netTools

axence

Podręcznik użytkownika

axence

Axence NetTools

Narzędzia sieciowe

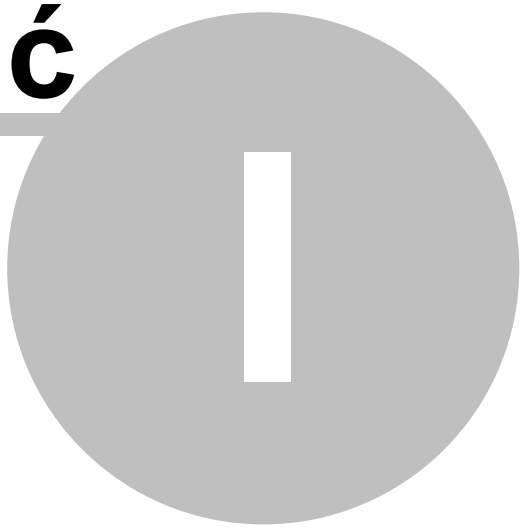
Axence Software, Inc

NetTools to świetne rozwiązanie służące do monitorowania urządzeń sieciowych (z alarmowaniem), mierzenia wydajności sieci i szybkiego diagnozowania problemów. Najbardziej zaawansowane narzędzie to NetWatch, monitorujący urządzenia w sieci, z możliwością alarmowania oraz graficznym narzędziem multiping pokazującym historię czasu odpowiedzi oraz procent utraconych pakietów (umożliwia monitorowanie dostępności komputerów). NetTools zawiera także inne popularne narzędzia IP: ping, szybki traceroute (pełny trace w 1 sekundę), lookup, skaner portów i sieci oraz przeglądarkę SNMP. O unikalności NetTools, wg naszych klientów, decyduje jego najbardziej intuicyjny interfejs użytkownika.

Axence NetTools

Spis treści

Część



1 netTools

1.1 netTools - Wprowadzenie

netTools - świetne rozwiązanie do monitorowania działania sieci oraz szybkiego diagnozowania problemów sieciowych. Najbardziej zaawansowane narzędzie to NetWatch, monitorujący urządzenia w sieci, z możliwością alarmowania oraz graficznym narzędziem NetWatch pokazującym historię czasu odpowiedzi oraz procent utraconych pakietów (umożliwia monitorowanie dostępności komputerów). netTools zawiera także inne popularne narzędzia IP: ping, szybki traceroute (pełny trace w 1 sekundę), lookup, skaner portów i sieci oraz przeglądarkę SNMP. O unikalności netTools, wg naszych klientów, decyduje jego bardzo intuicyjny interfejs użytkownika.

Aktualna wersja PDF podręcznika dostępna jest pod adresem:
http://axence.net/help/netTools/pl/netTools.pdf

1.2 Co nowego

Wersja 5.0 (12/09/2012)

Wersja 5.0 wprowadza:

- NetWatch - już nie tylko PING!
  - monitoring serwisów TCP/IP – monitorowanie czasu odpowiedzi i procentu utraconych pakietów serwisów: HTTP, POP3, SMTP, FTP i 50 innych
  - monitoring dowolnego portu TCP
  - identyfikacja hostów po adresie DNS; automatyczne sprawdzanie adresów co 10min
  - eksport/import hostów
  - obsługa protokołów TLS/SSL w e-mailach alertowych
- Przeglądarka SNMP - kompilator plików MIB – możliwość dodania nowego obiektu bazy MIB w celu obsługi dowolnych nowych urządzeń SNMP
- Traceroute - mapa geograficzna hostów - informacja graficzna o kolejnych hostach na trasie pakietów.
- Geolokacja – informacja o lokalizacji geograficznej (w postaci kraju) zdalnego adresu IP (w narzędziach: NetStat, NetWatch, Ping, Trace). Opcja ta może ułatwić wykrycie podejrzanych połączeń tworzonych przez złośliwe programy. Informacja geograficzna jest też dostępna dla podanego adresu w każdym narzędziu.
- Wake on LAN jako parametr wywołania netTools - możliwość zdalnego uruchamiania oraz wybudzania komputerów przez kartę sieciową

Wersja 4.0 (03/03/2009)

Wersja 4.0 wprowadza:

- netTools jest całkowicie DARMOWE i bez limitów. Wymaga jednak dalej aktywacji. Po aktywacji wszystkie narzędzia pozostają aktywne.
- Oba programy Free Axence netTools i Axence netTools Proffessional nie są już dostępne - obecnie dostępny jest tylko Axence netTools Pro, który jest nową darmową wersją.
- Ulepszony resolwer DNS - wszystkie narzędzia mają niezależne resolwery i działają szybciej.
- Nazwy urządzeń w NetWatch - długo oczekiwana identyfikacja monitorowanych urządzeń.
- Kilka innych poprawek.

Wersja 3.1 (10/09/2007)

Wersja 3.1 wprowadza:

- Linia poleceń. Można stworzyć skróty do często wykonywanych zadań.
- Poprawione alarmy mailowe.

Wersja 3.0 (11/13/2006)

Wersja 3.0 wprowadza wiele nowych narzędzi, które pomogą Ci w codziennych zadaniach administratora:

- WinTools - Podaje wyczerpujące informacje o komputerach Windows (za pomocą WMI). Posiada wiele predefiniowanych zapytań, umożliwiających oczytanie listy serwisów, informacji o dysku, listy procesów etc. Pozwala edytować rejestr i tworzyć własne zapytania.
- NetStat - prezentuje wszystkie połączenia przychodzące i wychodzące z Twojego komputera oraz wszystkie otwarte porty, włącznie z informacjami o otwartych portach TCP i UDP, adresie IP i stanach połączenia. NetStat pokazuje także nazwę procesu wykorzystującego połączenie (socket).
- Local info - Przedstawia kilka tabel z ważnymi informacjami o lokalnej konfiguracji: statystyki dla TCP/UDP i ICMP, tabela adresów IP, tabela ARP i routingu, informacje o kartach sieciowych.
- TCP/IP workshop - Pozwala uzyskać niskopoziomowe połączenie TCP i UDP w celu testowania i wykrywania problemów z serwisami sieciowymi. Za pomocą tego narzędzia można wysyłać dane do dowolnego portu na zdalnym komputerze oraz nasłuchiwać na porcie lokalnym, aby zobaczyć wszystkie nadsyłane dane.
- Ulepszony system powiadamiania emailem w narzędziu NetWatch - Cały komponent odpowiedzialny za wysyłanie alarmów przez emaile został napisany od nowa, aby zapewnić jego niezawodność.
    - Program nie wymaga żadnego zewnętrznego serwera SNMP, aby wysyłać emaile z powiadomieniami.
    - Można przetestować jego działanie, aby mieć pewność, że wszystkie opcje są wprowadzone prawidłowo.
    - Podczas testowania, można zobaczyć wiadomości opisujące potencjalne problemy.
    - Program zapisuje informacje o każdym powiadomieniu wysłanym emailem, można więc sprawdzić, czy działa prawidłowo.

1.3 Wymagania systemowe

System operacyjny

- Windows XP/2003/Vista/2008/7/2008R2/8/2012
- Wymagane są prawa administratora (zobacz poniżej)

Sprzęt

- Procesor 500 MHz lub więcej
- Co najmniej 128 MB RAM
- Wideo: 800x600 lub więcej, tryb High-Color
- Karta sieciowa podłączona do sieci LAN/WAN

Prawa administratora

Aby prawidłowo użytkować program, wymagane są prawa administratora. W innym przypadku netTools nie będzie mógł wysyłać żądań ICMP - dostępność tej funkcji Windows jest ograniczona wyłącznie dla administratorów. Jeśli jesteś administratorem, ale program dalej nie działa, uruchom program jako administrator - wybierz "Run as..." z menu kontekstowego ikony i podaj dane logowania. Jest to szczególnie ważne na Windows Vista i Windows 7.

Programy firewall

Jeśli używasz programów firewall/antivirus, które blokują żądania ICMP/SNMP, dodaj netTools do listy wyjątków.

1.4 Dostępne narzędzia

NetWatch
Narzędzie o ogromnych możliwościach, pozwalające monitorować dostępność wielu urządzeń w sieci oraz ich czas odpowiedzi. Możesz także ustawić kilka warunków przy których netTools powiadomi Cię poprzez email, wiadomość lub dźwięk w razie wystąpienia problemów (np. brak odpowiedzi od urządzenia, wolne łącze czy zbyt dużo utraconych pakietów).

NetWatch prezentuje przejrzyste wykresy z aktualnymi i historycznymi danymi czasu odpowiedzi oraz procentem utraconych pakietów. Razem z alarmowaniem jest najważniejszą częścią netTools, ponieważ pomaga śledzić dostępność urządzeń oraz oszacować obciążenie sieci w danym czasie.

WinTools
Narzędzie to pomaga odczytywać informacje WMI o komputerach Windows. Posiada wiele zdefiniowanych zapytań, umożliwiających oczytanie listy serwisów, informacji o dysku, listy procesów etc. Pozwala także tworzyć własne zapytania.

Lokalne
Przedstawia kilka tabel z ważnymi informacjami o lokalnej konfiguracji: statystyki dla TCP/UDP i ICMP, tabela adresów IP, tabela ARP i routingu, informacje o kartach sieciowych.

NetStat (część Lokalnych)
Prezentuje wszystkie połączenia przychodzące i wychodzące z Twojego komputera oraz wszystkie otwarte porty, łącznie z informacjami o otwartych portach TCP i UDP, adresie IP i stanach połączenia. NetStat pokazuje także nazwę procesu wykorzystującego połączenie (socket).

Ping
Wizualne narzędzie zastępujące ping z systemu Windows, dodatkowo zawiera 5-minutową historię. Bardzo łatwe w użyciu jeśli chcesz szybko sprawdzić jeden adres.

Trace
To narzędzie to dużo więcej niż polecenie tracert w Windows. Prezentuje informacje o każdym komputerze pomiędzy twoim a docelowym adresem: czas odpowiedzi oraz liczbę pakietów utraconych. Dzięki temu można szybko określić miejsce powstawania problemów z połączeniem. Bardzo łatwo zlokalizować wolne lub przeciążone routery. Dodatkowo, prezentowana jest informacja graficzna o kolejnych hostach na trasie

pakietów.

Lookup
Działa podobnie jak nslookup, ale pokazuje wszystkie rekordy DNS na raz. Nie musisz się martwić o parametry linii komend czy nazwy rekordów. Dostajesz także informację WHOIS na temat wybranej domeny.

Przepustowość
Jeśli chciałbyś dowiedzieć się jak szybka jest Twoja sieć, to narzędzie jest idealne. Co istotne, zmierzy przepustowość bez przeciążania połączenia.

NetCheck
Narzędzie to sprawdza jakość sprzętu sieciowego w sieci LAN. Niskiej jakości gniazdka lub łącza mogą spowolnić sieć. Bez NetCheck bardzo trudno jest znaleźć przyczynę problemu.

TCP/IP workshop
Pozwala uzyskać niskopoziomowe połączenie TCP i UDP w celu testowania i wykrywania problemów z serwisami sieciowymi.

Skaner portów i serwisów
Pozwala sprawdzić wszystkie otwarte porty oraz działające serwisy (HTTP, POP3, MS SQL, Oracle i 50 innych). Nie tylko sprawdza czy port jest otwarty, ale wysyła zapytanie i sprawdza, czy odpowiedź spełnia określone kryteria. Skaner może także wykryć niektóre trojany i spyware.

Skaner sieci
Czy chciałbyś wykryć wszystkie komputery w sieci (również zdalnej)? Nie ma problemu. Wpisz adres IP z tej sieci a błyskawicznie otrzymasz listę wszystkich komputerów oraz serwisów na nich działających.

Przeglądarka SNMP
Pełna przeglądarka SNMP, tak łatwa, że możesz jej używać jeśli nawet nie wiesz nic o SNMP. Przygotowaliśmy wiele ogólnych kategorii dla każdego systemu, nie trzeba więc przeglądać wielu tysięcy parametrów SNMP — możesz to jednak oczywiście zrobić, jeśli jesteś specjalistą.

1.5 Aktywacja

Możesz używać netTools przez dowolny czas, ale po 30 dniach konieczna jest bezpłatna aktywacja. Aby aktywować, postępuj zgodnie z instrukcjami w programie. Po aktywacji dostępne będą wszystkie narzędzia.

1.6 Układ okna

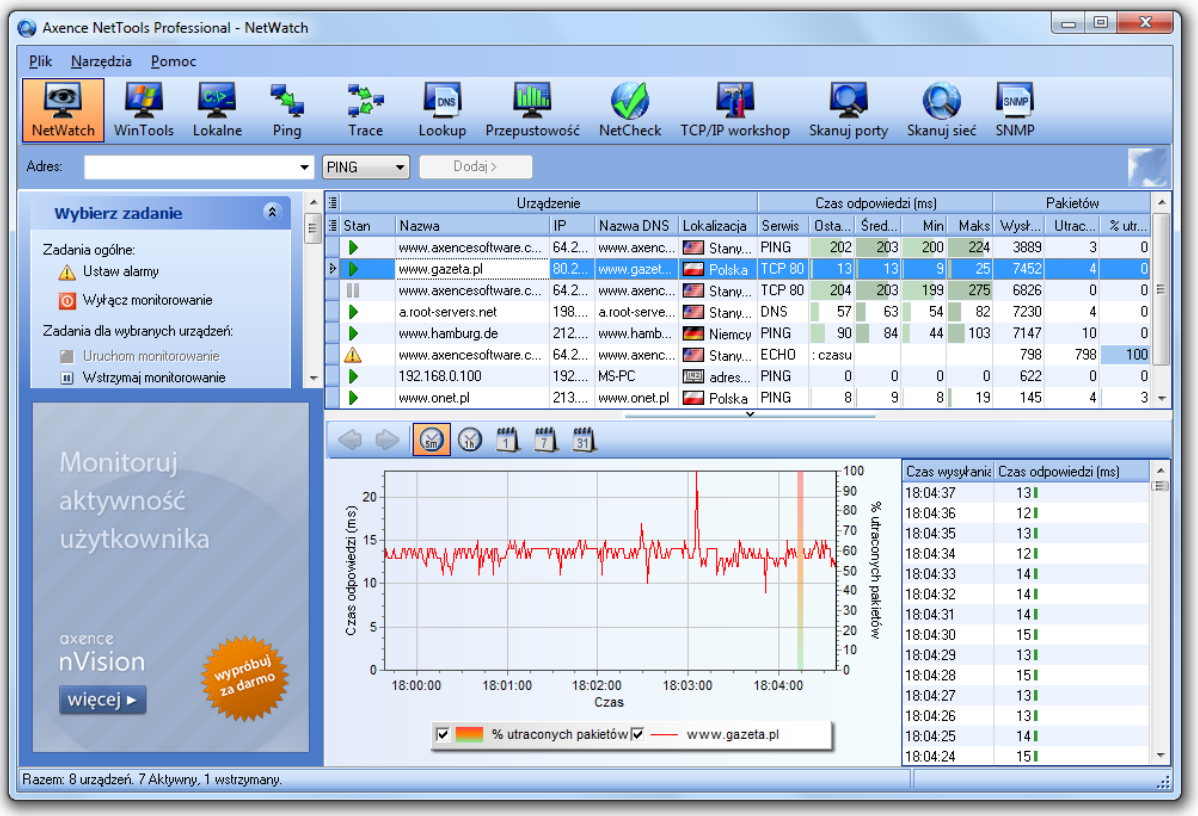
Układ okna netTools jest bardzo intuicyjny i łatwy w obsłudze.

Paski nawigacji i adresu

Paski nawigacji i adresu znajdują się na górze okna. Skorzystaj z zakładki nawigacji, aby wybrać narzędzie, którego chcesz użyć, a z zakładki adresu, aby wprowadzić nazwę DNS (lub IP) urządzenia, które chcesz sprawdzić lub przeskanować (w zależności od wybranego narzędzia).

Boczny pasek narzędzi

Boczny pasek narzędzi znajduje się po lewej stronie okna. Zwykle zawiera ogólne informacje (np. liczbę wysłanych pakietów) i opcje.



Główny obszar

Główny obszar zawiera różne dane kontrolne (tabele, wykresy etc.), w zależności od wybranego narzędzia. W przykładzie powyżej (NetWatch) pokazana jest tabela prezentująca wszystkie urządzenia oraz wykres pokazujący czasy odpowiedzi i utracone pakiety.

Boks reklamowy

W lewym dolnym narożniku okna znajduje się boks reklamowy, w którym wyświetlane są informacje o produktach firmy Axence.

Część II

2 Jak...?

2.1 Jak monitorować urządzenia?

Jeśli chcesz monitorować dane urządzenie przez dłuższy czas, użyj narzędzia NetWatch. Monitoruje ono urządzenia korzystając z ICMP (ping) i zachowuje dla przyszłych analiz czas odpowiedzi oraz procent utraconych pakietów. NetWatch nie tylko monitoruje urządzenia, ale również alarmuje o wszelkich problemach poprzez email, wiadomość, dźwięk oraz zasobnik systemowy (tzw. icon tray).

Aby szybko sprawdzić dostępność jednego urządzenia, użyj narzędzia Ping.

2.2 Jak sprawdzić dostępność urządzeń?

Aby szybko sprawdzić dostępność jednego urządzenia, użyj narzędzia Ping. Wysyła ono pakiety ping (ICMP) do danego urządzenia i na wykresie przedstawia czas odpowiedzi.

Jeśli chcesz sprawdzić jakość połączenia do tego urządzenia, użyj narzędzia Przepustowość. Zmierzy ono szybkość połączenia pomiędzy Twoim komputerem a wybranym urządzeniem.

