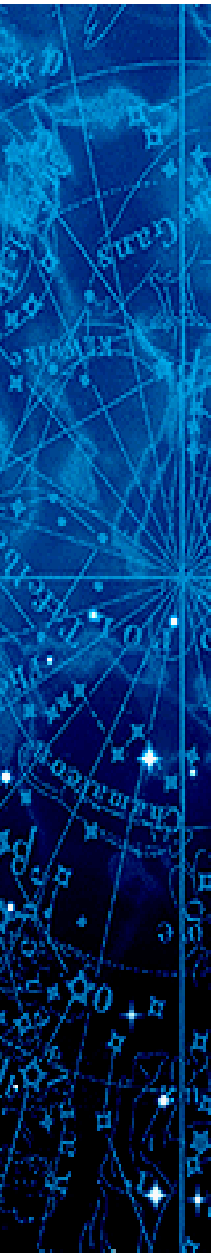


Usługi katalogowe i protokół LDAP

Grzegorz Blinowski

"CC"

Grzegorz.Blinowski@cc.com.pl

http://www.cc.com.pl/

tel (22) 646-68-73; faks (22) 606-370-80

Co to są usługi katalogowe?

- Spis - książka telefoniczna, typu "Białe" lub "Żółte stronice"
- …. i więcej niż książka telefoniczna
- Odzwierciedla strukturę organizacyjną firmy
- Przykłady tradycyjnego systemu katalogowego:
  - Ksiażka adresowa programu pocztowego
  - DNS (translacja nazw na adresy IP)

Potrzeba zapewnienia usług katalogowych

- Intranet
  - Książki adresów e-mail, telefonów, itd.
  - inne atrybuty osób dla aplikacji typu: pracy grupowej, zarządzania procesami, itd.
  - informacja dla PBN i QoS
- Ekstranet
  - autoryzacja i profile partnerów
- Internet
  - handel wirtualny (bezpieczeństwo)

Potrzeba zapewnienia usług katalogowych

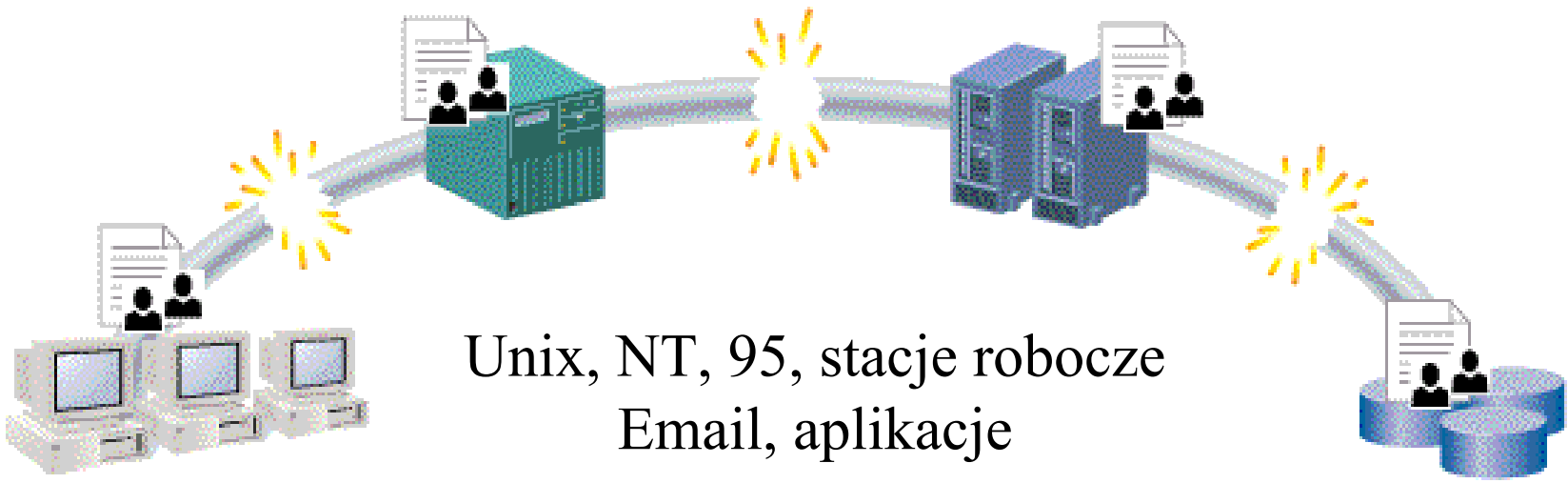
- Dramatyczne zwiększenie rozmiaru sieci:
  - W odseparowanej niewielkiej sieci LAN wystarczą b. proste usługi katalogowe
  - W większych sieciach lokalizacja osób i obiektów zaczyna być problemem
- Rozwój potrzeb:
  - w przeszłości niezbędne było wyłącznie tłumaczenie adresów fizycznych lub sieciowych komputerów na czytelne nazwy oraz książka adresów e-mail
  - obecnie wymagany jest dostęp do wielu atrybutów opisujących obiekty i osoby

