QTECH
МИР ДОСТУПНЕЕ

КОНФИГУРАЦИЯ ФУНКЦИЙ БЕЗОПАСНОСТИ

Коммутатор агрегации

СЕРИЯ QSW-8400

www.qtech.ru

Оглавление

1 КОНФИГУРИРОВАНИЕ ACL 4
1.1 Введение в ACL 4
1.1.1 Список доступа 4
1.1.2 Группа доступа 4
1.1.3 Операции списка доступа и глобальные операции, выполняемые по умолчанию 5
1.2 Конфигурация ACL 5
1.2.1 Настройка списка доступа 6
1.2.2 Настройка функции фильтрации пакетов 20
1.2.3 Настройка функции time range (временной диапазон) 21
1.2.4 Привязка списка доступа к конкретному направлению в заданном порту 22
1.2.5 Очистка фильтрующей информации указанного порта 22
1.3 Примеры ACL 23
1.4 Поиск неисправностей ACL 27
2 КОНФИГУРИРОВАНИЕ ПРОТОКОЛА 802.1X 28
2.1 Введение в 802.1x 28
2.2 Настройка протокола 802.1x 30
2.3 Примеры использования протокола 802.1x 33
2.3.1 Пример гостевой VLAN 33
2.3.2 Пример IPv4 RADIUS 36
2.3.3 Пример IPv6 RADIUS 37
2.4 Поиск неисправностей 802.1x 37
3 ОГРАНИЧЕНИЯ ПО MAC- И IP-АДРЕСАМ НА ПОРТУ, КОНФИГУРАЦИЯ VLAN 39
3.1 Общие сведения 39
3.2 Конфигурация количества ограничений MAC и IP-адресов на портах и VLAN 40
3.3 Примеры ограничения MAC и IP-адресов на порту и на VLAN 43
3.4 Поиск неисправностей в функциях ограничения MAC, ARP и ND 43
4 КОНФИГУРИРОВАНИЕ ФУНКЦИИ AM 45
4.1 Введение в функцию AM 45
4.2 Настройка функции AM 45
4.3 Пример использования функции AM 47
4.4 Поиск неисправностей функции AM 48
5 КОНФИГУРИРОВАНИЕ TACACS+ 49
5.1 Введение в TACACS+ 49
5.2 Настройка TACACS+ 49

5.3 Пример использования TACACS+ 50
5.4 Поиск неисправностей TACACS+ 51
6 КОНФИГУРИРОВАНИЕ RADIUS 52
6.1 Введение в RADIUS и принцип AAA 52
6.2 Структура сообщений RADIUS 52
6.3 Настройка RADIUS 55
6.4 Пример использования RADIUS 57
6.4.1 Пример IPv4 RADIUS 57
6.4.2 Пример IPv6 RADIUS 58
6.5 Поиск неисправностей RADIUS 58
7 КОНФИГУРИРОВАНИЕ ФУНКЦИИ RA SECURITY 60
7.1 Введение в RA Security 60
7.2 Настройка RA Security 60
7.3 Пример использования RA Security 61
7.4 Поиск неисправностей RA Security 62
8 КОНФИГУРИРОВАНИЕ VLAN-ACL 63
8.1 Введение в VLAN-ACL 63
8.2 Настройка VLAN-ACL 63
8.3 Пример использования VLAN-ACL 65
8.4 Поиск неисправностей VLAN-ACL 66
9 КОНФИГУРИРОВАНИЕ MAB 67
9.1 Введение в MAB 67
9.2 Настройка MAB 67
9.3 Пример использования MAB 69
9.4 Поиск неисправностей MAB 71

1 КОНФИГУРИРОВАНИЕ ACL

1.1 Введение в ACL

Списки управления доступом ACL (Access Control List) — это механизм фильтрации пакетов, используемый коммутатором для управления сетевым трафиком путем разрешения или запрета прохождения его через коммутатор, что значительно повышает безопасность сети. Пользователь может задать набор правил обработки пакетов, несущих ту или иную конкретную информацию, в каждом правиле указаны операции (разрешить или запретить прохождение пакета), которые необходимо применить, если обнаружено, что пакет содержит соответствующую информацию. Пользователь может применять эти правила к входящим и исходящим потокам портов, при этом потоки данных соответствующих направлений в заданном порту будут удовлетворять назначенным для них правилам ACL.

1.1.1 Список доступа

Список доступа — это последовательность условий, соответствующих конкретному правилу. Каждое правило содержит фильтрующую информацию и выполняемую операцию. Информация правила представляет собой комбинацию условий воздействия, например, IP-адреса источника и назначения, номер IP-протокола и TCP порта. Списки доступа могут быть классифицированы по следующим критериям:

- Критерий на основе фильтрующей информации: Список доступа по IP-адресам (информация уровня 3 и более высоких уровней), список доступа по MAC-адресам (информация уровня 2), список доступа на основе MAC- IP- адресов (уровни 2 или 3, либо более высокие уровни).
- Критерий сложности настройки: стандартная, расширенная настройка. При расширенной настройке применяется более специфическая фильтрующая информация.
- Критерий на основе номенклатуры: По номерам, по именам.

В содержании списка доступа должны быть отражены три аспекта, перечисленные выше.

1.1.2 Группа доступа

Когда набор списков доступа создан, они могут быть применены к трафику любых направлений во всех портах. Группа доступа — это описание привязки списка доступа к тому или иному направлению в заданном порту. Когда группа доступа создана, все пакеты указанного направления, проходящие через порт, будут проверяться на согласование с правилом доступа. По результатам согласования будет приниматься решение — разрешить или запретить доступ.

Текущая версия прошивки поддерживает только входящие листы доступа.

1.1.3 Операции списка доступа и глобальные операции, выполняемые по умолчанию

Имеется всего две операции списков доступа (они же являются операциями, назначенными по умолчанию): “permit” (разрешить) и “deny” (запретить). Применяются следующие правила:

- Список доступа может содержать несколько правил. При фильтрации пакеты проверяются на соответствие условиям правил, начиная с первого. Если при проверке определенного правила достигается соответствие, остальные правила не обрабатываются, они игнорируются.
- Операции, определенные глобально, применяются в портах только к входящим IP-пакетам. Для IP-пакетов, не являющихся входящими, а также для всех исходящих пакетов, операцией, назначенной по умолчанию, является “permit”.
- Глобальная операция, назначенная по умолчанию, применяется только в том случае, когда в порту включен фильтр пакетов и нет списка доступа ACL либо других привязок ACL, ограничивающих доступ к порту.

1.2 Конфигурация ACL

Порядок действий конфигурации следующий:

Настройка списка доступа

1. Настройка стандартного нумерованного списка доступа для IP-адресов
2. Настройка расширенного нумерованного списка доступа для IP-адресов
3. Настройка стандартного нумерованного списка доступа для IP-адресов по номенклатуре
   a) Создание стандартного нумерованного списка доступа для IP-адресов по номенклатуре
   b) Указание операций «permit» или «deny» для правила
   c) Выход из режима настройки списков доступа ACL
4. Настройка расширенного нумерованного списка доступа для IP-адресов по номенклатуре
   a) Создание расширенного нумерованного списка доступа для IP-адресов по номенклатуре
   b) Указание операций «permit» или «deny» для правила
   c) Выход из режима настройки списков доступа ACL
5. Настройка стандартного нумерованного списка доступа для MAC-адресов
6. Настройка расширенного нумерованного списка доступа для MAC-адресов
7. Настройка расширенного нумерованного списка доступа для MAC-адресов по номенклатуре
   a) Создание расширенного нумерованного списка доступа для MAC-адресов по номенклатуре
   b) Указание операций «permit» или «deny» для правила
   c) Выход из режима настройки списков доступа ACL
8. Настройка расширенного нумерованного списка доступа для MAC-IP-адресов

9. Настройка расширенного нумерованного списка доступа для MAC-IP-адресов по номенклатуре
   a) Создание расширенного нумерованного списка доступа для MAC-IP-адресов в по номенклатуре
   b) Указание операций «permit» или «deny» для правила
   c) Выход из режима настройки списков доступа по MAC-IP-адресам
10. Настройка стандартного нумерованного IPv6 списка доступа
11. Настройка расширенного нумерованного IPv6 списка доступа
12. Настройка стандартного IPv6 листа доступа, основанного на номенклатуре
    a) Создание стандартного IPv6 листа доступа, основанного на номенклатуре
    b) Определение множественного доступа или правил запрета
    c) Выход из режима конфигурации ACL
13. Настройка расширенного IPv6 листа доступа, основанного на номенклатуре
    a) Создание расширенного IPv6 листа доступа, основанного на номенклатуре
    b) Определение множественного доступа или правил запрета
    c) Выход из режима конфигурации ACL

Настройка функции фильтрации пакетов

1. Включение функции фильтрации пакетов в глобальном режиме конфигурирования
2. Настройка операции, выполняемой по умолчанию

Настройка функции time range (временной диапазон)

1. Создание имени временного диапазона
2. Настройка периодичности временного диапазона
3. Настройка абсолютного временного диапазона

Привязка списка доступа к конкретному направлению в заданном порту

Очистка фильтрующей информации указанного порта

1.2.1 Настройка списка доступа

1. Настройка стандартного нумерованного списка доступа для IP-адресов.

Команда	Описание
Общий режим	
access-list *<num>* {deny | permit} {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} **no access-list *<num>***	Позволяет создать стандартный нумерованный список доступа для IP-адресов. Если список доступа уже существует, в него будет добавлено правило. Команда no удаляет стандартный нумерованный список доступа для IP-адресов.

2. Настройка расширенного нумерованного списка доступа для IP-адресов.

Команда	Описание
Общий режим	
access-list *<num>* {deny | permit} icmp {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr>* *<dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<icmp-type>* [*<icmp-code>*]] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]	Позволяет создать расширенное нумерованное ICMP-правило доступа для IP-адресов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в команде.
access-list *<num>* {deny | permit} igmp {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr>* *<dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<igmp-type>*] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]	Позволяет создать расширенное нумерованное IGMP-правило доступа для IP-адресов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в команде
access-list *<num>* {deny | permit} tcp {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} [s-port {*<sPort>* | range *<sPortMin>* *<sPortMax>*}] {{*<dIpAddr>* *<dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [d-port {*<dPort>* | range *<dPortMin>* *<dPortMax>*}] [ack+fin+psh+rst+urg+syn] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]	Позволяет создать расширенное нумерованное TCP-правило доступа для IP-адресов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в команде.
access-list *<num>* {deny | permit} udp {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} [s-port {*<sPort>* | range *<sPortMin>* *<sPortMax>*}] {{*<dIpAddr>* *<dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [d-port {*<dPort>* | range *<dPortMin>* *<dPortMax>*}] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]	Позволяет создать расширенное нумерованное UDP-правило доступа для IP-адресов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в команде.
access-list *<num>* {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | *<protocol-num>*} {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr>* *<dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [precedence *<prec>*] [tos *<tos>*][time-range*<time-*	Позволяет создать расширенное нумерованное IP-правило доступа для IP-адресов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в

***range-name>*]**	команде.
no access-list *<num>*	Удаляет расширенный нумерованный список доступа для IP-адресов.

3. Настройка стандартного нумерованного списка доступа для IP-адресов по номенклатуре:
   a) Создание стандартного нумерованного списка доступа для IP-адресов по номенклатуре.

Команда	Описание
Общий режим	
ip access-list standard <*name*> **no ip access-list standard <*name*>**	Позволяет создать стандартный список доступа для IP-адресов по номенклатуре. Команда no удаляет стандартный список доступа для IP-адресов по номенклатуре

   b) Указание операций «permit» или «deny» для правила

Команда	Описание
Режим стандартных ACL для IP-адресов	
[no] {deny | permit} {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}}	Позволяет создать стандартное правило доступа для IP-адресов на основе имен. Команда no удаляет стандартное правило доступа для IP-адресов на основе имен

   c) Выход из режима настройки списков доступа ACL

Команда	Описание
Режим стандартных ACL для IP-адресов	
Exit	Осуществляет выход из режима настройки стандартных списков доступа ACL для IP-адресов на основе имен.

4. Настройка расширенного нумерованного списка доступа для IP-адресов по номенклатуре:
   a) Создание расширенного нумерованного списка доступа для IP-адресов по номенклатуре.

Команда	Описание
Общий режим	
ip access-list extended <*name*> **no ip access-list extended <*name*>**	Позволяет создать расширенный список доступа для IP-адресов по номенклатуре. Команда no удаляет расширенный список доступа для IP-адресов по номенклатуре.

   b) Указание операций «permit» или «deny» для правила

Команда	Описание
Режим расширенных ACL для IP-адресов	
[no] {deny | permit} icmp {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr> <dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<icmp-type>* [*<icmp-code>*]] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]	Позволяет создать расширенное именное ICMP-правило доступа для IP-адресов на основе имен. Команда no удаляет расширенное правило доступа для IP-адресов на основе имен.
[no] {deny | permit} igmp {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr> <dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<igmp-type>*] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]	Позволяет создать расширенное именное IGMP-правило доступа для IP-адресов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в команде.
[no] {deny | permit} tcp {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}} [s-port {*<sPort>* | range *<sPortMin> <sPortMax>*}] {{*<dIpAddr> <dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [d-port {*<dPort>* | range *<dPortMin> <dPortMax>*}] [ack+fin+psh+rst+urg+syn] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]	Позволяет создать расширенное именное TCP-правило доступа для IP-адресов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в команде.
[no] {deny | permit} udp {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}} [s-port	Позволяет создать расширенное именное UDP-правило доступа для IP-

{*<sPort>* | range *<sPortMin> <sPortMax>*}] {{*<dIpAddr> <dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [d-port {*<dPort>* | range *<dPortMin> <dPortMax>*}] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]	адресов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в команде.
[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num>} {{*<sIpAddr> <sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr> <dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]	Позволяет создать расширенное именное IP-правило доступа для IP-адресов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в команде.

c) Выход из режима расширенной настройки списков доступа ACL

Команда	Описание
Режим расширенных ACL для IP-адресов	
Exit	Осуществляет выход из режима настройки расширенных списков доступа ACL для IP-адресов на основе имен.

5. Настройка стандартного нумерованного списка доступа для MAC-адресов.

Команда	Описание
Общий режим	
access-list*<num>*{deny|permit}{any-source-mac|{host-source-mac*<host_smac>*}|{*<smac><smac-mask>*}} **no access-list *<num>***	Позволяет создать стандартный нумерованный список доступа для MAC-адресов. Если список доступа уже существует, в него будет добавлено правило. Команда no удаляет стандартный нумерованный список доступа для MAC-адресов.

6. Настройка расширенного нумерованного списка доступа для MAC-адресов.

