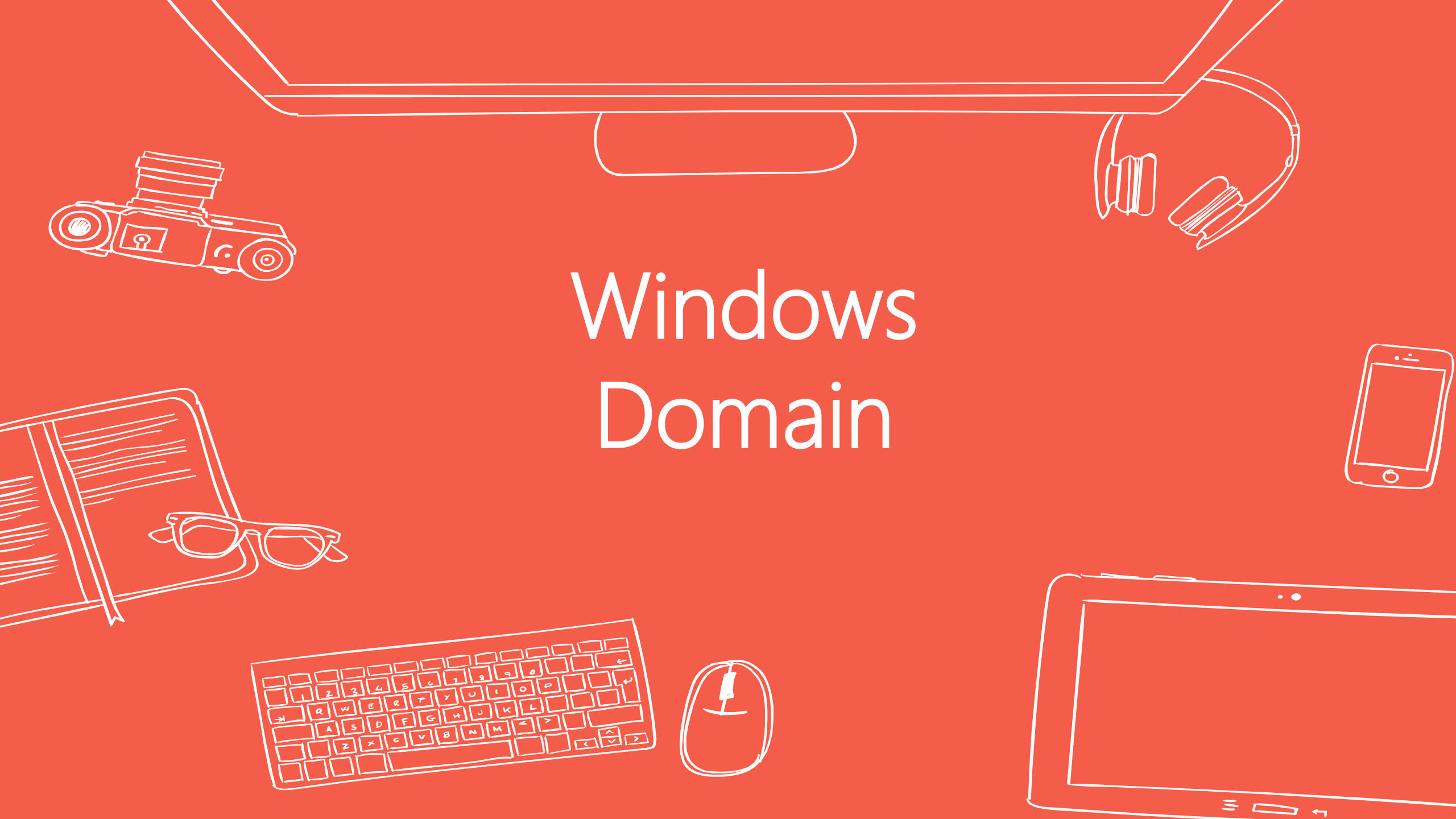
