Case Study Report for Computer Networks (19CSE301)

IMPLEMENTATION NETWORK VIRTUALIZATION FOR

**Disaster Recovery**

**BACHELORS OF TECHNOLOGY**

In Computer Science & Engineering

2020-2024

**Contributors:**

|  |  |
| --- | --- |
| **Name** | **Roll No** |
| N. Jai Vardhan | CB.EN.U4CSE20126 |
| Kancharla Satya Sai Karthik | CB.EN.U4CSE20129 |
| Pola Yogeshwar Reddy | CB.EN.U4CSE20148 |

**Introduction**

**Importance of Networking in our application**

In the world filled with numerous cybercrimes, it is imperative for all organizations to be prepared to face disasters that could affect their systems at any time.

There are many options to safeguard your systems against the various threats, the best one being virtualization. It helps reduce the time required to get your systems up and running after they’ve been hit by a disaster.

Networking is important in disaster recovery because it enables effective communication and coordination among various organizations and individuals involved in the recovery effort. This can include first responders, emergency management agencies, government agencies, non-profit organizations, and volunteers. Good networking allows for the efficient sharing of information, resources, and expertise, which can help to speed up the recovery process and minimize the impact of the disaster on affected communities. Networking can also help to build relationships and trust among different groups, which can be critical for effective collaboration in the aftermath of a disaster.

**Problem Statement**

A virtualization disaster recovery plan is a plan that outlines the steps that should be taken to recover a virtualized IT infrastructure in the event of a disaster. The goal of such a plan is to minimize downtime and ensure that critical systems and services are quickly restored to operation.

**Plan for Virtualized Disaster Recovery**

**Identifying Your Critical Virtual Machines**

Virtual Machines (VM) are a huge part of organizations’ systems. From servers to databases and business applications, virtual machines are a part of all business processes.

However, not all of these numerous virtual machines are critical to the functioning of your organization. Some VMs are more important than others.

Here, we need to understand that the more resources we need to restore, the more is the time required for the system to start functioning after a disaster.

Thus, to reduce this time, it is vital to identify the main virtual machines for your organization. Make sure they are monitored closely and backed up regularly.

**Defining a Backup and Recovery Strategy**

To start with, you will need to decide on the aptest software for creating and storing the backup in the virtual environment for your recovery strategy.

A solution that provides the capability of getting your working environment running while the files are being transferred back to your main host system would prove to be useful.

What we should understand here is that a snapshot is not the same as a backup. Snapshots are the state and data of the system at that point in time and are often stored in the same storage as the virtual machine.

In this scenario, if there is a hardware failure, the snapshot would be lost as well. Thus, it is necessary to store a backup of the virtual machine in the host rather than where the virtual machine resides.

**Ensuring Proper Connectivity Between the Primary Site and the Disaster Recovery Site**

It is a good practice to have the primary site and the disaster recovery site in different locations.

This is because, if the primary site is affected, there would still be a good probability that the disaster recovery site is not affected.

This arrangement also makes it necessary to have good connectivity between the two sites for backup as well as for the recovery process.

**Testing the Disaster Recovery Process Thoroughly**

The next thing we should do here is, thorough testing of the system in place. Although it might not be feasible to test the entire recovery system all at once, it can be tested in parts.

It is necessary to test the system properly for regular backups. We should also check the system for the time required, and the recovery process as well to make sure no issues arise during the process.

**Implementing Automation for Various Tasks**

While it reduces our workload, automation also reduces the possibility of human error, as well.

Automating tasks such as regular backups will ensure that at no point in time, a scheduled backup is missed. This makes sure you are prepared against any disaster at any point in time.

**Agenda (What Do We Do)**

In this Case Study, we defined a simulation of disaster recovery networking based on wireless networking.

**Main Server:**

|  |  |  |
| --- | --- | --- |
| No. of switches | No. of PC | No. of printers |
| 1 | 5 | 1 |

**Backup Server 1:**

|  |  |  |
| --- | --- | --- |
| No. of switches | No. of PC | No. of printers |
| 1 | 5 | 1 |

**Back Server 2:**

|  |  |  |
| --- | --- | --- |
| No. of switches | No. of PC | No. of printers |
| 1 | 4 | 1 |

**Client:**

|  |  |  |
| --- | --- | --- |
| No. of switches | No. of PC | No. of Servers |
| 1 | 1 | 3(WEB, DNS, FTP) |

In order to provide equal functionality to all the users, we have added DNS and HTTP servers for the maximum utilization of resources.

