D-Link
Building Networks for People

Технологии, применяемые при построении сетей на основе коммутаторов D-Link Расширенный функционал

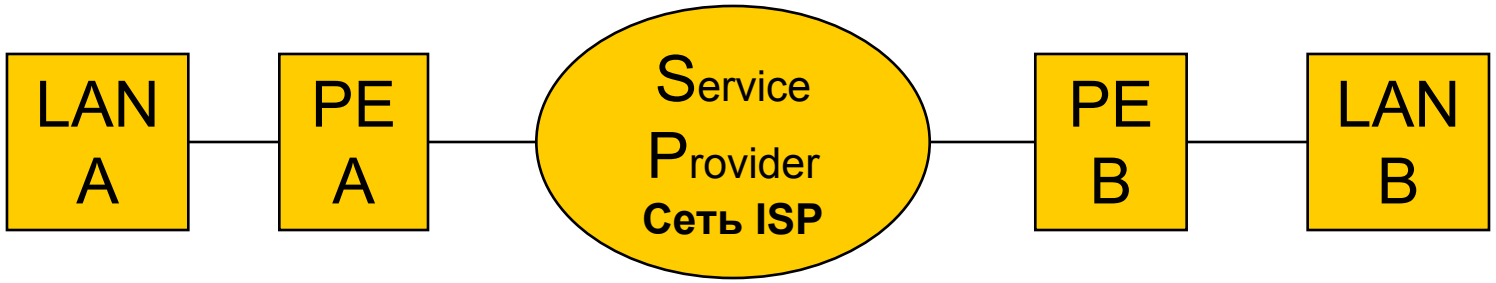
Дёмин Иван, консультант по проектам

idemin@dlink.ru

Double VLAN (Q-in-Q)

Введение в технологию Double VLAN

Назначение технологии: Transparent LAN services (TLS), прозрачные сервисы для сетей LAN



PE: Provider Edge – оконечное оборудование провайдера
SP: Service Provider – сервис-провайдер

Введение в технологию Double VLAN

Что такое “Double VLAN”?

Данная функция поддерживает инкапсуляцию тегов IEEE 802.1Q VLAN в теги второго уровня 802.1Q tag на провайдерских граничных коммутаторах Provider Edge (PE)

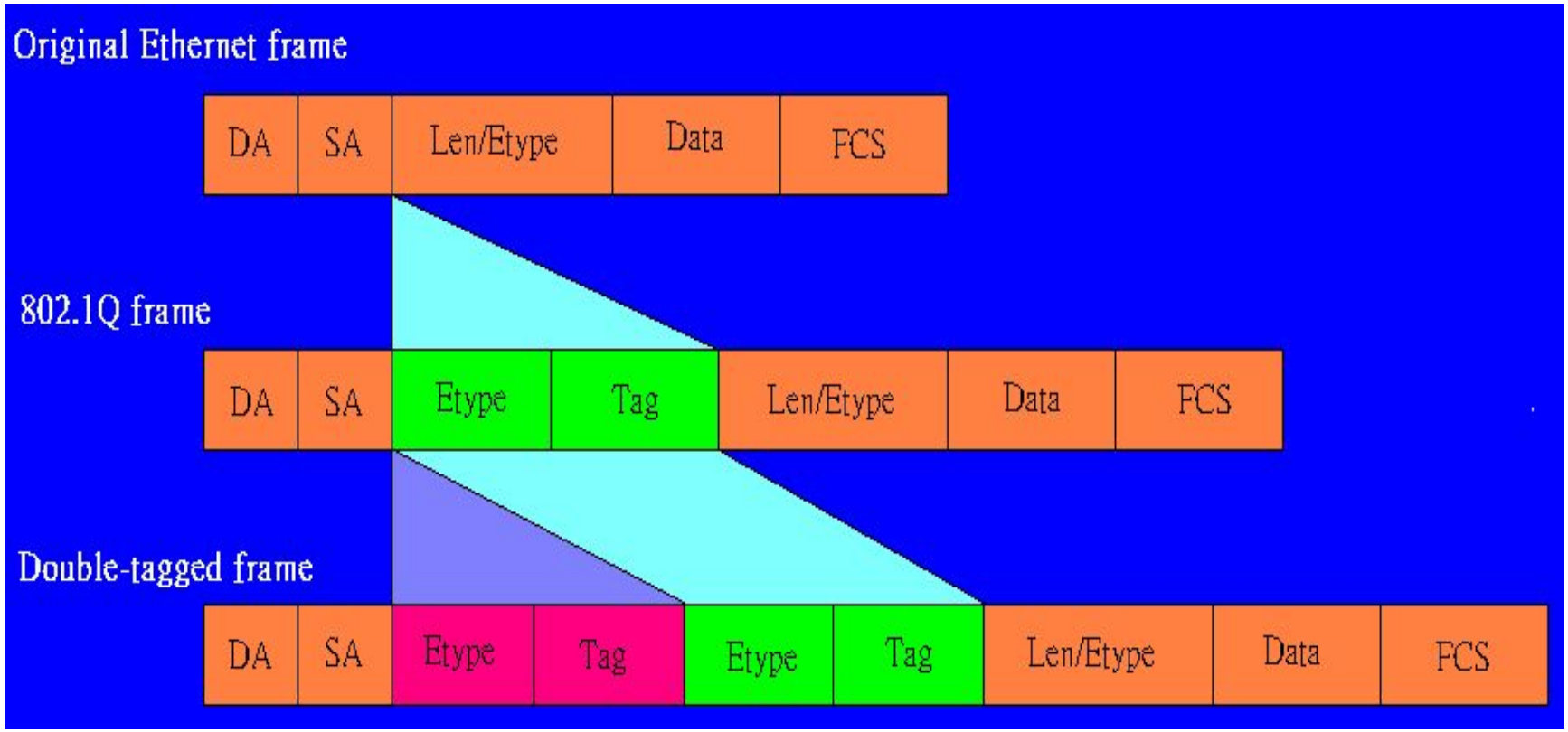
При помощи Double VLAN сервис провайдер может использовать уникальные VLAN (называемые Service-provider VLAN ID, или SP-VLAN ID) для предоставления услуг клиентам, которые имеют несколько VLAN в своих сетях.

VLAN клиента, или Customer VLAN IDs (CVLAN IDs) в этом случае сохраняются и трафик от различных клиентов сегментируется даже если он передается в одном и том же VLAN.

D-Link
Building Networks for People

Введение в технологию Double VLAN

Формат пакета Double Tagging VLAN

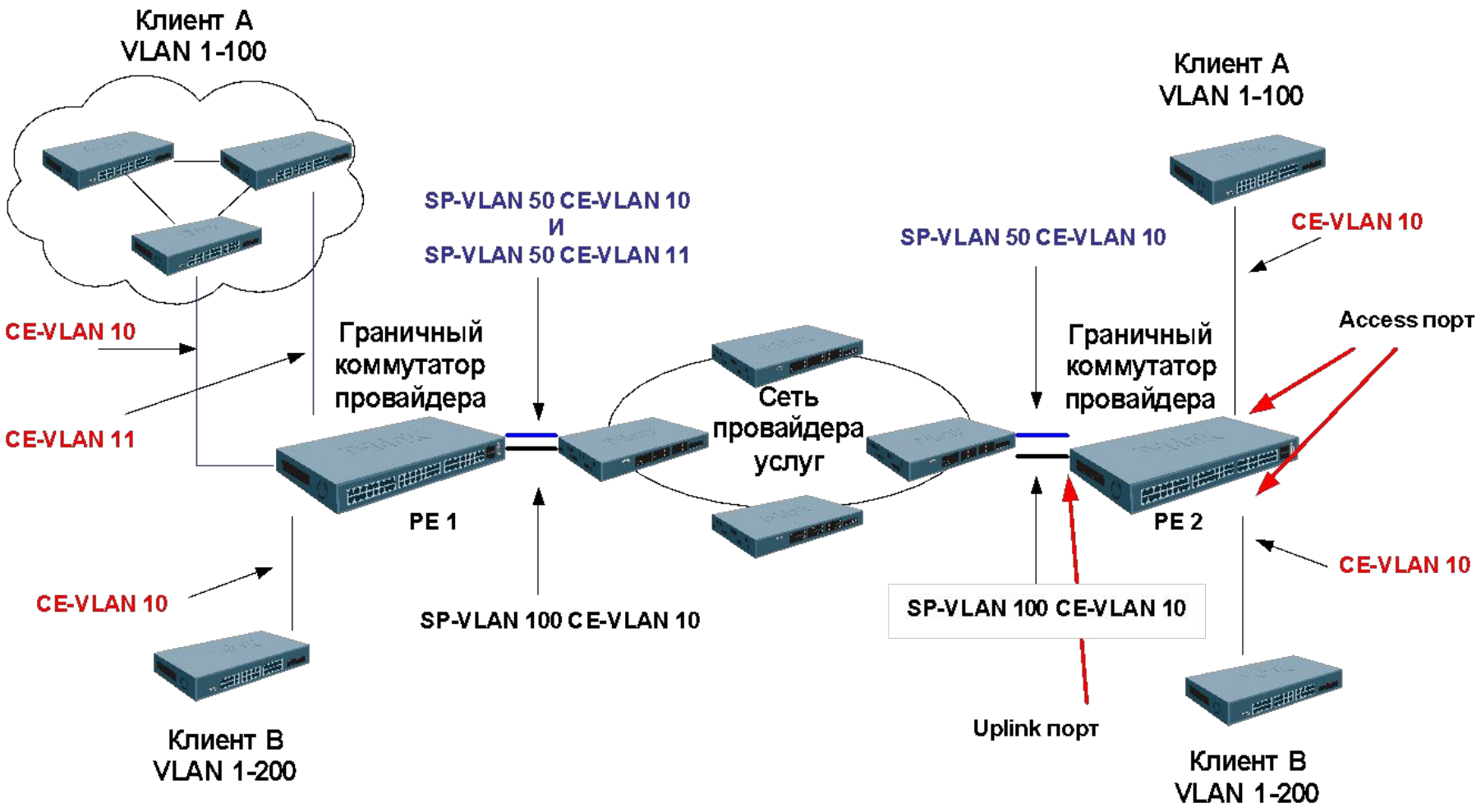


Количество 802.1q VLAN равно 4094

При использовании Double VLAN мы получаем 4094 * 4094 = 16,760,836 VLAN

D-Link
Building Networks for People

Базовая архитектура сети



D-Link
Building Networks for People

Понятия Access Port и Uplink Port

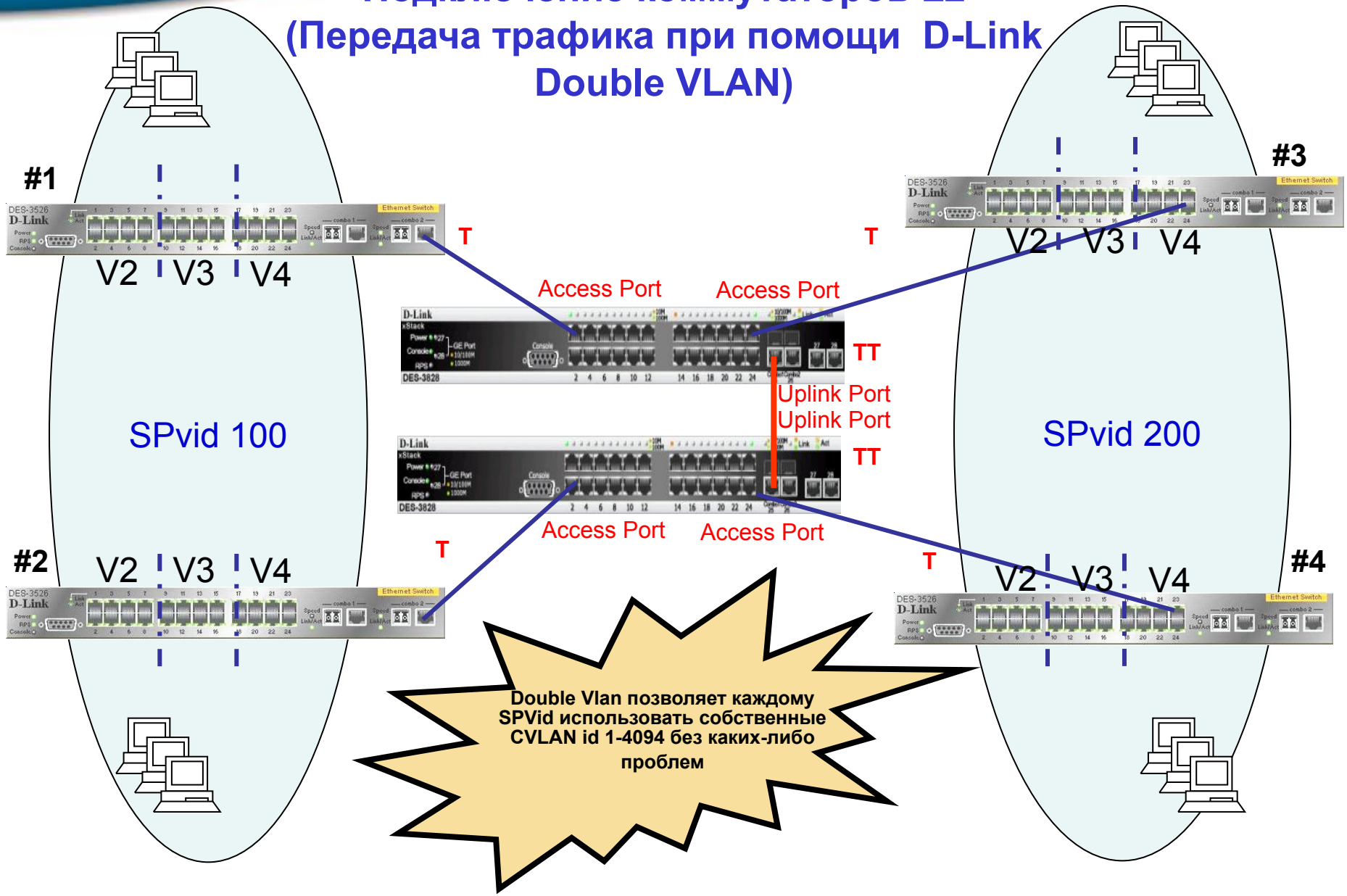
Граничные коммутаторы провайдера Provider Edge (PE1 & PE2) настроены для обработки Double VLAN для 2-х клиентских VLAN. Каждому пользователю назначен уникальный VLAN провайдера: SP-VLAN 100 для клиента A и SP-VLAN 200 для клиента B. Когда пакет поступает на Access Port, подключенный к сети клиента, коммутатор PE добавляет еще один тег 802.1Q, называемый SP-VLAN.

- Если исходящий для пакета порт является портом Access Port, тогда коммутатор PE удаляет тег SP-VLAN из пакета.
- Если исходящий порт это Uplink Port, то пакет будет передан дальше вместе с тегом SP-VLAN и тегом CVLAN (если изначально в пакете тег содержался) или только с тегом SP-VLAN (если это был пакет без тега)
- Access Port используется для подключения к PE клиентских VLAN
- Uplink Port используется для подключения PE к сети провайдера

Примечание: В DES-3800 порты Ethernet 10/100 могут быть только Access Port; гигабитные порты должны быть портами Uplink

D-Link
Building Networks for People

Подключение коммутаторов L2 (Передача трафика при помощи D-Link Double VLAN)



D-Link
Building Networks for People

Настройка устройств

- DES-3828 #1,#2

reset config
enable double_vlan
All setting will return to default setting.
Are you sure to change the system
vlan mode?(y/n)y
config double_vlan default delete 1-28
create double_vlan d100 spvid 100
create double_vlan d200 spvid 200
config double_vlan d100 add access 1-12
config double_vlan d200 add access 13-24
Uplink – порты могут быть назначены
только на гигабитных портах #
config double_vlan d100 add uplink 25-28
config double_vlan d200 add uplink 25-28
save

- DES-3526 #1,#2,#3,#4

reset config
config vlan default delete 1-26
create vlan v2 tag 2
create vlan v3 tag 3
create vlan v4 tag 4
config vlan v2 add untagged 1-8
config vlan v2 add tagged 25-26
config vlan v3 add untagged 9-16
config vlan v3 add tagged 25-26
config vlan v4 add untagged 17-24
config vlan v4 add tagged 25-26
save

Примечание

В настоящее время функция Double VLAN соответствует драфту стандарта 802.1ad

D-Link
Building Networks for People

Безопасность на уровне портов и защита от вторжений

D-Link
Building Networks for People

IP-MAC-Port Binding
(Привязка IP-MAC-порт)

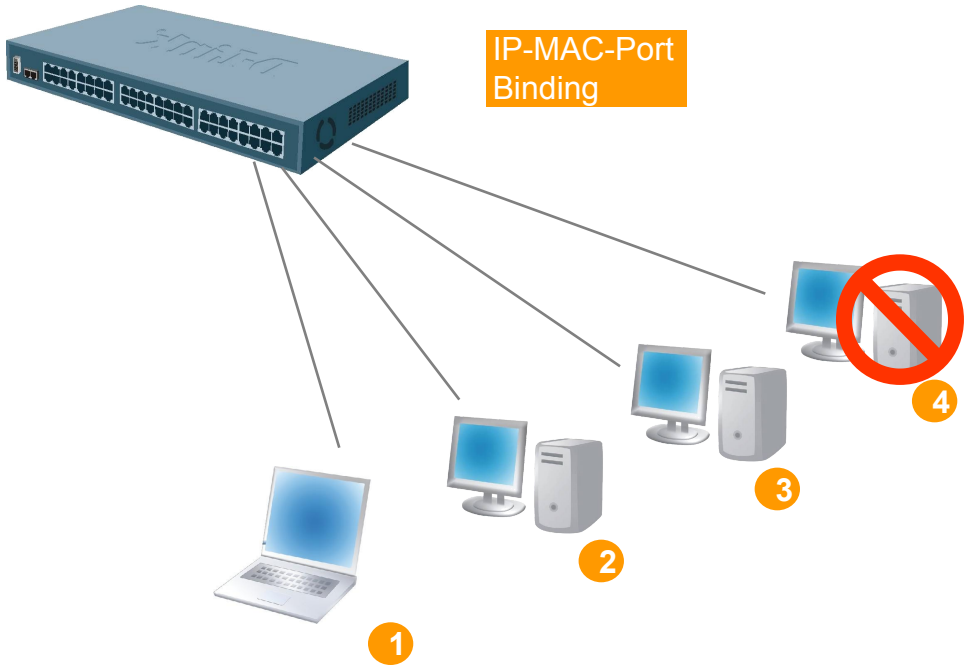
IP-MAC-Port Binding

- **Проверка подлинности компьютеров в сети**

Привязка IP-MAC-порт (IP-MAC-Port Binding)

Функция *IP-MAC-Port Binding* в коммутаторах D-Link позволяет контролировать доступ компьютеров в сеть на основе их IP и MAC-адресов, а также порта подключения. Если какая-нибудь составляющая в этой записи меняется, то коммутатор блокирует данный MAC-адрес с занесением его в блок-лист.

Эта функция специально разработана для управления сетями ETTH/ ETTB и офисными сетями



Связка IP-MAC-порт не соответствует разрешённой – MAC-адрес компьютера заблокирован !!

D-Link
Building Networks for People

Для чего нужна функция IP-MAC-Port binding?

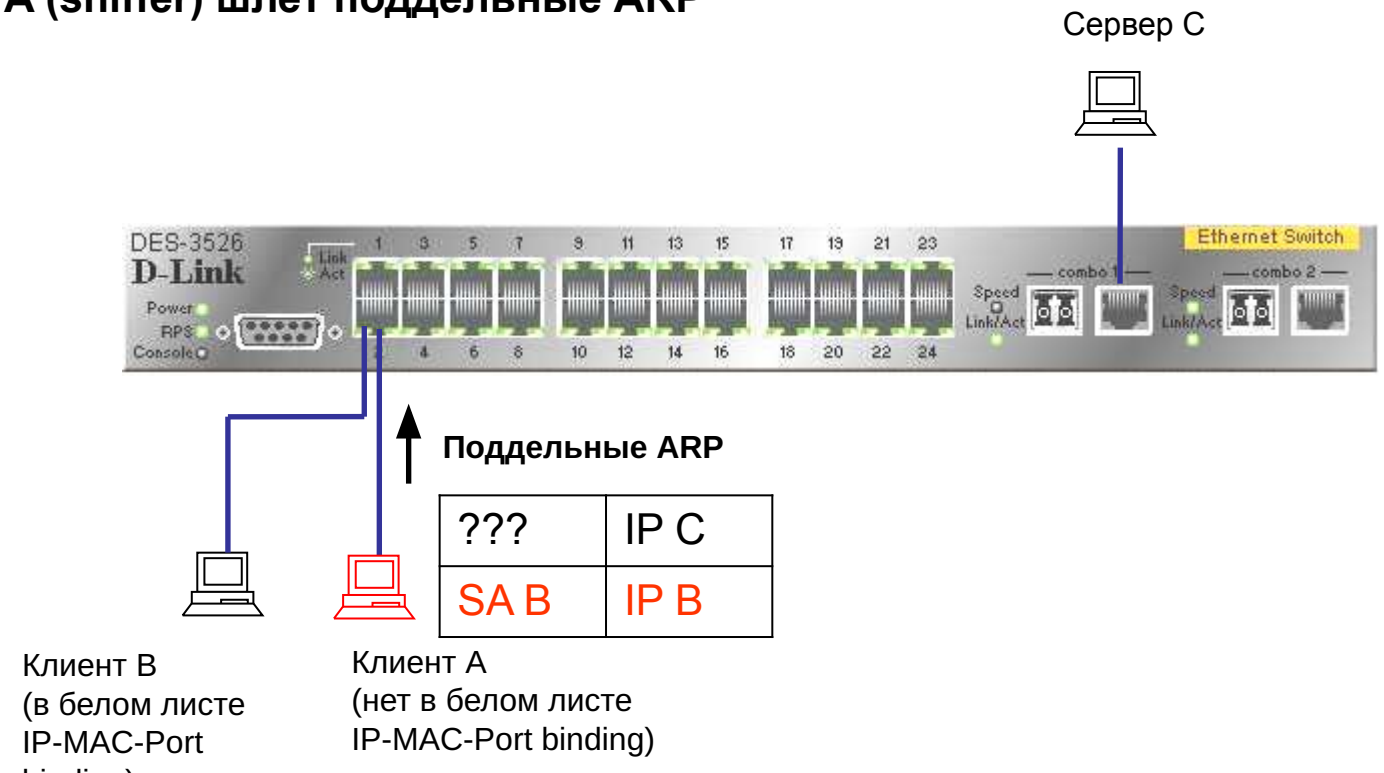
- D-Link расширил популярную функцию IP-MAC binding до более удобной в использовании IP-MAC-Port binding с целью повышения гибкости аутентификации пользователей в сети.
- IP-MAC-Port binding включает два режима работы: ARP (по умолчанию) и ACL. Сравнение этих двух режимов показано в таблице ниже:

	ARP режим	ACL режим
Плюсы	Простота в использовании и независимость от ACL	Позволяет предотвратить несанкционированное подключение даже если нарушитель использует статический MAC адрес
Минусы	Невозможность фильтрации в случае если hacker/sniffer присвоит себе статический MAC адрес для спуфинга коммутатора	Тратится профиль ACL, а также необходимо продумывать целиком всю стратегию ACL

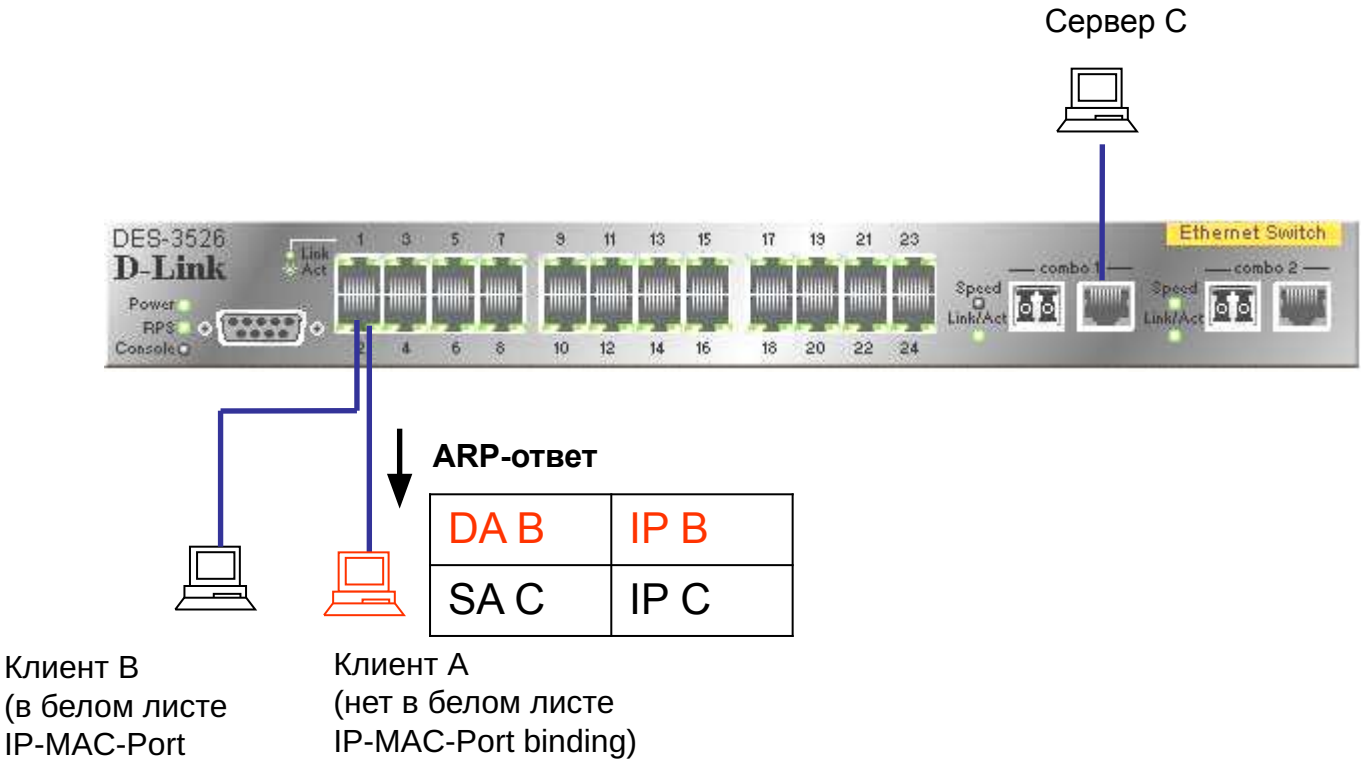
- IP-MAC-Port Binding поддерживается коммутаторами L2 серии xStack – DES-3000 (только ARP Mode), DES-3500 (R4 – ACL Mode), L3 - DES-3800 (R3), DGS-3600 и DGS-3400 (R2).
- Данный документ описывает примеры настройки IP-MAC-Port binding, например, против атак ARP Poison Routing.

Пример 1. Использование режима ARP или ACL для блокирования снифера

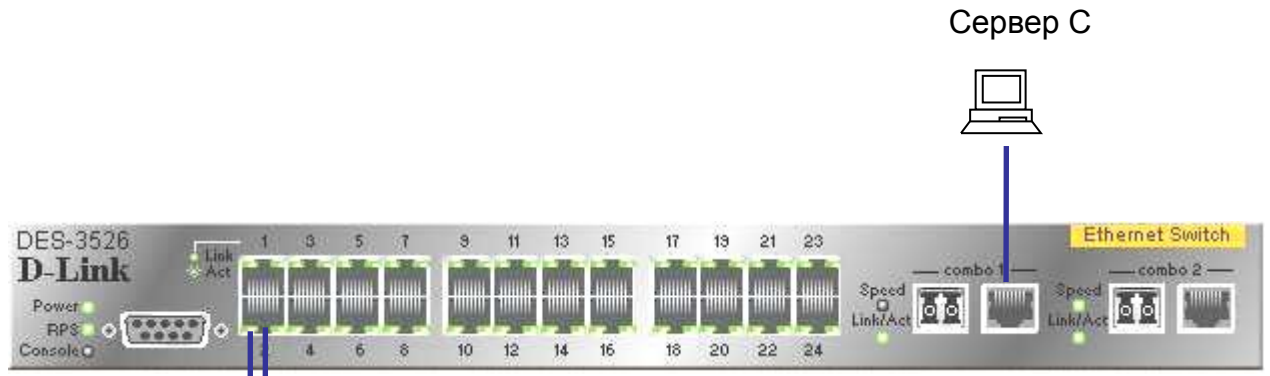
Шаг 1: Клиенты A и B подключены к одному порту коммутатора, клиент A (sniffer) шлет поддельные ARP



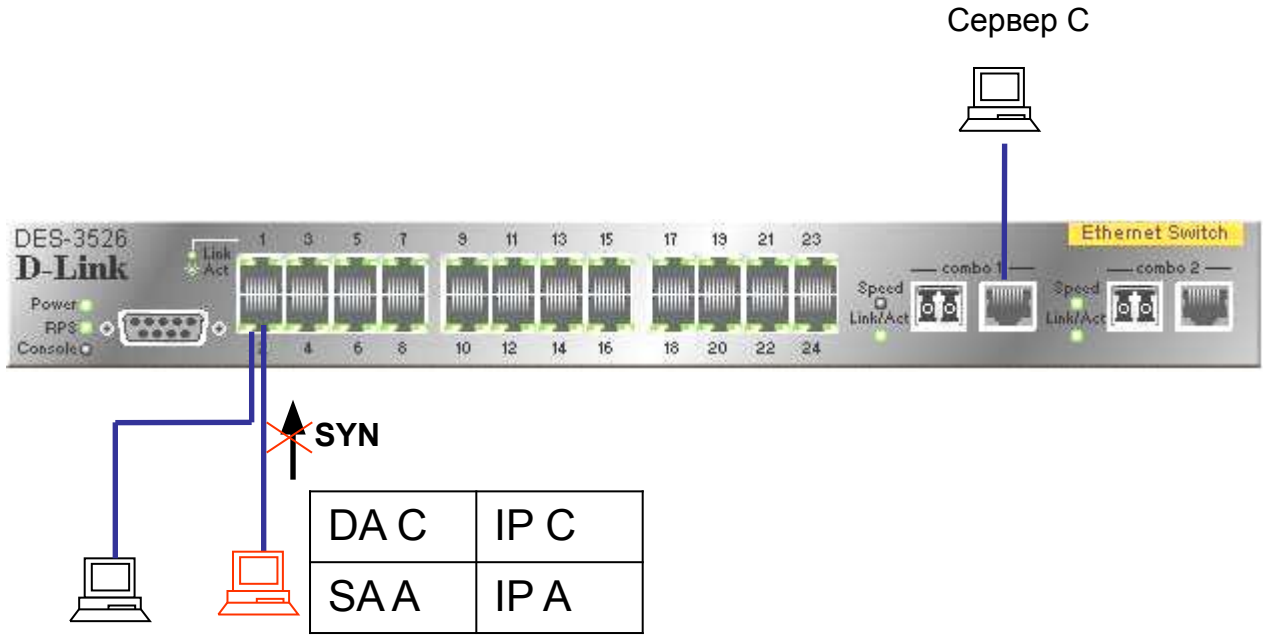
Шаг 2: Сервер C отвечает на запрос и изучает поддельную связку IP/MAC.



