**ZADANIE B: Simple Network Management Protocol wersje 1 i 2**

NUMER INSTRUKCJI   
(WEDŁUG LAB ROADMAP)

**118**

Protokół SNMP funkcjonuje w trybie **zapytanie-odpowiedź** (port **161 UDP**) oraz w trybie **pułapki** (automatyczne zgłoszenie raportu na skutek wystąpienia określonego zdarzenia a urządzeniu, port **162 UDP**).

Przedmiotem konfiguracji i monitorowania za pośrednictwem SNMP są rozmaite elementy **przestrzeni MIB (Management Information Base)** określanej w ramach zasobów MIB (często plikowych) - dostarczanych przez producentów lub standardy. Przestrzeń ma postać **drzewa**.

Węzły to encje określające pojedyncze ustawienia, stany urządzeń, zdarzenia itp.. Węzły te mogą mieć też postać kolekcji (wówczas posługujemy się dodatkowo indeksem).

Typowe oprogramowanie typu **MIB Browser:**

* utrzymuje bazę MIB,
* umożliwia wysyłanie zapytań do urządzeń,
* wizualizację odpowiedzi,
* odbieranie pułapek z urządzeń.

W **zaawansowanej** postaci - zarządzanie autorskimi **dodatkami MIB** (pobieranie z plików, kompilowanie, dodawanie do drzewa), automatyczne wysyłanie zapytań (np. w interwale czasowym w celu obrazowania stanu na wykresach) itp.

Skonfiguruj przełącznik lub ruter Cisco do obsługi agenta SNMP:

Zdefiniuj community strings dla sesji SNMP włączając tym samym agenta SNMP w urządzeniu:

Switch(config)# snmp-server community public rw

gdzie public to zdefiniowana nazwa community a rw to uprawnienie read-write (obok możliwych: ro - read only, view - tylko odczyt nazwanego MIB, lub numer będący identyfikatorem listy ACL z uprawnieniami szczegółowymi).

3. Pobierz i zainstaluj oprogramowanie testujące: **Cisco SNMP Tools**. W edytorze wizualnym Cisco SNMP Tools stwórz "nowe urządzenie" odpowiadające urządzeniu fizycznemu podłączonemu do sieci (ruter lub switch). Skonfiguruj adres IP oraz nazwę community zgodne z urządzeniem fizycznym (menu podręczne -> Edit device). Otwórz okno Cisco Device Info w tym samym menu i pobierz testowo informacje o urządzeniu (przycisk: Get General Info Uwaga: przed konfigurowaniem SNMP konieczne jest postawienie interfejsu IP. W przeciwnym wypadku otrzymamy: "*SNMP-3-SOCKET: can't open UDP socket*"

4. **Uruchom klienta SNMP** (SNMP Browser) na stacji PC (GUI).

* Skonfiguruj Zdalnego Agenta SNMP ustalając IP przełącznika i port UDP: 161 (wybierz na razie SNMP 1 lub 2 - bez logowania użytkowników).
* Wyślij testowe zapytania posługując się drzewem MIB (ścieżka prowadząca do przestrzeni urządzeń sieciowych: iso.org.dod.internet.mgmt.mib-2).
* Pobierz także wybraną tabelę z danymi (np. listę interfejsów) oraz tylko wybrany rekord z tej tabeli (opcje dostępne w drop-down menu).
* Przeszukaj poddrzewa "udp","tcp","ip","interfaces".

5. W zakładce **Modules** i **Editor** można ładować i walidować dodatkowe moduły MIB. Pliki z modułami znajdują się w katalogu **/mibs**. Pobierz z repozytorium MIB Cisco wybrany plik i zapisz go w katalogu. Załaduj plik MIB (przycisk "->").

**Uwaga** - należy sprawdzić czy wybrany MIB nie jest uzależniony od innego (wystąpi wtedy też błąd ładowania). W takim przypadku - inny moduł także trzeba dodać do katalogu. Poprawność Modułów można walidować w zakładce Editor. Dodane moduły Cisco w drzewie MIB będą widoczne pod adresem: iso.org.dod.internet.private.enterprices.cisco.

