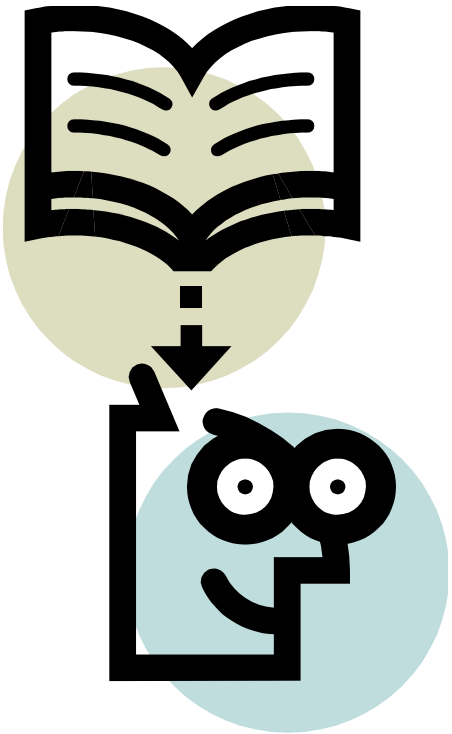
Projektowanie i Realizacja Sieci Komputerowych

Wykład 13

- **Bezpieczeństwo sieci**
- **Monitorowanie i zarządzanie węzłami sieci komputerowej**

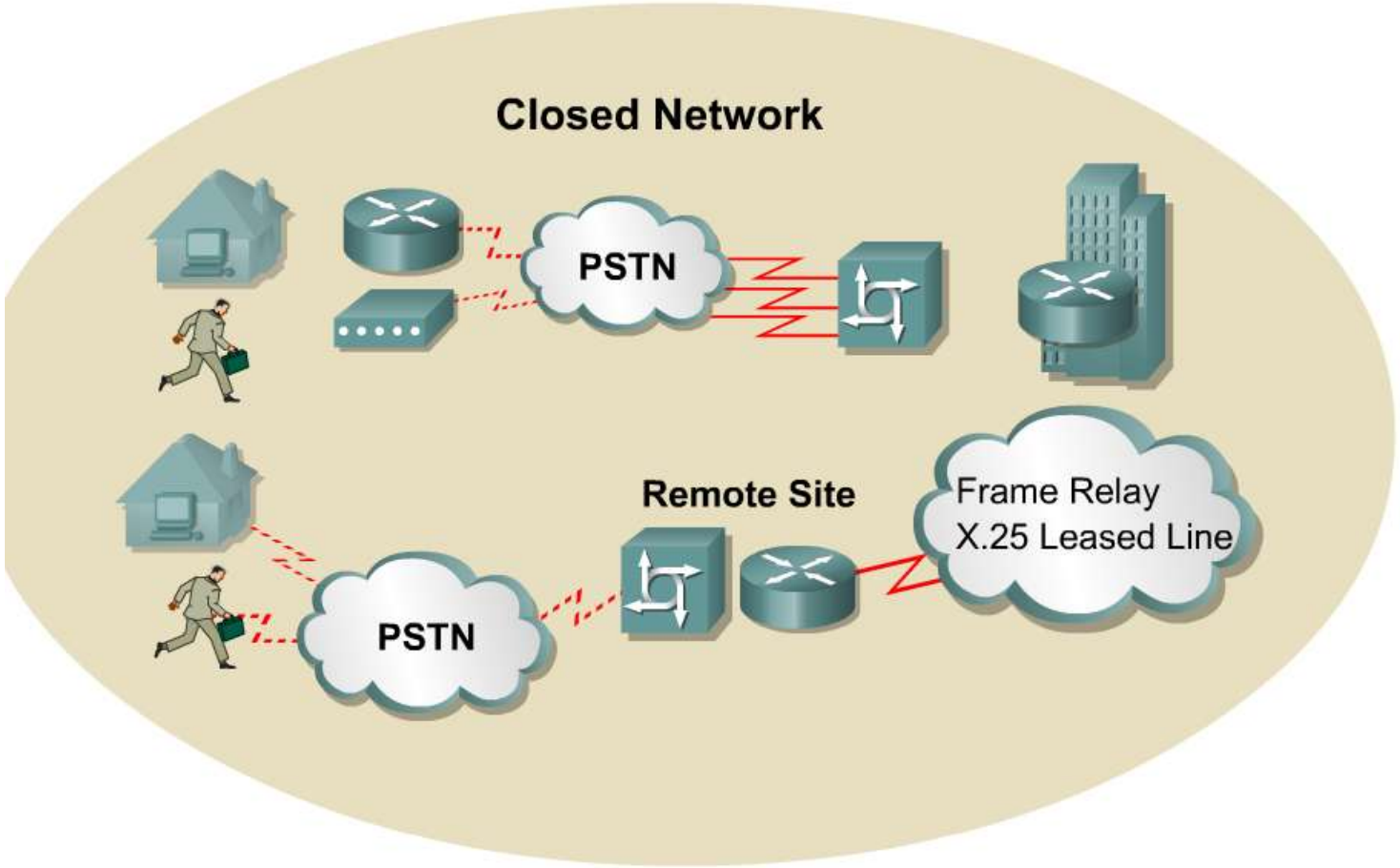


dr inż. Artur Sierszeń asiersz@kis.p.lodz.pl
dr inż. Łukasz Sturgulewski luk@kis.p.lodz.pl

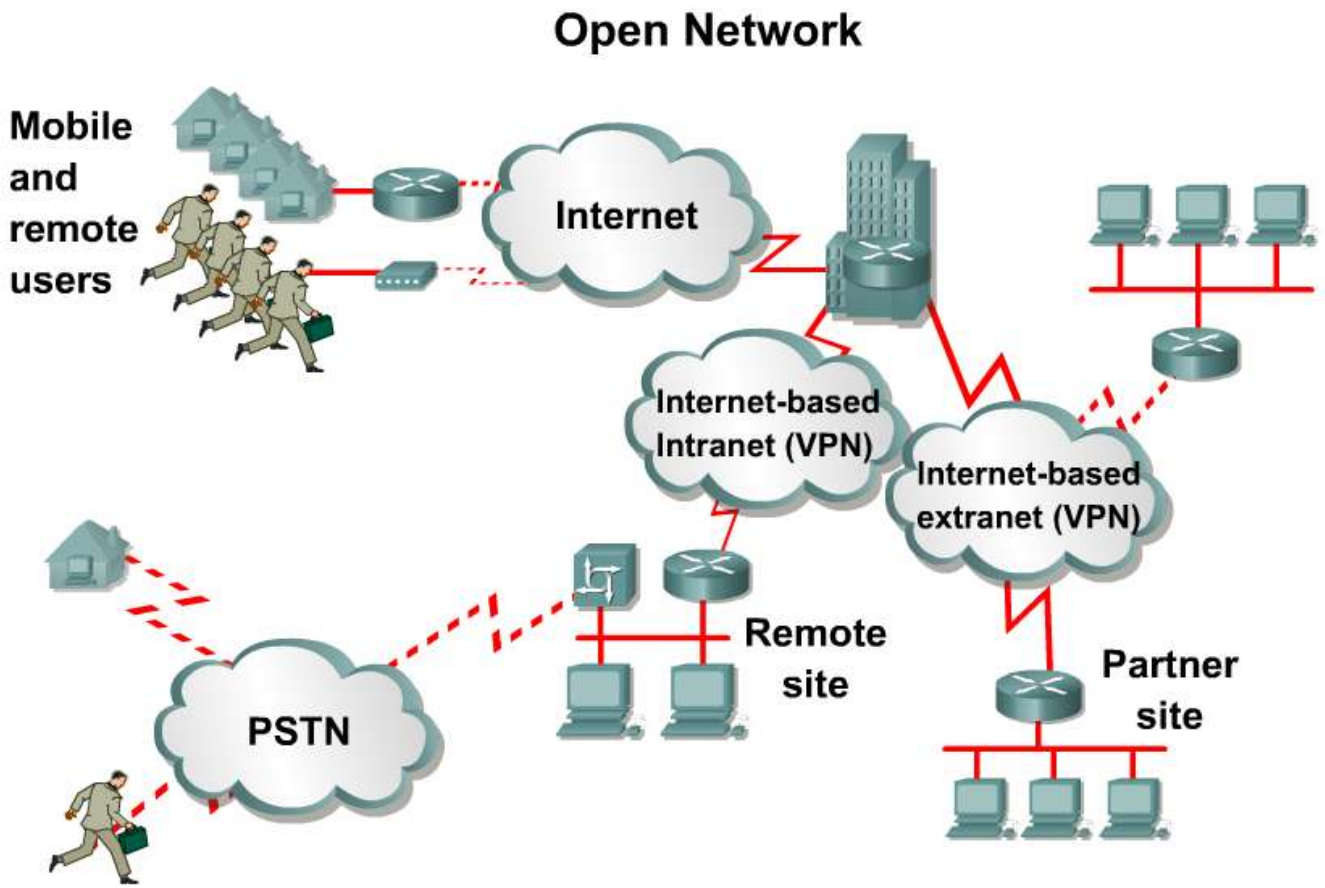
Terminy kluczowe

- Poufność - *Confidentiality*
- Integralność - *Integrity*
- Dostępność - *Availability*
- Podatność - Vulnerability
- Zagrożenia - *Threat*
- Rozpoznanie - *Reconnaissance*
- Dostęp - *Access*
- Odmowa usługi - *Denial of Service*
- Szyfrowanie - *Encryption*
- Koło bezpieczeństwa - *Security Wheel*

Zamknięte sieci



Współczesna sieć



Tendencje dotyczące bezpieczeństwa sieciowego

- Wzrost ilości ataków sieciowych
- Wzrost stopnia skomplikowania ataków
- Wzrost uzależnienia od sieci komputerowych
- Brak wykwalifikowanego personelu
- Brak świadomości użytkowników sieci
- Brak polityk bezpieczeństwa
- Bezprzewodowy dostęp
- Ustawodawstwo
- Spór prawny

