1 Laboratorium SNMP

1.1 Cel ćwiczenia

Celem ćwiczenia jest zapoznanie się z zarządzaniem urządzeniami sieciowymi za pomocą protokołu SNMP.

1.2 Informacje wstępne

SNMP to protokół zarządzania siecią działającą w oparciu o TCP/IP. Podstawą systemu zarządzania siecią jest baza danych, czyli baza informacji zarządzania MIB. Obejmuje protokół wymiany danych, specyfikacje struktury baz danych oraz grupy obiektów danych. Łączy stacje zarządzania i agenty.

SNMPv1 jest najprostszą wersją protokołu SNMP. Umożliwia wykonywanie następujących funkcji: **GetRequest**, **GetNextReguest**, **GetResponse**, **SetRequest** i **Trap**. Do drugiej wersji protokołu wprowadzono ulepszenia funkcjonalne. **SNMPv2** został wzbogacony o nowe funkcje: **GetBulkRequest** i **InformRequest**. Procedury udostępniane przez oba protokoły ilustruje Tab. 1:

Tab. 1. Procedury udostępniane przez SNMPv1 oraz SNMPv2

Jednostka PDU	Opis
GetRequest	Pozwala na pobranie wartości obiektu skalarnego przez stację zarządzającą od stacji zarządzanej.
GetNextRequest	Bardzo podobna do PDU GetRequest, jednak jej wynikiem jest wartość instancji obiektu, która jest następna w porządku leksykograficznym po podanej w zapytaniu.
GetResponse	Są to odpowiedzi agenta na polecenia get lub set.
SetRequest	Daje możliwość zarządcy na ustawienie wartości obiektów w agencie.
Trap	Dzięki tej funkcji agent może powiadamiać stację zarządzania o ważnych zdarzeniach, mimo braku żądania.
GetBulkRequest	Umożliwia odczyt wielu wartości w ramach jednego zapytania, co pozwala zminimalizować ilość transakcji.
InformRequest	Daje możliwość zarządcy na wysłanie żądania do innej jednostki zarządzania. Powiadamia o stanie informacji zarządzania w innym zarządcy.

Komunikaty GetRequest, GetNextRequest i GetBulkRequest mają między sobą pewne różnice. Pierwszy z tych komunikatów pozwala na odczyt wartości każdego z przedstawionych obiektów. Drugi umożliwia odczyt następnej wartości każdego z obiektów. Natomiast GetBulkRequest pozwala uzyskać duży zakres danych w ramach jednego zapytania. Dzięki temu koszty są zdecydowanie mniejsze. Na powyższe zapytania agent odsyła komunikat Response.

Mimo, że obie wersje protokołu są do siebie bardzo podobne, to jednak ze względu na kilka istotnych różnic, nie mogą one ze sobą bezpośrednio współdziałać. Aby stało się to możliwe, należy użyć pełnomocników. Jest to najlepszy sposób na zapewnienie współpracy między protokołami. Można pomiędzy zarządcą SNMPv2 a agentem SNMPv1 ustawić pełnomocnika proxy. Będzie on dokonywał dwukierunkowej konwersji protokołów SNMPv1 oraz SNMPv2.

Innym sposobem na komunikację między SNMPv1 oraz SNMPv2 jest zastosowanie stacji zarządzania obsługującej obie powyższe wersje protokołu. Wtedy, gdy np. zarządca SNMPv2 będzie komunikować się z agentami SNMPv1, to zarządca wspierający obie wersje protokołu będzie pośredniczył w komunikacji podobnie jak robi to agent proxy.

SNMPv3 został poszerzony o funkcje bezpieczeństwa i funkcje administracyjne. W tej wersji protokołu pojawiły się następujące zabezpieczenia:

Szyfrowanie – możliwość zaszyfrowania komunikatów PDU SNMP za pomocą symetrycznego szyfru blokowego (ang. Data Encryption Standard – DES). Tajny klucz użytkownika, który szyfruje dane musi być również znany odbiorcy tych danych.

