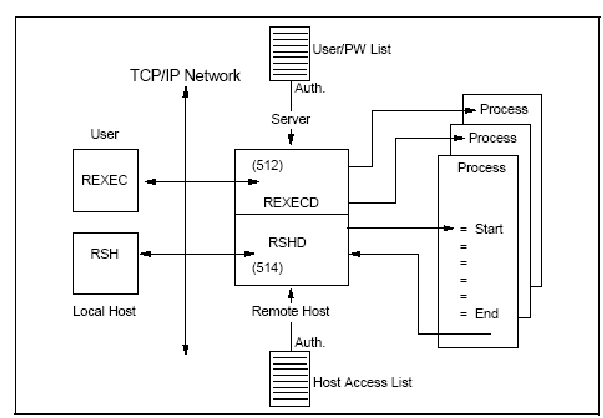
13.2.Giao thức dòng lệnh điều khiển truy cập từ xa (REXEC và RSH).

REXECD là một server mà cho phép thực thi các công việc đăng nhập từ một Host ở xa thông qua giao thức TCP/IP.Client thường sử dụng các câu lệnh REXEC hay RSH để truy nhập vào hệ thống.Bất cứ một kết quả truy nhập nào hay lỗi trong quá trình truy nhập cũng được gửi trở lại cho máy khác hoặc thực hiện cho tới khi thành công.

Nguyên tắc hoạt động:

REXECD là một server.Nó tiếp quản lý các câu lệnh được cung cấp cho Host bên ngoài và chuyển các câu lệnh cho các máy ảo thứ cấp của nó để thực thi.Server tự đông thực hiện đăng nhập cho người dùng và xác thực người dùng khi họ nhập vào ID và password.

Các câu lênh REXEC thường định nghĩa một ID,password,địa chỉ Host và yêu cầu xử lý để bắt đầu truy cập từ xa vào hệ thống.Tuy nhiên RSH không cần ta gửi username,pass mà nó thay thế bằng file của host truy cập(Trong đó có chứa đầy đủ các thông tin ).Cả Server và Client kết nối với nhau thông qua giao thức TCP/IP.REXEC sử dụng TCP qua cổng 512 RSH sử dụng cổng 514.



H1.Nguyên lý hoạt động của REXEC,RSH và REXECD server.

13.3. Giới thiệu môt trường tính toán phân tán (DCE).

DCE là một kiến trúc ,là một tập các chuẩn service mở và giao diện API mà hỗ trợ cho người lập trình và các nhà phát triển dự án trong các ứng dụng phân tán trong môi trường đa nền tảng,đa người dùng.

DCE là kết quả làm việc của OSF(Open Group) là sự cộng tác của nhiều nhà cung cấp phần cứng,phần mềm,khách hàng,các chuyên viên cố vấn.OSF bắt đầu thực hiện vào năm 1988 với mục đích hỗ trợ nghiên cứu,phát triển ,phân phối các công nghệ neural và các chuẩn công nghiệp.DCE version 1 được công bố năm 1992.

Các dịch vụ chính của DCE bao gồm:

-Thông tin các đối tượng.

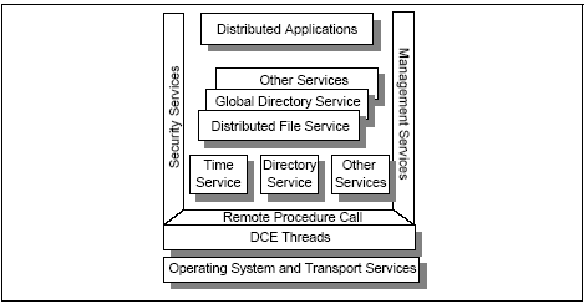
-Dịch vụ an ninh.

-Dịch vụ thời gian phân tán.

-Dịch vụ file phân tán.

-Các luồng.

-RPC(dịch vụ truy cập từ xa).



H2.Kiến trúc các bộ phân của DCE .

2.1.DCE directory service.

Khi làm việc trong một khu vực rộng lớn ,nhất là trong môi trường mạng phức hợp,một điều quan trọng là giữ thông tin về các vị trí ,tên ,và các dịch vụ (và nhiều chi tiết khác) của những người tham gia hệ thống cũng như các tài nguyên trên mạng.Điều này rất quan trọng để ta có thể truy cập thông tin một cách dễ dàng.Để thực hiện được điều này thông tin cần được lưu trữ trên một vị trí trung tâm logic và có thể truy cập thông tin qua các giao diện chuẩn.DCE Cell Directory Service cho phép thực hiện việc này.

