

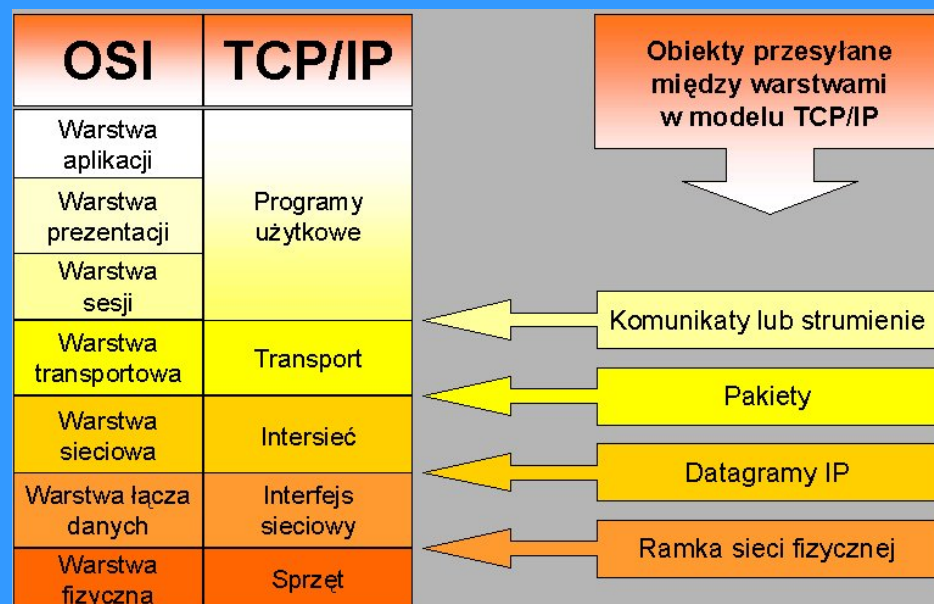
SNMP

***Simple Network Management
Protocol***

SNMP (Simple Network Management Protocol) jest obecnie najczęściej stosowanym protokołem komunikacyjnym używany do zarządzania.

Protokół powstał w 1989 r. z inicjatywy organizacji Internet Activities Board, a jego protoplastą był protokół SGMP (Simple Gateway Management Protocol).

SNMP używa do przesyłania pakietów w sieciach Internet dwóch protokołów komunikacyjnych wchodzących w skład TCP/IP: protokołu IP (Internet Protocol; warstwa sieci w modelu OSI) i UDP (User Datagram Protocol – bezpołączeniowy protokół posługujący się tzw. datagramami; warstwa transportowa w modelu OSI). Protokół SNMP jest opisany w RFC 1157.



SNMP Protokół zarządzania siecią (*Simple Network Management Protocol*)

SNMP jest jednym z najważniejszych zbiorów norm definiujących protokoły, usługi i bazy danych potrzebne do zarządzania sieciami TCP/IP. Na tą złożoną strukturę składają się cztery zasadnicze części:

- ❑ *Stacja zarządzania SMN (Station Management Network)*
- ❑ *Agent zarządzania*
- ❑ *Baza informacji MIB (Management Information Base)*
- ❑ *Protokół zarządzania siecią SNMP*

Stacja zarządzania SMN (*Station Management Network*)

Jest to najczęściej samodzielne urządzenie z oprogramowaniem menadżera systemu zarządzania siecią.

SMN dysponuje bazą informacji pochodzących z różnych zarządzanych jednostek oraz aplikacjami:

- analizującymi ruch,
- tworzącymi statystyki,
- korygującymi błędy itp..

Agent zarządzania

Jest to program instalowany na jednostce zarządzającej – routerze, przełączniku, zasilaczu UPS czy serwerze.

Każdy agent musi używać protokołu SNMP, UDP i IP.

W systemach, gdzie część urządzeń nie używa SNMP, funkcjonuje agent zastępczy proxy.

Baza informacji MIB (*Management Information Base*)

Baza informacji MIB opisuje obiekty zaimplementowane w określonym węźle sieci (ruterze, przełączniku itp.).

- Baza ta jest niezależna od protokołu SNMP.
- Zasoby sieci są reprezentowane przez obiekty.
- Każdy obiekt jest zmienną charakteryzującą jedną cechę zarządzania agenta. Zbiór tych cech stanowi bazę MIB. Obiekt może na przykład reprezentować tablicę adresów gromadzonych w węźle.
- Obiekt jest rozpoznawany po identyfikatorze OID (*Object Identifier*)

