UNIT 3 ADVANCED WINDOWS 2000 NETWORKING

Structure **Page Nos.**

3.0 INTRODUCTION

Windows 2000 provides an efficient networking environment. Domains, workgroups and trusted relationships describe the logical structure of Windows 2000. The physical structure of the domain hierarchy is completely segregated from the logical structure. As described in this unit, logical structure is made up of objects, Organisation Units (Ous), domains, trees and forests. The physical structure of the domain hierarchy is mainly composed of domain controllers and sites. A user account gives the user the ability to log on to the network or to a local machine. Everybody who regularly uses the network should have a network account. Group policies further refine the user management in Windows 2000.

Also discussed in this unit is auditing. Lastly, there is RRAS (Routing and Remote Access Screen) which is a very important feature of Windows 2000 that lets remote access possible and is a tool for maintaining network security in Windows 2000.

3.1 OBJECTIVES

After going through this unit you should be able to:

- describe Windows 2000 domains, workgroups and trusted relationships;
- manage efficiently user accounts in Windows 2000 networking environment;
- describe policies, auditing, active directory service in Windows 2000, and
- describe remote access in Windows 2000.

3.2 WINDOWS 2000 DOMAINS, WORKGROUPS & TRUSTED RELATIONSHIPS

In the following section we will introduce concepts of domains, workshops and trusted relationships.

3.2.1 Concept of Domains

A *Windows 2000* domain is a logical collection of network computers that share a centralised directory database referred to as Active Directory Service. In a domain this centralised information directory resides on a computer called domain controller. In Windows 2000 domain controllers are peers only.

Thus Windows 2000 domains provide the following advantages:

- They provide extensibility features to existing networks.
- Domains provide centralised control of all user information.
- Thus domain can be referred to as the basic unit that is used for network growth and security in Windows 2000 network.

Usually one or more domain controllers are associated with a domain. In Windows 2000 Server a domain controller is the computer that is responsible for storing an entire copy of domain directory. In Windows 2000 it is the Windows 2000 Active Directory service that divides an organisation's network logically and physically. Logical structuring facilitates the finding by a user of a resource by name not by its physical location.

Logical structure of a domain comprises:

- Objects
- Organisation Units (OU)
- Domains
- Trees
- Forests

Physical Structure of a domain comprises:

- Domain controllers
- Sites

Objects: A distinct named network resource can be referred to as an object. This object comprises certain related attributes. As an example, for an object printer, the attribute list may include printer name, make, etc. Similar objects can be grouped into classes.

Organisational Units: This is a container object. Container objects are objects that are residing within other objects. The purpose of an organisational unit is to organise the objects of a domain into logical administrative groups.

Domains: The basic unit of Active Directory Service is a domain. It is also referred to as a partition of an Active Directory Service. It is the domain only that is responsible for containing all network objects within it. It also serves as a security boundary to its objects. None of the security policies and settings, such as administrative rights, ACLs, ACE (Access Control Entries) can cross from one domain to another.

Trees: In order to support global sharing of resources trees are required. In a tree one or more Windows 2000 domains are arranged in a hierarchy. Thus by joining multiple domains in a hierarchy a large namespace can be constructed, which can further avoid name conflicts. All domains that are a part of a tree, or that share a tree can share information and resources. A domain tree has only one directory. As long as the user has the appropriate permissions he can use the resources of other domains in a tree. All domains in a tree share a common schema, which is a layout, a formal definition of all objects.

The central repository of information about objects in a tree or forest is called a **global catalog**. All domains belonging to a single tree share a global catalog. Domains in a tree also share a common namespace.

Forest: One or more trees can be grouped into a forest.

A forest comprises:

- One or more trees
- A common schema
- It serves transitions trust relationships between trees.
- Different namespaces between these trees.
- A global catalog that contains the list of all objects in the forest.

Different users while accessing user objects must be aware of the domain name.

3.2.2 Trust Relationships

A trust relationship refers to a link between two such domains, where one domain is referred to as the trusting domain and other as the trusted domain. Trusting domain lets the trusted domain logon.

User accounts and groups that are defined for a trusted domain can access trusting domain resource even though those accounts are not present in trusting domain directory database.

A **kerberos** (a security algorithm) transitive trust refers to a relationship type where

Domain I trusts Domain II,
Domain II trusts Domain III,
Domain I trusts Domain III.

So a domain joining a tree acquires trust relationships of every domain in the tree. In Windows NT and earlier versions, there used to be only one-way trust relationships among domains.

Physical Structure of an Active Directory Service is responsible for affecting efficiency of replication in domain controllers.

