ИРКУТСКИЙ ПОЛИТЕХ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Лекция по дисциплине
«Сети и телекоммуникации»

Протоколы прикладного уровня:

Domain Name System (DNS);

Simple Network Management Protocol (SNMP).

Руководитель лаборатории сетевых технологий
института ИТиАД ИРНИТУ:
Аношко Алексей Федорович
Telegram: @a_anoshko

Что такое DNS?

DNS расшифровывается как *Domain Name System*.

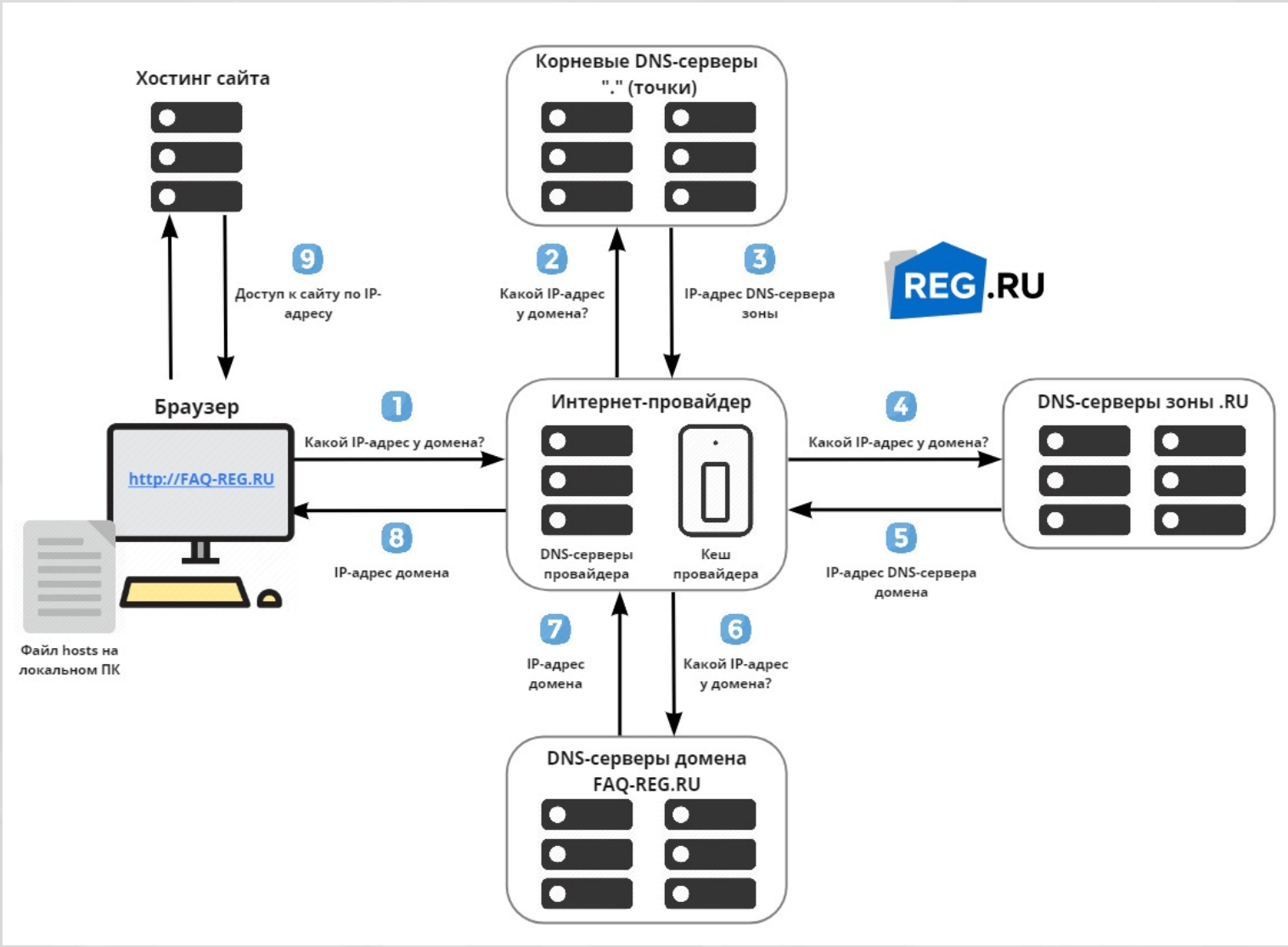
Это глобальное распределенное хранилище ключей и значений.

Сервера по всему миру могут предоставить вам значение по ключу, а если им неизвестен ключ, то они попросят помощи у другого сервера.

Ваш браузер (или любой другой сервис) запрашивает значение для ключа www.example.com, и получает в ответ 1.2.3.4.

Корневые домены или домены верхнего уровня в сети Internet управляются центром **InterNIC** (Public Information Regarding Internet Domain Name Registration Services).

Как работает DNS?



Как работает DNS?

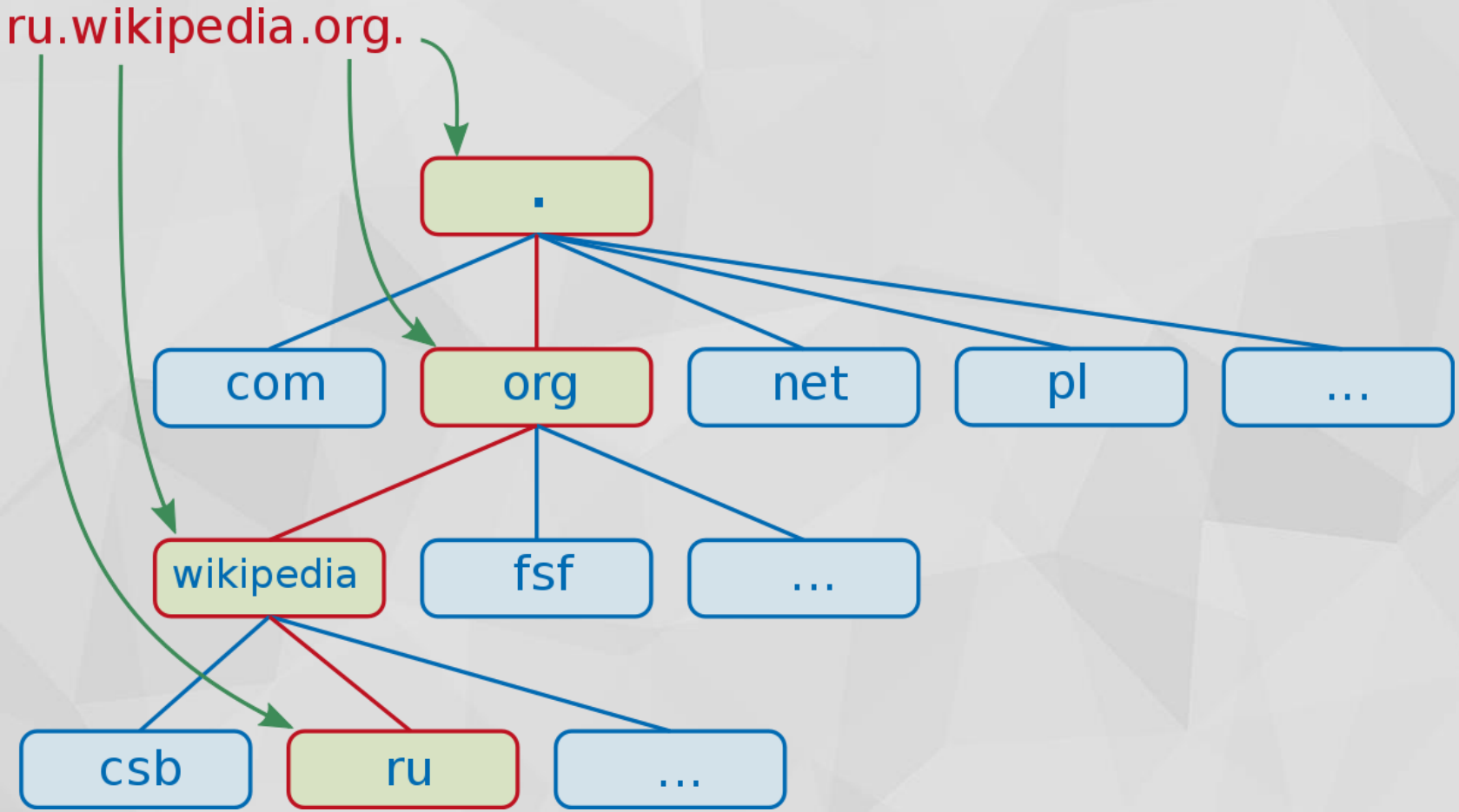
Принцип работы DNS похож на поиск и вызов контактов из телефонной книги смартфона. Ищем имя, нажимаем «позвонить», и телефон соединяет нас с нужным абонентом. Понятно, что смартфон в ходе звонка не использует само имя человека, вызов возможен только по номеру телефона. Если вы внесете имя без номера телефона, позвонить человеку не сможете.

Кроме того, DNS-серверы служат для хранения ресурсных записей доменов.

В Интернете огромное количество DNS-серверов и каждый выполняет свою функцию в общей системе.

База имен является распределенной, так как нет такого сервера, где бы хранилась вся эта информация.
Имя содержит несколько полей (длиной не более 63 символов), разделенных точками. Имя может содержать не более 255 октетов, включая байт длины. Анализ имени производится справа налево. Самая правая секция имени характеризует страну (двухсимвольные национальные коды смотри в приложении), или характер организации образовательная, коммерческая, правительственная и т.д.).

