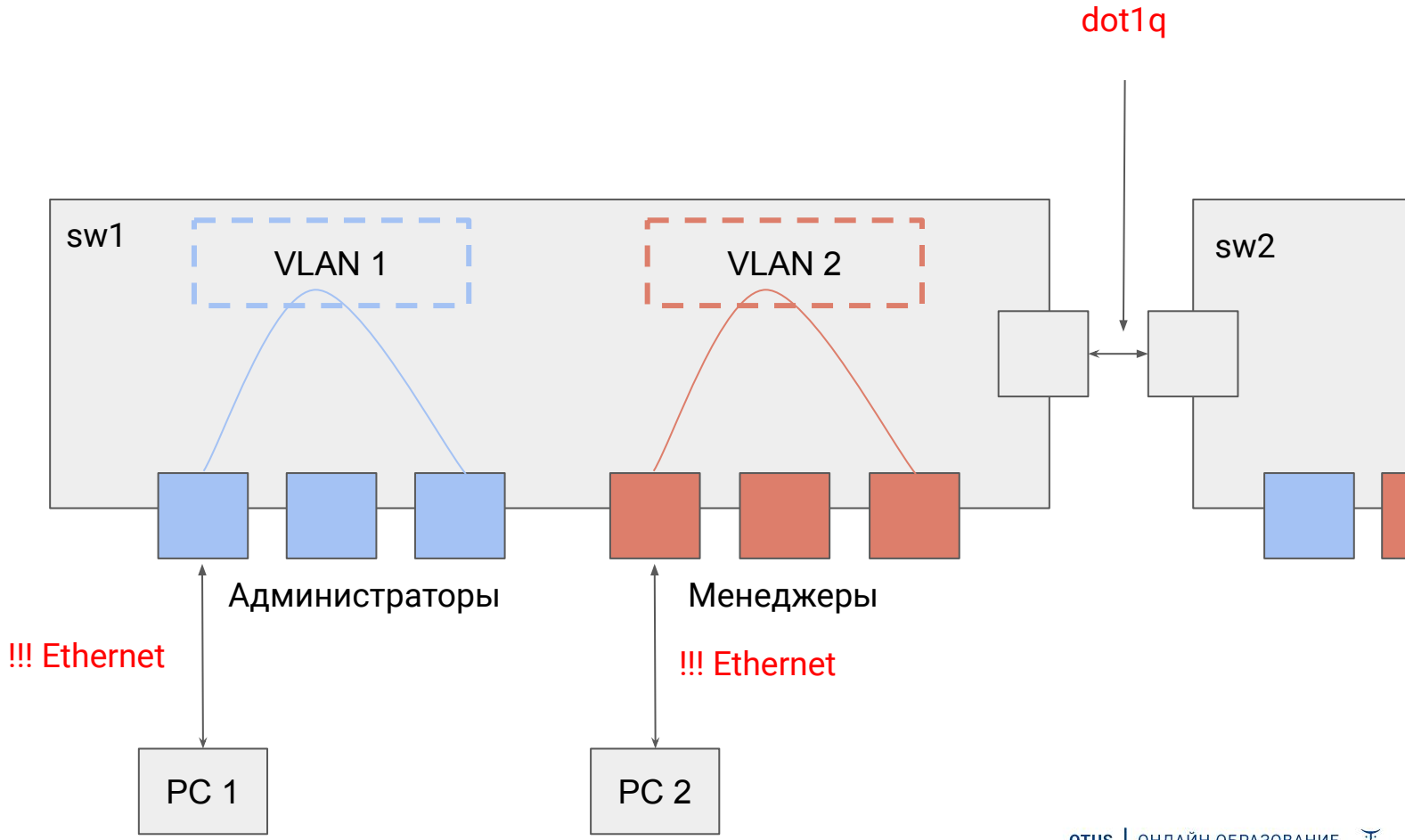
Особенности:

- используется процедура тегирования трафика
- теги инкапсулируются в Ethernet кадре
- поле для Vlan ID (VID) в теге - всего 12 бит
- после добавления тега пересчитывается контрольная сумма кадра
- максимальное количество VID - 4096, а точнее 4094, так как VID 0 и 4095 зарезервировано и не используется

dot1q


4 Bytes
Destination Address
Source Address
802.1Q VLAN Tag
Type/Len
Data
Frame Check
2 Bytes
2 Bytes (Tag Control Information)
Tag Protocol ID 0x8100
User Priority (3 Bits)
Canonical Format Indicator (1 Bit)
VLAN ID (12 Bits)

