

“Ну и запросы у вас... - сказала база данных и повисла.”

Управляем сетью легко: Волшебный SNMP

Докладчик: Алексей Мараховец

10-Strike Software

www.10-strike.com

Что такое SNMP?

- Простой протокол управления сетью;
- Универсальный язык общения с «умным» сетевым «железом»;
- Способ узнать об устройстве много интересного.

Как это работает?

- MIB – Men In Black?
- Таинственные OIDs в дереве MIB;
- Абстрактный синтаксис ASN.1.
- SNMP-агент;

Management Information Base

1: 1.2.840.10006.300.43.1.2.1.1.2.1 = 32768 [Integer]

...

746: 1.3.6.1.2.1.1.1.0 = "Cisco Internetwork Operating System Software IOS (tm) C2950 Software (C2950-I6Q4L2-

747: 1.3.6.1.2.1.1.2.0 = 1.3.6.1.4.1.9.1.324 [ObjectIdentifier]

748: 1.3.6.1.2.1.1.3.0 = 36,9:5:31.900 [TimeTicks]

749: 1.3.6.1.2.1.1.4.0 = "" [Octets]

750: 1.3.6.1.2.1.1.5.0 = "NIO-22_510" [Octets]

751: 1.3.6.1.2.1.1.6.0 = "" [Octets]

752: 1.3.6.1.2.1.1.7.0 = 2 [Integer]

753: 1.3.6.1.2.1.1.8.0 = 0,0:0:0.000 [TimeTicks]

754: 1.3.6.1.2.1.2.1.0 = 26 [Integer]

755: 1.3.6.1.2.1.2.2.1.1.1 = 1 [Integer]

759: 1.3.6.1.2.1.2.2.1.1.5 = 5 [Integer]

760: 1.3.6.1.2.1.2.2.1.1.6 = 6 [Integer]

761: 1.3.6.1.2.1.2.2.1.1.7 = 7 [Integer]

762: 1.3.6.1.2.1.2.2.1.1.8 = 8 [Integer]

763: 1.3.6.1.2.1.2.2.1.1.9 = 9 [Integer]

781: 1.3.6.1.2.1.2.2.1.2.1 = "FastEthernet0/1" [Octets]

782: 1.3.6.1.2.1.2.2.1.2.2 = "FastEthernet0/2" [Octets]

783: 1.3.6.1.2.1.2.2.1.2.3 = "FastEthernet0/3" [Octets]

...

11024: 1.3.6.1.4.1.9.9.134.1.1.3.0 = 1.3.6.1.6.1.1 [ObjectIdentifier]

Сложно?

Конечно можно проще!

IP-MIB DEFINITIONS ::= BEGIN

IMPORTS

MODULE-IDENTITY, OBJECT-TYPE, Integer32,
Counter32, IpAddress, mib-2 FROM SNMPv2-SMI
PhysAddress FROM SNMPv2-TC
MODULE-COMPLIANCE, OBJECT-GROUP FROM
SNMPv2-CONF;

ipMIB MODULE-IDENTITY

LAST-UPDATED "9411010000Z"
ORGANIZATION "IETF SNMPv2 Working Group"
CONTACT-INFO

" Keith McCloghrie
Postal: Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
US

Phone: +1 408 526 5260
Email: kzm@cisco.com"

DESCRIPTION

"The MIB module for managing IP and ICMP
implementations,
but excluding their management of IP routes."

REVISION "9103310000Z"

DESCRIPTION

"The initial revision of this MIB module was part of MIB-
II."

::= { mib-2 48}

-- the IP group

ip OBJECT IDENTIFIER ::= { mib-2 4 }

ipForwarding OBJECT-TYPE

SYNTAX INTEGER {

forwarding(1), -- acting as a router
notForwarding(2) -- NOT acting as a router

}

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"The indication of whether this entity is acting as an IP
router in respect to the forwarding of datagrams
received
by, but not addressed to, this entity. IP routers forward

1: 1.2.840.10006.300.43.1.2.1.1.2.1 = 32768 [Integer]

...