2.3 Jak zlokalizować źródło problemu?

Jeśli chcesz zlokalizować urządzenie generujące problemy w sieci, użyj narzędzia Trace. Wskaże Ci miejsce powstawania problemów z połączeniem pomiędzy Twoim komputerem a wybranym urządzeniem. Trace pokazuje czas odpowiedzi oraz liczbę utraconych pakietów, weryfikując każde urządzenie znajdujące się na drodze do sprawdzanego urządzenia.

2.4 Jak sprawdzić jakość połączenia i przepustowość sieci?

Aby sprawdzić jakość połączenia z wybranym urządzeniem, użyj narzędzia Przepustowość. Zmierzy ono szybkość połączenia sieciowego pomiędzy Twoim komputerem a wybranym urządzeniem.

Jeśli chcesz sprawdzić jakość sprzętu sieciowego w Twojej sieci LAN, użyj narzędzia NetCheck. Z reguły pozwala ono wykryć nieprawidłowo funkcjonujące gniazdka (sockets) i łącza.

2.5 Jak skanować porty, urządzenia, sieci?

Do skanowania urządzeń używaj narzędzia Skaner portów i serwisów. Pokazuje ono wszystkie działające serwisy i porty otwarte na danym urządzeniu.

Skaner sieci umożliwia wykrycie wszystkich działających komputerów w wybranej sieci. Listuje wszystkie urządzenia i działające na nich serwisy.

2.6 Jak korzystać z SNMP?

SNMP (Simple Network Management Protocol) nie jest w cale tak proste, jak wskazywałaby jego nazwa. Dzięki narzędziu Przeglądarka SNMP, możesz łatwo sprawdzić wszelkie informacje SNMP o urządzeniu, jeśli nawet nic nie wiesz o tym protokole, OID etc.

2.7 Jak korzystać z opcji Wake On LAN?

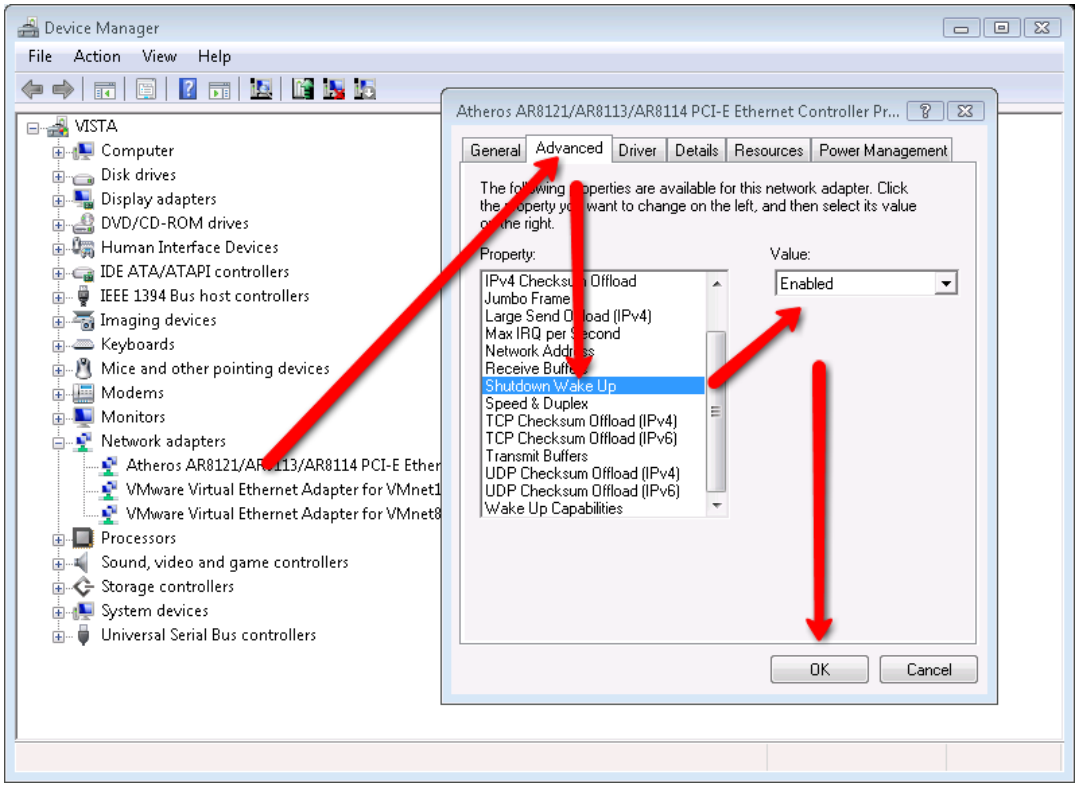
Wake On LAN to metoda zdalnego włączania komputerów. Można z niej korzystać, jeśli znany jest adres MAC komputera, który ma być włączony lub wybudzony. Oprócz tego, konieczne jest skonfigurowanie urządzenia (opisane poniżej) i ewentualne przekierowanie portu na routerze, jeśli komputer będzie wybudzany spoza sieci lokalnej.

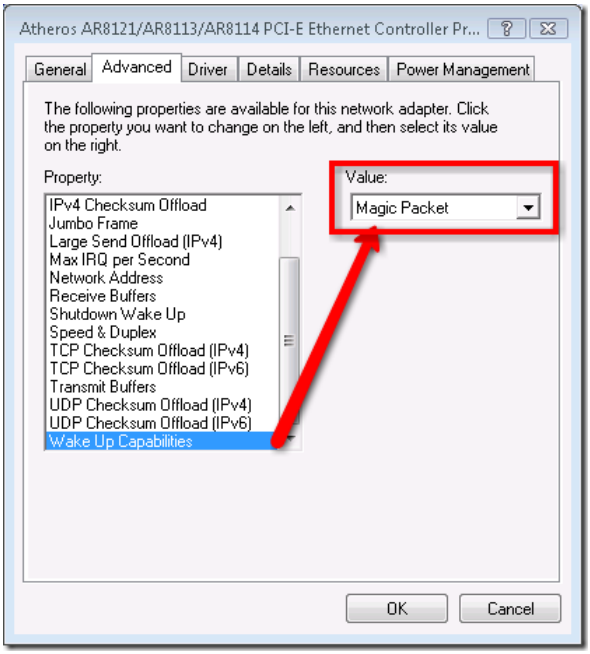
Aby uruchomić dane urządzenie monitorowane np. narzędziem NetWatch, kliknij prawym przyciskiem myszy na tym urządzeniu i wybierz z menu kontekstowego opcje **Narzędzia | Wake On LAN**.

Ustawienia wybudzanego urządzenia

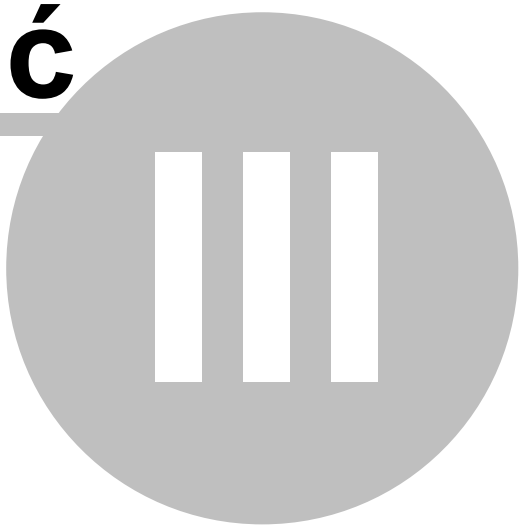
Konfiguracja zależy od konkretnego urządzenia. Przykładowe wymagania i ustawienia:

1. Aby możliwe było korzystanie z funkcji Wake On LAN, konieczny jest zasilacz ATX, przynajmniej 1A, +5Vsb.
2. Ustawienia BIOS-u:
   w zakładce Power (Management) lub Advanced włącz Wake On LAN - opcja może się różnie nazywać, np. Wake On LAN, MAC Resume From S3/S4, MACPME Power Up Control, Power On By Onboard LAN, Power Up By Onboard LAN, Resume by LAN, Resume By WOL, Resume on LAN, Resume on LAN/PME#, Wake on LAN from S5, Wake Up On LAN, WakeUp by Onboard LAN, WOL (PME#) From Soft-Off
3. Ustawienia karty sieciowej:
   a. Przejdź do ustawień karty sieciowej w Windows | Panel sterowania | Menadżer urządzeń.
   b. W zakładce "Zarządzanie energią" ustaw opcje tak, aby możliwe było wybudzanie komputera (nazwy opcji zależą od karty sieciowej, przykładowo "Zezwalaj temu urządzeniu na wyprowadzenie komputera ze stanu wstrzymania").
   c. W zakładce "Zaawansowane" włącz wybudzanie i Wake On LAN - opcje mogą się różnić w zależności od karty sieciowej, przykładowe ustawienia przedstawione są poniżej:





Część



3 NetWatch - Monitorowanie urządzeń

3.1 NetWatch

NetWatch to zaawansowane narzędzie do monitorowania dostępności urządzeń w sieci, serwisów TCP/IP (HTTP, POP3, SMTP, FTP i 50 innych) oraz portów TCP. Przez cały czas wysyła ono pakiety do wszystkich urządzeń na liście i pozwala monitorować czasy odpowiedzi i liczbę utraconych pakietów. Narzędzie to przechowuje historię tych wartości i prezentuje je na wykresach statusu urządzenia. NetWatch pozwala ustawić powiadomienia w razie, gdyby urządzenie nie odpowiadało lub w przypadku problemów z połączeniem. Aby uzyskać więcej informacji, przejdź do rozdziału Alarmy.

Rozpoczęcie monitorowania urządzenia

1. Wybierz narzędzie **NetWatch** z paska nawigacji.
2. Wprowadź nazwę DNS lub adres IP w pasku adresowym.
3. Wybierz rodzaj monitorowania: **Port TCP**, **PING** lub inną **Usługę**.
4. Kliknij **Dodaj** lub naciśnij Enter.

Dostępne informacje

Ogólne informacje o każdym urządzeniu znajdują się w głównej tabeli: nazwa DNS i adres IP, lokalizacja geograficzna zdalnego adresu IP (może ułatwić wykrycie podejrzanych połączeń tworzonych przez złośliwe programy), czasy odpowiedzi (min/max/średni), a także liczba pakietów wysłanych i utraconych.

Na głównym wykresie można zobaczyć czasy odpowiedzi i % pakietów utraconych w wybranym okresie czasu. Jeśli chcesz zobaczyć dokładny czas odpowiedzi w milisekundach, znajdziesz go w tabeli znajdującej się w pasku bocznym. Przechowuje ona czasy odpowiedzi z ostatnich 5 minut.

Główny wykres

Na głównym wykresie, możesz zobaczyć czasy odpowiedzi oraz % utraconych pakietów w wybranym okresie czasu. Czas odpowiedzi jest przedstawiony za pomocą wykresu liniowego, a % utraconych pakietów - warstwowego.

Nad wykresem znajduje się pasek narzędziowy, który pozwala zmienić rodzaj wykresu i przedział czasowy:

Zmiana przedziału czasowego wykresu

Możesz zobaczyć dane historyczne w różnych okresach czasu (np. ostatnie 5 minut, godzina, dzień, tydzień, miesiąc). Aby wybrać odpowiedni okres czasu, kliknij odpowiadającą mu ikonę na pasku narzędziowym wykresu.

Aby przewijać wykres do tyłu i do przodu, użyj ikon ze strzałkami, znajdujących się na pasku narzędziowym wykresu.

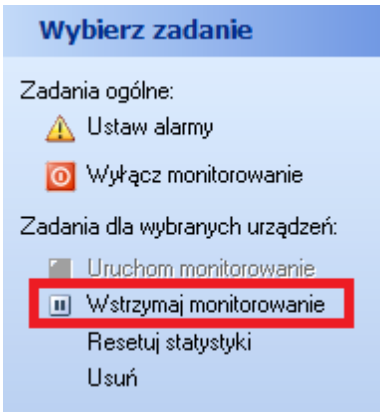
Opcje

Możesz wybrać, czy dane urządzenie ma być identyfikowane przez adres IP czy nazwę DNS. Jest to szczególnie przydatne w przypadku usług działających na zmiennym adresie IP.

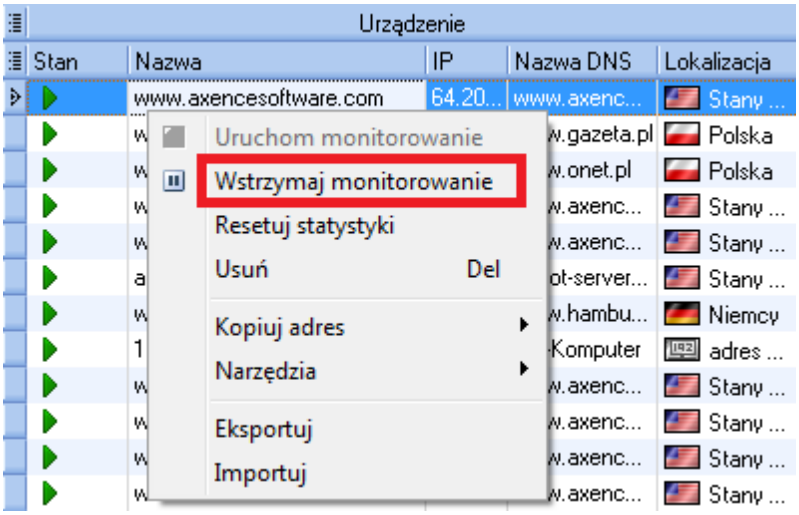
Możesz zmienić częstotliwość monitorowania i maksymalny czas odpowiedzi dla wybranych urządzeń. Wybierz jedno lub więcej urządzeń i w sekcji **Opcje** na pasku bocznym wprowadź preferowane wartości.

Wstrzymywanie monitorowania wybranych urządzeń

1. Wybierz w tabeli jedno lub więcej urządzeń.
2. Wybierz opcję **Wstrzymaj monitorowanie** znajdującą się w sekcji **Wybierz zadanie** na pasku bocznym.

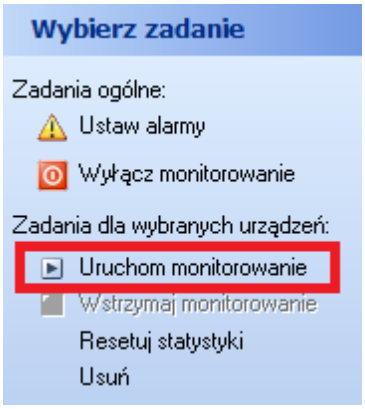


Aby wstrzymać monitorowanie urządzenia możesz także kliknąć prawym przyciskiem myszy na danym urządzeniu i wybrać z menu kontekstowego opcję **Wstrzymaj monitorowanie**.

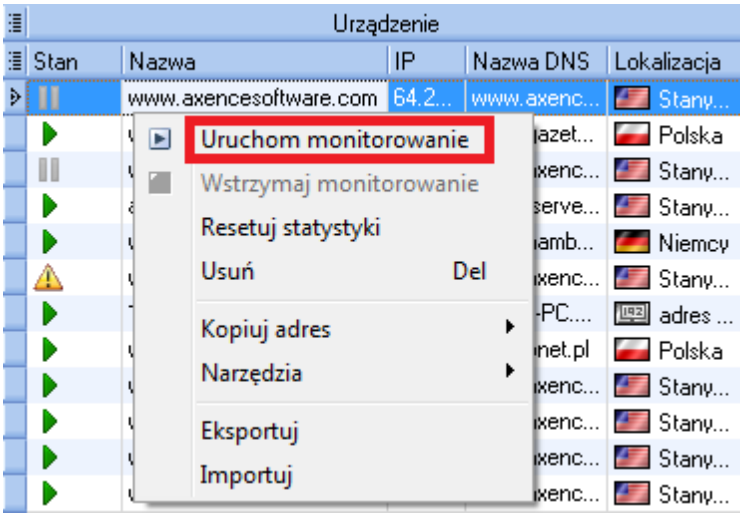


Kontynuowanie monitorowania wybranych urządzeń

1. Wybierz w tabeli jedno lub więcej urządzeń.
2. Wybierz opcję **Uruchom monitorowanie** znajdującą się w sekcji **Wybierz zadanie** na pasku bocznym.

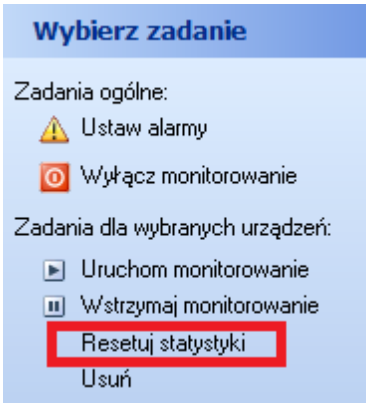


Aby uruchomić monitorowanie urządzenia możesz także kliknąć prawym przyciskiem myszy na danym urządzeniu i wybrać z menu kontekstowego opcję **Uruchom monitorowanie**.

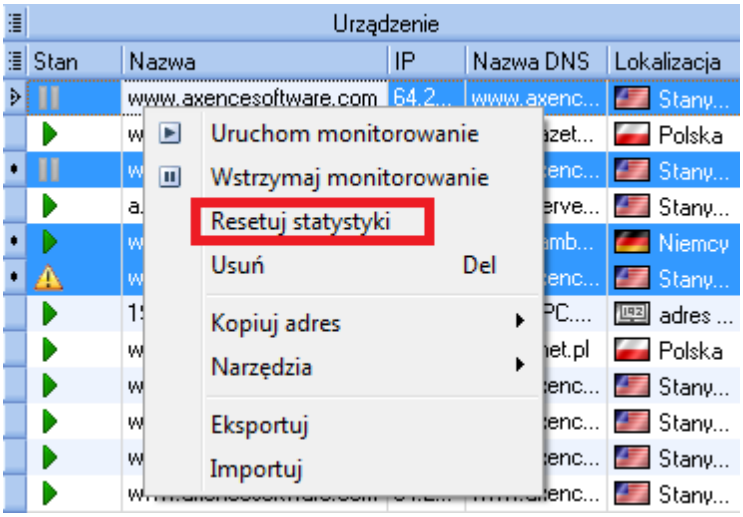


Resetowanie statystyk

1. Wybierz w tabeli jedno lub więcej urządzeń.
2. Wybierz opcję **Resetowanie statystyk** znajdującą się w sekcji **Wybierz zadanie** na pasku bocznym.
3. Program zapyta, czy chcesz usunąć zgromadzone dane statystyczne dla wybranych urządzeń (czas odpowiedzi i % utraconych pakietów). Jeśli nie są Ci one już potrzebne, w oknie wiadomości wybierz **Tak**. Jeśli chcesz je zachować, odpowiedz: **Nie**.

