XSTACK

Multiply your potential.

Обзор технологии : IP-MAC-Port Binding

Март 2006

D-Link

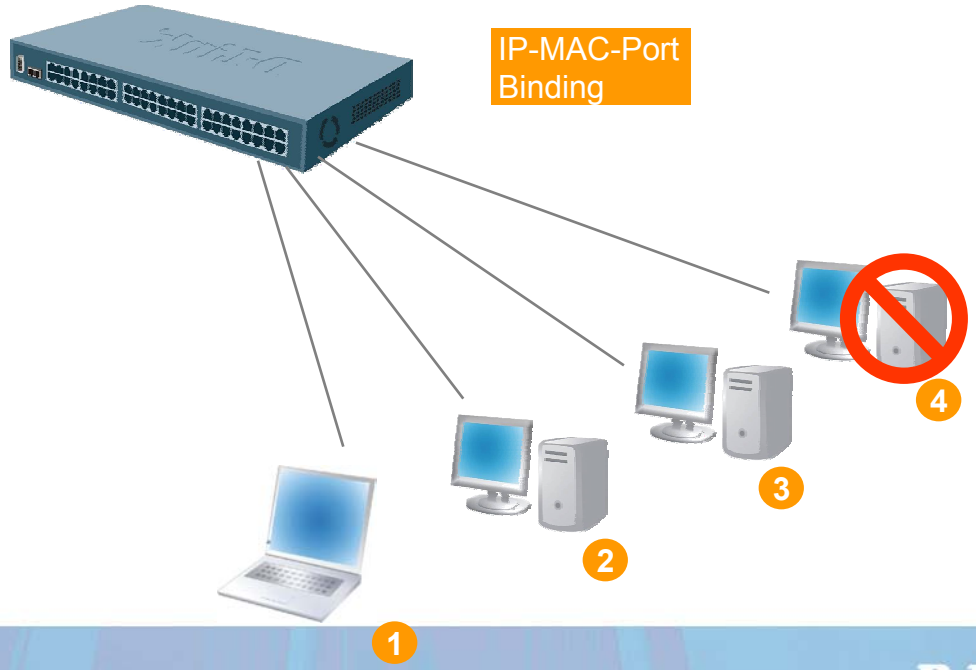
IP-MAC-Port Binding

- **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 !!

Для чего нужна функция IP-MAC-Port binding?

