*DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING*

**SCHOOL OF COMPUTING**

# SATHYABAMA

*INSTITUTE OF SCIENCE AND TECHNOLOGY*

**(DEEMED TO BE UNIVERSITY)**
**CATEGORY - 1 UNIVERSITY BY**
**UGC**
**Accredited "A++" by NAAC I Approved by AICTE**
**JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600119**

## Cisco AICTE Virtual Internship Program 2025

A Cisco AICTE Virtual Internship project report on networking submitted in partial fulfillment of the requirements for the AICTE-CISCO virtual Internship in networking Program 2025

Submitted By : Bharat P

| | | |
|---|---|---|
| **AICTE Internship Student Registration ID)** | **:** | STU662ce37781d091714217847 |
| **Student ID (Enrolment number)** | **:** | 43111298 |
| **Email** | **:** | btbharat005@gmail.com |
| **Contact Info** | **:** | +91 8610606589 |

# Automatic Network Topology Generation, Validation, and Simulation from Router Configuration Files

### *Introduction*

This project addresses a vital requirement in network management: automating the creation of hierarchical network topology directly from router and switch configuration files. It helps visualize how devices connect, validates configurations for errors, simulates network traffic and faults, and generates comprehensive reports. The solution aids network administrators, enhances understanding, and fixes network design and operational inefficiencies early

### *Problem Statement:*

Currently, there is no existing solution that can automatically generate a hierarchical network topology from individual router configuration files. The generated topology needs to include bandwidth awareness and traffic load management. The tool should detect configuration issues such as duplicate IPs, incorrect VLANs, gateways, MTU mismatches, network loops, and missing network components, and provide recommendations for optimization. Additionally, it should simulate day-1 scenarios and network fault conditions to evaluate network resilience and performance.

### *Objectives*

- Parse and extract network device configurations automatically.
- Construct a hierarchical, bandwidth-aware network topology graph.
- Validate device and link configurations, detecting missing devices, inconsistent VLANs, duplicated IPs, and gateway misassignments.
- Simulate normal traffic paths and network failure scenarios to assess resilience.
- Generate machine-readable and human-readable reports including network diagrams and validation issue logs.

### *Tools and Technologies*

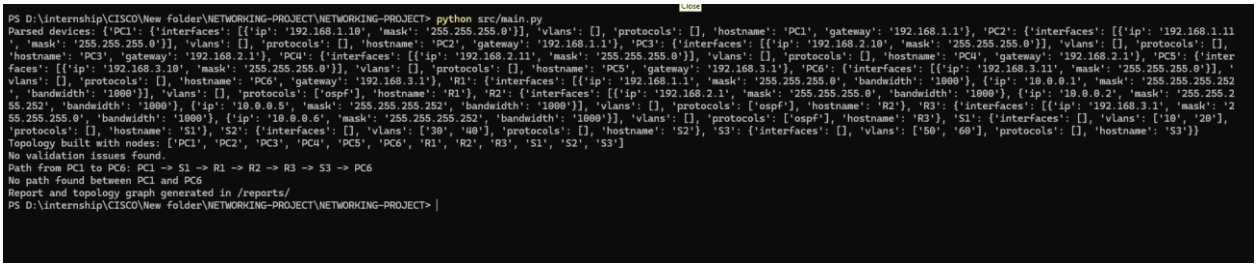
- Python programming language.
- NetworkX library for graph and network topology modeling.
- Matplotlib for visualization of network diagrams.
- JSON for structured report generation.
- Cisco Packet Tracer for conceptual network mapping and security simulations.