Cele ochrony sieciowej

- Dostępność
- Poufność
- Integralność

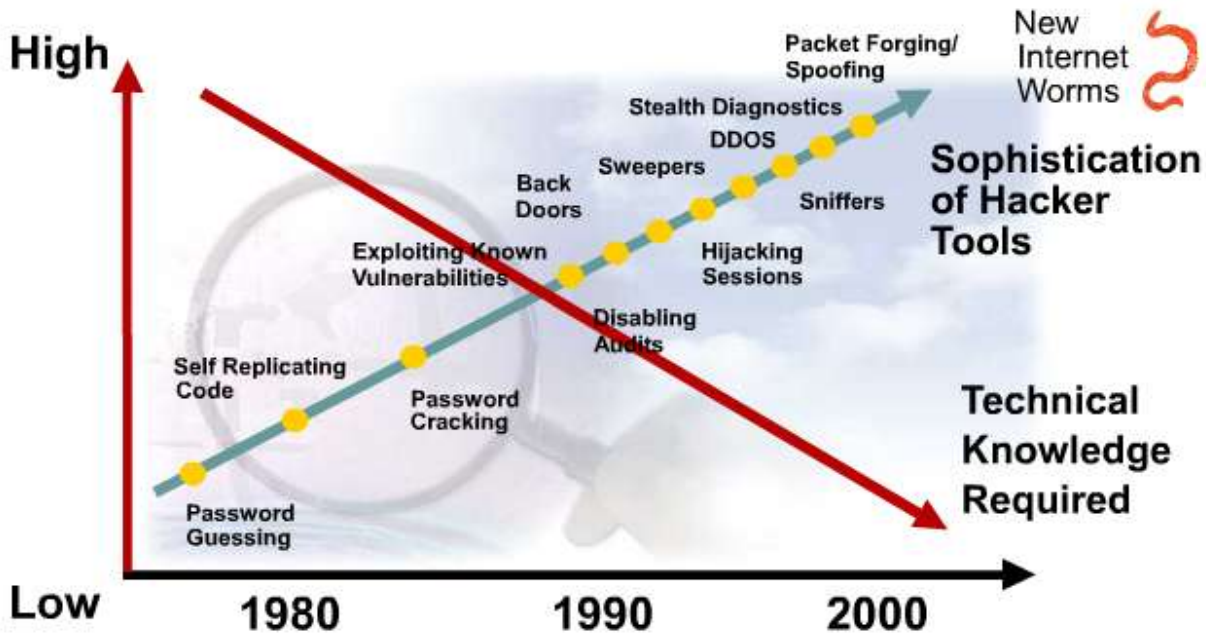
Kluczowe elementy ochrony sieci

Identity	Perimeter Security	Data Privacy	Security Monitoring	Security Management
				
Authentication Authorization Accounting	Firewalls	Virtual Private Network	Intrusion Detection Systems	Policy Management Tools

Wrażliwość sieci na ataki

- Technologia
- Konfiguracja
- Polityka bezpieczeństwa

Możliwość zagrożeń – bardziej niebezpieczny a łatwiejszy do użytkowania



Threats continue to become more sophisticated as the technical knowledge required to implement attacks deminishes.

Cztery klasy ataków sieciowych

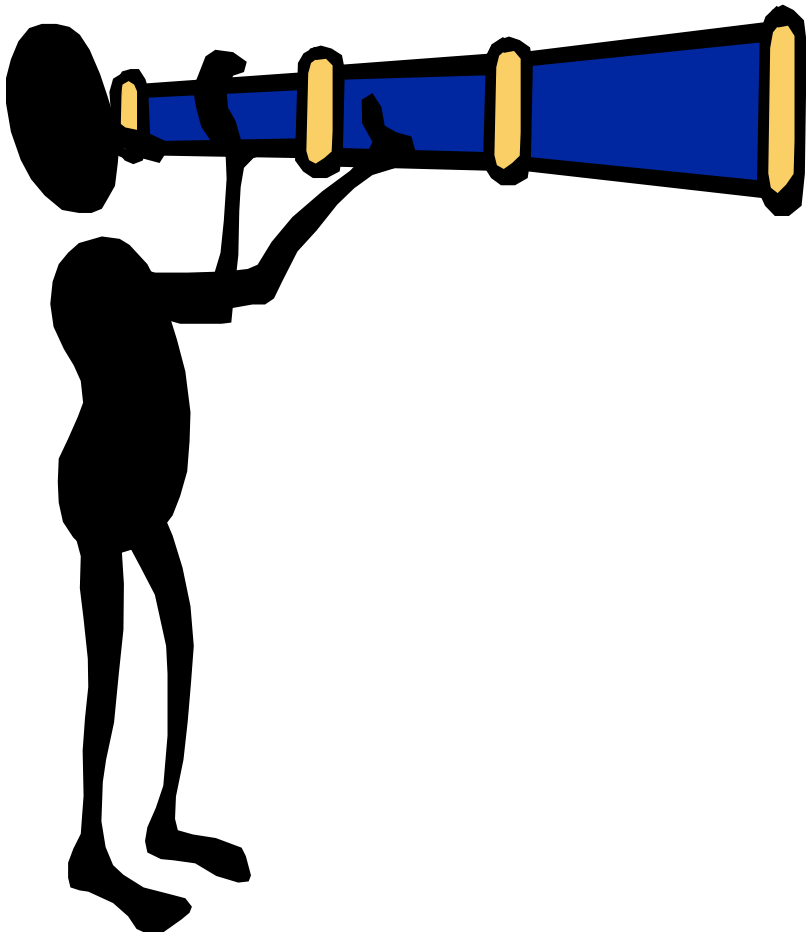
- Ataki rozpoznawcze
- Ataki dostępowe
- Odmowa usługi
- Robaki, wirusy i konie trojańskie

Specyficzne rodzaje ataków

- Poniższe zagrożenia mogą dotyczyć twojego systemu:
  - Packet sniffers
  - IP weaknesses
  - Password attacks
  - DoS or DDoS
  - Man-in-the-middle attacks
  - Application layer attacks
  - Trust exploitation
  - Port redirection
  - Virus
  - Trojan horse
  - Operator error
  - Worms

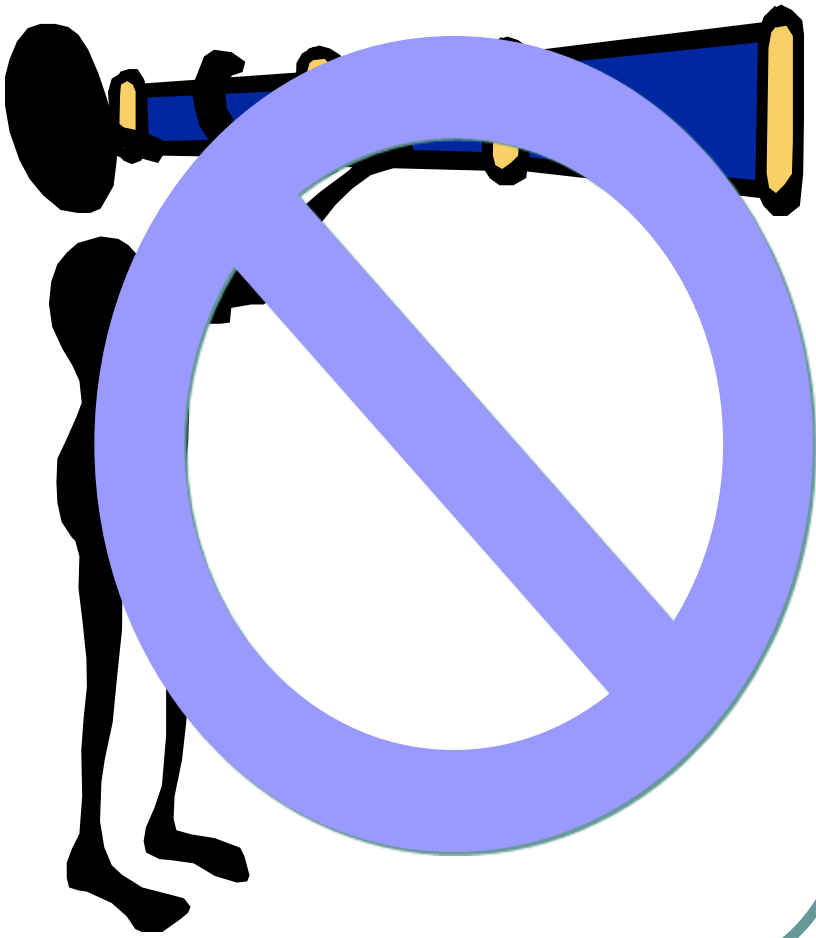
Ataki rozpoznawcze

- Rozpoznanie sieci odnosi się do zjawiska zbierania informacji na temat docelowej sieci przy użyciu ogólno dostępnych informacji i aplikacji.

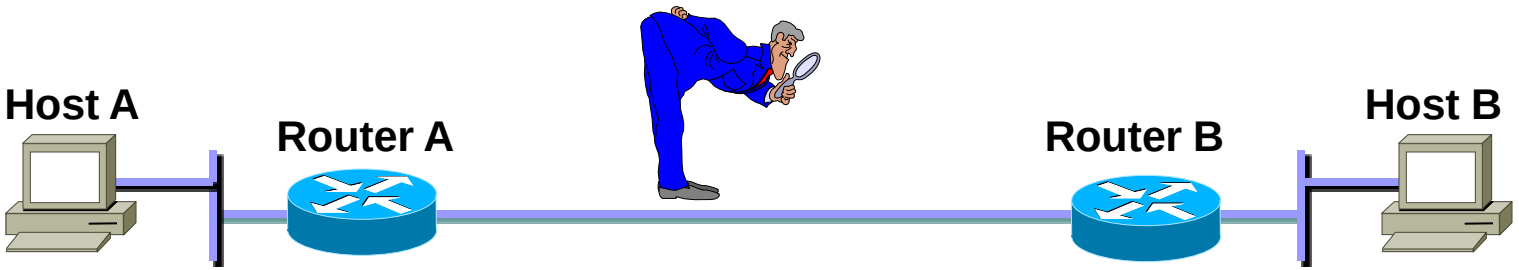


Zwalczanie ataków rozpoznawczych

- Nie można całkowicie zapobiec rozpoznaniu sieci.
- IDS w sieci i poziomy dostępu mogą z reguły powiadomić administratora kiedy przebiega atak rozpoznawczy (na przykład ping sweeps i skanowanie portów).