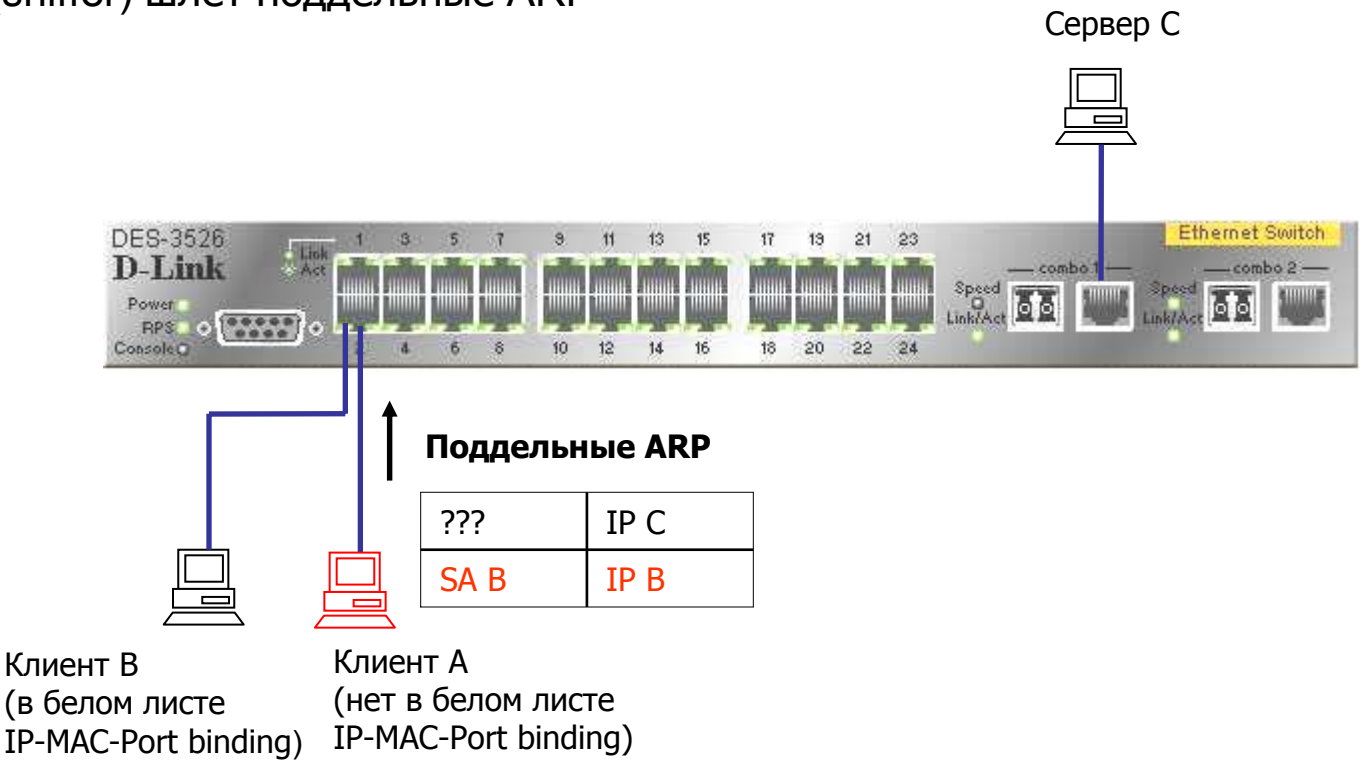
- D-Link расширил популярную функцию IP-MAC binding до более удобной в использовании IP-MAC-Port binding с целью повышения гибкости аутентификации пользователей в сети.
- IP-MAC-Port binding включает два режима работы: ARP (по умолчанию) и ACL.
  Сравнение этих двух режимов показано в таблице ниже:

	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

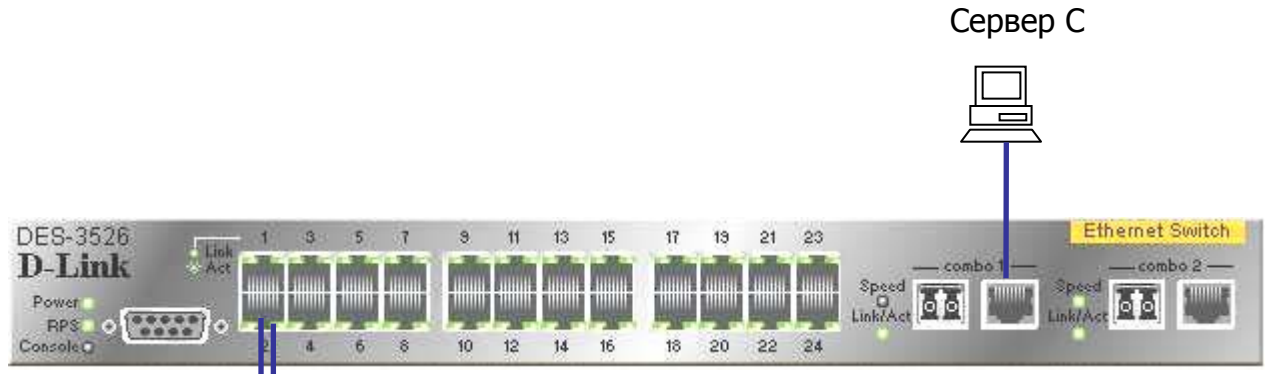
- IP-MAC-Port будет поддерживаться коммутаторами L2 серии xStack - DES-3500 (R4 – ACL Mode), DES-3800 (R3), and DGS-3400 (R2). На данный момент IP-MAC-Port Binding поддерживается коммутатором DES-3526.
- Данный документ описывает примеры настройки IP-MAC-Port binding, например, против атак ARP Poison Routing.

