Windows Administrator L2 Interview Question

1. What is the purpose of having AD?

Active directory is a directory service that identifies all resources on a network and makes that information available to users and services. The Main purpose of AD is to control and authenticate network resources.

2. Explain about sysvol folder?

The sysvol folder stores the server's copy of the domain's public files. The contents such as group policy, users, and groups of the sysvol folder are replicated to all domain controllers in the domain. The sysvol folder must be located on an NTFS volume.

3.Explain Functions of Active Directory?

AD enables centralization in a domain environment. The Main purpose of AD is to control and authenticate network resources.

4. What is the name of AD database?

AD database is NTDS.DIT

5. Explain briefly about AD Partition?

The Active Directory database is logically separated into directory partitions:

Schema Partition: Only one schema partition exists per forest. The schema partition is stored on all domain controllers in a forest. The schema partition contains definitions of all objects and attributes that you can create in the directory, and the rules for creating and manipulating them. Schema information is replicated to all domain controllers in the attribute definitions.

Configuration Partition: There is only one configuration partition per forest. Second on all domain controllers in a forest, the configuration partition contains information about the forest-wide active directory structure including what domains and sites exist, which domain controllers exist in each forest, and which services are available. Configuration information is replicated to all domain controllers in a forest.

Domain Partition: Many domain partitions can exist per forest. Domain partitions are stored on each domain controller in a given domain. A domain partition contains information about users, groups, computers and organizational units. The domain partition is replicated to all domain controllers of that domain. All objects in every domain partition in a forest are stored in the global catalog with only a subset of their attribute values.

Application Partition: Application partitions store information about application in Active Directory. Each application determines how it stores, categorizes

partition contains information about users, groups, computers and organizational units. The domain partition is replicated to all domain controllers of that domain. All objects in every domain partition in a forest are stored in the global catalog with only a subset of their attribute values.

Application Partition: Application partitions store information about application in Active Directory. Each application determines how it stores, categorizes, and uses application specific information. To prevent unnecessary replication to specific application partitions, you can designate which domain controllers in a forest host specific application partitions. Unlike a domain partitions, an application partition cannot store security principal objects, such as user accounts. In addition, the data in an application partition is not stored in the global catalog.

6. Explain different zone involved in DNS Server?

DNS has two different Zones Forward Lookup Zone and Reverse Lookup Zone. There two Zones are categorized into three zones and are as follows

Primary zone: It contains the read and writable copy of the DNS Database.

Secondary Zone: It acts as a backup for the primary zone and contains the read only copy of the DNS database.

Stub zone: It is also read-only like a secondary zone; stub zone contains only SOA, copies of NS and A records for all name servers authoritative for the zone.

7. Explain Briefly about Stub Zone?

It is also read-only like a secondary zone, so administrators can't manually add, remove, or modify resource records on it. But secondary zones contain copies of all the resource records in the corresponding zone on the master name server; stub zones contain only three kinds of resource records:

A copy of the SOA record for the zone.

Copies of NS records for all name servers authoritative for the zone.

Copies of A records for all name servers authoritative for the zone.

8. Explain File Replication Service (FRS).

File Replication Service is a Microsoft service which replicates folders stored in sysvol shared folders on domain controllers and distributed file system shared folders. This service is a part of Microsoft's Active Directory Service.

9. What is authoritative and non-authoritative restore?

9. What is authoritative and non-authoritative restore?

Nonauthoritative restore: When a nonauthoritative restore is performed, Active Directory is restored from backup media on the domain controller. This information is then updated during replication from the other domain controllers. The nonauthoritative restore method is the default method to restore system state data to a domain controller.

Authoritative restore: In an authoritative restore, Active Directory is installed to the point of the last backup job. This method is typically used to recover Active Directory objects that were deleted in error. An authoritative restore is performed by first performing a nonauthoritative restore, and then running the Ntdsutil utility prior to restarting the server. You use the Ntdsutil utility to indicate those items that are authoritative. Items that are marked as authoritative are not updated when the other domain controllers replicate to the particular domain controller.

10. What is the replication protocol involved in replication from PDC and ADC?

Normally Remote Procedure Call (RPC)is used to replicate data and is always used for intrasite replication since it is required to support the FRS. RPC depends on **IP** (internet protocol) for transport.
Simple Mail Transfer Protocol (SMTP)may be used for replication between sites.

11. What are the benefits of AD integrated DNS?

A few advantages that Active Directory-integrated zone implementations have over standard primary zone implementations are:

Active Directory replication is faster, which means that the time needed to transfer zone data between zones is far less.

The Active Directory replication topology is used for Active Directory replication, and for Active Directory-integrated zone replication. There is no longer a need for DNS replication when DNS and Active Directory are integrated.

Active Directory-integrated zones can enjoy the security features of Active Directory.

The need to manage your Active Directory domains and DNS namespaces as separate entities is eliminated. This in turn reduces administrative overhead.

When DNS and Active Directory are integrated; the Active Directory-integrated zones are replicated, and stored on any new domain controllers automatically. Synchronization takes place automatically when new domain controllers are deployed.

12. Explain some types of DNS records?

12. Explain some types of DNS records?

A Record: Binds an Name with an IP Address
PTR Record: Binds an IP Address with an Host Name
NS Record: Is name of an DNS Server
MX Record: Responsible for Mail receiving mail from different MTA

13. How many tables are there in NTDS.DIT?

The Active Directory ESE database, NTDS.DIT, consists of the following tables:

Schema table
the types of objects that can be created in the Active Directory, relationships between them, and the optional and mandatory attributes on each type of object. This table is fairly static and much smaller than the data table.

Link table
contains linked attributes, which contain values referring to other objects in the Active Directory. Take the Member Of attribute on a user object. That attribute contains values that reference groups to which the user belongs. This is also far smaller than the data table.

Data table
users, groups, application-specific data, and any other data stored in the Active Directory. The data table can be thought of as having rows where each row represents an instance of an object such as a user, and columns where each column represents an attribute in the schema such as Given Name.

14. What is the purpose of the command NETDOM?

NETDOM is a command-line tool that allows management of Windows domains and trust relationships. It is used for batch management of trusts, joining computers to domains, verifying trusts, and secure channels.

15. What is REPADMIN?

This command-line tool assists administrators in diagnosing replication problems between Windows domain controllers. Administrators can use Repadmin to view the replication topology (sometimes referred to as RepsFrom and RepsTo) as seen from the perspective of each domain controller.

16. What is the purpose of the command repmon?

16. What is the purpose of the command repmon?

Replmon displays information about Active Directory Replication.

17. How will take backup of registry using NTBACKUP?

Using System State.

18. Explain briefly about Super Scope.

Using a super scope, you can group multiple scopes as a single administrative entity. With this feature, a DHCP server can: Support DHCP clients on a single physical network segment (such as a single Ethernet LAN segment) where multiple logical IP networks are used. When more than one logical IP network is used on each physical subnet or network, such configurations are often called multinets.