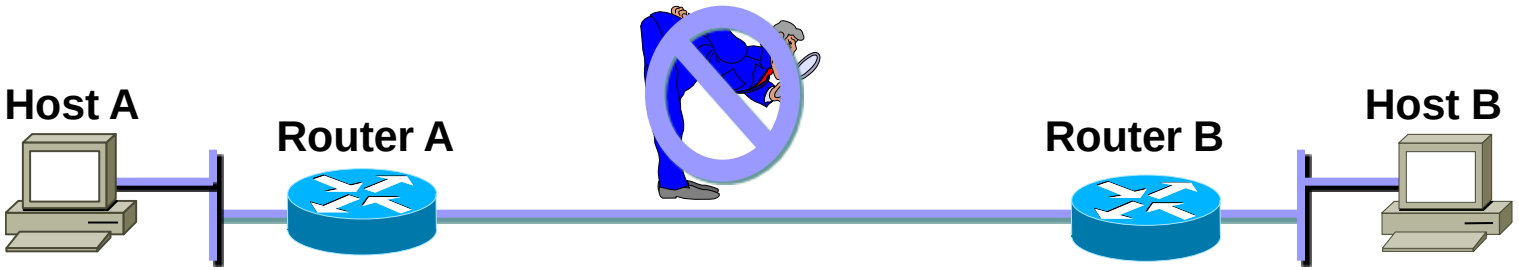


Snifing pakietów - Packet Sniffers



- Snifing pakietów to program, który wykorzystuje kartę sieciową w trybie nasłuchiwania aby przechwycić wszystkie pakiety sieciowe.
- Poniżej wypisano właściwości snifingu pakietów:
  - Snifing pakietów wykorzystuje przekazywane czystym tekstem. Protokoły, które przekazują informację w ten sposób to:
    - Telnet
    - FTP
    - SNMP
    - POP
  - Snifing pakietów mysi odbywać się w tej samej domenie kolizji.

Zwalczanie snifingu pakietów



- Poniższe techniki i narzędzia mogą być wykorzystane do zwalczania snifingu pakietów:
  - Uwierzytelnianie – używanie silnego uwierzytelniania np. poprzez hasła jednorazowe jest pierwszą opcją obrony .
  - Infrastruktura przyłączania — zastosowanie odpowiedniej infrastruktury przyłączania przeciwdziała stosowaniu snifingu pakietów w twoim środowisku.
  - Narzędzia antysnifingowe — zastosowanie takich narzędzi umożliwia uaktywnienie programów i sprzętu zaprojektowanego do wykrywania snifingu w sieci.
  - Szyfowanie — najskuteczniejsza metoda przeciwdziałania snifingowi; nie zabezpiecza i nie wykrywa snifingu, ale sprawia, że staje się on nieistotny.

IP Spoofing

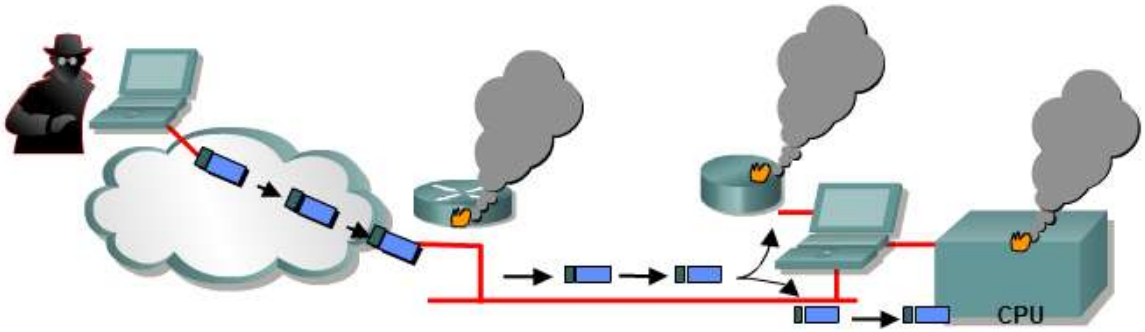
- IP spoofing występuje, kiedy haker na zewnątrz lub wewnątrz sieci używa zaufanego adresu IP.
- Podczas IP spoofing wykorzystuje się dwie techniki:
  - Haker używa adresu IP, który znajduje się pośród zaufanych adresów.
  - Haker używa uwierzytelnionego zewnętrznego adresu IP, który jest zaufany.
- IP spoofing wykorzystywany jest do:
  - IP spoofing jest z reguły ograniczony do wprowadzenia szkodliwych danych lub poleceń do istniejącego strumienia danych.
  - Haker zmienia tabele routingu, aby wskazać adres IP, pod który się podszywa w celu otrzymywania wszystkich sieciowych pakietów, które wysyłane są na ten adres. Może wtedy odpowiadać na nie jako zaufany użytkownik.

Zwalczanie IP Spoofing

- Zagrożenie IP spoofingiem może być zredukowane, ale nie wyeliminowane, przez zastosowanie następujących procedur:
  - Kontrola dostępu (Access control) — Najpopularniejsza metoda zapobiegania IP spoofingowi to odpowiednie skonfigurowanie kontroli dostępu.
  - Filtrowanie zgodne z RFC 2827 — Możesz zapobiegać IP spoofingowi innych sieci przez twoich użytkowników poprzez powstrzymanie ruchu na zewnątrz, który nie posiada adresu źródłowego należącego do zakresu twoich adresów IP.
  - Dodatkowe uwierzytelnianie nie wykorzystujące uwierzytelniania opartego na IP — Przykładem takiego uwierzytelniania może być:
    - szyfrowanie (zalecane)
    - silne, wieloskładnikowe, jednorazowe hasła

Ataki DoS – Denial of Service

DoS attacks prevent authorized people from using a service by using up system resources.



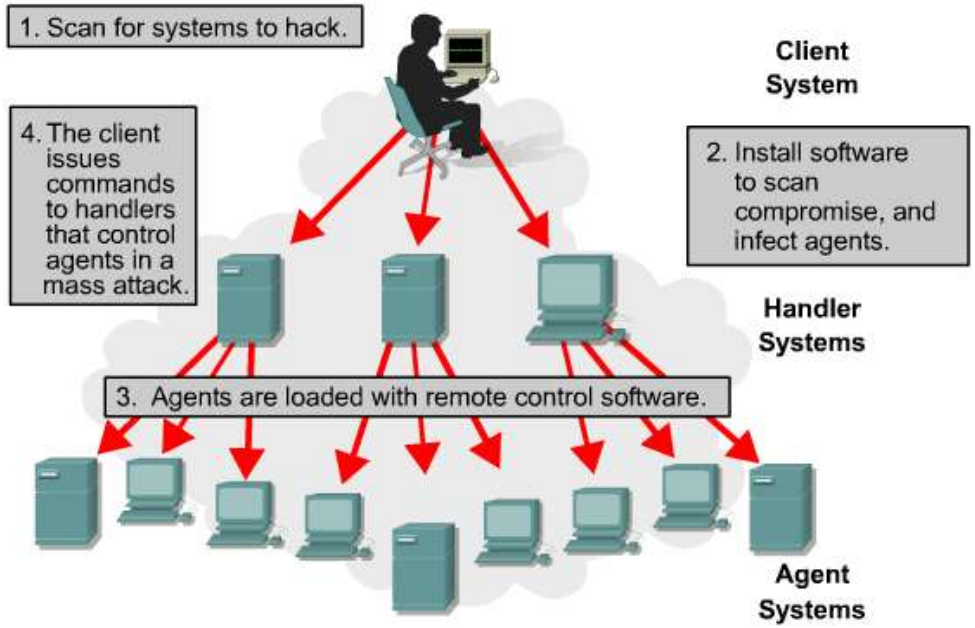
Resource overloads

- Disk space, bandwidth, buffers, and so on.
- Ping floods: smurf, and so on.
- Packet storms: UDP bombs, fraggle, and so on.

Malformed data

- Oversized packets: ping of death, and so on.
- Overlapping packets: winuke, and so on.
- Un-handled data: teardrop, and so on.

Przykład ataku DDoS – Distributed DoS



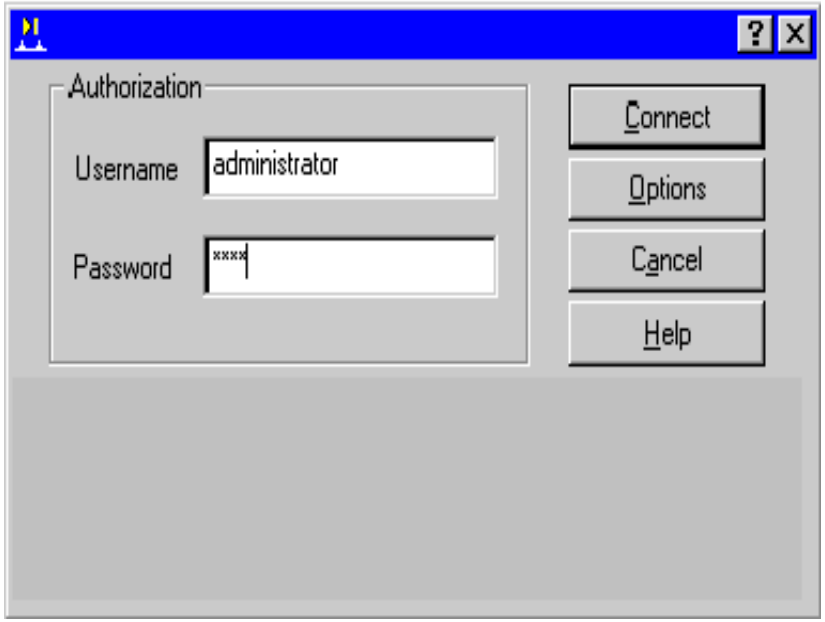
In a Distributed Denial of Service attack (DDoS) a hacker tricks other machines into flooding the target machine with nuisance traffic that robs system performance.