## *Methodology*

### 1. Configuration Parsing:

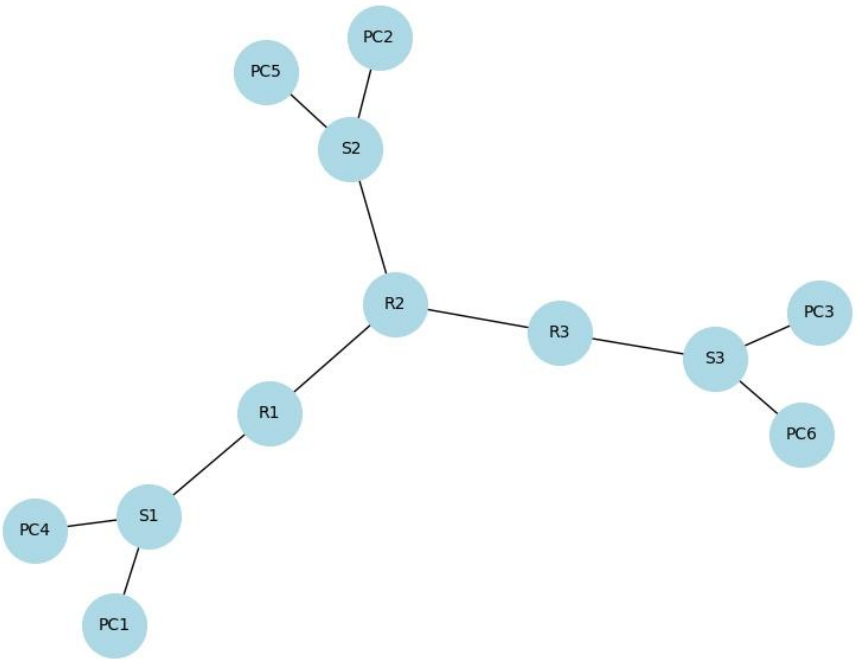
- The first step involved parsing the network device configuration files to extract critical information such as hostnames, interface IP addresses, subnet masks, VLAN assignments, routing protocols, and default gateways. This automated parsing was performed using a custom Python script.

- The following output shows the parsed device details printed in the console after executing the parsing routine. It confirms successful extraction of all relevant device parameters for routers, switches, and PCs.




### 2. Topology Construction Visualization:

- Using the extracted configuration data, a hierarchical network graph was constructed programmatically. Routers are linked sequentially to form the backbone, with switches connecting to routers and PCs attached to switches according to VLAN and subnet data.
- The generated topology graph below visually represents all nodes—including PCs, switches, and routers—and their interconnections. This head-start visual aids in verifying the network structure complies with expected design.



3. **Validation:**

    - The network configuration underwent automated validation to check for common issues such as duplicate IP addresses and missing gateways. The validation output confirmed no conflicts or missing configurations were present, indicating sound network design and configuration consistency.