746: 1.3.6.1.2.1.1.1.0 = "Cisco Internetwork Operating
System Software IOS (tm) C2950 Software
(C2950-I6Q4L2-

747: 1.3.6.1.2.1.1.2.0 = 1.3.6.1.4.1.9.1.324
[ObjectIdentifier]

748: 1.3.6.1.2.1.1.3.0 = 36,9:5:31.900 [TimeTicks]

749: 1.3.6.1.2.1.1.4.0 = "" [Octets]

750: 1.3.6.1.2.1.1.5.0 = "NIO-22_510" [Octets]

751: 1.3.6.1.2.1.1.6.0 = "" [Octets]

752: 1.3.6.1.2.1.1.7.0 = 2 [Integer]

753: 1.3.6.1.2.1.1.8.0 = 0,0:0:0.000 [TimeTicks]

754: 1.3.6.1.2.1.2.1.0 = 26 [Integer]

755: 1.3.6.1.2.1.2.2.1.1.1 = 1 [Integer]

759: 1.3.6.1.2.1.2.2.1.1.5 = 5 [Integer]

760: 1.3.6.1.2.1.2.2.1.1.6 = 6 [Integer]

761: 1.3.6.1.2.1.2.2.1.1.7 = 7 [Integer]

762: 1.3.6.1.2.1.2.2.1.1.8 = 8 [Integer]

763: 1.3.6.1.2.1.2.2.1.1.9 = 9 [Integer]

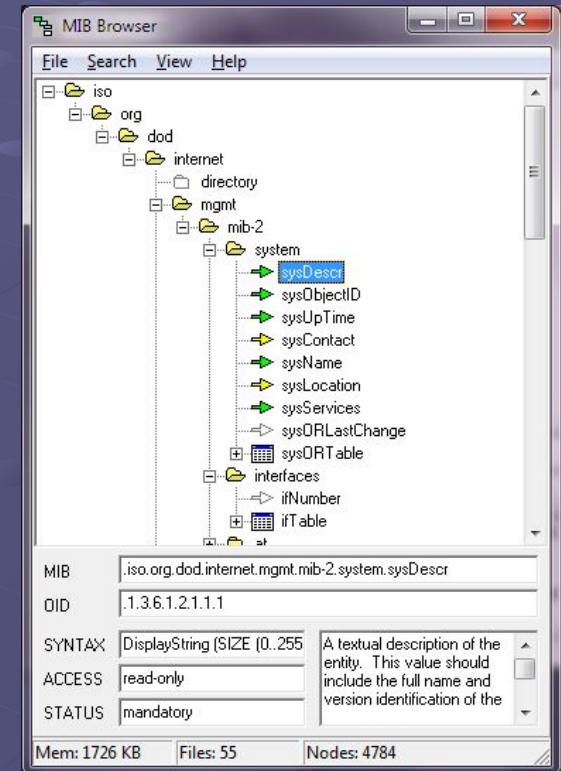
781: 1.3.6.1.2.1.2.2.1.2.1 = "FastEthernet0/1" [Octets]

782: 1.3.6.1.2.1.2.2.1.2.2 = "FastEthernet0/2" [Octets]

783: 1.3.6.1.2.1.2.2.1.2.3 = "FastEthernet0/3" [Octets]

...

11024: 1.3.6.1.4.1.9.9.134.1.1.3.0 = 1.3.6.1.6.1.1
[ObjectIdentifier]