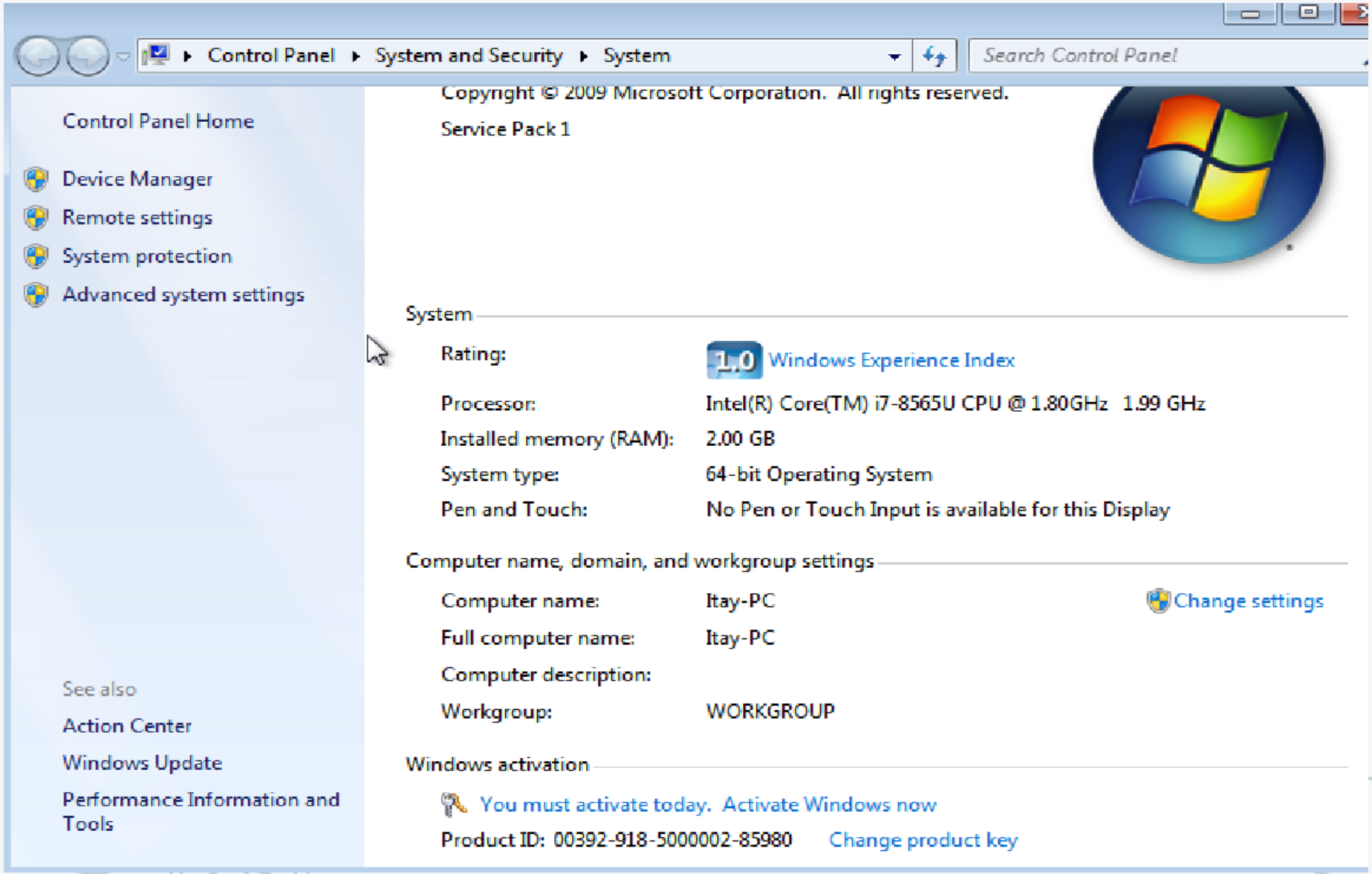
Windows Domain