Пример 1. Использование режима ARP или ACL для блокирования снифера

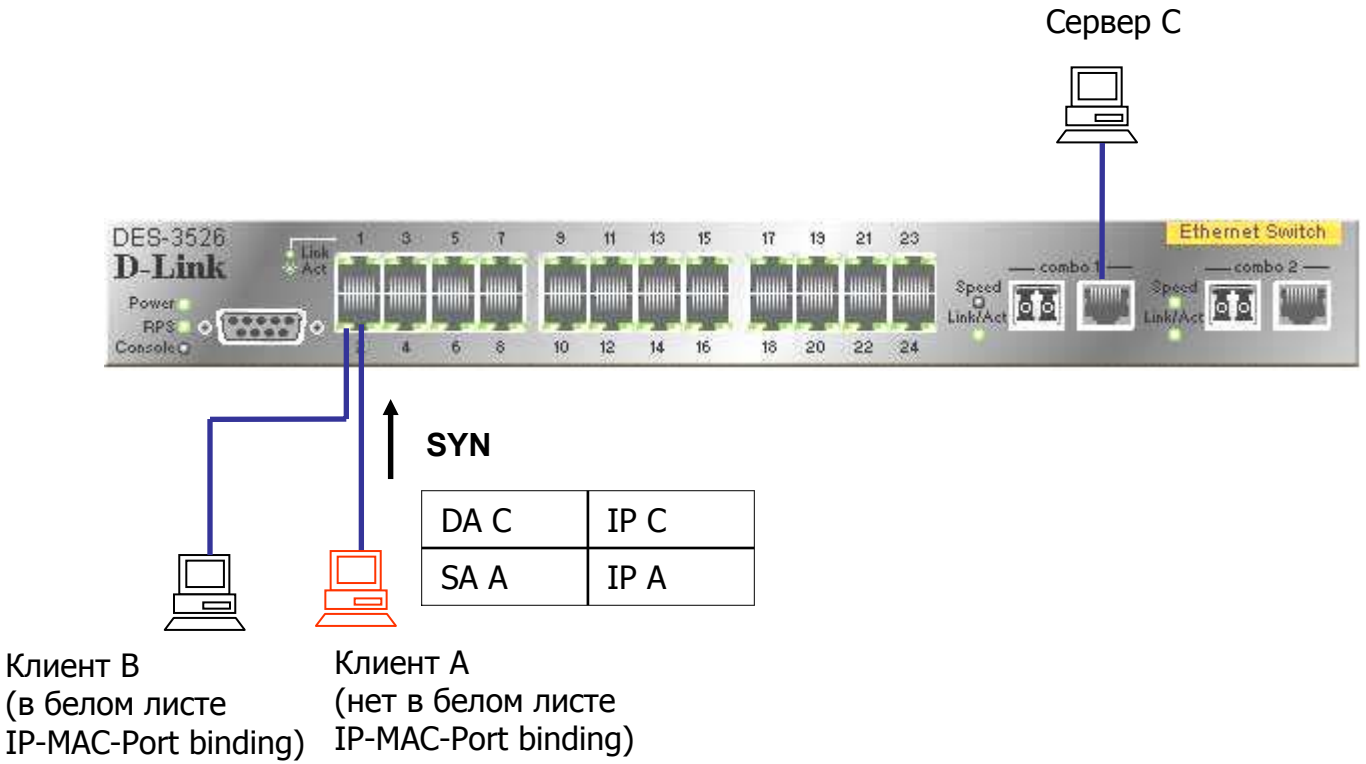
Шаг 1: Клиенты A и B подключены к одному порту коммутатора, клиент A (sniffer) шлет поддельные ARP



