Internet Engineering Task Force (IETF)
Request for Comments: 8519
Category: Standards Track
ISSN: 2070-1721

M. Jethanandani
VMware
S. Agarwal
Cisco Systems, Inc.
L. Huang
D. Blair

March 2019

YANG Data Model for Network Access Control Lists (ACLs)

Модель данных YANG для списков управления доступом (ACL)

Аннотация

Этот документ задаёт модель данных для списков управления доступом (Access Control List или ACL), представляющих собой упорядоченный пользователем набор правил, служащих для настройки поведения пересылки на устройстве. Каждое правило применяется для сопоставления с пакетами и задает выполняемые по отношению к пакетам действия.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке https://www.rfc-editor.org/info/rfc8519.

Оглавление

1. Введение

Списки управления доступом (ACL) являются одним из базовых элементов настройки поведения пересылающего устройства. Они применяются во многих сетевых технологиях, например, в маршрутизации на основе правил (Policy-Based Routing или PBR), межсетевых экранах и т. п. ACL - это упорядоченный пользователем список правил, служащих

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

для фильтрации трафика на сетевом устройстве. Каждое правило представляет в списке запись управления доступом (Access Control Entry или ACE). Каждая запись ACE имеет набор критериев сопоставления и набор действий.

Критерии сопоставления позволяют задать заголовки и метаданные пакетов, соответствующих правилу.

- Сопоставления заголовков применимы к видимым в пакете полям, таким как адрес, класс обслуживания (Class of Service или CoS), номер порта.
- Если производитель поддерживает это, можно применять сопоставления с полями, связанными с пакетом, которые не входят в заголовки, такими как входной интерфейс или размер пакета, полученного из линии.

Действия указывают, что делать с пакетом, соответствующим критериям сопоставления. Это могут быть любые операции, применимые к пакетам, такие как учёт, применение правил, пересылка и т. п. Набор доступных действий зависит от возможностей сетевого устройства.

Списки управления доступом часто называют просто ACL (произностися ak-uh l) или списками доступа (Access List). В этом документе все три варианта равноценны.

Сопоставление фильтров и действий в ACE/ACL запускается только после применения (присоединения) ACL на интерфейсе, экземпляре виртуальной маршрутизации и пересылки (Virtual Routing and Forwarding или VRF), в сессии vty/tty, политике QoS или протоколах в разных конфигурациях точек присоединения. После подключения списка он служит для сопоставления с ACE и выполнения соответствующих действий, заданных для ACE. Чтобы применить ACL в любой точке присоединения, отличной от интерфейса, производитель должен дополнить модель YANG ACL.

1.1. Определения и сокращения

ACE
Access Control Entry - запись управления доступом.

ACL
Access Control List - список управления доступом.

CoS
Class of Service - класс обслуживания (сервиса)

DSCP
Differentiated Services Code Point - код дифференцированного обслуживания.

ICMP
Internet Control Message Protocol - сообщение протокола управления Internet.

IP
Internet Protocol - протокол Internet.

IPv4
Internet Protocol version 4 - протокол Internet версии 4.

IPv6
Internet Protocol version 6 - протокол Internet версии 6.

MAC
Media Access Control - управление доступом к среде.

PBR
Policy-Based Routing - маршрутизация на основе правил (политики).

TCP
Transmission Control Protocol - протокол управления передачей.

UDP
User Datagram Protocol - протокол пользовательских дейтаграмм.

1.2. Уровни требований

Ключевые слова **должно** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

1.3. Диаграмма дерева

В этом документе применяется графическое представление данных, определённое в YANG Tree Diagrams [RFC8340].

2. Постановка задачи

Этот документ задаёт модель данных YANG 1.1 [RFC7950] для настройки ACL. Модель определяет правила сопоставления для наиболее распространённых протоколов, таких как Ethernet, IPv4, IPv6, TCP, UDP, ICMP. Для поддержки дополнительных протоколов модель может быть расширена. Пример расширения дан в Приложении A.

Реализации ACL в каждом устройстве моугт существенно различаться конструкицями фильтров и поддерживаемыми действиями, поэтому в документе предложена модель, которую можно дополнить стандартными и фирменными моделями.

3. Понимание фильтров и действий ACL

Хотя у разных производителей есть свои модели данных ACL, имеется базовое понимание, что такое ACL. В сетевых системах обычно имеются наборы ACL, каждый из которых содержит упорядоченный список правил, называемых ACE. Каждая запись ACE имеет набор критериев сопоставления и набор действий. Критерии позволяют указать заголовки пакетов или метаданные, если производитель их поддерживает. Сопоставление по заголовкам пакетов применяется к видимым в пакетах полям, таким как адреса, CoS, номер порта. Сопоставление метаданных применяется к связанным с пакетом полям, которые не являются заголовками пакета, таким как входной интерфейс, размер пакета или размер префикса отправителя или получателя. Действиями могут быть любые операции от записи в системный журнал до

ограничесния скорости, отбрасывания или обычной пересылки. Применяются действия первой соответствующей записи ACE без применения последующих ACE.

Модель включает конвейер для хранения общего рабочего состояния каждого списка ACL и каждой записи ACE. Один список ACL можно применять на устройстве к разным целям, таким как интерфейсы сетевого устройства, приложения и функции, работающие на устройстве и т. п. При использовании для интерфейсов сетевого устройства можно задать разные ACL на входе и выходе интерфейса.

Этот документ пытается использовать общие для всех производителей аспекты и создать базовую модель, которую можно дополнять фирменными моделями. Базовая модель проста в устройстве и это позволяет надеяться на достаточную гибкость, позволяющую каждому производителю расширять её.

Применение в модели операторов feature позволяет производителям анонсировать правила сопоставления, которые они хотят и могут поддерживать. Имеется два набора операторов feature, которые устройству нужно анонсировать. Первый набор указывает возможности устройства, такие как способность сопоставлять заголовки Ethernet или заголовки IPv4. Второй набор задаёт комбинации заголовков, которые устройство готово поддерживать, например только IPv6 ACL или комбинация Ethernet, IPv4 и IPv6 ACL.

3.1. Модули ACL

Модель включает два модуля YANG. Модуль ietf-access-control-list определяет базовые аспекты, которые относятся ко всем ACL, независимо от типа и производителя. Фактически модуль можно считать базовым «суперклассом» ACL. Этот модуль импортирует второй модуль ietf-packet-fields. Контейнер сопоставления в ietf-access-control-list применяет группировки из ietf-packet-fields для задания полей сопоставления, таких как номера портов и протоколы. Комбинация проверки if-feature и операторов must позволяет выбрать нужные поля сопоставления, которые пользователь может включить в правила.