Zwalczanie ataków Dos

- Zagrożenie atakami DoS może zostać zredukowane przez zastosowanie następujących trzech metod:
  - Właściwości antyspoofingu — Odpowiednia konfiguracja właściwości antyspoofingu na routerach i zaporach ogniowych
  - Właściwości anty-DoS — Odpowiednia konfiguracja właściwości anty-DoS na routerach i zaporach ogniowych
  - Ograniczenie poziomu ruchu — Zastosowanie ograniczenia poziomu ruchu do poziomu zgodnego z siecią ISP

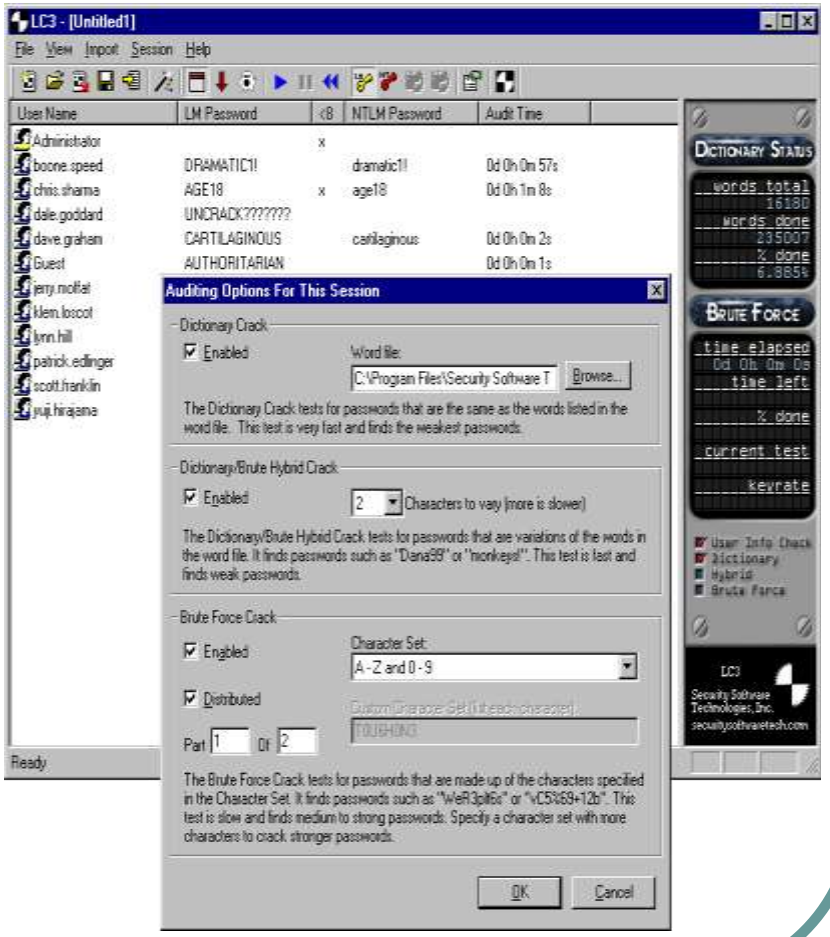
Ataki na hasło

- Hakerzy mogą stosować ataki na hasło, używając kilku różnych metod:
  - Ataki siłowe
  - Ataki słownikowe
  - Konie trojańskie
  - IP spoofing
  - Snifing pakietów



Przykład ataku na hasło

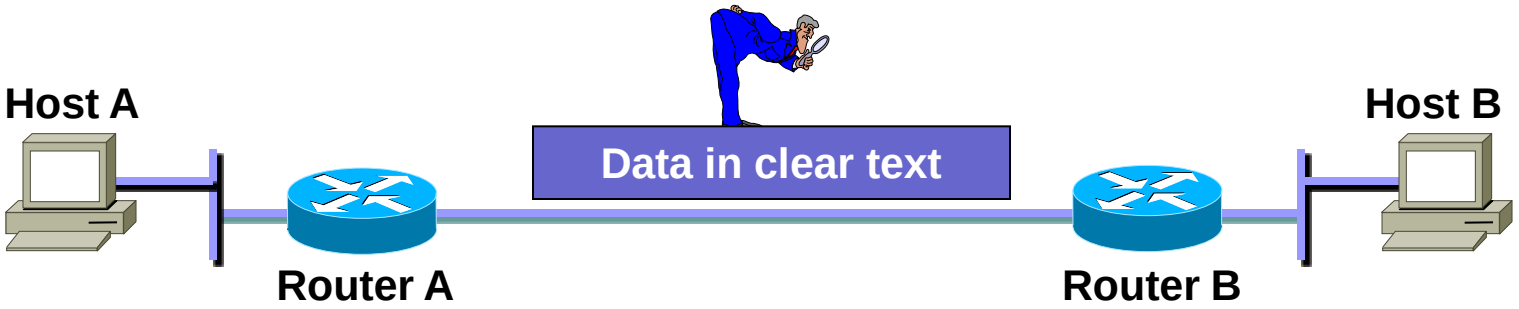
- L0phtCrack może pobrać zahaszowane znaki hasła i wygenerować z nich treść hasła. Hasła są łamane dwoma różnymi metodami:
  - Ataki słownikowe
  - Ataki siłowe



Zwalczanie ataków na hasło

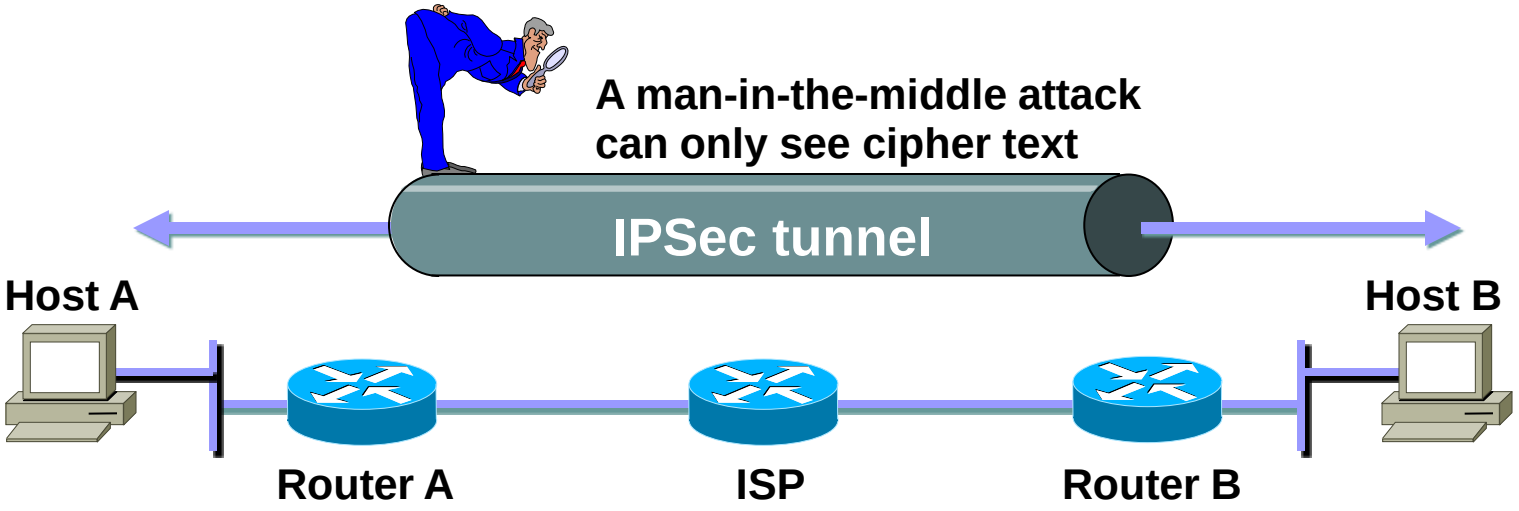
- Istnieją następujące metody zwalczania:
  - Nie pozwól użytkownikom używać takiego samego hasła na wielu systemach.
  - Wyłączaj konto po przekroczeniu określonej liczby nieudanych prób zalogowania.
  - Nie używaj haseł wyłącznie literowych. Zalecane są hasła szyfrowane lub OTP.
  - Używaj „silnych” haseł. Silne hasło to takie, którego długość wynosi przynajmniej 8 znaków i zawiera małe i duże litery, cyfry i znaki alfanumeryczne.

Ataki typu Man-in-the-Middle



- Ataki typu man-in-the-middle wymagają, aby haker posiadał dostęp do pakietów sieciowych, które przechodzą przez sieć.
- Implementacja ataku typu man-in-the-middle attack is implemented wymaga zastosowania:
  - Snifingu pakietów
  - Protokołów routingu i warstwy transportowej
- Możliwe zastosowania ataków typu man-in-the-middle:
  - Kradzież informacji
  - Przejęcie trwającej sesji
  - Analiza ruchu
  - DoS
  - Uszkodzenie transmitowanych danych
  - Wprowadzenie nowych informacji do sesji sieciowej

Zwalczanie ataków typu Man-in-the-Middle



- Ataki typu Man-in-the-middle mogą być skutecznie zwalczane tylko przy wykorzystaniu szyfrowania.

Ataki na warstwę aplikacji

- Ataki na warstwę aplikacji mają następujące właściwości:
  - Wykorzystują dobrze znane słabości, np. protokoły, które są nieodłącznym elementem aplikacji lub systemu (na przykład sendmail, HTTP i FTP)
  - Często korzystają z portów, które są przepuszczane przez zaporę ogniową (na przykład 80 port TCP używany do ataku na serwery WWW zza zapory ogniowej)
  - Nigdy nie mogą być zupełnie wyeliminowane, ponieważ wciąż odkrywane są nowe słabe punkty

Zwalczanie ataków na warstwę aplikacji

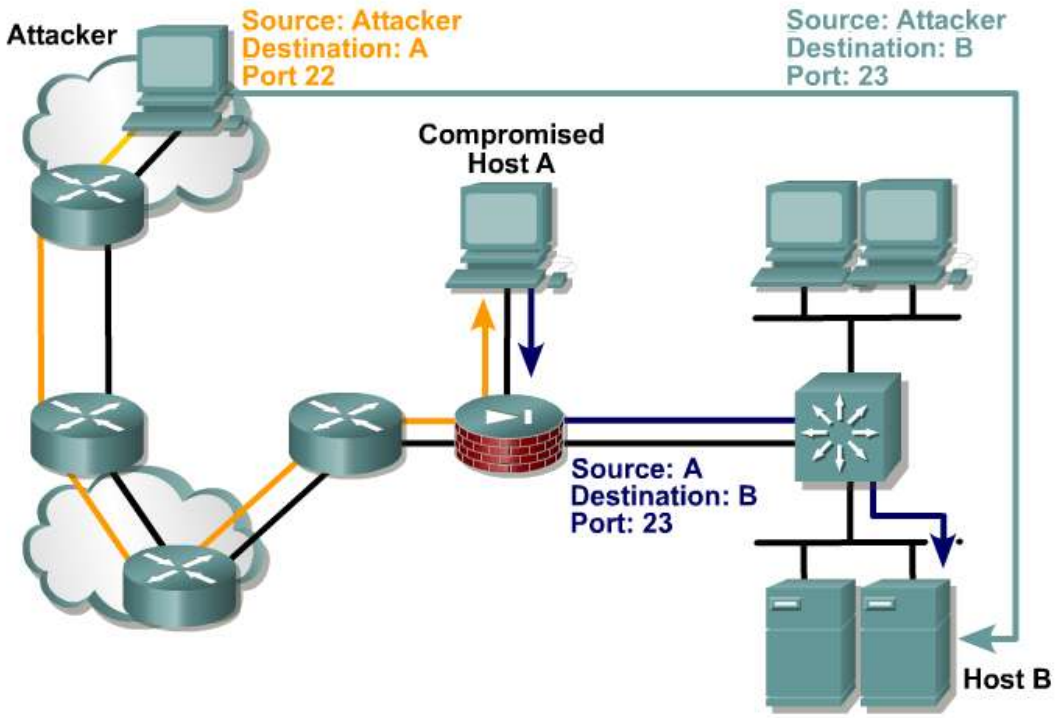
- Niektóre działania, jakie możesz podjąć w celu zredukowania ryzyka, to:
  - Przeczytaj logi systemu operacyjnego i sieci zanalizuj je za pomocą odpowiednich aplikacji.
  - Zapisz się na listy mailingowe, na których publikowane są informacje o słabych punktach.
  - Uaktualniaj swój system operacyjny i aplikacje najnowszymi patchami.
  - IDS może skanować w poszukiwaniu znanych ataków, monitorować i tworzyć logi ataku oraz, w niektórych przypadkach, zapobiegać atakom.