Шаг 3: Клиент A хочет установить TCP соединение с сервером C



Шаг 4: Т.к. клиент А не в белом листе, DES-3526 блокирует пакет, поэтому, соединение не сможет быть установлено

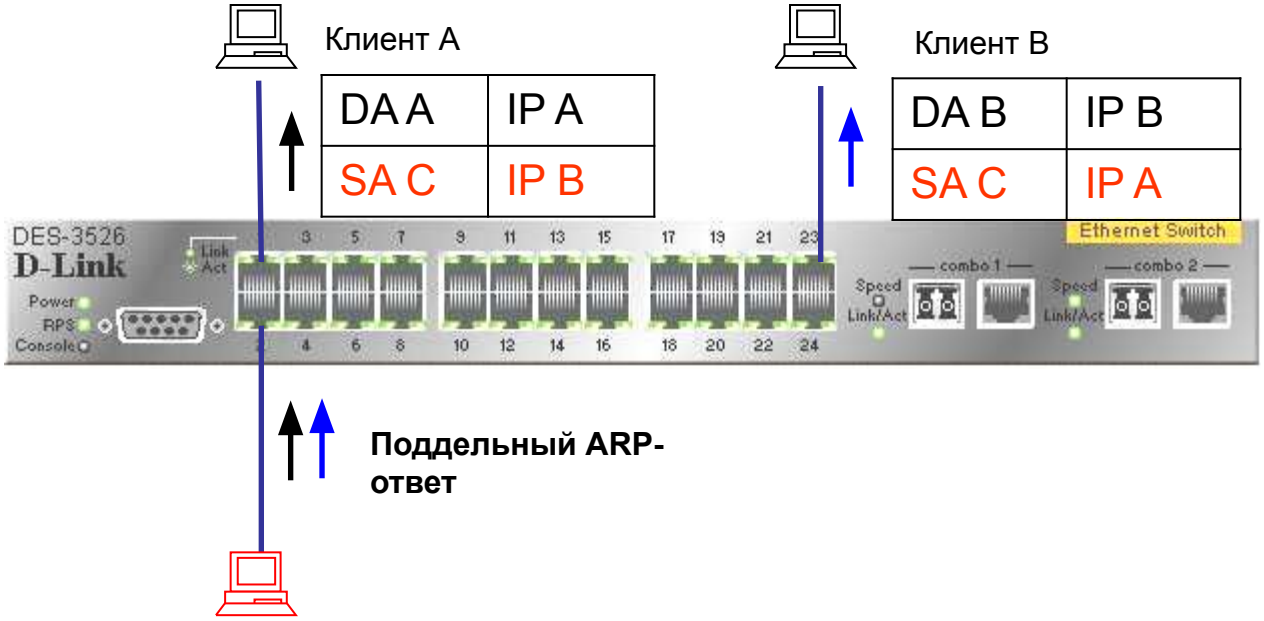


Клиент В
(в белом листе
IP-MAC-Port
binding)

Клиент А
(нет в белом листе
IP-MAC-Port binding)

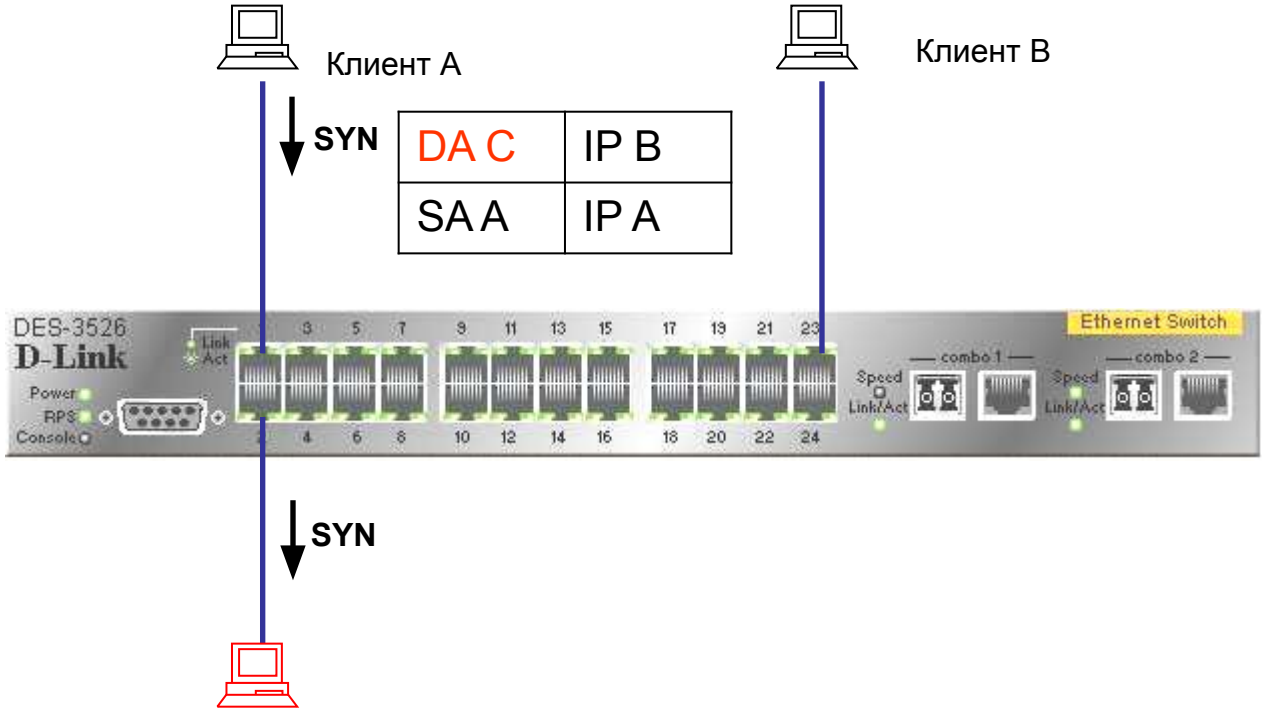
Пример 2. Использование режима ACL для предотвращения ARP атаки Man-in-the-Middle

Шаг 1: Sniffer C (Man in the middle) отсылает поддельный пакет ARP-Reply клиентам A и B



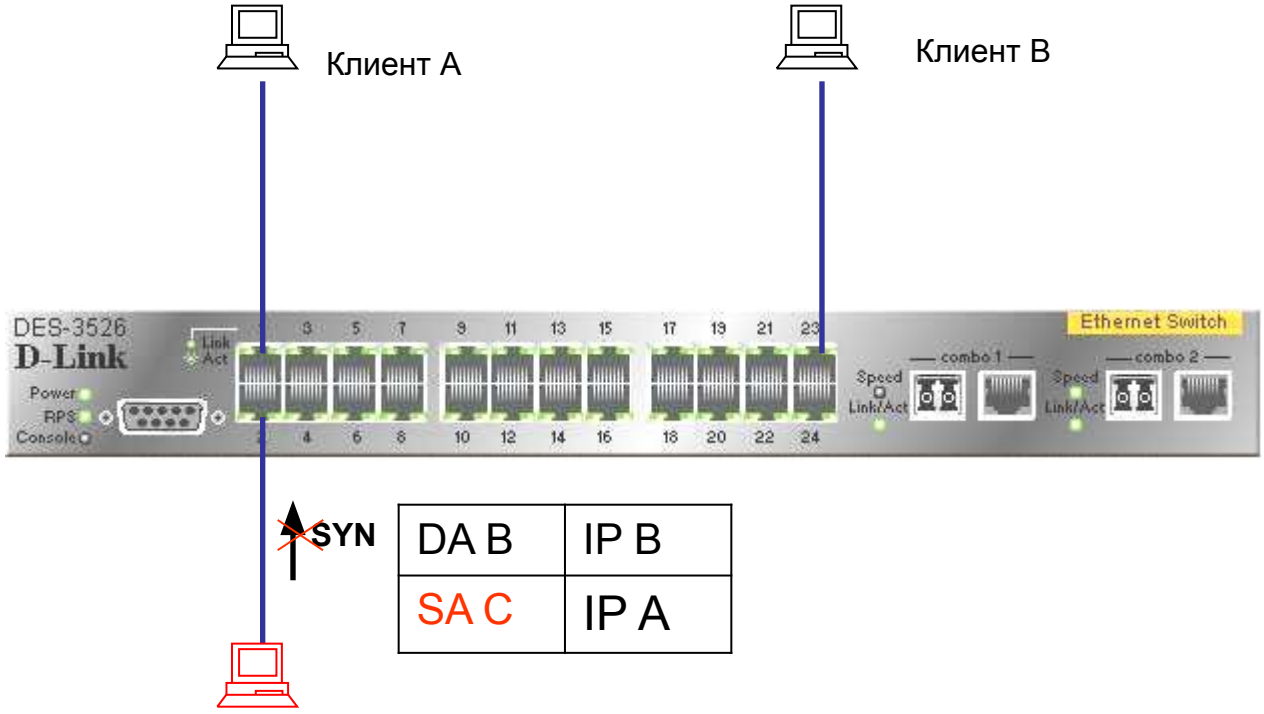
Снифер C (нет в белом листе IP-MAC-Port binding)

Шаг 2: Клиент A хочет установить TCP соединение с клиентом B



Снифер C (нет в белом листе
IP-MAC-Port binding)

Шаг 3: Т.к. С не в белом листе, DES-3526 блокирует пакет, поэтому, соединение не сможет быть установлено



Снифер С (нет в белом листе IP-MAC-Port binding)

D-Link
Building Networks for People

Комментарии по поводу D-Link IP-MAC-Port binding & Cisco DHCP Snooping + Dynamic ARP Inspection

- Cisco **DHCP snooping** + **Dynamic ARP** позволяет фильтровать ARP пакеты для источников, не включенных в таблицу IP-MAC-Port table, но не может предпринять никаких действий со статическими IP/MAC пакетами (пример 1), т.к. DHCP snooping контролирует только динамические IP, поэтому, хакер все же сможет установить соединение с любым хостом в сети. Также для того, чтобы клиент мог использовать DHCP, должна быть включена функция **IP Source Guard,** иначе любой трафик будет запрещен.
- Функция D-Link IP-MAC-Port binding в режиме ARP может легко решить ситуацию со статическим IP/MAC, т.к. коммутатор отслеживает широковещательные пакеты ARP и отслеживает соотношения IP-MAC (пример 1). Если MAC адрес не находится в белом листе IP-MAC-Port коммутатора, он будет автоматически занесен в таблицу блокирования на коммутаторе. Вне зависимости от того, какой пакет пошлет хост/снифер после этого (IP, ARP request, ARP reply), он будет заблокирован перманентно.
- В примере 2, при атаке man-in-the-middle, IP-MAC-Port binding в режиме ARP не может обнаружить подмену по пакету unicast ARP reply. Расширенный режим ACL может отфильтровать любой IP пакет, т.к. снифер не находится в белом листе, поэтому соединение не будет установлено.

D-Link
Building Networks for People

Комментарии по поводу D-Link IP-MAC-Port binding & Cisco DHCP Snooping + Dynamic ARP Inspection

- «За» и «против» решения Cisco:
  - «За»: Может отфильтровать любой незарегистрированный ARP пакет
  - «Против»: Сложная настройка, может понадобится модификация существующих настроек DHCP
- «За» и «против» решения D-Link:
  - «За»: Легко настраивать и эффективно фильтровать любое нелегальное соединение
  - «Против»: Не может защитить от отправки первого ARP пакета
- Допущение: В данном примере мы рассматриваем только TCP трафик, т.к. UDP (SNMP, tftp) используется сравнительно редко в реальных приложениях и потому может быть игнорирован.
- Резюме: Несмотря на то, что IP-MAC-Port binding не может блокировать первый пакет, этот механизм все же эффективно предотвращает установку нелегальных соединений, в то время, как для комплексного решения проблемы при помощи оборудования Cisco необходимо настроить 3 функции. Соответственно, можно сделать вывод, какое решение проще и удобнее в использовании.

Советы по настройке IP-MAC-Port binding ACL Mode

- ACL обрабатываются в порядке **сверху вниз** (см. рисунок 1). Когда пакет «соответствует» правилу ACL, он сразу же отбрасывается (если это запрещающее, правило, deny) либо обрабатывается (если это разрешающее правило, permit)
- При использовании IP-MAC-Port binding в режиме ACL автоматически создаются 2 профиля (и правила для них) в первых двух доступных номерах профилей.
  - Любое запрещающее правило после IP-MAC-Port binding становится **ненужным**, поэтому рекомендуется располагать все остальные ACL в более приоритетном порядке.
  - Нельзя включать одновременно функции IP-MAC-Port **ACL mode** и **ZoneDefense.** Т.к. правила привязки IP-MAC-Port создаются первыми, и правила, создаваемые **ZoneDefense** автоматически после этого, могут быть неправильными.

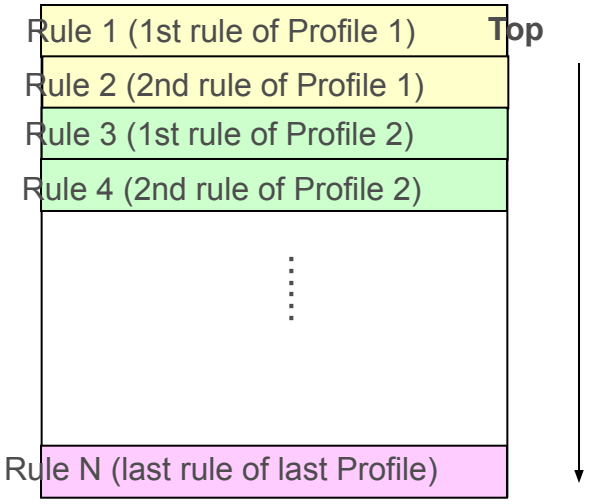
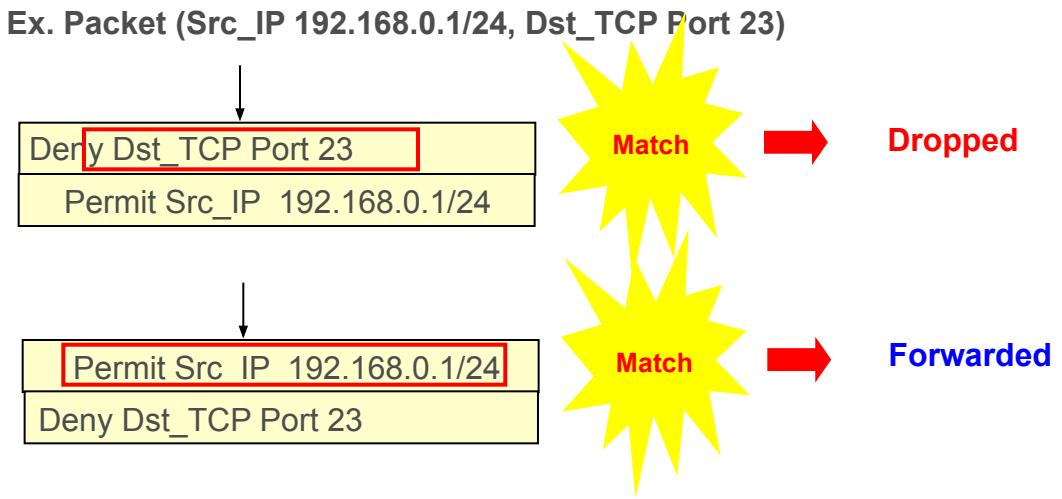


Рисунок 1. Обработка ACL



- Вопрос: Что делать, если необходимо создать еще один профиль, когда режим ACL уже включен (рисунок 2)?
  - Нужно использовать команды “disable address_binding acl_mode” (Рисунок 3) и затем “enable address_binding acl_mode” (Рисунок 4)

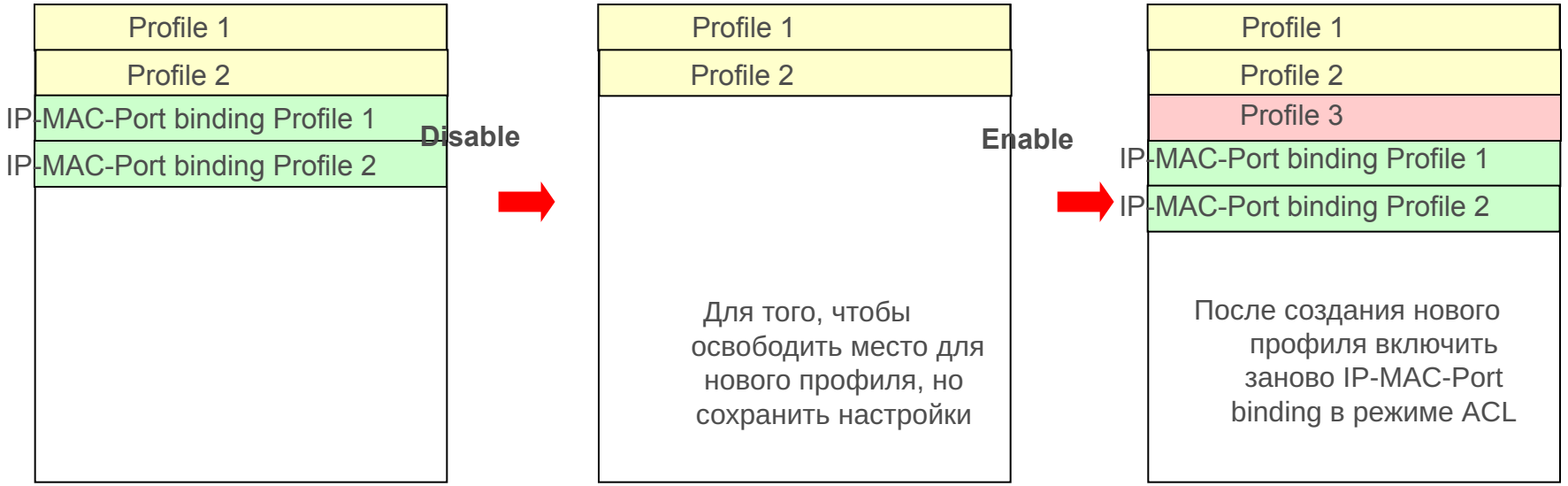


Рисунок 2 Рисунок 3 Рисунок 4

D-Link
Building Networks for People

IP-MAC-Port Binding (пример)

- Задача: Ограничить доступ на портах коммутатора по IP и MAC-адресам одновременно

- Команды для настройки коммутатора:

  1) **create address_binding ip_mac ipaddress 192.168.0.7 mac_address 00-03-25-05-5F-F3 ports 2**

  .

  .

  .

  2) **config address_binding ip_mac ports 2 state enable**

  .

  .

  .

IP-MAC-Port Binding ACL Mode (пример)

- Задача: Ограничить доступ на портах коммутатора по IP и MAC-адресам одновременно

- Команды для настройки коммутатора:

1) **create address_binding ip_mac ipaddress 192.168.0.7 mac_address 00-03-25-05-5F-F3 ports 2 mode acl**

.

.

.

2) **config address_binding ip_mac ports 2 state enable**

.

.

.

3) **enable address_binding acl_mode**

D-Link
Building Networks for People

Управление доступом 802.1x на базе портов/MAC-адресов

Управление доступом 802.1x

- **Проверка подлинности пользователей**

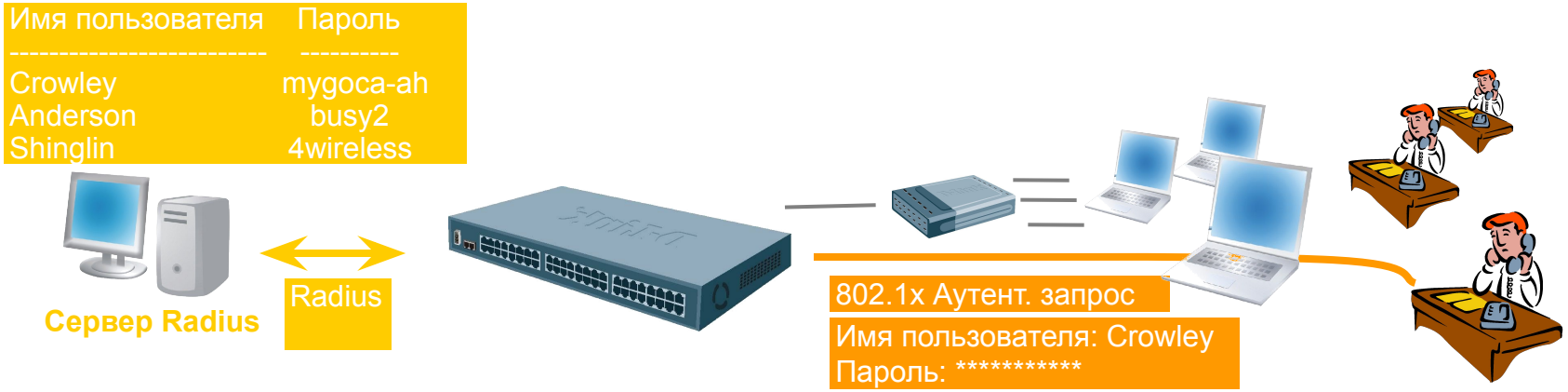
802.1x

Протокол 802.1x является ратифицированным IEEE протоколом аутентификации для LAN следующего поколения. Он позволяет использовать аутентификацию как в проводных, так и беспроводных сегментах сети. Ожидается его применение как стандарта de-facto в сетях обоих типов.

Протокол 802.1x является встроенным средством аутентификации последних версий ОС Microsoft Windows.

Решения на базе D-Link

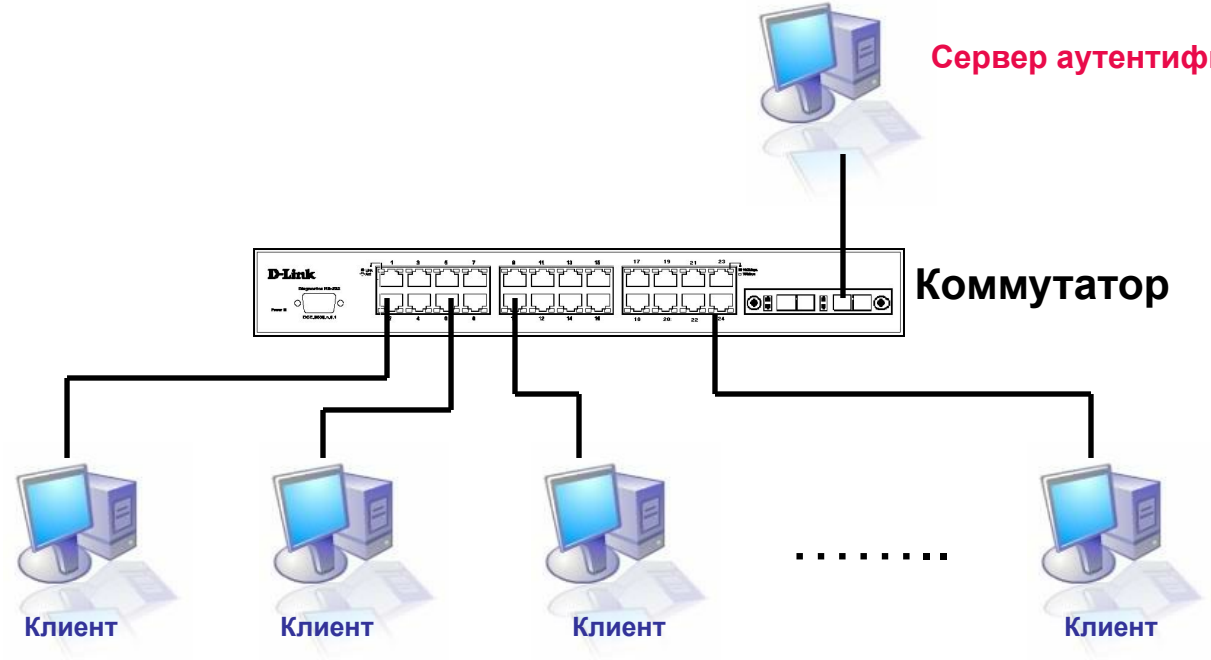
- **802.1x на базе портов:** пользователи должны пройти аутентификацию, перед тем как получить доступ к сети, и коммутаторы разблокируют порты после успешной аутентификации
- **802.1x на базе MAC-адресов:** Коммутатор D-Link может производить аутентификацию по MAC-адресам, что означает возможность каждого порта предоставлять авторизованный доступ многим компьютерам



D-Link
Building Networks for People

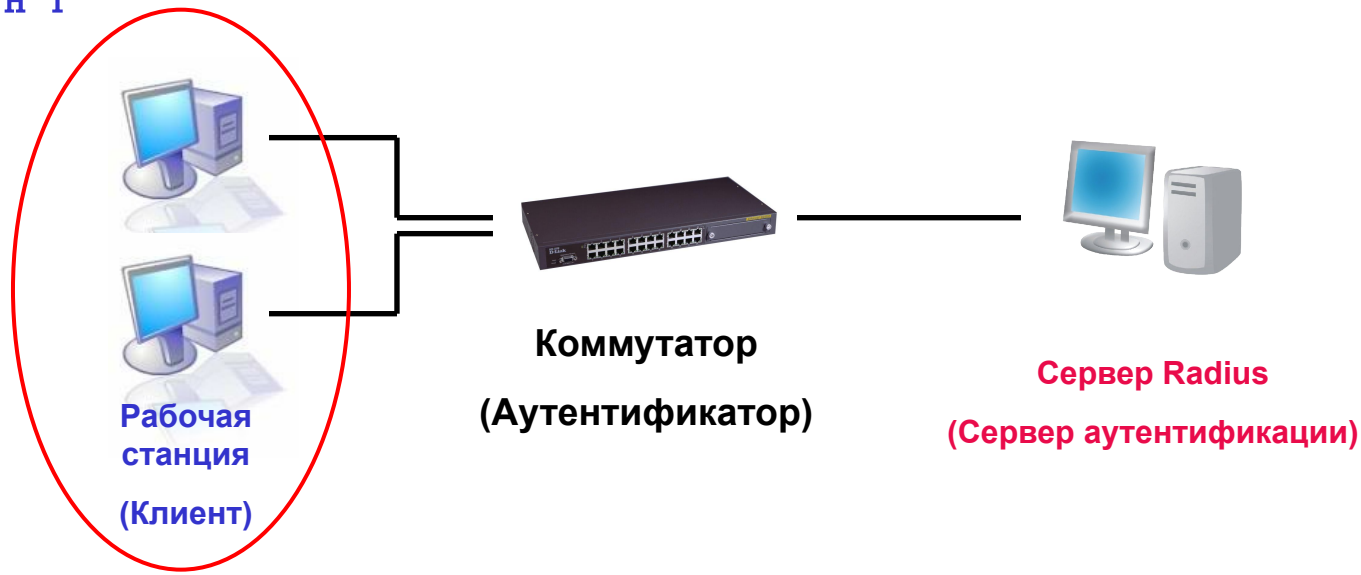
Определение стандарта IEEE 802.1x

802.1x является клиент/серверным протоколом контроля доступа и аутентификации, ограничивающим доступ неавторизованных устройств к локальной сети через публично доступные порты. Сервер аутентификации производит проверку подлинности каждого клиента, подключённого к порту коммутатора, перед тем, как обеспечить доступ к сервисам, предоставляемым сетью или отдельным коммутатором.



