Politechnika Białostocka

Wydział Elektryczny

Katedra Telekomunikacji i Aparatury Elektronicznej

Instrukcja do zajęć laboratoryjnych

Temat ćwiczenia:

Konfiguracja i badanie systemów zarządzania i monitorowania stacji sieciowych z wykorzystaniem protokołów SNMP i RMON

Numer ćwiczenia: 2

Laboratorium z przedmiotu:
Zarządzanie i bezpieczeństwo w sieciach teleinformatycznych

Kod przedmiotu: TS1D6220

Instrukcję opracował:
dr inż. Andrzej Zankiewicz

Białystok 2020

1. Ogólna charakterystyka ćwiczenia

Współczesne systemy teleinformatyczne są strukturami na tyle złożonymi, że zarządzanie nimi z wykorzystaniem klasycznych rozwiązań takich jak indywidualne połączenia administracyjne z poszczególnymi urządzeniami poprzez protokół telnet czy nawet WWW stają się często nieefektywne. Dotyczy to zwłaszcza rozbudowanych sieci obejmujących duże obszary, obsługujących wielu użytkowników i korzystających z połączeń redundantnych (nadmiarowych, wykorzystywanych np. w przypadku awarii). Dlatego opracowane zostały specjalne rozwiązania ułatwiające scentralizowane zarządzanie złożonymi sieciami teleinformatycznymi. Rozwiązania te najczęściej składają się z uniwersalnej programowalnej platformy zarządzającej komunikującej się z zarządzanymi urządzeniami sieciowymi poprzez określone protokoły.

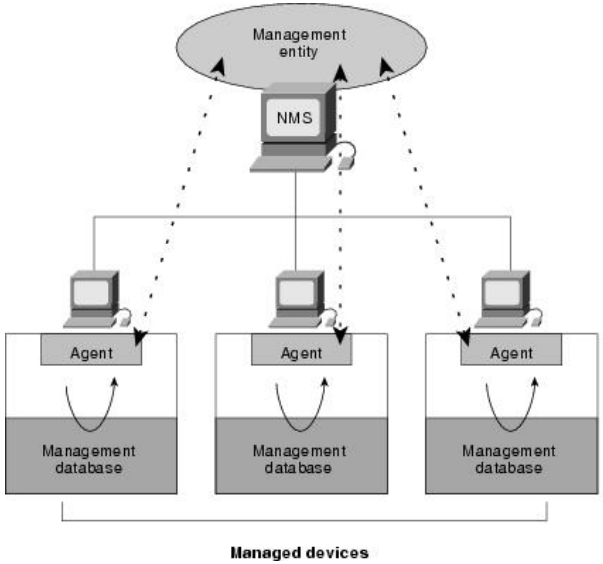
Obecnie najszerzej wykorzystywanym protokołem stosowanym do zarządzania systemami teleinformatycznymi jest protokół SNMP (*Simple Network Management Protocol*) przeznaczony dla sieci wykorzystujących w warstwach 3 i 4 modelu OSI rodzinę protokołów TCP/IP. Pierwsza wstępna specyfikacja protokołu SNMP została opublikowana w końcu lat osiemdziesiątych. W 1993 roku opublikowano specyfikację drugiej wersji tego protokołu – SNMPv2 wprowadzającą m.in. komendy odczytu całych tabel oraz komunikacji pomiędzy stacjami zarządzającymi. Ostatnim rozszerzeniem jest wersja trzecia, opublikowana w 1998 roku, wprowadzająca zabezpieczenia wykorzystujące algorytmy kryptograficzne. Obecnie najbardziej rozpowszechnione są protokoły SNMPv1 i SNMPv2.

Poniższy rysunek przedstawia ogólną strukturę systemu sieciowego zarządzanego z wykorzystaniem protokołu SNMP. Składa się on ze stacji zarządzającej (NMS – *Network Management Station)* oraz stacji zarządzanych. Każda stacja zarządzana posiada moduł agenta odpowiedzialnego za komunikację protokołem SNMP ze stacją zarządzającą oraz z wewnętrzną strukturą danego urządzenia. Integralną częścią systemu są też bazy MIB (*Management Information Base*) przechowujące rekordy odwzorowujące aktualny stan urządzenia.

