Zarządzanie sieciami komputerowymi

Część 2 wykładu

SKO2

Mapa wykładu

- Wprowadzenie do zarządzania sieciami
- Standardy X.500, X.700 i TMN
- Protokół SNMP
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - RMON
  - Komunikaty protokołu SNMP
  - Problem prezentacji i kodowanie ASN
  - Ochrona informacji w SNMP
- Usługi katalogowe
  - DNS, NIS/NIS+
  - LDAP

Remote MONitoring

- RMON to baza MIB
- RMON gromadzi informacje dla całej podsieci
  - MIB-2 pozwala najwyżej na informacje lokalne dla 1 urządzenia
- RMON-1 dotyczy warstwy łącza danych
- RMON-2 dotyczy wszystkich wyższych warstw
- Standardy: RFC 1271, RFC 1757, RFC 1513
- Urządzenia monitorujące RMON zwane są próbnikami, agentami RMON

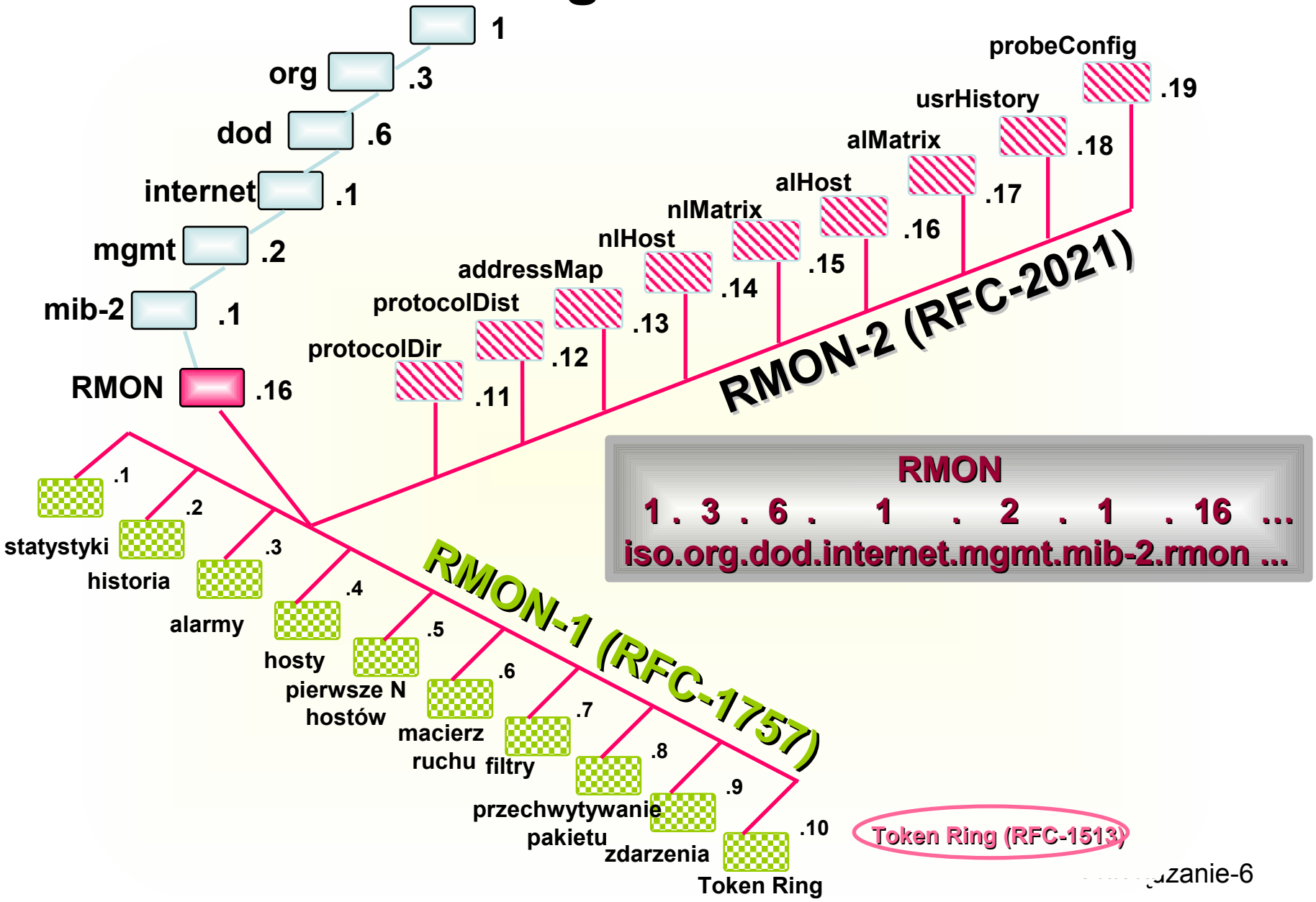
Funkcje monitorowania RMON

- 9 grup
  - statystyki
    - wykorzystanie i błędy
  - historia
    - próbki danych statystycznych z przeszłości
  - alarmy
    - ustalanie progów i okresów próbkowania
  - hosty
    - pomiary ruchu do i z hosta

Funkcje monitorowania RMON

- 9 grup
  - pierwszych N hostów
    - raport o pierwszych N hostach z grupy hostów
  - macierz ruchu
    - statystyki dla par komunikujących się węzłów
  - filtry
    - mechanizm wybierający ramki/pakiety odpowiadające wzorcowi
  - przechwytywanie pakietów
    - sposób buforowania odfiltrowanych pakietów
  - zdarzenia
    - umożliwia rejestrowania pułapek wraz z czasem wystąpienia

Remote MONitoring MIB



Mapa wykładu

- Wprowadzenie do zarządzania sieciami
- Standardy X.500, X.700 i TMN
- Protokół SNMP
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - RMON
  - Komunikaty protokołu SNMP
  - Problem prezentacji i kodowanie ASN
  - Ochrona informacji w SNMP
- Usługi katalogowe
  - DNS, NIS/NIS+
  - LDAP

