Toruń, 26 kwietnia 1994

X.500 Directory

M. Górecka
T. M. Wolniewicz
J. Żenkiewicz

UMK Toruń

1 Wstęp

Dynamiczny rozwój sieci komputerowych umożliwia kontakt pomiędzy rozproszonymi użytkownikami oraz wzajemny dostęp do zasobów i wymianę informacji o zasięgu zarówno lokalnym jak i globalnym.

Jednym z najbardziej rozpowszechnionych zastosowań sieci komputerowych są m.in. usługi poczty elektronicznej i dostępu do zasobów informacyjnych. Różnorodność i mnogość sieci komputerowych oraz protokołów sieciowych spowodowała konieczność unifikacji poczty elektronicznej i usług w sieciach komputerowych. Przykładem tego podejścia jest rozwój, w ramach standardów OSI, protokołów poczty elektronicznej X.400 i usług informacyjnych X.500 Directory.

Niniejszy referat zawiera podstawowe informacje o usługach X.500 (X.500 Directory Services) oraz przedstawia koncepcję rozwoju pilotowej sieci X.500 Directory dla środowiska naukowo-akademickiego w Polsce w oparciu o Naukową i Akademicką Sieć Komputerową NASK.

2 Ogólne informacje o X.500 Directory

2.1 Definicje

X.500 jest zbiorem norm CCITT z 1988 roku, uaktualnionych w 1992. Normy te definiują system rozproszonej bazy danych opartej na wielorakich protokołach łączności.

W założeniu X.500 miało służyć powstaniu globalnej informacji adresowej wykorzystywanej między innymi przy transporcie poczty elektronicznej (X.400).

Obecnie przez X.500 rozumie się zarówno sam zbiór norm, jak również działającą ogólnoświatową służbę, w ramach europejskiego projeku PARADISE i amerykańskiego White Pages .

2.2 ISODE

ISODE (ISO Development Environment) jest implementacją wybranych protokołów i aplikacji OSI, które pracują w szerokim zakresie środowiska systemów operacyjnych UNIX lub UNIX-o podobnych.

Pakiet ten jest w chwili obecnej absolutnie dominującym na rynku dostępnego oprogramowania implementujacego OSI Directory services. Spowodowane jest to przede wszystkim tym, że ta dojrzała implementacja była do tej pory dostępna bez ograniczeń. Z końcem roku 1992 zakończone zostały prace nad ogólnodostępnymi wersjami ISODE. Sytuacja ta najprawdopodobniej ułatwi wejście na rynek innym — komercyjnym implementacjom standardu; przez długi okres należy jednak spodziewać się dominacji ISODE zwłaszcza, że ośrodkom uniwersyteckim udostępniane ono będzie w formie niedopłatnych licencji.

Zasadnicze komponenty ISODE to:

- obsługa katalogów OSI Directory Service (QUIPU): DSA (Directory System Agent) oraz DUA (Directory User Agent),
- implementacja systemu dostępu i zarządzania transferem zbiorów (FTAM),
- implementacja protokołu zdalnego dostępu (VT — virtual terminal),
- implementacja protokołu SNMP w postaci serwera i prostego klienta,
- obsługa poczty MHS (Message Handling Services) : MTA (Message Transfer Agent) — oprogramowanie PP korzysta z bibliotek ISODE.

Cześć ISODE obejmująca X.500 Directory (QUIPU) jest kompletną implementacją zarówno serwera (DSA) jak i kilku interfejsów użytkownika (DUA). Dokładniejszy ich opis podajemy w cześci „Dostęp do zasobów".

Poza ISODE na szczególną uwagę zasługuje implementacja LDAP (Lightweight Directory Access Protocol) tworzona na Uniwersytecie w Michigan, która nadzwyczajnie upraszcza tworzenie interfejsów DUA.

