# Microtik The Dude

## Akwizycja danych z hostów z wykorzystaniem protokołu SNMP ( RouterOS / Windows)

**Protokół SNMP** (ang. Simple Network Managment Protocol) jest związany z procesem monitorowania systemów podłączonych do sieci, oraz zarządzania nimi. Protokół SNMP pozwala na wysyłanie żądań diagnostycznych do urządzeń znajdujących się w sieci, oraz pozwala na monitorowanie wielu parametrów jednocześnie. Urządzenie monitorujące jak i monitorowane muszą być wyposażone w oprogramowanie, które wysyła i odbiera informację SMNP.

Moduł serwera nosi nazwę **Agenta SNMP. Protokół SNMP** pracuje na porcie **TCP** i **UDP 161** Obecnie zdecydowana większość urządzeń podłączanych do sieci ma zaimplementowany protokół SNMP.

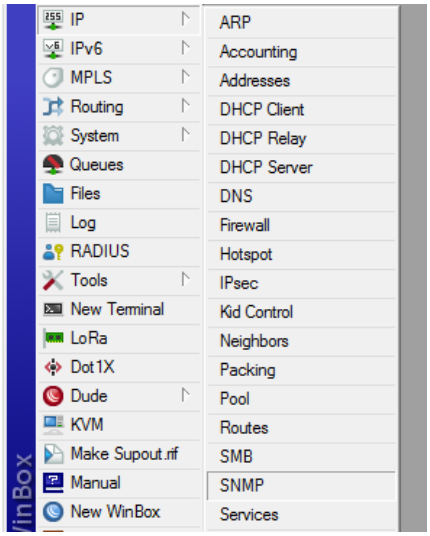
Poniżej zostaną przedstawione kolejne kroki konfiguracji środowiska opartego na narzędziu Microtik The Dude. Do celów testowych zostanie również zaprojektowana sieć złożona z wielu hostów.

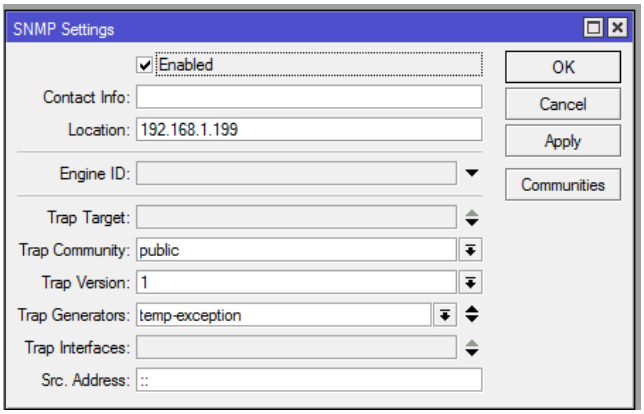
Testy zostaną przeprowadzone na routerach wyposażonych w system RouterOS oraz w systemie Windows.

Ważne, aby wersje oprogramowania The Dude i Router OS były zgodne, gdyż w przeciwnym wypadku nie będzie możliwe nawiązanie połączenia.

### Mikrotik

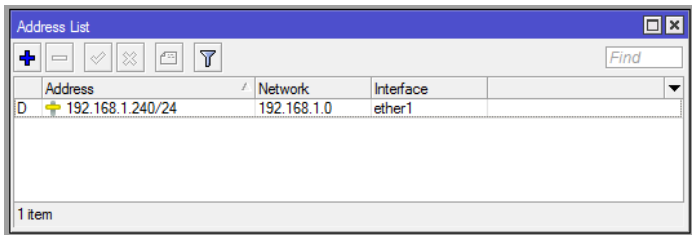
W pierwszym kroku uruchamiamy protokół SNMP na routerze, który chcemy monitorować. Domyślnie ten protokół jest wyłączony. Bez tego protokołu program The Dude nie będzie mógł pobierać szczegółowych informacji dotyczących bieżącej konfiguracji urządzenia, lub odczytywać jego parametrów, np. temperatury, napięcia zasilania itp.



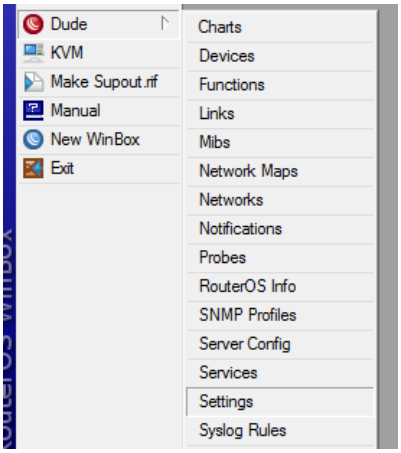



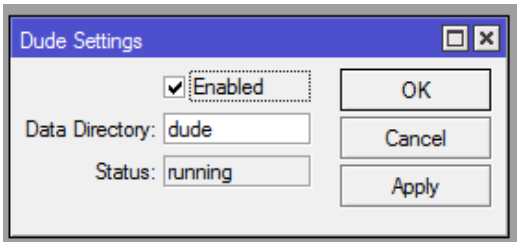

W konfiguracji podajemy adres IP urządzenia, które będzie odbierać zdarzenia typu TRAP. Urządzenia które przesyłają komunikaty protokołem SNMP powinny mieć taką samą nazwę Trap Community, zwykle przyjmuje się że jest to nazwa "public".

Następnie sprawdzamy, jaki mamy adres IP ustawiony na routerze, będzie potrzeby do konfiguracji klienta The Dude.

