PBS 08

mgr inż. Roman Krzeszewski roman@kis.p.lodz.pl
mgr inż. Artur Sierszeń asiersz@kis.p.lodz.pl
mgr inż. Łukasz Sturgulewski luk@kis.p.lodz.pl

Plan wykładu

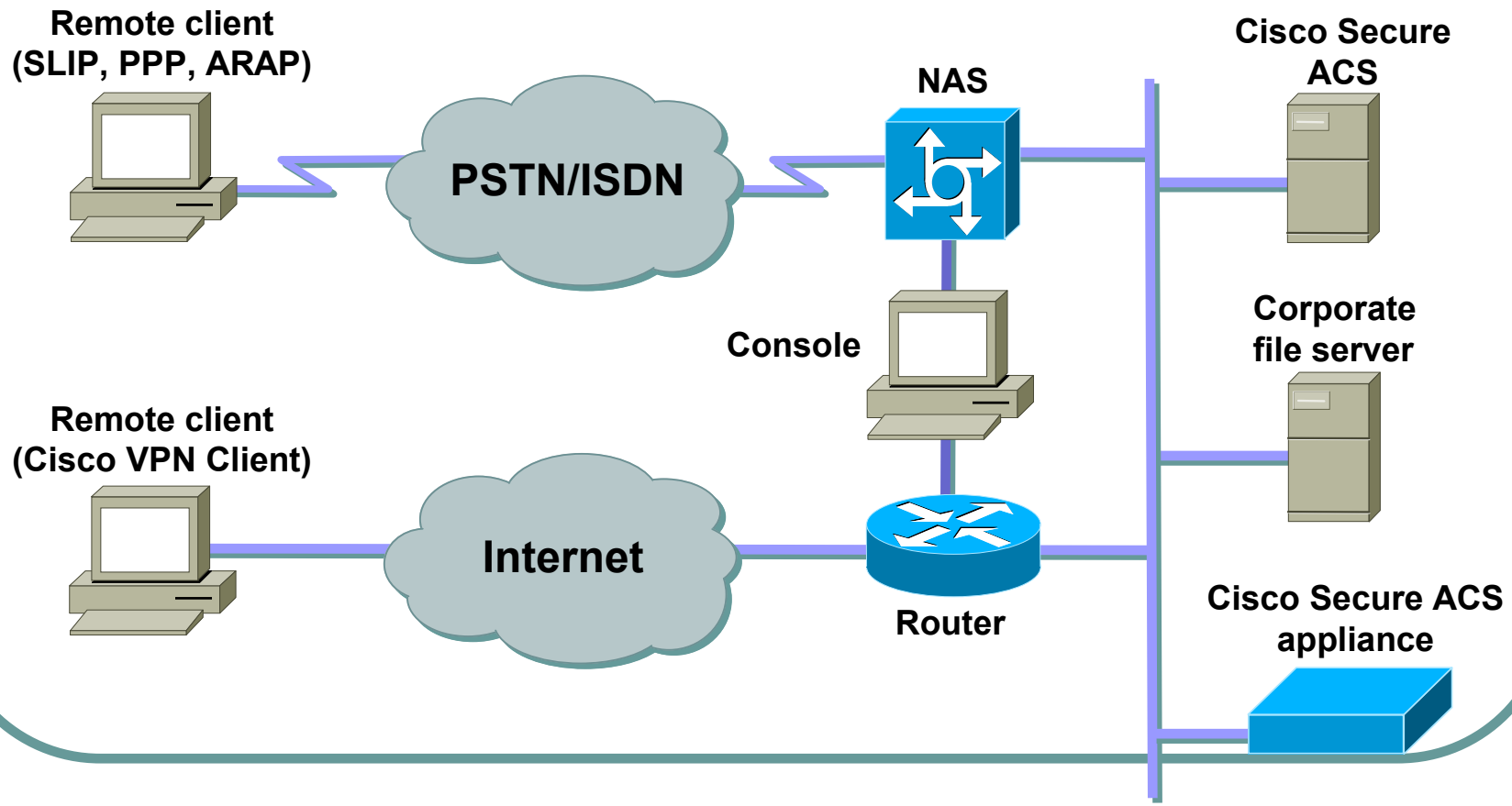
- **RADIUS** - Remote Authentication Dial-In User Service.
- **SNMP** - Simple Network Management Protocol.

Model AAA

- **A**uthentication
  - Kim jesteś?
  - "Jestem użytkownikiem *Jerzy*, potwierdzam to znanym mi hasłem"
- **A**uthorization
  - Co możesz robić? Do czego masz dostęp?
  - "Mam prawo dostępu do hosta *2000_Server* poprzez Telnet."
- **A**ccounting
  - Co robiłeś? Jak długo to robiłeś? Jak często to robisz?
  - "Pracowałem na hoście *2000_Server* poprzez Telnet przez 30 minut."

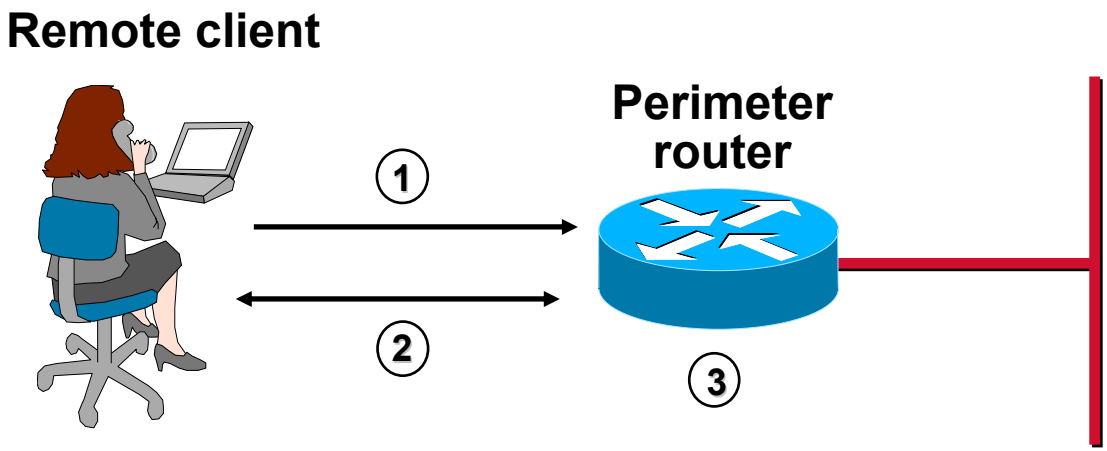
Zastosowania

- Dostęp administracyjny do urządzeń sieciowych.
- Zdalny dostęp do sieci.