2.3 Struktura X.500 Directory w ramach projektu PARADISE

X.500 Directory jest rodzajem „światowej książki telefonicznej". Zawiera szeroki wachlarz informacji o organizacjach, jednostkach i osobach, łącznie z możliwością zapisu fotograficznego i dźwiękowego. Zasada działania X.500 Directory jest podobna do internetowych Name-Serwerów. Ustanowiona jest sieć serwerów, komunikujących się między sobą za pomocą specjalnego protokołu X.500 (DSP — Directory Service Protocol). Zaimplementowana jest metoda replikacji i buforowania danych przez serwery.

Projekt pilotowy X.500 Directory jest inicjatywą rozwijająca się głównie w środowisku akademickim znaną w Europie jako PARADISE Project. Analogiczna inicjatywa w USA znana jest jako PSI White Pages Project. Zadaniem PARADISE było ustanowienie pilotowej instalacji X.500 i wykorzystanie jej do testowania protokołu i jego różnych implementacji.

Każdy kraj biorący udział w projekcie ma serwer na szczeblu kraju, zarejestrowany w serwerze poziomu „root". Administrator serwera poziomu krajowego jest odpowiedzialny za koordynację łączności (komunikacji) z serwerami niższego poziomu, które obsługują organizacje. Organizacje mogą być podzielone na mniejsze jednostki obsługiwane przez serwery niższych szczebli. Analogicznie jak administratora poziomu krajowego, ustanawia się administratorów serwerów niższych poziomów z podobną odpowiedzialnością.

Inicjatywa projektu PARADISE sponsorowana przez RARE powstała w 1990 roku w ramach programu COSINE. Eksperymentalna wersja projektu pilotowego PARADISE została zakończona. Kontynuacja będzie w przyszłości koordynowana w oparciu o składki od uczestniczących w projekcie krajów pokrywające koszty służb centralnych.

Rozwój fazy pilotowej X.500 Directory w poszczególnych krajach jest bardzo zróżnicowany. Część krajów ma szeroko zakrojone programy i udostępnia znaczne ilości danych, inne mają bardzo wyrywkowe dane, rzadko aktualizowane. W obecnej chwili w projekcie biorą udział wszystkie kraje europejskie z wyjątkiem krajów dawnej Jugosławii i niektórych krajów byłego Związku Radzieckiego. Najbardziej zaawansowane są W. Brytania, Holandia, Szwajcaria, Dania, Finlandia, Francja i Norwegia.

Pilotowy program PARADISE koordynowany był do tej pory przez University College London. Usługi X.500 Directory zabezpiecza University of London Computer Centre (ULCC) przy wsparciu firmy NEXOR. Punktem podstawowym usług jest udostępnienie centralnego DSA (serwera) i DUA (interfejsu użytkownika).

Polska bierze udział projekcie PARADISE od lipca 1992. Od października 1992 patronat nad polskim projektem sprawuje NASK. W chwili obecnej pracuje sześć serwerów (centralny — na UMK Toruń oraz regionalne: Toruń, Warszawa, Kraków, Wrocław, Poznań). Regionalny serwer toruński prezentuje kompletne dane na temat Uniwersytetu Mikołaja Kopernika, pozostałe serwery są w fazie rozruchowej lub eksperymentalnej.

2.4 Dostęp do zasobów

Jak już zostało wspomniane X.500 jest rozproszoną bazą danych przechowującą zasoby w serwerach DSA. Konkretna implementacja samego serwera nie jest oczywiście zdefiniowana przez X.500. W przypadku QUIPU hierarchiczna struktura X.500 Directory jest odwzorowywana wprost na strukturze drzewa katalogów serwera. Dane przechowywane są w postaci tekstowej i w całości ładowane do pamięci w momencie startu serwera; nie ładuje się jedynie danych przechowywanych w postaci oddzielnych zbiorów (np. obraz czy dźwięk). Z uwagi na taki sposób rozwiązania serwera, duże bazy danych wymagają maszyn o rozbudowanej pamięci operacyjnej. Kolejne wersje ISODE mają mieć możliwość odwoływania się do danych bezpośrednio na dysku i w ten sposób umożliwiać obsługę dużych baz bez zajmowania wielkich obszarów pamięci operacyjnej.