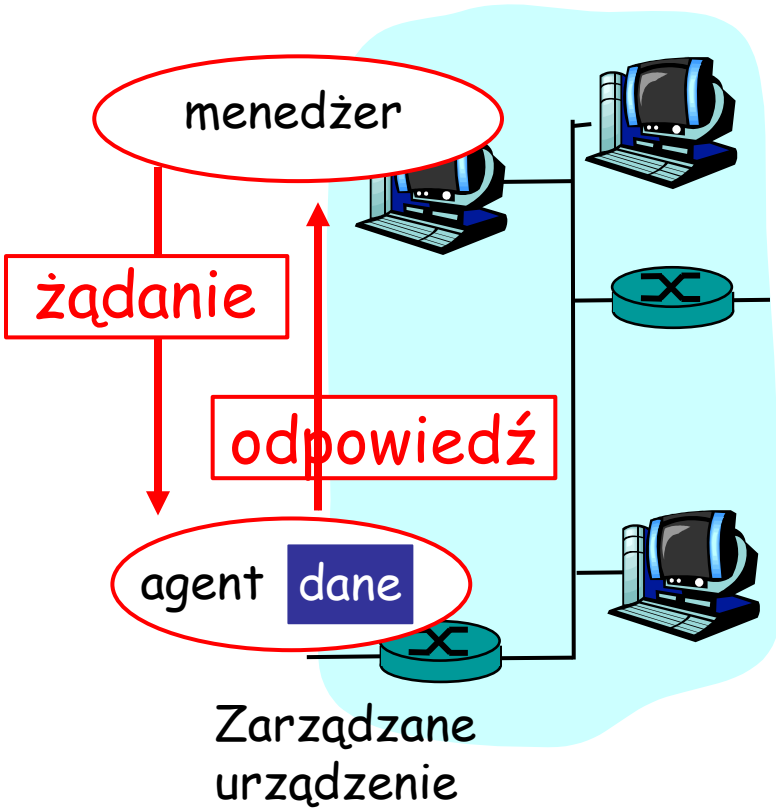
Protokół SNMP

- Protokół pobierający dane z bazy MIB (od agenta SNMP).
- Może być wykorzystywany przez:
  - linię komend (snmpwalk),
  - GUI (MIB Browser), lub
  - większą aplikację (n.p. Sun Net Manager) zwaną *Network Management Software* (NMS).
- NMS składa się z mniejszych aplikacji służących do zarządzania siecią wraz z interfejsem graficznym (diagramy, wykresy itd)
- NMS działa na hoście zwanym *Network Management Station* (także NMS), na którym może działać wiele różnych aplikacji NMS.

Protokół SNMP

Dwa rodzaje komunikacji w protokole:

- żądanie-odpowiedź (synchroniczne)
- komunikaty o zdarzeniach (asynchroniczne)



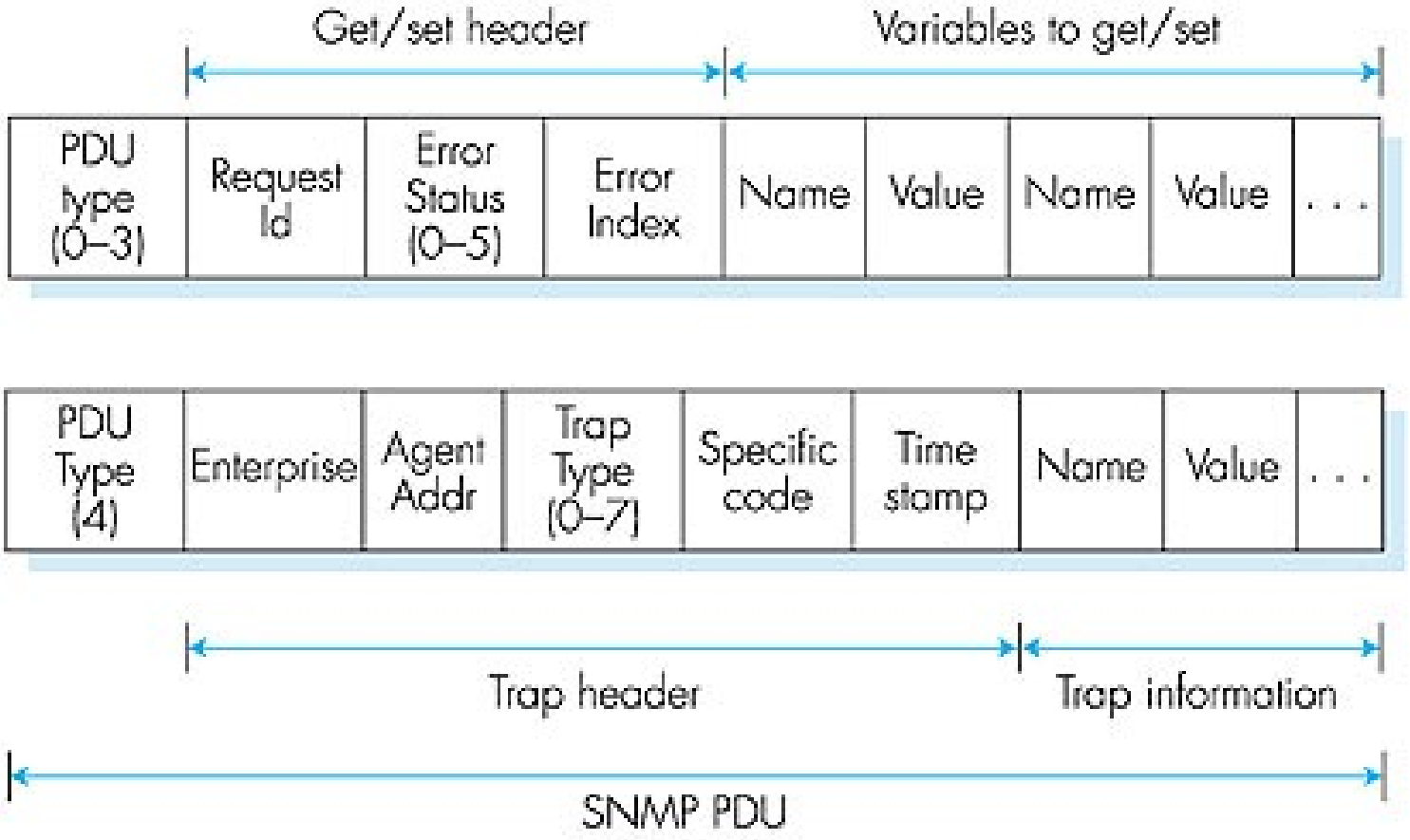
tryb żądanie-odpowiedź

Komunikat o zdarzeniu

Protokół SNMP v1,2: rodzaje komunikatów

Komunikat	Funkcja
GetRequest GetNextRequest GetBulkRequest (v2)	Menedżer do agenta: "daj mi dane" (instację, następną na liście, blok)
InformRequest	Menedżer do menedżera: oto wartość z MIB
SetRequest	Menedżer do agenta: ustaw wartość w MIB
Response	Agent do Menedżera: wartość, odpowiedź na żądanie
Trap	Agent do Menedżera: informuje menedżera o zdarzeniu