Поля DNS имени



Стандартизованные суффиксы имен

Поле адреса	Тип сети
.aero	Фирма или организация, относящаяся к сфере авиации;
.arts	Культура и досуг;
.biz	Организация, относящаяся к сфере бизнеса;
.com	Коммерческая организация;
.firm	Коммерческое предприятие;
.gov	Государственное учреждение (США);
.info	Открытая TLD-структура (регистрация имен доменов)
.org	Бесприбыльная организация;
.edu	Учебное заведение;
.jobs	Работодатели;
.mil	Военное предприятие или организация (США);
.mobi	Сайты и сервисы, ориентированные на работу с мобильными телефонами и беспроводными устройствами
.museum	Имя домена музея
.name	Имя домена частного лица
.net	Большая сеть;
.pro	Профессионал, достойный доверия. Управляется RegistryPro (http://www.nic.pro/);
.int	Международная организация;
.rec	Развлечения;
.tel	Хранение и управление персональными и корпоративными контактными данными;
.travel	Турагенства;
.tv	Телевидение. (см. Национальные коды доменов в Интернет этот домен записан попрежнему за TUVALU)
.web	Организация, вовлеченная в WEB-активность

Типы ресурсных записей DNS

Тип	Расшифровка названия (англ.)	Код	Описание	RFC
A	Address	1	Адресная запись, соответствие между именем и IP-адресом	RFC 1035
AAAA	Address IPv6	28	Адрес в формате IPv6	RFC 3596
CNAME	Canonical name	5	Каноническое имя для псевдонима (одноуровневая переадресация)	RFC 1035
MX	Mail Exchanger	15	Адрес почтового шлюза для домена. Состоит из двух частей — приоритета (чем число больше, тем ниже приоритет), и адреса узла	RFC 1035
NS	Authoritative name server	2	Адрес узла, отвечающего за доменную зону. Критически важна для функционирования самой системы доменных имён	RFC 1035
PTR	pointer	12	Соответствие адреса имени — обратное соответствие для A и AAAA.	RFC 1035
SIG	Cryptographic public key signature	24	Сигнатура публичной подписи	RFC 2931
SOA	Start of authority	6	Указание на авторитетность информации, используется для указания на новую зону	RFC 1035
DS	Delegation signer	43	Отпечаток (fingerprint) ключа подписи в DNSSEC	RFC 3658
SRV	Server selection	33	Указание на местоположение серверов для сервисов (Jabber, AD)	RFC 2782
X25	PSDN address	19	Адрес в формате X.25	RFC 1183
DNSKEY	DNS Key record	48	Ключ подписи в DNSSEC	RFC 4034

NS записи

Назначение:
Определяют DNS-сервера, которые являются авторитативными для данной зоны.

Формат:
Хост NS Значение
Примеры:
Если домен test.ru делегирован с DNS-серверами ns1.r01.ru и ns2.r01.ru, то на них должны присутствовать следующие NS-записи:

test.ru. NS ns1.r01.ru.
test.ru. NS ns2.r01.ru.

Если домен делегирован с DNS-серверами, принадлежащими той же зоне (допустим, test.ru делегирован с ns1.test.ru. 192.168.0.1 и ns2.test.ru. 192.168.0.2), то NS-записи необходимо дополнить A-записями (так называемые glue-records):

test.ru. NS ns1.test.ru.
test.ru. NS ns2.test.ru.
ns1.test.ru. A 192.168.0.1
ns2.test.ru. A 192.168.0.2

А-ЗАПИСИ

Назначение:
Задают преобразование имени хоста в IP-адрес.

Формат:
Хост А Значение

Пример:
Преобразованию имени test.ru в IP-адрес 192.168.0.1 соответствует следующая А-запись:

test.ru. A 192.168.0.1

MX записи

Назначение:
MX-запись определяет почтовый ретранслятор для доменного имени, т.е. узел, который обработает или передаст дальше почтовые сообщения, предназначенные адресату в указанном домене.

При наличии нескольких MX-записей сначала происходит попытка доставить почту на ретранслятор с наименьшим приоритетом.

Формат:
Хост MX Приоритет Значение

Пример:
Идентифицировать mail.test.ru как почтовый ретранслятор для test.ru с приоритетом 10 можно следующей записью:

test.ru. MX 10 mail.test.ru.

CNAME записи

Назначение:
CNAME-запись определяет отображение псевдонима в каноническое имя узла.

Формат:
Хост CNAME Значение

Пример:
Прописать bbb.test.ru как псевдоним aaa.test.ru можно следующей записью:

bbb.test.ru. CNAME aaa.test.ru.

SRV записи

Назначение:
SRV-запись позволяет получить имя для искомой службы, а также протокол, по которому эта служба работает.
Приоритет SRV-записи работает аналогично приоритету MX-записи: чем меньше приоритет, тем более желательно использование связанной цели.
Веса SRV-записей позволяют администраторам зоны распределять нагрузку между целями. Клиент должен опрашивать цели одного приоритета в пропорции к их весам.
Порт SRV-записи определяет порт, по которому работает искомая служба.

Формат:
Хост SRV Приоритет Вес Порт Значение

Пример:
Предположим, мы хотим по запросу FTP-клиента для доступа по FTP к test.ru направлять клиент сначала на ftp1.test.ru. через 21 порт, а затем на ftp2.test.ru. через 21 порт, если ftp1.test.ru. недоступен. Это можно сделать следующими записями:

_ftp._tcp.test.ru. SRV 1 0 21 ftp1.test.ru.
_ftp._tcp.test.ru. SRV 2 0 21 ftp2.test.ru.

TXT записи

Назначение:
TXT-запись содержит общую текстовую информацию. Эти записи могут использоваться в любых целях, например, для указания месторасположения хоста.

Формат:
Хост TXT Текст

Пример:
Прописать в DNS информацию о месторасположении сервера mail.test.ru:

mail.test.ru. TXT "Location this machine: Moscow"

AAAA записи

AAAA-ЗАПИСИ

Назначение:
Задает преобразование имени хоста в IPV6-адрес.

Формат:
Хост AAAA Значение

Пример:
Преобразованию имени test.ru в адрес 222:10:2521:1:210:4bff:fe10:d24 соответствует следующая AAAA-запись:

test.ru. AAAA 222:10:2521:1:210:4bff:fe10:d24

DNSSEC rfc4034

DNS была первоначально создана в предположении, что DNS будет присылать один и тот же отклик вне зависимости от того, откуда пришел запрос, и что все DNS-данные общедоступны... Но…

Согласно DNSSEC, система сконструирована не для обеспечения конфиденциальности, списков для управления доступом, или других мер дифференциации запросов.

DNSSEC не предоставляет защиты от DoS-атак. Безопасные распознаватели и безопасные серверы имен уязвимы в отношении новых типов DoS-атак, основанных на криптографических операциях.

Расширения безопасности DNS предоставляют аутентификацию происхождения DNS-данных. Механизмы, описанные выше, не позволяют защитить операции зонного обмена и динамического обновления ([RFC2136], [RFC3007]). Схемы аутентификации сообщений, описанные в [RFC2845] и [RFC2931], адресованы к безопасности подобных операций.

Состояния информации DNSSEC

Данная спецификация определяет поведение подписантов зон, безопасных серверов имен и безопасных распознавателей и служит для валидации данных с целью определения их состояния. Безопасный распознаватель может идентифицировать 4 состояния информации:

Безопасная: Валидирующий распознаватель имеет доверительную ссылку, имеет доверительную цепочку, и способен верифицировать все подписи в отклике.

Небезопасная: Валидирующий распознаватель имеет доверительную ссылку, имеет доверительную цепочку, и, в некоторых точках делегирования, подписанное доказательство несуществования записи DS. Это индицирует, что последующие ветви дерева вероятно небезопасны. Валидирующий распознаватель может иметь локальную политику пометки частей доменного пространства, как небезопасных.

Фальсифицированная: Валидирующий распознаватель имеет доверительную ссылку, безопасное делегирование, которое индицирует, что дочерние данные подписаны, но отклик по некоторым причинам не проходит валидацию: отсутствуют подписи, истек срок действия подписи, подписи выполнены с помощью неизвестного алгоритма, отсутствуют данные, которые согласно NSEC RR должны присутствовать, и т.д..

Промежуточная: Отсутствует доверительная ссылка, которая бы указывала, что определенная часть дерева является безопасной.

Пример файла зоны:

```
$TTL 1h @ 86400 IN SOA ns.example.com. hostmaster.example.com.
( 2009092102 ;
Serial 10600 ;
Refresh 800 ;
Retry 3400000 ;
Expire 86400 ) ;
TTL
)
;;; NS ;;;
            NS ns1.my-ns-server.com.
            NS ns.my-secondary-ns.com.
;;; MX ;;;
            MX 10 mx.example.com.
;;; A ;;;
            A       192.168.0.1
www         CNAME   @
mx          A       192.168.0.1
```

Все директивы и ресурсные записи вводятся в отдельной строке, комментарии размещаются после точки с запятой (;).

SOA (start of authority record)

Основополагающая запись DNS — **SOA** (start of authority record) или начальная запись зоны: запись, указывающая местоположение эталонной записи о данном домене, содержит контактную информацию лица, ответственного за данную зону, тайминги кеширования зонной информации и данные о взаимодействиях DNS-серверов.

Serial – Серийный номер самого файла зоны. Серийный номер увеличивается каждый раз при изменении данных домена. Когда вторичный сервер проверяет необходимость обновления данных, он проверяет серийный номер записи SOA на первичном сервере.

Refresh — значение времени в секундах. Показывает время, через которое вторичный сервер будет пытаться обновить данные зоны с первичного сервера (читая SOA первичного сервера). Рекомендуется устанавливать значения от 1200 до 43200 секунд. Низкое значение (1200) устанавливается при частой необходимости обновления данных. Высокое 43200 (12 часов), если такой необходимости нет.

Retry — значение времени в секундах. Определяет время между попытками, если вторичный сервер не может связаться с первичным сервером, когда время обновления истекло. Рекомендуемые значения от 180 (3 минуты) до 900 (15 минут) и выше.

Expire — значение времени в секундах. Значение срока. Если попытки обновления данных не привели к успеху, то по истечении срока вторичный сервер перестаёт отвечать на запросы для данного домена и стирает свою копию файла зоны. Если контакт установлен, значения срока и обновления сбрасываются, и цикл начинается снова. Рекомендуется устанавливать значения от 1209600 до 2419200 секунд (2-4 недели).

Директивы файла зоны

Директивы начинаются со знака доллара ($), после которого вводится имя директивы. Зачастую директивы пишут в начале файла зоны.
Ниже приведены часто используемые директивы:

$ INCLUDE — Позволяет включить другой файл зоны в этот файл зоны в месте, где появляется директива. Это позволяет хранить дополнительные настройки файла зоны отдельно от основного файла зоны.

$ ORIGIN — Добавляет имя домена к относительному доменному имени. По умолчанию $ORIGIN принимает значение доменного имени, указанного в операторе zone.

$ TTL – Устанавливает значение времени жизни по умолчанию (TTL) для зоны. Это время, на протяжении которого запись ресурса этой зоны действительна в кэше других серверов. Каждая запись ресурса может содержать свое собственное значение TTL , который перекрывает эту директиву.