Uwierzytelnianie – do uwierzytelniania i ochrony przed modyfikacją danych stosowany jest kod uwierzytelniania wiadomości (ang. Message Authentication Code – MAC). Tutaj też tajny klucz musi być znany zarówno nadawcy jak i odbiorcy wiadomości.

Ochrona przed odtworzeniem – w SNMPv3 do każdego komunikatu nadawca dołącza wartość bazującą na liczniku, który istnieje u odbiorcy. Dzięki temu można upewnić się, że odebrany komunikat nie jest odtworzoną wersją komunikatu wysłanego wcześniej. Komunikat jest akceptowany, jeśli wartość licznika w otrzymanej wiadomości jest w miarę podobna do rzeczywistej wartości licznika.

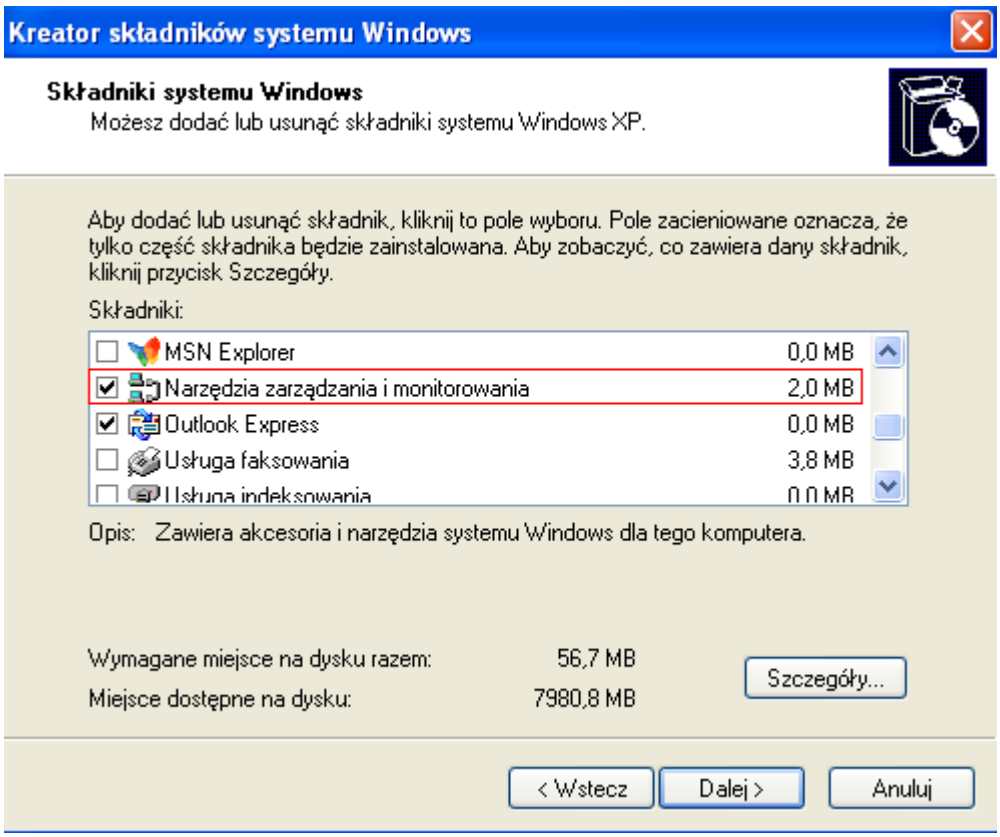
Kontrola dostępu – w SNMPv3 występuje kontrola dostępu oparta na widokach. Dzięki temu można ustawić do jakich informacji mają dostęp poszczególni użytkownicy. Informacje o polityce dostępu i uprawnieniach są przechowywane w lokalnej bazie danych konfiguracyjnych (ang. Local Configuration Datastore – LCD).

1.3 Przebieg ćwiczenia

Ćwiczenia będą wykonywane na bezpłatnej wersji programu iReasoning MIB Browser. Poniższa konfiguracja jest przedstawiona dla Windowsa XP.