Роли устройств 802.1x

- Роли устройств:
  Клиент

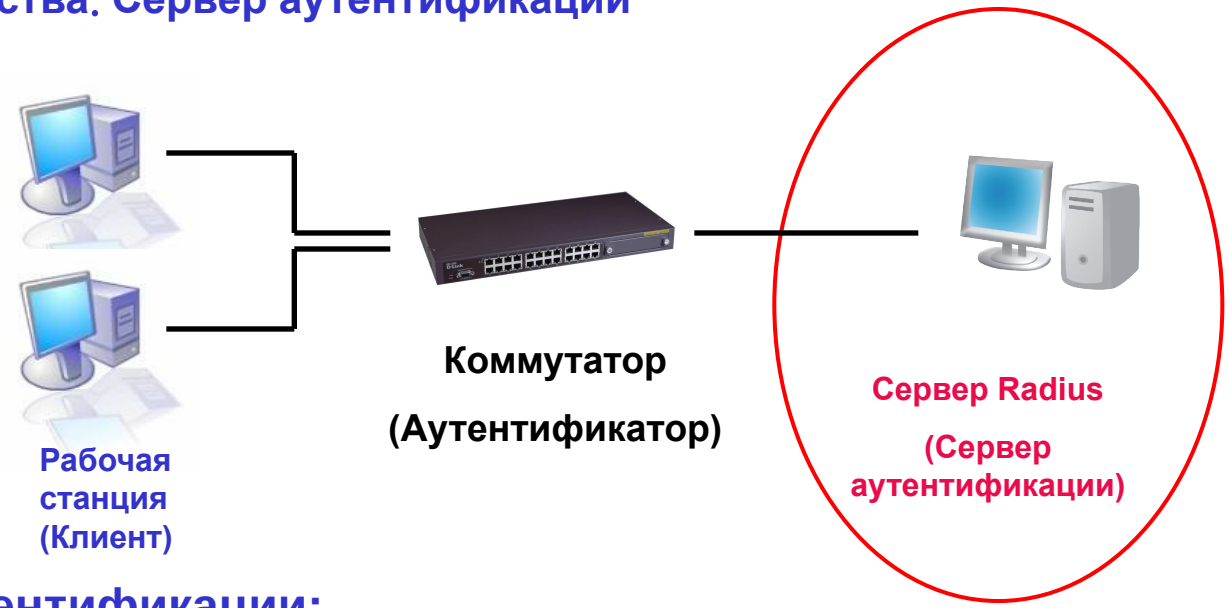


Клиент:

Устройство (Рабочая станция), которая запрашивает доступ к локальной сети и сервисам коммутатора и отвечает на запросы коммутатора. На рабочей станции должно быть запущено 802.1x-совместимое клиентское ПО, например, встроенный клиент 802.1x Microsoft Windows

Роли устройств 802.1x

- **Роль устройства: Сервер аутентификации**



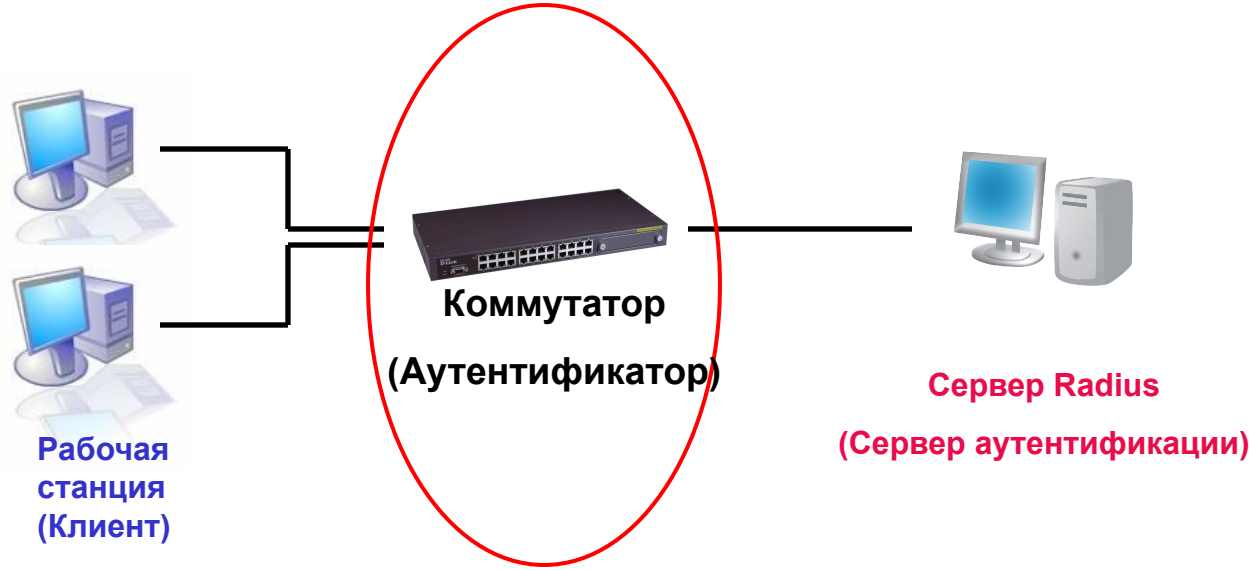
Сервер аутентификации:

Сервер аутентификации проверяет подлинность данных клиента и извещает коммутатор имеет ли клиент права доступа к ресурсам сети и самого коммутатора. *RADIUS* функционирует в режиме клиент/сервер, при котором происходит обмен шифрованными данными аутентификации между *RADIUS*-сервером и одним или многими *RADIUS*-клиентами.

* Remote Authentication Dial-In User Service **(RADIUS)**

Роли устройств 802.1x

- **Роли устройств: Аутентификатор**

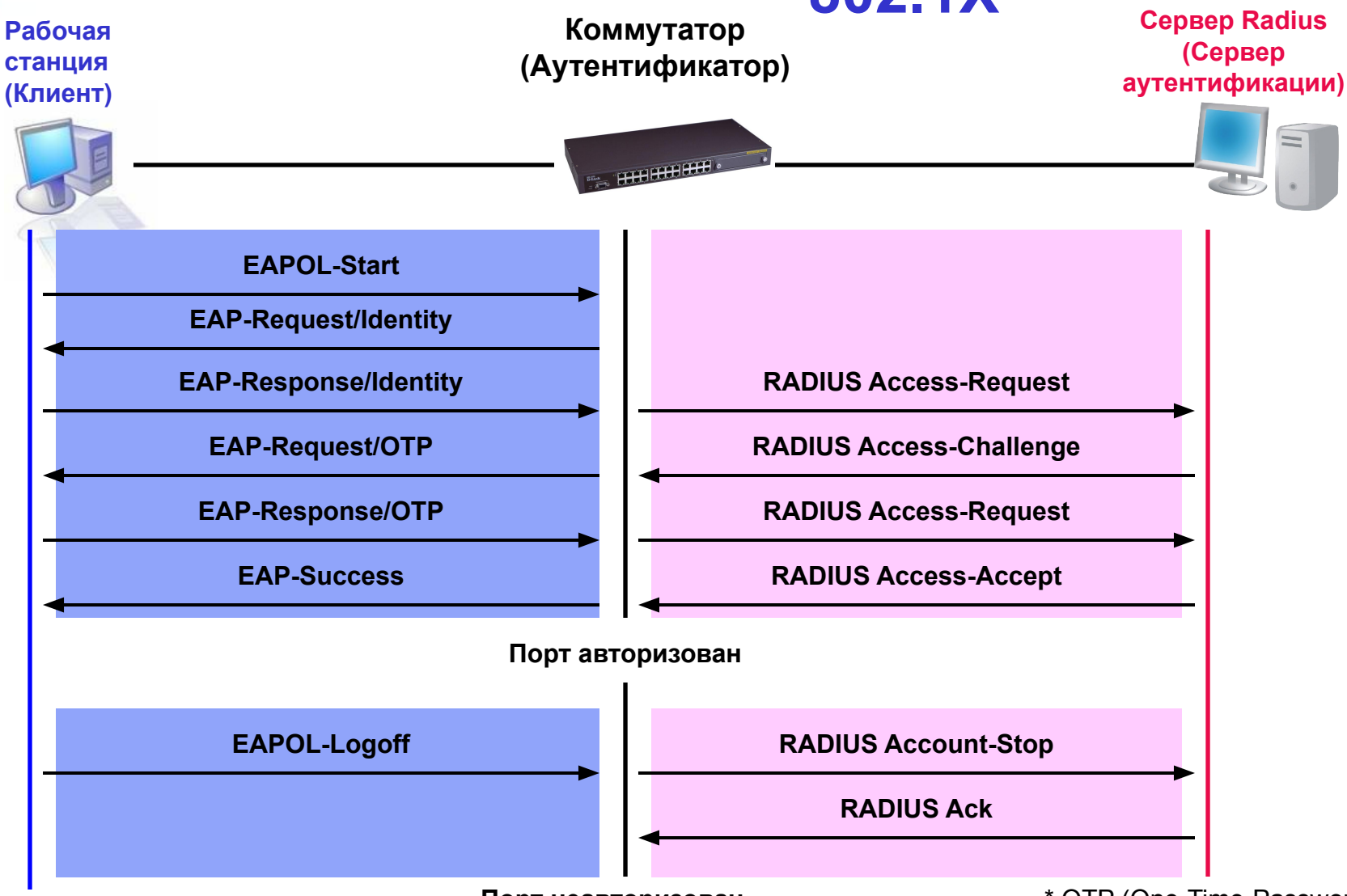


Аутентификатор:

Аутентификатор играет роль посредника (прокси) между Клиентом и Сервером Аутентификации, запрашивает учётные данные у Клиента, пересылает их на Сервер Аутентификации и перенаправляет ответ обратно Клиенту.

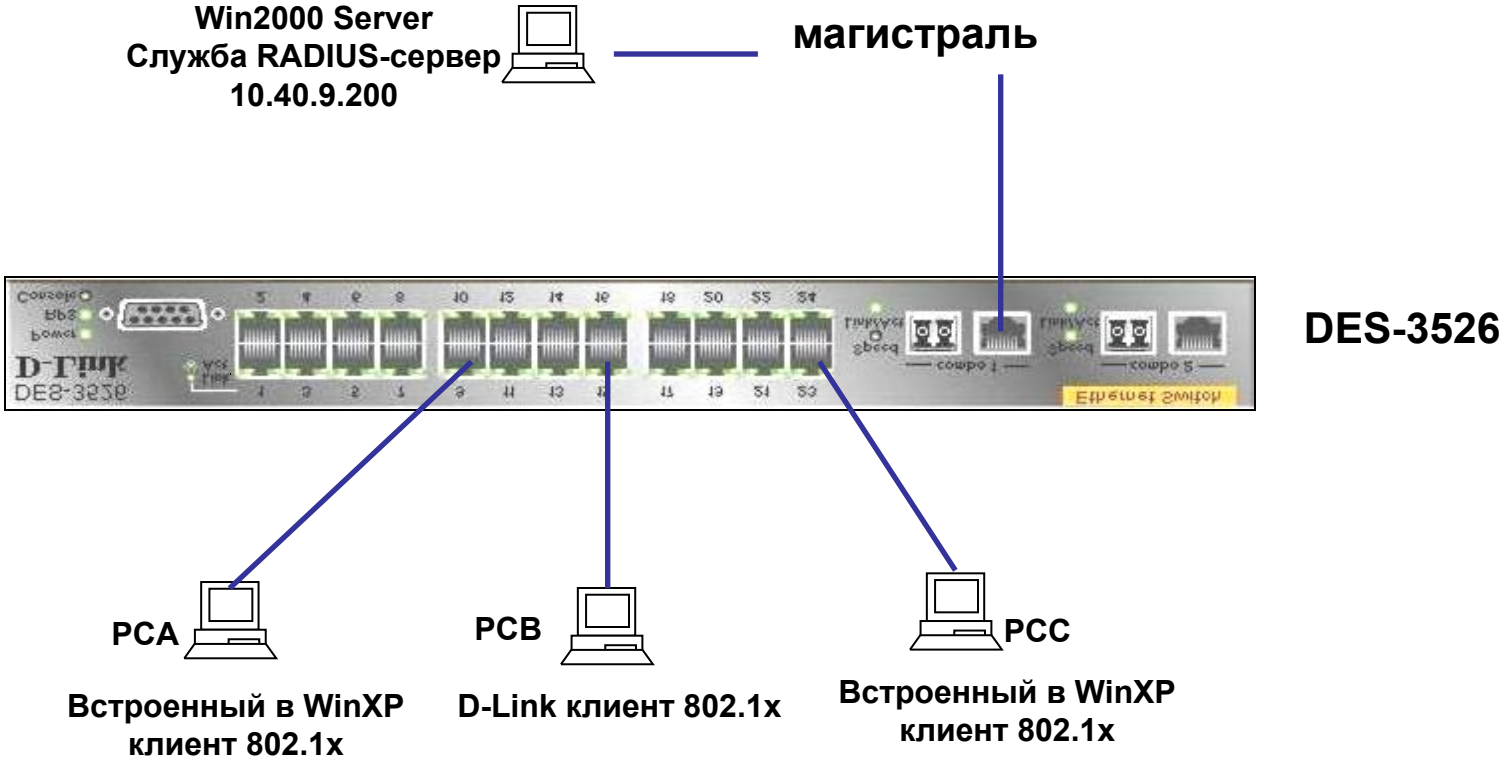
D-Link
Building Networks for People

Процесс аутентификации 802.1X



* OTP (One-Time-Password)

802.1x на основе портов (пример)



Перед прохождением аутентификации с использованием клиентского ПО 802.1x с вводом правильных имени пользователя/пароля, порт заблокирован. Порт будет разблокирован успешной аутентификации клиента по протоколу 802.1x

D-Link
Building Networks for People

802.1x на основе портов (пример)

- Рабочая станция: Встроенный клиент 802.1x Windows XP. В противном случае необходимо любое другое клиентское ПО 802.1x.

- Коммутатор:
  1. Включить 802.1x на каждом устройстве
     enable 802.1x
  2. Сконфигурировать клиентские порты. (Примечание: На порту связи с вышестоящим коммутатором (Uplink) не следует задавать режим «аутентификатор»).
     config 802.1x capability ports 1-24 authenticator
  3. Настроить параметры сервера Radius
     config radius add 1 10.40.9.200 key 04009 default

- Radius: Служба Radius-сервер Windows NT/Windows 2000 Server или сервер RADIUS стороннего разработчика.

D-Link
Building Networks for People

802.1x
Сравнение реализаций на базе портов и MAC-адресов

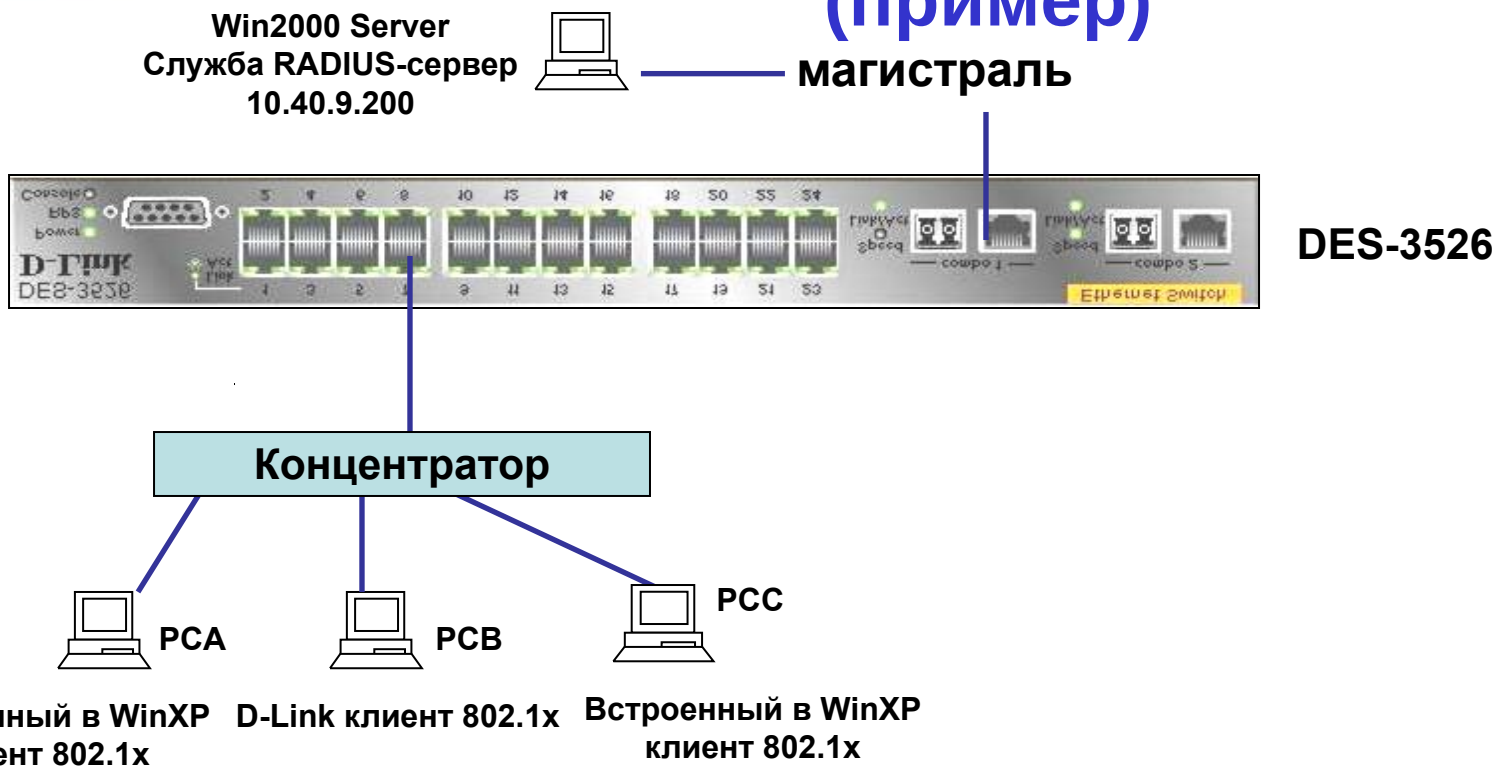
802.1x на базе портов

С того момента как клиент авторизован на определённом порту, любой другой клиент, подключённый к этому же порту может получить доступ к сети.

802.1x на базе MAC-адресов

В данном случае проверяются не только учётные данные, но и достигнуто ли максимальное количество разрешённых на порте MAC-адресов. Если достигнуто, то новый MAC-адрес блокируется.

802.1x на базе MAC-адресов (пример)



Каждый клиент должен иметь возможность ввести правильные учётные данные (имя пользователя/пароль) для прохождения аутентификации и получения доступа к сети.

Замечание: Концентратор может быть заменён на коммутатор, поддерживающий передачу пакетов 802.1x. В противном случае пакет 802.1x (MAC-адрес назначения 0180c2000003, принадлежащий к зарезервированному IEEE диапазону 0180c2000001~0F) будет отброшен коммутатором и не достигнет DES-3526.

D-Link
Building Networks for People

802.1x на базе MAC-адресов (пример)

- Рабочая станция: Встроенный клиент 802.1x Windows XP. В противном случае необходимо любое другое клиентское ПО 802.1x.

- Коммутатор:

1. Включить 802.1x на каждом устройстве и переключиться в режим 802.1x на базе MAC-адресов.
   enable 802.1x
   config 802.1x auth_mode mac_based

2. Сконфигурировать клиентские порты.
   config 802.1x capability ports 1-24 authenticator
3. Настроить параметры сервера Radius
   config radius add 1 10.40.9.200 key 04009 default

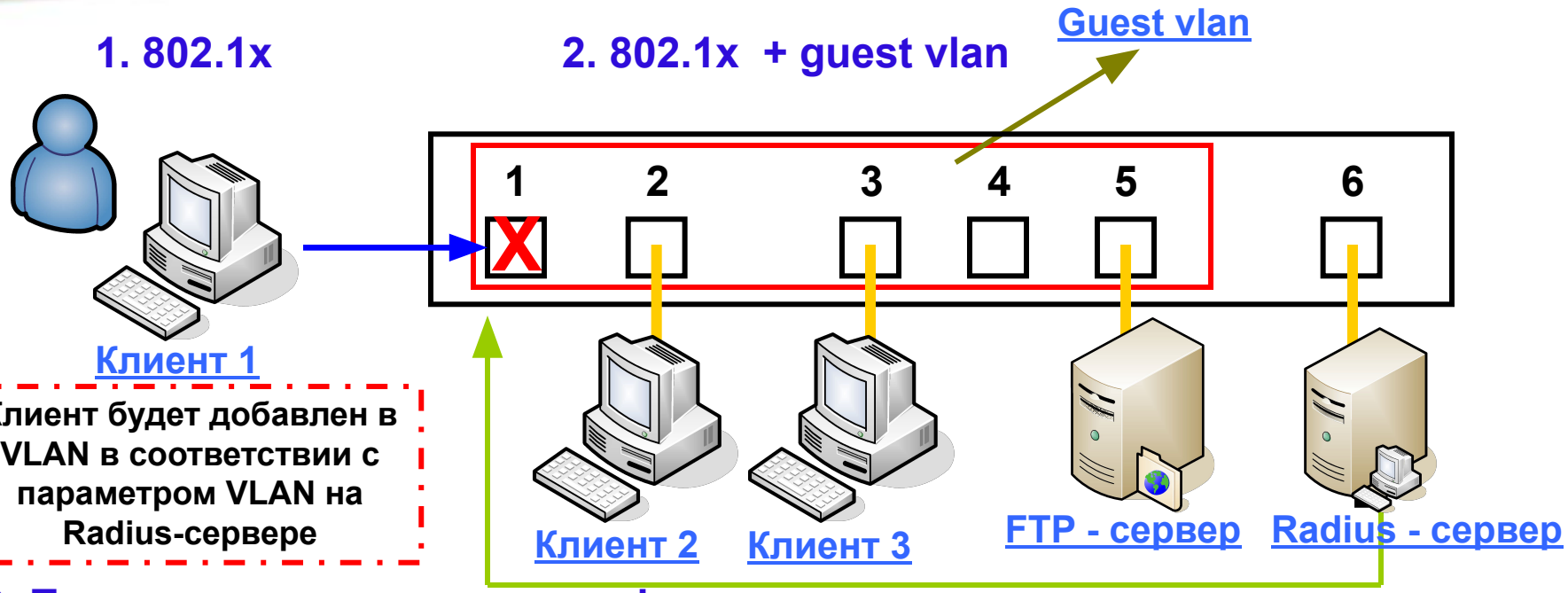
- Radius: Служба Radius-сервер Windows NT/Windows 2000 Server или сервер RADIUS стороннего разработчика.

D-Link
Building Networks for People

802.1x Guest VLAN

D-Link
Building Networks for People

Что такое 802.1x Guest VLAN



3. После того как порт аутентифицирован

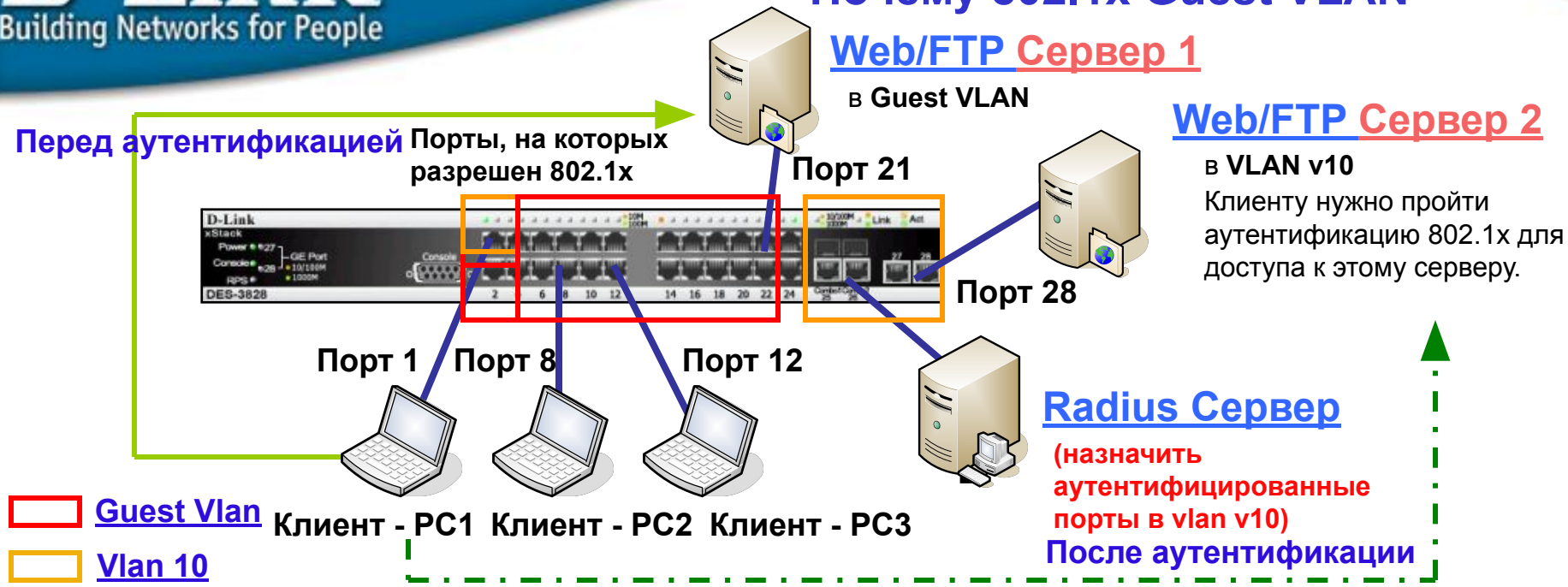
1. **Члены Guest VLAN могут иметь доступ друг к другу даже если они не прошли 802.1x аутентификацию.**

2. **Член Guest VLAN может быть переведён в Target VLAN (VLAN назначения) в соответствии с параметрами, указанными на RADIUS-сервере, после прохождения 802.1x аутентификации.**

(Guest VLAN поддерживает только 802.1x на базе портов, но не базе MAC-адресов)

D-Link
Building Networks for People

Почему 802.1x Guest VLAN

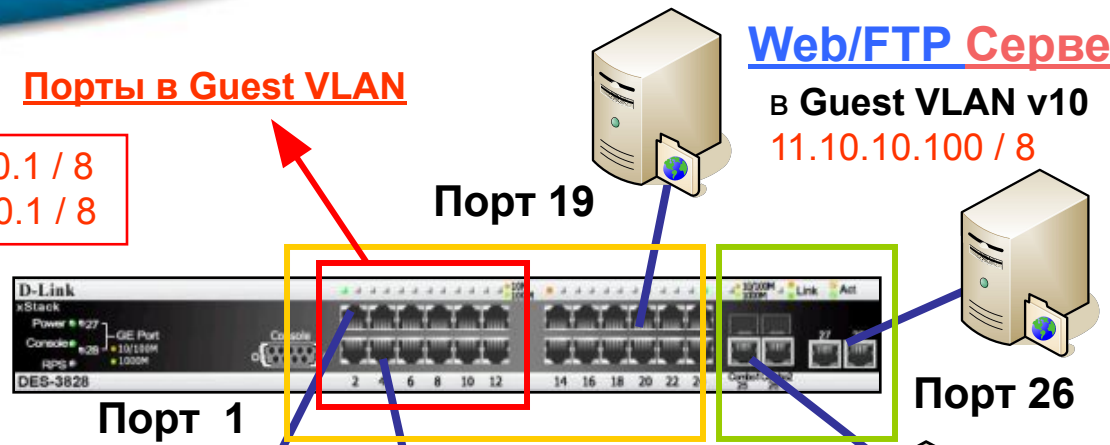


802.1x Guest VLAN может предоставлять клиентам ряд ограниченных сервисов до прохождения процесса 802.1x аутентификации. Например клиент может скачать и установить необходимое ПО 802.1x.

На рисунке, до того как клиент аутентифицирован, его PC может иметь доступ к публичному Web / FTP серверу в Guest VLAN для получения необходимой информации.

После того как клиент аутентифицирован в сети, клиентский порт добавляется в соответствующий VLAN и может получить доступ ко всем сервисам в этом VLAN.

Пример 802.1x Guest VLAN



1. Две VLAN: v10 и v20
   - v10 статические порты: 1-24
   - v20 статические порты: 25-28
2. Guest VLAN VID=10
3. Порты 1-12 добавлены в Guest VLAN
4. Добавить порт в обе VLAN

Пример 802.1x Guest VLAN: настройки

1. Конфигурация DES3828

Создайте VLAN v10 и v20
config vlan default delete 1-28
create vlan v20 tag 20
config vlan v20 add untagged 25-28
config ipif System ipaddress 10.10.10.1/8 vlan v20
create vlan v10 tag 10
config vlan v10 add untagged 1-24
create ipif p10 11.10.10.1/8 v10
Включите 802.1x и Guest VLAN
enable 802.1x
create 802.1x guest_vlan v10
config 802.1x guest_vlan ports 1-12 state enable
Сделайте коммутатор посредником в процессе 802.1x
config 802.1x capability ports 1-12 authenticator

config radius add 1 10.10.10.101 key 123456 default

1. Создаётся 2 VLAN V10 и V20
2. Включается 802.1x и Guest VLAN
3. Коммутатор назначается посредником в процессе 802.1x на портах с 1 по 12
4. Задаётся Radius сервер

2. Конфигурация PC клиента:

Запустите ПО 802.1x D-Link.

