SNMP

Protokół SNMP

SNMP (ang Simple Network Management Protocol) to standard protokołu używanego do nadzoru i zarządzania różnymi elementami sieci komputerowych, takimi jak routery, przełączniki, komputery, itp. działającego w warstwie aplikacji.

Został on opracowany pod koniec lat osiemdziesiątych przez IETF (Internet Engineering Task Force) jako uniwersalny protokół do zarządzania sieciami. Począwszy od 1993 r. zyskał popularność jako metoda zarządzania sieciami TCP/IP i wchodzącymi w ich skład urządzeniami.

Protokół może mieć również zastosowanie w innych typach sieci

Protokół SNMP (Cd)

Istnieją obecnie trzy wersje protokołu SNMP (SNMPv1, SNMPv2, SNMPv3).

Szczególnie interesująca może być wersja druga, gdyż jest ona rozwinięciem pierwszej i jest najczęściej stosowana.

Wersja trzecia jest najbardziej skomplikowaną i przez to rzadziej używaną. Sam protokół w wersji drugiej też dzieli się na kilka odmian w zależności od zastosowanych usprawnień związanych z bezpieczeństwem:

- SNMPv2p (ang. party-based),
- SNMPv2c (ang. community-based),
- SNMPv2u (ang. user-based)

Protokół SNMP (Cd)

Najpopularniejszą z nich jest wersja SNMPv2c stosująca ten sam rodzaj zabezpieczeń co SNMPv1 a mianowicie community-string.

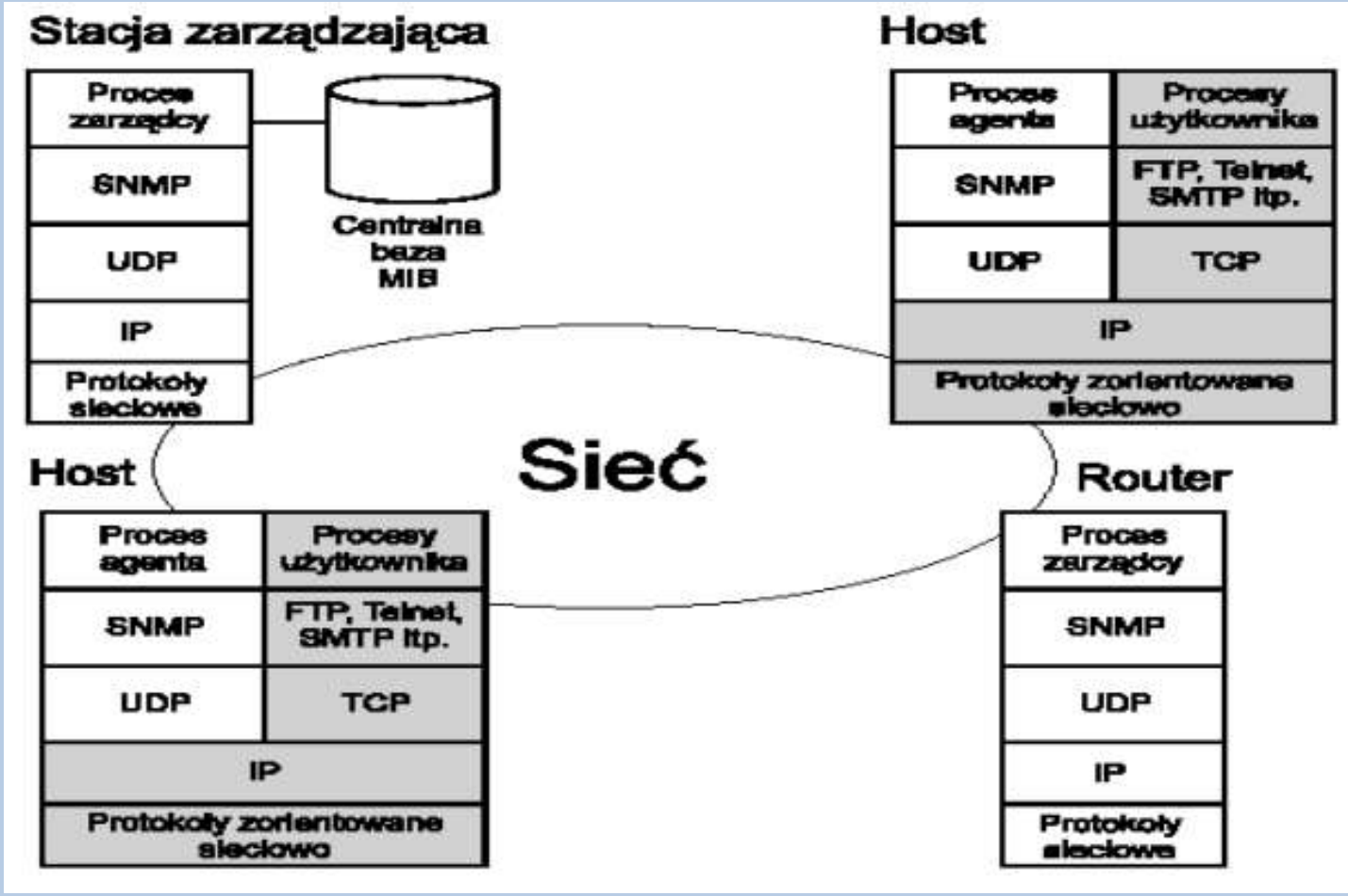
Standardy protokołów SNMP opisane są w następujących dokumentach:

- RFC 1065, RFC 1066, RFC 1067 (SNMPv1)
- RFC 1441, RFC 1452 (SNMPv2p)
- RFC 1901, RFC 1908 (SNMPv2c)
- RFC 1909, RFC 1910 (SNMPv2u)
- RFC 3411, RFC 3418, RFC 3584 (SNMPv3)

Protokół SNMP - działanie

Model zarządzania wykorzystuje następujące podstawowe elementy składowe:

- Stację zarządzającą (Management station);
- Agenta zarządzania (Management agent);
- Bazę danych informacji zarządzania (Management Information Base - MIB);
- Protokół zarządzania sieciowego (Network management protocol).



Protokół SNMP - działanie

Stacja zarządzająca pełni funkcję interfejsu pomiędzy operatorem i systemem zarządzania zasobami systemowymi. Powinna być wyposażona przynajmniej w następujące elementy:

- Zestaw aplikacji zarządzania umożliwiających analizowanie danych, likwidację zagrożeń i uszkodzeń itp.;
- Interfejs pozwalający na monitorowanie i sterowanie funkcjonowaniem sieci;
- Funkcje translacji poleceń i komend operatora na akcje nadzorowania oddalonych elementów systemu;
- Bazę danych umożliwiającą przechowywanie informacji pozyskanych z baz MIB wszystkich zarządzanych elementów nadzorowanej sieci.

Protokół SNMP - działanie

Aplikacja agenta – uruchomiona jest w kluczowych elementach sieciowych typu hosty, routery, mostki i inne, odpowiada na żądania kierowane do nich ze stacji zarządzającej. W niektórych przypadkach możliwe jest również powiadamianie realizowane wyłącznie z inicjatywy agenta.

Całość zasobów systemu posiada reprezentację w postaci obiektów rozumianych jako *zmienne reprezentujące istotne aspekty funkcjonalne*. Zestaw tych zmiennych stanowi zawartość bazy MIB, która jest udostępniana stosownie do aktualnych potrzeb.

Protokół SNMP - działanie

Normatywy SNMP nie określają wymaganej ilości stacji zarządzających ani liczby aplikacji agenta przypadających na pojedynczą stację.