Przekierowanie portów - Port Redirection

Port redirection is a type of trust-exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped.

It is mitigated primarily through the use of proper trust models.

Antivirus software and host-based IDS can help detect and prevent a hacker installing port redirecting utilities on the host.



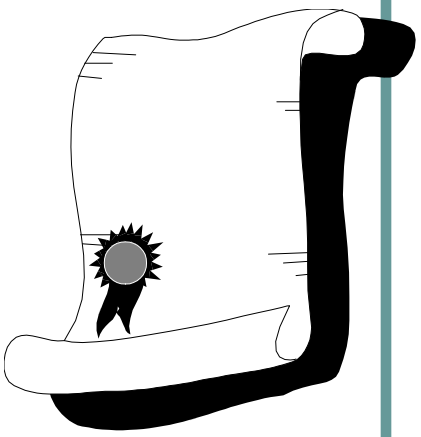
Wirusy i konie trojańskie

- Wirusy odnoszą się do złośliwego oprogramowania, które jest dołączane do innego programu w celu wykonania szczególnej niechcianej funkcji na stacji roboczej. Końcowe stacje robocze są podstawowym celem wirusów.
- Koń trojański różni się jedynie tym, że cały program został napisany tak, aby wyglądał jak coś innego, podczas gdy jest on w rzeczywistości narzędziem ataku. Koń trojański jest zwalczany przez oprogramowanie antywirusowe na poziomie użytkownika i jeżeli jest to możliwe, na poziomie sieci.

Słabe punkty istnieją na wszystkich warstwach modelu OSI

Co jest polityką bezpieczeństwa ?

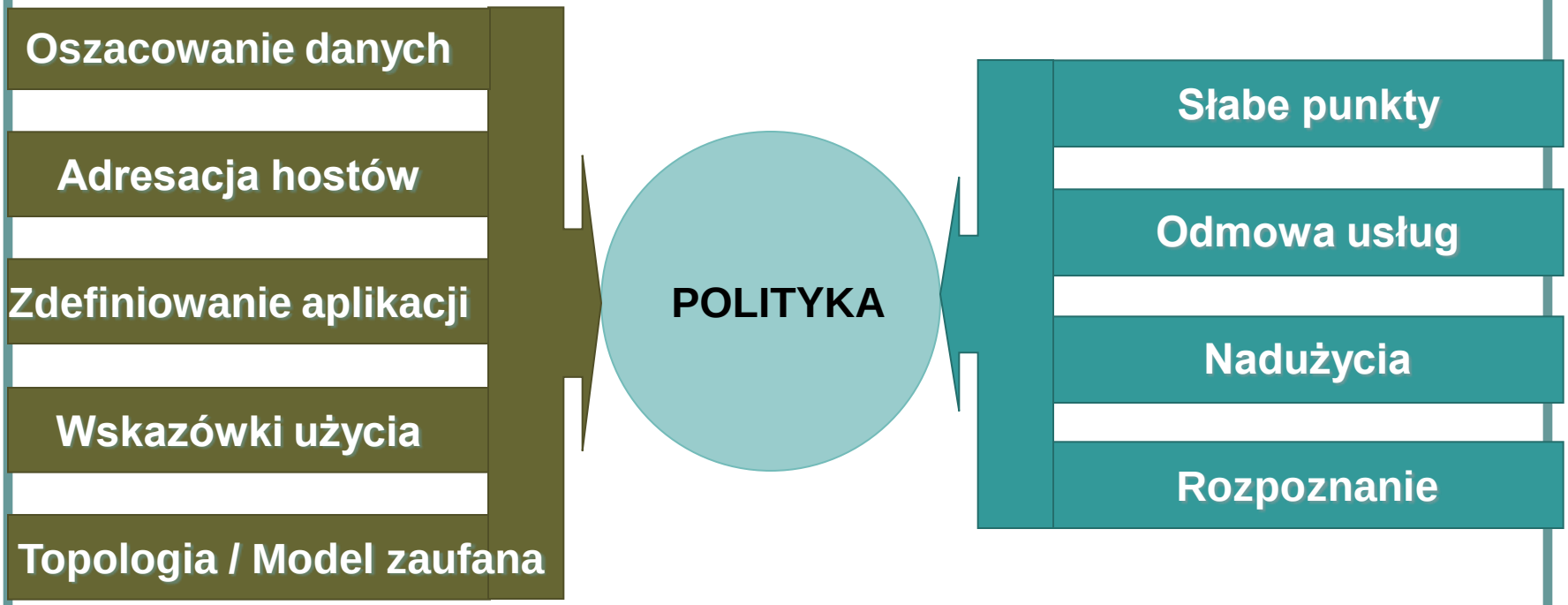
- "A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."
- „Polityka bezpieczeństwa jest formalnym zbiorem zasad, którymi kierować się muszą ludzie, mający dostęp do technologii i zasobów informacyjnych organizacji."
- (RFC 2196, Site Security Handbook)



Po co tworzymy politykę bezpieczeństwa ?

- Aby stworzyć podstawę dla ochrony
- Aby ustalić ramy implementacji zabezpieczeń
- Aby zdefiniować dozwolone i niedozwolone zachowania
- Aby pomóc określić niezbędne narzędzia i procedury
- Aby ustanowić consensus i zdefiniować role
- Aby ustalić, jak radzić sobie z przypadkami utraty bezpieczeństwa

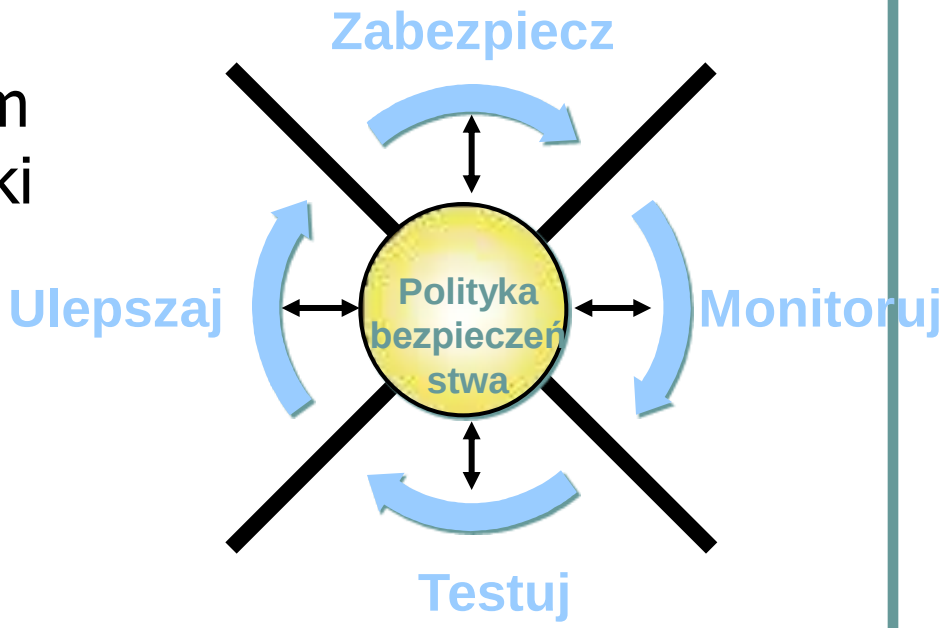
Elementy polityki bezpieczeństwa



- Na lewo znajdują się czynniki projektu sieci, na których oparta jest polityka bezpieczeństwa
- Na prawo znajdują się podstawowe kierunki zagrożeń internetowych, w celu zwalczania których projektuje się politykę bezpieczeństwa

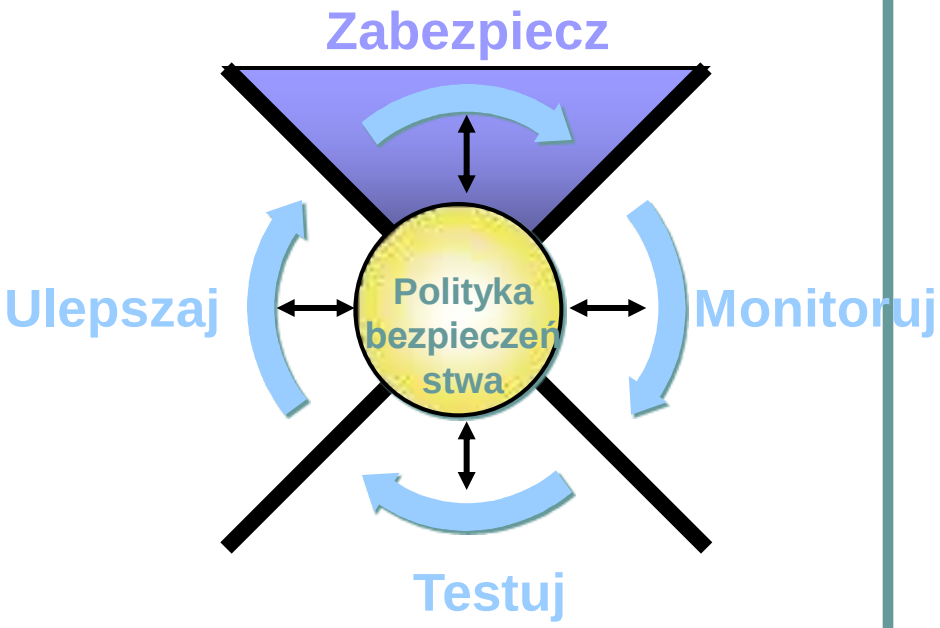
Bezpieczeństwo sieciowe jako nieustający proces