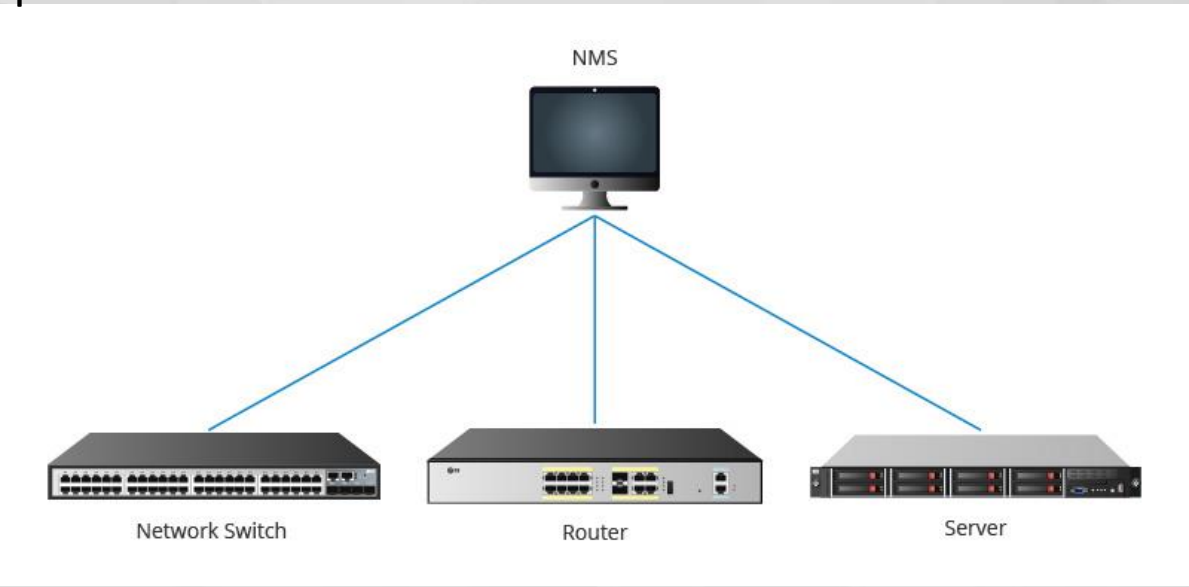
DNS-over-TLS и DNS-over-HTTPS

Как известно, протокол DNS не шифрует запросы и данные передаются в открытом виде. DNS-трафик уязвим перед злоумышленниками, т.к. появляется возможность "подслушать" канал связи и перехватить незащищенные персональные данные. Интернет-провайдеры могут осуществлять наблюдение за трафиком и собирать данные о том, какие сайты вы посещаете.

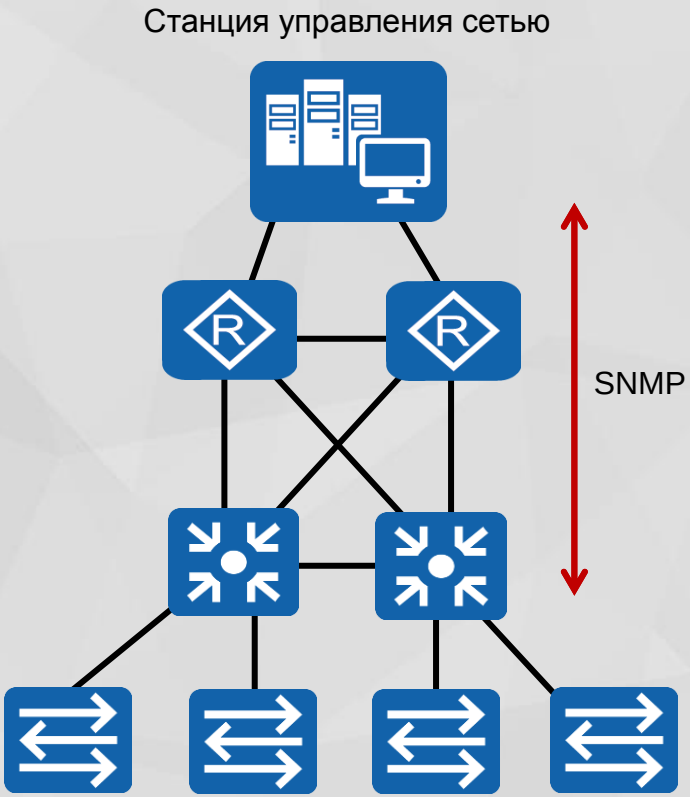
Для безопасности DNS-трафика были реализованы специальные протоколы DNS over TLS (DNS поверх TLS, DoT, RFC7858) и DNS over HTTPS (DNS поверх HTTPS, DoH, RFC8484). Их основная задача - зашифровать DNS-трафик для предотвращения перехвата и обеспечения дополнительной конфиденциальности и безопасности. В данной статье мы не будем подробно останавливаться на теории. Информацию о том как работают DoT и DoH вы найдете на следующих страницах:
https://adguard.com/ru/blog/adguard-dns-announcement.html
https://ru.wikipedia.org/wiki/DNS поверх TLS
https://ru.wikipedia.org/wiki/DNS поверх HTTPS
Список публичных DNS-сервисов с поддержкой DoT/DoH:
https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Public+Resolvers
https://github.com/curl/curl/wiki/DNS-over-HTTPS
https://kb.adguard.com/ru/general/dns-providers

Простой протокол управления сетью (SNMP)

SNMP (Simple Network Management Protocol (*RFC-1157, -1215, -1187, -1089 разработан в 1988 году*)) представляет собой стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP, который позволяет отслеживать управляемые сетевые устройства, включая маршрутизаторы, сетевые коммутаторы, серверы, принтеры и другие устройства, которые включены по IP через единую систему управления/программное обеспечение.

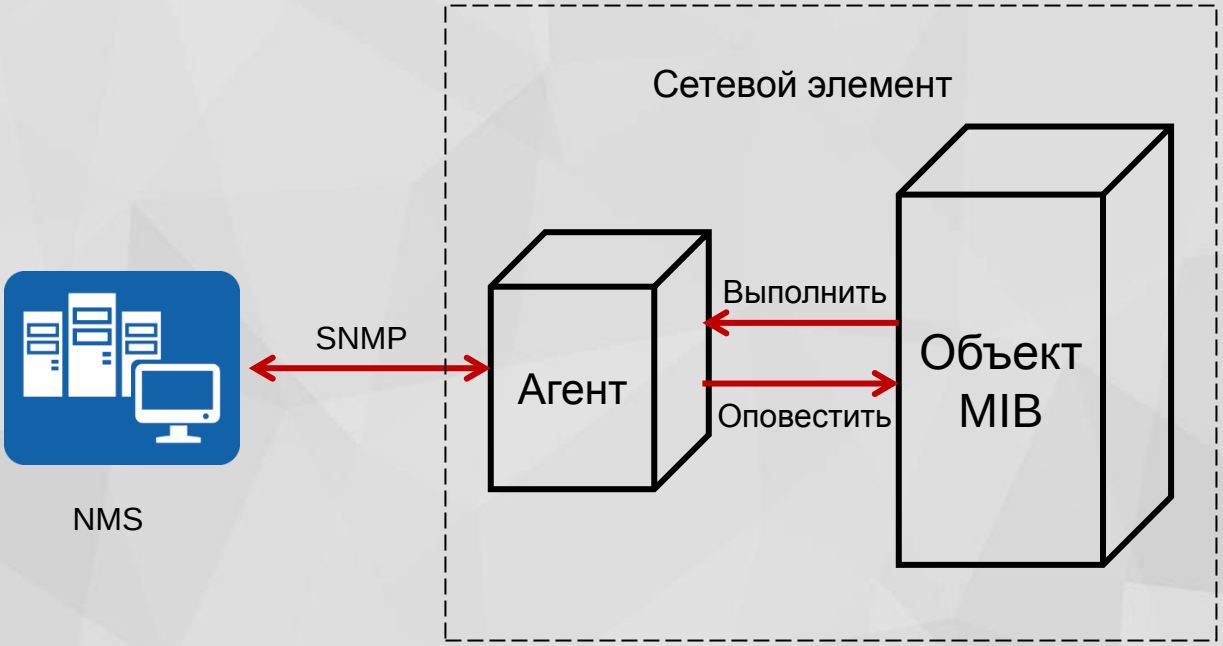


Применение SNMP



SNMP используется для передачи управляющей информации между станциями управления сетью и сетевыми элементами.

Архитектура SNMP



Взаимодействие с NMS (Network Management System) с целью извлечения или изменения переменных параметров в MIB осуществляется через агентов сетевых элементов.