1.3.1 Uruchom i skonfiguruj protokół SNMP.

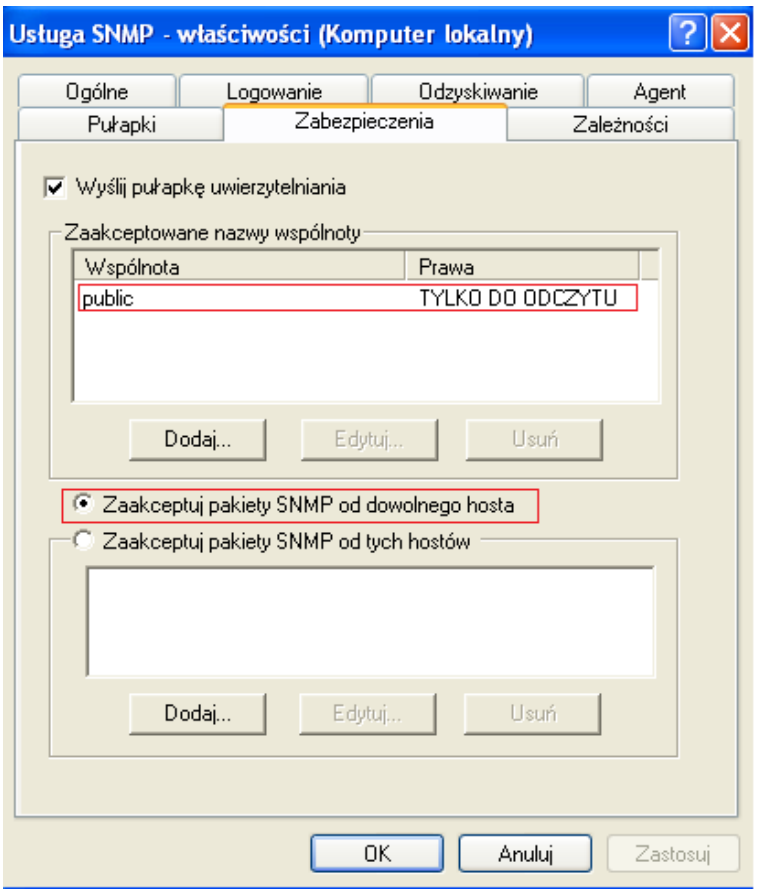
1. W tym celu uruchom kolejno **Panel sterowania –> dodaj lub usuń programy** –> **dodaj/usuń składniki systemu Windows**.
2. W nowo otwartym oknie (Rys. 1) sprawdź czy jest zaznaczone pole wyboru przy składniku systemu Windows – **Narzędzia zarządzania i monitorowania**.
3. Jeśli nie, to zaznacz i kliknij przycisk dalej.



Rys. 1. Składniki systemu Windows

4. Następnie wejdź w **Panel sterowania** –> **narzędzia administracyjne** –> **zarządzanie komputerem** –> **usługi i aplikacje** –> **usługi**.
5. Z listy wybierz **usługę SNMP** poprzez dwukrotne kliknięcie. Pojawi się okno takie jak ilustruje Rys. 3.
6. Przejdź na zakładkę **zabezpieczenia** i sprawdź czy w okienku **zaakceptowane nazwy wspólnoty** jest ustawiona wspólnota o nazwie **public** na prawach **tylko do odczytu**.
7. Jeśli nie, to poprzez przycisk **dodaj** utwórz taką wspólnotę.
8. Powinna być również zaznaczona opcja **zaakceptuj pakiety SNMP od dowolnego hosta**.
9. Wyłącz zaporę systemu Windows, aby dochodziły komunikaty SNMP. Aby to zrobić kliknij na pasku narzędzi w miejscu zaznaczonym na Rys. 2.