Domain Controllers contains a copy of domain database. Wherever an update in the directory takes place, Windows 2000 automatically replicates the change to all other domain controllers in a domain. In a domain having multiple domains controller's directory information is replicated from time to time.

Only those computers running Windows 2000 Server, Advanced Server, or Data Center server can become domain controllers.

Sites is a grouping of IP subnets (ranges). For example, one site can be 192.168.20.0/24 to 192.168.30.0/24

3.2.3 Building Domains

A computer can join Windows 2000 domain only after an account has been created in or added to the domain database. For that a user must have the **Join A Computer to the Domain permission**.

By default, permission is granted to Administrator Members, Domain Administrator or Members of Administrators, Account Operators and Domain Administrator groups.

To join a domain a computer account for that computer should have been created in advance or it may be created during the installation process by selecting the check box '**Create a Computer Account in the Domain**'.

3.3 USER ADMINISTRATION

This section discusses user account administration. For a user to log onto a Windows 2000 network, a user account must be created. It is unique to every user and includes a user name and a password for authentication. A user can logon as a local user and a domain user as well. Thus by having an account a user has access to all network resources. As discussed in previous sections, in the Windows 2000 operating system two kinds of user accounts can be created:

- Domain account
- Local account

User account Administration includes setting up user profiles and name directories and modifying existing user accounts.

The next section discusses Group Account Administration.

Existing User Accounts Modification

Many different kinds of modifications are required with user accounts. These modifications may be required because of organisational or personal changes. An instance is whenever a new employee joins, the company may want to modify an existing account and give access to the new employee. Also, personal profiles may need to be updated at times.

Modification may include the following:

- Renaming
- Erasing
- Disabling
- Deleting User Accounts

1. To Rename a user Account: Normally renaming an account is done so that all access services to an account remain intact. When an account that has been created for a particular user is to be assigned to another user, all permissions, rights, properties set for that account are retained.
2. To Enable/Disable a user account: A user account is disabled when it is not needed for some time but would be accessed after a certain period of time. It is a situation when a user temporarily disables the account and needs access to it after a fixed period of time.
3. To Delete a user account: When a user no longer needs it, it is deleted.

Use Active Directory Users And Computers Snap-In,

Modify properties. To Reset the User Password:

1. Open Active Directory Users And Computers Snap-In and select the user object.
2. Activate the Action menu, click Reset Password. In the Reset Password dialog box, enter a password and select.

User must change password at next logon to force the user to change his or her password the next time that the user logs on.

Managing User Profiles

A user profile contains all data pertaining to a user. It also contains current desktop settings, all connected networked computers and all mapped drives. Modifying

desktop settings can modify a user profile. It is created the first time when a user logs on to a computer.

When you log on to a network computer in Windows 2000 environment you get individual desktop settings and connections.

Windows 2000 supports Roaming User Profiles (RUPs), for users who work on more than one computer. A user set up a RUP on a network server and it is available to all the computers or the domain network. It is copied to client computer from Windows 2000 server when a user logs on. Thus, unlike user profile, with a Roaming User Profile the user always gets his individual desktop settings. Also a local user profile is on single client computer only.

Home Folder: A home folder is one that is provided to the user in addition to my documents folder to store personal data. It is not included in RISP (Routing and Remote Access Screen).

Group Accounts Administration

User accounts can be collected together. Such collections are called as groups. The grouping simplifies administration as new access permissions are assigned to a group rather than to individual accounts. All user accounts belonging to that group have access privileges. Moreover user(s) can belong to multiple groups.

In Windows 2000 environment there are two kinds of groups, Security groups and Distribution groups.

Windows 2000 has 4 built-in groups:

- Global groups
- Domain Local groups
- Local groups
- System groups.

Common types of user accounts are contained in groups. The group scope is responsible for membership of a group. Active Directory Users and Computers Snap-in are used to create a user group in a domain.

Group Policy

A group policy primarily comprises configuration settings that determine the layout of an object and its successors (children) objects. Group policies provide for controlling the programs, desktop settings, and network. In a network, group policies are normally set for the domain. Policy administrators administer group policies.

Types of Group Policies:

- Scripts: let the policy administrator specify applications and batch files to run at specified times.
- Software settings execute the applications. These policies can automate application installation.
- Security Settings are responsible for restricting user access to files etc.
- Remote Installation Services (RIS).
- While executing client installation wizard, it controls RIS installation options.
- Folder Redirection facilitates movement of Windows 2000 folders from their default user profile location to a place where they can be managed centrally.

- Administration Templates consist of registry based group policies for managing registry settings, etc.

