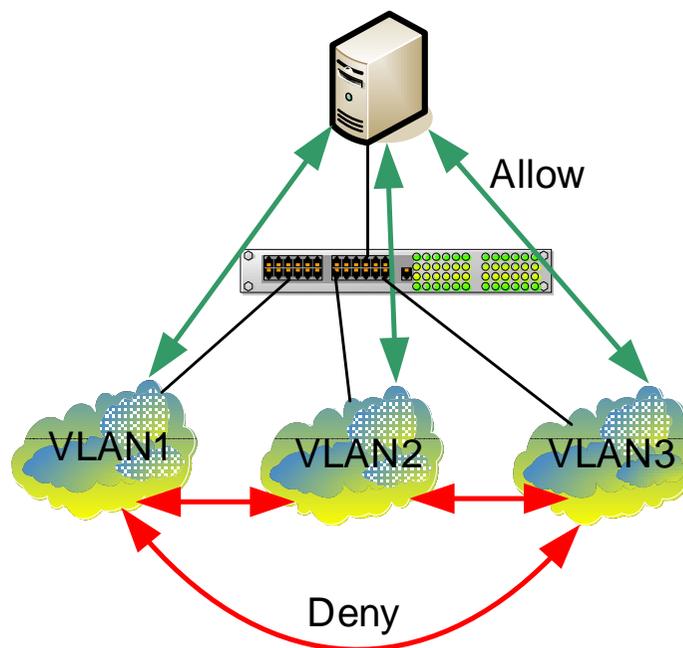


Настройка функции Traffic Segmentation
для разделения общих ресурсов используя
коммутаторы D-Link 2 уровня

Совместно используемые информационные ресурсы



Общие ресурсы/серверы (почтовые серверы , файл-серверы, FTP/HTTP службы) могут быть доступны всем пользователям в группах VLAN1, VLAN2, VLAN3, но доступ между собой этим группам не разрешен (для обеспечения производительности или для обеспечения политики безопасности)

Решение на коммутаторах 2 уровня: Асимметричные VLAN или Traffic Segmentation

Решение на коммутаторах 3 уровня: Коммутатор 3 уровня + ACL (списки доступа) для ограничения доступа между группами

Асимметричные VLAN в сравнении с Traffic Segmentation

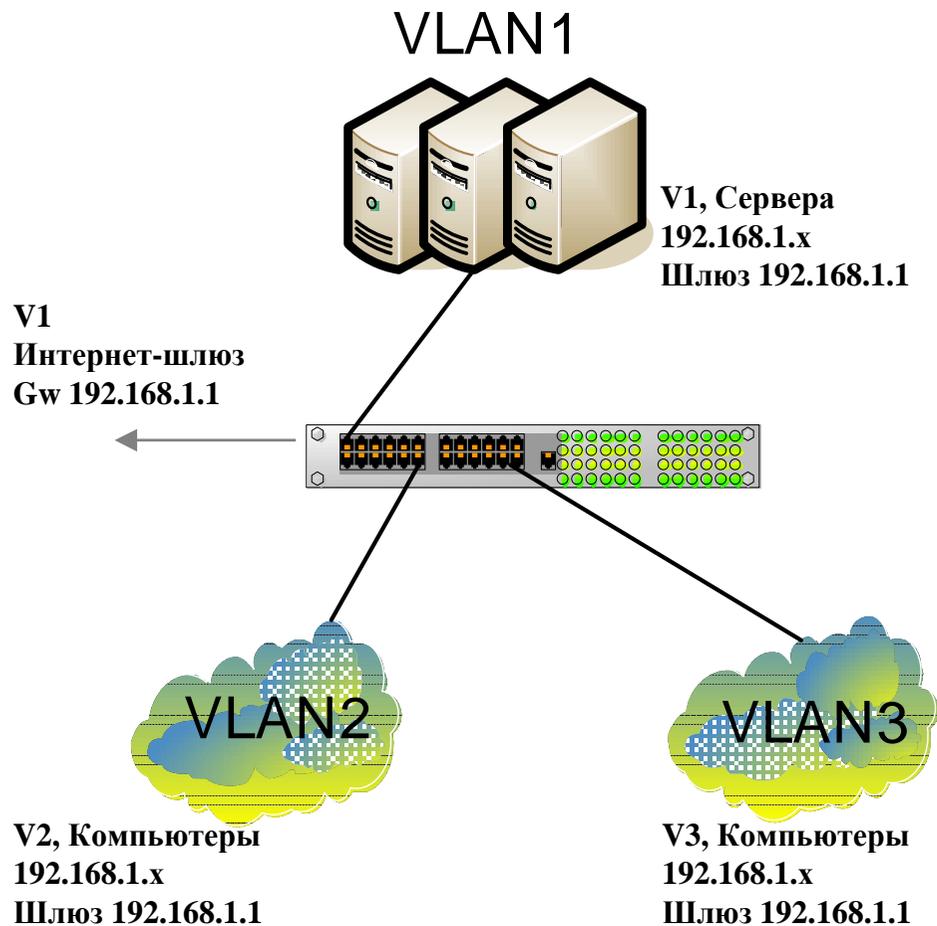
Асимметричные VLAN:

- Необходимы хорошие знания стандарта 802.1q
- Участники VLAN могут быть на разных коммутаторах, и общие ресурсы (напр., сервер) могут находиться где угодно.
- Необходима специальное расширение для 802.1q (возможность использования одного и того же порта Untagged в нескольких VLAN)
- Может не поддерживаться IGMP snooping
- Максимальное количество VLAN ограничено 4096

Traffic Segmentation:

- Простота настройки, нет необходимости в знании 802.1q
- Участники одной группы не могут быть подключены к разным коммутаторам
- IGMP snooping будет работать по прежнему.
- Traffic Segmentation может быть представлен в виде иерархического дерева. Нет ограничений на создание групп.
- Общие ресурсы/сервера должны быть на “вершине” коммутатора (когда используется иерархическая структура)

Traffic Segmentation



V1: port 1-8

Общие сервера и Интернет-шлюз

V2: port 9-16

VLAN2 пользователи(компьютеры или хабы/свитчи)

V3: port 17-24

VLAN3 пользователи(компьютеры или коммутаторы)

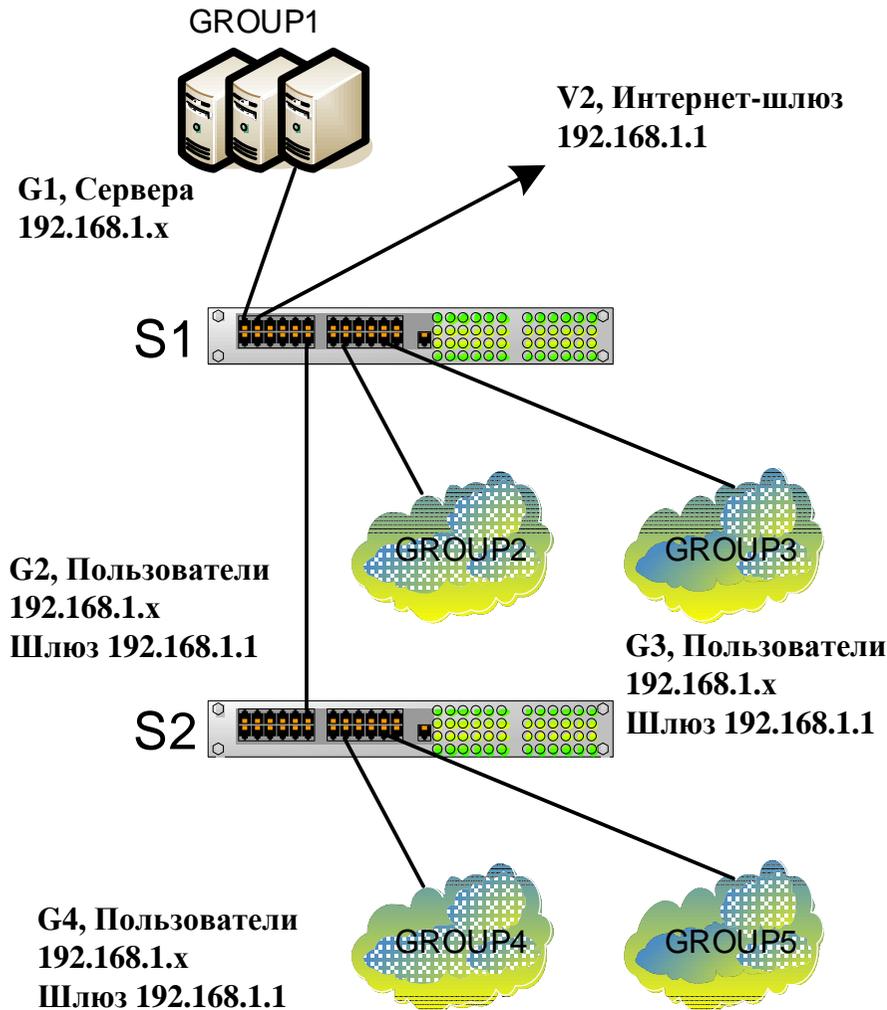
Необходимые условия

