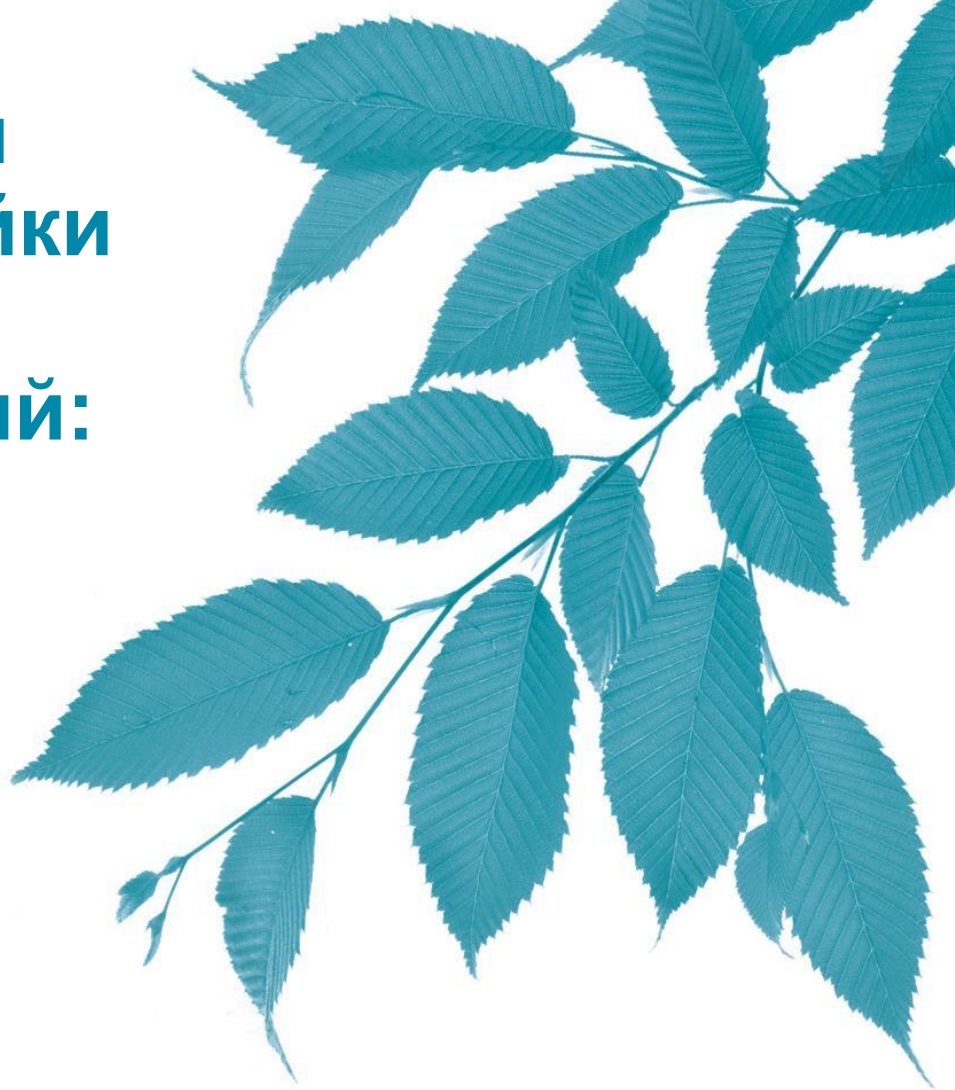
Новый механизм создания и настройки ACL правил на коммутаторах серий:

DES-3200 H/W:C1
DGS-3120-XX
DGS-3420-XX
DGS-3620-XX



Бигаров Руслан, консультант по проектам

e-mail: rbigarov@dlink.ru

D-Link®
Building Networks for People

- Новая архитектура ACL механизма
- Порядок приоритета для каждого профиля
- Параллельный процесс для всех профилей

Новая архитектура ACL механизма

Особенности ACL коммутаторов серии DES-3200 C1

- ✔ Максимально можно создать 4 ACL профиля и 1024 правил для входящего трафика
- ✔ Каждое правило можно привязать к порту или нескольким портам

Особенности профилей

Ethernet профиль:
1. Максимум 3 профиля на коммутатор
2. Максимально 256 правил на профиль

IP профиль:
1. Максимум 3 профиля на коммутатор
2. Максимально 256 правил на профиль

IPv6 профиль:
1. Максимум 2 профиля на коммутатор
2. Максимально 256 правил на профиль

PCF профиль:
1. Максимум 1 профиля на коммутатор
2. Максимально 256 правил на профиль

Системные ACL*

Коммутатор зарезервирует 2 профиля под системные нужды:

1. Ethernet профиль и 62 правила
2. IP профиль и 62 правила

Остальные правила данных профилей будут доступны для настройки и использования.

