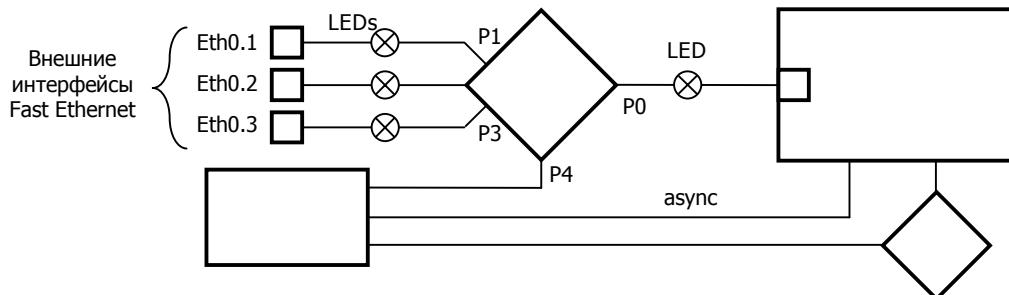


## Использование коммутатора Ethernet в устройствах NSG-700

Устройства NSG-700 оснащены встроенным коммутатором Fast Ethernet с поддержкой VLAN. Коммутатор имеет 5 физических интерфейсов:

- phy 0 — подключён к внутреннему порту eth0, находящемуся на процессоре
- phy 1 ... phy 3 — подключены к разъёмам Eth0.1 ... Eth0.3 на корпусе устройства, соответственно
- phy 4 — подключён к разъёму расширения s1, если в него установлен модуль IM-SDSL h/w ver.2.

Внутренняя архитектура устройств в части Ethernet показана на рисунке.



Для настройки коммутатора используются следующие команды в меню (config-nsg)#:

ethernet-switch

Вход в меню коммутатора. Дальнейшая настройка выполняется в меню (config-ethernet-switch)#:

mode { normal | vlan }

Режим работы коммутатора:

- normal Обычная коммутация между всеми портами без учёта тегов VLAN.
- vlan Передача пакетов на основе тегов VLAN и заданной таблицы коммутации.

show

В режиме VLAN: показать текущую таблицу коммутации. Примеры таблиц коммутации см. ниже.

Если коммутатор работает в режиме VLAN, то для каждого идентификатора VLAN, указанного в настройках хотя бы одного порта, создаётся так называемая VLAN-группа. Каждую такую группу можно рассматривать как отдельный коммутатор с собственным набором физических интерфейсов phy 0 ... phy 4, работающий независимо от остальных. Максимальное число VLAN-групп — 15, т.е. число идентификаторов VLAN, обрабатываемых индивидуально, для всей совокупности интерфейсов не может превышать 15. Помимо этого, всегда существует одна специальная группа other, в которую каждый интерфейс также может включаться или не включаться.

phy <0...4> norm vlan-group { no | <vid> }

phy <0...4> vlan vlan-groups { no | <vid\_list> } { deny-other | permit-other }

Только в режиме VLAN: режим работы для указанного физического интерфейса коммутатора и его принадлежность к VLAN-группам. Данная команда относится как к внешним физическим интерфейсам, так и к внутреннему, подключённому к порту Ethernet процессора.

norm Предполагается, что к интерфейсу подключён сегмент обычной сети Ethernet, т.е. входящие и исходящие пакеты не имеют тегов VLAN. Интерфейс включается в единственную VLAN-группу с указанным идентификатором <vid>. Если вместо этого указано значение vlan-group no, то интерфейс не включён ни в одну VLAN-группу, т.е. работа через него запрещена.

vlan Предполагается, что к интерфейсу подключён физический сегмент с одной или более VLAN, т.е. входящие и исходящие пакеты имеют теги VLAN. Список VLAN, поддерживаемых на данном интерфейсе, может содержать одиночные идентификаторы VLAN и диапазоны из двух идентификаторов, разделенных знаком "-"; элементы списка разделяются запятыми. Интерфейс включается во все VLAN-группы с перечисленными идентификаторами. Дополнительный параметр определяет принадлежность интерфейса к специальной группе other:

deny-other Включить интерфейс в VLAN-группу other.

permit-other Исключить интерфейс из VLAN-группы other.

В частности, если для интерфейса типа vlan установлено vlan-groups no deny-other, то интерфейс не включён ни в одну VLAN-группу, т.е. работа через него запрещена.