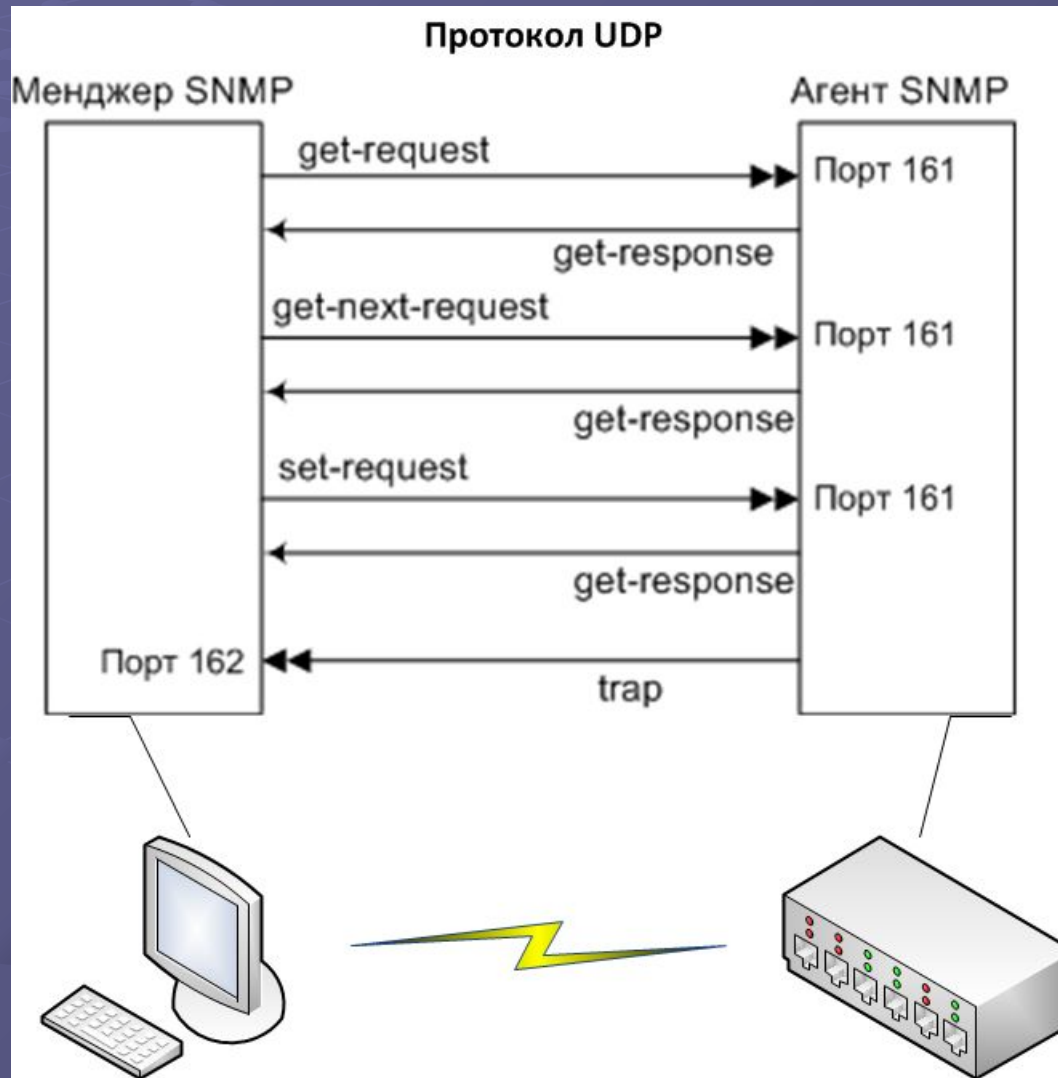


Язык запросов

- GET
- GET NEXT
- BULK (v2+)
- SET
- TRAP, INFORM

И всё?

Немного картинок



Где это работает?

ВЕЗДЕ



- Windows
- Linux и другие *nix
- MAC OS
- IOS ≠ iOS
- SUN Solaris

Реализация в разных ОС



Системная «Служба SNMP»



Демон `snmpd` из разных пакетов; утилиты Net-SNMP



Mac OS X Server 10.1.5+ включает пакет UCD-SNMP. Агент `snmpd`



Функция ОС. Прошивка ПЗУ



Демон `snmpd` из пакета «netsnmp»

Безопасность

SNMP v1, 2, 2c Read / write community (“**public**”)

SNMP v3:

- User-Based Security Model (модуль аутентификации, модуль шифрования и модуль контроля времени);
- Аутентификация HMAC-MD5 и HMAC-SHA;
- Шифрование данных по DES-56, в планах - Diffie-Hellman, CBC-AES-128;
- 3 уровня безопасности: **noAuthNoPriv** - пароли передаются в открытом виде, конфиденциальность данных отсутствует; **authNoPriv** - аутентификация без конфиденциальности; **authPriv** - аутентификация и шифрование, максимальный уровень защищенности.

Применение

- Управление сетевыми устройствами
- Мониторинг состояния устройств и каналов связи
- Визуализация топологии сети (LLDP, CDP, LLTD)
- Сигнализация
- Инвентаризация устройств

Ваши вопросы!