Internetowe serwery w projekcie PARADISE nasłuchują z reguły na porcie 17003, ale jest to parametr zawarty w opisie każdego serwera i może być dowolnie modyfikowany. Serwer QUIPU jest w stanie obsługiwać wielokrotne połączenia nie rozczłonkowując się (bardzo istotne ze względu na duże rozmiary programu).

Struktura danych jest całkowicie modyfikowalna i zapisywana w tekstowych plikach

konfiguracyjnych. Oczywiście niezbędne jest zachowywanie umiaru w wykorzystywaniu tych możliwości konfiguracyjnych, tak aby nie doprowadzić do nieczytelności danych przez nieprzystosowane specjalnie interfejsy.

X.500 zawiera mechanizmy ochrony danych. Możliwe jest udostępnianie tylko części atrybutów wszystkim użytkownikom, a wszystkich jedynie wybranej grupie. Można żądać, aby każdy użytkownik musiał być zarejestrowany w bazie X.500, podobnie można wymagać, aby tożsamość była potwierdzana podaniem hasła. Istnieją mechanizmy pozwalające na przykład, na wyświetlanie zasobów bazy, ale nie dopuszczające do jej przeszukiwania. Trzeba przy tym podkreślić, że ochrona danych jest obecnie mało stosowana, ale trwają prace nad jej rozszerzeniem, prowadzone w ramach projektu PASSWORD.

W skład ISODE wchodzi DSA oraz kilka DUA, miedzy innymi interfejs administratora (dish), prosty interfejs dla terminali tekstowych (de) i zaawansowany interfejs dla X-windows (pod).

W oparciu o biblioteki ISODE rozwijane są DUA nie będące częścią składową ISODE, ale znacznie wzbogacające możliwości kontaktu użytkownika z Directory. Wspomniany wcześniej LDAP jest systemem pośredniczącym pomiędzy klientem a serwerem. Jest to proces, który spełnia rolę klienta dla DSA oraz serwera dla specjalnie skonstruowanego DUA. Standardowy protokół dostępu do danych (DAP — Directory Access Protocol) jest bardzo rozbudowany i w wiekszości wypadków klient wykorzystuje zaledwie część możliwości. W tej sytuacji protokół implementujący tylko te najważniejsze cechy DAP umożliwia znaczne „odchudzenie" programów i uproszczenie ich tworzenia. W oparciu o LDAP powstaje większość nowych interfejsów. Zaimplementowane są między innymi interfejsy sprzęgające X.500 z pocztą elektroniczną, gopherem i WWW, jak również implementacje DUA na komputerach klasy PC czy Macintosh.

Wiele ośrodków posiada anonimowe konta udostępniające interfejsy `de` i `dish`. Przykładowo w Polsce konta takie są na komputerach: `jaguar.cc.uni.torun.pl` oraz `anna.mat.uni.torun.pl`. Podstawowe funkcje interfejsu `de` są tak proste w obsłudze, że nie wymagają żadnej instrukcji. Bardziej zaawansowane opisane są w dokumentacji autorstwa M. Kus *X.500 Directory — opis użytkowy programu DE.*

Dostęp do danych można uzyskać rownież za pomocą gophera (np. na `gopher.mat.uni.torun.pl`) czy WWW (`http://jaguar.cc.uni.torun.pl:8888/MC=PL`). Poczta na adres `X.500@mat.uni.torun.pl` uruchamia e-mailowy interfejs do zasobów UMK. List zawierający linię `help` spowoduje wysałnie prostej instrukcji obsługi.

3 Koncepcja X.500 Directory w sieci NASK

3.1 Stuktura danych w X.500 Directory

Zgodnie z założeniami X.500 Directory struktura danych jest zgodna z administracyjno-organizacyjnym podziałem. Dokładniej mówiąc dane należą z reguły do jednej z kategorii: *kraj* (`country`), *instytucja* (`organization`), *jednostka organizacyjna* lub *oddział* (`organizationalUnit`), *osoba* (`person`). Istnieje również kategoria obiektu `locality`,

jest ona jednak stosowana rzadko i tylko w przypadkach nie dających się wpasować do wspomnianych powyżej schematów, np. organizacje z natury międzynarodowe znajdują się bezpośrednio pod `locality=Europe`.