Protokół SNMP jest protokołem warstwy aplikacyjnej i zapewnia komendy pozwalające na odczyt i zapis informacji w bazie MIB. Do transportu komend SNMP wykorzystywany jest protokół UDP (stacje zarządzane nasłuchują na porcie 161, a stacje zarządzające na porcie 162). Protokół SNMP w wersji 1 udostępnia następujące komendy:

- **GetRequest** – polecenie odczytu określonej wartości z bazy MIB, wysyłane przez stację zarządzającą do agenta w zarządzanym urządzeniu;
- **GetNextRequest** – polecenie wysyłane przez stację zarządzającą do agenta w zarządzanym urządzeniu i będące żądaniem odczytu zmiennej z bazy MIB stanowiącej dana zapisaną jako następna w kolejności chronologicznej drzewa bazy MIB (względem adresu podanego jako argument polecenia);
- **SetRequest** – polecenie wysyłane przez stację zarządzającą do agenta w zarządzanym urządzeniu i będące żądaniem zapisu wartości w bazie MIB danego urządzenia;
- **GetResponse** – odpowiedź zwracana w wyniku wykonania poleceń GetRequest, GetNextRequest, SetRequest;

- **Trap** – komunikat wysyłany automatycznie (bez osobnego zapytania) przez agenta do stacji zarządzającej w sytuacji zaistnienia określonego zdarzenia w zarządzanym urządzeniu (np. przejście interfejsu sieciowego w stan nieaktywny, przekroczenie wartości pewnej zmiennej itp.)

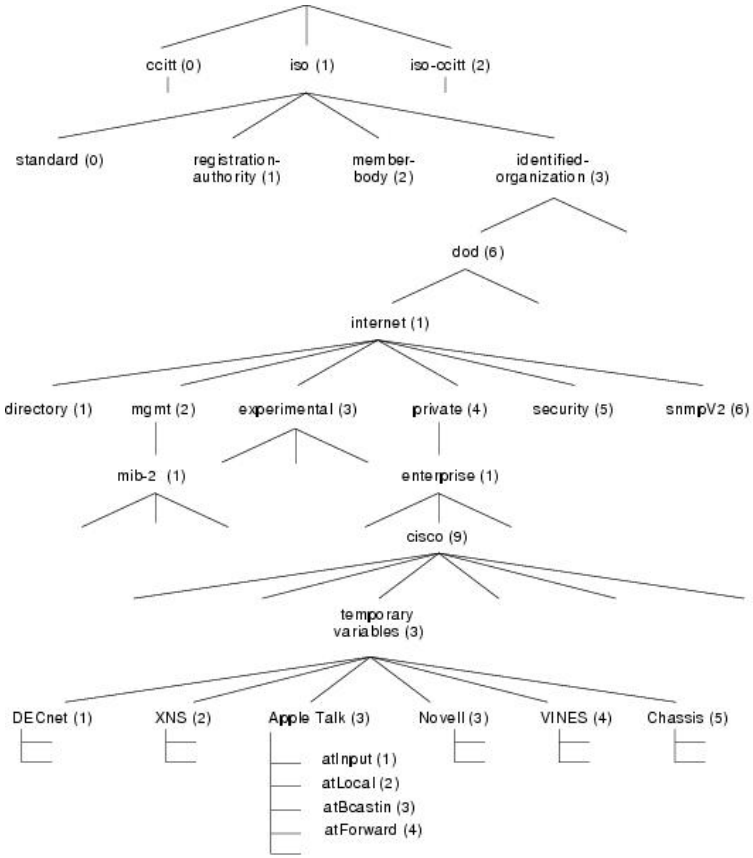


Rys. 1. Ogólna struktura systemu zarządzania z protokołem SNMP [6]

Baza MIB stanowi hierarchiczną strukturę obiektów odwzorowujących stan danego urządzenia. Specyfikacja baz MIB została opisana w dokumencie RFC 1213. Jak przedstawiono na rysunku 2, baza MIB stanowi jedną z gałęzi drzewa przypisaną na głównym poziomie do organizacji standaryzacyjnej ISO.

Do zadań związanych z administrowaniem systemami sieciowymi należy też ciągłe monitorowanie pracy tych systemów. W odróżnieniu od pojedynczych akcji związanych z zarządzaniem, monitorowanie jest to ciągły proces zbierania danych dotyczących pracy określonego węzła sieci (przykładowo mogą to byś statystyki ruchu na poszczególnych interfejsach routera lub przełącznika).

