

Internet Engineering Task Force (IETF)
Request for Comments: 9249
Category: Standards Track
ISSN: 2070-1721

N. Wu
D. Dhody, Ed.
Huawei
A. Sinha, Ed.
A. Kumar S N
RtBrick Inc.
Y. Zhao
Ericsson
July 2022

A YANG Data Model for NTP

Модель данных YANG для NTP

Аннотация

Этот документ задаёт модель данных YANG, которая может служить для настройки и управления протоколом сетевого времени (Network Time Protocol или NTP) версии 4, а также версии 3. Модель включает данные конфигурации и состояния.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF¹ и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG². 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/rfc9249>.

Авторские права

Copyright (c) 2022. Авторские права принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

Оглавление

1. Введение.....	2
1.1. Рабочее состояние.....	2
1.2. Терминология.....	2
1.3. Диаграммы деревьев.....	2
1.4. Префиксы в именах узлов данных.....	2
1.5. Ссылки в модели.....	2
1.6. Уровни требований.....	2
2. Модель данных NTP.....	2
3. Связи с NTPv4-MIB.....	3
4. Связи с RFC 7317.....	4
5. Правила доступа.....	4
6. Управление ключами.....	4
7. Версия NTP.....	4
8. Модуль NTP YANG.....	4
9. Пример использования.....	21
9.1. Индивидуальная ассоциация.....	21
9.2. Первичные эталонные часы.....	22
9.3. Настройка аутентификации.....	22
9.4. Настройка доступа.....	23
9.5. Групповая конфигурация.....	23
9.6. Конфигурация manycast.....	25
9.7. Состояние часов.....	26
9.8. Получение всех ассоциаций.....	26
9.9. Глобальная статистика.....	27
10. Взаимодействие с IANA.....	27
10.1. IETF XML Registry.....	27
10.2. YANG Module Names.....	27
11. Вопросы безопасности.....	27

¹Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

²Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

12. Литература.....	28
12.1. Нормативные документы.....	28
12.2. Дополнительная литература.....	29
Приложение А. Полное дерево YANG.....	29
Благодарности.....	31
Адреса авторов.....	31

1. Введение

Этот документ задаёт модель данных YANG [RFC7950], которая может служить для настройки и управления протоколом NTP версии 4 [RFC5905]. Отметим, что модель также подходит для протокола NTPv3 [RFC1305] (см. 7. Версия NTP).

Модель данных охватывает настройку системных параметров NTP, таких как правила доступа, проверка подлинности, привязка маршрутизации и пересылки VPN (VPN Routing and Forwarding или VRF), различные режимы NTP и параметры на уровне интерфейсов. Обеспечивается также доступ к рабочему состоянию реализации NTP.

1.1. Рабочее состояние

Рабочее состояние NTP включено в одно дерево с конфигурацией NTP в соответствии с архитектурой хранилищ данных управления сетью (Network Management Datastore Architecture или NMDA) [RFC8342]. Текущее состояние и статистика NTP, а также статус ассоциации NTP также поддерживаются в рабочем состоянии.

1.2. Терминология

Используемые в документе термины соответствуют [RFC5905] и [RFC1305].

1.3. Диаграммы деревьев

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

1.4. Префиксы в именах узлов данных

В этом документе имена узлов данных, действий и других объектов модели данных используются без префиксов, если из контекста очевидно, в каком модуле YANG они определены. В остальных случаях имена указываются со стандартным префиксом соответствующего модуля YANG (Таблица 1).

Таблица 1. Префиксы и соответствующие модули YANG.

Префикс	Модуль YANG	Документ
yang	ietf-yang-types	[RFC6991]
inet	ietf-inet-types	[RFC6991]
if	ietf-interfaces	[RFC8343]
sys	ietf-system	[RFC7317]
acl	ietf-access-control-list	[RFC8519]
rt-types	ietf-routing-types	[RFC8294]
nacm	ietf-netconf-acm	[RFC8341]

1.5. Ссылки в модели

В таблице 2 указаны документы, на которые ссылается определяемая в документе модель.

Таблица 2. Ссылки в модуле YANG.

Название	Документ
Network Time Protocol Version 4: Protocol and Algorithms Specification	[RFC5905]
Common YANG Data Types	[RFC6991]
A YANG Data Model for System Management	[RFC7317]
Common YANG Data Types for the Routing Area	[RFC8294]
Network Configuration Access Control Model	[RFC8341]
A YANG Data Model for Interface Management	[RFC8343]
YANG Data Model for Network Access Control Lists (ACLs)	[RFC8519]
Message Authentication Code for the Network Time Protocol	[RFC8573]
The AES-CMAC Algorithm	[RFC4493]
The MD5 Message-Digest Algorithm	[RFC1321]
US Secure Hash Algorithm 1 (SHA1)	[RFC3174]
FIPS 180-4: Secure Hash Standard (SHS)	[SHS]

1.6. 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.

2. Модель данных NTP

Этот документ определяет модуль YANG ietf-ntp, сжатая структура которого показана ниже.

```

module: ietf-ntp
  +--rw ntp!
    +--rw port?                inet:port-number {ntp-port}?
    +--rw refclock-master!
      | +--rw master-stratum?  ntp-stratum
      +--rw authentication {authentication}?
      | +--rw auth-enabled?    boolean

```

```

| +--rw authentication-keys* [keyid]
|   +--rw keyid      uint32
|   +--...
+--rw access-rules {access-rules}?
| +--rw access-rule* [access-mode]
|   +--rw access-mode  identityref
|   +--rw acl?         -> /acl:acls/acl/name
+--ro clock-state
| +--ro system-status
|   +--ro clock-state  identityref
|   +--ro clock-stratum ntp-stratum
|   +--ro clock-refid  refid
|   +--...
+--rw unicast-configuration* [address type]
|   {unicast-configuration}?
|   +--rw address      inet:ip-address
|   +--rw type         identityref
|   +--...
+--rw associations
|   +--ro association* [address local-mode isconfigured]
|     +--ro address      inet:ip-address
|     +--ro local-mode  identityref
|     +--ro isconfigured boolean
|     +--...
|     +--ro ntp-statistics
|     +--...
+--rw interfaces
|   +--rw interface* [name]
|     +--rw name          if:interface-ref
|     +--rw broadcast-server! {broadcast-server}?
|     | +--...
|     +--rw broadcast-client! {broadcast-client}?
|     +--rw multicast-server* [address] {multicast-server}?
|     | +--rw address
|     | | rt-types:ip-multicast-group-address
|     | +--...
|     +--rw multicast-client* [address] {multicast-client}?
|     | +--rw address      rt-types:ip-multicast-group-address
|     +--rw manycast-server* [address] {manycast-server}?
|     | +--rw address      rt-types:ip-multicast-group-address
|     +--rw manycast-client* [address] {manycast-client}?
|     | +--rw address
|     | | rt-types:ip-multicast-group-address
|     | +--...
+--ro ntp-statistics
+--...

rpcs:
+---x statistics-reset
+---w input
+---w (association-or-all)?
+---: (association)
| +---w associations-address?
| | -> /ntp/associations/association/address
| +---w associations-local-mode?
| | -> /ntp/associations/association/local-mode
| +---w associations-isconfigured?
| | -> /ntp/associations/association/isconfigured
+---: (all)

```

Полное дерево модели данных для модуля YANG ietf-ntp приведено в Приложении А.

Эта модель определяет один контейнер верхнего уровня, включающий конфигурацию и рабочее состояние NTP вместе с правилами доступа, проверкой подлинности, ассоциациями, индивидуальными (unicast) конфигурациями, интерфейсами, статусом и ассоциациями системы.

3. Связи с NTPv4-MIB

Если устройство поддерживает NTPv4-MIB [RFC5907], узлы данных модуля YANG можно сопоставить с объектами NTPv4-MIB, как показано в таблицах 3 и 4.

<i>Узлы данных YANG в /ntp/ clock-state/system-status</i>	<i>Объекты NTPv4-MIB</i>
clock-state	ntpEntStatusCurrentMode
clock-stratum	ntpEntStatusStratum
clock-refid	NtpEntStatusActiveRefSourceId ntpEntStatusActiveRefSourceName
clock-precision	ntpEntTimePrecision
clock-offset	ntpEntStatusActiveOffset
root-dispersion	ntpEntStatusDispersion

Таблица 4. Узлы данных YANG NTP в /ntp/associations/ и объекты NTPv4-MIB.

<i>Узлы данных YANG в /ntp/associations/</i>	<i>Объекты NTPv4-MIB</i>
address	ntpAssocAddressType ntpAssocAddress
stratum	ntpAssocStratum
refid	ntpAssocRefId
offset	ntpAssocOffset

delay	ntpAssocStatusDelay
dispersion	ntpAssocStatusDispersion
ntp-statistics/packet-sent	ntpAssocStatOutPkts
ntp-statistics/packet-received	ntpAssocStatInPkts
ntp-statistics/packet-dropped	ntpAssocStatProtocolError

4. Связи с RFC 7317

В этом разделе описаны связи с определениями NTP в параграфе 3.2 (Управление системным временем) [RFC7317]. Узлы данных YANG в /ntp/ поддерживают настройку на уровне интерфейса, которой нет в /system/ntp. При реализации описанной здесь модели данных YANG ветвь /system/ntp **не следует** использовать и она **должна** игнорироваться.