- Bezpieczeństwo sieciowe jest nieustającym procesem utworzonym dookoła polityki bezpieczeństwa.
  - Krok 1: Zabezpiecz
  - Krok 2: Monitoruj
  - Krok 3: Testuj
  - Krok 4: Ulepszaj



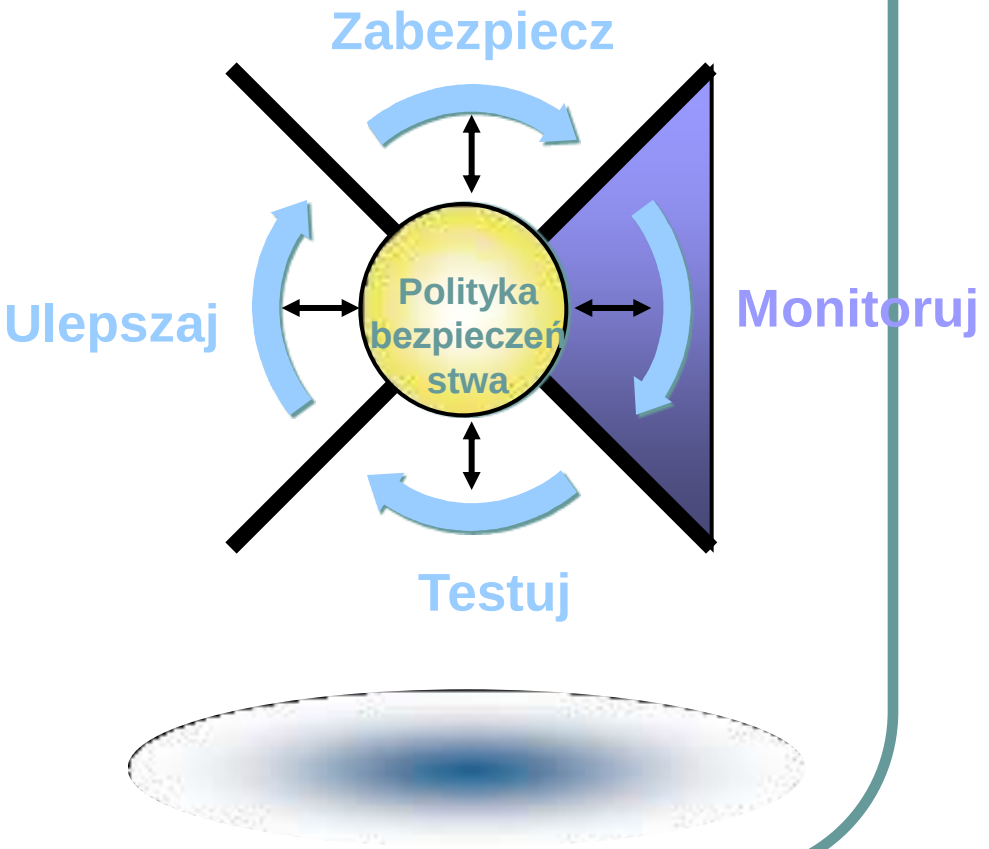
Ochrona sieci

- Wprowadź rozwiązania bezpieczeństwa, aby powstrzymać lub zapobiec nieautoryzowanemu dostępowi lub nieautoryzowanym działaniom i aby zabezpieczyć informacje:
  - Uwierzytelnianie
  - Szyfrowanie
  - Firewall
  - „Łatanie” wrażliwych miejsc (patching)



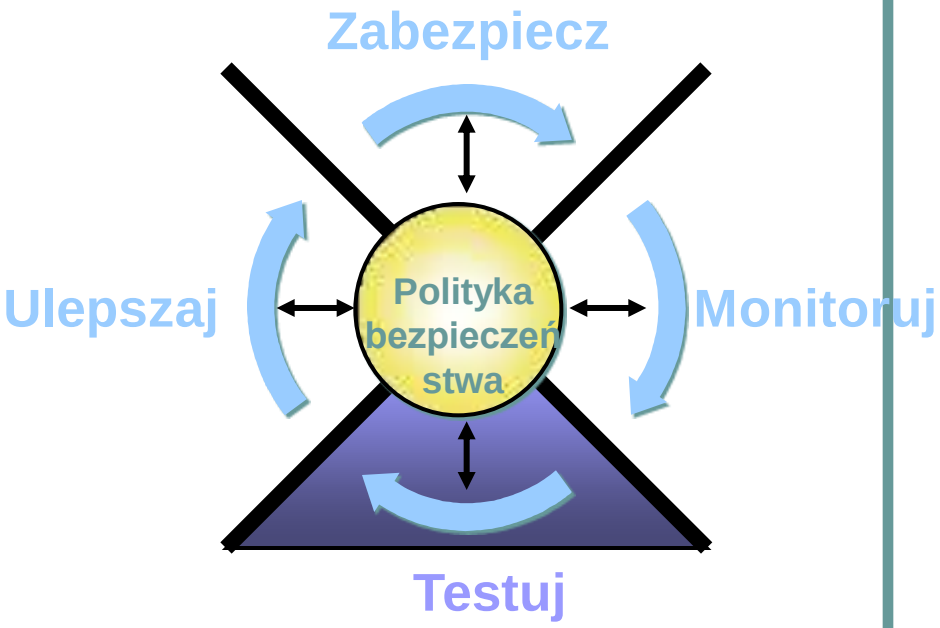
Monitorowanie bezpieczeństwa

- Wykrywa złamanie reguł polityki bezpieczeństwa
- Polega na przesłuchiwaniu systemu i detekcji włamań w czasie rzeczywistym
- Weryfikuje implementację zabezpieczeń z Kroku 1



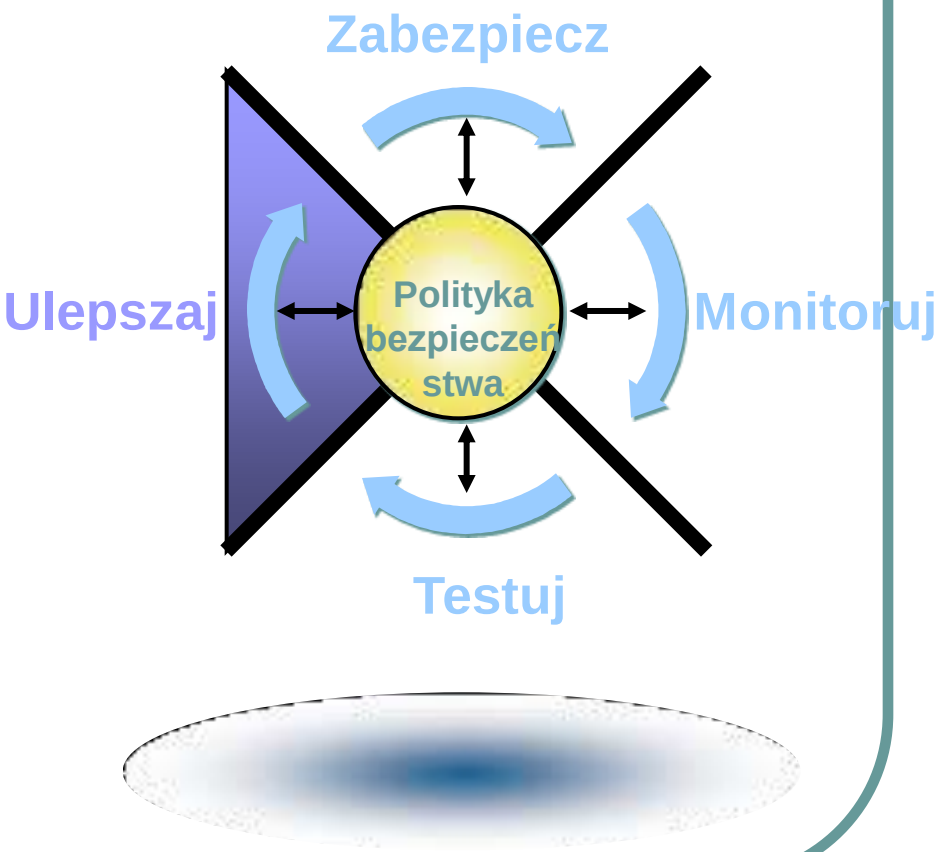
Testowanie bezpieczeństwa

- Weryfikuje skuteczność polityki bezpieczeństwa przez przesłuchiwanie systemu i skanowanie słabości