DCE Directory bao gồm các bộ phận sau:

-Cell Directory Service (CDS)

-Global Directory Service (GDS)

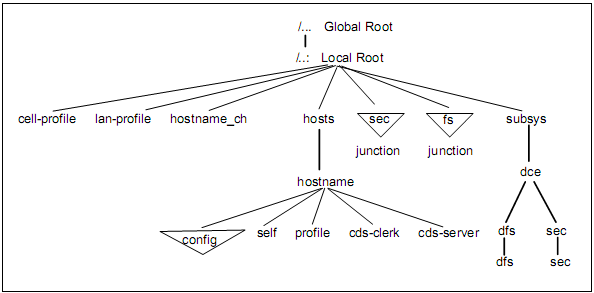
-Global Directory Agent (GDA)

-Application program interface (API)

Cell Directory Service:Quản lý cơ sở dữ liệu lưu trữ các thông tin về tài nguyên trong một nhóm các Host làm việc cùng nhau mà được gọi là các cell.Một DCE cell có tính co giãn và có thể bao gồm hàng trăm thực thể.Tiêu biểu là các tập đoàn có nhiều tổ chức trong một cell.Các cơ sở dữ liệu bao gồm cây phân cấp các tên tượng trưng cho các máy logic ,các ứng dụng ,các ứng dụng,người sử dụng và các tài nguyên trong cell.Các tên này thường nằm trong các thư mục bộ phận.Cây phân cấp tên này cũng thường gọi là không gian têm.Tất cả các Cell chứa ít nhất một Directory Service.

CDS gồm hai đặc tính quan trọng là:nó có thể được phân tán cũng có thể được nhân bản.Phân tán có nghĩa là các thực thể dữ liêu không được cư trú trên một máy nào trong một cell.Các dữ liệu có thể chia thành nhiều đoạn và cu trú trên nhiều máy riêng.

CDS chỉ có thể được sử dụng khi nó xác thực với DCE security service để ngăn chặn sự giả mạo.



H3.Cấu trúc phân cấp của không gian tên CDS

Không phải các DCE name đều được lưu trữ trên DCE directory service.Một số tài nguyên có thể được quản lý trên vài service ví dụ như Security service và được phân tán trên các file hệ thống kết nối với CDS qua một bộ phận đặc biệt gọi là Junction.Một junction bao gồm nhiều các thông tin ẩn giấu và một Client có thể kết nối tới nó thông qua directory Service

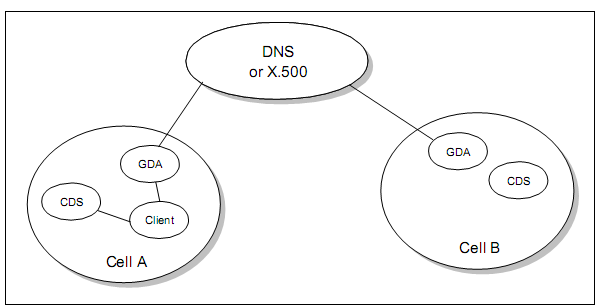
Global Directory Service and Agent.

CDS chỉ trả lời vị trí các tài nguyên trong cell mà nó quản lý.Tuy nhiên trong mạng có thể có rất nhiều cell.Vì thế người ta đưa ra Global Directory Namespace mà là cây phân cấp của các cell name. Global Directory Service (GDS) có khả năng phân giải cho chúng ta các tài nguyên mà nằm ngoài hệ thống.Ví dụ như trong trường hợp một công ty muốn kết nối với các hệ thống ngoài phạm vi của nó trên mạng internet.

Để tìm kiếm các cell khác cần có sự trao đổi thông tin giữa các cell.hiện nay có hai cách để thực hiện điều này:  
-CCITT X.500

-Internet Domain Name Services (DNS)

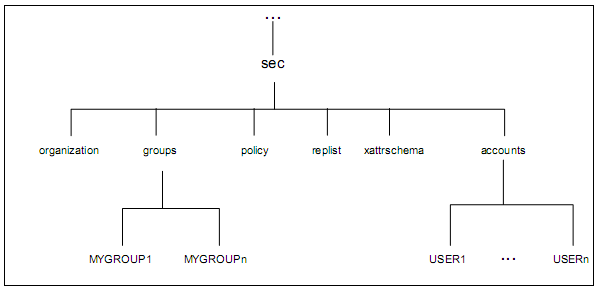
Để nhiều cell có thể giao tiếp với nhau một bộ phận khác cần được đưa ra Global Directory Agent.GDA là trung gian giữa local cell và GDS.Trong ví dụ trong hình dưới CDS không biết vị trí của tài nguyên nào đó bên ngoài nó yêu cầu client hỏi GDA.GDA kết nối tới không gian tên GDS và trả về kết quả.



H4.DCE GDA(Global Directory Agent).

DCE Security Service.

