CompTIA® Server+ Exam Notes : Server Form Factors

examguides.com/Serverplus/server-plus-1.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

1. Server Architecture

1.1 Server Form Factors

Rack mount:

Dimensions

- A 19-inch rack is a standardized frame or enclosure for mounting multiple equipment modules. Each module has a front panel that is 19 inches (482.6 mm) wide, including edges or ears that protrude on each side which allow the module to be fastened to the rack frame with screws.
- 1U equals 1.75-inches (44.45mm) of rack height. Therefore, a 2U rack mount height would be 2 x 1.75", which equals 3.5-inches high. A 3U height would be 3 x 1.75" = 5.25-inches.
- Rack unit is a measure used to describe the height of a server, network switch or other similar device mounted in a rack. One rack unit is 44.45 mm (1.75 in). One rack unit is commonly designated as "1U"; similarly, 2 rack units are "2U" and so on. The size of a piece of rack-mounted equipment is usually described as a number in "U". The number of rack units available in 8-inch space is 8/1.75 or 4U (fractional part has been trimmed).
- Server rack is useful for arranging the servers in a structured manner, one above the other, saving precious floor space.

Blade technology:

A Blade server is self-contained computer server, designed for high density, and efficient space utilization. A blade enclosure provides services such as power, cooling, networking, various interconnects and management. Together these form the blade system.

Tower:

A tower computer will have diagnostic lamps (LEDs) at the rear of the tower. Other features of tower computer include ability to add additional components (such as HDD, or DVD drive), better internal cooling due to more space, and more power because bigger power supply may be used to accommodate future expansion.

CompTIA® Server+ Exam Notes : Server Components

examguides.com/Serverplus/server-plus-2.htm

1. Server Architecture

1.2 Server Components

Server-grade processors: A few notable server-grade processors are given below:

1. Processor types: Intel Core i7 (900 series), Intel Xeon (35xx, 36xx, 55xx,56xx series), Intel Celeron

- Package type (pin count): LGA (1366)
- Bus transfer rate: 4.8-6.4 GT/s (GT stands for Giga transfers per second.)

2. Intel Itanium 9300-series

- Package type (pin count): LGA (1248)
- Bus speed: 4.8 GT/s

3. Intel Xeon 6500/7500-series

- Package type(pin count) : LGA (1567)
- Bus speed: 4.8-6.4 GT/s

4. AMD Opteron 6000

- package type (pin count): LGA (1974)
- Bus speed: 3.2 Ghz

5. AMD Phenom II, Athlon 2, Sempron, Opteron 3xxx

- Package type (pin count): PGA-ZIF (942)
- Bus speed: 3.2 GHz

Multi-threaded Processor: A multi-threaded processor executes the instructions in parallel, but shares the other resources like registers. A multi-processor system, on the other hand have independent support units. Therefore, other things being equal, a multi processor system is more efficient than a multi-threaded processor based computer. Further, a multi-threaded processor is a single chip where as a multi-processor system will have several independent processor chips

Socket types: Socket 1366, also called LGA1366 or Socket B, is a Land Grid Array (LGA) socket used by the latest generation of server-class Intel Core i7 and Xeon microprocessors. The socket supports triple-channel or six-channel DDR3 SDRAM memory controller with frequencies up to 3.2 GHz. The socket 1366 along with the socket 1156 superseded socket 775.

DMA enables the data to be written to or Read from the Memory directly. The processor is almost free to execute other instructions as programmed during the DMA process.

The following are the important features of multiprocessing:

1. Normally, multiprocessing (SMP) does not require separate memory for each processor. The processors share the same computer resources.

2. The Operating System software has to be written specifically to support multiprocessing.

3. Theoretically, there is no upper or lower limit on the processors requirement. Normally at least 2 processors are required to utilize the strengths of a multiprocessing operating system. Some computers support as many as 64 CPUs in multiprocessing architecture.

4. Applications that are developed keeping in view the multiprocessing architecture can benefit from the same.

5. In a multi-processor system, the CPU speeds and the L2 cache must match.

Some important points to remember:

- Normally, the CPUs, Motherboard, and Operating System are specifically built for supporting multiprocessing system. Memory is not normally build specifically for any multiprocessing system.
- Note that a transfer rate of up to 4.8 Giga transfers per second (Gt/sec) is normally achieved by high-end processors.
- A dramatic increase in the value of processor interrupts without a corresponding increase in system activity indicates a hardware problem. Identify the network adapter causing the interrupts and replace it.
- When you are upgrading an Operating System, or any other devices within the Server, it may often be required to upgrade the BIOS to enable fault free up gradation. The recommended place to check for available BIOS upgrades is the vendor's Website. If required, write to the vendor about the requirement and download appropriate version of the BIOS firmware.

Troubleshooting resource problems:

1) Pages/sec: Pages/sec is a memory object that indicates how often data is written to and read from the paging file. The normal limit is about 6 pages/sec. For example, a reading of 21 pages/sec indicates insufficient memory. Note that the paging file usage can to up to 80%.

2) Processor utilization contraint: Processor time utilization has a maximum allowed limit of 80%. Fpr example, with a processor time utilization of 96%, you may consider enhancing the processing capacity by upgrading the processor or adding a second processor.

3) Heating issues in small form factor computers and laptops: CPU throttling is a technique used in some computers to run the CPU at a reduced speed than the rated speed. As a result, the processor consumes lesser power and also produces less heat. This may be advantageous in small form factor computing devices such as laptops and mobile phones.

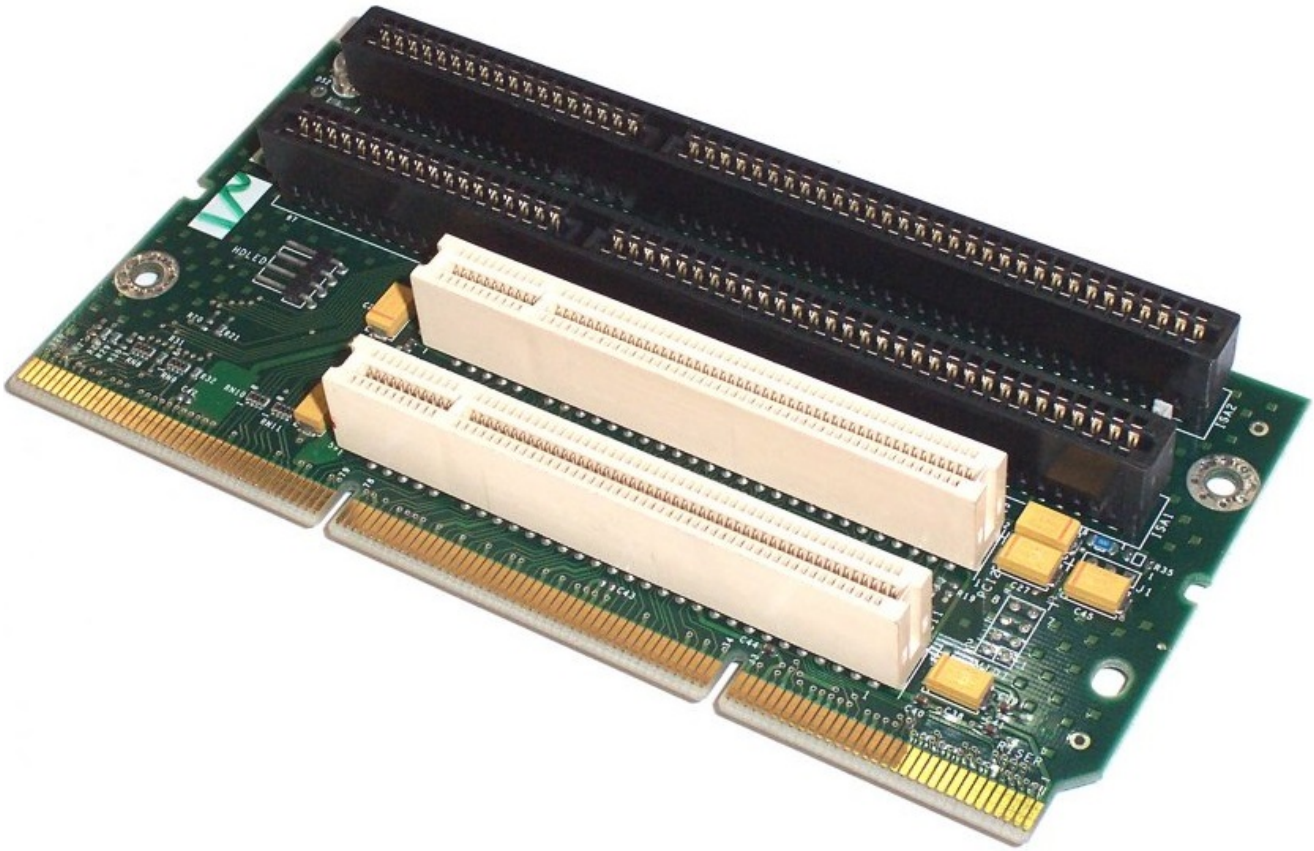
Running a CPU at a speed higher than the rated speed is called overclocking.

Enabling a single processor to execute two or more streams of instructions at the same time is called Hyperthreading

Overlapping of steps involved in processing CPU instructions is called Pipelining.

4) Troubleshooting using Event Log: The events log in a server contains the exact nature of the problem encountered when installing or initializing the application. After identifying the exact problem, an administrator may proceed to further remedial action.

Riser card: A riser card is a board that plugs into the system board and provides additional slots for adapter cards. Because it rises above the system board, it enables you to connect additional adapters to the system in an orientation that is parallel to the system board and save space within the system case. Please see the figure below:



Riser cards are often used to allow adding expansion cards to a system enclosed in a low-profile case where the height of the case doesn't allow for a perpendicular placement of the full-height expansion card. Riser cards allow the addition of expansion cards, such as video and graphic cards, to a system that doesn't allow for perpendicular placement of the expansion cards. Riser cards plug into and rise above the system board, while providing additional expansion card slots. Riser cards enable the connection of additional cards in a parallel orientation to the system board, as opposed to perpendicular, which conserves space within the system case.

BIOS/UEFI: UEFI (Unified Extensible Firmware Interface) is a standard firmware interface for PCs designed to replace the BIOS.

Notable advantages are given below:

1. Better security - The biggest benefit of UEFI is its security over BIOS. UEFI can allow only authentic drivers and services to load at boot time, making sure that no malware can be loaded at computer startup. Microsoft implemented this feature to counter piracy issues in Windows, while Mac has been using UEFI for quite some time now. Secure Boot works by requiring a digital signature of boot loaders which should require digital signature by the Kernel.

2. Faster startup times and resuming from hibernation - Since UEFI is platform independent, it may be able to enhance the boot time and speed of the computer.

3. Support for drives larger than 2.2 terabytes (TB): BIOS uses the Master Boot Record (MBR) to save information about the hard drive data while UEFI uses the GUID partition table (GPT). The major difference between the two is that MBR uses 32-bit entries in its table which limits the total physical partitions to only 4. Each partition can only be a maximum of 2TB in size, while GPT uses 64-bit entries in its table which dramatically extends the support for size possibilities of the hard drive.

4. Support for 64-bit firmware device drivers - UEFI provides support for 64-bit firmware device drivers.

5. It does not have to replace BIOS. UEFI can sit on top of the traditional BIOS and act as an interface between it and the operating system. Like BIOS, it presents a standardized view of the hardware to the operating system, allowing operating system makers to build on top of it and have their OSes work on a variety of motherboards.

Memory (RAM) Types:

ECC: ECC is mainly used for servers and other mission critical applications that requires extra security and stability. Non-ECC are for regular use like for gaming and home pc. ECC rams are a bit slower since it works with extra steps that prevents errors and are a bit expensive in most cases. You can use both in a Non-ECC motherboard, but you have to use an ECC supported motherboard to use the ECC feature of the ECC RAMs.

Double data rate (DDR): DDR is clock - doubled SDRAM (covered later in this section). The memory chip can perform reads and writes on both sides of any clock cycle (both the up and the down), thus doubling the effective memory executions per second. So, if you're using DDR SDRAM with a 600 MHz memory bus, the memory will execute reads and writes at 1200 MHz

By performing two transfers per cycle of a quadrupled clock, a 64-bit wide DDR3 memory module can achieve a transfer rate of up to 64 times the clock speed in megabytes per second (MBps). In addition, the DDR3 standard permits chip capacities of up to 8 GB.

Typical speeds of DDR3 memory are given below:

Memory module type: DDR3-800

Speed: 6400 MBps

Standard: PC3-6400

Memory module type: DDR3-1600

Speed: 12,800 MBps

Standard: PC3-12800

12,800 MBps may be arrived from the clock speed of 1600MHz as below:

```
Take a clock rate =1 unit.
Two transfers per sec (on both raising and falling edge): 2x1
Clock rate quadrapled: 2x4=8
64-bit data bus can transfer 8 bytes (64/8) at a time.
Therefore, the transfer speed would be: 8x8 or 64 times the clock speed.
So, multiply the clock speed of 1600MHz with 64 (8x8) = 102,400 bits per second or
12,800 mega bytes per second (MBPs)
```

DDR4 SDRAM is the abbreviation for "double data rate fourth generation synchronous dynamic random-access memory," the latest variant of memory in computing. DDR4 chips support transfer rates between 2133 MT/s (million transfers per second) and 4266 MT/s. By comparison, DDR3 technology supports only up to 800 to 2133 MT/s. This significant memory transfer boost will enable hardware developers to produce DDR4 chips with more powerful processors. This new memory also uses less power, 1.2 Volts compared to 1.65 Volts of DDR3 chips.

SIMMs: SIMMs need to be installed in pairs. SIMM stands for Single In-line Memory Module

Dual inline memory modules (DIMMs) have two rows of pins and twice the contact with the motherboard than older single inline memory modules (SIMMs). DIMMs differ in the number of conductors, or pins, that each particular physical form factor uses. Some common examples are 168-pin (SDR RAM), 184-pin (DDR, DDR2), and 240-pin (DDR3) configurations. DIMMs can be installed one at a time.

Bus Types:

Important features of PCI 2 bus are given below:

1. PCI-X 2.0 is a higher speed version of the PCI X (more specifically PCI-X 66 and PCI-X 133) standard.

2. PCI X 2.0 provides for two new speed grades: PCI-X 266 and PCI-X 533, offering up to 4.3 gigabytes per second of bandwidth

3. PCI 2 is up to 32 times faster than traditional PCI bus speed

4. Doubles and quadruples PCI-X bandwidth.

5. Full hardware and software backward compatibility (i.e. compatible with PCI, and PCI X).

6. Uses the same form factor, pin-outs, connector, bus widths, and protocols.

7. PCI-X 2.0 offers enhanced system reliability. ECC support has been added, providing automatic single-bit error recovery and double-bit error detection.

The throughput offered by 133MHz, 64-bit bus is 133X(64/8) Megabytes per sec or 1064 MB per sec.

The most probable cause for hard disk thrashing is that the RAM may need to be increased. Check for too many page file accesses, which may be resulting in disk thrashing.

Adapter teaming: Adapter teaming is also known as port aggregation. It is useful when you need to increase the bandwidth over the network media. High bandwidth utilization is experienced with bandwidth intensive applications such as video streaming, or downloads. Adapter teaming provides load balancing, and network redundancy. You need to assign the same IP address for both network cards when implementing adapter teaming. Adapter teaming provides increased bandwidth, and network redundancy. You need at least two network cards to implement adapter teaming. On the other-side of the network cables, you need a switch that can support adapter teaming.

The following are the features of adapter teaming:

1. In adapter teaming, single IP address is used. Even though there multiple adapters, all of them use a single IP address.

2. Adapter teaming provides fault tolerance. Even if one of the adapter connections fail (say due to cable cut), then the network connection still exists through the second adapter.

3. Adapter teaming requires at least two network adapters on a server to implement.

4. If you use adapter teaming on the server side, and connect the cables to a hub, then the resulting solution may not improve the available bandwidth. You need a switch that supports adapter teaming (or load balancing) on the other side of the network. A hub inherently can support adapter teaming.

Previous Contents Next

CompTIA® Server+ Exam Notes : Power And Cooling Components

examguides.com/Serverplus/server-plus-3.htm

1. Server Architecture

1.3 Power and cooling components

Cooling: The cooling methods used in PCs range from simple fan exhaust to pump out hot air to complicated systems like Heat pipes and Peltier coolers.

Heat sinks: Fans may not be sufficient to cool the computer system where the computer is housed with high power processors. In such cases heat sinks are attached to the processor using conductive thermal compound to distribute the heat in the surroundings. Here, the heat is radiated using convection from hot surface to cooler surroundings.

Heat pipes: If the heat generated in the computer is high enough that the heat sinks are unable to cool the devices sufficiently, it may be necessary to cool the devices using fluids. Heat pipes are small tubes, built into cooling fins, that are filled with thermally conductive fluid. On heat absorption, the fluid vaporizes. The vaporized fluid gets transferred to a different part of the system, and condensed.

Peltier coolers: A Peltier device is an electronic component that gets colder whn an voltage is applied. The method is more suitable if the ambient temperatures inside the computer are high, and other methods of cooling are inefficient.

Baffle/shroud: A baffle/shroud is a plastic or metal conduit that directs air to (or from) a CPU or any other heat producing device for cooling the device. In the server room or data-center, baffles may be deployed to channel the air in a desirable fashion as well.

In row cooling, a dedicated cooling unit is placed within the row of racks. This unit cools all the racks in the row.

1. Active cooling uses a fan directly mounted onto the heat-sink for forced-air cooling.

2. Example: Case fan refers to a computer fan is any fan inside, or attached to, a computer case used for active cooling, and may refer to fans that draw cooler air into the case from the outside, expel warm air from inside, or move air across a heat sink to cool a particular component.

3. Passive cooling does not use a fan or other means of forced-air cooling. Passive cooling relies on natural convection cooling.

4. Pseudo-passive cooling does not use a fan mounted directly onto the heat-sink but does use forced air cooling from a nearby fan. May incorporate a fan duct or shroud.