Management Information Base (MIB

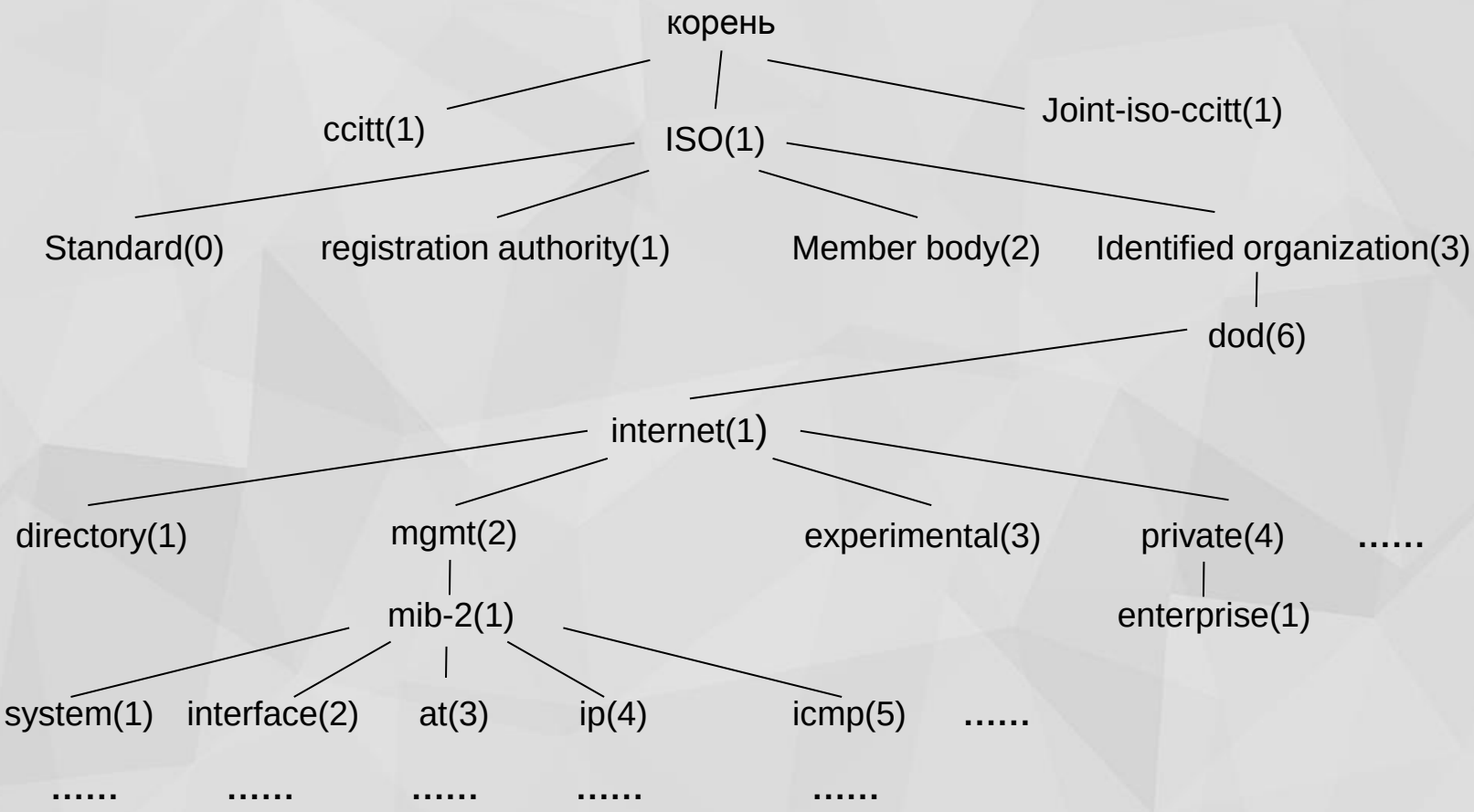
Management Information Base (MIB

Management Information Base (**MIB**, база управляющей информации) - *виртуальная база данных, используемая для управления объектами в сети связи*.

Хотя термин MIB предназначен для обозначения всей доступной информации об объекте, он также часто используется для обозначения конкретного подмножества, которое правильнее называть MIB-модулем. Объекты в MIB, согласно RFC 2578, определяются с помощью подмножества "Structure of Management Information Version 2" (SMIv2) стандарта ASN.1. Программное обеспечение, выполняющее разбор, называется MIB-компилятором.

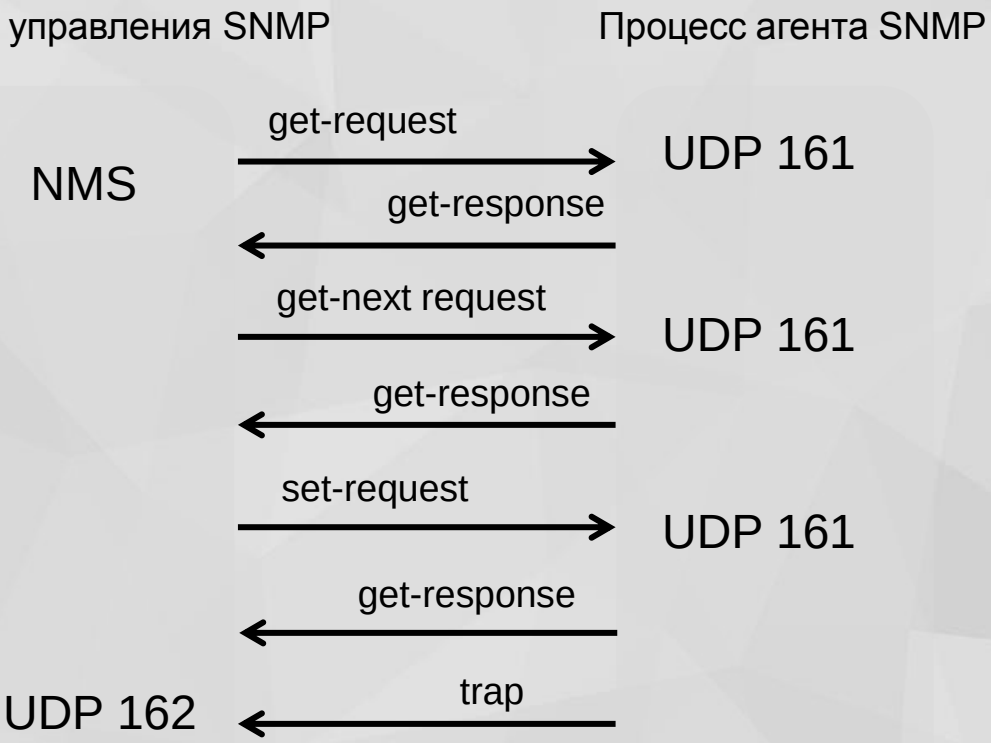
База данных имеет иерархическую (древовидную) структуру. К записям можно обратиться через идентификаторы объектов (англ. object identifier, OID). Базы MIB обсуждаются в документациях RFC, в частности в RFC 1155 и сопутствующих ему RFC 1213 и RFC 1157.

Объекты MIB



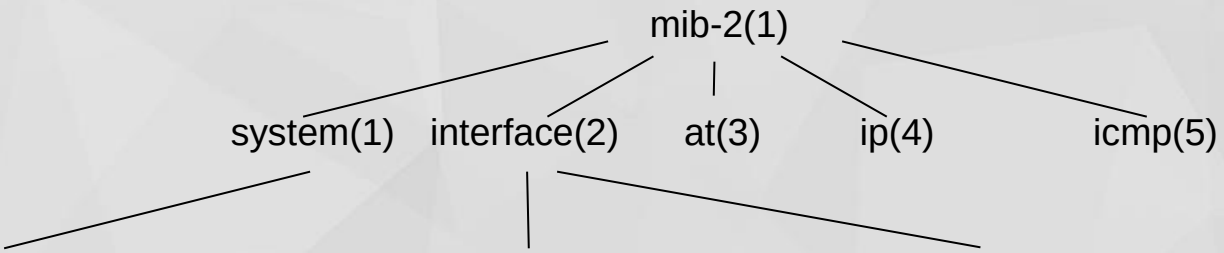
MIB выступает в качестве виртуального хранилища данных управления объектами.

Простой протокол управления сетью (SNMP)



Запросы принимаются агентом SNMP на UDP-порту 161.

SNMPv2c



sysUpTime OBJECT-TYPE
SYNTAX TimeTicks
ACCESS read-only
STATUS mandatory
ОПИСАНИЕ «Время (в сотых долях секунды) с момента последней повторной инициализации элемента управления сетью системы»
::= { system 3 }

ifSpeed OBJECT-TYPE
SYNTAX Gauge
ACCESS read-only
STATUS mandatory
ОПИСАНИЕ «Оценка текущей полосы пропускания интерфейса в битах в секунду»
::= { ifEntry 5 }

ifOutOctets OBJECT-TYPE
SYNTAX Counter
ACCESS read-only
STATUS mandatory
ОПИСАНИЕ «Общее количество октетов, передаваемых интерфейсом, включая символы кадровой синхронизации»
::= { ifEntry 16 }

- Включены новый блок PDU — запрос Get-bulk и информационный запрос.
- В новых 64-разрядных счетчиках устранена проблема сброса.

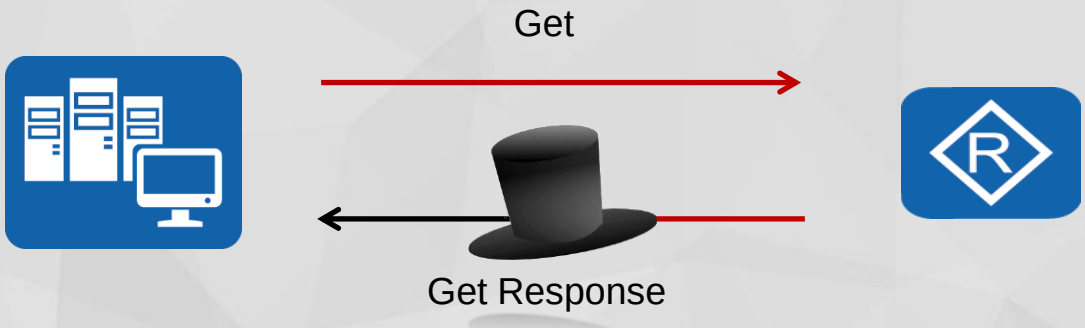
Структура SNMP

Здесь используется SNMPv2c для объяснения принципов работы SNMP. Он выполняет следующие операции для извлечения данных, изменения переменных объекта SNMP и отправки уведомлений.

Get	GetNext	GetBulk	Set	Response	Trap	Inform
Это запрос, отправленный NMS на управляемое устройство. И это выполняется для получения одного или нескольких значений из MIB.	Это похоже на GET. Но обычно он получает значение следующего OID (Идентификатор объекта) в дереве MIB.	Он используется для получения массы данных из большой таблицы MIB.	Он выполняется NMS для изменения значения управляемого устройства.	Он выполняется NMS для изменения значения управляемого устройства. Он выполняется агентом в ответ на операции GetRequest, GetNextRequest, GetBulkRequest и SetRequest.	Эта операция инициируется агентом. Он используется для уведомления NMS о ошибке или событии, которое происходит на управляемом устройстве.	Эта операция инициируется агентом. Это похоже на TRAP, но после того, как агент отправит запрос на информирование, NMS должна отправить пакет InformResponse в качестве ответа агенту.

Обратите внимание, что SNMPv1 не поддерживает операции GetBulk и Inform.

SNMPv3



Механизмы безопасности SNMPv3 поддерживают:

- целостность данных,
- аутентификацию источника данных,
- конфиденциальность и своевременную доставку.

SNMP - версии

SNMP версии 1 (SNMPv1) является первоначальной версией протокола и определён RFC 1157. Безопасность SNMPv1 основывается на т.н. общности (Community). Есть три вида общности: слежение (разрешены лишь операции чтения), управление (разрешены операции чтения и записи) и прерывание (Trap) (лишь право на передачу прерываний). Пароль передаётся в незашифрованном виде. Этот стандарт используется очень многими производителями оборудования.

SNMP версии 2 (SNMPv2) называют базирующимся на строках общности (community string based) SNMPv2. Технически, SNMPv2 является уже версией SNMPv2c. Протокол определён RFC 3416, RFC 3417 ja RFC 3418.

SNMP версии 3 (SNMPv3) является самой новой версией SNMP. Основное отличие от предыдущих версии заключаются в обеспечении безопасности. В протокол добавлена возможность сильной аутентификации и шифрования соединения между управляющими единицами. Стандарт определён следующими документами: от RFC 3410 до RFC 3418 и RFC 2576.