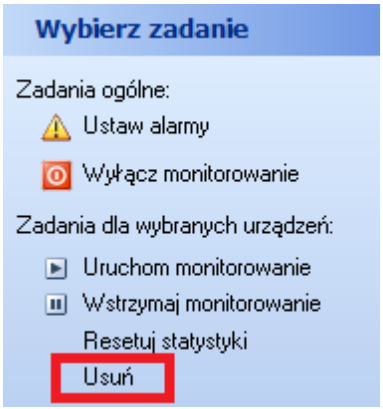


Aby zresetować statystyki urządzenia możesz także kliknąć prawym przyciskiem myszy na danym urządzeniu i wybrać z menu kontekstowego opcję **Resetuj statystyki**.

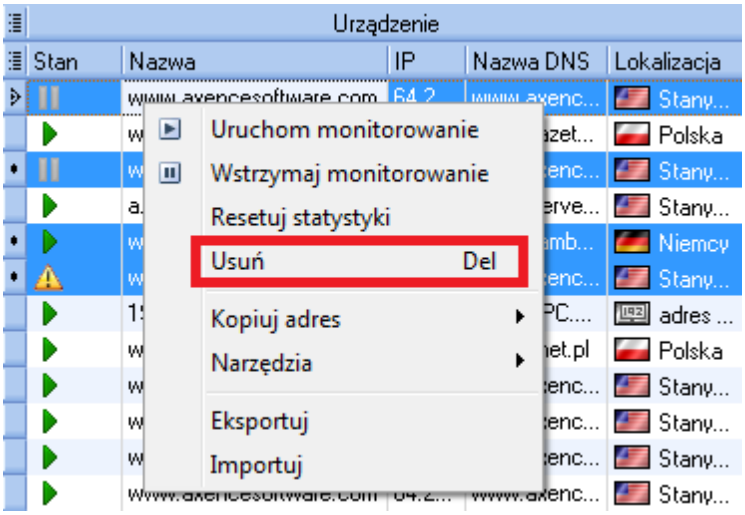


Usuwanie jednego lub więcej urządzeń

1. Wybierz w tabeli jedno lub więcej urządzeń.
2. Wybierz opcję **Usuń** znajdującą się w sekcji **Wybierz zadanie** na pasku bocznym.
3. Program zapyta, czy chcesz usunąć zgromadzone dane statystyczne dla wybranych urządzeń (czas odpowiedzi i % utraconych pakietów). Jeśli nie są Ci one już potrzebne, w oknie wiadomości wybierz **Tak**. Jeśli chcesz je zachować, odpowiedz: **Nie**. Jeśli zachowasz dane, będą dostępne po ponownym dodaniu tego samego urządzenia.

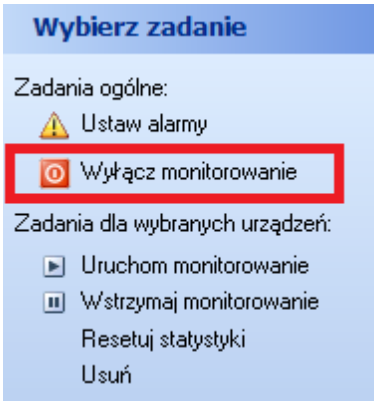


Aby usunąć urządzenia możesz także kliknąć prawym przyciskiem myszy na danym urządzeniu i wybrać z menu kontekstowego opcję **Usuń** lub wcisnąć klawisz **Del**.



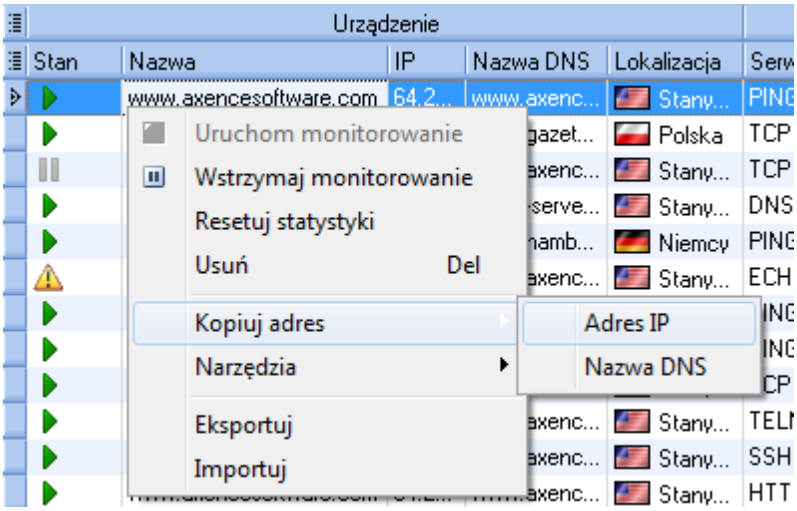
Wyłączanie/włączanie monitorowania wszystkich urządzeń

Możesz całkowicie wyłączyć monitorowanie, wybierając opcję **Wyłącz monitorowanie**, znajdującą się w dziale **Wybierz zadanie** na pasku bocznym. Nie zmieni to stanu żadnego urządzenia (aktywny/zatrzymany). Polecenie **Włącz monitorowanie** włącza monitorowanie z powrotem, po tym jak zostało ono wstrzymane.



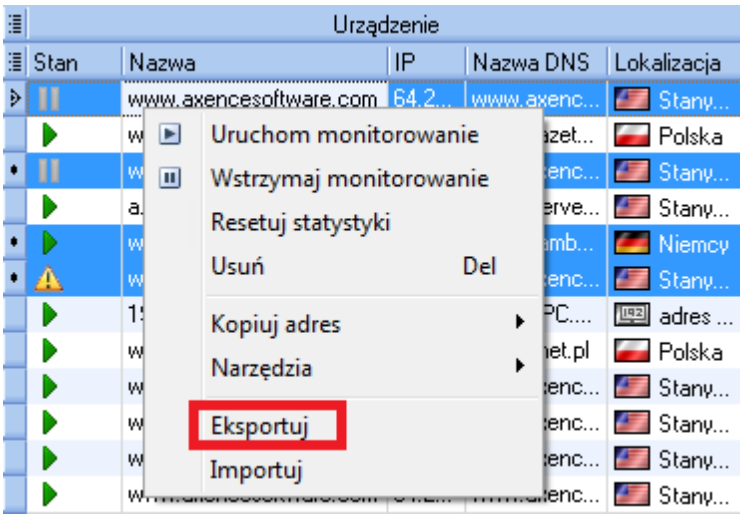
Kopiowanie nazwy DNS lub adresu IP do schowka

Możesz skopiować do schowka nazwę DNS lub adres IP wybranego urządzenia. Kliknij prawym przyciskiem myszki wybrane urządzenie w tabeli i wybierz **Kopiuj adres | Adres IP** lub **Kopiuj adres | Nazwa DNS** z menu kontekstowego.



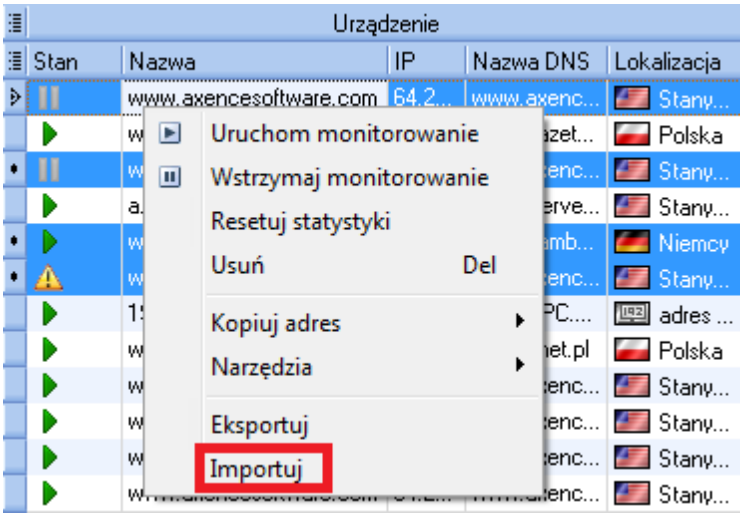
Eksportowanie danych

Aby wyeksportować tabelę zawierającą dane o urządzeniach, z menu kontekstowego wybierz opcję **Eksportuj**. Następnie wybierz jeden z formatów: **html**, **xml**, **txt**, **xls**, **json** (plik netTools). Jeśli chcesz wyeksportować jedynie listę adresów, wybierz opcję **Lista adresów (*.txt)**.



Importowanie danych

Możesz zaimportować do NetWatch dwa rodzaje danych: plik tekstowy z listą adresów i monitorowanych usług oraz plik programu netTools w formacie json. Aby wykonać import, z menu kontekstowego wybierz opcję **Importuj**.



Narzędzia

Z menu kontekstowego danego urządzenia można wywołać następujące narzędzia:

- Trace
- Lookup
- Zużycie łącza
- Wake On LAN

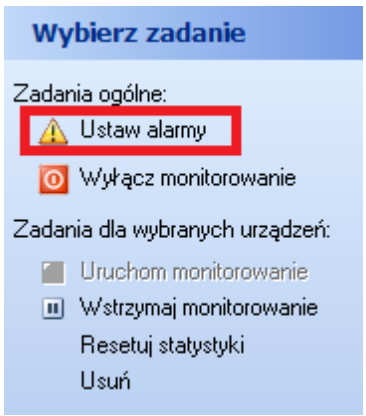
Aby dowiedzieć się więcej, przejdź do rozdziałów dotyczących tych funkcji.

3.2 Alarmy

3.2.1 Alarmy - informacje ogólne

W razie problemów z połączeniem lub monitorowanym urządzeniem, NetWatch może wysłać powiadomienie do administratora. Można zdefiniować kilka warunków kiedy alarm będzie zainicjowany i kilka akcji notyfikacyjnych. netTools może także powiadomić o zakończeniu problematycznej sytuacji - np. kiedy problematyczne urządzenie zacznie odpowiadać.

Aby włączyć alarm, wybierz opcję **Ustaw alarmy** znajdującą się w sekcji **Wybierz zadanie** na pasku bocznym.

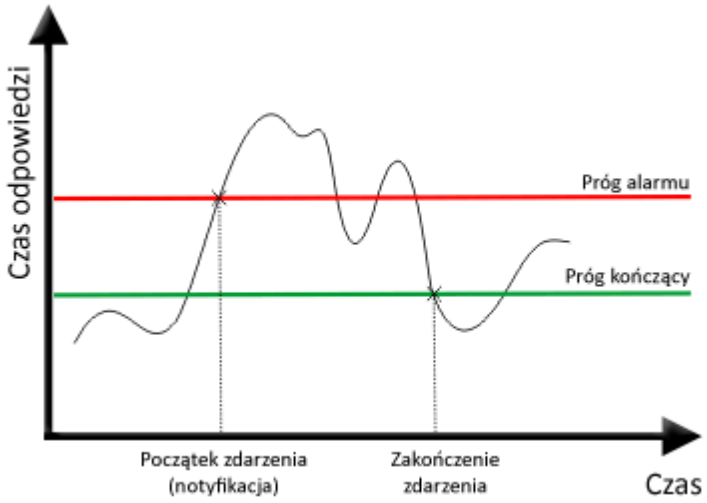


Kiedy alarm jest inicjowany?

Alarm może być inicjowany w 3 przypadkach (typy zdarzeń):

1. **Urządzenie nie odpowiada**. Oznacza, że urządzenie w ogóle nie odpowiada na sprawdzenia.
2. **Zbyt wiele utraconych pakietów**. Możesz zdefiniować procent utraconych pakietów, powyżej którego alarm będzie zainicjowany.
3. **Zbyt długi czas odpowiedzi**. Można ustawić wartość progową. Jeśli średni czas odpowiedzi przekroczy próg, zostanie zainicjowany alarm.

W punktach 2 i 3 definiowana jest wartość progu kończącego. Jest to ważne, ponieważ inaczej alarm byłby generowany za każdym razem, gdy warunki są spełnione. Oznaczałoby to generowanie alarmu co minutę. Dlatego mierzona wartość musi najpierw spaść poniżej progu kończącego, zanim następny alarm będzie mógł być zainicjowany. Przedstawia to poniższy wykres.



Czerwona linia oznacza próg alarmu. Kiedy czas odpowiedzi lub procent utraconych pakietów wzrośnie ponad ten próg, spowoduje to zainicjowanie alarmu. Jednak aby kolejny alarm mógł być zainicjowany, wartość ta musi spaść poniżej wartości progu kończącego. Zapobiega to generowaniu wielokrotnych alarmów dla tego samego zdarzenia.

Powiadomienie o przywróceniu połączenia

Dla każdego typu zdarzeń można włączyć notyfikację w razie jego zakończenia. Dla zdarzeń "Zbyt wiele utraconych pakietów" i "Zbyt długi czas odpowiedzi" należy zdefiniować próg kończący. Kiedy wartość spada poniżej progu, program uznaje, że zdarzenie się zakończyło. Zdarzenia "Urządzenie nie odpowiada" kończy się z chwilą odebrania odpowiedzi od urządzenia.

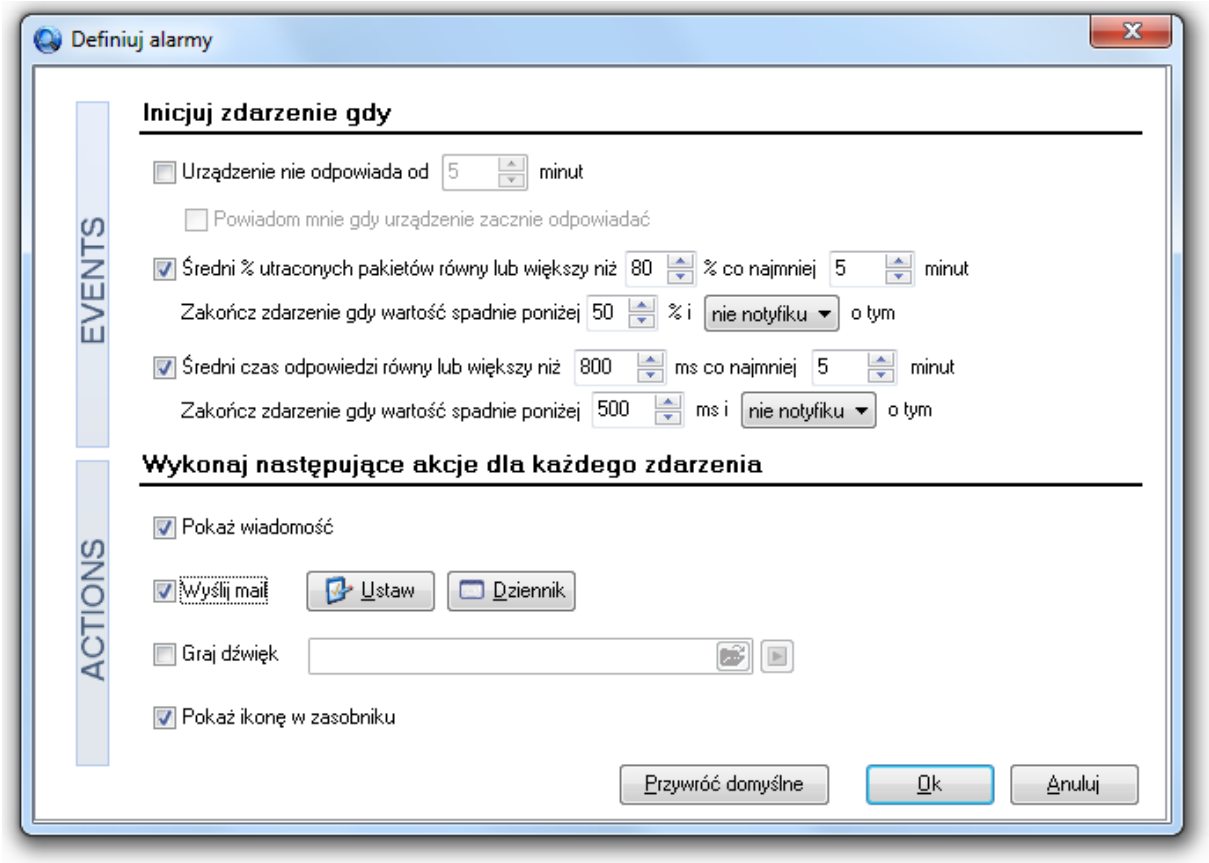
Po zakończeniu zdarzenia, jeśli notyfikacja została włączona, program wykona akcję notyfikacyjną.

Akcje

Możesz zdefiniować akcje, które będą wykonywane dla każdego zdarzenia. Dostępne są następujące akcje:

1. **Pokaż wiadomość**. W razie alarmu, netTools pokaże okno dialogowe pokazujące wszystkie alarmy.
2. **Wyślij mail**. netTools może wysłać e-mail do wielu adresów. E-mail ten zawiera nazwę urządzenia, adres oraz informację o zdarzeniu.

3. **Graj dźwięk**. W razie alarmu może być odegrany dźwięk.
4. **Pokaż ikonę w zasobniku**. W razie alarmu, ikona programu w zasobniku systemowym zmieni się na .