Таблица 5. Узлы данных в модели YANG NTP и соответствующие узлы из RFC 7317.

Узлы данных YANG в /ntp/

ntp!
unicast-configuration
unicast-configuration/address
unicast-configuration/port
unicast-configuration/type
unicast-configuration/iburst
unicast-configuration/prefer

Узлы данных YANG в /system/ntp

enabled
server server/name
server/transport/udp/address
server/transport/udp/port
server/association-type
server/iburst
server/prefer

5. Правила доступа

Правила доступа в этом разделе относятся к управлению доступом к серверу NTP в линии (on-the-wire) и никак не связаны с какими-либо API управления доступом, например, NETCONF Access Control Model (NACM) [RFC8341].

Списки управления доступом (Access Control List или ACL) являются одним из основных элементов настройки поведения устройств пересылки. ACL - это упорядоченный пользователем список правил, применяемых для фильтрации трафика на сетевом устройстве.

В соответствии с [RFC1305] (для NTPv3) и [RFC5905] (для NTPv4) протокол NTP может включать функцию контроля доступа, предотвращающую несанкционированный доступ и управляющую партнёрами, которым разрешено обновлять локальные часы. Кроме того, полезно различать виды доступа и связывать с каждым своё правило acl-rule. Для этого модуль YANG поддерживает конфигурацию через ветвь /ntp/access-rules. Сами правила access-rule настраиваются в соответствии с [RFC8519]. Поддерживаемые режимы доступа перечислены ниже.

Peer - партнёр

Разрешает другим синхронизировать их часы с сущностью NTP и наоборот. Запросы управления NTP воспринимаются.

Server - сервер

Разрешает другим синхронизировать их часы с сущностью NTP, но не наоборот. Запросы управления NTP воспринимаются.

Server-only - только сервер

Разрешает другим синхронизировать их часы с сущностью NTP, но не наоборот. Запросы управления NTP не воспринимаются.

Query-only - только запросы

Воспринимаются только запросы управления.

Режим Query-only задаёт наибольшие ограничения, а Peer даёт полный доступ. Возможность задавать разные правила ACL для разных режимов доступа обеспечивает контроль со стороны оператора.

6. Управление ключами

В соответствии с [RFC1305] (для NTPv3) и [RFC5905] (для NTPv4) протокол NTP при включённой аутентификации использует криптографические контрольные суммы, рассчитываемые отправителем и проверяемые получателем, вместе с набором заранее распространённых алгоритмов и криптографических ключей, индексируемых идентификаторами, включаемыми в сообщение NTP. Идентификатором keyid служит 32-битовое целое число без знака, которое **должно** быть настроено на партнёрах NTP до начала применения аутентификации. Поэтому данный модуль YANG поддерживает такую настройку в ветви /ntp/authentication/authentication-keys/. Значение keyid указывается при настройке ассоциации NTP (например, unicast-сервер).

Правило nasm:default-deny-all служит для предотвращения доступа к фактическому ключу после его установки.

7. Версия NTP

Эта модель YANG позволяет задать версию NTP для ассоциации, т. е. оператор может выбрать использование NTPv3 [RFC1305] или NTPv4 [RFC5905] для каждой создаваемой ассоциации. Это обеспечивает совместимость с унаследованными системами. Отметим, что протокол NTPv3 [RFC1305] отменён версией NTPv4 [RFC5905].

8. Модуль NTP YANG

```
<CODE BEGINS> file "ietf-ntp@2022-07-05.yang"
module ietf-ntp {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-ntp";
  prefix ntp;

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

```

prefix inet;
reference
  "RFC 6991: Common YANG Data Types";
}
import ietf-interfaces {
  prefix if;
  reference
    "RFC 8343: A YANG Data Model for Interface Management";
}
import ietf-system {
  prefix sys;
  reference
    "RFC 7317: A YANG Data Model for System Management";
}
import ietf-access-control-list {
  prefix acl;
  reference
    "RFC 8519: YANG Data Model for Network Access Control
    Lists (ACLs)";
}
import ietf-routing-types {
  prefix rt-types;
  reference
    "RFC 8294: Common YANG Data Types for the Routing Area";
}
import ietf-netconf-acm {
  prefix nacm;
  reference
    "RFC 8341: Network Configuration Access Control Model";
}

organization
  "IETF NTP (Network Time Protocol) Working Group";
contact
  "WG Web: <https://datatracker.ietf.org/wg/ntp/>
  WG List: <mailto:ntp@ietf.org>
  Editor: Dhruv Dhody
  <mailto:dhruv.ietf@gmail.com>
  Editor: Ankit Kumar Sinha
  <mailto:ankit.ietf@gmail.com>";
description
  "Этот документ задаёт модель данных YANG, которая может служить
  для настройки и управления NTP версии 4, а также позволяет
  настраивать и поддерживать версию 3. Модель включает данные
  конфигурации и состояния.

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

  Авторские права (Copyright (c) 2021) 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 9249, где правовые
  аспекты приведены более полно.";

revision 2022-07-05 {
  description
    "Исходный выпуск";
  reference
    "RFC 9249: A YANG Data Model for NTP";
}

/* Определения типов */

typedef ntp-stratum {
  type uint8 {
    range "1..16";
  }
  description
    "Уровень каждого сервера в иерархии определяется «слоем»
    (stratum). Первичные серверы образуют stratum 1, вторичным
    серверам на каждом уровне назначается stratum на 1 больше,
    чем у предшествующего уровня.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 3";
}

```

```
typedef ntp-version {
    type uint8 {
        range "3..max";
    }
    default "4";
    description
    "Текущая версия NTP, поддерживаемая соответствующей
    ассоциацией";
    reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 1";
}

typedef refid {
    type union {
        type inet:ipv4-address;
        type uint32;
        type string {
            length "4";
        }
    }
    description
    "Код, указывающий определённый сервер или эталонные часы.
    Интерпретация зависит от stratum. Это может быть адрес IPv4,
    первые 32 бита хэш-значения MD5, адрес IPv6 или строка для
    Reference Identifier и kiss-кодов. Например,
    - идентификатор эталонных часов 127.127.1.0 для локальной
    синхронизации
    - индивидуальная, групповая или широковещательная ассоциация
    вида 203.0.113.1 для IPv4 и 0x4321FEDC для IPv6
    - синхронизация с первичным источником вида DCN, NIST, ATOM
    - kis-коды имеют вид AUTH, DROP, RATE

    Хэш MD5 для адресов IPv6 не служит для криптографии.";
    reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 7.3";
}

typedef ntp-date-and-time {
    type union {
        type yang:date-and-time;
        type uint8;
    }
    description
    "Соответствует формату даты и времени при наличии пригодных
    значений. В иных случаях позволяет задавать особые значения,
    такие как 0.";
    reference
    "RFC 6991: Common YANG Data Types";
}

typedef log2seconds {
    type int8;
    description
    "8-битовое целое число со знаком для log2 от числа секунд.";
}

/* Свойства (функции) */

feature ntp-port {
    description
    "Поддержка настройки порта NTP.";
    reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 7.2";
}

feature authentication {
    description
    "Поддержка аутентификации NTP с симметричным ключом.";
    reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 7.3";
}

feature deprecated {
    description
    "Поддержка аутентификации MD5 (RFC 8573), SHA-1 или иного
    устаревшего механизма. Это разрешено для совместимости с
    унаследованными системами, не поддерживающими криптографии,
    а также для строк ключей в формате ASCII.";
    reference
    "RFC 1321: The MD5 Message-Digest Algorithm,
    RFC 3174: US Secure Hash Algorithm 1 (SHA1),
```

```
SHS: Secure Hash Standard (SHS) (FIPS PUB 180-4)";
}

feature hex-key-string {
  description
    "Поддержка шестнадцатеричных строк для ключей.";
}

feature access-rules {
  description
    "Поддержка управления доступом для NTP.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 9.2";
}

feature unicast-configuration {
  description
    "Поддержка режима NTP клиент-сервер или активный-пассивный
    в индивидуальных сессиях";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 3";
}

feature broadcast-server {
  description
    "Поддержка ширококвещательного сервера.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 3";
}

feature broadcast-client {
  description
    "Поддержка ширококвещательных клиентов.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 3";
}

feature multicast-server {
  description
    "Поддержка multicast-сервера.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 3.1";
}

feature multicast-client {
  description
    "Поддержка multicast-клиентов.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 3.1";
}

feature manycast-server {
  description
    "Поддержка manycast-сервера.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 3.1";
}

feature manycast-client {
  description
    "Поддержка manycast-клиентов.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 3.1";
}

/* Идентификаторы (отождествления) */
/* Типы unicast-конфигураций */

identity unicast-configuration-type {
  if-feature "unicast-configuration";
  description
    "Задаёт режим NTP unicast для индивидуальных сессий.";
}

identity uc-server {
  if-feature "unicast-configuration";
  base unicast-configuration-type;
  description
    "Использовать режим клиентской ассоциации, когда задан
```

```
    unicast-адрес сервера.";
}

identity uc-peer {
  if-feature "unicast-configuration";
  base unicast-configuration-type;
  description
  "Использовать режим симметричной активной ассоциации, когда
  настроен адрес партнёра.";
}