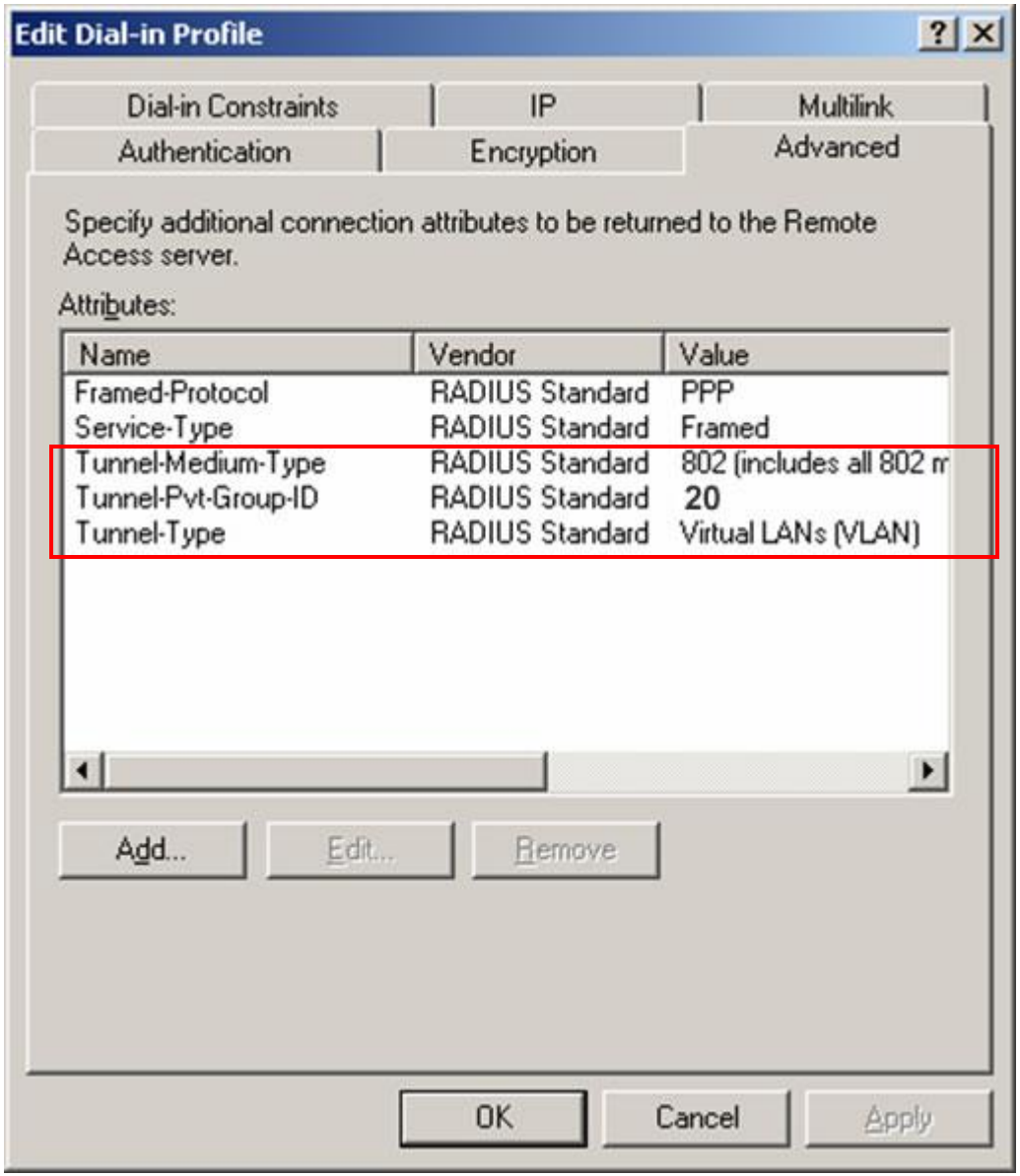
3. Конфигурация RADIUS-сервера:

Создайте имя пользователя и задайте пароль. Задайте следующие атрибуты для пользователя:
Tunnel-Medium-Type (65) = 802
Tunnel-Pvt-Group-ID (81) = 20 **VID**
Tunnel-Type (64) = VLAN

D-Link
Building Networks for People

Настройки Radius-сервера Windows 2003

Задайте следующие параметры RADIUS для пользователя:
Tunnel-Medium-Type (65) = 802
Tunnel-Pvt-Group-ID (81) = **20** **VID**
Tunnel-Type (64) = VLAN



Пример 802.1x Guest VLAN: настройки

Перед тем, как порт 1 DES-3828 пройдёт процесс аутентификации 802.1x

Команда: **show vlan**

```
VID           : 1        VLAN Name     : default
VLAN TYPE     : static   Advertisement : Enabled
Member ports  :
Static ports  :
Current Untagged ports :
Static Untagged ports  :
Forbidden ports :

VID           : 10       VLAN Name     : v10
VLAN TYPE     : static   Advertisement : Disabled
Member ports  : 1-24
Static ports  : 1-24
Current Untagged ports : 1-24
Static Untagged ports  : 1-24
Forbidden ports :

VID           : 20       VLAN Name     : v20
VLAN TYPE     : static   Advertisement : Disabled
Member ports  : 25-28
Static ports  : 25-28
Current Untagged ports : 25-28
Static Untagged ports  : 25-28
Forbidden ports :
```

Команда: **show 802.1x auth_state**

Port	Auth PAE State	Backend State	Port Status
1	**Connecting**	**Idle**	**Unauthorized**
2	Disconnected	Idle	Unauthorized
3	Disconnected	Idle	Unauthorized
4	**Connecting**	**Idle**	**Unauthorized**
5	Disconnected	Idle	Unauthorized
6	Disconnected	Idle	Unauthorized
7	Disconnected	Idle	Unauthorized
8	Disconnected	Idle	Unauthorized
9	Disconnected	Idle	Unauthorized
10	Disconnected	Idle	Unauthorized
11	Disconnected	Idle	Unauthorized
12	Disconnected	Idle	Unauthorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized

На этом этапе, порты 1-24 DES3828 port 1-24 могут передавать данные друг другу, например на Web/FTP Сервер 1 на порту 19 в Guest VLAN, но не имеют доступа к FTP/Web Серверу 2 на порту 26 в VLAN20.

Пример 802.1x Guest VLAN: настройки

После прохождения портом 1 DES-3828 процесса аутентификации 802.1x

Команда: **show vlan**

```
VID           : 1        VLAN Name     : default
VLAN TYPE     : static   Advertisement : Enabled
Member ports  :
Static ports  :
Current Untagged ports :
Static Untagged ports  :
Forbidden ports :

VID           : 10       VLAN Name     : v10
VLAN TYPE     : static   Advertisement : Disabled
Member ports  : 2-24
Static ports  : 2-24
Current Untagged ports : 2-24
Static Untagged ports  : 2-24
Forbidden ports :

VID           : 20       VLAN Na
VLAN TYPE     : static   Advertisement : Disabled
Member ports  : 1, 25-28
Static ports  : 1, 25-28
Current Untagged ports : 1, 25-28
Static Untagged ports  : 1, 25-28
Forbidden ports :
```

Порт 1 прошёл аутентификацию, т.о. он был назначен в v20, так как на Radius-сервере указан параметр vid=20

Команда: **show 802.1x auth_state**

Port	Auth PAE State	Backend State	Port Status
1	**Authenticated**	**Idle**	**Authorized**
2	Disconnected	Idle	Unauthorized
3	Disconnected	Idle	Unauthorized
4	**Connecting**	**Idle**	**Unauthorized**
5	Disconnected	Idle	Unauthorized
6	Disconnected	Idle	Unauthorized
7	Disconnected	Idle	Unauthorized
8	Disconnected	Idle	Unauthorized
9	Disconnected	Idle	Unauthorized
10	Disconnected	Idle	Unauthorized
11	Disconnected	Idle	Unauthorized
12	Disconnected	Idle	Unauthorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized

PC на порту 1 имеет доступ к FTP/Web Серверу 2 в VLAN20, так как этот порт стал членом VLAN20.

D-Link
Building Networks for People

802.1x Guest VLAN: результаты тестов

Результаты тестов:

1. **Перед** тем как PC1 пройдёт процесс 802.1x аутентификации, PC1 имеет доступ к PC2 и FTP/WEB Серверу 1, находящимся в Guest VLAN.

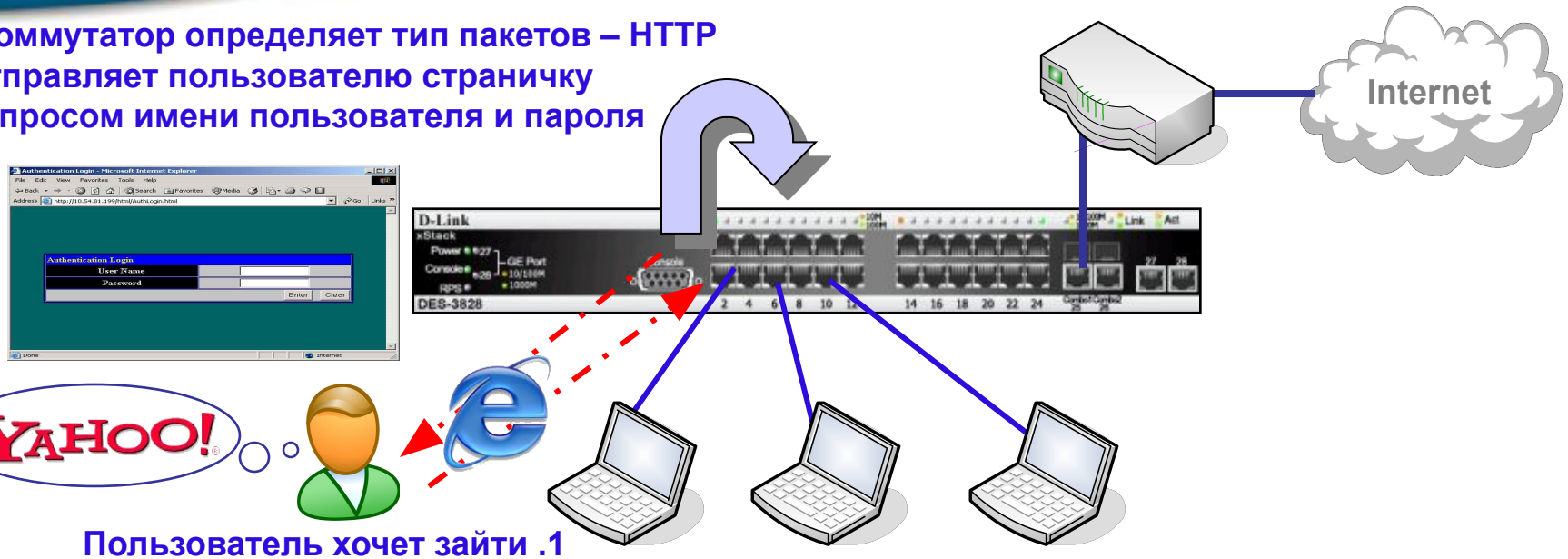
2. **После** того как PC1 пройдёт процесс аутентификации, PC1 имеет доступ к FTP/WEB Серверу 2, потому что PC1 переведён в VLAN20 из Guest VLAN VID 10 Radius-сервером. (PC 1 не имеет доступа к PC2 и FTP/WEB Серверу 1)

D-Link
Building Networks for People

Web-Based Authentication – аутентификация на базе WEB (WAC)

Почему аутентификация на основе WEB

2. Коммутатор определяет тип пакетов – HTTP и отправляет пользователю страничку с запросом имени пользователя и пароля



Пользователь хочет зайти .1 на WEB-сайт Yahoo

Клиент - PC1 **Клиент - PC2** **Клиент - PC3**

Перед прохождением процесса аутентификации коммутатор блокирует все HTTP-пакеты

Если нужна аутентификация по имени пользователя/паролю, и пользователь не хочет использовать 802.1x аутентификацию (например, клиентское ПО 802.1x не предустановлено на PC). Есть ли другой способ соблюсти это требование?

Ответ: Web-Based Authentication (WAC).

Аутентификация на основе WEB

Web-Based Authentication (WAC) функция, специально разработанная для аутентификации пользователя при попытке доступа к сети через коммутатор. Это **альтернативный вариант аутентификации на основе портов** по отношению к IEEE802.1X.

Процесс аутентификации использует **протокол HTTP**. Когда пользователи хотят открыть WEB-страницу (например, http://www.google.com) посредством WEB-браузера (например, IE) и коммутатор обнаруживает HTTP-пакеты и то, что порт не аутентифицирован, тогда браузер отобразит окно с запросом имени пользователя/пароля. Если пользователь вводит правильные данные и проходит процесс аутентификации, это означает, что порт аутентифицирован, и пользователь имеет доступ к сети.

Роль коммутатора

Коммутатор сам может выступать в роли **сервера аутентификации** и производить аутентификацию на основе локальной базы данных пользователей, или в роли **RADIUS - клиента** и осуществлять процесс аутентификации совместно с удалённым RADIUS - сервером.

1. **Сервер аутентификации** – для небольших сетей рабочих групп

2. **RADIUS - клиент** – для крупных корпоративных сетей

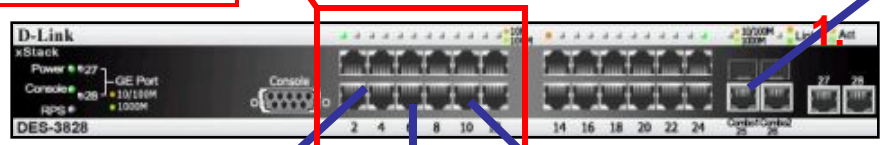
D-Link
Building Networks for People

Аутентификация на основе WEB: пример
- с использованием локальной базы данных пользователей

2. Порты с включенной аутентификацией (порты 1-12)

DI-624 (10.10.10.10)
DHCP IP Pool
10.10.10.50 – 10.10.10.100

Web Сервер
IP: 10.10.10.101



10.10.10.1

1. На какую WEB-страницу Вы хотите перенаправить запрос?

Пользователь	Пароль
James	123
Will	456
….	…..

Клиент - PC1
10.10.10.11

Клиент - PC2
10.10.10.12

Клиент - PC3
10.10.10.13

3. Локальная база данных пользователей (создать пользователей)

Порты 1-12 сконфигурированы как порты с включенной аутентификацией. Каждый PC, подключённый к этим портам, должен пройти процесс аутентификации по имени пользователя/паролю. После этого, они получают доступ к сети. База данных имя пользователя/пароль/VLAN в этом примере хранится на коммутаторе. Т.о., в этом примере нет RADIUS-сервера.

Примечание: В текущей реализации, максимальной количество записей в локальной базе данных равно числу портов коммутатора. Например, DES-3828 поддерживает 28 записей (т.е. максимум 28 локальных пользователей).

D-Link
Building Networks for People

Аутентификация на основе WEB: пример
- с использованием локальной базы данных пользователей

Конфигурация коммутатора:

1. # Задайте WEB-страницу для перенаправления трафика. Пользователь может использовать свою собственную WEB-страницу для перенаправления.

config wac default_redirpath www.dlink.com (10.10.10.101)

2. # Сконфигурируйте порты как порты с WAC-аутентификацией.

config wac vlan default method local ports 1-12 state enable
enable wac

3. # Создайте пользователя в локальной базе данных имя пользователя/пароль/VLAN.
Например, имя пользователя/пароль=u1/u1
и порт будет добавлен в VLAN default после прохождения процесса аутентификации.

create wac user u1 vlan default

Клиент - PC:
Нет необходимости в каком либо специальном ПО. Откройте WEB-браузер (например, IE) и пройдите процесс аутентификации.

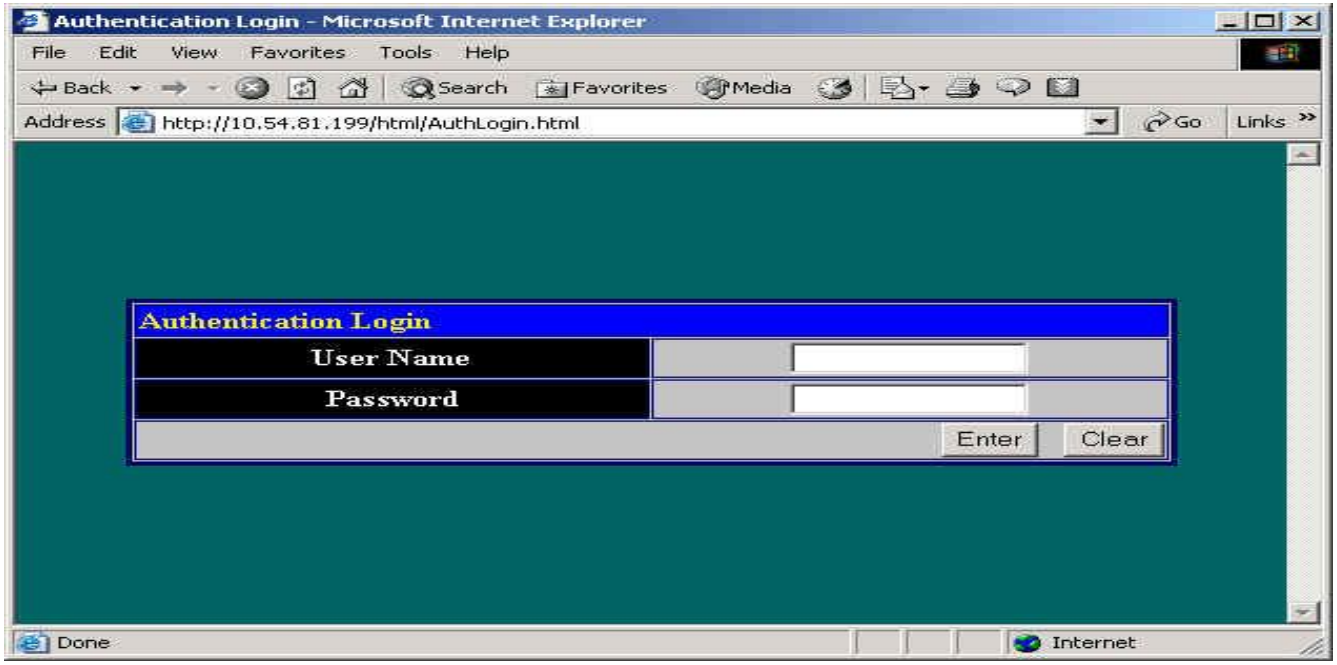
D-Link
Building Networks for People

Аутентификация на основе WEB: пример

- с использованием локальной базы данных пользователей

1. Когда Вы заходите на наш WEB-сайт (10.10.10.101) Результат аутентификации:

2. Откроется окно с запросом имени пользователя и пароля

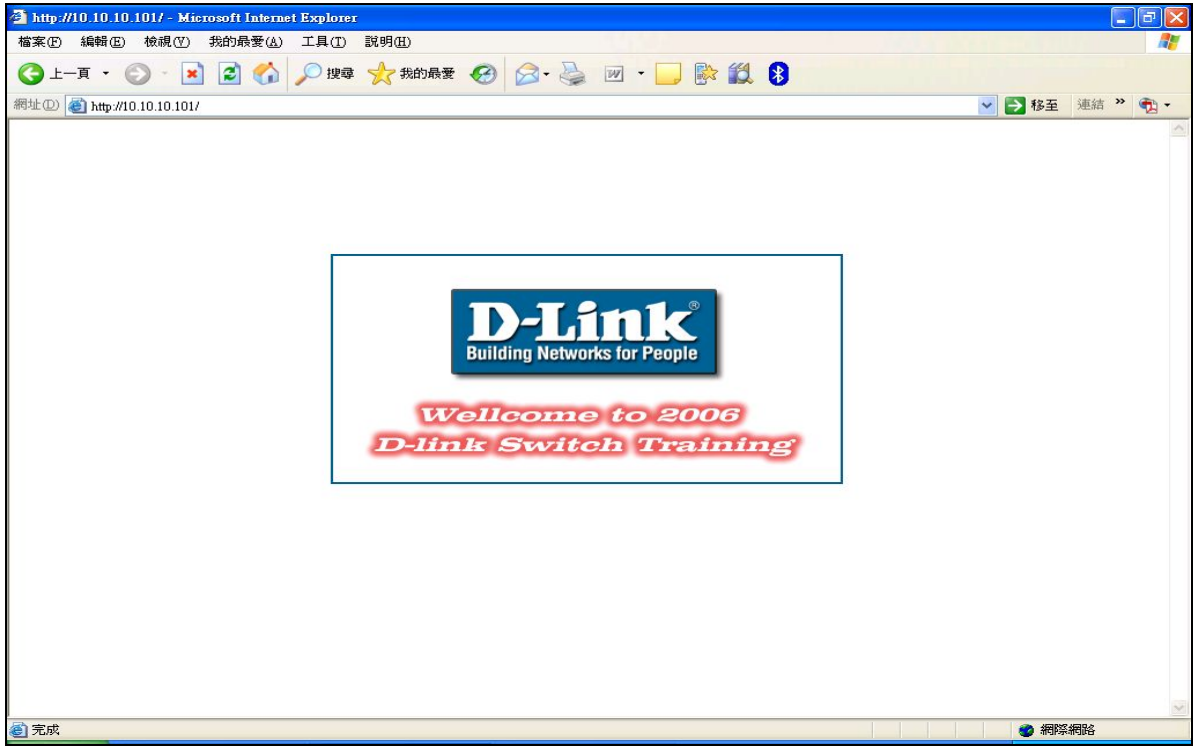


Аутентификация на основе WEB: пример

- с использованием локальной базы данных пользователей

Результаты WEB аутентификации:

3. Когда пользователь вводит корректные учётные данные и проходит аутентификацию, будет выведено сообщение об успешном входе в сеть “successful logged in”, и затем пользователь будет перенаправлен на 10.10.10.101, как указано в конфигурации. Пользователь может затем получить доступ к другим ресурсам сети.



D-Link
Building Networks for People

Аутентификация на основе WEB: пример
- с использованием локальной базы данных пользователей

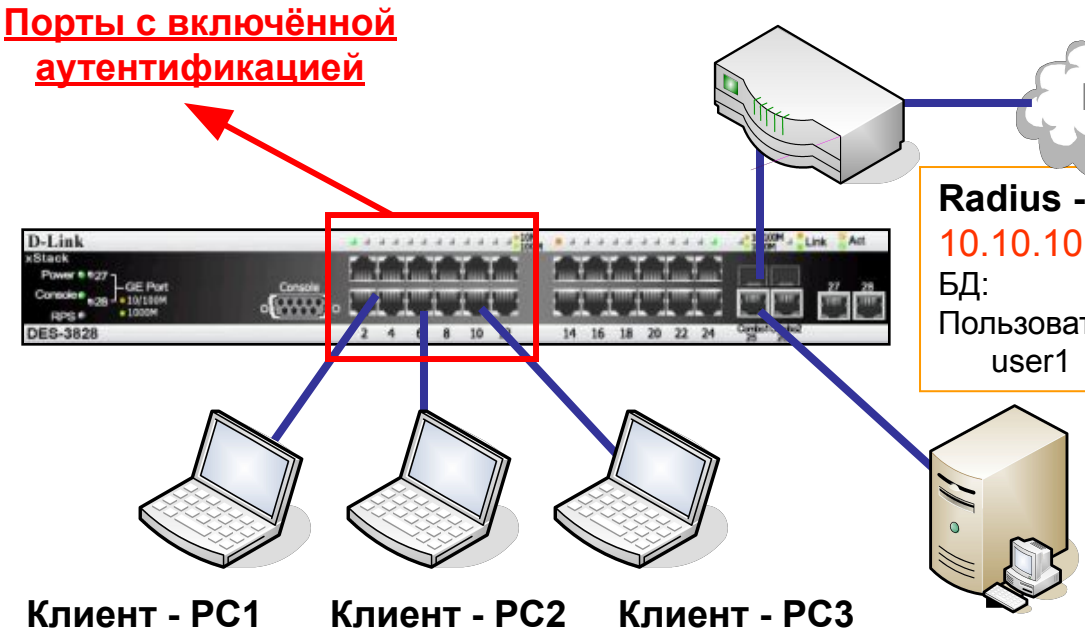
Результаты WEB аутентификации:

4. И затем пользователь может получить доступ к любому ресурсу сети, не обязательно WEB - серверу. Из CLI, Вы может посмотреть статус любого WAC - порта.

```
DES-3800:4# show wac ports all
Command: show wac ports all
Port  State    Username          IP address       Auth status     Assigned
VLAN
----  -------  ----------------  ---------------  --------------
-------------
1     Enable   u1                10.54.81.1       Authenticated   1
2     Enable                     0.0.0.0          Unauth          1
3     Enable                     0.0.0.0          Unauth          1
4     Enable                     0.0.0.0          Unauth          1

....
```

Аутентификация на основе WEB: пример
- с использованием внешнего RADIUS - сервера



Если количество уникальных пользователей превышает размеры локальной БД или в сети уже есть работающий RADIUS - сервер, функция WAC также может использовать записи имя пользователя/пароль/VLAN на RADIUS - сервере для осуществления аутентификации пользователей.

В некоторых крупных корпоративных сетях, Radius - сервер может быть использован как решения для построения масштабируемых сетей.

D-Link
Building Networks for People

Аутентификация на основе WEB: пример
- с использованием внешнего RADIUS - сервера

Конфигурация коммутатора:

1. # Задайте WEB-страницу для перенаправления трафика.

```
config wac default_redirpath www.dlink.com
```

2. # Задайте удалённый RADIUS – сервер.

```
config radius add 1 10.10.10.101 key 123456 default
```

3. # Сконфигурируйте порты как порты с WAC-аутентификацией.

```
config wac vlan default method radius ports 1-12 state enable
enable wac
```

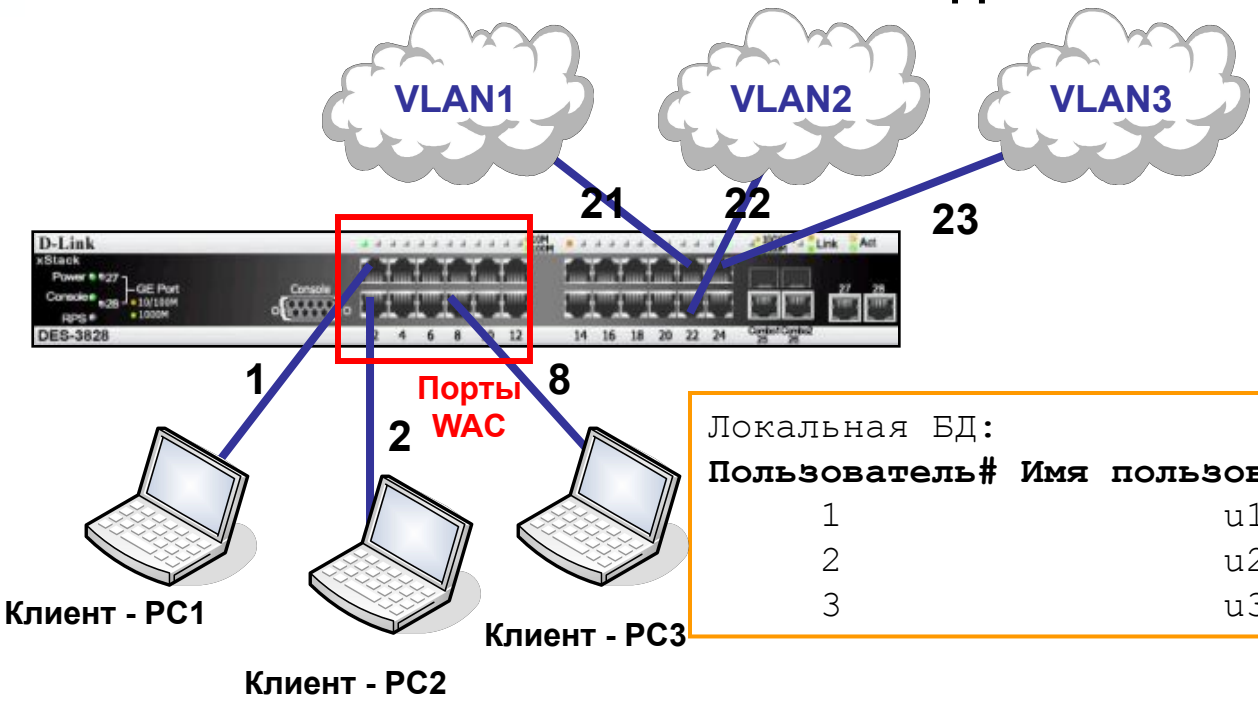
Клиент - PC:

Нет необходимости в каком либо специальном ПО. Откройте WEB-браузер (например, IE) и пройдите процесс аутентификации.