Protokół SNMP v1,2: formaty komunikatów



SNMP v2 oraz v2c

- Protokół SNMPv2c enkapsułuje komunikaty protokołu SNMPv2 w komunikatach protokołu SNMPv1
- SNMPv2 ma nowy komunikat: GetBulkRequest
- SNMPv2 wprowadza 64-bitowe liczniki do bazy MIB

SNMP v3

- Dodaje funkcje ochrony informacji: poufność, integralność
- Dodaje lepsze uwierzytelnienie (użytkownik i hasło) zamiast "community"
- Dodaje funkcjonalność kontroli dostępu za pomocą perspektyw (ang. *views*)

Różnice w wersjach SNMP

	Wersja 1	Wersja 2c	Wersja 3
Powiadomienia	Nie	Tak	Tak
RMON/Zdarzenia	Nie	Tak	Tak
Uwierzytelnienie	Community	Community	Użytkownik
Poufność	Nie	Nie	Tak
Obsługa w NMS	Powszechnie	Dobra	Ograniczona

SNMP a CMIP (TMN)

	Internet/SNMP	OSI/CMIP
Model	Przepytywanie i zdarzenia	Zdarzenia
Agent	Mała złożoność	Duża złożoność
Model informacji	zmienne brak dziedziczenia	obiekty dziedziczenie
Bezpieczeństwo community uwierzytelnienie poufność kontrola dostępu	v1 v2 tak tak nie tak:MD5 nie tak:DES nie nie	 nie hasło dla asocjacji opcjonalne tak
nazwy wystąpień	jednoznaczne u jednego agenta zależne od typu obiektu	globalnie jednoznaczne

Mapa wykładu

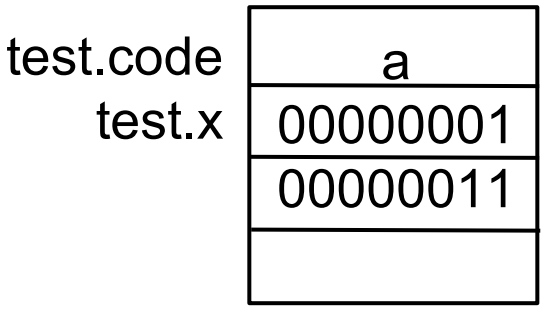
- Wprowadzenie do zarządzania sieciami
- Standardy X.500, X.700 i TMN
- Protokół SNMP
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - RMON
  - Komunikaty protokołu SNMP
  - Problem prezentacji i kodowanie ASN
  - Ochrona informacji w SNMP
- Usługi katalogowe
  - DNS, NIS/NIS+
  - LDAP

Problem prezentacji

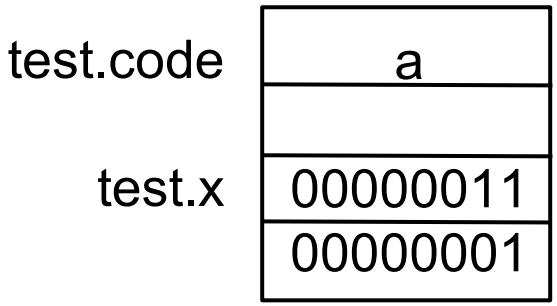
Pytanie: czy do komunikacji wystarcza idealna kopia informacji z pamięci do pamięci?

Odpowiedź: nie zawsze!

```
struct {
   char code;
    int x;
    } test;
test.x = 256;
test.code='a'
```



format na hoście 1



format na hoście 2

problem: różne formaty danych, konwencje przechowywania

Problem prezentacji „z życia wzięty”:

babcia

balanga

podstarzała
hipiska z lat 60

balanga

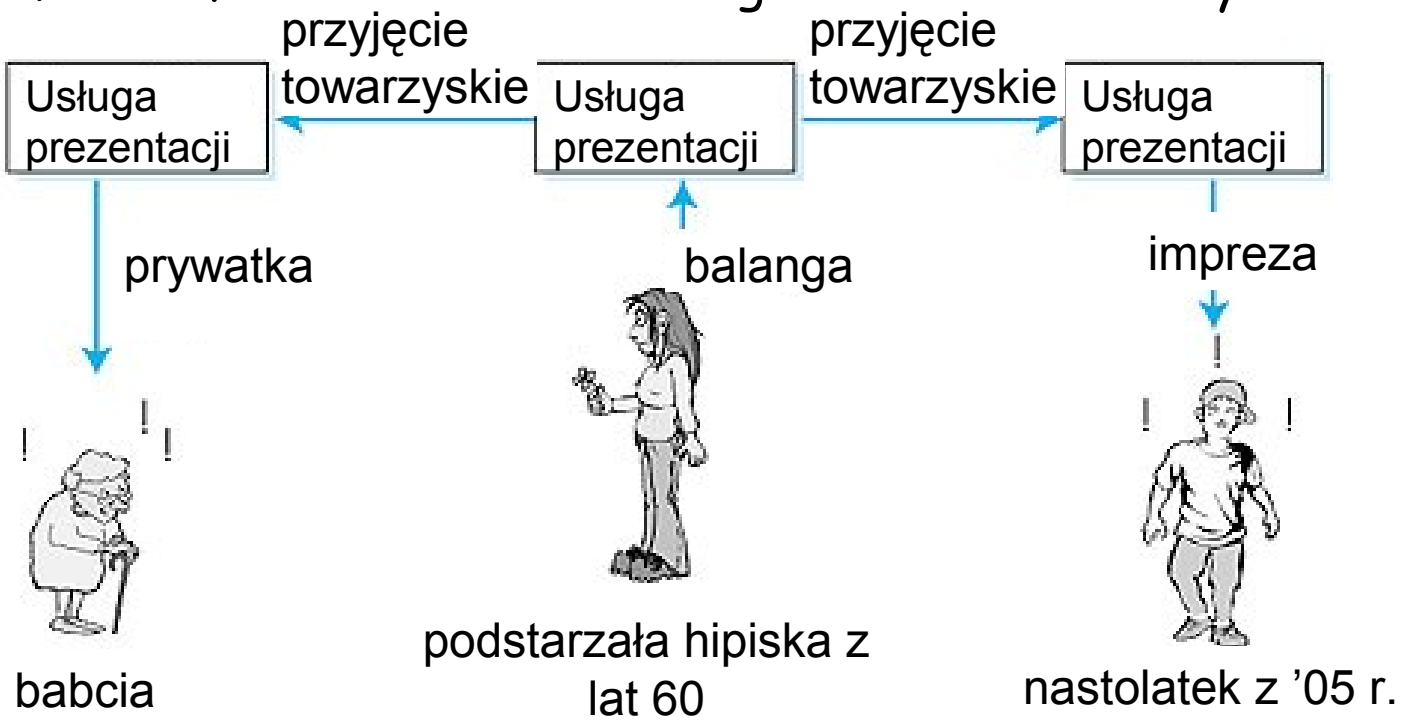
nastolatek z ’05 r.