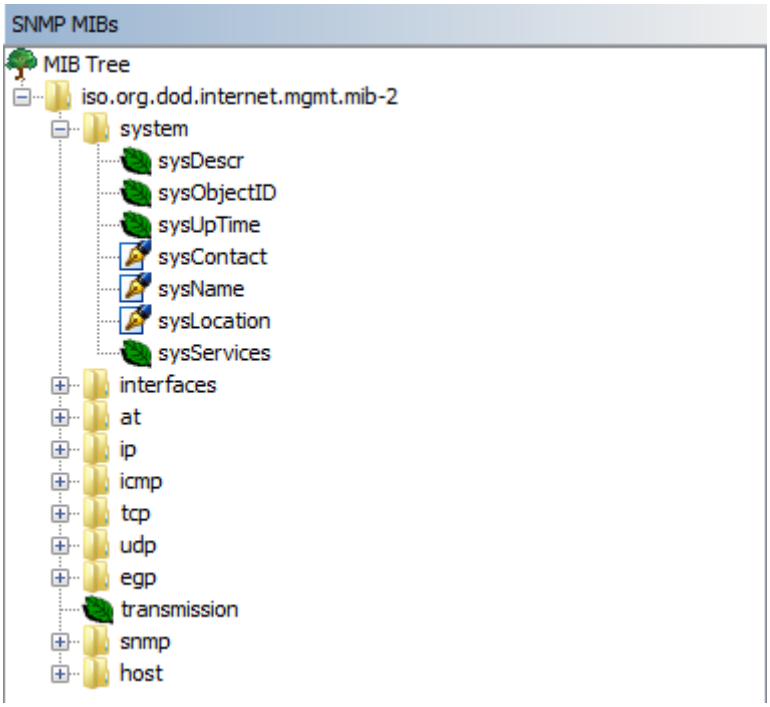
Rys. 2. Zapora systemu Windows



Rys. 3. Konfiguracja protokołu SNMP

1.3.2 Uruchom program iReasoning MIB Browser.

1.3.3 Zapoznaj się ze strukturą bazy MIB.



Rys. 4. Struktura bazy MIB

Po zaznaczeniu danego obiektu możesz poniżej odczytać informacje na jego temat. Przedstawia to Rys. 5.

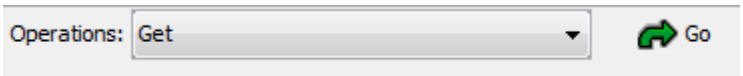
Name	sysUpTime
OID	.1.3.6.1.2.1.1.3
MIB	RFC1213-MIB
Syntax	TimeTicks
Access	read-only
Status	mandatory
DefVal	
Indexes	
Descr	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

Rys. 5. Informacje o danym obiekcie

1.3.4 Odczytaj informacje z grupy system.

1. W okienku **address** wpisz adres IP lub nazwę swojego komputera.
2. Następnie zaznacz dowolny obiekt z grupy **system** i z listy rozwijanej **operations** (Rys. 6) wybierz **Get.**

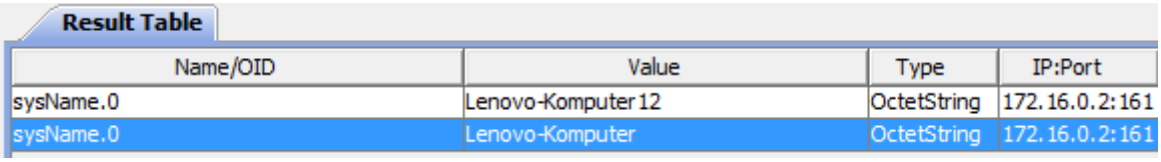
3. Wciśnij przycisk **Go.**
4. Wypróbuj też działanie operacji **GetNext** oraz **GetBulk.**



