1st Proceeding of International Conference on Science and Technology UISU (ICST)
"Contribution of Engineering Disciplines to Achieving Sustainable Development Goals Research Realizing the Vision of Golden Indonesia 2045"
ISSN: 3063-7929 (Online)
DOI: https://doi.org/10.30743/icst

Network Hierarchy Model using Spanning Tree Protocol (STP) and Hot Standby Router Protocol (HSRP)

1st Oris Krianto Sulaiman*, 2nd Mohamad Ihwani, 3rd Muhammad Basri

[1)]*Dept. Informatic Engineering, Universitas Islam Sumatera Utara*Medan 20217 Indonesia
oris.ks@ft.uisu.ac.id
[2)]*Universitas Negeri Medan*, Medan 20221, Indonesia
ihwani@unimed.ac.id
[3)]*Universitas Muhammadiyah Sumatera Utara* Medan 20238 Indonesia
mhdbasri@umsu.ac.id

Abstract— To create a network on a large scale, several techniques are needed so that the network can work optimally and reliably in dealing with various problems that arise, large-scale networks certainly require high-level network devices, where the performance of these devices can overcome the problems that arise later, but these high-level devices will not be optimal without a reliable network administrator in managing the network, One way to improve the performance of these devices is to use a hierarchy network design or hierarchical network design, where this design will divide each of these devices into layers that will be aligned with their functions, this design has 3 layers, namely, core layer, distribution layer and access layer. A well-organized design will make the network easier to monitor, data communication between large-scale networks also needs to be designed such as creating redumdancy or backup links, one technique for creating redundancy using Spanning Tree Protocol (STP) which will select the main port and backup port for determining the path and in combination with the Hot Standby Router Protocol (HSRP) which functions as a gateway replacement if one of the devices is down.

Keywords— Hierarchy Network Design, Spanning Tree Protocol (STP), Hot Standby Router Protocol (HSRP)

1. INTRODUCTION

Large-scale networks must provide infrastructure that has the ability to anticipate problems that arise, network problems will have an impact on the income of network users, for example, if the company experiences interference in the network, the company cannot communicate with the company's branches, a large network in the company is not located in just one area, namely the central area, but there are branch areas, and later there will be new branches that result in changes to the scale of the network, over time this network will continue to grow according to the success of the company. How to optimize and manage large-scale networks that continue to grow, as for the strategies used, one of which is the hierarchical design of the network. The purpose of this design is to limit the number of single network devices affected by interference, make plans for network development and create a reliable network.
Things that need to be considered in large-scale networks are:

1. The network is able to optimize network traffic density.
2. The network is able to support various needs in the future, for example if there are sudden network changes in the network or the addition of devices to keep it up to date.
3. Provide centralized network control to facilitate network maintenance quickly and precisely.
4. Network support with critical applications both local and internet.

Hierarchical Network Design

To optimize bandwidth usage, the network must manage which networks should be localized and not spread to the internet network. To adjust this requires proper design such as hierarchical network design.

The hierarchical network design divides this large-scale network into 3 parts, namely:

1. Core layer
2. Distribution layer
3. Access layer

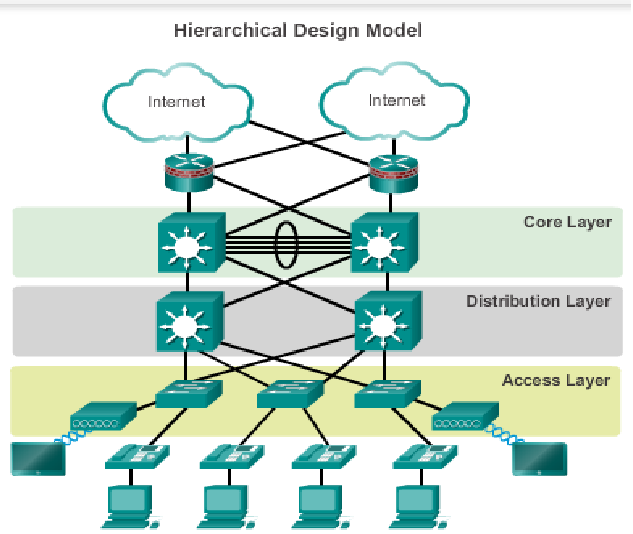

Figure 1. Hierarchical networ design

Each layer is designed to fulfill certain functions. The access layer provides connectivity for users or end users, the distribution layer is used to forward from one local network to another, for example forwarding a local network to the internet, the core layer is a high-speed layer where this layer is the highest layer of the network hierarchy design. This design will limit domain failure or domain failure, for example at the access layer for each switch representing its own network, each switch has its own domain, if one switch dies, only the domain is down while the other switch network is not disturbed, but if the multi-layer switch domain at the distribution layer dies, the switch or device below it will be down. Using this design makes the network on a large scale more optimal, besides that large networks also need a way so that data communication is not disrupted, one way or technique that can be used to optimize the hierarchical network design is to provide network redundancy or network backup, one of which can use protocols such as STP and combined with HSRP.