Skala usług katalogowych

Katalog	#Rekordów	#Odczytów/dzień	#zapisów/dzień
Osobisty	100-1000	10-100	1-10
Wydziałowy	1000-10000	100-1000	10-100
Korporacyjny	10000-100000	100000-1000000	100-1000
Globalny	10M-100M	100M - 1 Mld	10000 - 100000

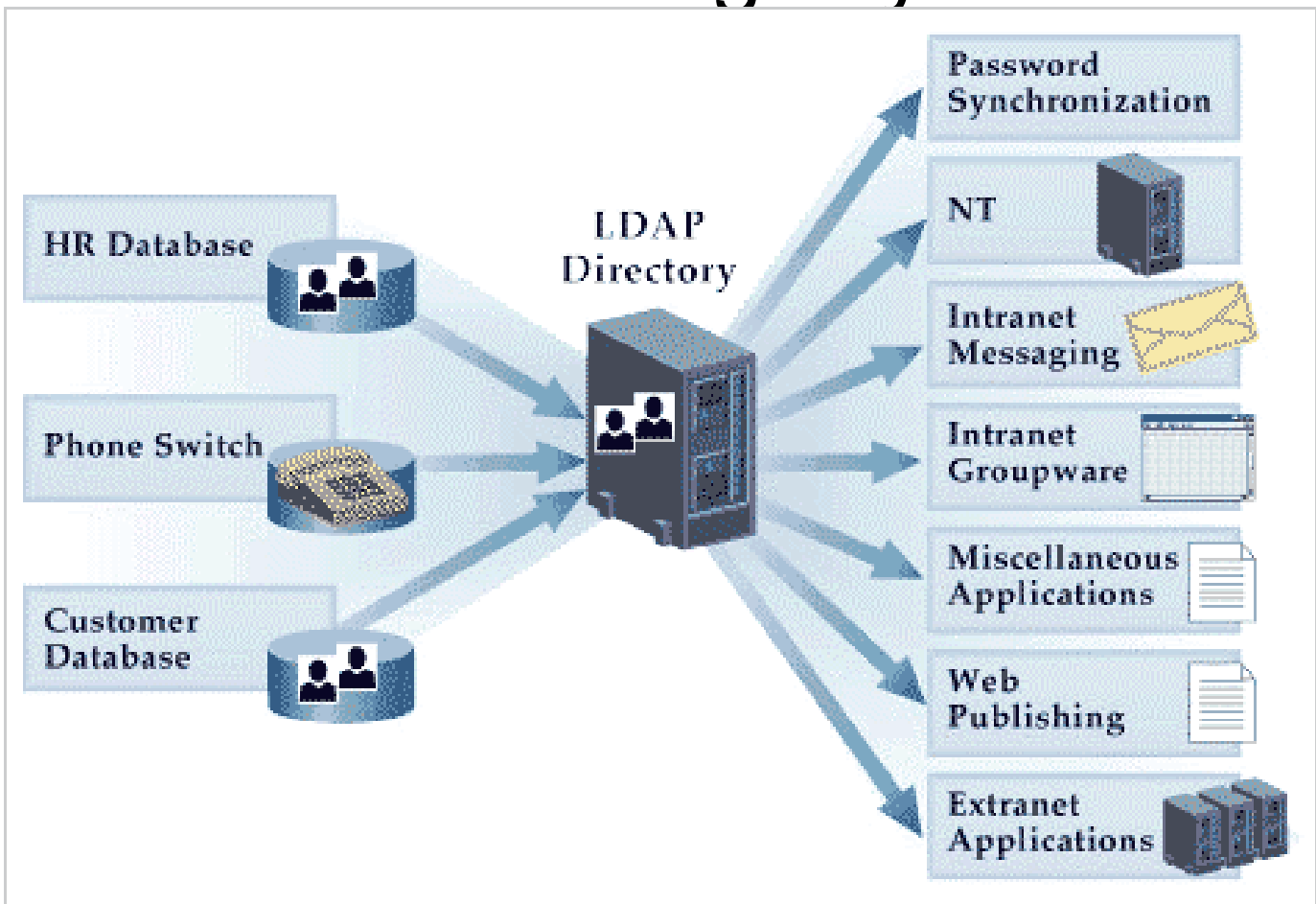
System informatyczny bez zcentralizowanego serwisu katalogowego