Rys. 6. Lista operacji

1.3.5 Działanie operacji Set.

1. Wyświetl obiekt **sysName.**
2. Spróbuj użyć operacji **Set** na tym obiekcie.
3. Jeśli nie działa, to uruchom **panel sterowania** –> **narzędzia administracyjne** –> **zarządzanie komputerem** –> **usługi i aplikacje** –> **usługi**.
4. Z listy wybierz usługę **SNMP**.
5. Na karcie **zabezpieczenia** zaznacz wspólnotę **public**, naciśnij przycisk **edytuj** i ustaw **prawa wspólnoty** na **odczyt zapis**.
6. Nie zamykając okna powróć do programu iReasoning MIB Browser i ponownie spróbuj użyć operacji **Set** na obiekcie **sysName.**
7. Jeśli operacja się powiodła, to wyświetl po raz drugi obiekt **sysName,** aby przekonać się, że nazwa uległa zmianie, tak jak na Rys. 7**.**
8. Teraz ponownie ustaw **prawa wspólnoty** na **tylko do odczytu,** aby wyeliminować możliwość zdalnej zmiany wartości.



Rys. 7. Przykład działania operacji Set

1.3.6 Rozwiń grupę interfaces.

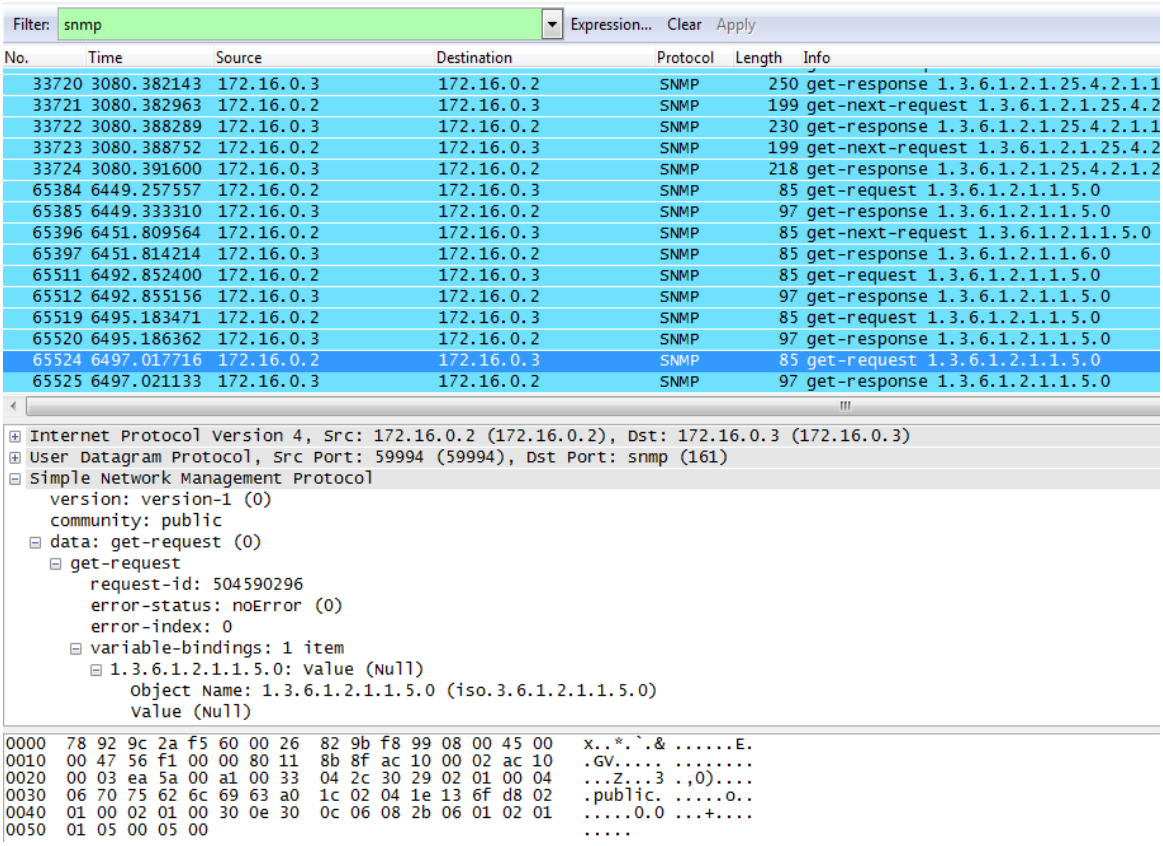
Całą tabelę interfejsów możesz wyświetlić zaznaczając obiekt **ifTable** i wykonując operację **Table View.** Grupę **interfaces** możesz natomiast przejrzeć wykonując operację **Get Subtree** na zaznaczonej grupie **interfaces.**

