International Islamic University Chittagong

Department of Computer Science and Engineering

Course: Computer Networks Lab
Course Code: CSE3634
Section: 7AF Semester: Autumn Year: 2022

A Project Report on

Enhanced Network Resilience

Authors:

Team Name: Binary Wing

Team Leader: Efter Jahan Ema (C193229)

Members:

1. Tehsim Fariha (C193207)
2. Sahana Akter (C193209)
3. Raisa Ahmed (C193220)

Completion Date: 15-06-23

Course Instructor	Course TA
______________________________ **AbdullahilKafi** **Assistant Professor** **Department of CSE, IIUC**	______________________________ **Department of CSE, IIUC**

Abstract

This project outlines the design and implementation of a network topology aimed at achieving high availability and fault tolerance through ISP redundancy and interconnected switches. The objective is to establish a resilient network infrastructure that ensures uninterrupted connectivity and efficient data transfer. By integrating two cloud-based Internet Service Providers (ISP-1 and ISP-2) with a central router, reliable and redundant internet connectivity is established. Switch-1 and Switch-2 are interconnected to enable seamless communication and provide failover capabilities. Additionally, Switch-3 acts as a distribution switch, connecting endpoints PC1 and PC2 to the network. The project aims to demonstrate the effectiveness of ISP redundancy and interconnected switches in maintaining network availability, ensuring data integrity, and providing seamless failover mechanisms. In the event of an ISP outage or link failure, the network should automatically transition to an alternate ISP or switch, ensuring uninterrupted connectivity and minimizing downtime .The proposal outlines the project's goals, network topology, and expected outcomes, emphasizing the importance of network resilience in today's connected world. This report outlines the design, implementation, and evaluation of the network resilience solution, highlighting its effectiveness in maintaining continuous network connectivity.

Acknowledgements

We would like to extend our heartfelt gratitude to all the individuals and organizations that have played a significant role in the successful completion of the Net Overload GNS3 project. Without their support, expertise, and dedication, this project would not have been possible. We would like to acknowledge and express our thanks to the following:

1. Our project teacher, whose guidance and mentorship have been invaluable throughout the duration of this project. Your insights and feedback have shaped the direction of our work and helped us achieve our goals.
2. The team members who actively participated in the project, contributing their time, effort, and expertise. Each team member played a crucial role and demonstrated exceptional teamwork, leading to the success of this project.
3. The contributors to the GNS3 community, who have developed an excellent network simulation tool. GNS3 has been instrumental in enabling us to simulate and analyze complex network scenarios. We are grateful for this open-source software and the opportunities it has provided us.
4. Our friends, whose unwavering support and encouragement have been a source of motivation throughout this project. We appreciate their belief in our abilities and understanding during challenging times.
5. The individuals who participated in user testing and provided valuable feedback on our project. Your input has been invaluable in refining and improving our solution, ensuring its effectiveness and usability.

We extend our sincere appreciation to all those mentioned above and anyone else who has contributed in any way to the completion of the Net Overload GNS3 project. Thank you for your support, expertise, and encouragement. We are grateful for the opportunity to work on this project and for the contributions that have made it a success.

Sincerely,
The Binary Wing Team

Table of Contents

1. Introduction:

The objective of this lab report is to present the goals, methodology, and findings of our project conducted in an ISP (Internet Service Provider) cloud environment. The project focuses on establishing a network structure involving two ISP clouds interconnected through routers, with additional routers connecting individual PCs. This report provides an overview of our project goals, summarizes the work completed, highlights our key findings, and outlines the subsequent sections of the report.

Project Goals:
The primary goal of our project is to design and implement a robust network infrastructure using the ISP cloud model. We aim to leverage the advantages of ISP clouds, such as redundancy, load balancing, and improved network performance. By interconnecting routers and PCs, we seek to create a scalable and resilient network architecture that can effectively handle diverse network traffic requirements.

Summary of Work:
To achieve our goals, we began by setting up the ISP cloud environment. This involved configuring and connecting two ISP clouds using a central router. Additionally, we established connections between the central router and two additional routers, which, in turn, were connected to individual PCs. The network configuration required careful attention to routing protocols, addressing schemes, and ensuring seamless connectivity between components.

Throughout the implementation phase, we encountered challenges related to network configuration, performance optimization, and troubleshooting connectivity issues. By employing systematic methodologies and troubleshooting techniques, we were able to overcome these challenges and successfully establish the desired network structure.

Key Findings:
Our project yielded several important findings. Firstly, the interconnection of routers within the ISP cloud environment introduced enhanced network redundancy. This redundancy significantly improves network resilience by minimizing the impact of failures or downtime. Secondly, the load balancing capability offered by the interconnected routers allows for efficient distribution of network traffic, resulting in optimized performance and reduced congestion.

Furthermore, our project demonstrated the practical aspects of working with ISP cloud environments. We gained insights into the advantages of such architectures, such as scalability and flexibility, while also becoming aware of the challenges associated with configuration complexity and troubleshooting.

Rest of the Report:
The subsequent sections of this report will provide detailed information on the methodology employed, including the specific configurations and settings implemented for each component of the network. We will present the results of our performance tests, including metrics such as network latency, throughput, and packet loss. Additionally, we will discuss any limitations or constraints encountered during the project and propose potential areas for further improvement or expansion.

By documenting our project structure, goals, methodology, and findings, we aim to provide a comprehensive understanding of our work in the ISP cloud environment. This report serves as a valuable resource for network engineers and researchers interested in implementing similar network architectures and exploring the benefits and challenges of ISP cloud environments.

2. Background:

The project conducted in an ISP cloud environment holds significant importance in the field of networking and cloud computing. As the demand for reliable and scalable network infrastructures continues to grow, ISP clouds offer a promising solution. These environments enable Internet Service Providers to deliver high-performance services by leveraging distributed resources and intelligent routing techniques.

The importance of the project lies in its exploration of the benefits and challenges associated with ISP cloud architectures. By interconnecting multiple routers and PCs, the project aims to enhance network redundancy, load balancing, and overall performance. The findings from this project can have practical implications for real-world network deployments, especially in scenarios where network resilience and efficient traffic management are critical.

Tools and Methods Used:

Routers: Routers are essential networking devices used to forward data packets between different networks. In this project, routers play a crucial role in connecting the ISP clouds, interconnecting the additional routers, and enabling communication between the PCs.

ISP Cloud Environment: The ISP cloud model provides a framework for distributing network resources and services across multiple locations. By utilizing the ISP cloud environment, we can simulate real-world scenarios and assess the effectiveness of the proposed network architecture.

Network Configuration: The project involves configuring the routers, assigning IP addresses, and defining routing protocols. Network configuration tools, such as command-line interfaces or graphical user interfaces provided by router manufacturers, were used to set up and manage the network components.

Routing Protocols: To facilitate efficient routing within the ISP cloud environment, various routing protocols such as OSPF (Open Shortest Path First) or BGP (Border Gateway Protocol) may be employed. These protocols help establish optimal paths for data packets and enable dynamic routing decisions.

Performance Testing: The project includes performance testing to evaluate the effectiveness of the implemented network architecture. Network monitoring tools, such as Wireshark or NetFlow analyzers, can be utilized to measure network latency, throughput, and packet loss, providing insights into the network's performance and identifying potential bottlenecks.

Troubleshooting and Debugging: Throughout the project, troubleshooting and debugging techniques are essential to address any connectivity issues, network configuration errors, or performance anomalies. Command-line tools provided by the router manufacturers, along with network diagnostic utilities, aid in identifying and resolving these issues.

The combination of these tools and methods allows for the effective implementation, monitoring, and evaluation of the ISP cloud network architecture. By employing these resources, the project aims to gain practical insights into the benefits and challenges of ISP cloud environments while demonstrating the importance of robust network infrastructures in modern networking scenarios.

3. literature review:

3.1. Campus Network:

In the context of networking, a campus network refers to a network infrastructure that connects various buildings within a specific geographical area, such as a university campus or a corporate office. Campus networks typically consist of multiple interconnected switches and routers, providing connectivity to devices such as computers, printers, and servers. These networks play a crucial role in facilitating efficient communication and resource sharing within a campus environment.

Understanding the concepts and design principles of campus networks is essential for our project as it involves interconnecting routers and PCs within the ISP cloud environment. By reviewing relevant literature on campus networks, we can gain insights into best practices for network architecture, scalability, and security.

3.2. IPv4 and VLSM:

Internet Protocol version 4 (IPv4) is the most widely used protocol for routing packets across the internet. It employs a 32-bit addressing scheme, allowing for approximately 4.3 billion unique IP addresses. Variable Length Subnet Masking (VLSM) is a technique used to allocate IP addresses more efficiently by subnetting a network into smaller subnets of varying sizes.

In our project, a comprehensive understanding of IPv4 addressing and subnetting, including VLSM, is crucial for proper network configuration and IP address assignment. Reviewing literature on IPv4 addressing and VLSM will provide us with the necessary knowledge to design an efficient addressing scheme for our ISP cloud environment.

3.3. GNS3:

GNS3 (Graphical Network Simulator 3) is a widely used network simulation tool that allows users to create and emulate complex network topologies. It provides a platform for virtualizing network devices, such as routers, switches, and firewalls, enabling users to design, configure, and test network environments without the need for physical hardware.

In our project, GNS3 can be utilized to create a virtualized representation of the ISP cloud environment, facilitating network configuration, testing, and troubleshooting. Exploring literature on GNS3 will provide insights into its features, capabilities, and best practices for its effective utilization in our project.

3.4. Routing:

Routing is a critical aspect of network communication, responsible for directing data packets from a source to a destination across interconnected networks. Various routing protocols, such as OSPF (Open Shortest Path First) or BGP (Border Gateway Protocol), are employed to determine optimal paths for data transmission.

Understanding different routing protocols and their characteristics is vital for our project, as we aim to establish efficient communication within the ISP cloud environment. Reviewing literature on routing protocols will help us make informed decisions regarding the selection and configuration of appropriate protocols to achieve desired network performance and reliability.

3.5. Cisco Images:

Cisco images refer to the operating system images used to run Cisco network devices, such as routers and switches. These images contain the necessary software components and functionalities required for the proper functioning of Cisco devices.

In our project, selecting and utilizing the appropriate Cisco images for the virtual routers within the GNS3 environment is crucial. Reviewing literature on Cisco images will help us understand the available options, their compatibility with GNS3, and the steps involved in image installation and configuration.