Plug types:

NEMA plug: These connectors are power plugs and receptacles used for AC mains electricity in North America and other countries that use the standards set by the US National Electrical Manufacturers Association (NEMA).

Edison plug: An ordinary household electrical plug in the United States. Characterized by having two flat blades and a semi-round ground pin. Grounded connector will have three pins and ungrounded connector will have only 2 pins, and the earthing pin will be missing.

Twist lock: Twist-locking connectors refer to NEMA locking connectors. The plug is pushed into the receptacle and turned, causing the now-rotated blades to latch. See figure below:

Previous Contents Next

CompTIA® Server+ Exam Notes : Server Operating Systems

examguides.com/Serverplus/server-plus-4.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

2. Server Administration

2.1 Server Operating systems

Performance baseline: Building a baseline of performance data is an important part of any Server management function. The baseline shows what performance is like under certain load conditions, when the server is known to be operating properly. The data can be used as a yardstick for measuring the impact of configuration changes or for capacity planning.

The most appropriate time for making baseline performance measurements is during the normal utilization of the server resources. This will reflect the normal load, and can be used for future reference. If the baseline performance statistics are taken during idle time or during backup time, it may not truly reflect the actual load on the server. Also, it is recommended to regularly monitor the performance and compare the same with baseline measurements, so that any trend can be detected at an early stage.

Note that, if baseline is taken without load (during weekend) then it will not correspond to the normal activity and is not much useful for later troubleshooting (when actual problem arises).

The most appropriate way to ensure that the newly installed servers are performing in expected lines is to make baseline performance measurements and compare with the known results taken on the other servers in the farm. However, the users also form an important constituent in identifying the bottlenecks. Sometimes, the problem may not have been identified early enough if we depend on user feedback for performance tuning.

File system Types:

FAT32: FAT32 is an older file system that's largely relegated to USB flash drives and other external drives. Windows uses NTFS for its system drive, and it's also ideal for other internal drives. ExFAT32 doesn't have any realistic file-size or partition-size limits. exFAT is a modern replacement for FAT32

exFAT32: It's a file system optimized for flash drives. It's designed to be a lightweight file system like FAT32 without all NTFS's extra features and overhead, but without FAT32's limitations. Works with all versions of Windows and modern versions of Mac OS X, but requires additional software on Linux.

NTFS: NTFS, an acronym that stands for New Technology File System, is a file system first introduced by Microsoft in 1993 with the release of Windows NT 3.1.

NTFS is the primary file system used in Microsoft's Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, and Windows NT operating systems.

The Windows Server line of operating systems also primarily use NTFS.

ReiserFS: ReiserFS is a general-purpose, journaled computer file system. ReiserFS is currently supported on Linux. The Reiser File System was the default file system in SUSE Linux distributions. Reiser FS was designed to remove the scalability and performance limitations that exist in EXT2 and EXT3 file systems.

Note: A journaling file system is a fault-resilient file system in which data integrity is ensured because updates to directories and bitmaps are constantly written to a serial log on disk before the original disk log is updated. In the event of a system failure, a full journaling filesystem ensures that the data on the disk has been restored to its pre-crash configuration.

UFS: The Unix file system (UFS; also called the Berkeley Fast File System, the BSD Fast File System or FFS) is a file system used by many Unix and Unix-like operating systems.

Virtual Machine File System (VMFS): VMFS is a scalable and high performance symmetric clustered file system for hosting virtual machines (VMs) on shared block storage.

ZFS(Zettabyte File System): ZFS is a local file system and logical volume manager created by Sun Microsystems Inc. for highly scalable storage. ZFS runs on Solaris, FreeBSD and Linux variants, and includes built-in data services and features such as replication, deduplication, compression, snapshots and data protection.

Previous Contents Next

CompTIA® Server+ Exam Notes : Server Roles And Requirements

examguides.com/Serverplus/server-plus-5.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

2. Server Administration

2.2 Server Roles and requirements

Network Services Server

DNS: The Domain Name System (DNS) is a central part of the Internet, providing a way to match names (a website you're seeking) to numbers (the numeric address for the website). Anything connected to the Internet - laptops, tablets, mobile phones, servers hosting your websites - has an Internet Protocol (IP) address made up of numbers. Your website might have an IP address like 64.202.189.170, but this is obviously not easy to remember. However a domain name such as mywebsite.com is something people can recognize and remember. DNS syncs up domain names with IP addresses enabling humans to use memorable domain names while computers on the Internet can use IP addresses. Hostnames in TCP/IP based network are resolved either with a static HOSTS file on your PC or from a DNS service (usually offered by your Internet Service Provide).

WINS: WINS is used for NetBIOS name resolution. WINS, LMHOSTS is used for resolution of NetBIOS names to IP addresses. NetBIOS names is based on an older protocol and should be used within a LAN only and registers itself on that network Windows Internet Name Service (WINS) is more than just an IP address resolver. It enables centralized management of NetBIOS namespace data and eliminates the need to remotely manage multiple LMHOSTS files (which perform the same function for NetBIOS lookup that Hosts

file perform for DNS lookup). Everytime that PC is powered up or rebooted using LMHOSTS, broadcasts or WINS to provide resolution of a NetBIOS hostname to it's IP address. NetBIOS names are limited to 16 characters in length with 15 characters visible.

DHCP: Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e. a scope) configured for a given network. DHCP leases IP addresses and other parameters like subnet mask, default gateway to client computers dynamically. You have to assign the IP address for your DHCP server statically. A DHCP server can't assign an IP address to itself. Similarly, some other Servers which need static assignment of IP addresses are your DNS server, WINS server, Default gateway.

Some important point to remember:

- Event viewer can be used for analyzing what has gone wrong with the service.
- WINS primarily supports clients that run early versions of the Windows operating system and applications that require NetBIOS. Later versions of Windows use Domain Name System (DNS) names in addition to NetBIOS names. Environments that include older computers that continue to use NetBIOS names on the same network as computers that use DNS names must use WINS servers in addition to the DNS servers.
- If you are not supporting any applications that require NetBIOS names, Microsoft(R) recommends that you establish DNS as your only method of name resolution.

Since all the computers on the network are Windows based, only resolution of NetBIOS names is required. Therefore, WINS service need to be installed.

Mail Server: Mail servers serve as an outbound client and inbound retrieval server for electronic messages, commonly via the STMP (simple mail transfer) protocol. Microsoft Exchange servers are the most common form of mail servers.

Remote Access Server (RAS): RAS is a type of server that provides a suite of services to remotely connected users over a network or the Internet. It operates as a remote gateway or central server that connects remote users with an organization's internal local area network (LAN). Once connected with a RAS, a user can access his or her data, desktop, application, print and/or other supported services.

Having a dedicated server for a specific purpose can speed up processing times and ensure sufficient resources are available during peak volumes. If the load on any specific server is not high, then you may consider installing two or more servers on the same physical computer.

Application server: Application servers can power shared apps, games, output from scripts and programs as well as serving data from an API (application protocol interface.) Modern application servers are optimized for load balancing and are often located in a cloud, which enables them to distribute data more efficiently.

File server: File servers can store a variety of media for distribution, including movies, audio and animation, rendering media at high speeds to client machines for games, movies and other forms of applications.

Directory Services Server: A Directory Services Server verifies the credentials of users and authenticates them. In addition, it also provides them with access to resources using single sign-on (SSO). SSO allows users to authenticate once and not be required to authenticate again to access the resources to which they have been given access.

Database server: Database servers manage data with the help of specialized software such as "SQL Server" or MySQL server. When you have large amount of queries, and a large amount of data to be parsed, you may need a dedicated database server with appropriate hardware resources such as memory, CPU, and disk capacity.

A Proxy Server usually sits in between your LAN and the external Internet. It directs all the requests to the Internet from the LAN.

An SQL Server is Microsoft's version of an client/server type database Server.

Previous Contents Next

CompTIA® Server+ Exam Notes : Access And Control Method To Administer A Server

examguides.com/Serverplus/server-plus-6.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

2. Server Administration

2.3 Access and control method to administer a server

Local Hardware administration:

KVM: A KVM (an abbreviation for Keyboard, Video, Mouse) switch is a hardware device that allows a user to control multiple computers from a single keyboard, video monitor and mouse. A user connects a monitor, keyboard, and mouse to the KVM device, then uses cables to connect the KVM device to individual computers. Control is switched from one computer to another by the use of buttons on the KVM device, with the KVM passing the signals between the computers and the keyboard, mouse and monitor depending on which computer is currently selected. Most devices also allow control to be switched through keyboard commands. If you need to control multiple PCs, then you need to purchase several sets of keyboard, mouse and monitor. This is not the most effective management since not only is it space-consuming but also costly. Thus the KVM switch saves space, costs, and increases management efficiency.

KVM over IP Switches are designed to enable remote access to computers and servers across a LAN/WAN, the Internet or even ISDN/56K modem.

A KVM (Keyboard, Video, Mouse) switch allows you to connect several computers to a single key board, mouse, and monitor. A KVM usually consists of the following:

1. Monitor

2. Keyboard

3. Mouse

4. Server

If you are getting keyboard error, you need to do one of the following things:

1. Check if the keyboard needs to be cleaned

2. Check if the keyboard cable has become loose

3. Check if one or more of the keys are stuck

4. If required, replace the keyboard.

ILO: Short for Integrated Lights-Out, it's an intelligent remote management processor integrated in many HP ProLiant servers that provides IT professions with virtual presence. An admin can get complete control of the server from remote sites akin to being local and using the server directly. ILO features include setup, group configuration, remote power on/off, Secure Socket Layer (SSL) security, detailed server status, virtual indicators and diagnostics.

IDRAC: An integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller is embedded in every Dell PowerEdge server. It provides functionality that helps you deploy, update, monitor and maintain Dell PowerEdge servers with or without a systems management software agent. Because it is embedded within each server from the factory, the Dell iDRAC with Lifecycle Controller requires no operating system or hypervisor to work. As an integral part of iDRAC, the Dell Lifecycle Controller simplifies server lifecycle management tasks like provisioning, deployment, servicing, user customization, patching and updating.

Virtual Administration Console: To manage several servers in a virtual environment, virtualization software provider offer administration consoles that allow an admin to connect from one server to another for the purpose of maintenance and administration. Examples include the VMware Server Console and the Virtual Machine Manager Console in Windows Hyper-V.

Remote Desktop Protocol (RDP): RDP is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

SSH: SSH, short for Secure Socket Shell is a network protocol that provides administrators with a secure way to access a remote computer. You can use SSH to tunnel your traffic, transfer files, mount remote file systems, and more. SSH tunneling allows a remote SSH server to function as a proxy server. Network traffic from your local system can be sent through the secure connection to the SSH server.

Virtual Network Computing (VNC): VNC is a graphical desktop sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer.

Previous Contents Next

CompTIA® Server+ Exam Notes : Server Maintenance Techniques

examguides.com/Serverplus/server-plus-7.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

1. Use wrist straps.

2. Use static protective bags

3. Ensure grounding of proper static protected work stations

4. Check periodically to ensure that static protected work station is alright.

Question: You are administrator of a Server with several client computers. The server also runs an SQL Server application. At times clients need access to the Server computer to configure database connectivity. What are the best practices that you follow when users need to configure the server?

Answer: For best practices,

1. It is recommended to accompany if someone else want to make changes to the software as required.

2. If it can be done by yourself, ask them to e-mail changes so that you can set it up for them.

3. It is not recommended to give away the password and the key to some one else and expecting that everything would be OK. It is possible that some one may intentionally or unintentionally cause harm to the Server and the network itself.

Clustering: Clustering for high availability significantly reduces system down time caused by both unplanned and planned hardware and software failures. The two most popular methods adopted are to use server clustering to deal with fail over (Active/Passive Mode) and load balancing (Active/Active).

Active/Active cluster: In an active/active cluster, both the servers will be actively servicing the workload. It is not necessary that both servers are running the same apps. They may be running different apps, for example one server running file server and another the Exchange server. However, when one server fails, it is important that the other server takes up the work load. In Active/Active clustering, both nodes are accessible and active. If a node fails, then its resources would shift to the other active node. The node that survives would then carry the load for both nodes. The advantage of Active/Active clustering is that the resources are available and used at all times. However, you need to ensure that in an Active/Active environment that individual nodes could sustain the traffic generated for both nodes. This could be tested practically by switching off one of the nodes during normal working hours. Then the whole load falls on the surviving node. The surviving node should be able to take the traffic. The test can be repeated for each of the nodes sequentially. In active/active clustering, when one node fails or is taken offline, the other node in the cluster takes over for the failed node. However, because the failover causes the other node to take on additional processing operations, the overall performance of your cluster may be reduced. This is different from active/passive clustering where only one member of a cluster provides service to users at a time.

Active/Passive cluster: Active/Passive means that your cluster has an active node and a passive mode. If your active node failed, then its defined resources would shift to the passive node and it would become active. The passive node is not accessible unless the primary node fails, in which event the passive node takes charge. In an active/passive cluster, at one of the servers in the cluster is not actively working but simply sitting idle until a failure occurs. When a failure occurs, it takes over the responsibilities of the failed server. In active/Passive clustering, the passive (a.k.a. failover) node serves as a backup that's ready to take over as soon as the active (a.k.a. primary) node gets disconnected or is unable to serve. Since, usually both the nodes are of same hardware/software, the performance levels are guaranteed in active/passive clustering. Active/passive is the preferred recommended cluster configuration.

Note that a cluster may have more than two servers. Two servers is the minimum configuration required for server clustering.

There are two types of fail over clustering in Windows:

1. Active/Passive and

2. Active/Active.

Following are true about clustering:

1. Clustering improves the availability of the network.

2. Processing load is distributed among the clustered servers.

3. Clustering allows for better scalability.

4. If one of the servers in a cluster fails, other server(s) in the cluster take over the entire load of the failed server without interruption to the services.

5. Clustering takes atleast 2 computers to work

6. Active/active clustering describes clustering when both members of the cluster are online and able to accept user service requests.

Note that adapter teaming, and network load balancing do not necessarily provide continuous availability.

Failover is a backup operation that automatically switches to a standby server or network if the primary system fails or is temporarily shut down for servicing. Failover is widely used for mission-critical systems that rely on constant accessibility.

Failover sever takes responsibilities of the failed server (or network) automatically and transparently to the user. A fail-over describes a mechanism, where if the primary node in a cluster fails, and the secondary node takes over the load of the failed node. During a fail-over, usually the failure (or fail-over) is not noticed by the clients.

Failsafe: Failsafe is an operation which ensures that a failure of equipment, or system does not propagate beyond the immediate environs of the failing entity.

Mean Time To Repair (MTTR): MTTR is a basic measure of the maintainability of repairable items. It represents the average time required to repair a failed component or device. MTBF (mean time between failures) is a measure of how reliable a hardware product or component is.

Previous Contents Next

CompTIA® Server+ Exam Notes : Asset Management And Documentation

examguides.com/Serverplus/server-plus-8.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

2. Server Administration

2.5 Asset management and documentation

Documentation

DFD: A Data-Flow Diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling its process aspects. A DFD is often used as a preliminary step to create an overview of the system, which can later be elaborated.

Architecture diagram: A Software Architecture Design is an important step for software and application developers to describe the basic software structure by separating functional areas into layers. It depicts how a typical software system might interact with its users, external systems, data sources, and services.

Recovery documentation: A disaster recovery plan (DRP) that is documented with clear set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster.

Baseline documentation: A performance baseline is a vital part of your system documentation. A baseline should be established immediately after a new system has entered production, and should be repeated with regular intervals. That way you can see

how your system performs over time and make informed decisions about when a system will have to be upgraded etc. The primary tool you use to capture a baseline on the Windows platform is Performance Monitor (or just Performance or PerfMon).

Service Manuals: Service Manuals (SM) are the manuals provided by manufacturers which cover the servicing, maintenance and repair of their products.

SLA: A Service-Level Agreement (SLA) is a contract between a service provider and its internal or external customers that describes the service, usually in measurable terms, to be furnished.

Previous Contents Next

CompTIA® Server+ Exam Notes : Virtualization

examguides.com/Serverplus/server-plus-9.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

2. Server Administration

2.6 Virtualization

Virtualization is the use of software to allow a piece of hardware to run multiple operating system images at the same time. The simulated machines are called virtual machines.

Recently, CPU's are equipped with virtualization features. Intel VT and AMD's AMD-V are two examples of CPU virtualization.

Clone: A clone is a copy of an existing virtual machine. The existing virtual machine is called the parent of the clone. Installing a guest operating system and applications can be time consuming. With clones, you can make many copies of a virtual machine from a single installation and configuration process.

Hardware compatibility list: The first thing that one need to ascertain is to make sure that the upgrade is compatible with the existing hardware. This can usually be ensured by going through HCL (Hardware Compatibility Lists). You can also see the manufacturer's documentation for this purpose. HCL is a list of computer hardware that is compatible with a particular operating system or device management software. A hardware compatibility list is a database of hardware models and their compatibility with certain operating system.

A third party device can be installed if:

1. It is on the HCL (Hardware Compatibility List) of the OS vendor. Or

2. That the device manufacturer supplies appropriate driver software for use with a given Operating System (that you are going to install/use).

Hypervisor: A Hypervisor also known as Virtual Machine Monitor (VMM) can be a piece of software, firmware or hardware that allows multiple operating systems to share a single host computer hardware. The hypervisor manages requests by virtual machines to access to the hardware resources (RAM, CPU, NIC etc) acting as an independent machine.

The Hypervisor is mainly divided into three types as explained below:

Type 1 Native/Bare Metal Hypervisor: This is also known as Bare Metal or Embedded or Native Hypervisor. It works directly on the hardware of the host and can monitor operating systems that run above the hypervisor. It is completely independent from the Operating System.

The hypervisor is small as its main task is sharing and managing hardware resources between different operating systems. A major advantage is that any problems in one virtual machine or guest operating system do not affect the other guest operating systems running on the hypervisor.

Type 2 Hosted Hypervisor: also known as Hosted Hypervisor. the hypervisor is installed on an operating system and then supports other operating systems above it. It is completely dependent on host Operating System for its operations. While having a base operating system allows better specification of policies, any problems in the base operating system affects the entire system as well even if the hypervisor running above the base OS is secure.