1.3.7 Działaj w parze z osobą przy drugim stanowisku komputerowym.

1. W polu **address** wpisz adres ip sąsiada.
2. Uruchom analizator **Wireshark**.
3. Rozpocznij rejestrację pakietów.
4. Filtruj ruch **SNMP**.

1.3.8 Pobierz jakąś wartość z drugiego komputera (np. sysName) za pomocą operacji Get.

W **Wiresharku** (Rys. 8) sprawdź jakie pola w PDU umieszcza jednostka wysyłająca i odbierająca.



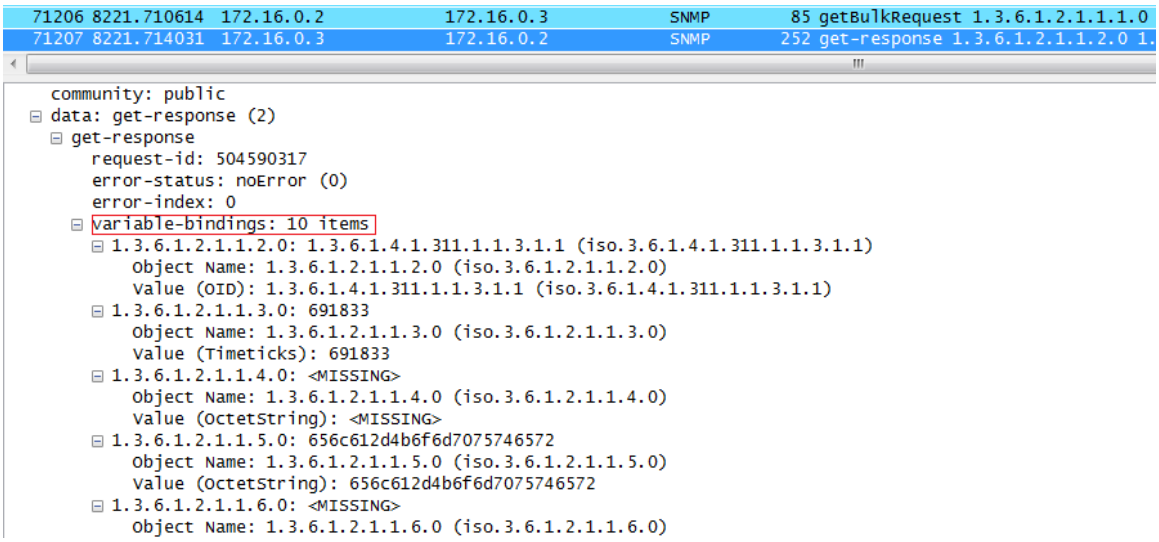
Rys. 8. Format jednostki GetRequest-PDU

1.3.9 Zaobserwuj w analizatorze Wireshark czy w jednostce typu GetResponse pojawiają się jakieś błędy, gdy próbujemy odczytać np. całą tabelę za pomocą polecenia Get.

1.3.10 Porównaj w Wiresharku działanie poleceń Get i GetNext.

Zwróć uwagę, że w przypadku PDU **GetRequest** każda zmienna w liście **variable-bindings** odnosi się do instancji obiektu, której wartość ma być odesłana. Natomiast przy PDU **GetNextRequest** dla każdej wymienionej zmiennej w odpowiedzi otrzymamy wartość tej instancji obiektu, która jest następna po podanej.