Если нужно задать новый выбор (choice) matches, например, IP Flow Information Export (IPFIX) [RFC7011], контейнер matches можно дополнить (augment).

```
module: ietf-access-control-list
  +--rw acls
     +--rw acl* [name]
     |  +--rw name    string
     |  +--rw type?   acl-type
     |  +--rw aces
     |     +--rw ace* [name]
     |        +--rw name          string
     |        +--rw matches
     |        |  +--rw (l2)?
     |        |  |  +--:(eth)
     |        |  |     +--rw eth {match-on-eth}?
     |        |  |        +--rw destination-mac-address?
     |        |  |        |       yang:mac-address
     |        |  |        +--rw destination-mac-address-mask?
     |        |  |        |       yang:mac-address
     |        |  |        +--rw source-mac-address?
     |        |  |        |       yang:mac-address
     |        |  |        +--rw source-mac-address-mask?
     |        |  |        |       yang:mac-address
     |        |  |        +--rw ethertype?
     |        |  |                eth:ethertype
     |        |  +--rw (l3)?
     |        |  |  +--:(ipv4)
     |        |  |  |  +--rw ipv4 {match-on-ipv4}?
     |        |  |  |     +--rw dscp?
     |        |  |  |     |       inet:dscp
     |        |  |  |     +--rw ecn?
     |        |  |  |     |       uint8
     |        |  |  |     +--rw length?
     |        |  |  |     |       uint16
     |        |  |  |     +--rw ttl?
     |        |  |  |     |       uint8
     |        |  |  |     +--rw protocol?
     |        |  |  |     |       uint8
     |        |  |  |     +--rw ihl?
     |        |  |  |     |       uint8
     |        |  |  |     +--rw flags?
     |        |  |  |     |       bits
     |        |  |  |     +--rw offset?
     |        |  |  |     |       uint16
     |        |  |  |     +--rw identification?
     |        |  |  |     |       uint16
     |        |  |  |     +--rw (destination-network)?
     |        |  |  |     |  +--:(destination-ipv4-network)
     |        |  |  |     |     +--rw destination-ipv4-network?
     |        |  |  |     |             inet:ipv4-prefix
     |        |  |  |     +--rw (source-network)?
     |        |  |  |        +--:(source-ipv4-network)
     |        |  |  |           +--rw source-ipv4-network?
     |        |  |  |                   inet:ipv4-prefix
     |        |  |  +--:(ipv6)
     |        |  |     +--rw ipv6 {match-on-ipv6}?
     |        |  |        +--rw dscp?
     |        |  |        |       inet:dscp
```

```
|         |   |         +--rw ecn?
|         |   |         |       uint8
|         |   |         +--rw length?
|         |   |         |       uint16
|         |   |         +--rw ttl?
|         |   |         |       uint8
|         |   |         +--rw protocol?
|         |   |         |       uint8
|         |   |         +--rw (destination-network)?
|         |   |         |  +--:(destination-ipv6-network)
|         |   |         |     +--rw destination-ipv6-network?
|         |   |         |             inet:ipv6-prefix
|         |   |         +--rw (source-network)?
|         |   |         |  +--:(source-ipv6-network)
|         |   |         |     +--rw source-ipv6-network?
|         |   |         |             inet:ipv6-prefix
|         |   |         +--rw flow-label?
|         |   |                 inet:ipv6-flow-label
|         |   |  +--rw (l4)?
|         |   |  |  +--:(tcp)
|         |   |  |  |  +--rw tcp {match-on-tcp}?
|         |   |  |  |     +--rw sequence-number?          uint32
|         |   |  |  |     +--rw acknowledgement-number?   uint32
|         |   |  |  |     +--rw data-offset?              uint8
|         |   |  |  |     +--rw reserved?                 uint8
|         |   |  |  |     +--rw flags?                    bits
|         |   |  |  |     +--rw window-size?              uint16
|         |   |  |  |     +--rw urgent-pointer?           uint16
|         |   |  |  |     +--rw options?                  binary
|         |   |  |  |     +--rw source-port
|         |   |  |  |     |  +--rw (source-port)?
|         |   |  |  |     |     +--:(range-or-operator)
|         |   |  |  |     |        +--rw (port-range-or-operator)?
|         |   |  |  |     |           +--:(range)
|         |   |  |  |     |           |  +--rw lower-port
|         |   |  |  |     |           |  |       inet:port-number
|         |   |  |  |     |           |  +--rw upper-port
|         |   |  |  |     |           |          inet:port-number
|         |   |  |  |     |           +--:(operator)
|         |   |  |  |     |              +--rw operator?     operator
|         |   |  |  |     |              +--rw port
|         |   |  |  |     |                      inet:port-number
|         |   |  |  |     +--rw destination-port
|         |   |  |  |        +--rw (destination-port)?
|         |   |  |  |           +--:(range-or-operator)
|         |   |  |  |              +--rw (port-range-or-operator)?
|         |   |  |  |                 +--:(range)
|         |   |  |  |                 |  +--rw lower-port
|         |   |  |  |                 |  |       inet:port-number
|         |   |  |  |                 |  +--rw upper-port
|         |   |  |  |                 |          inet:port-number
|         |   |  |  |                 +--:(operator)
|         |   |  |  |                    +--rw operator?     operator
|         |   |  |  |                    +--rw port
|         |   |  |  |                            inet:port-number
|         |   |  |  +--:(udp)
|         |   |  |  |  +--rw udp {match-on-udp}?
|         |   |  |  |     +--rw length?             uint16
|         |   |  |  |     +--rw source-port
|         |   |  |  |     |  +--rw (source-port)?
|         |   |  |  |     |     +--:(range-or-operator)
|         |   |  |  |     |        +--rw (port-range-or-operator)?
|         |   |  |  |     |           +--:(range)
|         |   |  |  |     |           |  +--rw lower-port
|         |   |  |  |     |           |  |       inet:port-number
|         |   |  |  |     |           |  +--rw upper-port
|         |   |  |  |     |           |          inet:port-number
|         |   |  |  |     |           +--:(operator)
|         |   |  |  |     |              +--rw operator?     operator
|         |   |  |  |     |              +--rw port
|         |   |  |  |     |                      inet:port-number
|         |   |  |  |     +--rw destination-port
|         |   |  |  |        +--rw (destination-port)?
|         |   |  |  |           +--:(range-or-operator)
|         |   |  |  |              +--rw (port-range-or-operator)?
|         |   |  |  |                 +--:(range)
|         |   |  |  |                 |  +--rw lower-port
|         |   |  |  |                 |  |       inet:port-number
|         |   |  |  |                 |  +--rw upper-port
|         |   |  |  |                 |          inet:port-number
|         |   |  |  |                 +--:(operator)
|         |   |  |  |                    +--rw operator?     operator
|         |   |  |  |                    +--rw port
|         |   |  |  |                            inet:port-number
|         |   |  |  +--:(icmp)
|         |   |  |     +--rw icmp {match-on-icmp}?
```

```
       |        |  |        +--rw type?             uint8
       |        |  |        +--rw code?             uint8
       |        |  |        +--rw rest-of-header?   binary
       |        |  +--rw egress-interface?    if:interface-ref
       |        |  +--rw ingress-interface?   if:interface-ref
       |        +--rw actions
       |        |  +--rw forwarding    identityref
       |        |  +--rw logging?      identityref
       |        +--ro statistics {acl-aggregate-stats}?
       |           +--ro matched-packets?   yang:counter64
       |           +--ro matched-octets?    yang:counter64
       +--rw attachment-points
          +--rw interface* [interface-id] {interface-attachment}?
             +--rw interface-id    if:interface-ref
             +--rw ingress
             |  +--rw acl-sets
             |     +--rw acl-set* [name]
             |        +--rw name              -> /acls/acl/name
             |        +--ro ace-statistics* [name] {interface-stats}?
             |           +--ro name
             |           |       -> /acls/acl/aces/ace/name
             |           +--ro matched-packets?   yang:counter64
             |           +--ro matched-octets?    yang:counter64
             +--rw egress
                +--rw acl-sets
                   +--rw acl-set* [name]
                      +--rw name              -> /acls/acl/name
                      +--ro ace-statistics* [name] {interface-stats}?
                         +--ro name
                         |       -> /acls/acl/aces/ace/name
                         +--ro matched-packets?   yang:counter64
                         +--ro matched-octets?    yang:counter64
```

4. Модели YANG ACL

4.1. Модуль IETF Access Control List

Модуль ietf-access-control-list определяет контейнер acls с набором всех acl. Каждый узел acl имеет сведения, указывающие список доступа по имени (name) и список правил (aces), связанных с name. Каждая из записей списка (aces), индексируемая строкой name, имеет контейнеры, задающие сопоставления (matches) и действия (actions).

Модель определяет несколько типов и действий ACL в форме идентификаторов и свойств. Свойства применяются разработчиками для выбра типов ACL, которые система модет поддерживать, а идентификаторы служат для проверки пригодности выбранных типов. Эти типы неявно наследуются ace, защищая от ошибочной настройки типов ace в acl.

Контейнер matches задаёт критерии, служащие для идентификации шаблонов в ietf-packet-fields. Операторы выбора (choice) в контейнере сопоставления позволяют выбрать один из типов заголовков среди l2, l3 и l4. Контейнер actions определяет поведение в случае совпадения (match). В дополнение к разрешению (permit) и отказу (deny) опция записи (logging) для сопоставления позволяет регистрировать совпадения, что позднее можно использовать для нахождения соответствующих правил. Модель также задаёт возможность присоединения списков ACL к определённому интерфейсу.

В ACL можно собирать статистику для ace и interface. Заданные для статистики операторы feature позволяют выбрать статистику, собираемую для ace или interface.