Problem prezentacji: możliwe rozwiązania

1. Nadawca poznaje format odbiorcy. Nadawca tłumaczy na format odbiorcy. Nadawca wysyła.
   - analogie w życiu codziennym?
   - za i przeciw?
2. Nadawca wysyła. Odbiorca poznaje format nadawcy. Odbiorca tłumaczy na swój własny format
   - analogie w życiu codziennym?
   - za i przeciw?
3. Nadawca tłumaczy na format niezależny od hosta (standardowy). Wysyła. Odbiorca tłumaczy na swój własny format.
   - analogie w życiu codziennym?
   - za i przeciw?

Rozwiązywanie problemu prezentacji

1. Przetłumacz z formatu lokalnego na format standardowy
2. Wyślij informacje w standardowym formacie
3. Przetłumacz z formatu standardowego na format lokalny



ASN.1: Abstract Syntax Notation 1

- Standard ISO X.680
  - używany szeroko w Internecie
  - jest jak jedzenie warzyw: wiadomo, że to "dla zdrowia"!
- definiuje typy danych, konstruktory obiektów
  - podobnie jak SMI
- BER: Basic Encoding Rules
  - określają, jak obiekty zdefiniowane w ASN.1 mają być komunikowane
  - każdy przesyłany obiekt ma Typ, Długość, i Wartość

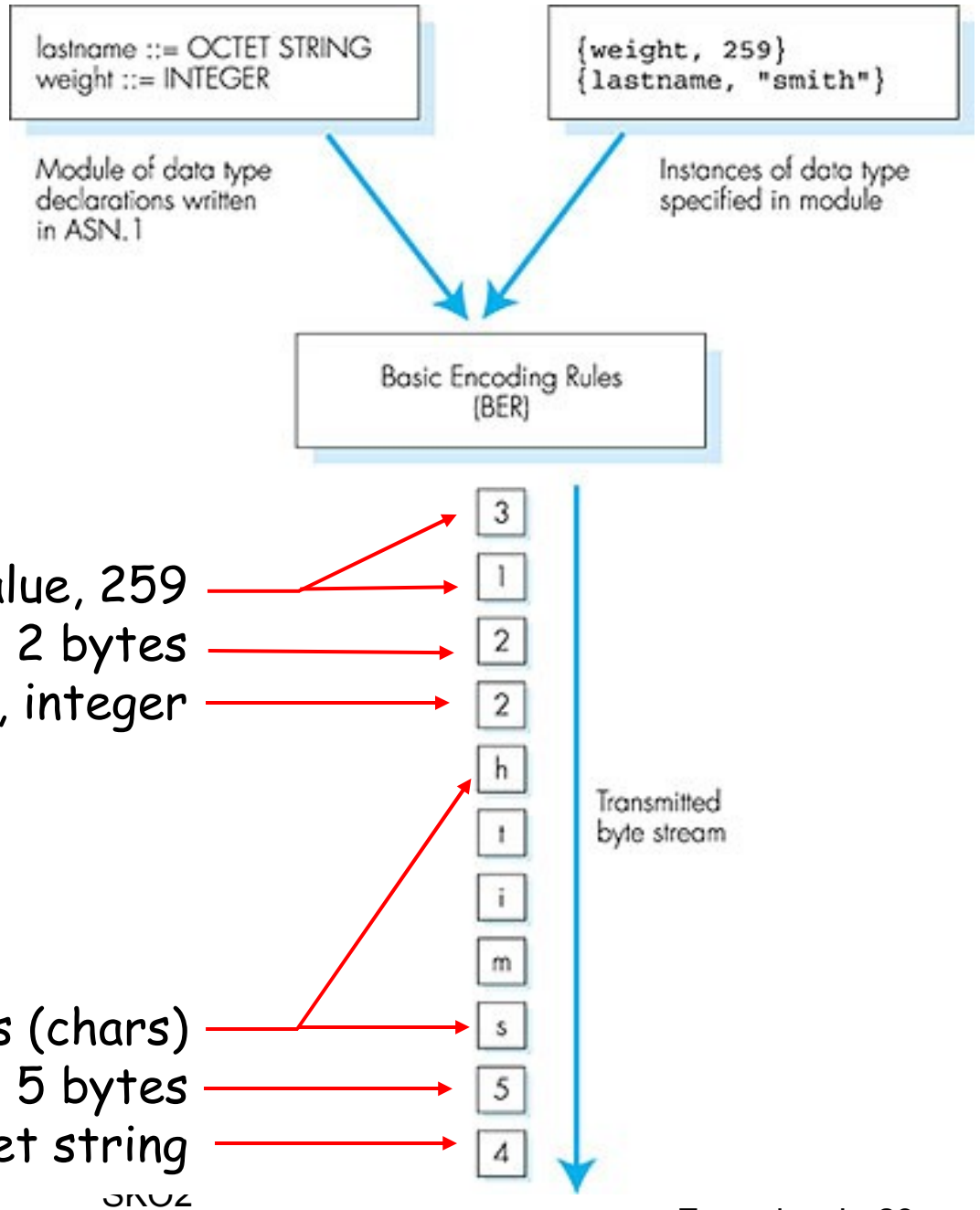
Kodowanie TLV

Pomysł: komunikowane dane same się identyfikują

- T: typ danych, jeden z typów zdefiniowanych w ASN.1
- L: długość danych w bajtach
- V: wartość danych, kodowana według standardu ASN.1

Wartość znacznika	Typ
1	Boolean
2	Integer
3	Bitstring
4	Octet string
5	Null
6	Object Identifier
9	Real

Kodowanie TLV: przykład



Mapa wykładu

- Wprowadzenie do zarządzania sieciami
- Standardy X.500, X.700 i TMN
- Protokół SNMP
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - RMON
  - Komunikaty protokołu SNMP
  - Problem prezentacji i kodowanie ASN
  - Ochrona informacji w SNMP
- Usługi katalogowe
  - DNS, NIS/NIS+
  - LDAP