/* Режимы ассоциаций */

identity association-mode {
  description
  "Режимы ассоциаций NTP.";
  reference
  "RFC 5905: Network Time Protocol Version 4: Protocol and
  Algorithms Specification, Section 3";
}

identity active {
  base association-mode;
  description
  "Использовать симметричную активную ассоциацию (режим 1).
  Устройство может синхронизироваться от партнёра NTP или
  синхронизировать заданного партнёра NTP.";
}

identity passive {
  base association-mode;
  description
  "Использовать симметричную пассивную ассоциацию (режим 2).
  Устройство получило эту ассоциацию динамически и может
  синхронизироваться от партнёра NTP.";
}

identity client {
  base association-mode;
  description
  "Использовать клиентскую ассоциацию (режим 3).
  Устройство не синхронизирует заданный сервер NTP.";
}

identity server {
  base association-mode;
  description
  "Использовать серверную ассоциацию (режим 4).
  Устройство обеспечивает синхронизацию для клиентов NTP.";
}

identity broadcast-server {
  base association-mode;
  description
  "Использовать режим широковещательного сервера (режим 5).
  Сервер работает как широковещательный или групповой.";
}

identity broadcast-client {
  base association-mode;
  description
  "Режим широковещательного (6) или группового клиента.";
}

/* Режимы доступа */

identity access-mode {
  if-feature "access-rules";
  description
  "Задаёт режимы доступа NTP (применение ACL для NTP).";
  reference
  "RFC 5905: Network Time Protocol Version 4: Protocol and
  Algorithms Specification, Section 9.2";
}

identity peer-access-mode {
  if-feature "access-rules";
  base access-mode;
  description
  "Позволяет другим синхронизировать себя от NTP и наоборот.
  Запросы управления NTP воспринимаются.";
}

identity server-access-mode {
  if-feature "access-rules";
  base access-mode;
}
```



```
description
    "Позволяет другим синхронизировать себя от NTP, но не наоборот.
    Запросы управления NTP воспринимаются.";
}

identity server-only-access-mode {
    if-feature "access-rules";
    base access-mode;
    description
        "Позволяет другим синхронизировать себя от NTP, но не наоборот.
        Запросы управления NTP не воспринимаются.";
}

identity query-only-access-mode {
    if-feature "access-rules";
    base access-mode;
    description
        "Воспринимаются только запросы управления.";
}

/* Состояния часов */

identity clock-state {
    description
        "Задаёт состояние часов NTP на высоком уровне.";
}

identity synchronized {
    base clock-state;
    description
        "Локальные часы синхронизированы с сервером NTP
        или эталонными часами.";
}

identity unsynchronized {
    base clock-state;
    description
        "Локальные часы не синхронизированы с каким-либо сервером NTP";
}

/* ntp-sync-state */

identity ntp-sync-state {
    description
        "Состояние синхронизации часов NTP на более детальном уровне.
        Это называется «определением состояния часов» в RFC 5905.";
    reference
        "RFC 5905: Network Time Protocol Version 4: Protocol and
        Algorithms Specification, Appendix A.1.1";
}

identity clock-never-set {
    base ntp-sync-state;
    description
        "Часы никогда не устанавливались.";
}

identity freq-set-by-cfg {
    base ntp-sync-state;
    description
        "Частота часов задана настройкой NTP или файлом.";
}

identity spike {
    base ntp-sync-state;
    description
        "Обнаружен «всплеск» spike.";
}

identity freq {
    base ntp-sync-state;
    description
        "Указывает режим частоты (frequency mode).";
}

identity clock-synchronized {
    base ntp-sync-state;
    description
        "Часы синхронизированы.";
}

/* Криптоалгоритм */

identity crypto-algorithm {
    description
        "Базовый идентификатор для криптографических алгоритмов.";
```

```
}

identity md5 {
  if-feature "deprecated";
  base crypto-algorithm;
  description
    "Алгоритм MD5. В RFC 8573 отменено использование
    аутентификации на основе MD5.";
  reference
    "RFC 1321: The MD5 Message-Digest Algorithm";
}

identity sha-1 {
  if-feature "deprecated";
  base crypto-algorithm;
  description
    "Алгоритм SHA-1.";
  reference
    "RFC 3174: US Secure Hash Algorithm 1 (SHA1)";
}

identity hmac-sha-1 {
  if-feature "deprecated";
  base crypto-algorithm;
  description
    "Алгоритм аутентификации HMAC-SHA-1.";
  reference
    "SHS: Secure Hash Standard (SHS) (FIPS PUB 180-4)";
}

identity hmac-sha-12 {
  if-feature "deprecated";
  base crypto-algorithm;
  description
    "Алгоритм HMAC-SHA1-12.";
}

identity hmac-sha-256 {
  description
    "Алгоритм аутентификации HMAC-SHA-256.";
  reference
    "SHS: Secure Hash Standard (SHS) (FIPS PUB 180-4)";
}

identity hmac-sha-384 {
  description
    "Алгоритм аутентификации HMAC-SHA-384.";
  reference
    "SHS: Secure Hash Standard (SHS) (FIPS PUB 180-4)";
}

identity hmac-sha-512 {
  description
    "Алгоритм аутентификации HMAC-SHA-512.";
  reference
    "SHS: Secure Hash Standard (SHS) (FIPS PUB 180-4)";
}

identity aes-cmac {
  base crypto-algorithm;
  description
    "Алгоритм AES-CMAC, требуемый RFC 8573 для MAC в NTP.";
  reference
    "RFC 4493: The AES-CMAC Algorithm,
    RFC 8573: Message Authentication Code for the Network
    Time Protocol";
}

/* Группировки */

grouping key {
  description
    "The key";
  nasm:default-deny-all;
  choice key-string-style {
    description
      "Стиль строк ключей";
    case keystack {
      leaf keystack {
        if-feature "deprecated";
        type string;
        description
          "Строки ключей в формате ASCII.";
      }
    }
    case hexadecimal {
```

```

    if-feature "hex-key-string";
    leaf hexadecimal-string {
        type yang:hex-string;
        description
            "Ключ в форме шестнадцатеричной строки. По сравнению с
            ASCII такие строки повышают уровень энтропии при том же
            числе символов в строке ключа. Кроме того, это
            препятствует использованию общеизвестных слов и чисел.";
    }
}
}
}

grouping authentication-key {
    description
        "Задание ключа аутентификации для источника времени NTP.";
    leaf keyid {
        type uint32 {
            range "1..max";
        }
        description
            "Идентификатор ключа аутентификации.";
    }
    leaf algorithm {
        type identityref {
            base crypto-algorithm;
        }
        description
            "Алгоритм аутентификации. RFC 8573 отменяет использование
            аутентификации MD5 и рекомендует применять AES-СМАС.";
    }
    container key {
        uses key;
        description
            "Ключ. RFC 8573 отменяет использование использование
            аутентификации на основе MD5.";
    }
    leaf istrusted {
        type boolean;
        description
            "Доверие к Keyid.";
    }
    reference
        "RFC 5905: Network Time Protocol Version 4: Protocol and
        Algorithms Specification, Sections 7.3 and 7.4";
}

grouping authentication {
    description
        "Аутентификация.";
    choice authentication-type {
        description
            "Тип аутентификации.";
        case symmetric-key {
            leaf keyid {
                type leafref {
                    path "/ntp:ntp/ntp:authentication/"
                        + "ntp:authentication-keys/ntp:keyid";
                }
                description
                    "Идентификатор ключа, указанного в этой ассоциации.";
            }
        }
    }
}

grouping statistics {
    description
        "NTP packet statistic";
    leaf discontinuity-time {
        type ntp-date-and-time;
        description
            "Время последнего разрыва одного или нескольких счетчиков
            NTP. Если разрывов не было, указывается время
            (ре) инициализации ассоциации NTP.";
    }
    leaf packet-sent {
        type yang:counter32;
        description
            "Общее число пакетов NTP, переданных транспортному сервису
            этим объектом NTP в данной ассоциации. Разрывы этого
            счётчика могут возникать при «холодном» перезапуске,
            реинициализации объекта NTP или системы управления, а также
            в иных случаях.";
    }
    leaf packet-sent-fail {

```

```
type yang:counter32;
description
  "Число отказов при передаче пакетов NTP.";
}
leaf packet-received {
type yang:counter32;
description
  "Общее число пакетов NTP, доставленных этому объекту NTP в
данной ассоциации. Разрывы этого счётчика могут возникать
при «холодном» перезапуске, реинициализации объекта NTP или
системы управления, а также в иных случаях.";
}
leaf packet-dropped {
type yang:counter32;
description
  "Общее число пакетов NTP, доставленных этому объекту NTP в
данной ассоциации, которые не были обработаны в результате
ошибки NTP. Разрывы этого счётчика могут возникать
при «холодном» перезапуске, реинициализации объекта NTP или
системы управления, а также в иных случаях.";
}
}

grouping common-attributes {
description
  "Базовые атрибуты NTP для конфигурации";
leaf minpoll {
type log2seconds;
default "6";
description
  "Минимальный интервал опроса в этой ассоциации.";
reference
  "RFC 5905: Network Time Protocol Version 4: Protocol and
Algorithms Specification, Section 7.2";
}
leaf maxpoll {
type log2seconds;
default "10";
description
  "Максимальный интервал опроса в этой ассоциации.";
reference
  "RFC 5905: Network Time Protocol Version 4: Protocol and
Algorithms Specification, Section 7.2";
}
leaf port {
if-feature "ntp-port";
type inet:port-number {
range "123 | 1024..max";
}
default "123";
description
  "Порт, используемый для отправки пакетов NTP.";
reference
  "RFC 5905: Network Time Protocol Version 4: Protocol and
Algorithms Specification, Section 7.2";
}
leaf version {
type ntp-version;
description
  "Версия NTP.";
}
reference
  "RFC 5905: Network Time Protocol Version 4: Protocol and
Algorithms Specification";
}

grouping association-ref {
description
  "Указывает режим ассоциации NTP.";
leaf associations-address {
type leafref {
path "/ntp:ntp/ntp:associations/ntp:association"
+ "/ntp:address";
}
description
  "Указывает адрес ассоциации, задавший синхронизацию часов.";
}
leaf associations-local-mode {
type leafref {
path "/ntp:ntp/ntp:associations/ntp:association"
+ "/ntp:local-mode";
}
description
  "Указывает локальный режим ассоциации, задавший
синхронизацию часов.";
}
}
```