Nie ma ograniczeń co do ilości szczebli instytucji czy jednostek organizacyjnych; przesadne rozbudowanie drzewa doprowadza jednak do zaciemnienia obrazu i nie jest zalecane.

Dane przechowywane są w serwerach (DSA) i struktura danych musi być odzwierciedlona w strukturze serwerów. Optymalnym rozwiązaniem jest, gdy poszczególne instytucje posiadają własne serwery. Na obecnym stopniu rozwoju techniki sieci komputerowych unikać należy zbytniego rozczłonkowania sieci serwerów w ramach pojedynczych instytucji, tak aby nie doprowadzać do sytuacji, w której w celu odszukania pojedynczego hasła (osoby) na terenie danej instytucji konieczna jest konsultacja ze znaczną ilością serwerów niższego szczebla i w efekcie uruchamianie dużej ilości połączeń, startowanie ze stanu uśpienia kilku serwerów, co w rezultacie znacznie spowalnia dostęp do danych. Z drugiej jednak strony bardzo duże zbiory danych stanowią znaczne obciążenie dla poszczególnych komputerów, a budowa sieci w oparciu o niewielką tylko ilość serwerów zwiększa szanse chwilowej niedostępności dużych zbiorów danych.

3.2 Organizacja i utrzymanie zasobów

Przewidujemy, że faza pilotowa rozwijać się będzie pod patronatem NASK w ośrodkach akademickich kraju. Ze względu na ograniczenia organizacyjno-sprzętowe oraz stosunkowo niewielką ilość danych (w początkowej fazie projektu) można uznać za wystarczające, jeżeli uruchamiane serwery będą odgrywały rolę serwerów regionalnych, obsługując kilka uczelni zlokalizowanych w pobliżu. Do lokalnych administratorów należeć będzie decyzja, czy odpowiedzialność za dane poszczególnych instytucji przekażą reprezentantom tych instytucji.

Finansowanie projektu w 1994 r. opierać się będzie o grant grant KBN przeznaczony na ładowanie pilotowych baz danych, fundusze JBR NASK oraz wsparcie partycypujących uczelni w postaci udostępnienia sprzętu.

Wyniki prac będą udostępnione zainteresowanym użytkownikom poprzez sieć naukowo-akademicką NASK.

Jednym z podstawowych zadań, jakie stoją przed polskim projektem X.500 jest dostosowanie go do naszych lokalnych potrzeb (polskie znaki). Szczęśliwie, w X.500 znaki spoza standardowego zestawu ASCII reprezentowane są w standardzie T.61, który zawiera wszystkie polskie znaki diakrytyczne. Oprogramowanie ISODE dopuszcza jednak po stronie DUA jedynie znaki z tabeli ISO-Latin 1 i niezbędne jest zmodyfikowanie DUA, tak aby wyświetlane były również znaki Latin 2. Opracowania wymagają również standardy wprowadzania polskich danych, tak aby mogły one być wykorzystywane zarówno na obszarze Polski (w poprawnej pisowni) jak i z zagranicy (z wykorzystaniem niemodyfikowanych DUA). Wstępne prace we wspomnianym zakresie są już obecnie prowadzone.

Bardzo ważnym zagadnieniem jest rozwijanie samej bazy danych. Przewidywana jest w tym zakresie miedzy innymi współpraca z Ośrodkiem Przetwarzania Informacji (OPI). Konieczne będzie zaimplementowanie mechanizmów, które pozwalałyby powiązać X.500 z

istniejącymi kadrowymi bazami danych, przynajmniej w stopniu umożliwiającym weryfikację prawidłowości zasobów X.500.