Результаты WEB аутентификации:

те же самые, что в предыдущем примере

Пример настройки WAC - Присвоить VLAN исходя из имени пользователя



Локальная БД:

Пользователь#	Имя пользователя/Пароль/VLAN
1	u1/u1/default
2	u2/u2/v2
3	u3/u3/v3

Также как и с функцией Guest VLAN, порт с включённой функцией WAC также может быть добавлен в определённый VLAN в соответствии с именем пользователя в локальной базе данных на коммутаторе. В этом примере, когда пользователь “u2” аутентифицируется в сети, порт будет добавлен в VLAN v2 и он соответственно получит доступ к VLAN2. **Эта функция может быть использована для предоставления разного уровня обслуживания разным пользователям.**

D-Link
Building Networks for People

Пример настройки WAC - Присвоить VLAN исходя из имени пользователя

Конфигурация коммутатора

```
## Создайте VLAN – ы, причём каждый VLAN должен иметь один Uplink - порт (порты 21, 22, 23).
config vlan default delete 21-23
config vlan default add untagged 21
create vlan v2 tag 2
config vlan v2 add untagged 22
create vlan v3 tag 3
config vlan v3 add untagged 23

 # Задайте WEB-страницу для перенаправления трафика.
config wac default_redirpath www.dlink.com

## Конфигурация WAC основана на локальной базе данных.
## Разные пользователи добавляются в разные VLAN-ы.
config wac method local vlan default ports 1-8 state enable
create wac user u1 vlan default
create wac user u2 vlan v2
create wac user u3 vlan v3
enable wac
```

Пример настройки WAC - Присвоить VLAN исходя из имени пользователя

Перед тем как пользователи будут аутентифицированы, порты добавлены в следующие VLAN-ы:

DES-3800:4# **show vlan**
Command: show vlan

VID : 1 VLAN Name : default
VLAN TYPE : static Advertisement : Enabled
Member ports : 1-21,24-28 **Порты 1, 2 и 8, к которым подключены PC, находятся в VLAN default**
Static ports : 1-21,24-28
Current Untagged ports : 1-21,24-28
Static Untagged ports : 1-21,24-28
Forbidden ports :

VID : 2 VLAN Name : v2
VLAN TYPE : static Advertisement : Disabled
Member ports : 22
Static ports : 22
Current Untagged ports : 22 **Только порт 22 находится в VLAN v2**
Static Untagged ports : 22
Forbidden ports :

VID : 3 VLAN Name : v3
VLAN TYPE : static Advertisement : Enabled
Member ports : 23
Static ports : 23
Current Untagged ports : 23 **Только порт 23 находится в VLAN v3**
Static Untagged ports : 23
Forbidden ports :

Total Entries : 3

D-Link
Building Networks for People

Пример настройки WAC - Присвоить VLAN исходя из имени пользователя

Перед тем, как пользователи будут аутентифицированы, статус портов WAC следующий:

DES-3800:4# **show wac ports all**
Command: show wac ports all

Port	State	Username	IP address	Auth status	Assigned VLAN
1	**Enable**		**0.0.0.0**	**Unauth**	**1**
2	**Enable**		**0.0.0.0**	**Unauth**	**1**
3	Enable		0.0.0.0	Unauth	1
4	Enable		0.0.0.0	Unauth	1
5	Enable		0.0.0.0	Unauth	1
6	Enable		0.0.0.0	Unauth	1
7	Enable		0.0.0.0	Unauth	1
8	**Enable**		**0.0.0.0**	**Unauth**	**1**
9	Disable		0.0.0.0	Unauth	1
10	Disable		0.0.0.0	Unauth	1
11	Disable		0.0.0.0	Unauth	1
12	Disable		0.0.0.0	Unauth	1

. . .

D-Link
Building Networks for People

Пример настройки WAC - Присвоить VLAN исходя из имени пользователя

После того, как пользователи аутентифицировались в сети, порты добавляются в соответствующие VLAN-ы:

```
DES-3800:4# show vlan
Command: show vlan

VID              : 1          VLAN Name      : default
VLAN TYPE        : static     Advertisement  : Enabled
Member ports     : 1,3-7,9-21,24-28  ← Порты 2 и 8 удалены из VLAN default
Static ports     : 1,3-7,9-21,24-28
Current Untagged ports : 1,3-7,9-21,24-28
Static Untagged ports  : 1,3-7,9-21,24-28
Forbidden ports :

VID              : 2          VLAN Name      : v2
VLAN TYPE        : static     Advertisement  : Disabled
Member ports     : 2,22
Static ports     : 2,22
Current Untagged ports : 2,22  ← Порт 2 стал членом VLAN v2
Static Untagged ports  : 2,22
Forbidden ports :

VID              : 3          VLAN Name      : v3
VLAN TYPE        : static     Advertisement  : Enabled
Member ports     : 8,23
Static ports     : 8,23
Current Untagged ports : 8,23  ← Порт 8 стал членом VLAN v3
Static Untagged ports  : 8,23
Forbidden ports :

Total Entries : 3
```

D-Link
Building Networks for People

Пример настройки WAC - Присвоить VLAN исходя из имени пользователя

После того, как пользователи аутентифицировались в сети, статус портов WAC следующий:

```
DES-3800:4# show wac ports all
Command: show wac ports all
Port  State    Username          IP address       Auth status
Assigned VLAN
----  -------  ----------------  ---------------  --------------
-------------
1     Enable   u1                10.54.81.1       Authenticated   1
2     Enable   u2                10.54.81.2       Authenticated   2
3     Enable                     0.0.0.0          Unauth          1
4     Enable                     0.0.0.0          Unauth          1
5     Enable                     0.0.0.0          Unauth          1
6     Enable                     0.0.0.0          Unauth          1
7     Enable                     0.0.0.0          Unauth          1
8     Enable   u3                10.54.81.3       Authenticated   3
9     Disable                    0.0.0.0          Unauth
10    Disable                    0.0.0.0          Unauth
11    Disable                    0.0.0.0          Unauth
12    Disable                    0.0.0.0          Unauth
…
```

Примечание:

В текущей реализации, если использовать WAC в VLAN, **не являющейся System VLAN**, сообщение **“об успешно пройденной аутентификации”** и **“WEB-страница для перенаправления”** не будут отображены на PC. Несмотря на это, PC всё равно получит доступ к ресурсам сети в этом VLAN.

D-Link
Building Networks for People

Пример настройки WAC - Присвоить VLAN исходя из имени пользователя

Результаты теста:

1. Перед тем, как PC1, PC2, и PC3 будут аутентифицированы, эти PC не могут получить доступ к ресурсам сети в определённом VLAN по протоколу TCP.

2. После того, как эти PC аутентифицированы,

PC1 имеет доступ к ресурсам VLAN default (VID=1).

PC2 имеет доступ (по протоколу TCP, например, WEB, ftp) к ресурсам VLAN v2.

PC3 имеет доступ (по протоколу TCP, например, WEB, ftp) к ресурсам VLAN v3.

D-Link
Building Networks for People

Выводы по аутентификации на основе WEB

1. WAC предоставляет лёгкий в использовании и применении метод, основанный на протоколе HTTP. Перед прохождением процесса аутентификации, весь TCP - трафик будет заблокирован.
2. WAC может использовать локальную базу данных пользователей или RADIUS - сервер для осуществления аутентификации.
3. WAC также позволяет добавлять разных пользователей в разные VLAN. Это может быть использовано для предоставления разного уровня обслуживания для разных пользователей.

D-Link
Building Networks for People

ACL – Списки управления доступом, Классификация трафика, маркировка и отбрасывание

ACL (списки контроля доступа)

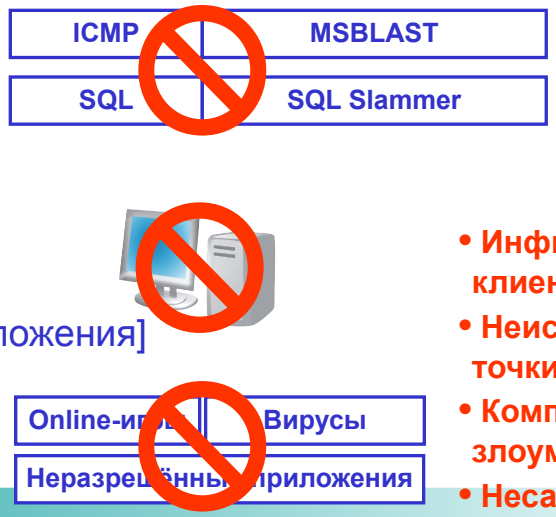
- **Контроль сетевых приложений**

L2/3/4 ACL (Access Control List)

Коммутаторы D-Link предоставляют наиболее полный набор ACL, помогающих сетевому администратору осуществлять контроль над приложениями. При этом не будет потерь производительности, поскольку проверка осуществляется на аппаратном уровне.

ACL в коммутаторах D-Link могут фильтровать пакеты, основываясь на информации разных уровней:

- ✔ Порт коммутатора
- ✔ MAC/ IP-адрес
- ✔ Тип Ethernet/ Тип протокола
- ✔ VLAN
- ✔ 802.1p/ DSCP
- ✔ TCP/ UDP-порт [тип приложения]
- ✔ Содержание пакета [поле данных приложения]



- **ACL могут проверять содержимое пакетов на предмет наличия новых изменённых потоков**
- **Инфицированные клиенты**
- **Неисправные сервера/ точки доступа**
- **Компьютеры злоумышленников**
- **Несанкционированные пользователи**

- **Управляемые коммутаторы D-Link могут эффективно предотвращать проникновение вредоносного трафика в сеть**

Указания к конфигурированию профилей доступа (Access Profile)

- Проанализируйте задачи фильтрации и определитесь с типом профиля доступа - Ethernet или IP
- Зафиксируйте стратегию фильтрации
- Основываясь на этой стратегии, определите какая необходима маска профиля доступа (access profile mask) и создайте её. (команда **create access_profile**)
- Добавьте правило профиля доступа (access profile rule), связанное с этой маской (команда **config access_profile**)
- Правила профиля доступа проверяются в соответствии с номером access_id. Чем меньше ID, тем раньше проверяется правило. Если не одно правило не сработало, пакет пропускается.
- При необходимости, когда срабатывает правило, биты 802.1p/DSCP могут быть заменены на новые значения перед отправкой пакета, выступая в качестве “**Маркера**” в модели DSCP PHB (Per-Hop Behavior – пошаговое поведение).

Типы профиля доступа

1. Ethernet:

- VLAN
- MAC источника
- MAC назначения
- 802.1p
- Тип Ethernet
- Порты*

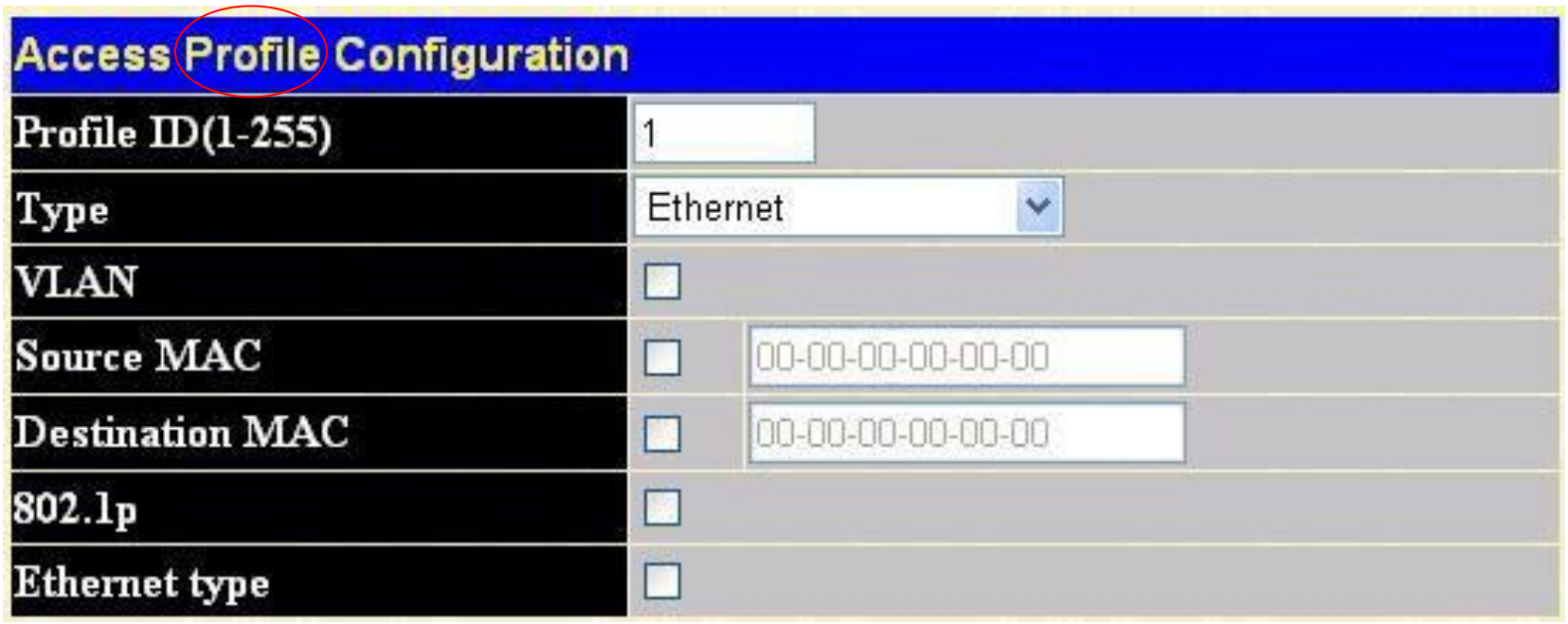
2. IP:

- VLAN
- Маска IP источника
- Маска IP назначения
- DSCP
- Протокол (ICMP, IGMP, TCP, UDP)
- TCP/UDP-порт
- Порты*

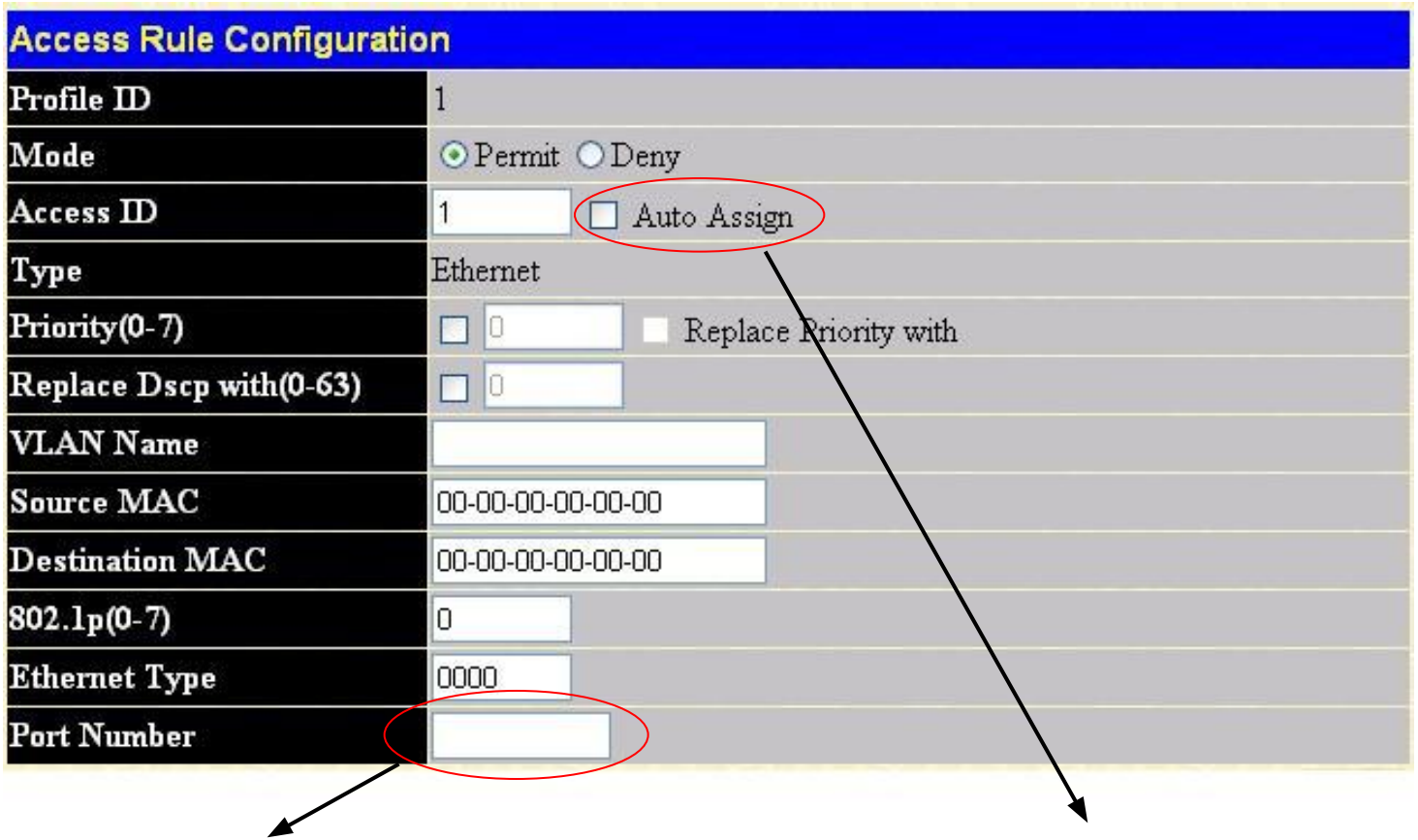
3. Фильтрация по содержимому пакета (первые 80 байт пакета)*. Доступно в моделях DES-35XX, DES-38XX, DES-3028/3052, DGS/DXS-33XX, DGS-34XX, DGS-36XX

D-Link
Building Networks for People

Профиль доступа Ethernet

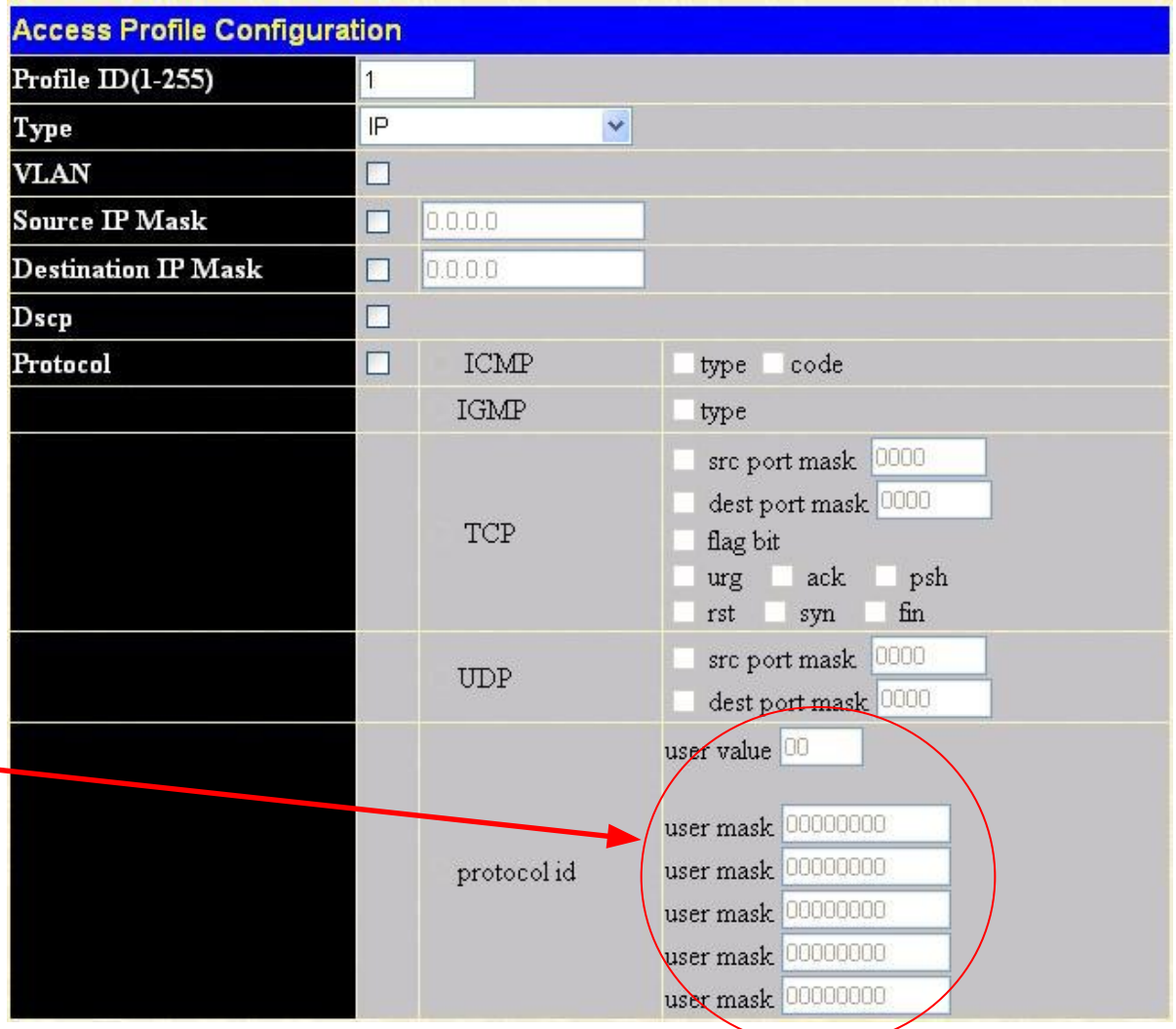


Правило доступа Ethernet



Когда нужно задать диапазон портов, галочка **Auto Assign** должна быть поставлена в поле **Access ID**.

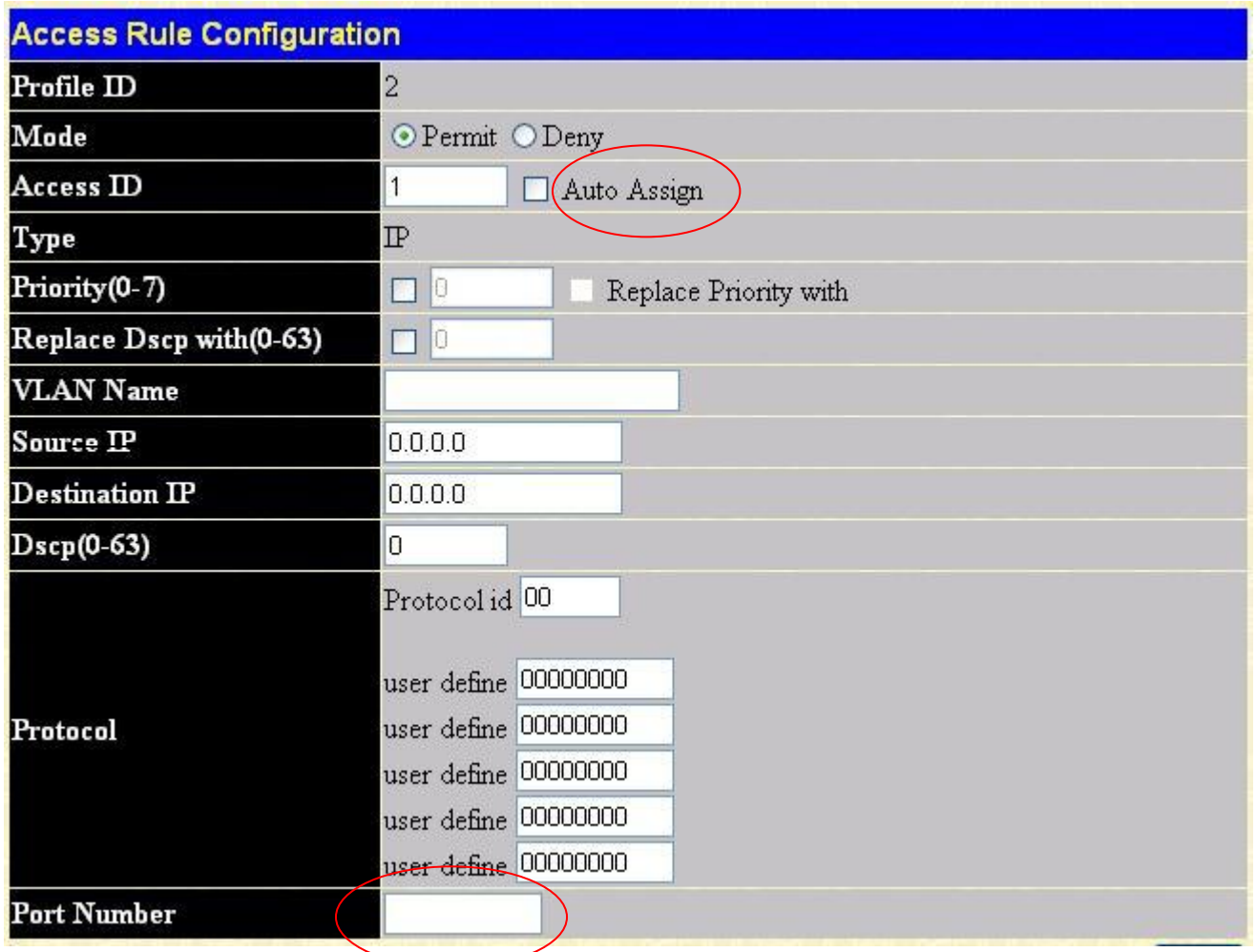
Маска IP профиля доступа



Можно задать до 5 масок портов уровня 4 для порта назначения в шестнадцатиричной форме (0x0-0xffffffff)

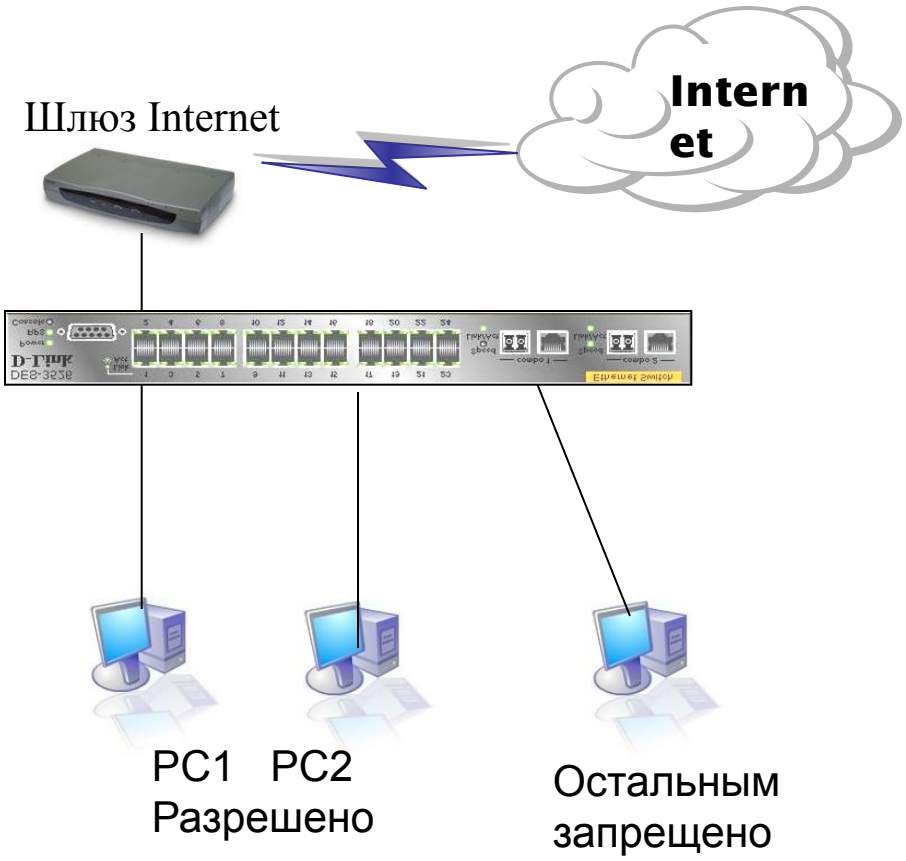
D-Link
Building Networks for People

Правило профиля доступа IP



ACL в коммутаторах Ethernet L2 – Пример I

Пример: Разрешить некоторым пользователям выход в Internet по MAC- адресам



Шлюз Internet:
IP = 10.254.254.251/8
0050BA999999

Разрешён доступ в Internet:
PC1:10.1.1.1/8,
0050ba111111
PC2:10.2.2.2/8,
0050ba222222
Шлюз = 10.254.254.251

Другие PC (доступ к Internet запрещён):
IP: 10.x.x.x/8

Ethernet ACL в коммутаторах
L2 – Пример I со старым правилом ACL

Правила:

Правило 1: Если MAC назначения = Шлюз и MAC источника = разрешённый PC1, разрешить
Если MAC назначения = Шлюз и MAC источника = разрешённый PC2, разрешить
(другие разрешённые MAC - PC3, PC4, и т.д.)

Правило 2: Если MAC назначения = Шлюз, запретить

Правило 3: В противном случае (разрешить всё остальное по умолчанию).

\# Правило 1

create access_profile ethernet source_mac FF-FF-FF-FF-FF-FF destination_mac FF-FF-FF-FF-FF-FF profile_id 10

config access_profile profile_id 10 add access_id 11 ethernet source_mac 00-50-ba-11-11-11 destination_mac 00-50-ba-99-99-99 permit

config access_profile profile_id 10 add access_id 12 ethernet source_mac 00-50-ba-22-22-22 destination_mac 00-50-ba-99-99-99 permit

\# добавить остальные разрешённые MAC в правилах с тем же ID профиля (10), но с разными ID доступа (13, 14, 15 и т.д.).

\# Правило 2

create access_profile ethernet destination_mac FF-FF-FF-FF-FF-FF profile_id 20

config access_profile profile_id 20 add access_id 21 ethernet destination_mac 00-50-ba-99-99-99 deny

\# Правило 3: Другие пакеты разрешены по умолчанию

Проверка:

PC1, PC2 могут получить доступ к Internet. (Разрешённые правилом 1 MAC могут получить доступ к Internet)

Другие компьютеры не могут получить доступ к Internet. (Другие PC не могут получить доступ к Internet, в соответствии с правилом 2)

PC1, PC2 и другие могут получить доступ друг к другу (Intranet OK, в соответствии с правилом 3)

D-Link
Building Networks for People

Ethernet ACL в коммутаторах
L2 – Пример I с новым правилом ACL

Правила:

Правило 1: Если MAC назначения = Шлюз, запретить

(другие порты, которые нужно запретить и т.д.)

Правило 2: В противном случае (разрешить всё остальное по умолчанию).

Правило 1

create access_profile ethernet destination_mac FF-FF-FF-FF-FF-FF profile_id 10

config access_profile profile_id 10 add access_id 10 ethernet destination_mac 00-50-ba-99-99-99 port 24 deny

добавить другие запрещающие правила с тем же ID профиля (10), но с другими ID доступа и портами (21, 22, 23 и т.д.).