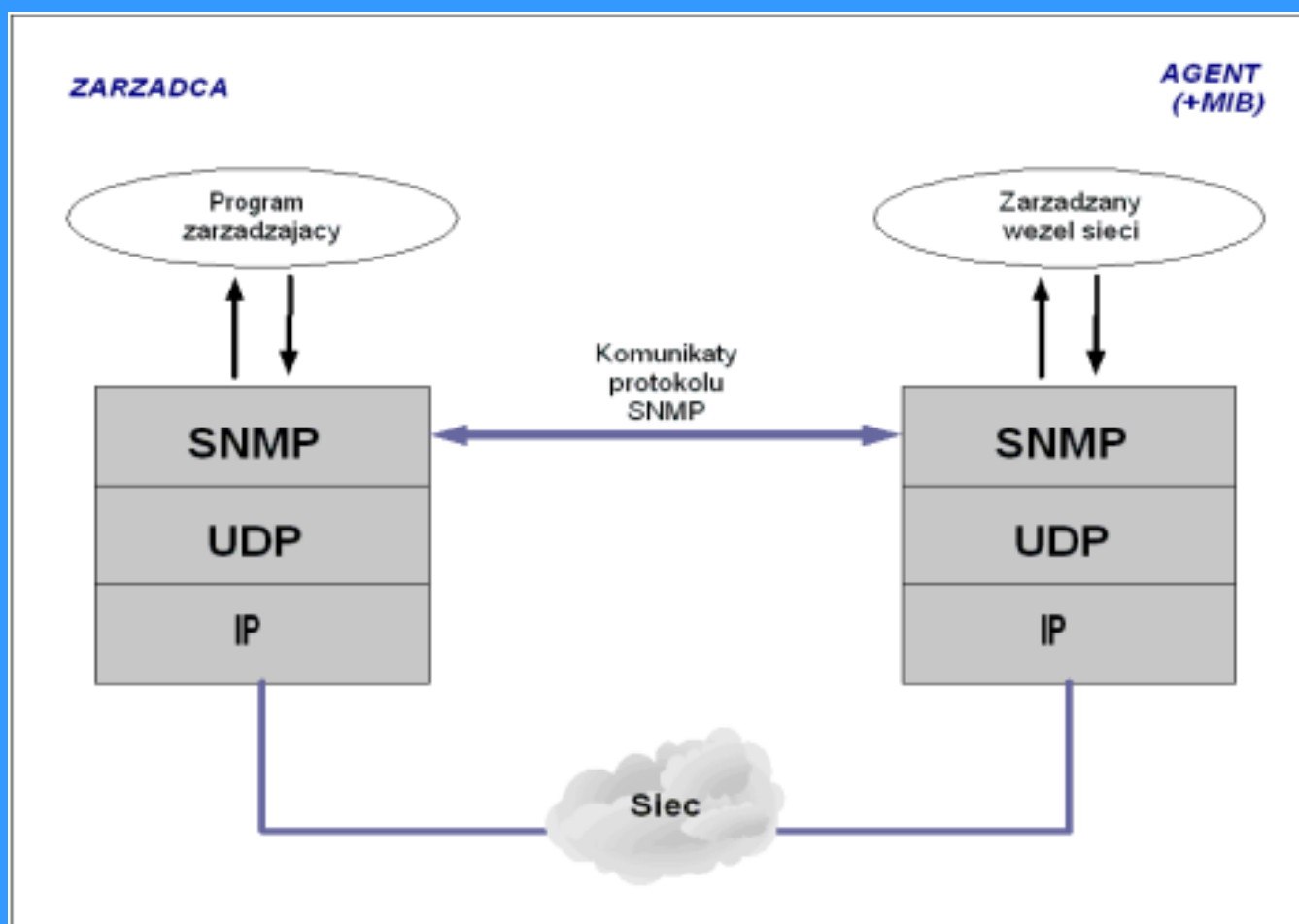
Protokół zarządzania siecią SNMP

Protokół zarządzania siecią - SNMP używany jest do przenoszenia informacji zarządzających między jednostkami SNMP.

- Wymiana informacji między menedżerem i agentem oraz między menedżerami ma formę komunikatu SNMP.
- Protokół SNMP nie ma ustalonego pakietu.
- Na ruch SNMP składają się pakiety przenoszące ściśle zdefiniowaną sekwencję SNMP, umieszczane w polu
- *Dane* protokołu UDP, który z kolei jest przenoszony przez IP.

Architektura SNMP

Integralną częścią systemu zarządzania opartego na protokole SNMP jest zawsze menedżer zarządzania (aplikacja zarządzająca siecią, rezydująca w pamięci komputera pełniącego rolę zarządcy) oraz bazy danych MIB (Management Information Base) i agenci instalowani w poszczególnych węzłach sieci.



Interfejs SNMP

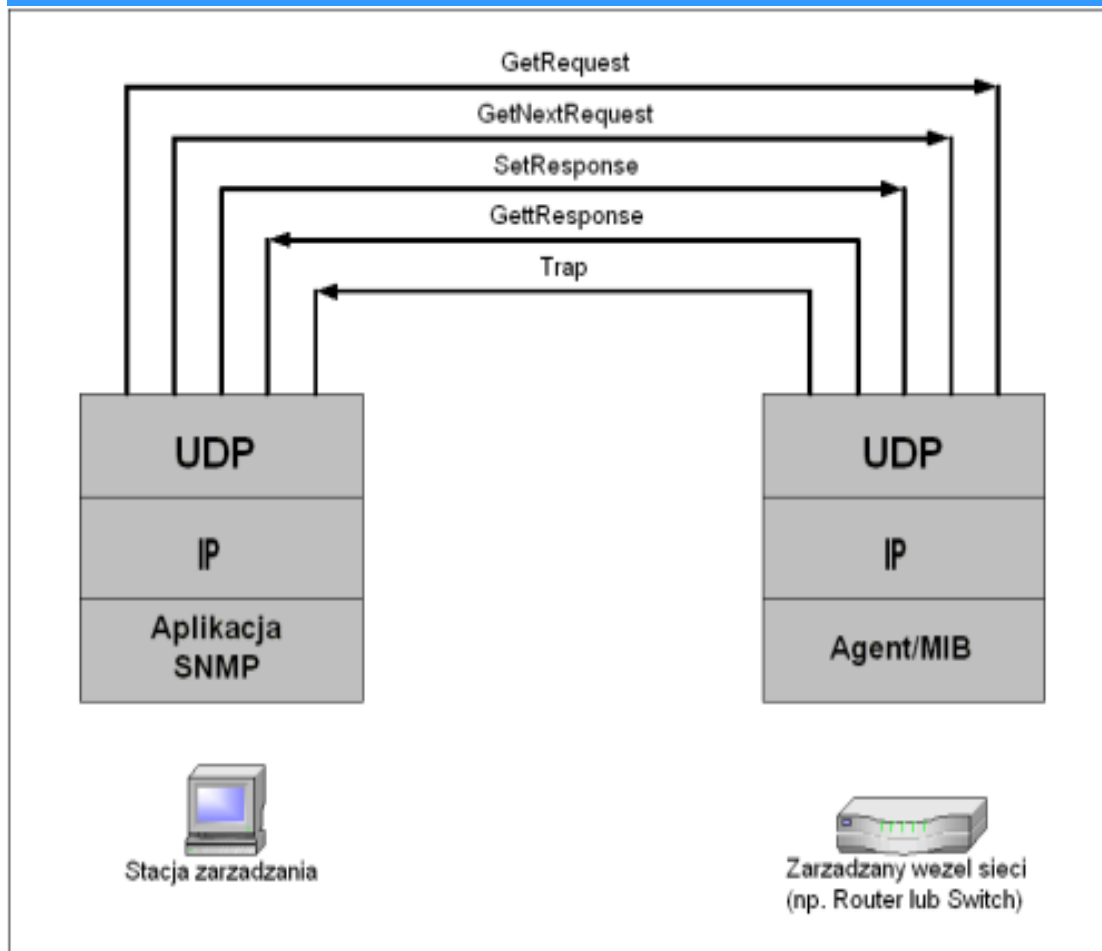
Funkcję interfejsu pomiędzy operatorem i systemem zarządzania zasobami systemowymi pełni stacja zarządzająca.

W interfejsy SNMP wyposażone są zarówno stacje zarządzające jak i zarządzane węzły sieci. Mówiąc najprościej, interfejs jest zbiorem poleceń wysyłanych do zarządzanej stacji (celem uzyskania przez stację zarządzającą interesujących ją informacji).

Stacja zarządzana z kolei wysyła w pewien uporządkowany sposób te informacje do stacji zarządzającej. Czyli jest to swego rodzaju prosty język, za pomocą którego zainstalowane w sieci węzły i urządzenia porozumiewają się z pakietem SNMP.

Polecenia protokołu SNMP

Standard SNMP definiuje pięć formatów jednostek danych, zwanych jednostkami PDU (Protocol Data Units)



- **Get Request**- stacja zarządzająca żąda od węzła wysłania danych o statusie obiektu
- **Get Next Request**- polecenie podobne do poprzedniego z tą różnicą, że baza danych MIB (Management Information Base) przeglądana jest po kolei sekwencyjnie
- **Get-response** - zwracany jest jako odpowiedź na get-request, get-next-request or set-request
- **Set Request**- polecenie żądające od agenta dokonania zmian w określonym obszarze bazy danych MIB
- **Trap**- agent powiadamia stację zarządzającą o pojawieniu się określonego zdarzenia, które wystąpiło podczas pracy węzła sieci.