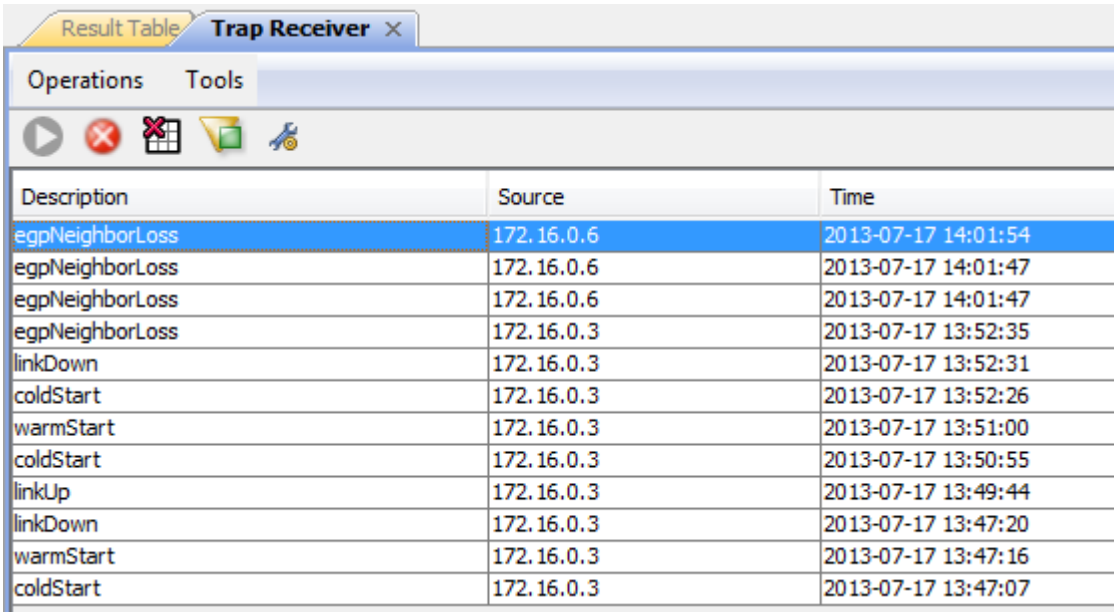
1.3.11 Sprawdź pole variablebindings w przypadku polecenia GetBulk. Zwróć uwagę, jakie zmienne przychodzą w odpowiedzi (Rys. 9).