Команда	Описание
Общий режим	
access-list*<num>* **{deny|permit} {any-source-mac| {host-source-mac***<host_smac>***}|{***<smac>***<***smac-mask***>}}{any-destination-mac|{host-destination-mac***<host_dmac>***}|{***<dmac>***<***dmac-mask***>}}[{untagged-eth2 | tagged-eth2 | untagged-802-3 | tagged-802-3} [*<offset1>* *<length1>* <value1> [*<offset2>* *<length2>* <value2> [<offset3> <length3> <value3> [*<offset4>* *<length4>* *<value4>*]]]]]** **no access-list** *<num>*	Позволяет создать расширенный нумерованный список доступа для MAC-адресов. Если список доступа уже существует, в него будет добавлено правило. Команда no удаляет расширенный нумерованный список доступа для MAC-адресов.

7. Настройка расширенного нумерованного списка доступа для MAC-адресов по номенклатуре:

a) Создание расширенного нумерованного списка доступа для MAC-адресов по номенклатуре.

Команда	Описание
Общий режим	
mac-access-list extended *<name>* **no mac-access-list extended** *<name>*	Позволяет создать расширенный список доступа для MAC-адресов по номенклатуре. Команда no удаляет расширенный список доступа для MAC-адресов по номенклатуре

b) Указание операций «permit» или «deny» для правила

Команда	Описание
Режим расширенных ACL для MAC-адресов	
[no]{deny|permit}{any-source-mac|{host-source-mac*<host_smac>***}|{***<smac>***<***smac-mask***>}} {any-destination-mac|{host-destination-mac** ***<host_dmac>*****} |{***<dmac>* *<dmac-mask>***}} [cos** ***<cos-val>*** **[***<cos-bitmask>***] [vlanId** ***<vid-value>***	Позволяет создать расширенное правило доступа для MAC-адресов на основе имен (проверка согласования MAC-кадров). Команда no удаляет это расширенное правило доступа для

[<*vid-mask*>][ethertype<*protocol*>[<*protocol-mask*>]]]] **[no]{deny|permit} {any-source-mac |{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [ethertype <*protocol*> [<*protocol-mask*>]]** **[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac |{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [vlanid <*vid-value*> [<*vid-mask*>][ethertype <*protocol*> [<*protocol-mask*>]]]**	MAC-адресов на основе имен.
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[untagged-eth2 [ethertype <*protocol*> [protocol-mask]]]	Позволяет создать расширенное правило доступа для MAC-адресов на основе имен (проверка согласования непомеченных кадров ethernet II). Команда no удаляет это расширенное правило доступа для MAC-адресов на основе имен.
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [untagged-802-3]	Позволяет создать правило доступа для MAC-адресов (проверка согласования непомеченных кадров 802.3). Команда no удаляет это правило доступа для MAC-адресов.
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[tagged-eth2 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]] [ethertype<*protocol*> [<*protocol-mask*>]]]	Позволяет создать правило доступа для MAC-адресов (проверка согласования помеченных кадров ethernet II). Команда no удаляет это правило доступа для MAC-адресов.
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [tagged-802-3 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]]]	Позволяет создать правило доступа для MAC-адресов (проверка согласования помеченных кадров 802.3). Команда no удаляет это правило доступа для MAC-адресов.

c) Выход из режима настройки списков доступа ACL.

Команда	Описание
Режим расширенных ACL для MAC-адресов	
Exit	Осуществляет выход из режима настройки расширенных списков доступа ACL для MAC-адресов на основе имен.

8. Настройка расширенного нумерованного списка доступа для MAC-IP-адресов

Команда	Описание
Общий режим	
access-list<*num*>{deny|permit} {any-source-mac| {host-source-mac <*host_smac*>} | {<*smac*> <*smac-mask*>}} {any-destination-mac | {host-destination-mac <*host_dmac*>} | {<*dmac*><*dmac-mask*>}} icmp {{<*source*> <*source-wildcard*>} |any-source| {host-source <*source-host-ip*>}} {{<*destination*> <*destination-wildcard*>} | any-destination | {host-destination <*destination-host-ip*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>] [time-range <*time-range-name*>]	Позволяет создать расширенное нумерованное mac-icmp правило доступа для mac-ip-адресов. Если список доступа с соответствующим номером не существует, он будет создан и в нем будет использован номер, указанный в команде.
access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Позволяет создать расширенное нумерованное mac-igmp правило доступа для mac-ip-адресов. Если список доступа с соответствующим номером не существует, он будет создан и в нем будет использован номер, указанный в команде.
access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port {<*port1*> | range	Позволяет создать расширенное нумерованное mac-tcp-правило доступа для другого специального протокола mac-tcp, либо для всех протоколов mac-tcp. Если список доступа с соответствующим номером

<*sPortMin*> <*sPortMax*>}] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port {<*port3*> | range <*dPortMin*> <*dPortMax*>}] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>][time-range<*time-range-name*>]	не существует, он будет создан и в нем будет использован номер, указанный в команде.
access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}udp {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} [s-port {<*port1*> | range <*sPortMin*> <*sPortMax*>}] {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}} [d-port {<*port3*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Позволяет создать расширенное нумерованное mac-ip-правило доступа для другого специального mac-ip-протокола, либо для всех mac-ip-протоколов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в команде.
access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Позволяет создать расширенное нумерованное mac-ip-правило доступа для другого специального mac-ip-протокола, либо для всех mac-ip-протоколов. Если соответствующий список доступа не существует, он будет создан и в нем будет использован номер, указанный в команде.
no access-list <*num*>	Позволяет удалить это расширенное нумерованное правило доступа для MAC-IP-адресов

9. Настройка расширенного нумерованного списка доступа для MAC-IP-адресов по номенклатуре
   a) Создание расширенного нумерованного списка доступа для MAC-IP-адресов в по номенклатуре

Команда	Описание
Общий режим	
mac-ip-access-list extended *<name>* **no mac-ip-access-list extended *<name>***	Позволяет создать расширенное MAC-IP-правило доступа на основе имен. Команда no удаляет это расширенное MAC-IP-правило доступа на основе имен.

b) Указание операций «permit» или «deny» для правила

Команда	Описание
Режим расширенных ACL для MAC-IP-адресов	
[no]{deny|permit} {any-source-mac|{host-source-mac *<host_smac>*}|{*<smac><smac-mask>*}} {any-destination-mac|{host-destination-mac *<host_dmac>*}|{*<dmac><dmac-mask>*}}icmp {{*<source><source-wildcard>*}|any-source| {host-source*<source-host-ip>*}} {{*<destination><destination-wildcard>*}|any-destination| {host-destination *<destination-host-ip>*}} [*<icmp-type>* [*<icmp-code>*]] [precedence *<precedence>*][tos*<tos>*][time-range*<time-range-name>*]	Позволяет создать расширенное MAC-ICMP-правило доступа на основе имен. Команда no удаляет это расширенное MAC-ICMP-правило доступа на основе имен.
[no]{deny|permit}{any-source-mac|{host-source-mac *<host_smac>*}|{*<smac><smac-mask>*}} {any-destination-mac|{host-destination-mac *<host_dmac>*}|{*<dmac><dmac-mask>*}}igmp {{*<source><source-wildcard>*}|any-source| {host-source*<source-host-ip>*}} {{*<destination><destination-wildcard>*}|any-destination| {host-destination *<destination-host-ip>*}} [*<igmp-type>*] [precedence *<precedence>*] [tos *<tos>*][time-range*<time-range-name>*]	Позволяет создать расширенное MAC-IGMP-правило доступа на основе имен. Команда no удаляет это расширенное MAC-IGMP-правило доступа на основе имен.
[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} [s-port {*<port1>* | range	Позволяет создать расширенное MAC-TCP-правило доступа на основе имен. Команда no удаляет это расширенное MAC-TCP-правило доступа на основе имен.

<*sPortMin*> <*sPortMax*>}] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}} [d-port {<*port3*> | range <*dPortMin*> <*dPortMax*>}] [ack+fin+psh+rst+urg+syn] [precedence<precedence>][tos<tos>][time-range<*time-range-name*>]	
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}udp {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} [s-port {<*port1*> | range <*sPortMin*> <*sPortMax*>}] {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination <*destination-host-ip*>}} [d-port {<*port3*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Позволяет создать расширенное MAC-UDP-правило доступа на основе имен. Команда no удаляет это расширенное MAC-UDP-правило доступа на основе имен.
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}} {eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}} [precedence<*precedence*>][tos<*tos*>][time-range<*time-range-name*>]	Позволяет создать расширенное MAC-IP-правило доступа для другого IP-протокола на основе имен. Команда no удаляет это расширенное MAC-IP-правило доступа на основе имен.

c) Выход из режима настройки списков доступа по MAC-IP-адресам

Команда	Описание
Режим расширенных ACL для MAC-IP-адресов	
Exit	Осуществляет выход из режима настройки расширенных списков доступа ACL для MAC-IP-адресов на основе имен.

10. Настройка стандартного нумерованного IPv6 списка доступа.

Команда	Описание
Общий режим	
ipv6 access-list *<num>* {deny | permit} {{*<sIPv6Addr>* *<sPrefixlen>*} | any-source | {host-source *<sIpv6Addr>*}} **no ipv6 access-list *<num>***	Позволяет создать стандартный нумерованный IPv6 список доступа. Если список доступа уже существует, в него будет добавлено правило. Команда no удаляет стандартный нумерованный IPv6 список доступа.

11. Настройка расширенного нумерованного IPv6 списка доступа

Команда	Описание
Общий режим	
ipv6 access-list <num-ext> {deny | permit} icmp {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl>][time-range<time-range-name>] **ipv6 access-list <num-ext> {deny | permit} tcp {{<sIPv6Prefix/<sPrefixlen>} | any-source | {host-source <sIPv6Addr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {{<dIPv6Prefix/<dPrefixlen>} | any-destination | {host-destination <dIPv6Addr>}} [dPort {<dPort> | range <dPortMin> <dPortMax>}] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <flowlabel>][time-range<time-range-name>]** **ipv6 access-list <num-ext> {deny | permit} udp {{<sIPv6Prefix/<sPrefixlen>} | any-source | {host-source <sIPv6Addr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {{<dIPv6Prefix/<dPrefixlen>} | any-destination | {host-destination <dIPv6Addr>}} [dPort {<dPort> | range <dPortMin> <dPortMax>}] [dscp <dscp>] [flow-label <flowlabel>][time-range<time-range-**	Позволяет создать расширенный нумерованный IPv6 список доступа. Если список доступа уже существует, в него будет добавлено правило. Команда no удаляет расширенный нумерованный IPv6 список доступа.

name>] **ipv6 access-list <num-ext> {deny | permit} <next-header> {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>][time-range<time-range-name>]** **no ipv6 access-list <num>**	

12. Настройка стандартного IPv6 листа доступа, основанного на номенклатуре

a) Создание стандартного IPv6 листа доступа, основанного на номенклатуре

Команда	Описание
Общий режим	
ipv6 access-list standard <name> **no ipv6 access-list standard <name>**	Позволяет создать стандартный IPv6 список доступа по номенклатуре. Команда no удаляет стандартный IPv6 список доступа по номенклатуре

b) Определение множественного доступа или правил запрета

Команда	Описание
Режим стандартных IPv6 ACL	
[no] {deny | permit} {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr> }}	Позволяет создать стандартное IPv6 правило доступа на основе имен. Команда no удаляет стандартное IPv6 правило доступа адресов на основе имен

c) Выход из режима конфигурации ACL

Команда	Описание
Режим стандартных IPv6 ACL	
Exit	Осуществляет выход из режима настройки стандартных IPv6 списков доступа ACL на

	основе имен.

13. Настройка расширенного IPv6 листа доступа, основанного на номенклатуре

a) Создание расширенного IPv6 листа доступа, основанного на номенклатуре

Команда	Описание
Общий режим	
ipv6 access-list extended <name> **no ipv6 access-list extended <name>**	Позволяет создать расширенный IPv6 список доступа по номенклатуре. Команда no удаляет расширенный IPv6 список доступа по номенклатуре

b) Определение множественного доступа или правил запрета

Команда	Описание
Режим расширенных IPv6 ACL	
[no] {deny | permit} icmp {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <flowlabel>] [time-range <time-range-name>]	Позволяет создать расширенное именное ICMP IPv6 правило доступа на основе имен. Команда no удаляет расширенное ICMP IPv6 правило доступа на основе имен.
[no] {deny | permit} tcp {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [d-port {<dPort> | range <dPortMin> <dPortMax>}] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]	Позволяет создать расширенное именное TCP IPv6 правило доступа. Команда no удаляет расширенное TCP IPv6 правило доступа на основе имен.
[no] {deny | permit} udp {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} [s-port {<sPort> | range <sPortMin> <sPortMax>}] {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [d-port {<dPort> | range <dPortMin> <dPortMax>}] [dscp <dscp>]	Позволяет создать расширенное именное UDP IPv6 правило доступа для IP-адресов Команда no удаляет расширенное UDP IPv6 правило доступа на основе имен.

[flow-label <fl>] [time-range<time-range-name>]	
[no] {deny | permit} <proto> {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <flowlabel>] [time-range <time-range-name>]	Позволяет создать расширенное именное IPv6 правило доступа для других IPv6 протоколов. Команда no удаляет расширенное IPv6 правило доступа на основе имен.
[no] {deny | permit} {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <flowlabel>] [time-range <time-range-name>]	Позволяет создать расширенное именное IPv6 правило доступа. Команда no удаляет расширенное IPv6 правило доступа на основе имен.

c) Выход из режима конфигурации ACL

Команда	Описание
Режим расширенных IPv6 ACL	
Exit	Осуществляет выход из режима настройки расширенных списков доступа IPv6 ACL на основе имен.

1.2.2 Настройка функции фильтрации пакетов

1. Включение функции фильтрации пакетов в глобальном режиме конфигурирования.

Команда	Описание
Общий режим	
firewall enable	Включает функцию фильтрации пакетов в глобальном режиме конфигурирования
firewall disable	Выключает функцию фильтрации пакетов в глобальном режиме конфигурирования

2. Настройка операции, выполняемой по умолчанию.

Команда	Описание
Общий режим	
firewall default {permit |deny [ipv4 | ipv6 | all]}	Устанавливает операцию по умолчанию («permit» или «deny») для функции фильтрации пакетов

1.2.3 Настройка функции time range (временной диапазон)

1. Создание имени временного диапазона.

Команда	Описание
Общий режим	
time-range *<time_range_name>*	Позволяет создать именованный временной диапазон (с именем <time_range_name>)
no time-range *<time_range_name>*	Отменяет именование временного диапазона (с именем time_range_name)

2. Настройка периодичности временного диапазона.

Команда	Описание
Режим настройки временного диапазона	
absolute-periodic {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} *<start_time>* to {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} *<end_time>*	Позволяет настроить временной диапазон для недели. Каждую неделю будет применяться заданный временной диапазон.
periodic {{Monday+Tuesday+Wednesday+Thursday+ Friday+Saturday+Sunday} | daily | weekdays | weekend} *<start_time>* to *<end_time>*	
[no] absolute-periodic {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |	Отменяет временной диапазон для

Sunday} *<start_time>* to {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} *<end_time>*	недели
[no] periodic {{Monday+Tuesday+Wednesday+Thursday+ Friday+Saturday+Sunday} | daily | weekdays | weekend} *<start_time>* to *<end_time>*	

3. Настройка абсолютного временного диапазона.

Команда	Описание
Общий режим	
absolute start *<start_time>* *<start_data>* [end *<end_time>* *<end_data>*]	Позволяет настроить абсолютный временной диапазон
[no] absolute start *<start_time>* *<start_data>* [end *<end_time>* *<end_data>*]	Отменяет абсолютный временной диапазон

1.2.4 Привязка списка доступа к конкретному направлению в заданном порту

Команда	Описание
Режим настройки физических интерфейсов, режим настройки интерфейсов VLAN	
{ip|ipv6|mac|mac-ip} access-group *<acl-name>* {in} [traffic-statistic] **no {ip|ipv6|mac|mac-ip} access-group *<acl-name>* {in}**	Применяет список доступа к указанному направлению порта. Команда no удаляет применение списка доступа на границе порта.

1.2.5 Очистка фильтрующей информации указанного порта

Команда	Описание
Режим администратора	
clear access-group (in) statistic interface { <interface-name> | ethernet *<interface-*	Очищает статистику указанного интерфейса.

name> **}**	

1.3 Примеры ACL

Сценарий 1

Пользователь предъявляет следующие требования к конфигурированию: порт 1/10 коммутатора присоединен к сегменту 10.0.0.0/24, использование FTP-протокола нежелательно.

Шаги конфигурации следующие:

1. Создать соответствующий список доступа ACL.
2. Настроить функцию фильтрации пакетов.
3. Привязать список доступа ACL к порту.

Процедура настройки:

```
Switch(config)#access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination
d-port 21
Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/3/2
Switch(Config-If-Ethernet1/3/2)#ip access-group 110 in
Switch(Config-If-Ethernet1/3/2)#exit
Switch(config)#exit
```

Результат конфигурации:

```
Switch#show firewall
Firewall status: enable.
Firewall default rule: permit.
Switch#show access-lists
access-list 110(used 1 time(s)) 1 rule(s)
access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch#show access-group interface ethernet 1/3/2
interface name:Ethernet1/3/2
the ingress acl use in firewall is 110, traffic-statistics Disable.
```

Сценарий 2

Пользователь предъявляет следующие требования к конфигурированию: порт 1/10 коммутатора присоединен к сегменту 00-12-11-23-XX-XX, прохождение пакетов 802.3 нежелательно.

Шаги конфигурации следующие:

1. Создать соответствующий список доступа ACL.

2. Настроить функцию фильтрации пакетов.
3. Привязать список доступа ACL к порту.

Процедура настройки:

```
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac untagged-802-3
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any
tagged-802
Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet1/3/2
Switch(Config-If-Ethernet1/3/2)#mac access-group 1100 in
Switch(Config-If-Ethernet1/3/2)#exit
Switch(config)#exit
```

Результат конфигурации:

```
Switch#show firewall
Firewall Status: Enable.
Firewall Default Rule: Permit.

Switch #show access-lists
access-list 1100(used 1 time(s))
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
untagged-802-3
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
Switch #show access-group interface ethernet 1/3/2
interface name:Ethernet1/3/2
MAC Ingress access-list used is 1100,traffic-statistics Disable.
```

Сценарий 3

Пользователь предъявляет следующие требования к конфигурированию: порт 1/10 коммутатора присоединен к сегменту 00-12-11-23-XX-XX, прохождение пакетов сегмента IP 10.0.0.0/24 и доступ по FTP нежелательны.

Шаги конфигурации следующие:

1. Создать соответствующий список доступа ACL.
2. Настроить функцию фильтрации пакетов.
3. Привязать список доступа ACL к порту.

Процедура настройки:

```
Switch(config)#access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
```

```
Switch(config)#access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp any-source 10.0.0.0 0.0.0.255

Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/3/2
Switch(Config-If-Ethernet1/3/2)#mac-ip access-group 3110 in
Switch(Config-Ethernet1/3/2)#exit
Switch(config)#exit
```

Результат конфигурации:

```
Switch#show firewall
Firewall Status: Enable.
Firewall Default Rule: Permit.

Switch#show access-lists
access-list 3110(used 1 time(s))
access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp any-source 10.0.0.0 0.0.0.255

Switch #show access-group interface ethernet 1/3/2
interface name:Ethernet1/3/2
MAC-IP Ingress access-list used is 3110, traffic-statistics Disable.
```

Сценарий 4

Пользователь предъявляет следующие требования к конфигурированию: протокол IPv6 работает на интерфейсе коммутатора 600, адрес IPv6 сети 2003:1:1:1::0/64. Пользователи, находящиеся в подсети с адресом 2003:1:1:1:66::0/80, должны быть изолированы от внешней сети.

Шаги конфигурации следующие:

1. Создать соответствующий список доступа ACL.
2. Настроить функцию фильтрации пакетов.
3. Привязать список доступа ACL к соответствующему интерфейсу.

Процедура настройки:

```
Switch(config)#ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-destination
Switch(config)#ipv6 access-list 600 deny 2003:1:1:1::0/64 any-destination

Switch(config)#firewall enable
```

```
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/3/2
Switch(Config-If-Ethernet1/3/2)#ipv6 access-group 600 in
Switch(Config-If-Ethernet1/3/2)#exit
Switch(config)#exit
```

Результат конфигурации:

```
Switch#show firewall
Firewall Status: Enable.
Firewall Default Rule: Permit.

Switch#show ipv6 access-lists
Ipv6 access-list 600(used 1 time(s))
ipv6 access-list 600 deny 2003:1:1:1::0/64 any-source
ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-source

Switch #show access-group interface ethernet 1/3/2
interface name:Ethernet1/3/2
IPv6 Ingress access-list used is 600, traffic-statistics Disable.
```

Сценарий 5

Пользователь предъявляет следующие требования к конфигурированию: интерфейсы 1/1/1, 1/1/2, 1/2/1, 1/2/3 принадлежат vlan100, хосты IP-адресом 192.168.0.1 должны быть изолированы от доступа на перечисленные интерфейсы.

Шаги конфигурации следующие:

1. Создать соответствующий список доступа ACL.
2. Настроить функцию фильтрации пакетов.
3. Привязать список доступа ACL к соответствующему интерфейсу.

Процедура настройки:

```
Switch (config)#firewall enable
Switch (config)#vlan 100
Switch (Config-Vlan100)#switchport interface ethernet 1/1/1;1/1/2;1/2/1;1/2/3
Switch (Config-Vlan100)#exit
Switch (config)#access-list 1 deny host-source 192.168.0.1
Switch (config)#interface ethernet1/1/1;1/1/2;1/2/1;1/2/3
Switch (config-if-port-range)#ip access-group 1 in
Switch (Config-if-Vlan100)#exit
```

Результат конфигурации:

```
Switch (config)#show access-group interface vlan 100
Interface VLAN 100:
```

```
Ethernet1/1/1:      IP  Ingress  access-list  used  is  1,  traffic-statistics
Disable.
Ethernet1/1/2:      IP  Ingress  access-list  used  is  1,  traffic-statistics
Disable.
Ethernet1/2/1:      IP  Ingress  access-list  used  is  1,  traffic-statistics
Disable.
Ethernet1/2/3:      IP  Ingress  access-list  used  is  1,  traffic-statistics
Disable.
```

1.4 Поиск неисправностей ACL

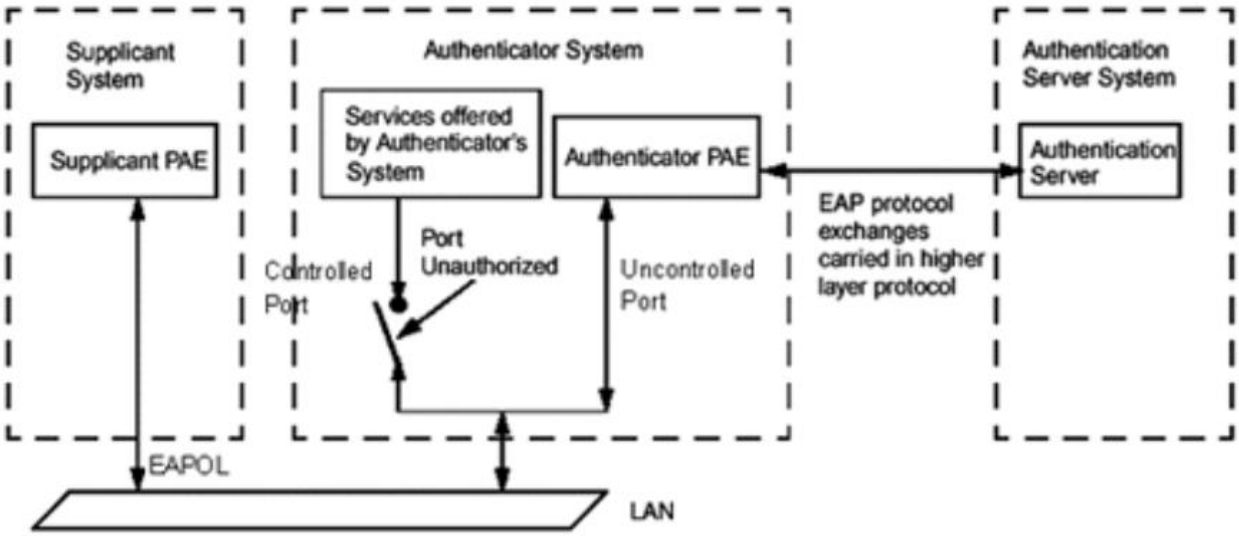
- Проверка по элементам списка ACL выполняется, начиная с первого элемента списка и продолжается до тех пор пока не будет достигнуто согласование. Как только оно достигнуто, последующие проверки не проводятся, их условия игнорируются.
- Для входящих пакетов в порту может существовать только один привязанный список ACL из перечисленных — один MAC-IP ACL, один IP ACL, один MAC ACL, один IPv6 ACL (через режим физического интерфейса или интерфейса VLAN)
- Когда привязанные четыре ACL и пакеты нескольких ACL одновременно совпадают, приоритет определяется в порядке сверху вниз. Для одного и того же списка ACL: чем раньше сконфигурировано правило, тем выше его приоритет.
  - ✓ Входящий IPv6 ACL.
  - ✓ Входящий MAC-IP ACL.
  - ✓ Входящий IP ACL.
  - ✓ Входящий MAC ACL.
- Число списков ACL, которые могут быть корректно привязаны к порту, определяется их контентом и ограничениями, налагаемыми аппаратными средствами. Если возникают проблемы на аппаратном уровне с привязкой ACL, то отображается соответствующее предупреждение.
- Если некоторые правила содержат одну и ту же фильтрующую информацию и конфликтуют с режимом списка доступа, то такой список не может быть привязан к порту; будет выведено сообщение об ошибке. Например: разрешено прохождение TCP-пакетов от любого источника к любому назначению, но одновременно с этим запрещено прохождение TCP-пакетов от любого источника к любому назначению.
- Вирусы, такие например, как «worm.blaster», могут быть блокированы путем настройки списков доступа ACL — в списках можно задать блокирование определенных ICMP- , либо TCP- или UDP-пакетов в порту.

2 КОНФИГУРИРОВАНИЕ ПРОТОКОЛА 802.1X

2.1 Введение в 802.1x

Протокол IEEE 802.1x реализует метод управления доступом к сети на основе портов, он управляет аутентификацией и устройствами доступа на физическом уровне доступа к сетевым устройствам. На физическом уровне доступа в данном случае находятся порты коммутатора. Если пользовательские устройства, подключенные к этим портам, удается идентифицировать, они получают доступ к ресурсам локальной сети, в противном случае доступ будет запрещен, что во многом эквивалентно физическому выключению. Стандарты IEEE 802.1x определяют протокол управления доступом к сети на основе портов. Протокол применим к соединению точка-точка между устройством доступа и портом доступа, при этом порт может быть логическим или физическим. В типичном случае один физический порт коммутатора присоединен только к одному терминирующему устройству (имеющему физические порты).

Архитектура IEEE 802.1x показана на рисунке ниже.



Надписи на рисунке:

- Supplicant System – клиентская система;
- Supplicant PAE – PAE клиентской системы;
- Autenthicator system – система аутентификатора;
- Autenthicator PAE – PAE аутентификатора;
- Services offered by Autenthicator's system – услуги, предоставляемые системой аутентификатора;
- Controlled Port – управляемый порт;
- Uncontrolled port – неуправляемый порт;
- EAP protocol exchanges carried in higher layer protocol – обмен сообщениями протокола EAP происходит через протокол более высокого уровня;
- Authentication Server system – система сервера аутентификации;

- Authentication Server – сервер аутентификации.

Архитектура IEEE 802.1x состоит из трех частей:

- Клиентской системы (пользовательское устройство доступа).
- Аутентифицирующей системы (устройство управления доступом).
- Сервера аутентификации.

Взаимодействие пользовательского устройства доступа (PC) и устройства управления доступом (коммутатором доступа) происходит по протоколу EAPOL, определенного стандартами IEEE 802.1x. Взаимодействие сервера аутентификации с устройством управления доступом происходит по протоколу EAP. Данные аутентификации инкапсулируются в пакеты EAP. Пакет EAP передается в пакетах протоколов более высоких уровней, например, RADIUS и, пройдя через сложную сеть, попадает на сервер аутентификации.

Порты, которые предоставляет устройство управления доступом на уровне порта, могут быть виртуальными портами двух типов: управляемые порты и неуправляемые порты. Неуправляемый порт всегда находится во включенном состоянии в обоих направлениях передачи пакетов аутентификации EAP. Управляемый порт, когда он авторизован на передачу трафика с коммутацией пакетов, всегда будет в подключенном состоянии. Если порт не авторизован, то он выключен и передача пакетов невозможна.

При IEEE 802.1x, коммутатор используется как устройство управления доступом; подключаемое пользовательское устройство — это устройство с клиентским ПО, поддерживающим 802.1x. Сервер аутентификации обычно находится в AAA-центре оператора и обычно является RADIUS-сервером.

Для улучшения безопасности и управления в коммутаторах реализовано различие между пользовательским доступом и аутентификацией IEEE 802.1x на основе MAC-адресов. Только аутентифицированные пользовательские устройства доступа, подключенные к одному и тому же физическому порту, могут получать доступ к сети. Неавторизованные устройства не получат доступа в сеть. Таким образом, даже если к одному физическому порту подключено много терминалов, коммутатор может аутентифицировать их и управлять каждым пользовательским устройством доступа индивидуально.

На основе функции аутентификации 802.1x по MAC-адресам реализована пользовательская аутентификация 802.1x (IP-адрес + MAC-адрес + порт). Это позволяет пользователям до прохождения ими аутентификации получать доступ к ограниченным ресурсам. При пользовательском управлении доступом имеется два режима: стандартное управление и расширенное управление. При стандартном пользовательском управлении доступ к ограниченным ресурсам не ограничивается, все пользователи порта имеют к ним доступ до аутентификации. После аутентификации пользователи получают доступ ко всем ресурсам. При расширенном пользовательском управлении доступом только специальные пользователи до аутентификации получат доступ к ограниченным ресурсам. После прохождения аутентификации эти специальные пользователи получат доступ ко всем ресурсам.

2.2 Настройка протокола 802.1x

1. Включение функции IEEE 802.1x.

Команда	Описание
Режим конфигурации порта	
dot1x enable **no dot1x enable**	Включает функцию 802.1x на коммутаторе и портах. Команда no выключает функцию 802.1x.
dot1x privateclient enable **no dot1x privateclient enable**	Включает на коммутаторе режим принудительного использования клиентским ПО формата сообщений аутентификации 802.1x. Команда no выключает этот режим, при этом клиентское ПО начинает использовать сообщения аутентификации 802.1x стандартного формата.
dot1x user free-resource <*prefix*> <*mask*> **no dot1x user free-resource**	Позволяет задать ограниченные ресурсы, которые могут быть доступны пользователям. Команда no используется для удаления ограниченных ресурсов.
dot1x unicast enable **no dot1x unicast enable**	Включает функцию 802.1x одноадресной сквозной передачи данных на коммутаторе. Команда no выключает данную функциюх.

2. Настройка состояния аутентификации порта.

Команда	Описание
Режим конфигурации порта	
dot1x port-control {auto|force-authorized|force-unauthorized } **no dot1x port-control**	Позволяет настроить состояние авторизации 802.1x. Команда no восстанавливает настройки, заданные по умолчанию.

3. Настройка метода управления доступом к порту: На основе MAC-адресов или на основе порта.

Команда	Описание
Режим конфигурации порта	
dot1x port-method {macbased | portbased | userbased {standard | advanced}} **no dot1x port-method**	Устанавливает метод управления доступом к порту. Команда no восстанавливает управление доступом на основе MAC-адресов.
dot1x max-user macbased *<number>* **no dot1x max-user macbased**	Позволяет задать максимальное число пользователей, которым разрешен доступ к указанному порту, при котором используется управление по MAC-адресам. Команда no восстанавливает настройки, заданные по умолчанию — допускается 1 пользователь.
dot1x max-user userbased <number> **no dot1x max-user userbased**	Позволяет задать максимальное число пользователей, которым разрешен доступ к указанному порту, при котором используется пользовательский режим управления доступом. Команда no восстанавливает настройки, заданные по умолчанию — допускается не более 10 пользователей.
dot1x guest-vlan *<vlanID>* **no dot1x guest-vlan**	Устанавливает гостевую сеть VLAN на настраиваемом порту. Команда no удаляет гостевую сеть VLAN.
dot1x portbased mode single-mode **no dot1x portbased mode single-mode**	Устанавливает одномодовый режим в режиме аутентификации на порту. Команда no отключает данную функцию.

4. Настройка функций расширенного управления 802.1x.

Команда	Описание
Общий режим	
dot1x macfilter enable **no dot1x macfilter enable**	Включает функцию 802.1x фильтрации адресов в коммутаторе. Команда no

	выключает функцию 802.1x фильтрации адресов.
dot1x accept-mac <*mac-address*> [interface <*interface-name*>] **no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]**	Позволяет добавить адреса в таблицу фильтрующих адресов 802.1x. Команда no удаляет адреса из таблицы фильтрующих адресов 802.1x.
dot1x eapor enable **no dot1x eapor enable**	Включает функцию передачи аутентификационных данных протокола EAP в коммутаторе. Команда no задает локальное окончание аутентификации.

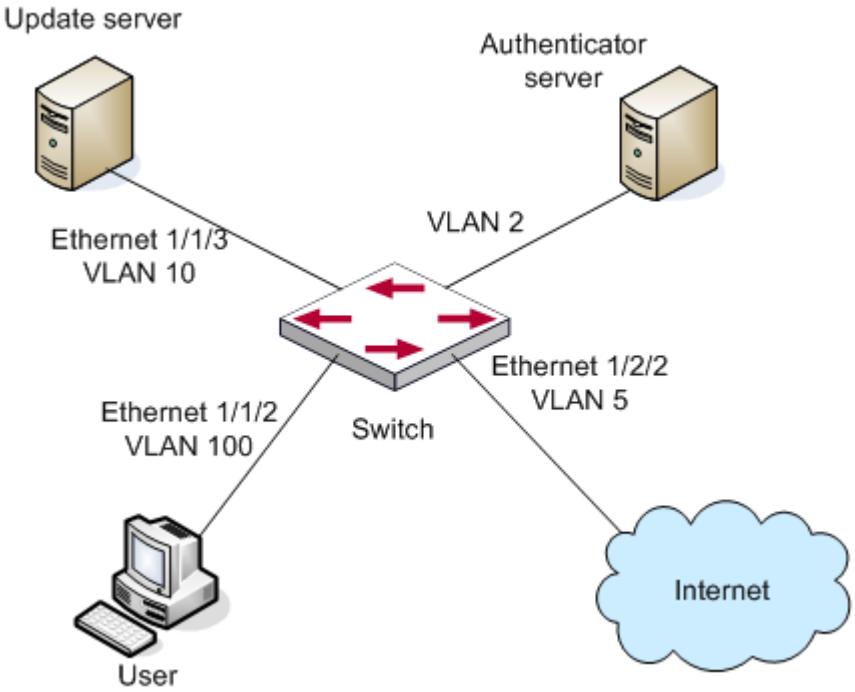
5. Настройка свойств пользовательских устройств доступа (опция).

Команда	Описание
Общий режим	
dot1x max-req <*count*> **no dot1x max-req**	Позволяет задать число запросов/кадров MD5, посылаемых перед тем, как коммутатор повторно инициирует аутентификацию при неполучении ответа от клиентской системы. Команда no восстанавливает настройки, заданные по умолчанию.
dot1x re-authentication **no dot1x re-authentication**	Включает периодическую аутентификацию клиентской системы. Команда no выключает данную функцию.
dot1x timeout quiet-period <*seconds*> **no dot1x timeout quiet-period**	Позволяет задать время бездействия в порту при сбое аутентификации. Команда no восстанавливает настройки, заданные по умолчанию.
dot1x timeout re-authperiod <*seconds*> **no dot1x timeout re-authperiod**	Позволяет задать интервал времени, по истечении которого выполняется повторная аутентификация клиентской системы. Команда no восстанавливает настройки, заданные по умолчанию.

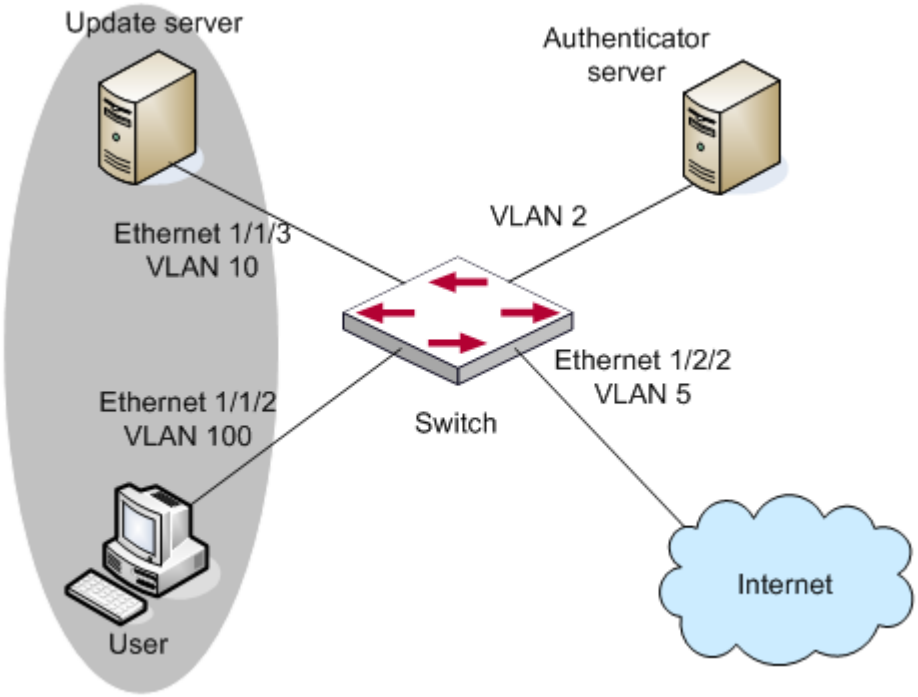
dot1x timeout tx-period <*seconds*> **no dot1x timeout tx-period**	Позволяет задать интервал времени, по истечении которого клиентской системой выполняется повторная передача запроса/кадра идентичности EAP. Команда no восстанавливает настройки, заданные по умолчанию.
dot1x re-authenticate [interface <*interface-name*>]	Включает повторную аутентификацию IEEE 802.1x во всех портах либо в указанном порту (при этом ожидания не потребуется).

2.3 Примеры использования протокола 802.1x

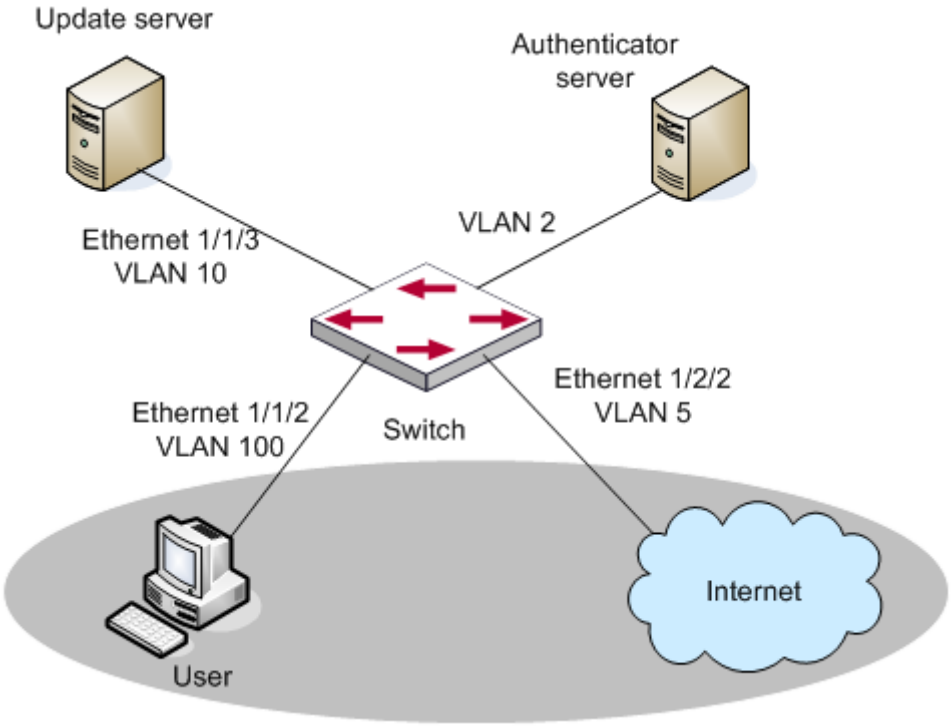
2.3.1 Пример гостевой VLAN



Как показано на следующем рисунке, коммутатор для доступа в сеть использует аутентификацию 802.1x с RADIUS-сервером в качестве сервера аутентификации. Порт Ethernet1/1/2, через который пользователи подключаются к коммутатору, принадлежит VLAN100, сервер аутентификации находится в VLAN2, сервер обновлений находится в VLAN10, порт Ethernet1/2/2, используемый коммутатором для выхода в Интернет, располагается в VLAN5.



Как показано на рисунке выше, на порту коммутатора Ethernet1/1/2 активирован 802.1x, и VLAN10 установлена как гостевая. Перед успешной или неудачной аутентификацией пользователя порт Ethernet1/1/2 добавлен в VLAN10, разрешая пользователю доступ к серверу обновлений.



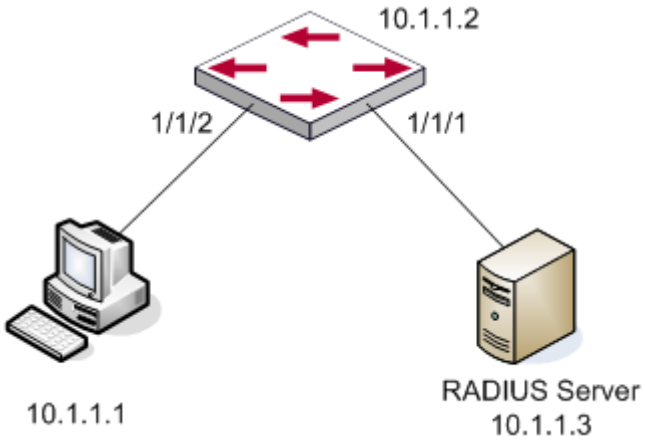
Как показано на рисунке выше, когда пользователи выходят в сеть после успешной аутентификации, сервер аутентификации назначит VLAN5 для пользователя и порта Ethernet1/2/2, чтобы пользователь получил доступ в Интернет.

Шаги конфигурации следующие:

```
# Configure RADIUS server.
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable

# Create VLAN100.
Switch(config)#vlan 100

# Enable the global 802.1x function
Switch(config)#dot1x enable

# Enable the 802.1x function on port Ethernet1/1/2
Switch(config)#interface ethernet1/1/2
Switch(Config-If-Ethernet1/1/2)#dot1x enable

# Set the link type of the port as access mode.
Switch(Config-If-Ethernet1/1/2)#switch-port mode access

# Set the access control mode on the port as portbased.
Switch(Config-If-Ethernet1/1/2)#dot1x port-method portbased

# Set the access control mode on the port as auto.
Switch(Config-If-Ethernet1/1/2)#dot1x port-control auto

# Set the port's Guest VLAN as 100.
Switch(Config-If-Ethernet1/1/2)#dot1x guest-vlan 100
Switch(Config-If-Ethernet1/1/2)#exit
```

Используя команды show running-config или show interface ethernet1/1/2, пользователи могут проверить конфигурацию гостевой сети. При помощи команды show vlan id 100 пользователи могут проверить настройки гостевой VLAN на порту.

2.3.2 Пример IPv4 RADIUS

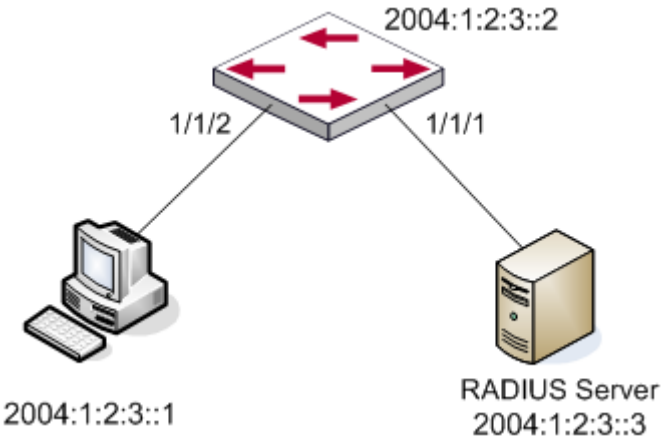


Компьютер подключен к порту 1/1/2 коммутатора. На порту включена функция аутентификации IEEE802.1, в качестве метода доступа по умолчанию используется аутентификация на основе MAC-адресов. IP-адрес коммутатора 10.1.1.2, все его порты (за исключением 1/1/2) подключены к серверу аутентификации RADIUS с IP-адресом 10.1.1.3. По умолчанию портами аутентификации и учета сетевых сервисов являются соответственно порт 1812 и порт 1813. Для выполнения аутентификации IEEE802.1x в компьютере установлено клиентское ПО.

Шаги конфигурации следующие:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/1/2
Switch(Config-Ethernet1/1/2)#dot1x enable
Switch(Config-Ethernet1/1/2)#dot1x port-control auto
Switch(Config-Ethernet1/1/2)#exit
```

2.3.3 Пример IPv6 RADIUS



Компьютер подключен к порту 1/1/2 коммутатора. На порту включена функция 802.1x, в качестве метода доступа по умолчанию используется аутентификация на основе MAC-адресов. IP-адрес коммутатора 2004:1:2:3::2, все его порты (за исключением 1/1/2) подключены к серверу аутентификации RADIUS с IP-адресом 2004:1:2:3::3. По умолчанию портами аутентификации и учета сетевых сервисов являются соответственно порт 1812 и порт 1813. Для выполнения аутентификации IEEE802.1x в компьютере установлено клиентское ПО.

Шаги конфигурации следующие:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ipv6 address 2004:1:2:3::2/64
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 2004:1:2:3::3
Switch(config)#radius-server accounting host 2004:1:2:3::3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/1/2
Switch(Config-If-Ethernet1/1/2)#dot1x enable
Switch(Config-If-Ethernet1/1/2)#dot1x port-control auto
Switch(Config-If-Ethernet1/1/2)#exit
```

2.4 Поиск неисправностей 802.1x

Может возникнуть такая ситуация — настройка 802.1x в портах выполнена, для аутентификации 802.1x задан режим auto (автоматически), но коммутатор не выполняет аутентификацию после того, как пользователь загружает клиентское ПО 802.1x на клиентской системе. Ниже перечислены некоторые возможные причины и способы разрешения проблем:

- Если 802.1x для порта включить не удается, удостоверьтесь в том, что: порт не участвует в работе протокола Spanning tree; не используется агрегация порта; порт не используется как магистральный. Для того чтобы аутентификация 802.1x работала, вышеперечисленные функции должны быть выключены.
- Если коммутатор правильно настроен, однако не может выполнить аутентификацию, проверьте соединение между коммутатором и RADIUS-сервером, клиентское ПО 802.1x , настройки порта и VLAN.
- Для поиска возможных причин используйте отчет о событиях RADIUS-сервера. В отчете о событиях регистрируются не только безуспешные попытки входа в систему, но и их причины. Если события отчета указывают на неправильный пароль аутентификатора, необходимо изменить ключ RADIUS-сервера. Если события отчета указывают, что аутентификатор отсутствует, необходимо добавить его в RADIUS-сервер. Если события отчета указывают, что нет пользователя с таким именем и паролем, то пароль и имя могут быть неверными, необходимо проверить их и ввести снова.

3 ОГРАНИЧЕНИЯ ПО MAC- И IP-АДРЕСАМ НА ПОРТУ, КОНФИГУРАЦИЯ VLAN

3.1 Общие сведения

Список MAC-адресов используется для определения взаимосвязей MAC-адресами пунктов назначения и портами коммутаторов. Существует два вида MAC-адресов в списке: статический и динамический. Статический MAC-адрес устанавливается пользователем, имеет высший приоритет (не может быть перезаписан динамическим адресом) и всегда эффективен. Динамический MAC-адрес, полученный от коммутатора при передаче пакетов, эффективен только в определённый период времени. Во время получения данных для передачи коммутатор распознаёт MAC-адрес источника и взаимосвязь с портом-получателем, далее ищет MAC-адрес пункта назначения в списке MAC-адресов. Если находится совпадение записей в списке, то коммутатор передаёт данные на соответствующий порт или выполняет широковещание на соответствующую сеть VLAN конечным пользователям. Если в течение долгого времени не находится соответствий для динамических MAC-адресов, коммутатор удаляет эти адреса из списка.

Как правило, коммутатор поддерживает оба метода конфигурирования MAC-адресов, из чего следует, что каждый порт может иметь более чем одну конфигурацию статического MAC-адреса, а также распознавать динамические MAC-адреса для передачи данных между портом и пунктами назначения с известными MAC-адресами. Когда MAC-адрес устаревает, он становится широковещательным. По умолчанию не задано никаких ограничений для портов по количеству MAC-адресов, каждый порт может иметь несколько MAC-адресов, статических или динамических, насколько позволяют аппаратные возможности. Чтобы избежать назначения слишком много количества адресов для порта, рекомендуется ограничить данное количество для каждого порта.

Для каждого интерфейса VLAN не существует ограничений по количеству IP-адресов, соответствующих количеству подключённых пользователей, которое в то же время является верхним пределом числа записей в списке ARP и ND. Не существует соответствующей конфигурационной команды для контроля количества посланных этих записей в списке. Для повышения безопасности и улучшения контроля над устройством необходимо контролировать количество MAC-адресов на каждом порту и количество ARP и ND на каждом интерфейсе VLAN. Количество статических и динамических MAC-адресов на порту, а также количество пользователей в каждом VLAN, не должно превышать текущую конфигурацию.

Ограничение количества MAC-адресов на портах и ARP записей поможет в достаточной степени избежать DOS атак. В случае систематических попыток подделать MAC-адреса и ARP записи успешные DOS атаки могут сильно облегчить попытку проникновения со стороны злоумышленников. Коммутатор может контролировать количество MAC-адресов и ARP/ND записей на портах, а также количество пользователей в VLAN, при помощи конфигурационных команд.

Ограничение количества динамических MAC- и IP-адресов на портах:

1. Ограничение количества динамических MAC-адресов. Если количество динамических MAC-адресов, распознанных коммутатором, равно или превышает установленный предел, то функция распознавания MAC-адресов на порту должна отключаться.
2. Ограничение количества динамических IP-адресов. Если количество динамических ARP/ND, распознанных коммутатором, равно или превышает установленный предел, то функция распознавания ARP/ND на порту должна отключаться.

Ограничение количества MAC, ARP и ND на интерфейсах.

1. Ограничение количества динамических MAC-адресов. Если количество динамических MAC-адресов, распознанных интерфейсом VLAN, равно или превышает установленный предел, то функция распознавания MAC-адресов для всех портов VLAN должна отключаться.
2. Ограничение количества динамических IP-адресов. Если количество динамических ARP/ND, распознанных интерфейсом VLAN, равно или превышает установленный предел, то функция распознавания ARP/ND на всех портах VLAN должна отключаться.

3.2 Конфигурация количества ограничений MAC и IP-адресов на портах и VLAN

1. Настройка ограничений количества MAC и IP-адресов на портах.

Команда	Описание
Режим конфигурации порта	
switchport mac-address dynamic maximum *<value>* **no switchport mac-address dynamic maximum**	Позволяет включить или отключить функцию ограничения количества MAC-адресов на портах.
switchport arp dynamic maximum *<value>* **no switchport arp dynamic maximum**	Позволяет включить или отключить функцию ограничения количества ARP на портах.
switchport nd dynamic maximum *<value>* **no switchport nd dynamic maximum**	Позволяет включить или отключить функцию ограничения количества ND на портах.

2. Настройка ограничений количества MAC и IP-адресов на интерфейсе VLAN.

Команда	Описание
Режим конфигурации VLAN	

vlan mac-address dynamic maximum *<value>* **no vlan mac-address dynamic maximum**	Позволяет включить или отключить функцию ограничения количества MAC-адресов на VLAN.
Режим конфигурации интерфейса	
ip arp dynamic maximum *<value>* **no ip arp dynamic maximum**	Позволяет включить или отключить функцию ограничения количества ARP на VLAN.
ipv6 nd dynamic maximum *<value>* **no ipv6 nd dynamic maximum**	Позволяет включить или отключить функцию ограничения количества ND на VLAN.

3. Настройка таймаута запроса динамического MAC-адреса.

Команда	Описание
Общий режим	
mac-address query timeout <seconds>	Позволяет настроить таймаут запроса динамического MAC-адреса.

4. Настройка режима нарушений для порта.

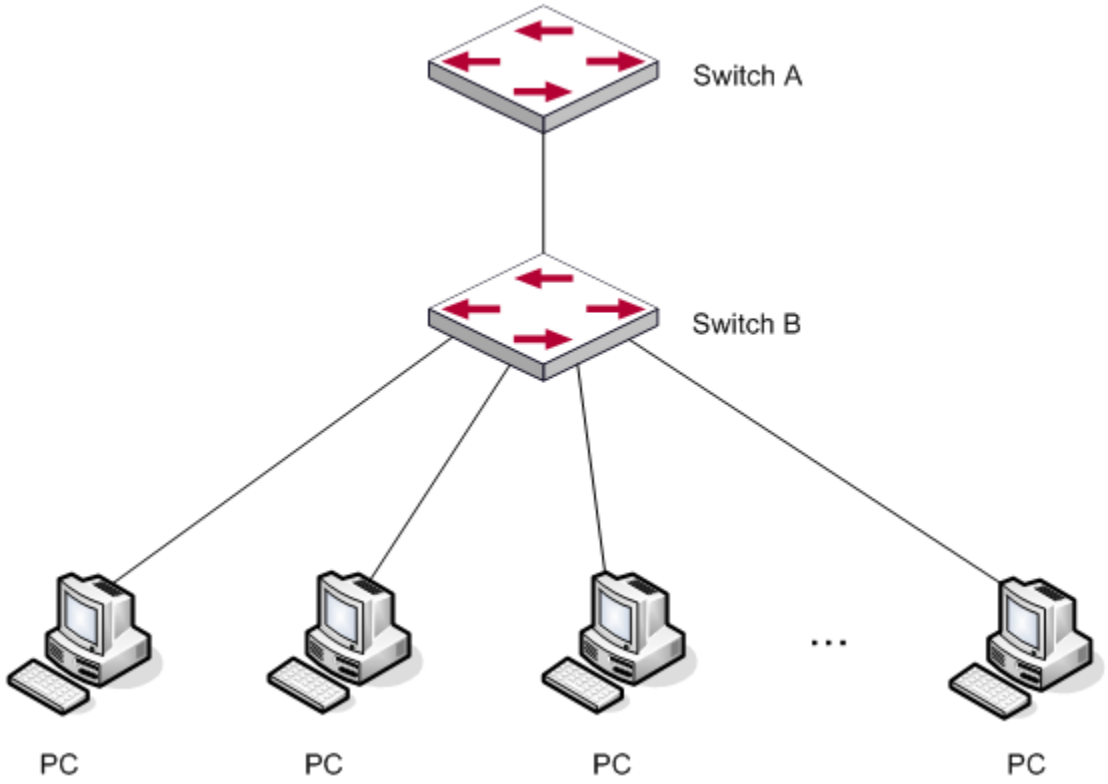
Команда	Описание
Режим конфигурации порта	
switchport mac-address violation {protect / shutdown} [recovery <5-3600>] **no switchport mac-address violation**	Позволяет настроить режим нарушений для порта. Команда no восстанавливает режим защиты для порта.

5. Отображение информации и отладка функций ограничения MAC и IP на портах.

Команда	Описание
Режим администратора	
show mac-address dynamic count {vlan *<vlan-id>*	Позволяет отобразить текущее количество динамических MAC-

| interface ethernet <portName> }	адресов на соответствующих портах и на VLAN.
show arp-dynamic count {vlan <vlan-id> | interface ethernet <*portName*> }	Позволяет отобразить текущее количество динамических ARP на соответствующих портах и на VLAN.
show nd-dynamic count {vlan <*vlan-id*> | interface ethernet <*portName*> }	Позволяет отобразить текущее количество динамических ND на соответствующих портах и на VLAN.
debug switchport mac count **no debug switchport mac count**	Позволяет выводить полную отладочную информацию по ограничениям MAC-адресов на порту.
debug switchport arp count **no debug switchport arp count**	Позволяет выводить полную отладочную информацию по ограничениям ARP на порту.
debug switchport nd count **no debug switchport nd count**	Позволяет выводить полную отладочную информацию по ограничениям ND на порту.
debug vlan mac count **no debug vlan mac count**	Позволяет выводить полную отладочную информацию по ограничениям MAC-адресов на VLAN.
debug ip arp count **no debug ip arp count**	Позволяет выводить полную отладочную информацию по ограничениям ARP на VLAN.
debug ipv6 nd count **no debug ipv6 nd count**	Позволяет выводить полную отладочную информацию по ограничениям ND на VLAN.

3.3 Примеры ограничения MAC и IP-адресов на порту и на VLAN



Как показано выше, многие ПК подключены к коммутатору SwitchB, при неактивной функции ограничения MAC и IP на портах и на VLAN коммутаторы SwitchA и SwitchB могут получить MAC-адреса, ARP и ND записи со всех ПК при отсутствии аппаратных ограничений. Поэтому ограничение пользователей на портах и VLAN поможет избегать DOS атак в известной степени.

На порту 1/1/1 коммутатора SwitchA установите максимальное количество динамических MAC-адресов 20, динамических ARP-адресов – 20, ND – 10. В VLAN1 установите максимальное количество динамических MAC-адресов 30, динамических ARP-адресов – 30, ND – 20.

```
SWITCH A configuration task sequence:
Switch (config)#interface ethernet 1/1/1
Switch (Config-If-Ethernet1/1/1)#switchport mac-address dynamic maximum 20
Switch (Config-If-Ethernet1/1/1)#switchport arp dynamic maximum 20
Switch (Config-If-Ethernet1/1/1)#switchport nd dynamic maximum 10
Switch (Config-if-Vlan1)#vlan mac-address dynamic maximum 30
```

3.4 Поиск неисправностей в функциях ограничения MAC, ARP и ND

Функция ограничения MAC, ARP и ND на портах и VLAN отключена изначально. Если не удаётся настроить данную функцию, проверьте, активированы ли функции Spanning Tree,

dot1x, транка на коммутаторе, или порт настроен как привязочный порт для MAC. Функция ограничения MAC, ARP и ND на портах и VLAN не работает одновременно с вышеперечисленными функциями, соответственно, при необходимости активировать и настроить её отключите функции Spanning Tree, dot1x, транка на коммутаторе.

При необходимости используются отладочные и информационные команды для получения полной информации о текущем состоянии на портах и VLAN с ограничениями.

4 КОНФИГУРИРОВАНИЕ ФУНКЦИИ AM

4.1 Введение в функцию AM

При AM (access management — управление доступом), информация принятых данных сообщений (IP-адрес источника или IP-адрес источника + MAC-адрес источника) сравнивается с настройками пула аппаратных адресов. При обнаружении совпадения сообщение передается, в противном случае – отбрасывается. Пул адресов AM — это список адресов, каждый элемент этого списка соответствует определенному пользователю. Каждый элемент списка состоит из адреса и порта, ему соответствующего. Адреса могут быть двух типов: IP-адрес (в IP-пуле) — это IP-адрес источника пользователя, соответствующий порту.

MAC-IP адрес (в mac-ip пуле) — это MAC-адрес и IP-адрес источника пользователя, соответствующие порту.

Операция AM, выполняемая по умолчанию — это операция deny (запретить). Когда AM включен, модуль AM будет запрещать прохождение всех IP-сообщений (за исключением тех, которые поступают от источников, адреса которых входят в IP-пул). Когда AM выключен, все пулы адресов отсутствуют.

4.2 Настройка функции AM

1. Включение/отключение функции AM.

Команда	Описание
Общий режим	
am enable **no am enable**	Включает функцию управления доступом (AM) для настройки пула адресов. Команда no отменяет AM и удаляет все пулы адресов.

2. Включение/отключение функции AM на интерфейсе.

Команда	Описание
Режим конфигурации порта	
am port **no am port**	Включает функцию AM физического интерфейса. При активированной на порту функции ни одно сообщение IP или ARP не будет переадресовано по умолчанию. Команда no выключает функцию AM

	физического интерфейса.

3. Настройка IP-адреса переадресации.

Команда	Описание
Режим конфигурации порта	
am ip-pool *<ip-address> <num>* **no am ip-pool *<ip-address> <num>***	Осуществляет настройку IP-адреса на физическом интерфейсе. Команда no удаляет настройки IP-адресов на интерфейсе.

4. Настройка MAC IP-адреса переадресации.

Команда	Описание
Режим конфигурации порта	
am mac-ip-pool *<mac-address> <ip-address>* **no am mac-ip-pool *<mac-address> <ip-address>***	Осуществляет настройку MAC IP-адреса на физическом интерфейсе. Команда no удаляет настройки MAC IP-адресов на интерфейсе.

5. Удаление всей конфигурации на интерфейсе.

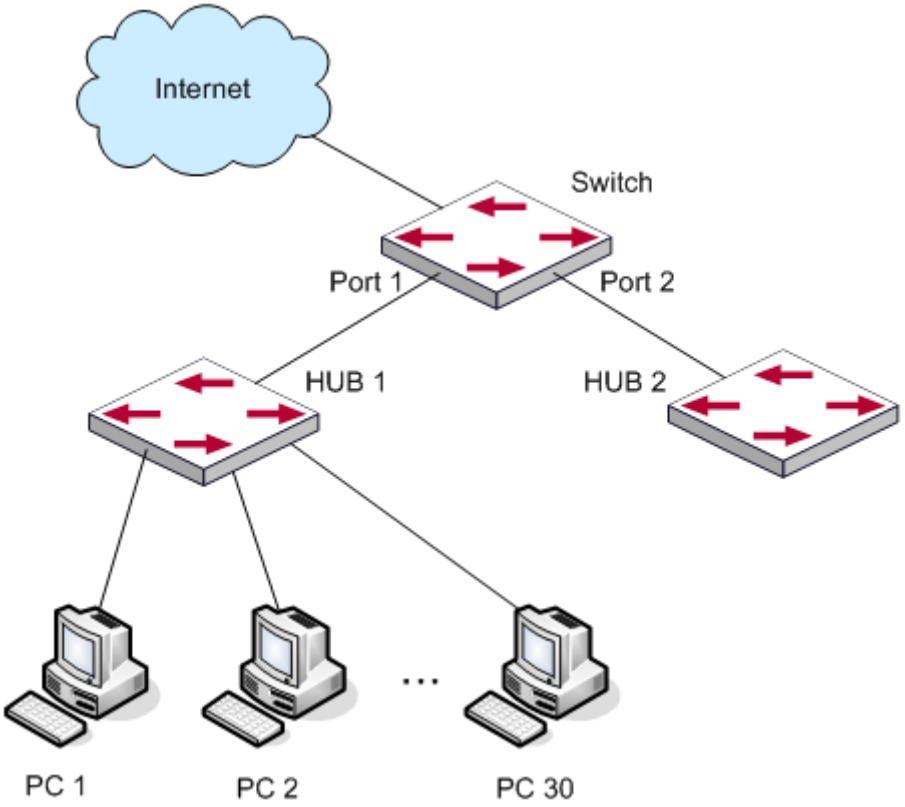
Команда	Описание
Режим конфигурации порта	
no am all [ip-pool|mac-ip-pool]	Удаляет все MAC-IP пулы или IP-пулы, созданные пользователями.

6. Отображение соответствующей конфигурационной информации AM.

Команда	Описание
Общий режим	

show am [interface *<interface-name>*]	Отображает соответствующую конфигурационную информацию AM по одному порту или всем.

4.3 Пример использования функции AM



Как показано выше, в сети 30 ПК, подключённых через концентратор (Hub 1) к коммутатору через интерфейс 1 (Port 1). IP-адреса этих ПК находятся в диапазоне от 100.10.10.1 до 100.10.10.30. Согласно политике безопасности, пользователь, управляющий сетью, будет расценивать эти 30 IP-адресов как легальные. Коммутатор будет пересылать только пакеты от этих IP-адресов, а пакеты от других адресов отбрасывать.

Конфигурация следующая:

```
Switch(config)#am enable
Switch(config)#interface ethernet1/1/1
Switch(Config-If-Ethernet 1/1/1)#am port
Switch(Config-If-Ethernet 1/1/1)#am ip-pool 10.10.10.1 10
```

4.4 Поиск неисправностей функции AM

Функция AM отключена по умолчанию, после активирования её можно настраивать. Пользователь может посмотреть информацию об активности функции AM на каждом интерфейсе при помощи команды «show am». Если возникают проблемы при функционировании AM, система выводит подробную информацию об ошибках.

5 КОНФИГУРИРОВАНИЕ TACACS+

5.1 Введение в TACACS+

TACACS+ представляет собой сеансовый протокол контроля доступа, похожий на протокол RADIUS, и использующий три независимые функции: Аутентификация, Авторизация и Аккаунтинг (учёт). В отличие от RADIUS протокол TACACS+ использует TCP для транспорта пакетов, что повышает уровень безопасности соединения. Однако протокол TACACS+ позволяет обрабатывать несколько запросов от пользователей одновременно, что повышает скорость его работы, также используется шифрование всего пакета, что весьма существенно сказывается на уровне безопасности.

5.2 Настройка TACACS+

1. Настройка ключа аутентификации TACACS+.

Команда	Описание
Общий режим	
tacacs-server key {0 | 7}*<string>* **no tacacs-server key**	Настраивает конфигурационный ключ TACACS+. Команда no удаляет текущий ключ.

2. Настройка TACACS+ сервера.

Команда	Описание
Общий режим	
tacacs-server authentication host *<ip-address>* [port *<port-number>*] [timeout *<seconds>*] [key {0 | 7} *<string>*] [primary] **no tacacs-server authentication host *<ip-address>***	Настраивает IP-адрес сервера, номер слушающего порта, значение таймаута и ключевую строку сервера. Команда no удаляет все текущие настройки сервера.

3. Настройка таймаута аутентификации на сервере TACACS+.

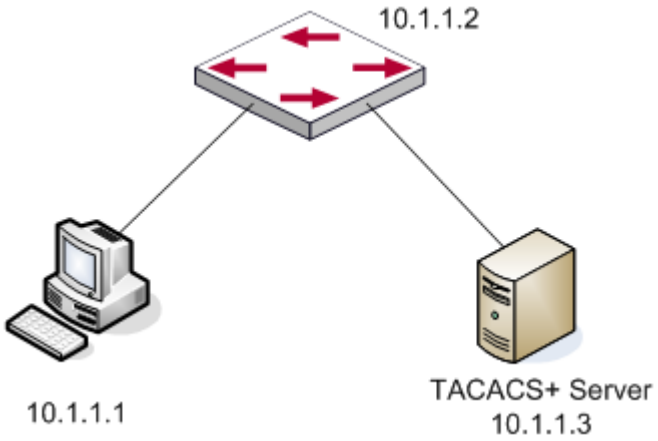
Команда	Описание
Общий режим	

tacacs-server timeout *<seconds>* **no tacacs-server timeout**	Настраивает значение таймаута аутентификации сервера TACACS+. Команда no удаляет все текущие настройки сервера.

4. Настройка IP-адреса NAS для сервера TACACS+.

Команда	Описание
Общий режим	
tacacs-server nas-ipv4 *<ip-address>* **no tacacs-server nas-ipv4**	Настраивает значение IP-адреса NAS для сервера TACACS+. Команда no удаляет все текущие настройки сервера.

5.3 Пример использования TACACS+



Как показано выше, ПК подключён к коммутатору с IP-адресом 10.1.1.2, который соединён с TACACS+ сервером аутентификации. IP-адрес сервера аутентификации 10.1.1.3 и порт по умолчанию 49. Процесс аутентификации на сервере TACACS+ отображается при помощи Telnet:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#tacacs-server authentication host 10.1.1.3
Switch(config)#tacacs-server key test
Switch(config)#authentication line vty login tacacs
```

5.4 Поиск неисправностей TACACS+

При использовании аутентификации TACACS+ могут возникать проблемы с физическим соединением или вследствие неправильной конфигурации. Проверьте следующие причины:

- В первую очередь проверяется физическое соединение с сервером аутентификации TACACS+.
- Во-вторых, все интерфейсы и протоколы соединения должны быть в активном состоянии.
- Далее следует убедиться, что ключ аутентификации на коммутаторе совпадает с ключом на TACACS+ сервере.
- Также следует убедиться, что подключение осуществляется к правильному TACACS+ серверу.

6 КОНФИГУРИРОВАНИЕ RADIUS

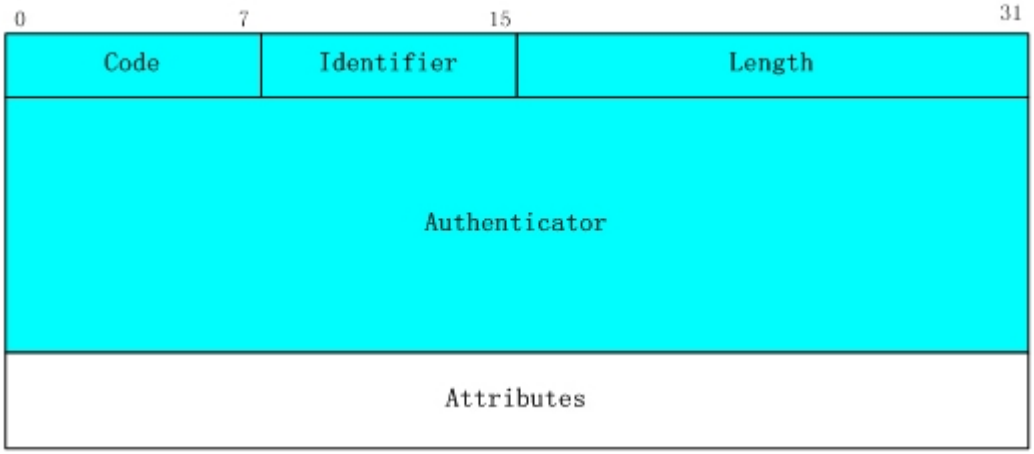
6.1 Введение в RADIUS и принцип AAA

Принцип трёх А (Аутентификация, Авторизация и Аккаунтинг (учёт)) используется в процессе предоставления доступа в Интернет и для контроля за ним. В процессе аутентификации пользователь идентифицируется, процесс авторизации определяет круг прав пользователя и в результате аккаунтинга учитываются используемые пользователем сервисы.

RADIUS (Remote Authentication Dial in User Service) это сетевой протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и аккаунтинга пользователей, подключающихся к различным сетевым службам. Клиент RADIUS используется, как правило, на сетевом устройстве для применения принципа AAA совместно с аутентификацией по протоколу 802.1x. RADIUS-сервер управляет базой данных для AAA и общается с клиентами RADIUS по протоколу RADIUS, который является самым распространённым для аутентификации в рамках AAA.

6.2 Структура сообщений RADIUS

Протокол RADIUS использует протокол UDP для транспорта пакетов. Формат пакетов показан ниже на схеме.



- Code (1 октет) – тип пакета RADIUS, доступные значения для данного поля перечислены ниже:
  - ✓ Access-Request.
  - ✓ Access-Accept.
  - ✓ Access-Reject.
  - ✓ Accounting-Request.
  - ✓ Accounting-Response.
  - ✓ Access-Challenge.
- Identifier (1 октет) – идентификатор для пакетов запроса и ответа.

- Length (2 октета) – длина всего пакета RADIUS.
- Authenticator (16 октетов) – поле используется для проверки пакетов, полученных от RADIUS-сервера, или для передачи зашифрованных паролей. Поле делится на две части: аутентификатор запросов и аутентификатор ответов.
- Attribute – поле используется для передачи детальной информации о AAA. Значение поля формируется из значений полей Type, Length, и Value:
  - ✓ Type field (1 октет) - тип атрибута, значения атрибутов представлены в таблице ниже.

Номер атрибута	Значение	Номер атрибута	Значение
1 - User-Name	Имя пользователя	23 - Framed-IPX-Network	Номер сети IPX для пользователя
2 - User-Password	Пароль	24 - State	Атрибут пакета Access-Challenge
3 - CHAP-Password	Значение отклика протокола CHAP	25 - Class	Атрибут пакета Access-Accept
4 - NAS-IP-Address	IP-адрес NAS-сервера	26 - Vendor-Specific	Спецификация вендора
5 - NAS-Port	Порт NAS-сервера	27 - Session-Timeout	Таймаут пользовательской сессии в секундах
6 - Service-Type	Тип сервиса	28 - Idle-Timeout	Таймаут непрерывного бездействия сессии
7 - Framed-Protocol	Тип кадров	29 - Termination-Action	Действие, выполняемое NAS по завершении сеанса
8 - Framed-IP-Address	Предоставленный пользователю IP-адрес	30 - Called-Station-Id	Номер телефона, набранный пользователем
9 - Framed-IP-Netmask	Предоставленная пользователю маска подсети	31 - Calling-Station-Id	Телефонный номер пользователя
10 - Framed-Routing	Метод маршрутизации для пользователя	32 - NAS-Identifier	Идентификатор NAS
11 - Filter-Id	Имя списка фильтров для пользователя	33 - Proxy-State	Атрибут пакета Access-Request
12 - Framed-	Значение MTU	34 - Login-	Система, к которой

MTU	(максимальный размер кадра)	LAT-Service	пользователь подключается по протоколу LAT
13 - Framed-Compression	Протокол компрессии	35 - Login-LAT-Node	Узел, к которому пользователь автоматически подключён по протоколу LAT
14 - Login-IP-Host	IP-адрес хоста для подключения пользователя	36 - Login-LAT-Group	Идентификатор кодов группы LAT
15 - Login-Service	Служба для входа пользователя в систему	37 - Framed-AppleTalk-Link	Номер сети AppleTalk, который следует для последовательного канала пользователя, который является другим маршрутизатором AppleTalk
16 - Login-TCP-Port	Порт TCP для подключения пользователя	38 - Framed-AppleTalk-Network	Номер сети AppleTalk, который серверу NAS следует проверить для выделения номера узла AppleTalk пользователю.
17 - (unassigned)	Не используется	39 - Framed-AppleTalk-Zone	Принятая по умолчанию зона AppleTalk
18 - Reply-Message	Текст, выводимый на консоль пользователя	40-59 - (reserved for accounting)	Зарезервировано для аккаунтинга
19 - Callback-Number	Номер для обратного звонка	60 - CHAP-Challenge	Запрос CHAP Challenge, передаваемый сервером NAS пользователю PPP CHAP
20 - Callback-Id	Идентификатор для обратного звонка	61 - NAS-Port-Type	Тип порта NAS-сервера
21 - (unassigned)	Не используется	62 - Port-Limit	Максимальное число портов NAS, открытых для подключения пользователя
22 - Framed-	Маршрутная информация	63 - Login-	Порт для подключения

Route	для пользователя NAS	LAT-Port	пользователя по протоколу LAT

- ✓ Length field (1 октет) – длина атрибута в октетах.
- ✓ Value field – значение атрибута.

6.3 Настройка RADIUS

1. Настройка функций аутентификации и аккаунтинга.

Команда	Описание
Общий режим	
aaa enable **no aaa enable**	Активирует функцию AAA для аутентификации. Команда no отключает функцию AAA для аутентификации.
aaa-accounting enable **no aaa-accounting enable**	Активирует функцию AAA для аккаунтинга. Команда no отключает функцию AAA для аккаунтинга.
aaa-accounting update {enable/disable}	Включает или отключает обновление функции аккаунтинга

2. Настройка ключа аутентификации RADIUS.

Команда	Описание
Общий режим	
radius-server key {0 | 7} *<string>* **no radius-server key**	Настраивает ключ шифрования для RADIUS-сервера. Команда no удаляет текущий ключ.

3. Настройка RADIUS-сервера.

Команда	Описание
Общий режим	
radius-server authentication host {*<ipv4-address>* | *<ipv6-address>*} [port *<port-*	Настраивает значение IPv4/IPv6 адреса и номер порта, а также основной статус

number>] [key {0 | 7} <string>] [primary] [access-mode {dot1x | telnet}] **no radius-server authentication host {*<ipv4-address>* | *<ipv6-address>***	RADIUS-сервера для аутентификации. Команда no удаляет все текущие настройки сервера.
radius-server accounting host {<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary] **no radius-server accounting host {<ipv4-address> / <ipv6-address>}**	Настраивает значение IPv4/IPv6 адреса и номер порта, а также основной статус RADIUS-сервера для аккаунтинга. Команда no удаляет все текущие настройки сервера.

4. Настройка параметров RADIUS-сервера.

Команда	Описание
Общий режим	
radius-server dead-time *<minutes>* **no radius-server dead-time**	Позволяет задать время восстановления RADIUS-сервера после его выключения и повторного включения Команда no удаляет все текущие настройки.
radius-server retransmit *<retries>* **no radius-server retransmit**	Позволяет настроить для RADIUS число попыток повторной передачи пакетов аутентификации. Команда no удаляет все текущие настройки.
radius-server timeout *<seconds>* **no radius-server timeout**	Позволяет настроить для RADIUS-сервера время таймаута. Команда no удаляет все текущие настройки.
radius-server accounting-interim-update timeout *<seconds>* **no radius-server accounting-interim-update timeout**	Позволяет задать интервал отправки сообщений обновления информации учета сервисов. Команда no удаляет все текущие настройки.

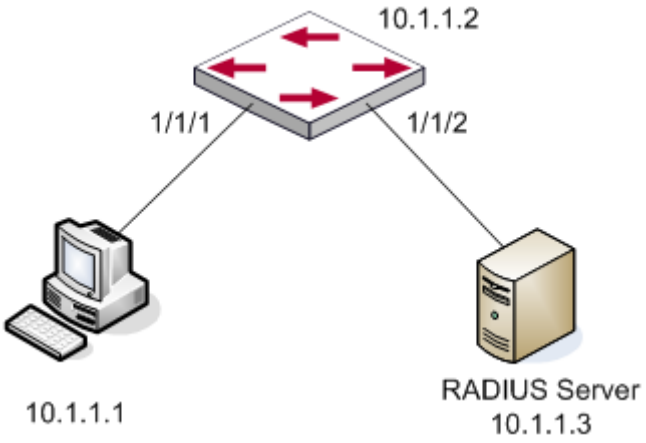
5. Настройка IP-адреса NAS-сервера.

Команда	Описание
Общий режим	

radius nas-ipv4 *<ip-address>* **no radius nas-ipv4**	Позволяет задать IPv4 адрес источника для пакетов RADIUS, посылаемых коммутатором. Команда no удаляет все текущие настройки.
radius nas-ipv6 *<ipv6-address>* **no radius nas-ipv6**	Позволяет задать IPv6 адрес источника для пакетов RADIUS, посылаемых коммутатором. Команда no удаляет все текущие настройки

6.4 Пример использования RADIUS

6.4.1 Пример IPv4 RADIUS

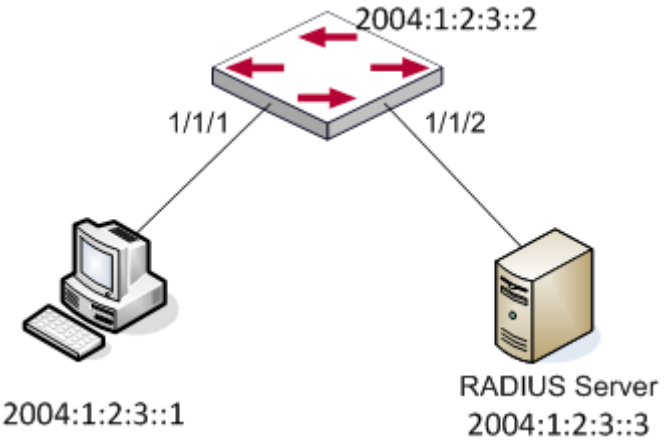


ПК соединён с коммутатором, IP-адрес которого 10.1.1.2. Коммутатор соединяется с RADIUS-сервером аутентификации без интерфейса Ethernet 1/1/2, IP-адрес RADIUS-сервера 10.1.1.3 и порт по умолчанию для аутентификации 1812, порт по умолчанию для аккаунтинга – 1813.

Шаги конфигурации следующие:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

6.4.2 Пример IPv6 RADIUS



ПК соединён с коммутатором, IP-адрес которого 2004:1:2:3::2. Коммутатор соединяется с RADIUS-сервером аутентификации без интерфейса Ethernet 1/1/2, IP-адрес RADIUS-сервера 2004:1:2:3::3 и порт по умолчанию для аутентификации 1812, порт по умолчанию для аккаунтинга – 1813.

Шаги конфигурации следующие:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ipv6 address 2004:1:2:3::2/64
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 2004:1:2:3::3
Switch(config)#radius-server accounting host 2004:1:2:3::3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

6.5 Поиск неисправностей RADIUS

При использовании аутентификации RADIUS могут возникать проблемы с физическим соединением или вследствие неправильной конфигурации. Проверьте следующие причины:

- В первую очередь проверяется физическое соединение с сервером аутентификации RADIUS.
- Во-вторых, все интерфейсы и протоколы соединения должны быть в активном состоянии.
- Далее следует убедиться, что ключ аутентификации на коммутаторе совпадает с ключом на RADIUS-сервере.
- Также следует убедиться, что подключение осуществляется к правильному RADIUS-серверу.

Для получения более детальной информации о работе RADIUS аутентификации используйте отладочную команду «debug ааа».

7 КОНФИГУРИРОВАНИЕ ФУНКЦИИ RA SECURITY

7.1 Введение в RA Security

Как правило, топология IPv6 сети включает маршрутизаторы, коммутаторы 2 уровня и IPv6 хосты. Маршрутизаторы объявляют о своём статусе сообщениями RA (Router Advertisement), которое содержит информацию о сетевом префиксе, адресе шлюза, адресах рекурсивных DNS серверов, MTU и множестве других параметров. При получении RA сообщения IPv6 хост создаёт сетевой адрес и устанавливает маршрутизатор по умолчанию в качестве рассылающего RA сообщения для развёртывания IPv6 сети. Если вредоносный IPv6 хост рассылает RA сообщения с целью подмены нормального RA маршрутизатора, злоумышленник может получить доступ к пользовательской информации и заблокировать доступ к сети для нормальных пользователей. Поэтому с целью сохранения безопасности и функциональности сети необходимо отклонять подозрительные RA сообщения на портах коммутатора.

7.2 Настройка RA Security

1. Активация функции RA Security.

Команда	Описание
Общий режим	
ipv6 security-ra enable **no ipv6 security-ra enable**	Активация или деактивация функции RA Security.

2. Активация функции RA Security на порту.

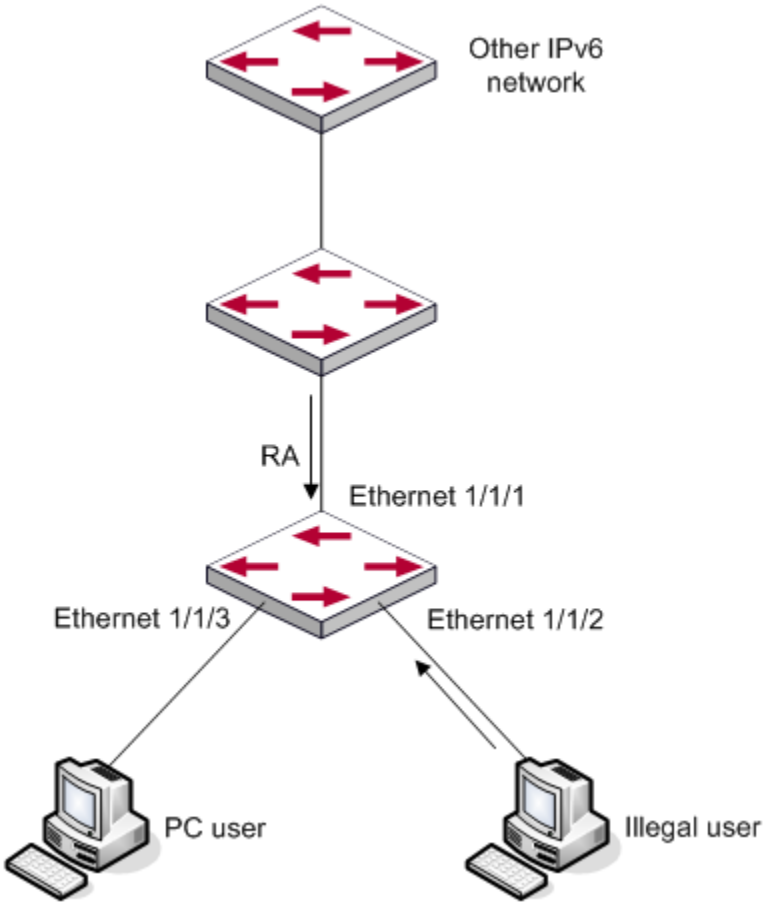
Команда	Описание
Режим конфигурации порта	
ipv6 security-ra enable **no ipv6 security-ra enable**	Активация или деактивация функции RA Security на текущем порту.

3. Отображение отладочной информации для функции RA Security.

Команда	Описание
Режим администратора	

debug ipv6 security-ra **no debug ipv6 security-ra**	Позволяет включить вывод отладочной информации функции RA security при IPv6. Команда no выключает данную функцию.
show ipv6 security-ra [interface *<interface-list>*]	Выводит на дисплей информацию обо всех интерфейсах, на которых включена функция IPv6 RA.

7.3 Пример использования RA Security



Как показано на схеме, если злоумышленник рассылает RA сообщения, то при получении такого сообщения обычным пользователем маршрутизатор по умолчанию подменяется вредоносным IPv6 хостом. Вследствие чего пользователь не получает доступа в сеть. Необходимо установить функцию RA Security на порту коммутатора 1/1/2, чтобы RA сообщения от злоумышленников не смогли влиять на конфигурацию сети.

Шаги конфигурации следующие:

```
Switch configuration task sequence:
Switch#config
```

```
Switch(config)#ipv6 security-ra enable
Switch(Config-If-Ethernet1/1/2)# ipv6 security-ra enable
```

7.4 Поиск неисправностей RA Security

Если функция RA Security работает каким-то образом неправильно, проверьте следующие причины:

- Конфигурация коммутатора должна быть корректной.
- На коммутаторе могут быть настроены некоторые правила, конфликтующие с RA Security, и вызывающие пересылку RA сообщений.

8 КОНФИГУРИРОВАНИЕ VLAN-ACL

8.1 Введение в VLAN-ACL

Пользователь может применять политику листов доступа ACL для всех портов VLAN, а VLAN-ACL помогает пользователю более целесообразно управлять сетью. Пользователю необходимо только настроить политику ACL для VLAN, и соответствующие действия будут применяться ко всем портам сети VLAN.

При одновременном наличии VLAN-ACL и Port-ACL первым используется принцип отказа в доступе. Исходящие ACL могут применяться для фильтрации входящих и исходящих пакетов, пакеты, соответствующие тем или иным правилам, могут отбрасываться или пропускаться.

ACL поддерживает IP ACL, MAC ACL, MAC-IP ACL, IPv6 ACL. Входящее направление VLAN может быть привязано к четырём видам списков доступа одновременно, в то время как на исходящем направлении VLAN одновременно не могут существовать четыре вида привязок. Если создаются одновременно три вида списков доступа, это должны быть IP, MAC и MAC-IP, либо IP, MAC и IPv6. При создании двух видов ACL можно использовать любые виды ACL.

8.2 Настройка VLAN-ACL

1. Настройка VLAN-ACL типа IP.

Команда	Описание
Общий режим	
vacl ip access-group {<1-299> | WORD} {in | out} [traffic-statistic] vlan WORD **no vacl ip access-group {<1-299> | WORD} {in | out} vlan WORD**	Настройка или удаление списка доступа IP ACL.

2. Настройка VLAN-ACL типа MAC.

Команда	Описание
Общий режим	
vacl mac access-group {<700-1199> | WORD} {in | out} [traffic-statistic] vlan WORD **no vacl mac access-group {<700-1199> |**	Настройка или удаление списка доступа MAC ACL.

WORD} {in | out} vlan WORD	

3. Настройка VLAN-ACL типа MAC-IP.

Команда	Описание
Общий режим	
vacl mac-ip access-group {<3100-3299> | WORD} {in | out} [traffic-statistic] vlan WORD **no vacl mac-ip access-group {<3100-3299> | WORD} {in | out} vlan WORD**	Настройка или удаление списка доступа MAC-IP ACL.

4. Настройка VLAN-ACL типа IPv6.

Команда	Описание
Общий режим	
vacl ipv6 access-group (<500-699> | WORD) {in | out} (traffic-statistic|) vlan WORD **no ipv6 access-group {<500-699> | WORD} {in | out} vlan WORD**	Настройка или удаление списка доступа IPv6 ACL.

5. Отображение отладочной информации для функции VLAN-ACL.

Команда	Описание
Режим администратора	
show vacl [in | out] vlan [<*vlan-id*>]	Выводит на дисплей информацию о VLAN-ACL.

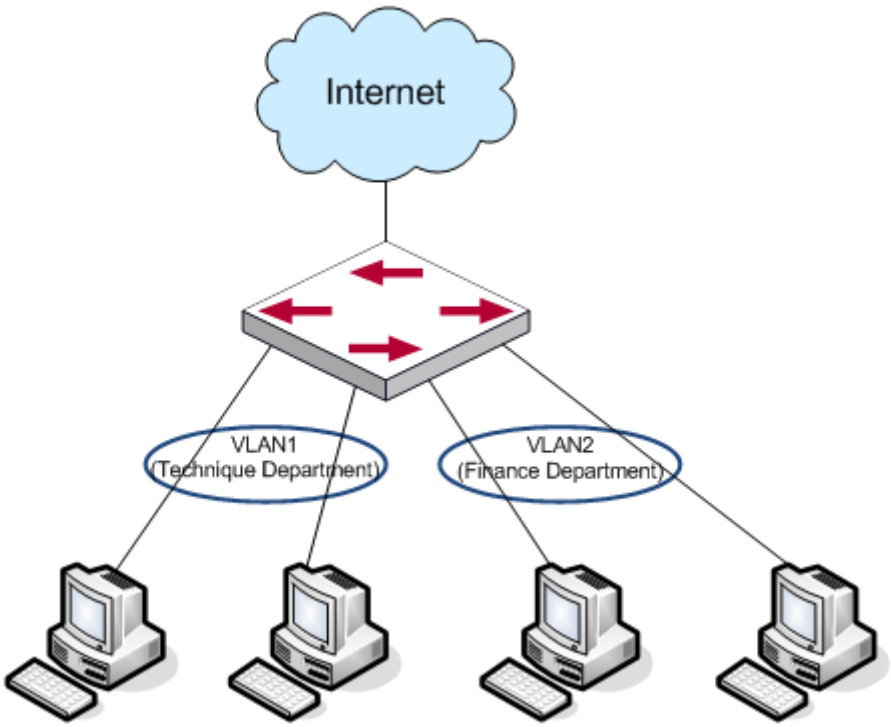
6. Очистка статистической информации VLAN-ACL.

Команда	Описание
Режим администратора	
clear vacl [in | out] statistic vlan [<*vlan-id*>]	Очищает статистическую информацию о VLAN-ACL.

8.3 Пример использования VLAN-ACL

Типичная корпоративная сеть имеет несколько различных сетей VLAN, соответствующих отделам. Как показано ниже на рисунке: VLAN1 – сеть технического отдела, VLAN2 – сеть финансового отдела. Политика компании требует, чтобы пользователи сети VLAN1 имели выход во внешнюю сеть, а пользователи сети VLAN2 – не имели. Выполняется настройка следующих политик:

- Установите политику VACL_A для технического отдела, заключающуюся в предоставлении доступа во внешнюю сеть согласно рабочему расписанию. Данная политика будет применяться для сети VLAN1.
- Установите политику VACL_B для финансового отдела, заключающуюся в отказе доступа во внешнюю сеть без ограничений по времени. Данная политика будет применяться для сети VLAN2.



Примеры конфигурации:

1. Настройте временной диапазон рабочего времени для доступа во внешнюю сеть:

```
Switch(config)#time-range t1
Switch(config-time-range-t1)#periodic weekdays 9:00:00 to 12:00:00
Switch(config-time-range-t1)#periodic weekdays 13:00:00 to 18:00:00
```

2. Настройте расширенный ACL_A, IP-адреса из которого будут иметь доступ в рамках рабочего времени к ресурсам внутри сети (например, 192.168.0.255):

```
Switch(config)# ip access-list extended vacl_a
Switch(config-ip-ext-nacl-vacl_a)#  permit  ip  any-source  192.168.0.0 0.0.0.255 time-range t1
Switch(config-ip-ext-nacl-vacl_a)# deny ip any-source any-destination time-range t1
```

3. Настройте расширенный ACL_B, IP-адреса из которого будут иметь доступ только к ресурсам внутри сети (например, 192.168.1.255):

```
Switch(config)#ip access-list extended vacl_b
Switch(config-ip-ext-nacl-vacl_a)#  permit  ip  any-source  192.168.1.0 0.0.0.255
Switch(config-ip-ext-nacl-vacl_a)# deny ip any-source any-destination
```

4. Примените конфигурацию к сети:

```
Switch(config)#vacl ip access-group vacl_a in vlan 1
Switch(config)#vacl ip access-group vacl_b in vlan 2
```

8.4 Поиск неисправностей VLAN-ACL

- При одновременном наличии VLAN-ACL и Port-ACL первым используется принцип отказа в доступе. Если пакеты совпадают с VLAN-ACL и Port-ACL, и первое правило регламентирует отбрасывать пакеты, то пакеты будут отброшены.
- Каждый тип ACL может быть применён только один раз к одной сети VLAN.

9 КОНФИГУРИРОВАНИЕ MAB

9.1 Введение в MAB

Во многих сетях присутствуют устройства, не имеющие возможности использовать аутентификацию по протоколу 802.1x (сетевые принтеры, КПК и др.). К таким устройствам применяется аутентификация MAB (MAC Authentication Bypass), которая основывается на MAC-адресе устройства и порте доступа. Пользователю не нужно устанавливать какого-либо клиента аутентификации или вводить логин и пароль в процессе. В процессе аутентификации коммутатор получает ARP-пакеты от MAB-пользователя, и после нахождения соответствия с аутентификационной информацией на сервере (порт и MAC-адрес источника) аутентификация будет успешной.

В настоящий момент MAB аутентификация поддерживает только использование RADIUS аутентификации. Используйте MAC-адрес MAB-пользователя в качестве логина и пароля, или заранее установленные логин и пароль.

9.2 Настройка MAB

1. Активация функции MAB аутентификации.

Команда	Описание
Общий режим	
mac-authentication-bypass enable **no mac-authentication-bypass enable**	Позволяет включить или отключить функцию MAB аутентификации.
Режим конфигурации порта	
mac-authentication-bypass enable **no mac-authentication-bypass enable**	Позволяет включить или отключить функцию MAB аутентификации на текущем порту.

2. Настройка логина и пароля для MAB аутентификации.

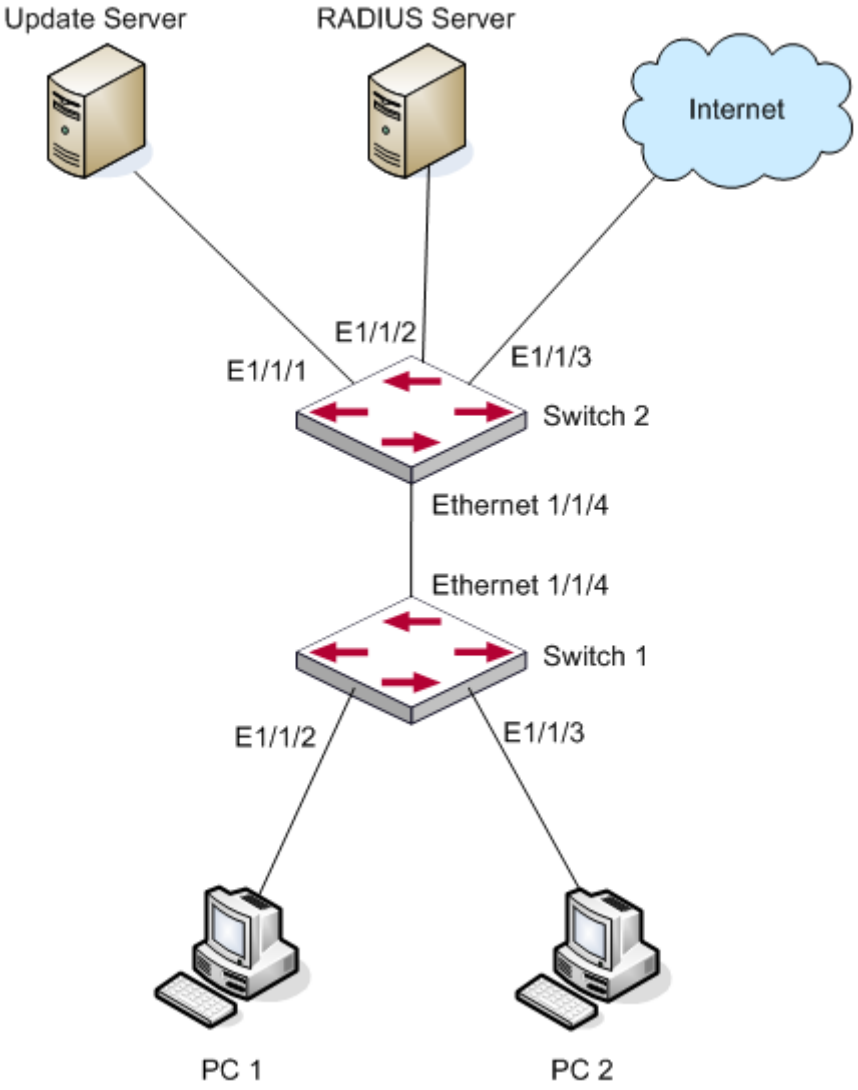
Команда	Описание
Общий режим	
mac-authentication-bypass username-format {mac-address | {fixed username WORD password WORD}}	Устанавливает метод MAB-аутентификации – использовать MAC-адрес в качестве логина и пароля или установить фиксированные значения логина и пароля.

3. Настройка параметров MAB.

Команда	Описание
Режим конфигурации порта	
mac-authentication-bypass guest-vlan <1-4094> **no mac-authentication-bypass guest-vlan**	Устанавливает гостевой VLAN для MAB аутентификации. Команда применяется только для гибридных портов, не для портов доступа. Команда no выключает данную функцию.
mac-authentication-bypass binding-limit <1-100> **no mac-authentication-bypass binding-limit**	Устанавливает максимальное количество привязок MAB.
Общий режим	
mac-authentication-bypass timeout reauth-period <1-3600> **no mac-authentication-bypass timeout reauth-period**	Устанавливает интервал повторной аутентификации для состояния неудачной аутентификации.
mac-authentication-bypass timeout offline-detect (0|<60-7200>) **no mac-authentication-bypass timeout offline-detect**	Устанавливает offline-время определения MAB привязок.
mac-authentication-bypass timeout quiet-period <1-60> **no mac-authentication-bypass timeout quiet-period**	Устанавливает период тишины (quiet-period) MAB привязок. Если аутентификация закончилась неудачно, во время этого периода коммутатор перестаёт отвечать на запросы аутентификации с этого MAC-адреса
mac-authentication-bypass timeout stale-period <0-60> **no mac-authentication-bypass timeout stale-period**	Устанавливает период, по прошествии которого удаляется привязка, после того, как MAB-порт перешел в состояние down.
mac-authentication-bypass timeout linkup-period <0-30> **no mac-authentication-bypass timeout linkup-**	Устанавливает период между переключениями состояний down и up, когда привязка VLAN на порту

period	меняется, для гарантии того, что пользователь может получить IP-адрес снова.
mac-authentication-bypass spoofing-garp-check enable **no mac-authentication-bypass spoofing-garp-check enable**	Активирует функцию spoofing-garp-check. Команда no выключает данную функцию.
authentication mab {radius | none} **no authentication mab**	Настраивает режим аутентификации и приоритет MAC-адресов. Команда no восстанавливает настройки, заданные по умолчанию.

9.3 Пример использования MAB



На схеме представлены следующие элементы:

- Switch 1 – коммутатор доступа 2 уровня.
- Switch 2 – коммутатор агрегации 3 уровня.
- Ethernet 1/1/1 – порт доступа Switch 1, соединённый с PC1, поддерживающий функцию 802.1x на базе порта и гостевую сеть VLAN8. Порт принадлежит VLAN8 и соединяется с сервером обновлений.
- Ethernet 1/1/2 – гибридный порт, соединённый с PC2, локальная сеть на порту VLAN1, гостевую сеть VLAN8. Порт объединяет VLAN1, VLAN8 и VLAN10 нетегированным методом и поддерживает функцию MAB. Порт также является портом доступа, принадлежащий VLAN9, и подключённый к RADIUS-серверу, который конфигурирует auto vlan как VLAN10.
- Ethernet 1/1/3 – порт доступа, соединённый с принтером и поддерживающий функцию MAB. Порт принадлежит VLAN10 и соединяется с Интернет ресурсами.
- Ethernet 1/1/4 – транк порт коммутатора Switch2, соединённый с Switch1.

Шаги конфигурации следующие:

1. Активируйте функции аутентификации 802.1x и MAB в общем режиме, настройте логин и пароль для MAB и IP-адрес RADIUS-сервера.

```
Switch(config)# dot1x enable
Switch(config)# mac-authentication-bypass enable
Switch(config)#mac-authentication-bypass username-format fixed username mabuser password mabpwd
Switch(config)#vlan 8-10
Switch(config)#interface vlan 9
Switch(config-if-vlan9)ip address 192.168.61.9 255.255.255.0
Switch(config-if-vlan9)exit
Switch(config)#radius-server authentication host 192.168.61.10
Switch(config)#radius-server accounting host 192.168.61.10
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

2. Активируйте функцию аутентификации на каждом порту.

```
Switch(config)#interface ethernet  1/1/1
Switch(config-if-ethernet1/1/1)#dot1x enable
Switch(config-if-ethernet1/1/1)#dot1x port-method portbased
Switch(config-if-ethernet1/1/1)#dot1x guest-vlan 8
Switch(config-if-ethernet1/1/1)#exit

Switch(config)#interface ethernet 1/1/2
Switch(config-if-ethernet1/1/2)#switchport mode hybrid
Switch(config-if-ethernet1/1/2)#switchport hybrid native vlan 1
Switch(config-if-ethernet1/1/2)#switchport hybrid allowed vlan 1;8;10 untag
```

```
Switch(config-if-ethernet1/1/2)#mac-authentication-bypass enable
Switch(config-if-ethernet1/1/2)#mac-authentication-bypass  enable  guest-vlan
8
Switch(config-if-ethernet1/1/2)#exit

Switch(config)#interface ethernet 1/1/3
Switch(config-if-ethernet1/1/3)#switchport mode access
Switch(config-if-ethernet1/1/3)#mac-authentication-bypass enable
Switch(config-if-ethernet1/1/3)#exit

Switch(config)#interface ethernet 1/1/4
Switch(config-if-ethernet1/1/4)# switchport mode trunk
```

9.4 Поиск неисправностей MAB

Если возникают какие-либо проблемы в функционировании MAB, проверьте следующие причины:

- Убедитесь в активации функции MAB в общем режиме и на каждом порту.
- Убедитесь в правильных используемых логине и пароле для аутентификации.
- Убедитесь в корректной конфигурации RADIUS-сервера. Выполните MAB offline-detect запрос для определения действительного динамического MAC-адреса. Не удаляйте привязку, если MAC-адрес содержится в таблице MAC-адресов. Реальное время без трафика составляет 1-2 периода старения MAC-адреса. Добавьте время 0-1 MAB offline-detect.