```

leaf associations-isconfigured {
  type leafref {
    path "/ntp:ntp/ntp:associations/ntp:association/"
      + "ntp:isconfigured";
  }
  description
    "Указывает, была ли ассоциация настроена явно
    (что привело к синхронизации часов).";
}

container ntp {
  when 'false() = boolean(/sys:system/sys:ntp)' {
    description
      "Применимо, если не используется /sys/ntp.";
  }
  presence "NTP включён и системе следует пытаться синхронизировать
    свои часы с сервером NTP из списка ntp/associations.";
  description
    "Параметры конфигурации для NTP.";
  leaf port {
    if-feature "ntp-port";
    type inet:port-number {
      range "123 | 1024..max";
    }
    default "123";
    description
      "Порт для передачи и приёма пакетов NTP.";
    reference
      "RFC 5905: Network Time Protocol Version 4: Protocol and
      Algorithms Specification, Section 7.2";
  }
  container refclock-master {
    presence "Первичные часы NTP разрешены.";
    description
      "Задаёт локальные часы этого устройства как сервер NTP.";
    leaf master-stratum {
      type ntp-stratum;
      default "16";
      description
        "Уровень stratum, с которым клиенты NTP синхронизируют
        свои часы.";
    }
  }
  container authentication {
    if-feature "authentication";
    description
      "Настройка аутентификации.";
    leaf auth-enabled {
      type boolean;
      default "false";
      description
        "Управляет применением аутентификации NTP на устройстве.";
    }
    list authentication-keys {
      key "keyid";
      uses authentication-key;
      description
        "Список ключей аутентификации.";
    }
  }
  container access-rules {
    if-feature "access-rules";
    description
      "Настройка управления доступом к сервису NTP с помощью
      функции NTP access-group. Значение access-mode указывает
      способ применения ACL для NTP.";
    list access-rule {
      key "access-mode";
      description
        "Список правил доступа.";
      leaf access-mode {
        type identityref {
          base access-mode;
        }
        description
          "Режим доступа NTP (peer, server, synchronization, query
          и т. п.).";
      }
      leaf acl {
        type leafref {
          path "/acl:acls/acl:acl/acl:name";
        }
        description
          "Применяемая конфигурация контроля доступа.";
      }
    }
  }
}

```

```
reference
  "RFC 5905: Network Time Protocol Version 4: Protocol and
  Algorithms Specification, Section 9.2";
}
}
container clock-state {
  config false;
  description
    "Рабочее состояние часов NTP.";
  container system-status {
    description
      "Cjcnjzybt cbcntvs NTP.";
    leaf clock-state {
      type identityref {
        base clock-state;
      }
      mandatory true;
      description
        "Состояние системных часов (синхронизированы,
        не синхронизированы).";
    }
    leaf clock-stratum {
      type ntp-stratum;
      mandatory true;
      description
        "Значение stratum объекта NTP. Следует устанавливать на
        1 больше, чем на предыдущем уровне. 16 говорит об
        отсутствии синхронизации.";
      reference
        "RFC 5905: Network Time Protocol Version 4: Protocol and
        Algorithms Specification, Section 3";
    }
    leaf clock-refid {
      type refid;
      mandatory true;
      description
        "Код, указывающий определённый сервер или эталонные часы.
        Интерпретация зависит от stratum. Это может быть адрес
        IPv4, первые 32 бита хэш-значения MD5, адрес IPv6 или
        строка для Reference Identifier и kiss-кодов. Например,
        - идентификатор эталонных часов 127.127.1.0 для
          локальной синхронизации
        - индивидуальная, групповая или широковещательная
          ассоциация вида 203.0.113.1 в IPv4 и 0x4321FEDC в IPv6
        - синхронизация с первичным источником вида DCN, NIST,
          ATOM
        - kis-коды имеют вид AUTH, DROP, RATE

        Хэш MD5 для адресов IPv6 не служит для криптографии.";
      reference
        "RFC 5905: Network Time Protocol Version 4: Protocol and
        Algorithms Specification, Section 7.3";
    }
  }
  uses association-ref {
    description
      "Ссылка на ассоциацию";
  }
  leaf nominal-freq {
    type decimal64 {
      fraction-digits 4;
    }
    units "Hz";
    mandatory true;
    description
      "Номинальная частота локальных часов. Идеальная частота с
      нулевой неопределенностью (погрешностью).";
  }
  leaf actual-freq {
    type decimal64 {
      fraction-digits 4;
    }
    units "Hz";
    mandatory true;
    description
      "Фактическая частота локальных часов.";
  }
  leaf clock-precision {
    type log2seconds;
    mandatory true;
    description
      "Точность часов этой системы в виде целого числа со
      знаком log2 секунд - (pres=2^(-n)). Значение 5
      указывает 2^-5 = 0,03125 секунд = 31.25 мсек.";
    reference
      "RFC 5905: Network Time Protocol Version 4: Protocol and
      Algorithms Specification, Section 7.3";
  }
}
```

```

}
leaf clock-offset {
  type decimal64 {
    fraction-digits 3;
  }
  units "milliseconds";
  description
    "Смещение от текущего источника точного времени,
    например, 0,032 мсек или 1,232мсек. Отрицательное
    значение указывает отставание локальных часов.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 9.1";
}
leaf root-delay {
  type decimal64 {
    fraction-digits 3;
  }
  units "milliseconds";
  description
    "Общая задержка на пути к эталонным часам.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Sections 4 and 7.3";
}
leaf root-dispersion {
  type decimal64 {
    fraction-digits 3;
  }
  units "milliseconds";
  description
    "Дисперсия локальных и корневых часов, например,
    6,927 мсек.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Sections 4, 7.3, and 10";
}
leaf reference-time {
  type ntp-date-and-time;
  description
    "Опорная метка времени - момент последней установки или
    корректировки системных часов.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 7.3";
}
leaf sync-state {
  type identityref {
    base ntp-sync-state;
  }
  mandatory true;
  description
    "Состояние синхронизации локальных часов, называемое
    «определением состояния часов» в RFC 5905.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Appendix A.1.1";
}
}
}
list unicast-configuration {
  if-feature "unicast-configuration";
  key "address type";
  description
    "Список unicast-конфигураций NTP.";
  leaf address {
    type inet:ip-address;
    description
      "Адрес для этой ассоциации.";
  }
  leaf type {
    type identityref {
      base unicast-configuration-type;
    }
    description
      "Тип unicast-конфигурации, например, unicast-server";
  }
}
container authentication {
  if-feature "authentication";
  description
    "Аутентификация для данной ассоциации.";
  uses authentication;
}
leaf prefer {
  type boolean;
  default "false";
}

```

```

description
  "Является ли ассоциация предпочтительной.";
}
leaf burst {
  type boolean;
  default "false";
  description
    "Задаёт отправку серии пакетов вместо одного в каждом
    интервале синхронизации для ускорения синхронизации.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 13.1";
}
leaf iburst {
  type boolean;
  default "false";
  description
    "Задаёт отправку серии пакетов вместо одного в каждом
    интервале начальной синхронизации для ускорения
    начальной синхронизации.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 13.1";
}
leaf source {
  type if:interface-ref;
  description
    "Интерфейс, чей адрес IP в этой ассоциации указывает
    источник.";
}
uses common-attributes {
  description
    "Базовые атрибуты, такие как порт, версия, минимальный
    и максимальный интервал опроса.";
}
}
container associations {
  description
    "Параметры ассоциации.";
  list association {
    key "address local-mode isconfigured";
    config false;
    description
      "Список ассоциаций NTP. Требуются поля address, local-mode,
      isconfigured для однозначного указания ассоциации.

      1) Если RT1 является ширококвещательным сервером, а RT2 -
      ширококвещательным клиентом, RT2 будет создавать
      динамическую ассоциацию с address RT1,
      local-mode client и isconfigured false.

      2) Если RT2 настроен с unicast-сервером RT1, RT2 будет
      создавать ассоциацию с address RT1,
      local-mode client, isconfigured true.