- **Każda aplikacja (dział) posiada własny system katalogowy**



- **Rozwój aplikcji i systemów wymaga rozwiazania zintegrowanego**

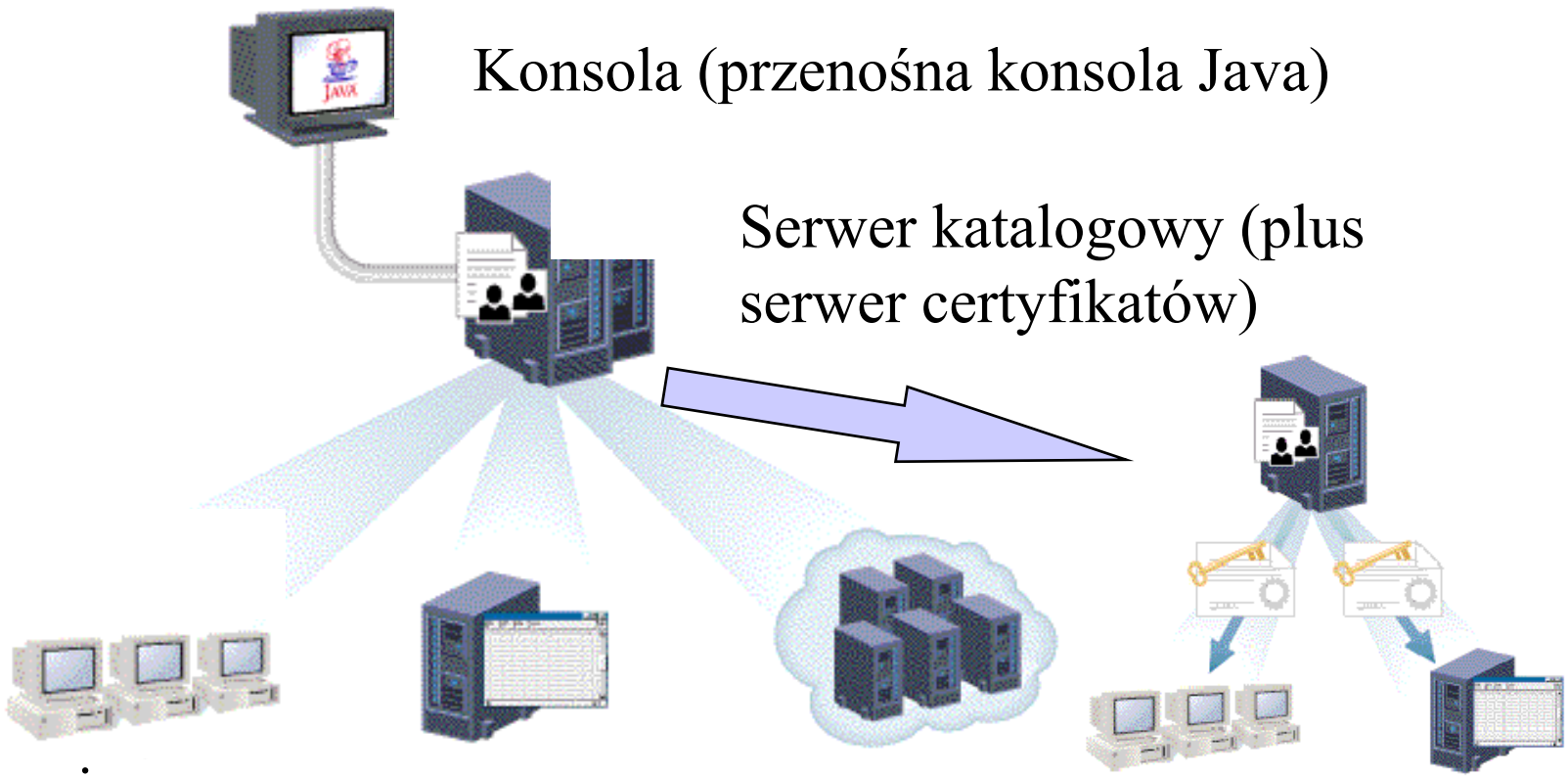
System informatyczny ze zcentralizowanym serwisem katalogowym