19. Explain how client obtain IP address from DHCP Server?

It's a four-step process consisting of (a) IP request, (b) IP offer, (c) IP selection and (d) acknowledgement.

20. Explain about SRV Record.

For mapping a DNS domain name to a specified list of DNS host computers that offer a specific type of service, such as Active Directory domain controllers.

21. What are the advantages of having RAID 5?

Strip set with Distributed Parity. Fault Torrance. 100% Data guarantee.

22. How client are get authenticated with Active Directory Server?

Using PDC Emulator roles involved in FSMO.
If you create same user name or Computer name, AD through an error that the object already exists, Can you explain how AD identifies the existing object?
Using RID Master roles involved in FSMO.

23. How will verify Active Directory successful installation?

Check DNS services and errors, check for domain name resolution, check for RPC, NTFRS, DNS and replication related errors

Check DNS services and errors, check for domain name resolution, check for RPC, NTFRS, DNS and replication related errors

24. Group Policy file extension in Windows 2003 Server

*.adm files

25. What is Global Catalog?

Global Catalog is a server which maintains the information about multiple domains with trust relationship agreement. The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory forest.

26. What is Active Directory schema?

The Active Directory schema contains formal definitions of every object class that can be created in an Active Directory forest it also contains formal definitions of every attribute that can exist in an Active Directory object.

27. What is a site?

one or more well-connected highly reliable and fast TCP/IP subnets. A site allows administrator to configure active directory access and replication topology to take advantage of the physical network.

28. What is the file that's responsible for keep all Active Directory database?

Schema master.

29. What is the ntds.dit file default size?

40Mb

30. What's the difference between local, global and universal groups?

Domain local groups assign access permissions to global domain groups for local domain resources. Global groups provide access to resources in other trusted domains. Universal groups grant access to resources in all trusted domains.

trusted domains. Universal groups grant access to resources in all trusted domains.

31. I am trying to create a new universal user group. Why can't I?

Universal groups are allowed only in native-mode Windows Server 2003 environments. Native mode requires that all domain controllers be promoted to Windows Server 2003 Active Directory.

32. What is LSDOU?

Its group policy inheritance model, where the policies are applied to Local machines, Sites, Domains and Organizational Units.

33. What is the command used to change computer name, Make Client Member of Domain?

Using the command netdom

34. Difference between SID and GUID?

A security identifier (SID) is a unique value of variable length that is used to identify a security principal or security group in Windows operating systems. Well-known SIDs are a group of SIDs that identify generic users or generic groups. Their values remain constant across all operating systems.

35. Explain FSMO in Details.

In a forest, there are at least five FSMO roles that are assigned to one or more domain controllers. The five FSMO roles are:
Schema Master: The schema master domain controller controls all updates and modifications to the schema. To update the schema of a forest, you must have access to the schema master. There can be only one schema master in the whole forest.

Domain naming master: The domain naming master domain controller controls the addition or removal of domains in the forest. There can be only one domain naming master in the whole forest.

Infrastructure Master: The infrastructure is responsible for updating references from objects in its domain to objects in other domains. At any one time, there can be only one domain controller acting as the infrastructure master in each domain.

Relative ID (RID) Master: The RID master is responsible for processing RID pool requests from all domain controllers in a particular domain. At any one time, there can be only one domain controller acting as the RID master in the domain.

Relative ID (RID) Master: The RID master is responsible for processing RID pool requests from all domain controllers in a particular domain. At any one time, there can be only one domain controller acting as the RID master in the domain.

PDC Emulator: The PDC emulator is a domain controller that advertises itself as the primary domain controller (PDC) to workstations, member servers, and domain controllers that are running earlier versions of Windows.

36. Which service is responsible for replicating files in SYSVOL folder?

File Replication Service (FRS)

37. Can you Move FSMO roles?

Yes, moving a FSMO server role is a manual process, it does not happen automatically. But what if you only have one domain controller in your domain? That is fine. If you have only one domain controller in your organization then you have one forest, one domain, and of course the one domain controller. All 5 FSMO server roles will exist on that DC. There is no rule that says you have to have one server for each FSMO server role.

38. What permissions you should have in order to transfer a FSMO role?

Before you can transfer a role, you must have the appropriate permissions depending on which role you plan to transfer:
Schema Master - member of the Schema Admins group

Domain Naming Master - member of the Enterprise Admins group

PDC Emulator - member of the Domain Admins group and/or the Enterprise Admins group

RID Master - member of the Domain Admins group and/or the Enterprise Admins group

Infrastructure Master - member of the Domain Admins group and/or the Enterprise Admins group

39. How to restore Group policy setting back to default?

The following command would replace both the Default Domain Security Policy and Default. Domain Controller Security Policy. You can specify Domain or DC instead of both, to onlyrestore one or the other.> dcgpofix /target: Both

40. What is caching only DNS Server?

When DNS is installed, and you do not add or configure any zones for the DNS server, the DNS server functions as a caching-only DNS server by default.

40. What is caching only DNS Server?

When DNS is installed, and you do not add or configure any zones for the DNS server, the DNS server functions as a caching-only DNS server by default. Caching-only DNS servers do not host zones, and are not authoritative for any DNS domain. The information stored by caching-only DNS servers is the name resolution data that the server has collected through resolving name resolution queries.

41. By Default how many shares in SYSVOL folder?

By default, a share with the domain name will be there under the SYSVOL folder.

Under the domain name share, two folders named Policies & Scripts will be there.

42. Zone not loaded by DNS server. How you troubleshoot?

Need to check Zone Transfer is enabled for all DNS Servers.

Also check the required Name Server has been added in the Authoritative Name Server Tab in DNS properties.

43. What is LDAP?

LDAP (lightweight directory access protocol) is an internet protocol which Email and other services is used to look up information from the server.

44. What is ADSIEDIT?

ADSIEdit is a Microsoft Management Console (MMC) snap-in that acts as a low-level editor for Active Directory. It is a Graphical User Interface (GUI) tool. Network administrators can use it for common administrative tasks such as adding, deleting, and moving objects with a directory service.

45. What are application partitions? When do I use them?

AN application directory partition is a directory partition that is replicated only to specific domain controller. Only domain controller running windows Server 2003 can host a replica of application directory partition. Using an application directory partition provides redundancy, availability or fault tolerance by replicating data to specific domain controller pr any set of domain controllers anywhere in the forest.

46. How do you create a new application partition?

46. How do you create a new application partition?

Use the DnsCmd command to create an application directory partition.

47. Why WINS server is required

Windows Internet Naming Service (WINS) is an older network service (a protocol) that takes computer names as input and returns the numeric IP address of the computer with that name or vice versa.

48. What is the purpose of the command ntdsutil?

To transfer or seize FSMO Roles.