Type 3 Hybrid: This is basically a Type II hypervisor, but it is integrated with a cloud. The best example of this is VMware Workstation version 12.

Network Connectivity:

A host system (host operating system) would be the primary & first installed operating system. If you are using a bare metal Virtualization platform like Hyper-V or ESX, there really isn't a host operating system besides the Hypervisor. If you are using a Type-2 Hypervisor like VMware Server or Virtual Server, the host operating system is whatever operating system those applications are installed into.

A guest system (guest operating system) is a virtual guest or virtual machine (VM) that is installed under the host operating system. The guests are the VMs that you run in your virtualization platform. Some admins also call the host & guest the parent and child.

VSwitch: A vSwitch or virtual switch is a software program that allows one virtual machine (VM) to communicate with another. Just like its counterpart, the physical Ethernet switch,

A **vNIC** is a virtualized Network Interface Card, used by a Virtual Machine as its network interface. A vNIC is assigned a MAC address. Each MAC address corresponds with a single virtual NIC, which is used by a virtual machine

Previous Contents Next

CompTIA® Server+ Exam Notes : Primary Storage Devices

examguides.com/Serverplus/server-plus-10.htm

3. Storage

3.1 Primary storage devices

Interfaces:

SCSI: If the termination is not done, a SCSI devices on the bus will not function properly. This is due to reflection of the signals at the end of the bus. To prevent this, both ends of the SCSI bus need to be terminated. If one end of the SCSI bus is terminated, you may find intermittent problems. Never terminate the bus at a device connected in between.

Each device in a SCSI chain need to have unique ID. For a 16-bit Wide SCSI, there are 16 possible SCSI Ids, 0-15. A standard 8-bit SCSI can support only 8 devices (including SCSI card), the Ids allowed are 0-7.

In a SCSI configuration, devices are distinguished between each other on a Bus by SCSI ID's.

On SCSI the numbered ID ranges from 0-7 for SCSI-1 or SCSI-2

The numbered ID's range from 0-15 on a single Channel SCSI-3 system and 0-31 ID's on a Dual Channel SCSI-3

Remember that each Device on the chain needs to be assigned a unique SCSI ID.

Also, highest ID device will have higher priority than lower value device.

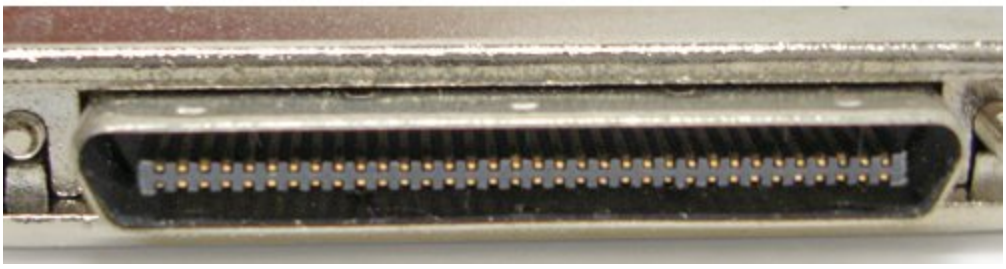
For example, on a SCSI bus with device Ids' 7-0: 7 is highest priority and 0 has the lowest priority.

Device support:

Most older specs: SCSI ID - 0=bootable drive, 7=controller, 1-6=any other devices SCSI 3 ultra-wide, Ultra320, Ultra640: 16 devices, 0=bootable drive, 15=controller

Internal parallel SCSI cables have two or more 50, 68, or 80-pin connectors attached. External cables have 50 or 68-pin connectors at each end, depending on the specific SCSI bus width supported.

The figure below shows the connectors configuration for 80-pin SCA (Single Connect Attachment):



All of these SCSI types are parallel - bits of data move through the bus simultaneously rather than one at a time. The newest type of SCSI, called Serial Attached SCSI (SAS), uses SCSI commands but transmits data serially. SAS uses a point-to-point serial connection to move data at 3.0 gigabits per second, and each SAS port can support up to 128 devices or expanders.

All the different SCSI varieties use controllers and cables to interface with devices

Note that older types were given for understanding purpose and you are unlikely to get any question on older SCSI types, such as SCSI-1, and 2.

Cable lengths used by SCSI devices are:

Single Ended (or un balanced) electronic signaling : 6 m

Differential signaling (HVD - High Voltage Differential) : 25 m or 82 ft (apx)

Differential signaling (LVD - Low Voltage Differential): 12 m

SCSI system uses the following types of terminations:

1. Passive: Uses passive resistors, not recommended usually.

2. Active: This terminator has a voltage regulator that ensures the correct termination voltage.

3. Forced Perfect Termination (FPT): A better implementation of active termination that clamps to the output of two regulated voltages.

The Ultra-High Density SCSI connector is an extremely compact 68-pin connector with a slot of contacts and securing screws. This connector is also compatible with LVD buses, and can also be referred to as SCSI-4.

High Voltage Differential signaling scheme is not compatible with Single Ended (SE) or unbalanced signaling scheme. LVD, on the other hand is compatible with Single Ended signaling scheme. Also, LVD is less susceptible to Noise and allows greater cable lengths.

Hot-Swapping: Hot-Swapping is the ability to add and remove devices to a computer while the computer is running and have the operating system automatically recognize the change. Hot plugging is also called hot swapping.

Some of the important terminologies relating to swapping are:

- Cold Swap: It means that you have to power down a server before the part is replaced.
- Warm Swap: It means that you may have to stop I/O functions corresponding to the part that need to be replaced by using appropriate instructions. The server need not be powered down.
- Hot Swap: Hot Swap allows the faulty part to be replaced without interrupting the Server or introducing any interruption in the I/O procedures.
- Obviously, hot-swap allows for easy replacement of faulty part.

USB: Universal Serial Bus (USB) and IEEE 1394 support hot plugging. This is also a feature of PCMCIA. USB enables you to daisy chain up to 127 USB devices. A USB hub is used for this purpose. Also, USB devices can be plugged in without turning on/off power. i.e. USB devices are hot swappable. The now-aging USB 2.0 standard can theoretically transfer data at a very high 480 megabits per second (mbps), or 60 megabytes per second (MBps). That's impressive, but not as much as the newer USB 3.0, which can handle up to 5gbps (640MBps - over ten times as fast as the 2.0 maximum).

Bus Types: There are 3 main types of buses used. These are a) SATA, b) SCSI, and c) Fiber Channel

a. Bus type: SATA

- Cable length: 1 meter (3 feet)
- Speed : Fast
- SATA I (revision 1.x) interface, formally known as SATA 1.5Gb/s
- SATA II (revision 2.x) interface, formally known as SATA 3Gb/s,
- SATA III (revision 3.x) interface, formally known as SATA 6Gb/s

b) Bus type: SCSI (there are several types of SCSI buses)

- Cable length: Typically 12 or 24 m
- Speed : Fast (different speeds exist depending on SCSI type), but less than FC (costlier than SATA)

c) Bus type: Fiber Channel (FC)

- Cable length: Up to 10Km (for single mode. Multi mode distances are less)
- Speed (cost): Very fast and expensive too. Typical speeds are 1, 2, 4, 8, 16, 32, and 128 gigabit per second and primarily used to connect computer data storage to servers.

Note: The major reason for choosing/paying for SCSI/SAS over SATA, is not speed, but reliability. SCSI interfaces are meant for server grade operation (24x7) where as SATA interfaces are typically not as reliable as SCSI and primarily meant for PCs or off-line use.

SATA: The following are true about Serial ATA (SATA):

1. Serial ATA (SATA) transfers data in a half-duplex channel at 1.5 Gbps With SATA II, introduced in 2003, speed was increased to 3 Gbps.

2. SATA drops the master/slave shared bus of Parallel ATA, giving each device a dedicated cable and dedicated bandwidth.

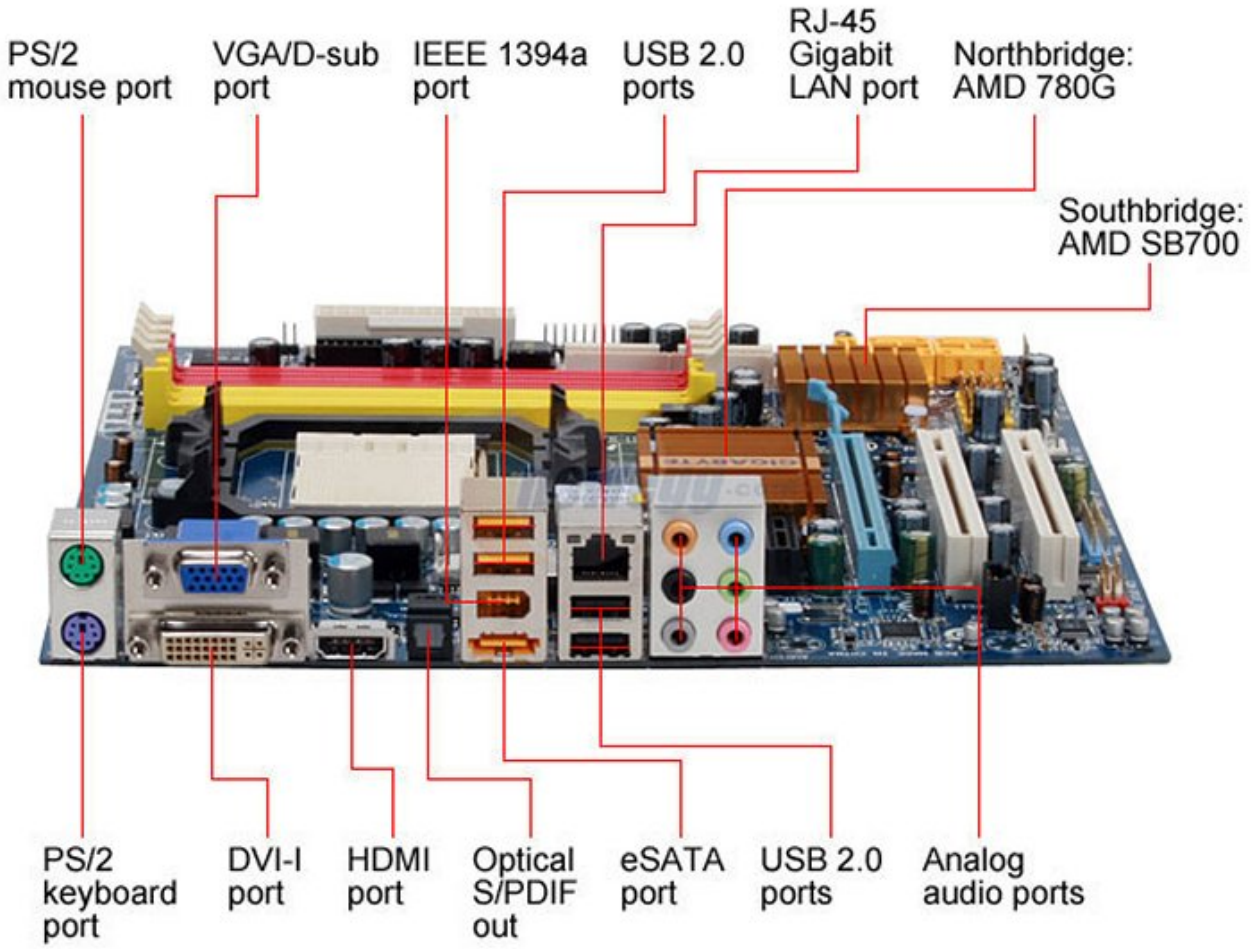
3. SATA allows hot swapping, whereas Parallel ATA does not.

4. SATA cables use 7-pin, and can be up to 1 m (39 in) long, PATA ribbon cables, in comparison, carry either 40 or 80 conductor wires and are limited to 46 m (18 in) in length.

5. SATA drives may be plugged into Serial Attached SCSI (SAS) controllers and communicate on the same physical cable as native SAS disks.

6. The power connector for SATA is completely different from that of PATA. While SATA uses 15-pin connector, PATA uses 4-pin Molex connector. Note that multiple pins are used for carrying same voltage in SATA.

Various motherboard connectors are shown in the figure below:



Hard drive vs SSD: SSD, short for Solid State Drive, has the following advantages over the conventional hard disk drive (HDD):

1. SSD reads contents much faster than a typical hard drive

2. Draws less power than hard drive. Draws about 2-3 wall where as a HDD draws about 8 Watts. This improves battery backup times and produces less heat.

3. Doesn't produce any noise as there are no moving parts.

4. Boot times are faster than that of hard drive. It typically takes 10-15 seconds to beet using SSD which is significantly less than 30-40 sec taken by HDD.

5. At this, though the price of SDD is slightly more than that of HDD for a given disk capacity, the prices of SDDs are falling dramatically over time.

6. The reliability is better in SSDs as there are no moving parts.

7. There are a variety of types of SSDs, including those that use SAS, SATA, and PCI-Express interfaces. ATA and PCI are not used with SSDs, usually.

CompTIA® Server+ Exam Notes : Raid Levels

examguides.com/Serverplus/server-plus-11.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

3. Storage

3.2 RAID levels

RAID controller caches can significantly increase performance when writing data. A typical example for such a cache might consist of 256, 512 or 1024 MB. Usually RAID system measures the cache in Megabytes. If the power were to fail, the content of this cache would be lost, unless the content has been protected by a battery backup unit (BBU) or battery backup module (BBM). BBUs and BBMs have integrated batteries, which can generally power the content of the cache for up to 72 hours. If the server is re-started during that period, the data in the cache can be recovered.

Important RAID levels are:

RAID 0: Disk Striping, in this configuration, the server will have multiple disks and the data is striped across the disks in blocks without parity. RAID 0 has no fault tolerance.

RAID 1: Disk Mirroring, or Disk Duplexing: there are two hard disks and any thing that is written on one disk is written onto the mirrored disk. Disk Mirroring provides fault tolerance, in the sense, that if one disk fails, the mirrored disk can take place of failed disk. The difference between disk mirroring and disk duplexing is that, in case of disk mirroring only one disk controller serving both the disks, whereas in disk duplexing, additional disk controller will be controlling the mirrored disk. In RAID1, or disk mirroring, one drive in

the array acts as a "mirror" drive, backing up all the data on the primary drive on-the-fly. Duplexing adds another disk controller. So in case one controller fails, the other can pick up without any interruption in service.

RAID 3: This takes a striped array as in RAID 0, then adds a parity hard disk drive to the array. This parity information is vital if one drive fails. If a drive should fail in this situation, the parity drive can be used to restore blocks that have been broken due to data corruption.

RAID 5: RAID5 is similar to mode 3, except the parity is spanned across all drives, this allows all drives to be able to rebuild the array should a drive fail. A minimum of three disks is required for RAID 5. In case of a single disk failure, the missing data can be calculated using the parity. RAID 5 is not a good choice because it doesn't offer faster read cycles as that of disk striping. RAID 5 utilizes the combination of striping and parity techniques. The capacity of the array is (N-1) times the size of the smallest member disk for the array of N disks

RAID 1+0 (also called RAID 10) has the advantage of faster read (due to disk striping) and redundancy (due to disk mirroring).

RAID 6: RAID6 also known as double-parity RAID, uses two parity stripes on each disk. It allows for two disk failures within the RAID set before any data is lost. A minimum of four disks is required to create RAID 6. The capacity of the array is (N-2) times the size of the smallest member disk for the array of N disks. RAID 6 is relatively expensive storage option. However, when it is needed a large and reliable storage, then RAID 6 is one of the best choices, because it protects data if two disks failure happens.

RAID 10: IN RAID10 READ and WRITE operations are much faster than RAID 6, and also the rebuilding a failed RAID is also faster in RAID 10. Hence, it is recommended to go for RAID 10 unless you have specific needs for redundancy that mandates RAID 6. A RAID 10 configuration requires a minimum of four disks, and stripes data across mirrored pairs. As long as one disk in each mirrored pair is functional, data can be retrieved. Only 50% of the total raw capacity of the drives (lowest capacity drive to be considered) is usable due to mirroring.

RAID levels comparison chart

	RAID0	RAID1	RAID 5	RAID6	RAID10
Min number of disks	2	2	3	4	4
Fault tolerance	None	1 disk	1 disk	2 disk	1 disk
Disk space overhead	None	50.00%	1 disk	2 disks	50.00%

Read speed	Fast	Fast	Slow		Fast
Write speed	Fast	Fair	Slow		Fair
Hardware cost	Cheap	High (disks)	High	Very high	High (disks)

For example, consider a RAID configuration of 1+0 (or RAID 10), the READ speeds for different configurations are as given below:

a) 4 disks with 80 GB each:

- Capacity 160 GB
- Speed gain 4x read and 2x write speed gain

b) 8 disks with 20GB each:

- Capacity 80 GB
- Speed gain 8x read and 4x write speed gain

c) Minimum 4 disks are required for RAID 10. Assuming 4 disks are available with 120GB each,

- Capacity 240 GB
- Speed gain 4x read and 2x write speed gain

d) 6 disks with 40 GB each:

- Capacity 120 GB
- Speed gain 6x read and 3x write speed gain

As seen from the above, we can say that 8 disks provide highest READ speeds among the given options. You may check for other RAID configurations to examine the same.

RAID 5 with 9 drives provides 640GB capacity (9 -1 = 8). This is the most efficient storage solution as only one spare disk is required.

Hardware vs Software RAID

A hot spare is a spare unit that is ready to take on the job of the main unit in the even of failure. Hot spare refers to the physical unit such as a disk drive or even a standby computer, such as in a clustered configuration. The failure may or may not be noticed by clients. For example, if the RAID system is configured with RAID 0, a failure may be noticed by the clients, whereas, if configured with RAID 5, the failure may not be noticed (in case of single point failure).

The following are the benefits of hardware RAID:

1. Hardware RAID provides better performance compared to Software RAID.

2. Software RAID is usually limited to RAID levels 0, 1 and 5. It is possible to implement several other RAID combinations with Hardware RAID.