Spanning Tree Protocol (STP)

Spanning Tree Protocol is a protocol that provides rendundancy so as to prevent network failure at one point. Rendundancy provides a backup link or backup device that will anticipate if the main link or one of the devices dies, problems arise when creating a backup link (rendundancy), namely loops and frame duplicates, where there will be 2 or more input links to the device, for example a switch, if there are 2 inputs, there will be 2 of the same path in one switch, causing loops and irregular frame distribution, to overcome this problem it can be overcome by using the spanning tree protocol (STP).

STP ensures that there is only one logical path (link) between network paths, and will make other links as backup paths, the port will be considered non-existent even though there is a link on the port. The path is disabled to prevent loops, but if the main path is disrupted, the blocked path will automatically function to replace the main path so that the network will be more avoided from domain failure.

Spanning Tree Algorithm

Spanning tree protocol (STP) uses the spanning tree algorithm (STA) to determine which switch ports should be blocked and which ports should be the main line.

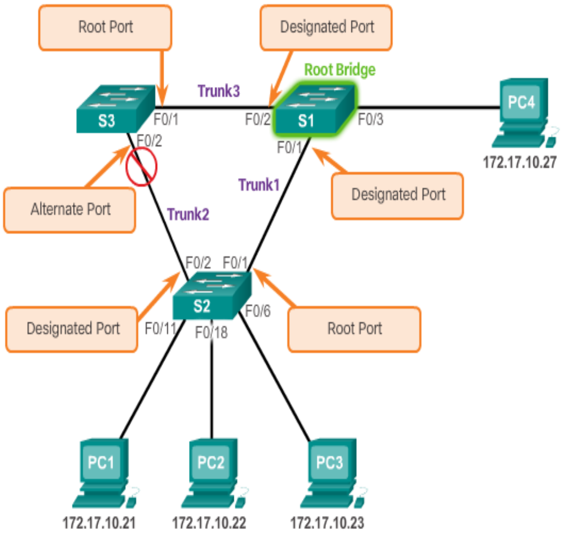

Figure 2. Schematic of the spanning tree algorithm

The message that will be exchanged by the switch is BPDU (Bridge Protocol Data Unit), each BPDU contains a BID which is the priority value of the switch, the MAC address of the sending switch, and the system ID.After forming the root bridge, the STA will calculate the shortest path to the root bridge, each switch will determine which port will be blocked.

The following is the process that occurs when the STP topology is running normally without any changes:

1. The root switch creates and sends Hello BPDUs with cost 0 out through all its active ports/interfaces.
2. The non-root switch receives the Hello from its root port. After converting the content of the Hello into the Bridge ID of the sending switch, the switch forwards the Hello to the designated port.
3. Steps 1 and 2 are repeated until there is a change in the STP topology.

When an interface or switch fails, the STP topology will change; in other words, STP convergence occurs.

1. Interface that remains in the same status, then there is no need for change.
2. Interface that must change from forwarding to blocking, then the switch will immediately change it to blocking.
3. The interface must change from blocking to forwarding, then the switch will first change it to listening, then to learning. After that the interface will be placed in the forwarding state.

When STP Convergence occurs, the switch will determine which interfaces to change their status to. However, changing the status from blocking to forwarding cannot be done immediately, because it can cause temporarer frame looping. To prevent temporarer looping, STP must change the port status to 2 transition states first before changing it to forwarding.

1. Listening: as with blocking, interfaces in the listening state do not forward frames. (15 seconds)
2. Learning: interfaces in this state are still not forwarding frames, but the switch has started to check the MAC address of frames received on this interface. (15 seconds).

The switch will wait 20 seconds before deciding to make a status change from blocking to forwarding, after which it takes 30 seconds to transition to Listening and Learning first. therefore the total required for a port to change from blocking to forwarding is 20+30=50 seconds.

2. HOT STANDBY ROUTER PROTOCOL (HSRP)

It is a protocol that can anticipate network gateway failures, this protocol creates virtual gateways as redundancy.