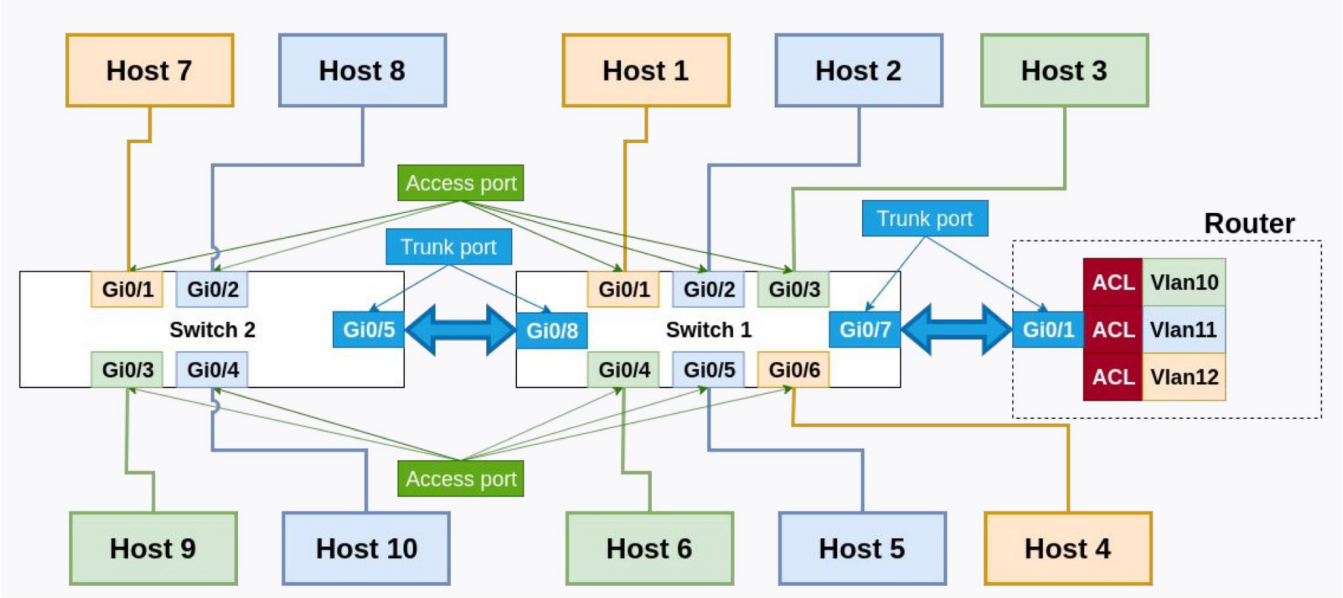
dot1q


dot1q
sw1
VLAN 1
VLAN 2
sw2
Администраторы
Менеджеры
!!! Ethernet
!!! Ethernet
PC 1
PC 2