GPO (Group Policy Objects)

These objects contain configuration settings for group policies. Information is stored in two ways in a GPO:

1. In containers
2. In Templates

Creation of GPOs takes place before group policies. Group Policies can be modified using:

1. Group Policy snap-in or
2. Using Active Directory Users and templates snap-in.

Only administrators, creator owner or a user with access to GPO can edit a group policy.

Auditing

Windows 2000 auditing is a facility responsible for security. It is responsible for tracking user activities, keeps a check on them. Windows 2000 maintains a security log. User events are written onto their security log. All the events related actions are entered onto security log. An audit entry in security log not only comprises action that takes place, but also the user and success or failure of the event and when the action occurred. Thus whatever event takes place in Windows 2000, Security Log has an entry for the same.

An audit group policy is configured for all domain controllers in a domain. Auditing is assigned to parent container and it passes it down the hierarchy to the child containers. However, if explicitly a child container is assigned a group policy then child container group overrides parent container settings.

To plan an audit policy, computers must identify on which auditing is to be applied. By default, auditing option is turned off.

Only certain specific events can be audited on computers:

- User logging on and off.
- User accounts and group changes.
- Changes to Active Directory Objects.
- Files access.
- Shutting down Windows 2000 Server
- Restarting Windows 2000 Server.

3.4 REMOTE ACCESS

Windows 2000 remote access mechanism lets remote clients connect to corporate networks or to the Internet. Windows 2000 supports two kinds of remote access connection methods (*Figure 1*).

- Dial up remote access
- VPN (Virtual Private Network) remote access.

VPN provides a secure network connection between two remote machines.

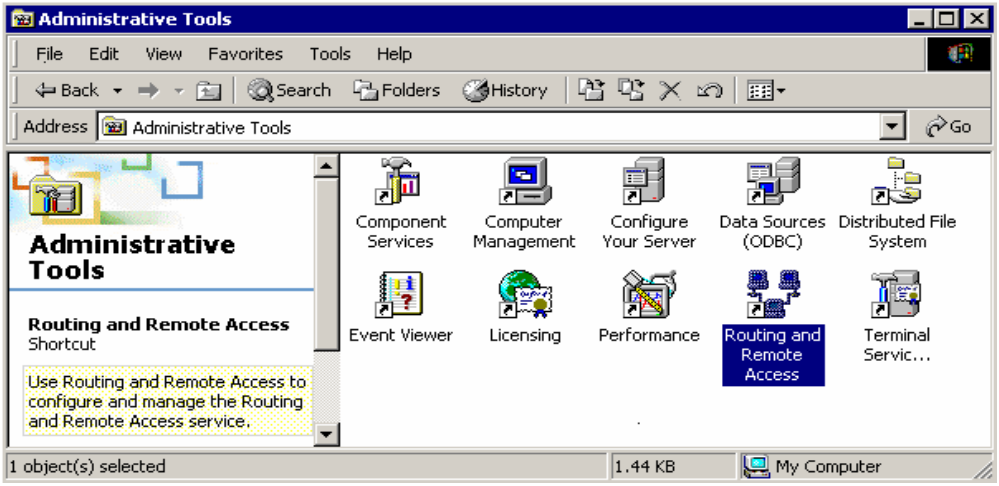

Figure 1: Dial up Remote Access Screen

With **dial up remote access** A remote access client uses telecommunication infrastructure to create a temporary physical structure to create a temporary network or a virtual network.

Right click on the server icon and select "configure and Enable Routing and Remote Access" as shown in *Figure 2*.

