**T301 Network Design**

**Due Date**

Final Assignment:  
  
  
Infrastructure Change:

**Weighting**

45%

**Submission Method**

A **private** GitHub repository displaying progress and an exported zip file uploaded to Moodle.  
Presentation uploaded to SharePoint.

**Conditions**

This assignment is to be completed individually.

**Faculty**

Humanities and Business

**Programme**

Bachelor of Information and Communications Technology

Graduate Diploma of Information and Communications Technology

**Learning Outcomes Assessed**

1. Assess and recommend appropriate network hardware and configuration/s for given scenario/s
2. Assess, evaluate and recommend the deployment of virtualisation/cloud/containerised infrastructure
3. Assess and respond to infrastructure requirement change/s
4. Implement network/virtualisation/cloud/containerised infrastructure for given scenario/s

**Lecturer**

**Moderator**

## Aim of the Assessment

To assess your ability to: Assess a given set of requirements then research and implement appropriate Ansible configuration to provision a network as described.

/opt/unetlab/wrappers/unl\_wrapper -a fixpermissions

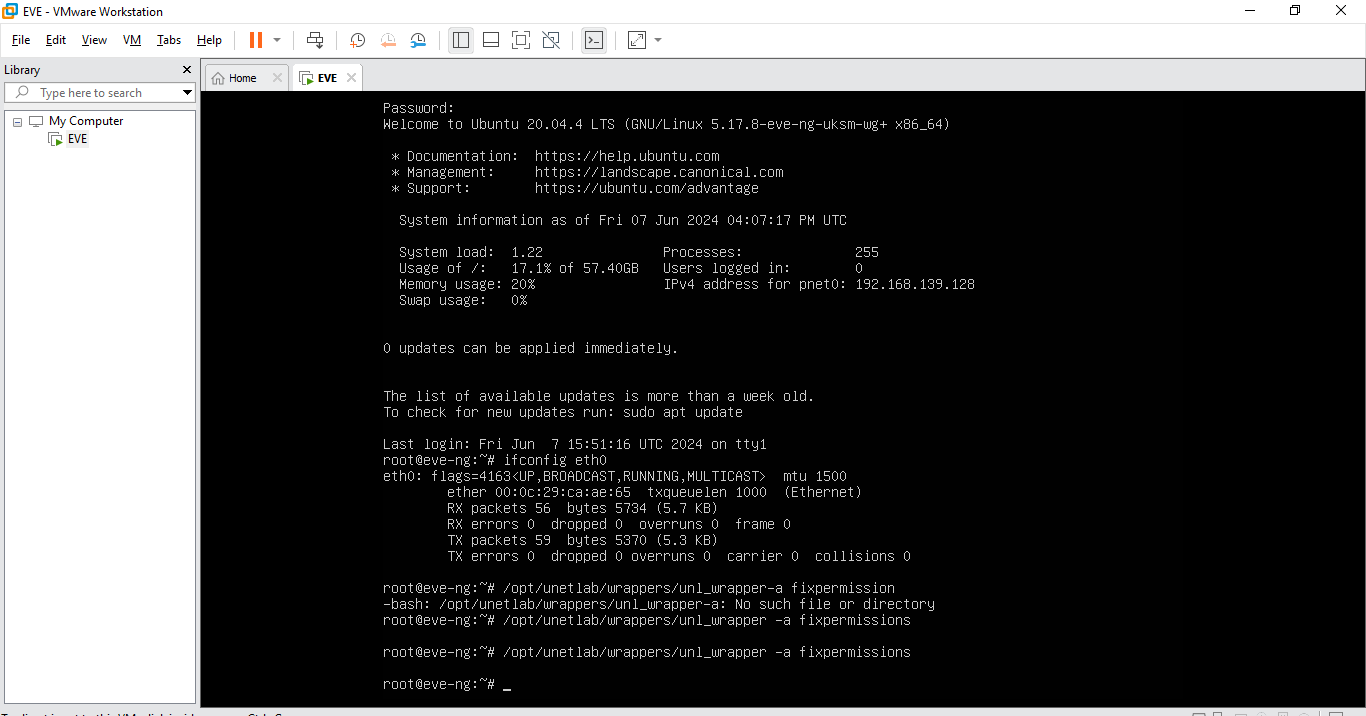
## Requirement Descriptions

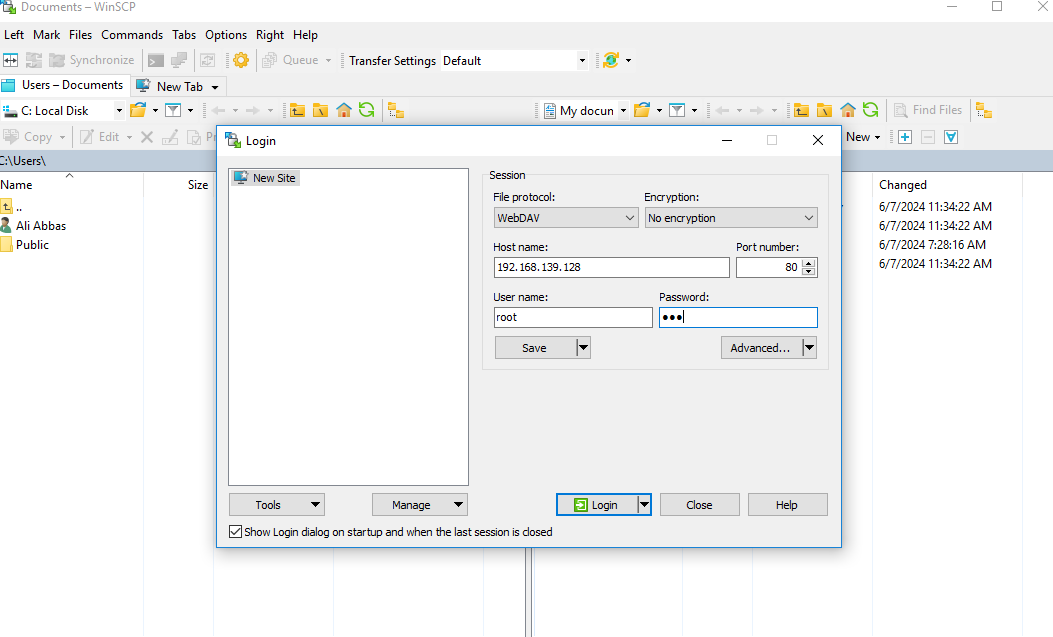
Following your recent work, the radio society would like to look at expanding the capabilities for part of the network infrastructure.

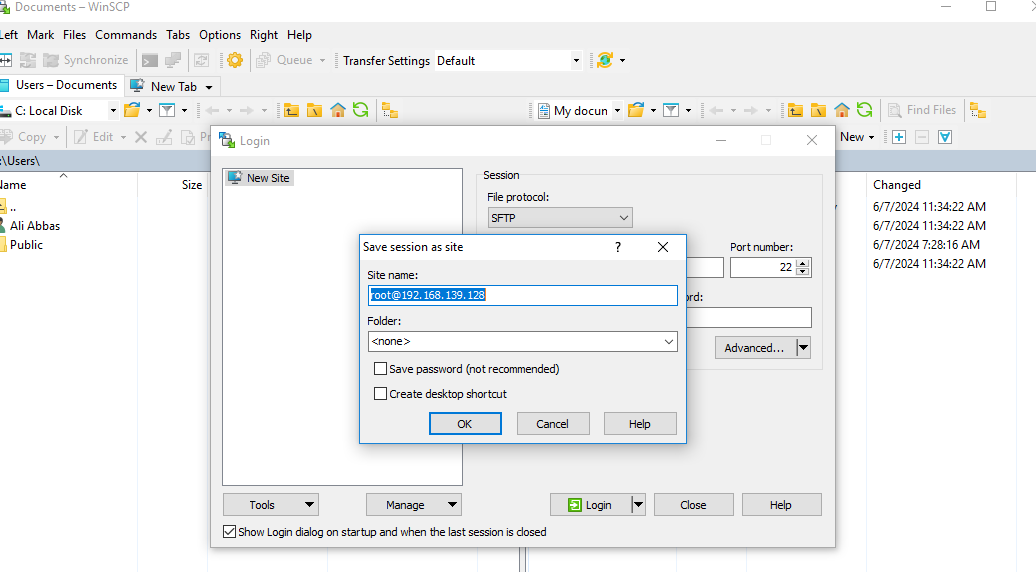
1. General Requirements:
   1. You are requested to provide a proof of concept that meets this specification document’s requirements; the use of EVE-ng is recommended.