6. W zakładce **Traps** można przeglądać otrzymane raporty z pułapek. Skonfiguruj urządzenie Cisco tak, aby wysyłało komunikat pułapki SNMP. W tym celu:

* określ host adresata komunikatów,
* wariant protokołu SNMP,
* community string.

**Warianty** protokołu to '1', '2c' lub '3':

Switch(config)#snmp-server host 192.168.123.100 version 1 cisco

Dodatkowo możliwe jest zezwolenie na przesyłanie konkretnych komunikatów do hosta:

Switch(config)#snmp-server host 192.168.123.100 version 1 cisco config

Switch(config)#snmp-server community cisco rw

Gdzie słowo 'config' oznacza wyłapywanie zdarzeń związanych z konfiguracją przełącznika czy rutera. Od tej pory komunikaty będą spływały do serwera monitorującego (w naszym przypadku 192.168.123.100).

Sprawdź inne opcje Włączenie wyłapywania konkretnych zdarzeń:

Switch(config)#snmp-server enable traps config

Switch(config)#snmp-server enable traps flash removal

Switch(config)#snmp-server enable traps snmp linkup i inne...

Wyłączanie pułapek:

Switch(config)#no snmp trap link-status

Sprawdź ustawienia SNMP:

Switch#show snmp host

7. Sprawdź pozostałą funkcjonalność narzędzia SNMP Browser w wersji protokołu SNMP 1

8. Włącz w **MIB Browser** wersję **2** protokołu SNMP. Wywołaj funkcję **Discovery** dla tej wersji (!) protokołu. Pobierz całą kolekcję danych MIB poprzez wywołanie funkcji **Get Bulk** (dostępna w drop-down menu) dla MIB Tree.

**ZADANIE C:** **Simple Network Management Protocol wersja 3. Zarządzanie szyfrowaniem i uprawnieniami użytkowników SNMP.**

Zdefiniuj przykładową konfigurację, w tym celu:

* Zdefiniuj "widok" określający gałąź MIB, której dotyczy zezwolenie (w przykładzie: 'iso')
* Zdefiniuj grupę użytkowników SNMP uprawniona do odczytu i bez obowiązku autoryzacji
* Zdefiniuj użytkownika dla tej grupy (z przypisaniem), gdzie auth określa technikę szyfrowania (sha lub md5),

Switch(config)#snmp-server view widok1 iso included

Switch(config)#snmp-server group grupa1 v3 priv read widok1 write widok1

Switch(config)#snmp-server user uzytkownik1 grupa1 v3 auth sha haslo priv des56 klucz

2. Do zarządzania uprawnieniami wykorzystywane są tradycyjnie **listy ACL**. Zdefiniuj w serwerze SNMP użytkownika z ograniczeniami przydzielając mu przykładowy dostęp listą ACL oraz zezwalając na przeglądanie tylko wycinków drzewa MIB. W tym celu:

- Zdefiniuj listę ACL dla hosta uprawnionego do komunikowania z urządzeniem Cisco:

Switch(config)#access-list 50 permit 192.168.123.100 0.0.0.255

- Zdefiniuj widok, grupę użytkowników z autoryzacją, użytkownika dla tej grupy,

Switch(config)#snmp-server view widok2 ifEntry.\* included

Switch(config)#snmp-server view widok2 udp included

Switch(config)#snmp-server group grupa2 v3 auth read widok2 access 50

Switch(config)#snmp-server user uzytkownik2 grupa2 v3 auth sha haslo

gdzie ifEntry.\* to ścieżka MIB określająca wszystkie pola w elementach kolekcji "ifEntry".

Dostępne kolekcje MIB można uzyskać komendą:

Switch#show snmp mib

**Uwaga**: Podczas składania zapytania SNMP w przypadku wyjścia **poza zakres uprawnionego** **widoku** lub poza uprawnienia z listy ACL urządzenie nie odrzuci żądania SNMP lecz zwróci wartość 0, pustą tabelę albo losową liczbę w odpowiedzi na to zapytanie. Przełączniki Cisco rzucają tez wtedy wyjątek **NULL TYPE/VALUE** lub **NO\_SUCH\_OBJECT\_EXCEPTION**. Monitorowanie tej sytuacji:

Switch#debug snmp packets

3. Skonfiguruj pułapkę SNMP aktywująca się gdy pojawił sie link na którymś z portów przełącznika:

Switch(config)#snmp-server community public rw

Switch(config)# snmp-server view widok3 iso included

Switch(config)# snmp-server group grupa3 v3 auth read widok3 write widok3 notify widok3

Switch(config)# snmp-server user uzytkownik3 grupa3 v3 auth sha haslo priv des56 klucz

Switch(config)# snmp-server enable traps snmp linkup

Switch(config)# snmp-server host 192.168.123.100 traps version 3 priv uzytkownik3

**Sprawdź ustawienia:**

Switch#show snmp user

Switch#show snmp host

Switch#show snmp view

**Uwagi**:

* wszelkie nazwy (zwłaszcza użytkowników) w narzędziach MIB Browser są **case sensitive**
* w przypadku niektórych systemów Cisco CatalystOS w nazwach użytkowników **nie są akceptowane duże litery**
* metoda szyfrowania nazwana w systemie Cisco CatalystOS sygnaturą "**des56**" to DES w rozumieniu protokołu SNMP (DES należy wybierać w programach MIB Browser)
* w przypadku pułapek autoryzacja jest wymagana przez oprogramowania MIB browser, uwierzytelnia się urządzenie sieciowe.
* **pułapki** funkcjonują na porcie **UDP 161**
* w przypadku pułapek w wersji 3 protokołu większość narzędzi MIB Browser wymaga **obowiązkowo** trybu "**authPriv**". Po wybraniu samego Auth występują błędy parsowania SNMP
* po skonfigurowaniu danych użytkownika w MIB Browser wskazane jest zamknięcie tego narzędzia i **uruchomienie** **ponownie** (stare dane zostają w cache)

4. **Uruchom klienta** SNMP (SNMP Browser) na stacji PC (GUI).

Skonfiguruj Zdalnego Agenta SNMP do pracy z wykorzystaniem SNMPv3 oraz danych logowania/szyfrowania zgodnych z powyższymi przykładami (menu Options -> Manage SNMPv3 USM Profiles -> prawy przycisk na pustym oknie "pprofiles" -> New USM Profile).

W SNMPv3 Properties należy także określić odpowiedni **security level** (authPriv, noAuthPriv, noAuthNoPriv) - zależnie od użytkownika, którego testujemy:

Wprowadź dane profilu, przypisz profil do połączenia (Okno Agent Profiles -> Profiles -> SNMPV3).

Sprawdź funkcjonowanie klienta SNMP:

* w pierwszych dwóch sytuacjach poprzez pobieranie danych za pośrednictwem MIB
* w trzeciej poprzez zaktywowanie pułapki (podłączenie kabla UTP). W tym przypadku wyniki należy wyszukać w zakładce traps, sprawdzając także treść Trap content -> Bindings.

**Zadanie D: Syslog i konsola zdalnego logowania komunikatów systemowych IOS.**

Uruchom ponownie Cisco SNMP Tools.

Włącz klienta zdalnego logowania (menu Cisco Tools -> Syslog and Debug Console)

2. Włącz system logowania w przełączniku łapiąc komunikaty **debug**:

Switch(config)# (config)#logging trap debugging

Określ **cel** dla przesyłania tych komunikatów:

Switch(config)#logging facility syslog

Przekieruj komunikaty na **konsolę zdalną** (do IP hosta, gdzie uruchomiony jest klient)

Switch(config)#logging 192.168.132.100

Sprawdź fukncjonowanie konsoli (Menu Cisco Tools -> Cisco Syslog and Debug Console w pakiecie Cisco SNMP Tools)

3. Zdefiniuj logowanie komunikatów z innych pułapek:

Switch(config)#logging trap ?

4. Przekieruj logowanie komunikatów do pliku w pamięci flash (np. komunikat request serwera HTTP):

Switch(config)#debug ip http url

Switch(config)#logging file flash:plik debugging

Skasuj plik po przeglądnięciu jego treści

5. **Dodatkowo**: Sprawdź funkcjonowanie SNMP w narzędziu Cisco SNMP Tools. Przeglądnij możliwości dodatku SNMP Tool (menu Cisco Tools -> Cisco SNMP Tools).