Implementacja AAA

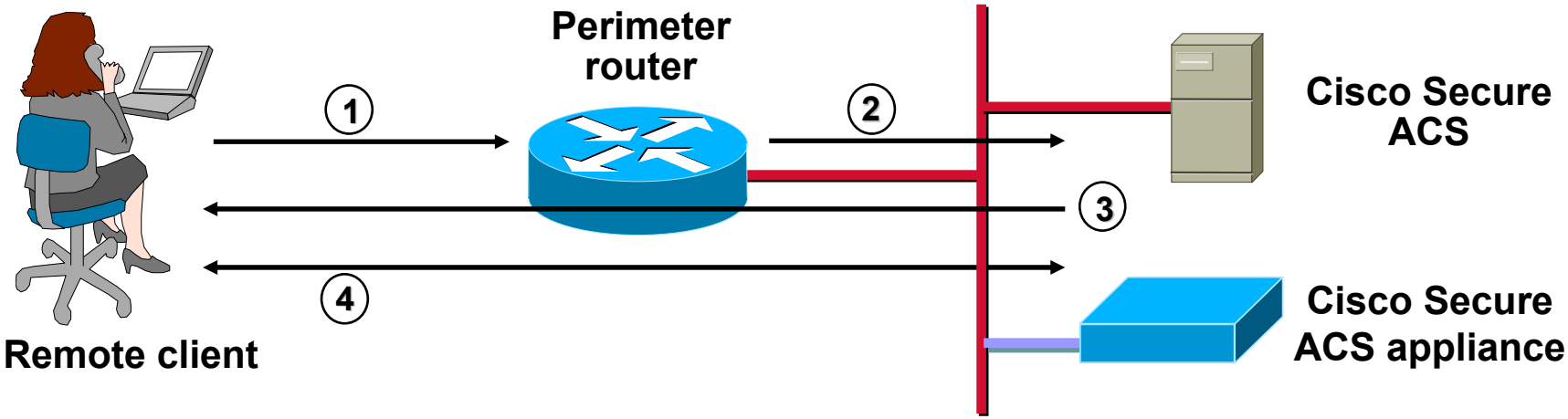
- Za pomocą lokalnej usługi.



1. Klient nawiązuje połączenie z router'em.
2. Router żąda: *username* i *password*.
3. Router autoryzuje użytkownika w lokalnej bazie danych. Użytkownik otrzymuje dostęp do sieci.

Implementacja AAA

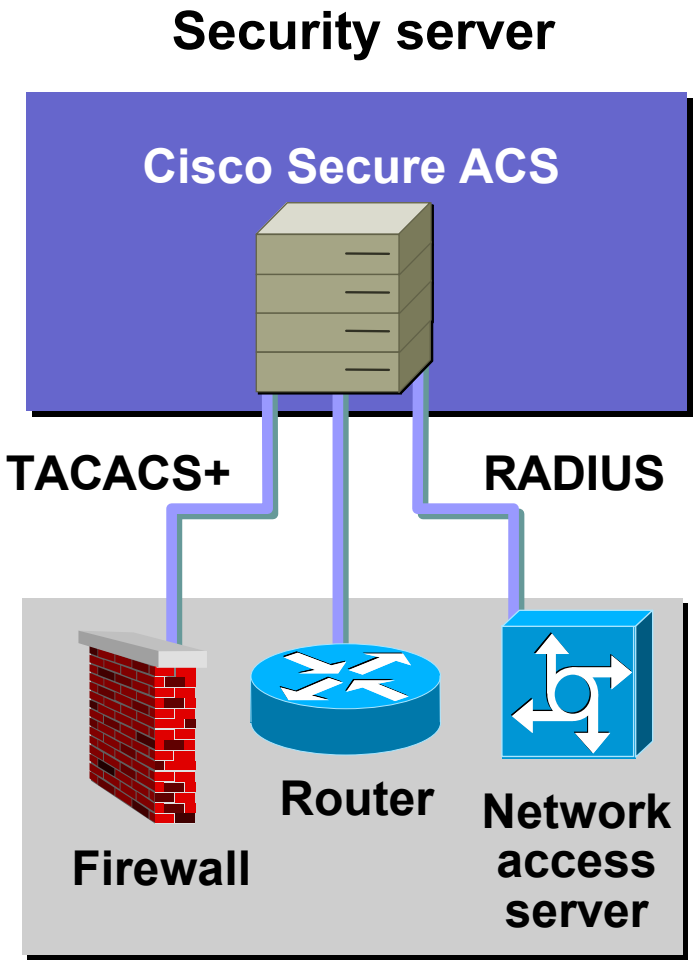
- Za pomocą zewnętrznego serwera.



1. Klient nawiązuje połączenie z router'em.
2. Router komunikuje się z zewnętrznym serwerem
3. Serwer żąda: *username* i *password*.
4. Serwer autoryzuje użytkownika w lokalnej bazie danych. Użytkownik otrzymuje dostęp do sieci.