49. Explain Forest Functional Level in Windows 2003 Server.

50. Explain Domain Functional Level in Windows 2003 Server.

51. How will you extend schema database?

52. What is the purpose of adprep command?

53. Briefly explain about netlogon?

54. What are forwarders in DNS server?

55. Explain about root hints.

56. Explain types of DNS queries?

57. How you will defragment AD Database?

Windows Administrator L1 Interview Question

1. What is the different between Workgroup and Domain? Domain Server has Centralized Control Where else Workgroup has no Centralized Control

Domain Network has higher level of security when compared to Workgroup.

Domain Network Implementation and Maintained cost is very less when compared to that of workgroup.

Time constrain is very less when compared to that of a Workgroup.

Administrator has overall control on the network where else workgroup has no control.

2. How will assign Local Administrator rights for domain user?

Navigate to Local User and Groups add the domain users to administrators group in the local system.

3. How will you restrict user logon timing in domain?

Navigate to Active Directory Users and Computers, User Properties select logon times and restrict the user logon timing as needed.

4. What is the purpose of sysvol?

The sysvol folder stores the server's copy of the domain's public files. The contents such as group policy, users, and groups of the sysvol folder are replicated to all domain controllers in the domain. The sysvol folder must be located on an NTFS volume.

5. What is OU? Explain its Uses.

Organization Unit is set of active directory object within a domain. It is used to design an organization structure, Restrict user’s visibility and to delegate control.

6. Explain different edition of windows 2003 Server?

Windows Server 2003, Standard Edition: - is aimed towards small to medium sized businesses. Standard Edition supports file and printer sharing, offers secure Internet connectivity, and allows centralized desktop application deployment.

secure Internet connectivity, and allows centralized desktop application deployment.

Windows Server 2003, Enterprise Edition: - is aimed towards medium to large businesses. It is a full-function server operating system that supports up to eight processors and provides enterprise-class features and support for up to 32 GB of memory.

Windows Server 2003, Web Edition: - is mainly for building and hosting Web applications, Web pages, and XML Web Services.

Windows Server 2003, Datacenter Edition: - is the flagship of the Windows Server line and designed for immense infrastructures demanding high security and reliability.

7. What is DNS Server?

Domain Name System is used to resolve domain name to IP Address and also used to resolve IP Address to Domain Name. It has two zones Forward and Reverse Lookup Zone. Forward Lookup Zone resolve Domain name to IP address. Reverse Lookup Zone is used to resolve IP address to Domain Name. Some records associate with DNS

A Record binds Name with IP Address

PTR Record binds IP Address to Name

8. Why DNS server is required for Active Directory?

The key reason for integrating DNS with AD is that client server communication takes place with Domain Name. Network needs IP address to reach the destination; In order to resolve Domain Name to IP Address we need DNS Server. If DNS Server is not configured properly the network becomes slow.

9. What is the Purpose of A and PTR Record?

A Record OR Host Record is used to bind a Name with IP Address.

PTR Record is used to bind an IP Address with Name

PTR Record is used to bind an IP Address with Name.

10. What is the purpose of DHCP Server?

DHCP Server is used to assign IP address automatically to all the clients' computers. It is useful in large enterprise network, where we may not able track the IP address and also used to avoid IP conflict.

11. Explain about Scope in DHCP Server?

Scope is collective information of assigning IP address for clients. It contains information like IP Address Range, Exclusion Range, Lease Period, Reservation, Router IP Address, DNS Address, etc. Based on the scope configuration DHCP allocates IP address to its entire client.

12. Explain about Group Scopes?

13. How will you backup DNS Server?

Backup the directory "%System Root%\System32\DNS".

14. How will backup DHCP Server?

First Method: Backup the directory in the %System Root%\System32\DHCP folder.

Alternate method: Open DHCP Console select server to backup and restore DHCP database.

15. Explain APIPA.

A Windows-based computer that is configured to use DHCP can automatically assign itself an Internet Protocol (IP) address if a DHCP server is not available or does not exist. The Internet Assigned Numbers Authority (IANA) has reserved 169.254.0.0-169.254.255.255 for Automatic Private IP Addressing (APIPA).

16. Explain about AD Database.

Windows 2003 Active Directory data store, the actual database file, is %System Root%\NTDS\NTDS.DIT. AD Database all information such as User Accounts, Groups, Computer Information, Domain Controller information, Group Policy, Organization Unit,etc.

17. Explain about Group Policy.

Group policies are used by administrators to configure and control user environment settings. Group Policy Objects (GPOs) are used to configure group

17. Explain about Group Policy.

Group policies are used by administrators to configure and control user environment settings. Group Policy Objects (GPOs) are used to configure group policies which are applied to sites, domains, and organizational units (OUs) .There is a maximum of 1000 applicable group policies.

18. What is the default time for group policy refresh interval time?

The default refresh interval for policies is 90 minutes. The default refresh interval for domain controllers is 5 minutes. Group policy object's group policy refresh intervals may be changed in the group policy object.

19. Explain Hidden Share.

Hidden or administrative shares are share names with a dollar sign ($) appended to their names. Administrative shares are usually created automatically for the root of each drive letter. They do not display in the network browse list.

20. What ports are used by DHCP and the DHCP clients?

Requests are on UDP port 68, Server replies on UDP 67.

21. How do I configure a client machine to use a specific IP Address?

By reserving an IP Address using client machine MAC or Physical address.

22. Name 3 benefits of using AD-integrated zones.

AD Integrated Zones allow Secure Dynamic Updates. I.e. there will not be any duplicate or unwanted records. Since all the information are validated in active directory.

By creating AD- integrated zone you can also trace hacker and spammer by creating reverse zone.

AD integrated zones are stored as part of the active directory and support domain-wide or forest-wide replication through application partitions in AD.

23. How do you backup & Restore AD?

Using Windows NTBackup Utility. In Backup select systemstate will include active directory backup. Restore the Same using NTBackup Utility.

Using Windows NTBackup Utility. In Backup select systemstate will include active directory backup. Restore the Same using NTBackup Utility.

24. How do you change the DS Restore admin password?

Using NTDSUTIL tool.

25. How can you forcibly remove AD from a server?

Using the command dcpromo /forceremoval

26. What will be the problem if DNS Server fails?

If your DNS server fails, No Client will able to reach the Domain Controller, which will create authentication and Control Issues.

27. How can you restrict running certain applications on a machine?

The Group Policy Object Editor and the Software Restriction Policies extension of Group Policy Object Editor are used to restrict running certain applications on a machine. For Windows XP computers that are not participating in a domain, you can use the Local Security Settings snap-in to access Software Restriction Policies.

28. What can you do to promote a server to DC?

Using the command dcpromo

29. How will map a folder through AD?

Specify the network share path (UNC) in the active directory users home directory.

