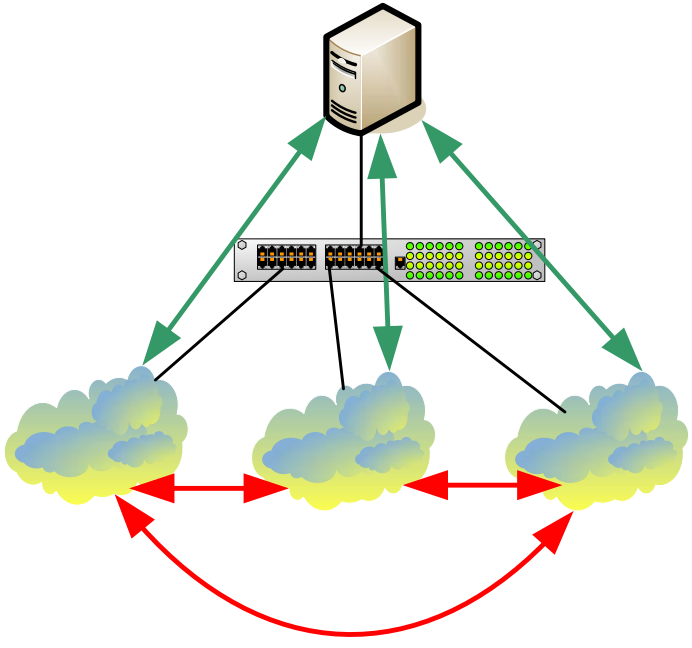
Настройка Асимметричных VLAN для разделения общих ресурсов используя коммутаторы D-Link 2 уровня

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

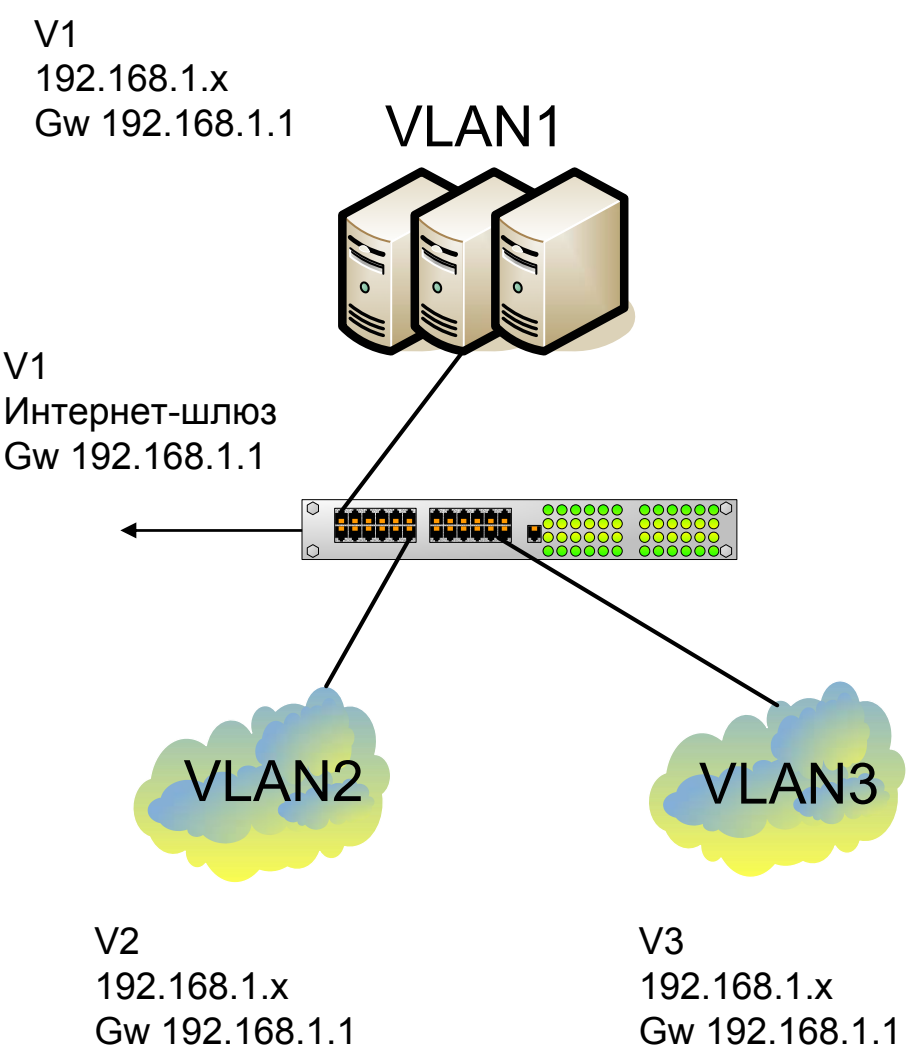
Решение на коммутаторах 3 уровня: Коммутатор 3 уровня + ACL (списки доступа) для ограничения доступа между группами