3. Hardware RAID allows multiple operating systems to access the RAID array, whereas Software RAID usually do not allow any other operating system other than the one used to create it.

4. Boot Volume Limitations: Since the operating system has to be running to enable the array, the operating system cannot boot from the RAID array! Therefore, it requires a separate, non-RAID partition to be created for the operating system.

5. One disadvantage of hardware RAID is that it is expensive.

Previous Contents Next

CompTIA® Server+ Exam Notes : Features Of Various Storage Technologies

examguides.com/Serverplus/server-plus-12.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

3. Storage

3.3 Features of various storage technologies

Internet Small Computer System Interface (iSCSI): iSCSI is a way of connecting storage devices over a network using TCP/IP. It can be used over a local area network (LAN), a wide area network (WAN), or the Internet. iSCSI devices are disks, tapes, CDs, and other storage devices on another networked computer that you can connect to.

Simply put, iSCSI is an Internet Protocol (IP)-based storage networking standard for linking data storage facilities, developed by the Internet Engineering Task Force (IETF). By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances. iSCSI is a data transport protocol used to carry block-level data over traditional Ethernet networks and the Internet. By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances. Because of the ubiquity of IP networks, iSCSI can be used to transmit data over local area networks (LANs), wide area networks (WANs), or the Internet and can enable location-independent data storage and retrieval.

The following are the notable points when compared with FC (Fiber Channel) or FcoE (Fiber Channel over Ethernet):

1. iSCSI is a storage networking protocol built on top of the TCP/IP networking protocol. It does not specifically require any extra hardware, which makes it comparatively inexpensive to implement.

2. FC is a dedicated storage networking architecture that was standardized in 1994. It requires its own networking hardware to implement.

3. FCoE uses standard multipurpose Ethernet networks to connect servers with storage. Unlike iSCSI, it does not run over TCP/IP - it has its own Ethernet protocol occupying a space next to IP in the OSI model.

4. Even though FCoE runs over the same general-purpose switches that iSCSI does, it experiences significantly lower end-to-end latency due to the fact that the TCP/IP header doesn't need to be created and interpreted. The dis-advantage is that it cannot be routed over a TCP/IP WAN.

5. iSCSI eliminates distance limitations imposed by SCSI transfers as it uses TCP/IP.

6. iSCSI is susceptible to network congestion as it uses the same networking channel used by other TCP/IP communications.

7. iSCSI is less expensive compared with Fiber Channel deployments. iSCSI is useful in smaller, quick deployments whereas FC is recommended in larger deployments.

8. Fibre Channel, or FC, is a high-speed network technology (commonly running at 2, 4, 8 and 16-gigabit per second rates) primarily used to connect computer data storage.

9. Fiber channel utilizes FCP (Fibre Channel Protocol) transport protocol that transports SCSI commands over Fibre Channel networks.

10. Fiber channel provides fastest speeds and SCSI follows Fiber channel in speed.

LUN: LUN stands for Logical Unit Number. LUN is used to identify a logical device that is an independent functional part of a SCSI device. SCSI-2 specification allows 8 logical units for each SCSI device address. The logical unit addresses are numbered 0 to 7. In computer storage, a logical unit number, or LUN, is a number used to identify a logical unit, which is a device addressed by the SCSI protocol or Storage Area Network protocols which encapsulate SCSI, such as Fibre Channel or iSCSI.

Ultra SCSI-3: 8-bit and 16-bit versions, both with 1.5 meter cable length. The 8-bit version supports up to 8 devices. The 16-bit version doubled the number of devices, and supports up to 16 devices (this includes the SCSI board itself).

Ultra-2 SCSI: 8-bit bus; 12 meters; 40 MBps; 8 devices.

Wide Ultra-2 SCSI: 16-bit bus; 12 meters; 80 MBps; 16 devices.

Traditional SCSI has been superseded by later attachment protocols such as Serial Attached SCSI (SAS) and iSCSI, which build on the earlier SCSI command structure.

SCSI Type	Transfer speed	Bus width
SCSI-1	5MBPS	8 bit bus
Fast Wide SCSI2	20MBPS	16 bit bus
Wide Ultra SCSI3	40MBPS	16 bit bus
Wide Ultra 2	80MBPS	16 bits bus
Narrow Ultra 2	40MBPS	8 bits bus
Ultra160	60MBPS	16 bits bus
Ultra320	320MBPS	16 bits bus
Ultra640	640 MBPS	16 bits bus

SCSI ID - 0=bootable drive, 7=controller, 1-6 = any other devices

SCSI 3 ultra-wide - 16 devices, 0=bootable drive, 15 = controller

Note: The table is given for historical review of SCSI standards, and need not be remembered for the exam.

Host Bus Aapter (HBA): HBA connects a host system (the computer) to other network and storage devices. The terms are primarily used to refer to devices for connecting SCSI, Fibre Channel and eSATA devices, but devices for connecting to IDE, Ethernet, FireWire, USB and other systems may also be called host adapters.

Auto Loader: An auto loader holds ten to twelve tapes, and usually only one tape drive. This is useful when the data to be backed up is more than one tape's capacity. It allows the admin to program and attend to other important works than wait for changing the tape.

Tape Library: A Tape Library contains multiple drives in it. As a result, multiple backups can be taken simultaneously. This is useful when you need to take huge backups in short time. However, remember that if the backups are taken across the network, the network speed limitations will come into play.

SAN(Storage Area Networks): SAN is a high-speed network of storage devices that also connects those storage devices with servers. It provides block-level storage that can be accessed by the applications running on any networked servers. SAN storage devices can

include tape libraries, and, more commonly, disk-based devices, like RAID hardware.

The important features of SAN (Storage Area Networks) and NAS (Network Attached Storage) are given below:

1. Only server class devices with SCSI Fibre Channel can connect to the SAN.

2. SAN uses Fibre Channel and based on SCSI protocol.

3. A SAN addresses data by disk block number and transfers raw disk blocks.

4. Backups and mirrors require a block by block copy, even if blocks are empty. A mirror machine must be equal to or greater in capacity compared to the source.

NAS (Network Attached Storage): Networked storage was developed to address the challenges inherent in a server- based infrastructure such as direct-attached storage.

A network-attached storage (NAS) device is a server that is dedicated to nothing more than file sharing. NAS does not provide any of the activities that a server in a server-centric system typically provides, such as email, authentication or file management.

Important features of NAS

1. NAS uses TCP/IP Networks: Ethernet, FDDI, ATM

2. Typically, any machine that can connect to the LAN can use NFS, CIFS or HTTP protocol to connect to a NAS and share files.

3. Backups and mirrors are done on files, not blocks, for a savings in bandwidth and time.

NAS copies files whereas SAN works by copying blocks of data. Even blocks with no data are copied using SAN. Hence NAS requires less bandwidth compared to SAN.

Direct-attached storage (DAS): DAS refers to a digital storage system directly attached to a server or workstation, without a storage network in between. It is a acronym, mainly used to differentiate non-networked storage from the concepts of storage area network (SAN) and network-attached storage (NAS). DAS is ideal for localized file sharing in environments with a single server or a few servers - for example, small businesses or departments and work groups that do not need to share information over long distances or across an enterprise.

Previous Contents Next

CompTIA® Server+ Exam Notes : Server Hardening Techniques

examguides.com/Serverplus/server-plus-13.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

4. Security

4.1 Server hardening techniques

Hardware hardening

There are several ways of hardening your server computer. These include disabling unneeded hardware and physical ports/devices:

1. BIOS password - Ensures that only authorized persons have access to change or view BIOS settings.

2. Disable WOL (Wake on LAN) - Ensures that the computer is not started remotely and compromised (say, by scanning for open ports, guest login, etc.)

3. Setup boot order - Ensures that a hacker is not using a USB drive to start the computer, and later gain access to the resources on the server.

4. Chassis locks / intrusion detection - Ensures that a hacker doesn't have access to internal components such as hard drive and can't change the physical settings.

Wake-on-lAN: Network administrator needs to maintain (update software etc.) the client computers often. In the past, they need to go to the client computer to power it ON. But with Wake-on-LAN, it is possible to remotely and automatically power up the client computers

for necessary maintenance. It is important to set up password protection for Wake-on-LAN features.

Anti-virus package: This is a program that checks the files for any virus infection. Upon detection of any virus, it typically warns the user of the existence of such virus and prompts for further action. It is important that servers are equipped with appropriate AV software for protection against malware.

Proxy server: Proxy server is used for accessing the public Internet from a private IP address. It basically translates the IP addresses from one to another, and allows several users with private IP addresses to access the Internet using one or more public IP addresses. A proxy server may be used to hide the internal network from external attacks.

Fire Wall: A fire wall is typically used for preventing unauthorized access to internal resources of a company.

Chassis intrusion detection: The chassis intrusion switch is used to ensure that the computer remains shut down when the case is open. Sometimes, it will also prevent booting of the computer (even after the case is closed) to warn that there was an intrusion.

Previous Contents Next

CompTIA® Server+ Exam Notes : Basic Network Security Systems And Protocols

examguides.com/Serverplus/server-plus-14.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

4. Security

4.2 Basic network security systems and protocols

Authentication protocols:

LDAP (Lightweight Directory Access Protocol): LDAP is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. "Active Directory" is Microsoft's solution for Windows domain networks and based on the LDAP protocol. Windows Server Operating systems is LDAP based. Windows 2000 Server Operating systems and NetWare are LDAP based. eDirectory is Novell's directory platform that is cross platform and LDAP based. Similarly, Active Directory is Microsoft's solution and based on the LDAP protocol.

VLAN: VLAN, short for Virtual LAN, provides a logical network of computers. A VLAN may span multiple physical segments. The advantages of using VLANs within a LAN is that it provides greater bandwidth and security. Computers on different VLANs do not see each other directly. A VLAN segregates the network at layer-2 of the OSI model.

A VLAN is a group of devices on one or more logically segmented LANs. All devices working on a VLAN will have same broadcast domain. Like routers, the switches (Layer 2) have ability to provide domain broadcast segmentation called a VLAN. Using VLAN technology,

you can group switch ports and their connected users into logically defined communities of interest. A VLAN operating on a Catalyst switch limits transmission of unicast, multicast, and broadcast traffic to only the other ports belonging to that VLAN, thereby controlling broadcasts.

The benefits of VLANS include:

1. Easy Administration resulting in reduced administration costs,

2. Increased Security due to broadcast control, if you are using simple hub, you can observe traffic corresponding to any node by simply inserting a Network analyzer.

3. Grouping based on functional requirements irrespective of physical location of nodes,

4. Simplify moves, adds, changes,

5. Distribution of traffic thereby using the network bandwidth more efficiently.

VPN: A Virtual Private Network (VPN) is a network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote offices or traveling users access to a central organizational network.

To use a VPN, both the network server (at the VPN provider's side) and the client (your computer) need to speak the same language. For this purpose, the provider's side a Remote Access Server (RAS) is used. It's this RAS that your computer connects to when using a VPN. The RAS requires your computer to provide valid credentials, which it authenticates using any one of a number of authentication methods. On the client side, your computer uses client software to establish and maintain your connection to the VPN. The client software sets up a tunneled connection to the RAS, as well as managing the encryption that secures your connection. Tunneling is a process by which data is sent privately over the internet, via a VPN. Data is encrypted while it transits the public Internet using any of the pre-negotiated protocols between the server and the client (your computer).

DMZ: A DMZ (Short for De-Militarized Zone) is a physical or logical sub-network that contains organization's external services such as Web server and exposes the same to the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN).

RADIUS: Radius is a protocol that enables a single server to become responsible for all remote-access authentication, authorization, and auditing (or accounting) services. It is an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes

access to the ISP system. RADIUS implements a client/server architecture, where typical client is a router, switch, or AP and the typical server is a Windows or Unix device that is running RADIUS software.

TACACS: Short for Terminal Access Controller Access Control System, is a client-server-oriented environment, and it operates in a manner similar to RADIUS. Extended TACACS (XTACACS) replaced the original version and combined authentication and authorization with logging to enable auditing.

TACACS+: a TCP-based access control protocol, TACACS+ allows a device to forward a user's username and password to an authentication server to determine whether access can be allowed. TACACS+ itself can also act as an authentication server, if configured so. TACACS+ can also provide authorization and accounting services. TACACS+ services are maintained in a database on a server with TACACS+ daemon running, typically, on a UNIX or Windows workstation. It provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service authentication, authorization, and accounting independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon. The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service.

NIDS: Short for Network Intrusion Detection System, NIDS is a system that attempts to detect hacking activities, denial of service attacks or port scans on a computer network or a computer itself. The NIDS monitors network traffic and helps to detect these malicious activities by identifying suspicious patterns in the incoming packets.

The NIDS can monitor incoming, outgoing, and local traffic. Inspecting outgoing or local traffic can yield valuable insight into malicious activities, just as inspecting incoming traffic can. Some attacks can originate and stay with the local network or be staged inside the network with an outside-the-network target. The NIDS also works with other systems, like a firewall, to help better protect against known attack sources (e.g., a suspected attacker IP address).

SSL/TLS(Secure Socket Layer/Transport Layer Security): SSL and TLS are both cryptographic protocols that provide authentication and data encryption between servers, machines and applications operating over a network (e.g. a client connecting to a web server). SSL is the predecessor to TLS. Over the years, new versions of the protocols have been released to address vulnerabilities and support stronger, more secure cipher suites and algorithms.

Physical security methods:

Biometrics: Biometrics is an authentication mechanism that relies on identification or verification based on unique physiological characteristics. Biometric devices employ fingerprint recognition, hand geometry, retina scanning, and other methods to identify or verify a person based on stored biometric information

Types of Biometrics systems include:

1. **Retina Scanner:** A retinal scan is a biometric technique that uses the unique patterns on a person's retina to identify them.

2. **Iris scanning:** biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance.

3. **Fingerprint reader:** refers to the automated method of verifying a match between two human fingerprints.

4. **Facial Biometrics:** Biometric face scanners identify a person by taking measurements of a person face. For example, the distance between the persons chin, eyes, nose, and mouth. These types of scanners can be very secure assuming they are smart enough to distinguish between a picture of a person and a real person.

Previous Contents Next

CompTIA® Server+ Exam Notes : Logical Access Control Methods

examguides.com/Serverplus/server-plus-15.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

4. Security

4.3 Logical access control methods

Access Control Lists

An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject, an operator, and an object. For instance, if a file has an ACL that contains (Mike, delete, config.exe), this would give Mike permission to delete the file config.exe. This is only to demonstrate what an ACL does, but in actual practice, ACLs could be very complex.

A Linux or UNIX file with the permission 755 means rwx for the owner, rx for the group and others. 4 = read(r) 2 = write (w), and 1= execute(x). In the question, the owner permission is 7, the group permission is 5 and others permission is also 5.

ACLs are basically a set of commands, grouped together by a number or name that is used to filter traffic entering or leaving an interface. ACLs are basically a set of commands, grouped together by a number or name that is used to filter traffic entering or leaving an interface. ACL statements are processed top-down until a match is found, and then no more statements in the list are processed. If no match is found in the ACL, the packet is dropped due to implicit deny. That is, you down type specifically to drop the traffic, but it is understood by the ACL to drop all traffic that does not match atleast one of the statements.

CompTIA® Server+ Exam Notes : Implement Proper Environmental Controls And Techniques

examguides.com/Serverplus/server-plus-16.htm

4. Security

4.4 Implement proper environmental controls and techniques

UPS: The primary purpose of a UPS is to allow saving the cache, and shutdown properly if required. This may take up to 5 minutes or even slightly more. Therefore, it is very important to check whether the UPS is capable of providing the minimum run-time (up-time) for the duration of cache saving and proper shutdown. Note that power rating gets factored while calculating for minimum run-time. Other useful features include intelligent serial and SNMP communication port, voltage boosting and trimming capability, regulation, and others.

The capacity of a UPS is rated in volts ampere (VA), and it is not same as maximum load. As a rule of thumb, if need to multiply the VA with power factor of 0.8, to get a rough estimate of the maximum load your UPC. So a UPS that is rated for 1000 VA cannot provide more than 800 watts. If either of these values is exceeded during operation, the UPS will fail to provide the power you need.

You need to take care of all the following precautions while upgrading the UPS:

1. Choose the UPS such that it meets the present and planned growth in the power requirements of the servers.

2. Ensure that there is sufficient room for placing the new UPS, as the UPS tend to be very bulky.

3. Check whether the UPS software supports the NOS that the server is running.

4. Verify whether the UPS is on the recommended hardware of the server manufacturer.

Remote notification and management have the following advantages:

1. It is possible to monitor the physical health of the server computer without being physically present at the server. It is possible to configure the notification hardware/software such that a pager or email alert is sent out when the problem occurs.