### ВНИМАНИЕ

Параметры deny-other и permit-other относятся не к идентификаторам VLAN, определённым на данном физическом интерфейсе, а ко всей совокупности VLAN, определённых на всех пяти интерфейсах коммутатора.

Обработка пакетов производится следующим образом:

- 1) Каждый входящий пакет приписывается к одной из групп по следующим правилам:
  - входящий пакет, имеющий тег VLAN, приписывается к группе с номером равным номеру тега. Если такой группы нет, то пакет приписывается к группе `other`.
  - входящий пакет, не имеющий тега VLAN и пришедший на физический интерфейс типа `norm`, приписывается к группе с номером, равным значению `<vid>` для этого порта. Если для интерфейса установлено `<vid>=no`, то пакет приписывается к группе `other`, но на следующем этапе он будет уничтожен.
  - входящий пакет, не имеющий тега VLAN и пришедший на физический интерфейс типа `vlan`, приписывается к группе `other`.

При этом сам пакет не изменяется.

- 2) Если группа, к которой приписан входящий пакет, не содержит в своём списке номер физического интерфейса, с которого пришел этот пакет, то пакет уничтожается. В частности, это относится:
  - ко всем пакетам, поступившим через интерфейс типа `norm` с настройкой `vlan-group no`
  - к пакетам без тегов VLAN, поступившим через интерфейс типа `vlan` с настройкой `deny-other`
  - к пакетам с тегами VLAN, поступившим через интерфейс типа `vlan` с настройкой `deny-other`, если идентификатор VLAN, указанный в теге, не относится ни к одной из явно определённых VLAN-групп.

Остальные пакеты передаются во все физические интерфейсы, указанные в списке данной группы.

- 3) На выходе из коммутатора каждый исходящий пакет может быть изменен по следующим правилам:
  - если пакет отправляется в физический интерфейс типа `norm` и имеет тег VLAN, то тег будет удален.
  - если пакет отправляется в физический интерфейс типа `vlan` и не имеет тега VLAN, то в этот пакет будет добавлен тег с номером группы, которой принадлежит пакет.
  - во всех остальных случаях пакет не изменяется.

Таким образом, в физические интерфейсы типа `norm` будут уходить только пакеты без тегов VLAN, а в физические интерфейсы типа `vlan` будут уходить только пакеты с тегами.

**ПРИМЕЧАНИЕ** Как можно видеть, конфигурация интерфейсов коммутатора может, в общем случае, не соответствовать природе физических сегментов сети, подключенных к ним. На практике, однако, рекомендуется следить за наличием такого соответствия, чтобы исключить вероятность ошибочной настройки. В частности, рекомендуется обратить внимание на согласованную настройку физического интерфейса `phy 0` коммутатора и порта `eth0` процессора. Рекомендуется также указывать списки используемых VLAN явным образом на каждом интерфейсе.

### Примеры конфигурирования.

#### а) Коммутатор и внутренний порт в нормальном режиме Ethernet:

```
ethernet-switch normal
port eth0 encapsulation ethernet
```

Это обычный режим работы единой физической сети Ethernet без VLAN.

#### б) Коммутатор в нормальном режиме Ethernet, внутренний порт в режиме VLAN:

```
ethernet-switch normal
port eth0 encapsulation vlan
```

Данный режим работы соответствует одной физической сети Ethernet, в которой определено несколько VLAN. Количество и номера VLAN могут быть произвольными.

#### в) Коммутация на основе VLAN — подключение 3 изолированных физических сегментов.

Обмен пакетами напрямую между интерфейсами коммутатора запрещён, каждый из физических интерфейсов соединён с определённой VLAN на внутреннем порту `eth0`. Данная конфигурация устанавливается командой `ethernet-switch mode vlan` по умолчанию.

!

```
nsg
  ethernet-switch
    mode vlan
    phy 0 vlan vlan-groups "101-103" deny-other
    phy 1 norm vlan-group 101
    phy 2 norm vlan-group 102
    phy 3 norm vlan-group 103
    phy 4 norm vlan-group no
  exit
```

```

port eth0
  encapsulation vlan
  vlan 101
    ip address 10.0.0.1/8
  exit
  vlan 102
    ip address 20.0.0.1/8
  exit
  vlan 103
    ip address 30.0.0.1/8
  exit
exit

```

Здесь на порту eth0 определены три IP-интерфейса eth0.101, eth0.102, eth0.103, каждый из которых соединён с соответствующим физическим сегментом сети. Результат выполнения данной настройки:

```

ethernet-switch show

Ethernet switch is in VLAN mode
VLAN memberships:

```

	P0	P1	P2	P3	P4
VLAN 101	X	X	.	.	.
VLAN 102	X	.	X	.	.
VLAN 103	X	.	.	X	.
others	.	.	.	.	.