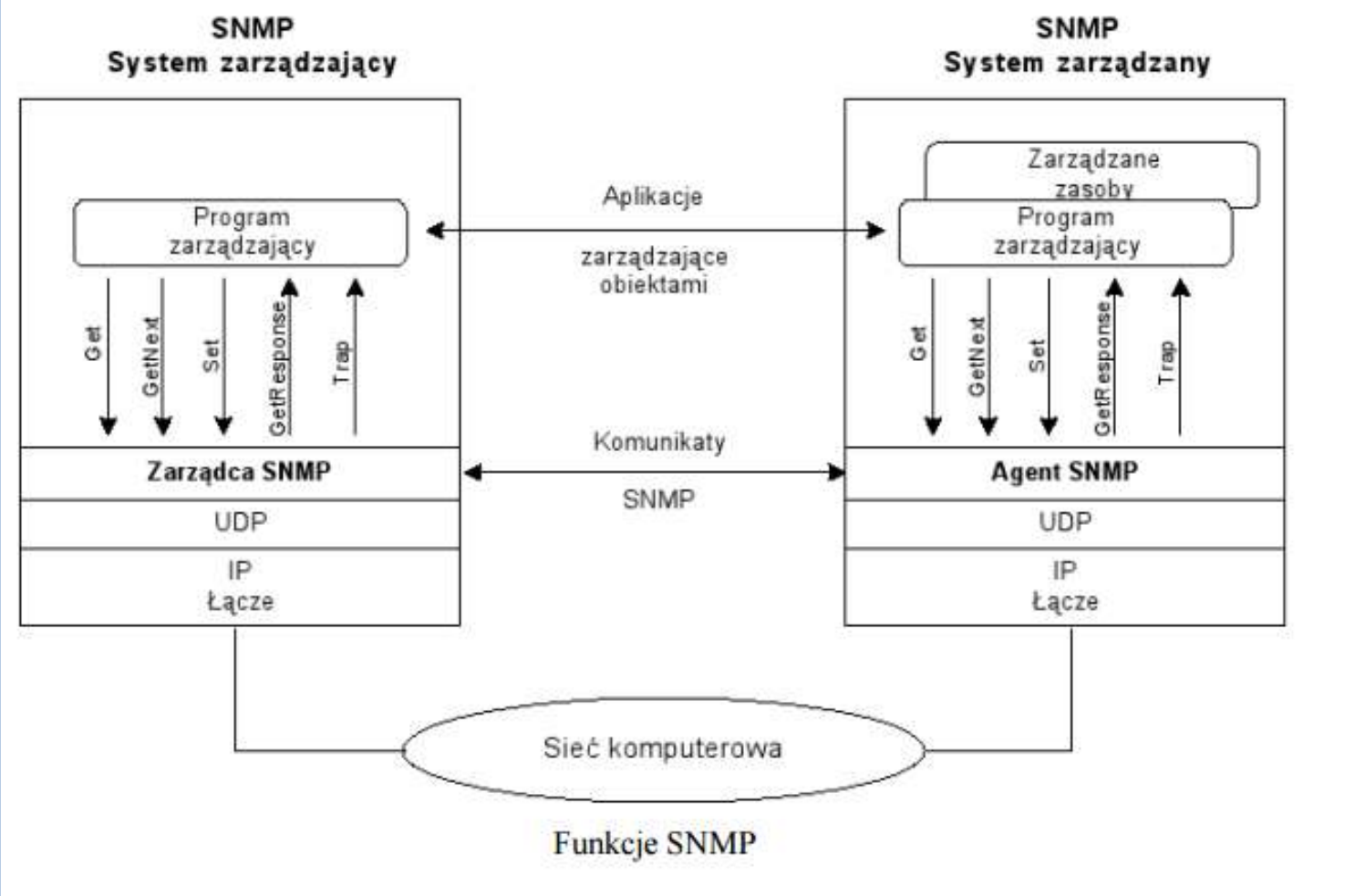
Jednak dobrą praktyką jest posiadanie co najmniej dwóch stacji zarządzających, co umożliwia bezpieczne funkcjonowanie systemu w przypadku awarii.