3.2.2 Ustawianie alarmów

Aby ustawić alarmy, należy zdefiniować warunki zdarzeń i skonfigurować akcje. Należy pamiętać, że zdefiniowane akcje wykonywane są dla każdego alarmu.

Aby ustawić alarmy

1. Wybierz narzędzie **NetWatch** na pasku nawigacyjnym.
2. Kliknij przycisk **Ustaw alarmy** w sekcji **Wybierz zadanie** na pasku bocznym.
3. Włącz zdarzenia dla których mają być generowane alarmy.
4. Włącz akcje do wykonania w razie alarmu.
5. Skonfiguruj zdarzenia i akcje według poniższego opisu.

Konfiguracja zdarzenia "Urządzenie nie odpowiada"

1. Zaznacz zdarzenie **Urządzenie nie odpowiada...**.
2. Wprowadź czas (w minutach), po którym zdarzenie zostanie rozpoczęte.

Konfiguracja zdarzenia "Zbyt wiele utraconych pakietów"

1. Zaznacz zdarzenie **Średni % utraconych pakietów...**.
2. Wprowadź wartość progową zdarzenia - zdarzenie zostanie rozpoczęte, gdy średni procent utraconych pakietów jest równy lub wyższy wartości progowej.
3. Wprowadź czas (w minutach), po którym zdarzenie zostanie rozpoczęte.
4. W drugiej linijce, wprowadź wartość progową kończącą zdarzenie. Zdarzenie zostanie zakończone, gdy procent utraconych pakietów spadnie poniżej tego progu.
5. Wybierz **notyfikuj** z rozwijanej listy, jeśli chcesz być powiadomiony o zakończeniu zdarzenia (gdy procent utraconych pakietów spadnie poniżej wartości progu kończącego).

Konfiguracja zdarzenia "Zbyt długi czas odpowiedzi"

1. Zaznacz zdarzenie **Średni czas odpowiedzi...**.
2. Wprowadź wartość progową zdarzenia - zdarzenie zostanie rozpoczęte, gdy średni czas odpowiedzi jest równy lub wyższy wartości progowej.
3. Wprowadź czas (w minutach), po którym zdarzenie zostanie rozpoczęte.
4. W drugiej linijce, wprowadź wartość progową kończącą zdarzenie. Zdarzenie zostanie zakończone, gdy czas odpowiedzi spadnie poniżej tego progu.
5. Wybierz **notyfikuj** z rozwijanej listy, jeśli chcesz być powiadomiony o zakończeniu zdarzenia (gdy czas odpowiedzi spadnie poniżej wartości progu kończącego).

Konfiguracja akcji

1. Zaznacz **Pokaż wiadomość**, jeśli chcesz, aby netTools pokazało okno dialogowe z listą alarmów dla każdego zdarzenia.
2. Zaznacz **Wyślij mail**, jeśli chcesz być powiadomiony e-mailem.
3. Jeśli włączyłeś powiadamianie e-mailem, musisz ustawić tą akcję.
4. Jeśli chcesz, aby dla każdego alarmu odtwarzany był dźwięk, zaznacz **Graj dźwięk**.
5. Jeśli wybrałeś powiadamianie dźwiękiem, wprowadź nazwę pliku lub plik dźwiękowy. Możesz kliknąć ikonę znajdującą się po prawej stronie, aby wybrać plik.
6. Jeśli wybrałeś **Pokaż ikonę w zasobniku**, netTools będzie pokazywał ikonę:  w zasobniku systemowym podczas każdego zdarzenia.

Konfiguracja akcji e-mailowej

1. Otwórz okno **Definiuj alarmy** i kliknij **Ustaw**.
2. W polu **Wyślij powiadomienie do** wprowadź listę adresów, na które chcesz wysyłać wiadomość. Każdy adres powinien być w oddzielnej linijce.
3. Wprowadź adres serwera pocztowego (SMTP/POP3).
4. Jeśli serwer wymaga autoryzacji, zaznacz odpowiednią opcję i wprowadź odpowiednio swoją nazwę użytkownika i hasło w polach **Nazwa użytkownika/Hasło**.
5. Wybierz opcje **Szyfrowania** (Bez szyfrowania, SSL v2/v3 lub TLS).
6. Wprowadź **Adres zwrotny** (prawdopodobnie będzie to Twój adres e-mail). Jest to bardzo ważne - jeśli adres nie jest prawidłowo ustawiony, niektóre serwery pocztowe mogą odrzucić e-mail.
7. Teraz kliknij przycisk **Test** i sprawdź, czy dostałeś e-mail. Jeśli nie, sprawdź ustawienia opcji.

Część IV

4 WinTools

4.1 WinTools

Narzędzie to ma na celu przedstawianie wyczerpującej informacji o komputerach Windows (za pomocą WMI). Zawiera kilka predefiniowanych zapytań pozwalających odczytywać listę usług, informację o dyskach, procesach, itp. Można także definiować własne zapytania. Aby móc użyć tego narzędzia, na zdalnym komputerze musi być dostępny protokół WMI - przejdź do rozdziału Włączanie WMI na zdalnych komputerach aby dowiedzieć się jak włączyć WMI.

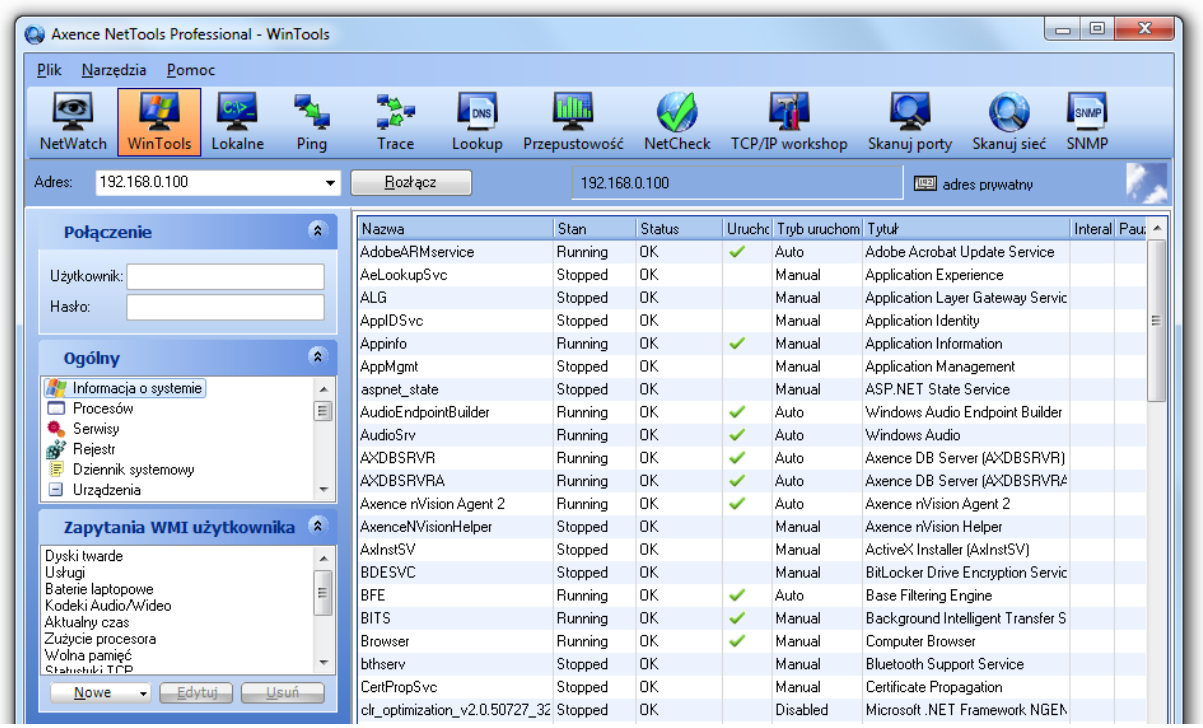
Aby użyć WinTools

1. Wybierz narzędzie **WinTools** na pasku nawigacyjnym.
2. Wpisz nazwę użytkownika (dla użytkowników domenowych należy użyć formatu użytkownik@domena) i hasło w grupie **Połączenie**. Jest to konieczne, aby odczytać dane WMI z komputera Windows. Może to nie być konieczne, jeśli już jesteś do tego komputera zalogowany.

Udostępniane informacje

Możesz zobaczyć wiele informacji wybierając właściwe zadanie w sekcji **Zadania** na pasku bocznym. Wiele predefiniowanych tabel znajduje się w grupach **Ogólne** i **Zapytania WMI**.

Możesz zdefiniować własne zapytania WMI aby uzyskać potrzebną informację. Kliknij przycisk **Nowe**, poniżej grupy **Zapytania WMI**. Pozwoli to na zdefiniowanie zapytania za pomocą wizualnego konstruktora zapytań. Można także wpisać zapytanie WMI ręcznie - kliknij strzałkę obok przycisku **Nowe** i wybierz **Podaj zapytanie**.



4.2 Włączanie WMI na zdalnych komputerach

Udostępnianie monitorowania liczników Windows

Protokół WMI (używany przez WinTools, zbieranie informacji o zasobach i monitorowanie liczników wydajności Windows) jest dostępny na Windows 2003 Server. Jednak aby uzyskać informację z komputerów z Windows XP Professional, Vista, Windows 7 i nowszych, należy wykonać kilka czynności. Aby je przyśpieszyć przygotowaliśmy program (WMIEnable.exe), który automatycznie wykona niezbędne operacje. Aby udostępnić WMI, należy uruchomić ten program na zdalnym komputerze. Można uruchomić go ze skryptu logowania, co zapewni dostępność WMI na wszystkich urządzeniach z Windows w sieci. Jeśli używasz jakiejkolwiek dodatkowej zapory na zdalnym komputerze, musisz otworzyć następujące porty: TCP 135, 139, 445, 593.

Aby używać WinTools lub odczytać zasoby z Windows XP Home należy pamiętać, że system zdalny musi mieć dokładnie te same dane logowania (nazwę użytkownika i hasło) co użytkownik zalogowany na komputerze gdzie działa netTools i nVision.

WMIEnable

Program ten udostępnia WMI na Windows. Poniżej znajduje się lista operacji wykonywanych przez program:

1. DCOM jest włączany przez ustawienie klucza rejestru [HKEY_LOCAL_MACHINE\Software \Microsoft\OLE\EnableDCOM] na wartość "Y".
2. Zdalny UAC na Windows Vista jest włączany przez ustawienie klucza rejestru [HKLM\SOFTWARE \Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy] na wartość 1.
3. Porty WMI (TCP 135,139,445,593) są otwierane na zaporze Windows przez wykonanie komendy: netsh firewall set service RemoteAdmin
4. Dostęp do WMI na Windows Vista jest udostępniany przez dodanie wyjątku zapory dla "Windows Management Instrumentation (WMI)".
5. Model autoryzacji jest ustawiany na "Local user authorize as themselves" przez ustawienie wartości klucza rejestru [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\forceguest] na wartość 0.

Zwykle restart systemu nie jest konieczny a WMI będzie dostępne zaraz po wykonaniu programu, można jednak wymusić restart systemu przez uruchomienie programu z parametrem **/restart**. Program nie dokona restartu jeśli ustawienie parametrów systemu się nie powiodło.

Jeśli WMI dalej nie działa

Jeśli WMI nie działa pomimo uruchomienia programu WMIEnable, należy sprawdzić:

1. Uruchom Local Security Settings (secpol.msc /s) wybierz Local Policies -> User Rights Assignement -> Access this computer from network. Sprawdź czy wszystkie właściwe grupy/ użytkownicy są dodani. Przynajmniej grupa Administrators lub Administrator powinni być dodani.
2. Uruchom Group Policy (gpedit.msc) i wybierz Windows Settings -> Security Settings -> Local Policies -> Security Options -> Network access: Sharing and security model for local accounts. Ustaw tą opcję na "Classic - local user authorize as themselves".
3. Sprawdź czy WMI działa przez wywołanie komendy : "**wbemtest**". WMI działa jeśli program ten działa poprawnie.
4. Sprawdź, czy następujące serwisy są uruchomione:
   COM+ Event System
   Remote Access Auto Connection Manager
   Remote Access Connection Manager

Remote Procedure Call (RPC)
Remote Procedure Call (RPC) Locator
Remote Registry
Server
Windows Management Instrumentation
Windows Management Instrumentation Driver Extensions
WMI Performance Adapter
Workstation

Wycieki pamięci przez starą wersjęRpcrt4.dll

W razie monitorowania liczników wydajności Windows, należy upewnić się, że zainstalowana jest najnowsza wersja pliku Rpcrt4.dll. Wszystkie poprzednie wersje powodują poważne wycieki pamięci w systemie, co może doprowadzić do awarii systemu. Problem ten jest opisany przez Microsoft na stronie http://support.microsoft.com/?kbid=911262
Dla Windows XP plik Rpcrt4.dll powinien być w wersji 5.2.3790.2900 lub wyższej.

4.3 WinTools nie działa

Rozdział ten wyjaśnia, dlaczego WinTools nie może podłączyć się do zdalnego komputera i co zrobić, aby wykonać powyższe zadania.

Dlaczego netTools tego nie wykonuje

WinTools podłącza sie za pomocą protokołu WMI. Musi on więc być uruchomiony i dostępny na zdalnym komputerze. Musisz upewnić się, że serwisy WMI są uruchomione, model autoryzacji jest prawidłowo ustawiony i że wszystkie wymagane porty są otwarte na zaporze. Kluczowe jest także podanie danych logowania urządzenia (nazwa użytkownika i hasło - dla użytkowników domenowych należy użyć formatu użytkownik@domena).

Na komputerach z Windows XP Professional i nowszymi systemami Windows WMI jest zablokowane przez zaporę i niewłaściwy model autoryzacji. Aby zautomatyzować wykonanie tych zadań, przygotowaliśmy specjalny program (WMIEnable.exe), który wykonuje wszystkie konieczne operacje. Aby dowiedzieć się więcej o WMIEnable.exe, przejdź do rozdziału Włączanie WMI.

Jak wykonać te zadania

Oto lista kroków, które musisz wykonać, aby uruchomić WMI:

1. **Uruchom WMIEnable.exe na zdalnym komputerze.**
   Znajduje się on w katalogu programu i należy go skopiować na zdalny komputer. Program ten wykonuje następujące czynności:
   - Włącza DCOM
   - Włącza Zdalny UAC na Windows Vista
   - Ustawia model autoryzacji na "Local user authorize as themselves"
   - Konfiguruje zaporę Windows tak, aby otworzyć wszystkie porty WMI.
2. **Otwórz porty WMI, jeśli jest to konieczne**
   Jeśli używasz jakiejkolwiek dodatkowej zapory na zdalnym komputerze, musisz otworzyć następujące porty: TCP 135, 139, 445, 593.
3. **Konfiguruje dane logowania.**
   Wpisz nazwę użytkownika i hasło (dla użytkowników domenowych należy użyć formatu użytkownik@domena). Naciśnij Enter. Program będzie próbował połączyć się ze zdalnym komputerem przez WMI i poinformuje, jaki jest tego rezultat.

Jeśli w dalszym ciągu funkcja nie działa

Przejdź do rozdziału Włączanie WMI na zdalnych komputerach, aby dowiedzieć się, jak ustalić przyczynę problemów.

Część V

5 Lokalne

5.1 Wprowadzenie

Narzędzie pokazuje kilka tabel z ważnymi informacjami o lokalnej konfiguracji: statystyki sieciowe dla TCP/UDP i ICMP, tabelę adresów IP, tabelę ARP i routingu IP, informacje o kartach sieciowych.

Aby zobaczyć lokalne informacje

1. Wybierz narzędzie **Lokalne** na pasku nawigacyjnym.
2. Wybierz właściwe zadanie, aby zobaczyć odpowiednie informacje: NetStat aby zobaczyć lokalne połączenia TCP/IP, lokalne informacje IP, tabele ARP i routingu lub statystyki.

Udostępniane informacje

Możesz zobaczyć kilka tabel, wybierając właściwe zadanie na pasku bocznym:

- NetStat - lista lokalnych połączeń
- Lokalna informacja IP - tabela adresów IP, interfejsy, karty sieciowe
- Tabela ARP i routingu - tabela ARP, tabela routingu
- Statystyki TCP/UDP/ICMP

Opcje

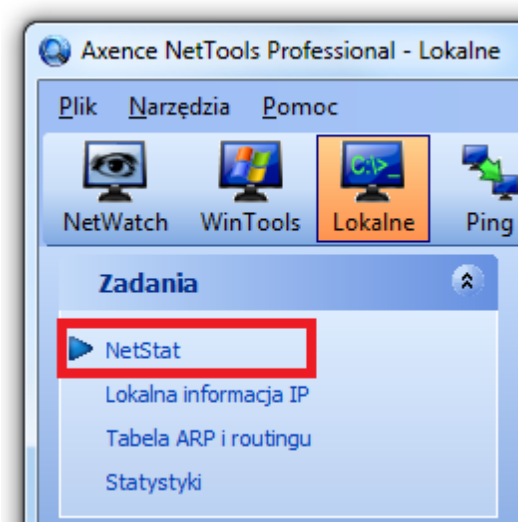
Możesz dostosować czas odświeżania. Wpisz wartość w sekcji **Opcje** na pasku bocznym.

5.2 NetStat

Narzędzie to zastępuje standardowe polecenie linii komend Windows - NetStat. Prezentuje wszystkie przychodzące i wychodzące połączenia z komputera i pokazuje wszystkie otwarte porty. Dodatkowo otwarte porty i połączenia mapowane są na aplikacje, które ich używają.