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 находится 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)

Пример1: Асимметричные VLAN



V1: порты 1-8, untagged
Общедоступные сервера или Интернет-шлюз.

V2: порты 9-16, untagged
VLAN2 пользователи (компьютеры и/или серверы)

V3: порты 17-24, untagged
VLAN3 пользователи (компьютеры или коммутаторы)

Необходимые условия
V2 и V3 могут получать доступ к V1 (с использованием IPX, других протоколов IP, AppleTalk, NetBEUI и т.д.)
V2 и V3 могут получать доступ с Интернет-шлюзу для доступа в интернет используя ту же сеть IP.
Группы V2 и V3 между собой общаться не должны.

Пример1: Асимметричные VLAN

PVID and VLAN settings:

ports	1-8	9-16	17-24
pvid	1..1	2..2	3..3
VLANS			
default	E..E	E..E	E..E
(V1)	U..U	U..U	U..U
V2	E..E	E..E	-..-
	U..U	U..U	-..-
V3	E..E	-..-	E..E
	U..U	-..-	U..U

```
enable asymmetric_vlan
create vlan v2 tag 2
create vlan v3 tag 3

config vlan v2 add untagged 1-16
config vlan v3 add untagged 1-8,17-24

config gvrp 1-8 pvid 1
config gvrp 9-16 pvid 2
config gvrp 17-24 pvid 3
save
```

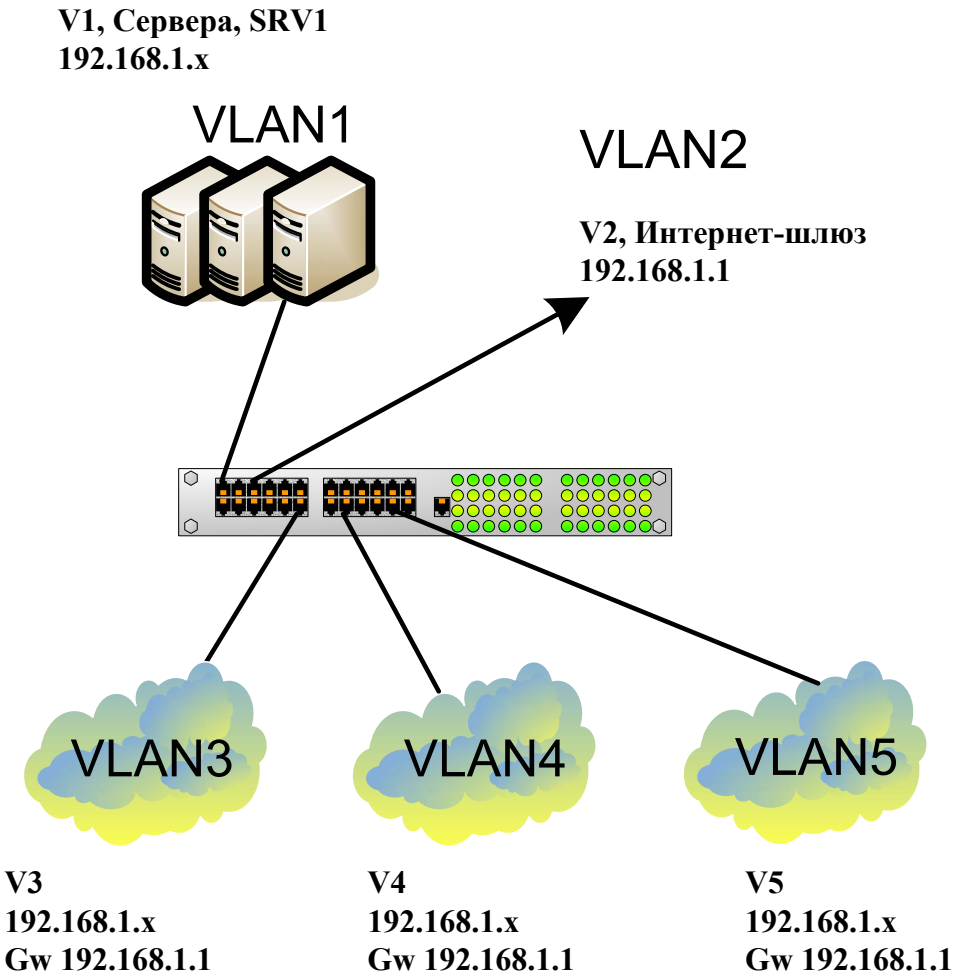
Тест:

Компьютеры из группы V2 получают доступ к группе V1 и интернет-шлюзу. Проверяется командой ping

Компьютеры из группы V3 получают доступ к группе V1 и интернет-шлюзу.

Компьютеры из группы V2 не могут видеть компьютеры из группы V3 и наоборот.

Пример 2: Асимметричные VLAN
Различные VLAN имеют различный уровень доступа



SRV1: ports 1,2
Интернет-шлюз: ports 3,4
VLAN3: 5-8
VLAN4: 9-16
VLAN5: 17-24

Необходимые условия:
V3 имеет доступ к V1 SRV1, но не имеет доступа к V2.
V4 имеет доступ к V1, и к V2
V5 имеет доступ к V2, но не имеет доступа к V1.
V3, V4, V5 не имеют доступа к друг другу.

Пример 2: Асимметричные VLAN
Различные VLAN имеют различный уровень доступа

PVID and VLAN settings:

VLAN	V1	V2	V3	V4	V5
ports	1-2	3-4	5-8	9-16	17-24
pvid	1..1	2..2	3..3	4..4	5..5
default	E..E	E..E	E..E	E..E	---
(V1)	U..U	U..U	U..U	U..U	---
V2	E..E	E..E	---	E..E	E..E
	U..U	U..U	---	U..U	U..U
V3	E..E	---	E..E	---	---
	U..U	---	U..U	---	---
V4	E..E	E..E	---	E..E	---
	U..U	U..U	---	U..U	---
V5	---	E..E	---	---	E..E
	---	U..U	---	---	U..U

Пример 2: Асимметричные VLAN
Различные VLAN имеют различный уровень доступа

```
enable asymmetric_vlan
# default vlan is created by default
create vlan v2 tag 2
create vlan v3 tag 3
create vlan v4 tag 4
create vlan v5 tag 5

config vlan default delete 17-24
config vlan v2 add untagged 1-4,9-24
config vlan v3 add untagged 1-2,5-8
config vlan v4 add untagged 1-4, 9-16
config vlan v5 add untagged 3-4, 17-24

config gvrp 1-2 pvid 1
config gvrp 3-4 pvid 2
config gvrp 5-8 pvid 3
config gvrp 9-16 pvid 4
config gvrp 17-24 pvid 5

save
```

Группа V3 имеет доступ к V1, но не имеет доступа к V2, и другим VLANs (V4, V5)

Группа V4 имеет доступ к V1 и V2, но не имеет доступ к V5.

Группа V5 имеет доступ к V2, но не имеет доступ к V1.

Ограничение асимметричных VLAN

IGMP Snooping не поддерживается при использовании асимметричных VLAN.

Решение: Использование коммутатора 3 уровня + ACL(листы доступа) + многоадресная (multicasting) маршрутизация + IGMP snooping

При использовании Assymetric VLAN не происходит изучение, а также добавление в таблицы коммутации, MAC-адресов с тегированных портов. Тем самым применение Assymetric VLAN ограничивается одним коммутатором.