30. Explain Quotas.

Disk Quota is a feature or service of NTFS which helps to restrict or manage the disk usage from the normal user. It can be implemented per user user per volume basis.By default it is disabled. Administrative privilege is required to perform the task. In 2003server we can control only drive but in 2008server we can establish quota in folder level.

31. Explain Backup Methodology.

The different types of backup methodologies are:

31. Explain Backup Methodology.

The different types of backup methodologies are:

Normal Backup:-This is default backup in which all files are backed up even if it was backed up before.

Incremental Backup:-In this type of backup only the files that haven't been backed up are taken care of or backed up.

Differential Backup:-This backup is similar to incremental backup because it does not take backup of those files backed up by normal backup but different from incremental because it will take backup of differentially backed up files at next time of differential backup.

System Backup:-This type of backup takes backup of files namely, Boot file, COM+Class Registry, Registry. But in server it takes backup of ADS.

ASR Backup:-This type of backup takes backup of entire boot partition including OS and user data. This should be the last troubleshooting method to recover an os from disaster.

32. Explain how to publish printer through AD.

Navigate to Active Directory Users and Computers, Create new printer and add the printer i.e. the printer share name (UNC) Path. Automatically the printer will be published in Active Directory.

33. Explain the functionality of FTP Server?

File Transfer Protocol is used transfer large volume of files and huge number of files simultaneous between different geographic locations.

34. Specify the Port Number for AD, DNS, DHCP, HTTP, HTTPS, SMTP, POP3 & FTP

AD - 389

DNS - 53

DHCP - 67,68

HTTP - 80

HTTP - 80

HTTPS - 443

SMTP - 25

POP3 - 110

FTP - 21,22

35. Explain Virtual Directory in IIS?

A virtual server can have one home directory and any number of other publishing directories. These other publishing directories are referred to as virtual directories.

36. What is Exclusion Range in DHCP Server?

Exclusion Range is used to hold a range IP addresses. Those IP Address can be used or may not be used in the network, but DHCP server does not assign those IP to its client.

37. Explain SOA Record.

Start Of Authority (SOA) Records indicate that Name Server is authoritative server for the domain.

38. What command is used to clear DNS cache in client PC?

Ipconfig /flushdns

39. Explain Secure Dynamic Updates in DNS Server.

39. Explain Secure Dynamic Updates in DNS Server.

Only when installing active directory and DNS in the same server (AD Integrated Zones) we can select Secure Dynamic Updates. Then all the records will automatically be updated in DNS. Since all the information is validated in active directory there will not be any duplicate or unwanted records.

40. Explain FRS in detail.

File Replication Service is a Microsoft service which replicates folders stored in sysvol shared folders on domain controllers and distributed file system shared folders. This service is a part of Microsoft's active directory service.

41. Explain the protocol involved in ADC replication.

Remote Procedure Call (RPC) is the protocol used in ADC replication.

42. Explain the difference between Patches and Service pack.

Patches are fixes, updates or enhancements for a particular program whereas service packs include a collection of

43. What is WSUS?

WSUS is Windows Software Update Services. It is server provided by Microsoft free of cost to manage patches for windows environment centralized.

44. How client server communication takes place in WSUS server?

Using Web Server or Web Services

45. What is the difference between Dynamic Disk and Basic Disk?

Basic Disk: Basic Disk uses a partition table to manage all partitions on the disk, and it is supported by DOS and all Windows versions. A disk with installed OS would be default initialized to a basic one. A basic disk contains basic volumes, such as primary partitions, extended partition, and all logical partitions are contained in extended partition.

Dynamic Disk: Dynamic Disk is supported in Windows 2000 and later operating system. Dynamic disks do not use a partition table to track all partitions, but use a hidden database (LDM) to track information about dynamic volumes or dynamic partitions on the disk. With dynamic disks you can create volumes that span multiple disks such as spanned and striped volumes, and can also create fault-tolerant volumes such as mirrored volumes and RAID 5 volumes. Compared to a Basic Disk, Dynamic Disk offers greater flexibility.

Compared to a Basic Disk, Dynamic Disk offers greater flexibility.

46. What is maximum Size of file system NTFS and FAT32?

NTFS - 16TB

FAT32 - 4GB

47. What is "hosts" files?

The hosts file is a computer file used in an operating system to map hostnames to IP addresses. The hosts file is a plain-text file and is traditionally named hosts.

48. What is "lmhosts" files?

The lmhosts files are a computer file used in an operating system to map NetBIOS name. It is equivalent that of WINS.

49. Explain About Global Catalog.

global catalog contains a complete replica of all objects in Active Directory for its Host domain, and contains a partial replica of all objects in Active Directory for every other domain in the forest.

50. Name some OU design considerations.

It is used to design an organization structure, Restrict user's visibility and to delegate control.

51. Name a few benefits of using GPMC.

GPMC is used to customize group policy.

It is easy to maintain different OU policy effectively.

Provide option to take backup and restore group policy.

52. You want to standardize the desktop environments (wallpaper, My Documents, Start menu, printers etc.) on the computers in one department. How would you do that?

52. You want to standardize the desktop environments (wallpaper, My Documents, Start menu, printers etc.) on the computers in one department. How would you do that?

Configure Group Policy based on OU.

53. By default, if the name is not found in the cache or local hosts file, what is the first step the client takes to resolve the FQDN name into an IP address?

Create a record in DNS Server

54. You are administering a network connected to the Internet. Your users complain that everything is slow. Preliminary research of the problem indicates that it takes a considerable amount of time to resolve names of resources on the Internet. What is the most likely reason for this?

DNS Issues

55. Describe how the DHCP lease is obtained.

It's a four-step process consisting of (a) IP request, (b) IP offer, (c) IP selection and (d) acknowledgement.

56. I can't seem to access the Internet, don't have any access to the corporate network and on ipconfig my address is 169.254.*.*. What happened?

The 169.254.*.* netmask is assigned to Windows machines running 98/2000/XP if the DHCP server is not available. The name for the technology is APIPA (Automatic Private Internet Protocol Addressing).

57. We've installed a new Windows-based DHCP server, however, the users do not seem to be getting DHCP leases off of it.

The server must be authorized first with the Active Directory.

58. How do you configure mandatory profiles?

Rename ntuser.dat to ntuser.man

59. What is Page File and Virtual Memory?

Page File Is Storage Space For The Virtual Memory, Page File Uses Hard Disk Space As a Memory To Provide Memory Allocation...

Page File Is Storage Space For The Virtual Memory, Page File Uses Hard Disk Space As a Memory To Provide Memory Allocation...

60. What is the difference between DNS in Windows 2000 & Windows 2003 Server?

We can rename or moved the domain name without rebuilding in windows 2003 server, but in windows 2000 server, we can't do that.

61. Where are group policies stored?

%SystemRoot%System32\Group Policy

62. What are GPT and GPC?

Group policy template and group policy container.