      Все листья служат ключами для указания ассоциации.";
    leaf address {
      type inet:ip-address;
      description
        "Удалённый адрес в этой ассоциации - индивидуальный,
        групповой или ширококвещательный адрес IP.";
    }
    leaf local-mode {
      type identityref {
        base association-mode;
      }
      description
        "Локальный режим для этой ассоциации NTP.";
    }
    leaf isconfigured {
      type boolean;
      description
        "Указывает, что ассоциация настроена (true) или
        определена динамически (false).";
    }
    leaf stratum {
      type ntp-stratum;
      description
        "Значение stratum для ассоциации.";
      reference
        "RFC 5905: Network Time Protocol Version 4: Protocol and
        Algorithms Specification, Section 3";
    }
    leaf refid {
      type refid;
      description

```



```

"Код, указывающий определённый сервер или эталонные часы.
Интерпретация зависит от stratum. Это может быть адрес
IPv4, первые 32 бита хэш-значения MD5, адрес IPv6 или
строка для Reference Identifier и kiss-кодов. Например,
- идентификатор эталонных часов 127.127.1.0 для
  локальной синхронизации
- индивидуальная, групповая или широковещательная
  ассоциация вида 203.0.113.1 в IPv4 и 0x4321FEDC в IPv6
- синхронизация с первичным источником вида DCN, NIST,
  АТОМ
- kis-коды имеют вид AUTH, DROP, RATE

  Хэш MD5 для адресов IPv6 не служит для криптографии.";
reference
"RFC 5905: Network Time Protocol Version 4: Protocol and
  Algorithms Specification, Section 7.3";
}
leaf authentication {
  if-feature "authentication";
  type leafref {
    path "/ntp:ntp/ntp:authentication/"
      + "ntp:authentication-keys/ntp:keyid";
  }
  description
    "Ключ аутентификации, применяемый в этой ассоциации.";
}
leaf prefer {
  type boolean;
  default "false";
  description
    "Является ли ассоциация предпочтительной.";
}
leaf peer-interface {
  type if:interface-ref;
  description
    "Интерфейс, применяемый для обмена данными.";
}
uses common-attributes {
  description
    "Базовые атрибуты, такие как порт, версия, минимальный
    и максимальный интервал опроса.";
}
leaf reach {
  type uint8;
  description
    "8-битовый регистр сдвига, отслеживающий генерацию и
    приём пакетов. Служит для определения доступности
    сервера и свежести данных.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Sections 9.2 and 13";
}
leaf unreach {
  type uint8;
  units "seconds";
  description
    "Счётчик секунд недоступности сервера, т. е. reach 0.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Sections 9.2 and 13";
}
leaf poll {
  type log2seconds;
  description
    "Интервал опроса для ассоциации в форме log2 секунд.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 7.3";
}
leaf now {
  type uint32;
  units "seconds";
  description
    "Время последнего приёма пакет NTP или синхронизации.";
}
leaf offset {
  type decimal64 {
    fraction-digits 3;
  }
  units "milliseconds";
  description
    "Смещение локальный часов от часов партнёра, например,
    0,032 мсек или 1,232 мсек. Отрицательное значение
    указывает отставание локальных часов.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and

```

```
    Algorithms Specification, Section 8";
}
leaf delay {
  type decimal64 {
    fraction-digits 3;
  }
  units "milliseconds";
  description
    "Сетевая задержка между локальными часами и часами
    партнёра.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 8";
}
leaf dispersion {
  type decimal64 {
    fraction-digits 3;
  }
  units "milliseconds";
  description
    "Корневая дисперсия между локальными часами и часами
    партнёра.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 10";
}
leaf originate-time {
  type ntp-date-and-time;
  description
    "Локальное время в формате временной метки для момента
    передачи партнёру последнего пакета NTP (T1).";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol and
    Algorithms Specification, Section 8";
}
leaf receive-time {
  type ntp-date-and-time;
  description
    "Локальное время в формате временной метки для момента
    доставки партнёру последнего пакета NTP (T2). При
    недоступности партнёра устанавливается значение 0.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 8";
}
leaf transmit-time {
  type ntp-date-and-time;
  description
    "Локальное время в формате временной метки для момента
    отправки партнёром последнего пакета NTP (T3). При
    недоступности партнёра устанавливается значение 0.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 8";
}
leaf input-time {
  type ntp-date-and-time;
  description
    "Локальное время в формате временной метки для момента
    прибытия от партнёра последнего пакета NTP (T4). При
    недоступности партнёра устанавливается значение 0.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 8";
}
container ntp-statistics {
  description
    "Статистика приёма и передачи пакетов для партнёра.";
  uses statistics {
    description
      "Статистика приёма и передачи пакетов NTP.";
  }
}
}
}
container interfaces {
  description
    "Параметры конфигурации для интерфейсов NTP.";
  list interface {
    key "name";
    description
      "Список интерфейсов.";
    leaf name {
      type if:interface-ref;
      description
        "Имя интерфейса.";
    }
  }
}
```

```
}
container broadcast-server {
  if-feature "broadcast-server";
  presence "Для этого интерфейса настроен широковещательный
    сервер NTP.";
  description
    "Конфигурация широковещательного сервера.";
  leaf ttl {
    type uint8;
    description
      "Срок действия (TTL) для широковещательного пакета.";
    reference
      "RFC 5905: Network Time Protocol Version 4: Protocol
        and Algorithms Specification, Section 3.1";
  }
}
container authentication {
  if-feature "authentication";
  description
    "Аутентификация для интерфейса.";
  uses authentication;
}
uses common-attributes {
  description
    "Базовые атрибуты, такие как порт, версия, минимальный
      и максимальный интервал опроса.";
}
reference
  "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 3.1";
}
container broadcast-client {
  if-feature "broadcast-client";
  presence "Для этого интерфейса настроен широковещательный
    клиент NTP.";
  description
    "Конфигурация широковещательного клиента.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
      and Algorithms Specification, Section 3.1";
}
list multicast-server {
  if-feature "multicast-server";
  key "address";
  description
    "Конфигурация группового сервера";
  leaf address {
    type rt-types:ip-multicast-group-address;
    description
      "IP-адрес для передачи групповых пакетов NTP.";
  }
  leaf ttl {
    type uint8;
    description
      "TTL для групповых пакетов.";
    reference
      "RFC 5905: Network Time Protocol Version 4: Protocol
        and Algorithms Specification, Section 3.1";
  }
}
container authentication {
  if-feature "authentication";
  description
    "Аутентификация для интерфейса.";
  uses authentication;
}
uses common-attributes {
  description
    "Базовые атрибуты, такие как порт, версия, минимальный
      и максимальный интервал опроса.";
}
reference
  "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 3.1";
}
list multicast-client {
  if-feature "multicast-client";
  key "address";
  description
    "Конфигурация группового клиента.";
  leaf address {
    type rt-types:ip-multicast-group-address;
    description
      "IP-адрес группы для присоединения.";
  }
}
reference
  "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 3.1";
```

```
}
list manycast-server {
  if-feature "manycast-server";
  key "address";
  description
    "Конфигурация manycast-сервера.";
  leaf address {
    type rt-types:ip-multicast-group-address;
    description
      "Групповой адрес IP для приёма клиентских сообщений
      manycast.";
  }
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 3.1";
}
list manycast-client {
  if-feature "manycast-client";
  key "address";
  description
    "Конфигурация manycast-клиента.";
  leaf address {
    type rt-types:ip-multicast-group-address;
    description
      "Групповой адрес IP, по которому manycast-клиент
      передаёт запросные сообщения.";
  }
}
container authentication {
  if-feature "authentication";
  description
    "Аутентификация для интерфейса.";
  uses authentication;
}
leaf ttl {
  type uint8;
  description
    "Максимальное значение TTL для расширения
    циклического поиска.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 3.1";
}
leaf minclock {
  type uint8;
  description
    "Минимальное число manycast-оставшихся в ассоциации.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 13.2";
}
leaf maxclock {
  type uint8;
  description
    "Максимальное число manycast-кандидатов в ассоциации.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 13.2";
}
leaf beacon {
  type log2seconds;
  description
    "Верхний предел интервала опроса. Когда TTL достигает
    своего предела без обнаружения минимального числа
    manycast-серверов, интервал опроса увеличивается, пока
    не достигнет значения beacon, после чего процесс
    возвращается к началу.";
  reference
    "RFC 5905: Network Time Protocol Version 4: Protocol
    and Algorithms Specification, Section 13.2";
}
uses common-attributes {
  description
    "Базовые атрибуты, такие как порт, версия, минимальный
    и максимальный интервал опроса.";
}
reference
  "RFC 5905: Network Time Protocol Version 4: Protocol
  and Algorithms Specification, Section 3.1";
}
}
}
container ntp-statistics {
  config false;
  description
    "Общая статистика пакетов NTP.";
  uses statistics {
```

```

    description
      "Статистика переданных и принятых пакетов NTP.";
  }
}
}

rpc statistics-reset {
  description
    "Сброс собранной статистики.";
  input {
    choice association-or-all {
      description
        "Сброс статистики одной или всех ассоциаций.";
      case association {
        uses association-ref;
        description
          "Сброс всех статистики для ассоциации.";
      }
      case all {
        description
          "Сброс всей собранной статистики.";
      }
    }
  }
}
}
<CODE ENDS>

```

9. Пример использования

В этом разделе приведены примеры, служащие для иллюстрации. Символ \ в конце строки служит для разделения длинных строк на части [RFC8792].

9.1. Индивидуальная ассоциация

Этот пример описывает настройку предпочтительного unicast-сервера с адресом 192.0.2.1 на порту 1025, ключом аутентификации 10 и версией 4 (принята по умолчанию).