Ochrona informacji w SNMP

- Gdzie jest stosowany SNMP
  - Najpopularniejszy protokół zarządzania siecią
  - Hosty, ściany ogniowe, rutery, przełączniki…UPS, zasilacze, karty ATM -- wszechobecny
- "Jeden z największych koszmarów bezpieczeństwa w dzisiejszych sieciach"

Luki bezpieczeństwa w SNMPv1

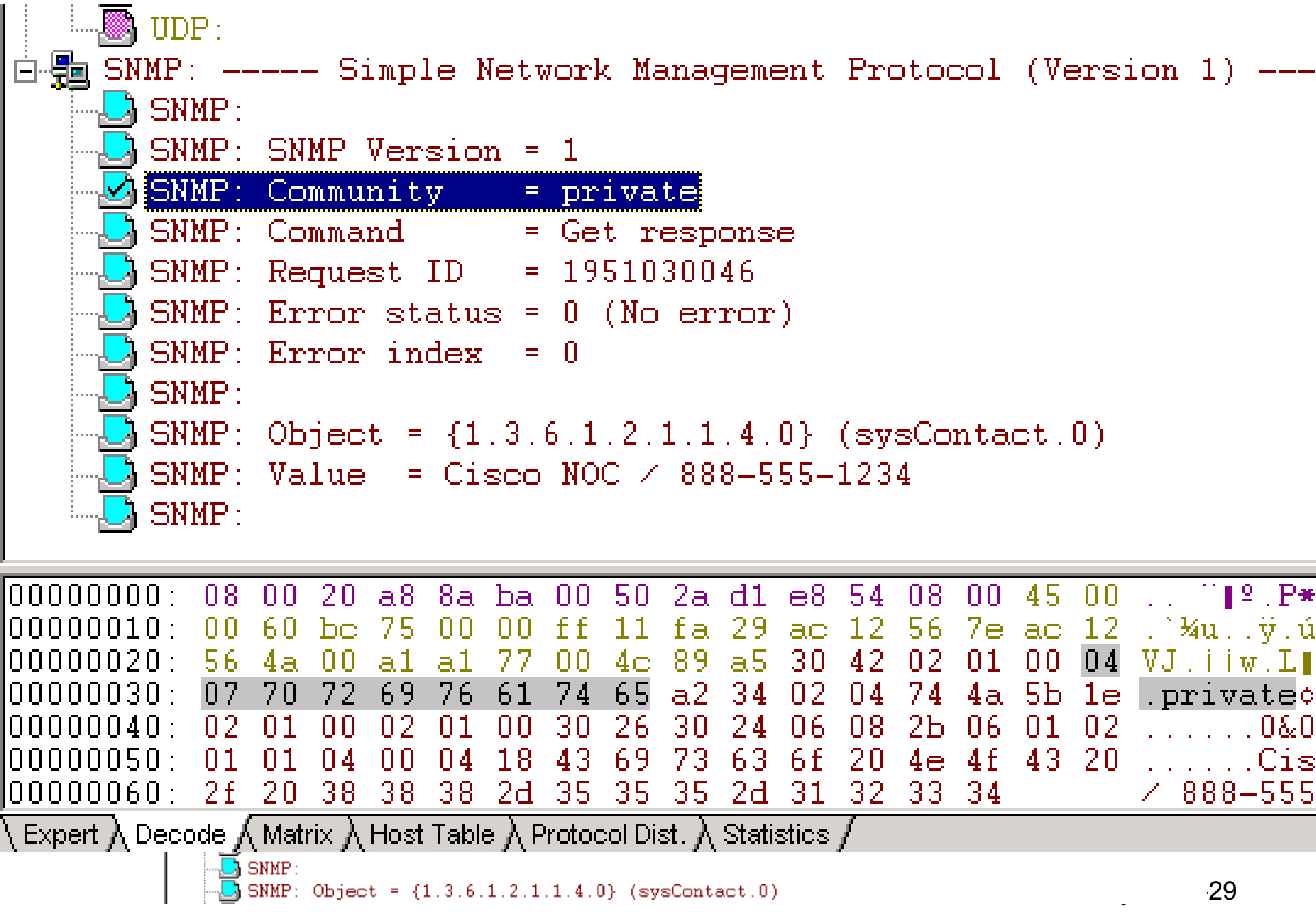
- Warstwy transportu i sieci
  - Modyfikacja informacji
  - Zablokowanie dostępu do usługi (DoS)
  - Powtarzanie
- Uwierzytelnienie
  - w oparciu o host
  - w oparciu o *„community”*
- Informacje ujawniane przez SNMP
  - Tablice rutingu
  - Topologia sieci
  - Rozkłady ruchu w sieci
  - Reguły filtrujące pakiety

Transport SNMP

- SNMP używa UDP
  - Zawodne – komunikaty nie muszą docierać do celu
  - Nadawca segmentu i pakietu może łatwo zostać sfałszowany
  - Łatwo zablokować usługę, bez ujawniania swojego adresu IP
  - Łatwo zmodyfikować pakiet
  - Łatwo nagrać pakiet i go powtórnie wysłać

Wady uwierzytelnienia SNMP

- W oparciu o hosta
  - Zawodzi z powodu transportu UDP
  - Zatruwanie schowków DNS
- W oparciu o *„community”*
  - wspólne hasło
  - przesyłane otwartym tekstem
  - Łatwe do odgadnięcia, lub brutalnego złąmania
  - Stosuje się domyślne wartości community


UDP:
SNMP: ----- Simple Network Management Protocol (Version 1) ---
SNMP:
SNMP: SNMP Version = 1
SNMP: Community = private
SNMP: Command = Get response
SNMP: Request ID = 1951030046
SNMP: Error status = 0 (No error)
SNMP: Error index = 0
SNMP:
SNMP: Object = {1.3.6.1.2.1.1.4.0} (sysContact.0)
SNMP: Value = Cisco NOC / 888-555-1234
SNMP:
00000000: 08 00 20 a8 8a ba 00 50 2a d1 e8 54 08 00 45 00
00000010: 00 60 bc 75 00 00 ff 11 fa 29 ac 12 56 7e ac 12
00000020: 56 4a 00 a1 a1 77 00 4c 89 a5 30 42 02 01 00 04
00000030: 07 70 72 69 76 61 74 65 a2 34 02 04 74 4a 5b 1e
00000040: 02 01 00 02 01 00 30 26 30 24 06 08 2b 06 01 02
00000050: 01 01 04 00 04 18 43 69 73 63 6f 20 4e 4f 43 20
00000060: 2f 20 38 38 38 2d 35 35 35 2d 31 32 33 34
Expert
Decode
Matrix
Host Table
Protocol Dist.
Statistics
SNMP:
SNMP: Object = {1.3.6.1.2.1.1.4.0} (sysContact.0)

Popularne wartości domyślne

- public
- private
- write
- "all private"
- monitor
- manager
- security
- admin
- lan

- default
- password
- tivoli
- openview
- community
- snmp
- snmpd
- system
- itd itd itd...