Этот модуль импортирует определения из Common YANG Data Types [RFC6991] и A YANG Data Model for Interface Management [RFC8343].

```
<CODE BEGINS> file "ietf-access-control-list@2019-03-04.yang"

module ietf-access-control-list {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-access-control-list";
  prefix acl;

  import ietf-yang-types {
    prefix yang;
    reference
      "RFC 6991 - Common YANG Data Types.";
  }

  import ietf-packet-fields {
    prefix pf;
    reference
      "RFC 8519 - YANG Data Model for Network Access Control
                  Lists (ACLs).";
  }

  import ietf-interfaces {
    prefix if;
    reference
      "RFC 8343 - A YANG Data Model for Interface Management.";
  }

  organization
    "IETF NETMOD (Network Modeling) Working Group.";
```

```
  contact
    "WG Web:  <https://datatracker.ietf.org/wg/netmod/>
     WG List: netmod@ietf.org

     Editor: Mahesh Jethanandani
             mjethanandani@gmail.com
     Editor: Lisa Huang
             huangyi_99@yahoo.com
     Editor: Sonal Agarwal
             sagarwal12@gmail.com
     Editor: Dana Blair
             dana@blairhome.com";

  description
    "Этот модуль YANG задаёт компонент, описывающий настройку и
     мониторинг списков управления доступом (ACL).

     Ключевые слова ДОЛЖНО, НЕДОПУСТИМО, ТРЕБУЕТСЯ, НУЖНО, НЕ НУЖНО,
     СЛЕДУЕТ, НЕ СЛЕДУЕТ, РЕКОМЕНДУЕТСЯ, НЕ РЕКОМЕНДУЕТСЯ, МОЖНО,
     НЕОБЯЗАТЕЛЬНО в этом документе трактуются в соответствии с
     BCP 14 (RFC 2119) (RFC 8174) тогда и только тогда, когда они
     указаны заглавными буквами, как показано здесь.

     Авторские права (Copyright (c) 2019) принадлежат IETF Trust и
     лицам, указанным как авторы. Все права защищены.

     Распространение и применение модуля в исходной или двоичной
     форме с изменениями или без таковых разрешено в соответствии с
     лицензией Simplified BSD License, изложенной в параграфе 4.c
     IETF Trust's Legal Provisions Relating to IETF Documents
     (https://trustee.ietf.org/license-info).

     Эта версия модуля YANG является частью RFC 8519, где правовые
     аспекты приведены более полно.";

  revision 2019-03-04 {
    description
      "Исходный выпуск.";
    reference
      "RFC 8519: YANG Data Model for Network Access Control
                 Lists (ACLs).";
  }

  /*
   * Идентификаторы (отождествления)
   */

  /*
   * Действия по пересылке пакета
   */

  identity forwarding-action {
    description
      "базовое отождествление для действий при пересылке.";
  }

  identity accept {
    base forwarding-action;
    description
      "Воспринять пакет.";
  }

  identity drop {
    base forwarding-action;
    description
      "Отбросить пакет без передачи сообщения ICMP об ошибке.";
  }

  identity reject {
    base forwarding-action;
    description
      "Отбросить пакет с передачей источнику сообщения ICMP об ошибке.";
  }

  /*
   * Действия по регистрации для пакетов
   */

  identity log-action {
    description
      "Базовый идентификатор для указания получателя сведений.";
  }

  identity log-syslog {
    base log-action;
```

```
    description
      "Информация syslog для пакета.";
  }

  identity log-none {
    base log-action;
    description
      "Нет регистрации (logging) для пакета.";
  }

  /*
   * Идентификаторы типов ACL
   */

  identity acl-base {
    description
      "Базовый тип для всех ACL.";
  }

  identity ipv4-acl-type {
    base acl:acl-base;
    if-feature "ipv4";
    description
      "ACL для сопоставления полей заголовка IPv4 (например, адрес
       получателя IPv4) и L4 (например, порт получателя TCP). ACL типа
       ipv4 не имеют сопоставления полей заголовков Ethernet и IPv6.";
  }

  identity ipv6-acl-type {
    base acl:acl-base;
    if-feature "ipv6";
    description
      "ACL для сопоставления полей заголовка IPv6 (например, адрес
       получателя IPv6) и L4 (например, порт получателя TCP). ACL типа
       ipv6 не имеют сопоставления полей заголовков Ethernet и IPv4.";
  }

  identity eth-acl-type {
    base acl:acl-base;
    if-feature "eth";
    description
      "ACL для сопоставления полей заголовка Ethernet или Wi-Fi. ACL
       типа ethernet не включают сопоставления полей заголовков IPv4
       IPv6, L4.";
  }

  identity mixed-eth-ipv4-acl-type {
    base acl:eth-acl-type;
    base acl:ipv4-acl-type;
    if-feature "mixed-eth-ipv4";
    description
      "ACL для сопоставления полей заголовков Ethernet и IPv4. Могут
       также включать сопоставления полей заголовка L4.";
  }

  identity mixed-eth-ipv6-acl-type {
    base acl:eth-acl-type;
    base acl:ipv6-acl-type;
    if-feature "mixed-eth-ipv6";
    description
      "ACL для сопоставления полей заголовков Ethernet и IPv6. Могут
       также включать сопоставления полей заголовка L4.";
  }

  identity mixed-eth-ipv4-ipv6-acl-type {
    base acl:eth-acl-type;
    base acl:ipv4-acl-type;
    base acl:ipv6-acl-type;
    if-feature "mixed-eth-ipv4-ipv6";
    description
      "ACL для сопоставления полей заголовков Ethernet, IPv4 и IPv6.
       Могут также включать сопоставления полей заголовка L4.";
  }

  /*
   * Свойства (функции)
   */

  /*
   * Функции, поддерживаемые устройством
   */
  feature match-on-eth {
    description
      "Устройство может сопоставлять заголовки Ethernet.";
  }
```

```
  feature match-on-ipv4 {
    description
      "Устройство может сопоставлять заголовки IPv4.";
  }

  feature match-on-ipv6 {
    description
      "Устройство может сопоставлять заголовки IPv6.";
  }

  feature match-on-tcp {
    description
      "Устройство может сопоставлять заголовки TCP.";
  }

  feature match-on-udp {
    description
      "Устройство может сопоставлять заголовки UDP.";
  }

  feature match-on-icmp {
    description
      "Устройство может сопоставлять заголовки ICMP (v4 и v6).";
  }

  /*
   * Комбинации сопоставления заголовков, поддерживаемые устройством
   */

  feature eth {
    if-feature "match-on-eth";
    description
      "Только Ethernet ACL.";
  }

  feature ipv4 {
    if-feature "match-on-ipv4";
    description
      "Только IPv4 ACL.";
  }

  feature ipv6 {
    if-feature "match-on-ipv6";
    description
      "Только IPv6 ACL.";
  }

  feature mixed-eth-ipv4 {
    if-feature "match-on-eth and match-on-ipv4";
    description
      "Ethernet и IPv4 ACL.";
  }

  feature mixed-eth-ipv6 {
    if-feature "match-on-eth and match-on-ipv6";
    description
      "Ethernet и IPv6 ACL.";
  }

  feature mixed-eth-ipv4-ipv6 {
    if-feature
      "match-on-eth and match-on-ipv4
       and match-on-ipv6";
    description
      "Ethernet, IPv4, IPv6 ACL.";
  }

  /*
   * Свойства (функции) статистики
   */
  feature interface-stats {
    description
      "Счётчики ACL доступны и возвращаются лишь для интерфейса.";
  }

  feature acl-aggregate-stats {
    description
      "Счётчики ACL доступны и возвращаются лишь для записи ACL.";
  }

  /*
   * Свойства (функции) точек присоединения
   */
  feature interface-attachment {
    description
      "ACL устанавливаются на интерфейсах.";
```

```
  }

  /*
   * Определения типов
   */
  typedef acl-type {
    type identityref {
      base acl-base;
    }
    description
      "Указывает тип ACL.";
  }

  /*
   * Группировки
   */
  grouping acl-counters {
    description
      "Базовая группа для счётчиков ACL.";
    leaf matched-packets {
      type yang:counter64;
      config false;
      description
        "Учёт числа пакетов, соответствующих текущей записи ACL.

         Всем реализациям следует поддерживать такие счётчики на уровне
         интерфейса и записи ACL,если это возможно.

         Если реализация поддерживает счётчики ACL лишь на уровне записи
         (не поддерживает на интерфейс), следует учитывать в значении
         все интерфейсы.

         Реализации, поддерживающей счётчики для записи на уровне
         интерфейса, не требуется предоставлять агрегированный счётчик,
         например, на запись. Предполагается, что пользователь способен
         выполнить такое агрегирование, если это требуется.";
    }

    leaf matched-octets {
      type yang:counter64;
      config false;
      description
        "Учёт числа октетов (байтов), соответствующих текущей записи ACL.

         Реализациям следует поддерживать такие счётчики на уровне
         интерфейса и записи ACL,если это возможно.

         Если реализация поддерживает счётчики ACL лишь на уровне записи
         (не поддерживает на интерфейс), следует учитывать в значении
         все интерфейсы.

         Реализации, поддерживающей счётчики для записи на уровне
         интерфейса, не требуется предоставлять агрегированный счётчик,
         например, на запись. Предполагается, что пользователь способен
         выполнить такое агрегирование, если это требуется.";
    }
  }

  /*
   * Узлы данных настройки и мониторинга
   */

  container acls {
    description
      "Контейнер верхнего уровня для ACL с 1 или множеством узлов acl.";
    list acl {
      key "name";
      description
        "ACL - упорядоченный список записей ACE, каждая из которых
         имеет список критериев и список действий. Поскольку имеется
         несколько типов ACL, реализуемых с разными атрибутами для
         различных производителей, модель позволяет настроить ACL для