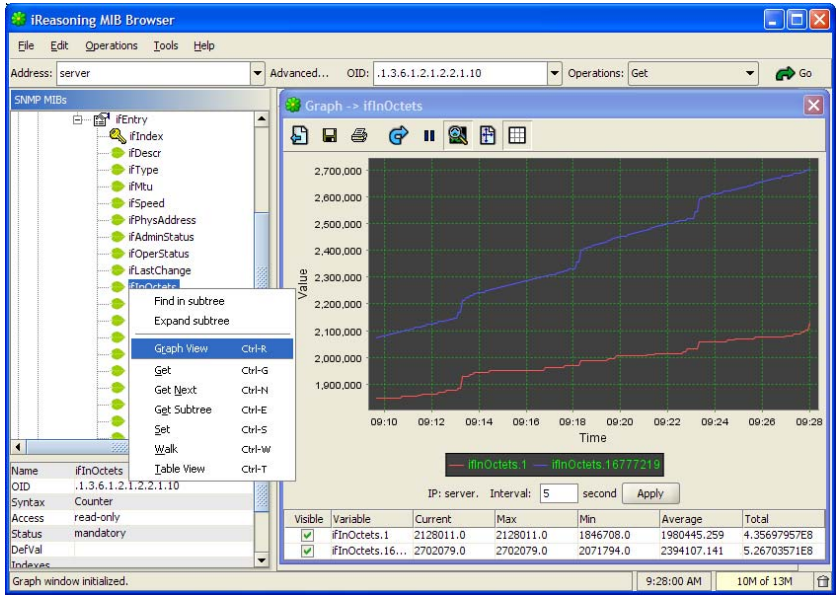
W celu ujednolicenia zadań monitorowania sieci opracowany został standard RMON (*Remote MONitoring*). Zdefiniowany jest on w dokumencie RFC1757 i od strony technicznej stanowi rozszerzenie zakresu bazy MIB o informacje związane z monitorowaniem sieci. Standard RMON wykorzystywany jest w urządzeniach nazywanych sondami, które przyłączane są w określonych punktach sieci i realizują zadania gromadzenia informacji o ruchu sieciowym w tym punkcie. Istnieje możliwość zarówno zbierania ogólnych danych statystycznych, jak i rejestracji ruchu (całego lub spełniającego warunki zdefiniowanych filtrów).



Rys. 2. Fragment struktury drzewa z bazą MIB [6]

Dane odczytywane protokołem SNMP mogą być prezentowane w czytelnej postaci (w tym graficznej) poprzez specjalistyczne oprogramowanie. Na rysunku 3 przedstawiono widok ekranu programu MIB Browser prezentujący wykres liczby pakietów odbieranych na wybranych interfejsach zarządzanego urządzenia.

Celem ćwiczenia jest praktyczne poznanie możliwości zarządzania i monitorowania struktury sieciowej z wykorzystaniem protokołów SNMP i RMON zaimplementowanych w urządzeniach sieciowych takich jak routery, przełączniki, zasilacze UPS oraz w systemach operacyjnych stacji roboczych i serwerów.



Rys. 3. Okno programu MIB Browser z wykresem ruchu na interfejsach.

2. Przygotowanie do zajęć

Przed przystąpieniem do wykonywania ćwiczenia należy zapoznać się z następującymi materiałami:

- Całość niniejszej instrukcji.
- Podstawowe informacje o protokołach SNMP, RMON oraz bazach MIB [1, 2].
- Rozdziały "*Configuring SNMP*" oraz "*Configuring RMON*" z dokumentu „*Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide*" (do pobrania z serwera laboratoryjnego oraz z witryny www.cisco.com.
- Opis struktury bazy MIB dla używanych w laboratorium urządzeń Cisco.

Zadanie opcjonalne

Wyszukać w Internecie bezpłatne oprogramowanie umożliwiające tworzenie wykresów na podstawie danych odczytywanych z protokołu SNMP i zapoznać się z jego obsługą i dostępnymi możliwościami konfiguracji.

Informacje zawarte w podanych powyżej źródłach stanowią minimum wiedzy teoretycznej **niezbędnej** do przystąpienia i prawidłowego wykonania ćwiczenia.