4 Dokumentacja

Dokumentacja ISODE składa się z pięciu tomów i jest zorganizowana zgodnie z warstwowym modelem odniesienia OSI. Charakteryzuje od podstaw usługi oferowane przez poszczególne warstwy. Dwa pierwsze tomy dokumentacji opisują narzędzia programowe, implementujące podstawową obsługę kolejnych warstw sieciowych, tom trzeci opisuje aplikacje utworzone na bazie tych usług. Czwarty tom przedstawia narzędzia służące do budowania aplikacji na bazie języka programowania, abstrahującego od modelu sieciowego. Tom piąty to kompletny opis implementacji X.500 Directory.

Dokumentacja ISODE, liczne RFC związane z tematyką X.500, jak również całość oprogramowania (w postaci źródłowej) jest dostępna na serwerze NASK `ocelot.mat.uni.torun.pl`.

UMK uruchomił w imieniu NASK „helpdesk" na tematy związane z instalacją i eksploatacją oprogramowania X.500. Pomoc dostępna jest za pomocą poczty elektronicznej pod adresem `help-X.500@cc.uni.torun.pl`.

4.1 Standardy OSI

1. CCITT X.500 / ISO DIS 9594-1: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Overview of Conspects, Models and Services.

2. CCITT X.501 / ISO DIS 9594-2: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Models.

3. CCITT X.509 / ISO DIS 9594-8: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Authentication Framework.

4. CCITT X.511 / ISO DIS 9594-3: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Abstract Service Definition.

5. CCITT X.518 / ISO DIS 9594-4: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Procedures for Distributed Operations.

6. CCITT X.519 / ISO DIS 9594-5: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Protocol Specifications.

7. CCITT X.520 / ISO DIS 9594-6: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Selected Attribute Types.

8. CCITT X.521 / ISO DIS 9594-7: [ISO: Information Processing Systems] Open Systems Interconnection - The Directory - Selected Object Classes.

9. CCITT X.200 / ISO DIS 7498: [ISO: Information Processing Systems] Open Systems Interconnection - Basic Reference Model.

10. CCITT X.208 / ISO DIS 8824: [ISO: Information Processing Systems] Open Systems Interconnection - Specifications of Abstract Syntax Notation One (ASN.1).

11. CCITT X.219 / ISO DIS 9072-1: [ISO: Information Processing Systems - Text Communication] Remote Operations [ISO: PART 1]: - Model, Notation and Service Definition.

12. CCITT X.229 / ISO DIS 9072-2: [ISO: Information Processing Systems - Text Communication] Remote Operations [ISO: PART 2]: - Protocol Specification.

4.2 Literatura uzupełniająca

1. Kille S.E.: *An Introduction to the ISODE Consortium*, University College London, March 12, 1992.

2. Kille S.E.: *The ISODE Consortium*, University College London, May 10, 1992.

3. Kirstein P.T.: *CCITT Recommendations of the X.500 Series, The Directory*, University College London, April 1992.

4. *PARADISE, International Report*, No.2, November 1991.

5. *PARADISE, International Report*, No.3, May 1991.

6. Robbins C.J., Kille S.E.: *The ISO Development Environment: Users Manual, Volume 5: QUIPU*, version 7, X-Tel Services Ltd., University College London, July 1, 1992.

7. Robbins C.J., Onions J.P.: *The ISO Development Environment: Users Manual*, Update Release, version 8, X-Tel Services Ltd., University College London, June 17, 1992.

8. Schnabel F.: *X.500 Directory and Information Services*, University of Technology, Graz, July 15, 1991.

9. M. Rose: RFC 1085 *ISO Presentation Services on top of TCP/IP based internets*, December 1988.

10. M. Rose *The Little Black Book*, Prentice Hall, 1992

11. Górecka M., Wolniewicz T., Żenkiewicz J.: *Projekt wstępny rozwoju X.500 w Polsce*, Toruń, listopad 1992.

12. M. Kus: *X.500 Directory — opis użytkowy programu DE.*