         каждого типа и производителя.";
      leaf name {
        type string {
          length "1..64";
        }
        description
          "имя списка доступа. Устройство МОЖЕТ дополнительно сокращать
           размер имени. Пробелы и специальные символы не допускаются.";
      }
      leaf type {
        type acl-type;
        description
          "Тип ACL, указывающий основной тип критериев соответствия
           (например, Ethernet, IPv4, IPv6, mixed и т. л.) в списке.";
```

```
    }
    container aces {
      description
        "Контейнер с узлами ACE.";
      list ace {
        key "name";
        ordered-by user;
        description
          "Список записей ACE.";
        leaf name {
          type string {
            length "1..64";
          }
          description
            "Уникальное имя записи ACE.";
        }
        container matches {
          description
            "Правила этого набора задают поля для сопоставления перед
             выполнением каких-либо действий. Правила выбираются на
             основе набора свойств (feature), заданного сервером, и
             acl-type. Если для конкретного контейнера не заданы
             сопоставления, ему будет соответствовать любой пакет.
             Если соппоставления не заданы ни в одной записи ACE,
             этой записи будет соответствовать любой пакет.";

          choice l2 {
            container eth {
              when "derived-from-or-self(/acls/acl/type, "
                 + "'acl:eth-acl-type')";
              if-feature "match-on-eth";
              uses pf:acl-eth-header-fields;
              description
                "Набор правил для сопоставления заголовков Ethernet.";
            }
            description
              "Сопоставление заголовков L2, например, Ethernet.";
          }

          choice l3 {
            container ipv4 {
              when "derived-from-or-self(/acls/acl/type, "
                 + "'acl:ipv4-acl-type')";
              if-feature "match-on-ipv4";
              uses pf:acl-ip-header-fields;
              uses pf:acl-ipv4-header-fields;
              description
                "Набор правил для сопоставления заголовков IPv4.";
            }

            container ipv6 {
              when "derived-from-or-self(/acls/acl/type, "
                 + "'acl:ipv6-acl-type')";
              if-feature "match-on-ipv6";
              uses pf:acl-ip-header-fields;
              uses pf:acl-ipv6-header-fields;
              description
                "Набор правил для сопоставления заголовков IPv6.";
            }
            description
              "Выбор заголовков IPv4 или IPv6.";
          }

          choice l4 {
            container tcp {
              if-feature "match-on-tcp";
              uses pf:acl-tcp-header-fields;
              container source-port {
                choice source-port {
                  case range-or-operator {
                    uses pf:port-range-or-operator;
                    description
                      "Определение порта источника из диапазона или
                       оператора.";
                  }
                  description
                    "Выбор определения порта источника с применением
                     range/operator или выбор для поддержки будущих
                     операторов case, таких как возможность указать
                     группу портов источника.";
                }
                description
                  "Определение порта источника.";
              }
              container destination-port {
                choice destination-port {
```

```
            case range-or-operator {
              uses pf:port-range-or-operator;
              description
                "Определение порта адресата из диапазона или
                 оператора.";
            }
            description
              "Выбор определения порта адресата с применением
               range/operator или выбор для поддержки будущих
               операторов case, таких как возможность указать
               группу портов адресата.";
          }
          description
            "Определение порта адресата.";
        }
        description
          "Набор правил для сопоставления заголовков TCP.";
      }

      container udp {
        if-feature "match-on-udp";
        uses pf:acl-udp-header-fields;
        container source-port {
          choice source-port {
            case range-or-operator {
              uses pf:port-range-or-operator;
              description
                "Определение порта адресата из range или
                 operator.";
            }
            description
              "Выбор определения порта источника с применением
               range/operator или выбор для поддержки будущих
               операторов case, таких как возможность указать
               группу портов источника.";
          }
          description
            "Определение порта источника.";
        }
        container destination-port {
          choice destination-port {
            case range-or-operator {
              uses pf:port-range-or-operator;
              description
                "Определение порта адресата из range или
                 operator.";
            }
            description
              "Выбор определения порта адресата с применением
               range/operator или выбор для поддержки будущих
               операторов case, таких как возможность указать
               группу портов адресата.";
          }
          description
            "Определение порта адресата.";
        }
        description
          "Набор правил для сопоставления заголовков UDP.";
      }

      container icmp {
        if-feature "match-on-icmp";
        uses pf:acl-icmp-header-fields;
        description
          "Набор правил для сопоставления заголовков ICMP.";
      }
      description
        "Выбор заголовков TCP, UDP или ICMP.";
    }

    leaf egress-interface {
      type if:interface-ref;
      description
        "Выходной интерфейс. Это не следует применять, если ACL
         подключён как выходной ACL (или значению следует
         совпадать с интерфейсом, куда подключён ACL).";
    }

    leaf ingress-interface {
      type if:interface-ref;
      description
        "Входной интерфейс. Это не следует применять, если ACL
         подключён как входной ACL (или значению следует
         совпадать с интерфейсом, куда подключён ACL).";
    }
  }
```

```
        container actions {
          description
            "Задание действий для этой записи ace.";
          leaf forwarding {
            type identityref {
              base forwarding-action;
            }
            mandatory true;
            description
              "Задаёт действие пересылки для записи ace.";
          }

          leaf logging {
            type identityref {
              base log-action;
            }
            default "log-none";
            description
              "Задаёт регистрацию (log) пакета и адресата для
               соответствующих пакетов. По умолчанию пакеты не
               регистрируются.";
          }
        }
        container statistics {
          if-feature "acl-aggregate-stats";
          config false;
          description
            "Статистика, собранная на всех точках присоединения
             данного ACL.";
          uses acl-counters;
        }
      }
    }
  }
  container attachment-points {
    description
      "Включающий (внешний) контейнер для списка точек присоединения,
       где установлены ACL.";
    /*
     * Группировки
     */
    grouping interface-acl {
      description
        "Группировка для данных входного ACL по интерфейсам.";
      container acl-sets {
        description
          "Включающий контейнер для списка входных ACL на
           интерфейсе.";
        list acl-set {
          key "name";
          ordered-by user;
          description
            "Список входных ACL на интерфейсе.";
          leaf name {
            type leafref {
              path "/acls/acl/name";
            }
            description
              "Ссылка на имя ACL, применяемого на входе.";
          }
          list ace-statistics {
            if-feature "interface-stats";
            key "name";
            config false;
            description
              "Список ACE.";
            leaf name {
              type leafref {
                path "/acls/acl/aces/ace/name";
              }
              description
                "Имя записи ace.";
            }
            uses acl-counters;
          }
        }
      }
    }

    list interface {
      if-feature "interface-attachment";
      key "interface-id";
      description
        "Список интерфейсов, где установлены ACL.";
```

```
        leaf interface-id {
          type if:interface-ref;
          description
            "Ссылка на ключ списка для идентификатора интерфейса.";
        }

        container ingress {
          uses interface-acl;
          description
            "ACL, примененные к входному интерфейсу.";
        }
        container egress {
          uses interface-acl;
          description
            "ACL, примененные к выходному интерфейсу.";
        }
      }
    }
  }
}
<CODE ENDS>
```