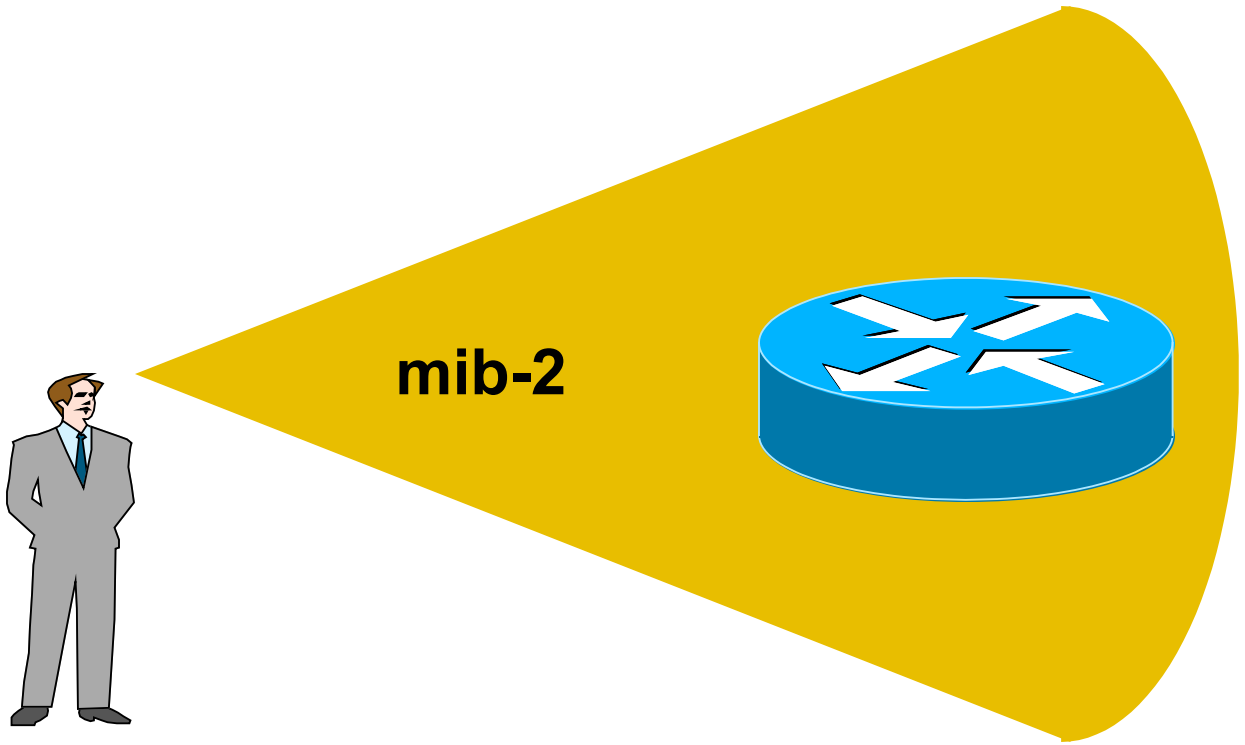
Bezpieczeństwo RMON i RMON2

- te same wady, co SNMPv1
- dodatkowe niebezpieczeństwa poprzez wprowadzenie obiektów "action invocation"
- zbiera wiele informacji o całej podsieci

Ochrona informacji SNMPv3 - zestawienie

- szyfrowanie: DES lub AES szyfruje komunikat SNMP
- uwierzytelnienie: oblicz, wyślij *Message Integrity Check*: MIC(m,k): wartość funkcji haszującej z wiadomości (m), tajnego klucza (k)
- ochrona przed atakiem przez powtórzenia: używać jednorazowych indentyfikatorów
- kontrola dostępu przez perspektywy
  - jednostka SNMP utrzymuje bazę danych z prawami dostępu, politykami dla różnych użytkowników
  - baza danych jest sama zarządzanym obiektem!