```

<edit-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <target>
    <running/>
  </target>
  <config>
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <unicast-configuration>
        <address>192.0.2.1</address>
        <type>uc-server</type>
        <prefer>true</prefer>
        <port>1025</port>
        <authentication>
          <symmetric-key>
            <keyid>10</keyid>
          </symmetric-key>
        </authentication>
      </unicast-configuration>
    </ntp>
  </config>
</edit-config>

```

В примере для IPv6 в листе address указывается адрес IPv6 (например, 2001:db8::1), а остальное не меняется.

```

<edit-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <target>
    <running/>
  </target>
  <config>
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <unicast-configuration>
        <address>2001:db8::1</address>
        <type>uc-server</type>
        <prefer>true</prefer>
        <port>1025</port>
        <authentication>
          <symmetric-key>
            <keyid>10</keyid>
          </symmetric-key>
        </authentication>
      </unicast-configuration>
    </ntp>
  </config>
</edit-config>

```

Ниже приведён пример извлечения unicast-конфигураций.

```

<get>
  <filter type="subtree">
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <unicast-configuration>
        </unicast-configuration>
    </ntp>
  </filter>
</get>

```

```

</ntp>
</filter>
</get>

<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
    <unicast-configuration>
      <address>192.0.2.1</address>
      <type>uc-server</type>
      <authentication>
        <symmetric-key>
          <keyid>10</keyid>
        </symmetric-key>
      </authentication>
      <prefer>true</prefer>
      <burst>false</burst>
      <iburst>true</iburst>
      <source/>
      <minpoll>6</minpoll>
      <maxpoll>10</maxpoll>
      <port>1025</port>
      <stratum>9</stratum>
      <refid>203.0.113.1</refid>
      <reach>255</reach>
      <unreach>0</unreach>
      <poll>128</poll>
      <now>10</now>
      <offset>0.025</offset>
      <delay>0.5</delay>
      <dispersion>0.6</dispersion>
      <originate-time>10-10-2017 07:33:55.253 Z+05:30\
</originate-time>
      <receive-time>10-10-2017 07:33:55.258 Z+05:30\
</receive-time>
      <transmit-time>10-10-2017 07:33:55.300 Z+05:30\
</transmit-time>
      <input-time>10-10-2017 07:33:55.305 Z+05:30\
</input-time>
      <ntp-statistics>
        <packet-sent>20</packet-sent>
        <packet-sent-fail>0</packet-sent-fail>
        <packet-received>20</packet-received>
        <packet-dropped>0</packet-dropped>
      </ntp-statistics>
    </unicast-configuration>
  </ntp>
</data>

```

9.2. Первичные эталонные часы

В этом примере показано, как настроить эталонные часы со stratum 8.

```

<edit-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <target>
    <running/>
  </target>
  <config>
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <refclock-master>
        <master-stratum>8</master-stratum>
      </refclock-master>
    </ntp>
  </config>
</edit-config>

```

Следующий пример показывает, как получить конфигурацию эталонных часов.

```

<get>
  <filter type="subtree">
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <refclock-master>
      </refclock-master>
    </ntp>
  </filter>
</get>

<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
    <refclock-master>
      <master-stratum>8</master-stratum>
    </refclock-master>
  </ntp>
</data>

```

9.3. Настройка аутентификации

Этот пример показывает включение проверки подлинности и настройку доверенного ключа аутентификации key 10 в режиме AES-CMAC с шестнадцатеричной строкой ключа.

```

<edit-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <target>
    <running/>
  </target>
  <config>
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <authentication>
        <auth-enabled>true</auth-enabled>
        <authentication-keys>
          <keyid>10</keyid>
          <algorithm>aes-cmac</algorithm>
          <key>
            <hexadecimal-string>
              bb1d6929e95937287fa37d129b756746
            </hexadecimal-string>
          </key>
          <istrusted>true</istrusted>
        </authentication-keys>
      </authentication>
    </ntp>
  </config>
</edit-config>

```

9.4. Настройка доступа

Этот пример показывает, как настроить режим peer-access-mode со списком доступа ACL 2000.

```

<edit-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <target>
    <running/>
  </target>
  <config>
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <access-rules>
        <access-rule>
          <access-mode>peer-access-mode</access-mode>
          <acl>2000</acl>
        </access-rule>
      </access-rules>
    </ntp>
  </config>
</edit-config>

```

Следующий пример показывает получение конфигурации, связанной с доступом.

```

<get>
  <filter type="subtree">
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <access-rules>
    </access-rules>
    </ntp>
  </filter>
</get>

<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
    <access-rules>
      <access-rule>
        <access-mode>peer-access-mode</access-mode>
        <acl>2000</acl>
      </access-rule>
    </access-rules>
  </ntp>
</data>

```

9.5. Групповая конфигурация

Этот пример описывает настройку группового сервера с адресом 224.0.1.1, портом 1025, версией 3 и ключом аутентификации 10.

```

<edit-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <target>
    <running/>
  </target>
  <config>
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <interfaces>
        <interface>
          <name>Ethernet3/0/0</name>
          <multicast-server>
            <address>224.0.1.1</address>
            <authentication>
              <symmetric-key>
                <keyid>10</keyid>
              </symmetric-key>
            </authentication>
            <port>1025</port>
            <version>3</version>
          </multicast-server>
        </interface>
      </interfaces>
    </ntp>
  </config>
</edit-config>

```

```

</interface>
</interfaces>
</ntp>
</config>
</edit-config>

```

Следующий пример иллюстрирует получение конфигурации, связанной с групповым сервером.

```

<get>
  <filter type="subtree">
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <interfaces>
        <interface>
          <multicast-server>
          </multicast-server>
        </interface>
      </interfaces>
    </ntp>
  </filter>
</get>

<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
    <interfaces>
      <interface>
        <name>Ethernet3/0/0</name>
        <multicast-server>
          <address>224.0.1.1</address>
          <ttl>8</ttl>
          <authentication>
            <symmetric-key>
              <keyid>10</keyid>
            </symmetric-key>
          </authentication>
          <minpoll>6</minpoll>
          <maxpoll>10</maxpoll>
          <port>1025</port>
          <version>3</version>
        </multicast-server>
      </interface>
    </interfaces>
  </ntp>
</data>

```

Ниже приведён пример настройки группового клиента с адресом 224.0.1.1.

```

<edit-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <target>
    <running/>
  </target>
  <config>
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <interfaces>
        <interface>
          <name>Ethernet3/0/0</name>
          <multicast-client>
            <address>224.0.1.1</address>
          </multicast-client>
        </interface>
      </interfaces>
    </ntp>
  </config>
</edit-config>

```

Далее показано, как получить связанную с групповым клиентом конфигурацию.

```

<get>
  <filter type="subtree">
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <interfaces>
        <interface>
          <multicast-client>
          </multicast-client>
        </interface>
      </interfaces>
    </ntp>
  </filter>
</get>

<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
    <interfaces>
      <interface>
        <name>Ethernet3/0/0</name>
        <multicast-client>
          <address>224.0.1.1</address>
        </multicast-client>
      </interface>
    </interfaces>
  </ntp>
</data>

```



```
</ntp>
</data>
```

9.6. Конфигурация manycast

Ниже показана конфигурация manycast-клиента с адресом 224.0.1.1, портом 1025 и ключом аутентификации 10.

```
<edit-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <target>
    <running/>
  </target>
  <config>
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <interfaces>
        <interface>
          <name>Ethernet3/0/0</name>
          <manycast-client>
            <address>224.0.1.1</address>
            <authentication>
              <symmetric-key>
                <keyid>10</keyid>
              </symmetric-key>
            </authentication>
            <port>1025</port>
          </manycast-client>
        </interface>
      </interfaces>
    </ntp>
  </config>
</edit-config>
```

Следующий пример иллюстрирует получение конфигурации, связанной с manycast-коинентом.

```
<get>
  <filter type="subtree">
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <interfaces>
        <interface>
          <manycast-client>
            </manycast-client>
          </interface>
        </interfaces>
      </ntp>
    </filter>
  </get>

<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
    <interfaces>
      <interface>
        <name>Ethernet3/0/0</name>
        <manycast-client>
          <address>224.0.1.1</address>
          <authentication>
            <symmetric-key>
              <keyid>10</keyid>
            </symmetric-key>
          </authentication>
          <ttl>8</ttl>
          <minclock>3</minclock>
          <maxclock>10</maxclock>
          <beacon>6</beacon>
          <minpoll>6</minpoll>
          <maxpoll>10</maxpoll>
          <port>1025</port>
        </manycast-client>
      </interface>
    </interfaces>
  </ntp>
</data>
```

Далее показано, как настроить manycast-сервер с адресом 224.0.1.1.

```
<edit-config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <target>
    <running/>
  </target>
  <config>
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <interfaces>
        <interface>
          <name>Ethernet3/0/0</name>
          <manycast-server>
            <address>224.0.1.1</address>
          </manycast-server>
        </interface>
      </interfaces>
    </ntp>
  </config>
```

`</edit-config>`

Ниже приведён пример извлечения конфигурации, связанной с manycast-сервером.

```
<get>
  <filter type="subtree">
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <interfaces>
        <interface>
          <manycast-server>
          </manycast-server>
        </interface>
      </interfaces>
    </ntp>
  </filter>
</get>

<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
    <interfaces>
      <interface>
        <name>Ethernet3/0/0</name>
        <manycast-server>
          <address>224.0.1.1</address>
        </manycast-server>
      </interface>
    </interfaces>
  </ntp>
</data>
```

9.7. Состояние часов

Ниже приведён пример получения текущего состояния часов.