* Будет реализовано в следующих версиях ПО

Новая архитектура ACL механизма

Особенности ACL коммутаторов других серий

Серия DGS-3120-XX:

1. ACL на вход : максимально 6 профилей и 256 правил на профиль
2. Каждое правило может быть привязано к порту, к нескольким портам или к **VLAN**

Серия DGS-3420-XX:

1. ACL на вход : максимально 6 профилей и 256 правил на профиль
2. ACL на выход : максимально 4 профилей и 128 правил на профиль
3. Каждое правило может быть привязано к порту, к нескольким портам

Серия DGS-3620-XX:

1. ACL на вход : максимально 6 профилей и 256 правил на профиль
2. ACL на выход : максимально 4 профилей и 128 правил на профиль
3. Каждое правило может быть привязано к порту, к нескольким портам

Внимание: Системные правила реализованы отдельно и не используют пользовательские профили и правила!

Порядок приоритета для каждого профиля

Сценарий:

Профиль ID	ACL правило ID	Действие
Profile 1 (IP)	Access ID #5	Drop
	Access ID #22	Replace Priority
Profile 2 (ethernet)	Access ID #1	Replace TOS
	Access ID #200	Mirror
Profile 3 (IPV6)	Access ID #10	Mirror
	Access ID #100	Drop
Profile 4 (IP)	Access ID #2	Replace DSCP
	Access ID #211	Replace DSCP

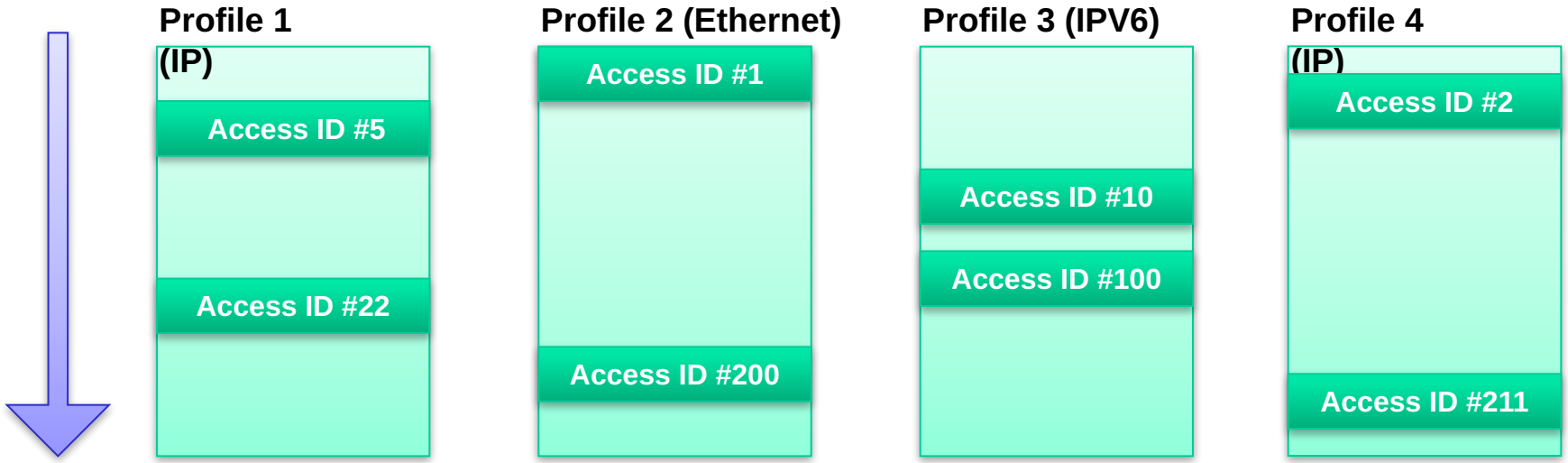
Порядок приоритета для каждого профиля

Порядок приоритета

- В рамках профиля, сопоставление начинается с правила с наименьшим ID (высокий приоритет).
- Однажды найдя сопоставление, коммутатор не продолжает сопоставлять пакет с другими правилами этого профиля.