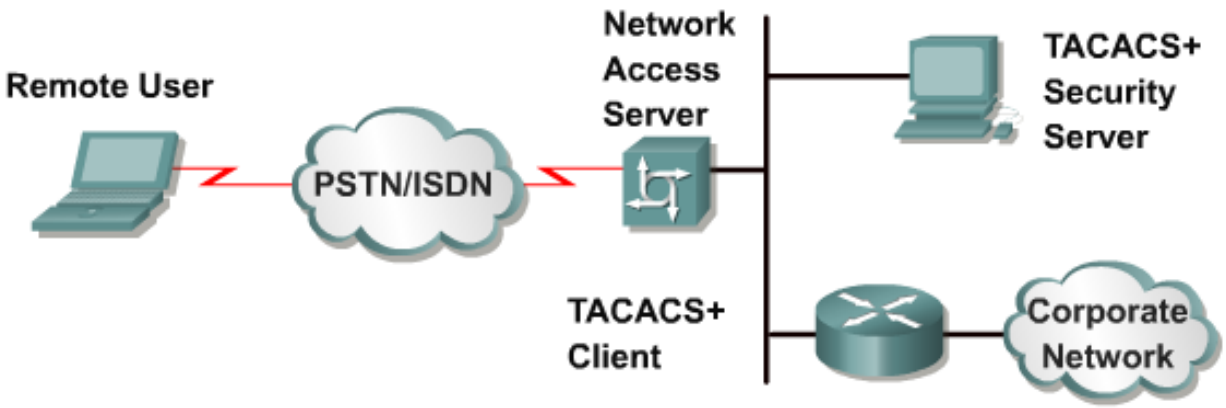
AAA – Protokoły

- Używane są dwa różne protokoły do komunikacji pomiędzy serwerami AAA a router'ami, NAS'ami, firewall'ami czy switch'ami.
- Cisco wspiera dwa rozwiązania TACACS+ i RADIUS:
  - **TACACS+** (bardziej bezpieczny od RADIUS).
  - **RADIUS** (ma lepsze API i bardziej zaawansowany *accounting*).



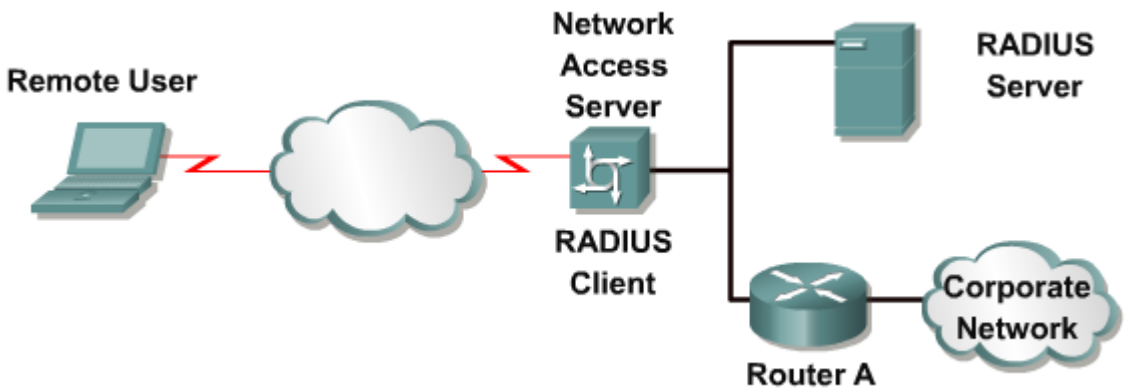
TACACS+

- TACACS+ jest rozwinięciem protokołu TACACS – możliwość niezależnego świadczenia usług AAA.
- TACACS+ został wprowadzony do Cisco IOS od wersji 10.3.
- Jest to całkowicie nowa wersja protokołu TACACS (RFC 1492) opracowana przez Cisco.
- TACACS+ został przedłożony do IETF jako projekt standardu.

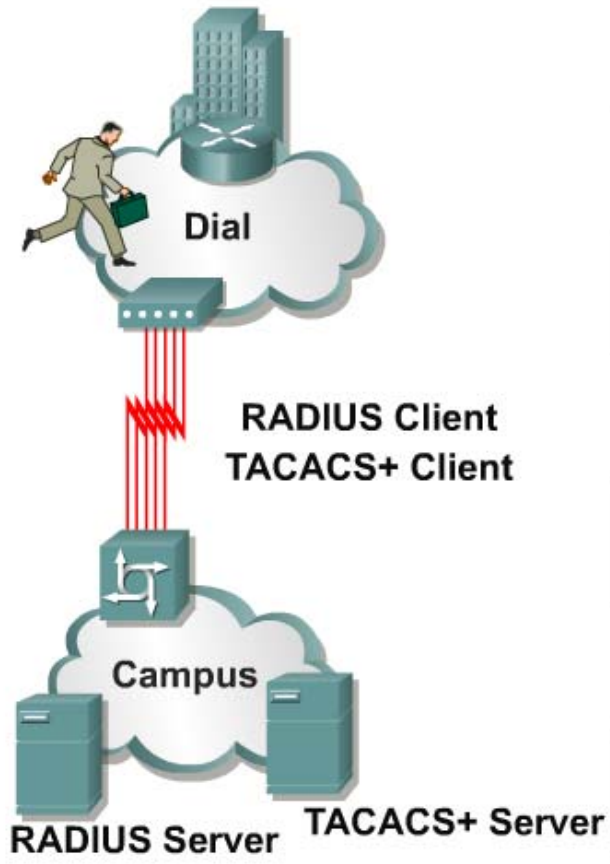


RADIUS

- Protokół RADIUS jest zdefiniowany w RFC 2138, zaś RADIUS *accounting* w RFC 2139.
- Opracowany został przez Livingston Enterprises, Inc (obecnie część Lucent Technologies).
- Zgodnie ze standardem IETF RADIUS obsługuje około 63 atrybutów.
- Lucent definiuje obecnie około 254 atrybutów. Dzięki dobrze zaprojektowanemu *Application Programming Interface* (API) możliwe jest szybkie opracowywanie nowych rozszerzeń protokołu.