**CONNECTION DETAILS:**

|  |  |
| --- | --- |
| **MAIN SERVER** | |
| PC-PT PC 10 | 192.168.4.3 |
| LAPTOP-PT LAPTOP0 | 192.168.4.4 |
| LAPTOP-PT LAPTOP1 | 192.168.4.5 |
| LAPTOP-PT LAPTOP10 | 192.168.4.6 |
| LAPTOP-PT LAPTOP13 | 192.168.4.8 |
| PC-PT PC 14 | 192.168.4.7 |
| PC-PT PC 13 | 192.168.4.9 |
| LAPTOP-PT LAPTOP12 | 192.168.4.10 |

|  |  |
| --- | --- |
| **BACKUP SERVER 1** | |
| PRINTER -PT | - |
| PC-PT CABIN | 192.168.2.2 |
| PC-PT 1 | 192.168.2.3 |
| PC-PT 2 | 192.168.2.4 |
| PC-PT 3 | 192.168.2.5 |
| PC-PT 4 | 192.168.2.6 |

|  |  |
| --- | --- |
| **BACKUP SERVER 2** | |
| PRINTER -PT | - |
| PC-PT OFFICE | 192.168.1.2 |
| PC-PT 1 | 192.168.1.3 |
| PC-PT 2 | 192.168.1.4 |
| PC-PT 3 | 192.168.1.5 |
| PC-PT 4 | 192.168.1.6 |

|  |  |
| --- | --- |
| **CLIENT** | |
| PRINTER -PT | - |
| PC-PT OFFICE | 192.168.3.2 |
| PC-PT 1 | 192.168.3.3 |
| PC-PT 2 | 192.168.3.4 |
| PC-PT 3 | 192.168.3.5 |
| PC-PT 4 | 192.168.3.6 |

**HARDWARE USED:**

**Router:**

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divides broadcast domains of hosts connected through it.

**Switch:**

A network switch (also called switching hub, bridging hub, officially MAC bridge is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

**Network Packet:**

A network packet is a formatted unit of data carried by a packet-switched network. A packet consists of control information and user data, which is also known as the payload.

**Server:**

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines, they are considered servers. There are many types of servers, including web servers, mail servers, and virtual servers.

Many networks contain one or more of the common servers. The servers used in our project are as follows:

* **DNS Server:**

DNS stands for Domain Name System servers which are application servers that provide a human-friendly naming method to the user computers in order to make IP addresses readable by users. The DNS system is a widely distributed database of names and other DNS servers, each of which can be used to request an otherwise unknown computer name. When a user needs the address of a system, it sends a DNS request with the name of the desired resource to a DNS server. The DNS server responds with the necessary IP address from its table of names.

* **WEB Server:**

One of the widely used servers in today’s market is a web server. A web server is a special kind of application server that hosts programs and data requested by users across the Internet or an intranet. Web servers respond to requests from browsers running on client computers for web pages, or other web-based services.

**Ethernet:**

This is the backbone of our network. It consists of the cabling and is typically able to transfer data at a rate of 100mb/s. It is a system for connecting several computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems. Among the different types of ethernet, we have used Gigabit Ethernet, which is a type of Ethernet network capable of transferring data at a rate of 1000 Mbps and fast Ethernet is a type of Ethernet network that can transfer data at a rate of 100 Mbps.

**Computing Device:**

Computing devices are the electronic devices that take user inputs, process the inputs, and then provide us with the end results. These devices may be Smartphones, PC Desktops, Laptops, printer, and many more.

**Internet Protocol:**

Internet Protocol (IP) is one of the fundamental protocols that allow the internet to work. IP addresses are a unique set of numbers on each network and they allow machines to address each other across a network. It is implemented on the internet layer in the IP/TCP model.