```
<get>
  <filter type="subtree">
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <clock-state>
      </clock-state>
    </ntp>
  </filter>
</get>

<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
    <clock-state>
      <system-status>
        <clock-state>synchronized</clock-state>
        <clock-stratum>7</clock-stratum>
        <clock-refid>192.0.2.1</clock-refid>
        <associations-address>192.0.2.1\
        </associations-address>
        <associations-local-mode>client\
        </associations-local-mode>
        <associations-isconfigured>yes\
        </associations-isconfigured>
        <nominal-freq>100.0</nominal-freq>
        <actual-freq>100.0</actual-freq>
        <clock-precision>18</clock-precision>
        <clock-offset>0.025</clock-offset>
        <root-delay>0.5</root-delay>
        <root-dispersion>0.8</root-dispersion>
        <reference-time>10-10-2017 07:33:55.258 Z+05:30\
        </reference-time>
        <sync-state>clock-synchronized</sync-state>
      </system-status>
    </clock-state>
  </ntp>
</data>
```

9.8. Получение всех ассоциаций

В примере показано, как получить все ассоциации, имеющиеся в системе.

```
<get>
  <filter type="subtree">
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <associations>
      </associations>
    </ntp>
  </filter>
</get>

<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
    <associations>
      <association>
        <address>192.0.2.1</address>
        <stratum>9</stratum>
      </association>
    </associations>
  </ntp>
</data>
```

```

<refid>203.0.113.1</refid>
<local-mode>client</local-mode>
<isconfigured>>true</isconfigured>
<authentication-key>10</authentication-key>
<prefer>true</prefer>
<peer-interface>Ethernet3/0/0</peer-interface>
<minpoll>6</minpoll>
<maxpoll>10</maxpoll>
<port>1025</port>
<version>4</version>
<reach>255</reach>
<unreach>0</unreach>
<poll>128</poll>
<now>10</now>
<offset>0.025</offset>
<delay>0.5</delay>
<dispersion>0.6</dispersion>
<originate-time>10-10-2017 07:33:55.253 Z+05:30\
</originate-time>
<receive-time>10-10-2017 07:33:55.258 Z+05:30\
</receive-time>
<transmit-time>10-10-2017 07:33:55.300 Z+05:30\
</transmit-time>
<input-time>10-10-2017 07:33:55.305 Z+05:30\
</input-time>
<ntp-statistics>
  <packet-sent>20</packet-sent>
  <packet-sent-fail>0</packet-sent-fail>
  <packet-received>20</packet-received>
  <packet-dropped>0</packet-dropped>
</ntp-statistics>
</association>
</associations>
</ntp>
</data>

```

9.9. Глобальная статистика

Ниже приведён пример извлечения глобальной статистики.

```

<get>
  <filter type="subtree">
    <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
      <ntp-statistics>
      </ntp-statistics>
    </ntp>
  </filter>
</get>

<data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ntp xmlns="urn:ietf:params:xml:ns:yang:ietf-ntp">
    <ntp-statistics>
      <packet-sent>30</packet-sent>
      <packet-sent-fail>5</packet-sent-fail>
      <packet-received>20</packet-received>
      <packet-dropped>2</packet-dropped>
    </ntp-statistics>
  </ntp>
</data>

```

10. Взаимодействие с IANA

10.1. IETF XML Registry

Этот документ регистрирует URI в реестре IETF XML Registry [RFC3688] в формате RFC 3688.

```

URI: urn:ietf:params:xml:ns:yang:ietf-ntp
Registrant Contact: The IESG.
XML: N/A; запрошенный URI является пространством имён XML.

```

10.2. YANG Module Names

Этот документ регистрирует модуль YANG в реестре YANG Module Names [RFC6020].

```

Name: ietf-ntp
Namespace: urn:ietf:params:xml:ns:yang:ietf-ntp
Prefix: ntp
Reference: RFC 9249

```

11. Вопросы безопасности

Заданный этим документом модуль YANG определяет схему для данных, предназначенную для доступа через сеть с использованием протоколов управления, таких как NETCONF [RFC6241] или RESTCONF [RFC8040]. Нижним уровнем NETCONF служит защищённый транспорт с обязательной поддержкой SSH (Secure Shell) [RFC6242]. Нижним уровнем RESTCONF служит протокол HTTPS с обязательной поддержкой защиты на транспортном уровне (TLS) [RFC8446].

Модель доступа к конфигурации сети (NACM – Network Configuration Access Control Model) [RFC8341] обеспечивает возможность разрешить доступ лишь определённых пользователей NETCONF или RESTCONF к заранее заданному подмножеству операций NETCONF или RESTCONF и содержимого.

В этом модуле данных YANG определено множество узлов данных, которые разрешают запись, создание и удаление (т. е. config true, как принято по умолчанию). Эти узлы могут быть конфиденциальными или уязвимыми в некоторых сетевых средах. Запись в такие узлы (например, edit-config) без должной защиты может негативно влиять на работу сети. Ниже перечислены ветви и узлы, которые могут быть конфиденциальными или уязвимыми.

/ntp/port

Задаёт номер порта для передачи пакетов NTP. Неожиданная смена может нарушать работу сети.

/ntp/authentication u /ntp/access-rules

Запись конфигураций аутентификации и контроля доступа. Эти параметры следует устанавливать осторожно.

/ntp/unicast-configuration

Записи для всех unicast-конфигураций (режим server или peer), опосредованно создающие или меняющие ассоциации NTP. Неожиданные изменения могут нарушать работу сети.

/ntp/interfaces/interface

Записи для всех unicast-конфигураций на уровне интерфейса, относящихся к широкополосному, групповому или индивидуальному режиму, опосредованно создающие или меняющие ассоциации NTP. Неожиданные изменения могут нарушать работу сети. Возможна также синхронизация от недоверенных источников.

Некоторые из доступных для чтения узлов в этом модуле YANG могут быть конфиденциальными или уязвимыми в той или иной сетевой среде. Важно контролировать доступ к таким объектам (например, get, get-config, notification). Ниже перечислены ветви и узлы, которые могут быть конфиденциальными или уязвимыми.

/ntp/authentication/authentication-keys

Записи списка содержат ключи аутентификации NTP. Несанкционированный доступ к ключам может обеспечить доступ к сервису NTP. Ключи конфиденциальны и несанкционированный доступ к ним требуется предотвращать.

/ntp/associations/association/

Этот список содержит все ассоциации NTP во всех режимах. Доступ к этим узлам может раскрывать топологию сети и отношения доверия. Несанкционированный доступ к записям требуется предотвращать.

/ntp/authentication and /ntp/access-rules

Записи этого списка содержат настройки аутентификации и контроля доступа. Доступ к этим узлам может раскрывать топологию сети и отношения доверия.

Некоторые из операций RPC в этом модуле YANG могут быть чувствительными или уязвимыми в той или иной сетевой среде. Важно контролировать доступ к таким операциям.

statistics-reset

Этот вызов RPC служит для сброса статистики. Несанкционированный доступ может влиять на мониторинг.

Лист `/ntp/authentication/authentication-keys/algorithm` может указывать криптографические алгоритмы, которые больше не считаются надёжными. В соответствии с [RFC8573] рекомендуется применять алгоритм AES-СМАС .

12. Литература

12.1. Нормативные документы

- [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>>.
- [RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, [RFC 3688](#), DOI 10.17487/RFC3688, January 2004, <<https://www.rfc-editor.org/info/rfc3688>>.
- [RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", [RFC 5905](#), DOI 10.17487/RFC5905, June 2010, <<https://www.rfc-editor.org/info/rfc5905>>.
- [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>>.
- [RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", [RFC 6991](#), DOI 10.17487/RFC6991, July 2013, <<https://www.rfc-editor.org/info/rfc6991>>.
- [RFC7317] Bierman, A. and M. Bjorklund, "A YANG Data Model for System Management", [RFC 7317](#), DOI 10.17487/RFC7317, August 2014, <<https://www.rfc-editor.org/info/rfc7317>>.
- [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>>.
- [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>>.
- [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>>.
- [RFC8294] Liu, X., Qu, Y., Lindem, A., Hopps, C., and L. Berger, "Common YANG Data Types for the Routing Area", [RFC 8294](#), DOI 10.17487/RFC8294, December 2017, <<https://www.rfc-editor.org/info/rfc8294>>.
- [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>>.
- [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>>.
- [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>>.
- [RFC8519] Jethanandani, M., Agarwal, S., Huang, L., and D. Blair, "YANG Data Model for Network Access Control Lists (ACLs)", [RFC 8519](#), DOI 10.17487/RFC8519, March 2019, <<https://www.rfc-editor.org/info/rfc8519>>.
- [RFC8573] Malhotra, A. and S. Goldberg, "Message Authentication Code for the Network Time Protocol", RFC 8573, DOI 10.17487/RFC8573, June 2019, <<https://www.rfc-editor.org/info/rfc8573>>.

12.2. Дополнительная литература

- [RFC1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation and Analysis", [RFC 1305](#), DOI 10.17487/RFC1305, March 1992, <<https://www.rfc-editor.org/info/rfc1305>>.
- [RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", [RFC 1321](#), DOI 10.17487/RFC1321, April 1992, <<https://www.rfc-editor.org/info/rfc1321>>.
- [RFC3174] Eastlake 3rd, D. and P. Jones, "US Secure Hash Algorithm 1 (SHA1)", [RFC 3174](#), DOI 10.17487/RFC3174, September 2001, <<https://www.rfc-editor.org/info/rfc3174>>.
- [RFC4493] Song, JH., Poovendran, R., Lee, J., and T. Iwata, "The AES-CMAC Algorithm", RFC 4493, DOI 10.17487/RFC4493, June 2006, <<https://www.rfc-editor.org/info/rfc4493>>.
- [RFC5907] Gerstung, H., Elliott, C., and B. Haberman, Ed., "Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)", RFC 5907, DOI 10.17487/RFC5907, June 2010, <<https://www.rfc-editor.org/info/rfc5907>>.
- [RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", [RFC 8342](#), DOI 10.17487/RFC8342, March 2018, <<https://www.rfc-editor.org/info/rfc8342>>.
- [RFC8792] Watsen, K., Auerswald, E., Farrel, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and RFCs", [RFC 8792](#), DOI 10.17487/RFC8792, June 2020, <<https://www.rfc-editor.org/info/rfc8792>>.
- [SHS] National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)", DOI 10.6028/NIST.FIPS.180-4, FIPS PUB 180-4, August 2015, <<https://doi.org/10.6028/NIST.FIPS.180-4>>.

Приложение А. Полное дерево YANG

Полное дерево модели данных YANG ietf-ntp приведено ниже.