Примеры NMS

IBM

Tivoli. software

Microsoft

Endpoint

Configuration Manager

CW

stands for

CiscoWorks

Abbreviations.com

Пример стоимости управляющих систем

PAESSLER PRTG NETWORK MONITOR

PRTG 500	PRTG 1000	PRTG 2500	PRTG 5000	PRTG XL1
Начните с малого и расширьте потом	Малые и средние среды	Среднемасштабные среды	Крупномасштабные среды	Сверхкрупные среды
$1,750 ЗА СЕРВЕРНУЮ ЛИЦЕНЗИЮ	$3,200 ЗА СЕРВЕРНУЮ ЛИЦЕНЗИЮ	$6,500 ЗА СЕРВЕРНУЮ ЛИЦЕНЗИЮ	$11,500 ЗА СЕРВЕРНУЮ ЛИЦЕНЗИЮ	$15,500 ЗА СЕРВЕРНУЮ ЛИЦЕНЗИЮ
НАЧАТЬ	НАЧАТЬ	НАЧАТЬ	НАЧАТЬ	НАЧАТЬ
Мониторинг до 500 аспектов сетевых устройств – обычно этого достаточно, чтобы контролировать параметры около 50 устройств	Мониторинг до 1.000 аспектов сетевых устройств – обычно этого достаточно, чтобы контролировать параметры около 100 устройств	Мониторинг до 2.500 аспектов сетевых устройств – обычно этого достаточно, чтобы контролировать параметры около 250 устройств	**Мониторинг до 5.000 аспектов сетевых устройств – обычно этого достаточно, чтобы контролировать параметры около 500 устройств**	Мониторинг около 10.000 аспектов сетевых устройств – обычно этого достаточно, чтобы контролировать параметры около 1.000 устройств*

Примеры NMS - OpenSource

ICINGA

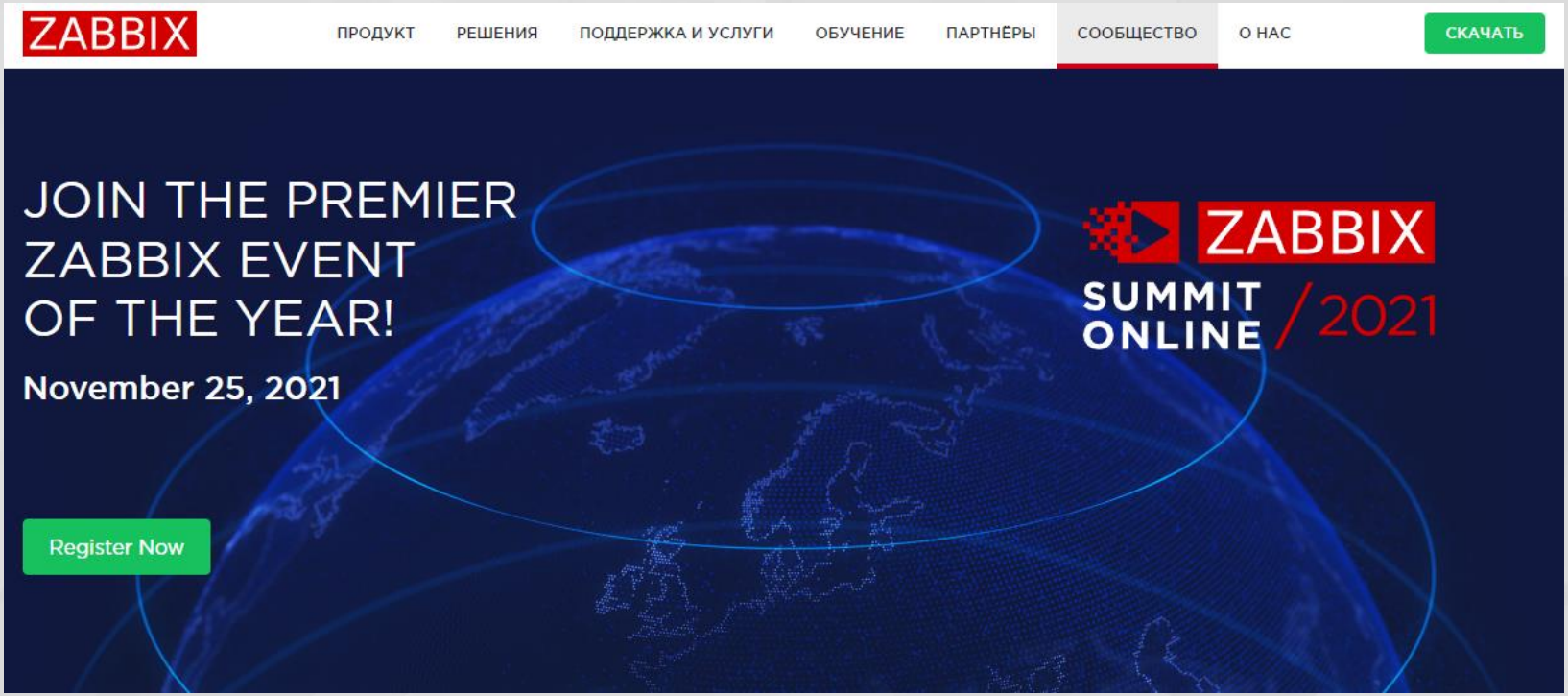
ZABBIX

openNMS®

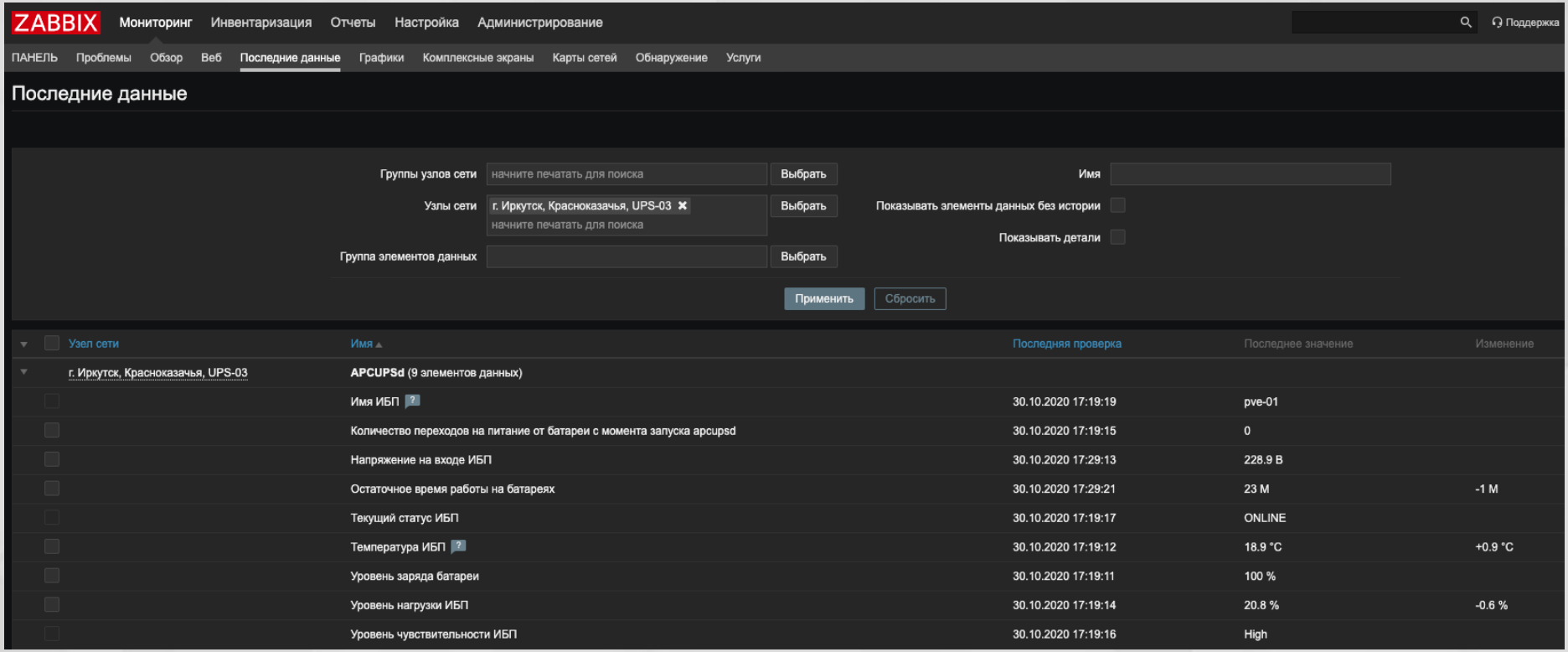
Nagios® Core™

CACTUS IT

ZABBIX



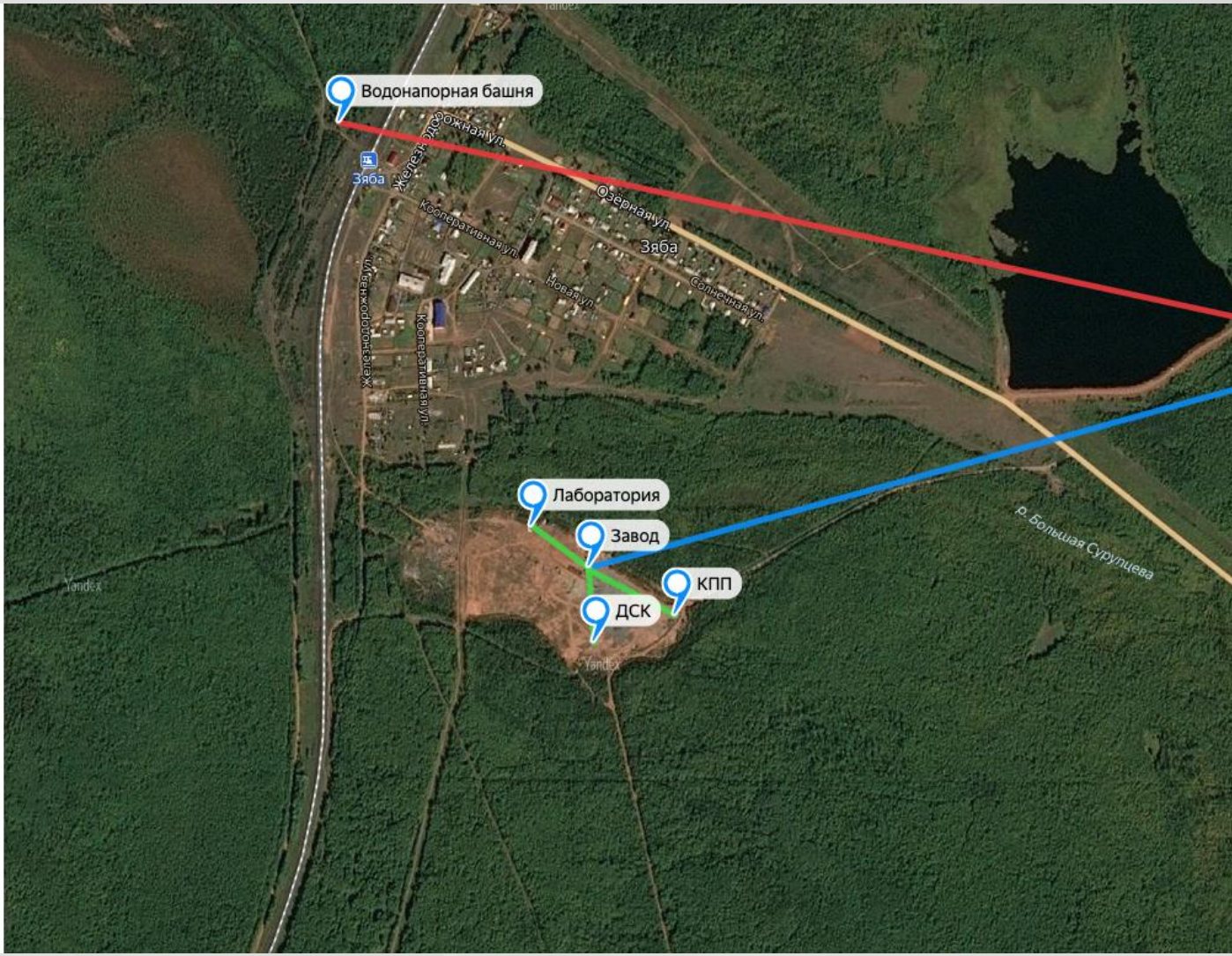
В этом году Zabbix Summit Online 2021 будет посвящен Zabbix 6.0. LTS , его новые функции, улучшенное удобство использования, технический и образовательный контент, отраслевые новости и информация о передовых методах работы от клиентов и партнеров со всего мира!