4.2. Модуль IETF Packet Fields

Модуль определяет требуемые группы для сопоставления полей пакетов, включая заголовки Ethernet, IPv4, IPv6 и транспортного уровня. Узел type определяет, какие из этих полей включаются в данный список ACL, кроме полей заголовков TCP, UDP и ICMP. Эти поля могут применяться вместе с указанными выше полями L2 или L3.

Поскольку критериев сопоставления очень много, базовая спецификация не включает их напрямую, а указывает из опреатором uses для сохранения простоты базового модуля. Если нужны дополнительные условия сопоставления, их можно добавить выбором дополнений (augment) в контейнере matches модели данных ietf-access-control-list.yang.

Этот модуль импортирует определения из Common YANG Data Types [RFC6991] и ссылается на Internet Protocol [RFC791], Internet Control Message Protocol [RFC792], Transmission Control Protocol [RFC793], Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers [RFC2474], The Addition of Explicit Congestion Notification (ECN) to IP [RFC3168], IPv6 Scoped Address Architecture [RFC4007], IP Version 6 Addressing Architecture [RFC4291], A Recommendation for IPv6 Address Text Representation [RFC5952], и Internet Protocol, Version 6 (IPv6) Specification [RFC8200].

```
<CODE BEGINS> file "ietf-packet-fields@2019-03-04.yang"

module ietf-packet-fields {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-packet-fields";
  prefix packet-fields;

  import ietf-inet-types {
    prefix inet;
    reference
      "RFC 6991 - Common YANG Data Types.";
  }

  import ietf-yang-types {
    prefix yang;
    reference
      "RFC 6991 - Common YANG Data Types.";
  }

  import ietf-ethertypes {
    prefix eth;
    reference
      "RFC 8519 - YANG Data Model for Network Access Control
                  Lists (ACLs).";
  }

  organization
    "IETF NETMOD (Network Modeling) Working Group.";

  contact
    "WG Web:  <https://datatracker.ietf.org/wg/netmod/>
     WG List: netmod@ietf.org

     Editor: Mahesh Jethanandani
             mjethanandani@gmail.com
     Editor: Lisa Huang
             huangyi_99@yahoo.com
     Editor: Sonal Agarwal
             sagarwal12@gmail.com
     Editor: Dana Blair
             dana@blairhome.com";

  description
    "Этот модуль YANG определяет группировки, применяемые модулем
     ietf-access-control-list. Их использование не ограничивается
     этим модулем и они могут применяться в любом подходящем месте.
```

```
    Авторские права (Copyright (c) 2019) принадлежат IETF Trust и
    лицам, указанным как авторы. Все права защищены.

    Распространение и применение модуля в исходной или двоичной
    форме с изменениями или без таковых разрешено в соответствии с
    лицензией Simplified BSD License, изложенной в параграфе 4.c
    IETF Trust's Legal Provisions Relating to IETF Documents
    (https://trustee.ietf.org/license-info).

    Эта версия модуля YANG является частью RFC 8519, где правовые
    аспекты приведены более полно.";

  revision 2019-03-04 {
    description
      "Исходный выпуск.";
    reference
      "RFC 8519: YANG Data Model for Network Access Control
                 Lists (ACLs).";
  }

  /*
   * Определения типов
   */
  typedef operator {
    type enumeration {
      enum lte {
        description
          "Меньше или равно.";
      }
      enum gte {
        description
          "Больше или равно.";
      }
      enum eq {
        description
          "Равно.";
      }
      enum neq {
        description
          "Не равно.";
      }
    }
    description
      "Определения диапазона портов источника и получателя можно
       уточнять с помощью типа operator. Это требуется лишь в случае,
       когда указан lower-port или не указан upper-port, поэтому
       operator уточняет только lower-port.";
  }

  /*
   * Groupings
   */
  grouping port-range-or-operator {
    choice port-range-or-operator {
      case range {
        leaf lower-port {
          type inet:port-number;
          must '. <= ../upper-port' {
            error-message
              "Значение lower-port должно быть не больше upper-port.";
          }
          mandatory true;
          description
            "Нижняя граница портов.";
        }
        leaf upper-port {
          type inet:port-number;
          mandatory true;
          description
            "Верхняя граница портов.";
        }
      }
      case operator {
        leaf operator {
          type operator;
          default "eq";
          description
            "Оператор для применения к порту, как указано ниже.";
        }
        leaf port {
          type inet:port-number;
          mandatory true;
          description
            "Номер порта и operator для применения.";
        }
      }
```

```
      description
        "Задание в operator диапазона или одного порта.";
    }
    description
      "Группировка для определений портов через оператор choice.";
  }

  grouping acl-ip-header-fields {
    description
      "Поля заголовка IP, общие для IPv4 и IPv6";
    reference
      "RFC 791: Internet Protocol.";

    leaf dscp {
      type inet:dscp;
      description
        "Код дифференцированного обслуживания (DSCP).";
      reference
        "RFC 2474: Definition of the Differentiated Services
                   Field (DS Field) in the IPv4 and IPv6
                   Headers.";
    }

    leaf ecn {
      type uint8 {
        range "0..3";
      }
      description
        "Явное уведомление о перегрузке (ECN).";
      reference
        "RFC 3168: The Addition of Explicit Congestion
                   Notification (ECN) to IP.";
    }

    leaf length {
      type uint16;
      description
        "В заголовке IPv4 это поле называют Total Length - размер
         дейтаграммы в октетах, включая заголовок и данные.

         В заголовке IPv6 это поле называют Payload Length - размер
         данных IPv6, т. е. части после заголовка IPv6 (в октетах).";
      reference
        "RFC 791: Internet Protocol
         RFC 8200: Internet Protocol, Version 6 (IPv6) Specification.";
    }
    leaf ttl {
      type uint8;
      description
        "Задаёт максимальное время, которое дейтаграмма может находиться
         в системе internet. При значении 0 дейтаграмма отбрасывается.

         В IPv6 это поле называют Hop Limit.";
      reference
        "RFC 791: Internet Protocol
         RFC 8200: Internet Protocol, Version 6 (IPv6) Specification.";
    }
    leaf protocol {
      type uint8;
      description
        "Номер протокола Internet, указывающий протокол в поле данных.
         В IPv6 это поле называют next-header и при наличии заголовков
         расширения протокол указывается в заголовке «верхнего уровня».";
      reference
        "RFC 791: Internet Protocol
         RFC 8200: Internet Protocol, Version 6 (IPv6) Specification.";
    }
  }

  grouping acl-ipv4-header-fields {
    description
      "Поля заголовка IPv4.";
    leaf ihl {
      type uint8 {
        range "5..60";
      }
      description
        "В поле заголовка IPv4 Internet Header Length (IHL) указывает
         размер заголовка internet в 32-битовых словах, что показывает
         начало данных. Отметим, что значение должно быть не меньше 5.";
    }
    leaf flags {
      type bits {
        bit reserved {
          position 0;
          description
```

```
            "Резерв. Должно быть 0.";
        }
        bit fragment {
          position 1;
          description
            "0 разрешает фрагментирование, 1 - запрещает.";
        }
        bit more {
          position 2;
          description
            "0 указывает последний фрагмент, 1 - наличие других.";
        }
      }
      description
        "Определения битов поля Flags в заголовке IPv4.";
    }
    leaf offset {
      type uint16 {
        range "20..65535";
      }
      description
        "Смещение фрагмента в 8-октетных (64 бита) блоках. Первый
         фрагмент имеет смщение 0. Размер поля 13 битов";
    }
    leaf identification {
      type uint16;
      description
        "Значение, заданное отправителем для использования при сборке
         дейтаграммы из фрагментов.";
    }

    choice destination-network {
      case destination-ipv4-network {
        leaf destination-ipv4-network {
          type inet:ipv4-prefix;
          description
            "Префикс адресата IPv4.";
        }
      }
      description
        "Выбор указания адреса или группы адресов получателя IPv4.";
    }

    choice source-network {
      case source-ipv4-network {
        leaf source-ipv4-network {
          type inet:ipv4-prefix;
          description
            "Префикс источника IPv4.";
        }
      }
      description
        "Выбор указания адреса или группы адресов источника IPv4.";
    }
  }

  grouping acl-ipv6-header-fields {
    description
      "Поля заголовка IPv6.";

    choice destination-network {
      case destination-ipv6-network {
        leaf destination-ipv6-network {
          type inet:ipv6-prefix;
          description
            "Префикс адресата IPv6.";
        }
      }
      description
        "Выбор указания адреса или группы адресов получателя IPv6.";
    }

    choice source-network {
      case source-ipv6-network {
        leaf source-ipv6-network {
          type inet:ipv6-prefix;
          description
            "Source IPv6 address prefix.";
        }
      }
      description
        "Выбор указания адреса или группы адресов источника IPv6.";
    }

    leaf flow-label {
      type inet:ipv6-flow-label;
```

```
      description
        "Метка потока IPv6 (Flow label).";
    }
    reference
      "RFC 4291: IP Version 6 Addressing Architecture
       RFC 4007: IPv6 Scoped Address Architecture
       RFC 5952: A Recommendation for IPv6 Address Text
                 Representation.";
  }

  grouping acl-eth-header-fields {
    description
      "Поля заголовка Ethernet.";
    leaf destination-mac-address {
      type yang:mac-address;
      description
        "Адрес получателя IEEE 802 MAC.";
    }
    leaf destination-mac-address-mask {
      type yang:mac-address;
      description
        "Маска адреса получателя IEEE 802 MAC.";
    }
    leaf source-mac-address {
      type yang:mac-address;
      description
        "Адрес источника IEEE 802 MAC.";
    }
    leaf source-mac-address-mask {
      type yang:mac-address;
      description
        "Маска адреса источника IEEE 802 MAC.";
    }
    leaf ethertype {
      type eth:ethertype;
      description
        "Тип Ethernet (или Length) в каноническом порядке IEEE 802,
         использующем символы нижнего регистра.";
      reference
        "IEEE 802-2014, Clause 9.2.";
    }
    reference
      "IEEE 802: IEEE Standard for Local and Metropolitan
       Area Networks: Overview and Architecture.";
  }

  grouping acl-tcp-header-fields {
    description
      "Поля заголовка TCP, которые можно задать в сопоставлении.";
    leaf sequence-number {
      type uint32;
      description
        "Порядковый номер в пакете.";
    }
    leaf acknowledgement-number {
      type uint32;
      description
        "Номер подтверждения в пакете.";
    }
    leaf data-offset {
      type uint8 {
        range "5..15";
      }
      description
        "Размер заголовка TCP в 32-битовых словах. Минимальное значение
         - 5, максимальное - 15, т. е. заголовок размером от 20 до 60
         байтов, позволяющий включить до 40 байтов опций.";
    }
    leaf reserved {
      type uint8;
      description
        "Резерв на будущее.";
    }
    leaf flags {
      type bits {
        bit cwr {
          position 1;
          description
            "Флаг сокращения окна перегрузки (Congestion Window Reduced
             или CWR), устанавливаемый передающим хостом для индикации
             приёма сегмента TCP с установленным флагом ECN-Echo (ECE) и
             ответа на него механизмом контроля перегрузок.";
          reference
            "RFC 3168: The Addition of Explicit Congestion
                       Notification (ECN) to IP.";
        }
```

```
        bit ece {
          position 2;
          description
            "ECN-Echo играет 2 роли в зависимости от флага SYN. Если
             SYN установлен (1), партнёр TCP поддерживает ECN, а при
             сброшенном флаге SYN пакет с установленным флагом CE
             (ECN=11) в заголовке IP был принят при нормальной передаче
             (добавлен в заголовок RFC 3168). Это служит для указания
             перегрузки сети (или её приближения) отправителю TCP.";
          reference
            "RFC 3168: The Addition of Explicit Congestion
                       Notification (ECN) to IP.";
        }
        bit urg {
          position 3;
          description
            "Говорит о значимости поля Urgent Pointer.";
        }
        bit ack {
          position 4;
          description
            "Указывает значимость флага Acknowledgement. Во всех пакетах
             от клиента после начального пакета SYN этот флаг следует
             устанавливать.";
        }
        bit psh {
          position 5;
          description
            "Функция Push, запрашивающая выталкивание буферизованных
             данных принимающему приложению.";
        }
        bit rst {
          position 6;
          description
            "Reset the connection.";
        }
        bit syn {
          position 7;
          description
            "Синхронизация порядковых номеров. Этот флаг устанавливается
             лишь в первом пакете каждой стороны. Некоторые флаги и поля
             могут менять смысл этого флага, другие действительны лишь
             при наличии этого флага, третьи - лишь при отсутствии.";
        }
        bit fin {
          position 8;
          description
            "Последний пакет от отправителя.";
        }
      }
      description
        "Известны также как Control Bit (9 однобитовых флагов).";
      reference
        "RFC 793: Transmission Control Protocol.";
    }
    leaf window-size {
      type uint16;
      units "bytes";
      description
        "Размер окна приёма, задаёт размер данных сверх номера
         в поле Acknowledgement, которые отправитель этого сегмента
         готов в данный момент воспринять.";
    }
    leaf urgent-pointer {
      type uint16;
      description
        "Смещение от порядкового номера, указывающего последний байт
         срочных (urgent) данных.";
    }
    leaf options {
      type binary {
        length "1..40";
      }
      description
        "Размер этого поля определяется полем Data Offset. Опции могут
         иметь до 3 полей: Option-Kind (1 байт), Option-Length (1 байт),
         и Option-Data (переменный). Поле Option-Kind указывает тип
         опции и является обязательным. В зависимости от типа опции
         включаются два других поля. Option-Length указывает размер
         опции, а Option-Data - значение опции.";
    }
  }

  grouping acl-udp-header-fields {
    description
      "Набор полей заголовка UDP для сопоставлений.";
```

```
    leaf length {
      type uint16;
      description
        "Размер заголовка и данных UDP в байтах. Минимальный размер - 8
         байтов (размер заголовка). Это поле задаёт теоретический предел
         65535 байтов (8 байтов заголовка и 65527 байтов данных) для
         дейтаграмм UDP. Однако фактический предел размера данных
         нижележащий протокол IPv4 сокращает до 65507 байтов (20 байтов
         занимает заголовок IP).
         В джамбограммах IPv6 пакеты UDP могут быть больше 65535 байтов.
         RFC 2675 задаёт установку Length = 0, если размер заголовка и
         данных UDP превышает 65535 байтов.";
    }
  }

  grouping acl-icmp-header-fields {
    description
      "Поля заголовка ICMP для сопоставлений.";
    leaf type {
      type uint8;
      description
        "Называются также управляющими сообщениями.";
      reference
        "RFC 792: Internet Control Message Protocol
         RFC 4443: Internet Control Message Protocol (ICMPv6)
                   for Internet Protocol Version 6 (IPv6)
                   Specification.";
    }
    leaf code {
      type uint8;
      description
        "Субтип ICMP. Называются также управляющими сообщениями.";
      reference
        "RFC 792: Internet Control Message Protocol
         RFC 4443: Internet Control Message Protocol (ICMPv6)
                   for Internet Protocol Version 6 (IPv6)
                   Specification.";
    }
    leaf rest-of-header {
      type binary;
      description
        "Размер не ограничен, содержимое зависит от типа и кода
         ICMP. В ICMPv6 называется Message Body.";
      reference
        "RFC 792: Internet Control Message Protocol
         RFC 4443: Internet Control Message Protocol (ICMPv6)
                   for Internet Protocol Version 6 (IPv6)
                   Specification.";
    }
  }
}
<CODE ENDS>
```