TACACS+ i RADIUS



	TACACS+	RADIUS
Functionality	Separates AAA	Combines Authentication/ Authorization
Transport Protocol	TCP	UDP
CHAP	Bidirectional	Unidirectional
Protocol Support	Multi-protocol support	No ARA No NetBeui
Confidentiality	Entire Packet-Encrypted	Password-Encrypted
Accounting	Limited	Extensive

Konfiguracja

router(config)#

```
radius-server host {host_name | host address} key
  shared_secret_text_string
```

router(config)#

```
tacacs-server host ipaddress key keystring
```

```
router(config)# tacacs-server host 10.1.2.4 key
  2bor!2b@?
```

Obszary zastosowania systemów zarządzania sieciami

Kluczowe obszary zastosowania systemów zarządzania sieciami określone przez OSI:

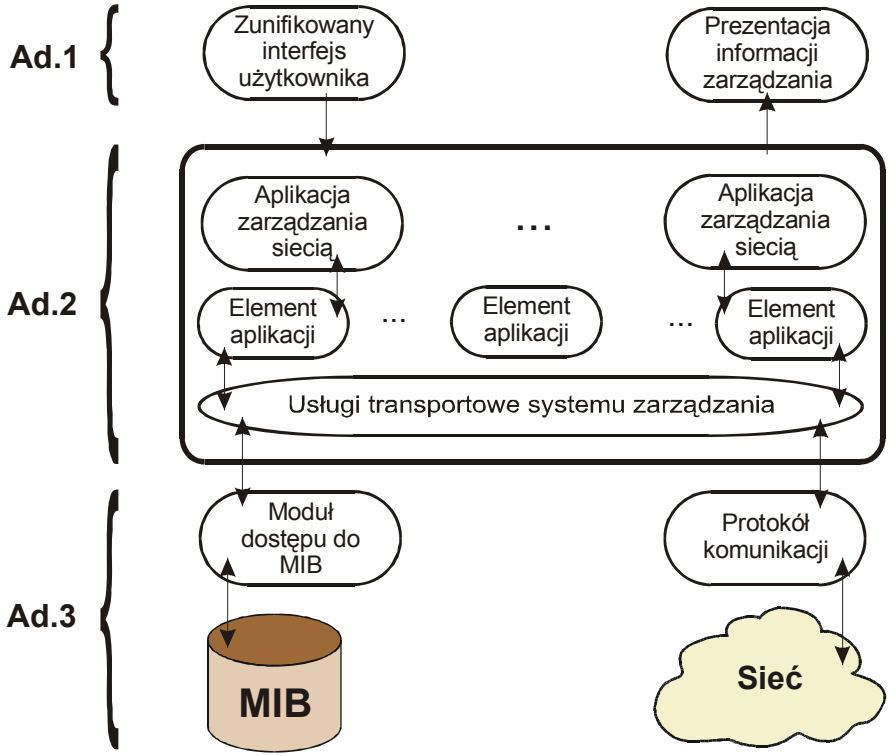
- Zarządzanie wydajnością.
- Zarządzanie uszkodzeniami, nieprawidłowościami.
- Zarządzanie kosztami.
- Zarządzanie konfiguracją i oznaczeniami.
- Zarządzanie bezpieczeństwem.

Architektura oprogramowania

Oprogramowanie zarządzania składa się z trzech głównych elementów:

- Interfejs użytkownika (oprogramowanie prezentujące dla użytkownika);
- Oprogramowanie zarządzania siecią;
- Oprogramowanie obsługujące komunikację oraz bazy danych.

Architektura oprogramowania



Rysunek 2.2 Architektura oprogramowania zarządzania siecią.

Architektura zarządzania sieciami

- Scentralizowany system zarządzania.
- Zdecentralizowany system zarządzania.

Monitoring sieci

Informacje, które są szczególnie ważne z punktu widzenia monitoringu, dotyczą:

- Analizy wydajności;
- Poprawności pracy środowiska;
- Analizy kosztów.

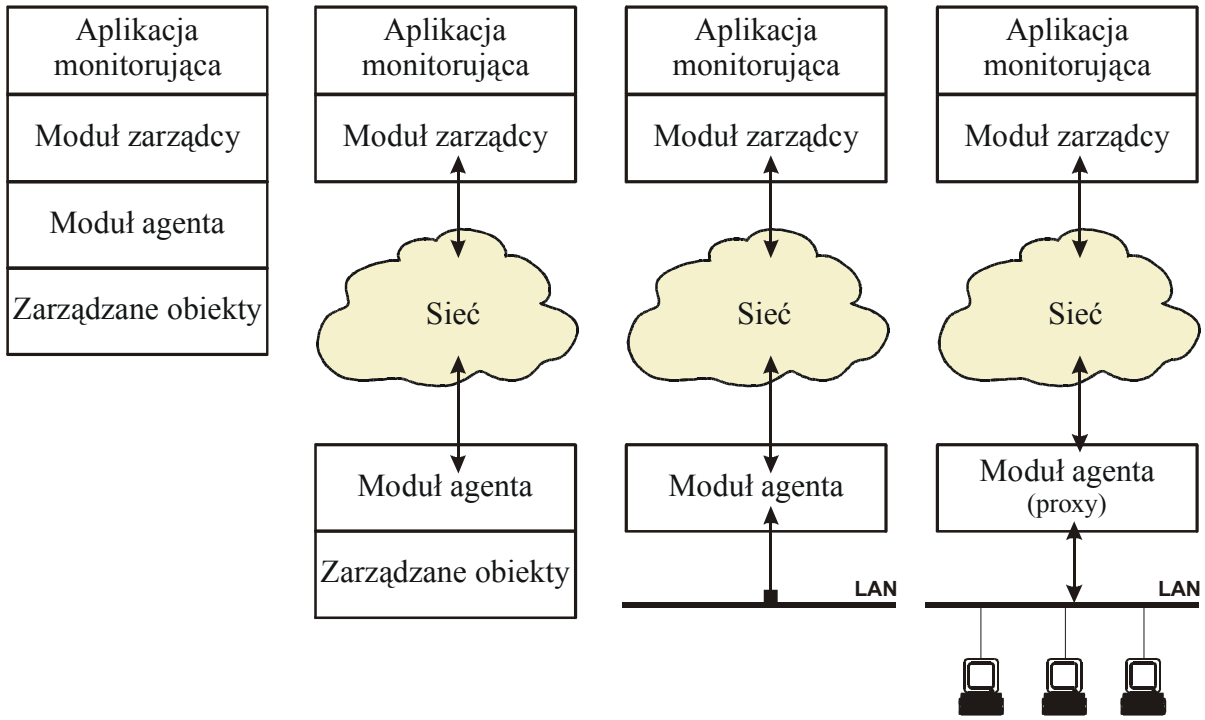
Monitoring sieci

Informacje monitoringu mogą być podzielone na trzy grupy:

- Statyczne;
- Dynamiczne;
- Statystyczne.

Informacje statystyczne są uzyskiwane na podstawie analizy danych dynamicznych i dostarczają nam informacji o zachowaniu węzła w określonym czasie np. średnia liczba utraconych pakietów w jednostce czasu.

Monitoring sieci



1. Wszystkie moduły znajdują się w jednym elemencie sieciowym

2. Najpowszechniejsze rozwiązanie. Jeden element pełni rolę zarządcy, a drugi agenta.

3. System monitorowania zawiera jednego lub więcej agentów,którzy śledzą ruch w sieci

4. Rozwiązanie wymagane dla elementów obsługujących inny protokół zarządzania niż menadżer.

Rysunek 2.6 Architektura monitoringu sieci.

Monitoring sieci

W systemach zarządzania istnieją dwa sposoby dostarczania informacji menadżerowi:

- Odpytywanie: pytanie – odpowiedź (*request - response*);
- Zgłaszanie wydarzeń;

Monitorowanie wydajności

Monitoring wydajności pozwala uzyskać odpowiedzi na następujące pytania:

- Czy ruch jest równomiernie rozłożony pomiędzy użytkownikami oraz czy istnieją pary szczególnie mocno obciążone?
- Jaki jest procentowy udział rodzajów przesyłanych pakietów?
- Jaki jest rozkład czasów opóźnień?
- Jaki jest stopień obciążenia kanału i dokładność?
- Jaka jest przyczyna błędnie przesyłanych pakietów (nieefektywny protokół, uszkodzony sprzęt)?

Uwaga

Pewną trudność stanowi wyłowienie tych wskaźników, które rzetelnie, prawidłowo opisują wydajność. Podczas ich wyboru możemy napotkać kilka problemów:

- Duża liczba wskaźników;
- Znaczenie wielu wskaźników nie jest zbyt dokładnie zrozumiałe lub jest źle interpretowane;
- Niektóre wskaźniki nie powinny być porównywane z innymi;
- Obliczanie wartości wskaźników w wielu przypadkach trwa zbyt długo, co źle wpływa na ich użyteczność dla kontroli środowiska;

Wskaźniki wydajności sieci

Dostępność.

- Procent czasu, przez który system sieciowy (wszystkie komponenty i aplikacje) jest dostępny dla użytkownika. Wysoki wskaźnik dostępności jest w wielu dziedzinach naszego życia kluczowy np. porty lotnicze, usługi medyczne czy parkiety giełdowe.
- Dostępność bazuje na niezawodności poszczególnych komponentów środowiska. Awarie komponentów są wyrażone przez średni czas pomiędzy awariami MTBF (*Mean Time Between Failure*). Czas potrzebny na jej usunięcie nazywamy średnim czasem naprawy MTTR (*Mean Time To Repair*). Dokładność *A* może być wyrażona jako iloraz:

$$A = \frac{MTBF}{MTBF + MTTR}$$

- Aby uzyskać większy stopień dostępności stosuje się rozwiązania wykorzystujące elementy nadmiarowe, co zmniejsza prawdopodobieństwo unieruchomienia całej lub istotnych części sieci.

Wskaźniki wydajności sieci

Czas odpowiedzi.

- Jest to czas potrzebny systemowi na udzielenie odpowiedzi, na żądanie wykonania określonego zadania. Często przyjmujemy, że jest to czas między zatwierdzeniem komendy przez użytkownika a rozpoczęciem wyświetlania rezultatu przez system. W zależności od typu aplikacji stawiane są różne wymagania, co do czasu odpowiedzi.
- Skracanie czasu odpowiedzi jest możliwe poprzez zwiększanie mocy obliczeniowej systemu oraz przepustowości łączy. Ważne jest także ustalenie odpowiednich priorytetów dla różnych procesów (w zależności od ważności zadań).
- Niestety powyższe przedsięwzięcia są zazwyczaj bardzo kosztowne a uzyskane efekty często nie są adekwatne do poniesionych kosztów.

Wskaźniki wydajności sieci

Dokładność.

- Określa jakość transmisji danych między elementami sieci. Korekcja błędów jest realizowana przez protokoły transmisyjne jednak analiza współczynnika błędów daje mnóstwo informacji o stanie połączenia.

Wskaźniki wydajności sieci

Wydajność.

- Aby prawidłowo powiązać wydajność projektowaną, żądaną i rzeczywistą określonego miejsca sieci należy obserwować wiele parametrów:
  - Liczba transakcji danego typu w określonym czasie;
  - Liczba sesji klientów w określonym czasie;
  - Liczba odwołań do zewnętrznego środowiska.

Wskaźniki wydajności sieci

Użytkowanie.

- Określa stopień użycia zasobu w określonym czasie. Najważniejszym zastosowaniem tego wskaźnika jest wyszukanie wąskich gardeł i przeciążeń sieci, ale także niewykorzystanych obszarów, które często są bardzo kosztowne w utrzymaniu.
- Najprostszą techniką określenia stopnia obciążenia różnych połączeń w sieci jest obserwacja różnicy między obciążeniem planowanym a bieżącym i średnim.
- Liniowy wzrost przeciążenia powoduje ekspotencjalny wzrost czasu odpowiedzi.
- Aby polepszyć wskaźniki omawianych połączeń należy:
  - Zreorganizować ruch;
  - Zbalansować planowane i rzeczywiste obciążenie;
  - Zredukować całkowitą wymaganą pojemność;
  - Używać zasobów bardziej efektywnie;

Monitorowanie uszkodzeń

Zadania, jakie powinien spełniać dobry system monitorowania błędów
(wymienione w kolejności ważności):

- Detekcja i raportowanie o błędach.
  Najprostszym sposobem realizacji tego zadania jest wyznaczenie agentowi zadania zapisywania informacji o niezwykłych wydarzeniach i błędach (tzw. logi).
- Powiadamianie zarządcy o wykrytych anomaliach.
- Przewidywanie wystąpienia błędów.
  Na przykład, jeśli jedna ze zmiennych stanu przekroczy ustalony próg, agent wysyła ostrzeżenie do zarządcy.