Struktura informacji generowanych przez SNMP



Każda wiadomość generowana przez SNMP zawiera:

- numer wersji SNMP
- nazwę wspólnoty wymieniającej informacje
- jeden z pięciu typów PDU (*Protocol Data Units*)

Jednostki PDU (*Protocol Data Units*)

Typ PDU	RequestID	0	0	Variablebindings
---------	-----------	---	---	------------------

PDU GetRequest, GetNextRequest, SetRequest

Typ PDU	RequestID	Error-status	Error-index	Variablebindings
---------	-----------	--------------	-------------	------------------

PDU GetResponse

Typ PDU	enterprise	Agent address	Generic trap	Specific trap	Time stamp	Variable-bindings
---------	------------	---------------	--------------	---------------	------------	-------------------

PDU trap

name1	value1	name2	value2	namen	valuen
-------	--------	-------	--------	-------	-------	--------

variablebindings

PDU typów *GetRequest*, *GetNextRequest* i *SetRequest* posiadają identyczny format jak

GetResponse PDU, przenosząc pola error-status i error-index ustawione wartościami 0.

Konwencja ta ogranicza ilość formatów wykorzystywanych przez SNMP do jednego.

Przeznaczenie pól informacyjnych

Pole	Opis
<code>version</code>	Wersja SNMP (RFC 1157 definiuje wersję 1)
<code>community</code>	Skojarzenie agenta SNMP ze zbiorem jednostek aplikacyjnych. Nazwa wspólnoty jest wykorzystywana do celów uwierzytelniania
<code>request- id</code>	Wyróżnik kolejnych żądań, które są obsługiwane równolegle
<code>error - status</code>	Wskazanie statusu przetwarzania żądania. Możliwe wartości: <code>noError</code> (0), <code>tooBig</code> (1), <code>noSuchName</code> (2), <code>badValue</code> (3), <code>readOnly</code> (4), <code>genErr</code> (5)
<code>error- index</code>	Przy różnym od zera statusie może dostarczać informacje o zmiennej z listy, która spowodowała wystąpienie błędu (zmienna stanowi reprezentację zarządzanego obiektu).
<code>variablebindings</code>	Lista nazw zmiennych oraz odpowiadających wartości. W niektórych przypadkach (np. <code>GetRequest PDU</code>) wartość pola wynosi <code>null</code> .
<code>Enterprise</code>	Typ obiektu, który wyzwolił pułapkę (bazuje na <code>sysObjectID</code>)
<code>agent-addr</code>	Adres obiektu, który wyzwolił pułapkę
<code>generic-trap</code>	Typ pułapki. Możliwe wartości: <code>coldStart</code> (0), <code>warmStart</code> (1), <code>linkDown</code> (2), <code>linkUp</code> (3), <code>authentication-Failure</code> (4), <code>egpNeighborLoss</code> (5), <code>enterprise-Specific</code> (6)
<code>specific -trap</code>	Kod pułapki typu <code>specific</code>
<code>time-stamp</code>	Czas pomiędzy (re)inicjalizacją jednostki i wyzwoleniem pułapki. Zawiera wartość <code>SysUpTime</code> .

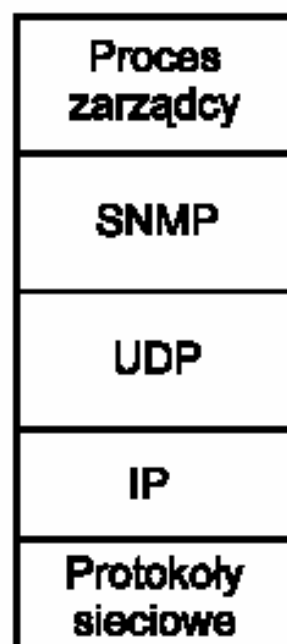
Agent zastępczy

W aplikacjach SNMP zarządzających sieciami spotykamy się nieraz z definicją agenta *proxy*. Agent tego rodzaju jest instalowany w tych węzłach sieci, czy stacjach roboczych, które nie wspierają standardowych rozwiązań proponowanych przez SNMP. Aby jednak można było nimi zarządzać przy użyciu aplikacji SNMP wymyślono agenta zastępczego, zwanego proxy.

Jest to właściwie specyficznego rodzaju konwerter, tłumaczący polecenia generowane przez SNMP na postać zrozumiałą przez zarządzaną stację. Jest to bardzo cenna opcja, pozwalająca zarządzać tymi urządzeniami sieciowymi, których konstrukcja nie jest przygotowana na wsparcie systemu SNMP.

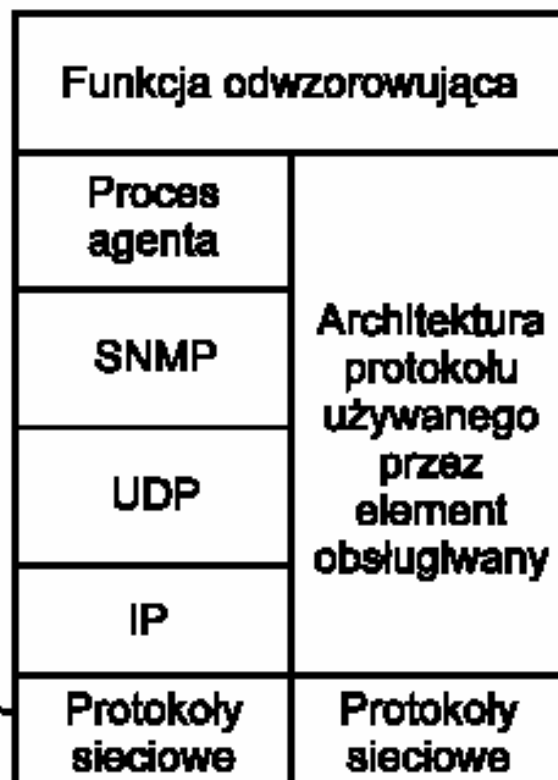
Schemat agenta zastępczego

**Stacja
zarządzająca**



Sieć

Agent proxy



Sieć

**Element
obsługiwany**



Przeglądanie pułapkowe

Jeśli stacja zarządzania nadzoruje dużą liczbę agentów, z których każdy obsługuje wiele obiektów, niemożliwa jest realizacja scenariusza regularnego odpytywania. W takim przypadku stosowana jest zmodyfikowana procedura, określana jako przeglądanie zorientowane na pułapkowanie (*trap-directed polling*).

W trakcie inicjalizacji, a także co pewien ustalony odstęp czasu (np. raz dziennie), stacja zarządzająca odpytuje wszystkich agentów, żądając przekazania kluczowych informacji. Ustanowienie tak rozumianej ogólnej orientacji na temat zarządzanego systemu pozwala na rezygnację z periodycznego przeglądania, które zostaje zastąpione przez opcję indywidualnego informowania aplikacji zarządzającej przez poszczególnych agentów.