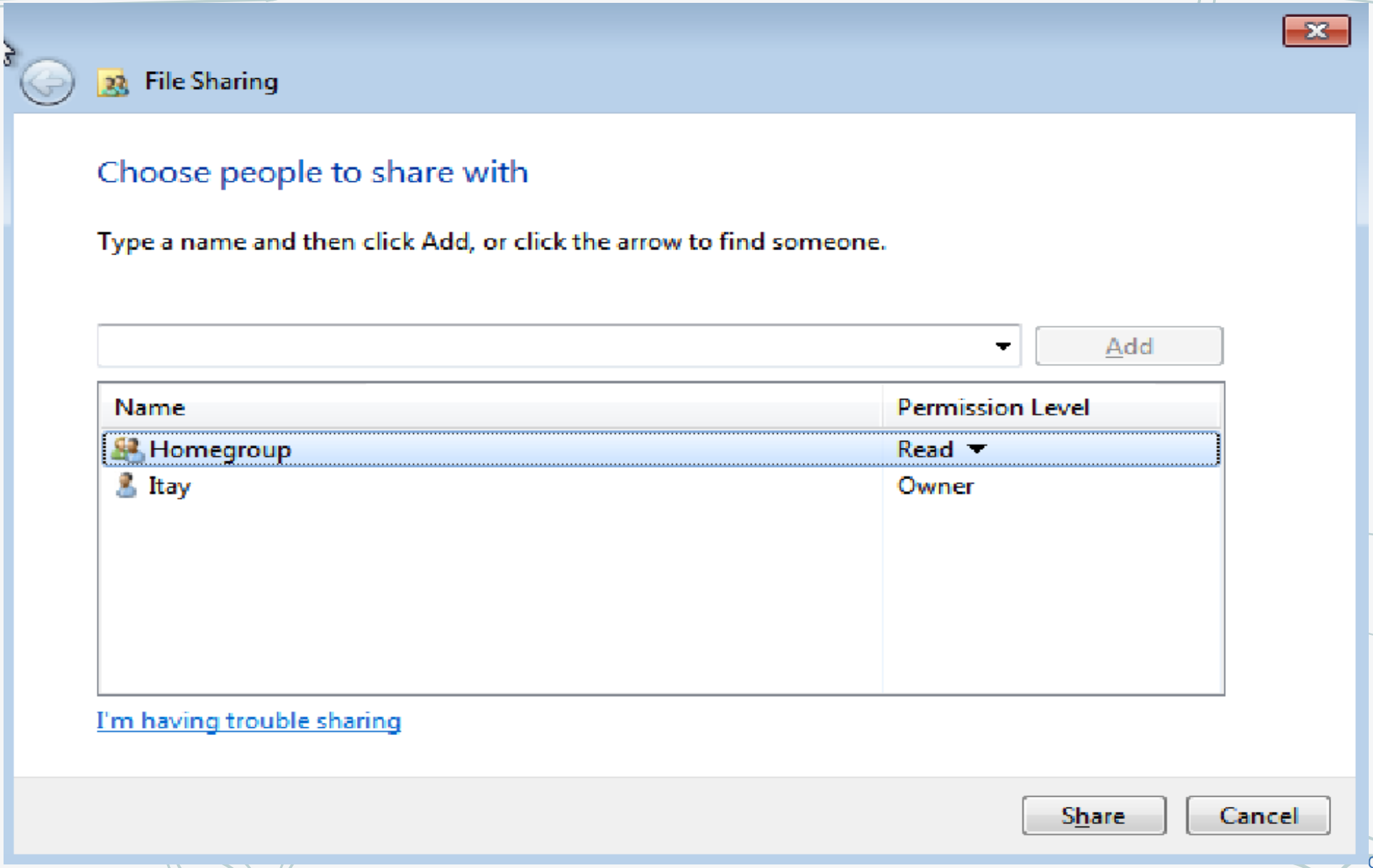
Windows Workgroup

- Windows Workgroup is a term used by Microsoft to describe a shared computer network
- The computers in the Windows Workgroup share various resources, such as network folders, printers, and more
- Each computer in the Workgroup is managed independently. That is, if there is a need for a some change in the computers, it is necessary to make a change in all the computers manually
- Each computer is by default associated with the Workgroup

Windows Workgroup



Windows Workgroup – File Sharing



Windows Workgroup - File Sharing

- All computers in the same workgroup will be able to access folder sharing and file reading
- If the computer is in the same workgroup, the File Share service is turned on, and Windows Sharing ports are enabled, we can access a folder from another computer on the network
- Each computer in the Workgroup is managed independently. That is, if there is a need for a some change in the computers, it is necessary to make a change in all the computers manually
- SMB protocol – port 445
- The sharing can be seen using the 'netstat-noa' command:

```
TCP    192.168.1.22:59416     192.168.1.24:445       ESTABLISHED     4
```

Windows Domain

- Windows Domain is defined as a network of shared computers that are managed by a central server called Domain Controller Server, which is responsible for managing the computers and is configured on the Windows Server operating system