4.3. Примеры ACL

Требование. Отвергать трафик tcp из подсети 192.0.2.0/24 в подсеть 198.51.100.0/24.

Ниже приведена конфигурация ACL в формате xml[1].

```
   <?xml version="1.0" encoding="UTF-8"?>
   <config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <acls
       xmlns="urn:ietf:params:xml:ns:yang:ietf-access-control-list">
       <acl>
         <name>sample-ipv4-acl</name>
         <type>ipv4-acl-type</type>
         <aces>
           <ace>
             <name>rule1</name>
             <matches>
               <ipv4>
                 <protocol>6</protocol>
                 <destination-ipv4-network>198.51.100.0/24</destination\
   -ipv4-network>
                 <source-ipv4-network>192.0.2.0/24</source-ipv4-network>
               </ipv4>
             </matches>
             <actions>
               <forwarding>drop</forwarding>
             </actions>
           </ace>
         </aces>
       </acl>
     </acls>
   </config>
```

[1]Здесь и далее символ \ в конце строки служит для разделения длинной строки на части в соответствии с форматом.

ACL и ACE можно задать командами CLI, как показано ниже.

```
        acl ipv4 sample-ipv4-acl
        deny tcp 192.0.2.0/24 198.51.100.0/24
```

Требование. Принимать весь трафик DNS, направленный в подсеть 2001:db8::/32, на порту 53.

```
<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <acls
    xmlns="urn:ietf:params:xml:ns:yang:ietf-access-control-list">
    <acl>
      <name>allow-dns-packets</name>
      <type>ipv6-acl-type</type>
      <aces>
        <ace>
          <name>rule1</name>
          <matches>
            <ipv6>
              <destination-ipv6-network>2001:db8::/32</destination-i\
pv6-network>
            </ipv6>
            <udp>
              <destination-port>
                <operator>eq</operator>
                <port>53</port>
              </destination-port>
            </udp>
          </matches>
          <actions>
            <forwarding>accept</forwarding>
          </actions>
        </ace>
      </aces>
    </acl>
  </acls>
</config>
```

4.4. Применение диапазона портов и другие примеры

При наличии lower-port и upper-port они задают диапазон портов, включающий оба значения. При наличии лишь port задан только порт, а диапазон определяет operator.

Приведённый ниже пример XML показывает конфигурацию с отбрасыванием трафика TCP из портов 16384 - 16387.

```
<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <acls
    xmlns="urn:ietf:params:xml:ns:yang:ietf-access-control-list">
    <acl>
      <name>sample-port-acl</name>
      <type>ipv4-acl-type</type>
      <aces>
        <ace>
          <name>rule1</name>
          <matches>
            <tcp>
              <source-port>
                <lower-port>16384</lower-port>
                <upper-port>16387</upper-port>
              </source-port>
            </tcp>
          </matches>
          <actions>
            <forwarding>drop</forwarding>
          </actions>
        </ace>
      </aces>
    </acl>
  </acls>
</config>
```

Следующий пример XML представляет конфигурацию с отбрасыванием всех эхо-запросов IPv4 ICMP.

```
<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <acls
    xmlns="urn:ietf:params:xml:ns:yang:ietf-access-control-list">
    <acl>
      <name>sample-icmp-acl</name>
      <aces>
        <ace>
          <name>rule1</name>
          <matches>
            <ipv4>
              <protocol>1</protocol>
            </ipv4>
            <icmp>
              <type>8</type>
              <code>0</code>
```

```
            </icmp>
          </matches>
          <actions>
            <forwarding>drop</forwarding>
          </actions>
        </ace>
      </aces>
    </acl>
  </acls>
</config>
```

Далее приведён пример XML с настройкой одного порта (21) для восприятия трафик TCP.

```
<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <acls
    xmlns="urn:ietf:params:xml:ns:yang:ietf-access-control-list">
    <acl>
      <name>sample-ipv4-acl</name>
      <type>ipv4-acl-type</type>
      <aces>
        <ace>
          <name>rule1</name>
          <matches>
            <tcp>
              <destination-port>
                <operator>eq</operator>
                <port>21</port>
              </destination-port>
            </tcp>
          </matches>
          <actions>
            <forwarding>accept</forwarding>
          </actions>
        </ace>
      </aces>
    </acl>
  </acls>
</config>
```

Ниже представлен пример XML с конфигурацией, задающей отбрасывание пакетов TCP для всех портов, кроме 21.

```
<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <acls
    xmlns="urn:ietf:params:xml:ns:yang:ietf-access-control-list">
    <acl>
      <name>sample-ipv4-acl</name>
      <type>ipv4-acl-type</type>
      <aces>
        <ace>
          <name>rule1</name>
          <matches>
            <tcp>
              <destination-port>
                <operator>neq</operator>
                <port>21</port>
              </destination-port>
            </tcp>
          </matches>
          <actions>
            <forwarding>drop</forwarding>
          </actions>
        </ace>
      </aces>
    </acl>
  </acls>
</config>
```

5. Вопросы безопасности

Модули YANG в этом документе задают схему для данных, предназначенную для доступа по протоколам управления сетью, таким как NETCONF [RFC6241] и RESTCONF [RFC8040]. Нижним уровнем NETCONF является защищённый транспорт в обязательной реализацией Secure Shell (SSH) [RFC6242]. Для RESTCONF нижним уровнем является HTTPS с обязательной реализацией защищённого транспорта TLS [RFC8446].

Модель доступа к конфигурации сети (Network Configuration Access Control Model или NACM) [RFC8341] обеспечивает способы предоставления доступа лишь конкретным пользователям NETCONF и RESTCONF для предопределённых подмножеств протокольных операций и содержимого NETCONF и RESTCONF.

В заданных здесь модулях YANG имеется множество узлов данных с возможностью записи, создания и удаления (config true, как задано по умолчанию). Эти узлы могут быть конфиденциальными или уязвимыми в некоторых сетевых средах. Операции записи в такие узлы (например, edit-config) без подобающей защиты могут оказывать негативное влияние на работу сети. Ниже показаны ветви и узлы данных, чувствительные или уязвимы в плане операций записи.

/acls/acl/aces

Этот список содержит все записи управления доступом, заданные на устройстве. Несанкционированная запись в этот список позволяет нарушителям изменять записи, чтобы разрешить запрещённый трафик или запретить

разрешенный. Первое может приводить к DoS-атакам или компрометации устройства, второе - к DoS-атакам. Несанкционированное чтение списка позволяет атакующему узнать действующие правила для организации атаки.

/acls/acl/aces/ace/actions/logging

Этот узел задаёт возможность регистрации пакетов, соответствующих записи. Несанкционированная запись позволяет атакующему включить регистрацию для одной или многих записей, перегружая сервер работой. Несанкционированное чтение позволяет злоумышленнику получить доступ к регистрируемым сведениям, что может послужить для организации атаки на сервер.

6. Взаимодействие с IANA

Этот документ регистрирует три URI и три модуля YANG.