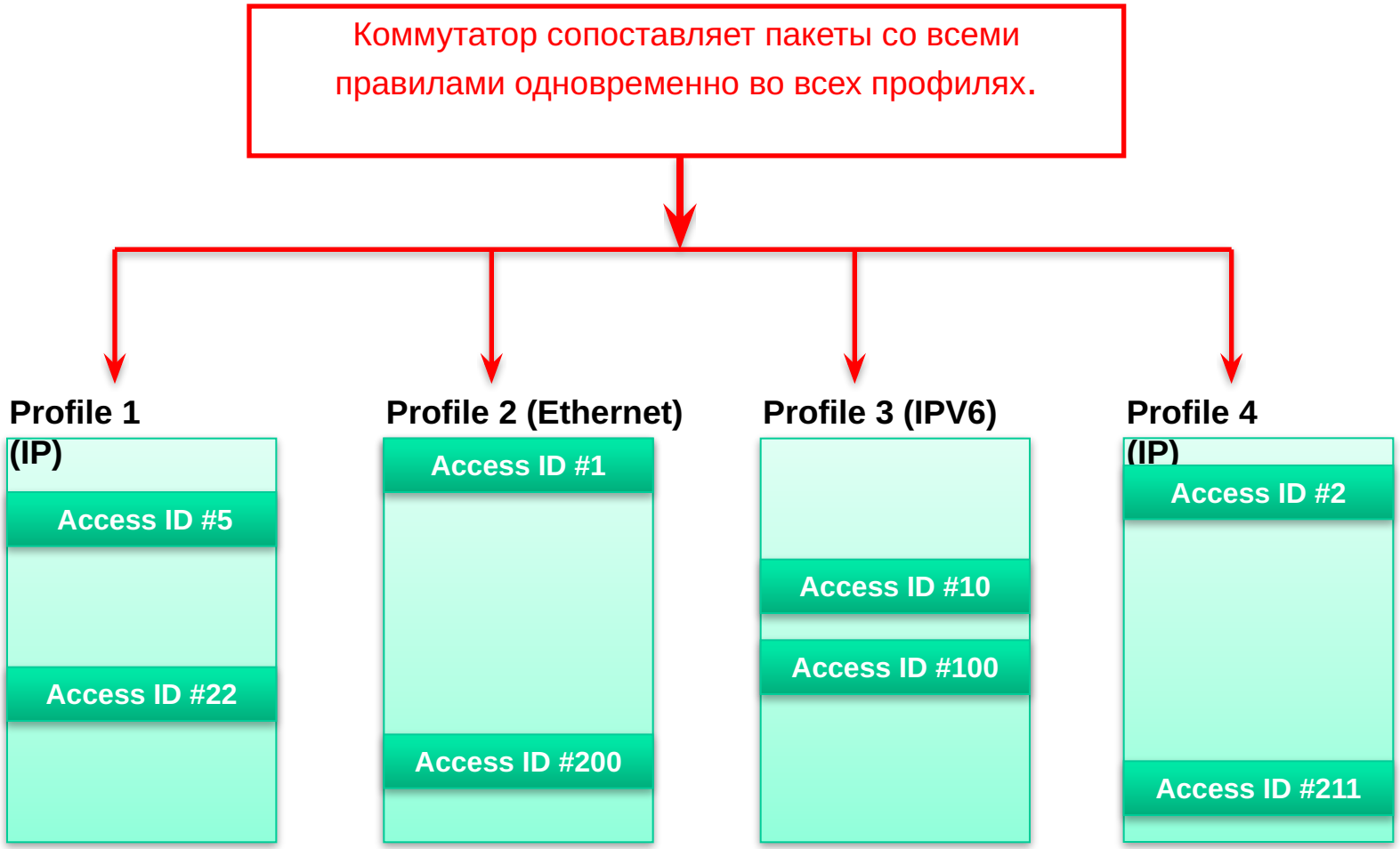
Приоритезация сопоставления в профилях:

B Profile 1 приоритетность: #Access ID 5 > #Access ID 22
B Profile 2 приоритетность: #Access ID 1 > #Access ID 200
B Profile 3 приоритетность: #Access ID 10 > #Access ID 100
B Profile 4 приоритетность: #Access ID 2 > #Access ID 211