Baza danych MIB (*Management Information Base*)

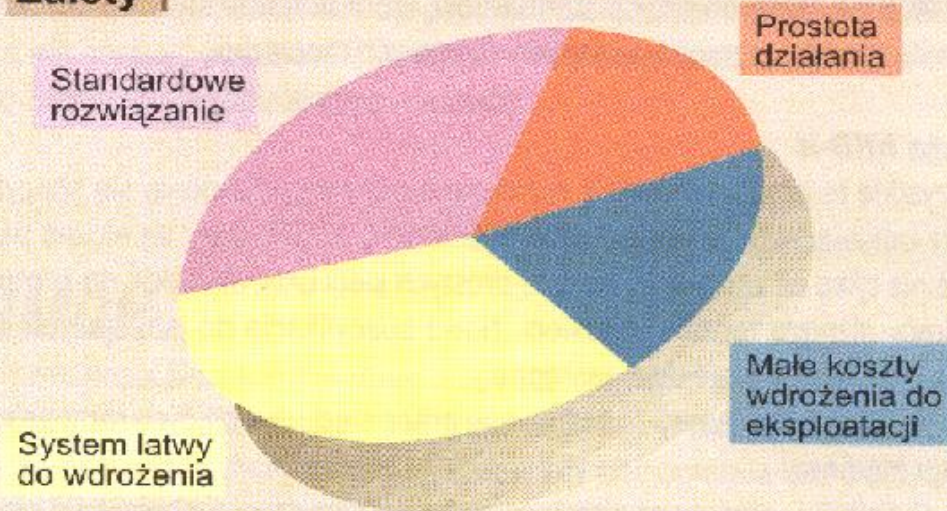
W bazie danych MIB znajdują się informacje o pracy tego urządzenia. Są to dane statyczne, identyfikatory urządzeń, tablice marszrut i szereg innych zmiennych, które są okresowo aktualizowane przez agenta i wysyłane do stacji zarządzającej. Informacje te pozwalają stacji zarządzającej sprawdzać stan węzła, śledzić poziom obciążenia sieci pakietami czy wykrywać awarie. Budowa standardowej bazy danych MIB jest opisana w RFC 1213.

Standardowa baza MIB składa się z blisko 100 definicji. Można podzielić je na osiem grup, zawierających innego rodzaju obiekty:

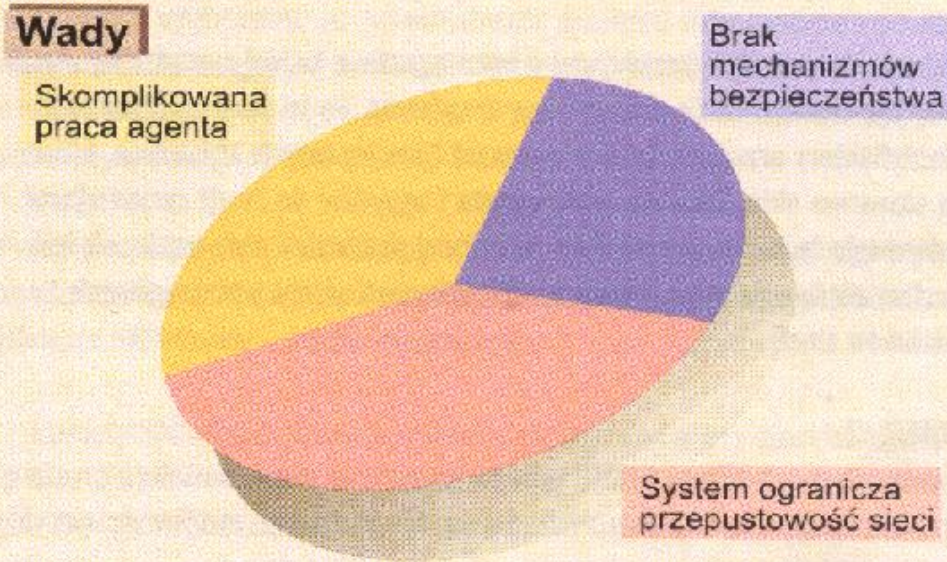
- **Obiekty systemowe**- zawierają informacje o statusie zarządzanych urządzeń.
- **Interfejsy**- informacje o interfejsach.
- **Tablice translacji**- konwersja adresów protokołu IP na inne protokoły.
- **IP**- obiekty protokołu Internet Protocol.
- **ICMP**- obiekty protokołu Internet Control Protocol.
- **TCP**- obiekty protokołu TCP (Transmission Control Protocol).
- **UDP**- obiekty protokołu UDP (User Datagram Protocol).
- **EGP**- obiekty protokołu EGP (Exterior Gateway Protocol).

Zalety i wady SNMP

Zalety



Wady



Zalety SNMP:

- stosunkowo małe obciążenie sieci pakietami (wykorzystanie UDP),
- instalowane w węzłach programy zajmują mało miejsca w pamięci,
- protokół pozwala kontrolować liczbę generowanych przez stację zarządzania powtórzeń żądań obsługi oraz czas oczekiwania na odpowiedzi urządzeń,
- możliwość wychwytywania konkretnych zdarzeń (informacje typu trap),
- powszechna dostępność aplikacji opartych na protokole SNMP.

Wady:

- skomplikowana praca samego agenta
- ograniczenie przepustowości sieci
- brak mechanizmów bezpieczeństwa

SNMP V2

SNMPv2 może być wykorzystywany do realizacji zarówno scentralizowanej, jak i rozproszonej strategii zarządzania. W ostatnim przypadku, niektóre jednostki mogą funkcjonować równocześnie jako zarządca oraz agent. Oznacza to, że akceptowane są komendy z elementu nadrzędnego, które powodują bądź udostępnianie informacji przechowywanej w stacji pośredniego szczebla, bądź zbiorczych danych na temat zbioru podporządkowanych jej agentów. Stacje pośrednie mogą również w stosunku do nadrzędnych funkcjonować w trybie wyzwalań pułapek.

Rozszerzenia wprowadzone przez SNMPv2 dotyczą następujących kategorii:

- struktury informacji zarządzania (SMI);
- wymiany danych pomiędzy stacjami zarządzającymi;
- specyficznych operacji protokołu.

Funkcje SNMP V2

- Nowe Typy Danych
- Zachowana integralność lub uporządkowanie zbiorów
- Lepsze Konwencje Definicji Tekstowych
- Lepsza kontrola dodawania / kasowania rzędów w tablicy
- Określone Możliwości Producentów
- Lepsze Definicje OBJECT- TYPE
- Wymagania Zgodności MIB

Protokół wymiany danych SNMP V2

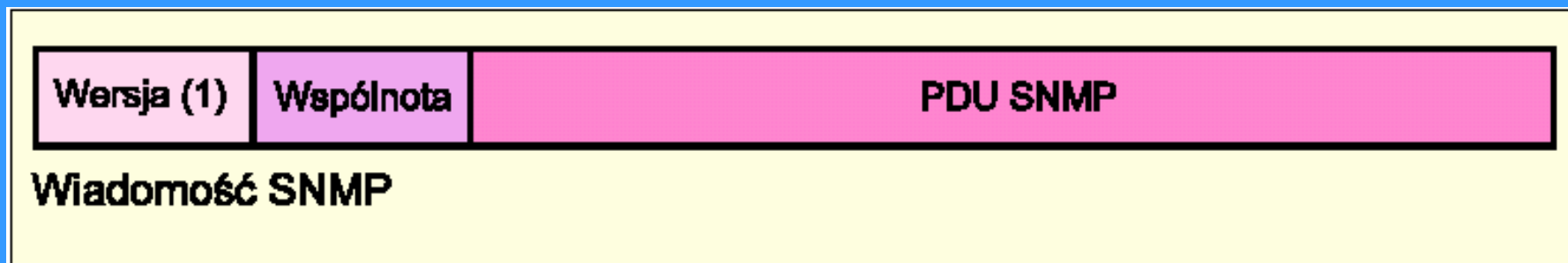
Jednostki danych protokołu SNMPv2 są, podobnie jak w poprzedniej wersji, przekazywane w ramach struktur znanych jako wiadomości. Struktury te zawierają elementy przeznaczone do realizacji funkcji bezpieczeństwa. Oznacza to, że format oraz znaczenie nagłówków wiadomości wyznacza przyjęty schemat administracyjny, stanowiący również politykę uwierzytelniania oraz zapewniania poufności.

SNMPv2 oferuje trzy typy dostępu do informacji zarządzania:

- ***Zarządca-agent; żądanie-odpowieź*** - wykorzystywany do pozyskiwania lub modyfikowania informacji skojarzonych z elementem zarządzanym.
- ***Agent-zarządca; bez potwierdzania*** - przeznaczony do powiadamiania jednostek zarządzających o wystąpieniu zdarzeń, które prowadzą do zmian informacji skojarzonej z elementem zarządzanym.
- ***Zarządca-zarządca; żądanie-odpowieź*** - tryb wzajemnego porozumiewania się jednostek zarządzających, przeznaczony do powiadamiania jednej ze stron o informacji zarządzania skojarzonej z drugim elementem.

Pierwsze dwa typy interakcji istnieją również w bazowej wersji SNMP. Jedynie ostatnia jest właściwa tylko SNMPv2.

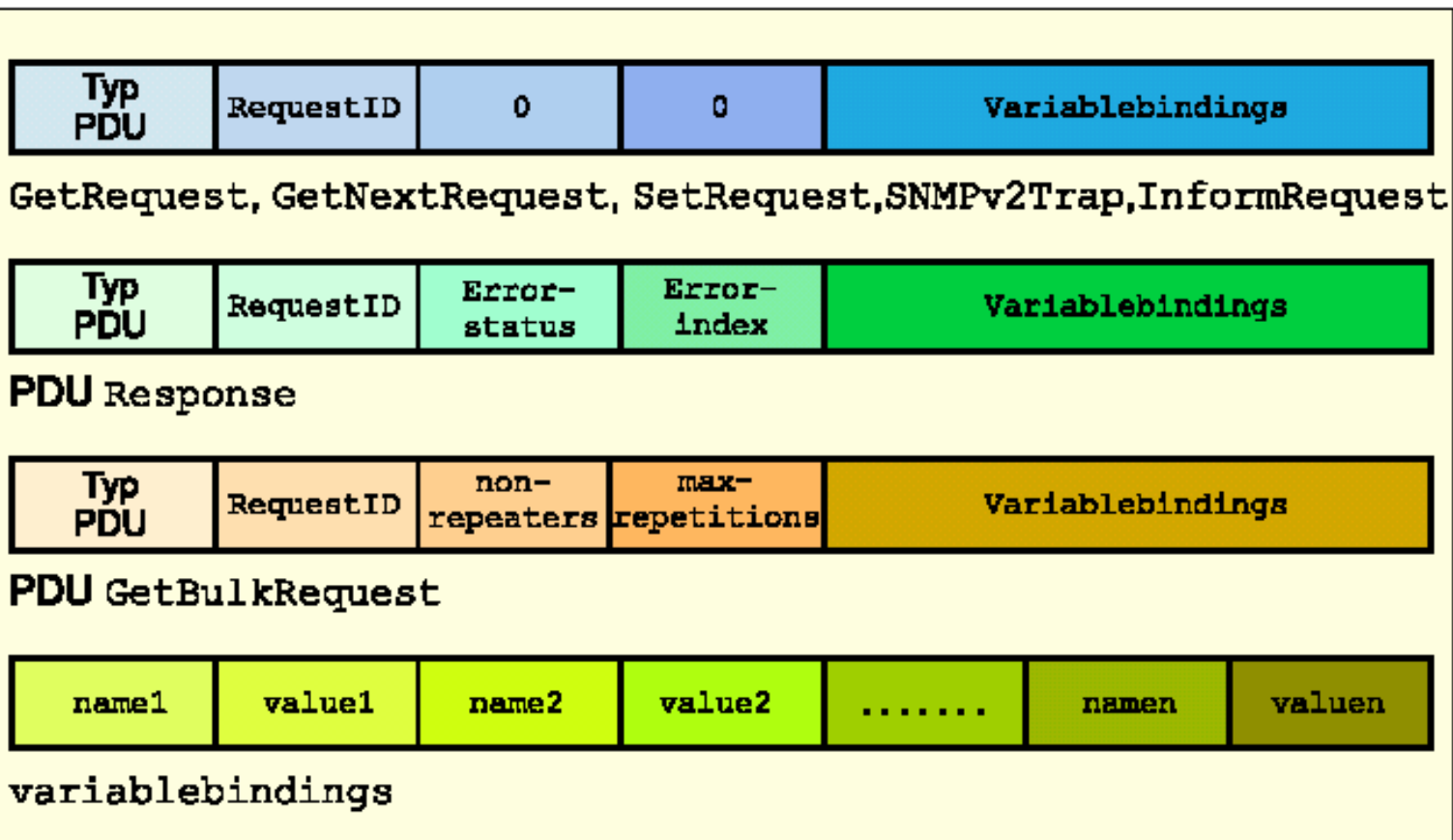
Jednostki PDU protokołu SNMPv2



Jednostki PDU protokołu SNMPv2 są przekazywane w ramach wiadomości zawierających również nazwę wspólnoty SNMP wykorzystywaną dla celów uwierzytelnienia. Wszystkie przedstawione dotychczas informacje, dotyczące nazw i profili wspólnoty oraz polityki sterowania dostępem, stosują się również do SNMPv2. W tym przypadku pole nagłówkowe version zawiera wartość 1 (SNMPv1 stanowi wersję 0). Wykorzystanie formatu wiadomości SNMPv1 jako zewnętrznej ramki jednostek PDU v2 jest określane mianem SNMPv2 bazującej na pojęciu wspólnoty (*community-based*) lub SNMPv2C.

Jednostki PDU (*Protocol Data Units*) SNMPv2

Struktura PDU SNMPv2



Jednostki typu Get Request, Get Next Request, Set Request oraz Trap posiadają taki sam format jak PDU Response i Inform Request, z polami error-status i error-index ustawionymi wartościami 0.

Wykorzystanie jednolitego formatu wiadomości pozwala na znaczne uproszczenie implementacji elementów systemów zarządzania.

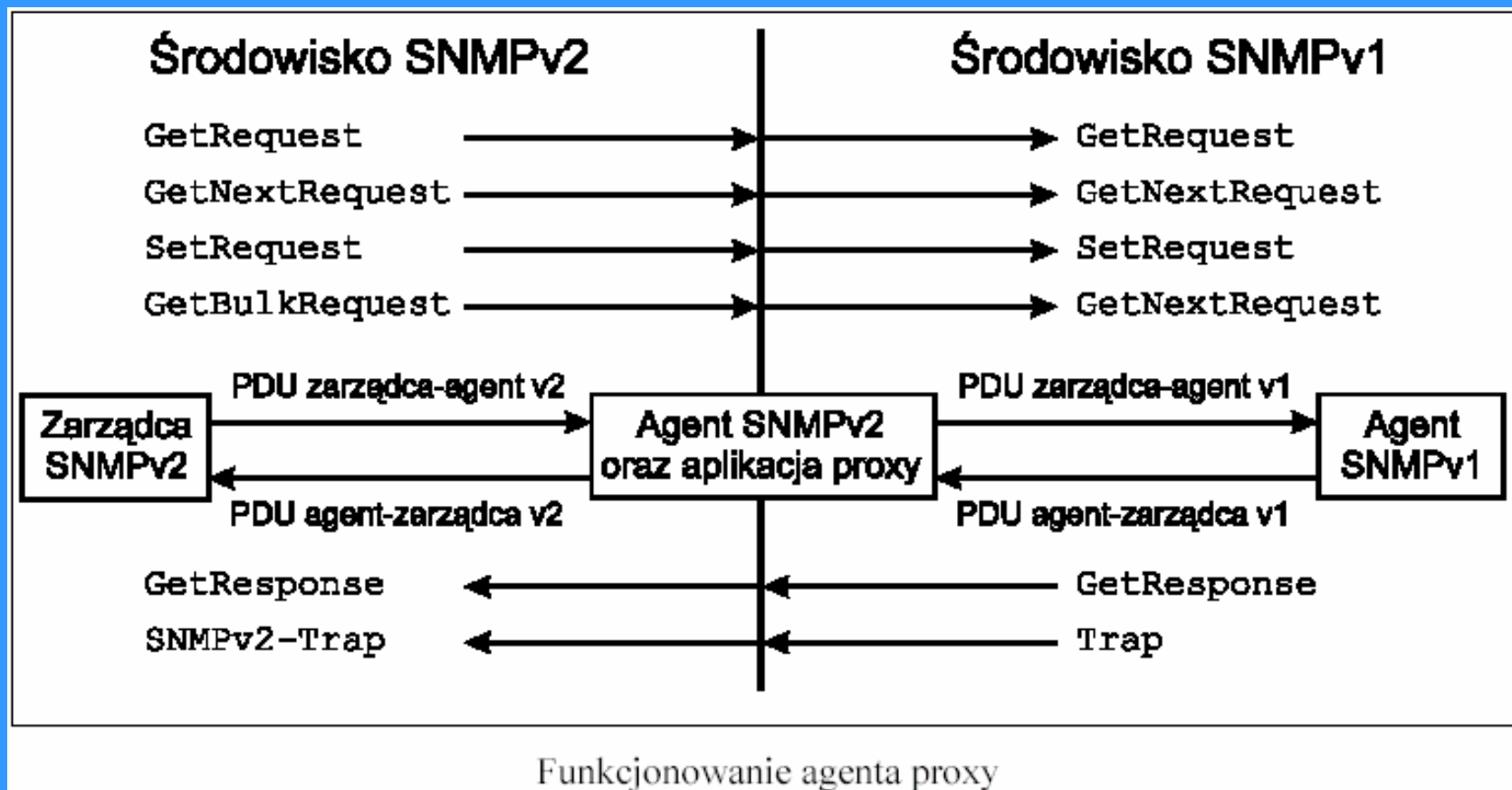
Zestawienie pól występujących we wszystkich jednostkach PDU SNMPv2 obejmuje następujące elementy:

- **request-id** - wartość tego pola w PDU stanowiącej odpowiedź musi być identyczna jak w powodującym ją żądaniu, co pozwala zarządcy na jednoznaczne ich przyporządkowanie podczas operacji wielokrotnych.
- **error-status** - wartość różna od zera wskazuje, że podczas przetwarzania żądania wystąpił wyjątek.
- **error-index** - jeśli pole error-status zawiera wartość różną od zera, pole errorindex wskazuje obiekt listy variable-bindings, który spowodował wystąpienie błędu. Pierwsza wartość listy posiada indeks 1, druga - 2 itd.
- **variablebindings** - pole umożliwia jednoczesne wywołanie operacji w stosunku do grupy reprezentacji obiektów, określonej sekwencją par wartości, z których pierwsza jest identyfikatorem, druga zaś elementem następującej listy:
 - **wartość** - stan konkretnego obiektu wskazanego w PDU typu request;
 - **unSpecified** - w żądaniu dostarczenia zawartości występuje wartość NULL;
 - **noSuchObject** - wskazanie, że agent nie obsługuje obiektu wskazanego w żądaniu;
 - **noSuchInstance** - wskazanie, że żądana reprezentacja nie istnieje;
 - **endOfMibView** - wskazanie, że podjęto próbę dostępu do obiektu o identyfikatorze wykraczającym poza zakres obsługiwany przez MIB agenta.

Porównanie PDU wersji 1 i 2 protokołu SNMP

SNMPv1	SNMPv2	Kierunek	Opis
GetRequest	GetRequest	Zarządca - agent	Żądanie wartości obiektu
GetNextRequest	GetNextRequest	Zarządca - agent	Żądanie następnej wartości
-	GetBulkRequest	Zarządca - agent	Żądanie wielu wartości
SetRequest	SetRequest	Zarządca - agent	Ustawienie wartości
-	InformRequest	Zarządca - zarządca	Przekaz bez wywołania
GetResponse	Response	Agent - zarządca lub zarządca - zarządca	Odpowiedź na żądanie zarządcy
Trap	SNMPv2-Trap	Agent - zarządca	Przekaz bez wywołania

Nowa wersja protokołu SNMP jest podobna do poprzedniej w części wykorzystującej już istniejące formaty PDU. Istotne zmiany wprowadziło natomiast zdefiniowanie operacji **GetBulkRequest** i **InformRequest**, a także modyfikacja trybu wykonywania opcji get poprzez rezygnację z jej niepodzielności. W efekcie pełna interoperacyjność jest możliwa pod warunkiem modyfikacji trybu funkcjonowania agenta proxy oraz zdefiniowaniu uniwersalnego algorytmu działania stacji zarządzającej.



Najprostszym rozwiązaniem ewolucyjnego przechodzenia na nową wersję protokołu jest pozostawienie istniejących agentów starszej wersji i komunikowanie się z nimi za pośrednictwem agentów proxy. Ich funkcje mogą realizować odpowiednio skonfigurowane aplikacje agentów SNMPv2, które pośredniczą w wymianie prowadzonej za pośrednictwem obydwu wersji protokołu.