- Domain establishment is necessary in large organizations that manage a large number of computers, users and network devices and with its establishment gets one central dedicated place to manage all the components of the organization

Windows Domain

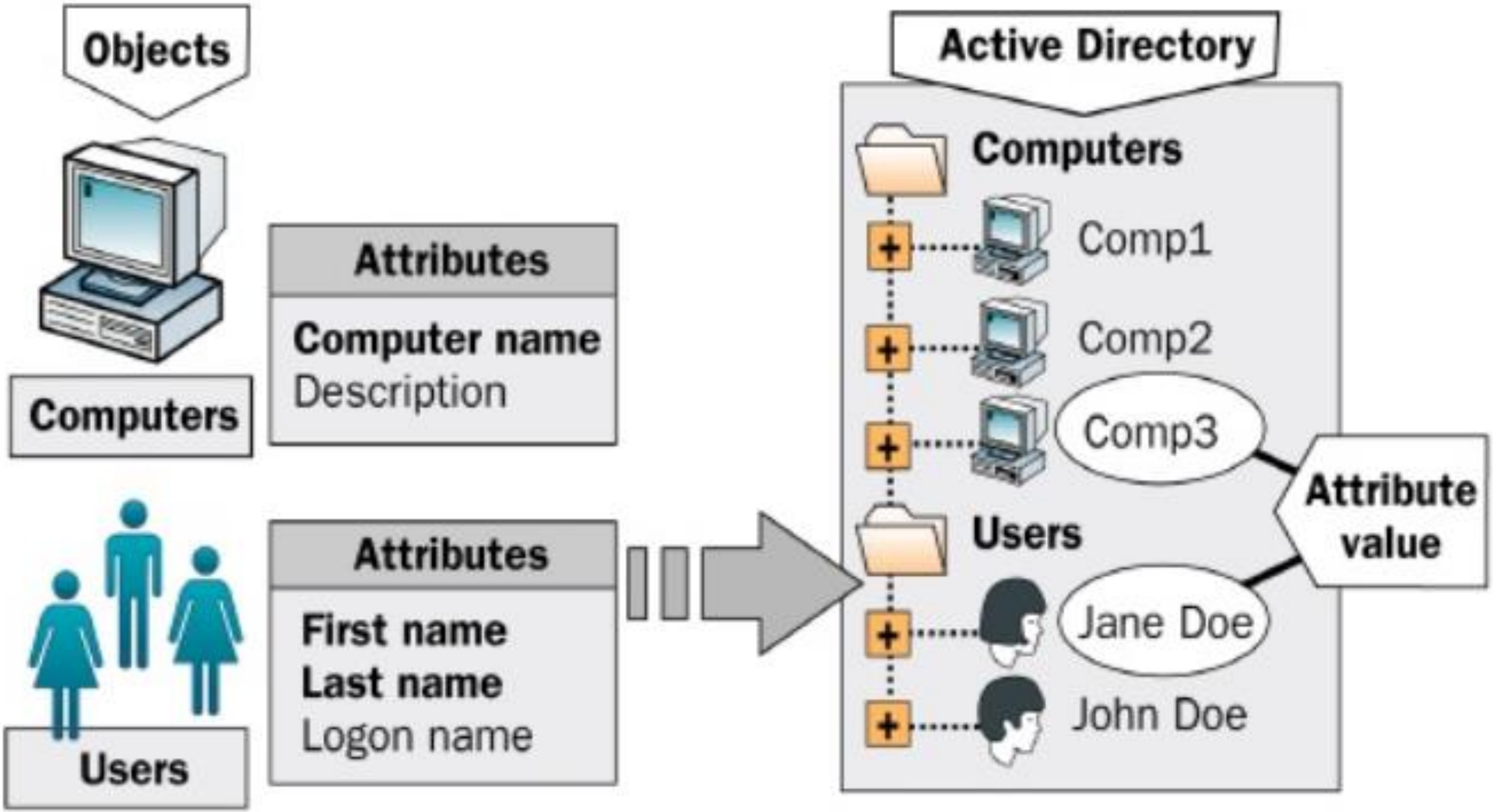
- File and resource sharing
- Network printers
- Manage users, groups and permissions
- Management of information security policy
  - Audit policy
  - Hardening policy
  - Password policy
  - Privilege policy