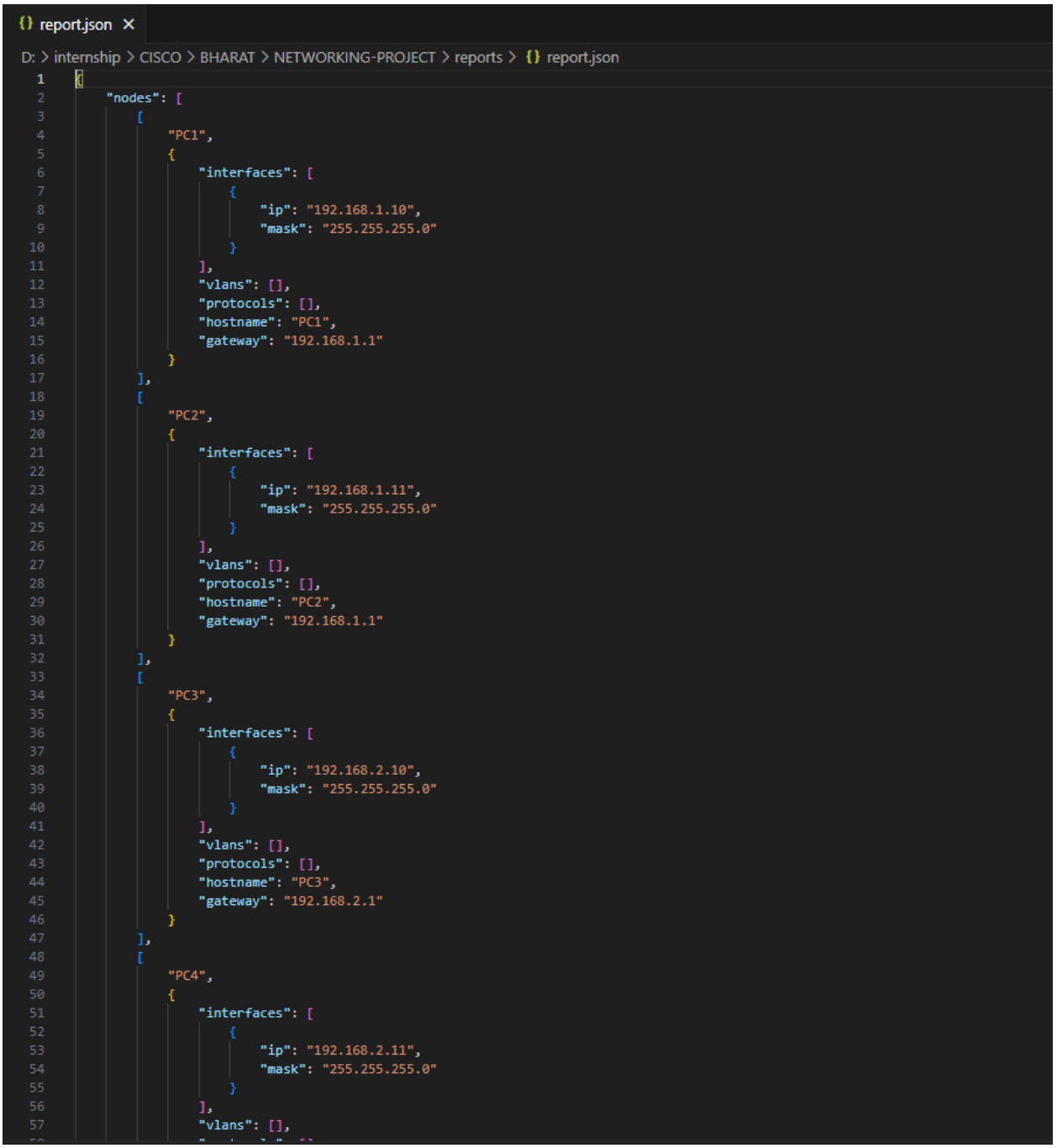
4. **Simulation of Network Paths and Faults:**

    - Network simulations were executed to identify shortest communication paths between endpoint devices. The simulation effectively revealed the established routing paths between PCs and demonstrated the impact of a node failure on connectivity.
    - By simulating router failures, we observed the resulting loss of connection between certain endpoints, highlighting critical nodes whose failure causes network partitioning.

5. **Reporting:**

    - Finally, the project produced structured JSON reports documenting the network graph's nodes, edges, and validation results. Alongside, topology visualizations were saved as image files to facilitate documentation and presentation.

    - These deliverables provide both machine-readable and graphical insights into the network's topology and health.


report.json
D: > internship > CISCO > BHARAT > NETWORKING-PROJECT > reports > report.json
{
"nodes": [
[
"PC1",
{
"interfaces": [
{
"ip": "192.168.1.10",
"mask": "255.255.255.0"
}
],
"vlans": [],
"protocols": [],
"hostname": "PC1",
"gateway": "192.168.1.1"
}
],
[
"PC2",
{
"interfaces": [
{
"ip": "192.168.1.11",
"mask": "255.255.255.0"
}
],
"vlans": [],
"protocols": [],
"hostname": "PC2",
"gateway": "192.168.1.1"
}
],
[
"PC3",
{
"interfaces": [
{
"ip": "192.168.2.10",
"mask": "255.255.255.0"
}
],
"vlans": [],
"protocols": [],
"hostname": "PC3",
"gateway": "192.168.2.1"
}
],
[
"PC4",
{
"interfaces": [
{
"ip": "192.168.2.11",
"mask": "255.255.255.0"
}
],
"vlans": [],