1. V2 и V3 должны иметь доступ к V1 (с использованием IPX, других протоколов IP, AppleTalk, NetBEUI и т.д.)
2. V2 и V3 должны иметь доступ к интернет-шлюзу используя ту же самую IP сеть.
3. Доступ между V2 и V3 должен быть запрещен.

Настройки DES-3526

```
config traffic_segmentation 1-24 forwarding_list 1-8  
config traffic_segmentation 9-16 forwarding_list 1-16  
config traffic_segmentation 17-24 forwarding_list 1-8,17-24
```

Traffic Segmentation- двухуровневая иерархия



S1port1-4: G1, untagged
Общие сервера и Интернет-шлюз

S1port 5-8, S2 port 1-2 , untagged
для связи с другими коммутаторами

S1port 9-16: G2, untagged
VLAN2 пользователи (компьютеры или коммутаторы)

S1port17-24: G3, untagged
Группа 3 пользователи (компьютеры или коммутаторы)

S2Port1: uplink port
S2port 3-16: G4, untagged
Группа 4 пользователи (компьютеры или коммутаторы)

S2port 17-24: G5
Группа 5 пользователи (компьютеры или коммутаторы)

Необходимые условия:

Все группы имеют доступ к группе G1.

G2, G3, G4, G5 не имеют доступа к друг другу.