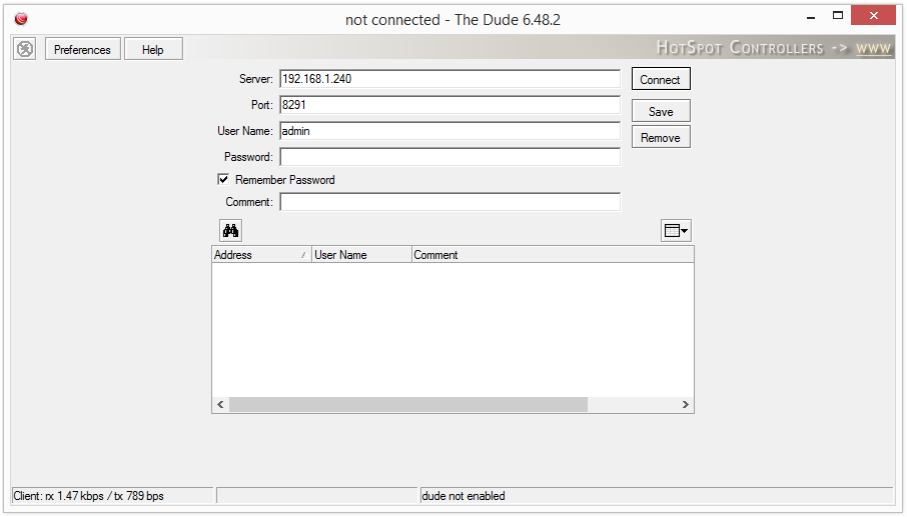



Na koniec włączamy serwer Dude w routerze:

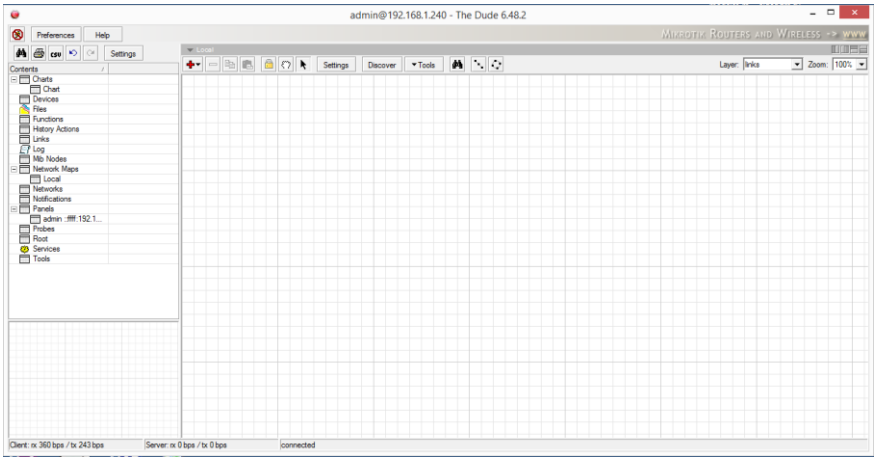



Uruchamiamy klienta The Dude, i podajemy adres IP Routera z działającym serwerem Dude:

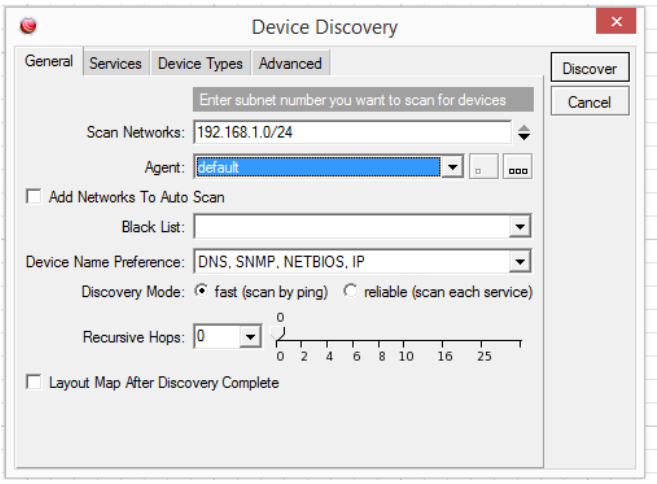



Jeśli serwer działa, to po chwili zostanie nawiązane połączenie:

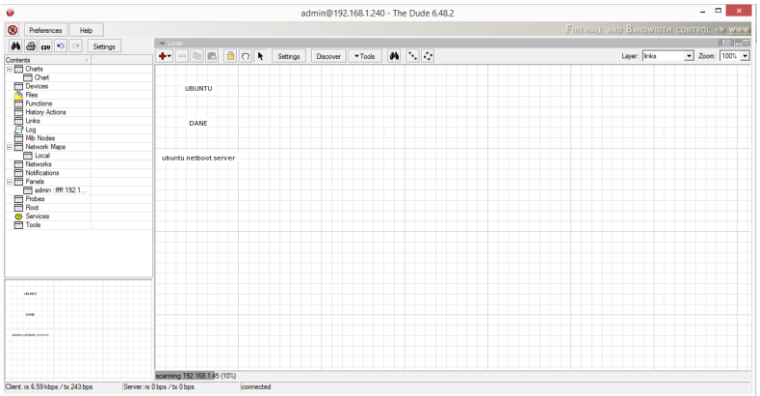


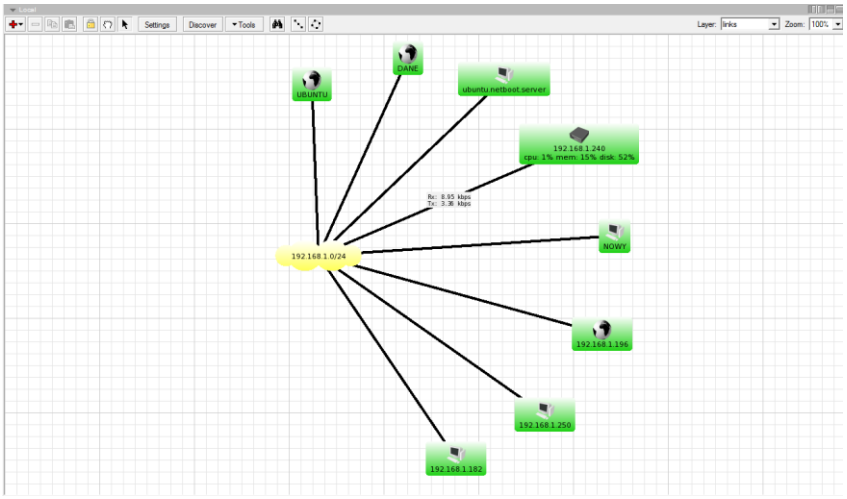

Jeśli chcemy wyszukać urządzenia znajdujące się w pobliżu, wybieramy opcję "Discover",

i podajemy, w jakiej sieci chcemy szukać hostów:

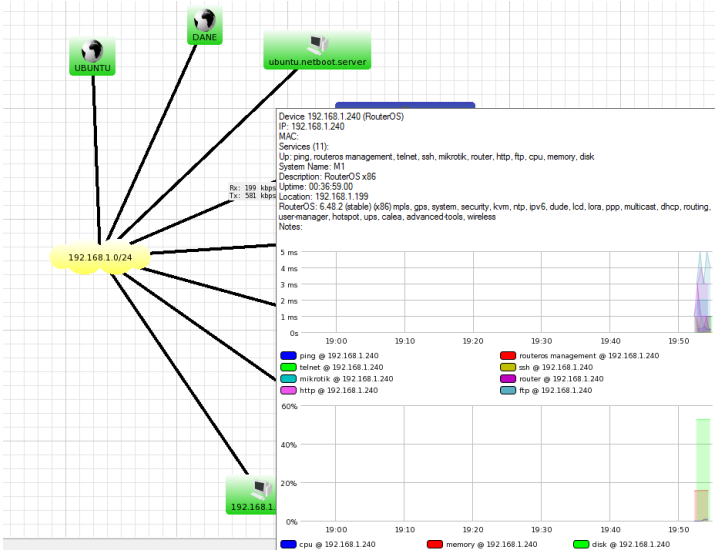



Rozpocznie się proces skanowania, po zakończeniu którego pojawią się ikony hostów wraz z połączeniami.

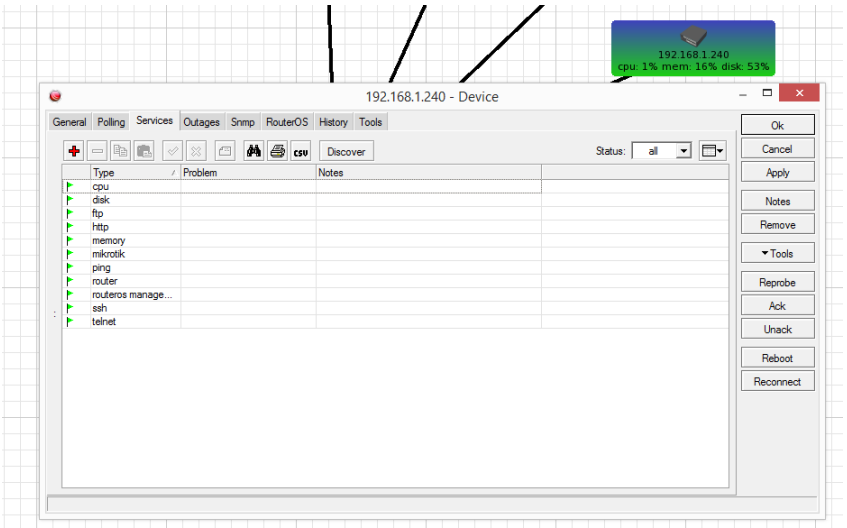




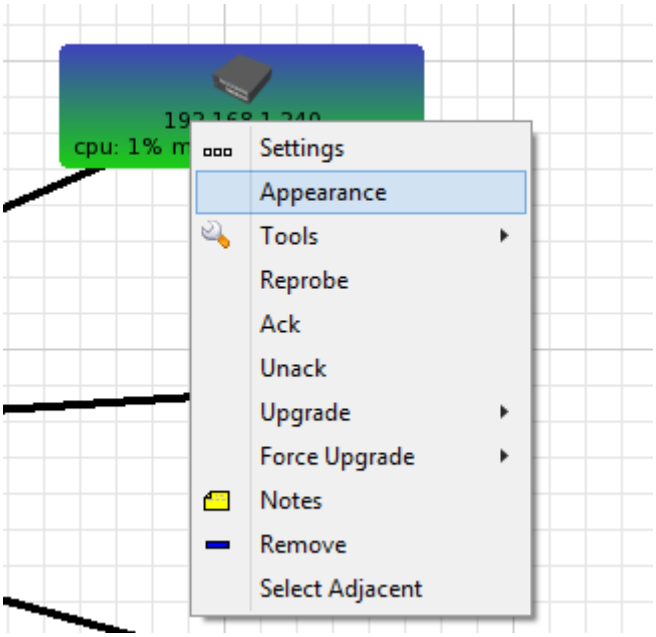

Po najechaniu myszką na hosta, może zobaczyć aktualne parametry hosta, które są na bieżąco aktualizowane:



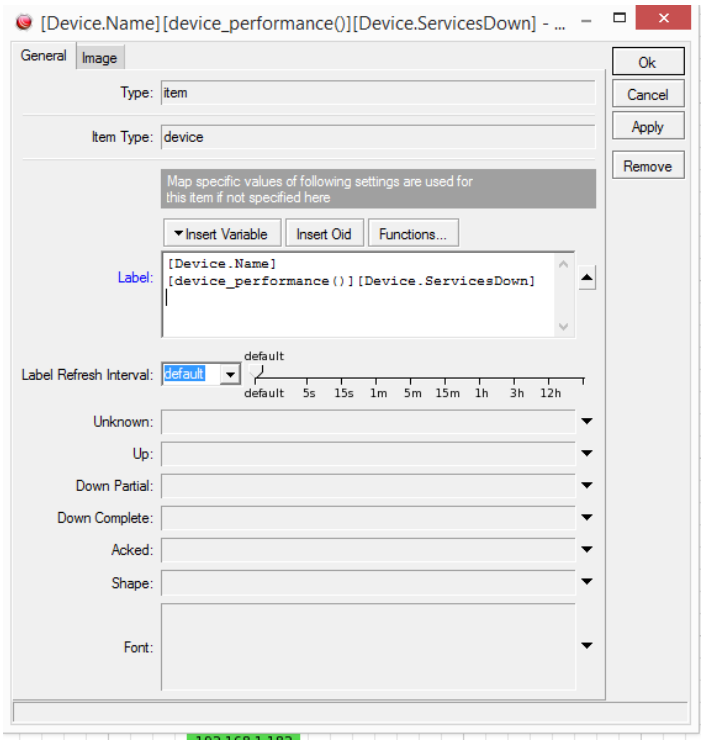

Jeśli chcemy sprawdzić, jakie usługi są uruchomione na danej maszynie, klikamy w ikonę hosta, i w wybieramy pozycję "Services".