ZABBIX
Мониторинг
Инвентаризация
Отчеты
Настройка
Администрирование
Поддержка
ПАНЕЛЬ
Проблемы
Обзор
Веб
Последние данные
Графики
Комплексные экраны
Карты сетей
Обнаружение
Услуги
Последние данные
Группы узлов сети
начните печатать для поиска
Выбрать
Имя
Узлы сети
г. Иркутск, Красноказачья, UPS-03
начните печатать для поиска
Выбрать
Показывать элементы данных без истории
Показывать детали
Группа элементов данных
Выбрать
Применить
Сбросить
Узел сети
Имя
Последняя проверка
Последнее значение
Изменение
г. Иркутск, Красноказачья, UPS-03
APCUPSd (9 элементов данных)
Имя ИБП
30.10.2020 17:19:19
pve-01
Количество переходов на питание от батареи с момента запуска apcupsd
30.10.2020 17:19:15
0
Напряжение на входе ИБП
30.10.2020 17:29:13
228.9 В
Остаточное время работы на батареях
30.10.2020 17:29:21
23 М
-1 М
Текущий статус ИБП
30.10.2020 17:19:17
ONLINE
Температура ИБП
30.10.2020 17:19:12
18.9 °C
+0.9 °C
Уровень заряда батареи
30.10.2020 17:19:11
100 %
Уровень нагрузки ИБП
30.10.2020 17:19:14
20.8 %
-0.6 %
Уровень чувствительности ИБП
30.10.2020 17:19:16
High

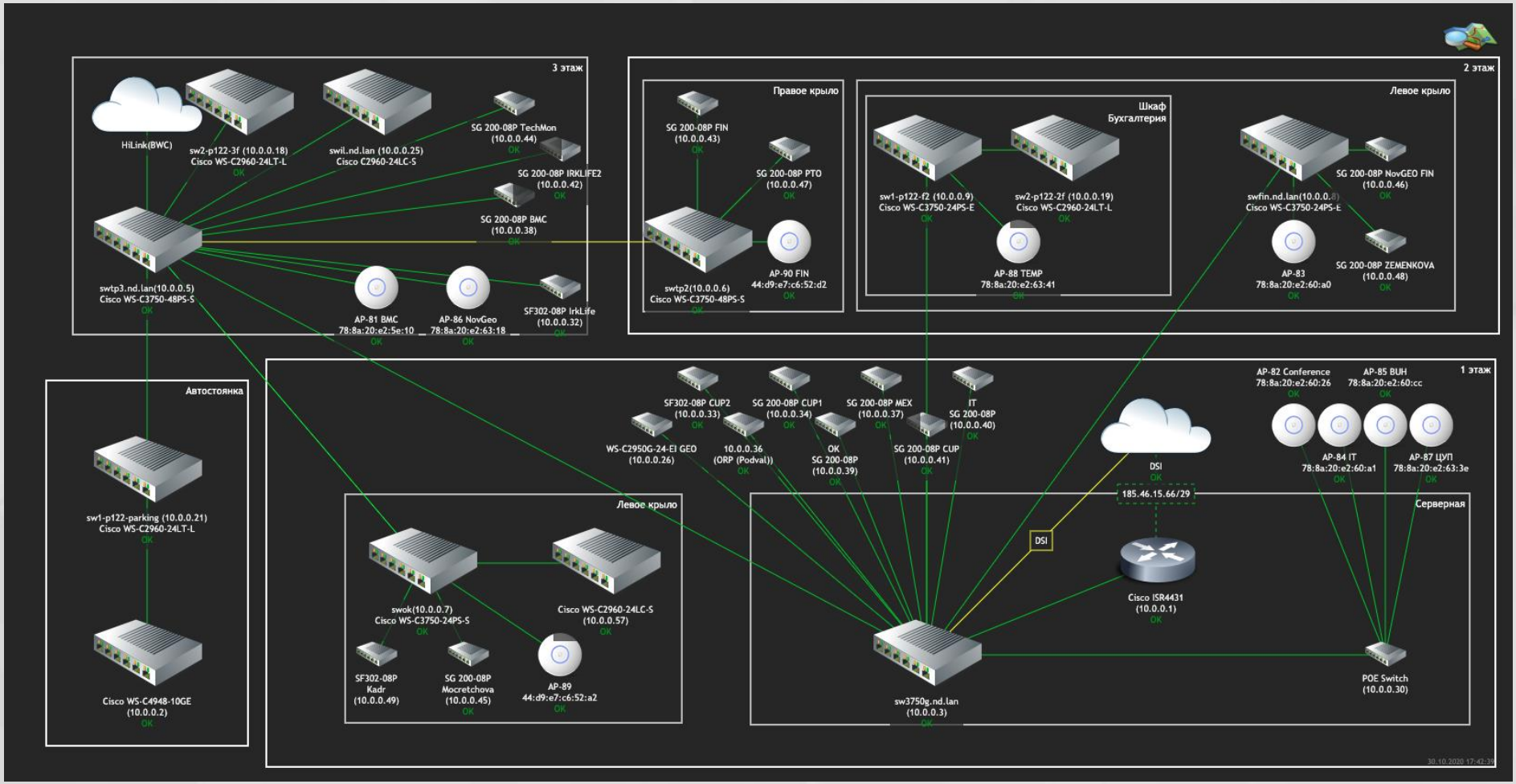
Создать новую карту

Последнее обновление: 28 мая 2019

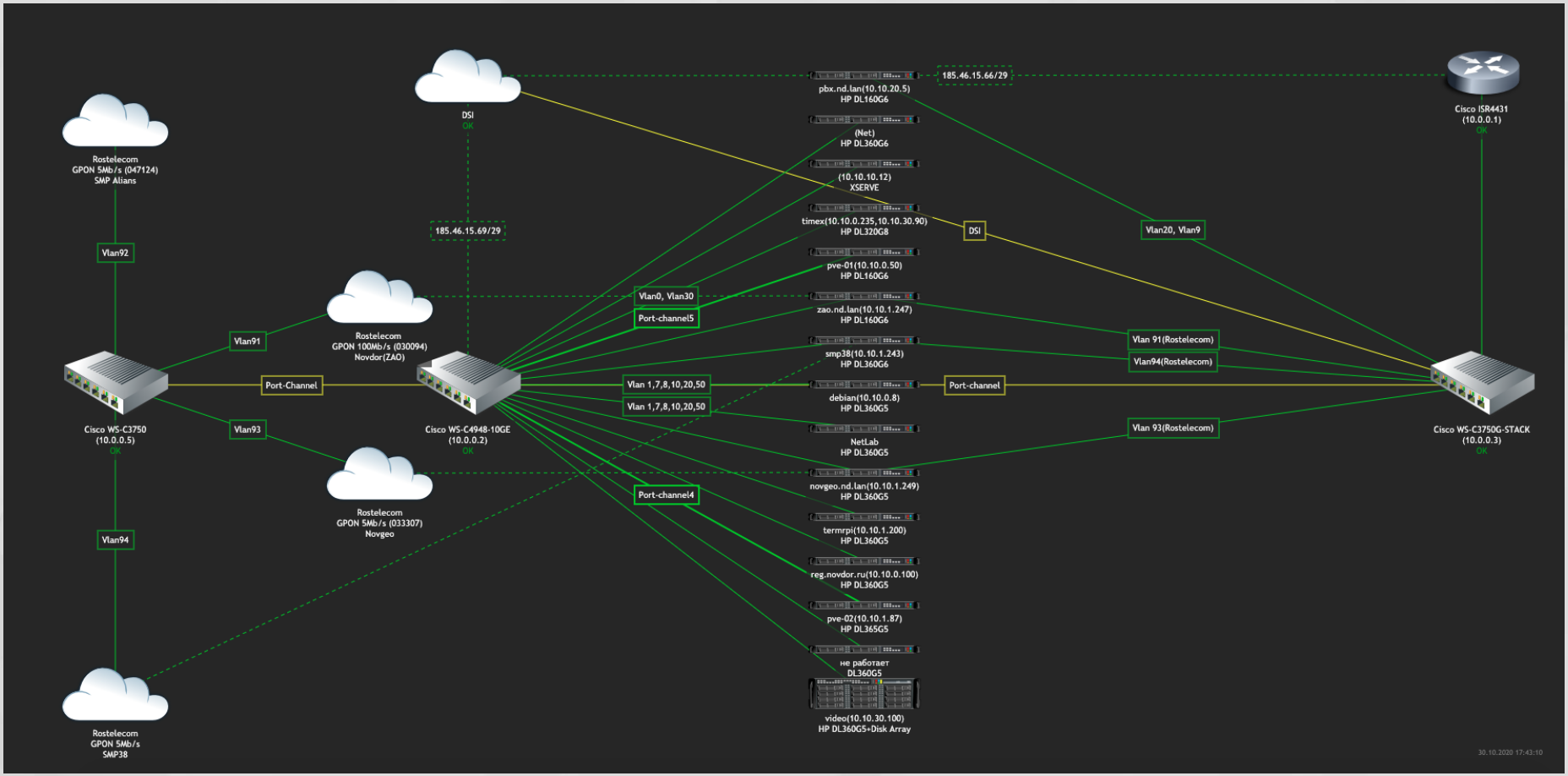
- Лаборатория
- Водонапорная башня
- ДСК
- Завод
- КПП
- РММ
- ЦУП
- Завод - ДСК — 160 м
- Завод - Лаборатория — 160 м
- База - РММ — 160 м
- Завод - КПП — 210 м
- Завод - База — 2 км
- Водонапорная башня (Теле2) - База — 2 км