2. It is possible to switch ON/OFF the server remotely. This include graceful shutdown of the server computer.

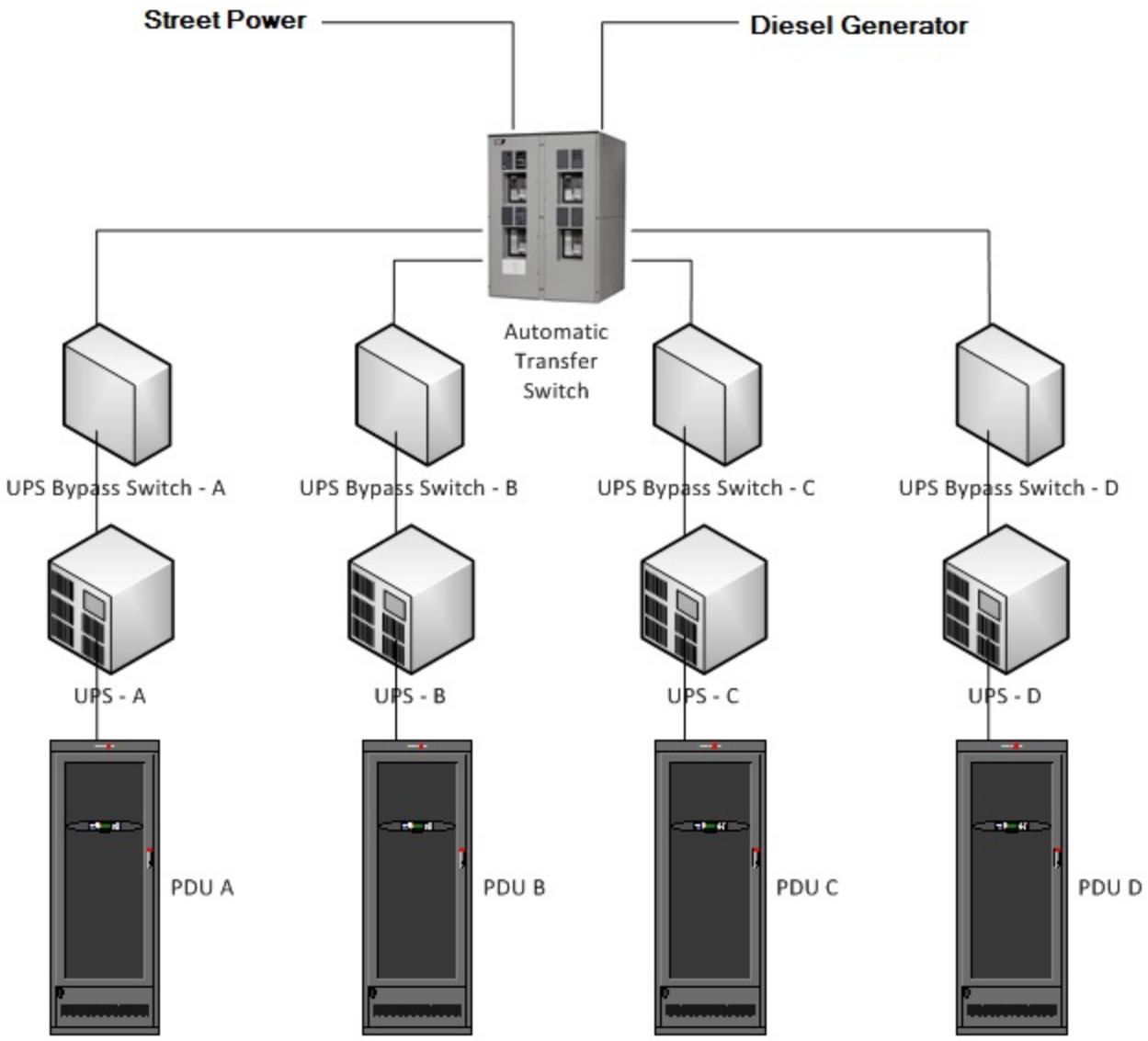
3. Remote management can also allow remote diagnostics on the server, and firmware/BIOS upgrades from a remote location.

4. It is possible to provide remote notification and management services for a server computer. By enabling such feature, failures such as this can be attended immediately. The notification can be in the form of a pager message, e-mail or a phone call.

HVAC: HVAC stands for Heating, Ventilation, and Air Conditioning. HAVAC is used for environmental conditioning of large computer rooms. HVAC is an acronym for heating, ventilating and air conditioning. As the name represents, HVAC system designer will take care of heating, ventilation, and air conditioning of the facility. Preventing fire is done by fire extinguishers, and are not necessarily a part of HVAC. Similarly, EMI shielding and physical security are not part of HVAc.

Blanking panels: Blanking panels also known as filler panels or rack spacer blanks or baffles are installed in server racks to maintain proper airflow. Using a rack without blanking panels results in improper cooling which can lead to thermal damage to the components. If any of the vertical space in a server cabinet remains open, the gaps between rack mount equipment causes a change in airflow through the rack and across the components.

Multiple circuits are useful when the reliability of a data center or a server room is critical to the operations of the organization. By using multiple circuits, it is possible to have redundant stable power supplies in the event of failure of one or the other power supply. A typical server room with multiple circuits is shown in the figure below:



As may be seen in the above diagram, typically, a power scheme consists of utility power and backup generator. The server room or the data center is then connected via UPS and PDU. The design may change depending on the exact requirements such as the up time required for the data center.

Various terms used are described below:

PDU: A Power Distribution Unit (PDU) or Mains Distribution Unit (MDU) is a device fitted with multiple outputs designed to distribute electric power, especially to racks of computers and networking equipment located within a data center.

UPS: Short for Uninterruptible Power Supply, allows a computer to keep running for at least a short time when the primary power source is lost. It also provides protection from power surges. You need to be careful while arriving at the minimum backup time required when buying a UPS. Ensure that you are able to shut down the server gracefully (with all applications closed) without any abrupt power failure.

Bypass Switch: A static bypass is fitted to almost all On-line UPS; it forms a second line of defense. Should the inverter fail, the static bypass ensures the load drops automatically onto the mains input feed.

With an On-line UPS, if an inverter fails, it will, in all probability, occur whilst mains power is present.

A static bypass is usually part of the UPS internal circuitry and may be invoked manually using an external switch. In larger UPS, it will probably synchronize the UPS output with the mains cycle before switching, so may take a few seconds to engage.

Maintenance Bypass: This is fitted externally to the UPS and enables the UPS to be isolated for maintenance or repair without interrupting power to the load.

Wet and Dry Systems: Note that the term wet and dry systems is associated with fire suppression systems.

The following affect the server room environment:

- Regulated power.
- Dust-free environment
- Proper cabling
- Physical security

All the following parameters need to be taken care of while choosing the Server room.

- Temperature / Humidity: Usually air-conditioned environment is suitable for the server room.
- Anti Static precaution: Precaution need to be taken to prevent static electricity build up in your server room. This can be done by choosing proper chairs/ tables, floor mats, and other anti static material.
- The power supply need to be very conditioned. UPS of appropriate rating is a good choice.

Issuing the command "**shutdown** *[minutes] [warning]*" will display a warning on the client computers, that are connected.

This will allow the clients to save their work before the server goes down.

Remember the following points with respect to the server room maintenance:

1. Limit access to the server room - The access to the server room should be limited to few people such as systems administrators, and Backup operators who need access for performing their duties. Others such as common users, and visitors should be restricted from entering the server room. The access can be restricted by using lock and key.

2. Regulate the server room environments as applicable. The server room environmental conditions such as humidity, and temperature must be regulated as required based on the vendors recommendations.

3. Do not allow dust to enter the server room. The server room should be maintained dust free. This will eliminate lot of potential problems that may result in storage media corruption, hardware failure, etc.

4. Use UPS: It is highly recommended to use UPS for server backup. If the mains fail or if there are any temporary power blockage, you need time to save the contents in the temporary memory to the disk and also to shut down the server if required. Note that the UPS must be able to provide a run-time that is at least sufficient to backup the cache, and for proper shutdown. Also, if the server services are required without interruption, procure a backup generator.

5. ESD protection: If you intend to do any diagnostics or card level repairs in the server room, ensure that the place is free from static electricity. Static electricity may easily damage memory and other cards if handled with bare hands without proper ESD protection.

6. Keep the backup tapes (at least weekly/monthly full backups) away from the server room at a different safe and secure place.

Safety

Automatic fire suppression systems control and extinguish fires without human intervention. Examples of automatic systems include fire sprinkler system, gaseous fire suppression, and condensed aerosol fire suppression.

When choosing the right system for your facility, you may have some questions whether you want to have "wet fire sprinklers" or "dry fire sprinklers."

Wet pipe systems: In wet pipe systems, the overhead sprinkler piping connected is filled with water under pressure. When a fire causes one or more of the connected sprinklers to activate, water immediately discharges from the sprinkler head. Wet pipe systems are the most common type of fire sprinkler system and the simplest.

Dry fire sprinkler systems: Dry fire sprinkler systems do not have water in the direct non-heated sprinkler piping, but only pressurized air or nitrogen. The pressurized air holds back the water supply at a main dry-pipe valve. When a fire occurs and the sprinkler activates, the air pressure drops and the main dry-pipe valve opens to release the water into the piping system to discharge from the sprinklers. These fire sprinkler systems are thus designed for environments with freezing temperatures like walk-in refrigerators, loading

docks, and warehouses. Because of its special air pressure needs and other components, dry pipe sprinklers are more complex than wet fire sprinklers and are thus more costly to install and maintain.

Lift techniques is associated with proper lifting of materials in a data center or server room without personal injury.

ESD, short for Electro Static Discharge is associated with handling of sensitive components so that they are not damaged due to ESD.

Rack Stability: This term is associated with securing server room racks properly to prevent any damage to the equipment as well as people working in the server room.

ESD(Electro Static Discharge) procedures: It is important to know that ESD damage may not be known immediately. A component may only suffer degradation in performance, which may show up only at a later date. In some cases, an ESD may result in the failure of the component instantly. ESD may irreversibly damage electronic components if proper precautions are not taken. Every time you open the computer case, ensure that you have taken appropriate ESD precautions to prevent damage to the sensitive components.

The following are the ESD(Electrostatic Discharge) precautions necessary while working on server computers

- Use wrist straps.
- Use static protective bags
- Ensure grounding of proper static protected work stations
- Check periodically to ensure that static protected work station is alright.

The following are required for appropriate ESD protection:

- Wear anti-static wrist or foot strap
- Use antistatic mat
- Ensure proper grounding of the anti-static workstation (The workstation includes an anti-static wrist/foot strap, anti-static mats).
- Also, make sure that you turned off the computer and removed the mains plug from the computer. Also remove any modem or battery connections.

Previous Contents Next

CompTIA® Server+ Exam Notes : Ip Addressing And Infrastructure Services

examguides.com/Serverplus/server-plus-17.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

5. Networking

5.1 IP addressing and Infrastructure services

Each computer on the Internet having a unique IP address is known as a HOST. IP address is a logical address and used for routing packets over an IP network.

IP addresses are written using decimal numbers separated by decimal points. This is called dotted decimal notation of expressing IP addresses.

The different classes of IP addresses is as below:

Class	Format	Leading Bit Pattern	Network address Range	Maximum networks	Maximum host/nodes
A	N.H.H.H	0	1.0.0.1 to 126.255.255.254	127	16,777,214
B	N.N.H.H	10	128.1.0.1 to 191.255.255.254	16,384	65,534
C	N.N.N.H	110	192.0.1.1 to 223.255.254.254	20,971,52	254

D	N.A.	N.A.	224.0.0.0 to 239.255.255.255	N.A.	N.A.

- Network address of all zeros means "This network or segment.
- Network address of all 1s means "all networks", same as hexadecimal of all Fs. 255.255.255.255 broadcasts to all hosts on the local network.
- Network number 127 is reserved for loopback tests, ie any IP in the range 127.x.x.x is reserved for the loopback or localhost, for example, 127.0.0.1 is the loopback address.
- Host(Node) address of all zeros mean "This Host (Node)".
- Host (Node) address of all 1s mean "all Hosts (Nodes) " on the specified network.
- The range of numbers from 224.0.0.0 to 239.255.255.255 is used for multicast packets. This is known as Class D address range.
- it doesn't have network and host bits. If it's a multi-cast address then one IP would go to multiple machines because all have that IP.
- Class E addresses are reserved for future use, or Research and Development Purposes.

Subnetting:

The following are the advantages of subnetting:

1. The network congestion improves

2. IP addresses can be efficiently used

3. Security can be improved (Since it requires a router to switch traffic from one subnet to another, only hosts on a particular subnet can see the packets)

Private and Public IP addressing:

A public IP address is the address that is assigned to a computing device to allow direct access over the Internet. A web server, email server and any server device directly accessible from the Internet are candidate for a public IP address. A public IP address is globally unique, and can only be assigned to a unique device.

A private IP address is the address space allocated by Inter NIC to allow organizations to create their own private network. There are three IP blocks (1 class A, 1 class B and 1 class C) reserved for a private use. The computers, tablets and smartphones sitting behind your home, and the personal computers within an organizations are usually assigned private IP addresses. A network printer residing in your home is assigned a private address so that only your family can print to your local printer.

When a computer is assigned a private IP address, the local devices see this computer via it's private IP address. However, the devices residing outside of your local network cannot directly communicate via the private IP address, but uses your router's public IP address to communicate. To allow direct access to a local device which is assigned a private IP address, a Network Address Translator (NAT) should be used.

NAT/PAT: NAT is the process of "translating" an IP Address in a router or firewall. This is most commonly done to present a private IP Address into a Public IP Address that is accessible on the Internet. For instance, you may want to have your E-mail server have a public address so that it can route mail.

The router will have a mapping of the internal and external IP Address Mappings. When any traffic from the inside interface travels over the outside interface, the router changes the source IP Address. When the return traffic gets back to the router the destination address will be the outside IP Address and will then be "translated" back to the internal IP Address.

PAT works in a very similar manner to the description of NAT above. The difference being that all of the internal machines can share a single translation address.

When an inside machine sends traffic to the router, the router builds a table with the inside IP Address, the source port and then uses a translated address and a new port ID. This way it can track where the traffic came from, so when the destination machine returns the traffic, the router knows where to send it.

IPv6 Addressing: IANA (Internet Assigned Numbers Authority) is the organization under the Internet Architecture Board (IAB) of the Internet Society that oversees the allocation of Internet Protocol addresses to Internet service providers (ISPs). ICANN (a non governmental organization) has now assumed responsibility for the tasks formerly performed by IANA. ISPs in turn allot IP addresses to small companies, and businesses.

The IPv6 protocol defines a set of headers, including the basic IPv6 header and the IPv6 extension headers. The following figure shows the fields that appear in the IPv6 header and the order in which the fields appear. IPv4 addresses use the last 32 bits of the IPv6 address.

```
Loopback address 1 0:0:0:0:0:0:0:1 (::1)
Private ranges: FEC0:: (proposed)
Auto-configured addresses FE80::
```

Note: Leading zeroes in a hextet can be left out and consecutive hexlets consisting of all zeroes can represented with a double colon.

3 types of addresses are supported in IPv6:

1. Unicast: one-to-one with various scopes (i.e. Global, Link, Unique Local, Compatible)

2. Anycast: one-to-nearest (allocated from unicast)

3. Multicast: one-to-many

Broadcast has disappeared as a term, but is considered one form of multicast.

IPv6 packet is 128 bits long. It will have basic packet header, and optional extension header. The next header field within an extension header points to the next header in the chain.

The extension header may include the following:

- Hop-by-Hop options
- Destination options
- Routing (specifies intermediate routers that the route must include forcing an administratively defined path)
- Fragment (Used to divide packets that are too large for the maximum unit (MTU))
- Authentication and Encapsulating Security Payload (ESP)

Multicast addresses from FF01:: through FF0F:: are reserved, well-known addresses. To identify all nodes for the node-local and link-local scopes, the following multicast addresses are defined:

- FF01::1 (node-local scope all-nodes address)
- FF02::1 (link-local scope all-nodes address)

To identify all routers for the node-local, link-local, and site-local scopes, the following multicast addresses are defined:

- FF01::2 (node-local scope all-routers address)
- FF02::2 (link-local scope all-routers address)
- FF05::2 (site-local scope all-routers address)

In an IPv6 network, a host can autoconfigure its IP address without the help of a DHCP server.

Question: Which of the following are valid IP addresses? (Choose 2 best answes).

a. 202.122.154.11

b. 127.96.187.22

c. 150.206.256.31

d. 175.207.180.66

Answer:

1. A valid IP address on a host / node can't start with 127. 127.X.X.X is reserved for local loop back.

2. A valid IP address can't be larger than 255 (in any octet).

The user is able to connect to the FTP server using IP address. The DNS server needs to be specified for connecting using FQDN (Fully Qualified Domain Name).

NIC (Network Interface Cards) teaming: NIC teaming is a technology in which multiple NICs are configured to form a single virtual connection to the external switch.

The purpose multiple network adapters on a computer are:

1. Bandwidth aggregation

2. Traffic failover to prevent connectivity loss in the event of a network component failure

Two or more NICs are grouped together forming one virtual connection. The entire group will have only one IP address. But all the NICs will have individual MAC addresses. There can be more than one group in a Server. NIC Teaming is also known as load balancing and failover (LBFO). Connecting each NIC to a separate switch offers best network connectivity.

Previous Contents Next

CompTIA® Server+ Exam Notes : Various Ports And Protocols

examguides.com/Serverplus/server-plus-18.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

5. Networking

5.2 Various ports and protocols

Some of the important protocols and the corresponding ports are as given below:

1. SNMP 161 : Simple Network Management Protocol (SNMP) is used for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. SNMP is used for remotely monitoring of a TCP/IP network.

2. SMTP 25 : SMTP is an abbreviation that stands for Simple Mail Transfer Protocol. This protocol allows applications to transmit email messages over the Internet. Basically, SMTP handles your outgoing mail. Your email application connects to your mail server via SMTP and sends the messages. Receiving emails, however, utilizes two other different protocols - POP3 or IMAP.

3. FTP 20/21: Short for File Transfer Protocol, FTP is a client - server protocol used sending and receiving files between two computers. For example, FTP is used by web developers to connect to the web server using FTP and send web pages to the server (acting as FTP server).

4. SFTP 22: The SSH File Transfer Protocol (SFTP), also known as the Secure File Transfer Protocol, enables secure file transfer capabilities between networked computers (hosts). Unlike the Secure Copy Protocol (SCP), SFTP additionally provides remote file system management functionality, allowing applications to resume interrupted file transfers, list the contents of remote directories, and delete remote files.

5. SSH 22 : The program SSH (Secure Shell) provides an encrypted channel for logging into another computer over a network, executing commands on a remote computer, and moving files from one computer to another. SSH provides strong host-to-host and user authentication as well as secure encrypted communications over the Internet.

6. SCP 22: Secure copy or SCP is a means of securely transferring computer files between a local host and a remote host or between two remote hosts. It is based on the Secure Shell (SSH) protocol.

7. NTP 123: NTP stands for Network Time Protocol, and it is an Internet protocol used to synchronize the clocks of computers to some time reference.

8. HTTP 80: HTTP, the Hypertext Transfer Protocol, is the application-level protocol that is used to transfer data on the Web (most popular use is on World Wide Web). HTTP comprises the rules by which Web browsers and servers exchange information. There are various flavors of HTTP.