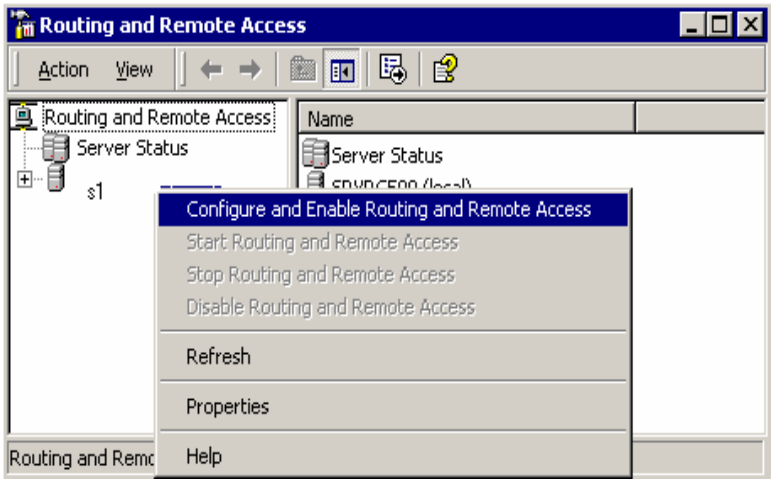

Figure 2: Renting and Remote Access Screen

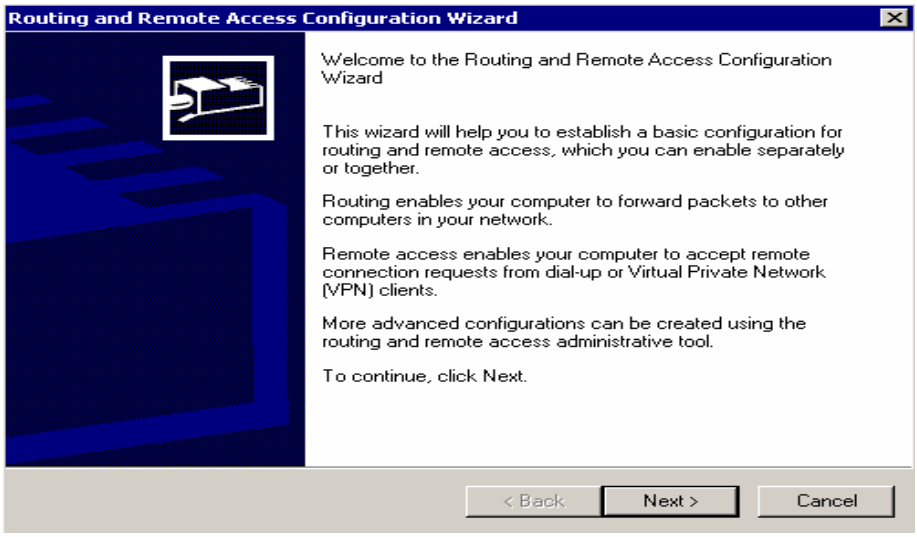

Figure 3: Routing and remote Access Configuration wizard

Using this, all devices for remote access can be enabled and the following screen appears (*Figure 3* (*a*)).

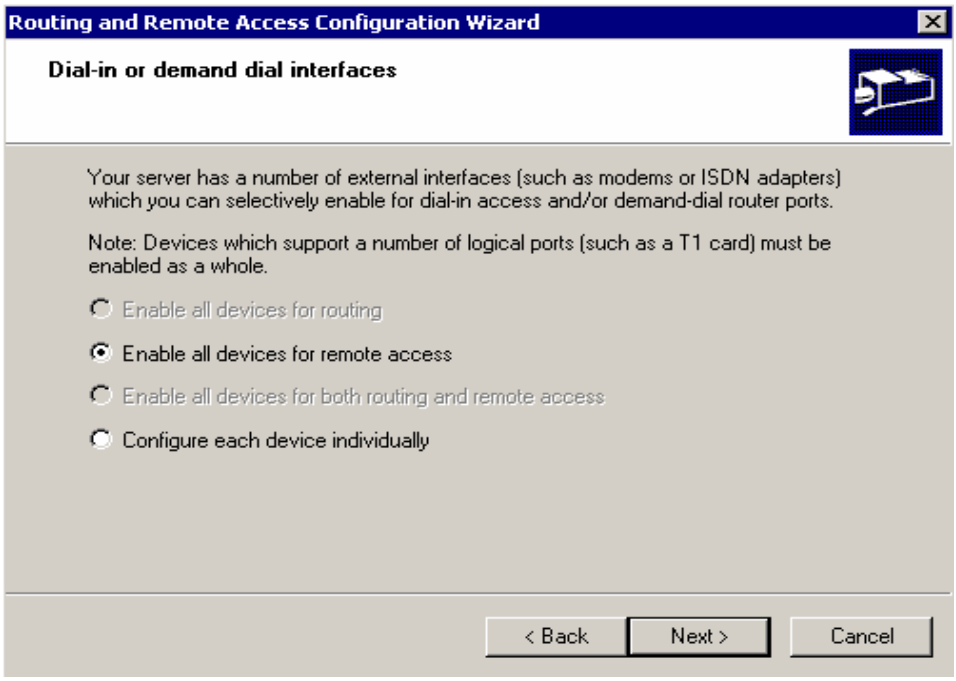

Figure 3(a): Routing and remote Access Configuration wizard

For security reasons use the following option as shown in *Figure 3*(*b*):