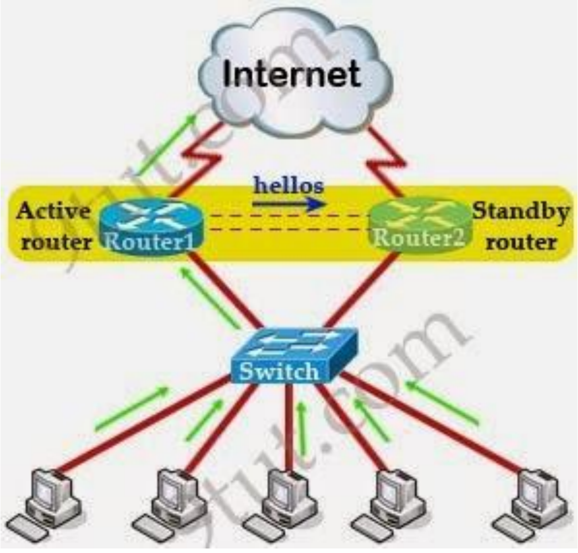

Figure 3. HSRP Schematic

In this scheme, the two routers will only be read as virtual routers so that it will only appear to use one router. The virtual IP and MAC addresses of the two routers to represent as a single default gateway for all hosts. For example, virtual IP address 192.168.1.254 and virtual MAC address 0000.0c07.AC0A. All hosts will point their default gateway at that IP address. The router chosen as the gateway is the active router, and the other routers are standby routers, both of these routers are equally functional but the active router works while the standby router is only a backup if at any time the active router is interrupted.

When a failure of the active router is detected, the standby router assumes the role of forwarding router. Since the new forwarding router uses the same (virtual) IP and MAC address, all hosts see no interruption in communication. A new standby router will also be selected at that time (in cases where there are more than two routers in the HSRP group).

By default, a hello packet is sent between HSRP standby group devices every 3 seconds, and a standby device becomes active when a hello packet is not received for 10 seconds (called hold time).

3. RESULT AND DISCUSSION

The designed topology must fulfill the 3 layers of hierarchical network design, namely the core layer, distribution layer and access layer.

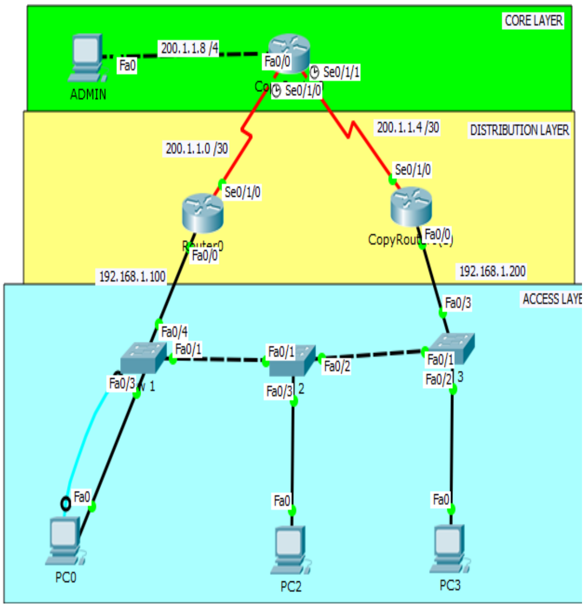

Figure 4. Topology design

The topology above shows the design of 3 layers, where these layers have each function, but the weakness of the hierarchical design is that there is no availability of redundancy or backup links, if sw1 to sw2 is disconnected then pc0 and pc2 cannot communicate, unless static routing is done, but static routing is not recommended for large networks due to inefficient configuration when network changes occur.

Spanning Tree Protocol is applied between switches as redundancy.

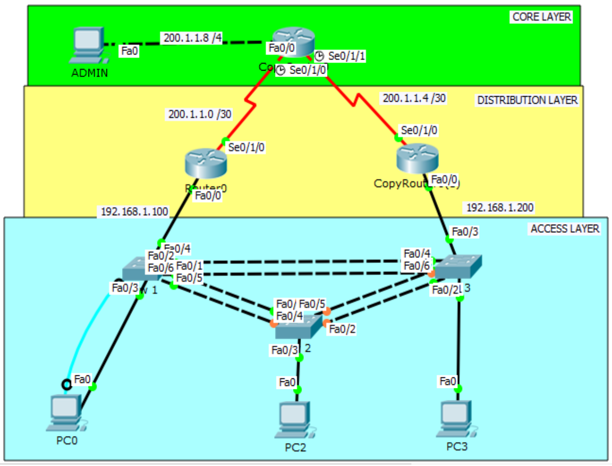

Figure 5. Spanning Tree Protocol

```
Spanning Tree Protocol (STP) port on switch 3
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3 Desg FWD 19 128.3 P2p
Fa0/2 Desg FWD 19 128.2 P2p
Fa0/1 Desg FWD 19 128.1 P2p
Fa0/4 Root FWD 19 128.4 P2p
Fa0/5 Desg FWD 19 128.5 P2p
Fa0/6 Altn BLK 19 128.6 P2p
```