63. Where is GPT stored?

%System Root%\SYSVOL\sysvol\domain name\Policies\GUID

64. You change the group policies, and now the computer and user settings are in conflict. Which one has the highest priority?

The computer settings take priority.

65. What hidden shares exist on Windows Server 2003 installation?

Admin$, Drive$, IPC$, NETLOGON, print$ and SYSVOL.

Desktop Administrator Interview Question

1. What is the difference between Windows XP & Windows 7?

Windows Defender, Parental Control, Windows Touch and Tap instead of point and Click, Multiple Active Firewall.

2. One Fine Morning System is not booting up. Explain what would be the problem.

2x2 or 2x4 Power Connector Not Plugged In

Processor Issues

Memory Issues

Monitor Issues

Power Supply and Chassis Issues

Cable Issues

Electrical Short or Overload

Defective Components

Defective Components

3. System No Display. What the steps are to Diagnoses the problem?

Check the monitor is switched on and the power indicator LED of the monitor is glowing. Check the monitor power connection.

Adjust the contrast/brightness knob of the monitor to maximum.

Check whether the monitor is connected properly to the video adapter of the system.

If your system has add-on video adapter, switch off the system and remove the power.

Check whether the CPU, memory are connected properly to the motherboard.

4. System is power on, but beep sound occurs. What would be the problem?

One long beep: Memory problem

One long and two short beeps: Video error

One long and three short beeps: Video error

Continuous beeps: Video/memory problem

Other beeps: Check the motherboard manual

5. Different and NTFS and FAT32.

NTFS

Allows access local to w2k w2k3 XP win NT4 with SP4 & later may get access for some file.

Allows access local to w2k w2k3 xp win NT4 with SP 4 & later may get access for some file.

Maximum size of partition is 2 Terabytes & more.

Maximum File size is up to 16TB.

File & folder Encryption is possible only in NTFS.

FAT 32

Fat 32 Allows access to win 95 98 win millennium win2k xp on local partition.

Maximum size of partition is up to 2 TB.

Maximum File size is up to 4 GB.

File & folder Encryption is not possible.

6. How will you convert FAT32 to NTFS?

To convert a volume to NTFS from the command prompt

Open Command Prompt.

In the command prompt window, type

convert drive_letter: /fs:ntfs

For example, typing convert D: /fs:ntfs would format drive D: with the ntfs format.

For example, typing convert D: /fs:ntfs would format drive D: with the ntfs format.

7. What are primary Partition, Extended Partition and Logical Partition?

A primary partition contains one file system. The first partition (C:) must be a primary partition..

An extended partition is a primary partition which contains *secondary partition(s)*. A hard disk may contain only one extended partition..

Extended partition that is sub divided into many drives is called as Logical partition..

8. In a computer how many primary partition can be held.

Four Primary partitions can be done...

9. Difference between Microsoft outlook and Outlook Express.

Microsoft Outlook:

Files will be saved in .PST Format.

Have some Additional Features like Address Book, Contacts, and Remainderetc...

Not a free product have to purchase it..

Outlook Express:

Files will be saved in .DBX Format.

Don’t have any additional features.

Don't have any additional features.

Free product that comes along with the OS Installation.

10. What is Virus?

Vital Information Resource under Seige.It is an executable Program which Performs Malicious activities in the system.

11. What is Antivirus?

An Antivirus Is a Software that protects the system from Virus Attack..

12. What is the difference between Delete and Quarantine in Action methodology for Virus Scanning?

Delete will delete all the virus infected files and Quarantine create a copy from an infected file and produce a new one..

13. What are the procedures for cleaning an infected virus system?

Unplug the system from the Network if it is in a Network & Scan the System with the Updated Antivirus..

14. What is SMTP Protocol? What is the port Number used by SMTP?

Simple Mail Transfer Protocol which performs all outgoing Mail. The port number is 25.

15. What is POP3 Protocol? What is the port Number used by POP3?

Post Office Protocol which performs all incoming mails. The Port number is 110.

16. Tell me the procedure for Backup and Restore Mail in Outlook Express.

Go to C:\Documents & Setting\User Profile\Application Data\Local Settings\Identities\Outlook Express & Copy the .DBX files and Save it in another location as

16. Tell me the procedure for Backup and Restore Mail in Outlook Express.

Go to C:\Documents & Setting\User Profile\Application Data\Local Settings\Identities\Outlook Express & Copy the .DBX files and Save it in another location as a Backup. Copy the files from the location that was saved as a Backup & Go to the same path & Paste it.

17. Tell me the Procedure for Backup and Restore Mail in Microsoft Express.

Go to C:\Documents & Setting\User Profile\Application Data\Local Settings\Microsoft \Outlook Express & Copy the .PST files and Save it in another location as a Backup..

Copy the files from the location that was saved as a Backup & Go to the same path & Paste it.

18. How will you repair a PST Files?

Using scanpst.exe files

19. How to set Password for PST Files?

Select Go | Folder List from the menu.

Click on the root item of the desired PST file with the right mouse button.

If you want to protect only certain email folders with a password, you can move them to a newly created PST file and assign a password only for that file.

Select Properties for... from the menu.

Click Advanced....

Now click Change Password....

Now click Change Password....

Enter the desired password under both New password: and Verify password:.

If a password had already been set for the PST file, enter that phrase under Old password:.

If you assign a password to a previously unprotected PST file, leave the Old password: field blank.

To remove the password from a PST file, enter it under Old password: and leave both New password: and Verify password: blank.

Click OK.

Click OK again.

Now click Cancel.

20. How to set store a mail copy in Server for 30 days while configuring mail in Microsoft outlook?

Go to Outlook 2007's Tools, Account Settings, and With the Account Settings dialog open, select the account and click Change, then click More Settings. Look on the Advanced tab..

21. How to set Rules in Microsoft outlook in order to organize mailbox?

Open Microsoft Outlook.

Click Tools.

Open Microsoft Outlook.

Click Tools.

Click Rules Wizard.

Click the New button and run through the wizard..

22. Explain about Junk Mail option in outlook.

Low. This level is designed to catch only the most obvious junk e-mail messages. You can make the filter more aggressive, but if you do it may catch legitimate messages sometimes. Any message that is caught by the Junk E-mail Filter is moved to a special **Junk E-mail** folder. You should review messages in the Junk E-mail folder from time to time to make sure that they are not legitimate messages that you want to see.

23. Explain about Registry?

This is a database used by Microsoft Windows to store configuration information about the software installed on a computer. This information includes things like the desktop background, program settings, and file extension associations.

24. How to backup and Restore Registry?

Import and Export from regedit.

25. When system booting "NTLDR file Missing" Error. What would be the solution?

Boot the System from the OS cd and Select Repair Option

26. When XP is booting up system gets restart automatically. What would be the solution?

May be RAM problem so replace it...
Virus would have affected..

May be RAM problem so replace it...
Virus would have affected..