Monitorowanie kosztów

- Najistotniejsze w monitoringu kosztów jest śledzenie użycia zasobów sieci przez użytkowników.
  W różnych środowiskach koszty mogą być całkiem innej natury. Czasami wystarcza analiza wykorzystania zasobu na poziomie grup użytkowników i zawiązanych z tym całkowitych kosztów, w innym przypadku obserwacja wykorzystania zasobu musi odbywać się na poziomie pojedynczego użytkownika, który wykonuje określone zadania.
- Przykłady zasobów, które są przedmiotem monitoringu kosztów:
  - Komunikacyjne systemy: LAN, WAN, dial-up, PBX;
  - Sprzęt komputerowy: Stacje robocze, serwery i inne;
  - Oprogramowanie i systemy: Aplikacje i narzędzia, centra danych;
  - Usługi: Wszelkie komercyjne usługi dostępu do łączy czy danych zgromadzonych w systemie sieciowym.
- Dane o kosztach powinny być zbierane dla każdego zasobu, zgodnie z postawionymi przez zarządcę wymogami.

Kontrola sieci

- Ważną częścią zarządzania siecią jest jej kontrola. Polega ona głównie na zmianie parametrów pracy węzła oraz przeprowadzaniu zdalnie, określonych akcji np. włączanie i wyłączenie urządzenia.
- W kwestii kontroli leżą głównie dwa ostatnie obszary zastosowania systemu zarządzania siecią, czyli konfiguracja i bezpieczeństwo.

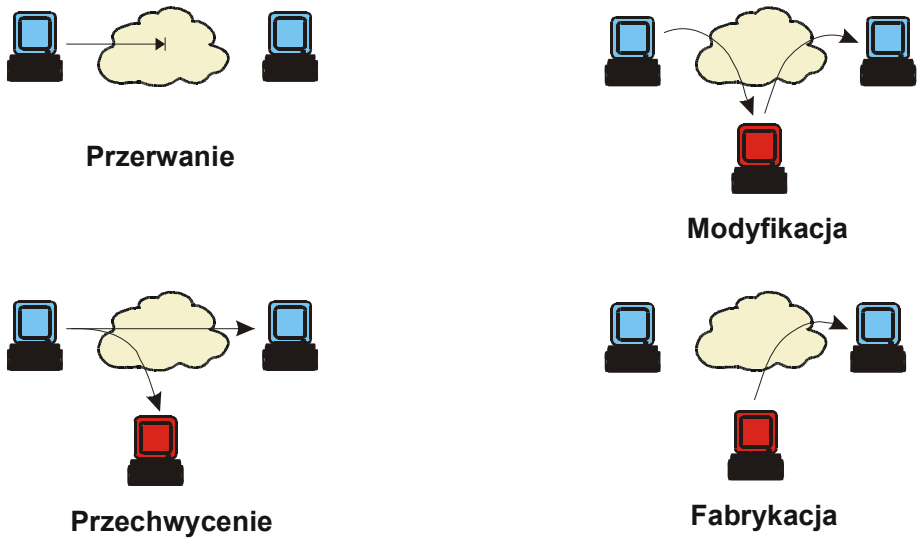
Kontrola konfiguracji

- Główne zadania kontroli konfiguracji to:
  - Inicjalizacja;
  - Konserwacja;
  - Wyłączanie.
- Podstawowe zadania zarządcy konfiguracji:
  - Definiowanie informacji konfiguracyjnych;
  - Ustawianie i modyfikowanie wartości atrybutów;
  - Definiowanie i modyfikacja powiązań;
  - Inicjalizacja i wyłączanie operacji sieciowych;
  - Dystrybucja oprogramowania;
  - Sprawdzanie wartości i powiązań atrybutów;
  - Raport o stanie konfiguracji.

  Dwa pierwsze punkty są istotą kontroli konfiguracji, zaś dwa ostatnie punkty to funkcje konfiguracyjno-monitorujące.

Kontrola bezpieczeństwa

- Typy zagrożeń.



Rysunek 2.10 Zagrożenia bezpieczeństwa.

Kontrola bezpieczeństwa

- Zadania zarządzania bezpieczeństwem:
  - Przechowywanie informacji bezpieczeństwa:
  - Przykłady obiektów wykorzystywanych przy zarządzaniu bezpieczeństwem: klucze, informacje o uprawnieniach i prawach dostępu, parametry operacyjne oraz usługi i mechanizmy bezpieczeństwa.
    Informacje, które należy gromadzić, aby ułatwić wykrycie nieuprawnionego dostępu:
    - Logowanie wydarzeń;
    - Monitorowanie bezpieczeństwa linii komunikacyjnych;
    - Monitorowanie użycia zasobów związanych z bezpieczeństwem;
    - Raportowanie o naruszeniu bezpieczeństwa;
    - Odbieranie zawiadomień o naruszeniu bezpieczeństwa;
    - Utrzymywanie kopii bezpieczeństwa danych związanych z bezpieczeństwem;
    - Utrzymywanie profili użytkowników i ich użycia przy dostępie do określonych zasobów.
  - Kontrola usług dostępu do zasobów.
  - Kontrola procesów kodowania.

Protokół zarządzania SNMPv1

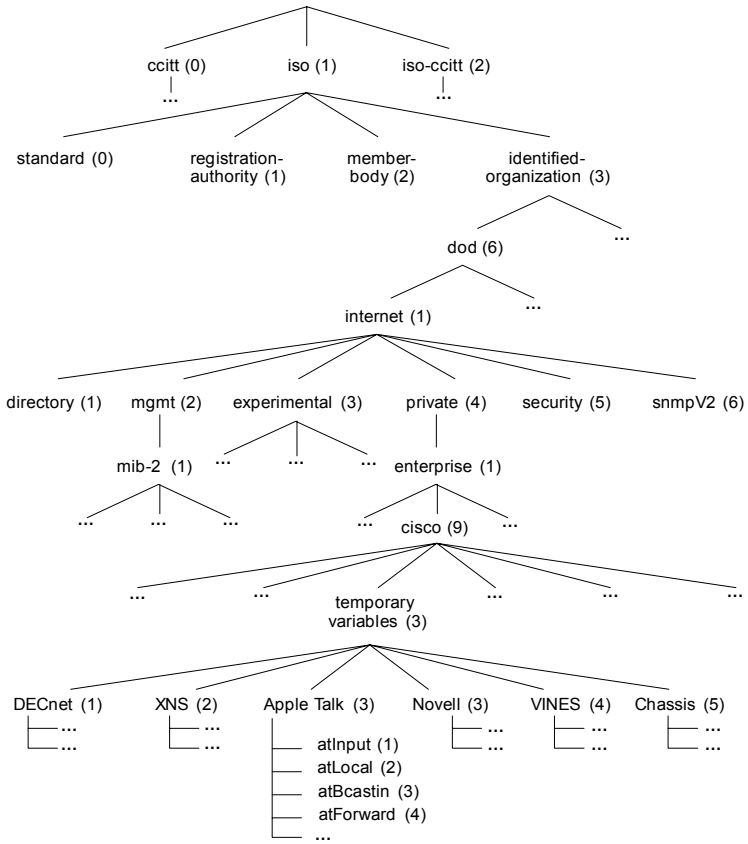
Protokoły zarządzania:

- HEMS (*High-Level Entity Management System*) uogólnienie prawdopodobnie pierwszego protokołu zarządzanie siecią – HMP (*Host Monitoring Protocol),*
- SNMP (*Simple Network Management Protocol*) rozbudowana wersja protokołu SGMP,
- CMIP over TCP/IP (*Common Management Information Protocol over TCP/IP* - CMOT) próba przeniesienia protokołu zarządzania stworzonego przez ISO/OSI na platformę TCP/IP.

Dokumentacja protokołu SNMPv1

Numer RFC	*Tytuł*	*Data publikacji*
1155	Structure and Identification of Management Information for TCP/IP-based Internets	Maj 1990
1157	A Simple Network Management Protocol (SNMP)	Maj 1990
1212	Concise MIB Definitions	Marzec 1991
1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II	Marzec 1991

Bazy danych MIB

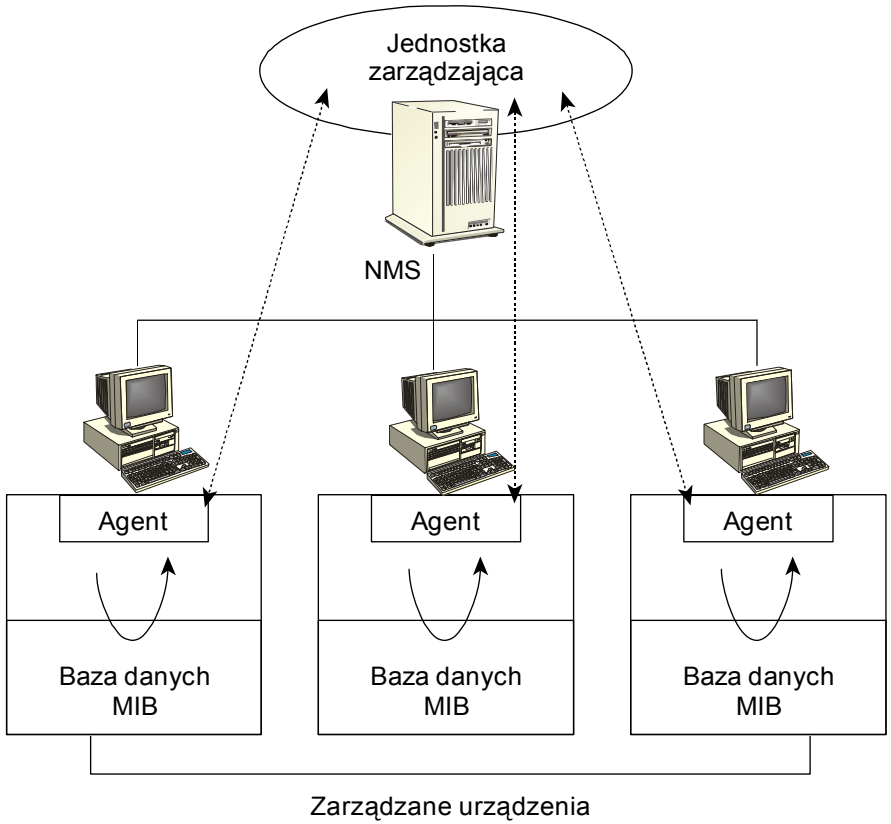


Rysunek 2.11 Drzewo MIB II.

Podstawowe typy danych w bazie MIB

Typ danych	*Opis*
INTEGER (UNIVERSAL 2) *liczba całkowita*	Typ danych reprezentujący liczebniki główne.
OCTET STRING (UNIVERSAL 4) *oktetowy ciąg znaków*	Typ danych reprezentujący ciąg oktetów, gdzie każdy z nich może przyjmować wartość od 0 do 255.
NULL (UNIVERSAL 5) *zero*	Typ danych traktowany jako znak-wypełniacz, ale obecnie nie używany.
OBJECT IDENTIFIER (UNIVERSAL 6) *identyfikator obiektu*	Typ danych reprezentujący identyfikator (nazwę) obiektu, która składają się z sekwencji wartości określających węzeł w drzewie MIB.
SEQUENCE (UNIVERSAL 16) *kolejność*	Typ danych wykorzystywany do tworzenia list w skład, których wchodzą obiekty o typach prostych ASN.1.
SEQUENCE OF (UNIVERSAL 16) *kolejność*	Typ danych wykorzystywany do tworzenia tabel, budowanych w oparciu o wcześniej zdefiniowane listy.

System zarządzania SNMP



Rysunek 2.14 Elementy systemu zarządzania stosującego protokół SNMP.

Operacje protokołu

Jednym z powodów, dla których SNMP jest uważany za prosty, jest fakt, że udostępnia on tylko trzy podstawowe czynności, które mogą być wykonywane na obiektach:

- *Set*: System zarządzania może zaktualizować lub zmienić wartość skalarnego obiektu MIB. Operacja ustawiania jest uprzywilejowanym poleceniem, ponieważ może być wykorzystywana do poprawiania konfiguracji urządzenia lub do kontrolowania jego stanu użytkowego.
- *Get*: System zarządzania może odczytywać wartość skalarnego obiektu MIB. Polecenie pobierania wartości jest najpopularniejszą czynnością protokołu SNMP, ponieważ jest to główny mechanizm wykorzystywany do zbierania informacji o urządzeniu sieciowym.
- *Trap*: Agent może samodzielnie wysyłać wiadomości do programu zarządzania siecią. Celem tej usługi jest zawiadomienie systemu zarządzania o zmianie warunków pracy urządzenia lub wykrytych problemach.