Правило 2: Другие пакеты разрешены по умолчанию

Проверка:

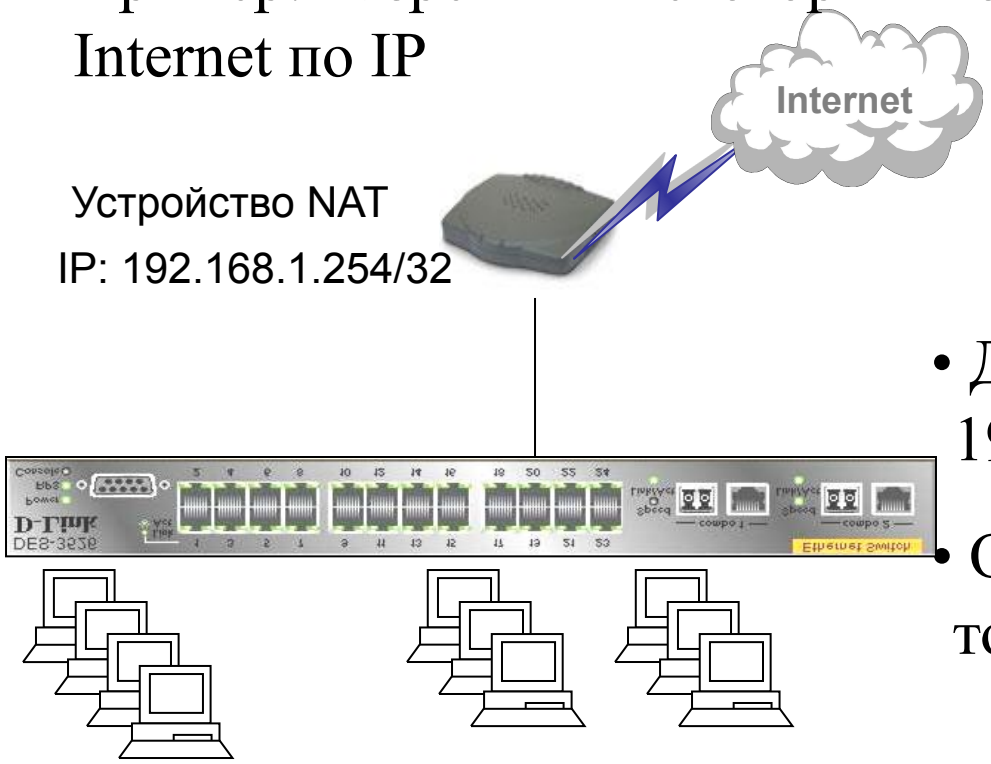
PC1, PC2 могут получить доступ к Internet. (Разрешённые правилом 1 MAC могут получить доступ к Internet)

Другие компьютеры не могут получить доступ к Internet. (Другие PC не могут получить доступ к Internet, в соответствии с правилом 2)

PC1, PC2 и другие могут получить доступ друг к другу (Intranet OK, в соответствии с правилом 3)

IP ACL в коммутаторах L2 – Пример II

Пример: Разрешить некоторым пользователям выход в Internet по IP



- Доступ в Internet разрешён: 192.168.1.1 ~ 192.168.1.63
- Остальные пользуются только Intranet

IP ACL в коммутаторах L2 – Пример II со старым правилом ACL

Правила:
Правило 1: Если IP назначения =192.168.1.254/24 и IP источника = 192.168.1.1/24, разрешить (Intranet OK)
Правило 2: Если IP источника = 192.168.1.1/26, разрешить (для .1 - .63 разрешить доступ в Internet)
Правило 3: Если IP источника = 192.168.1.1/24, запретить (для .1 - .254 запретить доступ в Internet)
Правило 4: В противном случае, разрешить всё остальное по умолчанию

Правило 1: .1 - .254 Intranet OK
create access_profile ip destination_ip_mask 255.255.255.0 source_ip_mask 255.255.255.0 profile_id 10
config access_profile profile_id 10 add access_id 11 ip destination_ip 192.168.1.254 source_ip 192.168.1.1 permit

Правило 2: Разрешить для .1 - .63 доступ в Internet
create access_profile ip source_ip_mask 255.255.255.192 profile_id 20
config access_profile profile_id 20 add access_id 21 ip source_ip 192.168.1.1 permit

Правило 3: Запретить для .1 - .254 доступ в Internet
create access_profile ip source_ip_mask 255.255.255.0 profile_id 30
config access_profile profile_id 30 add access_id 31 ip source_ip 192.168.1.1 deny

Правило 4: Всё остальное разрешено по умолчанию

Проверка:

1. 192.168.1.1 - 192.168.1.63 могут получить доступ к Internet (правило 2), и ко всем остальным PC .64 - .253 (правило 1).
2. PC .64 - .253 могут иметь доступ к PC .1 - .253 (правило 1), но не могут выйти в Internet (правило 3).

D-Link
Building Networks for People

IP ACL в коммутаторах L2 – Пример II с новым правилом ACL

Правила:
Правило 1: Если IP источника = 192.168.1.1/26, разрешить (для .1 - .63 разрешить доступ к Internet)
Правило 2: Если IP назначения = 192.168.1.254/32, запретить (запретить всем остальным)
Правило 3: В противном случае, разрешить всё остальное по умолчанию

Правило 1: Разрешить для .1 - .63 доступ к Internet
create access_profile ip source_ip_mask 255.255.255.192 profile_id 10
config access_profile profile_id 10 add access_id 10 ip source_ip 192.168.1.1 port 1 permit

Правило 2: Запретить остальным доступ к Internet
create access_profile ip destination_ip_mask 255.255.255.255 profile_id 20
config access_profile profile_id 20 add access_id 20 ip destination_ip 192.168.1.254 port 1 deny
Правило 3: Всё остальное разрешено по умолчанию

На основе рекомендаций с сайта CERT (http://www.cert.org/), можно фильтровать порты TCP/UDP для предотвращения распространения вирусов:

1. Фильтрация TCP потров 135,139,445.

Команды CLI:

create access_profile ip tcp dst_port_mask 0xFFFF deny profile_id 30
config access_profile profile_id 30 add access_id 1 ip tcp dst_port 135
config access_profile profile_id 30 add access_id 2 ip tcp dst_port 139
config access_profile profile_id 30 add access_id 3 ip tcp dst_port 445

2. Фильтрация UDP портов 135,139,445

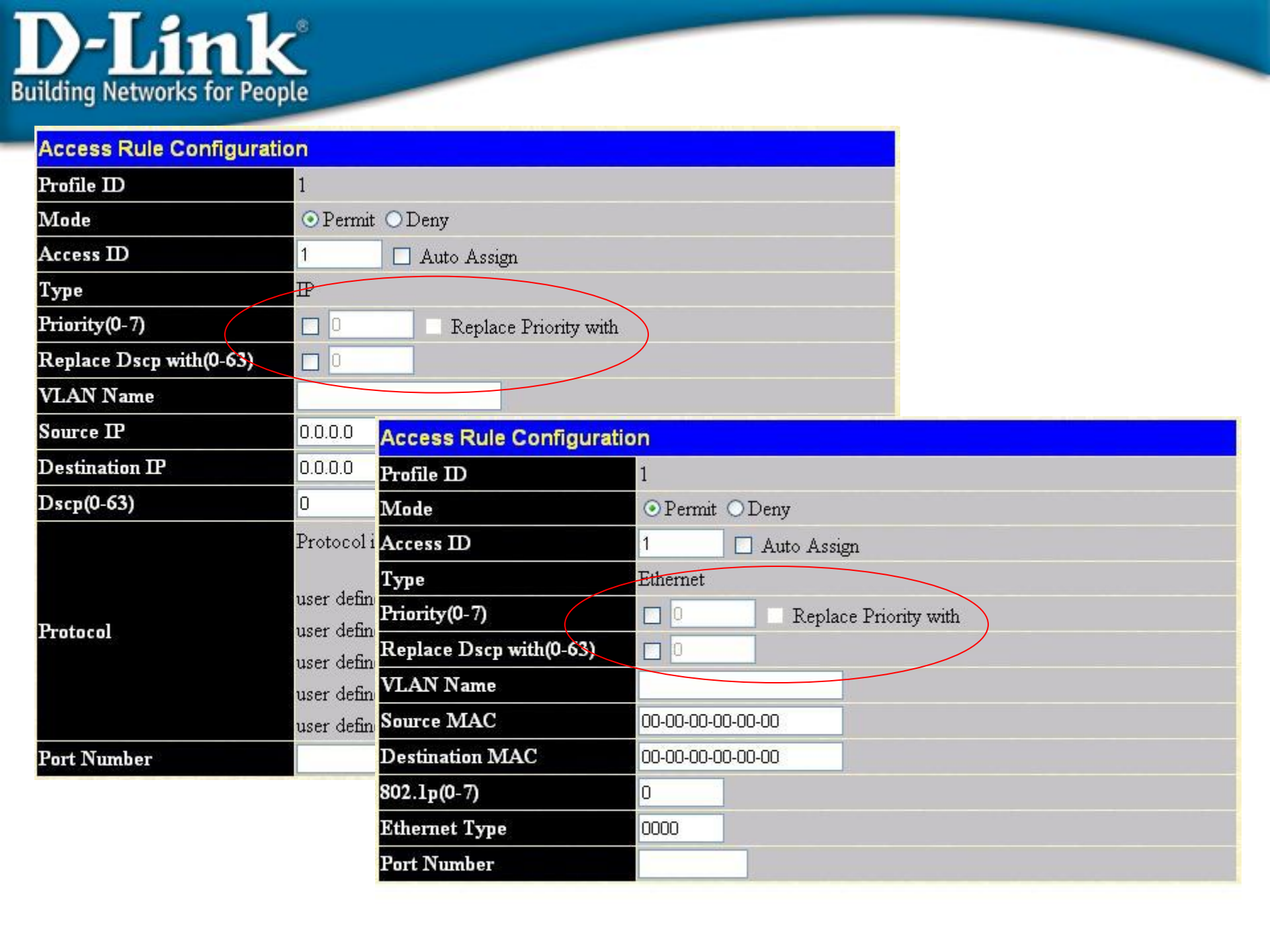
Команды CLI:

create access_profile ip udp dst_port_mask 0xFFFF deny profile_id 40
config access_profile profile_id 40 add access_id 1 ip udp dst_port 135
config access_profile profile_id 40 add access_id 2 ip udp dst_port 139
config access_profile profile_id 40 add access_id 3 ip udp dst_port 445

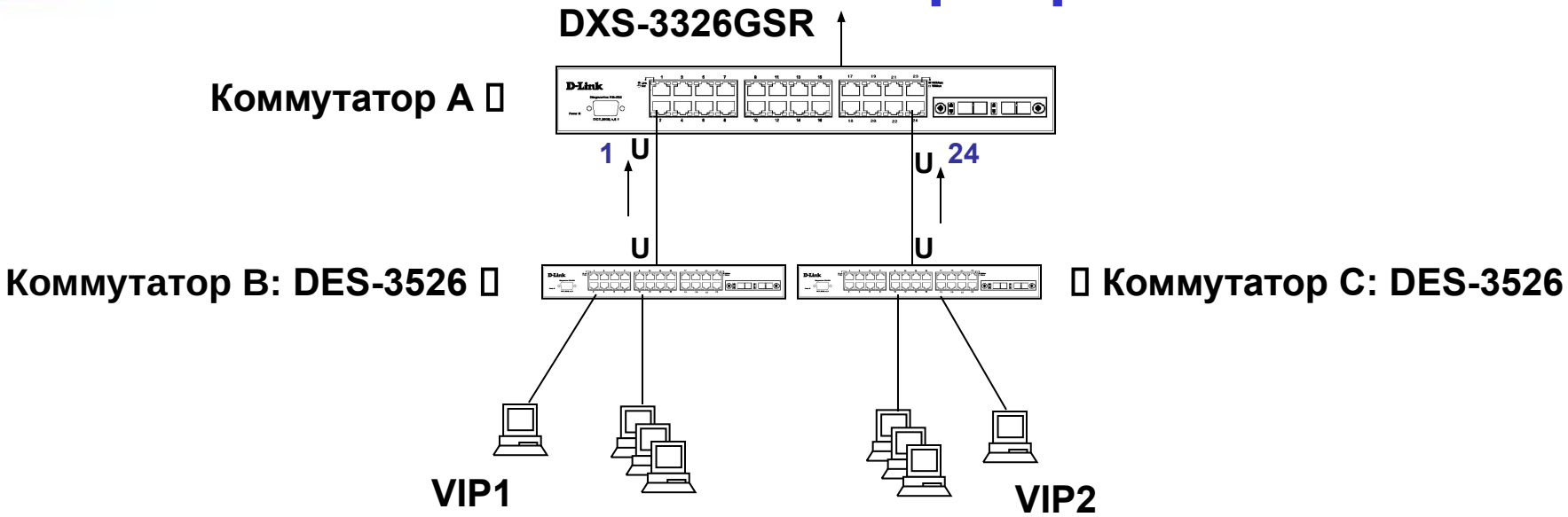
D-Link
Building Networks for People

ACL для QoS

1. При написании ACL, DSCP является одним из полей, которое может проверяться. Если мы хотим проверять поле DSCP, надо выбрать его (v) в “Маске IP профиля доступа”.
2. Следующим шагом является написание “Правила IP профиля доступа”. В этом правиле, мы уже можем добавить значение DSCP, которое будет проверяться. При совпадении, мы можем:
   - проассоциировать пакет с очередью приоритетов 1p
   - проассоциировать пакет с очередью приоритетов 1p и заменить значение 1p перед передачей пакета
   - задать пакету новое значение DSCP и выслать пакеты, играющие роль МАРКЕРОВ в модели PHB.
3. Если пакет проассоциирован с очередью приоритетов 1p, он, затем, будет обработан в соответствии с “Пользовательским приоритетом 802.1p” для проведения соответствия приоритета 1p одной из 4-х очередей приоритетов.


D-Link
Building Networks for People
Access Rule Configuration
Profile ID
1
Mode
Permit
Deny
Access ID
1
Auto Assign
Type
IP
Priority(0-7)
0
Replace Priority with
Replace Dscp with(0-63)
0
VLAN Name
Source IP
0.0.0.0
Destination IP
0.0.0.0
Dscp(0-63)
0
Protocol
Protocol i
user defin
user defin
user defin
user defin
user defin
Port Number
Access Rule Configuration
Profile ID
1
Mode
Permit
Deny
Access ID
1
Auto Assign
Type
Ethernet
Priority(0-7)
0
Replace Priority with
Replace Dscp with(0-63)
0
VLAN Name
Source MAC
00-00-00-00-00-00
Destination MAC
00-00-00-00-00-00
802.1p(0-7)
0
Ethernet Type
0000
Port Number

DSCP, 802.1p и очередь приоритетов



Пример – Промаркировать пакеты с определённым DSCP определённым приоритетом 1p и поставить в соответствующую очередь

Последующие правила промаркируют пакеты следующим образом:

Очередь 1 - данные с dscp = 10 = приоритет 802.1p = 3

Очередь 2 – данные с dscp = 20 = приоритет 802.1p = 5

Очередь 3 – данные с dscp = 30 = приоритет 802.1p = 7

create access_profile ip dscp profile_id 10

config access_profile profile_id 10 add access_id 10 ip dscp 30 port 1 permit priority 7 replace_priority

config access_profile profile_id 10 add access_id 20 ip dscp 30 port 24 permit priority 7 replace_priority

config access_profile profile_id 10 add access_id 30 ip dscp 20 port 1 permit priority 5 replace_priority

config access_profile profile_id 10 add access_id 40 ip dscp 20 port 24 permit priority 5 replace_priority

config access_profile profile_id 10 add access_id 50 ip dscp 10 port 1 permit priority 3 replace_priority

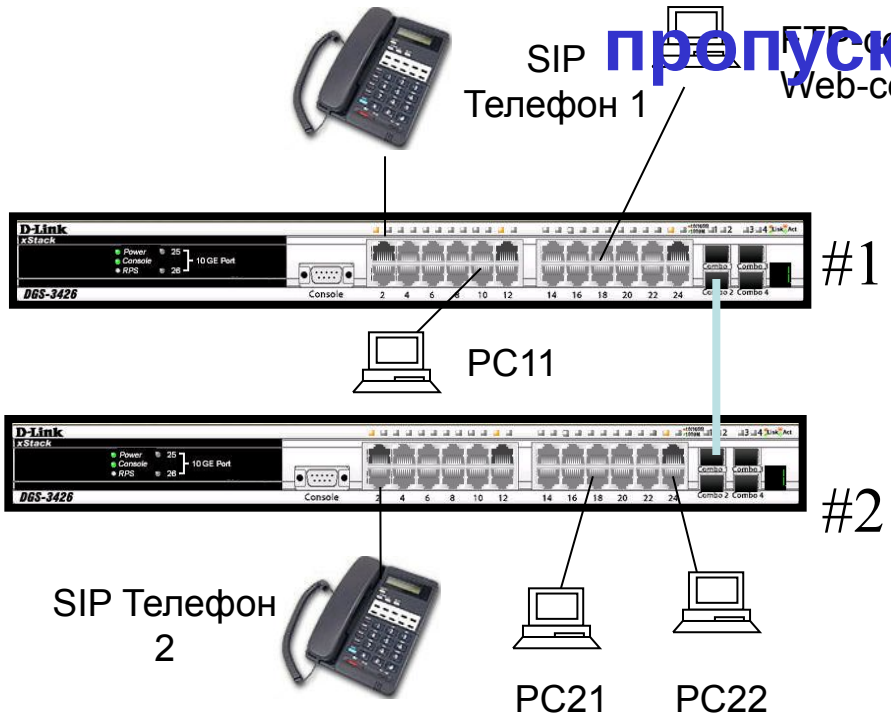
config access_profile profile_id 10 add access_id 60 ip dscp 10 port 24 permit priority 3 replace_priority

Основываясь на соответствии “802.1p User Priority” пакет будет поставлен в очередь с наивысшим приоритетом и будет обработан первым.

D-Link
Building Networks for People

Per-flow Bandwidth Control – контроль полосы пропускания по потокам

Почему контроль полосы пропускания по потокам



Как сконфигурировать QoS в соответствии со следующими требованиями?

1. VoIP (SIP Телефон) должен иметь наивысший приоритет в строгом режиме (чтобы исключить задержки при передаче голоса).

2. FTP-трафик (или любой другой трафик, сильно расходующий полосу пропускания, например, p2p) должен использовать только часть полосы пропускания (например, максимум 5 Мбит/с).

Условие (1) может быть выполнено настройкой ACL путём перемаркировки 802.1p/DSCP. **Но как реализовать пункт (2)??**

Решение: Новая функция “per-flow” bandwidth control (поддерживается серией DGS-3400).

Контроль полосы пропускания по потокам

Почему контроль полосы пропускания по потокам?

Серии DES-3800 или xStack поддерживают ACL только в режимах permit или deny (0 или 1). Если пользователь хочет разрешить определённый трафик с определённой полосой пропускания (например, FTP может максимально использовать 5 Мбит/с от общей полосы пропускания), такая реализация ACL не может в этом помочь.

DGS-3400 (и более поздние серии) могут, основываясь на совпадении по типу трафика, ограничивать полосу пропускания, благодаря поддержке нового механизма ACL.

Как работает контроль полосы пропускания по потокам?

Эта функция основана на новой политике ACL. DGS-34xx использует механизм ACL для просмотра определённого типа трафика и ограничения полосы пропускания. Весь этот процесс происходит на микросхемах портов - ASIC. Т.о., это не влияет на загрузку CPU и соответственно не снижает производительность коммутатора.

D-Link
Building Networks for People

Команды настройки контроля полосы пропускания по потокам

Команда настройки ACL без поддержки “per-flow bandwidth control” для того чтобы создать правило из нашего примера.

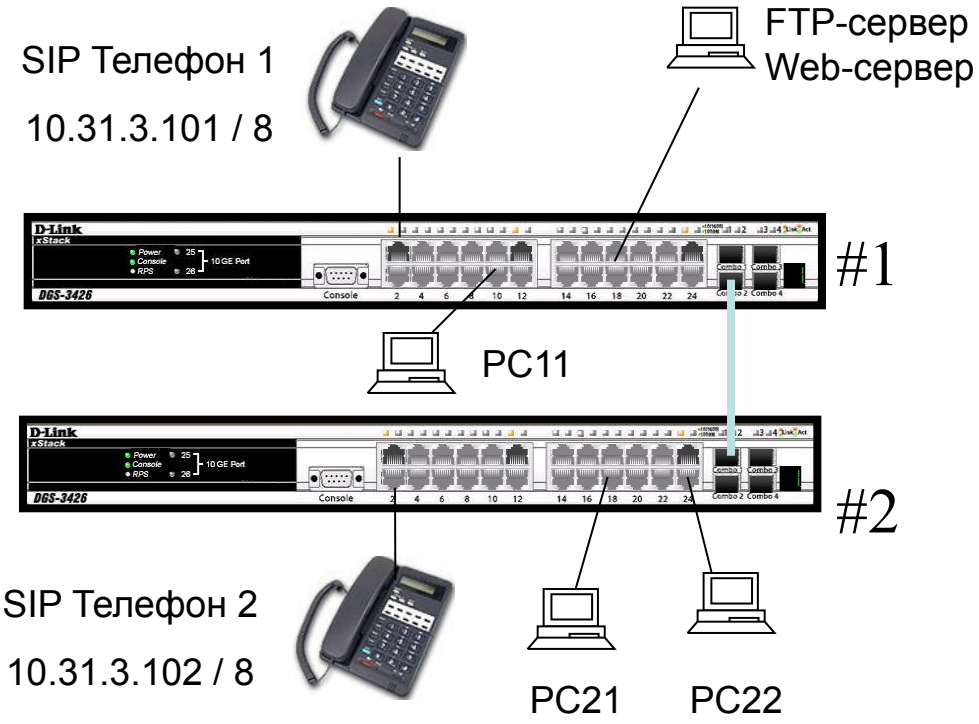
```
config access_profile profile_id <value 1-6> ip {
| source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value> | [ icmp | igmp
| tcp { src_port <value 0-65535> | dst_port <value 0-65535> | flag [all | { urg | ack | psh | rst | syn | fin }] }
| udp { src_port <value 0-65535> | dst_port <value 0-65535> }
| protocol_id <value 0 - 255> { user_define <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex
0x0-0xffffffff><hex 0x0-0xffffffff>} ] }
port <portlist>
[ permit { priority <value 0-7> {replace_priority_with <value 0-7>} | replace_dscp_with <value 0-63>}
| deny ]}
```

Команда настройки ACL с поддержкой “per-flow bandwidth control” для того, чтобы создать правило из нашего примера. Эта опция также поддерживается для типов ACL “ethernet”,”packet_content”, “ipv6” (не только для указанного типа).

```
config access_profile profile_id <value 1-6> ip {
| source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value> | [ icmp | igmp
| tcp { src_port <value 0-65535> | dst_port <value 0-65535> | flag [all | { urg | ack | psh | rst | syn | fin }] }
| udp { src_port <value 0-65535> | dst_port <value 0-65535> }
| protocol_id <value 0 - 255> { user_define <hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex 0x0-0xffffffff><hex
0x0-0xffffffff><hex 0x0-0xffffffff>} ] }
port <portlist>
[ permit { priority <value 0-7> {replace_priority_with <value 0-7>} | replace_dscp_with <value 0-63> |
rx_rate [ no_limit | <value 1-156249>] }
| deny ]}
```

Это означает, что при выборе действия “permit” – «разрешить», может быть задана полоса пропускания для определённого типа трафика на приём.

Пример настройки контроля полосы пропускания по потокам



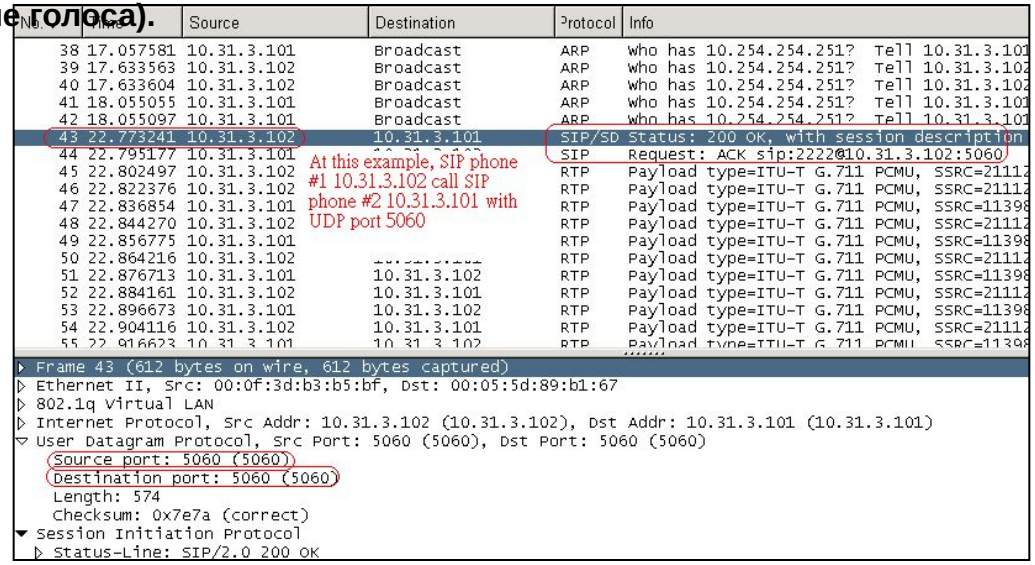
Задача:

1. **VoIP (SIP Телефон) должен иметь наивысший приоритет в строгом режиме (чтобы исключить задержки при передаче голоса).**

2. **FTP-трафик (или любой другой трафик, сильно расходующий полосу пропускания, например, p2p) должен использовать только часть полосы пропускания (например, максимум 5 Мбит/с).**

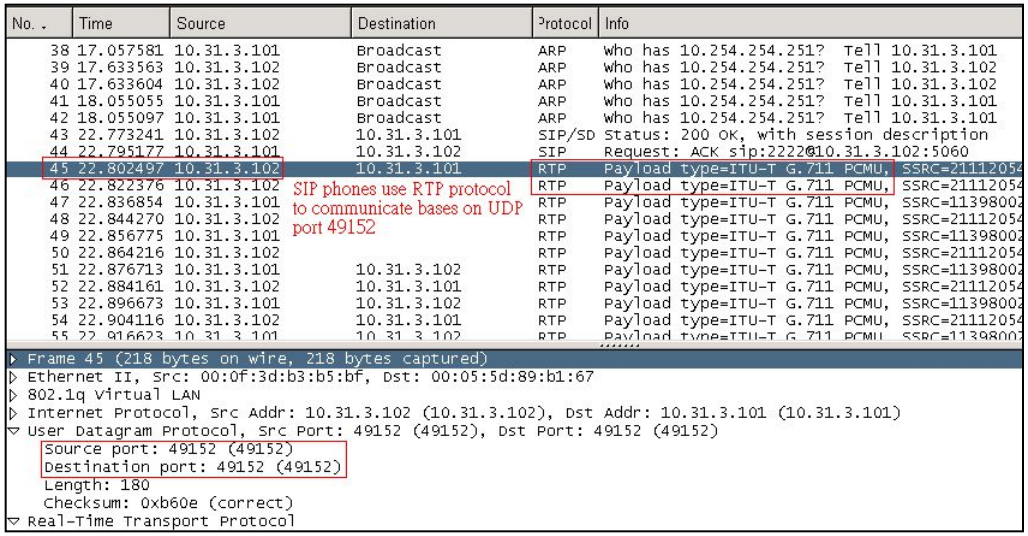
Пример настройки контроля полосы пропускания по потокам

1. VoIP (SIP Телефон) будет иметь наивысший приоритет в строгом режиме (чтобы исключить задержки при передаче голоса).



Формат пакета VoIP (SIP)

Формат управляющего пакета VoIP SIP, использующего UDP-порты источника/назначения 5060/5060



Формат пакета данных VoIP SIP, использующего UDP/RTP-порты источника/назначения 49152/49152.

Примечание: Различные VoIP-приложения могут использовать собственный порт UDP. Захватите сниффером пакеты для того, чтобы определить номер порта.