**Performance Parameters:**

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Meaning** | **Formula** |
| Bandwidth | Bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time | Expressed as [bits](https://web.archive.org/web/20190816003233/https:/whatis.techtarget.com/definition/bit-binary-digit) per second ([bps](https://web.archive.org/web/20190816003233/https:/searchnetworking.techtarget.com/definition/bits-per-second)), modern network links have greater capacity, which is typically measured in millions of bits per second ([megabits per second](https://web.archive.org/web/20190816003233/https:/searchnetworking.techtarget.com/definition/Mbps), or Mbps) or billions of bits per second ([gigabits per second](https://web.archive.org/web/20190816003233/https:/whatis.techtarget.com/definition/Gbps-billions-of-bits-per-second), or Gbps). |
| Throughput | Throughput measures the percentage of data packets that are successfully being sent; a low throughput means there are a lot of failed or dropped packets that need to be sent again. |  |
| Packet Loss | Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Due to network congestion. | Efficiency = 100% \* (transferred – retransmitted) / transferred.  Network Loss = 100 – Efficiency. |
| Transmission Time | The time required for transmission of a message depends on the size of the message and the bandwidth of the channel. | Transmission Time = Message Size / Bandwidth. |
| Propagation Time | Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed. | Propagation Time = Distance / Propagation Speed. |
| Processing Delay | Time taken by the processor to process the data packet is called processing delay. |  |
| Queuing Delay | Time spent by the data packet waiting in the queue before it is taken for execution is called queuing delay. |  |
| Jitter | Jitter is defined as the variation in time delay for the data packets sent over a network. This variable represents an identified disruption in the normal sequencing of data packets. Jitter is related to latency, since the jitter manifests itself in increased or uneven latency between data packets, which can disrupt network performance and lead to packet loss and network congestion. Although some level of jitter is to be expected and can usually be tolerated, quantifying network jitter is an important aspect of comprehensive network. | Latency = Sum of all Delays.  To measure Jitter, we take the difference between samples, then divide by the number of samples (minus 1). |

**Benefits of wireless networking over wired networking**

To better understand the wide usage of wireless networking in today’s world, is to start with the benefits it has over traditional wired networking is crucial for our project implementation. Some major aspects have been stated below that show the various advantages of a wireless network over wired ones.

* **Mobility:**

One of the major advantages of wireless is mobility. Users have the freedom to move within the area of the network with their computing devices staying connected to a network without being concerned about the cable connection.

* **Less Hassle:**

The wireless network helps in the reduction of large amounts of cables or wires which becomes chaotic and difficult to maintain, it makes the connection hassle-free.

* **Accessibility:**

Provide network access across your organization, even in areas that have been challenging to reach with the wired network, so your entire team can stay in touch.

* **Expandability:**

The wireless network helps in the expansion of the network to a wide range by adding multiple new users and locations without additional need to run cables and wires.

* **Guest Access:**

Offer secure network access to guest users, including customers and business partners, while keeping your network resources protected.

With lots of advantages, there come disadvantages as well, like security issues which can be resolved using strict protection passwords. Also, the Speed of wireless networks is slow and having low bandwidth when compared to the direct cable connection networks.

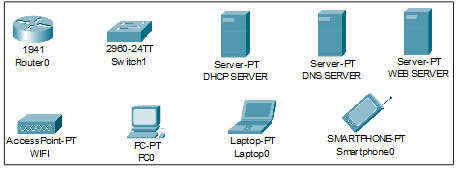
* **Simulation Environment**

The simulations of our network topology can be easily achieved using cisco packet tracer. Using a simulation mode, you can see packets flowing from one node to another and can also click on a packet to see detailed information about the OSI layers of the networking. Packet Tracer offers a huge platform to combine realistic simulation and visualize them simultaneously. Cisco Packet Tracer makes learning and teaching significantly easier by supporting multi-user collaboration and by providing a realistic simulation environment for experimenting with projects.

* **Network Requirements**

**Devices Used in the Network**

|  |  |
| --- | --- |
| **Devices** | **Quantity** |
| 1) Router (1941) | 3 |
| 2) Switches (2960-24TT) | 3 |
| 3) DNS server | 1 |
| 4) WEB server (HTTP) | 1 |
| 5) PCs | 12 |



* **BACKUP SERVER 1**
* **BACKUP SERVER 2**

* **CLIENT**

**Final Simulation**

Final Simulation for the network system to check all the connections.

* **Ping Test:**

Network connectivity and communication can be tested using the ping command, followed by the domain name or the IP address of the device (equipment) whose connectivity one wishes to verify.

**Ping Test for DNS Server**

**Ping Test for WEB Server**

**CONCLUSION**

Virtualization can be an effective tool for disaster recovery because it allows an organization to quickly and easily spin up virtual copies of their servers and applications in the event of a disaster. This can help minimize downtime and keep the business running smoothly. In addition, virtualization allows for the creation of backup copies of servers and applications, which can be used to restore the system in the event of a disaster. Overall, virtualization can provide a cost-effective and flexible solution for disaster recovery, making it an attractive option for many organizations.

One of the key benefits of using virtualization for disaster recovery is that it allows organizations to easily replicate their entire IT infrastructure in a virtual environment. This means that if a disaster strikes and physical resources are lost or damaged, the virtual infrastructure can be quickly brought online to take its place. This can help to ensure that essential business functions are maintained and that there is minimal disruption to operations.