Параллельный процесс для всех профилей

Процесс обработки

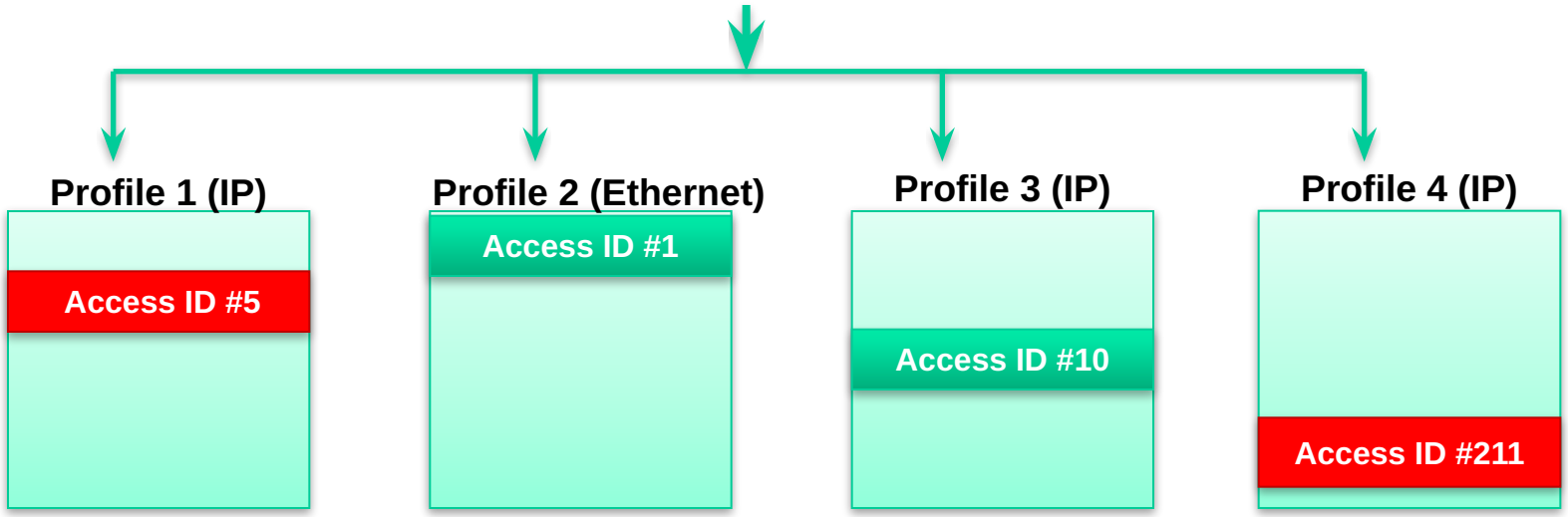


D-Link®
Building Networks for People

Рассмотрение сопоставлений трафика на примерах

- Пример 1 – Неконфликтующие ACL правила в разных профилях
- Пример 2 - Соответствие нескольким правилам ACL в пределах одного профиля
- Пример 3 - Соответствие нескольким правилам ACL нескольких профилей
- Пример 4 - Конфликт правил ACL нескольких профилей