By conducting a thorough literature review on these topics, we can gather valuable insights, best practices, and technical knowledge necessary for the successful implementation of our project in the ISP cloud environment.

4. Problem Statement:

Enhanced Network Resilience with Three Routers, One Switch, and ISP1 and ISP2

Introduction:
In network infrastructures, ensuring high resilience is crucial to maintain continuous connectivity and minimize downtime. This problem statement focuses on enhancing network resilience by utilizing three routers, one switch, and multiple ISPs, namely ISP1 and ISP2. The objective is to design and implement a robust network architecture that can withstand failures, provide efficient routing between ISPs, and ensure uninterrupted network connectivity.

Router Redundancy and Failover:
The problem statement aims to address the challenge of router redundancy and failover. By deploying three routers in the network infrastructure, it seeks to investigate mechanisms for automatic failover in case of router failures. This involves exploring protocols such as Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) to ensure seamless failover and continuous routing between ISPs, minimizing disruptions in network connectivity.

Load Balancing and Link Optimization:
To enhance network resilience and maximize utilization of available network resources, the problem statement includes load balancing and link optimization considerations. It explores techniques to distribute network traffic evenly across multiple ISPs, ensuring optimal utilization and preventing congestion. The use of protocols such as Border Gateway Protocol (BGP) and link aggregation (e.g., EtherChannel) can be examined to achieve load balancing and efficient link utilization.

ISP Redundancy and Routing:
To enhance network resilience, the problem statement addresses ISP redundancy and efficient routing between ISP1 and ISP2. It investigates mechanisms to establish failover and redundancy between the two ISPs, ensuring uninterrupted Internet connectivity in case of ISP failures. This includes exploring routing protocols such as BGP with Multi-Exit Discriminator (MED) or Community attributes to influence traffic routing decisions and optimize path selection between ISPs.

Switch Redundancy and High Availability:
In addition to router redundancy, the problem statement also focuses on switch redundancy and high availability. By deploying a single switch, it aims to explore techniques such as Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) to ensure redundant paths and rapid convergence in case of switch failures. The objective is to design a resilient switch infrastructure that can handle failures seamlessly and maintain uninterrupted connectivity.

Monitoring and Network Management:

To ensure effective network resilience, the problem statement investigates monitoring and network management practices. It explores tools and technologies for monitoring the health and performance of routers, switches, and ISPs. This includes network management protocols like Simple Network Management Protocol (SNMP) and monitoring systems that provide real-time visibility into the network infrastructure. The objective is to enable proactive monitoring, quick fault detection, and efficient troubleshooting to maintain network resilience.

5. Designs:

4.1.

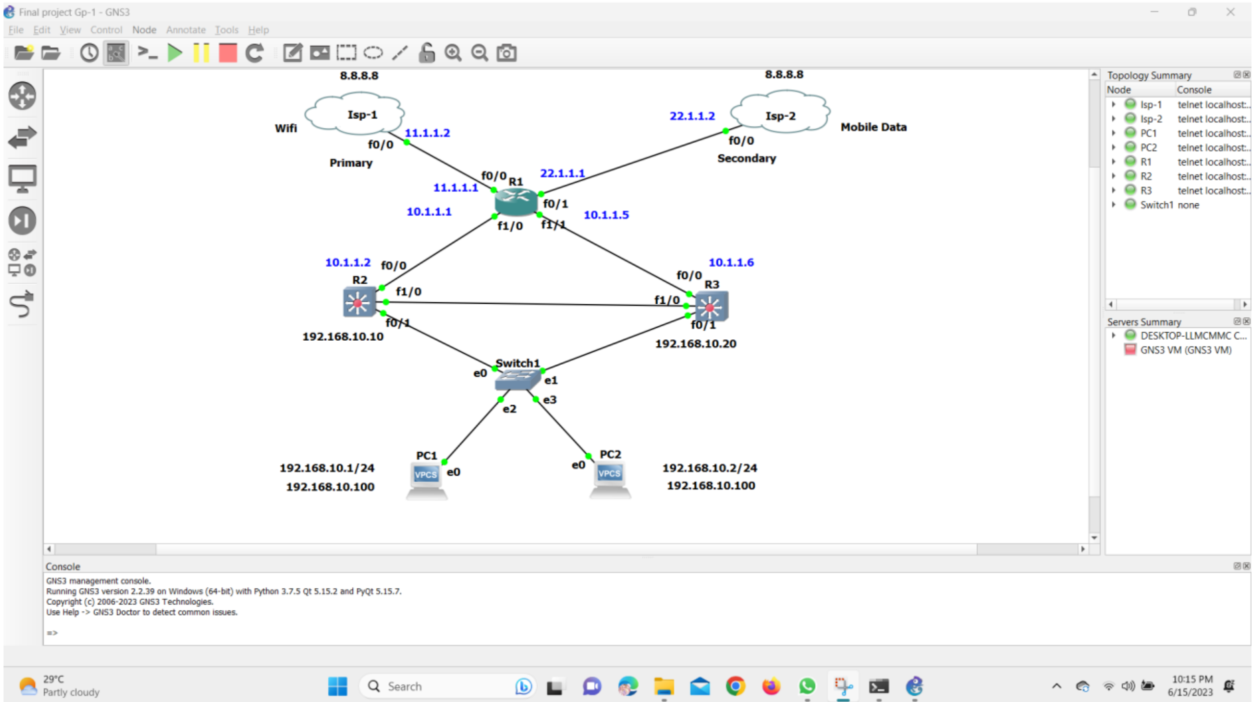


Figure1: Whole Network Topology

4.2. Calculations:

4.3. IP Tables:

4.4. Software and hardware

Software and Hardware Requirements: Net Overload GNS3 Project

To successfully undertake the Net Overload GNS3 project and utilize the GNS3 network simulation tool, the following software and hardware requirements should be considered:

Software Requirements:

1. GNS3: GNS3 is the primary software tool used for network simulation in this project. Ensure you have the latest version of GNS3 installed on your computer. GNS3 is available for Windows, macOS, and Linux operating systems.

2. Operating System: Ensure that your computer is running a compatible operating system, such as Windows 10, macOS Mojave or later, or a Linux distribution (e.g., Ubuntu, CentOS).

3. Virtualization Software: GNS3 relies on virtualization technologies to emulate network devices. You will need to install virtualization software, such as Oracle VirtualBox or VMware Workstation, to create and run virtual machines (VMs) within GNS3.

4. Network Device Images: Obtain the necessary network device images to be used within GNS3. These images can include Cisco IOS, Juniper JunOS, or other vendor-specific software images. Ensure that you have the legal rights to use these images.

Hardware Requirements:

1. Processor: A multicore processor (preferably Intel Core i5 or higher) is recommended for running GNS3 and handling the network simulations effectively.

2. Memory: Adequate RAM is crucial for running complex network simulations. A minimum of 8GB RAM is recommended, although higher capacities (16GB or more) will provide smoother performance.

3. Storage: Sufficient storage space is necessary for installing GNS3, virtual machine images, and other required software. Aim for at least 100GB of free disk space.

4. Network Interfaces: Your computer should have at least one physical network interface to connect to the simulated network in GNS3. Multiple network interfaces are advantageous for advanced scenarios involving routing and network traffic manipulation.

5. Graphics: A decent graphics card is recommended to handle the graphical rendering of network topologies and virtual machines within GNS3.

It is essential to review the specific software and hardware requirements of each component (GNS3, virtualization software, network device images, etc.) to ensure compatibility and optimal performance.

By meeting these software and hardware requirements, you can create and simulate network environments effectively within GNS3, facilitating the Net Overload GNS3 project and enabling the exploration of network overload scenarios and mitigation strategies.

4.5. Topology

The topology of the network design will follow the structure outlined earlier, where two ISP clouds are interconnected through a central router, which is further connected to two additional routers. The additional routers will connect to individual PCs. The interconnection between the routers will enable efficient routing and communication within the ISP cloud environment. The specific configuration and setup of the topology will be based on the project requirements and objectives, including considerations for redundancy, load balancing, and overall network performance.

6. Implementation

5.1. Install GNS3

To install GNS3, follow these steps:

1. Visit the official GNS3 website at https://www.gns3.com/ and navigate to the "Downloads" section.

2. Choose the appropriate version of GNS3 for your operating system (Windows, macOS, or Linux) and click on the corresponding download link.

3. Once the download is complete, locate the downloaded installer file (e.g., gns3-x.x.x.exe for Windows, gns3-x.x.x.dmg for macOS, or the appropriate package for your Linux distribution).

4. Run the installer file and follow the on-screen instructions to begin the installation process. Make sure to review and accept any license agreements, if prompted.

5. During the installation, you may be asked to choose additional components or dependencies to install. Select the desired components based on your requirements. For most basic installations, the default options should suffice.

6. Once the installation is complete, launch GNS3 from the desktop shortcut or the Start menu (Windows) / Applications folder (macOS).

7. Upon launching GNS3 for the first time, you will be prompted to configure certain settings. Follow the on-screen instructions to set up the required preferences, including the path to the network device images and the virtualization software (such as VirtualBox or VMware) you have installed.

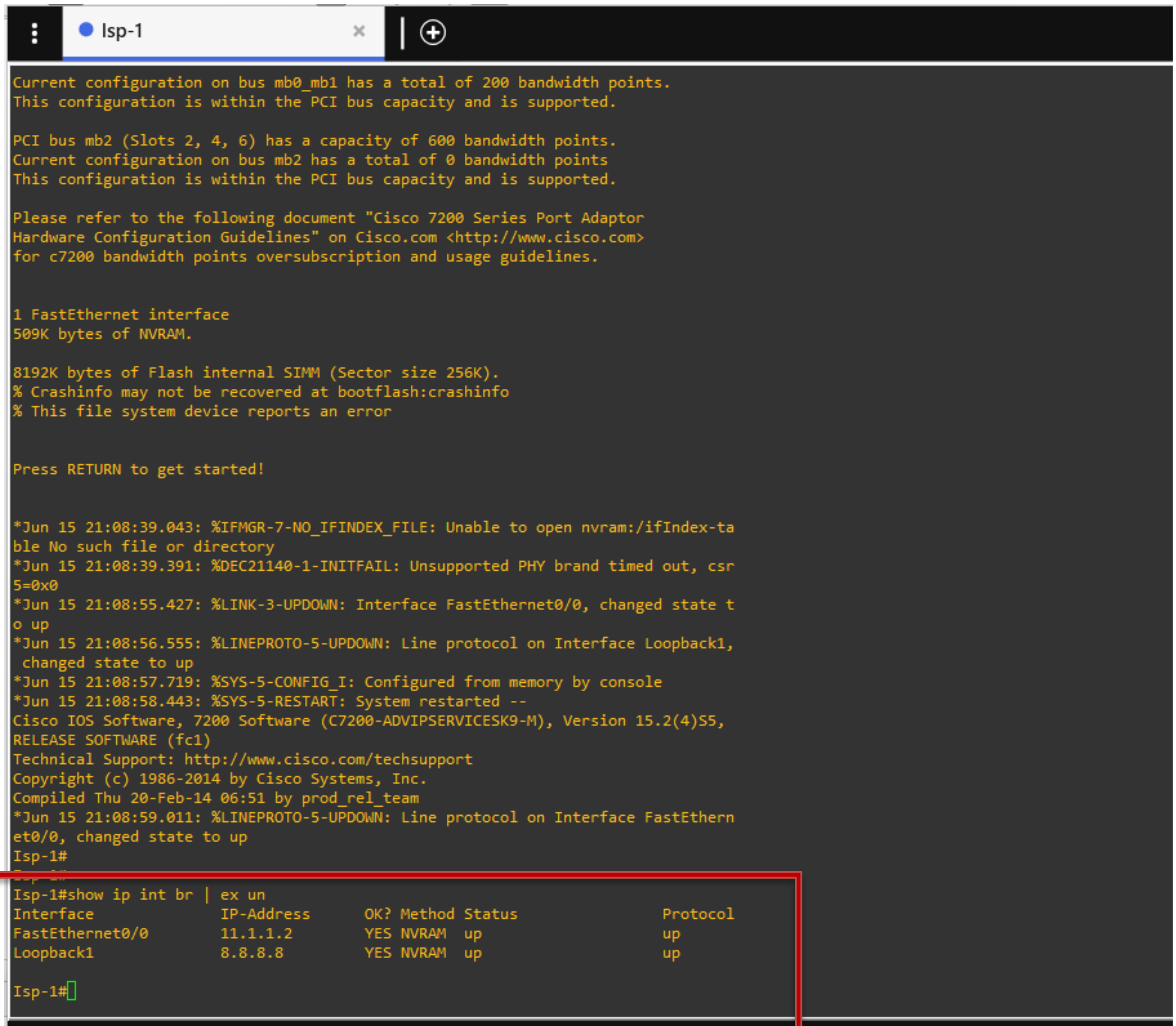
8. After the initial setup, GNS3 will be ready to use. You can create new network projects, import network device images, and design network topologies within the GNS3 graphical interface.

Remember that GNS3 relies on virtualization software to run network device images. Ensure that you have installed a compatible virtualization software (such as Oracle VirtualBox or VMware Workstation) before running GNS3.

It's important to note that GNS3 requires a certain level of technical expertise to set up and use effectively. If you encounter any issues during the installation process or while using GNS3, refer to the GNS3 documentation and user guides available on their website or seek assistance from the GNS3 community forums for troubleshooting and support.

5.2. Configurations

ISP-1



```
Isp-1

Current configuration on bus mb0_mb1 has a total of 200 bandwidth points.
This configuration is within the PCI bus capacity and is supported.

PCI bus mb2 (Slots 2, 4, 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 0 bandwidth points
This configuration is within the PCI bus capacity and is supported.

Please refer to the following document "Cisco 7200 Series Port Adaptor
Hardware Configuration Guidelines" on Cisco.com <http://www.cisco.com>
for c7200 bandwidth points oversubscription and usage guidelines.


1 FastEthernet interface
509K bytes of NVRAM.

8192K bytes of Flash internal SIMM (Sector size 256K).
% Crashinfo may not be recovered at bootflash:crashinfo
% This file system device reports an error


Press RETURN to get started!


*Jun 15 21:08:39.043: %IFMGR-7-NO_IFINDEX_FILE: Unable to open nvram:/ifIndex-ta
ble No such file or directory
*Jun 15 21:08:39.391: %DEC21140-1-INITFAIL: Unsupported PHY brand timed out, csr
5=0x0
*Jun 15 21:08:55.427: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Jun 15 21:08:56.555: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
 changed state to up
*Jun 15 21:08:57.719: %SYS-5-CONFIG_I: Configured from memory by console
*Jun 15 21:08:58.443: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVIPSERVICESK9-M), Version 15.2(4)S5,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Feb-14 06:51 by prod_rel_team
*Jun 15 21:08:59.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
Isp-1#
Isp-1#
Isp-1#show ip int br | ex un
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        11.1.1.2        YES NVRAM  up                    up
Loopback1              8.8.8.8         YES NVRAM  up                    up

Isp-1#
```