W kwestii liczby obsługiwanych aplikacji agenta obowiązuje zasada, że dopóki SNMP pozostanie rozwiązaniem relatywnie „prostym”, ilość ta może być duża i wynosić setki aplikacji.

Protokół SNMP - działanie

Transmisja odbywa się po kolei poprzez trzy warstwy zarówno u Zarządcy jak i Agenta, które reprezentują po jednym z protokołów: SNMP, UDP i IP.

Agent podczas komunikacji z Zarządcą korzysta z wbudowanej bazy informacji – MIB, która przechowuje informacje i statystyki, których może on od niego zażądać.



Funkcje SNMP

Protokół SNMP - działanie

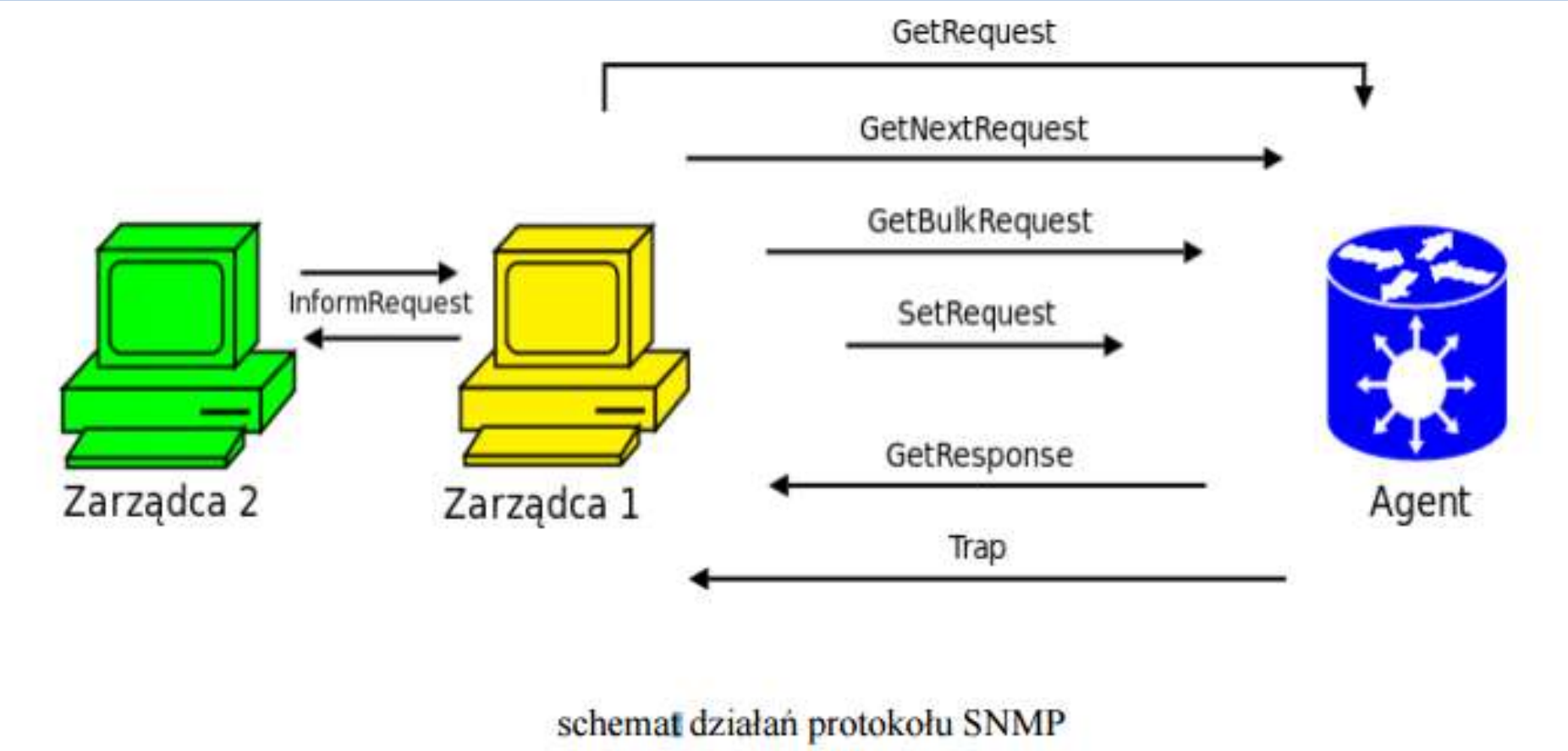
Komunikacja może odbywać się nie tylko między Zarządcą i Agentem, ale też między samymi Zarządcami w celu wymiany informacji w społeczności odpowiedzialnej za zarządzanie daną grupą urządzeń.