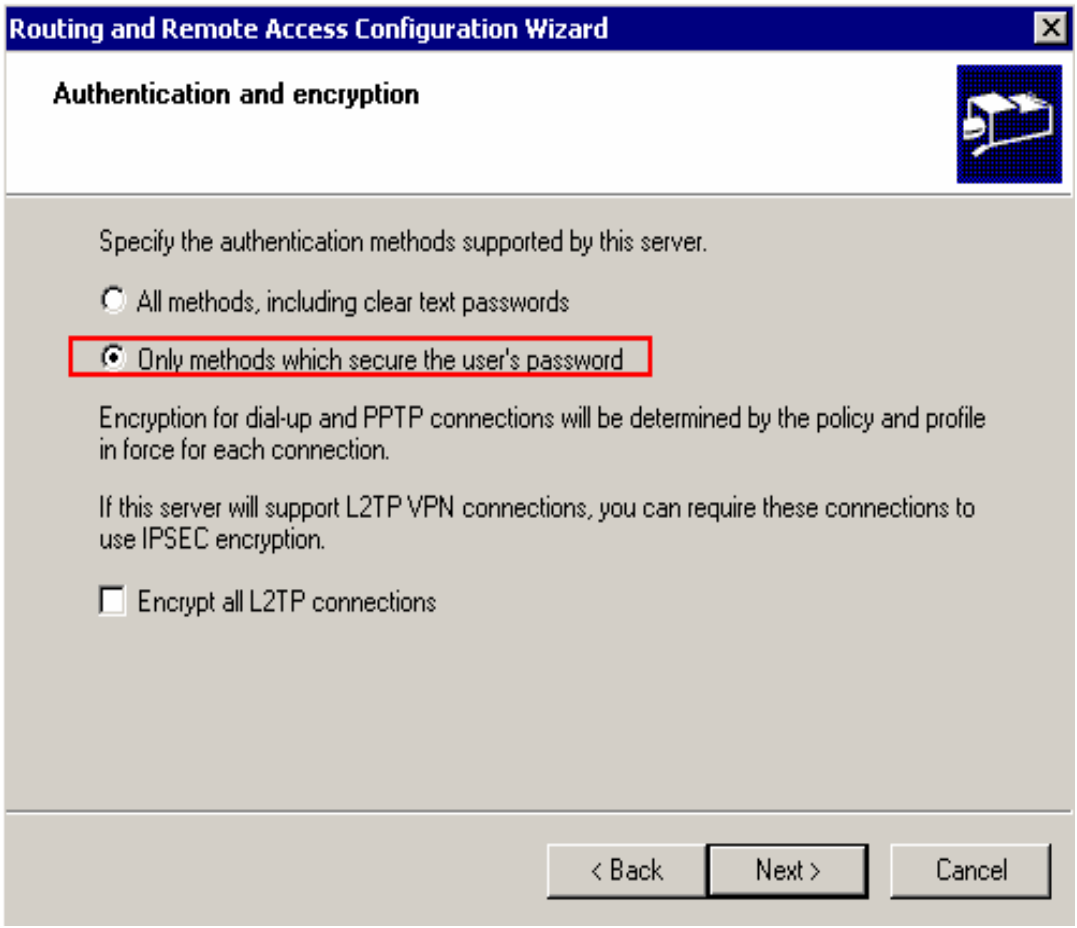

Figure 3(b): Routing and remote Access Configuration wizard

If you have TCP/IP then write TCP/IP as shown below in *Figure 3c*.