Aby rozpocząć monitorowanie połączeń

1. Wybierz narzędzie **Lokalne** info na pasku nawigacyjnym.
2. Wybierz **NetStat** na pasku bocznym.



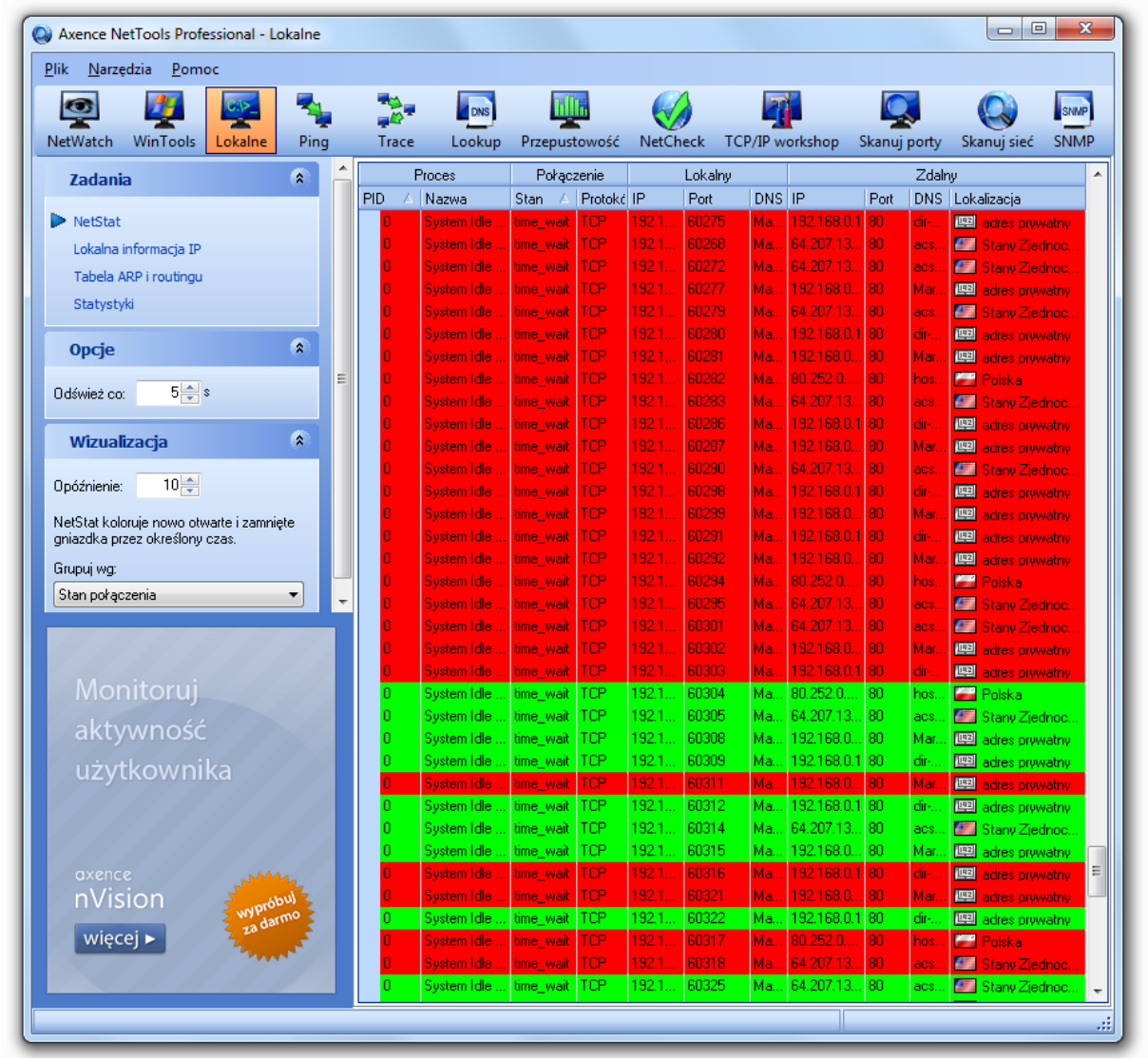
Udostępniane informacje

W głównej tabeli możesz zobaczyć wszystkie przychodzące i wychodzące połączenia. Dostępny jest też ID procesu oraz jego nazwa, protokół i stan połączenia, lokalny i zdalny adres IP/port, a także lokalizacja zdalnego adresu IP (opcja ta może ułatwić wykrycie podejrzanych połączeń).

W razie pojawiania się nowego połączenia, NetStat wyświetla je w kolorze zielonym. Podobnie, połączenia zamknięte pokazane są na czerwono, a następnie usuwane z tabeli.

Opcje

Możesz zmienić tempo odświeżania. Wpisz żądaną wartość w sekcji **Opcje** na pasku bocznym. Można zmienić także czas wyświetlania wierszy w kolorze.
Dane w tabeli można grupować i filtrować. Aby włączyć grupowanie, wybierz właściwe grupowanie w pasku bocznym wizualizacji. Aby filtrować dane, użyj strzałki obok nagłówka każdej kolumny.



Uwagi

- Połączenia UDP nie mają stanu oraz lokalnego adresu IP ze względu na swoją naturę.
- Aby skopiować do schowka zdalny adres IP lub zdalną nazwę DNS, kliknij prawym przyciskiem na

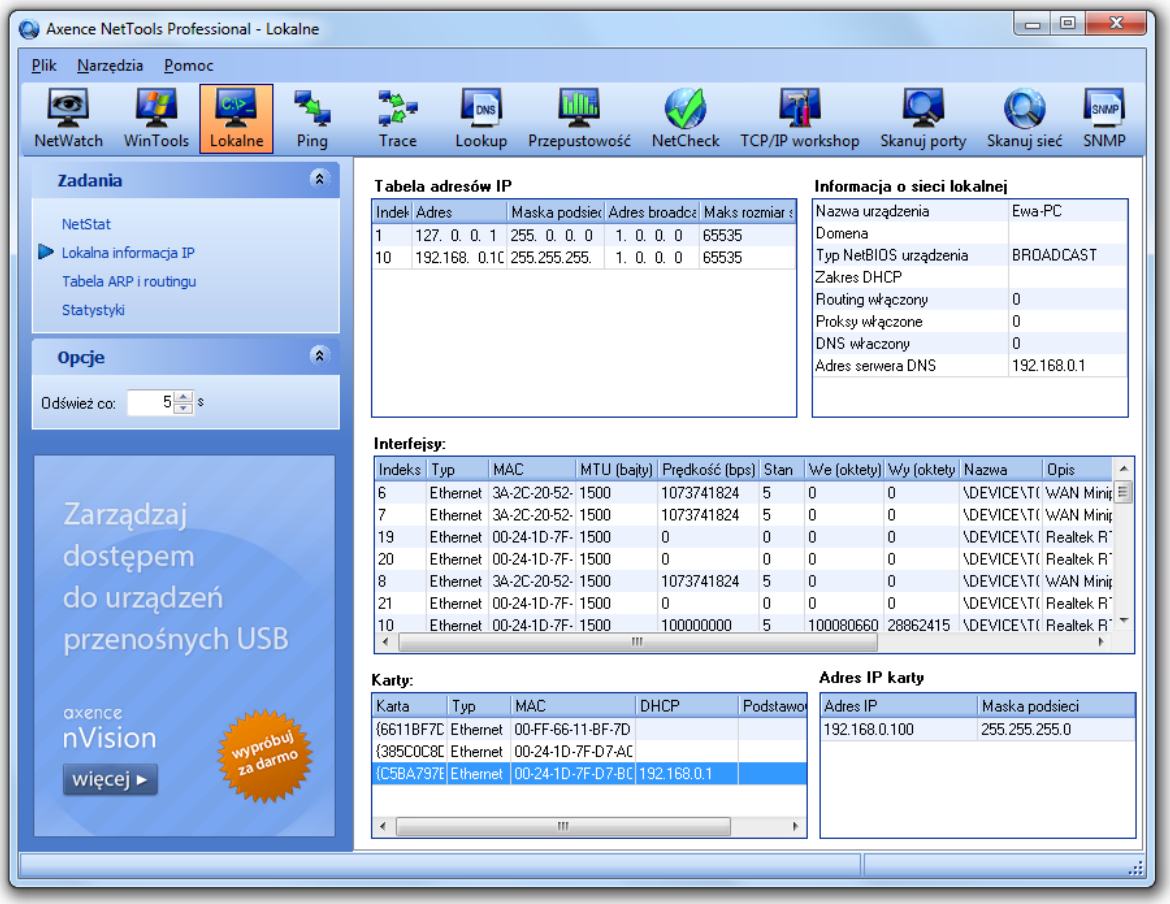
danym wierszu w tabeli i wybierz odpowiednią opcję z menu kontekstowego.

5.3 Lokalna informacja IP

Narzędzie pokazuje kilka tabel z ważnymi informacjami o lokalnej konfiguracji: tabelę adresów IP, informacje o sieci lokalnej, interfejsy oraz karty sieciowe.

Aby zobaczyć lokalne informacje IP

1. Wybierz narzędzie **Lokalne** info na pasku nawigacyjnym.
2. Wybierz opcję **Lokalna informacja IP** na pasku bocznym.



Uwagi

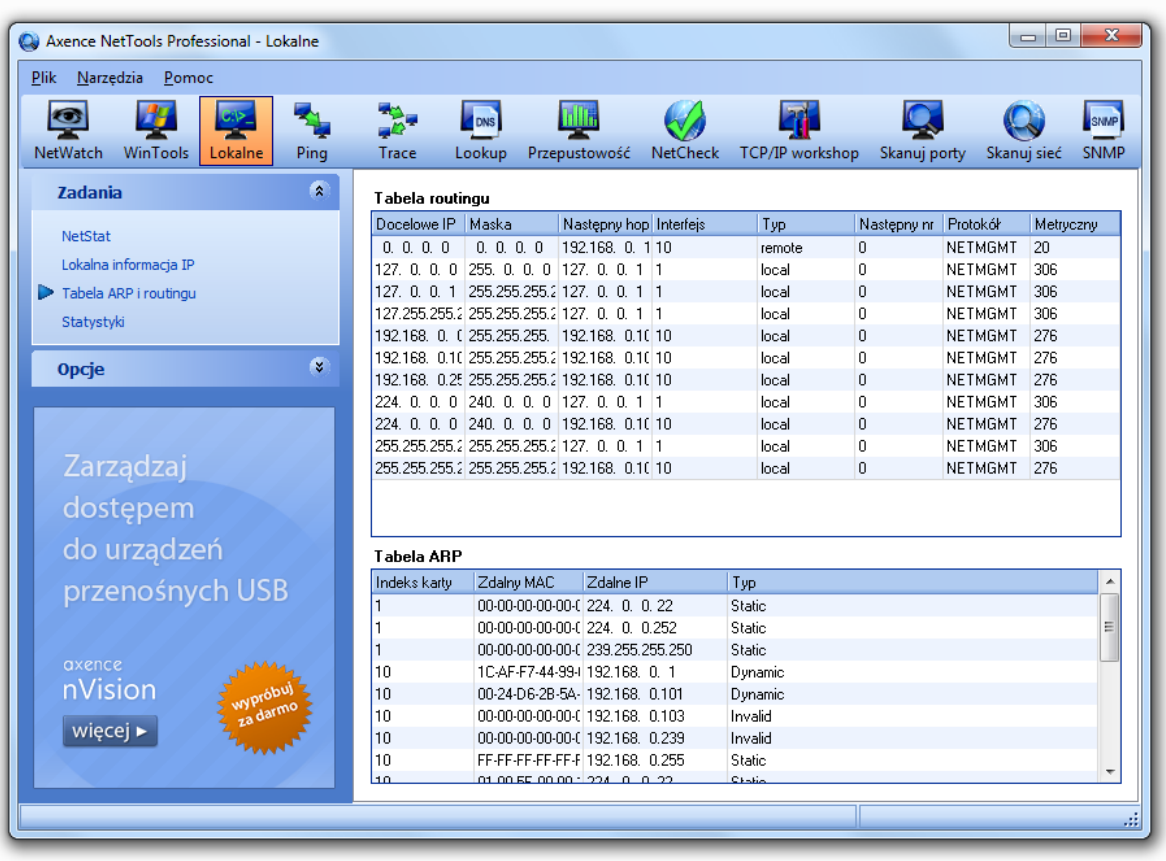
- Aby skopiować do schowka adres IP, kliknij prawym przyciskiem na danym wierszu w tabeli adresów IP i wybierz z menu kontekstowego opcję **Skopiuj adres IP**.
- Z poziomu menu kontekstowego możesz także skorzystać z opcji **Wake On LAN**. Aby dowiedzieć się więcej, przejdź do rozdziału Jak korzystać z opcji Wake On LAN?.

5.4 Tabela ARP i routingu

Narzędzie pokazuje tabelę routingu oraz tabelę ARP. Dane zawarte w tabeli ARP są wykorzystywane także przez narzędzie Skanuj sieć, do uzupełnienia adresów MAC

Aby zobaczyć tabele ARP i routingu

1. Wybierz narzędzie **Lokalne** info na pasku nawigacyjnym.
2. Wybierz opcję **Tabela ARP i routingu** na pasku bocznym.



Uwagi

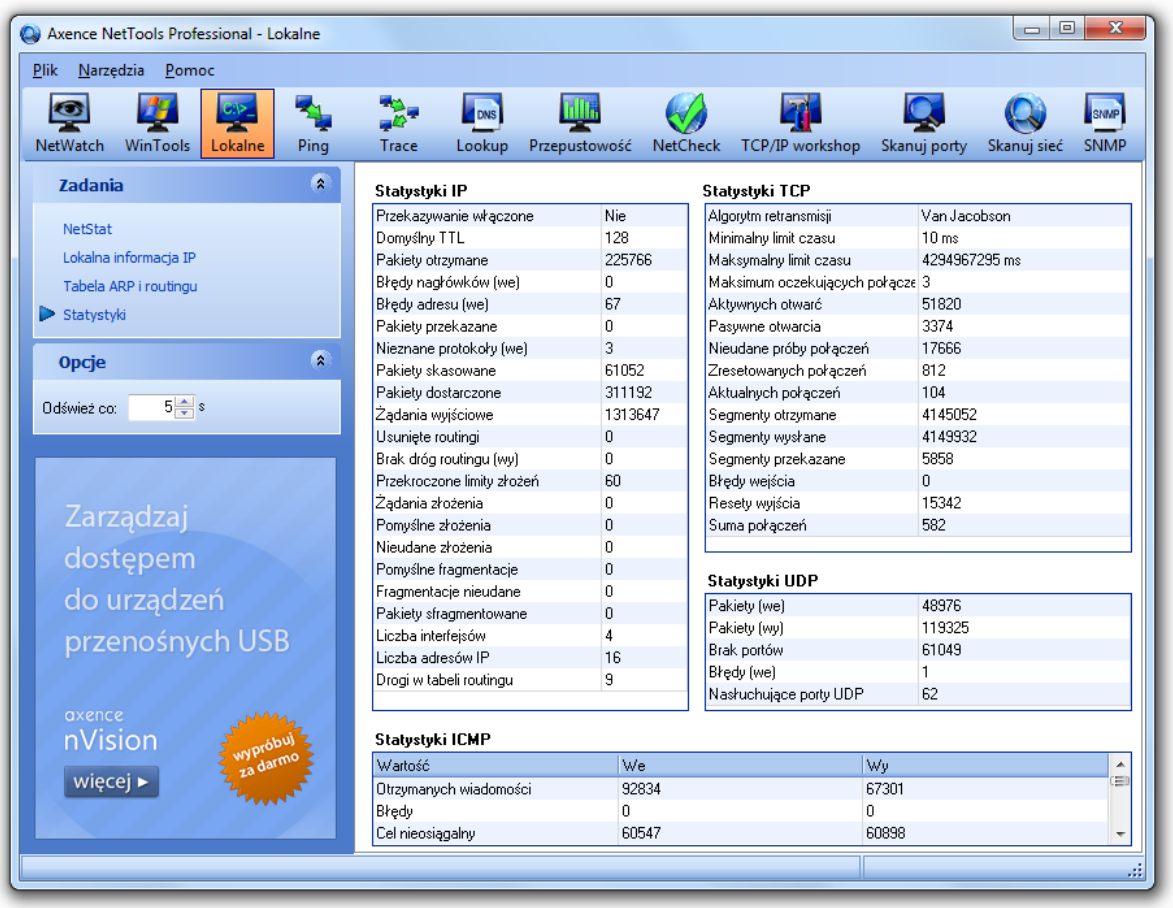
- Aby skopiować do schowka adres IP, kliknij prawym przyciskiem na danym wierszu w tabeli i wybierz z menu kontekstowego opcję **Skopiuj adres IP**.
- Z poziomu menu kontekstowego możesz także skorzystać z opcji **Wake On LAN**. Aby dowiedzieć się więcej, przejdź do rozdziału Jak korzystać z opcji Wake On LAN?.

5.5 Statystyki

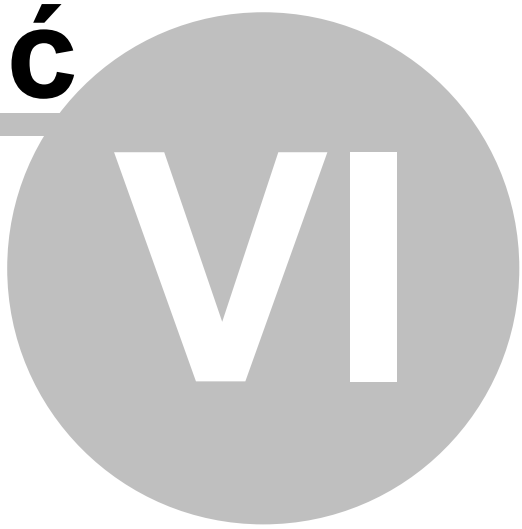
Narzędzie pokazuje tabele z informacjami dotyczącymi statystyk IP, TCP, UDP i ICMP.