9. HTTPS 443: Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP. The 'S' at the end of HTTPS stands for 'Secure'. All communications between your browser and the website are encrypted.

10. TELNET 23: Telnet is again a Client/Server protocol that allows you to connect to remote computers (called hosts) over a TCP/IP network (such as the Internet). Using telnet client software on your computer, you can login to a telnet server (i.e., the remote host). Once your telnet client establishes a connection to the remote host, your client becomes a virtual terminal, allowing you to communicate with the remote host from your computer. Usually, you need a pre-existing account to login to the remote host using telnet.

11. IMAP 143: IMAP (Internet Message Access Protocol) is a protocol for retrieving email messages and working with mailboxes on a mail server using an email client. Simple Mail Transfer Protocol is a corresponding protocol used to send outgoing mail to an IMAP server.

12. POP3 110: Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client, such as Mozilla Thunderbird or Outlook. POP3 allows you to download email messages on your local computer.

Telnet is used for terminal emulation.

FTP is used to transfer files.

HTTP (Hyper Text Transfer Protocol) and HTML (Hyper Text Markup Language) used for browsing the Web.

POP3 (used for incoming messages) Secure (SSL) port number: 995

SMTP Server (used for outgoing messages) Secure (SSL) port number:465

Previous Contents Next

CompTIA® Server+ Exam Notes : Cable Management Procedures

examguides.com/Serverplus/server-plus-19.htm

5. Networking

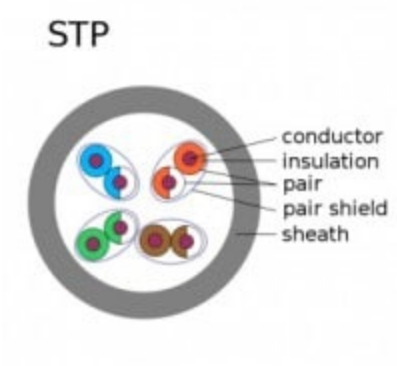
5.3 Cable management procedures

Cable assembly is a professional job. Improperly made cables may create network outages, and lost business. Unless one is well experienced and proper tools, the work be better outsourced.

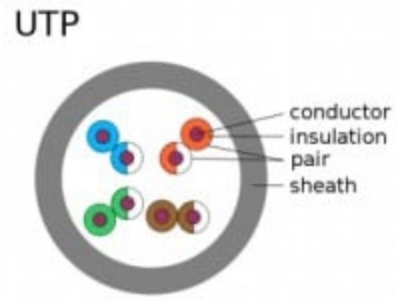
It is often recommended to lay the fiber for back bone, since it is immune to EMI and also can carry higher bandwidths.

Shielded Twisted Pair (STP): STP cables reduce electrical noise and electromagnetic radiation. In other words, they help to keep the signal steady, and reduce interference with other devices. Given below is a diagram showing a typical shielded twisted pair cable

Unshielded Twisted Pair (UTP): UTP cables do not have shielding to reduce interference. They are designed to cancel electromagnetic interference with the way the pairs are twisted inside the cable. Unshielded twisted cables are most widely used for office LANs, though recently wireless LANs are more widely used. Unshielded cables are lightweight, thin and flexible. They are also versatile and inexpensive. A typical UTP cable cross section is shown in the figure below:



The twisting of the pairs in typical Ethernet cabling provides some resistance to EMI/RFI, enough for use in the vast majority of applications. However, highly static prone areas like generator rooms or high voltage equipment rooms may need shielding of cables.



One dis-advantage of shielding is that you need to ground the connectors properly on the terminating ends of the cable, else static may build on the outer sheath of the cable and interfere with the signals, thus becoming worse than having no shielding at all.

1000BASE-T: 1000BASE-T, also known as IEEE 802.3ab is a standard for gigabit Ethernet over copper wiring. It requires, at least Category 5 cable, but Category 5e ("Category 5 enhanced") or Category 6 cable may also be used and are often recommended. 1000BASE-T requires all four pairs to be present and is far less tolerant of poorly installed wiring 10BaseT/100BaseT/1000BaseT use RJ-45 connector.

Different types of cabling standard

Ethernet cables are grouped into sequentially numbered categories ("cat") based on different specifications; sometimes the category is updated with further clarification or testing standards (e.g. 5e, 6a). These categories are how we can easily know what type of cable we need for a specific application.

	CAT3	CAT5	CAT5e	CAT6	CAT6e	CAT7
Speed	16 Mbps	100 Mbps	1000 Mbps	10/100/1000Mbps and 10 Gbps	10/100/1000 Mbps and 10 Gbps	10/100/1000 Mbps and 10 Gbps
Limitation	Ineffective for Higher - speed networks often found in older 10 BaseT networks	Range of 100 meters	Range of 100 meters	Range of 100 meters	Range of 100 meters	Range over 100 meters

Important points to remember

- Cat 5e or better cable type is used for Gigabit Ethernet network cabling. Cat5e cable contains four twisted pairs of wires for Gigabit Ethernet
- Category 3 - Used in 10BASE-T networks. Can transmit data at speeds up to 10 Mbps.
- Category 5 - Can transmit data at speeds up to 100 Mbps. Widely used in 100Base-T Ethernet networks.
- Category 5e - Used in networks running at speeds up to 1000 Mbps (1 gigabit per second [Gbps]). The Cat-5e cable may be used in 1000BaseT Ethernet network. Both Cat -5 and 5e are almost same, except for better noise (cross talk, etc.) specs associated with 5e.

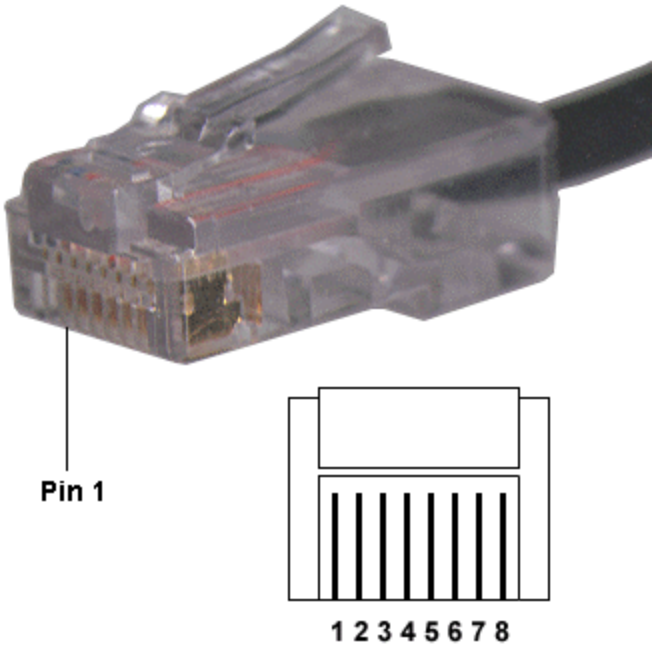
- Category 6 cable, commonly referred to as Cat-6, is a cable standard for Gigabit Ethernet and other network protocols that is backward compatible with the Category 5/5e and Category 3 cable standards. The cable contains four twisted copper wire pairs. This is the same as CAT5 and CAT5e copper cable standards. The cable standard is suitable for 10BASE -T / 100BASE-TX and 1000BASE -T / 1000BASE-TX (Gigabit Ethernet).
- The Category 7 cable standard has been created to allow 10 Gigabit Ethernet over 100 m of copper cabling. CAT 7 is backwards compatible with traditional Cat5 and Cat6 Ethernet. Cat7 offers strict specifications for crosstalk and system noise than Cat6. Shielding has been added for individual wire pairs on the Category 7 cable. Cat7 has been designed as a standard for Gigabit Ethernet over 100m of copper cabling The cable contains four twisted copper wire pairs, just like the earlier standards.

CAT6 is rated for gigabit Ethernet while CAT6e is thicker and rated for 10 gig Ethernet. Typically CAT5e is sufficient and can also handle gig Ethernet, but noise margin will be less.

Connectors

An RJ-45 connector has 8 connection pins and can accommodate 4 pairs of wires.

The connector shown in the exhibit is RJ-45 connector. RJ-45 connector is the most commonly used connector in 10BaseT, and 100BaseT networks. RJ-11 connectors are commonly available either with 4-wire or 6-wire, whereas RJ-45 has 8 wires (4-pairs). An RJ-45 connector has 8 connection pins and can accommodate 4 pairs of wires. Typically, a UTP cable with RJ-45 connectors is used to connect the NIC card on the home computer with the DSL broadband modem.

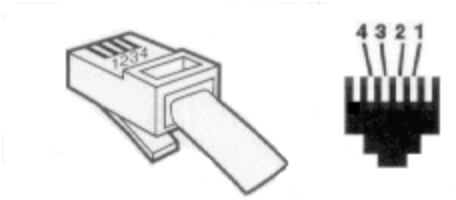


RJ-48C: RJ-48C connectors are 8-pin jacks (think RJ-45) used with T1 lines. Pins 1, 2, 4, and 5 are used for data (1 and 2 for receiving; 4 and 5 for transmitting), and pins 7 and 8 are used for cable shield integrity. Pins 3 and 6 are not used. A common connection type used to connect to a CSU/DSU is an RJ-48C.

RJ-11 (Registered Jack) connectors are small plastic connectors used on telephone cables.

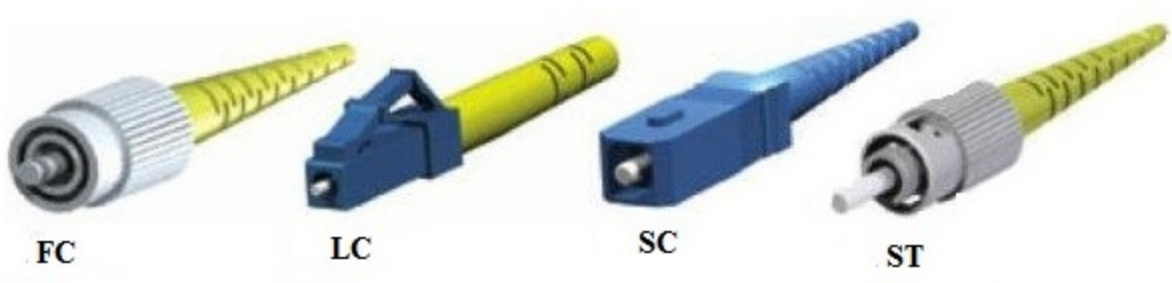
The connector shown in the exhibit is a 4-wire RJ-11 connector. RJ-11 connectors are also available in 6-wire.

Two frequently used Firewire connectors are 4-pin connector, and 6-pin connector. A 4-pin connector does not carry power through the connector, whereas a 6-pin connector carries the dc-power required for operating the connected device.



RS-232: RS-232 (Recommended Standard) is a TIA/EIA standard for serial transmission between computers and peripheral devices.

Fiber Connectors: The below figure shows the different fiber connector types .



1. ST connectors: These connectors are the most common type of commercial fiber optic connector. These connectors utilize an exposed plastic tube housing the optical fiber. This requires a connection to a matching cable on the other side, incorporating a connector that mates to the other. These combine in a spring-loaded twist, reminiscent of BNC connectors, and are noted for their reliability. ST connector is very popular in communication applications, such as LANs and CCTV systems.

2. SC-Connector: SC is short for Subscriber Connect is one of the most frequently used connectors. Used in fiber-optic networking, it has caps to prevent laser light reaching eyes. The connector usually in pairs (transmit and receive), often clipped together. connectors have the ferrule that houses the fiber mostly concealed. Probably the most similar commercial equivalent of To slink, SC connectors does not require a mating cable on the other side. Instead, these snap-on connectors simply push into their jacks with a click. SC connectors use a push-pull design and can be used for simplex or multiplex applications

3. FC connector: It is similar to ST connectors, these fiber optic connector's screws into their mating jacks. Additionally, the tube surrounding the optical fiber is typically shrouded in ceramic or metal, as opposed to being fully exposed. The inner ring of the connector is keyed to ensure positive mating to its corresponding jack. FC connectors are primarily used

with single mode fibers and used in telephone, instruments, and high-speed communication links. The style is similar to that of an ST connector, but it uses a threaded connection which makes it better suited for high vibration environments.

4. LC cables: latch and release into their jacks in a manner similar to Ethernet connectors. Smaller in form than SC connectors, their durability is not compromised, nor is cost increased. Instead of snapping or thermo forming the connector to the cable, it is glued. This makes it a popular connector for field use. LC connectors are used in private and public networks, and are gaining in popularity due to their small form factor (SFF) optical transmitter/receiver assemblie

LC connector is a miniaturized version of the fiber-optic SC connector. It looks just like the SC, but is half the size with a 1.25 mm ferrule instead of 2.5 mm. 1000BASE-FX should use SC, ST, LC, MTRJ or MIC connectors with SC being the preferred option. MT-RJ Connector, LC Connector are small form factor connectors.

Usually, cable modems use F-type female connector to connect to the broadband provider.

ST (Short for Straight Tip) connectors, and SC (short for Subscriber Connect) connectors are typically large connectors. MT-RJ, and LC (short for Local Connector) have small form factor, and allow higher port density. These connectors (MT-RJ and LC) allow higher number of fiber optic connections in a smaller area, and hence desirable when there are a large number of fiber optic terminations to be made.

SFP (Small Form-factor Pluggable): SFP is a small transceiver that plugs into the SFP port of a network switch and connects to Fibre Channel and Gigabit Ethernet (GbE) optical fiber cables at the other end. Superseding the GBIC transceiver, SFP modules are also called "mini-GBIC" due to their smaller size. By choosing the appropriate SFP module, the same electrical port on the switch can connect to fibers of different types (multi-mode or single-mode) and different wavelengths. If the fiber is upgraded, the SFP module is replaced.

The SFP converts the serial electrical signals to serial optical signals and vice versa. SFP modules are hot swappable and contain ID and system information for the switch.

Rollover cable (also known as Cisco console cable): It is a type of null-modem cable that is often used to connect a computer terminal to a router's console port. This is typically a flat blue color that distinguishes itself from other types of network cabling. It is most commonly used to connect a computer terminal to a router's console port.

Straight through and Cross over cables: Ethernet network cables are primarily straight or crossover. This Ethernet network cable is made of 4 pairs of wires that consists twisted pair conductors (totally 8 conducting wires) that used for data transmission. Both end of cable is terminated with RJ45 connector. The wires in straight through cable are connected

to the RJ-45 in the same pattern on either end of the cable, where as in Cross over cable, transmit and receive pin wires are interchanged. The straight through cable is used for connecting a computer to a hub or switch. The Cross over cable is used for connecting a switch to another switch or a hub.

Note: Sometimes, switches will have an "uplink" port. If you are connecting to an "uplink" port of a switch from the regular port of another switch/hub, you need to use straight-through cable. If you are connecting to a regular RJ-45 port of a switch from another switch's regular RJ-45 port, then you need to use Cross-over cable. Similarly, if you want to directly connect two computers, then you need to use Cross-over cable. This is because, the transmit at one end becomes receive port at the other end.

Patch cable is a generic term used, and may represent any cable that connects two networking devices. They are typically CAT5 / CAT5e/CAT6 Ethernet cables linking a computer to a nearby network hub, switch or router.

Previous Contents Next

CompTIA® Server+ Exam Notes : Disaster Recovery Concept

examguides.com/Serverplus/server-plus-20.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

6. Disaster Recovery

6.1 Disaster recovery principles

Disaster recovery plan: Disaster Recovery Planning is a practice in which organizations develop policies and procedures to ensure rapid restoration of computer systems and resumption of computer-based operations in the event of a systems disruption. In light of the essential role computers play in virtually all companies, DRP is a critical step in ensuring post-disaster business continuity.

Broadly, disaster recovery plan can be divided into:

1. Risk analysis

2. Establishment of budget,

3. Implementation and testing.

Site Types:

Hot Site: A Hot Site can be defined as a backup site, which is up and running continuously. A Hot Site allows a company to continue normal business operations, within a very short period of time after a disaster. Hot Site can be configured in a branch office, data center or even in cloud. Hot Site must be online and must be available immediately.

Hot site must be equipped with all the necessary hardware, software, network, and Internet connectivity. Data is regularly backed up or replicated to the hot site so that it can be made fully operational in a minimal amount of time in the event of a disaster at the original site. Hot Site must be located far away from the original site, in order to prevent the disaster affecting the hot site also.

Warm Site: A Warm Site is another backup site, is not as equipped as a Hot Site. Warm Site is configured with power, phone, network etc. May have servers and other resources. But a Warm Site is not ready for immediate switch over. The time to switch over from the disaster affected site to Warm Site is more than that of a Hot Site. But less cost is the attraction.

Cold Site: Cold Site contain even fewer facilities than a Warm Site. Cold Site will take more time than a Warm Site or Hot Site to switch operation but it is the cheapest option. Cold Site may contain tables, chairs, and basic technical facilities but will require days or even weeks to set up properly and start operation from Cold Site

Previous Contents Next

CompTIA® Server+ Exam Notes : Backup Techniques

examguides.com/Serverplus/server-plus-21.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

6. Disaster Recovery

6.2 Backup techniques

Grandfather-Father-Son: It is a backup strategy that provides reliable and complete backup plan for entire year. It contains incremental daily backups, FULL weekly backups, and monthly FULL backups. The daily backup tapes are rotated every week. If you take incremental backups 4 days a week, the tape gets rotated on the fifth working day. Therefore, you need 4 tapes for daily backups. The weekly FULL backup tape is rotated after every 4 weeks. That means you need 4 tapes for weekly backup. Also, FULL backup is taken every month. It is recommended to keep the monthly backup tape away from the server premises for safety and security reasons. For 12 months you need 12 tapes. Therefore, it adds up to:

4 incremental daily backup tapes + 4 weekly FULL backup tapes + 12 monthly FULL backup tapes. This is equal to 20.

The above is assuming a 5-day workweek. If you have 6-day workweek, you may tend to take incremental backups for 6 days a week (including Saturday). Then the tapes required for incremental backups become 5, and the total number of tapes required would be 21.