The ports that are disconnected are blocked ports, but if there is a disruption in the network, the blocked ports will become forward ports for network communication.

Complex network designs that have redundancy are not enough to overcome problems in the router network must also be an alternative as redundancy with HSRP. The router will form a virtal mac and ip address.

PC 0 will communicate with the admin PC at the core layer through the gateway 192.168.1.100.

```
PC>tracert 200.1.1.10
Tracing route to 200.1.1.10 over a maximum of 30 hops:
  1 1 ms 0 ms 0 ms 192.168.1.100
  2 10 ms 1 ms 1 ms 200.1.1.5
  3*0 ms 1 ms 200.1.1.10
Trace complete.
```

It can be seen that PC0 will pass through the router at the distribution layer to the core layer and forwarded to the admin PC, if there is a network failure or disruption at router one then PC0 cannot communicate with the admin PC.

```
PC>tracert 200.1.1.10
Tracing route to 200.1.1.10 over a maximum of 30 hops:
  1 * * * Request timed out.
  2 * * * Request timed out.
  3 * * * Request timed out.
  4 * * * Request timed out.
  5
Control-C
^C
PC>
```

HSRP will prevent this failure by finding another path through another router,

HSRP will create a virtual ip

```
Router(config-if)#standby 1 ip ?
  A.B.C.D Virtual IP address
<cr>
```

```
Router(config-if)#standby 1 ip 192.168.1.254
```

All computers will have this gateway even if the ip does not exist, router 1 and router 2 which have been set up with HSRP will find which priority is the main line and which router is for the backup line.

In this design, router 2 is the main line, the gateway on PC0 is virtual ip 192.168.1.254, if one router has a problem, the other router will become the main line, so the path from PC0 to the admin PC is

```
PC>tracert 200.1.1.10
Tracing route to 200.1.1.10 over a maximum of 30 hops:
  1 11 ms 1 ms 0 ms 192.168.1.200
  2 2 ms 1 ms 1 ms 200.1.1.2
  3 2 ms 1 ms 2 ms 200.1.1.10
Trace complete.
```

PC0 passes through router 2 because router 1 is experiencing interference, also because router 2 is the main line. If router 2 is experiencing interference, router 1 will take over the main line even though the gateway of each computer is a virtual IP but in the realization of the movement of the path he still reads the original ip address of the router.

The HSRP of router2 can be seen as follows

```
Router2#show standby
FastEthernet0/0 - Group 1 (version 2)
  State is Active
    7 state changes, last state change 00:00:36
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.701 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  Group name is hsrp-Fa0/0-1 (default)
```

It can be seen that HSRP forms a virtual ip address and mac address.

This network model is expected to reduce the risk of network failure because it has a design that prevents domain failure and has backup links and gateways.

4. CONCLUSION

From the above discussion it can be concluded that: Hierarchical network design is very efficient in overcoming problems that occur in the network, because of its organized and neat nature. STP allows for the creation of ring and mesh networks, so it has a reliable advantage in network link backup. HSRP will back up the gateway router using virtual ip and virtual mac so that if the main router goes down there is still a gateway router that handles network communication lines.

REFERENCES

[1] Agus Setiawan.CCNA Lab Guide Nixtrain_1st Edition, Bandung, Indonesia, January 2015, Nixtrain

[2] Todd Lamle.CompTIA Network+ StudyGuide, Canada, 2009, Wiley

[3] Imiefoh, Pedro. *Network Gateway Technology: The Issue of Redundancy towards Effective Implementation,* An International Multidisciplinary Journal, Ethiopia Vol. 6 (1), Serial No. 24, January, 2012

[4] Abhishek Kumar Singh and Abhay Kothari.*HSRP (Hot Stand by Routing Protocol) Reliability Issues Over the Internet Service Provider's Network,* An International Open Free Access, Peer Reviewed Research Journal, December 2011, Vol. 4, No. (2): Pgs. 399-404