# Redundant Datacenter Network

Stehen Cronin, Jakob Idland, Charles Gill Jr, Carter Caruso
IT Capstone Project 491-101
Osama Eljabiri
December 13, 2022

Authors: Chapter 1 - Stephen Cronin, Chapter 2 - Stephen Cronin, Chapter 3 - Carter Caruso, Chapter 4 - Charles Gill Jr, Chapter 5 - Jakob Idland, Chapter 6 - Charles Gill Jr

# Chapter 1: Introduction

A company's network is essential to its day-to-day operations, especially in a digital world. Most companies host important resources on their local intranet and conduct meetings virtually through collaboration software such as Microsoft Teams or Cisco Webex. However if a network outage occurs, employees may not be able to access the resources they need, won't be able to conduct important meetings, and could lose thousands of dollars by not being able to perform essential functions. A reason as to why many of these outages occur is because the datacenter network contains a single-points of failure. This means that if one link or device goes down, the entire network goes down with it. This poses huge problem as all IT infrastructure, especially networks, should have some sort of failover policy and implementation to prepare for a potential outage in advance.

Our mission for this project is to design a datacenter network with a keen focus on redundancy and availability. We not only want to make sure that the routing and switching works properly, but we want to ensure that the redundant links we implement work if one of the active links were to go down. Having these redundant links implemented will significantly decrease the chances of a prolonged outage in the datacenter's network and will increase the availability of the network as the network should continue to operate as normal if a link or device goes down as the redundant links will take over as the active links.

Authors: Chapter 1 - Stephen Cronin, Chapter 2 - Stephen Cronin, Chapter 3 - Carter Caruso, Chapter 4 - Charles Gill Jr, Chapter 5 - Jakob Idland, Chapter 6 - Charles Gill Jr

This project is very technical and especially the later portion of this report will include terms that the average person may not be familiar with. The following is a list of terms and definitions that whoever is reading this report should be informed about:

- Redundancy: When a communication pathway has additional links to connect all nodes in case one link goes down.
- CISCO Packet Tracer: A cross-platform visual simulation tool used to create network topologies and imitate modern computer networks.
- Router: A networking device that forwards data packets between networks.
- Switch: A networking device that connects devices on a network using packet switching to forward data to the destination device.
- Multi-Layered Switch: A switch that can operate at higher levels of the TCP/IP model.
- LAN: Local Area Network. A network that is located in the same physical area,
- WAN: Wide Area Network. A network that spans over a large geographical area.
- VLAN: Virtual Local Area Network. Logical overlay network that groups together a subset of devices that share a physical LAN.
- Data Link: A connection between two networking devices.
- Spanning Tree Protocol: A layer 2 network protocol used to prevent looping within a network topology.
- Routing Table: A set of rules that determine where data packets traveling over an IP Protocol go to and what routes they take.
- HSRP: Host Standby Router Protocol. Configures two or more routers as standby routers and one single router as the active router at a given time.
- Ping: A command-line tool that allows a user to test connectivity to another IP address.
- Traceroute: A command-line tool that traces the path an IP packet takes over one or many networks.
- CIA Triad: Confidentiality, integrity and availability is a model designed to guide policies for information security within an organization.

# Chapter 2: Project Management

**Roles:**

All members of the team served as Network Engineers and additionally as a subject matter expert in certain focal areas of the project. Each member of the team performed proficiently in their specialized roles.

**Stephen Cronin** - Project Manager / Network Engineer

**Jakob Idland** - Network Engineer / Routing Specialist

**Charles Gill** - Network Engineer / VLAN Architect

**Carter Caruso** - Network Engineer / Security Analyst

**Stephen Cronin** performed as the project manager for this project. The project manager was responsible for the creation and adherence of the gantt chart, creation and adherence to the FDD diagram, submission of progress reports, and timely submission of all project deliverables. In addition to these responsibilities, various operational tasks in relation to meeting times were accomplished.

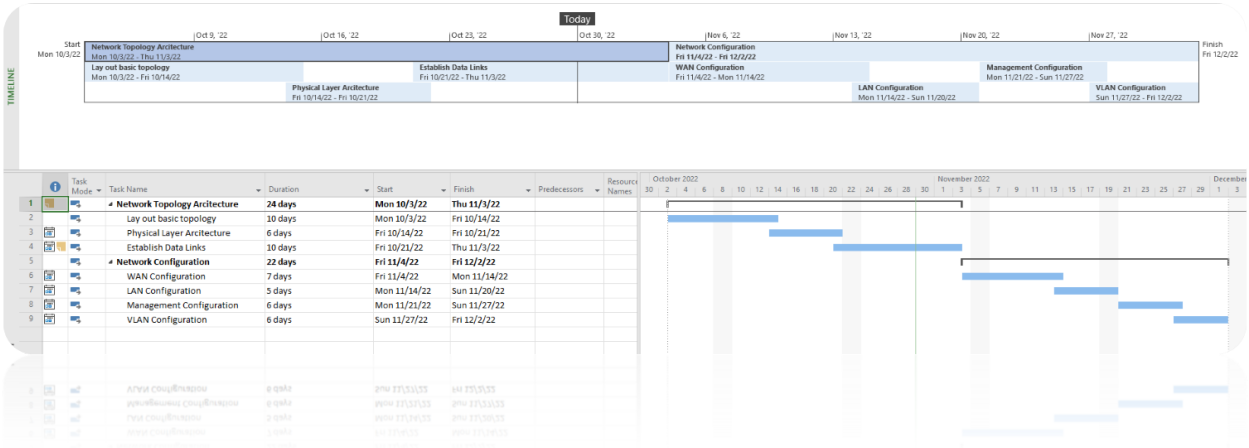
**Jakob Idland** performed as a network engineer for this project. Jakob stepped up and took responsibility for implementing routing in the network, ensuring packets get to their correct destination. Jakob successfully implemented the correct routing requirements for the project to be satisfactory and included fail-over routes to ensure the project met redundancy requirements.

**Charles Gill** performed as a network engineer for this project. Charles successfully architected and implemented VLANs for the datacenter network. The creation of these VLANs ensured that the project would meet its availability criteria by allowing the separate networks to communicate with each other. Charles also created and maintained a routing table for proper system documentation.

**Carter Caruso** performed as a network engineer for this project. Carter assisted in implementing security measures across the network to ensure availability and authenticity of the network. Carter set a username and password on all appropriate network equipment, secured non-essential ports and lines, and encrypted all passwords across this network. His work as a security analyst was paramount to making sure the network adhered to the CIA triad.

-

## Gantt Chart:



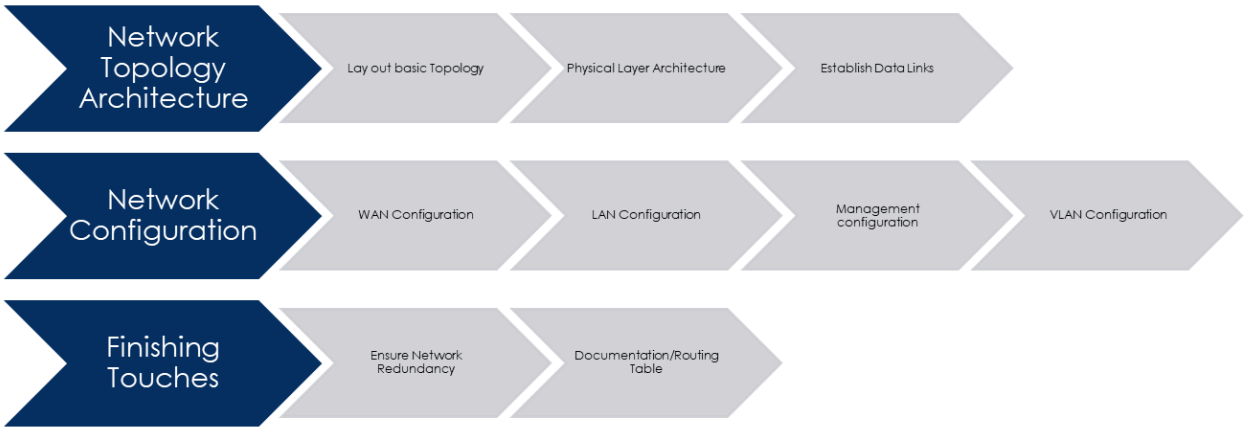

The Gantt chart for this project was divided into two different macro areas of Network Topology Architecture and Network Configuration.

The first area of focus being Network Topology Architecture, our group laid out the basic topology of the network during this period. Additionally the physical layer architecture was conducted during this period. The last part of the topology architecture work was establishing the physical data links in the network. All items of this area were completed on time and done proficiently.

The second macro area of focus was the Network Configuration. This was broken up into several smaller micro tasks. The first area of focus was the WAN configuration, which ended up taking the bulk of our efforts. Then the LAN configuration was completed after the WAN configuration.

This was another demanding area due to the redundancy requirements of our project. Lots of energy was put into these areas. Management and VLAN configuration were the last two micro areas of this task. All items of this area were completed on time and done proficiently.

**FDD Diagram:**




In addition to a Gantt Chart, our group also used an FDD Diagram for project management assistance. The FDD diagram was broken up into three macro areas: Network Topology Architecture, Network Configuration, and Finishing Touches.

**Network Topology Architecture:**

This area included three micro tasks of laying out the basic network topology, doing the physical layer architecture and establishing data links.

**Network Configuration:**

The bulk of our efforts went to accomplishing this part of the FDD diagram. This area was a particularly challenging one due to the redundancy requirements of our project. Our project required lots of network configuration in order to have it meet those redundancy requirements. WAN and LAN configuration took up the bulk of our efforts. Management configuration and VLAN configuration were also done in this macro area.

**Finishing Touches:**

The last macro area were smaller tasks like ensuring network redundancy, and conducting final documentation including routing tables. Ensuring network redundancy was accomplished before the final showcase. The bulk of the documentation we were able to put off after the final presentation, since there was no immediate demand for detailed documentation.

## Risk Identification and Management:

As with any project, our group faced risks and obstacles along the way. The following table presents the risks we faced and how we managed them:

| Risk | Probability | Consequence | Cause | Solution |
|---|---|---|---|---|
| Difficulty of finding a mutual time to meet. | 0.8 | 8 | Scheduling conflicts due to everyone having different class and work schedules. | Conduct meetings virtually, as it's easier to hop in a voice chat whenever than for everyone to commute back to campus, especially late at night. |
| One of the team members drops from the course | 0.1 | 7 | One of the teams members struggles with some of the course work early on, causing them to withdraw and leave the group with one less member | Have all team members involved with all aspects of the project to some degree, that way the other team members can pick up the work easily. |
| Conflicts with other courses | 1 | 4 | Other coursework may conflict with the needs of the 491 project | Synchronize meeting times that work for everyone with minimal conflicts |

**Difficulty finding a mutual time to meet:**

Difficulty finding a time to meet was given a .8 in probability due to all of us being busy college students. We identified this risk early on in the project and addressed it by conducting most of our meetings virtually to eliminate a commute to campus. By conducting as much of the work virtually as possible, we were able to streamline and effectively use our time to be as productive as possible.

**One of the team members drops from the course:**

One of our team members dropping the course was given a .1 probability due to all of us being good students. By having all members involved with all aspects of the project to some degree,

we ensured that if one person were to end up dropping out, another member of the team would be able to step in and take their role. Luckily we did not encounter this problem during the project, our initial assumption of this being not likely to happen was correct.

**Conflicts with other courses:**

Conflicts with other courses were given a 100% probability as we are all busy college students with full schedules. By synchronizing our meeting times virtually we were able to avoid major conflicts with other courses. Lots of the team was also taking IT490 this semester, which is a very demanding course, so we were expecting some conflict to happen. We were luckily able to synchronize meeting times to avoid conflicts with other coursework. We believe that conducting most of our tasks virtually helped us avoid serious conflicts.

# Chapter 3: Define

The requirements for this project are to ensure redundancy in case of network failure, ensure high availability to support normal traffic, and to ensure interconnectivity between endpoints when appropriate. We will need to properly configure a redundant management network and to configure the switches in this network for redundant networking. In order to do this, each switch will have multiple links trunking from other switches, so if one switch goes down the other switches will still be supporting the network traffic flow. Details of how we will implement this will be discussed in the later chapters.

The scope of this project is limited to a working proof of concept. This is because we have a limited budget and getting all the necessary networking equipment would be too expensive. This project also has a window of about 10 weeks to complete, and getting the necessary equipment to arrive on time would be very hard especially with global supply chain holdups. Therefore, we decided to use CISCO Packet Tracer to build a mock datacenter network, as it will still allow us to configure servers, switches, and routers the exact same as we would in real life and will show us the connection status between the different devices to confirm if our configuration is correct or not. This will allow our group to demonstrate our networking skills and show that our concept will work if implemented in a real datacenter network.

As with any project, our project has stakeholders involved. The first stakeholder in this project is the company that we are designing the redundant datacenter for. Our design and implementation of this network will directly affect this company, as the company's day-to-day functions rely on how well we implement these network upgrades. If the solution is implemented well, the company should experience less outages due to the implementation of redundant links

and correct routing configuration. If we do a poor job with the design or implementation of our solution, the company may experience more outages than before and could lose valuable time conducting business as well as a lot of money, which would be the exact opposite of what we want our solution to accomplish. The second stakeholder in this project is the clients of the company we are implementing this network for. For example, if the company provides a software-as-a-service to its clients and there's some troubleshooting on that service that needs to be done, the company's network needs to be up in order to update the platform as necessary. If the company's network starts experiencing outages due to our group poorly implementing our solution and can't troubleshoot issues on their service, then the clients won't be able to use a service that they might be paying for a prolonged amount of time since the company needs to troubleshoot their own network before they can troubleshoot their services. The last stakeholder is our project group, or in this scenario the network engineers. Our performance on this project will not only impact our relationship with the company we're implementing the redundant datacenter network for, but will affect our potential opportunities to secure contracts with other businesses as well. If we do a good job with this project, then there will be higher chance that the company we are working with will want to work on more projects in the future with us and recommend us to other companies as well. If not, then we will lose the trust of our client and risk our reputation in the networking industry becoming tarnished.

## Chapter 4: Design

What we managed to create, is a medium sized data center network, with a priority on redundancy. This network consists of two separate data centers, on two networks, that are connected via both redundant and static routes. Data center one is connected to the 10.16.0.0/24 network while the other data center is connected to the 10.18.0.0/24 network. Data center one is the home to routers 1 and 2, layer 3 switches 1 and 2, switches 1 through 4, and Servers 1 through 6. Data center two is the home to routers 3 and 4, layer 3 switches 3 and 4, switches 5 through 8, and Servers 7 through 12. We have two ISP connections coming in, with ISP1 connecting to routers 1 and 4, and ISP2 connecting to routers 2 and 3.

In terms of connectivity, we have connections between the vast majority of devices to one another within each data center as this creates the redundant links. In data center one, we have both router 1 and 2 connected to both layer 3 switches 1 and 2, along with a link between the routers themselves and a link between the layer 3 switches themselves. We have a link from each switch, 1 through 4, going to both layer 3 switches. Next, we have the first three servers connected to both switches 1 and 2. Finally, servers 4 through 6 are connected to both switches 3 and 4. In data center two, we have both router 3 and 4 connected to both layer 3 switches 3 and 4, along with a link between the routers themselves and a link between the layer 3 switches themselves. We have a link from each switch, 5 through 8, going to both layer 3 switches. Next, we have servers 7 through 9 connected to both switches 5 and 6. Finally, servers 10 through 12 are connected to both switches 7 and 8. Our network is configured into four different VLANs, with two for each datacenter. Servers 1 through 3 belong to VLAN 10, 4 through 6 belong to VLAN 20, 7 through 9 belong to VLAN 30, and 10 through 12 belong to VLAN 40.

## IP Table

Authors: Chapter 1 - Stephen Cronin, Chapter 2 - Stephen Cronin, Chapter 3 - Carter Caruso, Chapter 4 - Charles Gill Jr, Chapter 5 - Jakob Idland, Chapter 6 - Charles Gill Jr

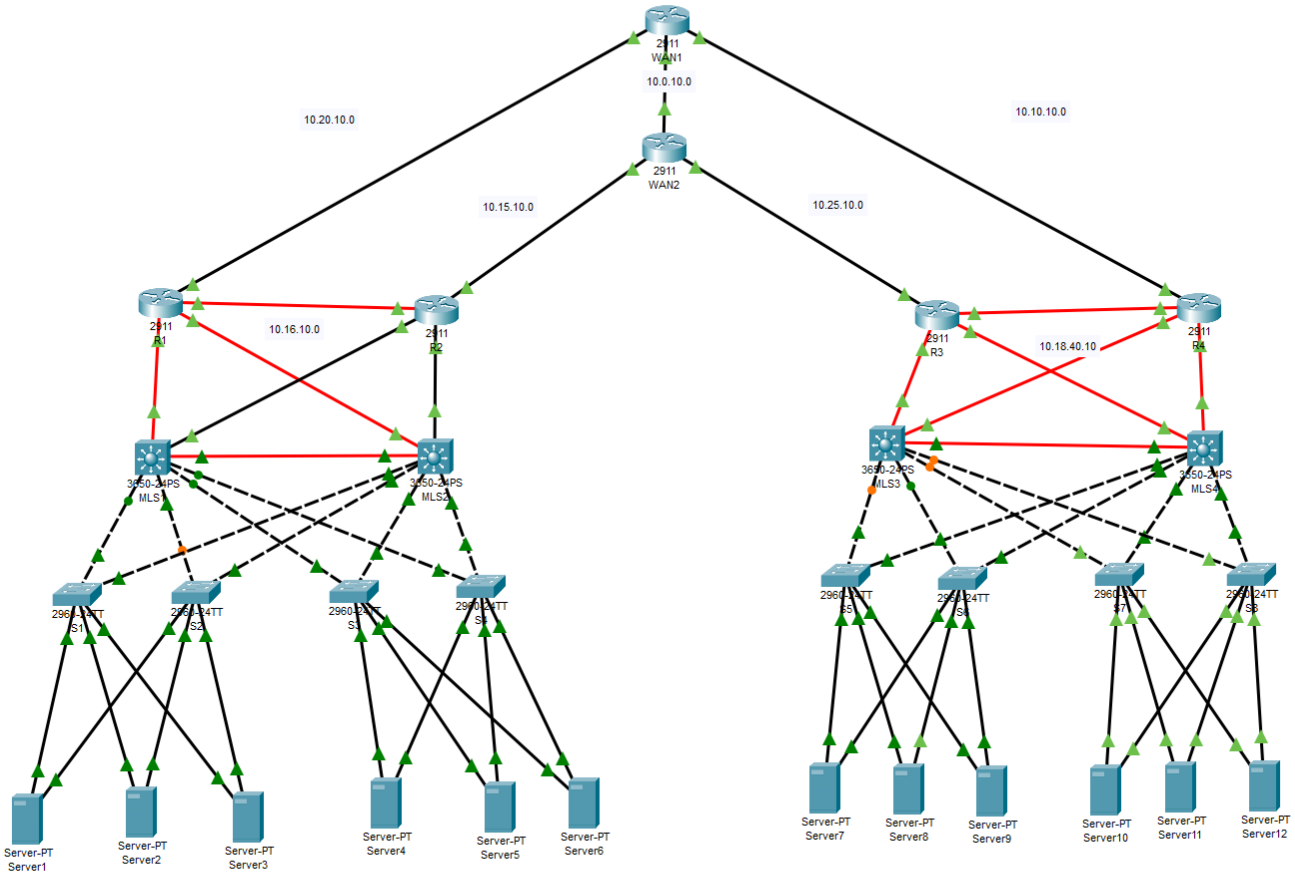
| Device Name | Port Number | IP |
|---|---|---|
| ISP1 | GigabitEthernet0/0 | 10.10.10.1/30 |
| | GigabitEthernet0/1 | 10.20.10.1/30 |
| | GigabitEthernet0/2 | 10.0.10.1/30 |
| ISP2 | GigabitEthernet0/0 | 10.15.10.1/30 |
| | GigabitEthernet0/1 | 10.25.10.1/30 |
| | GigabitEthernet0/2 | 10.0.10.2/30 |
| R1 | GigabitEthernet0/0 | 10.20.10.2/30 |
| | GigabitEthernet0/1/0 | 10.255.0.1/30 |
| | GigabitEthernet0/2/0 | 10.0.1.1/30 |
| | GigabitEthernet0/3/0 | 10.0.0.1/30 |
| R2 | GigabitEthernet0/0 | 10.15.10.2/30 |
| | GigabitEthernet0/1 | 10.0.2.1/30 |
| | GigabitEthernet0/2 | 10.0.3.1/30 |
| | GigabitEthernet0/1/0 | 10.255.0.2/30 |
| R3 | GigabitEthernet0/1 | 10.25.10.2/30 |
| | GigabitEthernet0/1/0 | 10.255.1.1/30 |
| | GigabitEthernet0/2/0 | 10.0.5.1/30 |
| | GigabitEthernet0/3/0 | 10.0.4.1/30 |
| R4 | GigabitEthernet0/0 | 10.10.10.2/30 |
| | GigabitEthernet0/1/0 | 10.255.1.2/30 |
| | GigabitEthernet0/2/0 | 10.0.7.1/30 |
| | GigabitEthernet0/3/0 | 10.0.6.1/30 |
| MLS1 | GigabitEthernet1/0/24 | 10.0.2.2/30 |
| | GigabitEthernet1/1/1 | 10.0.0.2/30 |

Authors: Chapter 1 - Stephen Cronin, Chapter 2 - Stephen Cronin, Chapter 3 - Carter Caruso, Chapter 4 - Charles Gill Jr, Chapter 5 - Jakob Idland, Chapter 6 - Charles Gill Jr

| | | |
|---|---|---|
| | Vlan 10 | 10.16.10.1/24 |
| | Vlan 20 | 10.16.20.1/24 |
| MLS2 | GigabitEthernet1/0/24 | 10.0.3.2/30 |
| | GigabitEthernet1/1/1 | 10.0.1.2/30 |
| | Vlan 10 | 10.16.10.2/24 |
| | Vlan 20 | 10.16.20.2/24 |
| MLS3 | GigabitEthernet1/0/24 | 10.0.4.2/30 |
| | GigabitEthernet1/1/1 | 10.0.6.2/30 |
| | Vlan 30 | 10.18.30.1/24 |
| | Vlan 40 | 10.18.40.1/24 |
| MLS4 | GigabitEthernet1/0/24 | 10.0.5.2/30 |
| | GigabitEthernet1/1/1 | 10.0.7.2/30 |
| | Vlan 30 | 10.18.30.2/24 |
| | Vlan 40 | 10.18.40.2/24 |
| S1 | Vlan 10 | 10.16.10.8/24 |
| S2 | Vlan 10 | 10.16.20.9/24 |
| S3 | Vlan 10 | 10.16.10.13/24 |
| S4 | Vlan 10 | 10.16.10.14/24 |
| S5 | Vlan 10 | 10.16.20.15/24 |
| S6 | Vlan 10 | 10.16.10.16/24 |
| S7 | Vlan 10 | 10.16.10.17/24 |
| S8 | Vlan 10 | 10.16.10.18/24 |
| Server1 | FastEthernet0 | 10.16.10.10/24 |
| Server2 | FastEthernet0 | 10.16.10.11/24 |
| Server3 | FastEthernet0 | 10.16.10.12/24 |