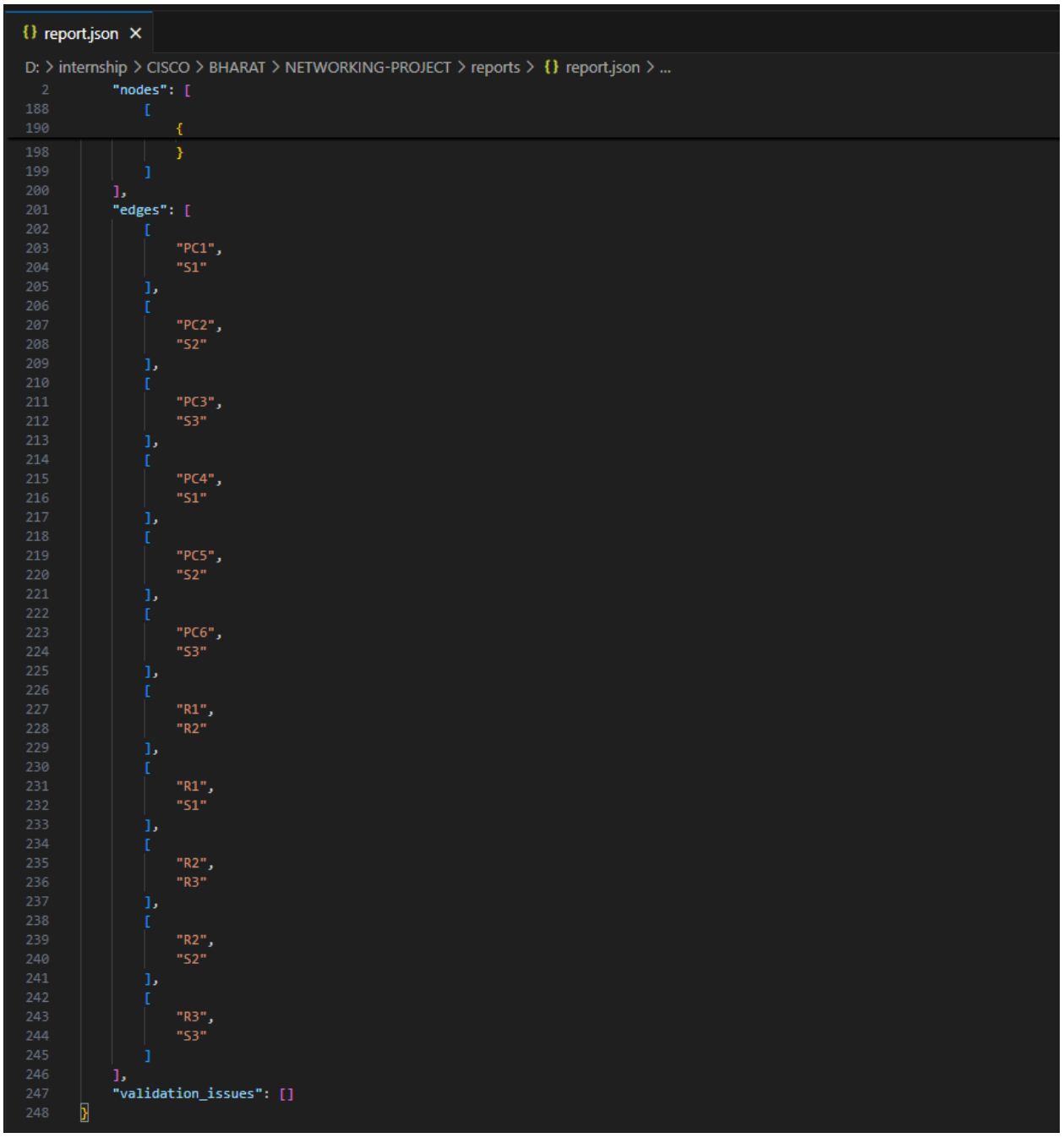

report.json
D: > internship > CISCO > BHARAT > NETWORKING-PROJECT > reports > report.json > ...
"nodes": [
[
{
"interfaces": [
}
],
"vlans": [],
"protocols": [],
"hostname": "PC4",
"gateway": "192.168.2.1"
}
],
[
"PC5",
{
"interfaces": [
{
"ip": "192.168.3.10",
"mask": "255.255.255.0"
}
],
"vlans": [],
"protocols": [],
"hostname": "PC5",
"gateway": "192.168.3.1"
}
],
[
"PC6",
{
"interfaces": [
{
"ip": "192.168.3.11",
"mask": "255.255.255.0"
}
],
"vlans": [],
"protocols": [],
"hostname": "PC6",
"gateway": "192.168.3.1"
}
],
[
"R1",
{
"interfaces": [
{
"ip": "192.168.1.1",
"mask": "255.255.255.0",
"bandwidth": "1000"
},
{
"ip": "10.0.0.1",
"mask": "255.255.255.252",
"bandwidth": "1000"
}
],

report.json

D: > internship > CISCO > BHARAT > NETWORKING-PROJECT > reports > report.json > ...


```
    "nodes": [
        [
            {
                "interfaces": [
                    {
                    }
                ],
                "vlans": [],
                "protocols": [
                    "ospf"
                ],
                "hostname": "R1"
            }
        ],
        [
            "R2",
            {
                "interfaces": [
                    {
                        "ip": "192.168.2.1",
                        "mask": "255.255.255.0",
                        "bandwidth": "1000"
                    },
                    {
                        "ip": "10.0.0.2",
                        "mask": "255.255.255.252",
                        "bandwidth": "1000"
                    },
                    {
                        "ip": "10.0.0.5",
                        "mask": "255.255.255.252",
                        "bandwidth": "1000"
                    }
                ],
                "vlans": [],
                "protocols": [
                    "ospf"
                ],
                "hostname": "R2"
            }
        ],
        [
            "R3",
            {
                "interfaces": [
                    {
                        "ip": "192.168.3.1",
                        "mask": "255.255.255.0",
                        "bandwidth": "1000"
                    },
                    {
                        "ip": "10.0.0.6",
