Warszawa, 02.01.2016

Zarządzanie  
Sieciami  
Telekomunikacyjnymi

Prowadzący  
dr inż. Mariusz Mycek

Jan Sobczak 261206  
Rafał Stobiecki 261195  
Michał Ziółkowski 261227

**Model informacyjny agenta SNMP**

1. **Środowisko testowe**

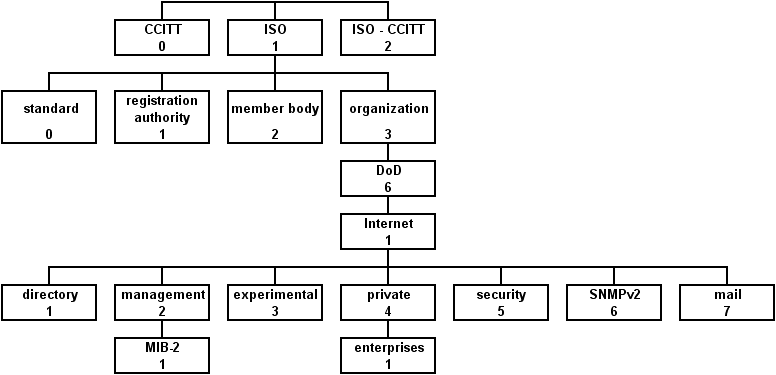
Jako klient SNMP do testów posłużyła nam aplikacja MIB Browser firmy iReasoning. Testy przeprowadzane były na 64 bitowym systemie Microsoft Windows 8.

1. **Przygotowanie systemu Windows**

Systemy z rodziny Microsoft Windows posiadają preinstalowanego fabrycznie klienta SNMP, jest on jednak domyślnie nieaktywny. W celu jego aktywacji należało uaktywnić usługę SNMP Service, oraz zezwolić na połączenia z nią aplikacjom zewnętrznym.

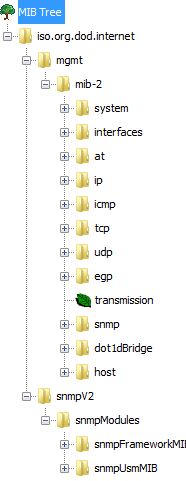
1. **Model agenta SNMP**

Używany agent SNMP implementuje model informacyjny o strukturze drzewiastej, służący do zarządzania sprzętem w sieci telekomunikacyjnej. Model ten stanowi baza danych zarządzania MIB (Management Information Base), w której wszystkie parametry urządzeń (komputera, drukarki, modułu itp.) reprezentowane są jako obiekty zawierające w sobie wartości skalarne lub tablice.

Jak wspomniano, baza MIB wykorzystuje hierarchiczną strukturę drzewiastą obiektów. Każdy obiekt charakteryzuje unikalny identyfikator OID (Object Identifier), którego budowa uwarunkowana jest położeniem obiektu w drzewie. Do obiektu możemy odwoływać się w dwojaki sposób, poprzez adres numeryczny (typu .1.2.3.4 itp. ) lub też za pomocą nazw węzłów (typu iso.org.dod.internet itp.)

Rysunek 1. : Przykładowa struktura drzewiasta MIB

1. Informacje przechowywane w bazie danych MIB



Jak widać po lewej, w przypadku testowanego przez nas MIB’a dzieli się on na dwie główne gałęzie, *mgmt* (*Management)* oraz *snmpV2.*

Ich zawartość przetestowaliśmy poleceniami GetNext, a następnie, aby uzyskać pełen obraz, Walk.

Na podstawie tych testów, oraz informacji pozyskanych z dodatkowych źródeł (głównie RFC 1155 oraz RFC 1495) możemy określić informacje przechowywane w poszczególnych gałęziach.

Poniżej zamieszczamy opisy zidentyfikowanych gałęzi wraz z przykładowymi obiektami.