27. Explain about Windows Firewall?

Firewall Restricts the System from Unwanted Traffic.

28. Difference between Administrators and Power Users?

Members of the Administrator group have total control over the computer and everything on it. The user named *Administrator* is the default account within this group

The Power User class can perform any task except for those reserved for Administrators. They are allowed to carry out functions that will not directly affect the operating system or risk security

29. What is Service Pack? Is it needed to be installed in all the system?

A **service pack** (in short **SP**) is a collection of updates, fixes and/or enhancements to a software program delivered in the form of a single installable package.
Yes it should be installed in all the systems.

30. What is Device Drivers? Why it is needed?

A device driver is a program that controls a particular type of device that is attached to your computer. There are device drivers for printers, displays, CD-ROM readers, diskette drives, and so on

31. Explain about Local Printer and Network Printer?

A network printer is shared by more than one computer using the IP Address that is assigned to the printer.
A local printer is directly connected to one computer & shared using sharing & security

32. Explain detail how to install a Network Printer?

 To install the printer using an IP address, go to Start>Control Panel>Printers and Faxes and then click the Add Printer icon. Next, click **Create a new port**,

32. Explain detail how to install a Network Printer?

To install the printer using an IP address, go to Start>Control Panel>Printers and Faxes and then click the Add Printer icon. Next, click **Create a new port**, then select **Standard TCP/IP Port** from the drop-down menu. You will then be asked to enter an IP address. Enter the **IP address** of the print server and click **Next**. You will be asked to select the printer manufacturer and the model from the list. If you do not see your printer listed, insert the disk that came with the printer and click Have Disk.
If you do not know the IP address of the printer, you can sometime select Browse for printer in the beginning of the process. If the networked printer is attached to another computer is being shared, you will need to enter the name of the computer followed by the share name of the printer. For example: \\computername\printername**.**

33. How does virus get loaded into computer?

Through Exe Files, Pen drive, CD, E-mail, Internet Etc...

34. What is Boot Process in a computer?

First is the POST, this stands for Power On Self-Test, for the computer. This process tests memory as well as a number of other subsystems. You can usually monitor this as it runs each test. After that is complete the system will run POST for any device that has BIOS (Basic Input-Output System).

35. What is the difference between RAM & ROM?

RAM – Random Access Memory which is called as Temporary Memory..
ROM- Read Only Memory which stores the data Permanently.

36. What is Cache Memory?

Cache memory is fast memory that is used to hold the most recently accessed data in slower main memory. The idea is that frequently accessed data will stay in cache, which allows the CPU to access it more quickly, which means it doesn't have to wait for the data to arrive.

37. What is the difference between Primary Storage and Secondary Storage?

Usually the primary storage is a hard drive(s). Secondary is a flash drive(s), cd and so on. But nowadays, it's mostly a game of words.

The primary memory of CPU is the place where computer program and data is stored during processing. this storage unite is often called either main

The primary memory of CPU is the place where computer program and data is stored during processing. this storage unite is often called either main memory or primary memory..

There is usually two types primary memory

1. RAM 2:.ROM
The devices of computer that store information such as software and data permanently are called secondary storage device.

There are many types of secondary storage devices such as ,magneticdisk, Hard disk floppy disk , CD Rom , magnetic tape etc...

38. How to increase or set virtual memory in Window XP?

Click Start, and then click Control Panel.

ClickPerformance and Maintenance, and then click System.

On the Advanced tab, under Performance, click Settings.

On the Advanced tab, under Virtual memory, click Change.

UnderDrive [Volume Label], click the drive that contains the paging file that you want to change.

UnderPaging file size for selected drive, click to Custom size check box. You can enter the amount of memory you would like to reserve for Virtual memory by entering the initial and maximum size. ClickSet

39. What are the advantages of having SATA HDD over PATA HDD?

39. What are the advantages of having SATA HDD over PATA HDD?

SATA HDD uses different channel for incoming and outgoing traffic. Wherelse PATA HDD uses same Channel for incoming and outgoing traffic.

40. What are Bidirectional and Unidirectional Bus?

The address bus (sometimes called the memory bus) transports memory addresses which the processor wants to access in order to read or write data. It is a unidirectional bus.
The data bus transfers instructions coming from or going to the processor. It is a bidirectional bus.

41. How does the browser know to go to a certain IP address when you enter a domain like google.com?

Whenever an address is typed on the browser it immediately connects with the DNS.This DNS Finds the IP address related to the Domain & connects with the Server & the requested web page will be displayed.

42. What's the difference between L1 and L2 cache?

Short for Level 1 cache, a memory cache built into the microprocessor.

Short for Level 2 cache, cache memory that is external to the microprocessor. In general, L2 cache memory, also called the secondary cache, resides on a separate chip from the microprocessor chip.

43. What is BIOS? How to clear password for BIOS?

BIOS or Basic Input/output System is the first program accessed by the processor during start up to ensure that all the other basic programs, hard drives, ports, peripherals and the central processing unit are in good working condition.
In order to clear the password for BIOS Just Remove the CMOS Battery & Insert it again after Sometime or Change the Jumper Settings.

44. What difference between original motherboard & chipset motherboard?

A chipset is a group of microchips designed to work as a unit in performing one or more related functions.
They are chip or chips on a motherboard containing various functions supporting the CPU.

Motherboard is the "heart" of your PC -- it handles system resources (IRQ lines, DMA channels, I/O locations), as well as core components like the CPU, and

Motherboard is the "heart" of your PC -- it handles system resources (IRQ lines, DMA channels, I/O locations), as well as core components like the CPU, and all system memory. It accepts expansion devices such as sound and network cards, and modems. The main printed circuit board in a computer that carries the system buses. It is equipped with sockets to which all processors, memory modules, plug-in cards, daughterboard, or peripheral devices are connected.

45. What is the SMPS? Explain about its output voltage?

Switch Mode Power Supply is an electronic power supply Unit that incorporates a switching regulator in order to provide the required output voltage

46. What is Power Good Signal? Explain its functionality.

In addition to the voltages and currents that a computer needs to operate, power supplies also provide a signal called the **Power-Good signal**, sometimes written as *Power_OK* or *Power Good* or you can distinguish it by its gray color. Its purpose is to tell the computer all is well with the power supply and that the computer can continue to operate normally. If the Power-Good signal is not present at startup, the CPU is held in reset state. If a Power-Good signal goes down during operation the CPU will shutdown. The Power-Good signal prevents the computer from attempting to operate on improper voltages and damaging itself.

47. What is the difference between AGP and PCI graphics cards?

AGP stands for 'Accelerated Graphics Port' the speed at which the AGP bus transfers data to and from the video card was too Fast.
PCI stands for 'Peripheral Component Interconnect' the speed at which the PCI bus transfers data to and from the video card was too Slow.

48. While Installing Windows XP File Missing Error Occurs. What would be the Problem?

If you are attempting to boot from a CD-ROM and are receiving this error message it is likely that the diskette does not have all the necessary files and/or is corrupt.