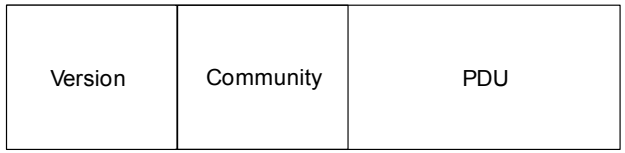
Społeczność

- Specyfikacja SNMP (RFC 1157) dostarcza bardzo prostego mechanizmu ochrony opartego na koncepcji społeczności.
- Nazwa społeczności jest definiowana lokalnie w agencie, dlatego te same nazwy mogą być używane przez różnych agentów. Każda wiadomość przesyłana ze stacji zarządzającej do agenta zawiera nazwę społeczności.
- Głównym powodem problemów z bezpieczeństwem jest to, że SNMP nie zapewnia żadnych funkcji kodowania lub innych mechanizmów, dzięki którym można upewnić się, że informacje o społeczności nie są kopiowane z sieci podczas wymiany pakietów SNMP.

Kontrola dostępu do zmiennych

MIB access	*SNMP access mode*	
	READ-ONLY	*READ-WRITE*
read-only	Dostępne dla operacji *get* i *trap*	Dostępne dla operacji *get* i *trap*
read-write	Dostępne dla operacji *get* i *trap*	Dostępne dla operacji *get*, *trap* oraz *set*
write-only	Dostępne dla operacji *get* i *trap*, lecz wartość zależy od specyfiki implementacji	Dostępne dla operacji *get*, *trap* oraz *set*, lecz wartość zależy od specyfiki implementacji
not accessible	niedostępny	

Format wiadomości SNMPv1



a.) Schemat blokowy.

```
Message ::=
    SEQUENCE {
        version        -- version-1 for RFC 1157
            INTEGER {
                version-1(0)
            },

        community      -- community name
            OCTET STRING,

        data           -- e.g., PDUs if trivial
            ANY        -- authentication is being used
    }
```

b.) Definicja zgodna z notacją ASN.1.

Rysunek 2.15 Format wiadomości protokołu SNMP.

Informacje, pomiędzy stacją zarządzającą a agentem, są wymieniane w formie komunikatów SNMP. Urządzenie odbiera wiadomości wykorzystując bezpołączeniowy protokół UDP na porcie 161. Jedynie wiadomości zawierające pułapki odbierane są na porcie 162.

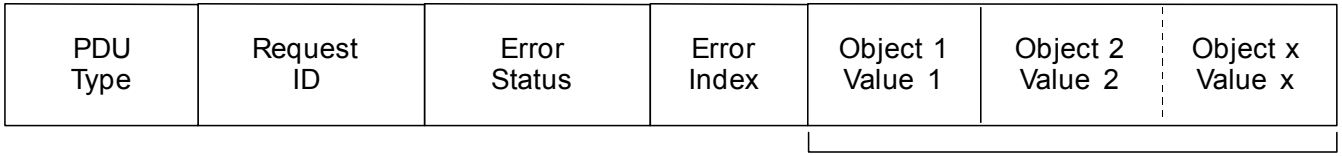
Format wiadomości SNMPv1

W SNMPv1 zdefiniowano pięć typów *PDU*:

- ***GetRequest;***
- ***GetNextRequest;***
- ***SetRequest;***
- ***GetResponse;***
- ***Trap;***

PDU GetRequest, GetNextRequest, SetRequest, GetResponse mają taki sam format.Dzięki temu uniknięto zbytecznej komplikacji protokołu. Jedynie *Trap-PDU*, ze względu na swoją specyfikę, ma inną strukturę.

Format wiadomości SNMPv1



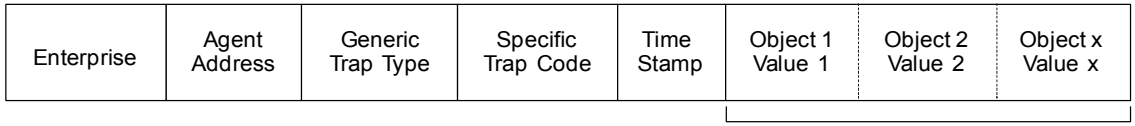
a.) Schemat blokowy.

```
PDU ::=
        SEQUENCE {
          request-id
              INTEGER,

          error-status      -- sometimes ignored
              INTEGER {
                  noError(0),
                  tooBig(1),
                  noSuchName(2),
                  badValue(3),
                  readOnly(4),
                  genErr(5)
              },

          error-index       -- sometimes ignored
              INTEGER,

          variable-bindings -- values are sometimes ignored
              VarBindList
        }
```

b.) Definicja zgodna z notacją ASN.1.

Rysunek 2.16 Format PDU: GetRequest, GetNextRequest, SetRequest, GetResponse.

Format wiadomości SNMPv1



a.) Schemat blokowy.

```
Trap-PDU ::=
    IMPLICIT SEQUENCE {
        enterprise      -- type of object generating
                        -- trap, see sysObjectID
            OBJECT IDENTIFIER,

        agent-addr      -- address of object generating
            NetworkAddress, -- trap

        generic-trap    -- generic trap type
            INTEGER {
                coldStart(0),
                warmStart(1),
                linkDown(2),
                linkUp(3),
                authenticationFailure(4),
                egpNeighborLoss(5),
                enterpriseSpecific(6)
            },

        specific-trap  -- specific code, present even
            INTEGER,   -- if generic-trap is not
                       -- enterpriseSpecific

        time-stamp     -- time elapsed between the last
            TimeTicks, -- (re)initialization of the
                       network
                       -- entity and the generation of the
                       trap

        variable-bindings -- "interesting" information
            VarBindList
    }
```

b.) Definicja zgodna z notacją ASN.1.

Rysunek 2.17 Format Trap-PDU.

Wykład RADIUS, SNMP

KONIEC