Protokół SNMP - komunikaty

Komunikacja między dwoma stacjami odbywa się za pomocą specjalnie zdefiniowanych poleceń protokołu SNMP zwanych PDU (Protocol Data Units).

- **GetRequest** – Zarządca żąda odczytania wartości określonego obiektu w bazie MIB Agenta,
- **GetNextRequest** – Zarządca wymaga podania wartości obiektów, które są powiązane z innymi obiektami, co powoduje sekwencyjne przeszukanie bazy MIB,
- **GetBulkRequest** – zapytanie Zarządcy o blok informacji (wiele rekordów bazy) – SNMPv2 i nowsze,
- **GetResponse** – odpowiedź Agenta zawierająca rekordy z bazy odczytane na żądanie Zarządcy,
- **SetRequest** – polecenie wprowadzenia zmiany do bazy MIB Agenta,
- **Trap** – komunikat Agenta o pojawieniu się sytuacji nadzwyczajnej lub jakiegoś zdarzenia,
- **InformRequest** – pakiet typu Trap przesyłany między różnymi stacjami Zarządzania służący do wymiany informacji – SNMPv2 i nowsze.

Protokół SNMP - komunikaty



schemat działań protokołu SNMP

Protokół SNMP - MIB

Każdy agent SNMP obsługuje własną niewielką bazę danych (MIB - Management Information Base), zawierającą informacje o stanie i historii pracy urządzenia, a także zmienne sterujące jego pracą. Specyfikacja SNMP umożliwia rozszerzenie standardowego zestawu wartości o zmienne charakterystyczne dla danego urządzenia (private MIB).

Urządzeniami tymi mogą być praktycznie dowolne urządzenia sieciowe - mostki, bramki, routery, serwery, modemy, drukarki itd.

Ukazały się dwie wersje tego standardu oznaczonego jako MIB-I i MIB-II. Nowsza wersja naprawiała pewne niedociągnięcia swojej poprzedniczki.

Protokół SNMP - MIB

Każdy komunikat dotyczy określonej zmiennej, tzw. OID (ang. Object IDentifier).

Dla przykładu zmienna OID o nazwie sysUpTime (czas pracy urządzenia od ostatniego włączenia) ma postać 1.3.6.1.2.1.1.3.0, co odpowiada jej adresowi w drzewie MIB.

Protokół SNMP – MIB-I

Standard ten definiuje rodzaje obiektów (ponad 100), jakie można zapisać bazie. Dzieli się je na osiem grup ze względu na zastosowanie:

1. **Obiekty systemowe** – obejmuje informacje dotyczące statusu urządzenia, tj. obecność uszkodzeń, czy ogólnym przeciążeniu ruchem,

2. **Interfejsy** – wszelkie dane jakie dotyczą interfejsów urządzenia, np. statyczne drogi routingu,

3. **Tablice translacji** – przechowujące odwzorowanie adresów IP na inne protokoły, np. adresy sprzętowe pobliskich routerów – ARP,

4. **IP** – informacje dotyczące protokołu, np. ilość błędów transmisji,

5. **ICMP** – dane dotyczące protokołu ICMP (Interent Control Message Protocol), np. ilość wystąpień pakietów żądających spowolnienia transmisji,

6. **TCP** – wszystko co opisuje TCP (Transmission Control Protocol), np. wielkość ramki danych,

7. **UDP** – obiekty protokołu UDP (User Datagram Protocol

8. **EGP** – obiekty protokołu EGP (Exterior Gateway Protocol).