Aby zobaczyć statystyki

1. Wybierz narzędzie **Lokalne** info na pasku nawigacyjnym.
2. Wybierz opcję **Statystyki** na pasku bocznym.



Część



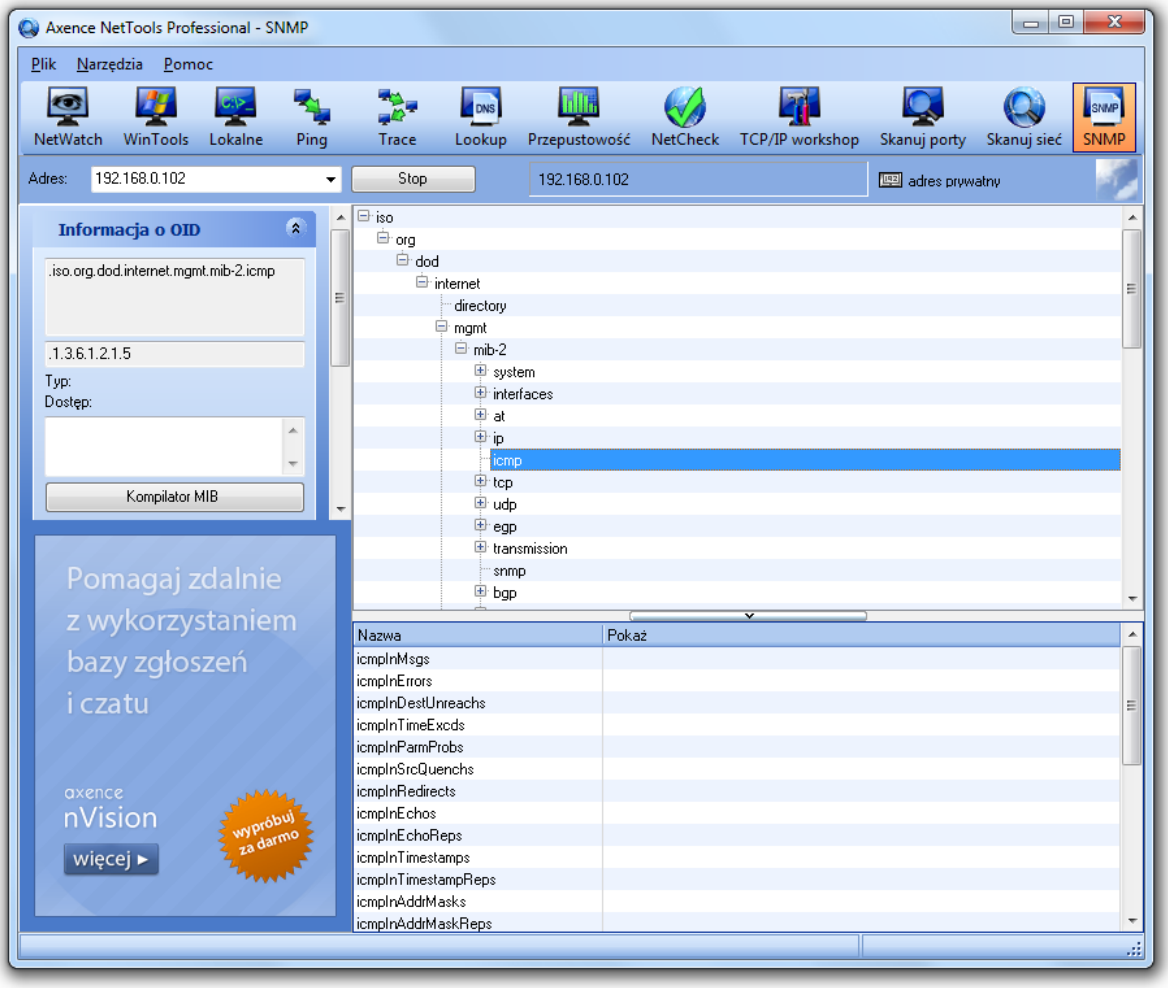
6 SNMP

6.1 SNMP

Narzędzie SNMP pozwala przeglądać drzewo SNMP OID i odczytywać te informacje z urządzenia. Informacja ta udostępniana jest przez agenty SNMP, które muszą być dostępne na monitorowanych urządzeniach.

Aby otrzymać informację SNMP

1. Na pasku nawigacyjnym wybierz narzędzie **SNMP**.
2. Wpisz **adres DNS** lub **IP** urządzenia w pasku adresu.
3. Wybierz w drzewie MIB kategorię OID, którą chcesz odczytać.
4. Kliknij przycisk **Sprawdź** lub naciśnij **Enter**.



Udostępniane informacje

Program pokazuje wszystkie OID'y dostępne w wybranej kategorii. Jeśli jest to tabela, wtedy wszystkie wiersze i kolumny będą pokazane (można wtedy zmieniać rozmiar i kolejność kolumn).

Ogólna informacja o każdym OID'dzie pokazana jest na pasku bocznym: nazwa OID, typ, dostęp i krótki opis.

Klikając w przycisk **Kompilator MIB** możesz dodać nowy obiekt bazy MIB w celu obsługi dowolnych nowych urządzeń SNMP. Aby dowiedzieć się więcej, przejdź do rozdziału Kompilator plików MIB.

Opcje

Opcje dostępne na pasku bocznym pozwalają zmienić wspólnotę, czas odświeżania oraz limit czasu odpowiedzi. Wspólnota jest hasłem używanym przez protokół SNMP. Musisz podać ten sam ciąg znaków, jaki ma agent SNMP na urządzeniu, które jest sprawdzane. W razie podania błędnej wspólnoty nie uda się odczytać żadnych danych SNMP.

Uwagi

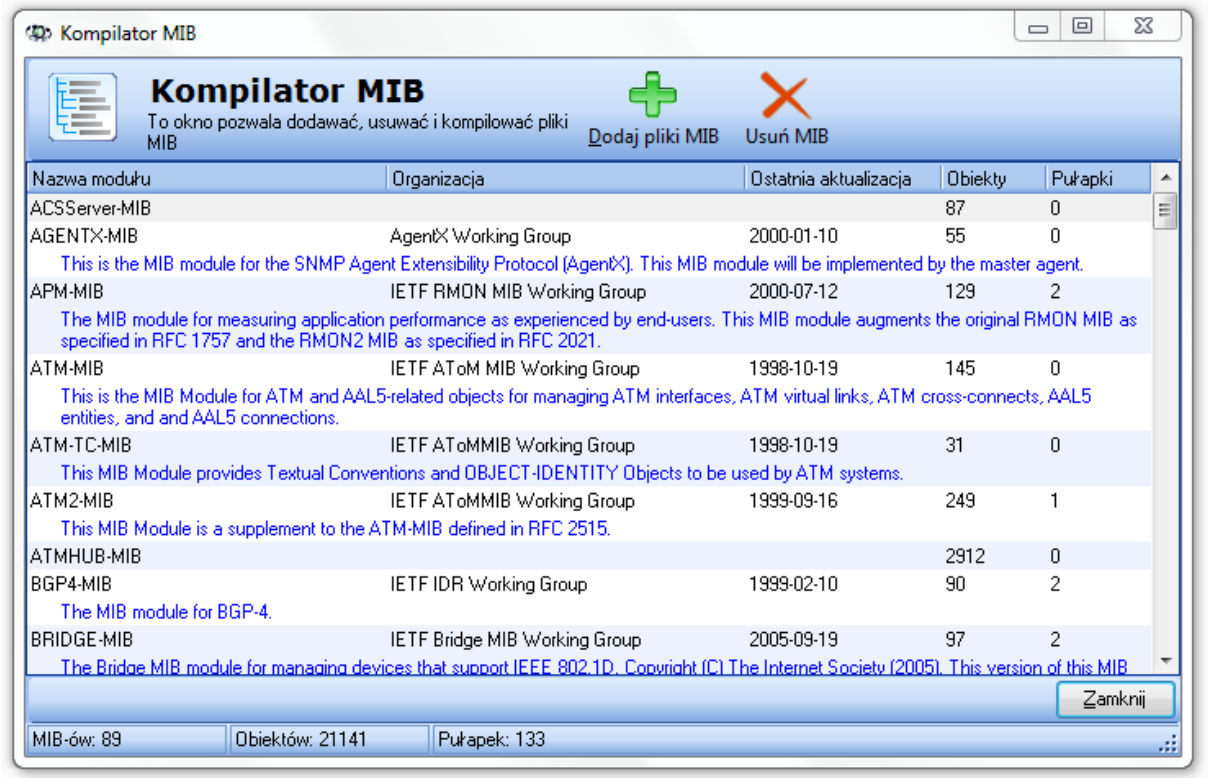
- Po prawej stronie paska adresu, możesz zobaczyć nazwę i IP urządzenia, które jest sprawdzane. Można je łatwo skopiować do schowka. Kliknij to pole prawym klawiszem i wybierz z menu kontekstowego **Kopiuj adres IP** lub **Kopiuj nazwę DNS**.
- Obok nazwy urządzenia znajduje się informacja o lokalizacji geograficznej (w postaci kraju) zdalnego adresu IP.

6.2 Kompilator plików MIB

Kompilator plików MIB pozwala na dodawanie nowych plików MIB, ich usuwanie i kompilowanie. Ułatwia gromadzenie informacji ze wszystkich urządzeń sieciowych: przełączników, routerów, drukarek, urządzenia VoIP itp. Program może skutecznie monitorować tysiące różnych urządzeń SNMP.

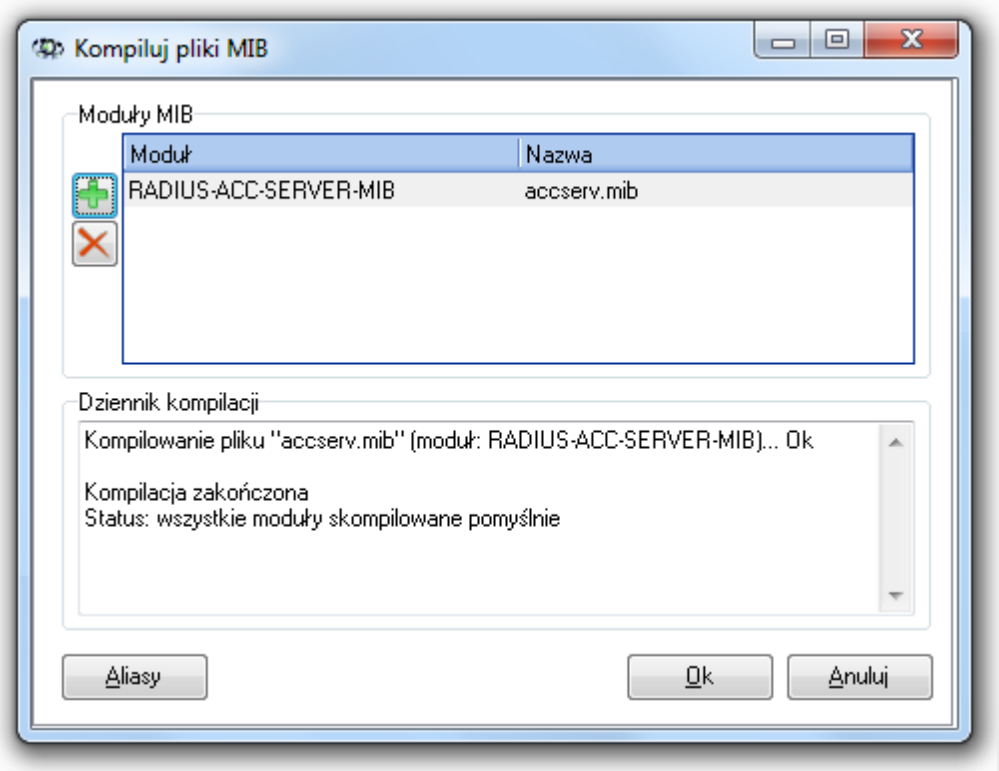
Aby korzystać z kompilatora MIB:

1. Wybierz opcję **Narzędzia | Kompilator MIB**. Okno kompilatora MIB zostanie otwarte.



2. Jeśli chcesz dodać nowy plik, kliknij na przycisk 

.
3. Dodaj moduł MIB, klikając na przycisk  i wybierając plik z jego lokalizacji. Dziennik kompilacji pojawia się po kompilacji.



4. Można również zdefiniować aliasy w Edytorze aliasów (przycisk **Aliasy**).

Część VII

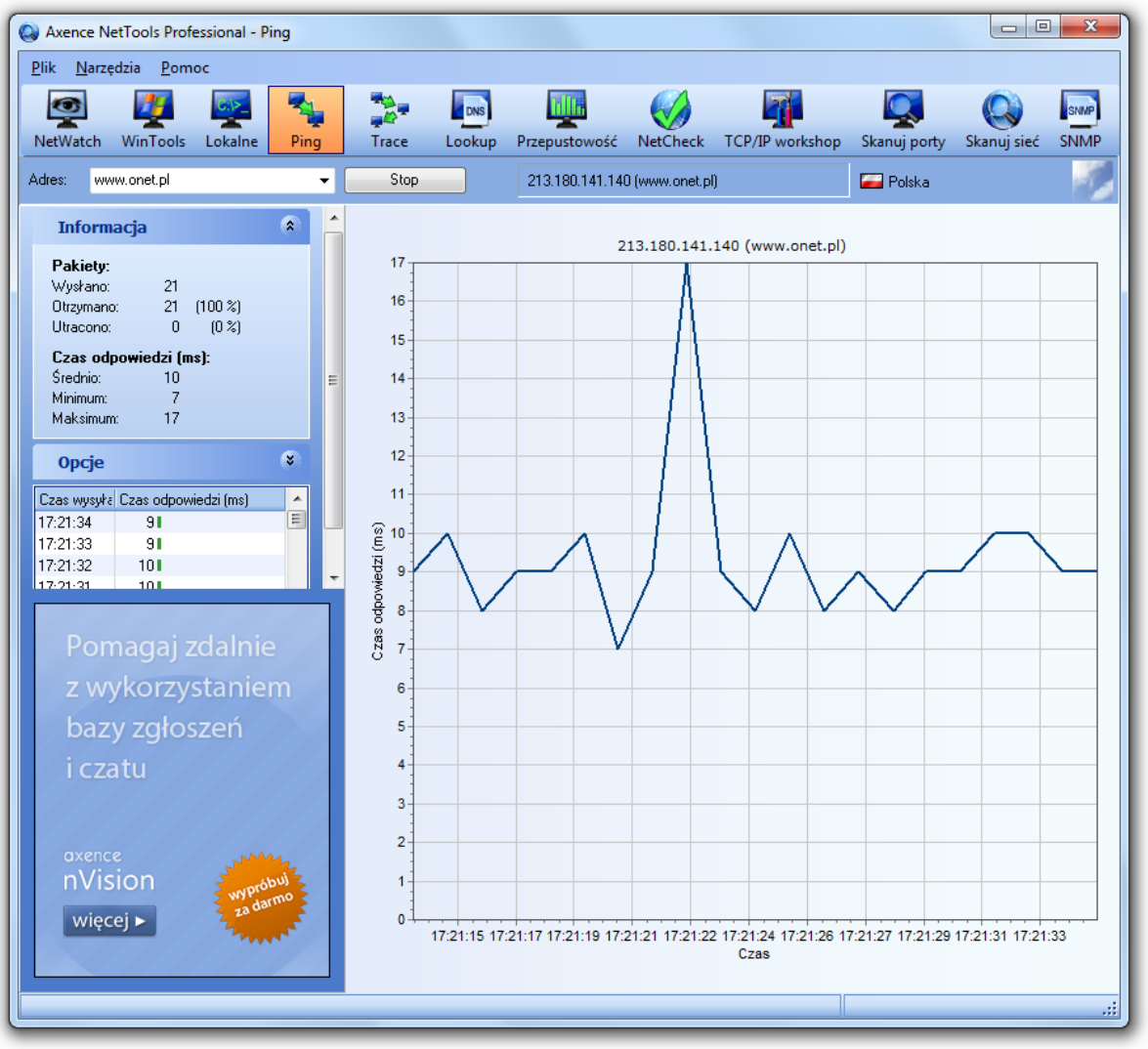
7 Inne narzędzia

7.1 Ping

Narzędzie Ping pozwala szybko sprawdzić połączenie z urządzeniem. Wysyła pakiety ICMP i pokazuje czas odpowiedzi i liczbę utraconych pakietów.

Aby rozpocząć monitorowanie

1. Na pasku nawigacyjnym wybierz narzędzie **Ping**.
2. Wpisz **adres DNS** lub **IP** urządzenia w pasku adresu.
3. Kliknij przycisk **Sprawdź** lub naciśnij **Enter**.



Udostępniane informacje

Na głównym wykresie można zobaczyć zmierzoną przepustowość dla ostatnich 5 minut. Aby zobaczyć dokładne wartości w milisekundach, skorzystaj z tabeli znajdującej się na pasku bocznym.

Na pasku bocznym znajduje się też ogólna, zbiorcza informacja: liczba pakietów wysłanych oraz min/max/średni czas odpowiedzi w milisekundach.

Opcje

Można dostosować częstotliwość pomiarów, rozmiar pakietu oraz limit czasu odpowiedzi. Podaj dane w sekcji **Opcje** na pasku bocznym. Zmiana rozmiaru pakietu wpływa na wyniki. Niektóre urządzenia mogą nie akceptować zbyt dużych pakietów. Dla takich pakietów należy też ustawić dłuższy limit czasu.

Eksportowanie

Aby wyeksportować graficzny plik z wykresem PING:

1. Kliknij prawym przyciskiem myszy na wykresie, kliknij **Eksportuj**.
2. Wpisz nazwę pliku i wybierz format pliku: **bmp**, **emf** lub **wmf**. **Zapisz** plik.