3. Plan wykonywania ćwiczenia laboratoryjnego

Część I - SNMP

1. Posługując się programem *MIB Browser* (np. iReasoning MIB Browser lub zawartym w pakiecie *SOLARWINDS Networking Management Software*) zapoznać się ze strukturą standardowej bazy MIB.
2. W znajdującym się na stanowisku laboratoryjnym komputerze PC uruchomić protokół SNMP (poprzez włączenie odpowiedniej usługi systemowej)..
3. Posługując się programem *MIB Browser* odczytać zawartość bazy MIB komputera z systemem operacyjnym Windows.
4. Dokonać uaktualnienia informacji systemowej w bazie MIB komputera wpisując w nim poprzez protokół SNMP własne dane. W tym celu można użyć programu *Update System MIB* z pakietu *SOLARWINDS Networking Management Software.* Następnie dokonać odczytu wprowadzonych informacji.
5. W znajdującym się na stanowisku laboratoryjnym urządzeniu sieciowym (np. przełączniku lub routerze) uruchomić protokół SNMP.
6. Posługując się programem *MIB Browser* odczytać zawartość bazy danych MIB badanego urządzenia.
7. Dokonać uaktualnienia informacji systemowej danego urządzenia wpisując w nim poprzez protokół SNMP własne dane. Następnie dokonać odczytu wprowadzonych informacji.
8. Posługując się analizatorem protokołów zarejestrować jednostki danych (PDU) protokołu SNMP przesyłane podczas operacji zapisu i odczytu danych w bazie MIB. Zidentyfikować i zinterpretować zawartość poszczególnych pól w tych jednostkach.
9. W badanym urządzeniu sieciowym skonfigurować wysyłanie komunikatów TRAP przy zaistnieniu dowolnego zdarzenia (brak podanego zdarzenia w instrukcji konfigurującej pułapkę powoduje, że będzie ona wysyłana przy wszystkich rodzajach zdarzeń (m.in. zmiana konfiguracji urządzenia, deaktywacja lub aktywacja interfejsu itd.).
10. Sprawdzić poprawność wysyłania komunikatów TRAP. Do odbierania tych komunikatów może być użyty np. program *Trap Receiver* z pakietu *SOLARWINDS Networking Management* lub serwer usługi *syslog*.
11. Zapoznać się z działaniem innym programów pakietu *SOLARWINDS Networking Management* a w szczególności tych związanych z protokołem SNMP (np. *MIB Viewer, MIB Walk, SNMP Graph*).

Część II - RMON

1. Posługując się programem MIB Browser odczytać zawartość grupy RMON (mib-2.16) w przełączniku w przypadku braku konfiguracji funkcji związanych z RMON.
2. Ustawić rejestrację statystyk RMON na wybranym interfejsie przełącznika Ethernet. Określić jakiego rodzaju informacje są gromadzone. Odczytać strukturę tabeli przechowującej statystyki.
3. Przyłączyć do przełącznika dwie stacje sieciowe (w tym jedną do skonfigurowanego w poprzednim punkcie interfejsu) i wygenerować ruch

pomiędzy nimi (np. poprzez operację kopiowania plików). Ponownie odczytać zarejestrowane na tym interfejsie statystyki RMON.

4. Skonfigurować rejestrowanie historii ruchu na wybranym interfejsie przełącznika z okresem próbkowania równym 5s. Odczytać zarejestrowane zapisy historii. Określić struktury tabel sterującej i danych przechowującej historię.
5. W oprogramowaniu MIB Browser skonfigurować graficzną prezentację statystyk ruchu pomiędzy przyłączonymi do przełącznika stacjami.
6. Skonfigurować wysyłanie pułapki SNMP (poprzez funkcje *alarmu* oraz *eventu* RMON) w przypadku gdy liczba wysyłanych ramek na wybranym interfejsie przełącznika przekroczy lub spadnie poniżej wybranych wartości. Okres próbkowania ustawić na 5s. Przedstawić struktury tabel utworzonych w efekcie wykonanej konfiguracji. Zarejestrować i opisać strukturę wysyłanych przez przełącznik pułapek.

W sprawozdaniu należy zamieścić wyniki uzyskane przy wykonywaniu poszczególnych części ćwiczenia wraz z danymi zarejestrowanymi analizatorem protokołów. Należy też scharakteryzować możliwości użytego oprogramowania rejestrującego i prezentującego dane z protokołów SNMP i RMON

4. Wymagania BHP

Zgodnie z podanymi na pierwszych zajęciach i potwierdzonymi przez studentów zasadami obowiązującymi w pomieszczeniu, w którym odbywają się ćwiczenia. Stosowny regulamin BHP jest też wywieszony w pomieszczeniu laboratorium.

5. Literatura

1. W. Stallings: *Protokoły SNMP i RMON. Vademecum profesjonalisty*. Wydawnictwo Helion, Gliwice 2003
2. *Vademecum teleinformatyka* tom I, praca zbiorowa, Wydawnictwo IDG, Warszawa 1999.
3. Instrukcja obsługi analizatora protokołów (np. *Wireshark)*
4. Dokumentacja pakietu *SOLARWINDS Networking Management Software*
5. Dokumentacja techniczna *Cisco* dotycząca przełącznika Catalyst 2950 (dostępna w laboratorium oraz w witrynie *www.cisco.com*).
6. Witryna *www.snmplink.org*