Пример настройки контроля полосы пропускания по потокам

1. VoIP (SIP Телефон) будет иметь наивысший приоритет в строгом режиме (чтобы исключить задержки при передаче голоса).

Конфигурация коммутатора #1 для передачи данных VoIP

1. Если в пакете DSCP=56, то перемаркировать пакет приоритетом 802.1p = 7 (и затем поместить в очередь с наивысшим приоритетом).
create access_profile profile_id 1 ip dscp
config access_profile profile_id 1 add access_id auto_assign ip dscp 56 port all permit priority 7

2. Если пакет является пакетом VoIP, перемаркировать пакет приоритетом 802.1p = 7 (и затем поместить в очередь с наивысшим приоритетом), и заменить поле DSCP на 56 (111000).
create access_profile profile_id 2 ip udp src_port_mask 0xFFFF dst_port_mask 0xFFFF
config access_profile profile_id 2 add access_id auto_assign ip udp src_port 5060 dst_port 5060 port all permit priority 7 replace_dscp 56
config access_profile profile_id 2 add access_id auto_assign ip udp src_port 49512 dst_port 49512 port all permit priority 7 replace_dscp 56

3. Убедитесь, что механизм обработки очередей строгий (strict).
config scheduling_mechanism strict

Конфигурация коммутатора #2 для передачи данных VoIP

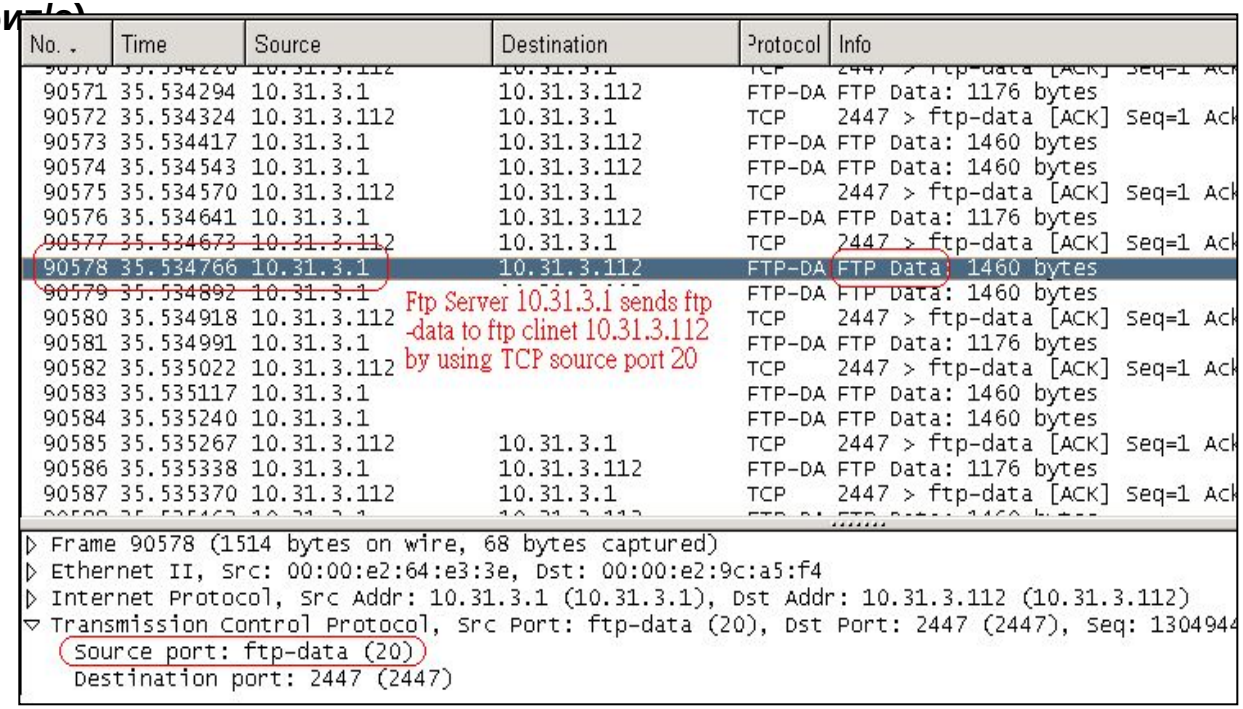
1. Если в пакете DSCP=56, то перемаркировать пакет приоритетом 802.1p = 7 (и затем поместить в очередь с наивысшим приоритетом).
create access_profile profile_id 1 ip dscp
config access_profile profile_id 1 add access_id auto_assign ip dscp 56 port all permit priority 7

2. Если пакет является пакетом VoIP, перемаркировать пакет приоритетом 802.1p = 7 (и затем поместить в очередь с наивысшим приоритетом), и заменить поле DSCP на 56 (111000).
create access_profile profile_id 2 ip udp src_port_mask 0xFFFF dst_port_mask 0xFFFF
config access_profile profile_id 2 add access_id auto_assign ip udp src_port 5060 dst_port 5060 port all permit priority 7 replace_dscp 56
config access_profile profile_id 2 add access_id auto_assign ip udp src_port 49512 dst_port 49512 port all permit priority 7 replace_dscp 56

3. Убедитесь, что механизм обработки очередей строгий (strict).
config scheduling_mechanism strict

Пример настройки контроля полосы пропускания по потокам

2. FTP-трафик должен использовать только часть полосы пропускания (например, максимум 5 Мбит/с)



Пакеты данных FTP используют TCP-порт источника 20

Конфигурация коммутатора #2 для ограничения полосы пропускания для ftp-трафика значением 5 Мбит/с.

create access_profile profile_id 2 ip tcp src_port_mask 0xFFFF

config access_profile profile_id 2 add access_id auto_assign ip tcp src_port 20 port 1-24 permit rx_rate 80

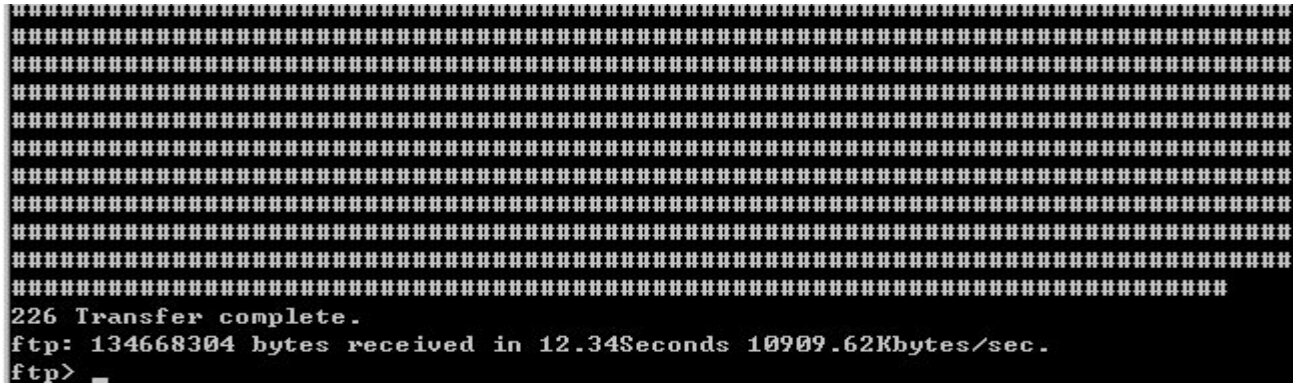
Примечание:

Шаг контроля полосы пропускания по потокам 64 Кбит/с. Например, rx_rate 80 = 80 * 64 Кбит/с = 5120 Кбит/с = 5 Мбит/с

Пример настройки контроля полосы пропускания по потокам

2. FTP-трафик должен использовать только часть полосы пропускания (например, максимум 5 Мбит/с)

До настройки функции контроля полосы пропускания по потокам ftp-трафик иметь полосы пропускания 10909 Кбайт/с



После настройки контроля полосы пропускания по потокам ftp-трафик имеет ограничение по полосе пропускания 632 Кбайт/с (около 5 Мбит/с)

Контроль полосы пропускания по потокам

Результаты тестов:

1. После настройки строгого режима QoS для пакетов VoIP, VoIP-трафик – голос, будет передаваться без задержек.

2. После настройки функции контроля полосы пропускания по потокам, применительно к FTP-трафику (или любому другому трафику, активно использующему полосу пропускания, например, p2p и т.д.), коммутатора не будет так сильно загружен передачей этого типа трафика, и другие приложения (такие как mail, web и т.д.) будут работать с меньшими задержками.

CPU Interface Filtering

D-Link
Building Networks for People

CPU Interface Filtering

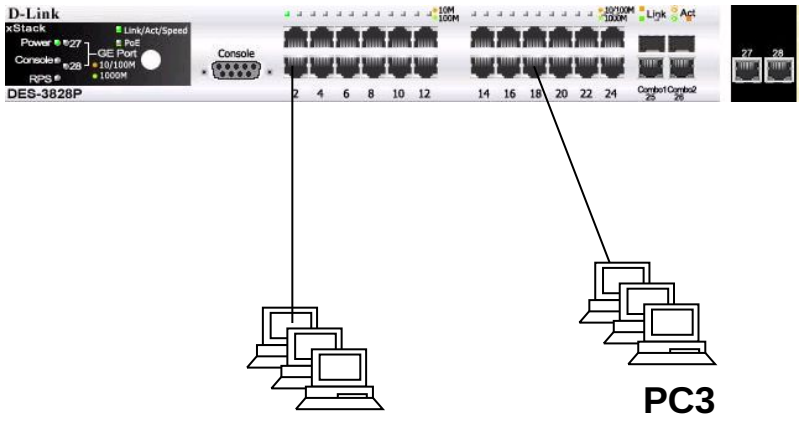
- Что такое CPU Interface Filtering?

  В текущей версии аппаратной платформы коммутаторов D-Link, некоторые пакеты, полученные коммутатором, должны быть направлены на обработку в CPU и эти пакеты не могут быть отфильтрованы аппаратными ACL. Например, пакет, в котором MAC-адрес назначения - это MAC-адрес коммутатора. (ping на IP-адрес коммутатора)

  Решение: CPU Interface Filtering. (Software ACL)

CPU Interface Filtering

IP-адрес коммутатора: 10.31.3.254/8



IP-адрес PC2: 10.31.3.2/8

IP-адрес PC3: 10.31.3.187/8

1. **PC2 имеет доступ к PC3.**
2. **PC3 имеет доступ к коммутатору.**
3. **PC2 не имеет доступа к коммутатору.**

Задача: PC2 имеет доступ к PC3, но PC2 не имеет доступа к коммутатору. PC3 имеет доступ и к PC2 и к коммутатору.

CPU Interface Filtering

Создайте профиль ACL для интерфейса CPU – процесс очень похож на создание обычного профиля ACL.
Сначала включите CPU Interface Filtering и создайте профиль, соответствующий заданию.
enable cpu_interface_filtering
create cpu access_profile ip source_ip_mask 255.255.255.128 icmp profile_id 1
config cpu access_profile profile_id 1 add access_id 1 ip source_ip 10.31.3.2 icmp deny
Command: show cpu access_profile
CPU Access Profile Table
CPU Access Profile ID : 1
Type : IP Frame Filter - ICMP
Masks :
Source IP Addr DSCP
--------------- -----
255.255.255.255
CPU Access ID: 1
Mode : Deny
--------------- -----
10.31.3.2 xx-xx
DES-3526:4#**show access_profile**
Command: show access_profile
В списке стандартных ACL профилей записей нет.

D-Link
Building Networks for People

CPU Interface Filtering

Результаты теста:

- Перед активацией функции CPU interface filtering, PC2 имеет доступ к коммутатору и PC3.
- После включения функции CPU interface, PC2 имеет доступ только к PC3.

Safeguard Engine

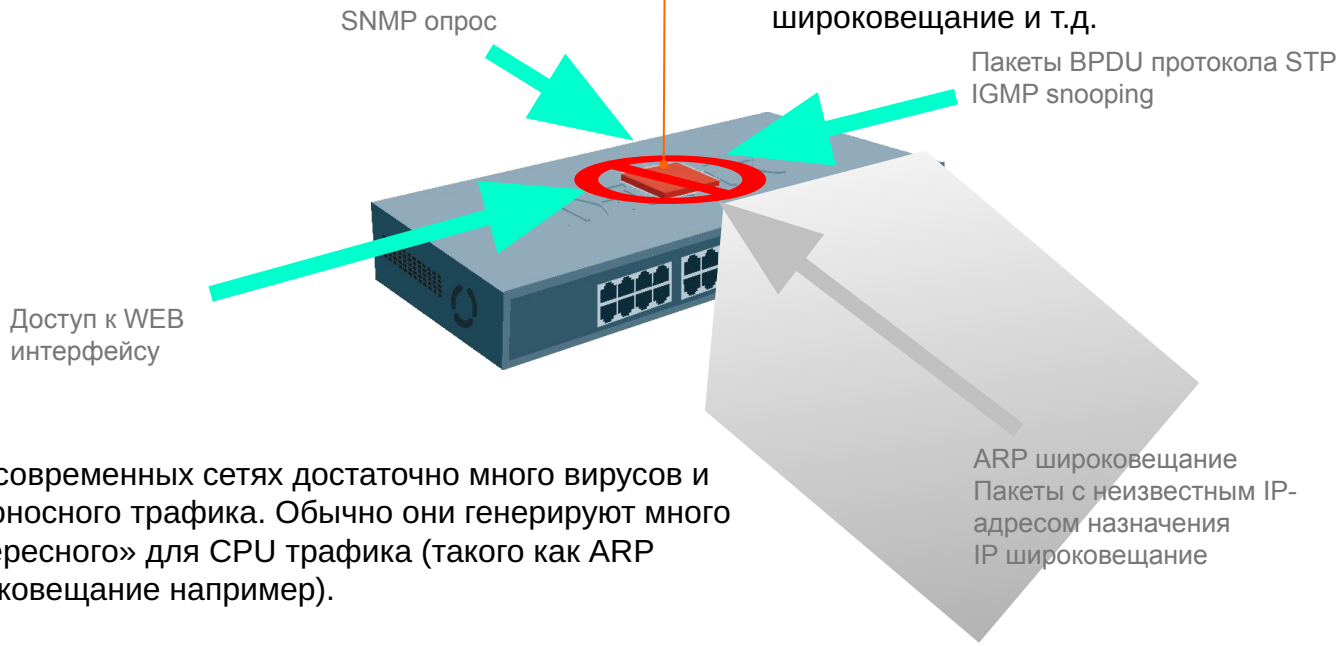
Почему Safeguard Engine?

Safeguard Engine™ разработан для того, чтобы повысить надёжность новых коммутаторов и общую доступность и отказоустойчивость сети.

Весь этот трафик загружает CPU и не даёт ему возможности обрабатывать более важные задачи, такие как административный доступ, STP, SNMP опрос.

CPU коммутатора предназначен для обработки управляющей информации, такой как STP, SNMP, доступ по WEB-интерфейсу и т.д.

Также CPU обрабатывает некоторый специфичный трафик, такой как ARP широковещание, пакеты с неизвестным IP-адресом назначения, IP широковещание и т.д.



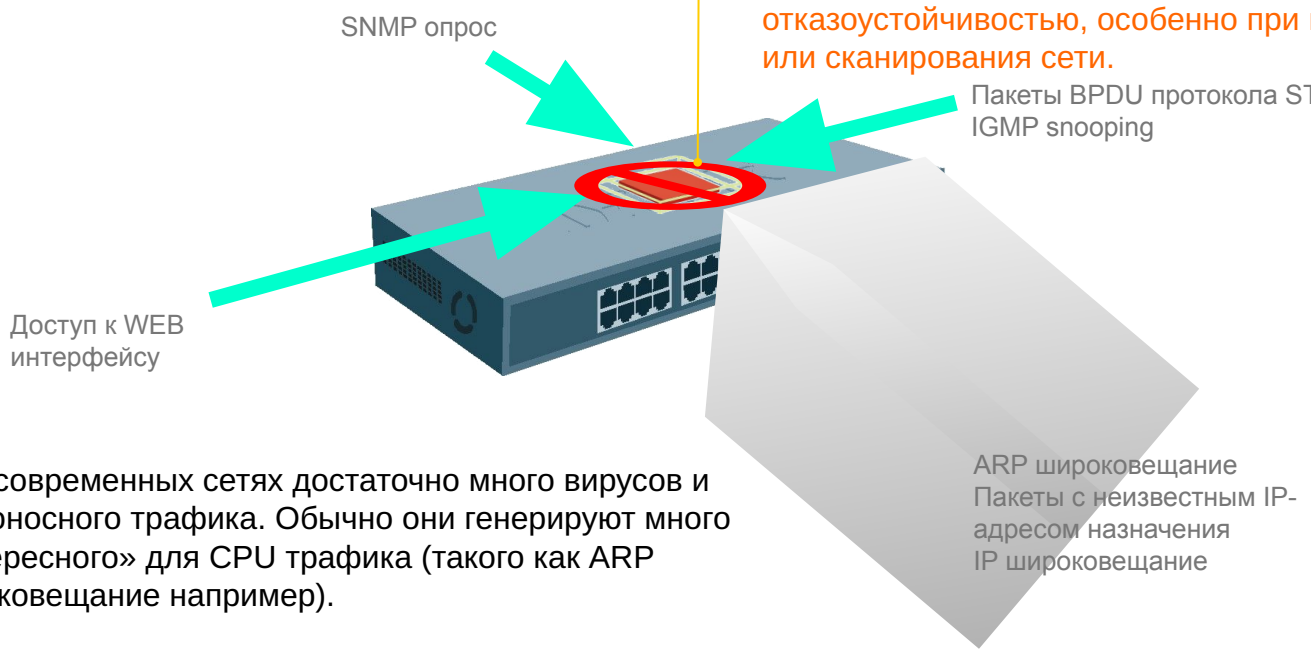
Но в современных сетях достаточно много вирусов и вредоносного трафика. Обычно они генерируют много «интересного» для CPU трафика (такого как ARP широковещание например).

Почему Safeguard Engine?

Safeguard Engine разработан для того, чтобы повысить надёжность новых коммутаторов и общую доступность и отказоустойчивость сети.

Весь этот трафик загружает CPU и не даёт ему возможности обрабатывать более важные задачи, такие как административный доступ, STP, SNMP опрос.

D-Link Safeguard Engine позволяет идентифицировать и приоритезировать этот «интересный» для CPU трафик с целью отбрасывания ненужных пакетов для сохранения функциональности коммутатора.
Таким образом с применением Safeguard Engine, коммутатор D-Link будет обладать отказоустойчивостью, особенно при вирусных атаках или сканирования сети.



Но в современных сетях достаточно много вирусов и вредоносного трафика. Обычно они генерируют много «интересного» для CPU трафика (такого как ARP широковещание например).

Обзор технологии

- Если загрузка CPU становится выше порога **Rising Threshold,** коммутатор войдёт в **Exhausted Mode (режим высокой загрузки**), для того, чтобы произвести следующие действия (смотрите следующий слайд).
- Если загрузка CPU становится ниже порога **Falling Threshold**, коммутатор выйдет из Exhausted Mode и механизм Safeguard Engine отключится.

Порог	Описание
Rising Threshold	•Пользователь может установить значение в процентах <20-100> верхнего порога загрузки CPU, при котором включается механизм Safeguard Engine. •Если загрузка CPU достигнет этого значения, механизм Safeguard Engine начнёт функционировать.
Falling Threshold	•Пользователь может установить значение в процентах <20-100> нижнего порога загрузки CPU, при котором выключается механизм Safeguard Engine. •Если загрузка CPU снизится до этого значения, механизм Safeguard Engine перестанет функционировать.

D-Link
Building Networks for People

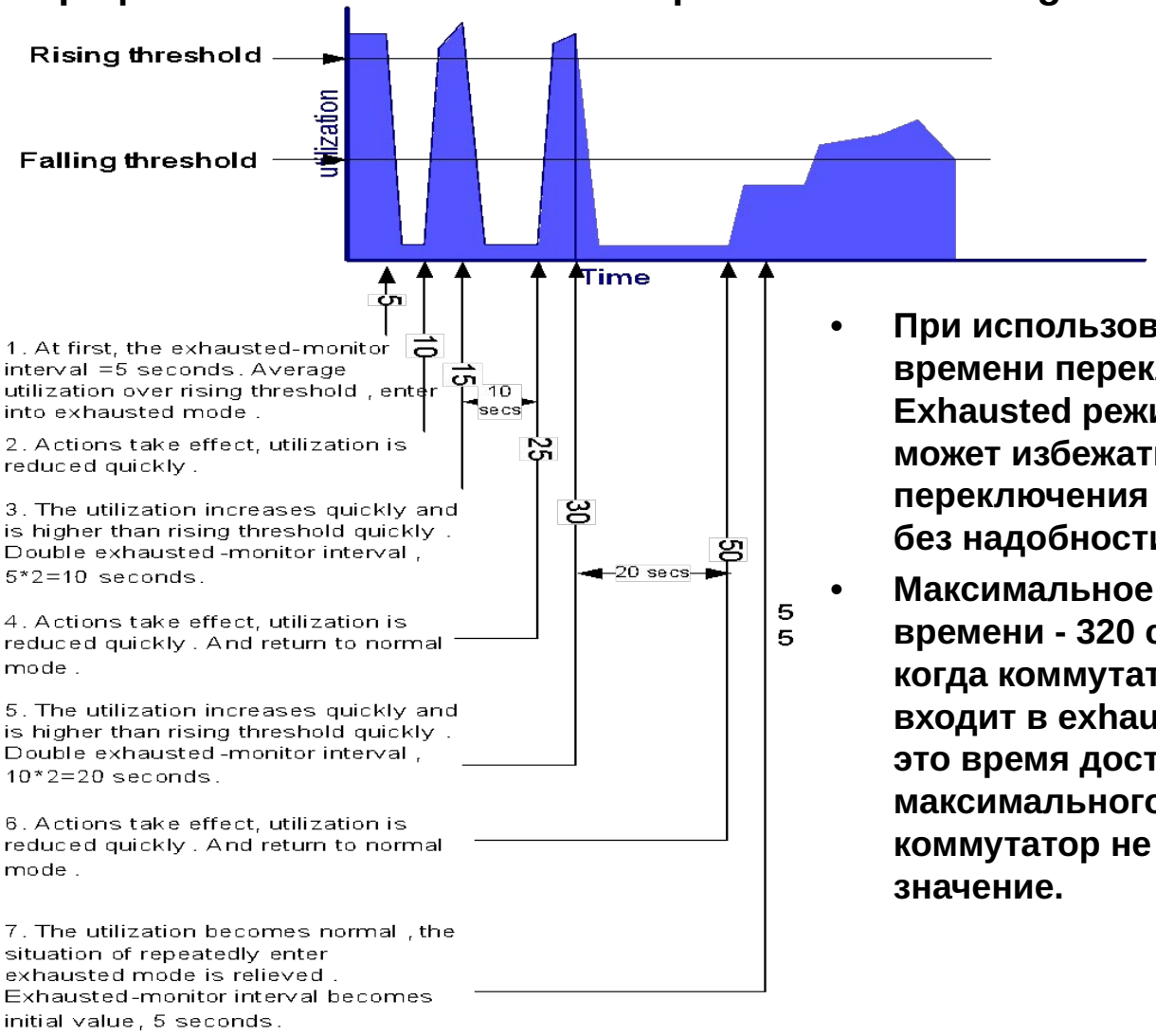
Обзор технологии

- **Функционирование Safeguard Engine**

Действие	Описание
Ограничение полосы пропускания для ARP-пакетов	•Пользователь может использовать эту функцию в двух режимах, в **Strict-Mode (Строгий режим)** или в **Fuzzy-Mode (Нестрогий режим)**. •Если выбран строгий режим, коммутатор **перестаёт получать ARP-пакеты.** •Если выбран нестрогий, коммутатор **минимизирует полосу пропускания для ARP-пакетов**, путём её динамического изменения.
Ограничение полосы пропускания для IP-широковещания	•Пользователь может использовать эту функцию в двух режимах, в **Strict-Mode (Строгий режим)** или в **Fuzzy-Mode (Нестрогий режим)**. •Если выбран строгий режим, коммутатор **перестаёт получать все широковещательные пакеты IP.** •Если выбран нестрогий, коммутатор **минимизирует полосу пропускания для широковещательных пакетов IP**, путём её динамического изменения.

Обзор технологии

- **График показывает механизм срабатывания Safeguard Engine**



- **При использовании ”Удвоенного времени переключения в Exhausted режим”, коммутатор может избежать постоянного переключения в exhausted mode без надобности.**
- **Максимальное значение этого времени - 320 секунд. В ситуации, когда коммутатор постоянно входит в exhausted mode, и когда это время достигает максимального значения, коммутатор не выйдет за это значение.**

D-Link
Building Networks for People

Модели коммутаторов, в которых реализована функция SafeGuard Engine

Модель коммутатора	Поддерживаемый режим Safeguard Engine	
	Strict Mode	Fuzzy Mode
DES-3500	V	X
DES-3800	V	X
DES-6500	V	V*
DGS-3400	V	V*
DGS-3600	V	V*
Примечание	* Поддержка режима Fuzzy требует аппаратной поддержки со стороны чипсета и доступна только для DES-6500 и DGS-3400/3600.	

D-Link
Building Networks for People

Модели коммутаторов, в которых реализована функция SafeGuard Engine

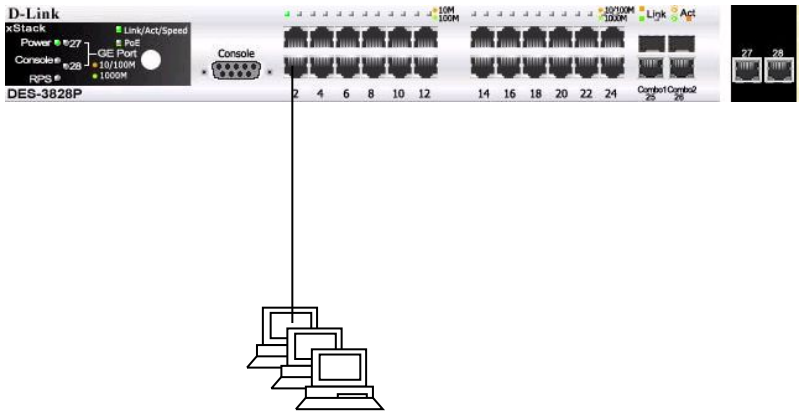
- Для обеспечения потребностей и простоты применения для заказчиков SMB, коммутаторы серии Smart II Series имеют другой механизм Safeguard Engine.
- Коммутаторы серии Smart II поддерживают Safeguard Engine только в режимах **"enable"** или **"disable“**, позволяя пользователю либо включить, либо выключить Safeguard Engine, и **по умолчанию функция включена.**
- **Механизм Safeguard Engine, реализованный в коммутаторах серии Smart II, имеет более простой подход.** Коммутаторы серии Smart II будут классифицировать трафик, предназначенный интерфейсу CPU, и распределять его по 4 очередям. Очередь 0 для ARP-широковещания, очередь 1 для управляющих пакетов от утилиты SmartConsole, очередь 2 для трафика с MAC-адресом назначения, равным MAC-адресу коммутатора, и очередь 3 для всего остального трафика. Для каждой очереди определена фиксированная полоса пропускания к интерфейсу CPU. Таким образом коммутаторы серии Smart II могут предотвратить перегрузку CPU при обработке конкретного типа трафика.
- Коммутаторы серии Smart II, которые поддерживают Safeguard Engine: **DES-1228/A1, DES-1252/A1, DGS-1216T/D1, DGS-1224T/D1 and DGS-1248T/B1.**

Возможные побочные эффекты

- После того как коммутатор переключится в режим exhausted при настроенном строгом режиме, административный доступ к коммутатору будет недоступен, так как в этом режиме отбрасываются все ARP-запросы. В качестве решения можно предложить указать MAC-адрес коммутатора в статической ARP-таблице управляющей рабочей станции, для того чтобы она могла напрямую обратиться к интерфейсу управления коммутатором без отсылки ARP-запроса.
- **Для коммутаторов L2/L3, переход в режим exhausted не будет влиять на коммутацию пакетов на уровне L2.**
- Для коммутатора L3, при переходе в строгий режим exhausted, не только административный доступ будет недоступен, но и связь между подсетями может быть нарушена тоже, поскольку будут отбрасываться ARP-запросы на IP-интерфейсы коммутатора тоже.
- Преимуществом нестрогого режима exhausted является то, что в нём он не просто отбрасываются все ARP-пакеты или пакеты IP-широковещания, а динамически изменяется полоса пропускания для них. Таким образом даже при серьёзной вирусной эпидемии, коммутатор L2/L3 будет доступен по управлению, а коммутатор L3 сможет обеспечивать взаимодействие между подсетями.

Safeguard Engine

IP-адрес коммутатора: 10.31.3.254/8



PC2

IP-адрес PC2: 10.31.3.2/8

1. **PC2 постоянно посылает ARP-пакеты, например со скоростью 1000 пакетов в секунду.**
2. **Загрузка CPU при этом изменяется от нормальной до 100%.**
3. **Если прекратить генерацию ARP пакетов на PC2, загрузка CPU опять станет в пределах нормы.**

Задача: Снизить загрузку CPU при помощи Safeguard Engine.

D-Link
Building Networks for People

Safeguard Engine

Включите Safeguard Engine следующей командой CLI
config safeguard_engine state enable

DES-3526:4#show safeguard_engine
Command: show safeguard_engine

Safe Guard Engine State : Enabled
Safe Guard Engine Current Status : Normal mode
==========
CPU utilization information:
Interval : 5 sec
Rising Threshold(20-100) : 100 %
Falling Threshold(20-100) : 20 %
Trap/Log : Disabled

Следующей командой можно задать пороги переключения режимов
config safeguard_engine cpu_utilization rising_threshold 100 falling_threshold 20

D-Link
Building Networks for People

Safeguard Engine

Результаты теста:

- Перед активацией Safeguard Engine, при генерации PC2 большого количества ARP пакетов, загрузка CPU будет держаться в районе 100%.
- После включения функции Safeguard Engine, PC2 продолжает генерировать большое количество ARP пакетов. Загрузка CPU снизиться до значения нижнего предела и коммутатор будет держать интервал между переключениями 5 секунд (значение по умолчанию).

Вывод:

Функция SafeGuard Engine функционирует следующим образом. При превышении загрузкой CPU верхнего предела, коммутатор отбрасывает все ARP пакеты. При значении загрузки между двумя пределами, коммутатор обрабатывает только ARP пакеты, предназначенные ему. При снижении загрузки ниже нижнего предела коммутатор обрабатывает все ARP пакеты.

D-Link
Building Networks for People

DHCP Relay (Option 82) – информация от агента DHCP Relay

D-Link
Building Networks for People

DHCP Relay (Option 82) – информация от агента DHCP Relay

- Option 82 используется Relay Agent (агентом перенаправления запросов) для добавления дополнительной информации в DHCP – запрос клиента. Эта информация может быть использована для применения политик, направленных на увеличение уровня безопасности и эффективности сети.

- Она описана в стандарте RFC 3046.

Когда вы включаете опцию DHCP relay agent option 82 на коммутаторе D-link, происходит следующее:

- Компьютер в сети (DHCP - клиент) генерирует DHCP - запросы и широковещательно рассылает их в сеть.