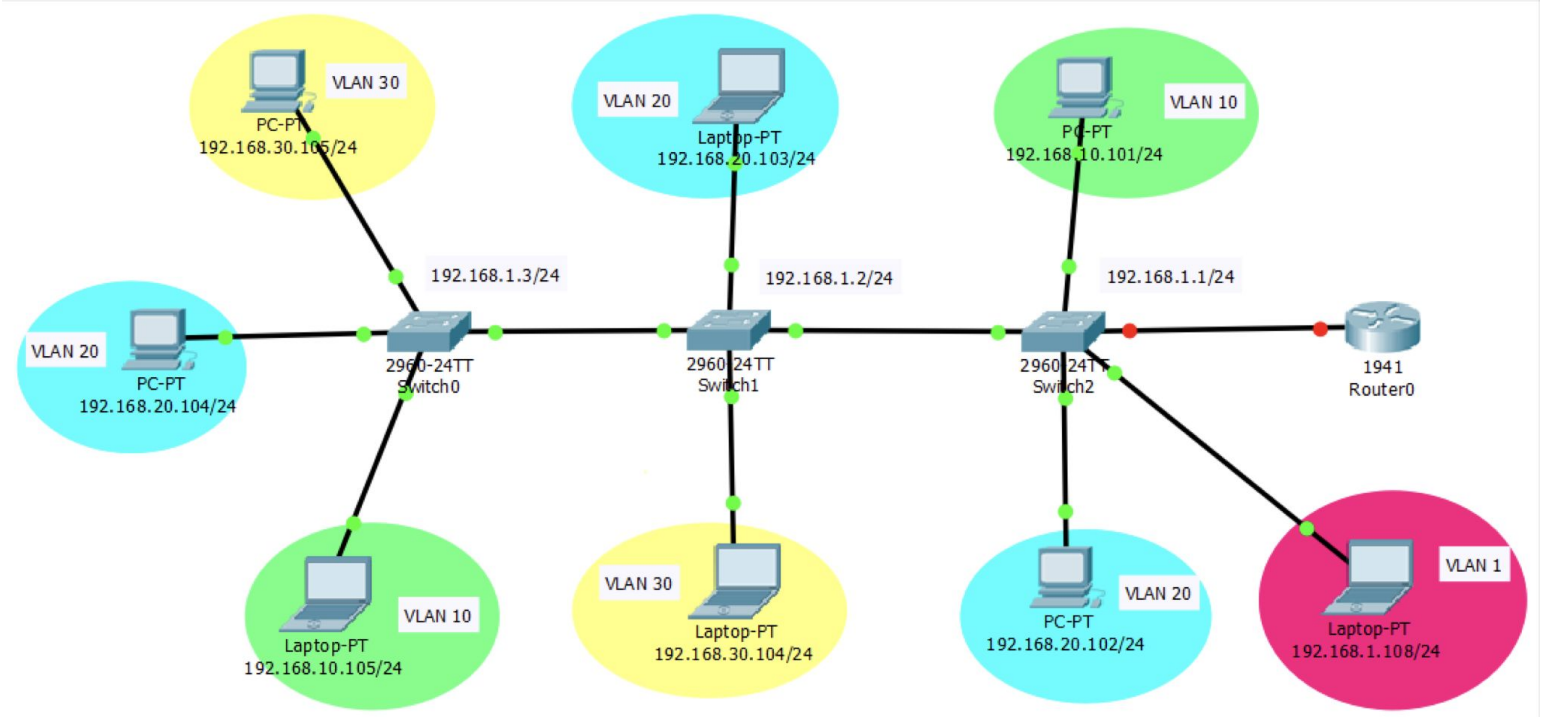
Trunk port

Trunk port (магистральный порт) — порт, передающий тегированный трафик.

Как правило, этот порт поднимается между сетевыми устройствами.



Пример сети


VLAN 30
PC-PT
192.168.30.105/24
VLAN 20
Laptop-PT
192.168.20.103/24
VLAN 10
PC-PT
192.168.10.101/24
192.168.1.3/24
192.168.1.2/24
192.168.1.1/24
VLAN 20
PC-PT
192.168.20.104/24
2960-24TT
Switch0
2960-24TT
Switch1
2960-24TT
Switch2
1941
Router0
VLAN 10
Laptop-PT
192.168.10.105/24
VLAN 30
Laptop-PT
192.168.30.104/24
VLAN 20
PC-PT
192.168.20.102/24
VLAN 1
Laptop-PT
192.168.1.108/24

Все хорошо?
Есть ли вопросы?

LACP

Агрегирование каналов

Агрегирование каналов (англ. link aggregation) — технологии объединения нескольких параллелыных каналов передачи данных в сетях Ethernet в один логический, позволяющие увеличить пропускную способность и повысить надёжность.