"Klienci" usług katalogowych

- **Użytkownicy**: poszukiwanie adresów e-mail, numeru telefonu, itd.
- **Administrator**: jedna "konsola" serwera katalogowego zastępuje wiele "konsol" systemowych
- **Aplikacje**: autoryzacja na podstawie dodatkowych atrybutów
- **Sieci**: realizacja PBN (Policy-based networks) wymaga znajomości profilu osoby

Zcentralizowany system katalogowy



Usługi katalogowe z historycznego punktu widzenia

- Lokalizacja komputerów
- Określanie adresów e-mail i telefonów
- Aplikacje: serwery WWW, serwery e-mail, serwery aplikacji
- Sprzęt sieciowy (rutery, adaptery sieciowe, modemy)

- 1980

1990

1996

1999 -

OSI X.500

- Katalog poziomu aplikacyjnego
- Wymaga protokołów OSI
- Służy do mapowania użytkowników na adresy e-mail systemu X.400
- Zorientowany obiektowo i hierarchiczny
- X.500 definiuje: przeszukiwanie, replikacje i zarządzanie katalogami
- Wady: b. skomplikowany, wymaga stosu OSI, rozbieżne implementacje

Cztery typy serwisów katalogowych

- Zamknięte
- Oparte na standardach (X.500, LDAP)
- Hybrydowe
- Usługi meta-katologowe (meta-directory)

Systemy zamknięte

- Własny standard: katalogu i protokołu komunikacji z klientem
- Zalety: zwykle dość wydajne, choć nie zawsze skalowalne
- Wady: nie umożliwiają rozbudowy i integracji z innymi serwisami
- Obecnie praktycznie w zaniku

Oparte na standardach

- Całkowicie zgodne z uznanymi standardami (X.500 lub LDAP)
- Zalety: b. dobra integracja z innym oprogramowaniem, dobra skalowalność i wydajność (LDAP)
- Wady: konieczność utrzymania zgodności ze standardem może blokować rozwój cech, których domagają się użytkownicy
- Dynamiczny rozwój (LDAP)

Hybrydowe

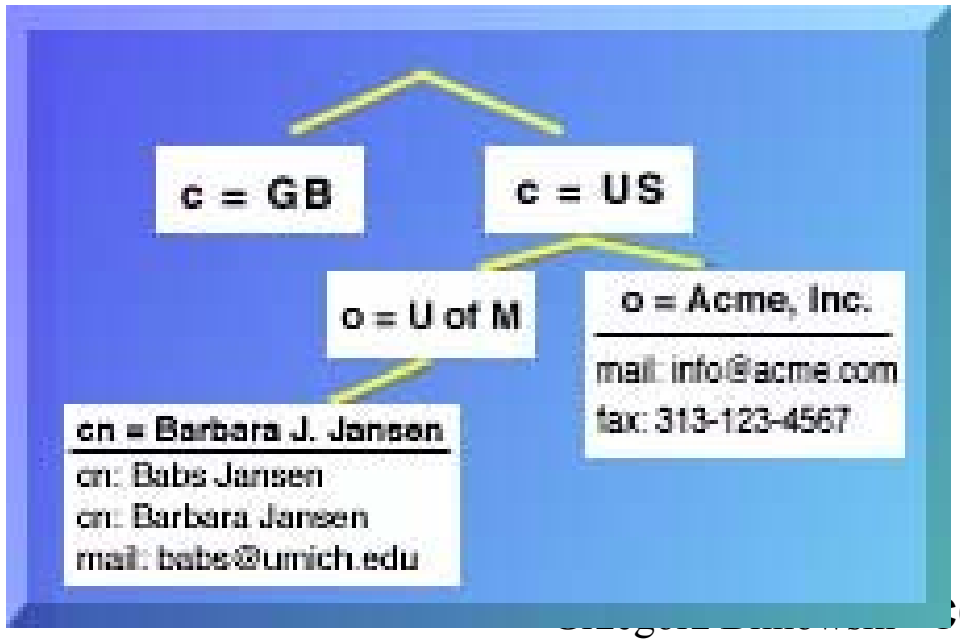
- Łączą zamknięte "jądro" z interfejsem zgodnym ze standardem X.500 i/lub LDAP
- Zalety: dobra integracja z systemem operacyjnym serwera, dość dobra wydajność
- Wady: trudna adminstracja (podwojenie czynności: katalog "generyczny" i bramka do usług zgodnych ze standardem); przekłamania w bramce X.500/LDAP; ograniczona skalowalność
- Microsoft Exchange, Lotus Notes 5.0, NDS