* **system** – zawiera ogólne informacje o stanie systemu tzn
  + *sysDescr* - informacje o używanej płycie głównej i systemie
  + *sysObjectID* - identyfikator urządzenia sieciowego (dla dostawcy)
  + *sysUpTime* - czas działania urządzenia
  + *sysContact* - opcjonalnie informacje o osobie kontaktowej odpowiedzialnej za ten podzespół
  + *sysName* - nazwę systemu
  + *sysLocation* - opcjonalnie jego lokalizacje
  + *sysServices* - ilość oferowanych usług
* **interfaces** – informacje o interfejsach systemowych
  + *ifNumber* - liczba interfejsów sieciowych obecnych w tym urządzeniu niezależnie działających czy nie
  + *ifTable*: lista interfejsów sieciowych obecnych w tym urządzeniu (nazwa, typ, producent, aktualny stan itp.)
* **at** – konwersja adresów protokołu IP
  + *atTable* - tablica translacji adresów na ich fizyczne odpowiedniki
* **ip** – obiekty protokołu Internet Protocol
  + *ipForwarding* – informuje czy urządzenie zachowuje się jako brama forwardująca datagramy ip przychodzące do niej czy nie
  + *ipDefaultTTL* – domyślna wartość ustawiana w polu TTL datagramów
  + *ipInReceives* – całkowita liczba otrzymanych datagramów (w tym tych błędnych)
  + *ipInHdrError* / *ipInAddrError* – liczba odrzuconych datagramów z powodu
  + *ipIsUnknownProtos* – liczba poprawnie odebranych datagramów odrzuconych z powodu niezgodności protokołów
  + *ipOutNoRoutes* – liczba datagramów odrzuconych z powodu niemożności przesłania ich do ich celu
  + *ipAddrTable* – tablica informacji adresowych ważnych dla tego urządzenia
  + *ipRouteTable* – tablica routingowa urządzenia
  + *ipNetToMediaTable* – tablica służąca do mapowania adresów IP na adresy fizyczne
* **icmp** – obiekty protokołu Internet Control Message Protocol
  + *icmpInMsgs* – całkowita liczba odebranych przez urządzenie wiadomości ICMP
  + *icmpInDestUnreachs* – liczba otrzymanych wiadomość „cel nieosiągalny”
  + *icmpInTimeExcds* – liczba otrzymanych wiadomości „przekroczono czas żądania”
  + *icmpOutMsgs* – liczba wiadomości ICMP wysłanych przez urządzenie
  + *icmpOutErrors* – liczba wiadomości ICMP niewysłanych przez urządzenie z powodu błędów
* **tcp** – obiekty protokołu Transmission Control Protocol
  + *tcpRtoAlgorithm* – rodzaj algorytmu używanego przy określaniu timeout’u
  + *tcpMaxConn* – maksymalna ilość połączeń TCP jakie obsłużyć może dane urządzenie. W przypadku gdy maksymalna ich liczba jest ustalana dynamicznie, przyjmuje wartość -1
  + *tcpCurrEstab* – aktualna liczba połączeń o statusach „utworzone” lub „czeka na zamknięcie”
  + *tcpInSegs* – całkowita liczba otrzymanych przez urządzenie segmentów, wliczając te błędne
  + *tcpConnTable* – lista znanych połączeń TCP wraz z opisem (stan, nazwa, adresy itp.)
* **udp** – obiekty protokołu User Datagram Protocol
  + *udpInDatagrams* – liczba datagramów UDP dostarczonych do użytkowników UDP
  + *udpNoPorts* – całkowita liczba otrzymanych datagramów UDP dla których nie odnaleziono aplikacji na wyznaczonym porcie
  + *udpTable* – tablica zawierająca informację o aplikacjach nasłuchujących UDP
* **egp** – obiekty protokołu Exterior Gateway Protocol
  + *egpInMsgs* – liczba poprawnie odebranych wiadomości EGP
  + *egpNeighTable* – tablica sąsiedztwa EGP
  + *egpAs* – autonomiczny numer systemu tego EGP
* **snmp** – obiekty protokołu SNMP
  + *snmpInPkts* – całkowita liczba wiadomości dostarczonych do jednostki SNMP
  + *snmpInBadCommunityNames* – całkowita liczba wiadomości dostarczonych do jednostki SNMP używających nieznanych wartości parametru „community name”
  + *snmpOutSetRequests* – liczba poleceń SNMP SET wysłanych przez tą jednostkę SNMP
  + *snmpEnableAuthenTraps* – określa czy agent SNMP ma pozwolenie na generowanie Traps po fiasku autentykacji
* **host** – obiekty zawierające informacje o hoście
  + *hrSystemDate* – zawiera aktualną datę systemową
  + *hrSystemNumUsers* – liczba sesji użytkowników dla których system przechowuje informacje o ich stanie
  + *hrSystemProcesses* – liczba aktualnie działających w systemie procesów
  + *hrMemorySize* – ilość pamięci fizycznej RAM posiadanej przez hosta
  + *hrStorageTable* – konceptualna lista pamięci operacyjnej hosta
  + *hrDeviceTable* – tabela urządzeń podłączonych do hosta
  + *hrFSTable* – tabela systemów plików używanych w hoście
  + *hrSWRunTable* – tabela aplikacji działających w hoście
  + *hrSWInstalledTable* – tabela aplikacji aktualnie zainstalowanych na hoście

W gałęzi snmpV2 mamy natomiast:

* snmpModules
  + snmpMib - SNMP Management Information Base - zawiera informacje niezbędne do wysyłania powiadomień takich jak linkDown (łączę nieaktywne) lub tworzenia specjalnych grup.
  + snmpFrameworkMIB - architektura zarządzania SNMP
  + snmpUsmMIB- zabezpieczenia o użytkowników dla SNMPv3. Każdy użytkownik może mieć pewien zestaw zabezpieczeń, ograniczeń itp.
  + snmpVacmMIB - zabezpieczenia oparte o widoki mające pewien stopień zabezpieczeń i wskazane konkretne widoki (tzn. możliwość widoku lub zmiany konkretnych liści)
* snmpDomains - obiekty zawierające informacje o mapowaniu SNMP np. po UDP
* snmpProxys (przestarzałe) - proxy transportowe (domena) dla SNMP po UDP