6.1. Регистрация URI

Документ регистрирует указанные ниже URI в реестре IETF XML Registry [RFC3688].

```
URI: urn:ietf:params:xml:ns:yang:ietf-access-control-list
URI: urn:ietf:params:xml:ns:yang:ietf-packet-fields
URI: urn:ietf:params:xml:ns:yang:ietf-ethertypes
Registrant Contact: The IESG.
XML: N/A; запрошенный URI является пространством имён XML.
```

6.2. Регистрация имён модулей YANG

Документ регистрирует три модуля YANG в реестре YANG Module Names [RFC6020].

```
Name: ietf-access-control-list
Namespace: urn:ietf:params:xml:ns:yang:ietf-access-control-list
Prefix: acl
Reference: RFC 8519

Name: ietf-packet-fields
Namespace: urn:ietf:params:xml:ns:yang:ietf-packet-fields
Prefix: packet-fields
Reference: RFC 8519

Name: ietf-ethertypes
Namespace: urn:ietf:params:xml:ns:yang:ietf-ethertypes
Prefix: ethertypes
Reference: RFC 8519
```

7. Литература

7.1. Нормативные документы

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <https://www.rfc-editor.org/info/rfc792>.

[RFC793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <https://www.rfc-editor.org/info/rfc2474>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, DOI 10.17487/RFC3168, September 2001, <https://www.rfc-editor.org/info/rfc3168>.

[RFC4007] Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", RFC 4007, DOI 10.17487/RFC4007, March 2005, <https://www.rfc-editor.org/info/rfc4007>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, DOI 10.17487/RFC5952, August 2010, <https://www.rfc-editor.org/info/rfc5952>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8343] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 8343, DOI 10.17487/RFC8343, March 2018, <https://www.rfc-editor.org/info/rfc8343>.

7.2. Дополнительная литература

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

Приложение A. Примеры расширения модели ACL

A.1. Пример фирменного модуля

Модуль example-newco-acl служит примером фирменной модели организации, дополняющей модуль ietf-acl. Он показывает применение оператора augment в выражении XPath для добавления критериев соответствия, действий о операций по умолчанию при соответствии записи ACE. Все это является фирменными расширениями или расширениями свойств системы. Модуль example-newco-acl является лишь примером и предполагается разработка производителями своих фирменных моделей.

```
module example-newco-acl {
  yang-version 1.1;
  namespace "http://example.com/ns/example-newco-acl";
  prefix example-newco-acl;

  import ietf-access-control-list {
    prefix acl;
  }

  organization
    "Группа моделирования Newco.";

  contact
    "abc@newco.com";
  description
    "Этот модуль YANG дополняет модуль YANG IETF ACL.";

  revision 2019-03-04 {
    description
      "Фирменные расширения NewCo для модели ietf-acl.";

    reference
      "RFC 8519: YANG Data Model for Network Access Control
                 Lists (ACLs).";
  }

  augment "/acl:acls/acl:acl/"
        + "acl:aces/acl:ace/"
        + "acl:matches" {
    description
      "Сопоставления для простых фильтров Newco.";

    choice protocol-payload-choice {
      description
        "Фирменное сопоставление Newco для содержимого.";
      list protocol-payload {
        key "value-keyword";
        ordered-by user;
        description
          "Содержимое протокола (payload).";
        uses match-simple-payload-protocol-value;
      }
    }

    choice metadata {
      description
```

```
          "Фирменное сопоставление Newco для интерфейсов.";
        leaf packet-length {
          type uint16;
          description
            "Сопоставление размера пакетов.";
        }
      }
    }

    augment "/acl:acls/acl:acl/"
          + "acl:aces/acl:ace/"
          + "acl:actions" {
      description
        "Действия простых фильтров Newco.";
      choice action {
        description
          "Выбор фирменных действий Newco.";
        case count {
          description
            "Число пакетов в именованном счетчике.";
          leaf count {
            type uint32;
            description
              "Значение счётчика.";
          }
        }
        case policer {
          description
            "Имя правила (policer) для ограничения скорости трафика.";
          leaf policer {
            type string;
            description
              "Имя правила.";
          }
        }
        case hierarchical-policer {
          leaf hierarchical-policer {
            type string;
            description
              "Имя иерархического правила (policer).";
          }
          description
            "Имя иерархического правила для ограничения скорости
             трафика.";
        }
      }
    }

    augment "/acl:acls/acl:acl"
          + "/acl:aces/acl:ace/"
          + "acl:actions" {
      leaf default-action {
        type identityref {
          base acl:forwarding-action;
        }
        default "acl:drop";
        description
          "Действия при соответствии ACE.";
      }
      description
        "Фирменное действие Newco по умолчанию.";
    }

    grouping match-simple-payload-protocol-value {
      description
        "Newco proprietary payload";
      leaf value-keyword {
        type enumeration {
          enum icmp {
            description
              "Протокол ICMP.";
          }
          enum icmp6 {
            description
              "Протокол ICMPv6.";
          }
          enum range {
            description
              "Диапазон значений.";
          }
        }
        description
          "(null).";
      }
    }
  }
```

Ниже представлено дерево модуля example-newco-acl. Здесь /ietf-acl:acls/ietf-acl:acl/ietf-acl:aces/ietf-acl:ace/ietf-acl:matches дополняется двумя операторами choice: protocol-payload-choice и metadata. Первый использует группировку с перечислением всех поддерживаемых протоколов. Метаданные сопоставляются с полями, связанными с пакетом, такими как общий размер пакета. В другом случае /ietf-acl:acls/ietf-acl:acl/ietf-acl:aces/ietf-acl:ace/ietf-acl:actions дополняется выбором действий.

```
module: example-newco-acl
  augment /acl:acls/acl:acl/acl:aces/acl:ace/acl:matches:
    +--rw (protocol-payload-choice)?
    |  +--:(protocol-payload)
    |     +--rw protocol-payload* [value-keyword]
    |        +--rw value-keyword    enumeration
    +--rw (metadata)?
       +--:(packet-length)
          +--rw packet-length?      uint16
  augment /acl:acls/acl:acl/acl:aces/acl:ace/acl:actions:
    +--rw (action)?
       +--:(count)
       |  +--rw count?                  uint32
       +--:(policer)
       |  +--rw policer?                string
       +--:(hierarchical-policer)
          +--rw hierarchical-policer?   string
  augment /acl:acls/acl:acl/acl:aces/acl:ace/acl:actions:
    +--rw default-action?   identityref
```

A.2. Linux nftables

Поскольку платформа Linux становится популярней сетевой платформы, модель данных Linux изменяется. Ранее списки ACL в Linux были строго привязаны к протоколам и применялись разные утилиты (iptables, ip6tables, arptables, ebtables) со своими моделями данных. Недавно это было изменено и разработан единый пакет nftables. Он позволяет использовать одну модель данных для фильтров межсетевых экранов и очень похода на модуль ietf-access-control, описанный в этом документе. Пакет nftables поддерживает входные и выходные ACE и в каждой записи ACE можно задать сопоставления и действия. Пример из параграфа 4.3. Примеры ACL можно настроить с помощью инструмента nft, как показано ниже.

```
nft add table ip filter
nft add chain filter input
nft add rule ip filter input ip protocol tcp ip saddr \
    192.0.2.1/24 drop
```

Записи конфигурации будут иметь вид

```
table ip filter {
  chain input {
    ip protocol tcp ip saddr 192.0.2.1/24 drop
  }
}
```

Очевидно сходство Linux nftables и моделей YANG IETF ACL, а также их расширений. Модель YANG ACL из этого документа легко преобразовать в модель Linux nftables.