SNMP V3

W swojej ostatecznej formie, SNMPv2 nie posiada prawie żadnych mechanizmów gwarantowania bezpieczeństwa. W celu eliminacji tej istotnej niedogodności wprowadzono do użytku kolejne rozszerzenie, znane jako SNMPv3. Określenie nowej wersji mianem „rozszerzenia” jest jak najbardziej uzasadnione, ponieważ jej specyfikacja obejmuje jedynie funkcje związane z aspektem bezpieczeństwa, odwołując się w pozostałych obszarach do uregulowań zdefiniowanych we wcześniejszych wersjach protokołu SNMP.

Trzecia wersja SNMP (SNMP v.3) opublikowana została w RFC 2271 i 2275 w Styczniu 1998 r. Wersja ta zbudowana jest na podstawie wersji poprzednich. Powiększa ona specyfikację SNMP i SNMPv2 o dodatkowe środki bezpieczeństwa i możliwości administrowania.

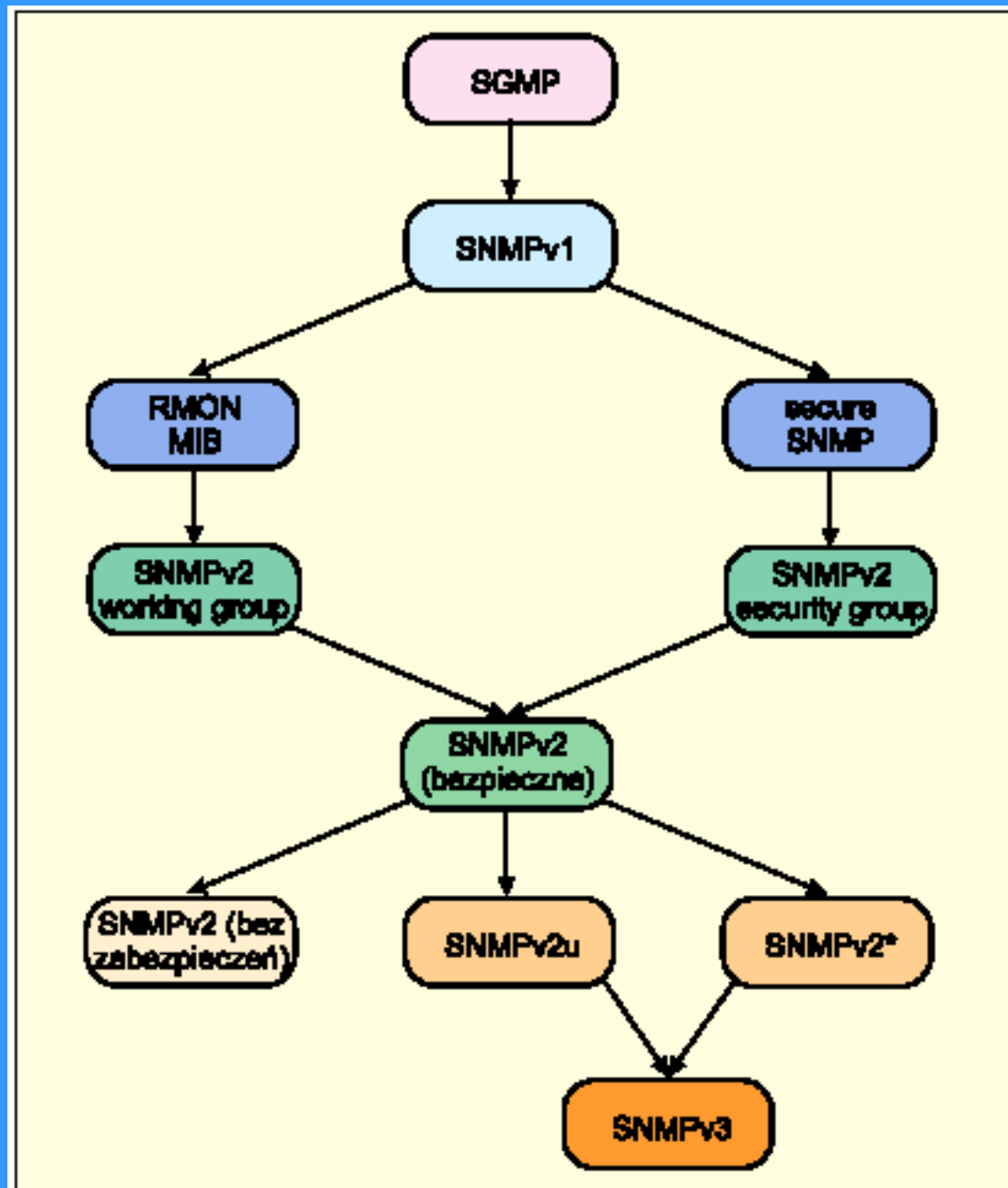
Nowe cechy SNMPv3 to np. :