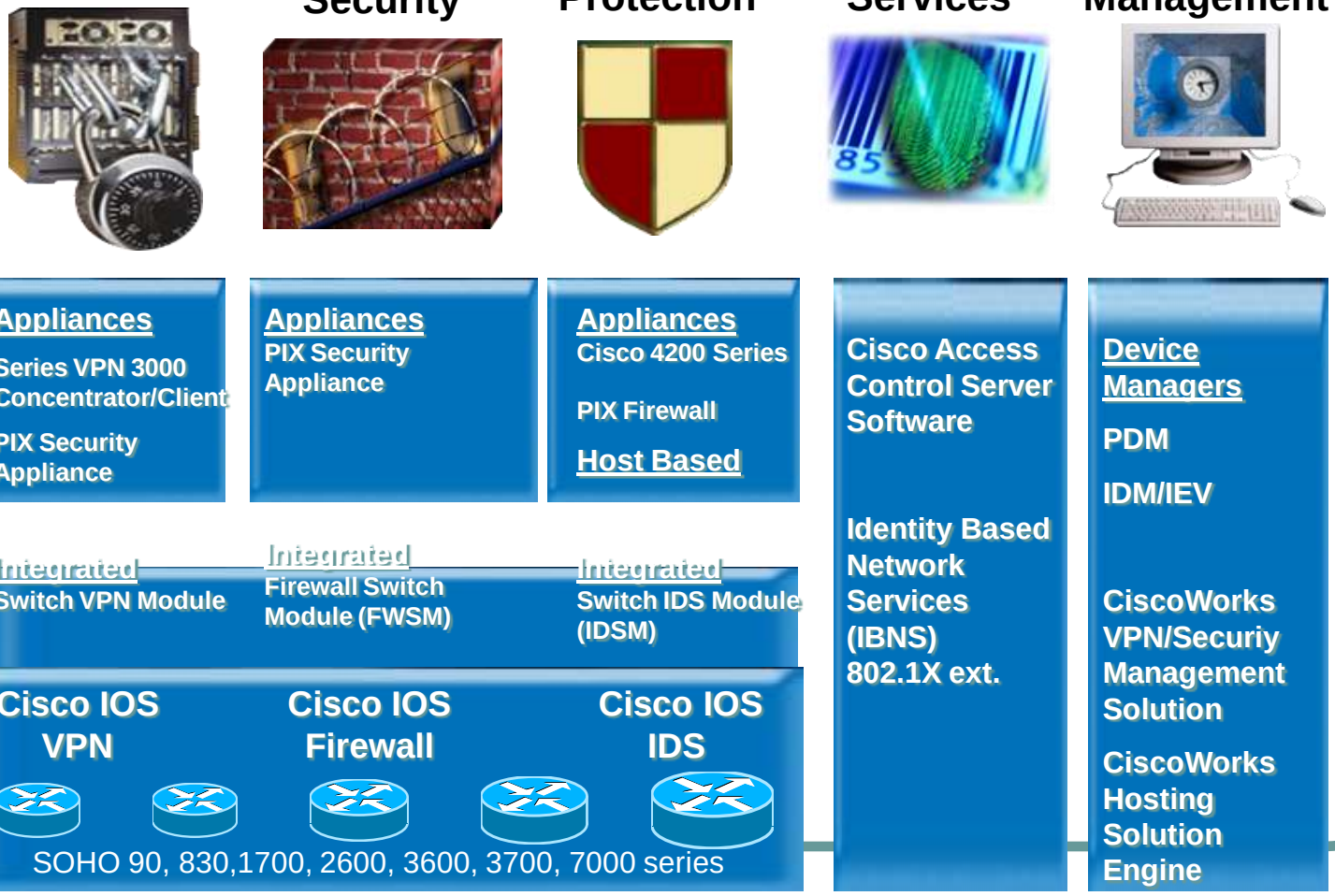


Ulepszanie bezpieczeństwa

- Używaj informacji uzyskanych przez monitorowanie i testowanie do wprowadzania ulepszeń do zaimplementowanych zabezpieczeń.
- Dostosuj politykę bezpieczeństwa w miarę identyfikacji słabości i zagrożeń.



Produkty i rozwiązania zabezpieczające sieci



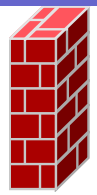
Tożsamość użytkownika

- Mechanizmy udowadniania, kim jesteś
  - Stosuje się zarówno do uwierzytelniania ludzi, jak i urządzeń
- Trzy atrybuty uwierzytelniania:
  - Coś, co wiesz
  - Coś, co masz
  - Coś, czym jesteś
- Najczęstsze podejścia do tożsamości:
  - Hasła
  - Tokeny
  - PKI (certyfikaty cyfrowe)
  - Podejście biometryczne

Typy zapór ogniowych

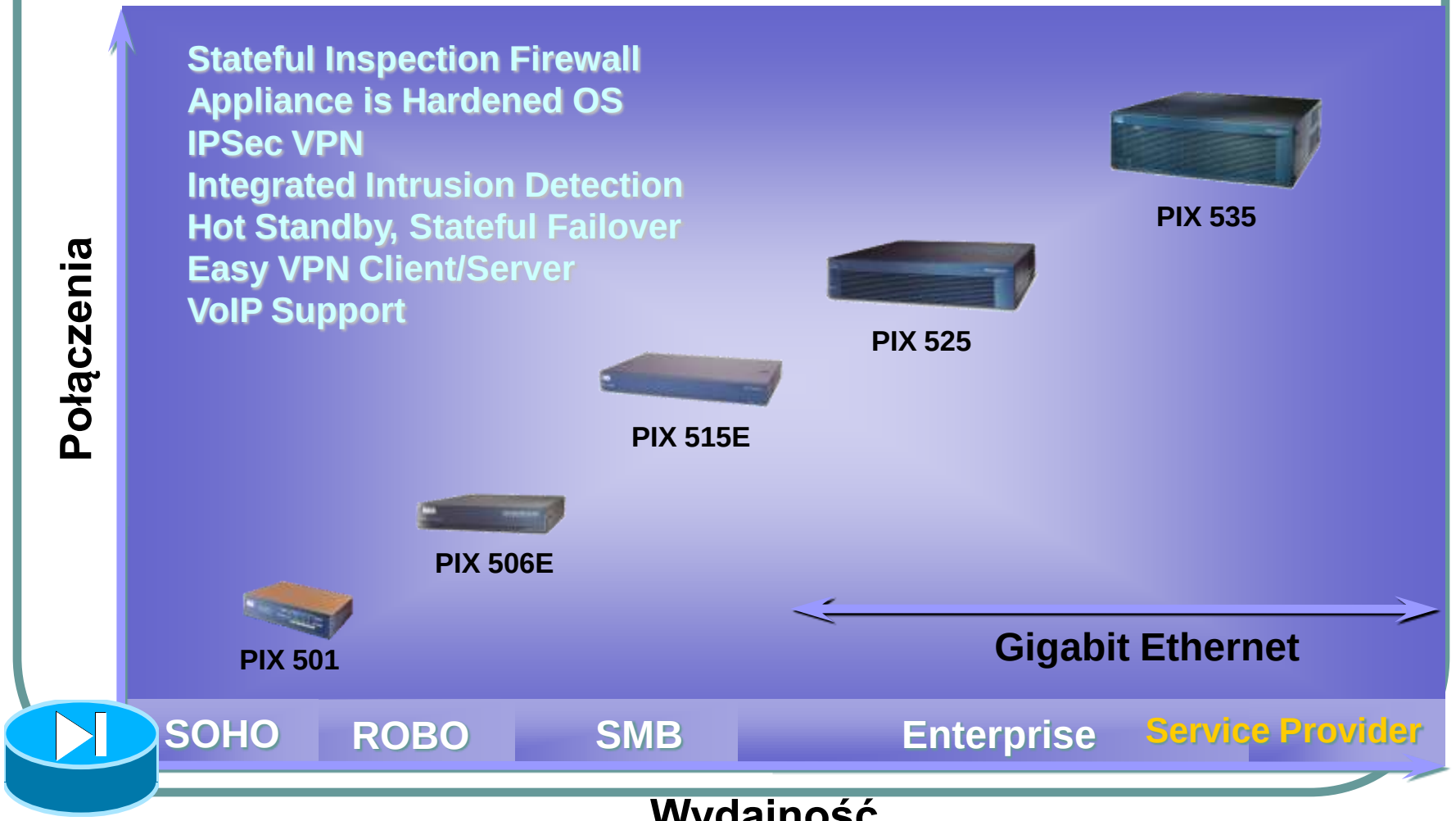
- Bazujące na serwerach
  - Microsoft ISA
  - CheckPoint
  - BorderManager
- Osobne urządzenie
  - PIX Security Appliance
  - Netscreen
  - SonicWall
- Osobiste
  - Norton
  - McAfee
  - ZoneAlarms
- Zintegrowane
  - IOS Firewall
  - Switch Firewall

Rozwiązania zapór ogniowych



		Solution Breadth				
PIX Appliance		PIX 501	PIX 506E	PIX 515E	PIX 525	PIX 535
Switch Module		Firewall Service Module (FWSM)				
IOS FW Router		800	1700	2600	3xxx	7xxx
VPN Client		VPN Client Software — Built in Personal FW				
Mgmt		Secure CLI		Web UI Embedded Mgr		Enterprise Mgmt VMS

PIX Security – wykres urządzeń



Obszary zastosowania systemów zarządzania sieciami

Kluczowe obszary zastosowania systemów zarządzania sieciami określone przez OSI:

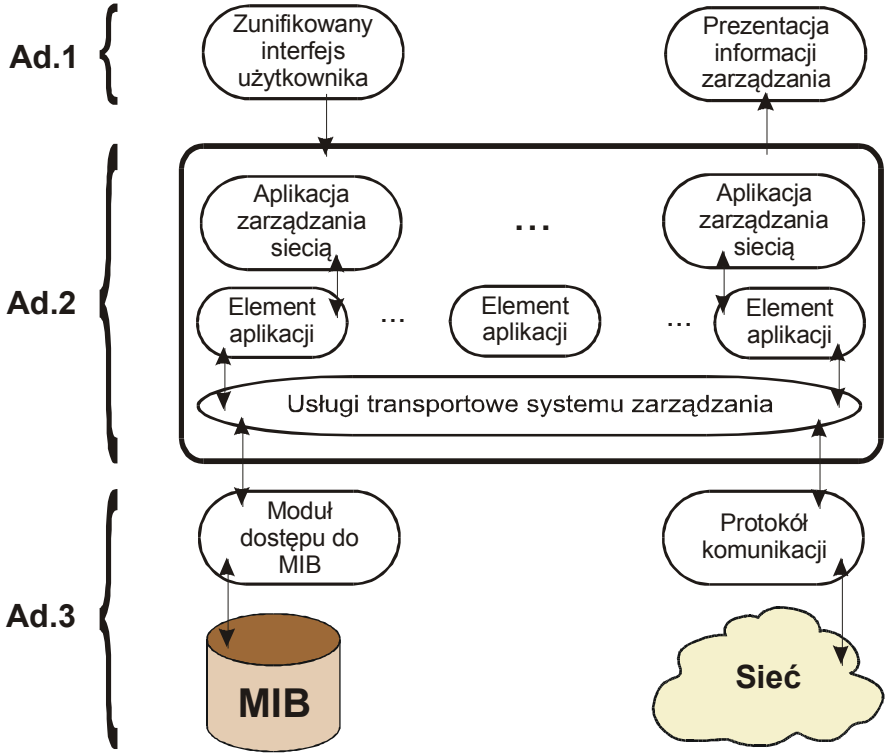
- Zarządzanie wydajnością.
- Zarządzanie uszkodzeniami, nieprawidłowościami.
- Zarządzanie kosztami.
- Zarządzanie konfiguracją i oznaczeniami.
- Zarządzanie bezpieczeństwem.

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



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.