Uwagi

- Ping zapisuje czas odpowiedzi dla ostatnich 5 minut. Dlatego cały wykres reprezentuje 5 minut. Aby monitorować urządzenie dłuższy czas, użyj narzędzia NetWatch.
- Po prawej stronie paska adresu, możesz zobaczyć nazwę i IP urządzenia, które jest sprawdzane. Można je łatwo skopiować do schowka. Kliknij to pole prawym klawiszem i wybierz z menu kontekstowego **Kopiuj adres IP** lub **Kopiuj nazwę DNS**.
- Możesz łatwo otworzyć ten adres w innym narzędziu netTools wybierając z menu kontekstowego jedną z opcji: **Dodaj do NetWatch**, **Trace**, **Lookup**, **Zużycie łącza**.
- Obok nazwy urządzenia znajduje się informacja o lokalizacji geograficznej (w postaci kraju) zdalnego adresu IP.

7.2 Trace

Narzędzie Trace pozwala sprawdzić połączenie do urządzenia. W razie problemów zobaczysz który hop powoduje problemy. Trace pokazuje czas odpowiedzi oraz ilość utraconych pakietów dla każdego urządzenia po drodze, aby można było szybko zlokalizować problematyczne urządzenia. W dolnej części okna umieszczona jest graficzna mapa kolejnych hostów na trasie pakietów.

Aby rozpocząć sprawdzenie drogi do urządzenia

1. Na pasku nawigacyjnym wybierz narzędzie **Trace**.
2. Wpisz **adres DNS** lub **IP** urządzenia w pasku adresu.
3. Kliknij przycisk **Sprawdź** lub naciśnij **Enter**.

Udostępniane informacje

W głównej tabeli dostępna jest ogólna informacja o każdym urządzeniu: numer, nazwa DNS i adres IP, lokalizacja, czas odpowiedzi (min/max/średni), oraz liczba wysłanych pakietów.

Liczba wykonanych testów jest dostępna w sekcji **Opcje** na pasku bocznym.

Opcje

Można dostosować częstość wykonywania sprawdzenia, limit czas oraz liczbę hopów (TTL - time to live). Liczba hopów określa maksymalną liczbę urządzeń, która będzie sprawdzona.

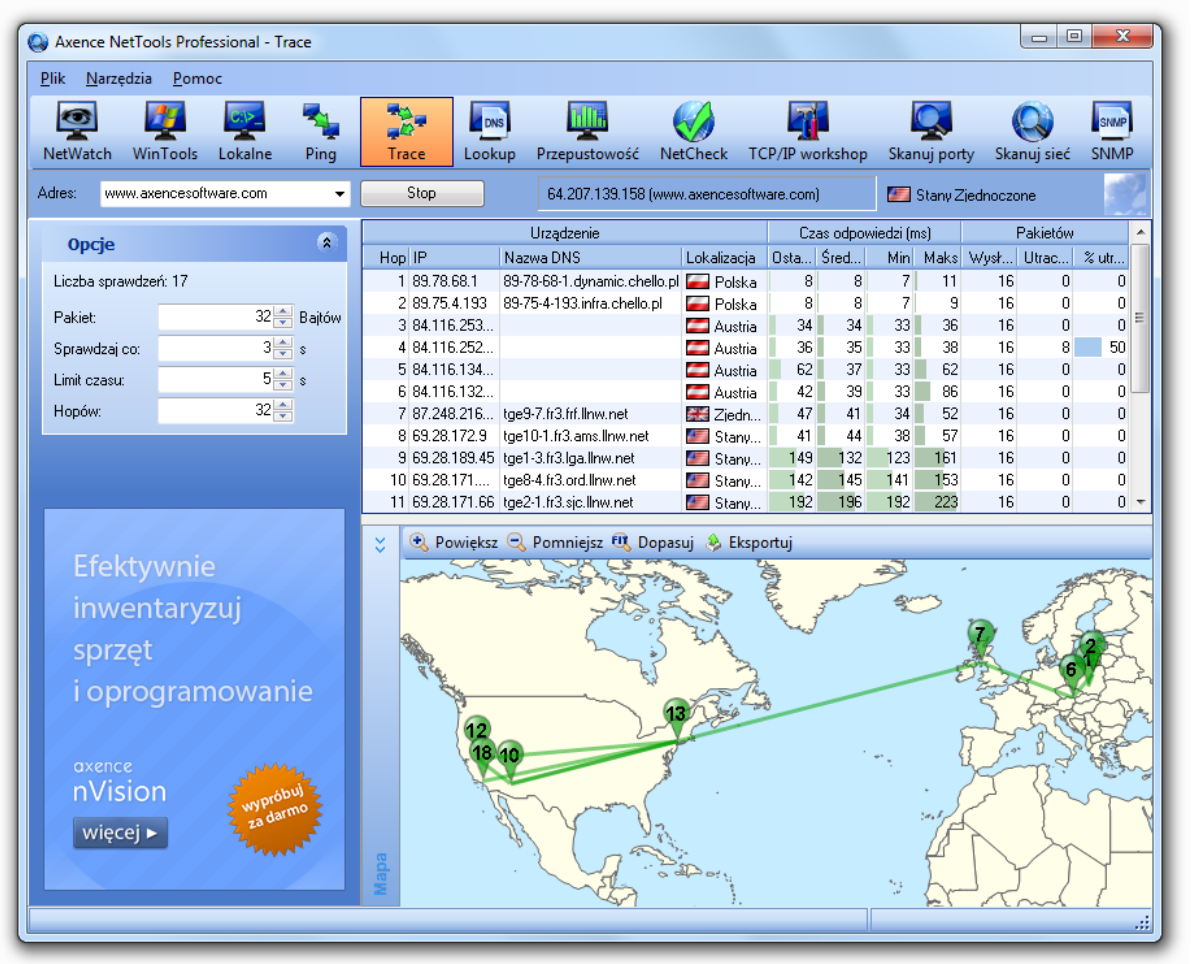
Możesz łatwo skopiować nazwę i IP wybranego urządzenia. Kliknij urządzenie prawym klawiszem i wybierz z menu kontekstowego **Kopiuj adres IP** lub **Kopiuj nazwę DNS**.

Możesz łatwo otworzyć dowolny adres z tabeli w innym narzędziu netTools wybierając z menu kontekstowego **Narzędzia** i jedną z opcji: **Dodaj do NetWatch**, **Lookup**, **Zużycie łącza**.

Eksportowanie

Aby wyeksportować tabelę zawierającą dane o urządzeniach, z menu kontekstowego wybierz opcję **Eksportuj**. Następnie wybierz jeden z formatów: **html**, **xml**, **txt**, **xls**.

Aby wyeksportować mapę do formatu **bmp**, wybierz opcję Eksportuj, wpisz nazwę pliku i **Zapisz**.



Uwagi

- Po prawej stronie paska adresu, możesz zobaczyć nazwę i IP urządzenia, które jest sprawdzane. Można je łatwo skopiować do schowka. Kliknij to pole prawym klawiszem i wybierz z menu kontekstowego **Kopiuj adres IP** lub **Kopiuj nazwę DNS**.
- Obok nazwy urządzenia znajduje się informacja o lokalizacji geograficznej (w postaci kraju) zdalnego adresu IP.

7.3 Lookup

Narzędzie Lookup działa podobnie jak nslookup. Podaje jednak od razu wszelkie informacje DNS o urządzeniu i domenie. Nie trzeba określać typu rekordu - pokazane będą wszystkie rekordy w jednej tabeli.

Dodatkowo Lookup podaje informację WHOIS na temat domeny, nawet jeśli podano nazwę DNS

urządzenia (np. www.google.com) zamiast domeny.

Aby sprawdzić adres

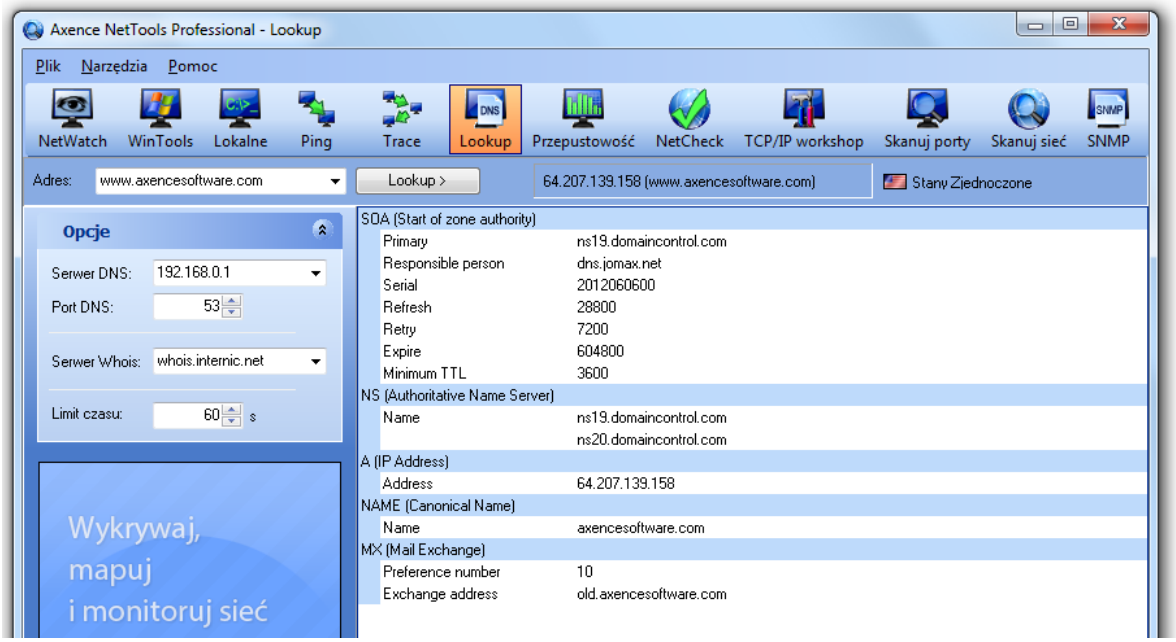
1. Na pasku nawigacyjnym wybierz narzędzie **Lookup**.
2. Wpisz **adres DNS** lub **IP** urządzenia w pasku adresu.
3. Kliknij przycisk **Sprawdź** lub naciśnij **Enter**.

Udostępniane informacje

Wszystkie rekordy DNS oraz informacje WHOIS zostaną przedstawione w tabeli. Informacja WHOIS pojawia się na dole.

Opcje

Możesz zmienić adresy serwera DNS i WHOIS, port DNS, oraz limit czasu odpowiedzi (dla obu serwisów: DNS i WHOIS).



Uwagi

- Po prawej stronie paska adresu, możesz zobaczyć nazwę i IP urządzenia, które jest sprawdzane. Można je łatwo skopiować do schowka. Kliknij to pole prawym klawiszem i wybierz z menu kontekstowego **Kopiuj adres IP** lub **Kopiuj nazwę DNS**.
- Obok nazwy urządzenia znajduje się informacja o lokalizacji geograficznej (w postaci kraju) zdalnego adresu IP.

7.4 Przepustowość

Narzędzie Przepustowość mierzy szybkość transmisji do urządzenia. Proces ten nie przeciąża sieci.

Aby rozpocząć pomiar przepustowości

1. Na pasku nawigacyjnym wybierz narzędzie **Przepustowość**.
2. Wpisz **adres DNS** lub **IP** urządzenia w pasku adresu.
3. Kliknij przycisk **Sprawdź** lub naciśnij **Enter**.

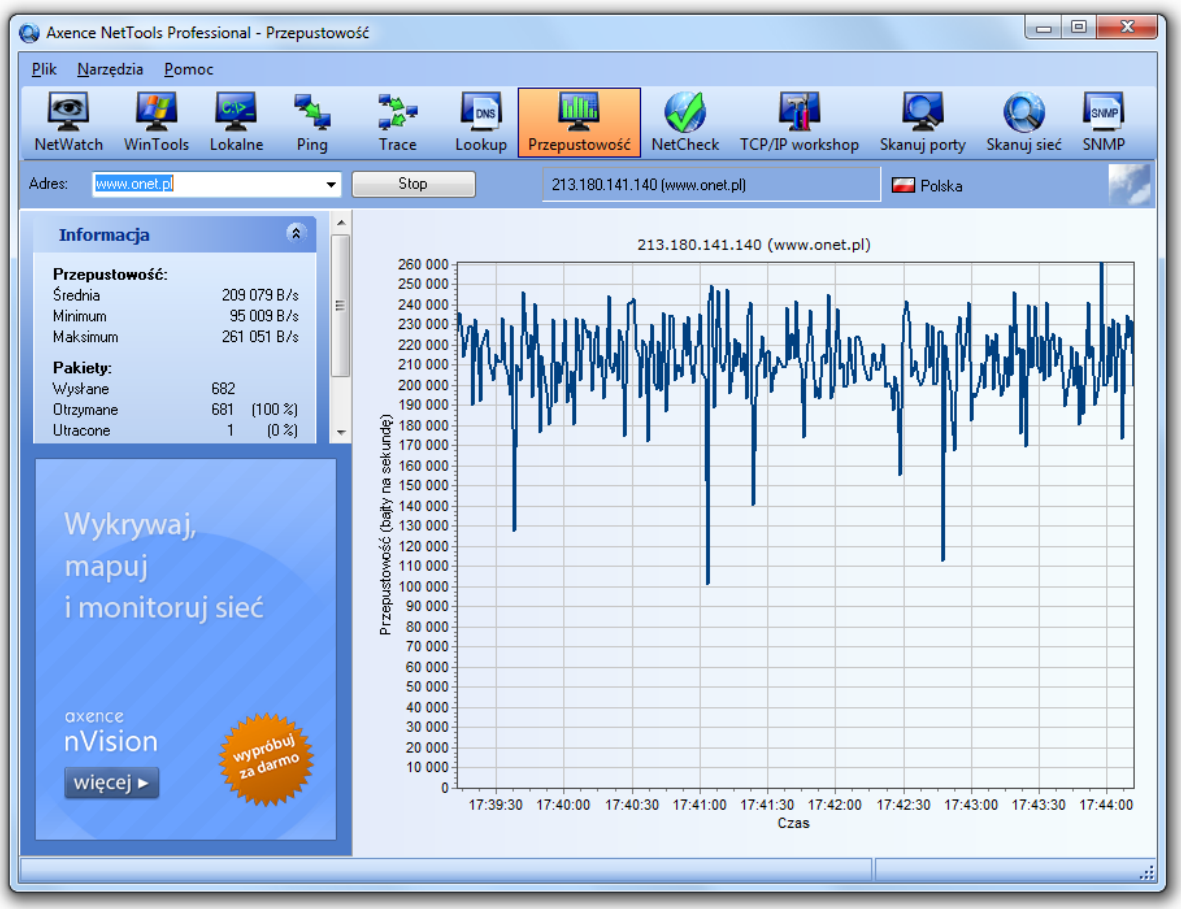
Udostępniane informacje

Na głównym wykresie można zobaczyć zmierzoną przepustowość dla ostatnich 5 minut.

Na pasku bocznym znajduje się ogólna - zbiorcza informacja: liczba pakietów wysłanych oraz min/max/średnia przepustowość.

Opcje

Można dostosować częstotliwość pomiarów, rozmiar pakietu oraz limit czasu odpowiedzi. Podaj dane w sekcji **Opcje** na pasku bocznym. Zmiana rozmiaru pakietu wpływa na wyniki. Niektóre urządzenia mogą nie akceptować zbyt dużych pakietów. Dla takich pakietów należy też ustawić dłuższy limit czasu.



Uwagi

- Narzędzie zużycia łącza zapisuje czas odpowiedzi dla ostatnich 5 minut, dlatego cały wykres reprezentuje 5 minut.
- Po prawej stronie paska adresu, możesz zobaczyć nazwę i IP urządzenia, które jest sprawdzane. Można je łatwo skopiować do schowka. Kliknij to pole prawym klawiszem i wybierz z menu

kontekstowego **Kopiuj adres IP** lub **Kopiuj nazwę DNS**.

- Obok nazwy urządzenia znajduje się informacja o lokalizacji geograficznej (w postaci kraju) zdalnego adresu IP.

7.5 NetCheck

Narzędzie NetCheck pozwala szybko sprawdzić jakość połączenia do urządzenia. Wysyła serię pakietów ICMP o różnych rozmiarach, aby wykryć wszelkie możliwe problemy. Wyniki są od razu interpretowane, więc nie trzeba nawet mieć szerokiej wiedzy o zarządzaniu sieciami.

Aby sprawdzić połączenie do urządzenia

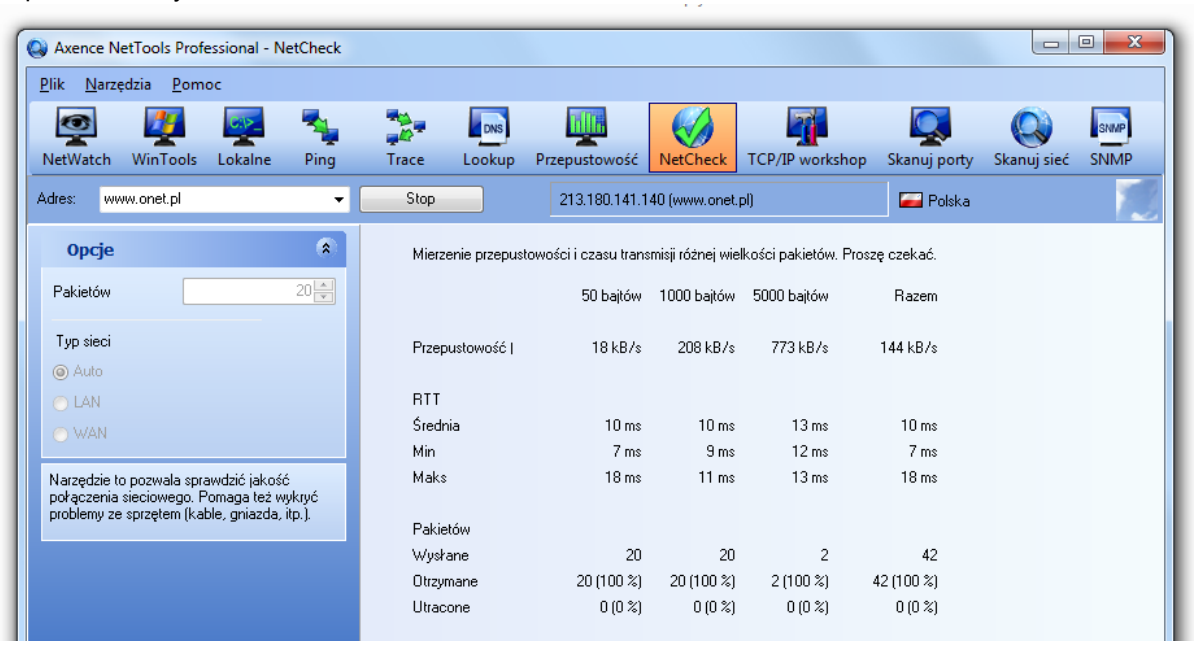
1. Na pasku nawigacyjnym wybierz narzędzie **NetCheck**.
2. Wpisz **adres DNS** lub **IP** urządzenia w pasku adresu.
3. Kliknij przycisk **Sprawdź** lub naciśnij **Enter**.