Windows Domain – Domain Controller

- The servers that control the Active Directory service and store all the AD information in their database
- Cluster is defined between the DCs servers and the SCHEMA information on the domain is replicated
- SCHEMA - A file that contains all the information about the domain expands and is updated depending on the changes in the domain
- Sends the Access Control Key to the user who has logged on to the domain, which contains the set of permissions and security policies contained on it and the computer that has logged in from it

Windows Domain – Active Directory

- Active Directory - A service developed by Microsoft for managing enterprise computer networks. The service includes:
  - Authorization services, user management, groups and computers and security
  - NTLM or KERBEROS based authentication and authentication services
  - LDAP services
  - DNS services
  - DHCP services


Objects
Computers
Attributes
Computer name
Description
Users
Attributes
First name
Last name
Logon name
Active Directory
Computers
Comp1
Comp2
Comp3
Users
Jane Doe
John Doe
Attribute value

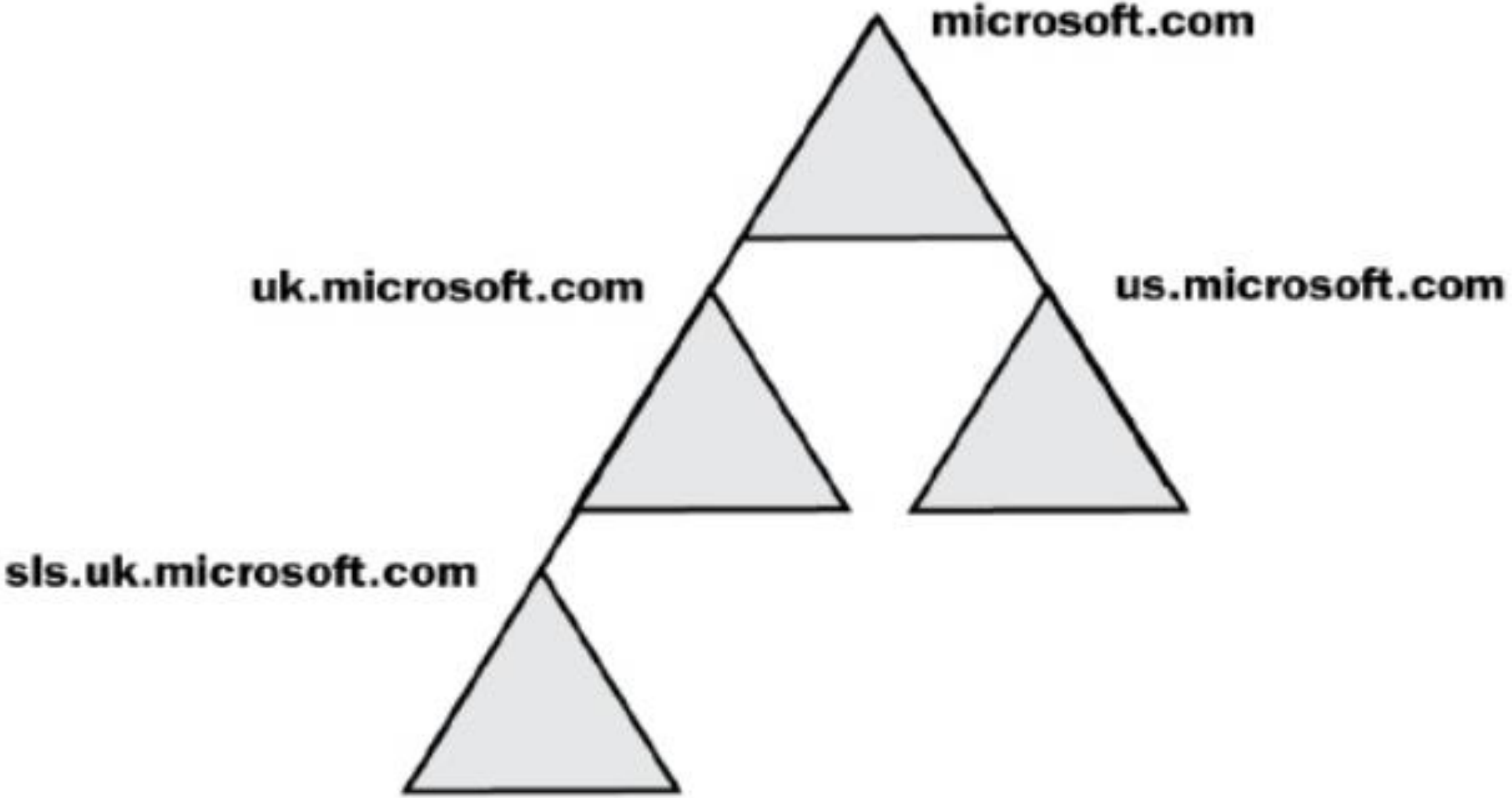
Windows Domain – Domain Tree

- Let’s take for example a corporate organization like Microsoft. It is an international organization with branches all over the world

- Of course, it is not possible to create domain servers for all the organization's computers in just one physical place, which will make it difficult to access the network and manage the computers. To create a subdomain

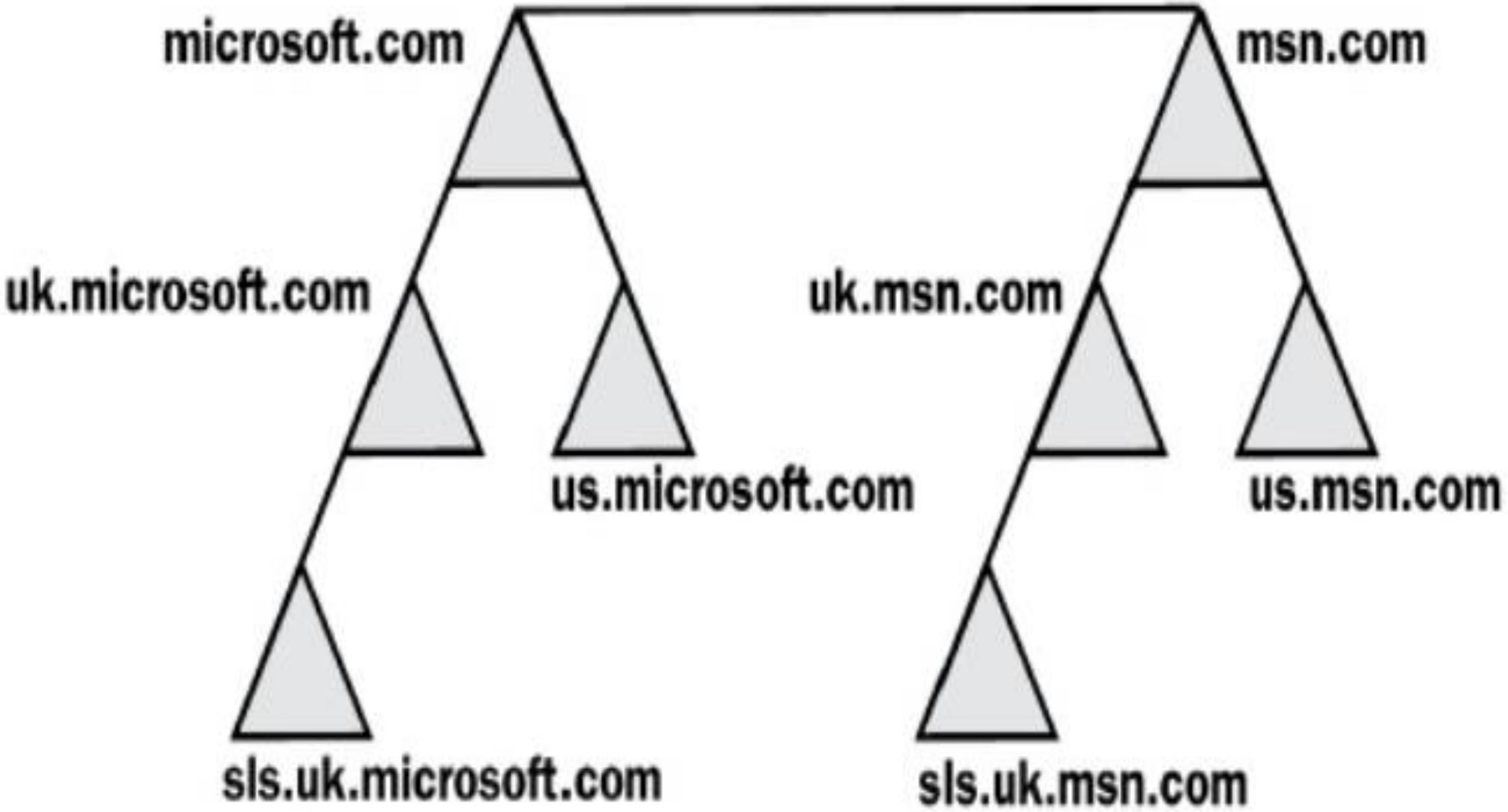
- Sub Domain is an independent domain, but connected to the primary domain hierarchically and administratively. In the Microsoft example we will define SYSTEM administrator for each Sub Domain who will independently manage their area. But, if necessary, the SYSTEM administrator of the main domain will be able to access and manage the Sub Domain themselves