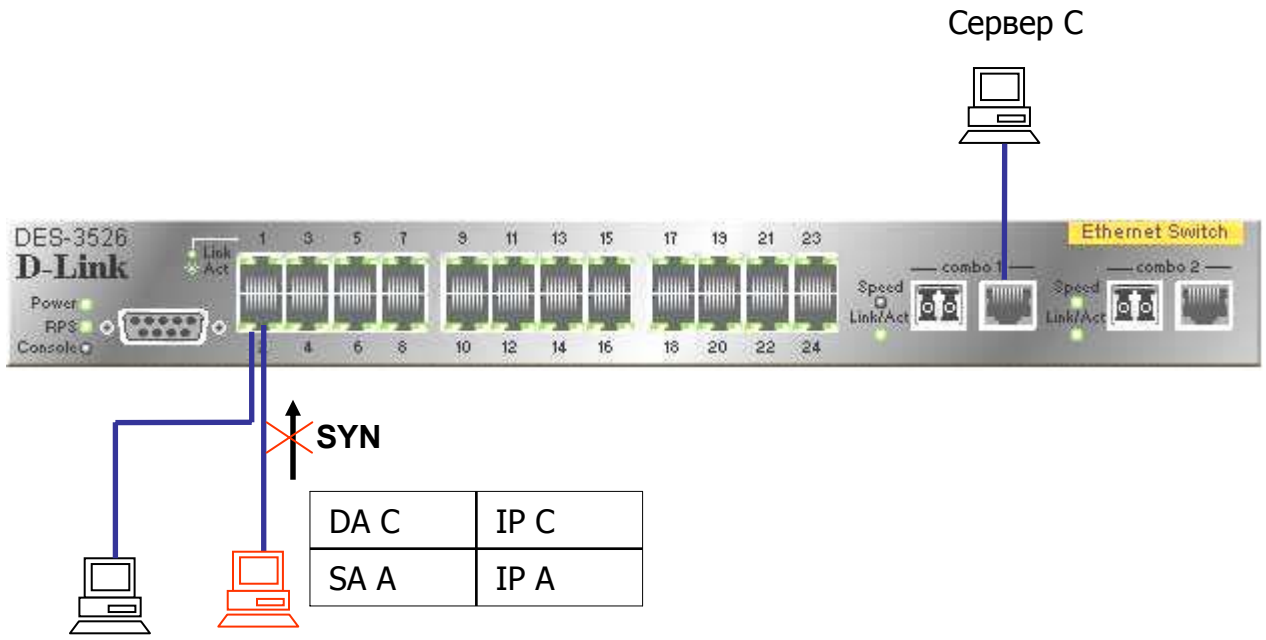
Шаг 2: Сервер C отвечает на запрос и изучает поддельную связку IP/MAC.