Traffic Segmentation- двухуровневая иерархия

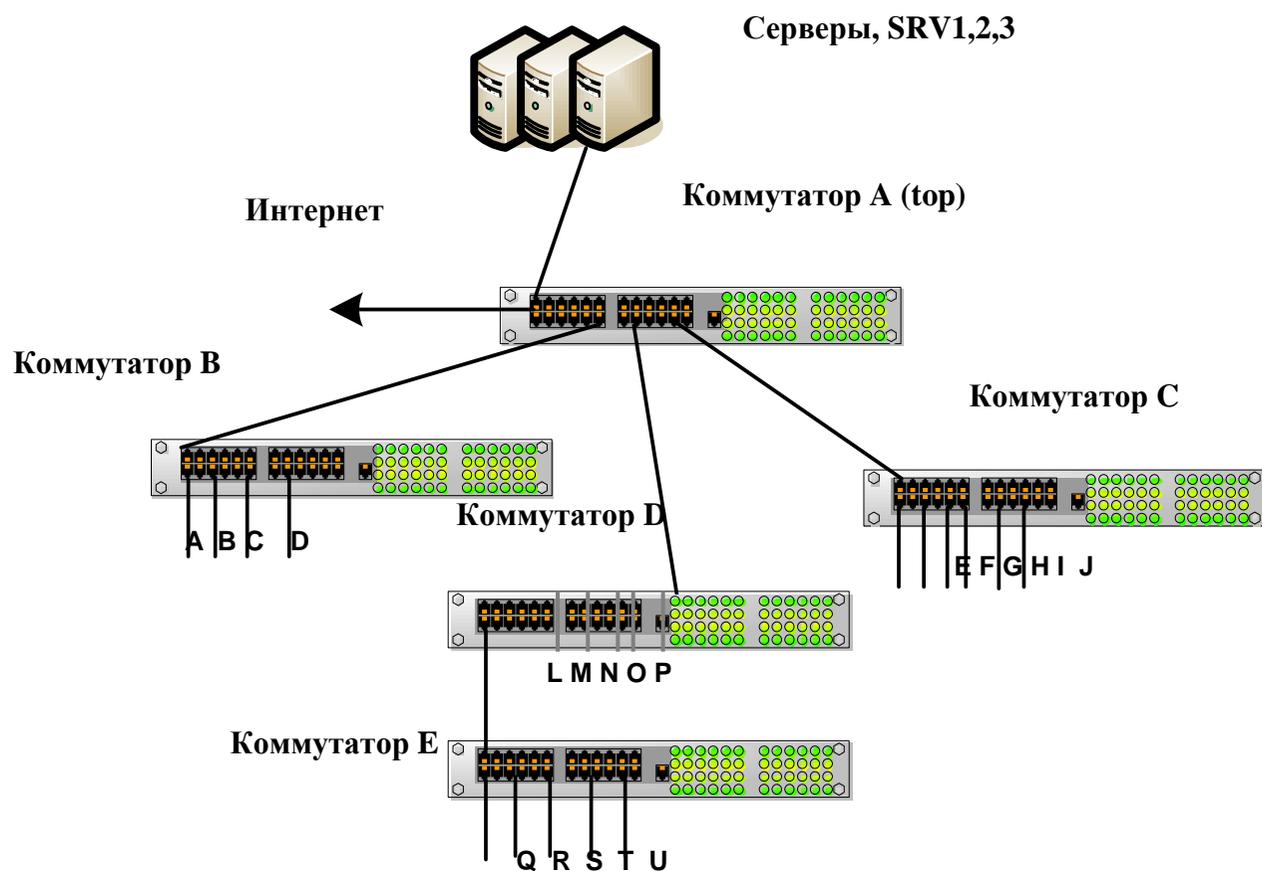
Настройки S1

```
config traffic_segmentation 1-4 forwarding_list 1-24  
config traffic_segmentation 5 forwarding_list 1-5  
config traffic_segmentation 9-16 forwarding_list 1-4, 9-16  
config traffic_segmentation 17-24 forwarding_list 1-4, 17-24
```

Настройки S2

```
config traffic_segmentation 1 forwarding_list 1-24  
config traffic_segmentation 2-16 forwarding_list 1-16  
config traffic_segmentation 17-24 forwarding_list 1,17-24
```

Иерархическая структура Traffic Segmentation



- 1) Все компьютеры (от А до U) не «видят» друг друга.
- 2) Все компьютеры (от А до U) должны «видеть» Srv1, Srv2, Srv3 and Интернет.
- 3) Все свитчи DES-3526.
- 4) Одна и та же IP сеть на всех компьютерах

Настройка

Коммутатор А (top)

```
config traffic_segmentation 1-4 forwarding_list 1-26  
config traffic_segmentation 5 forwarding_list 1-5  
config traffic_segmentation 6 forwarding_list 1-4,6  
config traffic_segmentation 7 forwarding_list 1-4,7  
(repeat for other downlink ports)
```

Коммутаторы В, С, D, E,...

```
config traffic_segmentation 1 forwarding_list 1-26  
config traffic_segmentation 2-24 forwarding_list 1
```