49. What is Defragmentation? Why it's needed?

Defragmentation is a process that reduces the amount of fragmentation in file systems. It does this by physically organizing the contents of the disk to store the pieces of each file close together and contiguously.

50. One fine morning system is not able to login into domain. What could be the problem?

50. One fine morning system is not able to login into domain. What could be the problem?

May be Network problem.

Password would have expired.

May be some restriction policy applied.

51. In a workgroup environment how many system can access a shared folder simultaneously.

10 Systems

52. What is command to view computer name?

Ipconfig /all or hostname

53. Explain Ping command in detail.

Packet Internet Gopher is a simple command line network tool that you can use to verify your connectivity to a network.

54. What would the problem if system gets restarted frequently?

RAM problem, Virus Attack, Dust in processor FAN.

55. What would the problem if the system gets hanged off?

RAM problem,OS Corrupt,Virus Attack,Hard Disk Problem.

56. What could be the problem if hard disk gets in problem?

Disk boot failure, Hard Disk not detected, CableProblem, BlueScreen, No power supply, Bad Sectors.

57. What is msconfig? Why it is used?

57. What is msconfig? Why it is used?

Microsoft System Configuration Utility is a utility to troubleshoot the Windows startup process.

58. What is Remote Desktop? Why it is used?

Remote Desktop is used to take another network system remotely Remote desktop allows you to control the desktop and, indeed, the entire contents of a computer from another machine entirely

59. How to run legacy application in windows xp?

In both XP , right click on the executable of the application you wish to run.
Select "Properties".

Select the "Compatibility" tab on the "Properties" dialogue box.

There will be a number of options. Choose "Windows 95 or 98 compatibility mode"

60. What is the command to shutdown and restart the computer?

Shutdown –s –t 00

61. What is system restore? Why it is used?

System Restore helps you restore your computer's system files to an earlier point in time. It's a way to undo system changes to your computer without affecting your personal files, such as email, documents, or photos.

62. What is Ghost?

Ghost is a software product from Symantec that can clone (copy) the entire contents of a hard disk to another computer's hard disk or to storage media, automatically formatting and partitioning the target disk. This product is especially useful where one system is to be replicated on a number of computers or when someone wants to back up everything on their personal computer.

63. Difference between Public and Private IP?

63. Difference between Public and Private IP?

Check systemadministrator.in Website

64. Difference between Windows Vista and Windows 7?

Check systemadministrator.in Website

65. Difference between Core2duo and Dual Core Processor?

Check systemadministrator.in Website

66. Difference between Core i3, Core i5 & Core i7?

Check systemadministrator.in Website

67. How will you deploy Windows XP or Windows 7 in 100 Computers simultaneously?

Using SCCM (System Center Configuration Manager), MDT (Microsoft Deployment Toolkit), WDS (Windows Deployment Services) tools

68. How will update patches or Service pack in multiple computers?

Using WSUS (Windows Software Update Service) tool.

69. Which are the tools you use for remote support?

Dame Ware, Remote Assistance, Remote Desktop, Ammy Admin

70. What is bitlocker?

BitLocker lets you encrypt the hard drive(s) on your Windows 7 and Vista Enterprise, Windows 7 and Vista Ultimate or Windows Server 2008 and R2.

71. What are Host & LMHosts Files?

Host File: Windows Internet Explorer is set to automatically take instructions from a special file that can be found as part of the default installation of the Operating system.Windows XP it is in C:\WINDOWS\SYSTEM32\DRIVERS\etc
LMHOSTS:LMHOSTS file is for LAN Manager name resolution with the TCP/IP protocol. The file is similar in format to the HOSTS file, but its function is to resolve IP addresses for a server that is not on the local subnet (the same wire)

72. Difference between 32 bit and 64bit OS Versions?

73. What are Ping and Traceroute?

Ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer.Traceroute is a utility that records the route (the specific gateway computers at each hop) through the Internet between your computer and a specified destination computer. It also calculates and displays the amount of time each hop took.

74. How can recover a file encrypted using EFS?

Use Domain Recovery Agents

74. How can recover a file encrypted using EFS?

Use Domain Recovery Agents

75. What is telnet?

Telnet is a protocol that allows you to connect to remote computers (called hosts) over a TCP/IP network (such as the Internet).

76. What is VPN?

A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. Large corporations, educational institutions, and government agencies use VPN technology to enable remote users to securely connect to a private network

77. Difference between Hub and Switch?

78. How will you fine tune OS?

Clean tmp Files, Run Defragmentation, Run Scan Disk, Disk Cleanup, Check for Antivirus, Increase system virtual memory,

79. Difference between Safe and Normal mode?

Safe mode is an alternate boot method for Windows operating systems that makes it easier to diagnose problems. The only startup programs loaded are the operating system and drivers for the mouse, keyboard, and display modes display.

80. BSOD. Blue screen on Death

Security Administrator Level 1 Question

1. What is a Firewall?

Firewall is a device will acts as security layer for all incoming and outgoing traffic for a network

2. What is a gateway?

Gateway is entry and exit point for a network.

3. Will firewall acts as a gateway?

Yes

4. What are the basic configurations you do while configuring a new firewall?

Configure LAN Network in the firewall

Configure WAN Network in the firewall

Write policies to allow internet, mail, etc.

5. What is all the firewall you handle?

Fortigate, Juniper, Sonicwall

6. Explain few Fortigate firewall model?

40c, 60c, 110c, 210b

7. Explain few sonic wall firewall model?

NSA 240, NSA 2400, TZ Series

8. Explain few juniper firewall model?

SSG Model, SRX Models

9. What is Firmware version in Fortigate?

Fortios 4.0 or Fortios 5.0

10. What is Firmware version in Sonic Wall?

Sonicos 5.0

11. What is Firmware version in Juniper?

Junos 11.0

12. How do mange firewall remotely?

By enabling HTTP or HTTPS access to wan interface

13. What is a difference between Proxy & Firewall?

Proxy server will never acts a gateway devices but firewall acts as gateway devices

13. What is a difference between Proxy & Firewall?

Proxy server will never acts a gateway devices but firewall acts as gateway devices

14. What is NAT?

Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.

15. Explain Different types of NAT?

Source NAT, Destination NAT, Static NAT

16. Tell the port no for the following

HTTP – 80, HTTPS – 443, FTP – 20 & 21, RDP – 3389,SSH - 22,IMAP-143,SMTP – 25,POP3 – 110,MSSQL – 1433,LDAP – 389

17. Describe in general how you manage a firewall.

Configuring firewall to acts a gateway device

Configure firewall for Load balancing/Failover with two ISP's

Configure firewall for writing LAN to WAN & WAN to LAN Policies

Configure firewall for UTM Feature

Configure firewall as VPN Server

Monitor Network traffic and log

18. What are the different types of Policy can be configured in firewall?

LAN to LAN Policy, LAN to WAN Policy, WAN to LAN Policy

19. Can we set time based policy in firewall?

Yes

20. What is the difference between router ACLs and Firewall Polices?

21. What is DMZ?

DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

22. Explain a scenario in which situation we plan for DMZ?

Server or separate Networks

23. Is it possible to terminate more than two ISP's in a firewall?

Yes

24. What is UTM?

Unified Threat Management indicates you get a security solution with Anti Spam, Anti Virus, Web Filtering, Web Proxy, Mail Proxy, Content Filtering, VPN and Firewall.