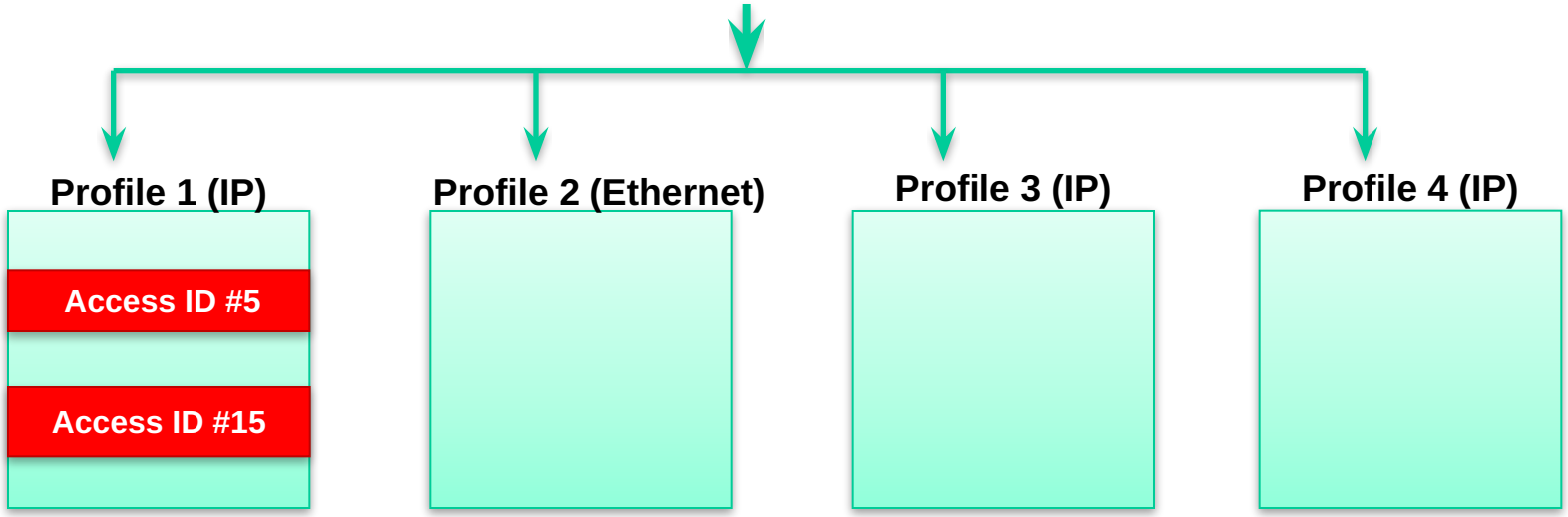
Пример №1 – Неконфликтующие ACL правила в разных профилях



Профиль 1 : Правило ID#5 действие: Replace Priority 5
Профиль 2 : Правило ID#1 действие: Drop
Профиль 3 : Правило ID#10 действие: Replace DSCP 2
Профиль 4 : Правило ID#211 действие: Replace DSCP 3

Если входящий пакет попадает под Профиль 1 - Правилos ID #5 и Профиль 4 - Правило ID #211, тогда финальное действие будет:
Replace Priority 5 и Replace DSCP 3

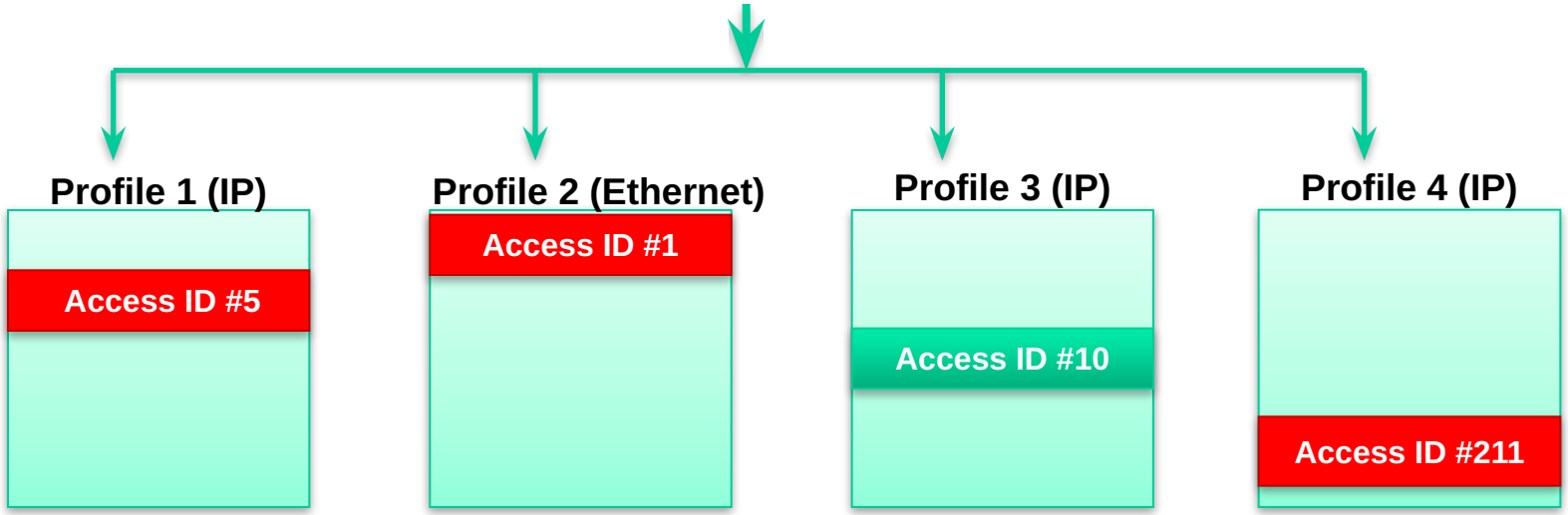
Пример №2 – Соответствие нескольким правилам ACL в пределах одного профиля



Профиль 1 : Правило ID#5 действие: Replace Priority 5
Профиль 1 : Правило ID#15 действие: Replace DSCP 3

Если входящий пакет попадает под Профиль 1 - Правилos ID #5 и Профиль 1 - Правило ID #15, тогда финальное действие будет: **Replace Priority 5**

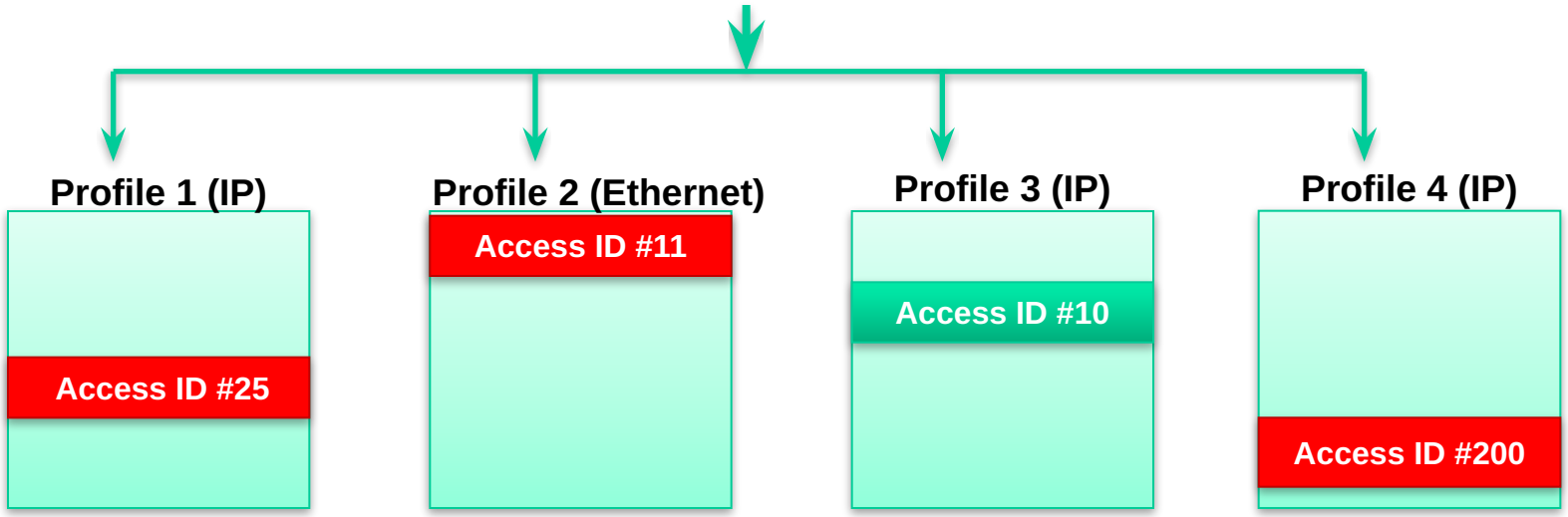
Пример №3 - Соответствие нескольким правилам ACL нескольких профилей



Профиль 1 : Правило ID#5 действие: Replace Priority 5
Профиль 2 : Правило ID#1 действие: Drop
Профиль 3 : Правило ID#10 действие: Replace DSCP 2
Профиль 4 : Правило ID#211 действие: Replace DSCP 3

Если входящий пакет попадает под Профиль 1 - Правилos ID #5 и Профиль 2 - Правилos ID #1 и Профиль 4 - Правило ID #211, тогда финальное действие будет: **Drop**

Пример №4 – Конфликт правил ACL нескольких профилей



Профиль 1 : Правило ID#25 действие: Replace Priority 5
Профиль 2 : Правило ID#11 действие: Drop
Профиль 3 : Правило ID#10 действие: Replace DSCP 4
Профиль 4 : Правило ID#200 действие: Mirror

Если входящий пакет попадает под Профиль 1 - Правилos ID #25 и Профиль 2 - Правилos ID #11 и Профиль 4 - Правило ID #200, тогда финальное действие будет: **Drop и Mirror**

Как переделать ACL правила от DES-3200 B1 для DES-3200 C1

D-Link®
Building Networks for People

Как переделать ACL правила от DES-3200 B1 для DES-3200 C1

Пример:

DES-3200 B1:

```
create access_profile  ip  udp src_port_mask 0xFFFF    profile_id 1
config access_profile profile_id 1  add access_id 1  ip  udp src_port 67  port 25-26 permit
config access_profile profile_id 1  add access_id 2  ip  udp src_port 67  port 1-24 deny
create access_profile  ip  vlan 0xFFF udp src_port_mask 0xFFFF    profile_id 100
config access_profile profile_id 100  add access_id 1  ip  vlan default udp src_port 68  port 1-24 permit priority 6 replace_dscp_with 48
create access_profile  ip  udp dst_port_mask 0xFFFF    profile_id 101
config access_profile profile_id 101  add access_id 1  ip  udp dst_port 53  port 1-26 permit priority 1 replace_dscp_with 10
create access_profile  ip  igmp  profile_id 102
config access_profile profile_id 102  add access_id 1  ip  igmp  port 1-26 permit priority 4 replace_dscp_with 34
```

DES-3200 C1:

```
create access_profile profile_id 1 profile_name ip_profile ip vlan 0xFFF protocol_id_mask 0xFF user_define_mask 0xFFFFFFFF
config access_profile profile_id 1 add access_id 1 ip protocol_id 17 user_define 0x430000 mask 0xFFFF0000 port 25-26 permit
config access_profile profile_id 1 add access_id 2 ip protocol_id 17 user_define 0x430000 mask 0xFFFF0000 port 1-24 deny
config access_profile profile_id 1 add access_id 3 ip vlan default protocol_id 17 user_define 0x440000 mask 0xffff0000 port 1-24 permit priority 6 replace_dscp_with 48
config access_profile profile_id 1 add access_id 4 ip protocol_id 17 user_define 0x35 mask 0xffff port 1-26 permit priority 1 replace_dscp_with 10
config access_profile profile_id 1 add access_id 5 ip protocol_id 2 port 1-26 permit priority 4 replace_dscp_with 34
```

Схемы использования ACL.
Возможная проблема и путь её решения.

D-Link®
Building Networks for People

Схемы использования ACL.

Есть две схемы реализации использования ACL:

- Что не запрещено, то разрешено
- Что не разрешено, то запрещено

“**Что не запрещено, то разрешено**” – в этом случае создаются запрещающие правила для выборочного трафика, все остальное разрешено по умолчанию.

“**Что не разрешено, то запрещено**” – в этом случае создаются разрешающие правила для выборочного трафика, все остальное запрещается последним правилом.

При решении “Что не разрешено, то запрещено.“ для отбрасывания всего остального трафика выборка осуществляется по IP адресу источника с маской 0.0.0.0 или по MAC адресу источника с маской 00-00-00-00-00-00. Все отработает штатно, если задача решена одним профилем. Если используются несколько профилей, то можно столкнуться с особенностью примера №3 “Соответствие нескольким правилам ACL нескольких профилей”, т.е. правило “**deny**” **имеет наибольший приоритет по отношению к остальным**, т.е. будет отбрасываться полезный трафик.

Схемы использования ACL.

Решение:

- DHCP Snooping
- Traffic Control
- Красить трафик метками QoS 802.1p и DSCP
- Отбрасывать выборочный трафик

DHCP Snooping – будет жестко контролировать MAC адрес источника и IP адрес источника в приходящем от клиента трафике, а также защищает от ARP Spoofing атак.

Traffic Control – контролирует Broadcast и Multicast трафик приходящий от клиента.

Раскраска трафика метками QoS 802.1p и DSCP – позволит гарантированно доставлять трафик нужных сервисов: Internet, IPTV, VoIP и т.д.

Отбрасывание выборочного трафика, например: SMB, Src MAC 00-00-00-00-00-00, недействительные DHCP сервера и т.д., поможет разгрузить магистраль от избыточного, ненужного трафика и избежать проблем, связанных с действиями пользователей.

Спасибо за внимание!

Бигаров Руслан, консультант по проектам
e-mail: rbigarov@dlink.ru