Istnieje również możliwość modyfikacji podglądu informacji wyświetlany na ikonie hosta, przez konfigurację parametrów etykiety. Aby przejść do tych ustawień, klikamy prawym przyciskiem na ikonie hosta, i wybieramy "Appearance":

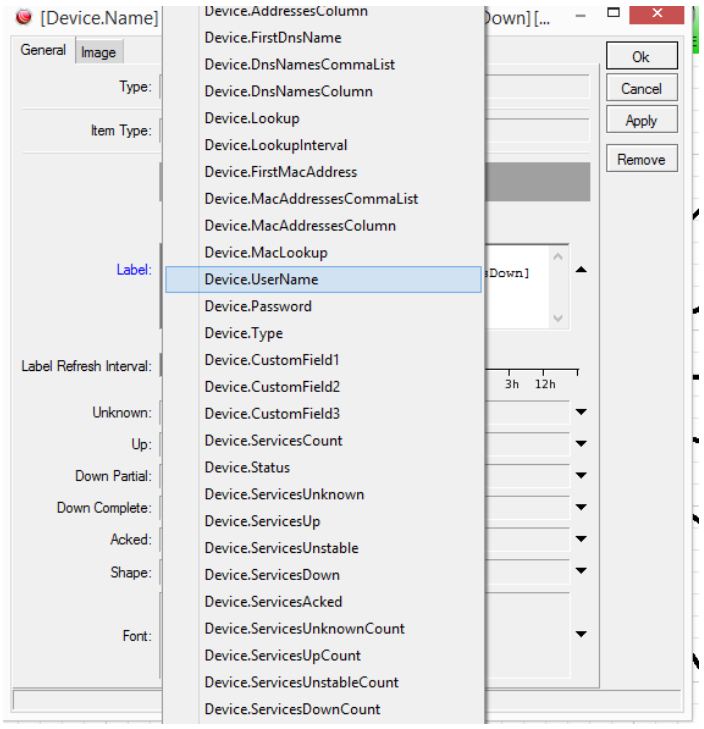


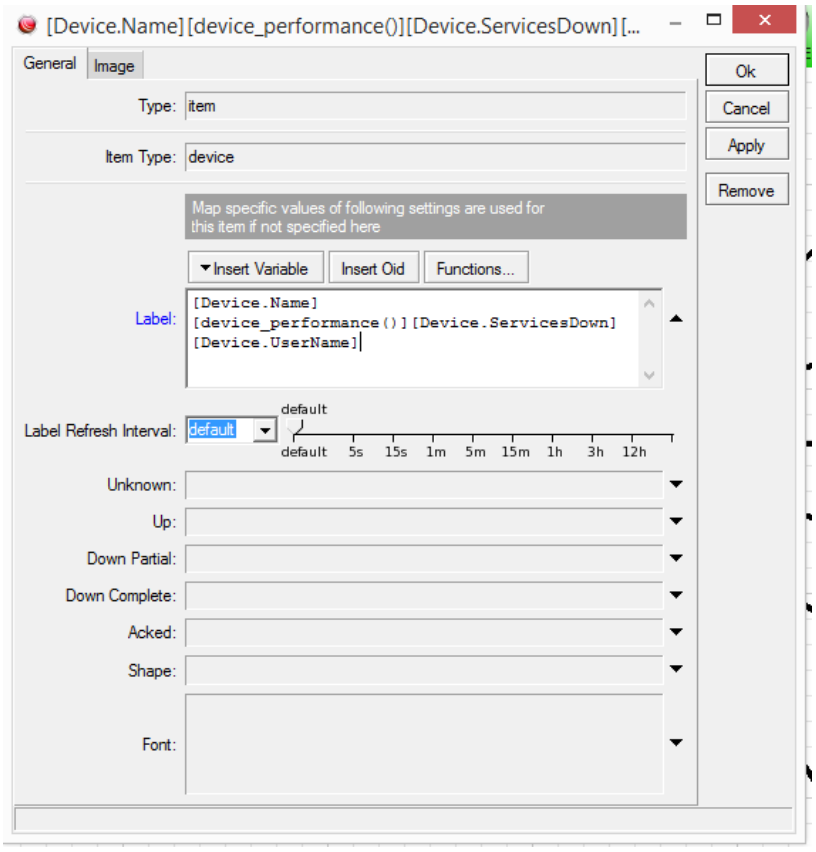

a następnie edytujemy pole Label:




Każdy wiersz, to pojedyncza informacja wyświetlana na ikonie hosta.

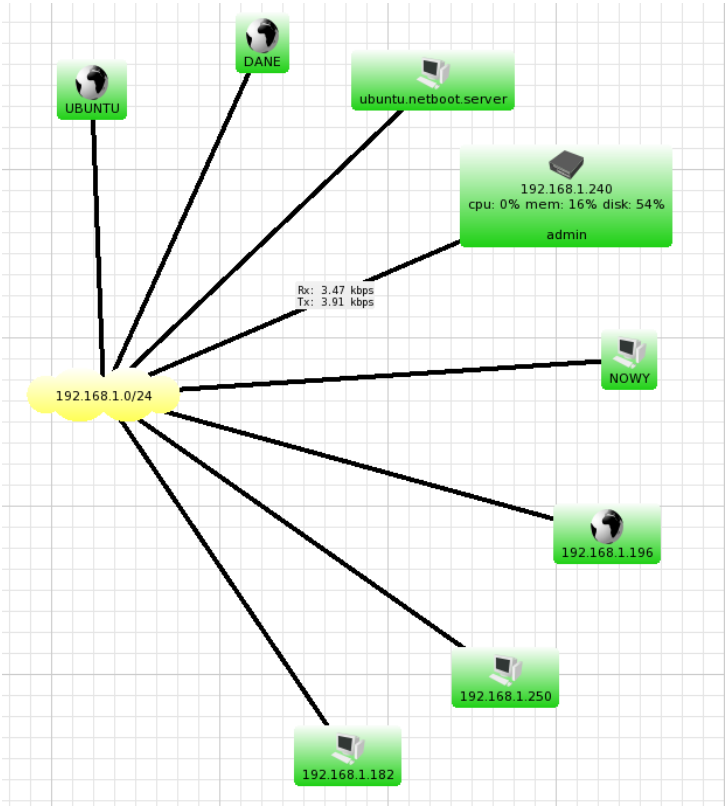
Nowe pozycje można dodawać, wciskając przycisk "Insert Variable", np. nazwę użytkownika:



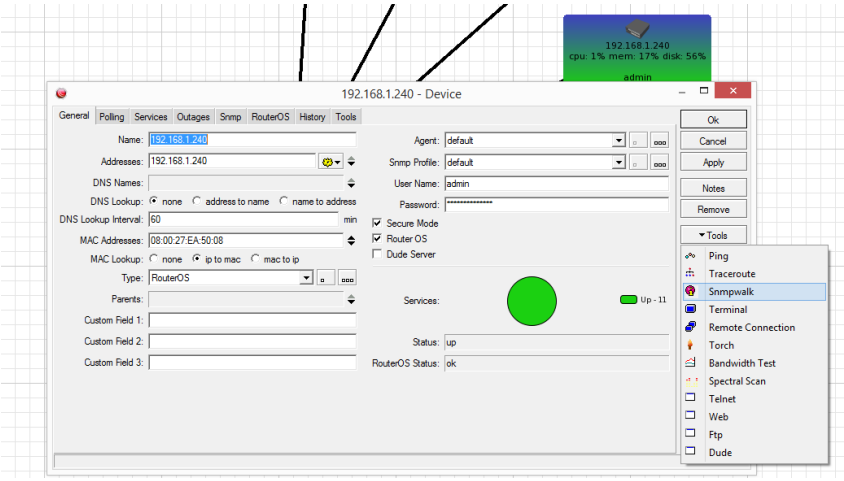

i zatwierdzamy wybór przyciskiem OK.

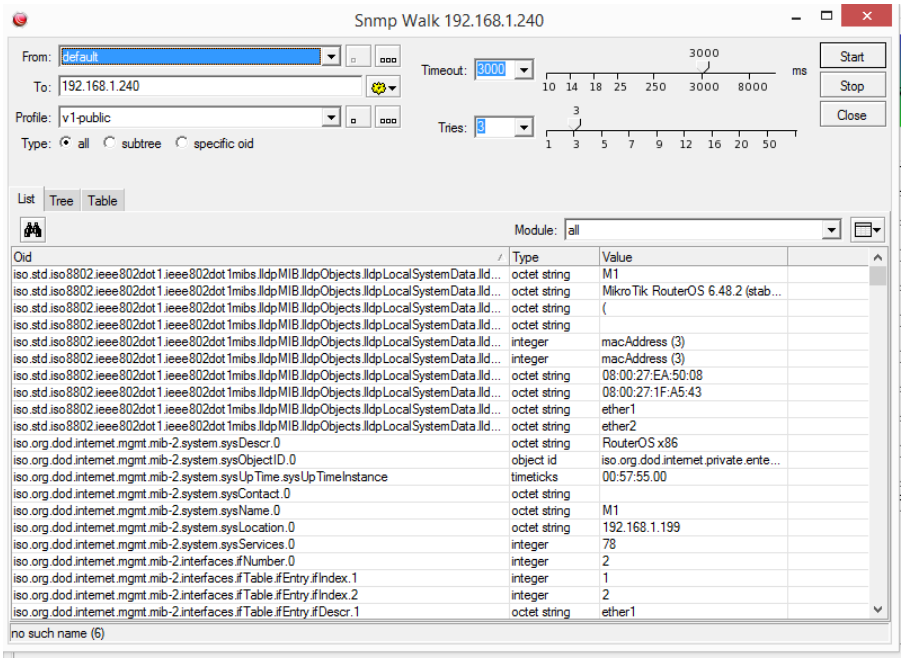
W efekcie na ikonce przypisanej do urządzenia pojawi się dodatkowo nazwa użytkownika.




Możemy również podać specjalny ciąg wskazujący na konkretną własność systemu jaką chcemy monitorować. Parametr nosi nazwę Oid, listę dostępnych wartości dla danego urządzenia należy wyszukać w dokumentacji technicznej.

Jeśli urządzenie wspiera protokół SNMP, to możemy odpytać hosta, jakie parametry są dostępne. Wykonujemy to zadanie, przez wybranie opcji Snmpwalk, po wcześniejszym przejściu do szczegółów urządzenia (dwukrotne kliknięcie w ikonę hosta).

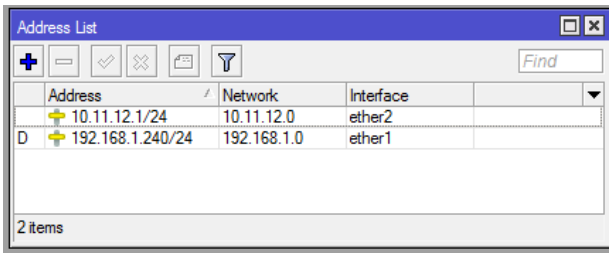




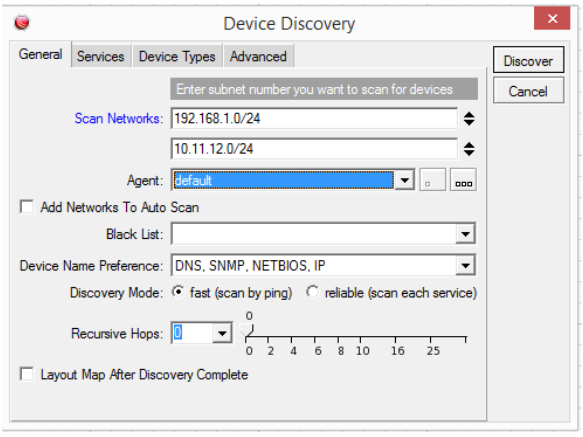

Przykładowy ciąg, jaki należy wpisać dla systemu Windows7, aby uzyskać informacje o sprzęcie:

HW: [oid("1.3.6.1.2.1.1.1.0")]

Program umożliwia również skanowanie kilku sieci jednocześnie, np. dla poniższych sieci możemy wykonać skanowanie hostów:



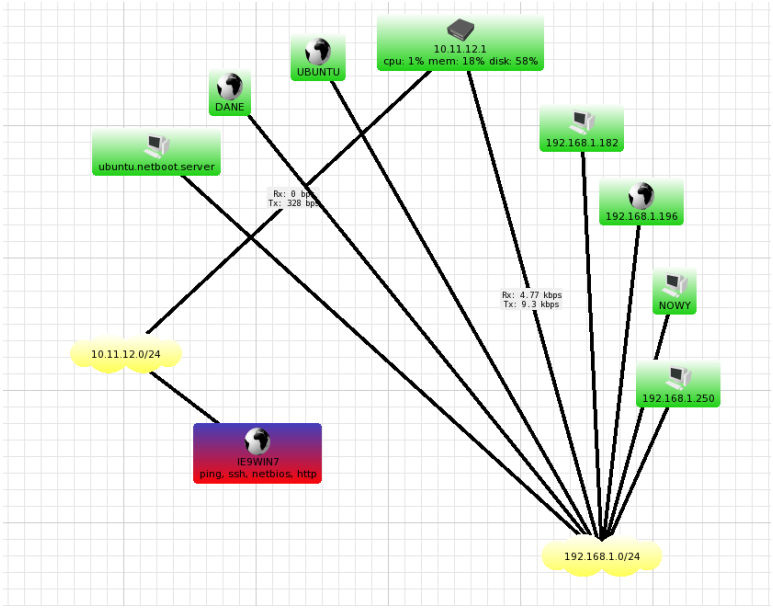

w sposób następujący:



Po przeskanowaniu widzimy, że program wykrył maszynę z systemem Windows, ale nie wyświetlił żadnych dodatkowych informacji. Jeśli protokół SNMP działa na danej maszynie, to oprócz szczegółowych informacji o systemie, analizowany jest ruch sieciowych, co jest wyświetlane na ścieżce połączenia.

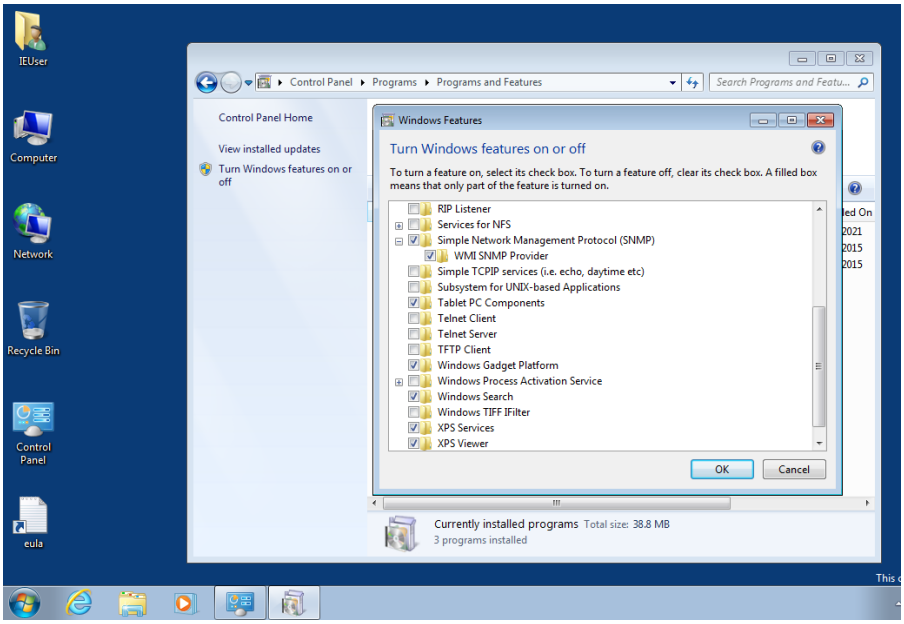
Aby sprawdzić, czy maszyna ma włączoną usługę SNMP, można przejść w opcjach hosta na zakładkę Snmp, i jeśli nie ma tam żadnych pozycji, to mamy pewność, że protokół jest wyłączony.

W przypadku gdy stan maszyny ulegnie zmianie, zmienia się również kolor ikonki reprezentujący hosta:

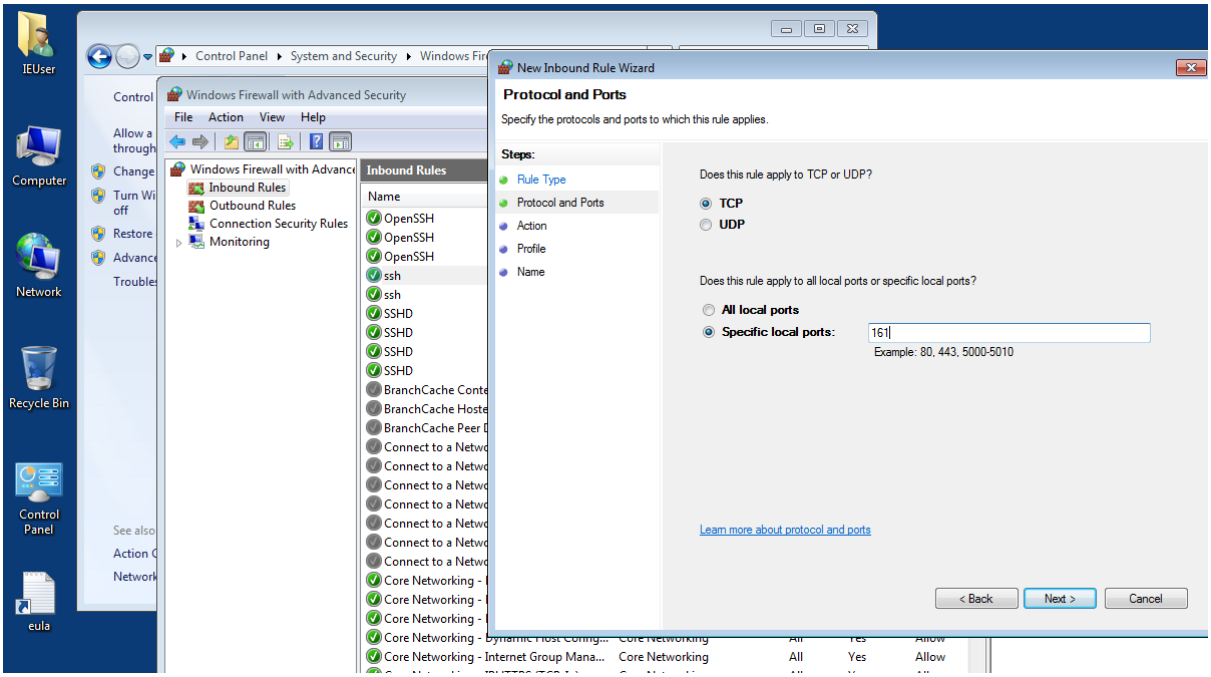



## Windows - konfiguracja SNMP

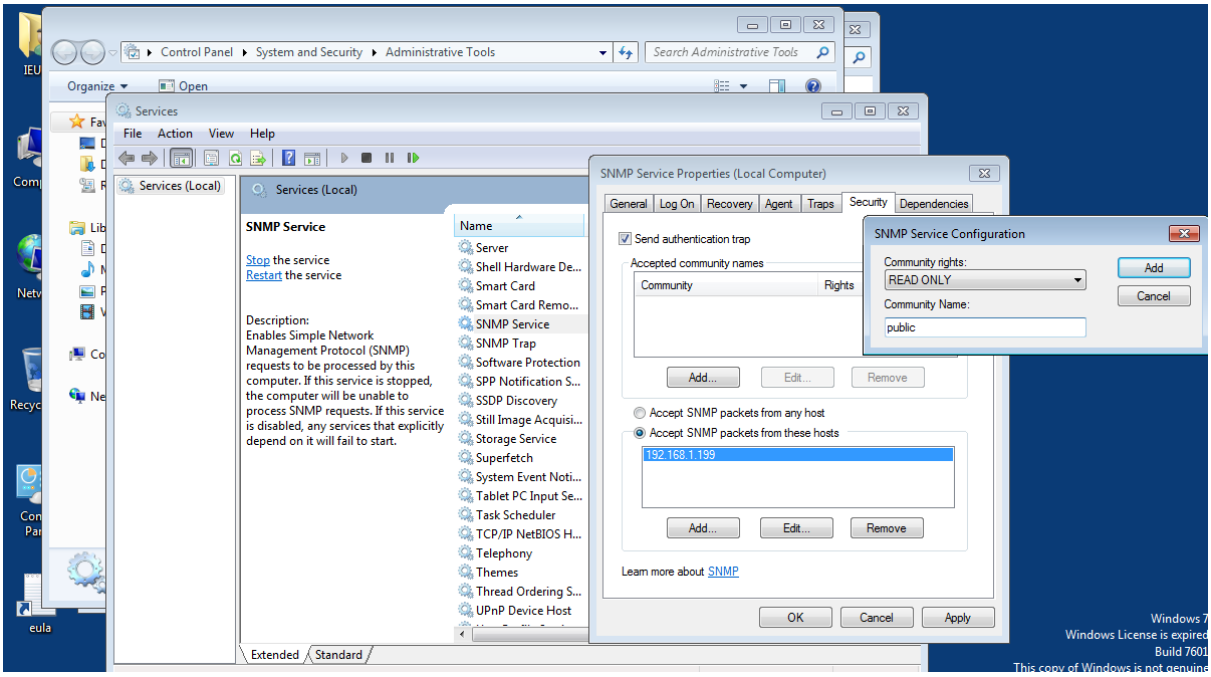
Konfigurację serwisu należy rozpocząć, od włączenie oprogramowania dostępnego w systemie Windows. W panelu sterowania zaznaczamy właściwość "Simple Network Management Protocol (SNMP)



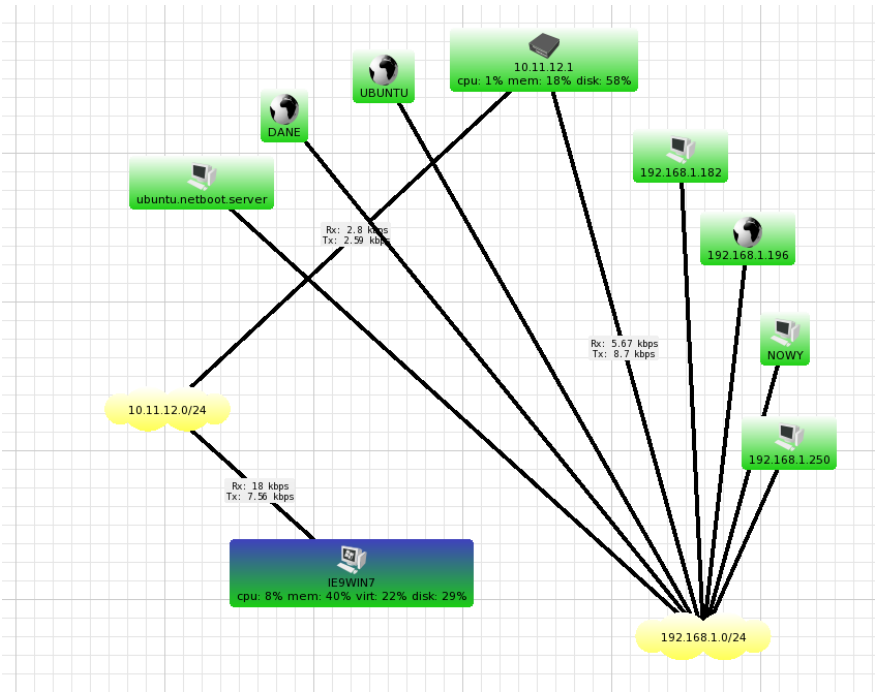

Następnie konfigurujemy firewall, aby umożliwić komunikację z usługą, zezwalamy na ruch przychodzący na porcie 161 dla protokołów TCP i UDP:



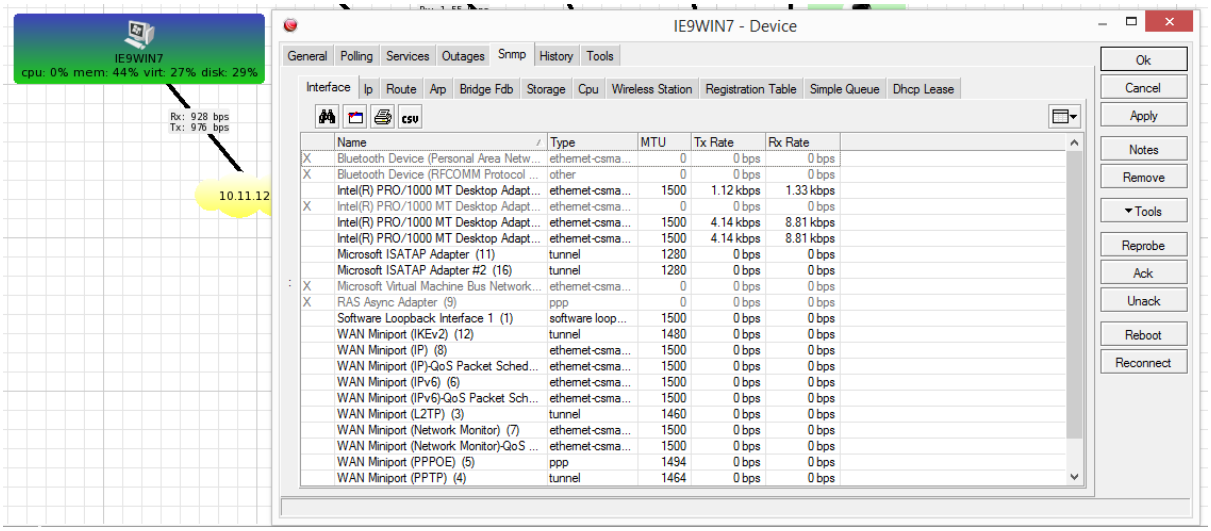

W ostatnim kroku, konfigurujemy usługę SNMP, podając odpowiednią nazwę pola "Community", w naszym przypadku "public", oraz ustawiamy adres IP, z którego będą mogły przychodzić żądania. Jeśli nie chcemy ograniczać połączeń do jednej maszyny, to można zaznaczyć opcję "Accept ... from any host".




Jeśli serwer został poprawnie skonfigurowany, to powinniśmy uzyskać szczegółowe informacje o hoście, po stronie klienta:




Możemy również sprawdzić stan usług dostępny przez protokół SNMP, w odpowiedniej zakładce właściwości hosta:


IE9WIN7
cpu: 0% mem: 44% virt: 27% disk: 29%
Rx: 928 bps
Tx: 976 bps
10.11.12
IE9WIN7 - Device
General
Polling
Services
Outages
Snmp
History
Tools
Interface
Ip
Route
Arp
Bridge Fdb
Storage
Cpu
Wireless Station
Registration Table
Simple Queue
Dhcp Lease
csv
Name
Type
MTU
Tx Rate
Rx Rate
X Bluetooth Device (Personal Area Netw... ethernet-csma... 0 0 bps 0 bps
X Bluetooth Device (RFCOMM Protocol ... other 0 0 bps 0 bps
Intel(R) PRO/1000 MT Desktop Adapt... ethernet-csma... 1500 1.12 kbps 1.33 kbps
X Intel(R) PRO/1000 MT Desktop Adapt... ethernet-csma... 0 0 bps 0 bps
Intel(R) PRO/1000 MT Desktop Adapt... ethernet-csma... 1500 4.14 kbps 8.81 kbps
Intel(R) PRO/1000 MT Desktop Adapt... ethernet-csma... 1500 4.14 kbps 8.81 kbps
Microsoft ISATAP Adapter (11) tunnel 1280 0 bps 0 bps
Microsoft ISATAP Adapter #2 (16) tunnel 1280 0 bps 0 bps
X Microsoft Virtual Machine Bus Network... ethernet-csma... 0 0 bps 0 bps
X RAS Async Adapter (9) ppp 0 0 bps 0 bps
Software Loopback Interface 1 (1) software loop... 1500 0 bps 0 bps
WAN Miniport (IKEv2) (12) tunnel 1480 0 bps 0 bps
WAN Miniport (IP) (8) ethernet-csma... 1500 0 bps 0 bps
WAN Miniport (IP)-QoS Packet Sched... ethernet-csma... 1500 0 bps 0 bps
WAN Miniport (IPv6) (6) ethernet-csma... 1500 0 bps 0 bps
WAN Miniport (IPv6)-QoS Packet Sch... ethernet-csma... 1500 0 bps 0 bps
WAN Miniport (L2TP) (3) tunnel 1460 0 bps 0 bps
WAN Miniport (Network Monitor) (7) ethernet-csma... 1500 0 bps 0 bps
WAN Miniport (Network Monitor)-QoS ... ethernet-csma... 1500 0 bps 0 bps
WAN Miniport (PPPOE) (5) ppp 1494 0 bps 0 bps
WAN Miniport (PPTP) (4) tunnel 1464 0 bps 0 bps
Ok
Cancel
Apply
Notes
Remove
Tools
Reprobe
Ack
Unack
Reboot
Reconnect