24. What is UTM?

Unified Threat Management indicates you get a security solution with Anti Spam, Anti Virus, Web Filtering, Web Proxy, Mail Proxy, Content Filtering, VPN and Firewall.

25. Explain about gateway antivirus?

A feature of network security appliances that provides integrated antivirus security on the appliance to block potential threats before reaching the network. Gateway antivirus allows corporate and enterprise to check for viruses at the application layer using a web-based scanning service.

26. What is web filter?

Web filter is a feature in firewall to block website based on category (jobs, Politics, Web Based Email, etc…), from database provided by the firewall product vendor.

27. How web filter works?

Web Filter works with license provided by firewall, Web filter works if the firewall is able to communicate with web filter database server provided by the firewall vendor.

28. How Application filter works?

Application filter is same as web filter to block unwanted application getting access using the common service like HTTP, HTTPS, etc…

29. What is denial of Service attack?

Denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks.

30. What is vulnerability test and how to you perform the test?

Vulnerability test is a penetration test to find all the security issues in the Network, based on the test we can take action. Tools to test vulnerability is Nessus, Openvas

31. What is zero day attack prevention?

The implications of a Zero-Day attack are that the software vendors can't address the vulnerability and patch the software prior to the vulnerability's exposure. When a Zero-Day attack gets exposed along with a newly-discovered vulnerability, it may take several weeks or months for the software vendors to create a patch. In the meantime, each computer that carries the vulnerable software is exposed to the attack.

32. Is it possible to configure firewall for User Authentication for Internet Access? Explain how

Yes, using Identity based polices

33. Explain IPS / IDS?

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Intrusionpreventionsystem is used in computer security. It provides policies and rules for network traffic along with an intrusion detection system for alerting

Intrusionpreventionsystem is used in computer security. It provides policies and rules for network traffic along with an intrusion detection system for alerting system or network administrators to suspicious traffic, but allows the administrator to provide the action upon being alerted. Some compare an IPS to a combination of IDS and an application layer firewall for protection.

34. Explain the difference between trusted and untrusted networks?

Trusted network is protected network i.e. LAN where else untrusted network is open network i.e. WAN

35. What is the difference between IPsec and SSL VPN?

Traditional VPN's rely on IPsec (Internet Protocol Security) to tunnel between the two endpoints. IPsec works on the Network Layer of the OSI Model-securing all data that travels between the two endpoints without an association to any specific application.

SSL is a common protocol and most web browsers have SSL capabilities built in. Therefore almost every computer in the world is already equipped with the necessary "client software" to connect to an SSL VPN.

36. What is site to site VPN?

Site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations.

37. What is SSL?

Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.

38. How do we create SSL Certificate?

We can create SSL Certificate using Certificate Server or with service providers like godaddy, etc.

39. What is the advantage of having SSL VPN over IPsec?

SSL VPN's have been gaining in prevalence and popularity; however they are not the right solution for every instance. Likewise, IPsec VPN's are not suited for every instance either.

40. What are the different types of VPN?

IPsec, SSL, PPTP, L2TP

41. What requirements should a VPN fulfill?

VPN Devices, VPN Encryption and VPN Components.

42. How many ways are there to implement VPN architecture?

43. What are the different ways authentication mechanisms in VPN?

EAP authentication method, MS Chap Authentication method, unencrypted passwords (PAP), Shiva Password Authentication Protocol (SPAP)

43. What are the different ways authentication mechanisms in VPN?

EAP authentication method, MS Chap Authentication method, unencrypted passwords (PAP), Shiva Password Authentication Protocol (SPAP)

44. Explain the basic of encryption in VPN?

VPN can optionally use encryption. Traditionally it use IPSEC with an encryption method such as AES or 3DES. Encryption takes a plain text and a key and then applies an algorithm to produce a ciphertext. The keys can be static or negotiated.

45. Explain different components in PKI?

A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

46. Explain tunneling?

A technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

47. Can you explain static and dynamic tunnels?

Static Tunnel: The manually created tunnels are called Static Tunnels. Static tunnels creation is the only choice when global discovery of hosts and tunnel partners are disabled by enhancing Xpress tunnels into manually created tunnels. The priority is higher when compared with static tunnel.

Dynamic Tunnel: The tunnels that are auto-discovered are known as dynamic tunnels. Dynamic tunnels are created quickly and automatically after the Packet Shaper is reset. At the time of preventing automatic tunnel, dynamic tunnels are allowed to setup the situation.

48. Provide an overview of various components in IPsec?

IPsec contains the following elements:

Encapsulating Security Payload (ESP): Provides confidentiality, authentication, and integrity.

Authentication Header (AH): Provides authentication and integrity.

Internet Key Exchange (IKE): Provides key management and Security Association (SA) management.

49. Describe the Authentication Header (AH) Protocol?

Authentication Header (AH) is a member of the IPsec protocol suite. AH guarantees connectionless integrity and data origin authentication of IP packets. Further, it can optionally protect against replay attacks by using the sliding window technique and discarding old packets

50. What is ESP (Encapsulating Security Payload)?

Encapsulating Security Payload (ESP) is a member of the IPsec protocol suite. In IPsec it provides origin authenticity, integrity, and confidentiality protection of packets. ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure.

protection of packets. ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure.

51. What is Transport and Tunnel mode?

IPsec can be run in either tunnel mode or transport mode. Each of these modes has its own particular uses and care should be taken to ensure that the correct one is selected for the solution:

Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.

Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host

52. Explain IKE (Internet Key Exchange)

Internet Key Exchange (IKE) is an IPsec (Internet Protocol Security) standard protocol used to ensure security for virtual private network (VPN) negotiation and remote host or network access.The IKE protocol ensures security for Security Association (SA) communication without the preconfiguration that would otherwise be required.

53. Explain IKE phases?

IKE phase 1. IKE authenticates IPsec peers and negotiates IKE SAs during this phase, setting up a secure channel for negotiating IPsec SAs in phase 2.

IKE phase 2. IKE negotiates IPsec SA parameters and sets up matching IPsec SAs in the peers.

54. Explain IKE modes

Main Mode&Aggressive Mode

55. Explain the features and model of the firewall in your organization?

56. What is your vision for organization security?

57. Tell me how firewall is placed in your organization?