Meta-directory

- System zgodny z LDAP lub X.500 replikujący usługi dedykowane
- Zalety: praktycznie jedyne rozwiązanie dla dużych i rozwiniętych systemów, b. dobra skalowalność i wydajność.
- Wady: trudna administracja

Cechy LDAP

- Standard: RFC-1777, RFC-1778, RFC 1823, RFC 2251-2256
- Serwis TCP/IP, port: 389
- Rekordy (entries) identyfikowane przez DN (*distinguished name*)
- Rekordy posiadają wiele atrybutów, np. mail (adres e-mail)
- Struktura rekordów jest hierarchiczna



Obiekty katalogu LDAP

- Przykład DN:
  cn=Grzegorz Blinowski, o=CC,c=PL
- Atrybuty obiektów mogą być tekstowe lub binarne (kodowane tekstowo) - np. w formacie JPEG
- Typ obiektu określa atrybut ***objectclass***
  np. ***objectclass=acl***
- Uwaga: DN obiektu nie musi być znany (serwer kat. może obiekt odnaleźć)

Protokół

- Oryginalnie LDAP pełnił wyłącznie rolę protokołu "bramkowania" TCP/IP do OSI/X.500: LDAP - Lightweight DAP (DAP - Directory Access Protocol X.500)
- LDAP zastępuje skomplikowane protokoły OSI przez TCP/IP
- "Referal" - serwer w przypadku odwołania, którego nie może obsłużyć odsyła do innego serwera LDAP
- Bezpieczeństwo - poprzez protokół SSL
- Replikacja

Operacje

- Operacja na katalogu zaczyna się od połączenia (binding) poprzez podanie nazwy domeny bazowej, np. o=CC, c=PL
- Dostępne są operacje: odczytu, wyszukania, zapisu, porównania oraz usuwania obiektów
- Szukanie - do serwera można przekazać filtr określający kryteria szukania (RFC-1558) - operacja przeszukania odbywa się w całości na serwerze

Kontrola dostępu i bezpieczeństwo

- Katalog może przechowywać atrybuty związane z bezpieczeństwem, np. atrybuty certyfikatu X.509v3
- LDAP może być przenoszony przez SSL
- Katalog może przechowywać listy kontroli dostępu (ACL)

Implementacja

- Serwer:
  - darmowe implementacje dla Unix-a (slpad, ldapd) z uniwerstytetu w Michigan
  - Komercyjne: Netscape, Sun
- Klient - dostępne w przeglądarce Netscape Navigator, darmowy klient w źródłach (często w postaci bramki WWW)

Firmy tworzące systemy zgodne z "czystym" LDAP

Polityka Firm

- Netscape - własny zgodny ze standardami serwer (Directory Server) zintegrowany z innymi serwerami
- Sun - j.w. - produkt młodszy niż w przypadku Netscape, słabsza integracja z serwerami
- Novell - bramka LDAP do NDS, niejasne plany przeniesienia serwera LDAP Netscape
- Microsoft - bramka LDAP do Active Directory

Największe wdrożenia LDAP

Home Depot

- Aplikacje intranetowe i extranetowe obejmujące 600 sklepów
- Skalowalność i niezawodność

VeriSign

- Ponad 3 miliony certyfikatów dostępnych w sieci Internet

Ford

- Rozwiązanie "single logon" dla 250,000 użytkowników i ponad 20 aplikacji

X.500 a LDAP

- Podobieństwa: hierarchiczność, obiektowość, zaawansowane wyszukiwanie, atrybuty
- Różnice: protokoły podstawowe (OSI, TCP/IP), przeznaczenie (obsługa X.400, uniwersalny), stopień skomplikowania, format danych (strukturalny, tekstowy)
- LDAP opiera się na najlepszych cechach X.500 jest jednak pozbawiony jego bagażu

Efektywność kosztowa LDAP

- LDAP jest tani w implementacji - protokół bazowy - TCP/IP jest dostępny powszechnie
- Dostępnych jest szereg API dla LDAP
- LDAP jest (stosunkowo) prosty w implementacji oraz przejrzysty dla programisty i administratora
- LDAP jest standardem

Perspektywy rozwoju

- Bezpieczeństwo:
  - serwer-serwer
  - ochrona danych
- Sortowanie i pozyskiwanie danych od serwera w porcjach
- "Server discovery"
- standardyzacja API

Wskazówki dla kupujących

- Ewaluacja, pilot, wdrożenie - opracować koncepcję hierarchii
- Lepsze rozwiązania "z półki" (w przeciwieństwie do bramek)
- Wydajność i skalowalność
- Zgodność ze standardami