Perspektywy SNMP



enterprises

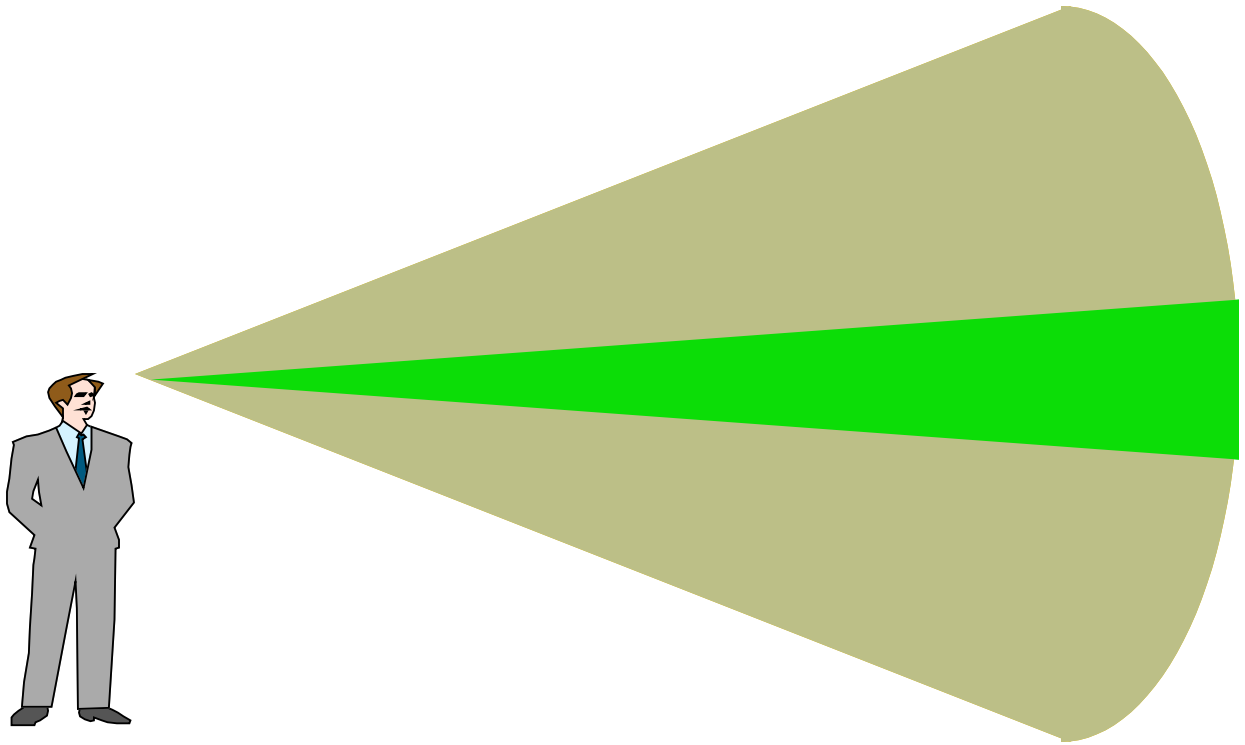
rttmon

interfaces

bgp

ipRouteTable

Perspektywy SNMP



enterprises

rttmon

interfaces

bgp

ipRouteTable

Ochrona informacji w SNMP

Wersja	Poziom	Uwierzytelnienie	Szyfrowanie
SNMPv1		community	
SNMPv2c		community	
SNMPv3	noAuthNoPriv	użytkownik i hasło	
SNMPv3	authNoPriv	MD5 lub SHA	
SNMPv3	authPriv	MD5 lub SHA	DES-56, AES

Ograniczanie nadużyć w SNMP

- SNMP powinno być dostępne tylko dla NMS
- Należy używać list kontroli dostępu (ang. *Access Control List, ACL*)
- Gdy tylko jest to możliwe, należy używać SNMPv3
- Należy ograniczyć dane widoczne przez SNMP za pomocą „perspektyw"

Mapa wykładu

- Wprowadzenie do zarządzania sieciami
- Standardy X.500, X.700 i TMN
- Protokół SNMP
  - Structure of Management Information: SMI
  - Management Information Base: MIB
  - RMON
  - Komunikaty protokołu SNMP
  - Problem prezentacji i kodowanie ASN
  - Ochrona informacji w SNMP
- Protokoły katalogowe
  - DNS, NIS/NIS+, domeny Microsoft, X.500
  - LDAP

Usługi katalogowe

- Usługa "katalogowa" jest strukturalizowanym repozytorium informacji o ludziach lub zasobach w organizacji
  - zywkle, baza danych z dostępem do sieci
    - zapytania i odpowiedzi zawierają małą ilość informacji
    - modyfikacje są znacznie rzadsze niż zapytania
  - usługa katalogowa implementuje oraz umożliwia kontrolę praw dostępu
    - zarówno do samej usługi katalogowej, jak i do innych zasobów i usług
  - struktura umożliwia zadawanie zapytań poprzez nazwy (identyfikatory) obiektów

Katalogi

- Typowe przykłady:
  - książki telefoniczne
  - listy adresowe (email, listy adresów IP, itd)

- Każdy wpis jest dostępny przez klucz:
  - znając imię i nazwisko, wyszukujemy telefon
    - uwaga: taki klucz nie jest unikalny – a powinien
  - znając imię i nazwisko, wyszukujemy adres e-mail

Aplikacje

- Niektóre aplikacje po prostu udostępniają *interfejs* do usługi katalogowej.
  - elektroniczna książka telefoniczna.

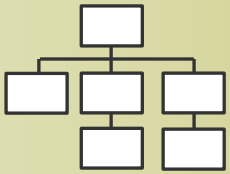
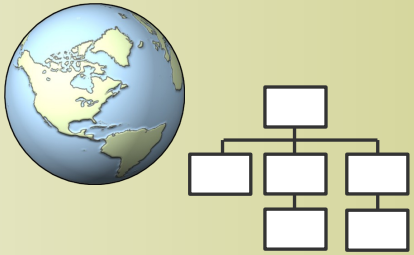
- Inne aplikacje używają usługi katalogowej do przechowywania informacji konfigurującej, pomocniczych baz danych, itd.

Struktura informacji

- Zwykle, informacja w katalogu ma strukturę hierarchiczną (lecz nie zawsze).

- Struktura danych (hierarchia) jest często użyteczna w wyszukiwaniu danych i stanowi (minimalną) relację pomiędzy rekordami.

Struktury usług katalogowych

Model administracyjny	Struktura katalogu w oparciu o:
Geograficzny 	Lokalizację geograficzną
Strukturalny 	Strukturę organizacji
Biznesowy 	Funkcje organizacji
Hybrydowy 	▪ Lokalizację dla głównych jednostek ▪ Strukturę organizacji dla mniejszych jednostek

Przykład: DNS

Domain Name System jest przykładem usługi katalogowej:

- hierarchiczna struktura
- dla każdego rekordu, jest jednoznaczny klucz (nazwa DNS) i grupa atrybutów:
  - adres IP
  - serwer poczty
  - informacje o hoście
  - itd...
- przykłady użycia DNS przez inne aplikacje/usługi
  - Realtime Blackhole List (RBL): filtrowanie spamu
  - rekordy SRV: zawierają host udostępniający usługę

NIS/NIS+

- *Network Information Service* (NIS), znane wcześniej jako *Yellow Pages*
- Tworzą *domenę* w sieci lokalnej (jak w MS)
  - identyfikowana przez unikalną nazwę
- NIS – płaska struktura, informacje na serwerze NIS, każdy host ma klienta
  - *ypbind* – wyszukuje serwery
- Serwer ma bazę danych, tworzoną na podstawie plików konfiguracyjnych
  - */etc/ethers, hosts, networks, protocols, services, aliases*
- NIS może zastąpić DNS
  - nsswitch.cons – kolejność tłumaczenia nazw (NIS, DNS)

NIS/NIS+

- NIS+: tylko Solaris
- Architektura hierarchiczna, rozproszona
  - skalowalność: dowolnie duże domeny
- Bardziej złożone struktury danych
  - tabele wielokolumnowe
  - NIS – tylko 2 kolumny
- Mechanizm bezpieczeństwa
  - NIS nie ma uwierzytelnienie klienta/serwera
  - NIS+: uwierzytelnienie, szyfrowanie DES
  - NIS+: określenie poziomów dostępu (NIS: brak!)
- Lepiej zapomnieć o NIS, jeśli można użyć NIS+

Domeny Microsoft

- Active Directory: usługa katalogowa Microsoft
  - implementuje standard LDAP
  - rozszerza znacznie funkcjonalność LDAP
  - zamknięty system

- Posiada rozbudowane funkcje
  - kontroli dostępu
  - replikacji
  - zarządzania zaufaniem

X.500

- X.500 jest usługą katalogową, która jest już w użyciu od dawna
  - Używa stosu protokołów OSI
    - używa warstw wyższych (niż transport) stosu OSI
  - *Ciężka* usługa (protokół)
    - bardzo rozbudowana
    - bardzo szczegółowa
    - bardzo kosztowna w implementacji

LDAP

- Powstało kilka *lekkich* implementacji X.500 – najnowszą jest LDAP:
  - Lightweight Directory Access Protocol
  - Używa TCP (lecz można go przenieść na inne protokoły).
  - 90% funkcjonalności X.500
  - 10% kosztu

LDAP i Uniwersytet w Michigan

- LDAP powstał na Uniwersytecie w Michigan.
- LDAP może być "nakładką" (ang. *frontend*) do X.500 lub samodzielnie.