В различных конкретных реализациях агрегирования используются альтернативные наименования: транкинг портов (англ. port trunking), связывание каналов (link bundling), склейка адаптеров (NIC bonding), сопряжение адаптеров (NIC teaming)

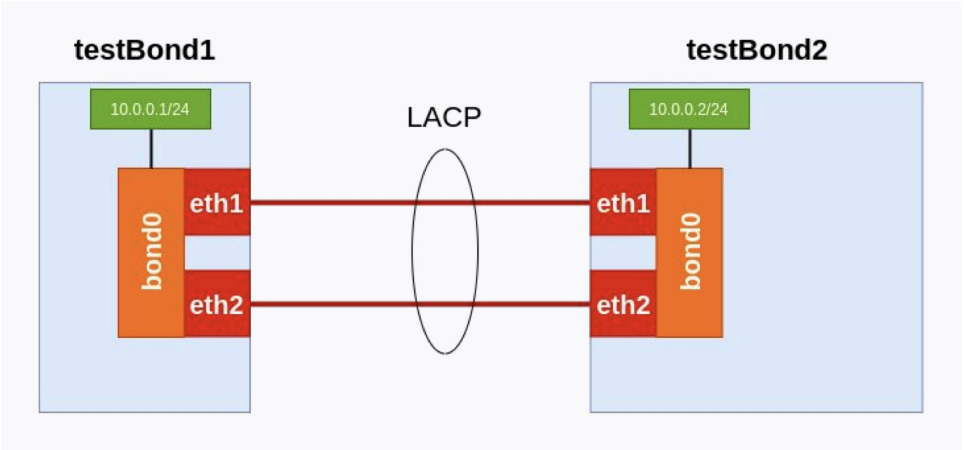
LACP

LACP (англ. link aggregation control protocol) — открытый стандартный протокол агрегирования каналов, описанный в документах IEEE 802.3ad и IEEE 802.1aq. Многие производители для своих продуктов используют не стандарт, а патентованные или закрытые технологии, например, Cisco применяет технологию EtherChannel (разработанную в начале 1990-х годов компанией Kalpana), а также нестандартный протокол PAgP

Bonding

Bonding — метод агрегации каналов в Linux

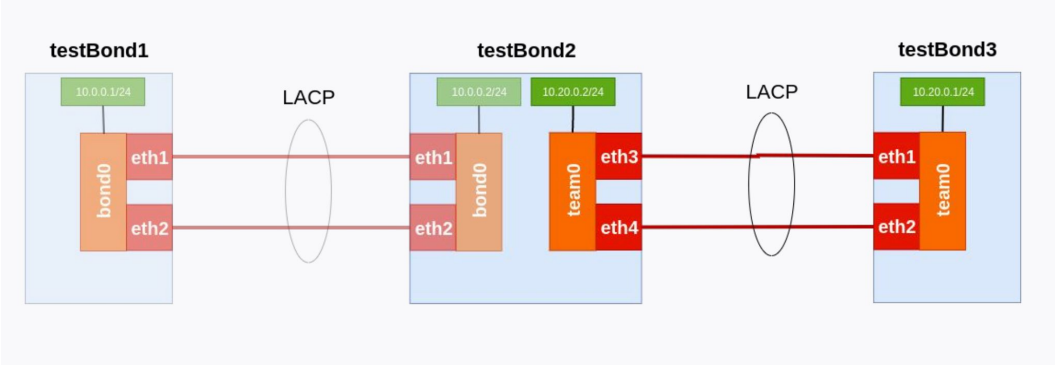
- работает на уровне ядра
- позволяет объединить 2 и более сетевых интерфейса в один логический интерфейс
- позволяет обеспечить отказоустойчивость канала
- позволяет обеспечить распределение нагрузки и балансировку
- позволяет увеличить пропускную способность



Teaming

Teaming — метод агрегации каналов в Linux

- работает на уровне ядра
- позволяет объединить 2 и более сетевых интерфейса в один логический интерфейс
- позволяет обеспечить отказоустойчивость канала
- позволяет обеспечить распределение нагрузки и балансировку
- позволяет увеличить пропускную способность



Как настроение?
Есть ли вопросы?