The only tape required would be the FULL monthly backup tape corresponding to the said month. Note that daily incremental backup tapes get rotated every week, and the weekly full backup tapes get rotated every 4 weeks. Only monthly backup tapes are stored securely for

one full year. Therefore, to restore a file that was 6 months before, you need only one monthly backup tape corresponding to that period.

The name Grandfather-Father-Son (GFS) name has come as below: The oldest tapes correspond to Grandfather. Here monthly backup tapes are the oldest tapes, since these backups are taken only once a month and stored away at a secure place. The older tapes (weekly full backups) correspond to father. These tapes are younger than monthly backup tapes, but older than daily incremental backup tapes. And finally, the daily incremental backup tapes correspond to Son (daily incremental backups contain the youngest data). Hence the name Grandfather-Father-Son (GFS).

Grandfather-father-son (GFS) and Tower of Hanoi are two good rotation schedules providing a long and varied history of file versions. Both provide comprehensive recovery capabilities.

Grandfather-Father-Son:

In GFS, "Son" is the incremental or differential daily back-up, "Father" is the full weekly back-up, and "Grandfather" is the monthly full back-up.

Tower Of Hanoi:

Tower of Hanoi got its name from an ancient Chinese game using recursive techniques. In the game, you move a stack of disks from one of the pegs to another peg and a smaller disk can only be placed on a larger disk. Like the game, many multiple media sets are rotated through in incremental and full back-ups. It uses more media sets than GFS for increased safety.

There are three main Backup strategies:

1. Full Backup: Backs up all data. Takes the longest time to backup, but easy to restore since all files are at one place and you don't need previous back-ups.

2. Incremental backup: Only backs up files added or changed since last backup. Quick to back up, but restore requires multiple tapes (last full backup tape plus all incremental tapes since the last full backup). Incremental backup is a backup of all changes made since the last backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changes made since the last backup. The result is a much faster backup then a full backup for each backup run. Storage space used is much less than a full backup and less than with differential backups.

3. Only backs up files: Since last FULL backup. Each backup takes a little longer, but restore requires only two tapes (most recent full backup and most recent differential backup).

Both Full backup and Incremental backups reset the archive attribute on a file.

It is important to ensure that your back-up is proper. This can be checked by performing a restore procedure on a redundant computer or on a disk directory. There is always a chance to backup data that can't be restored. Even doing double back-up may not be very helpful, unless you ensure that the backup is proper.

Previous Contents Next

CompTIA® Server+ Exam Notes : Troubleshooting Theory And Methodologies

examguides.com/Serverplus/server-plus-22.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

7. Troubleshooting

7.1 Troubleshooting theory and methodologies

For better security, clearly defined, implemented and documented security policies and procedures need to be developed. All the people concerned in your organization need to be aware of these policies.

It often occurs that a user or a group of users are not able to login or unable to access certain resources. The possible causes are given below:

1. Incorrect password or error typing the password: In most OSes, the passwords are case sensitive. Ensure that the User has entered the password correctly.

2. Account disabled or locked or expired: It is often possible that an admin enable password expiry after certain number of days, or that a User account is locked up after certain number of unsuccessful login attempts. Check for the same.

Inability to contact the domain controller or the DNS Server: Provided that there are no networking problems, it is possible that the User computer is configured wrongly due to whatsoever reason. Verify the the domain controller (if used for User authentication) is

reachable from the User computer. Similarly, inability to reach DNS server or that the DNS server is not UP, may result in the User login failure. Check that proper IP address, net mask and gateway are properly configured.

There are several stages in troubleshooting a server problem as given below:

1. Identifying the problem and determine the scope

2. Establishing a theory of probable cause

3. Testing the theory to determine cause

4. Establishing a plan of action to resolve the problem and notify impacted users

5. Implementing the solution one step at a time and escalate if necessary

6. Verifying the full system functionality and if applicable implement preventative measures

7. Perform a root cause analysis

8. Document findings, actions and outcomes throughout the process

As may be seen from the above, you need to document the findings, actions and outcomes throughout the process.

More realistic password policy is that

1. Ensure that the users change the pass words at regular intervals

2. Ensure that the length of the password is above certain minimum characters/digits.

Previous Contents Next

CompTIA® Server+ Exam Notes : Troubleshooting Hardware Problems

examguides.com/Serverplus/server-plus-23.htm

7. Troubleshooting

7.2 Troubleshooting hardware problems

POST (Power On Self Test): It is a vital part of PC boot process. The first thing that BIOS does is to call POST for inspecting various parts of your PC hardware before actual BIOS boot process starts. POST continues even after the BIOS boot process is started, checking various parts of the PC such as memory as it boots.

BIOS/POST (Power On Self Test) produces audio beep codes and/or video message indicating the boot status. Less known is the fact that BIOS of most PCs also send out diagnostic test codes to a specified memory location. By using a special card, called BIOS POST Diagnostic card, it is possible to diagnose the exact nature, and location of the fault. These cards come with an LED display that displays the codes. The POST Diagnostic cards usually work with either ISA, EISA OR PCI.

There are several error codes that are built into POST. Some of these are:

1. CMOS memory size mismatch - This error indicates that the stored memory size value is not matching what is measured currently. If this error occurs during first boot or after memory up gradation, just ignore this error. However, if this error occurs repeatedly, there might be some problem.

Note that there are no POST error codes such as Hard disk data read error or Network card failure. It is important to go through the process of POST and BIOS boot sequence and observe various events.

2. Wake-On-LAN facilitates server maintenance remotely. If you find any problem with connecting to a remote server, it is likely that the operating system has not detected the network card properly. Therefore, it is recommended to install appropriate driver that was supplied by the vendor along with the card.

Improper shutdown: Some problems may arise due to improper shutdown. User appropriate shutdown command.

1. Windows 2008/2012: Issue shutdown /s command at the command prompt. Various other options are also available.

2. Unix/ Linux: There are various options and versions. Generally "Shutdown now" will start the shutdown process. In addition, you can add -r option to the command to make the system to reboot after shutdown.

Sever Assembly checklist:

The following precautions need to be taken before the actual assembly process:

1. Wear antistatic wrist or foot strap

2. Use antistatic mat

3. Ensure proper grounding of the anti-static workstation (The workstation includes an anti-static wrist/foot strap, anti-static mats).

4. Avoid material such as carpeted floors, packing foam, wool, and plastic.

5. Avoid holding the cards by their finger contacts. Always hold the cards by their edges or rails.

6. DO NOT remove the cards from their anti-static bags unless they are ready to be assembled. Remove the card from the anti-static bag only when you are assembling it.

7. Ensure that the power is switched off and the power cord is taken out of the mains.

Server Hardening:

It is recommended to disable unused ports in a server computer as part of hardware and software hardening. Two ways that you could disable USB ports are:

1. By using Device Manager

2. By using BIOS

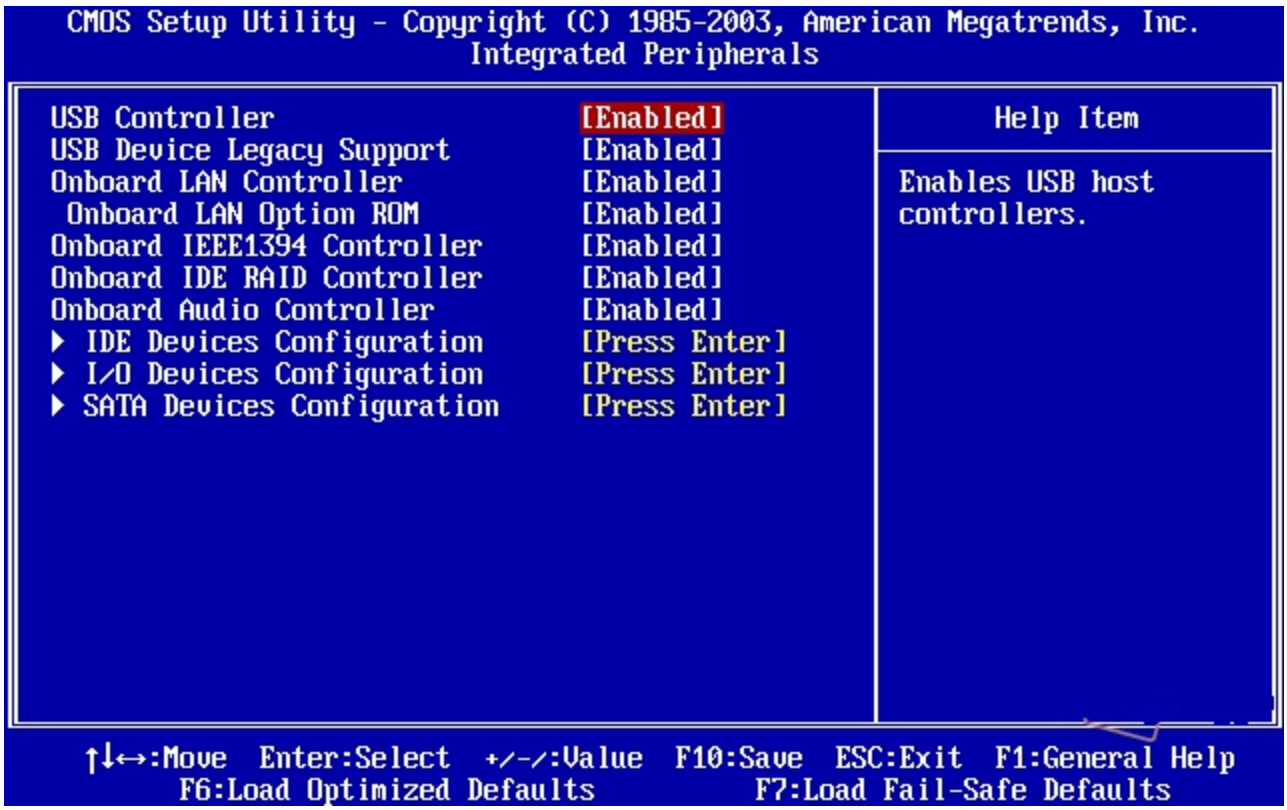
1. By using Device Manager: The Device Manager may be opened in several way as mentioned below:

You can open Device Manager in any of the following ways:

- Using the Windows interface (Control panel -> Hardware and Sound -> Device Manager)
- Using Computer Management (Start -> Right Click Computer -> Manage, then select Device Manager))
- Using a command line (At a command prompt, in the Start Search box, or the Run box, type the command: mmc compmgmt.msc)

Once you are in the Device Manager, you can right click the USB Controller, and select Disable. This will disable the device.

2. By Using BIOS: This is another way to disable USB ports on a computer. Just go to the BIOS setup while starting the computer, and disable the USB ports. Note that you had set the BIOS password prior to making any hardening using BIOS. A sample display is shown below:



You can set the USB controller to Disabled state using toggle key.

Note that WOL, short for Wake On LAN is used to start a computer remotely without being physically present at the computer itself. For server computers, it is recommended to disable WOL for security reasons.

Generally, the following precautions need to be taken when upgrading or troubleshooting memory:

1. Ensure that the memory modules are seated properly: Make sure the notches in your module are lined up with the keys in the slot, then press down. You may need to apply a lot of pressure to properly "seat" the module. If installed properly, the clips on the side of module should snap into place on their own.

2. Update your BIOS: If your computer is older, it may need a BIOS (Basic Input Output System) update in order to work with today's technology. To update your BIOS, contact your system or motherboard manufacturer and they'll direct you to where you can download the software and provide update instructions.

3. Use same type of memory: Make sure that your new memory is the same type as your old memory (i.e. FPM/EDO/SDRAM, parity/non-parity/ECC, buffered/unbuffered).

4. Fill your slots starting with the largest density and working to the smallest (put the largest module in slot 0, and the second largest in slot 1, and so on). Some systems go in reverse order, so if this doesn't work, try reversing the procedure.

5. Memory mismatch error: If you get a memory mismatch error follow the prompts to enter setup, then select save and exit. (This is not an error - some systems must do this to update their CMOS settings.)

When an additional memory is installed, it is usual to get an error during initial start-up that the memory is incorrect. Just enter the BIOS and specify that the new memory value is correct.

Upgrading Server:

Generally, the following Server components may have the BIOS of their own, which need to be considered during any upgrade to the Server.

The actual firmware upgrade takes only a few minutes. However, planning the upgrade and obtaining the suitable firmware upgrade and preparing a checklist of activities may take much longer.

1. SCSI adapters

2. RAID Controllers

3. Video cards

4. Mother boards

Note that, some times a network card may misbehave and produce higher than normal interrupts causing process problems. If this were the case, the processor utilization would be low and can be identified poor processor utilization.

It is often required that the system BIOS may need to be upgraded for adding a second processor. One need to check with the documentation and the vendors web site for details before going ahead with the up gradation.

Now that there are several command options available to you to restore the server to the working state.

a) The most useful option is just to scan the whole system immediately, which will scan and attempt to repair any files that are changed or corrupted. You can do that with this command: :**sfc /scannow**

Alternatively, you can use the command **sfc /verifyonly** to scan for problems, but not perform any repairs.

b) To troubleshoot and repair for the following items

A master boot record (MBR)

A boot sector

A Boot Configuration Data (BCD) store

use the BOOTREC command with appropriate option as described below:

To rebuild the boot configuration data (BCD), execute the following command: **BOOTREC /REBUILDBCD**

To repair the Master Boot record, execute the following command: **BOOTREC /FIXMBR**

To repair the boot sector, execute the following command: **BOOTREC /FIXBOOT**

Finally, to apply the master boot code that is compatible with BOOTMGR, execute the following command, where Drive is the drive where the installation media resides:**Drive:\boot\Bootsect.exe /NT60**

Note that you may need to apply one or more commands to repair the OS as necessary.

Boot loader: Boot loader is the first program, that runs, when a computer is switched on. It later transfers control to an operating system kernel. GRUB (GRand Unified Boot loader) is the default boot loader for many Linux distributions, including Ubantu. Grub (latest GRUB-2) typically gets over ridden when you install Windows or another Operating System. To make Ubuntu control the boot process, you need to reinstall (Repair/Restore) Grub using a Ubuntu Live CD.

Typical steps involved this process are given below:

1. Mount the partition your Ubuntu Installation is on.

2. Bind the directories that grub needs access to to detect other operating systems.

3. Now we jump into that using chroot.

4. Now install, check, and update grub.

This time you only need to add the drive letter (usually a) to replace X, for example: grub-install /dev/sda, grub-install - recheck /dev/sda.

The command used for this purpose are:

grub-install /dev/sdX

grub-install --recheck /dev/sdX

update-grub

5. Now grub is back, you can exit the chrooted system and unmount everything.

6. Shut down and turn your computer back on, and you will be met with the default Grub2 screen.

The best place to verify compatibility is manufacturers Web site. The necessary drivers can be down-loaded from respective vendor sites. It is important to take a back-up before proceeding with the up gradation.

UNIX/Linux is usually administered by writing scripts and through configuration files. Other operating systems like Windows NT and Netware are GUI based and relatively easy to administer.

Normally, continued hum is associated with moving parts. The components susceptible for this kind of a problem are fan, hard drive, and floppy disk. Since a network card or any other PCA (printed circuit assembly) consist of only ICs, it is not likely to be the source of the noise.

The most effective way of knowing any disk drive failures is to configure remote notification on the server.

Surge Protector: A surge protector (or surge suppressor) is an appliance designed to protect electrical devices from voltage spikes. A surge suppressor attempts to limit the voltage supplied to an electric device by either blocking or by shorting to ground any unwanted voltages above a safe threshold.

Previous Contents Next

CompTIA® Server+ Exam Notes : Troubleshooting Software Problems

examguides.com/Serverplus/server-plus-24.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

7. Troubleshooting

7.3 Troubleshooting software problems

The following are good practices that are recommended to be followed for securing a server

1. Password protecting the Servers

2. Lock the Servers room, or limit access to the room to authorized server administrators only.

3. Lock the cabinet that the server is mounted or sitting in if you cannot lock the actual room.

4. Locate all the server back-ups, the server, and the emergency recovery disks at the same place for convenience.

You want to prevent your server from being broken through the network. This can be prevented by using:

1. Appropriate firewall to limit access to the server

2. Choosing a difficult to guess password, so that it is difficult to guess.

3. Checking the logs periodically to monitor if anybody tried to login to your server without any success, so that you can take appropriate measures.

OS boot failure: The message "Missing operating system" occurs when the system found a boot device, but could not boot because operating system files are missing or corrupt.

The message **"No boot device available"** appears when the bootable drive itself is not found. In such case, both floppy and hard disk drives are faulty or not present. It is important to be familiar with various boot time messages and probable causes.

You need to follow the manufacturer's recommendation regarding updates. Microsoft recommends that you enable automatic updates on your client as well as server operating systems so that the latest patches and fixes may be applied.

A network mapper is a tool that identifies what the devices connected to the network and the operating systems being used, if any. Firewall, proxy server, and web security gateway are used for network/host security. System mapper is given to divert the attention from the basic question.

Software backout: Software backout procedure is a term used for restoring the system or software in the event of any recent failure due to upgrade.

Memory leaks are bugs where the application fails to release memory when no longer needed. Over time, memory leaks affect the performance of both the particular application as well as the operating system. A large leak might result in unacceptable response times due to excessive paging. Eventually the application as well as other parts of the operating system will experience failures.

Performance Monitor and Resource Monitor can monitor and graph resource use over time. You may use these tools and a few other tools Application Verifier to find the problem.

Common Problems:

A runaway process is a process that consumes one or more processors, causing your system to become sluggish and sometimes causing other applications to freeze or crash. Often you can find such problems quickly by using Task Manager to view information about running processes. The common way to solve a runaway-process problem is to just kill the process, but this is only a temporary fix; the runaway process will likely recur. To troubleshoot processes that consume large amounts of CPU clock cycles, two tools by name Process Explorer and Adplus are useful.

In Linux, you may use the command "kill <process ID>" to kill the offending process. Alternatively, you may use the System Monitor GUI to kill the process. It looks a lot like the Windows Task manager.

