Poseidon House
Castle Park
Cambridge CB3 0RD
United Kingdom

TELEPHONE: **Cambridge (01223) 515010**
INTERNATIONAL: **+44 1223 515010**
FAX: **+44 1223 359779**
E-MAIL: **apm@ansa.co.uk**

Training

ANSAwise - DCE Distributed Services

Chris Mayers

Abstract

Organizations wish to understand the capabilities and limitations of OSF DCE

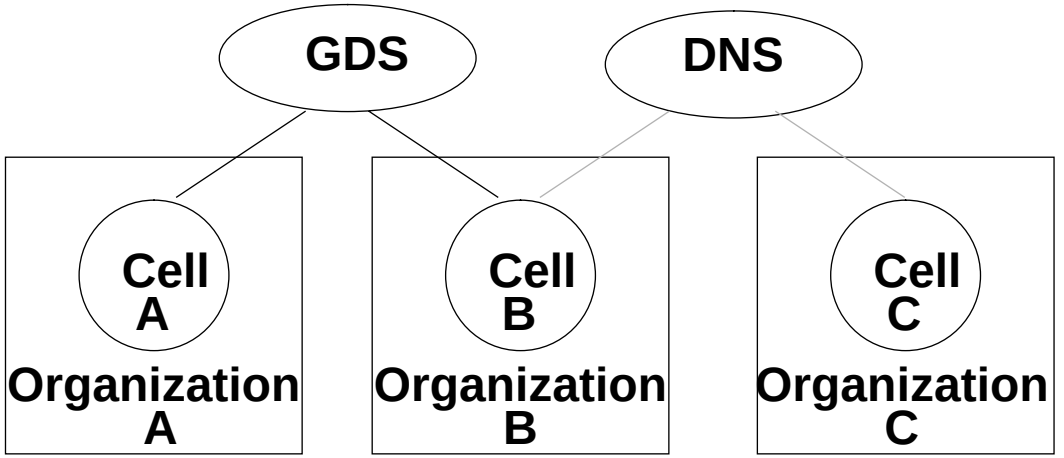
The DCE documentation (although well-written and comprehensive) is difficult to read in isolation, and sometimes does not distinguish current and future features.

This module of the ANSAwise training programme reviews the fundamental DCE services (as it happens, those in the DCE Secure Core), identifies their limitations, and shows how they will evolve in future versions of DCE.

APM.1373.02 **Approved** 15th February 1996
Briefing Note

Distribution:
Supersedes:
Superseded by:

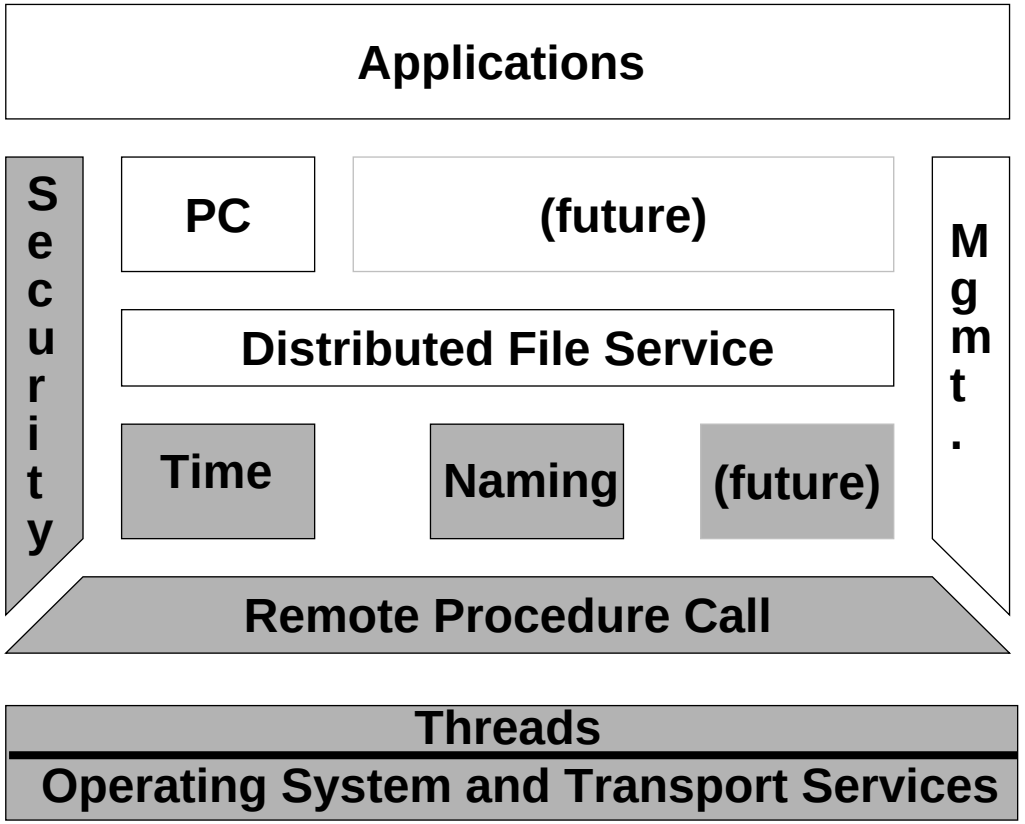
DCE Distributed Services



In this session

- ***Explain the DCE distributed services***
- ***Show how these services relate to each other***
- ***Show how these services will evolve in future***

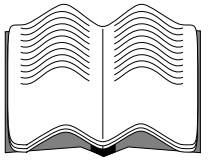
The DCE Component Architecture



DCE System Configurations

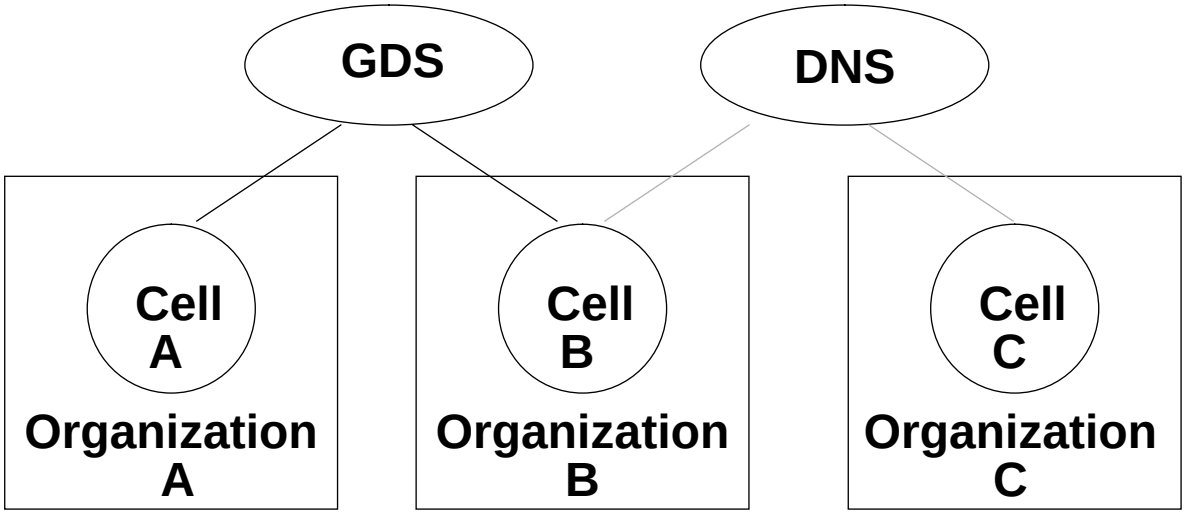
- *Organized into administrative domains called cells*
- *A machine can only be in one cell*
- *Resources are registered in cells*
- *Cells are intended to support up to thousands of machines - or more*

Directory Service



- *Consists of three components*
  - Cell Directory Service (CDS)
  - Global Directory Service (GDS)
  - Global Directory Agent (GDA)
- *The Directory Service is itself distributed and replicated*
- *Client-side caching is used to improve performance*

Cell Interconnection

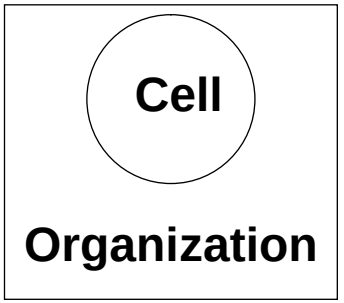


- ***Cells can be interconnected via X.500 GDS, Internet DNS, or both***

Global Directory Agent (GDA)

- *An intermediary between CDS and GDS/DNS*
  - handles CDS calls directed to other (foreign) cells...
  - ... selecting either a GDS or DNS server, depending on the format of the global name
- *GDA is not visible to the end-user*
  - and the only administration required is to start and stop the GDA server
- *One or more GDA servers per cell*

Cell Directory Service (CDS)



- ***Based on Digital's DNA Name Service***
- ***At least one CDS Server per cell***
- ***CDS Components:***
  - **CDS Server**
  - **CDS Clerk**
  - **CDS Administration Programs**

CDS Server

- ***Runs on a server machine***

- ***Accesses a local database storing the directory information***

  - **called a clearinghouse**

CDS Clerk

- ***Runs on the client machine***

- ***Maintains a local cache of directory information***

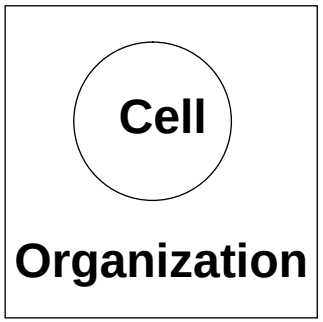
  - **cache is persistent; is saved to disk, and preserved across client machine crashes**

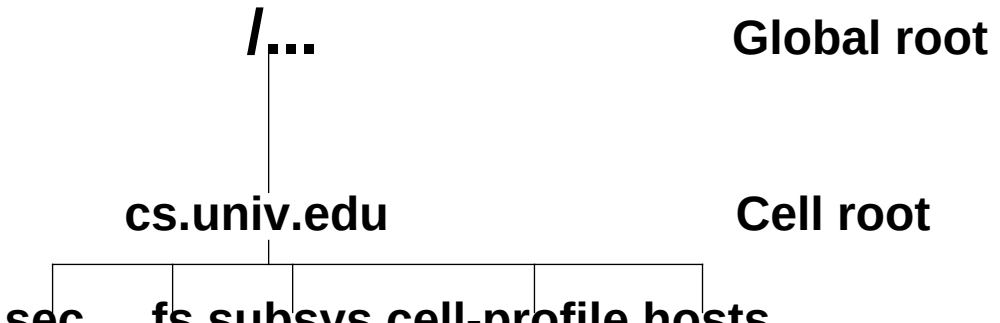
CDS Administration Programs

- ***cdscp - CDS system administration***
  - **must be used to create CDS directories**
- ***CDS Namespace Browser***
  - **a Motif GUI application**

The DCE Namespace

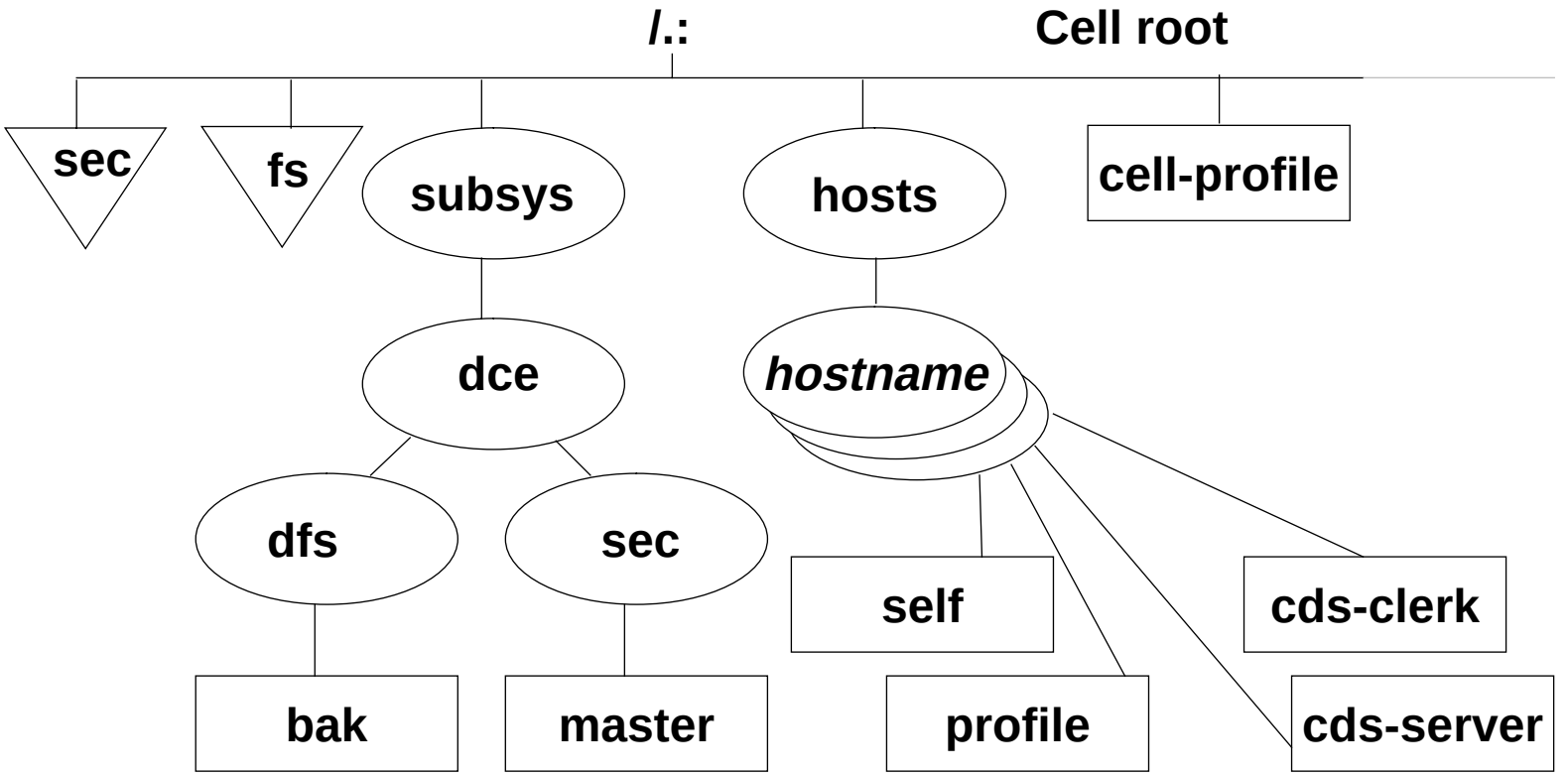
- *It's hierarchical*





- *Parts of the namespace are not handled by the DCE Directory Service*
  - the Security Service Database (sec)
  - the Fileset Location Service (fs)

The DCE Namespace after configuration



DCE Names

- *Global names have a '/...' prefix*
  - either using GDS

    `/.../C=US/O=SNI/TY=Muenchen/subsys/druecker/docs`
  - or using DNS

    `/.../dev.dce.osf.org/subsys/printers/docs`
- *Local names (within the current cell) have a '/.:' prefix*

  `/.:/subsys/druecker/docs`

  `/.:/subsys/printers/docs`

CDS Replication

- *CDS information consists of directory entries, directories, and clearinghouses*
- *A CDS directory is the logical unit of replication*
  - there can be one or more copies (replicas) of a directory
- *A clearinghouse is a physical database*
  - containing replicas stored on a particular CDS Server

CDS Consistency

- ***Consistency between replicas is maintained by***
  - **immediate propagation**
  - **skulking (bulk update)**
- ***Replica consistency is 'loose'***
  - **even 'immediate' propagation does not guarantee atomic update...**
  - **...CDS is not a general-purpose distributed database**
- ***Client application can bypass CDS cache (maintained by CDS Clerk) if necessary***

CDS Administration

- ***Inconsistent and bogus entries can persist in the name space***
  - **for example, stale bindings after application server crashes**
- ***Careful client error handling can tolerate these problems***
- ***System administrators will have to periodically remove these rogue entries***

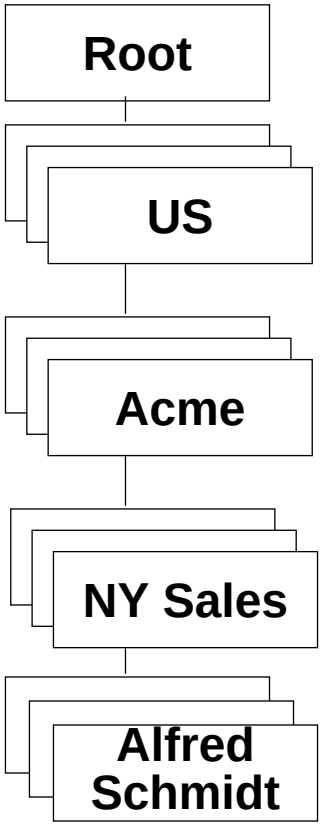
Global Directory Service (GDS)

- *Used when looking up names outside the current cell*
- *Based on X.500(1988)/ISO 9594*
  - uses the OSI protocol stack
  - defined in ASN.1
  - hierarchical and object-oriented
- *Internet DNS (Domain Name Service) can be used instead of GDS*
  - for interconnecting cells

GDS Structure

- *Directory Information Base (DIB)*
  - all the information in the GDS directory
- *Directory Information Tree (DIT)*
  - the structure of the GDS namespace; the hierarchy of GDS names
- *Directory Schema*
  - structuring rules for DIT and DIB...
  - ... a GDS interpretation that complies with the X.500 schema recommendations

Example with the Directory Information Tree (DIT)



Countries

Organizations

Organizational Units

Organizational Persons

/...

C=US

O=Acme

OU=NY Sales

CN=Alfred Schmidt

Global Name in GDS form

- *This person could be identified as*

  `/.../C=US/O=Acme/OU=NY Sales/CN=Alfred Schmidt`

- *The GDS directory is not limited just to naming people and organizations*
  - the DIT allows for naming application processes, for example
- *The DIrectory Schema determines the structure of DIT*
  - for example, Countries must be at the top of the tree...
  - ... Organizations must be below Countries,...
- *Aliases (alternative names) are supported*

GDS Components

- *Directory System Agent (DSA)*
  - server that manages the GDS database
- *Directory User Agent (DUA)*
  - library that implements the GDS client
- *Directory User Agent Cache*
  - client process shared by all users of the machine

More GDS Components

- ***C-Stub and S-Stub***
  - **equivalent to DCE RPC client and server stubs**
- ***Cache Update and Shadow Update Processes***
  - **for GDS client cache and GDS server replicas**
- ***GDS Administration Programs***
  - **gdssysadm: configuration, server activation, and backup**
  - **gdsditadm: remote administration**
  - **gdscacheadm: local DUA cache administration**

Other Differences between CDS and GDS

- *GDS has search capability; CDS does not*
- *Security is implemented differently*
- *Some punctuation characters are allowed in CDS, but not in GDS*

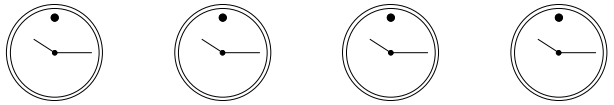
Directory Service APIs

- *Many applications won't need to use them*
  - server location lookup is done automatically by DCE RPC
- *Two sets of APIs*
  - X/Open Directory Service (XDS)
  - X/Open Object Management (XOM)
- *XDS interfaces to both CDS and GDS/DNS*
  - but be aware of differences between CDS and GDS/DNS names
- *The XDS interface has a few extensions beyond the X/Open APIs*
  - for security and cache management

Profiles

- *Profiles are (DCE) directory search paths*
- *Profiles allow clients to locate closer servers first*
- *Users can set up their own application search paths*
  - **best done by linking the user's profile to organization-specific default (group-wide or cell-wide)**

Distributed Time Service (DTS)



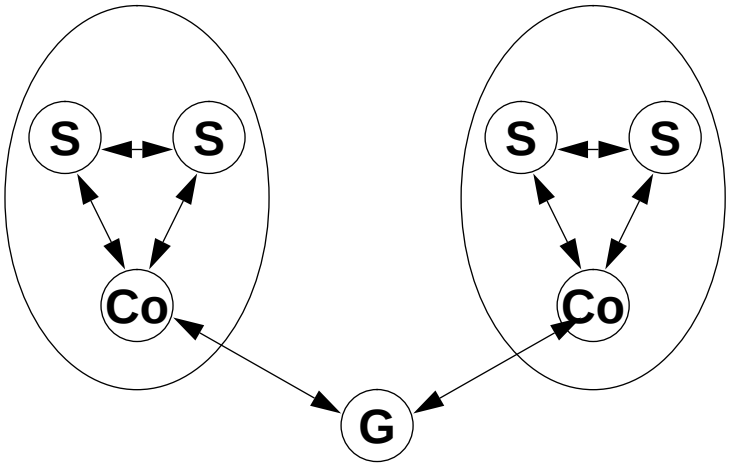
- *Keeps machine clocks approximately synchronized*
- *Can interwork with the Internet Network Time Protocol (NTP)*
  - NTP and DTS servers can provide time to each other
- *Programmers unlikely to interact directly with DTS*
  - but must be prepared to handle approximate time if they do...
  - ... with overlapping time intervals, neither is ‘earlier’ than the other

DTS Components

- *Time Clerk*
  - runs on client
  - periodically synchronizes with Time Server
- *Time Server*
  - typically 3 time servers per LAN in each DCE cell
  - synchronizes with the other time servers

Time Synchronization between LANs

- *Each LAN can have a Courier Time Server...*

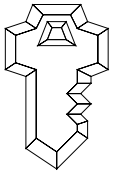


- *...synchronized with a Global Time Server*

Time Provider interface

- *Time Servers are responsible for synchronization*
- *The actual time source comes from an External Time Provider*
  - a hardware source
  - the system administrator

DCE Security Services



- ***Based on MIT Project Athena's Kerberos technology (Version 5)...***
- ***... and POSIX 1003.6 (Draft 12) Access Control Lists***
- ***The DCE security protocols are complex, but even the programmer need not see it***
  - **the security services are the interface**

DCE Security Components

- *Authentication Service*
  - allows a process to verify the identity of another process
- *Authorization (Privilege) Service*
  - allows a server to determine whether client access should be granted to a resource
- *Registry Service*
  - maintains the DCE security database
- *Access Control List Facility*
  - allows users to grant and revoke access to resources they own
- *Login Facility*
  - authenticates a user to the security service by means of a password

Using DCE Security

- *End-users use the Login Facility*
  - and probably the Access Control List Facility
- *Administrators use the Registry service*
  - for creating user accounts
  - for cross-cell authentication, between clients and servers in different cells
- *Administrators control security servers*
  - including controlling the replication of security data
- *Administrators control local machine access*

Distributed Security Is Mutual

- *Servers must protect themselves against clients*
- *Clients must protect themselves against servers*
- *Client applications do not need to use the security services directly*
  - typically, they just use Authenticated RPC
- *Server applications use Authenticated RPC too*
  - and also Access Control Lists to control client access to their objects

Authenticated RPC Options

- ***Authentication service***
  - **No authentication**
  - **Secret Key**
- ***Protection level***
  - **Beginning of RPC session only**
  - **Message/packet integrity**
  - **Encryption**
- ***Authorization service***
  - **Uncertified**
  - **Certified**

Authentication Responsibility

- ***Authentication is a shared responsibility...***

	Server Preference No Authentication	Server Preference Authentication
Client Preference No Authentication	Unauthenticated	Unauthenticated
Client Preference Authentication	*(Fails)*	Authenticated

- ***... but servers must beware!***

- ***Servers must check client preference, if they wish authentication***

Issues with DCE 1.0

- ***Administration is tiresome***
- ***Many vendors have non-integrated login***
  - **must log in to operating system and DCE separately**
- ***Security loopholes***
  - **trivial passwords allowed even under the strictest policy**
  - **no password expiry**
  - **unlimited login attempts**
  - **no auditing**
- ***Only 32 ACL permissions***

DCE Present and Future

- *DCE 1.1*
  - Improved administration
  - Security enhancements
  - Internationalization
- *DCE 1.2*
  - to be determined

Summary

- *DCE services are available to distributed clients*
  - the DCE services are themselves distributed
- *The big gaps remain in debugging, testing, and administration*
  - opportunities for third parties
- *For more on DCE*
  - on DCE generally, see *Introduction to DCE* (OSF)
  - for answers to Frequently Asked Questions, see via the World Wide Web http://www.osf.org:8001/
- *For X.500, see CCITT Blue Book Volume VIIII - Fascicle VIII.8: Recommendations X.500-X.521*