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

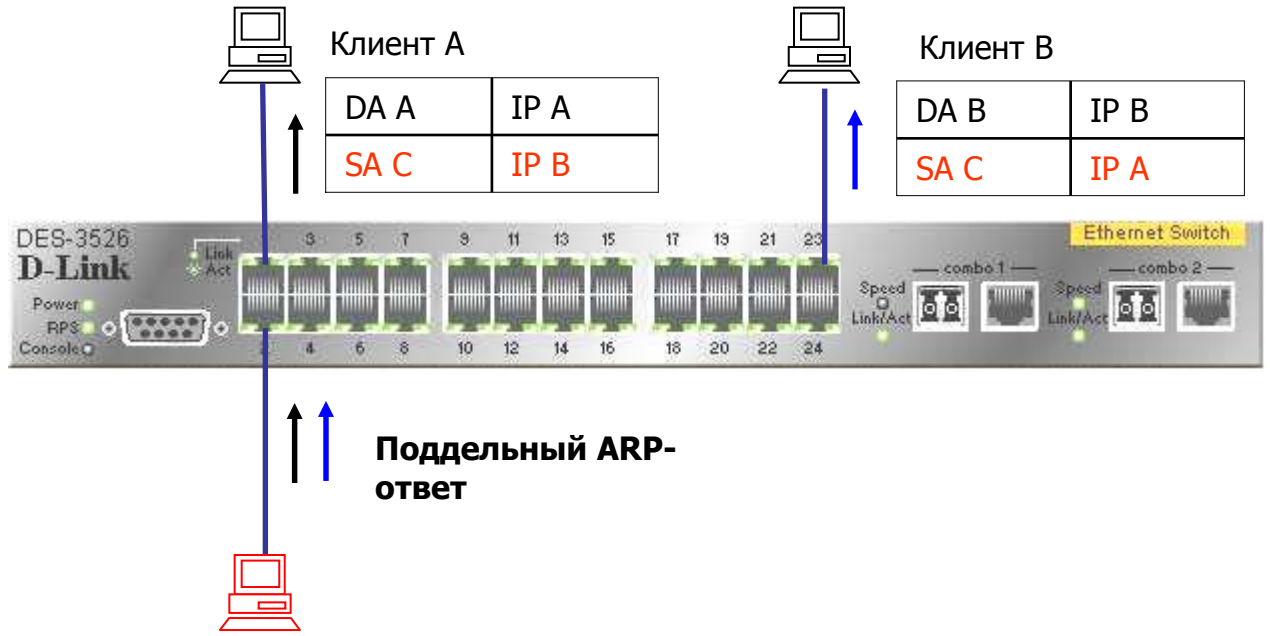


Клиент В
(в белом листе
IP-MAC-Port binding)

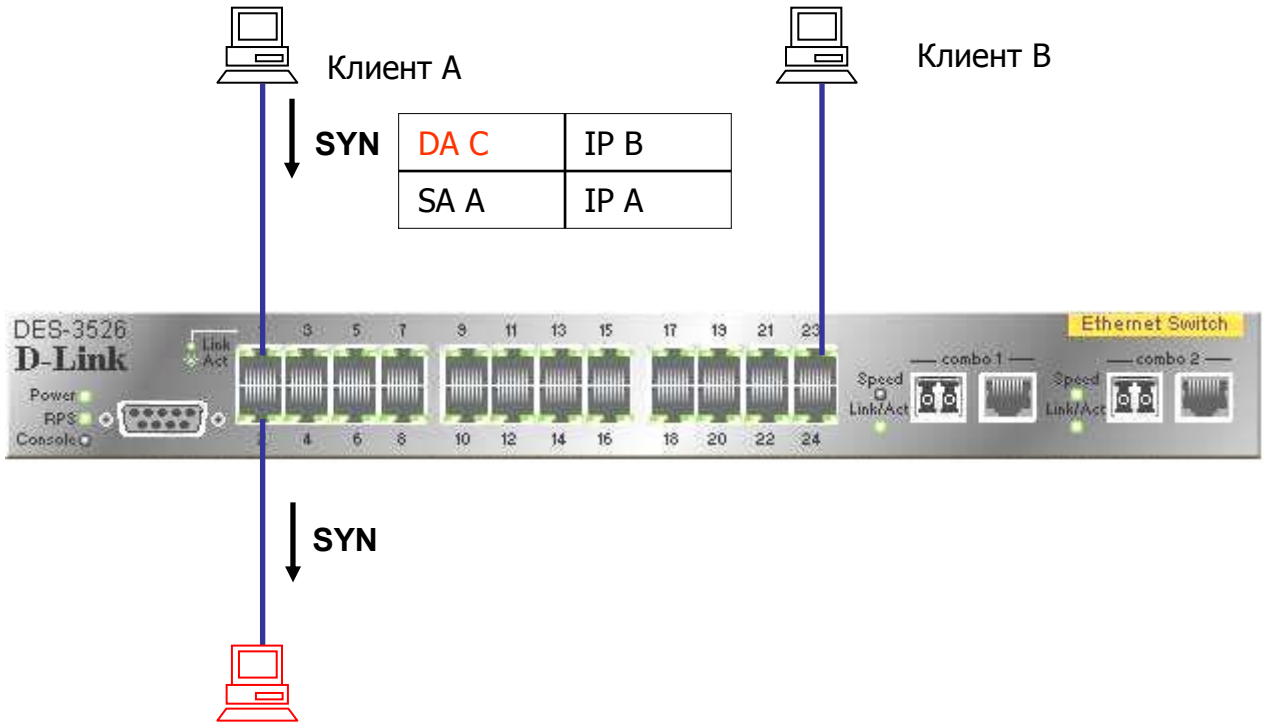
Клиент А
(нет в белом листе
IP-MAC-Port binding)