- The whole architecture is called Domain Tree


microsoft.com
uk.microsoft.com
us.microsoft.com
sls.uk.microsoft.com

Windows Domain – Domain Forest

- We will continue with the example of Microsoft, and remember that Microsoft bought MSN
- Following the acquisition, there was a need to create an administrative link between Microsoft users and MSN users, it's meant to link the two different domains
- We connect the two domains of the domain controllers of the two organizations, and so we will actually define Domain Forest, which is a combination of two or more domains
- The whole architecture is called Domain Forest


microsoft.com
msn.com
uk.microsoft.com
uk.msn.com
us.microsoft.com
us.msn.com
sls.uk.microsoft.com
sls.uk.msn.com

Windows Domain – Site Domain

- A domain located in a geographical or logical area is different from the Domain Collector area located in my Data Center
- Defined as Satellite Offices
- Capable of replication with the Domain Controller servers in the Data Center
- Site Domain Management can be given by settings in the Organization Unit, all network administrators can manage their Organization Unit only

Windows Domain – Trust Relationship

- Trust is defined as a management and connection link between two different domains, for the purposes of information sharing, user identifications and groups

- Implicit Two-Way Transitive Trust

  - A two-way trust between different domains, and has a Transitive capability that indicates consent to third-party access if the main domain recognizes it