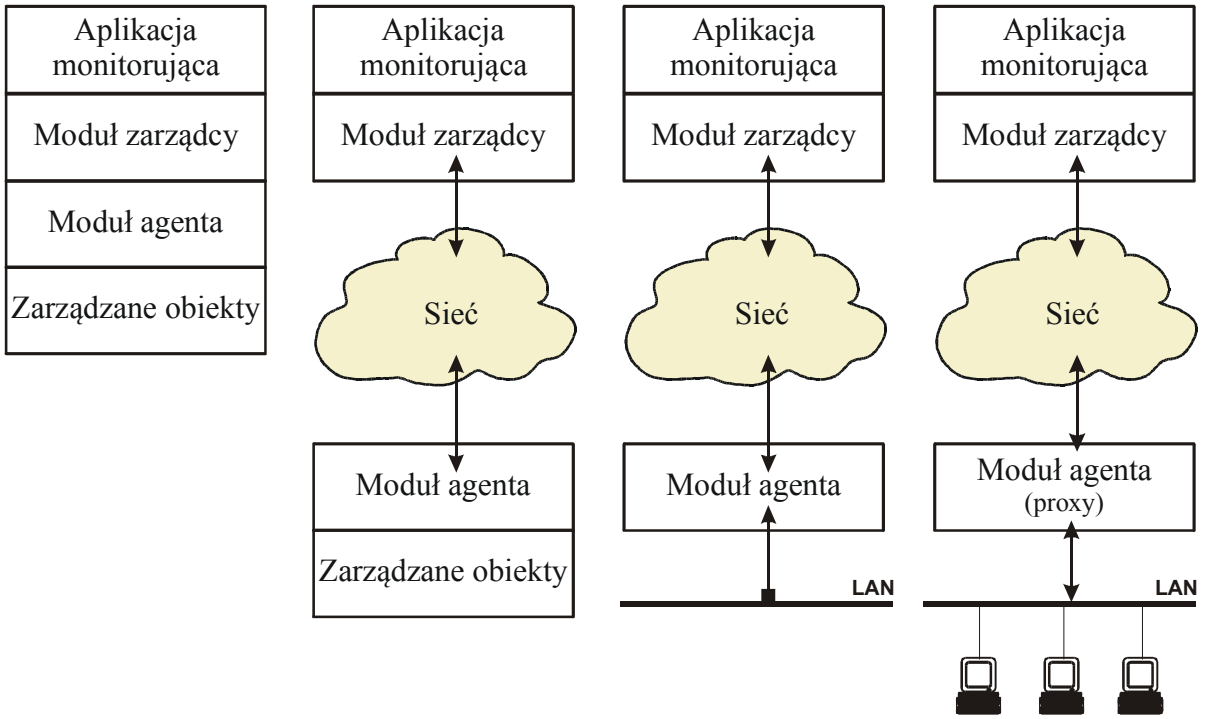
Monitoring sieci

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.

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.

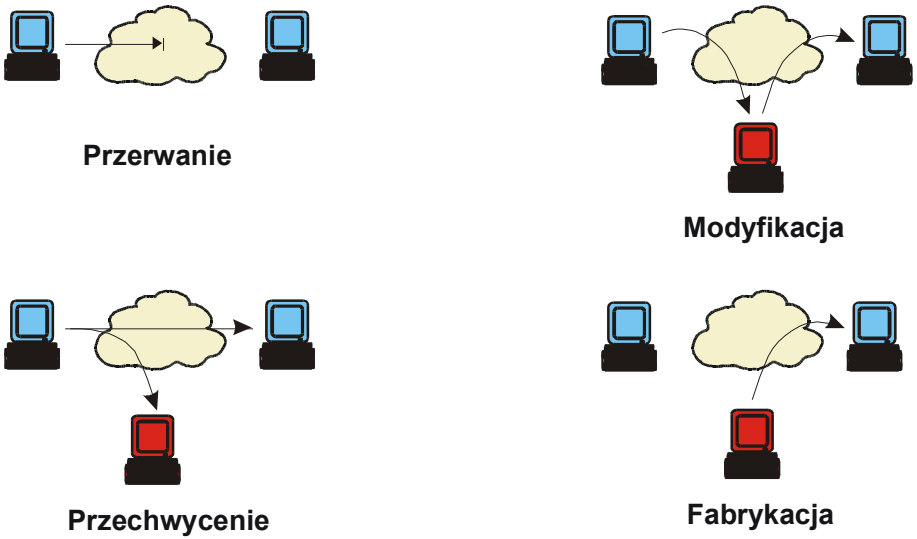
Kontrola konfiguracji

- 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.



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

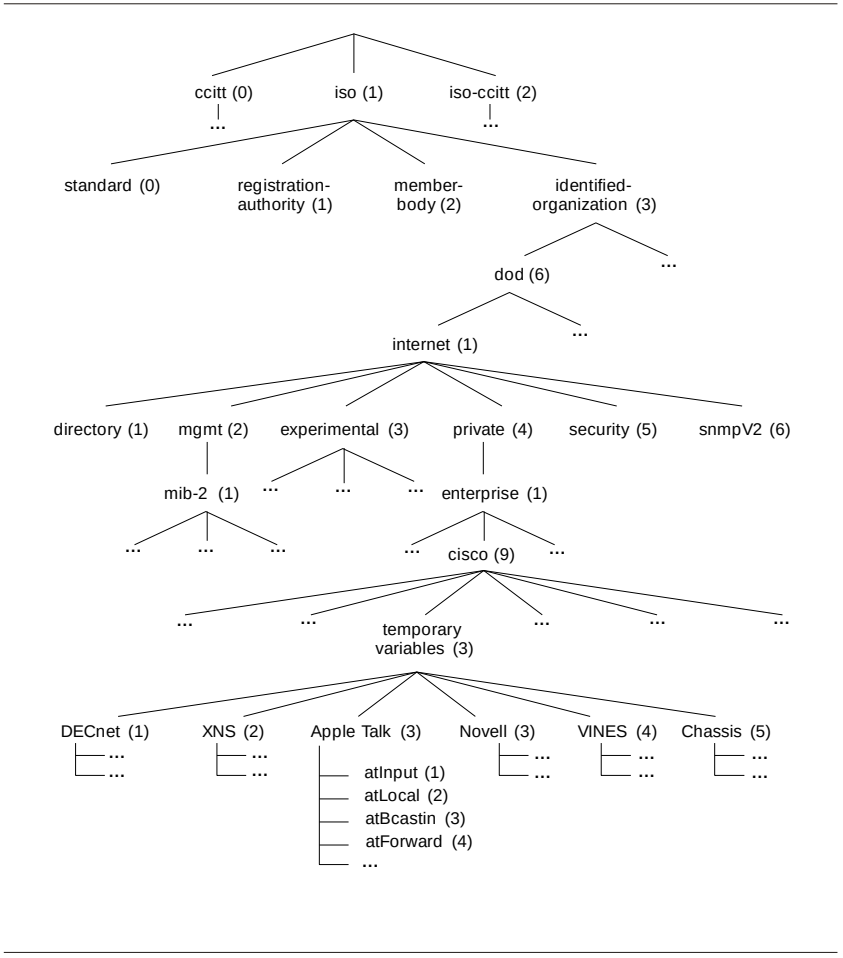
Protokoły zarządzania:

- 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

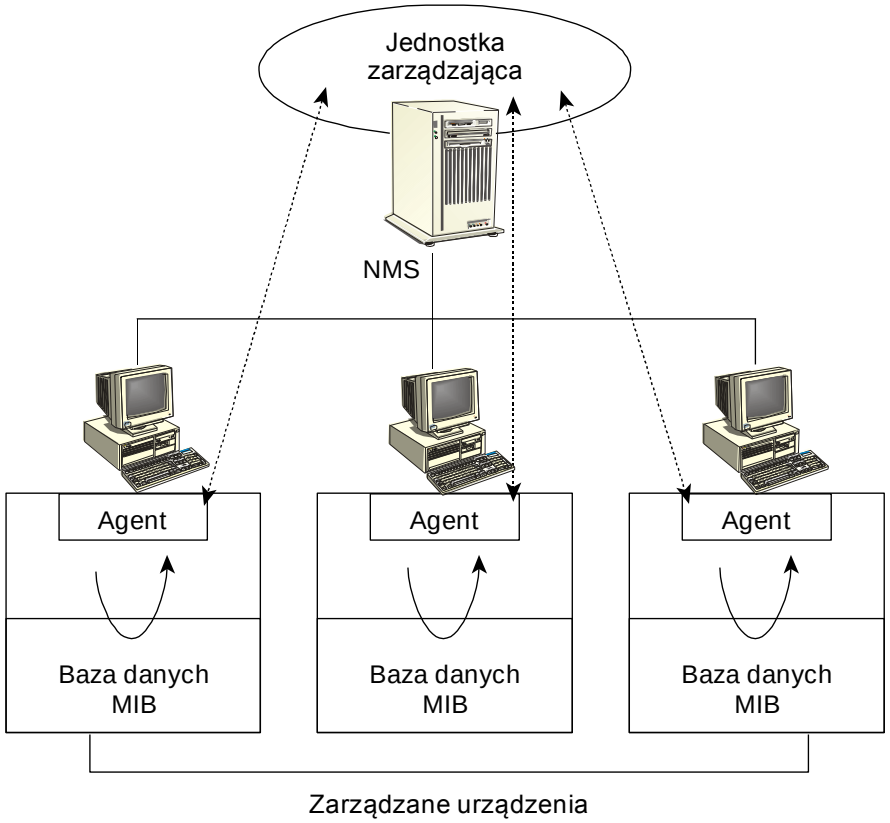
Bazy danych MIB



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



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.

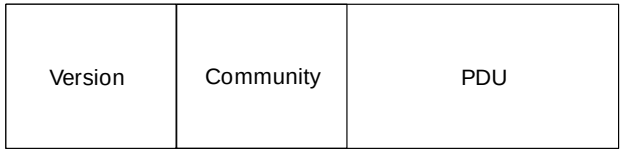
Społeczność

- 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.

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.

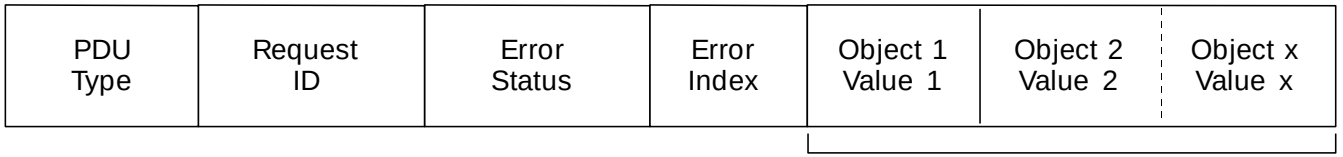
Format wiadomości SNMPv1

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

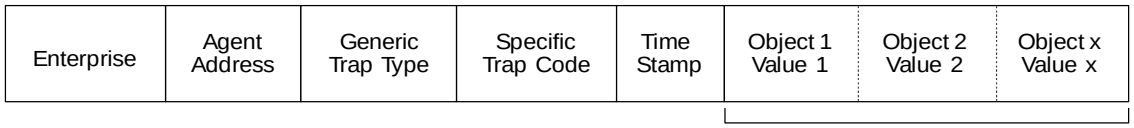


a.) Schemat blokowy.

```
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.

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.

Wykład 13

KONIEC