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

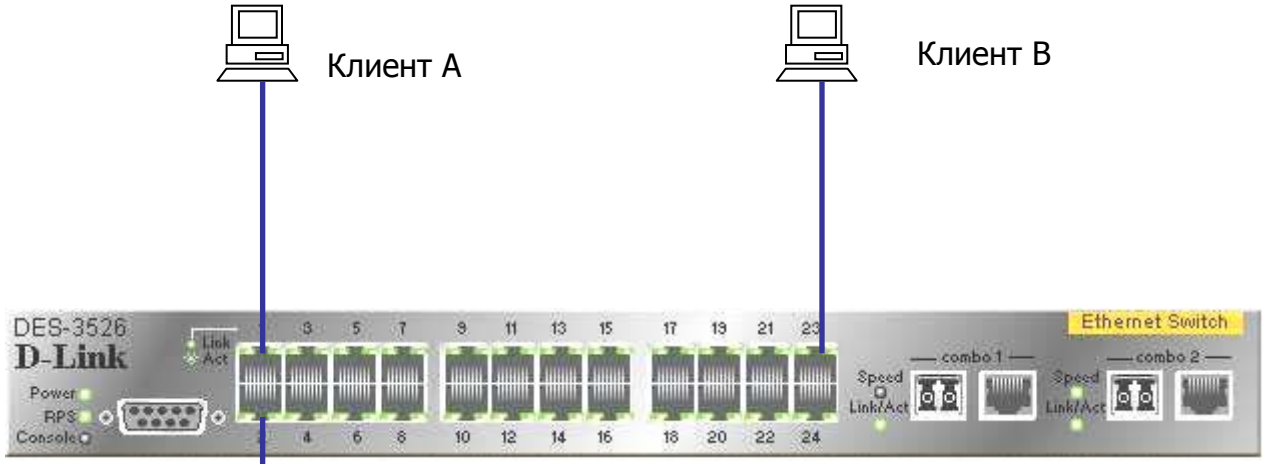


Шаг 2: Клиент A хочет установить TCP соединение с клиентом B



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

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



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

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.