- LDAP jest dostępny komercyjnie od szeregu producentów

Definicja LDAP

- RFC 1777:
  - sposób reprezentacji danych
  - określa operacji i ich realizację przy pomocy protokołu żądanie/odpowiedź.
- RFC 1823: Application Programming Interface (stał się standardem)

Udostępnione API – nie potrzeba programowania gniazd!

Reprezentacja danych w LDAP

- Każdy rekord ma jednoznaczny klucz nazywany *distinguished name* (w skrócie **DN**).
- Klucz DN (RFC 1779) ma być używany przez ludzi (nie tylko komputery).
- Każdy **DN** jest ciągiem składników.
  - Każdy składnik jest *łańcuchem znaków* zawierającym parę atrybut=wartość.

Przykładowy DN

CN=Adam Wierzbicki,
OU=SK,
O=PJWSTK,
C=PL

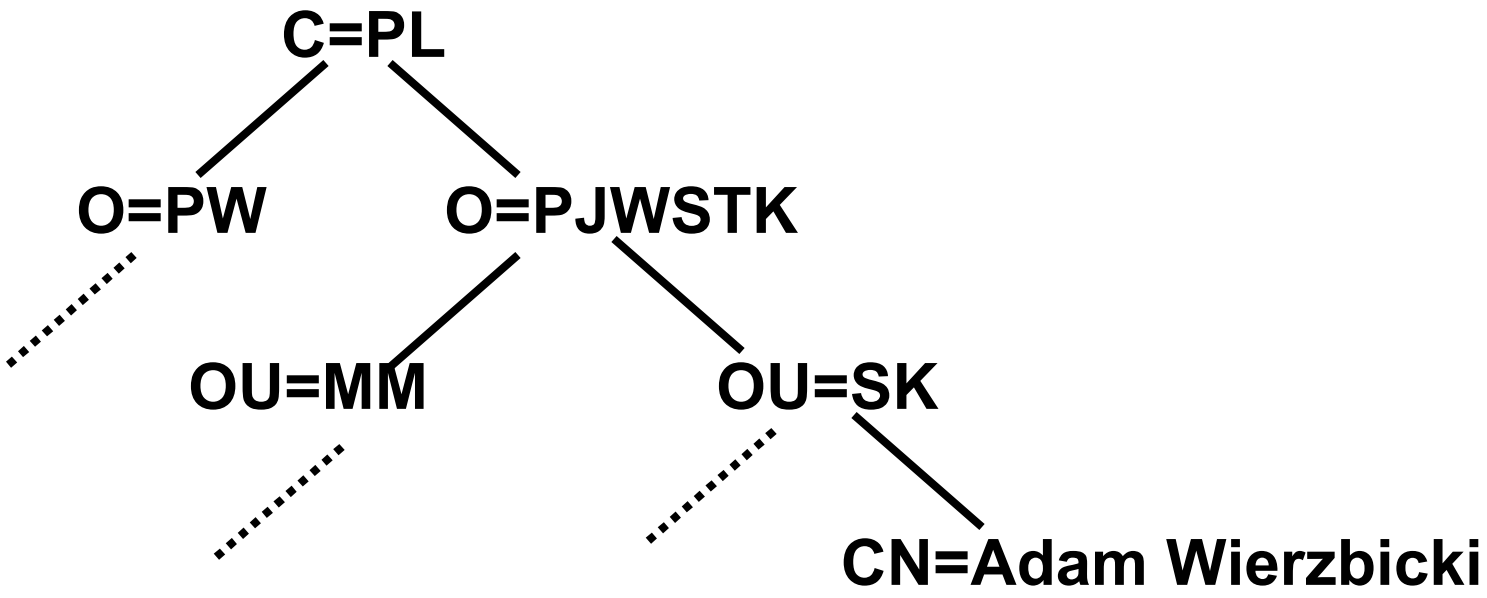
Zwykle pisany jest w jednej linii.

Hierarchia

- Jak nazwy DNS, klucz DN może być interpretowany jako część hierarchii.
- Ostatni składnik klucza **DN** jest na najwyższym poziomie w hierarchii.

```
CN=Krzysztof Kalinowski,OU=MM,O=PJWSTK,C=PL
```

Przykładowa hierarchia



Atrybuty używane w składnikach

- Składniki mogą zawierać dowolne atrybuty, ale istnieje standardowa hierarchia (dla *globalnej przestrzeni nazw* LDAP):

C	*nazwa kraju*
O	*nazwa organizacji*
OU	*nazwa części organizacji*
CN	*nazwa własna*
L	*nazwa lokalizacji*
ST	*stan lub region*
STREET	*adres*

Operacje LDAP

- Dodanie, usunięcie, modyfikacja rekordu
- Zmiana klucz rekordu (dn).
- Wyszukiwanie (główna operacja)
  - Wyszukaj *w części katalogu* rekordy, które spełniają określone kryteria.

Uwierzytelnienie

- Uwierzytelnienie LDAP może używać prostych haseł (otwarty tekst) lub Kerberos.
- LDAP V3 obsługuje inne techniki uwierzytelnienia, w tym używające kluczy publicznych.

Bibliografia o LDAP

- dokumentacja serwera LDAP firmy Netscape
- publikacje o LDAP z Uniwersytetu Michigan
- www.openldap.org
- RFC: 1777, 1773, 1823, ...

Podsumowanie zarządzania sieciami

- Zarządzanie sieciami stanowi obecnie 80% kosztu utrzymania sieci
- Zarządzanie sieciami to bardziej sztuka, niż nauka
  - co mierzyć, monitorować?
  - Jak reagować na awarie?
  - Jak filtrować, korelować powiadomienia o awariach?
  - Jak wygodnie i bezpiecznie zarządzać kontami, uprawnieniami, hasłami?
  - Jak zarządzać usługami w sieci?