Figure2: ISP-1 configuration

ISP-2

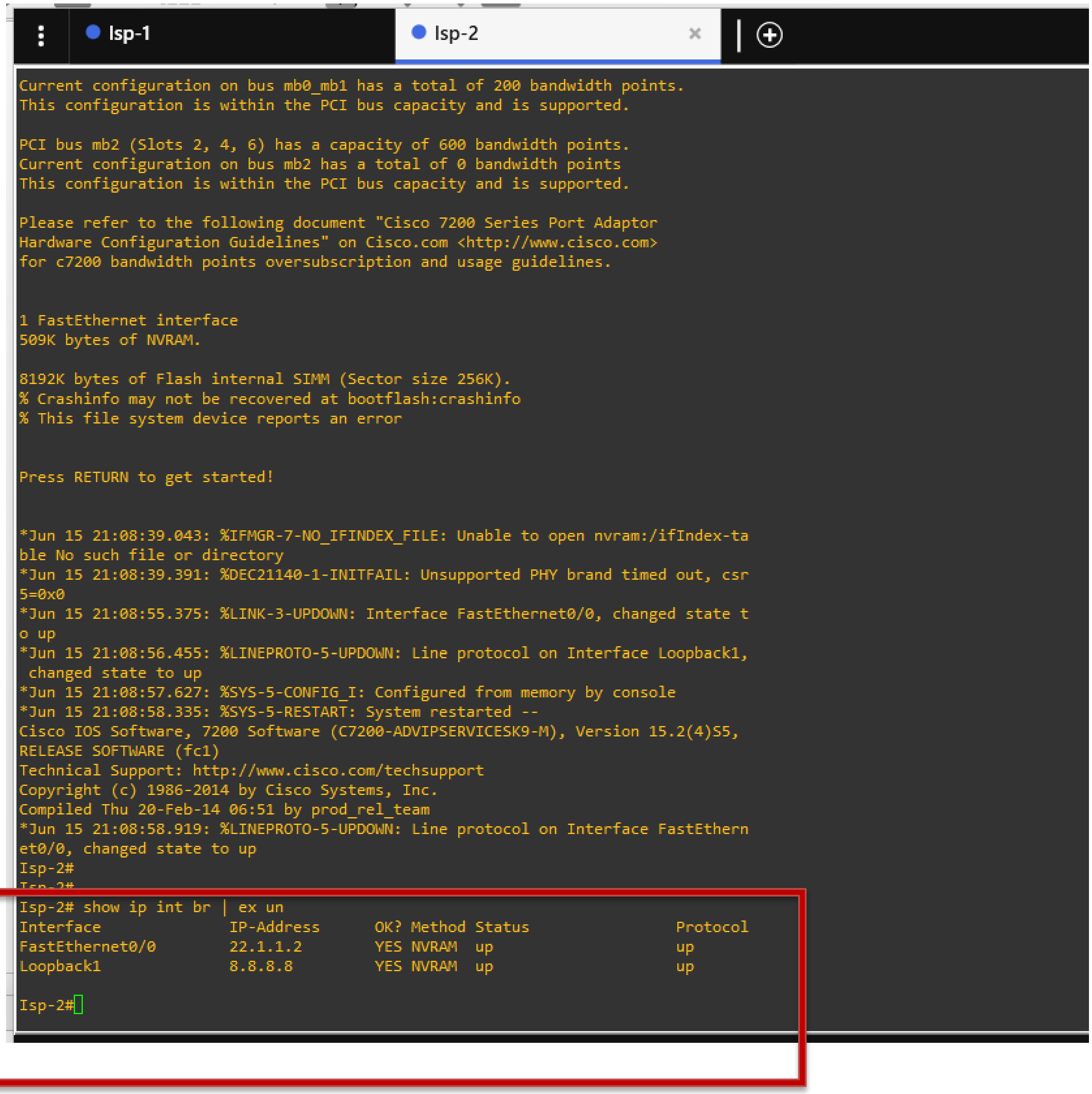


Figure3: ISP-2 configuration

PC-1

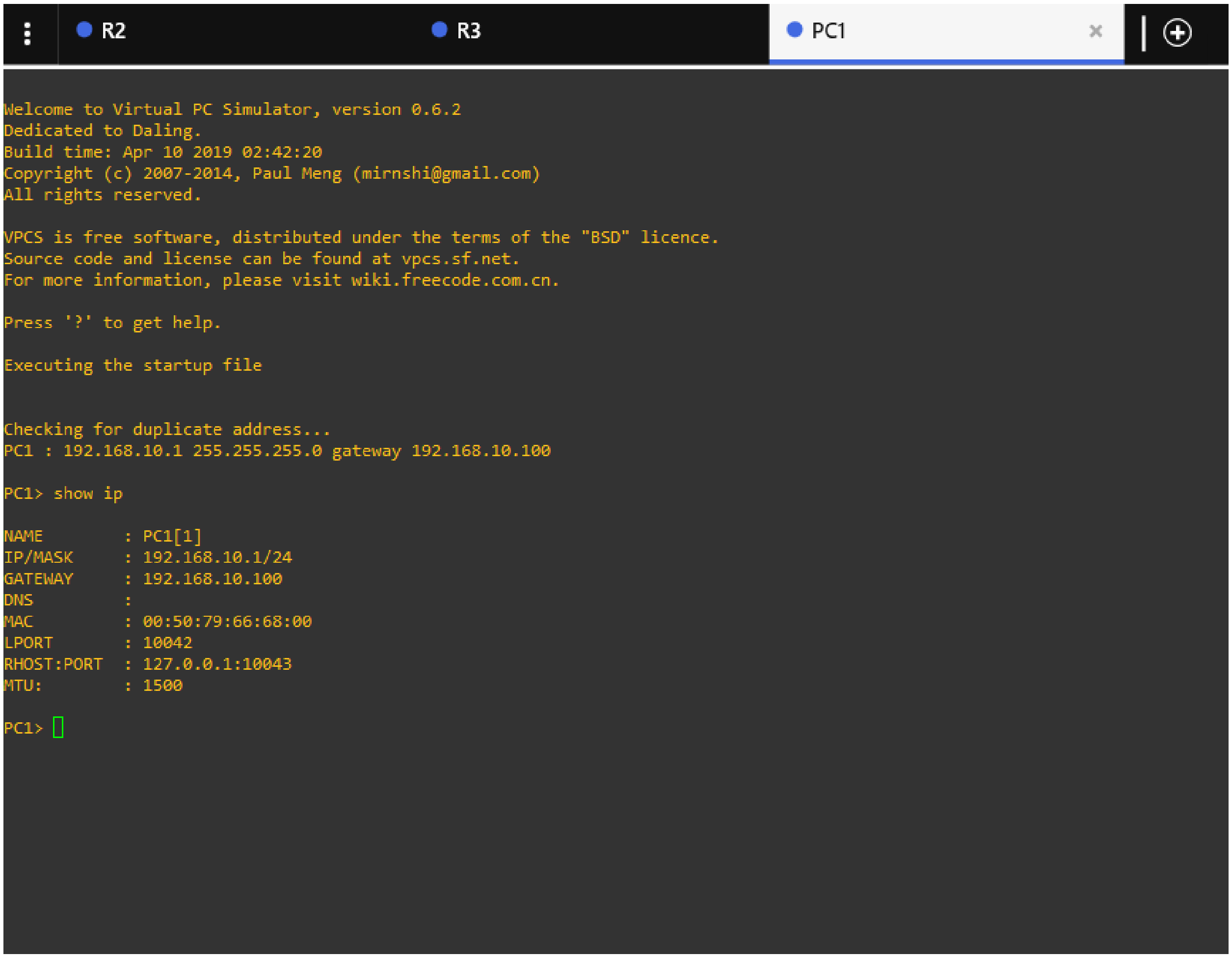


Figure4: PC1 Addressing

PC-2

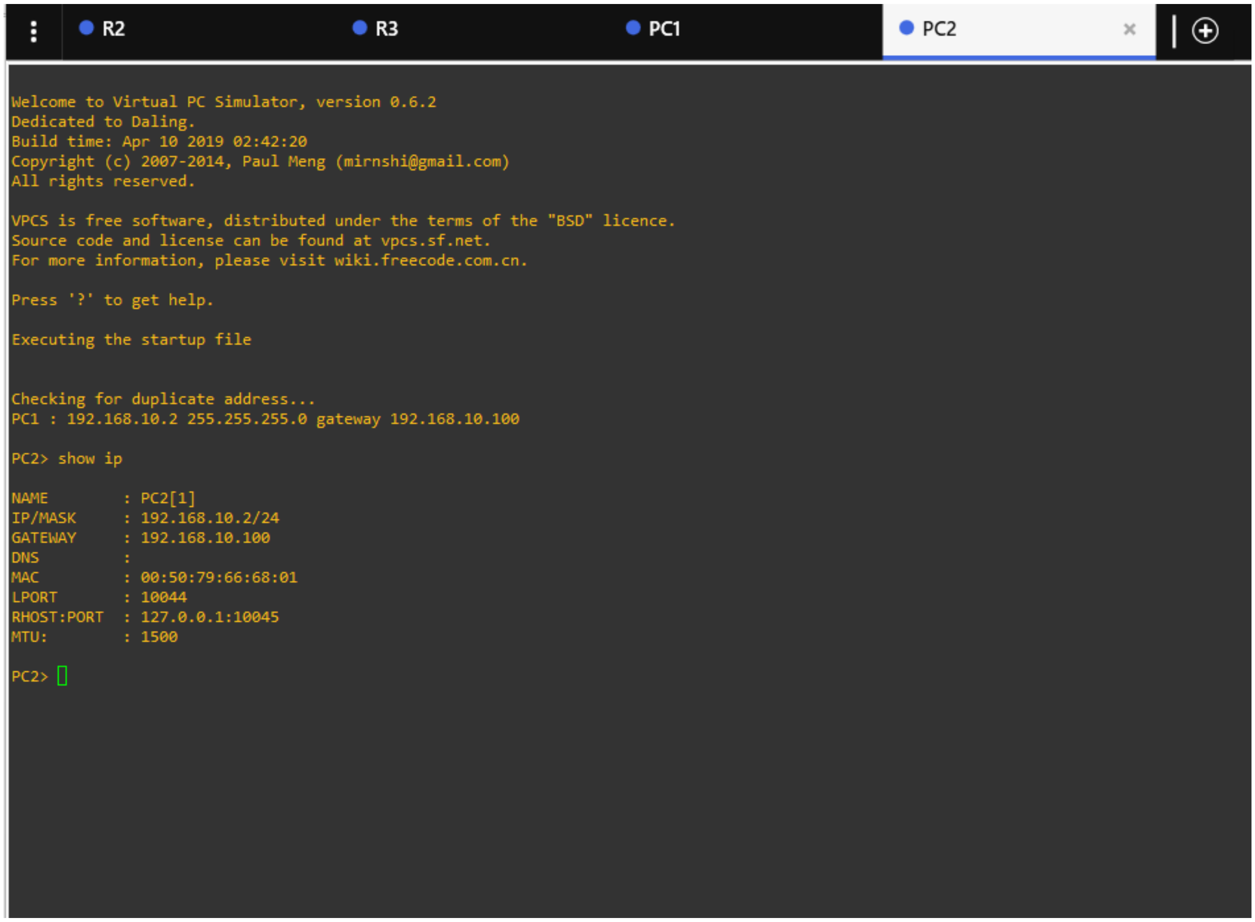
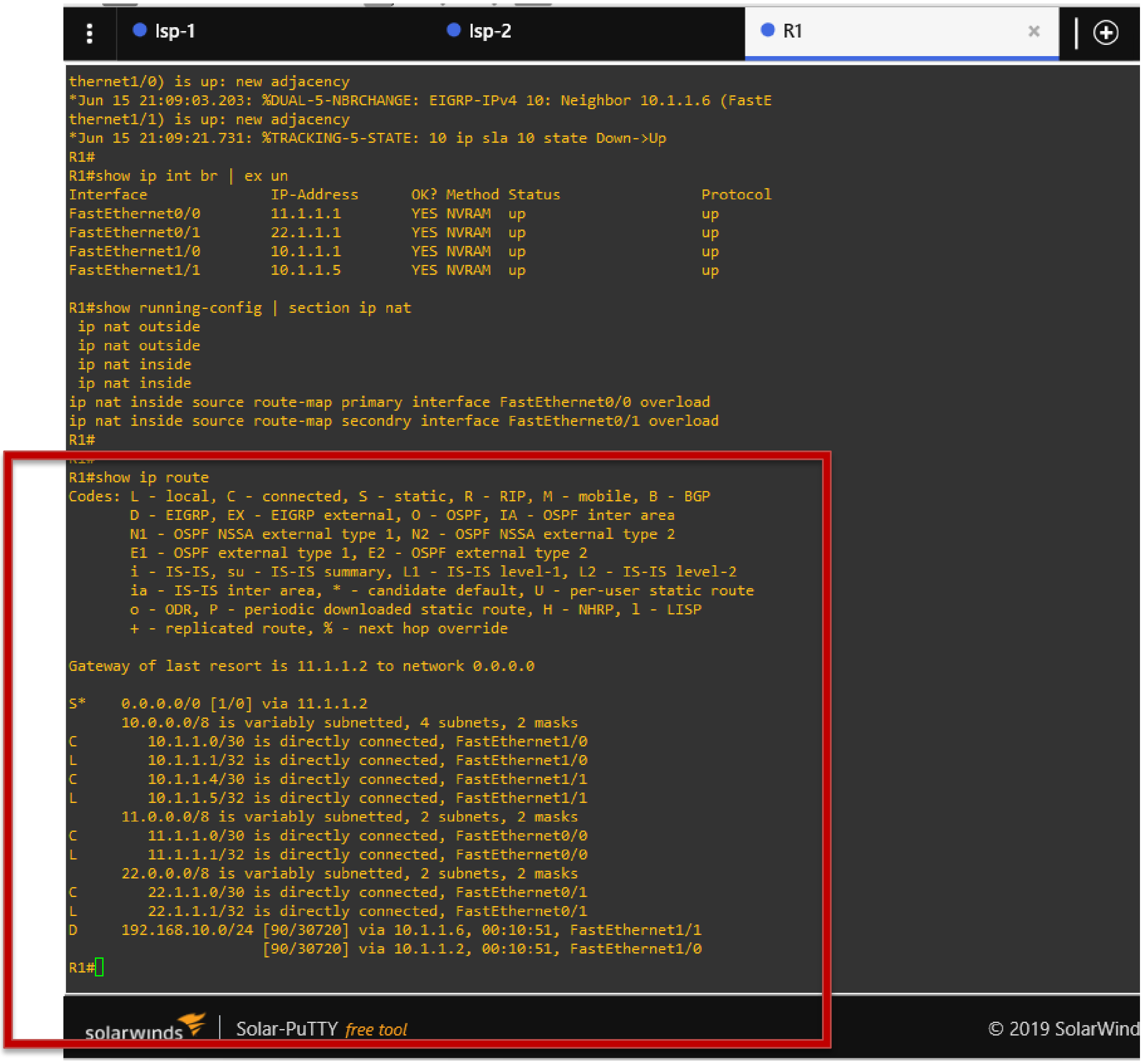


Figure5: PC2 Addressing

R1:



```
thernet1/0) is up: new adjacency
*Jun 15 21:09:03.203: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 10.1.1.6 (FastE
thernet1/1) is up: new adjacency
*Jun 15 21:09:21.731: %TRACKING-5-STATE: 10 ip sla 10 state Down->Up
R1#
R1#show ip int br | ex un
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        11.1.1.1        YES NVRAM  up                    up
FastEthernet0/1        22.1.1.1        YES NVRAM  up                    up
FastEthernet1/0        10.1.1.1        YES NVRAM  up                    up
FastEthernet1/1        10.1.1.5        YES NVRAM  up                    up

R1#show running-config | section ip nat
 ip nat outside
 ip nat outside
 ip nat inside
 ip nat inside
ip nat inside source route-map primary interface FastEthernet0/0 overload
ip nat inside source route-map secondry interface FastEthernet0/1 overload
R1#
R1#
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 11.1.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 11.1.1.2
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, FastEthernet1/0
L        10.1.1.1/32 is directly connected, FastEthernet1/0
C        10.1.1.4/30 is directly connected, FastEthernet1/1
L        10.1.1.5/32 is directly connected, FastEthernet1/1
      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        11.1.1.0/30 is directly connected, FastEthernet0/0
L        11.1.1.1/32 is directly connected, FastEthernet0/0
      22.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        22.1.1.0/30 is directly connected, FastEthernet0/1
L        22.1.1.1/32 is directly connected, FastEthernet0/1
D     192.168.10.0/24 [90/30720] via 10.1.1.6, 00:10:51, FastEthernet1/1
                      [90/30720] via 10.1.1.2, 00:10:51, FastEthernet1/0
R1#
```


Figure6: Router 1 configuration

R2:

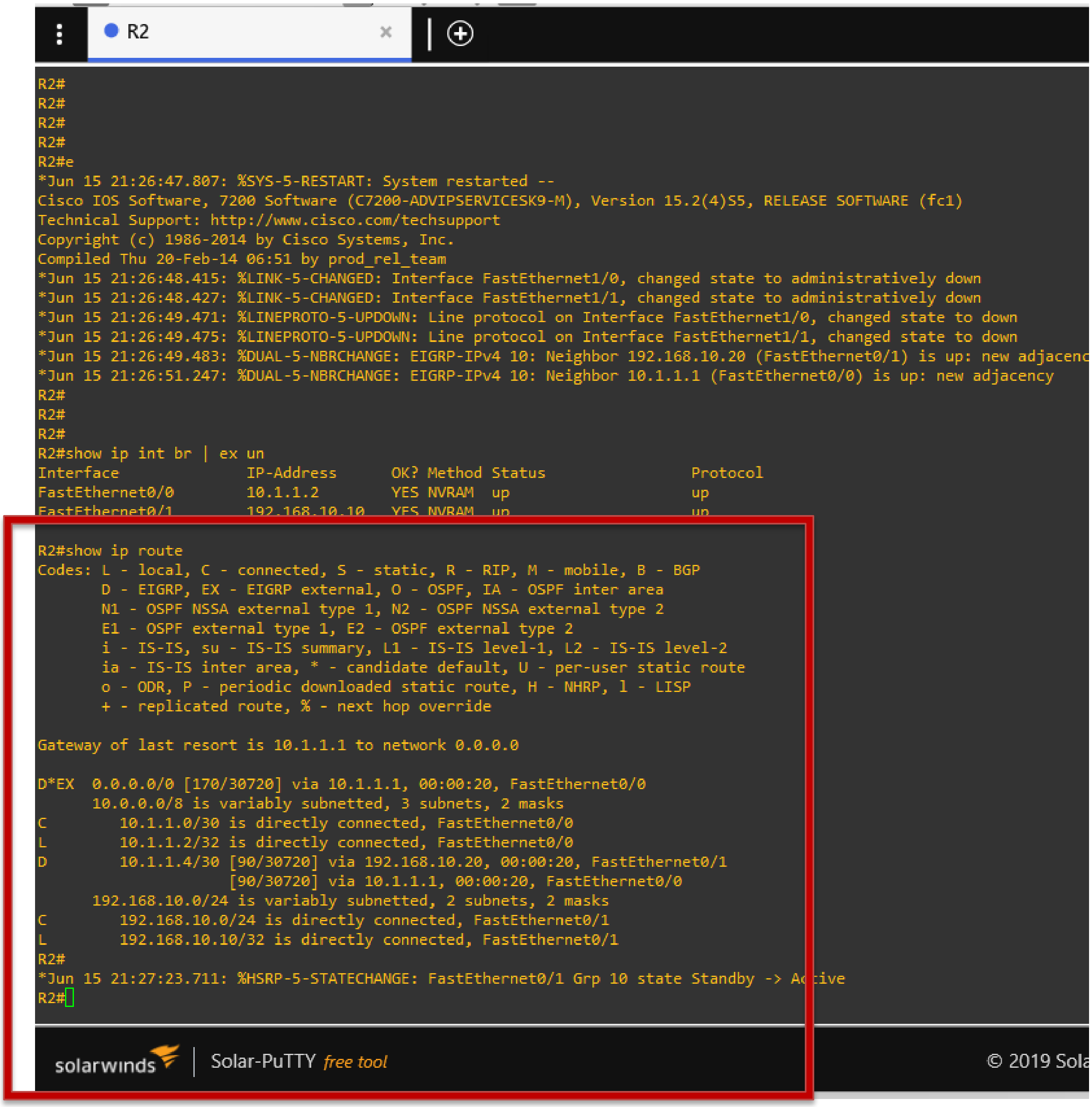
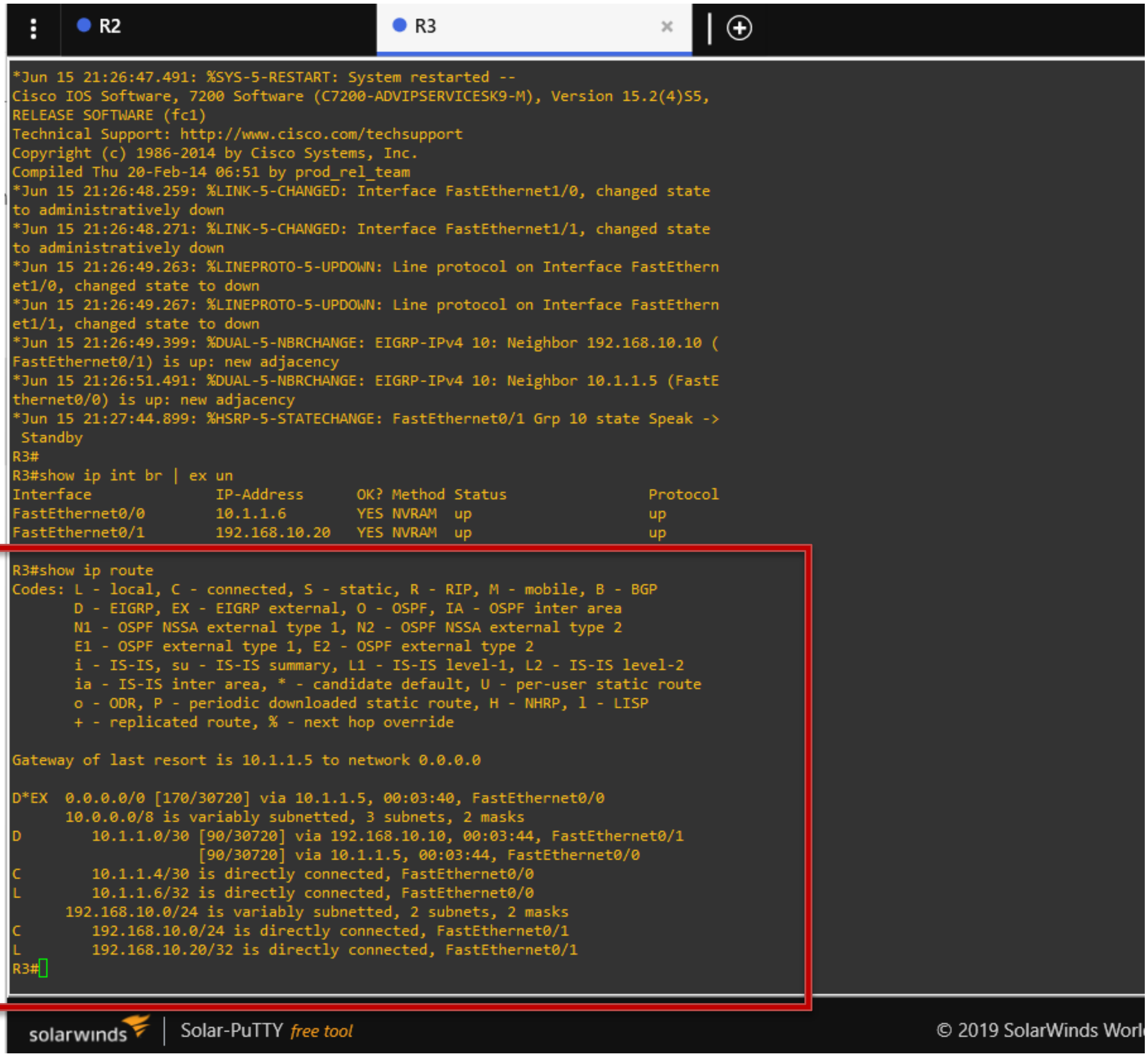


Figure7: Router 2 configuration

R3:



```
*Jun 15 21:26:47.491: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVIPSERVICESK9-M), Version 15.2(4)S5,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Feb-14 06:51 by prod_rel_team
*Jun 15 21:26:48.259: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state
to administratively down
*Jun 15 21:26:48.271: %LINK-5-CHANGED: Interface FastEthernet1/1, changed state
to administratively down
*Jun 15 21:26:49.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to down
*Jun 15 21:26:49.267: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/1, changed state to down
*Jun 15 21:26:49.399: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 192.168.10.10 (
FastEthernet0/1) is up: new adjacency
*Jun 15 21:26:51.491: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 10.1.1.5 (FastE
thernet0/0) is up: new adjacency
*Jun 15 21:27:44.899: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 10 state Speak ->
 Standby
R3#
R3#show ip int br | ex un
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.1.1.6        YES NVRAM  up                    up
FastEthernet0/1        192.168.10.20   YES NVRAM  up                    up

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.5 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/30720] via 10.1.1.5, 00:03:40, FastEthernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D        10.1.1.0/30 [90/30720] via 192.168.10.10, 00:03:44, FastEthernet0/1
                     [90/30720] via 10.1.1.5, 00:03:44, FastEthernet0/0
C        10.1.1.4/30 is directly connected, FastEthernet0/0
L        10.1.1.6/32 is directly connected, FastEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, FastEthernet0/1
L        192.168.10.20/32 is directly connected, FastEthernet0/1
R3#
```


Figure8: Router 3 configuration

7. Experimental and Theoretical Results:

7.1. Pinging the Core router:

R1 to ISP1:

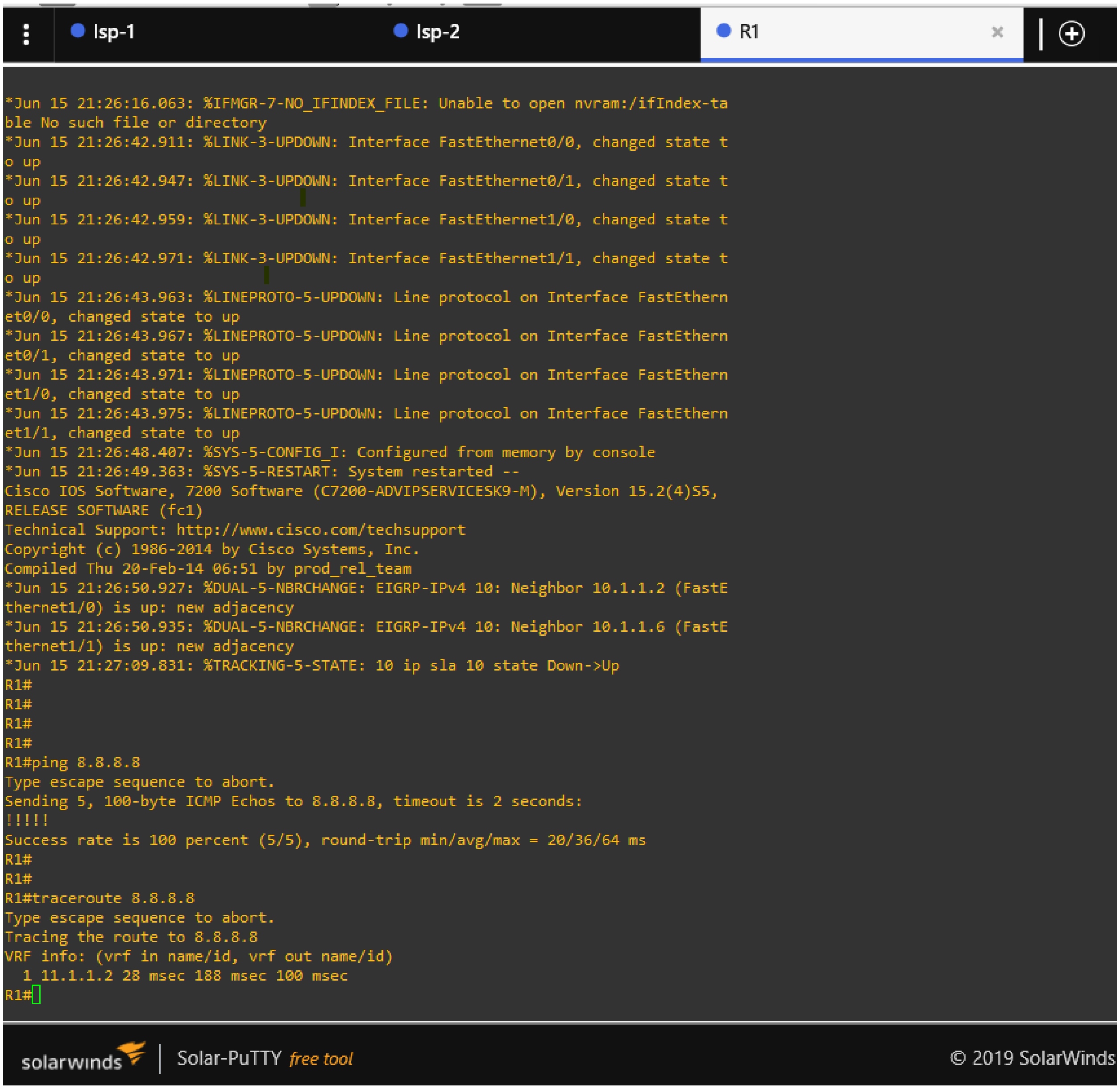


Figure9: R1 to ISP1 ping

R1 to ISP2:


```
*Jun 15 21:26:49.363: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVIPSERVICESK9-M), Version 15.2(4)S5,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Feb-14 06:51 by prod_rel_team
*Jun 15 21:26:50.927: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 10.1.1.2 (FastE
thernet1/0) is up: new adjacency
*Jun 15 21:26:50.935: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 10.1.1.6 (FastE
thernet1/1) is up: new adjacency
*Jun 15 21:27:09.831: %TRACKING-5-STATE: 10 ip sla 10 state Down->Up
R1#
R1#
R1#
R1#
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/36/64 ms
R1#
R1#
R1#traceroute 8.8.8.8
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
  1 11.1.1.2 28 msec 188 msec 100 msec
R1#
R1#
R1#
R1#
R1#
*Jun 15 21:37:44.835: %TRACKING-5-STATE: 10 ip sla 10 state Up->Down
R1#
R1#
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/88/152 ms
R1#
R1#
R1#traceroute 8.8.8.8
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
  1 22.1.1.2 32 msec 24 msec 24 msec
R1#
```

Figure10: R1 to ISP2 ping

R3 to ISP1:


```
thernet0/0) is up: new adjacency
*Jun 15 21:27:44.899: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 10 state Speak ->
 Standby
R3#
R3#show ip int br | ex un
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.1.1.6        YES NVRAM  up                    up
FastEthernet0/1        192.168.10.20   YES NVRAM  up                    up

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.5 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/30720] via 10.1.1.5, 00:03:40, FastEthernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D        10.1.1.0/30 [90/30720] via 192.168.10.10, 00:03:44, FastEthernet0/1
                     [90/30720] via 10.1.1.5, 00:03:44, FastEthernet0/0
C        10.1.1.4/30 is directly connected, FastEthernet0/0
L        10.1.1.6/32 is directly connected, FastEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, FastEthernet0/1
L        192.168.10.20/32 is directly connected, FastEthernet0/1
R3#
R3#
R3#
R3#
R3#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/100/304 ms
R3#
R3#
R3#traceroute 8.8.8.8
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.5 24 msec 32 msec 28 msec
  2 11.1.1.2 68 msec 56 msec 52 msec
R3#
```


Figure11: R3 to ISP1 ping

When ISP1 = Shutdown;
R1 to ISP2:

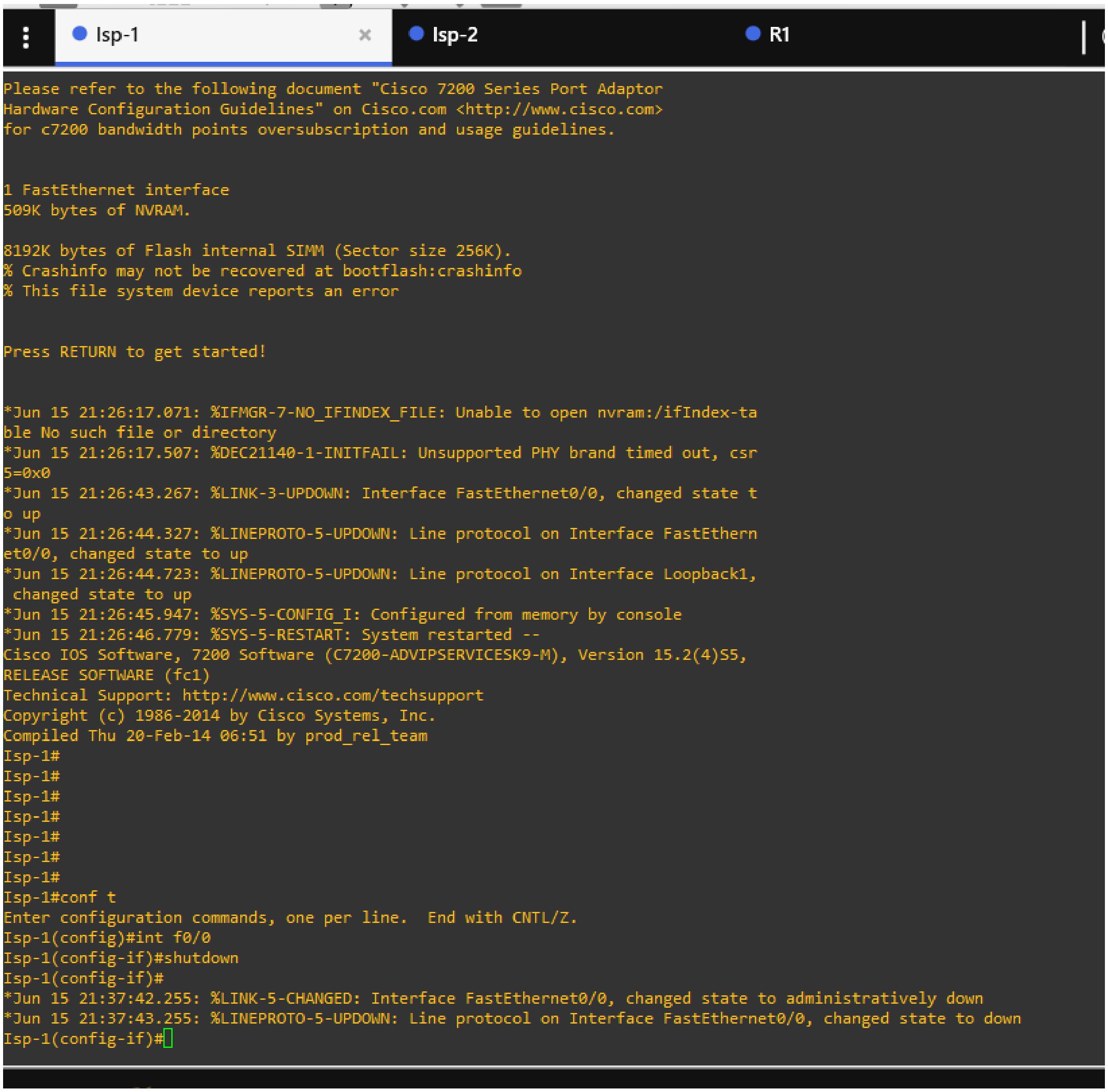
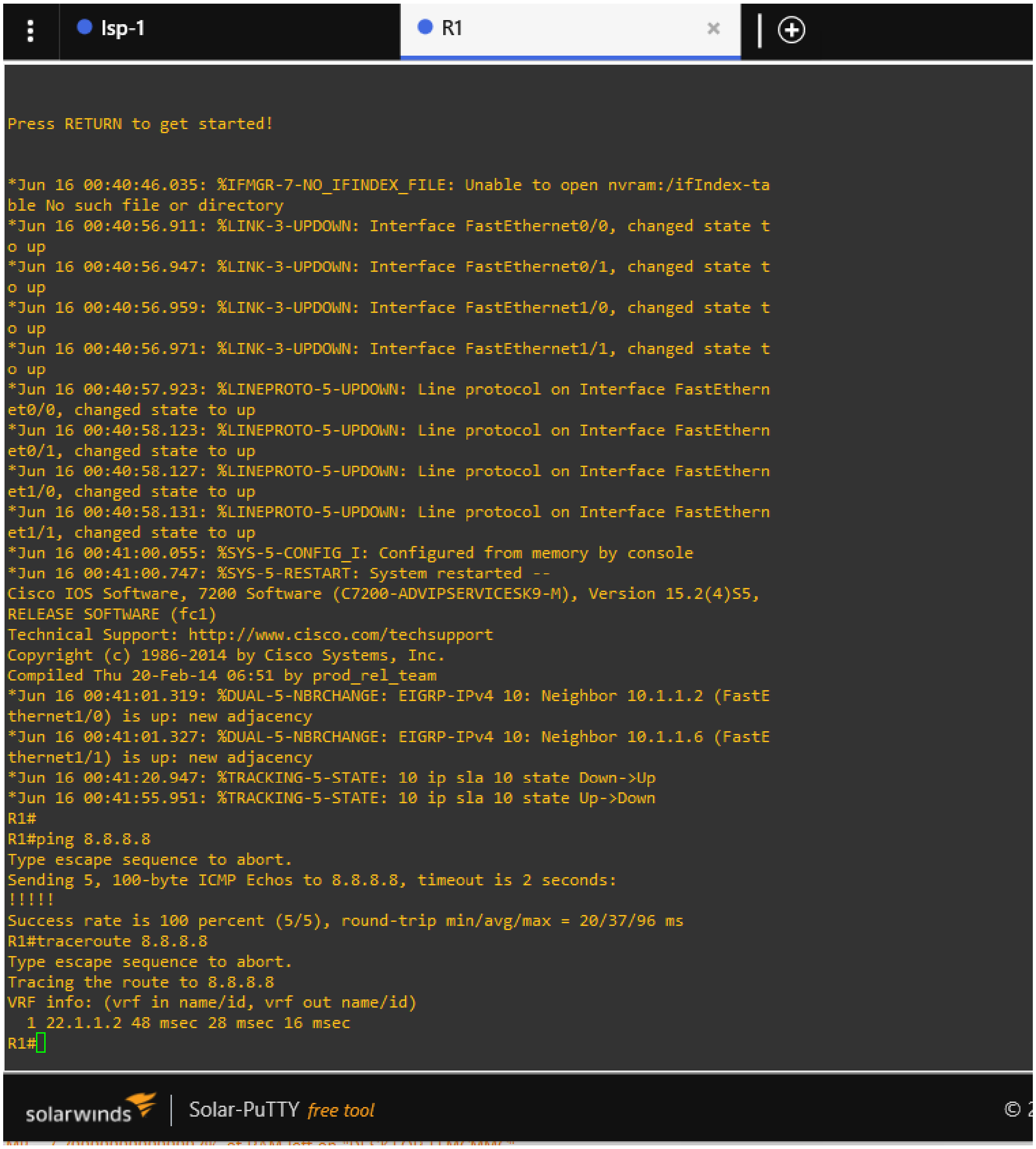


Figure12: ISP1 Shutdown

R1 to ISP2:




```
Press RETURN to get started!


*Jun 16 00:40:46.035: %IFMGR-7-NO_IFINDEX_FILE: Unable to open nvram:/ifIndex-ta
ble No such file or directory
*Jun 16 00:40:56.911: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Jun 16 00:40:56.947: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Jun 16 00:40:56.959: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state t
o up
*Jun 16 00:40:56.971: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state t
o up
*Jun 16 00:40:57.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
*Jun 16 00:40:58.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
*Jun 16 00:40:58.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to up
*Jun 16 00:40:58.131: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/1, changed state to up
*Jun 16 00:41:00.055: %SYS-5-CONFIG_I: Configured from memory by console
*Jun 16 00:41:00.747: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVIPSERVICESK9-M), Version 15.2(4)S5,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Feb-14 06:51 by prod_rel_team
*Jun 16 00:41:01.319: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 10.1.1.2 (FastE
thernet1/0) is up: new adjacency
*Jun 16 00:41:01.327: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 10.1.1.6 (FastE
thernet1/1) is up: new adjacency
*Jun 16 00:41:20.947: %TRACKING-5-STATE: 10 ip sla 10 state Down->Up
*Jun 16 00:41:55.951: %TRACKING-5-STATE: 10 ip sla 10 state Up->Down
R1#
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/37/96 ms
R1#traceroute 8.8.8.8
Type escape sequence to abort.
Tracing the route to 8.8.8.8
VRF info: (vrf in name/id, vrf out name/id)
  1 22.1.1.2 48 msec 28 msec 16 msec
R1#
```

Figure13: R1 to ISP2 ping

ISP1 = Active;
R2 to ISP1:

Figure14: R2 to ISP1 ping (ISP1 active)

When ISP1 = Shutdown;
R2 to ISP2:

Figure15: R2 to ISP2 (ISP1 shutdown)

PC1 to ISP1:

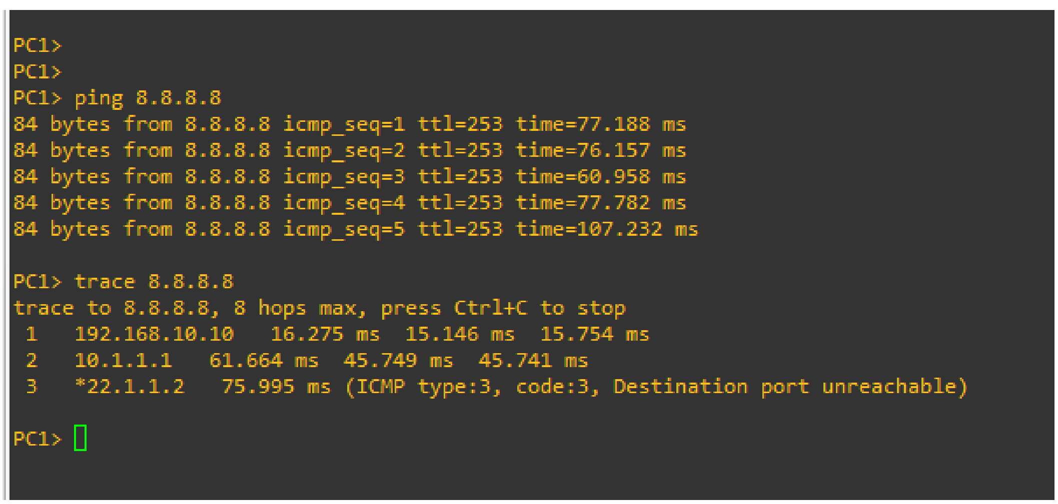

```
PC1> ping  8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=288.952 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=75.822 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=253 time=75.890 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=253 time=75.604 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=253 time=75.737 ms

PC1> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   192.168.10.10   16.524 ms  15.398 ms  15.516 ms
 2   10.1.1.1   46.673 ms  46.047 ms  44.631 ms
 3   *11.1.1.2   76.812 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

Figure16: PC1 to ISP1

ISP1 = Shutdown
PC1 to ISP2:



```
PC1>
PC1>
PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=77.188 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=76.157 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=253 time=60.958 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=253 time=77.782 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=253 time=107.232 ms

PC1> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   192.168.10.10   16.275 ms  15.146 ms  15.754 ms
 2   10.1.1.1   61.664 ms  45.749 ms  45.741 ms
 3   *22.1.1.2   75.995 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

Figure17: PC1 to ISP2 (ISP1 shutdown)

ISP1 = Shutdown

PC2 to ISP2:

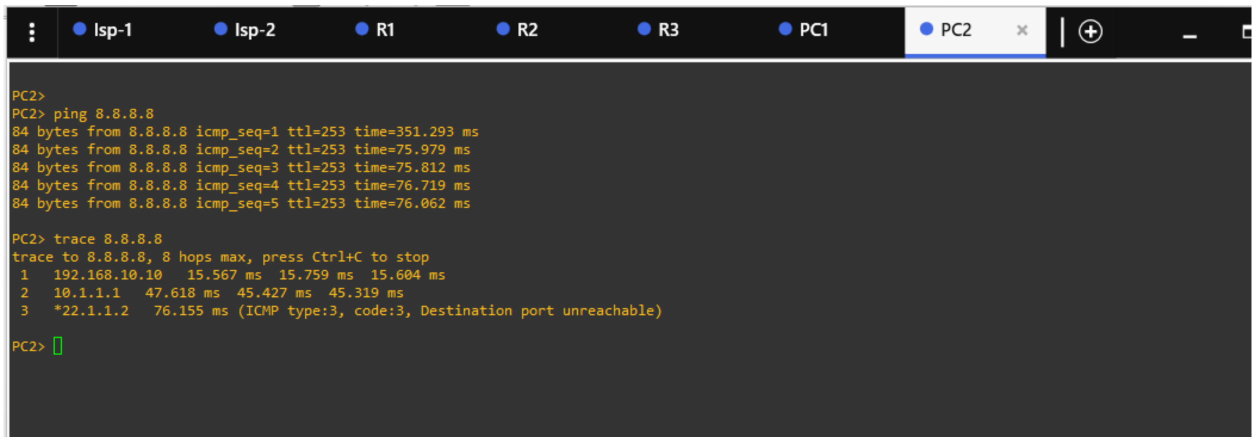


Figure18: PC2 to ISP2 (ISP1 shutdown)

R2 = Shutdown

PC2 to ISP1:

Figure19: PC2 to ISP1 (R2 shutdown)

When R2 port (f0/0) = Shutdown

```
R2#
R2#
R2#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int f0/0
R2(config-if)#shutdown
R2(config-if)#
*Jun 15 21:54:22.875: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 10.1.1.1 (FastEthernet0/0) is down: interface down
R2(config-if)#
*Jun 15 21:54:24.827: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Jun 15 21:54:25.827: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
R2(config-if)#no shutdown
R2(config-if)#
R2(config-if)#
```