- Коммутатор (DHCP Relay Agent) перехватывает DHCP - запрос packet и добавляет в него информацию relay agent information option (option 82). Эта информация содержит MAC – адрес коммутатора (поле опции **remote ID**) и SNMP ifindex порта, с которого получен запрос (поле опции **circuit ID**).

- Коммутатор перенаправляет DHCP – запрос с полями опции option-82 на DHCP - сервер.

- DHCP – сервер получает пакет. Если сервер поддерживает опцию option-82, он может использовать поля remote ID и/или circuit ID для назначения IP-адреса и применения политик, таких как ограничения количества IP-адресов, выдаваемых одному remote ID или circuit ID. Затем DHCP – сервер копирует поле опции option-82 в DHCP - ответе.
  - Если сервер не поддерживает option 82, он игнорирует поля этой опции и не отсылает их в ответе.

- DHCP - сервер отвечает в Unicast-е агенту перенаправления запросов. Агент проверяет предназначен ли он его клиенту, путём анализа IP – адреса назначения пакета.

- Агент удаляет поля опции option-82 и направляет пакет на порт, к которому подключён DHCP - клиент, пославший пакет DHCP – запроса.

D-Link
Building Networks for People

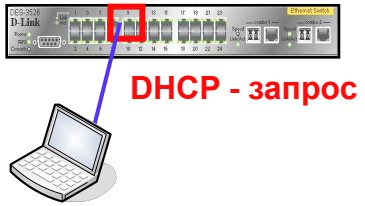
Формат полей опции DHCP option 82 специализированного DHCP Relay Agent-a

Поле опции DHCP option 82 DES-3526/DES-3550 имеет следующий формат :

Формат поля опции Circuit ID:

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	Module	Port
1 байт	1 байт	1 байт	1 байт	2 байта	1 байт	1 байт

1. Тип подопции
2. Длина: длина поля с октета 3 по октет 7
3. Тип Circuit ID
4. Длина: длина поля с октета 5 по октет 7
5. VLAN: номер VLAN ID в DHCP – пакете клиент.
6. Модуль: Для отдельно стоящего коммутатора, поле Модуль всегда равно 0; Для коммутатора в стеке, поле Модуль это Unit ID.
7. Порт: номер порта, с которого получен DHCP - запрос, номер порта начинается с 1.



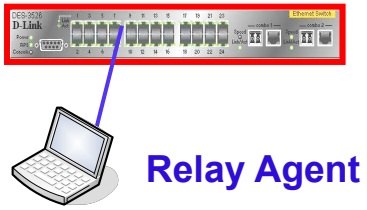
С какого порта получен DHCP - запрос

Локальный идентификатор агента, который получил DHCP – пакет от клиента.

Формат поля опции Remote ID:

1.	2.	3.	4.	5.
2	8	0	6	MAC address
1 байт	1 байт	1 байт	1 байт	6 байт

1. Тип подопции
2. Длина
3. Тип Remote ID
4. Длина
5. MAC-адрес: MAC-адрес коммутатора.



Для идентификации удалённого узла. DHCP – сервер может использовать эту опцию для выбора специфических параметров пользователей, узлов. Поле remote ID должно быть уникально в сети.

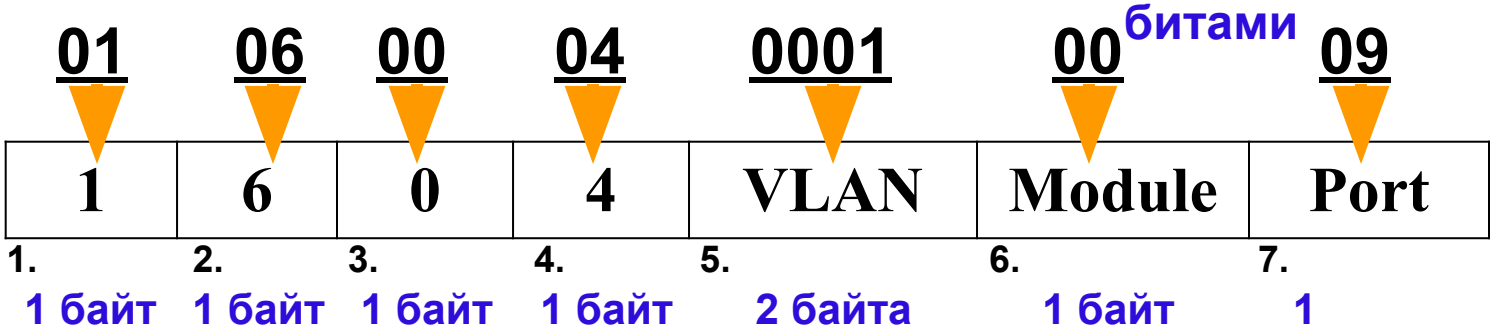
D-Link
Building Networks for People

Формат поля опции Circuit ID

9 = 1001 4 бита

Circuit ID 010600040001 0009

Шестнадцатиричный формат: Каждая цифра представлена четырьмя битами



1. Тип подопции 01 (подопция Agent Circuit ID)
2. Длина 06
3. Тип Circuit ID 00
4. Длина 04
5. VLAN: VLAN ID в DHCP – пакете клиента. 0001
6. Модуль: Для отдельно стоящего коммутатора, поле Модуль всегда равно 0; Для коммутатора в стеке, поле Модуль это Unit ID. 00
7. Порт: номер порта, с которого получен DHCP – пакет клиента, номер порта начинается с 1. 09

D-Link
Building Networks for People

Формат поля опции Remote ID:

Remote ID ▶ **02080006000F3D849FFF**

02 08 00 06 0080c835260a

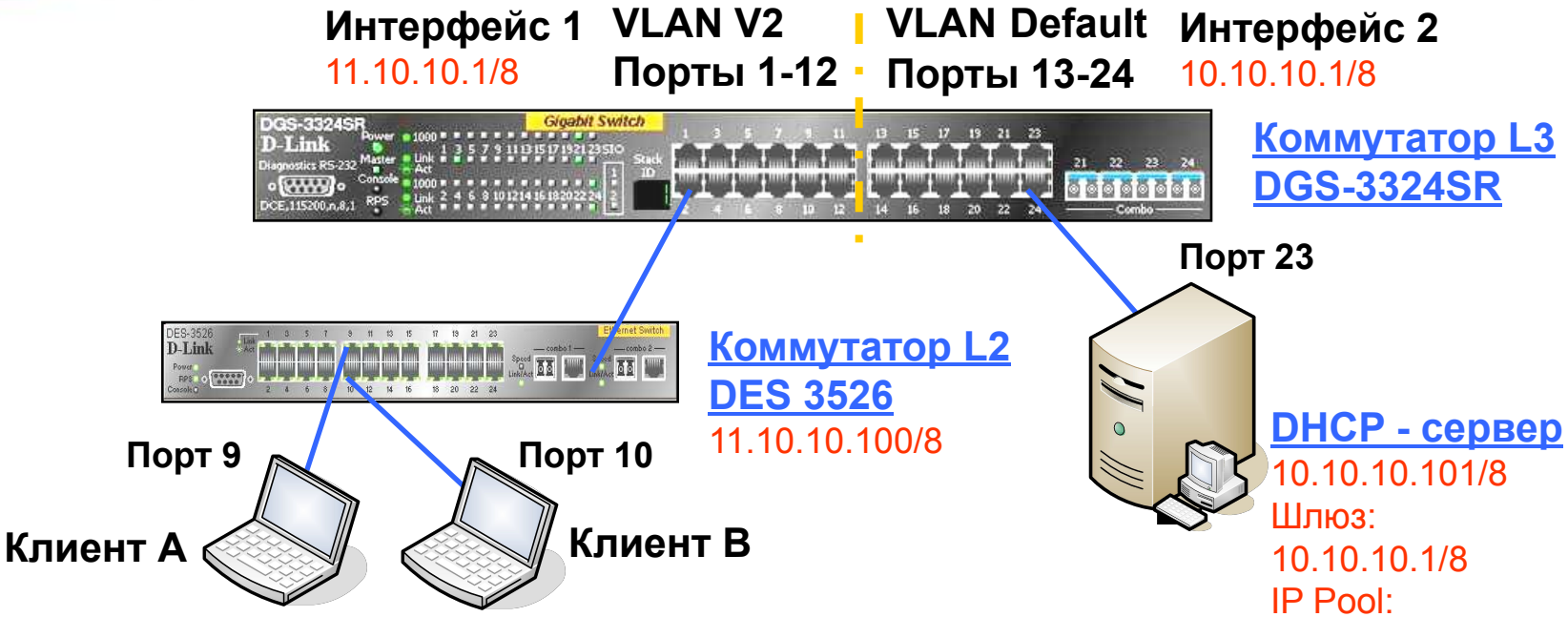
1. Тип подопции 02 (подопция Agent Remote ID)
2. Длина 08
3. Тип Remote ID 00
4. Длина 06
5. MAC-адрес : MAC-адрес коммутатора. 0080C835260A

Circuit ID
(0106)000400010009
+
(0208)00060080c835260a
Remote ID

▶ **000400010009000600 80c835260a**

DHCP – сервер назначит определённый IP-адрес, исходя из этой информации

Пример настройки Option 82



Устройства:

1. DHCP - сервер 10.10.10.101 в подсети 10.0.0.0/8
2. Маршрутизатор или коммутатор L3, выступающий в роли шлюза для 2-ух подсетей
   10.10.10.1 в подсети 10.0.0.0/8
   11.10.10.1 в подсети 11.0.0.0/8
1. Коммутатор L2 (DES-3526/DES-3550) выступает в роли DHCP Relay Agent
   11.10.10.100 в подсети 11.0.0.0/8
   MAC – адрес 00-80-C8-35-26-0A
1. 2 ноутбука, выступающих в роли DHCP – клиентов, подключённых к коммутатору L2 - порт 9, порт 10 соответственно

Сервер с поддержкой DHCP Option 82

1. DHCP – сервер использует динамический пул IP-адресов 11.10.10.101 – 11.10.10.200 для назначения IP-адресов любому DHCP – клиенту, запрос от которого будет перенаправлен DHCP Relay Agent-ом 10.10.10.100 (Если DHCP – клиент, подключён к любому порту коммутатора, кроме портов 9 и 10, он получит IP-адрес из пула.)

--- Для обычного DHCP – запроса клиента

1. Когда какой-либо DHCP – клиент подключается к порту 9 коммутатора L2, DHCP – сервер выдаст ему IP-адрес 11.10.10.9; когда DHCP – подключается к порту 10 коммутатора L2, DHCP – сервер выдаст ему IP-адрес 11.10.10.10. (например, DHCP – клиент, подключённый к порту 9 коммутатора, получит IP-адрес 11.10.10.9)

--- Для DHCP – запросов клиента с option 82

D-Link
Building Networks for People

Конфигурация коммутаторов

Настройка коммутатора L3 (DGS-3324SR):

config vlan default delete 1:1-1:12
create vlan v2 tag 2
config vlan v2 add untagged 1:1-1:12

Сконфигурируйте и создайте IP-интерфейсы в VLAN 2 и default
config ipif System ipaddress 10.10.10.1/8
create ipif p2 11.10.10.1/8 v2
save

Настройка коммутатора L2 (DES-3526/DES-3550):

Задайте IP-адрес коммутатора
config ipif System ipaddress 11.10.10.100/8
Задайте маршрут по умолчанию
create iproute default 11.10.10.1
Сконфигурируйте DHCP Relay
config dhcp_relay add ipif System 10.10.10.101
config dhcp_relay option_82 state enable
enable dhcp_relay
save

D-Link
Building Networks for People

Настройка DHCP – сервера - 1

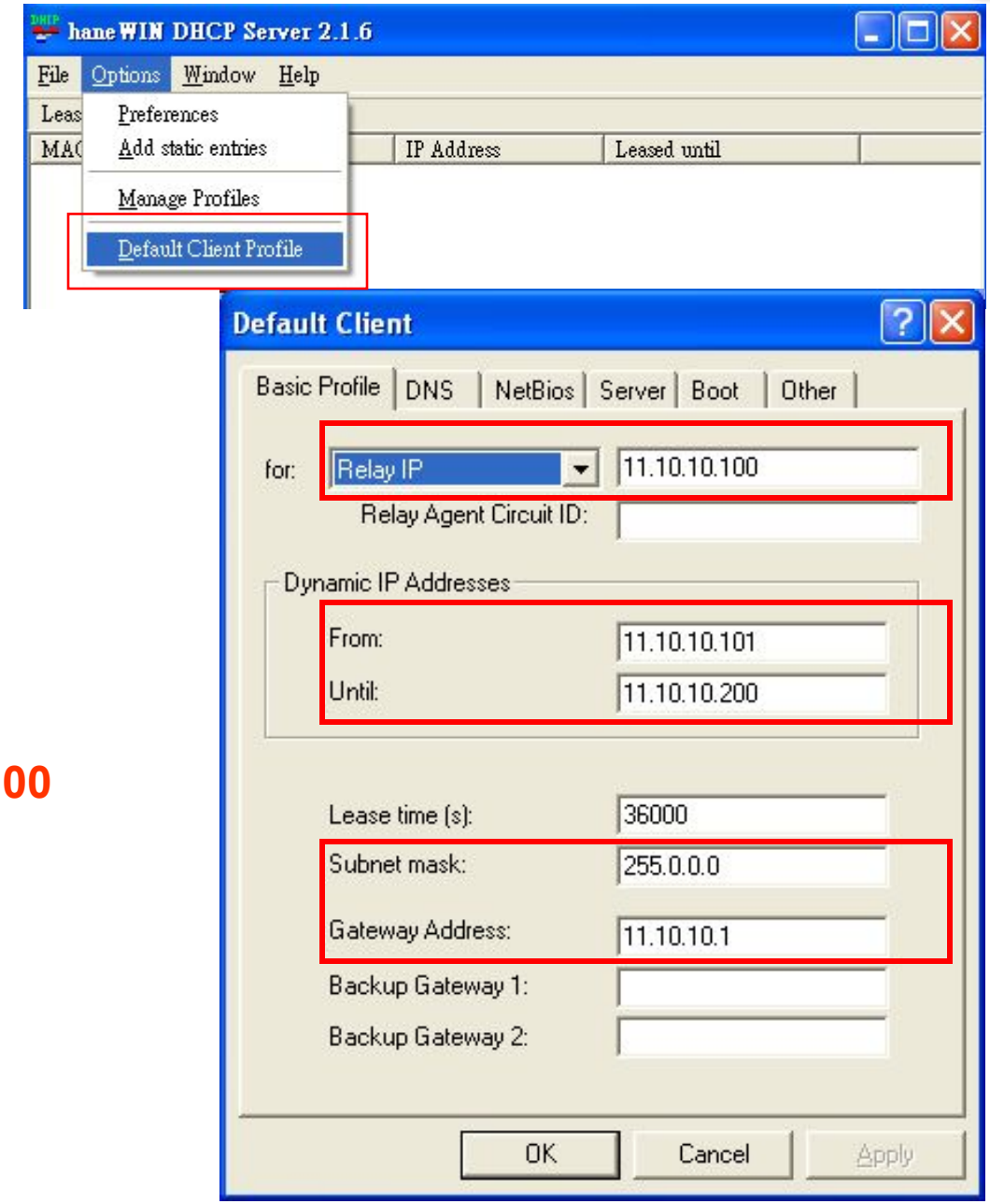
Существует большое количество разных DHCP – серверов, для примера использовался ”haneWIN” DHCP – сервер. (http://www.hanewin.de/homee.htm)

Сконфигурируйте “Basic Profile”

- Relay IP : 11.10.10.100

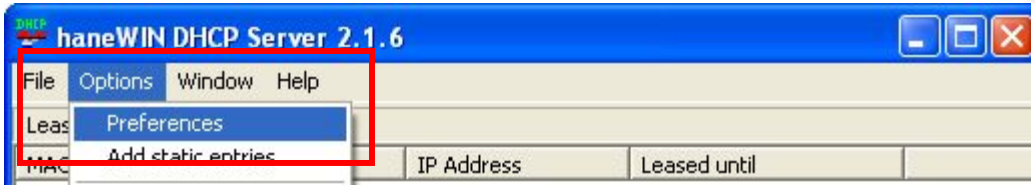
Динамические IP-адреса:

- От **11.10.10.101** до **11.10.10.200**
- Маска подсети: 255.0.0.0
- Адрес шлюза: 11.10.10.1

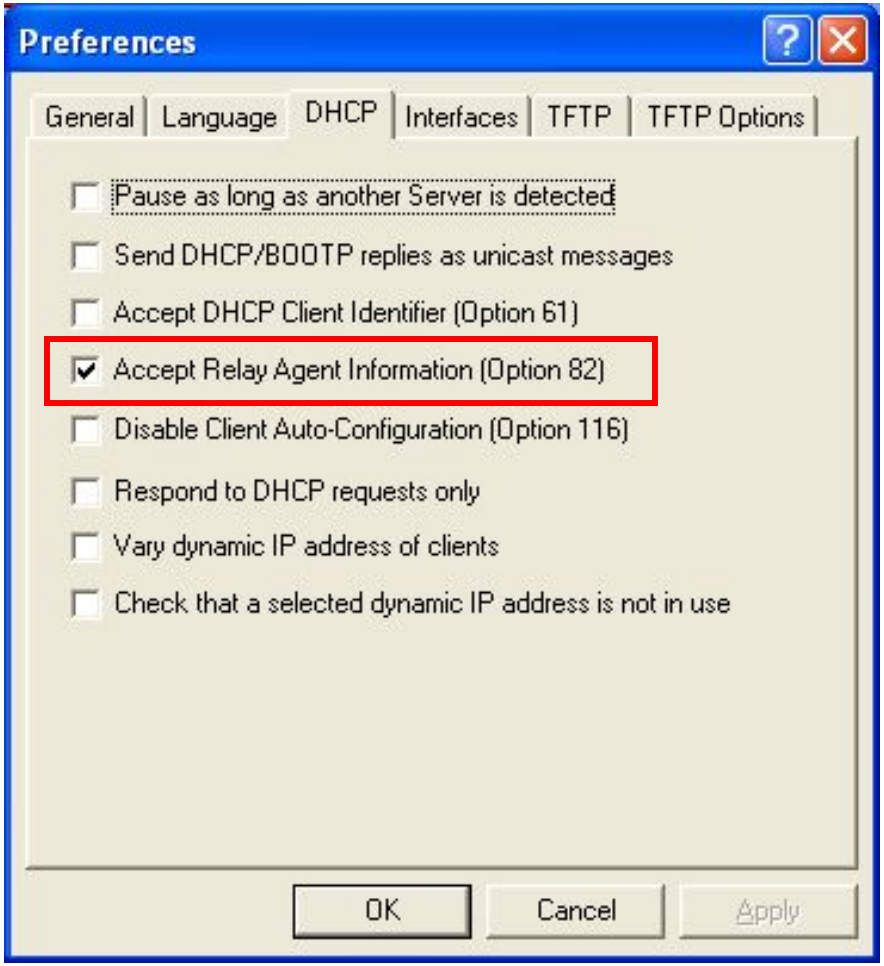


D-Link
Building Networks for People

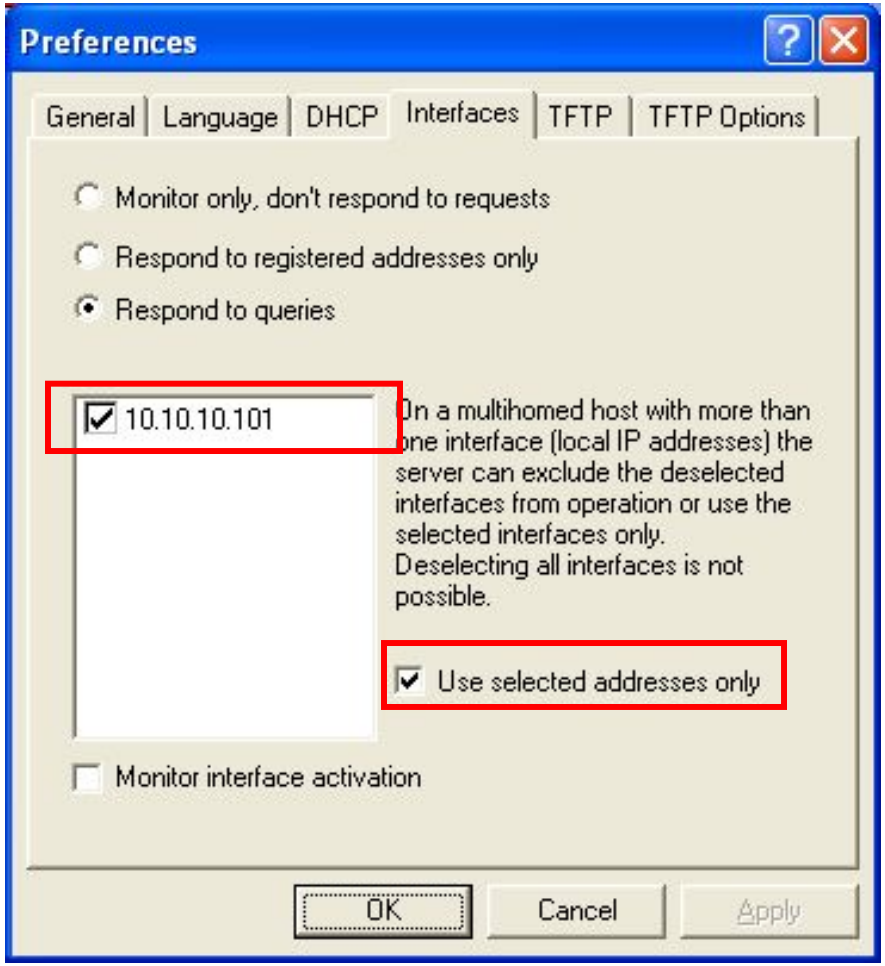
Настройка DHCP – сервера - 2



Опции -> Свойства -> DHCP



Опции -> Свойства -> Интерфейсы



D-Link
Building Networks for People

Настройка DHCP – сервера - 3

Сконфигурируйте DHCP option 82

Назначьте IP-адрес **11.10.10.9** DHCP - клиенту A, подключённому к **порту 9 коммутатора L2**

“Add static entries”

поставьте галочки “Circuit Identifier” и “Remote Identifier”

Hardware Address : 00040001000900060 00F3D849FFF

IP Address : 11.10.10.9

Назначьте IP-адрес **11.10.10.10** DHCP – клиенту B, подключённому к **порту 10 коммутатора L2**

“Add static entries”

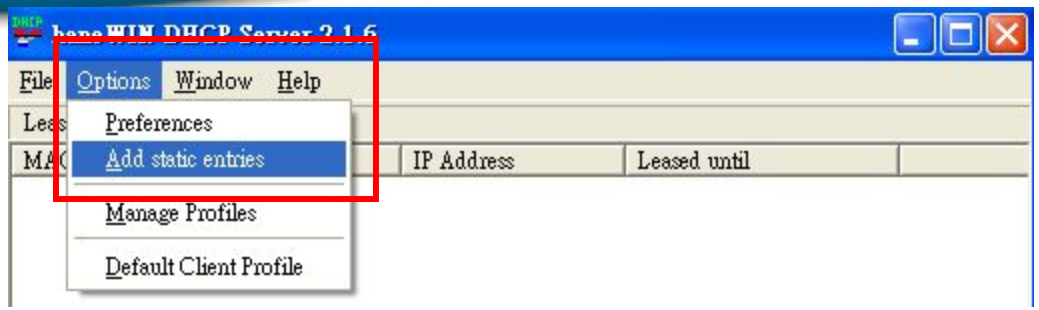
поставьте галочки “Circuit Identifier” и “Remote Identifier”

Hardware Address : 00040001000a0006000F3D849FFF

IP Address : 11.10.10.10

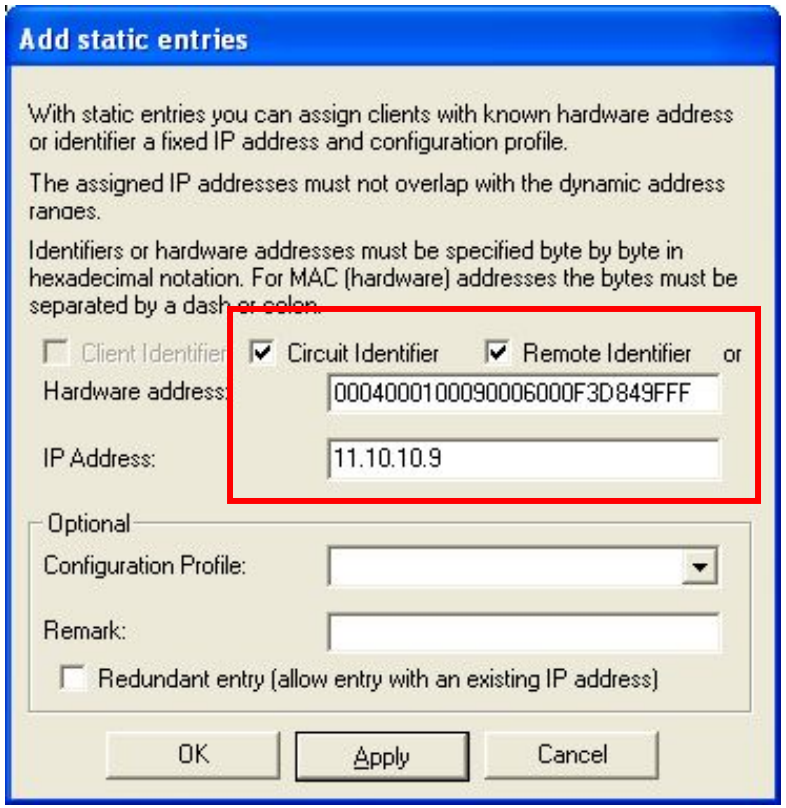
D-Link
Building Networks for People

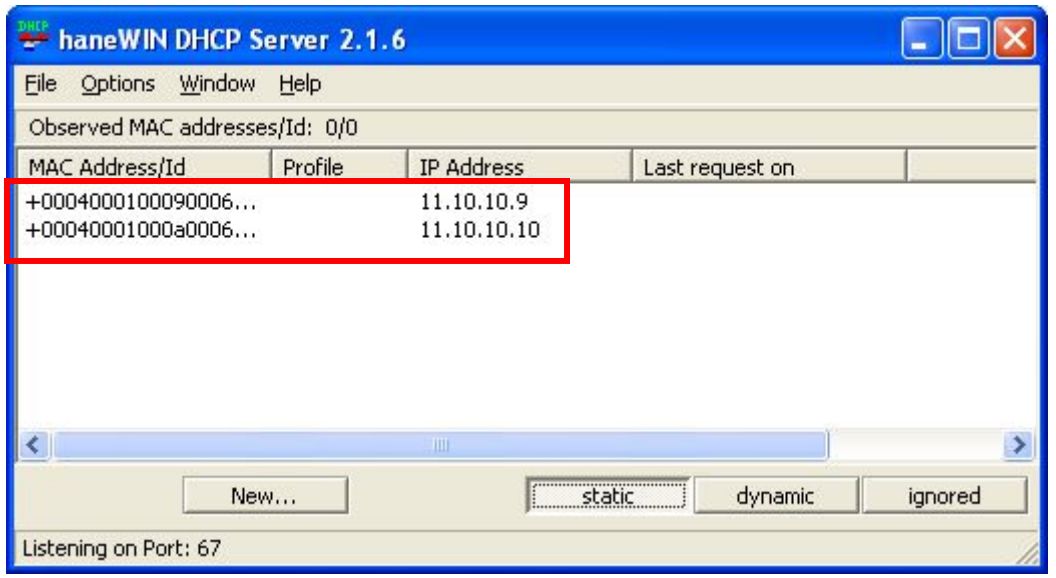
Настройка DHCP – сервера - 4



Опции -> Добавить статические записи

Эти записи на DHCP - сервере





D-Link
Building Networks for People

Информация DHCP Relay Agent (Option 82)

Результаты теста:

1. Клиенту A будет выдан IP-адрес **11.10.10.9**
2. Клиенту B будет выдан IP-адрес **11.10.10.10**

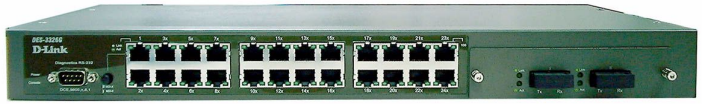
Функции управления и мониторинга

Управление при помощи SNMP

D-View 5.1

IP=10.1.1.2/8
Для чтения = public
Для чтения/записи = private

Что означает
~~1.3.6.1.2.1.1.1~~
1.3.6.1.2.1.1.1 = “Des3226”



IP=10.1.1.1/8
SNMP community String
Для чтения = public
Для чтения/записи = private

Проблемы протокола SNMP версии 1

- Обеспечение безопасности только на основе параметра Community String. Параметр передается в текстовом незашифрованном виде.
- Содержание пакетов SNMP также в виде *plain-text*.
- Если параметр Community String корректен, все дерево MIB может быть просмотрено или изменено.

Решение: SNMP v3

D-Link
Building Networks for People

Новые возможности в SNMPv3

- Обеспечение функций безопасности
  - Шифрация/Дешифрация пакетов
  - Возможность настройки уровня привилегий пользователя
  - SNMP v3 включает следующие 4 модели:
    - MPD(RFC2572)
    - TARGET(RFC2573)
    - USM(RFC2574): User-based Security Model
    - VACM(RFC2575): View-based Access Control Model
- D-View 5.1 поддерживает SNMPv1 и SNMP V3.
- Управляемые устройства D-Link также поддерживают SNMP v1 & V3.

D-Link®
Building Networks for People

Спасибо!