```

module: ietf-ntp
  +--rw ntp!
    +--rw port?                               inet:port-number {ntp-port}?
    +--rw refclock-master!
      | +--rw master-stratum? ntp-stratum
    +--rw authentication {authentication}?
      | +--rw auth-enabled? boolean
      | +--rw authentication-keys* [keyid]
      |   +--rw keyid uint32
      |   +--rw algorithm? identityref
      |   +--rw key
      |     | +--rw (key-string-style)?
      |     |   +--:(keystring)
      |     |   | +--rw keystring? string {deprecated}?
      |     |   +--:(hexadecimal) {hex-key-string}?
      |     |   +--rw hexadecimal-string? yang:hex-string
      |     +--rw istrusted? boolean
    +--rw access-rules {access-rules}?
      | +--rw access-rule* [access-mode]
      |   +--rw access-mode identityref
      |   +--rw acl? -> /acl:acls/acl/name
    +--ro clock-state
      | +--ro system-status
      | +--ro clock-state identityref
      | +--ro clock-stratum ntp-stratum
      | +--ro clock-refid refid
      | +--ro associations-address?
      |   | -> /ntp/associations/association/address
      | +--ro associations-local-mode?
      |   | -> /ntp/associations/association/local-mode
      | +--ro associations-isconfigured?
      |   | -> /ntp/associations/association/isconfigured
      | +--ro nominal-freq decimal64
      | +--ro actual-freq decimal64
      | +--ro clock-precision log2seconds
      | +--ro clock-offset? decimal64
      | +--ro root-delay? decimal64
      | +--ro root-dispersion? decimal64
      | +--ro reference-time? ntp-date-and-time
      | +--ro sync-state identityref
    +--rw unicast-configuration* [address type]
      | {unicast-configuration}?
  
```

```

| +--rw address          inet:ip-address
| +--rw type             identityref
| +--rw authentication {authentication}?
| | +--rw (authentication-type)?
| | | +--:(symmetric-key)
| | | | +--rw keyid?    leafref
| +--rw prefer?         boolean
| +--rw burst?          boolean
| +--rw iburst?         boolean
| +--rw source?         if:interface-ref
| +--rw minpoll?        log2seconds
| +--rw maxpoll?        log2seconds
| +--rw port?           inet:port-number {ntp-port}?
| +--rw version?        ntp-version
+--rw associations
| +--ro association* [address local-mode isconfigured]
| | +--ro address          inet:ip-address
| | +--ro local-mode       identityref
| | +--ro isconfigured     boolean
| | +--ro stratum?        ntp-stratum
| | +--ro refid?          refid
| | +--ro authentication?
| | | -> /ntp/authentication/authentication-keys/keyid
| | | {authentication}?
| | +--ro prefer?         boolean
| | +--ro peer-interface? if:interface-ref
| | +--ro minpoll?        log2seconds
| | +--ro maxpoll?        log2seconds
| | +--ro port?           inet:port-number {ntp-port}?
| | +--ro version?        ntp-version
| | +--ro reach?          uint8
| | +--ro unreach?        uint8
| | +--ro poll?           log2seconds
| | +--ro now?            uint32
| | +--ro offset?         decimal64
| | +--ro delay?          decimal64
| | +--ro dispersion?     decimal64
| | +--ro originate-time? ntp-date-and-time
| | +--ro receive-time?   ntp-date-and-time
| | +--ro transmit-time?  ntp-date-and-time
| | +--ro input-time?     ntp-date-and-time
| | +--ro ntp-statistics
| | | +--ro discontinuity-time? ntp-date-and-time
| | | +--ro packet-sent?        yang:counter32
| | | +--ro packet-sent-fail?   yang:counter32
| | | +--ro packet-received?    yang:counter32
| | | +--ro packet-dropped?     yang:counter32
+--rw interfaces
| +--rw interface* [name]
| | +--rw name          if:interface-ref
| | +--rw broadcast-server! {broadcast-server}?
| | | +--rw ttl?        uint8
| | | +--rw authentication {authentication}?
| | | | +--rw (authentication-type)?
| | | | | +--:(symmetric-key)
| | | | | | +--rw keyid?    leafref
| | | +--rw minpoll?    log2seconds
| | | +--rw maxpoll?    log2seconds
| | | +--rw port?       inet:port-number {ntp-port}?
| | | +--rw version?    ntp-version
+--rw broadcast-client! {broadcast-client}?
+--rw multicast-server* [address] {multicast-server}?
| +--rw address
| | rt-types:ip-multicast-group-address
| +--rw ttl?          uint8
| +--rw authentication {authentication}?
| | +--rw (authentication-type)?
| | | +--:(symmetric-key)
| | | | +--rw keyid?    leafref
| | +--rw minpoll?    log2seconds
| | +--rw maxpoll?    log2seconds
| | +--rw port?       inet:port-number {ntp-port}?
| | +--rw version?    ntp-version
+--rw multicast-client* [address] {multicast-client}?
| +--rw address      rt-types:ip-multicast-group-address
+--rw manycast-server* [address] {manycast-server}?
| +--rw address      rt-types:ip-multicast-group-address
+--rw manycast-client* [address] {manycast-client}?
| +--rw address
| | rt-types:ip-multicast-group-address
+--rw authentication {authentication}?
| +--rw (authentication-type)?
| | +--:(symmetric-key)
| | | +--rw keyid?    leafref
+--rw ttl?          uint8
+--rw minclock?     uint8

```

```

|         +--rw maxclock?          uint8
|         +--rw beacon?            log2seconds
|         +--rw minpoll?           log2seconds
|         +--rw maxpoll?           log2seconds
|         +--rw port?              inet:port-number {ntp-port}?
|         +--rw version?           ntp-version
+--ro ntp-statistics
  +--ro discontinuity-time?        ntp-date-and-time
  +--ro packet-sent?              yang:counter32
  +--ro packet-sent-fail?         yang:counter32
  +--ro packet-received?          yang:counter32
  +--ro packet-dropped?           yang:counter32

rpcs:
  +---x statistics-reset
    +---w input
      +---w (association-or-all)?
        +---: (association)
          | +---w associations-address?
          | |         -> /ntp/associations/association/address
          | +---w associations-local-mode?
          | |         -> /ntp/associations/association/local-mode
          | +---w associations-isconfigured?
          |         -> /ntp/associations/association/isconfigured
          +---: (all)

```

Благодарности

Авторы признательны Sladjana Zoric, Danny Mayer, Harlan Stenn, Ulrich Windl, Miroslav Lichvar, Maurice Angermann, Watson Ladd, Rich Salz за их рецензии и предложения.

Спасибо Andy Bierman за рецензию YANG doctor.

Спасибо Dieter Sibold за выполнение функций Document Shepherd и Erik Kline - за Responsible AD.

Спасибо Takeshi Takahashi за рецензию SECDIR, Tim Evens - за рецензию GENART.

Особая благодарность Tom Petch за очень подробную рецензию YANG и множество предложений и улучшений.

Спасибо за рецензию IESG от Benjamin Kaduk, Francesca Palombini, Eric Vyncke, Murray Kucherawy, Robert Wilton, Roman Danyliw, Zaheduzzaman Sarker.

Адреса авторов

Nan Wu
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing
100095
China
Email: eric.wu@huawei.com

Dhruv Dhody (editor)
Huawei
Divyashree Techno Park, Whitefield
Bangalore 560066
Kanataka
India
Email: dhruv.ietf@gmail.com

Ankit Kumar Sinha (editor)
RtBrick Inc.
Bangalore

Kanataka
India
Email: ankit.ietf@gmail.com

Anil Kumar S N
RtBrick Inc.
Bangalore
Kanataka
India
Email: anil.ietf@gmail.com

Yi Zhao
Ericsson
China Digital Kingdom Bld., No.1 WangJing North Rd.
Beijing
100102
China
Email: yi.z.zhao@ericsson.com

Перевод на русский язык

Николай Малых
nmalykh@protokols.ru