A.3. Ethertype

Модуль ACL зависит от определений Ethertype, выделение которых контролирует IEEE. Приведённая ниже модель включена для того, чтобы обеспечить возможность включения этих типов, пока IEEE не опубликует модель с определениями Ethertype, которая отменит эту модель.

```
<CODE BEGINS> file "ietf-ethertypes@2019-03-04.yang"

module ietf-ethertypes {
  namespace "urn:ietf:params:xml:ns:yang:ietf-ethertypes";
  prefix ethertypes;

  organization
    "IETF NETMOD (Network Modeling) Working Group.";

  contact
    "WG Web:   <https://datatracker.ietf.org/wg/netmod/>
     WG List:  <mailto:netmod@ietf.org>

     Editor:   Mahesh Jethanandani
               <mjethanandani@gmail.com>";

  description
    "Этот модуль содержит базовые определения для Ethertype,
     применяемых в других модулях. Это временный модуль, пока IEEE
     не начнёт определение этих Ethertype и не опубликует стандарт.
     После этого модуль утратит силу.

     Авторские права (Copyright (c) 2019) принадлежат IETF Trust и
     лицам, указанным как авторы. Все права защищены.

     Распространение и применение модуля в исходной или двоичной
     форме с изменениями или без таковых разрешено в соответствии с
     лицензией Simplified BSD License, изложенной в параграфе 4.c
     IETF Trust's Legal Provisions Relating to IETF Documents
     (https://trustee.ietf.org/license-info).
```

```
     Эта версия модуля YANG является частью RFC 8519, где правовые
     аспекты приведены более полно.";

   revision 2019-03-04 {
     description
       "Initial revision.";
     reference
       "RFC 8519: YANG Data Model for Network Access Control
                  Lists (ACLs).";
   }

   typedef ethertype {
     type union {
       type uint16;
       type enumeration {
         enum ipv4 {
           value 2048;
           description
             "Протокол IPv4 с шестнадцатеричным значением 0x0800.";
           reference
             "RFC 791: Internet Protocol.";
         }
         enum arp {
           value 2054;
           description
             "Протокол ARP с шестнадцатеричным значением 0x0806.";
           reference
             "RFC 826: An Ethernet Address Resolution Protocol: Or
                       Converting Network Protocol Addresses to 48.bit
                       Ethernet Address for Transmission on Ethernet
                       Hardware.";
         }
         enum wlan {
           value 2114;
           description
             "Wake-on-LAN с шестнадцатеричным значением 0x0842.";
         }
         enum trill {
           value 8947;
           description
             "TRILL с шестнадцатеричным значением 0x22F3.";
           reference
             "RFC 6325: Routing Bridges (RBridges): Base Protocol
                        Specification.";
         }
         enum srp {
           value 8938;
           description
             "Протокол резервирования потоков со значением 0x22EA.";
           reference
             "IEEE 801.1Q-2011.";
         }
         enum decnet {
           value 24579;
           description
             "DECnet Phase IV с шестнадцатеричным значением 0x6003.";
         }
         enum rarp {
           value 32821;
           description
             "RARP с шестнадцатеричным значением 0x8035.";
           reference
             "RFC 903: A Reverse Address Resolution Protocol.";
         }
         enum appletalk {
           value 32923;
           description
             "Appletalk (Ethertalk) со значением 0x809B.";
         }
         enum aarp {
           value 33011;
           description
             "Appletalk ARP с шестнадцатеричным значением 0x80F3.";
         }
         enum vlan {
           value 33024;
           description
             "Кадр с тегом VLAN (IEEE 802.1Q) и Shortest Path Bridging
              IEEE 802.1aq с совместимостью с NNI. Значение 0x8100.";
           reference
             "IEEE 802.1Q.";
         }
         enum ipx {
           value 33079;
           description
```

```
      "Протокол IPX с шестнадцатеричным значением 0x8137.";
  }
  enum qnx {
    value 33284;
    description
      "QNX Qnet с шестнадцатеричным значением 0x8204.";
  }
```

```
    description
      "Протокол IPv6 с шестнадцатеричным значением 0x86DD.";
    reference
      "RFC 8200: Internet Protocol, Version 6 (IPv6)
                 Specification
       RFC 8201: Path MTU Discovery for IP version 6.";
  }
  enum efc {
    value 34824;
    description
      "Управление потоком данных Ethernet с применением кадров
        pause. Значение 0x8808.";
    reference
      "IEEE 802.1Qbb.";
  }
  enum esp {
    value 34825;
    description
      "Протокол Ethernet Slow со значением 0x8809.";
    reference
      "IEEE 802.3-2015.";
  }
  enum cobranet {
    value 34841;
    description
      "CobraNet с шестнадцатеричным значением 0x8819.";
  }
  enum mpls-unicast {
    value 34887;
    description
      "Индивидуальный трафик MPLS со значением 0x8847.";
    reference
      "RFC 3031: Multiprotocol Label Switching Architecture.";
  }
  enum mpls-multicast {
    value 34888;
    description
      "Групповой трафик MPLS со значением 0x8848.";
    reference
      "RFC 3031: Multiprotocol Label Switching Architecture.";
  }
  enum pppoe-discovery {
    value 34915;
    description
      "PPPoE в процессе обнаружения. Значение 0x8863.";
    reference
      "RFC 2516: A Method for Transmitting PPP Over Ethernet
                 (PPPoE).";
  }
  enum pppoe-session {
    value 34916;
    description
      "PPPoE в сессии. Значение 0x8864.";
    reference
      "RFC 2516: A Method for Transmitting PPP Over Ethernet
                 (PPPoE).";
  }
  enum intel-ans {
    value 34925;
    description
      "Intel Advanced Networking Services. Значение 0x886D.";
  }
  enum jumbo-frames {
    value 34928;
    description
      "Кадры Jumbo или кадры Ethernet размером более 1500 байтов
       (до 9000).";
  }
  enum homeplug {
    value 34939;
    description
      "Различные протоколы для коммуникаций по цепям питания.
       Значение 0x887B.";
  }
  enum eap {
    value 34958;
    description
      "EAP в ЛВС  с шестнадцатеричным значением 0x888E.";
    reference
      "IEEE 802.1X.";
  }
  enum profinet {
    value 34962;
    description
      "PROFINET с шестнадцатеричным значением 0x8892.";
  }
```

```
        enum hyperscsi {
          value 34970;
          description
            "SCSIoE с шестнадцатеричным значением 0x889A.";
        }
        enum aoe {
          value 34978;
          description
            "ATAoE с шестнадцатеричным значением 0x88A2.";
        }
        enum ethercat {
          value 34980;
          description
            "EtherCAT с шестнадцатеричным значением 0x88A4.";
        }
        enum provider-bridging {
          value 34984;
          description
            "Provider Bridging (802.1ad) и Shortest Path Bridging
             (801.1aq). Значение 0x88A8.";
          reference
            "IEEE 802.1ad and IEEE 802.1aq).";
        }
        enum ethernet-powerlink {
          value 34987;
          description
            "Ethernet Powerlink со значением 0x88AB.";
        }
        enum goose {
          value 35000;
          description
            "GOOSE с шестнадцатеричным значением 0x88B8.";
          reference
            "IEC/ISO 8802-2 and 8802-3.";
        }
        enum gse {
          value 35001;
          description
            "Generic Substation Events. Значение 88B9.";
          reference
            "IEC 61850.";
        }
        enum sv {
          value 35002;
          description
            "Sampled Value Transmission. Значение 0x88BA.";
          reference
            "IEC 61850.";
        }
        enum lldp {
          value 35020;
          description
            "LLDP с шестнадцатеричным значением 0x88CC.";
          reference
            "IEEE 802.1AB.";
        }
        enum sercos {
          value 35021;
          description
            "Sercos Interface. Значение 0x88CD.";
        }
        enum wsmp {
          value 35036;
          description
            "WSMP с шестнадцатеричным значением 0x88DC.";
        }
        enum homeplug-av-mme {
          value 35041;
          description
            "HomePlug AV Mobile Management Entity (MME). Значение
             of 88E1.";
        }
        enum mrp {
          value 35043;
          description
            "MRP с шестнадцатеричным значением 0x88E3.";
          reference
            "IEC 62439-2.";
        }
        enum macsec {
          value 35045;
          description
            "MAC Security. Значение 0x88E5.";
          reference
            "IEEE 802.1AE.";
        }
```

```
          enum pbb {
            value 35047;
            description
              "PBB с шестнадцатеричным значением 0x88E7.";
            reference
              "IEEE 802.1ah.";
          }
          enum cfm {
            value 35074;
            description
              "CFM с шестнадцатеричным значением 0x8902.";
            reference
              "IEEE 802.1ag.";
          }
          enum fcoe {
            value 35078;
            description
              "FCoE с шестнадцатеричным значением 0x8906.";
            reference
              "T11 FC-BB-5.";
          }
          enum fcoe-ip {
            value 35092;
            description
              "FCoE Initialization Protocol. Значение 0x8914.";
          }
          enum roce {
            value 35093;
            description
              "RoCE с шестнадцатеричным значением 0x8915.";
          }
          enum tte {
            value 35101;
            description
              "TTE с шестнадцатеричным значением 0x891D.";
            reference
              "SAE AS6802.";
          }
          enum hsr {
            value 35119;
            description
              "HSR с шестнадцатеричным значением 0x892F.";
            reference
              "IEC 62439-3:2016.";
          }
        }
      }
      description
        "заполнитель типа uint16 определён для обеспечения пользователю
         возможности управлять своими ethertype, не включёнными в этот
         модуль. Можно также использовать определения enum для наиболее
         часто применяемых ethertype.";
    }
  }
  <CODE ENDS>
```

Благодарности

Alex Clemm, Andy Bierman и Lisa Huang начали с набросков первых версий на нескольких прошлых конференциях IETF. Этот документ включает структуру модели YANG ACL и большой набор сопоставления, а также подтверждает вклад Louis Fourie, Dana Blair, Tula Kraiser, Patrick Gili, George Serpa, Martin Bjorklund, Kent Watsen, Phil Shafer. Многие люди рецензировали предварительные версии документа в рамках IETF.

Dean Bogdanovic, Kiran Agrahara Sreenivasa, Lisa Huang и Dana Blair по отдельности оценивали модель YANG в предварительных версиях и совместно создавали предварительную версию ACL, поддержанную разными производителями. В этом документе исключены специфические для производителей свойства и даны примеры, позволяющие производителям расширить модель своими фирменными ACL. Этот предварительный вариант был переопределен настоящим документом с участием многих производителей.

Авторы благодарны Jason Sterne, Lada Lhotka, Juergen Schoenwalder, David Bannister, Jeff Haas, Kristian Larsson, Einar Nilsen-Nygaard за их рецензии и предложения.

Адреса авторов

Mahesh Jethanandani
VMware
Email: mjethanandani@gmail.com

Sonal Agarwal
Cisco Systems, Inc.
Email: sagarwal12@gmail.com

Lisa Huang
Email: huangyi_99@yahoo.com

Dana Blair
Email: dana@blairhome.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru