An Introduction to Directory Services

Unit 5 – Network Management
Overview

• The computer industry responded to the needs of users to share resources between machines over a network by creating peer-to-peer network.

• As networks grew larger, peer-to-peer networks started losing their appeal because of the difficulty of administration.

• Microsoft, along with other network development organisations, moved to a client-server networking model, in which they introduced their domain concept.
Eventually, as with peer-to-peer networks, companies started to outgrow their domains, and multi-domain environments needed a better way for computers to interact across domains. Consequently, Microsoft introduced a new directory service called Active Directory to make it easier to locate resources within a large, complex network.
Overview

• Microsoft’s latest server product, Windows Server 2003, still supports all of these concepts.

• You can use Windows Server 2003 in any network model, from peer-to-peer to Active Directory domain.
Client-Server Networking

• Client-server networking is based on the idea of centralised sharing and centralized control.

• Think of it this way: if you had five children, you could buy each his or her own box of crayons, or you could buy one larger box that they all would share.

• For less than what you would pay for five individual boxes of 20 crayons, you could buy one large 100-piece box of crayons.

• This would allow each of the children to have more colours available and would save you some money in the process.
Client-Server Networking

• Client-server networking does something similar for computers.

• Instead of sharing resources from each other’s machines, users attach to dedicated servers where all the network resources are stored.

• This allows you to use less powerful machines for desktops and put your money where it really matters, into your servers.

• As with the crayons, you are getting more for less.
Client-Server Networking

• Users get better performance out of the higher end servers, and administrators get the benefits of centralised authentication and control.

• This makes for a more secure environment.
Centralised Authentication

• A good rule of thumb when working with end users is to keep it simple. Most users want to log on to their PCs and work.

• They do not want to remember five different user account names and passwords, as is often the case when accessing resources on different workstations in a peer-to-peer network.

• Client-server networking makes things simple, because all shared files and printers are stored on the server.
Centralised Authentication

• Users authenticate once to the server and they are done.
• They don’t have to remember one password for printing and another for accessing files.
• One account does it all. In fact, once authenticated to the domain, they can also access resources on other workstations in the domain (to which they have permission) without needing to have local accounts on those workstations.
Centralised Authentication

• For an administrator, client-server networking is the only way to go.

• Because everything is centralised, you will find it easier to manage shared files and printers, create and manage accounts, back up and restore data, and secure the network.

• If you have more than 5 to 10 machines, client-server networking is much more efficient than peer-to-peer networking.
Client-Server versus Peer-to-Peer Networking

- Peer-to-peer networking is networking in its simplest form.
- When you link two or more computers together without a centralised authentication server, you have a peer-to-peer network (also called a workgroup).
- Peer-to-peer networks allow file and printer sharing, but unlike client-server networking, authentication is not centralised.
- In a peer-to-peer network, every machine has its own local user accounts that can access files.
Client-Server versus Peer-to-Peer Networking

• If you want to access data on four machines, then you must have an account on each of the four machines.

• This is fine if there are only a few machines on the network, but when there are, for example, 50 machines, you have to use 50 different accounts.

• This means that you have to remember the passwords for all 50 and keep them synchronised (if possible).
Client-Server versus Peer-to-Peer Networking

A workgroup or peer-to-peer network
Client-Server versus Peer-to-Peer Networking

- Client-server networking puts all shared objects on a centralised server, allowing everyone who has been granted permission to access them.
- Now, instead of having four user accounts to remember, you only have one.
- As discussed previously, this provides centralised administration and centralised authentication, which make it easier for administrators to manage and easier for users to understand.
The Domain Concept

- Microsoft used the concepts of client-server networking when they created the domain model for Windows NT.
- The dictionary definition of domain is “a territory over which rule or control is exercised.”
- In other words, a domain is a control boundary.
- You can control objects within a domain together, as if they were one.
The Domain Concept

- Microsoft used the concepts of client-server networking when they created the domain model for Windows NT.
- The dictionary definition of domain is “a territory over which rule or control is exercised.”
- In other words, a domain is a control boundary.
- You can control objects within a domain together, as if they were one.
The Domain Concept

The Domain based network model
Directory Services

• *Directory services* has been a popular buzzword since the development of directory services standards, especially since Novell implemented their Novell Directory Service (NDS) for NetWare.

• It seems as if everyone is talking about or using some type of directory service.

• Different OSs even have their own directory services; Novell currently has eDirectory, and Microsoft has Active Directory.
Directory Services

• One of the first network operating system directories was Banyan VINES’ StreetTalk, which could be added onto Windows NT to provide a full fledged directory service.

• Directory services can be used to store all types of information, including account authentication information.

• If you are going to work in the computer networking sector, it is likely that you will eventually implement some sort of directory service.
What Are Directory Services?

• In its simplest form, a directory service is a way of storing information in a directory so it can easily be retrieved and used later.

• Directories predate electronic data; think of the telephone directory, product catalogues, and other directories published in print form.

• A directory service should include a set of rules to follow for naming its objects (the items entered in the directory), and a set of rules on how to store those objects.
What Are Directory Services?

• You should be able to add to and remove from a directory service as things change.

• In computer networking, a directory service is a network-wide database that stores information including (but not limited to) information on people, files, printers, and applications.

• The directory service functions as a central point of management for the network OS in use, and assists in locating information or objects on the network.
What Are Directory Services?

• The directory can store authentication credentials, user preferences and profiles, network configuration information, and so forth.

• Directories differ from other databases in that they are more often read than written to.

• The rules that govern information format and how it is stored are located in a *schema*, which can be modified to meet the needs of your particular organisation.
What Are Directory Services?

• The basic components of a directory service include:
  • A schema that defines the types of objects stored in the directory (object classes) and the attributes that can be assigned to them. Objects, which are representations of users, printers, applications, computers, and other entities, information about which is stored in the directory.
  • Object classes, which are specific types of entities that can be stored in the directory.
What Are Directory Services?

• Attributes, which are the properties of an object (for example, user attributes would include the user’s full name, account name, address, telephone number, and so forth.).
• A way to search the directory for information about the objects stored there.
History of Directory Services

• The first directories were paper directories like the telephone book or TV guides. Some of the first electronic directories were DNS and WHOIS.

• Later, application directory services appeared in e-mail products such as Microsoft Exchange, Novell GroupWise, Lotus cc:Mail, and in online directory services functioning as electronic phonebooks such as Four11, Switchboard, and BigFoot.
History of Directory Services

• It might be difficult to think of an electronic telephone book as a directory service, but it does match our definition.

• It has a set of rules for naming its objects (last name, first name) and a set of rules for storing its objects (alphabetically based on function).

• You can add to and remove from the telephone book as people move and their phone numbers change, and items can easily be retrieved from the phone book when needed.
History of Directory Services

• The most recent type of directory services to show up are network operating systems (NOS) directory services such as Novell Directory Services, Banyan VINES, and Microsoft Active Directory.
Directory Services Standards

• Most directories in use today are based on the X.500 standards.
• The X.500 standards are recommendations published by the International Organization for Standardisation (ISO) and International Telecommunications Union (ITU), that define how to organise a directory.
Directory Services Standards

- X.500 is not itself a directory, it is a model that vendors can use to build their own directories.
- Standards make compatibility between different products possible.
- If two separate vendors use the same model for their directories, then data sharing between the two directories should be possible.
- X.500 is to directories what the OSI model is to networking.
- X.500 defines standards for (among other things) creating a schema, defining attributes, and organising data within the directory.
Active Directory

• Active Directory first appeared in Windows 2000 Server and is based on the X.500 standards.

• It has been improved and is still in use in Windows Server 2012.

• Active Directory does not use a flat structure; instead, it is hierarchical in design (sometimes referred to as a *tree structure*).

• This allows logical separation within the directory for organisation and management.
Active Directory

- Active Directory allows you to customize your directory into an intuitive structure for your environment.
- In addition to domains, Active Directory uses additional structural elements such as domain trees, forests, and organisational units (OUs) for directory organisation.