Практика

Настройка Bonding (nmcli)

```
# Просмотр сетевых интерфейсов
$ nmcli con
# Задаем интерфейс bond0, задаем режим и ip-адрес
$ nmcli con add type bond con-name bond0 ifname bond0 mode active-backup ip4 10.16.10.7/24
# Добавляем сетевые интерфейсы в логический интерфейс
$ nmcli con add type bond-slave ifname  eth0 master bond0
$ nmcli con add type bond-slave ifname eth1 master bond0
# Последовательно поднимаем интерфейсы
$ nmcli con up bond-slave-eth0
$ nmcli con up bond-slave-eth1
$ nmcli connection up bond0
```

Настройка Bonding (через конфиги 1)

```
$ vim /etc/sysconfig/network-scripts/ifcfg-bond0
DEVICE=bond0
NAME=bond0
TYPE=Bond
BONDING_MASTER=yes
IPADDR=10.0.0.1
NETMASK=255.255.255.0
ONBOOT=yes
BOOTPROTO=static
BONDING_OPTS="mode=1 miimon=100 fail_over_mac=1"
NM_CONTROLLED=no
USERCTL=no
```

Настройка Bonding (через конфиги 2)

```
$ vim /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=none
MASTER=bond0
SLAVE=yes
NM_CONTROLLED=no
USERCTL=no

$ vim /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
ONBOOT=yes
BOOTPROTO=none
MASTER=bond0
SLAVE=yes
NM_CONTROLLED=no
USERCTL=no
```

Настройка Teaming (nmcli)

```
# Просмотр сетевых интерфейсов
$ nmcli con

# Задаем интерфейс bond0, задаем режим и ip-адрес
$ nmcli con add type team con-name team0 ifname team0 mode active-backup ip4 10.16.10.7/24

# Добавляем сетевые интерфейсы в логический интерфейс
$ nmcli con add type team-slave ifname eth0 master team0
$ nmcli con add type team-slave ifname eth1 master team0

# Последовательно поднимаем интерфейсы
$ nmcli con up team-slave-eth0
$ nmcli con up team-slave-eth1
$ nmcli connection up team0
```

Настройка Teaming (через конфиги 1)

```
$ vim /etc/sysconfig/network-scripts/ifcfg-team0
DEVICE=team0
IPADDR=10.20.0.2
NETMASK=255.255.255.0
ONBOOT=yes
NM_CONTROLLED=no
USERCTL=no
BOOTPROTO=none
DEVICETYPE="Team"
TEAM_CONFIG='{ "runner" : { "name" : "activebackup", "hwaddr_policy" : "by_active" },
"link_watch" : { "name" : "ethtool" } }'
```

Настройка Teaming (через конфиги 2)

```
$ vim /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=none
NM_CONTROLLED=no
USERCTL=no
DEVICETYPE="TeamPort"
TEAM_MASTER="team0"
TEAM_PORT_CONFIG='{ "prio" : -100 }

$ vim /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
ONBOOT=yes
BOOTPROTO=none
NM_CONTROLLED=no
USERCTL=no
DEVICETYPE="TeamPort"
TEAM_MASTER="team0"
TEAM_PORT_CONFIG='{ "prio" : -100 }
```

Настройка VLAN (nmcli)

```
# Добавляем vlan-интерфейс с именем eth0.12 и VID 12
$ nmcli con add type vlan con-name eth0.12 dev eth0 id 12


# То же самое, но добавляется ip адрес на vlan-интерфейс
$ nmcli con add type vlan con-name eth0.12 dev eth0 id 12 ip4 192.168.100.1/24

# Смотрим существующие интерфейсы
$ nmcli connection
$ nmcli device
```

Настройка VLAN (через конфиги)

```
$ vim /etc/sysconfig/network-scripts/ifcfg-vlan10
ONBOOT=yes
TYPE=Ethernet
VLAN=yes
VLAN_NAME_TYPE=DEV_PLUS_VID_NO_PAD
DEVICE=vlan10
PHYSDEV=eth0
VLAN_ID=10
BOOTPROTO=static
IPADDR=192.168.0.15
NETMASK=255.255.255.0
NM_CONTROLLED=no
```

Вопросы?

Ставим “+”,
если вопросы есть

Ставим “–”,
если вопросов нет

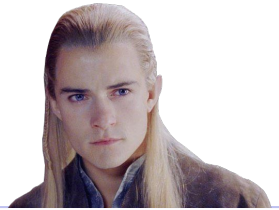
Рефлексия

Цели вебинара

К концу занятия вы сможете

1. Понять как работает VLAN

2. Понять как работает агрегирование каналов



3. Настраивать teaming

Рефлексия

С какими впечатлениями уходите с вебинара?

Как будете применять на практике то,
что узнали на вебинаре?

Заполните, пожалуйста, опрос о занятии по ссылке в чате