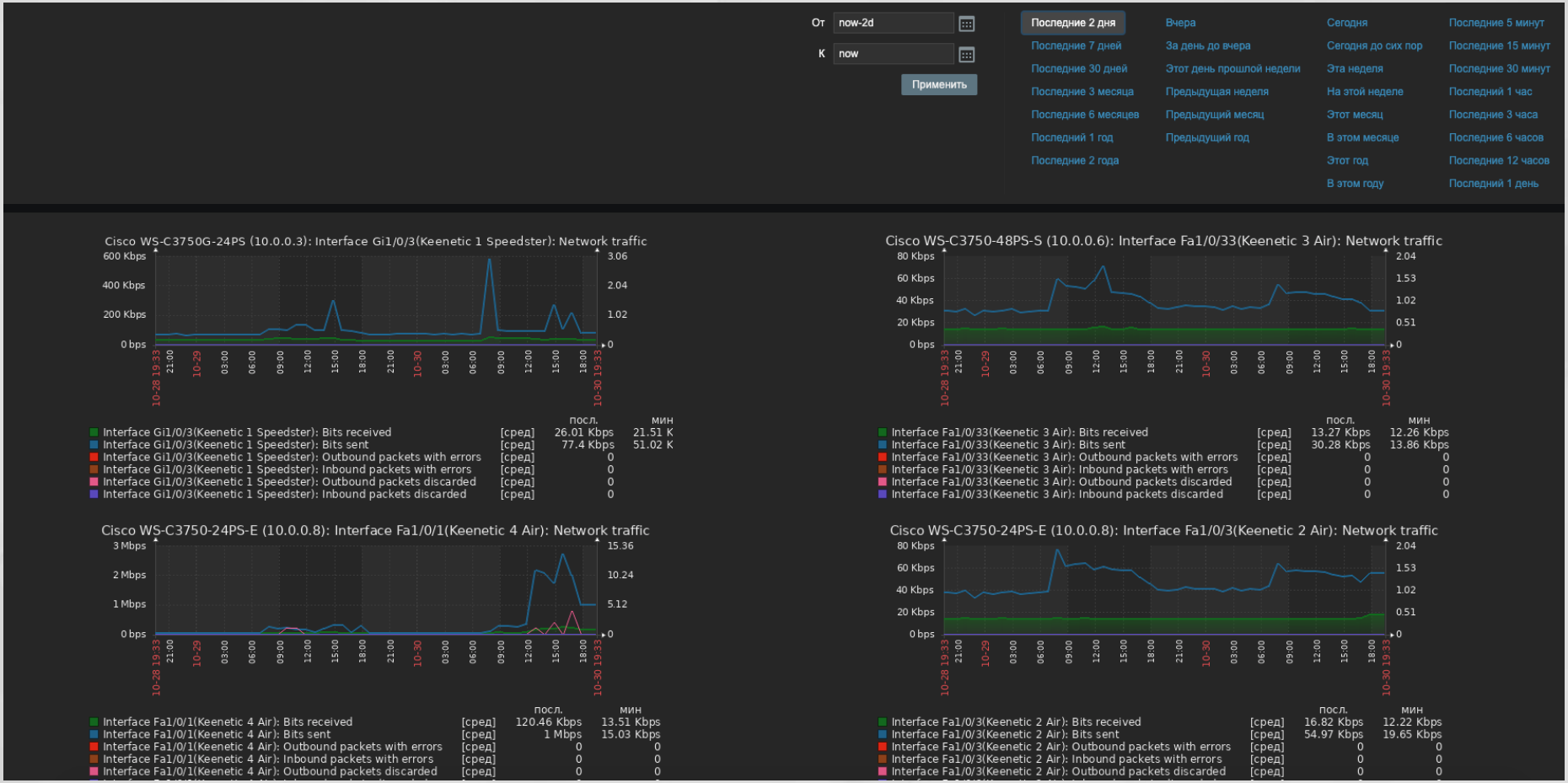
ZABBIX


3 этаж
HiLink(BWC)
sw2-p122-3f (10.0.0.18)
Cisco WS-C2960-24LT-L
swil.nd.lan (10.0.0.25)
Cisco C2960-24LC-S
SG 200-08P TechMon
(10.0.0.44)
SG 200-08P IRKLIFE2
(10.0.0.42)
SG 200-08P BMC
(10.0.0.38)
swtp3.nd.lan(10.0.0.5)
Cisco WS-C3750-48PS-S
AP-81 BMC
78:8a:20:e2:5e:10
AP-86 NovGeo
78:8a:20:e2:63:18
SF302-08P IrkLife
(10.0.0.32)
2 этаж
Правое крыло
SG 200-08P FIN
(10.0.0.43)
SG 200-08P PTO
(10.0.0.47)
swtp2(10.0.0.6)
Cisco WS-C3750-48PS-S
AP-90 FIN
44:d9:e7:c6:52:d2
Шкаф
Бухгалтерия
sw1-p122-f2 (10.0.0.9)
Cisco WS-C3750-24PS-E
sw2-p122-2f (10.0.0.19)
Cisco WS-C2960-24LT-L
AP-88 TEMP
78:8a:20:e2:63:41
Левое крыло
swfin.nd.lan(10.0.0.8)
Cisco WS-C3750-24PS-E
SG 200-08P NovGEO FIN
(10.0.0.46)
AP-83
78:8a:20:e2:60:a0
SG 200-08P ZEMENKOVA
(10.0.0.48)
Автостоянка
sw1-p122-parking (10.0.0.21)
Cisco WS-C2960-24LT-L
Cisco WS-C4948-10GE
(10.0.0.2)
1 этаж
SF302-08P CUP2
(10.0.0.33)
SG 200-08P CUP1
(10.0.0.34)
SG 200-08P MEX
(10.0.0.37)
IT
SG 200-08P
(10.0.0.40)
WS-C2950G-24-EI GEO
(10.0.0.26)
10.0.0.36
(ORP (Podval))
OK
SG 200-08P
(10.0.0.39)
SG 200-08P CUP
(10.0.0.41)
AP-82 Conference
78:8a:20:e2:60:26
AP-85 BUH
78:8a:20:e2:60:cc
AP-84 IT
78:8a:20:e2:60:a1
AP-87 ЦУП
78:8a:20:e2:63:3e
DSI
185.46.15.66/29
DSI
Cisco ISR4431
(10.0.0.1)
Серверная
Левое крыло
swok(10.0.0.7)
Cisco WS-C3750-24PS-S
Cisco WS-C2960-24LC-S
(10.0.0.57)
SF302-08P
Kadr
(10.0.0.49)
SG 200-08P
Mocretchova
(10.0.0.45)
AP-89
44:d9:e7:c6:52:a2
sw3750g.nd.lan
(10.0.0.3)
POE Switch
(10.0.0.30)