When a system admin finds that a required service is not starting, there are two things to do:

1. Manually Start the Service: If you notice that a required service is not running, then the first thing that you should do is to attempt to manually start the service. To do so, just right click on the service and choose the Start command from the resulting shortcut menu. It is possible that the service starts without any problems. You can check the Dependencies tab and verify if the Service depends on another Service or Services, and troubleshoot for those Service(s).

2. Check the Event Log: If the manual start fails, the next best thing to do is to check the Event Viewer. If there are hundreds of events, then you use Event Viewer's find feature to locate the event of interest. When you find a log entry related to your problem, just double-click on the entry to view it. If the Event Log doesn't provide specific information, you can use the information provided and search Microsoft Technet for solution.

Over a period of time, it is possible that a Server computer (for that matter, even a PC) becomes slow in performance. This might happen due to various reasons, including the following:

1. The disk is almost full with junk files, temp files, and other un-necessary programs. This may be fixed by running disk clean-up software.

2. Defragment: It is possible that the hard drive has been fragmented considerably over a period of time. By defragmenting the drives, the performance may improve.

3. OS updates: Some times, by installing the latest Operating System updates, OS performance is improved.

4. Corrupt files: It is possible that some process has got corrupt due to some or other reason. You may check if any process is taking a lot of system resources by using Task Manager. You may need to end the process till it is resolved.

5. Virus and other malware: Last, but not the least, it is possible that some virus or malware has infected your server computer. Scan the computer from time to time to ensure that the system is free of any malware.

Cause of common problems

Corrupt or missing file(s): When the operating system fails to start and the hardware is not a fault, it is because of one or more essential files that the operating system needs to start have come corrupt or missing. Common error messages include an invalid boot disk and inaccessible boot drive or missing BOOTMGR. In Windows Server 2012 R2, the causes are most likely due to corrupted system file, BCD, boot sector, or master boot record (MBR).

There might be various reasons for a user not being able to access a resource on the network. This includes the following:

1. The admin has not given sufficient rights to access the resource

2. The user computer is not configured properly. For example, improper DNS server address or the Default gateway address or a simple IP address conflict.

3. The DNS server itself may not be functioning at that point of time.

4. If using an AD, check if the AD is working, and that the user is given sufficient permissions.

A patch is an important component of software update and it usually fixes some known bugs. If you need to apply it on a server, where the downtime is critical, it is recommended practice to install the patch on a lab server first. Install it on the production server once you find it satisfactory.

Previous Contents Next

CompTIA® Server+ Exam Notes : Diagnosing The Network Problems

examguides.com/Serverplus/server-plus-25.htm

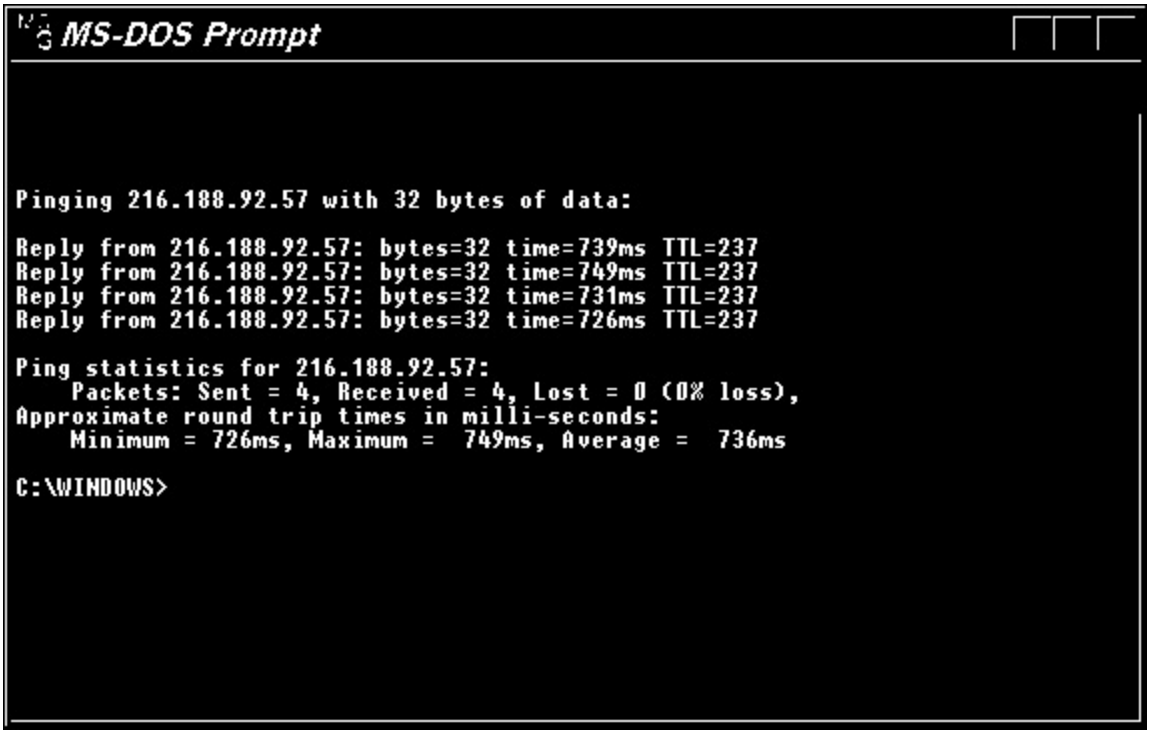
7. Troubleshooting

7.4 Diagnosing the network problems

Networking tools:

PING: Used to ping the remote system (or the local host) to see that the TCP/IP connection is through. The following fig shows output from ping command.

You can ping the loop back address at 127.0.0.1. A response ensures that the TCP/IP stack is installed properly on your computer.



List of ping command

1. Ping -r: this ping command option used to specify the number of hops between your computer and the target computer or device that you'd like to be recorded and displayed.

2. Ping -a: This ping command option will resolve, if possible, the hostname of an IP address target.

3. Ping -v: This option allows you to set a Type of Service (TOS) value. Beginning in Windows 7, this option no longer functions but still exists for compatibility reasons.

4. Ping -n: This option sets the number of ICMP Echo Request messages to send. If you execute the ping command without this option, four requests will be sent.

5. Ping -t: this option will ping the target until you force it to stop using Ctrl-C.

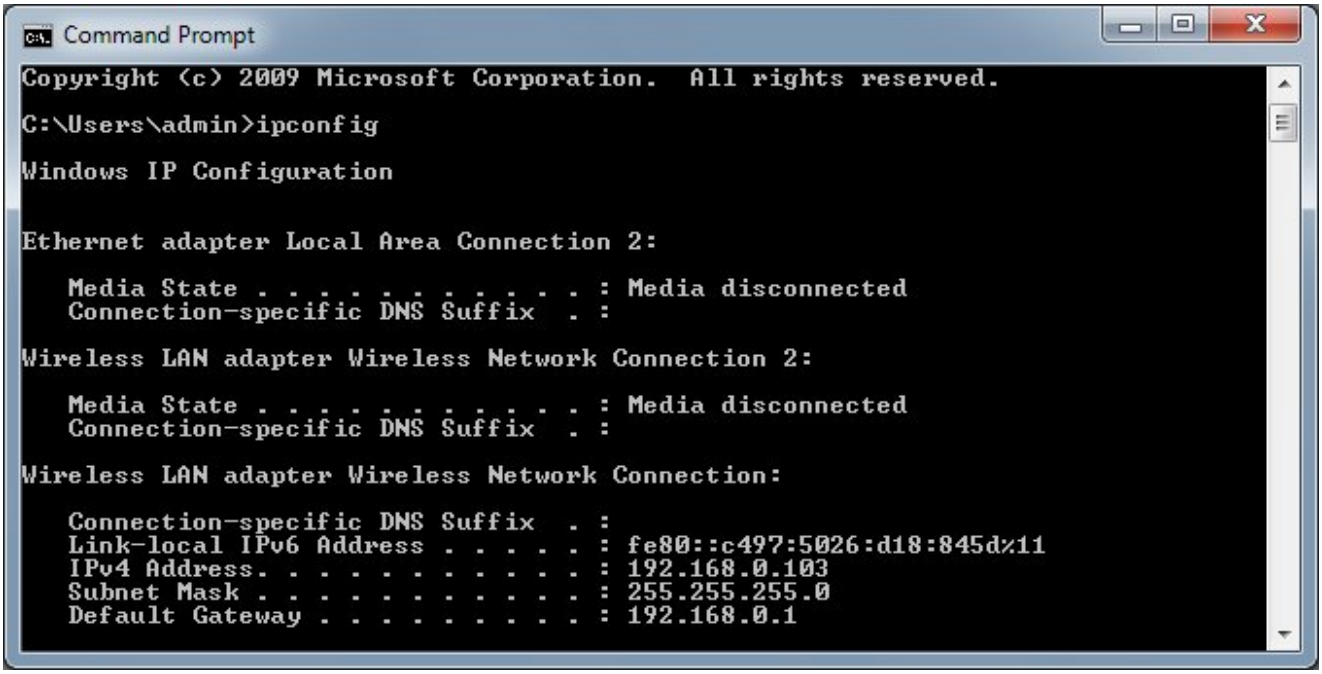
The pathping command is a route tracing tool that combines features of the ping and tracert commands with additional information that neither of those tools provides.

NBTSTAT: This utility displays current NetBIOS over TCP/IP connections, and display NetBIOS name cache. It Displays protocol statistics and current TCP/IP connections since the server was last booted. NETSTAT is used to review all inbound / outbound connection to a server.

NSLOOKUP: This utility enables users to interact with a DNS server and display resource records.

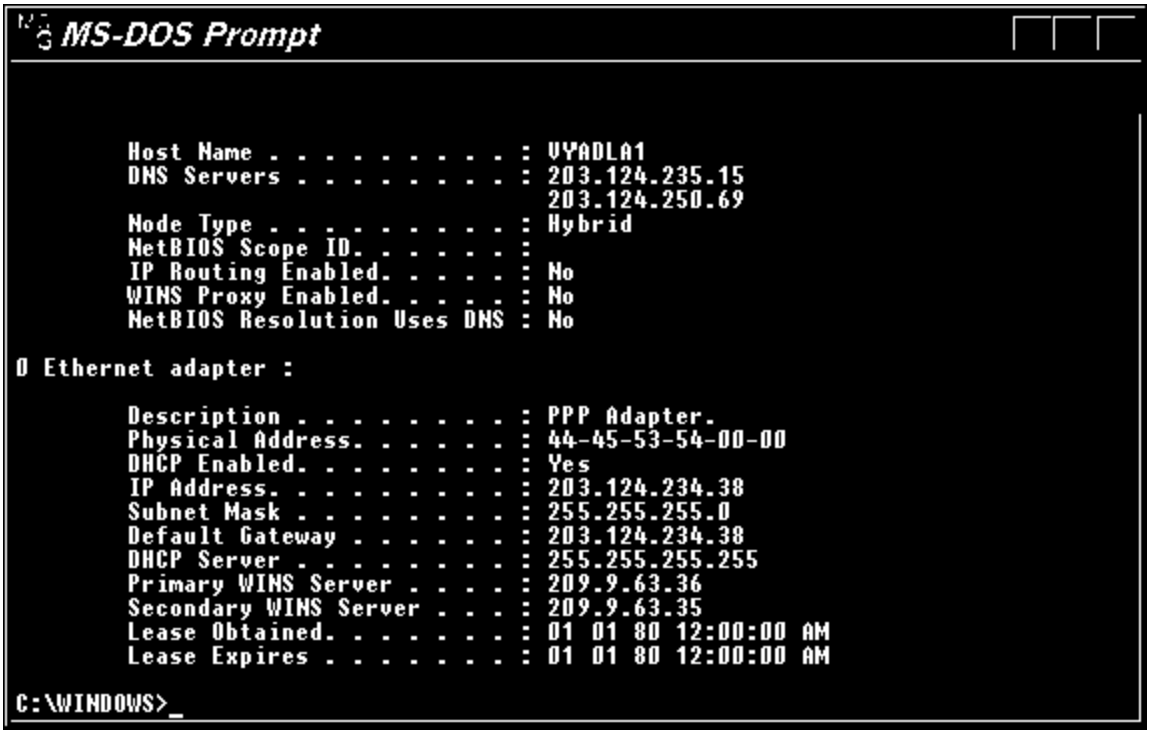
ROUTE: Used to display and edit static routing tables.

PCONFIG: Internet Protocol Configuration in Microsoft Windows is a console application that displays all current TCP/IP network configuration values and can modify Dynamic Host Configuration Protocol DHCP and Domain Name System DNS settings. The following fig shows the output of ipconfig command.



ipconfig /all: Displays the full TCP/IP configuration for all adapters. Without this parameter,

ipconfig displays only IPv6/IPV4 addresses, subnet mask, and default gateway values for each adapter. The command IPCONFIG/ALL shows additional parameters such as host name, DNS servers etc. compared to IPCONFIG command which doesn't show these details



ifconfig (short for interface configuration) is a system administration utility in Unix-like operating systems to configure, control, and query TCP/IP network interface parameters from a command line interface (CLI) or in system configuration scripts. Ifconfig is used to configure and display network interfaces. If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only. If a single -a argument is given, it displays the status of all interfaces, even those that are down.

netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics. It is available on Unix-like operating systems including OS X, and Linux, and is available on Windows NT-based operating systems including Windows 7/8, and Windows 10.

Netstat provides statistics for the following:

- Protocol
- The name of the protocol (TCP or UDP).
- Local Address

- The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).
- Foreign Address
- The IP address and port number of the remote computer to which the socket is connected. The names that corresponds to the IP address and the port are shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).
- (state)
- Indicates the state of a TCP connection.

Examples

To display both the Ethernet statistics and the statistics for all protocols, type the following command:**netstat -e -s**

To display the statistics for only the TCP and UDP protocols, type the following command:**netstat -s -p tcp udp**

TRACERT: Used to determine which route a packet takes to reach its destination from source. The tracert utility traces the path to the destination. It is accomplished by controlling the TTL (Time To Live) of the packets in the increments of 1 (one). When the TTL reaches 0, the router sends back an error message saying that the TTL has elapsed. This information is used to find the intermediate devices over the path to destination. Note that some routers may be programmed not to respond to TTL 0 packets. In such event, you may not receive any response.

Tracert and Ping use ICMP as their base protocol. ICMP messages are carried in IP datagrams. The command tracert/traceroute displays the time taken while a packet reach the destination. You will be able to see the time taken by each hop, and identify the faulty link.

The following fig shows tracert command output

```
TRACERT

Tracing route to w2.rc.scd.yahoo.com [66.218.71.113]
over a maximum of 30 hops:

  1   270 ms   261 ms   261 ms  203.124.235.5
  2     *      368 ms   259 ms  203.124.235.1
  3   675 ms   681 ms   682 ms  202.131.156.246
  4     *      847 ms   695 ms  202.131.152.1
  5  2030 ms   681 ms   694 ms  202.131.156.5
  6     *      832 ms   682 ms  cr1-brd.nyc1.ftign.net [64.95.12.60]
  7   676 ms   681 ms   681 ms  border11.fe5-7.fusion-2.nyc.pnap.net [216.223.55
.193]
  8   661 ms   681 ms   694 ms  core2.ge3-1-bbnet2.nyc.pnap.net [209.191.128.130
]
  9     *      885 ms   681 ms  POS1-2.GW7.NYC4.ALTER.NET [157.130.50.85]
 10   674 ms   681 ms   694 ms  210.at-6-0-0.XR4.NYC4.ALTER.NET [152.63.25.118]

 11   674 ms   695 ms   681 ms  210.at-1-0-0.XR2.NYC8.ALTER.NET [152.63.29.117]

 12   688 ms   681 ms   682 ms  0.so-2-2-0.XL2.NYC8.ALTER.NET [152.63.19.33]
 13   689 ms   694 ms   681 ms  POS7-0.BR3.NYC8.ALTER.NET [152.63.21.125]
 14   691 ms   708 ms   681 ms  204.255.169.126
 15   683 ms   681 ms   681 ms  ae0-52.mp2.NewYork1.Level3.net [64.159.17.34]
 16   769 ms   774 ms   773 ms  so-2-0-0.mp1.SanJose1.Level3.net [209.247.9.114]

 17  _
```

Given below are some of the precautions that may be required to secure the local network resources:

1. Rename default accounts so that blind attacks will not succeed

2. Use strong passwords and change passwords periodically

3. Secure the server rooms with lock and key

4. Use strong encryption for user names and passwords

Note that disabling local admin access is not an option because your manager wants to administer the servers locally. Anti virus software will not protect a server from un-authorized login.

Previous Contents Next

CompTIA® Server+ Exam Notes : Diagnosing Security Issues

examguides.com/Serverplus/server-plus-26.htm

Ad
CertExams.Com
Practice Exams | Network Simulators
Cisco: CCENT
CCNA
CCNA Security
CCNP
CompTIA:
A+ Network+
Security+
Server+
Netsims for
CCENT, CCNA, and Juniper JUNOS
Labsims For
Comptia A+, and Network+

7. Troubleshooting

7.5 Diagnosing security issues

Security tools:

Port/Network Scanner: Port scanner is an application designed to probe a server or host for open ports. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for open ports to break into your computer. Network mapper (Nmap), an open source software is an example of port scanner.

Sniffer: A sniffer is an application that can capture network packets. Sniffers are also known as network protocol analyzers. While protocol analyzers are really network troubleshooting tools, they are also used by hackers for hacking network.

Cipher: A cipher (pronounced SAI-fuhr) is any method of encrypting text (concealing its readability and meaning). Cipher-text is encrypted text. Plain-text is what you have before encryption, and cipher-text is the encrypted result.

Telnet Client: Telnet is a protocol that allows you to connect to remote computers (called hosts) over a TCP/IP network (such as the Internet). Using telnet client software on your computer, you can make a connection to a telnet server (i.e., the remote host).

Anti-malware software: Anti-malware software protects against infections caused by many types of malware, including viruses, worms, Trojan horses, rootkits, spyware, key-loggers, ransomware and adware. Another popular software is anti-virus software. However, anti-virus software is targeted towards removing certain types of malware such as virus. Malware is a generic term given to any harmful software and includes virus.

Previous Contents