| | | |
|---|---|---|
| Server4 | FastEthernet0 | 10.16.20.10/24 |
| Server5 | FastEthernet0 | 10.16.20.11/24 |
| Server6 | FastEthernet0 | 10.16.20.12/24 |
| Server7 | FastEthernet0 | 10.16.30.10/24 |
| Server8 | FastEthernet0 | 10.16.30.11/24 |
| Server9 | FastEthernet0 | 10.16.30.12/24 |
| Server10 | FastEthernet0 | 10.16.40.10/24 |
| Server11 | FastEthernet0 | 10.16.40.11/24 |
| Server12 | FastEthernet0 | 10.16.40.12/24 |

# Chapter 5: Development




For this project two mock data centers were created in order to be able to configure redundant failover routing and switching. Each router has been configured to only speak to one ISP and another router Would handle the second ISP. Having two ISPs is very important since if one ISP experiences a problem with their network then the data center can use the other ISP link. There is an interconnect cable between the two routers so in case one ISP does go down the router will send the traffic over to the other router. The ISPs have been linked together to simulate how each ISP is connected to the global network. Each of the routers in the data are interconnected to the layer 3 switch so no matter what switch is up it will still be able to reach both routers. Then each of the layer 2 switches are interconnected with the layer 3 switches to ensure further redundancy for the servers in the datacenter.

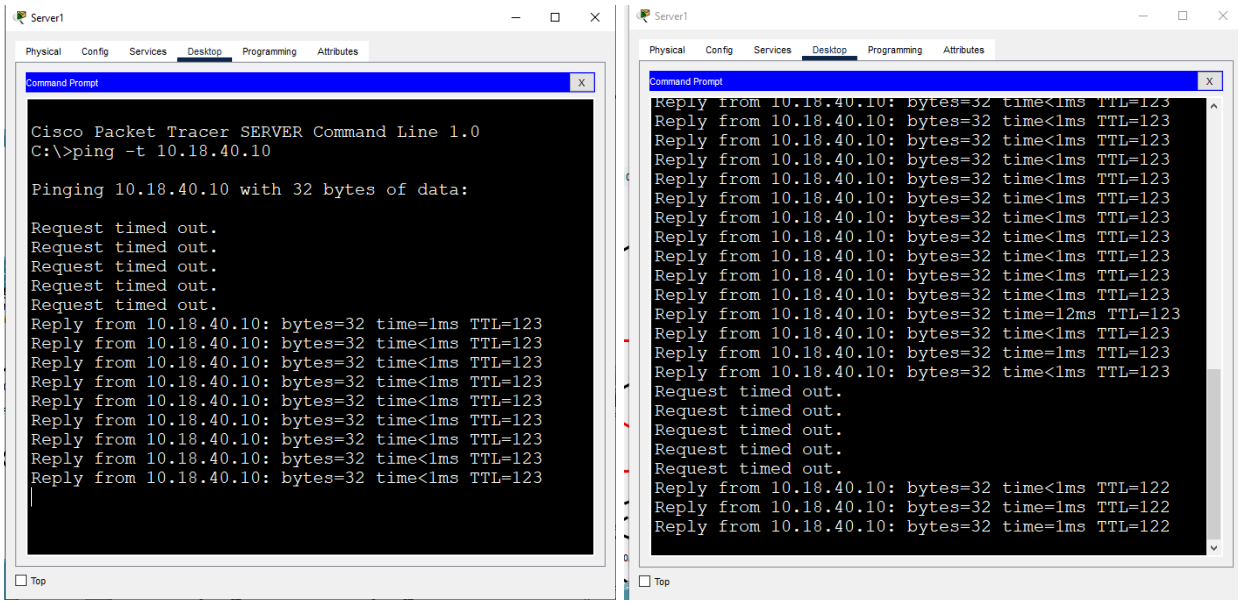
Authors: Chapter 1 - Stephen Cronin, Chapter 2 - Stephen Cronin, Chapter 3 - Carter Caruso, Chapter 4 - Charles Gill Jr, Chapter 5 - Jakob Idland, Chapter 6 - Charles Gill Jr