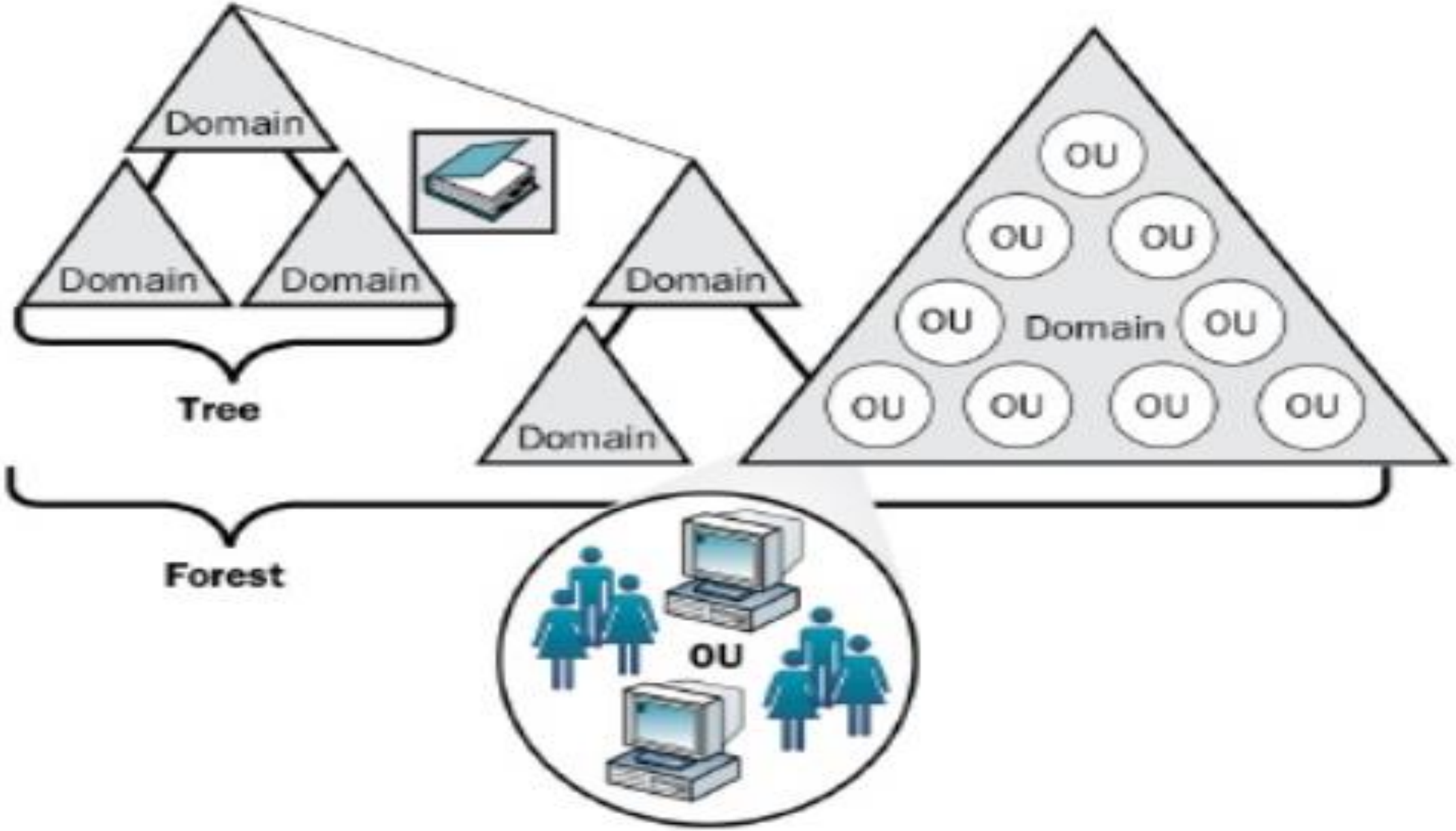
- Explicit one-way Trust

  - One-wat trust only, in case there is a primary domain that wants to connect to another domain to manage it, but does not want to allow it to connect to it.

Windows Domain – Organization Unit

- Organiztion Unit (OU) includes the users, groups, computers, network components such as printers, tablets, etc .. of a particular organizational area, on which specific settings can be deployed or managed individually

- After setting up users, computers, and network components in Active Directory. And after we have defined groups as needed in the domain. All the components can be assigned to the desired OU


Domain
Domain
Domain
Tree
Domain
Domain
OU
OU
OU
OU
Domain
OU
OU
OU
OU
OU
Forest
OU

Windows Domain – Permission & Security

- Permission – Set up your access to network resources - network folders, printers, etc

- Security Policy - Group Policy Object (GPO) - What you are allowed to do in the system: software installation, changing system settings, accessing drives, running and updating software, password policy and management and authentication

- Group Policy allows you to manage groups of computers according to a policy set by the network administrator and contained on the managed computers. The policy enforced on the computer sets restrictions and options for using the computer.

- The computers in the domain are set to receive updates from the Group Policy at any given time. If necessary, an update from the GPO can be activated manually by command:

```
gpupdate /target:<computer_ip> /force
```

Windows Domain – Authentication Methods

- NTLM

- Windows NT LAN Manager (NTLM) is a challenge-response authentication protocol used to authenticate a client to a resource on an Active Directory domain. When the client requests access to a service associated with the domain, the service sends a challenge to the client, requiring that the client to perform a mathematical operation using its authentication token, and then return the result of this operation to the service. The service may validate the result or send it to the Domain Controller (DC) for validation. If the service or DC confirm that the client's response is correct, the service allows access to the client

- NTLM is generally considered insecure because it uses outdated cryptography that is vulnerable to several modes of attacks. NTLM is also vulnerable to the pass-the-hash attack and brute-force attacks

Windows Domain – Authentication Methods

- KERBEROS

- Kerberos is a computer network security protocol that authenticates service requests between two or more trusted hosts across an untrusted network, like the internet. It uses secret-key cryptography and a trusted third party for authenticating client-server applications and verifying user's identities

- Kerberos is the best security access protocol available today. The protocol is flexible enough to employ more robust encryption algorithms to help combat new threats, and if users practice good password choice policies

Windows Domain

- Steps to set up Windows Domain:
  - Installing a Windows Server
  - Configure a static IP address on the network
  - Add Roles to a server through Server Manager
  - Add Features to the server through the Server Manager
  - Restart to server

Q\A