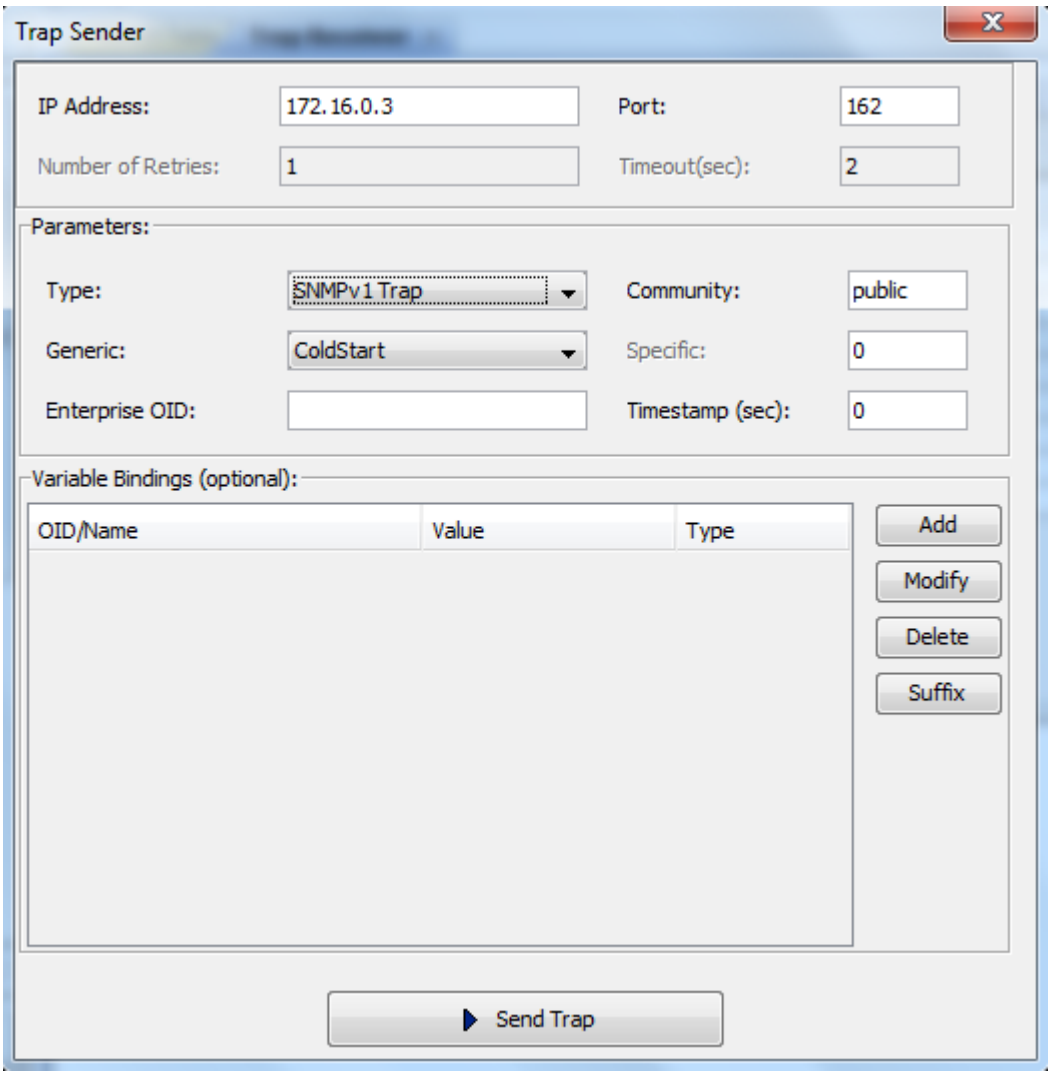
Rys. 9. Format jednostki Response-PDU

1.3.12 Pułapki

1. W programie **iReasoning MIB Browser** ustaw odbieranie pułapek za pomocą **Tools –> Trap Receiver.** Otworzy się okno jak na Rys. 10.
2. Następnie posługując się **Tools –> Trap Sender** (Rys. 11) wyślij różne rodzaje pułapek (zakładka **Generic**) do drugiego komputera z pary.
3. Zaobserwuj też w programie **Wireshark** jak wygląda struktura pułapki.



Rys. 10. Odebrane pułapki



Rys. 11. Wysyłanie pułapek

4. Na jednym komputerze z pary zmień w usłudze **SNMP** nazwę wspólnoty z **public** na dowolną inną.
5. Upewnij się czy jest zaznaczona opcja **„Wyślij pułapkę uwierzytelnienia”**.
6. Na tym samym sprzęcie w zakładce **„Pułapki”** usługi SNMP ustaw nazwę społeczności **public** oraz jako miejsce docelowe pułapek wpisz adres IP drugiego komputera z pary.
7. Teraz na drugim hoście użyj polecenia **Get**, aby odczytać jakąś wartość z pierwszego urządzenia.
8. Sprawdź czy została odebrana pułapka uwierzytelnienia.

1.3.13 Poddrzewo private bazy MIB

1. Do poddrzewa **private** wejdź wpisując ręcznie odpowiednie **OID.**
2. Wpisz **.1.3.6.1.4** i za pomocą operacji **Walk** lub **GetSubtree** przeanalizuj jakie informacje są zawarte w wynikach.

1.4 Sprawozdanie i wnioski

Studenci pracują przy osobnych stanowiskach komputerowych, ale dobrane pary współdziałają ze sobą. Poszczególne zalecane ćwiczenia laboranci wykonują samodzielnie lub przy współpracy. Duety przygotowują wspólne sprawozdanie uwzględniając wyniki uzyskane w laboratorium. Jednakże wnioski końcowe powinny być opracowane indywidualnie.

Opracował: Piotr Łękawa