Protokół SNMP – MIB-I

Główne wady MIB-I

• Brak rekordów odnoszących się do rodzaju medium transmisyjnego, np. światłowód, skrętka, kabel koncentryczny, linia radiowa.

• Brak opisu obiektów dotyczących zarządzania pracą mostów i regeneratorów.

• Nie obecność otwartych standardów pozwalających na prowadzenie prac rozwojowych przez producentów sprzętu nad rozwiązaniami firmowymi.

Protokół SNMP – MIB-II

Nowa wersja bazy danych została opisana dokumentem RFC 1757, który poprawiał wszystkie wyżej wymienione niedociągnięcia wersji poprzedniej i wprowadzała w związku z tym nowe grupy obiektów:

1. Obiekty transmisji – do gromadzenia informacji i statystyk pracy mediów transmisyjnych,

2. SNMP – statystyki obciążenia węzłów sieci i natężenia ruchu.

Protokół SNMP – MIB-II

SMI SNMPv3

Specyfikacja bazy danych MIB od tej wersji weszła do specyfikacji standardu SNMP.

Baza danych tak jak poprzednio jest zbudowana z modułów. Liczba modułów cały czas rośnie i w 2002 roku przekroczyła 100, zaś ilość obiektów w nich zawartych była większa niż 100 tysięcy.

Dodatkowo rośnie też liczba modułów MIB zdefiniowanych przez poszczególnych producentów sprzętu, konsorcja i grupy rozwojowe

Protokół SNMP – zalety

Największą zaletą SNMP jest jego popularność - praktycznie każde zarządzalne urządzenie sieciowe wyposażone jest w agenta SNMP. Umożliwia to zastosowanie jednolitej metodyzarządzania dla wszystkich urządzeń pracujących w sieci.

Druga zaleta to elastyczność i rozszerzalność, wsparta klarownym mechanizmem przekazywania charakterystyki agenta do programu zarządzającego w postaci plików ASN.1.

Dużymi zaletami są także stosunkowo małe dodatkowe obciążenie sieci generowane przez sam protokół oraz niskie koszty wdrożenia do eksploatacji.

Protokół SNMP – wady

Implementowanie protokołu jest dość skomplikowane, być może adekwatne byłoby użycie w nazwie słów "umiarkowanie prosty".

SNMP nie należy również do najbardziej efektywnych - każdy komunikat jest opatrzony numerem wersji SNMP i zawiera wiele deskryptorów, dodatkowo identyfikatory zmiennych przesyłane są w postaci ciągów znaków. Wszystko to wiąże się z koniecznością transmisji sporych ilości niekoniecznie potrzebnych danych.

Słabość w kwestiach związanych z bezpieczeństwem (wersje pierwsza i druga). Jedyne zabezpieczenie w tym protokole, tzw. community string będący de facto hasłem, jest wysyłany poprzez sieć w postaci niezaszyfrowanej. Pozwala to na jego podsłuchanie przy użyciu programów typu sniffer.

SNMPv3 znacząco poprawia bezpieczeństwo protokołu poprzez wprowadzenie bardziej zaawansowanych metod uwierzytelniania

Protokół SNMP – podsumowanie

Mimo wszystko jednak SNMP dowiódł przez lata swej skuteczności, co usuwa jego niedostatki na dalszy plan. O ile proste narzędzia sieciowe, takie jak ping, rsh i netstat czy okresowe sprawdzanie urządzeń telnetem mogą dostarczyć sporej ilości informacji o stanie sieci, o tyle SNMP pozostaje jedyną efektywną metodą zarządzania dużymi sieciami.

Biorąc pod uwagę powszechność protokołu i wzajemną zgodność oprogramowania i urządzeń, SNMP raczej nie ma alternatywy - dotyczy to znacznej części funkcji zarządzania sieciami.


End