Figure20: R2 port (f0/0) shutdown

Then
PC1 to ISP1:

```
PC1>
PC1>
PC1>
PC1>
PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=106.583 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=92.309 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=253 time=91.375 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=253 time=91.455 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=253 time=91.157 ms

PC1> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   192.168.10.10   15.567 ms  15.867 ms  15.080 ms
 2   192.168.10.20   75.491 ms  31.546 ms  32.221 ms
 3   10.1.1.5   60.089 ms  61.070 ms  60.686 ms
 4   *11.1.1.2   91.416 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

Figure21: PC1 to ISP1 ping

When R2 & R3 both = Shutdown
PC cannot reach network

```
PC2> ping 8.8.8.8
host (192.168.10.100) not reachable

PC2>
```

Figure22: PC cannot reach ISP

When ISP1 & ISP2 both = Shutdown
PC cannot reach network

```
PC2>
PC2>
PC2> ping 8.8.8.8
8.8.8.8 icmp_seq=1 timeout
8.8.8.8 icmp_seq=2 timeout
8.8.8.8 icmp_seq=3 timeout
8.8.8.8 icmp_seq=4 timeout
8.8.8.8 icmp_seq=5 timeout

PC2> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   192.168.10.10   16.583 ms  15.775 ms  15.227 ms
 2   10.1.1.1   46.926 ms  45.363 ms  45.593 ms
 3     *  *  *
```

Figure23: PC cannot reach ISP

7.2. Pinging in the same Network:

PC1 to PC2:

```
PC1

Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


Checking for duplicate address...
PC1 : 192.168.10.1 255.255.255.0 gateway 192.168.10.100

PC1> ping 192.168.10.2
84 bytes from 192.168.10.2 icmp_seq=1 ttl=64 time=0.947 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=64 time=1.005 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=64 time=1.410 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=64 time=1.004 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=64 time=0.835 ms

PC1>
```

Figure24: PC1 to P

7.3. Table of ping results:

	A	B	C	D	E	F	G	H	I	J
1	PC1 Ping To	Seq1_Time(ms)	Seq2_Time(ms)	Seq3_Time(ms)	Sqe4_Time(ms)	Seq5_Time(ms)	Count	Minimum(ms)	Maximum(ms)	Average(ms)
2	ISP1	288.952	75.822	75.89	75.604	75.737	5	2.154	17.157	6.0786
3	ISP2	77.188	76.157	60.958	77.782	107.232	5	60.958	107.232	79.8634
4		47.43	62.643	48.366	50.014	63.06	5	47.43	63.06	54.3026
5		Not Reachable								
6		Not Reachable								
7										
8	PC2 Ping To	Seq1_Time(ms)	Seq2_Time(ms)	Seq3_Time(ms)	Sqe4_Time(ms)	Seq5_Time(ms)	Count	Minimum(ms)	Maximum(ms)	Average(ms)
9	ISP1	75.067	105.511	77.695	76.351	75.302	5	75.067	105.511	81.9852
10	ISP2	351.293	75.979	75.812	76.719	76.062	5	75.812	351.293	131.173
11										

Figure25: Ping results from PC1 and PC2 to ISP1 and ISP2

7.4. Bar chart of Ping results:

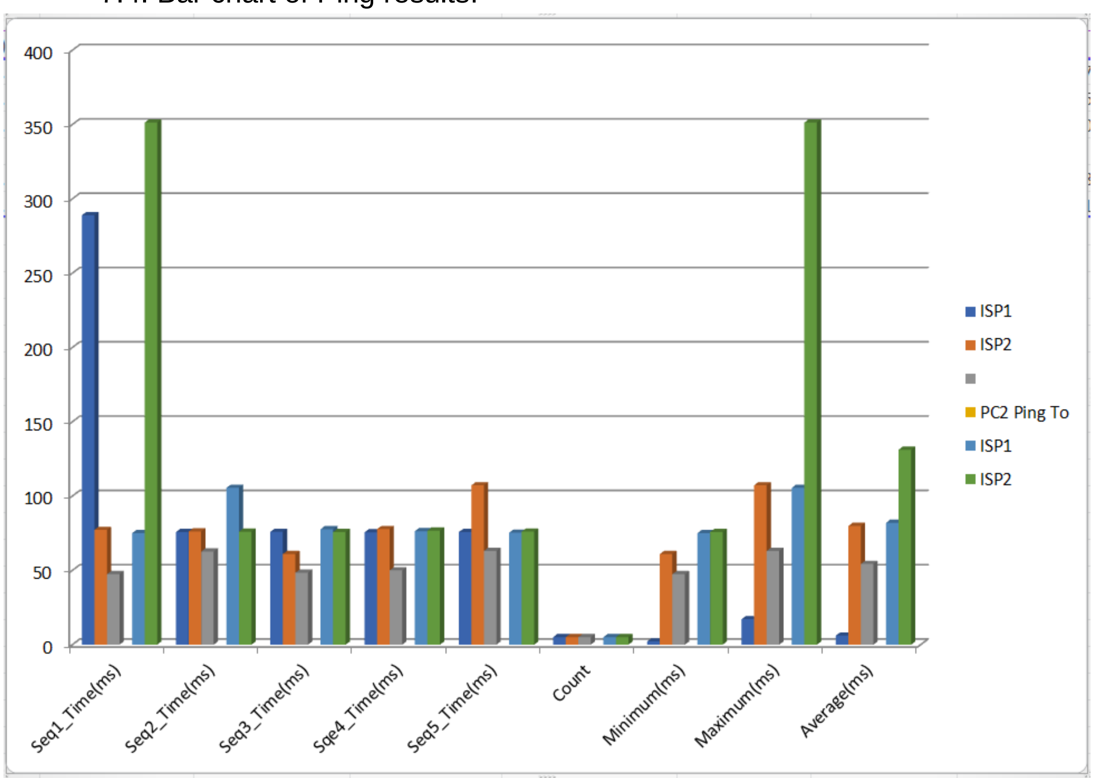


Figure26: Bar chart of Ping result

7.5. Discussion on result:

We successfully have been able to increase the enhancement of the network by connecting two ISPs' through routers, PCs. Here we selected ISP1 as primary cloud environment, which means ISP1 will always be selected for data transferring. If ISP1 is failed or shutdown, then ISP2 will work as a secondary cloud environment. Overall, the project of enhancing network resilience with three routers and two ISPs is crucial for organizations that require uninterrupted connectivity, efficient routing, and resilience against network failures.

By implementing redundancy mechanisms, load balancing techniques, efficient routing protocols, and monitoring practices, organizations can achieve a highly available and resilient network infrastructure. It aimed at designing and implementing a robust and highly available network infrastructure. This project addresses the need for uninterrupted connectivity, efficient routing, and redundancy in the face of router or ISP failures.

8. Future Work:

Performance Optimization: As the project progresses, future work can focus on optimizing the performance of the ISP cloud environment. This can involve fine-tuning routing protocols, adjusting network configurations, and implementing load balancing techniques to ensure efficient data transmission, minimize latency, and enhance overall network performance.

Network Security Enhancements: In the future, further emphasis can be placed on enhancing network security within the ISP cloud environment. This may include implementing advanced firewall rules, intrusion detection and prevention systems, and encryption mechanisms to protect against potential threats and ensure the confidentiality and integrity of data transmitted across the network.

Scalability and Expansion: As network requirements grow or change, future work can focus on designing and implementing mechanisms to scale the ISP cloud infrastructure. This can involve introducing additional routers, expanding network segments, and integrating new services or technologies to accommodate increased network demands and facilitate future expansion.

Network Monitoring and Management: Implementing robust network monitoring and management solutions can be a focus of future work. This can involve deploying network monitoring tools to collect and analyze network performance data, implementing proactive monitoring for detecting and addressing network issues, and integrating network management systems for centralized control and configuration management.

High Availability and Redundancy: Future work can also focus on enhancing the reliability and availability of the ISP cloud environment. This may include implementing redundancy mechanisms such as link aggregation, deploying backup routers, or utilizing protocols like Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP) to ensure seamless failover and uninterrupted network connectivity.

Integration with Cloud Services: As cloud computing continues to evolve, future work can explore the integration of the ISP cloud environment with cloud services and platforms. This may involve connecting the ISP cloud infrastructure to public or private cloud environments, implementing hybrid cloud architectures, or leveraging cloud-based networking technologies to enhance the scalability, flexibility, and resource utilization of the network.

Overall, future work in the project can encompass various aspects, including performance optimization, network security enhancements, scalability and expansion, network monitoring and management, high availability and redundancy, and integration with cloud services. These areas of focus will contribute to the continuous improvement and evolution of the ISP cloud environment, meeting the ever-growing demands of modern networking scenarios.

9. Conclusions:

In conclusion, our project focused on designing and implementing an efficient network infrastructure within an ISP cloud environment. Through the implementation of various components, such as IPv4 subnetting, routing protocols, and configuration of routers and PCs, we aimed to achieve optimal IP address utilization, secure communication, and seamless connectivity.

During the project, we conducted a literature review to gather insights on campus networks, IPv4 subnetting, GNS3 simulation tool, routing protocols, and Cisco images. This review helped us understand best practices and techniques relevant to our project.

We successfully implemented the project by following the defined designs and configurations. We installed GNS3, imported the necessary routers, and performed the required configurations, including network addressing, routing protocols, and connectivity settings. Through these steps, we established a functioning ISP cloud environment that supports efficient data transmission and interconnectivity between multiple networks.

Future work can focus on further optimizing the performance of the ISP cloud environment, enhancing network security measures, ensuring scalability and expansion capabilities, implementing robust network monitoring and management solutions, establishing high availability and redundancy, and exploring integration with cloud services.

Overall, the project provided valuable hands-on experience in designing and implementing network infrastructures and addressing the challenges specific to an ISP cloud environment. The knowledge gained through this project can be applied to real-world scenarios, contributing to the efficient and secure functioning of network infrastructures within ISP cloud environments.

10. References:

Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Pearson Education.

Forouzan, B. A. (2013). Data Communications and Networking (5th ed.). McGraw-Hill Education.

https://gns3.com/trying-to-connect-my-gns3-network-to-the-interface-but-my-router-cant-ping-its-default-gateway