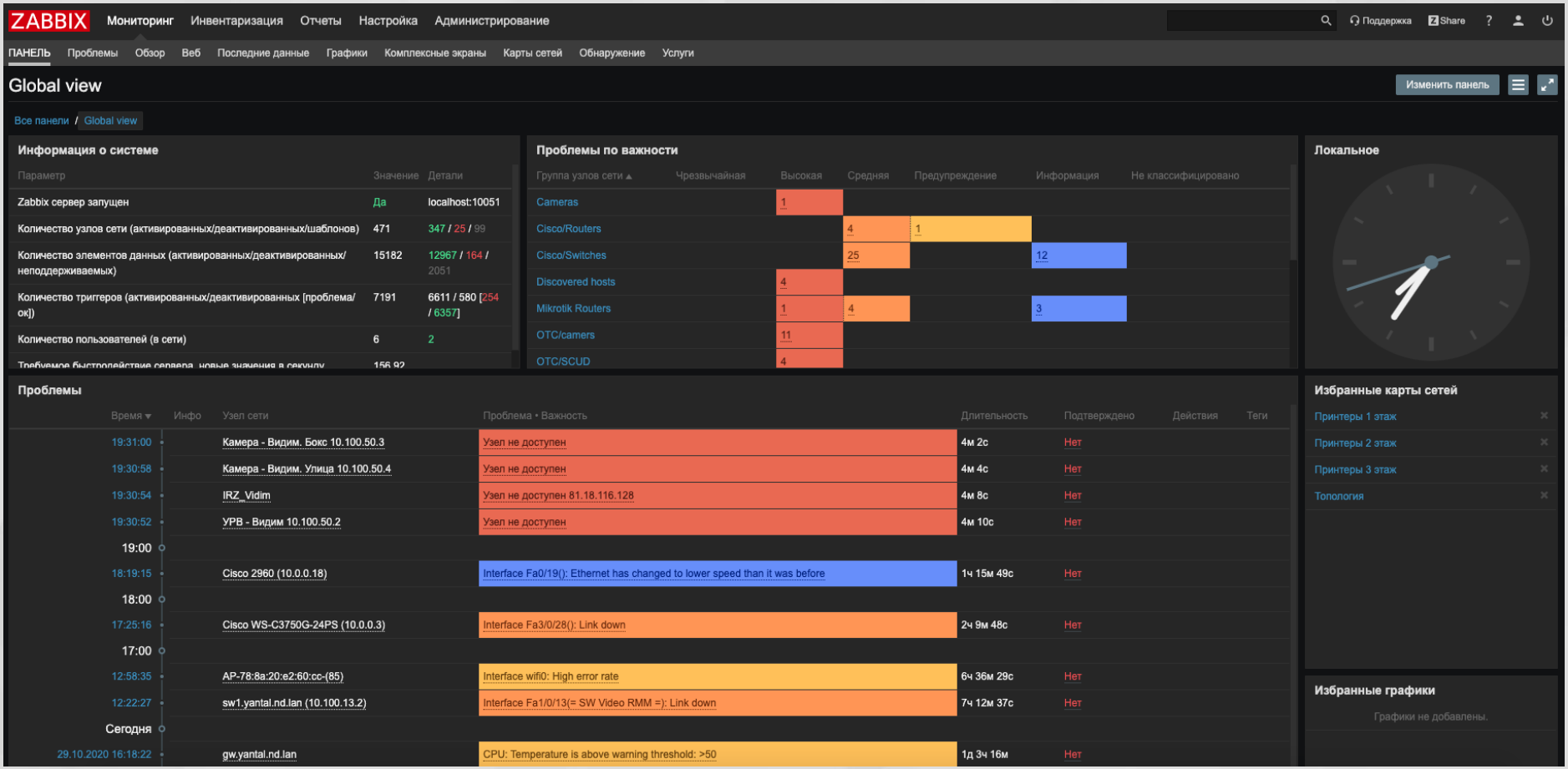
ZABBIX


DSI
OK
185.46.15.66/29
pbx.nd.lan(10.10.20.5)
HP DL160G6
Cisco ISR4431
(10.0.0.1)
OK
Rostelecom
GPON 5Mb/s (047124)
SMP Alians
(Net)
HP DL360G6
(10.10.10.12)
XSERVE
185.46.15.69/29
timex(10.10.0.235,10.10.30.90)
HP DL320G8
DSI
Vlan20, Vlan9
Vlan92
pve-01(10.10.0.50)
HP DL160G6
Vlan0, Vlan30
Port-channel5
zao.nd.lan(10.10.1.247)
HP DL160G6
Rostelecom
GPON 100Mb/s (030094)
Novdor(ZAO)
Vlan91
smp38(10.10.1.243)
HP DL360G6
Vlan 91(Rostelecom)
Vlan94(Rostelecom)
Port-Channel
Vlan 1,7,8,10,20,50
Vlan 1,7,8,10,20,50
debian(10.10.0.8)
HP DL360G5
Port-channel
Cisco WS-C3750
(10.0.0.5)
OK
Vlan93
Cisco WS-C4948-10GE
(10.0.0.2)
OK
NetLab
HP DL360G5
Vlan 93(Rostelecom)
Cisco WS-C3750G-STACK
(10.0.0.3)
OK
novgeo.nd.lan(10.10.1.249)
HP DL360G5
Port-channel4
Rostelecom
GPON 5Mb/s (033307)
Novgeo
termrpi(10.10.1.200)
HP DL360G5
Vlan94
reg.novdor.ru(10.10.0.100)
HP DL360G5
pve-02(10.10.1.87)
HP DL365G5
не работает
DL360G5
Rostelecom
GPON 5Mb/s
SMP38
video(10.10.30.100)
HP DL360G5+Disk Array
30.10.2020 17:43:10

ZABBIX


От
now-2d
К
now
Применить
Последние 2 дня
Последние 7 дней
Последние 30 дней
Последние 3 месяца
Последние 6 месяцев
Последний 1 год
Последние 2 года
Вчера
За день до вчера
Этот день прошлой недели
Предыдущая неделя
Предыдущий месяц
Предыдущий год
Сегодня
Сегодня до сих пор
Эта неделя
На этой неделе
Этот месяц
В этом месяце
Этот год
В этом году
Последние 5 минут
Последние 15 минут
Последние 30 минут
Последний 1 час
Последние 3 часа
Последние 6 часов
Последние 12 часов
Последний 1 день
Cisco WS-C3750G-24PS (10.0.0.3): Interface Gi1/0/3(Keenetic 1 Speedster): Network traffic
600 Kbps
400 Kbps
200 Kbps
0 bps
3.06
2.04
1.02
0
10-28 19:33
10-29
10-30
10-30 19:33
посл.
мин
Interface Gi1/0/3(Keenetic 1 Speedster): Bits received [сред] 26.01 Kbps 21.51 K
Interface Gi1/0/3(Keenetic 1 Speedster): Bits sent [сред] 77.4 Kbps 51.02 K
Interface Gi1/0/3(Keenetic 1 Speedster): Outbound packets with errors [сред] 0
Interface Gi1/0/3(Keenetic 1 Speedster): Inbound packets with errors [сред] 0
Interface Gi1/0/3(Keenetic 1 Speedster): Outbound packets discarded [сред] 0
Interface Gi1/0/3(Keenetic 1 Speedster): Inbound packets discarded [сред] 0
Cisco WS-C3750-48PS-S (10.0.0.6): Interface Fa1/0/33(Keenetic 3 Air): Network traffic
80 Kbps
60 Kbps
40 Kbps
20 Kbps
0 bps
2.04
1.53
1.02
0.51
0
Interface Fa1/0/33(Keenetic 3 Air): Bits received [сред] 13.27 Kbps 12.26 Kbps
Interface Fa1/0/33(Keenetic 3 Air): Bits sent [сред] 30.28 Kbps 13.86 Kbps
Interface Fa1/0/33(Keenetic 3 Air): Outbound packets with errors [сред] 0 0
Interface Fa1/0/33(Keenetic 3 Air): Inbound packets with errors [сред] 0 0
Interface Fa1/0/33(Keenetic 3 Air): Outbound packets discarded [сред] 0 0
Interface Fa1/0/33(Keenetic 3 Air): Inbound packets discarded [сред] 0 0
Cisco WS-C3750-24PS-E (10.0.0.8): Interface Fa1/0/1(Keenetic 4 Air): Network traffic
3 Mbps
2 Mbps
1 Mbps
0 bps
15.36
10.24
5.12
0
Interface Fa1/0/1(Keenetic 4 Air): Bits received [сред] 120.46 Kbps 13.51 Kbps
Interface Fa1/0/1(Keenetic 4 Air): Bits sent [сред] 1 Mbps 15.03 Kbps
Interface Fa1/0/1(Keenetic 4 Air): Outbound packets with errors [сред] 0 0
Interface Fa1/0/1(Keenetic 4 Air): Inbound packets with errors [сред] 0 0
Interface Fa1/0/1(Keenetic 4 Air): Outbound packets discarded [сред] 0 0
Cisco WS-C3750-24PS-E (10.0.0.8): Interface Fa1/0/3(Keenetic 2 Air): Network traffic
80 Kbps
60 Kbps
40 Kbps
20 Kbps
0 bps
2.04
1.53
1.02
0.51
0
Interface Fa1/0/3(Keenetic 2 Air): Bits received [сред] 16.82 Kbps 12.22 Kbps
Interface Fa1/0/3(Keenetic 2 Air): Bits sent [сред] 54.97 Kbps 19.65 Kbps
Interface Fa1/0/3(Keenetic 2 Air): Outbound packets with errors [сред] 0 0
Interface Fa1/0/3(Keenetic 2 Air): Inbound packets with errors [сред] 0 0
Interface Fa1/0/3(Keenetic 2 Air): Outbound packets discarded [сред] 0 0

ZABBIX


ZABBIX
Мониторинг
Инвентаризация
Отчеты
Настройка
Администрирование
Поддержка
Share
ПАНЕЛЬ
Проблемы
Обзор
Веб
Последние данные
Графики
Комплексные экраны
Карты сетей
Обнаружение
Услуги
Global view
Изменить панель
Все панели / Global view
Информация о системе
Параметр
Значение
Детали
Zabbix сервер запущен
Да
localhost:10051
Количество узлов сети (активированных/деактивированных/шаблонов)
471
347 / 25 / 99
Количество элементов данных (активированных/деактивированных/неподдерживаемых)
15182
12967 / 164 / 2051
Количество триггеров (активированных/деактивированных [проблема/ок])
7191
6611 / 580 [254 / 6357]
Количество пользователей (в сети)
6
2
Проблемы по важности
Группа узлов сети
Чрезвычайная
Высокая
Средняя
Предупреждение
Информация
Не классифицировано
Cameras
Cisco/Routers
Cisco/Switches
Discovered hosts
Mikrotik Routers
OTC/camers
OTC/SCUD
Локальное
Проблемы
Время
Инфо
Узел сети
Проблема • Важность
Длительность
Подтверждено
Действия
Теги
19:31:00
Камера - Видим. Бокс 10.100.50.3
Узел не доступен
4м 2с
Нет
19:30:58
Камера - Видим. Улица 10.100.50.4
Узел не доступен
4м 4с
Нет
19:30:54
IRZ_Vidim
Узел не доступен 81.18.116.128
4м 8с
Нет
19:30:52
УРВ - Видим 10.100.50.2
Узел не доступен
4м 10с
Нет
19:00
18:19:15
Cisco 2960 (10.0.0.18)
Interface Fa0/19(): Ethernet has changed to lower speed than it was before
1ч 15м 49с
Нет
18:00
17:25:16
Cisco WS-C3750G-24PS (10.0.0.3)
Interface Fa3/0/28(): Link down
2ч 9м 48с
Нет
17:00
12:58:35
AP-78:8a:20:e2:60:cc-(85)
Interface wifi0: High error rate
6ч 36м 29с
Нет
12:22:27
sw1.yantal.nd.lan (10.100.13.2)
Interface Fa1/0/13(= SW Video RMM =): Link down
7ч 12м 37с
Нет
Сегодня
29.10.2020 16:18:22
gw.yantal.nd.lan
CPU: Temperature is above warning threshold: >50
1д 3ч 16м
Нет
Избранные карты сетей
Принтеры 1 этаж
Принтеры 2 этаж
Принтеры 3 этаж
Топология
Избранные графики
Графики не добавлены.

Grafana

https://grafana.com/grafana/download

Grafana — это инструмент с открытым исходным кодом, имеющий лицензию Apache 2.0, разработанный Torkel Ödegaard (который все еще отвечает за его разработку и обслуживание) и созданный в январе 2014 года.

Этот шведский разработчик начал свою карьеру в области **.NET** и с 2012 года до в настоящее время он продолжает предлагать услуги по разработке и консалтингу через эту популярную платформу, одновременно разрабатывая бесплатное программное обеспечение.

Grafana


Sign ups
275
Logins
193
Sign outs
276
Logins
193
Google hits
55
Memory
110 B
Logouts
221
Memory / CPU
7 B
6 B
5 B
4 B
3 B
2 B
1 B
0 B
8%
6%
4%
2%
0%
22:50
23:00
23:10
23:20
23:30
23:40
memory
cpu
logins
timeshift -1h
100
80
60
40
20
0
21:50
22:00
22:10
22:20
22:30
22:40
logins
logins (-1 hour)