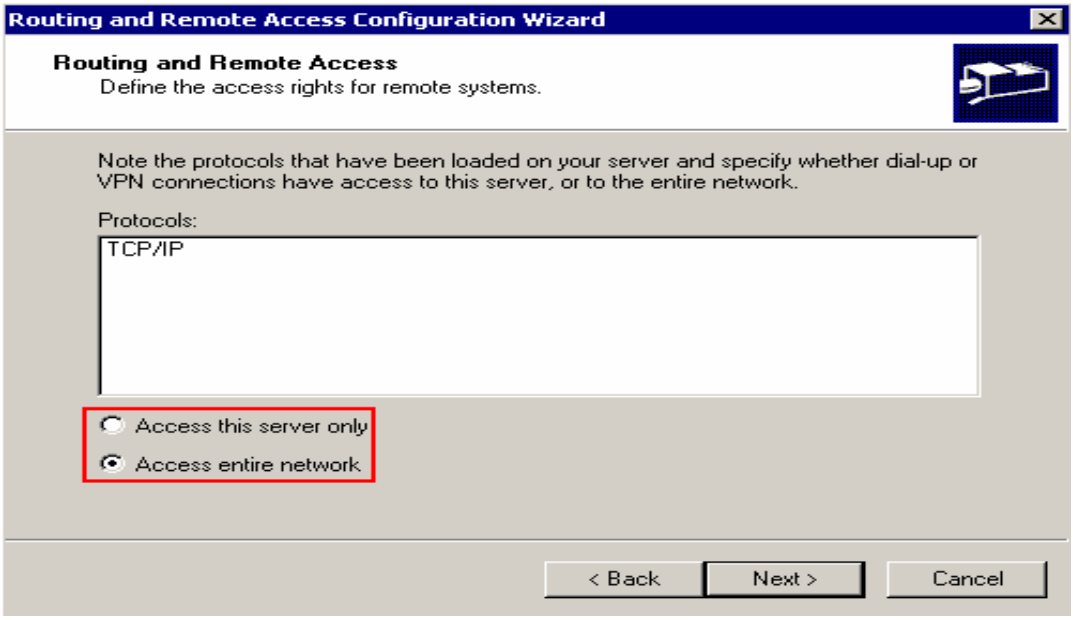

Figure 3 (c): Routing and remote access configuration wizard

Once all the requisites are complete then the following wizards (*Figure 3(c), 3(d*) and *3(f)*) appear:

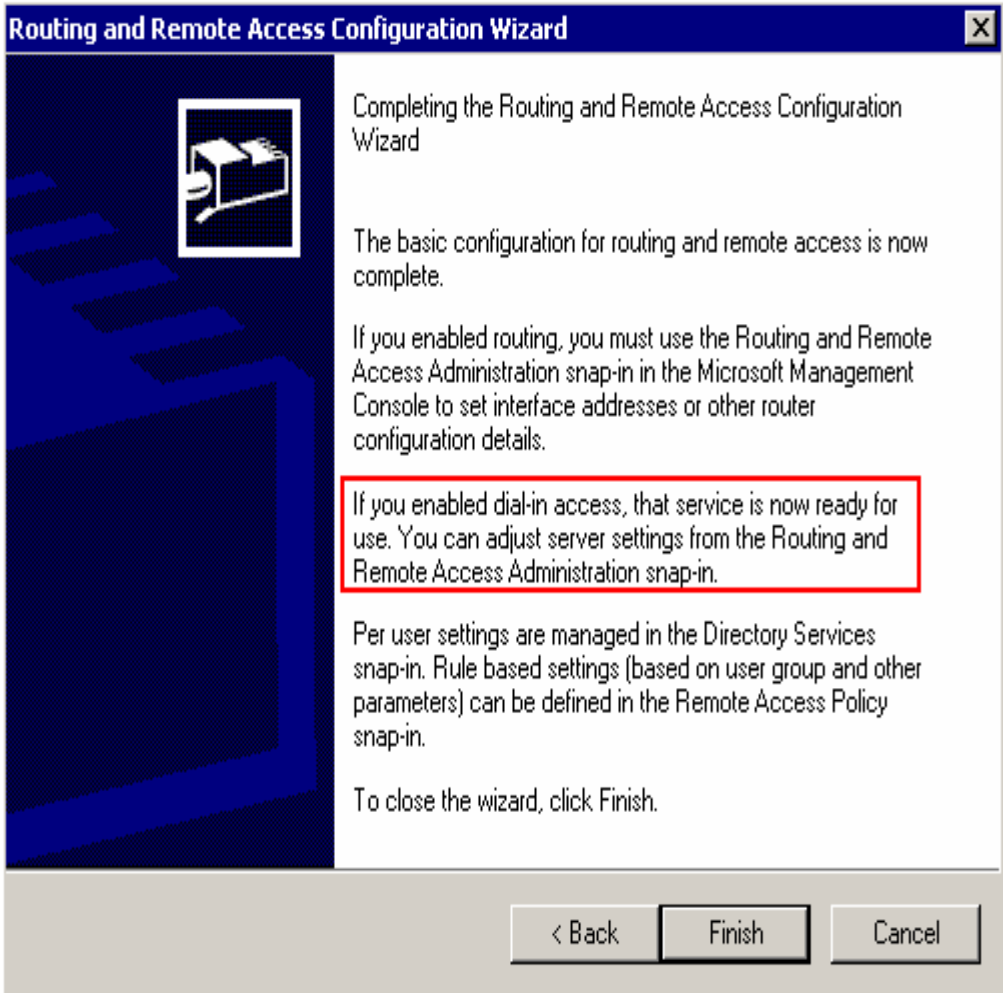

Figure 3(d): Routing and remote Access Configuration wizard

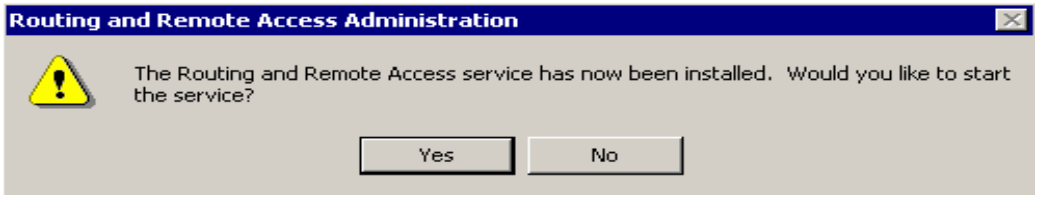

Figure 3(e): Routing and remote Access Configuration (RRAS) wizard

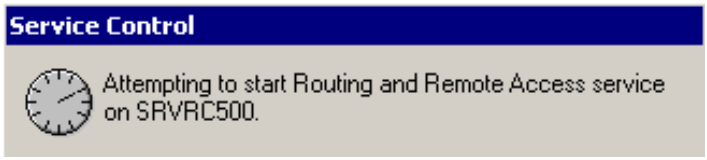

Figure 3(f): Routing and remote Access Configuration wizard

After this screen RRAS is now configured and the contents can be viewed as *Figure 4*:

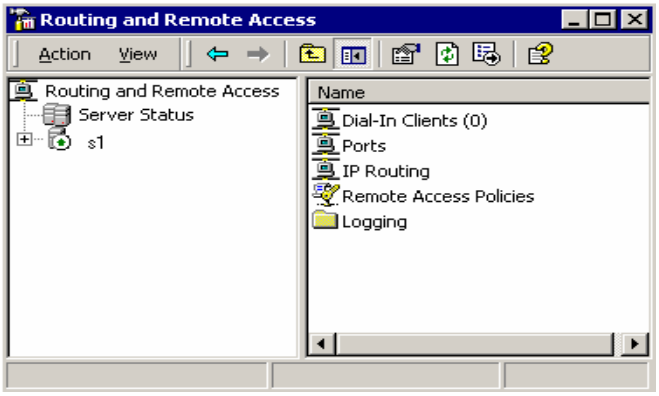

Figure 4: Routing and Remote Access

By default, Windows 2000 creates automatically 5 PPTP and 5 L2TP port for incoming VPN-connections (*Figure 5*).

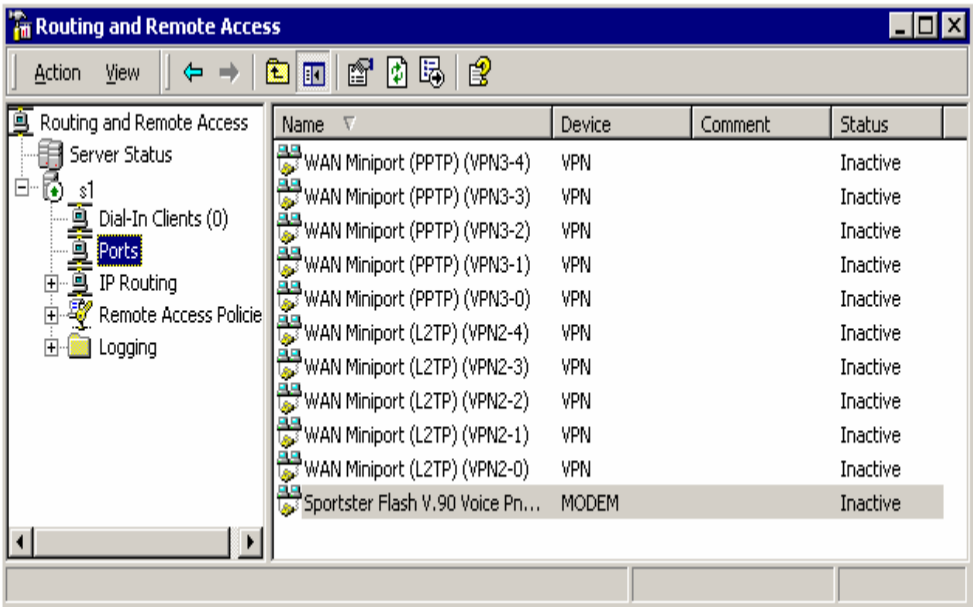

Figure 5: Remote Access Connection Screen

With **VPN remote access** – remote access of a VPN client uses an IP network to create virtual point-to-point connection with a RAS server acting as a VPN server. A dial up Remote Access Connection consist of :

- Remote access client
- Remote access server
- WAN infrastructure.

Remote Access Clients: Windows 2000, Win NT, WIN 98, Windows 95, MS-DOS, MS LAN Manger are remote access clients that can connect to Windows2000 remote access server. Third party clients like UNIX and Apple Macintosh too can connect to windows 2000 remote access server.