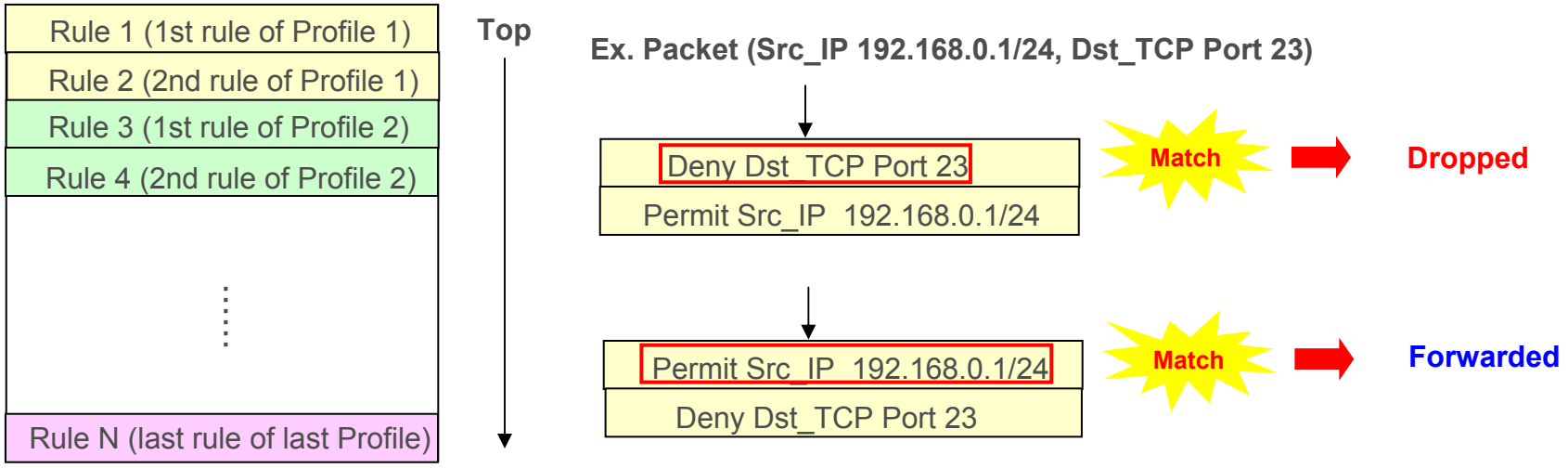


Рисунок 1. Обработка ACL

- 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)

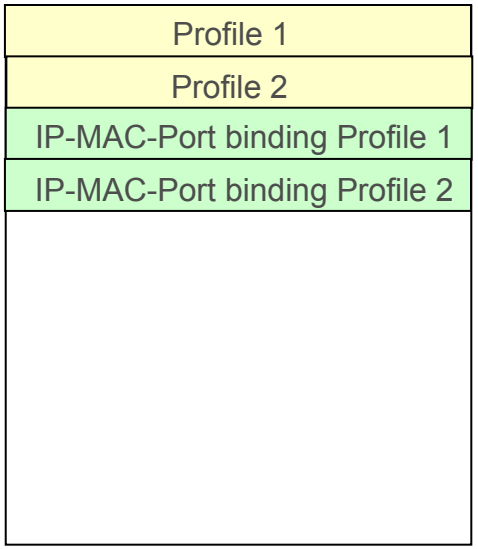


Рисунок 2

Disable

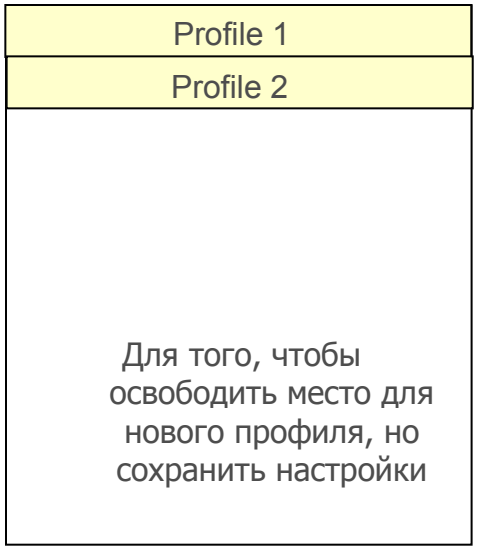


Рисунок 3

Enable

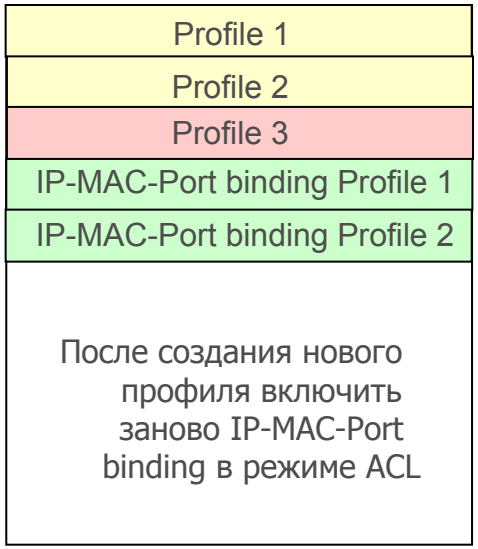


Рисунок 4

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**