Vấn đề an ninh luôn là một vấn đề trở ngại trong môi trường mạng.Nói một cách rộng hơn đó là môi trường hệ phân tán,vấn đề chủ yếu là đảm bảo tất cả các bên tham gia trong hệ thống phải là những người dùng hợp lệ và có quyền truy cập đối với dữ liệu.Hai mối quan ngại chính là vấn đề xác thực và ủy quyền.Xác thực tức là nhận dạng người dùng và dịch vụ khi anh ta truy cập vào hệ thống.Còn ủy quyền tức là sau khi anh ta đăng nhập vào hệ thống thì anh ta có thực hiện đúng các quyền được cấp hay không

DCE Security đảm bảo rằng môi trường truyền thông cũng như quá trình truy cập dữ liệu trên mạng là an toàn.DCE Security cũng có một Database mà lưu trữ các thông tin về người sử dụng hệ thống như Account,nhóm,tổ chức,chính sách…Database nay được gọi là Registry được lưu trữ trên các server riêng.Registry thường được biểu diễn dưới dạng cây như sau: 

H5.Registry Directory Structure

DCE security thường bao gồm các bộ phận sau:

Authentication service:điều khiển quá trình xác thực(nhận dạng chính xác người sử dụng).Nó cũng bao gồm ticket granting service mà cho phép truyền thông an toàn.

Privilege Service cung cấp các quyền cho người sử dụng và gửi các thông tin đó lên DCE server .

Registry service lưu trữ các thông tin của người sử dụng gồm account,group…

Access control list facility cung cấp các cơ chế để phối hợp các truy nhập tài nguyên

Login facility cung cấp môi trường cho người sử dụng login và khởi tạo môi trường làm việc an toàn.

2.2.Authentication service.

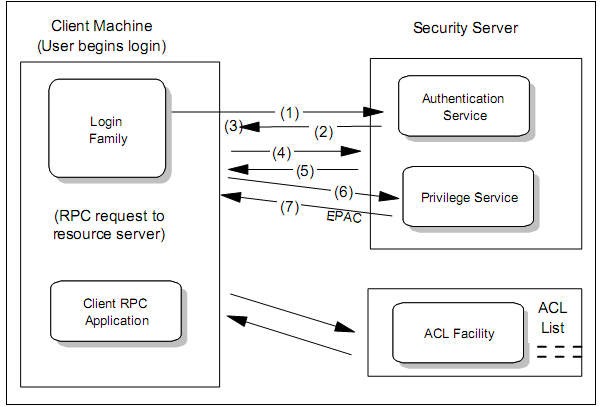
Nhiệm vụ chủ yếu của AS là cho phép nhận dạng các bên tham gia trong mạng DCE.Bao gồm cả người sử dụng,các xác thực dịch vụ trong trong môt trường DCE,không giống như trong hầu hết các mô hìn client/server nơi mà chỉ người dùng được xác thực.Có hai giai đoạn xác thực.Trong giai đoạn khởi tạo Kerberos third-party protocol được sử dụng để xác nhận yêu cầu của Client .Tiếp theo ta trả lại kết quả gồm giấy ủy quyền phiên làm việc với DCE Server khi mà người sử dụng muốn truy cập vào tài nguyên.

Trong DCE Version 1.1 một ý tưởng được đưa ra là ngoài sử dụng giao thức xác thực Kerberos.Còn có quá trình xác thực lại nhằm đảm bảo an toàn cho dịch vụ khi mà kẻ tấn công cố tình đoán ID của người dùng để tấn công hệ thống.Trong DCE 1.1 có 3 giao thức dùng để xác thực lại gồm:

No preauthentication dùng cho các phiên bản trước 1.1

Timestamps được sử dụng trong DCE Client 1.1 mà không dùng giao thức xác thực ba bên.Một nhãn thời gian được mã hóa và gừi cho Server bảo mật.Nhãn thời gian được giải mã nếu trong thời gian 5 phút thì ngươi sử dụng được xác thực lại

Third-party nó tương tự như nhãn thời gian nhưng thêm các thông tin Client được mã hóa với một khóa khác.



H5.Quá trình xác thực theo Third-party.

3.3.DCE threads.

Trong các ứng dụng truyền thống (được viết bằng các ngôn ngữ như C,cobol …) có rất nhiều đoạn chương trình được thực hiện một cách tuần tự.Tại một thời điểm chỉ có một điểm được thực hiện.Đây có thể coi như một Single Thread.Một luồng là một dòng thực thi của một đơn vị trong một tiến trình.Để tăng hiệu năng cho ứng dụng ta có thể thực hiện nhiều vùng trong cùng một thời gian điều này được coi như là đa luồng trong ứng dụng.Khả năng thực hiện đa luồng phụ thuộc vào hệ điều hành.

Trong môi trường tính toán phân tán dựa trên mô hình Client/Server nhiều luồng được cung cấp thêm khả năng thực hiện nhiều thủ tục trong một thời điểm.Công việc được tiến hành một cách liên tục tại luồng hiện tại trong khi một luồng khác bị block.Một server có thể cung cấp nhiều thủ tục có thể thực hiện đồng thời gọi là các tiến trình.Khi một luồng đợi để kết thúc quá trình vào ra một tiến trình khác có thể thực hiện.

Để chức năng này có thể thực hiện tốt hơn,luồng phải được tích họp trong hệ điều hành,nếu một luồng được thực hiện trong ứng dụng ở mức cao thì hiệu năng của nó sẽ thấp hơn khi được tiến hành trong hên điều hành.

*DCE Remote Procedure Call*

DCE Remote Procedure Call là một nền tảng của quá trình truyền thông Client/Server trên môi trường DCE

RPC cung cấp khả năng cho các ứng dụng phân tán có thể truy cập vào nhiều hệ thống tại bất cứ nơi nào trên mạng.

Một ứng dụng viết bằng DCE RPC được cấp cho một Client mà có thể đưa ra các RPC request và một Server mà nhận RPC request,xử lý chúng sau đó gửi lại kết quả cho Client.RPC có 3 thành phần chính:

-Interface Definition Language (IDL) và trình biên dịch của nó.Từ file được chỉ ra nó sinh ra các header file,Client stub,và Server Stub.Điều này cho phép một ứng dụng có thể cung cấp các RPC giống như nó cung cấp các thủ tục trên máy local.

-Thành phần trình bày dữ liệu trên mạng,mà định nghĩa các định dạng dữ liệu như các tham số đầu vào và đầu ra.Điều này đảm bảo chắc chắn rằng các bit có thể được sắp xếp và có Platform mà máy nhận có thể chuyển sang định dạng của nó.Quá trình sử lý định dạng dữ liệu cho RPC được gọi là marshalling .

-Runtime library che dấu đi các chi tiết của ứng dụng khi chúng được truyền thông từ Client đến Server.

Người lập trình ứng dụng có thể sử dụng đa luồng khi thực hiện RPC.

RPC có thể được sử dụng để xây dựng các ứng dụng như sử dụng các tiện ích DCE khác như CDS hay security service.CDS có thể được sử dụng để tìm kiếm hoặc quảng bá các địa chỉ của service cho client truy nhập.Trong khi security service được sử dụng để xác thực RPC và mà hóa dữ liêh trên đường truyền hay thực hiện ủy quyền.

2.4 Distributed Time Service.

Đồng bộ thời gian trên các host khác nhau là rất khó khăn vì có sự sai khác giữa các đồng hồ vật lý.Vấn đề hiện nay trong các ứng phân tán là phụ thuộc vào thứ tự thời gian của các sự kiện trong suốt quá trình thực thi.Ví dụ khi một lập trình viên biên dịch code của anh ta trên máy trạm và gòi tới một vài file trên máy chủ nếu máy trạm và máy chủ không được đồng bộ với nhau có thể quá trình biên dịch sẽ bị ngừng mãi mãi vì thời gian giữa hai máy là khác nhau.Vấn đề này cacngf trở lên quan trọng khi trong hệ thống phân tán có hàng trăm máy tính khác nhau.

DCE Distributed Time Service (DTS) cung cấp một phần mềm chuẩn cho phép đồng bộ giữa các Host khác nhau trong môi trường hệ phân tán.Nó cũng cung cấp cách thức để giữ thời gian trên các host gần với thời gian tuyệt đối .

Distributed Time Service gồm các thành phần sau:

-Local time server

-Global time server

-Courier and backup courier time server

Local time server chịu trách nhiệm phản hồi các request về thời gian của các Time Clerk trong LAN.Nó giúp đồng bộ trên một LAN.Nếu Time Clerk không được phản hồi từ LTS nó sẽ kết nối với global time server thông qua CDS lookup.

Global time server (GTS) quảng bá chính nó trong các CDS namespace cho tất cả các hệ thống có thể biết nó một cách dễ dàng.Một đối tượng tham gia GTS cũng sử dụng GTS như trên local LAN nhưng rõ ràng khả năng cung cấp thông tin của GTS là cao hơn rất nhiều.

Courier roles :local hay global time server cũng có thể có courier role.Chúng có thể là các courier, backup couriers hay non-couriers. Courier hoạt động như local time server hay như các bên tham gia trong tiến trình đồng bộ thời gian.Tuy nhiên các courier không có đồng hồ thời gian cho chính nó.Nó request thời gian từ global time server về thời gian của các LAN khác ,hay của các bộ phận khác trong cell bởi vì thời gian trên các LAN là khác nhau nên nó phải remote vào các LAN segment và đồng bộ thời gian của chúng.

Backup courier role cung cấp các trợ giúp trong trường hợp Primary couter cho một LAN nào đó không hoạt động. Backup courier sẽ giàn xếp để chỉ định một courier mới cho LAN đó và đồng bộ với GTS.