In this project we used a couple of different routing protocols. We used dynamic static routing for determining which link a router should send data on. When configured the primary link would have a cost of 1, and the secondary would have a cost of 5. Adding these costs would allow the router to always choose to send data on the primary link. Then when the primary link goes down it is able to use the secondary link to then start forwarding the data. For the gateways on the layer 3 switches we used Hot Standby Router Protocol (HSRP) which allowed us to assign a virtual IP address for the routers to share. The primary router would claim the IP meaning all the data forwarded to the gateway would go through that router. If that primary router then failed the secondary router would then pick up the virtual IP making itself the gateway allowing for data to continue to flow making it appear like the default gateway never failed. For STP we configured one of the switches to be the route node which only allowed the layer 2 switches to connect to one of the layer 3 switches, but if the switch then failed it would then switch over to the other layer 3 switch. For security of the datacenter we configured all of the hardware to require a password and SSH from a dedicated VLAN.

Authors: Chapter 1 - Stephen Cronin, Chapter 2 - Stephen Cronin, Chapter 3 - Carter Caruso, Chapter 4 - Charles Gill Jr, Chapter 5 - Jakob Idland, Chapter 6 - Charles Gill Jr

# Chapter 6: Evaluation and Conclusion

To test our solution we went into the command prompt in the servers and used the ping -t and traceroute commands. Ping -t like ping tests the connectivity between two end devices, but does it continuously. This allowed us to keep the ping running while powering off a certain device and would let us see how fast the redundant links would kick in. Due to not being able to set a static ARP Cache, it usually took a ping or two for the connection between end devices to be re-established. In the left screenshot, you can see that our route from Server 1 to Server 10 took 5 pings to create the valid ARP Cache. In the right screenshot, we turned off Router 1 and you can see that it took another 5 pings for R2 to build out its own ARP Cache, however the pings resume after.




We then used traceroute to track the route the packet from one server was taking to the other server. This includes the switches and routers the packet goes through before getting to its

destination. Traceroute allowed us to see the change of the route a packet takes from one server to another when a router or switch goes down.

```
C:\>tracert 10.18.40.10

Tracing route to 10.18.40.10 over a maximum of 30
hops:

  1    0 ms      4294967294 ms0 ms      10.16.10.1
  2    0 ms      0 ms      0 ms      10.0.0.1
  3    0 ms      0 ms      0 ms      10.20.10.1
  4    0 ms      0 ms      0 ms      10.10.10.2
  5    0 ms      0 ms      0 ms      10.0.7.2
  6    0 ms      0 ms      0 ms      10.18.40.10

Trace complete.

C:\>
```

This project has given us an incredible opportunity to familiarize ourselves with the Cisco Command Line Interface and the real-world configuration of network equipment. This class and project has quite literally been the culmination of our time here at NJIT and has given us the opportunity to showcase those networking skills. Through this project, we have learned how to configure switches, routers, routing, as well as how to create redundancy in a network in order to create the Layer-Three redundant network that also provides device security and SSH remote access to each network device on either datacenter network that we have presented to you.

Works Cited

INC, C. (2022, October 28). *Support - Cisco Support and downloads – documentation, tools, cases*. Cisco. Retrieved October 30, 2022, from https://www.cisco.com/c/en/us/support/index.html

*Cisco packet tracer*. Networking Academy. (2022, June 17). Retrieved October 30, 2022, from https://www.netacad.com/courses/packet-tracer