                        "mask": "255.255.255.252",
                        "bandwidth": "1000"
                    }
                ],
                "vlans": [],
```


report.json
D: > internship > CISCO > BHARAT > NETWORKING-PROJECT > reports > report.json > ...
"nodes": [
[
{
"interfaces": [
}
],
"vlans": [],
"protocols": [
"ospf"
],
"hostname": "R3"
}
],
[
"S1",
{
"interfaces": [],
"vlans": [
"10",
"20"
],
"protocols": [],
"hostname": "S1"
}
],
[
"S2",
{
"interfaces": [],
"vlans": [
"30",
"40"
],
"protocols": [],
"hostname": "S2"
}
],
[
"S3",
{
"interfaces": [],
"vlans": [
"50",
"60"
],
"protocols": [],
"hostname": "S3"
}
]
],
"edges": [
[
"PC1",
"S1"
],
[
"PC2",




### *Results and Discussion*

- Automated parsing successfully extracted all network device info.
- Generated topology matches expected physical and logical network layout.
- Validation confirmed no addressing or gateway conflicts.
- Simulation highlighted correct routing paths and clearly showed network partitions on failure.
- Reports comprehensively documented topology and validation findings with visual support.

### *Tools and Technologies Used*

- Python (for config parsing, topology building, simulation, validation, report generation)
- NetworkX (graph building and network simulation)
- Matplotlib (graph visualization)
- Cisco Packet Tracer (network topology mapping and cybersecurity simulation)
- JSON (report formatting)

## *Future Enhancements*

- Extend protocol support beyond OSPF to BGP and others, with optimization suggestions.
- Detailed traffic modeling with link utilization and QoS considerations.
- Real IP packet simulation and multithreaded packet processing for more realistic network behavior.
- Integration of advanced network security analytics and automated remediation.
- Expanded fault injection scenarios allowing more granular network failure tests.

## *Conclusion*

This project demonstrates an automated solution to parse router configurations, generate hierarchical network topology, validate network consistency, and simulate network functionality under normal and failure conditions. Coupled with cybersecurity mappings and cloud infrastructure redesign recommendations, it forms a well-rounded approach to modern network management and resilience.