#### г) Подключение к VLAN сегменту простых (не VLAN) сегментов.

!

```

nsg
  ethernet-switch
    mode vlan
    phy 0 vlan vlan-groups "55,77" permit-other
    phy 1 norm vlan-group 55
    phy 2 norm vlan-group 77
    phy 3 vlan vlan-groups "55,77" permit-other
    phy 4 norm vlan-group no
  exit
  port eth0
    encapsulation vlan
    vlan 101
      ip address 10.0.0.1/8
    exit
    vlan 102
      ip address 20.0.0.1/8
    exit
    vlan 103
      ip address 30.0.0.1/8
    exit
    vlan 55
      ip address 50.0.0.1/8
    exit
    vlan 77
      ip address 70.0.0.1/8
    exit
  exit

```

Результат выполнения данной настройки:

```

ethernet-switch show

Ethernet switch is in VLAN mode
VLAN memberships:

```

	P0	P1	P2	P3	P4
VLAN 55	X	X	.	X	.
VLAN 77	X	.	X	X	.
others	X	.	.	X	.

Здесь все узлы первого сегмента будут частью VLAN 55 из третьего сегмента; также к ней относится субинтерфейс eth0.55 процессора. Аналогично с VLAN 77. Пакеты всех остальных VLAN из третьего сегмента

будут переданы только на интерфейс eth0 процессора. Однако из их числа устройство обработает только пакеты с тегами VLAN 101, 102, 103, 55 и 77; остальные будут уничтожены драйвером порта Ethernet.

#### д) VLAN сеть с ограничением доступа.

```
!  
nsg  
  ethernet-switch  
    mode vlan  
    phy 0 vlan vlan-groups "101,102" permit-other  
    phy 1 vlan vlan-groups "101,102" deny-other  
    phy 2 vlan vlan-groups "101" permit-other  
    phy 3 norm vlan-group no  
    phy 4 norm vlan-group no  
  exit
```

Результат выполнения данной настройки:

```
ethernet-switch show  
  
Ethernet switch is in VLAN mode  
VLAN memberships:  
      P0  P1  P2  P3  P4  
-----  
VLAN 101  X  X  X  .  .  
VLAN 102  X  X  .  .  .  
others    X  .  X  .  .
```

Здесь коммутатор пропустит из первого сегмента только пакеты с тегами VLAN 101 и 102, все остальные будут уничтожены.

Необходимо обратить внимание, однако, что и из второго сегмента не все пакеты пройдут через коммутатор, несмотря на то, что для него сконфигурировано permit-other. Если через физический интерфейс 2 поступит пакет с тегом VLAN 102, то он будет приписан к VLAN группе 102. Но, согласно таблице, эта группа содержит только физические интерфейсы 0 и 1, поэтому пакет будет уничтожен. Чтобы все пакеты сегмента 2 были пропущены, необходимо настроить интерфейс следующим образом:

```
phy 2 vlan vlan-groups "101,102" permit-other
```

#### е) Объединение двух сегментов без доступа к устройству NSG-700.

```
!  
nsg  
  ethernet-switch  
    mode vlan  
    phy 0 norm vlan-group 700  
    phy 1 norm vlan-group 666  
    phy 2 norm vlan-group 666  
    phy 3 vlan vlan-groups "700" deny-other  
    phy 4 norm vlan-group no  
  exit  
  port eth0  
    ip address 10.0.0.7/8  
  exit
```

Результат выполнения данной настройки:

```
ethernet-switch show  
  
Ethernet switch is in VLAN mode  
VLAN memberships:  
      P0  P1  P2  P3  P4  
-----  
VLAN 666  .  X  X  .  .  
VLAN 700  X  .  .  X  .  
others    .  .  .  .  .
```

Здесь первый и второй физические сегменты соединены друг с другом, но не имеют доступа ни в третий сегмент, ни к интерфейсу eth0. Физический интерфейс 0 имеет тип norm, поэтому и для внутреннего порта eth0 необходимо использовать encapsulation ethernet (это настройка по умолчанию). Порт eth0 будет принадлежать VLAN 700 в третьем сегменте, причём присвоение и удаление тегов VLAN в данном случае производится на интерфейсе коммутатора. Никакие другие пакеты через коммутатор пропущены не будут.