Remote Access server: Windows 2000 server accepts requests from client's connections and forwards it to other clients or to the network.

WAN Infrastructure depends upon the type of connection being made. There are various networks like:

PSTN(Public switched telephone network
ISDN(Integrated services digital network
X.25 (ITY-T Protocol based WAN)

Windows 2000 support three types of Remote Access protocols PPP, SLIP and asynchronous NetBEUI, also TCP/IP, IPX, AppleTalk.

Windows 2000 remote Access provides a variety of security features like:

- User Authentication
- Mutual authentication
- Data encryption
- Call back
- Caller id
- Remote access account lock out.

Remote Access Management involves managing users, addresses, accesses and authentication.

Virtual private network is an extension of private network that involves encapsulation, encryption, authentication to links across shared or private networks. A VPN mimics the properties of a dedicated Private network through Internet; allowing data transfer between two computers in a network. Corporate offices can use two different methods to connect to a network over the Internet:

Using dedicated lines or dial up lines VPN uses tunneling to transfer data in a VPN. Tunneling is a secure method of using an internetwork infrastructure to transfer a payload.

A tunneling protocol comprises tunnel maintenance protocol and tunnel data transfer protocols. Two basic types of are:

1. Voluntary tunnels
2. Compulsory tunnels.

Protocols used by WIN 2000 for VPN are PPTP (Print to print tunnel Protocol), L2TP (Layer 2 Transfer Protocol), IPSec (IP security), IP-IP.

VPN management involves managing user addresses, servers access, authentication, and encryption. Troubleshooting VPN involves checking connectivity, remote access connection establishment, routing, IPSec.

Windows 2000 provides a set of RRAS tools:

- **Routing And Remote Access Snap In** enables RRAS, management of routing interfaces, IPX routing configuration, creation of static IP address pool, configuring remote access policies. This is available from Administrative Tools folder.
- **Net Shell Command:** Windows 2000 Netshell command is a command line and scripting utility. It is named Netsh.exe and is installed in % systemroot %\system32 when a Window 2000 is installed.

☞Check Your Progress 1

1) Give the default order of group policy implementation through Active Directory service hierarchy.

……

……

……

2) Is it possible to set up encryption on a compressed folder?

……

……

……

3) When should security groups be used instead of distribution groups?

……

……

……

4) If the domain mode is switched over from mixed mode to native mode, what are the implications?

……

……

……

5) If a remote access client wants to connect to RAS server but connection is not allowed how will this error be solved?

……

……

……

6) Write the purpose of VPN and name VPN technologies supported by Windows 2000?

……

……

……

3.5 SUMMARY

This unit highlights working of a domain, workgroups and trusted relationships in a Windows 2000 network. Windows 2000 provides a secure network environment for efficient resource sharing. Logical structure of domain hierarchy comprises objects,

organisational units, domains, trees and forests. Domain controller and sites make up the physical structure of a domain. Many types of group policies exist, software settings, scripts, security settings, folder redirection etc. Group policies are a set of configuration settings that apply to one or more objects in the directory store. The structure of a group policy is made up of group policy objects, templates and containers. Group objects must be created before the creation of group policies.

Auditing is the process of tracking both user and Windows 2000 events. Windows 2000 writes the events to the security log on each computer. An audit entry contains information about the event that occurred, user responsible for performing that event, success and failure of that action. Another interesting feature in Windows 2000 is RRAS that lets the remote access possible.

3.6 SOLUTIONS/ ANSWERS

Check Your Progress 1

1) Group policy is implemented in the order site, domain, and organisational unit.

2) Encryption and compression cannot be applied simultaneously to a file. In order to set up encryption on a file it needs to be decompressed first.

3) Security groups are used to assign permissions. Whereas it is recommended to use distribution groups only when the group is required to perform a security related function.

4) Once you switch from mixed mode to native mode you cannot revert to mixed mode.

5) Do the following measures to correct the error:

   i. Verify Event logging enable (d) and view System Event Log, on computer running RRAS.
   ii. On the server, open Authentication Methods dialog Box and check Allow Remote systems to connect without authentication check box.
   iii. On remote access client, access the properties the dial up device like a modem, click Diagnostic tab check the Record a Log check Box.

6) It provides secure data transfer over a public network. Windows 2000 supports PPTP and L2TP.

3.7 FURTHER READINGS

1. www.microsoft.com/ windows2000 OS living

2. "*Operating system concepts*" Silberschatz, Galvin & Gagne Sixth Edition, John Wiley and Sons.