Udostępniane informacje

NetCheck prezentuje informacje zebrane podczas testów sieci: przepustowość, czas odpowiedzi oraz ilość utraconych pakietów dla różnych rozmiarów pakietów. Po zakończeniu testu pokaże się interpretacja wyniku testu.

Opcje

Można dostosować liczbę pakietów wysyłanych podczas każdego testu. Podaj wartość w sekcji **Opcje** na pasku bocznym.



Uwagi

- Po prawej stronie paska adresu, możesz zobaczyć nazwę i IP urządzenia, które jest sprawdzane. Można je łatwo skopiować do schowka. Kliknij to pole prawym klawiszem i wybierz z menu kontekstowego **Kopiuj adres IP** lub **Kopiuj nazwę DNS**.
- Obok nazwy urządzenia znajduje się informacja o lokalizacji geograficznej (w postaci kraju) zdalnego adresu IP.

7.6 TCP/IP workshop

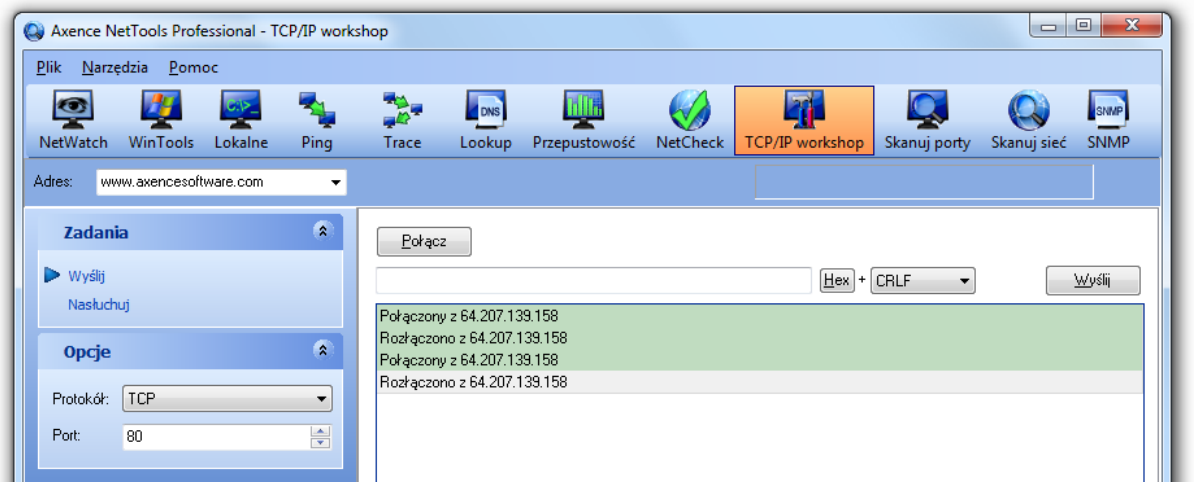
Narzędzie TCP/IP Workshop pozwala na ustanowienie niskopoziomowego połączenia TCP i UDP, aby móc testować i rozwiązywać problemy związane z różnymi serwisami sieciowymi. Za pomocą tego narzędzia można wysyłać dowolne dane do wybranego portu na zdalnym komputerze. Można także nasłuchiwać na lokalnym porcie, aby zobaczyć wszystkie dane jakie zdalne komputery nadsyłają.

Aby użyć TCP/IP workshop

1. Wybierz narzędzie **TCP/IP Workshop** na pasku nawigacyjnym.
2. Zaznacz **Wyślij** na pasku bocznym, aby połączyć się ze zdalnym portem TPC/IP i wysłać dane lub zaznacz **Nasłuchuj**, aby rozpocząć oczekiwanie na przychodzące połączenia i dane.
3. Wpisz dane i kliknij odpowiedni przycisk - **Połącz** lub **Nasłuchuj**.

Opcje

Możesz zmienić protokół i port używany przez narzędzie. Wpisz właściwe wartości w sekcji **Zadania** na pasku bocznym.



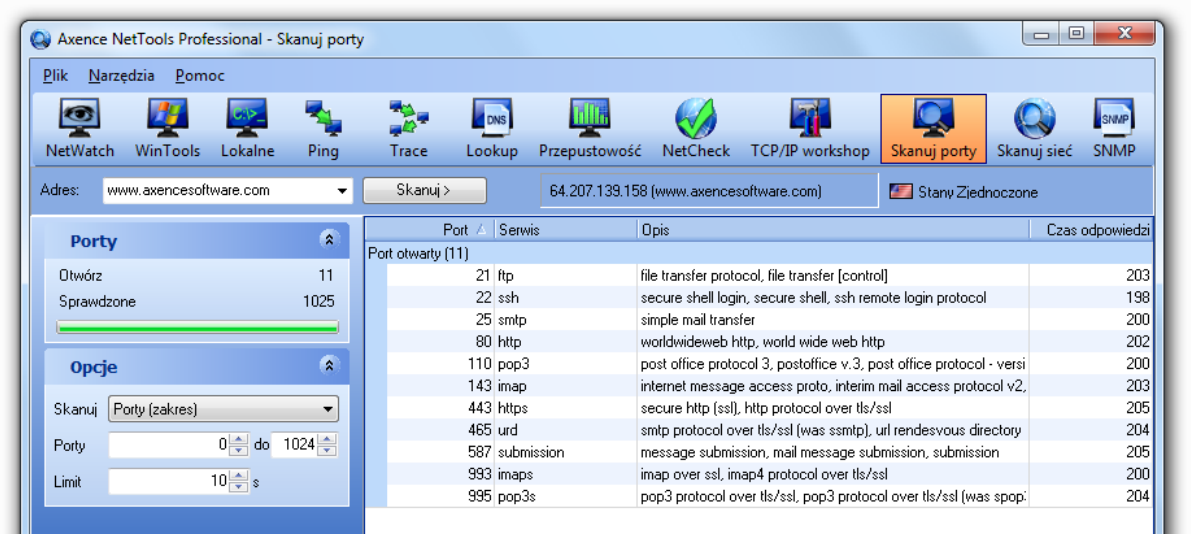
7.7 Skaner portów

Narzędzie Skaner urządzenia pozwala wykryć otwarte porty TPC oraz serwisy działające na urządzeniu. Prezentuje działające serwisy, sprawdza otwarte porty a także stara się wykryć ewentualne trojany.

Podczas skanowania serwisów, netTools wysyła żądanie i sprawdza czy odpowiedź pasuje do określonych kryteriów - co daje pewność, że na określonym porcie działa wybrany serwis. Ma to znaczenie w przypadku, gdy ten sam port byłby wykorzystywany przez różne serwisy. Skanowane mogą być serwisy działające zarówno na TCP jak i UDP.

Aby rozpocząć skanowanie urządzenia

1. Wybierz narzędzie **Skaner portów** w pasku nawigacyjnym.
2. Wpisz **adres DNS** lub **IP** urządzenia w pasku adresu.
3. Za pomocą opcji znajdujących się w pasku bocznym, określ co chcesz skanować: porty lub serwisy.
4. Kliknij przycisk **Skanuj** lub naciśnij **Enter**.



Udostępniane informacje

Główna tabela pokazuje informację o serwisach działających lub otwartych portach na urządzeniu. Serwisy prezentowane są w 3 grupach:

Grupa	Opis
Działa	Serwis działa na urządzeniu
Działa (ale błędna odpowiedź)	Serwis działa - odpowiedział na wysłane żądanie, jednak odpowiedź nie jest prawidłowa.
Port otwarty	Port jest otwarty, ale nie została odebrana żadna odpowiedź.

Na pasku bocznym pokazana jest także informacja o liczbie portów/serwisów sprawdzonych i działających (wykrytych).

Opcje

Opcje pozwalają zmienić limit czasu odpowiedzi i wybrać sposób skanowania:

Opcja	Opis
Serwisy	netTools wykryje wszystkie serwisy działające na urządzeniu, poprzez wysłanie określonego żądania i sprawdzenie czy odpowiedź pasuje do zdefiniowanego wzorca.
Porty (well known)	Opcja ta pozwala sprawdzić wszystkie otwarte, znane porty (porty well known).
Porty (well known - rozszerzone)	Opcja jw., zawierająca dodatkowo wiele rzadko używanych serwisów.
Porty (zakres)	Skanuje podany zakres portów.

Uwagi

- Po prawej stronie paska adresu możesz zobaczyć nazwę i IP urządzenia, które jest sprawdzane. Można je łatwo skopiować do schowka. Kliknij to pole prawym klawiszem i wybierz z menu kontekstowego **Kopiuj adres IP** lub **Kopiuj nazwę DNS**.
- Obok nazwy urządzenia znajduje się informacja o lokalizacji geograficznej (w postaci kraju)

zdalnego adresu IP.

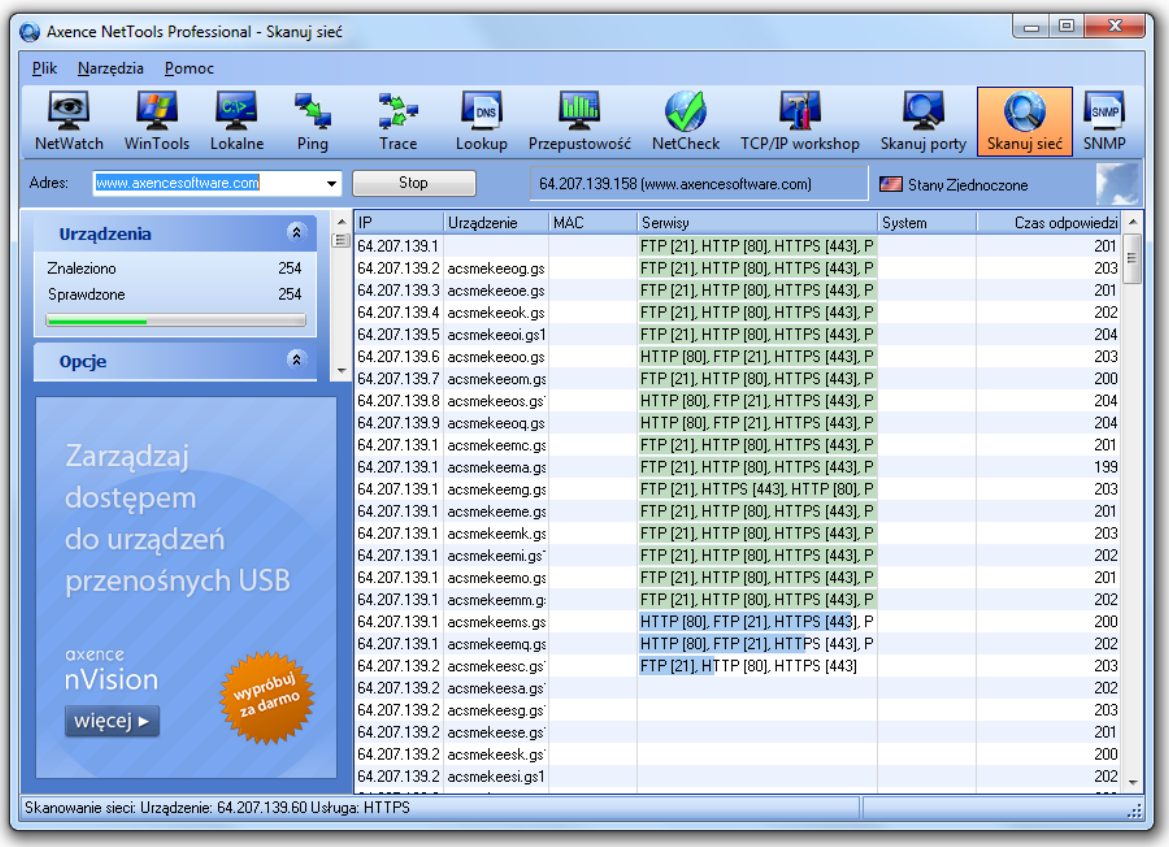
7.8 Skaner sieci

Narzędzie Skaner sieci pozwala wykryć urządzenia działające w wybranej sieci. Pokazuje ono wszystkie urządzenia oraz serwisy na nich działające.

netTools najpierw wykrywa dostępne urządzenia za pomocą ICMP (Ping). Oznacza to, że może wykryć tylko te urządzenia, które odpowiadają na żądania ICMP. Następnie wykrywane są wszystkie serwisy działające na dostępnych urządzeniach. Podczas skanowania serwisów działających na wykrytych urządzeniach, netTools wysyła żądanie i sprawdza czy odpowiedź pasuje do określonych kryteriów - co daje pewność, że na określonym porcie działa wybrany serwis. Ma to znaczenie w przypadku, gdy ten sam port byłby wykorzystywany przez różne serwisy . Skanowane mogą być serwisy działające zarówno na TCP jak i UDP.

Aby rozpocząć skanowanie sieci

1. Wybierz narzędzie **Skaner sieci** w pasku nawigacyjnym.
2. Wpisz **adres DNS** lub **IP** urządzenia w pasku adresu. netTools rozpocznie skanowanie sieci klasy C zawierającej ten adres. Przykładowo: jeśli podasz 192.168.0.34, wtedy program przeskanuje 255 adresów pomiędzy 192.168.0.1 and 192.168.0.254.
3. Kliknij przycisk **Skanuj** lub naciśnij Enter.



Udostępniane informacje

Główna tabela pokazuje informację o wykrytych urządzeniach i serwisach na nich działających lub otwartych portach. Po zaznaczeniu urządzenia na liście, możesz zobaczyć informację o wykrytych serwisach/portach w sekcji Informacja o urządzeniu na pasku bocznym.

Na pasku bocznym dostępna jest też informacja o liczbie adresów sprawdzonych i wykrytych.

Opcje

Opcje pozwalają zmienić następujące ustawienia:

Opcja	Opis
Tylko urządzenia	Włączenie tej opcji spowoduje, że netTools sprawdzi tylko dostępne urządzenia. Serwisy/porty nie będą już skanowane.
Serwisy	netTools wykryje wszystkie serwisy działające na urządzeniu, poprzez wysłanie określonego żądania i sprawdzenie czy odpowiedź pasuje do zdefiniowanego wzorca.
Porty (well known)	Opcja ta pozwala sprawdzić wszystkie otwarte, znane porty (porty well known).
Porty (well known - rozszerzone)	Opcja jw., zawierająca dodatkowo wiele rzadko używanych serwisów.
Porty (zakres)	Skanuje podany zakres portów.

Uwagi

- Możesz łatwo skopiować nazwę i IP wybranego urządzenia. Kliknij urządzenie prawym klawiszem i wybierz z menu kontekstowego **Kopiuj adres IP** lub **Kopiuj nazwę DNS**.
- Obok nazwy urządzenia znajduje się informacja o lokalizacji geograficznej (w postaci kraju) zdalnego adresu IP.
- Adres MAC uzupełniany jest na podstawie danych zawartych w tabeli ARP w **Lokalnych** oraz danych **SNMP**.

7.9 Linia poleceń

netTools może być uruchomiony z parametrami w linii komend. Pozwala to stworzyć skróty do najczęściej wykonywanych zadań. Składnia lini poleceń:

netTools.exe -<narzędzie> <adres urządzenia> [parametry]

Poniższa tabela opisuje sposób uruchamiania poszczególnych narzędzi.

Właściwość	Opis
-netstat	Narzędzie to pokazuje tylko lokalne informacje i nie wymaga żadnych parametrów.
-netwatch [adres urządzenia]	Dodaje urządzenie do NetWatch'a.
-wintools [adres urządzenia] [użytkownik]	Uruchamia WinTools na podanym adresie. Podaj użytkownika/hasło, aby automatycznie podłączyć się do

Właściwość	Opis
[hasło]	zdalnego komputera.
-ping [adres urządzenia]	Uruchamia Ping na podanym adresie.
-trace [adres urządzenia]	Uruchamia Trace na podanym adresie.
-lookup [adres urządzenia]	Uruchamia Lookup na podanym adresie.
-bandwidth [adres urządzenia]	Uruchamia Bandwidth na podanym adresie.
-netcheck [adres urządzenia]	Uruchamia NetCheck na podanym adresie.
-tcpipworkshop [adres urządzenia]	Uruchamia TCPIP Workshop na podanym adresie.
-scanhost [adres urządzenia]	Skanuje urządzenie o podanym adresie.
-scannetwork [adres urządzenia]	Skanuje sieć z podanym adresem.
-snmp [adres urządzenia] [wspólnota]	Uruchamia SNMP na podanym adresie. Podaj wspólnotę, aby automatycznie podłączyć się do zdalnego urządzenia.

Indeks

- U -

- W -

- Z -