Bezpieczeństwo

- autentykacja i prywatność
- autoryzacja i kontrola dostępu

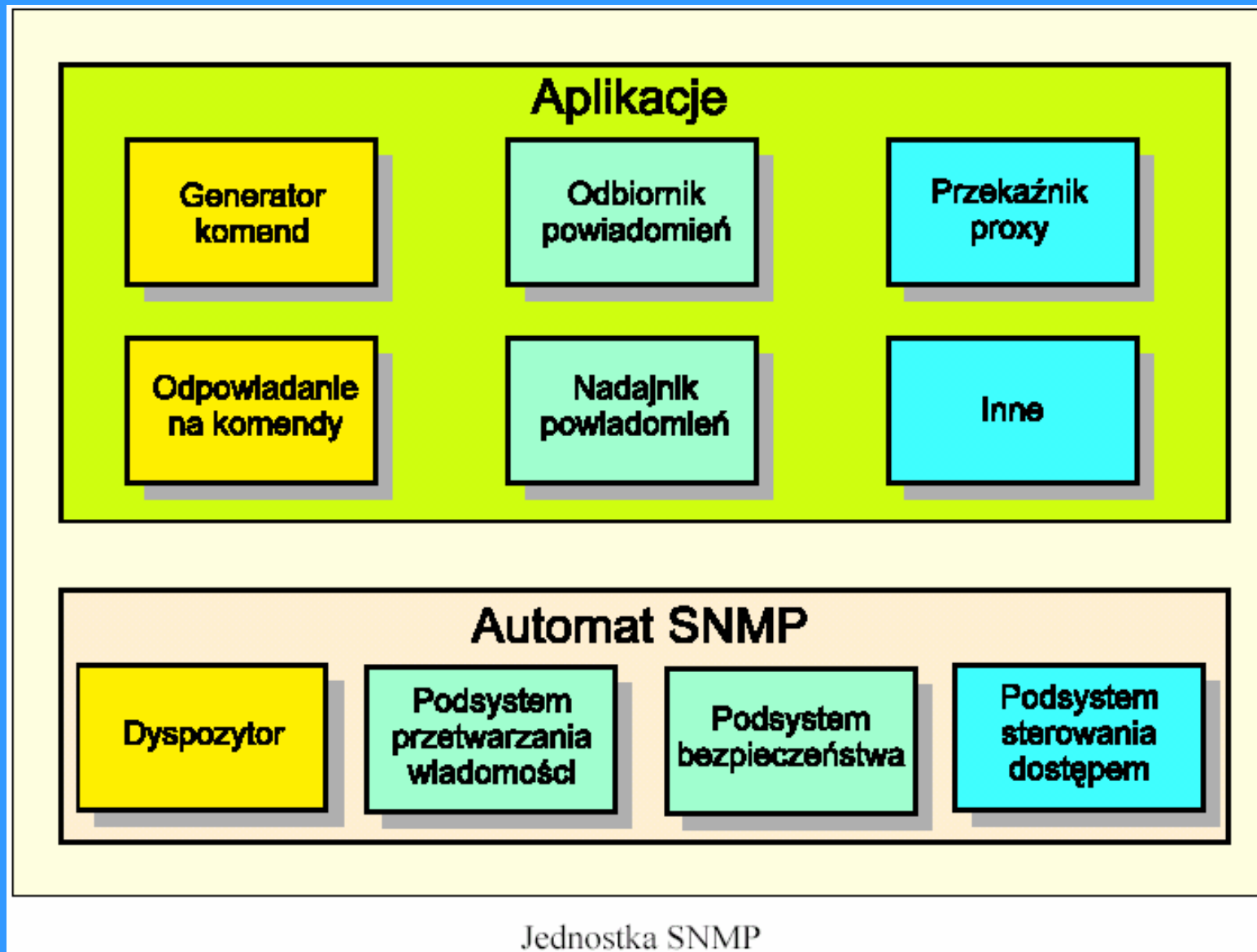
Administrowanie

- nazywanie jednostek
- nazwy użytkowników i zarządzanie kluczami
- zawiadomienie o przeznaczeniu
- związki proxy
- zdalne konfigurowanie poprzez operacje SNMP

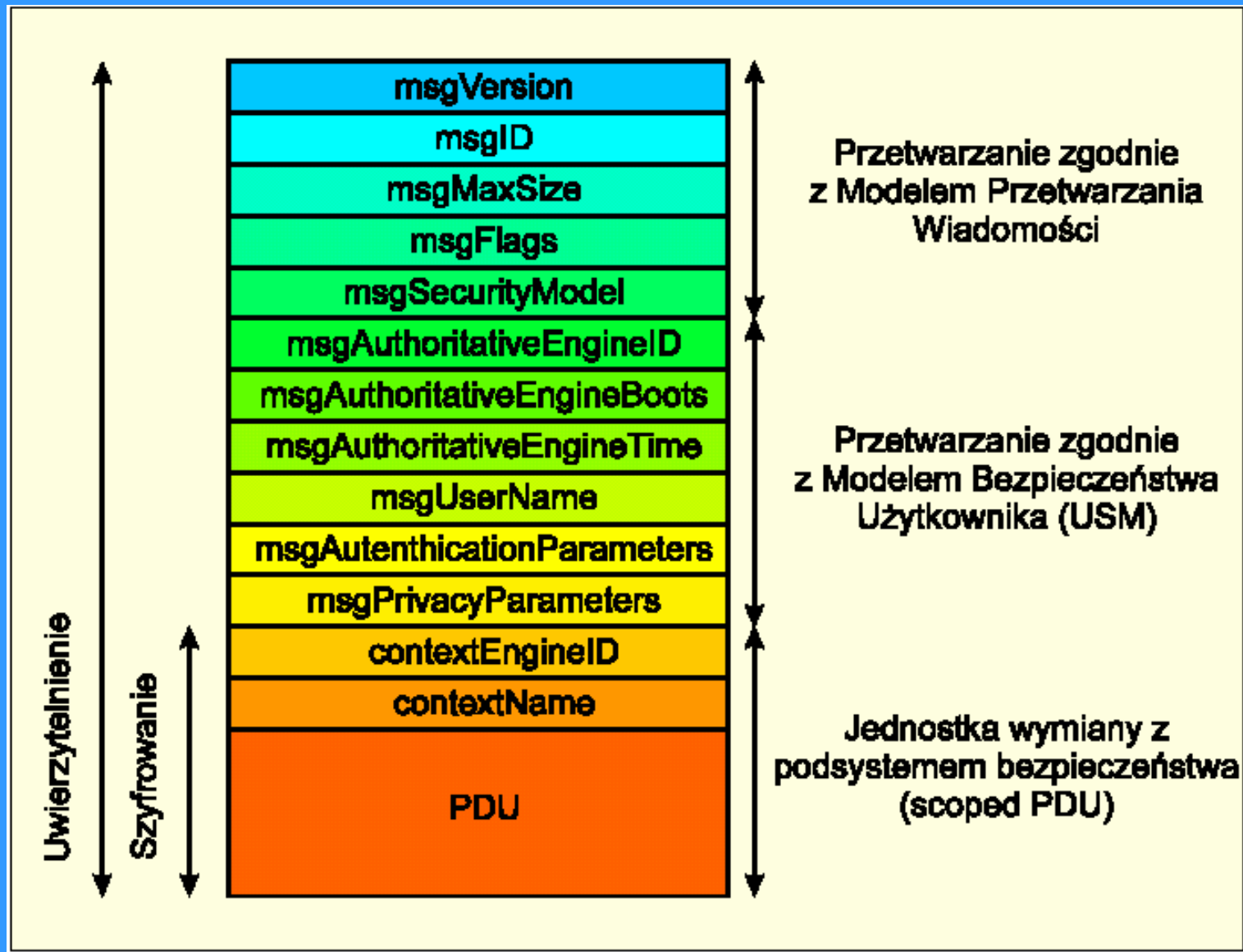


Etapy rozwojowe SNMP

Architektura SNMP



Przetwarzanie wiadomości



Struktura wiadomości SNMP V3

Podsumowanie

SNMPv2 stanowił istotne rozszerzenie SNMPv1, pozostawiające równocześnie pierwotną łatwość rozumienia mechanizmów funkcjonalnych oraz łatwość ich implementacji.

Wersja 2 została w szczególności lepiej przystosowania do funkcjonowania w rozproszonym środowisku sieciowym oraz oferuje lepsze parametry użytkowe.

Wspólne niedostatki v1 oraz v2, a zwłaszcza brak profesjonalnie realizowanych funkcji bezpieczeństwa zostały usunięte dzięki zdefiniowaniu wersji 3 SNMP, oferującej poufność, uwierzytelnianie i sterowanie dostępem. Równocześnie, dostawcy oprogramowania uzyskali większe możliwości adaptacyjne, pozwalające na lepsze dostosowanie swoich produktów do wymagań klienta.

Skróty:

- SNMP- Simple Network Management Protocol
- MIB- Management Information Base
- SGMP- Simple Gateway Management Protocol
- IP- Internet Protocol
- UDP- User Datagram Protocol
- PDU- Protocol Data Units
- TCP- Transmission Control Protocol
- RFC- Requests For Comments
- OSI- Open Systems Interconnection