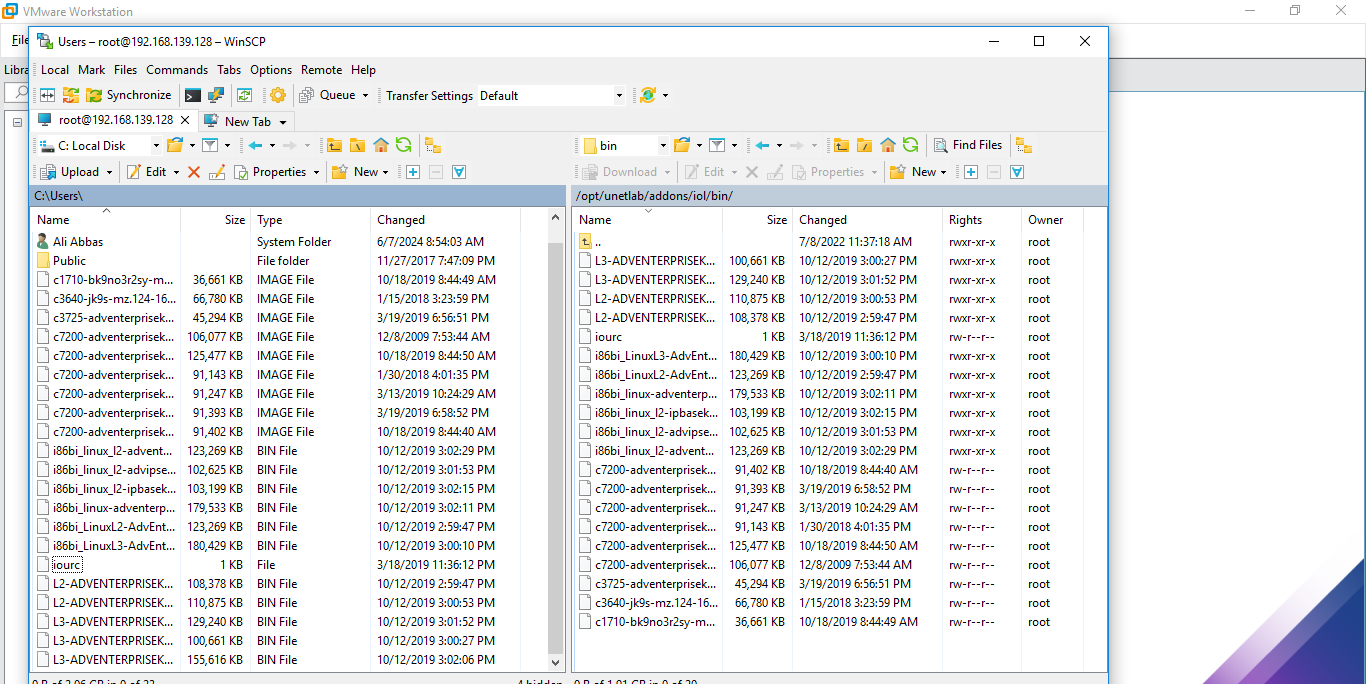
\*Solution

We download EVE-NG OVF file and installed as a virtual machine by dedicated physical server with virtualization software is recommended, as layered virtualization is inefficient. We must use EVE management interface on laptops by use the NAT adapter option which linked to a different SSID. We connecting a NAT adapter to avoid IP changes in the EVE administration interface. The server's use EVE HDD configured thick suggested. This must use hard drive after installation. This deployments involving bare metal as highly recommended static IP address to proceed for configuration. We must use laboratories which allows users to create, delete, and modify files and nodes. We must recommended license operations as Eve Web GUI, to login as the Administrator. We must Unchecked CPU Limit option which allows node to boot CPU, templates typically setup CPU limit.



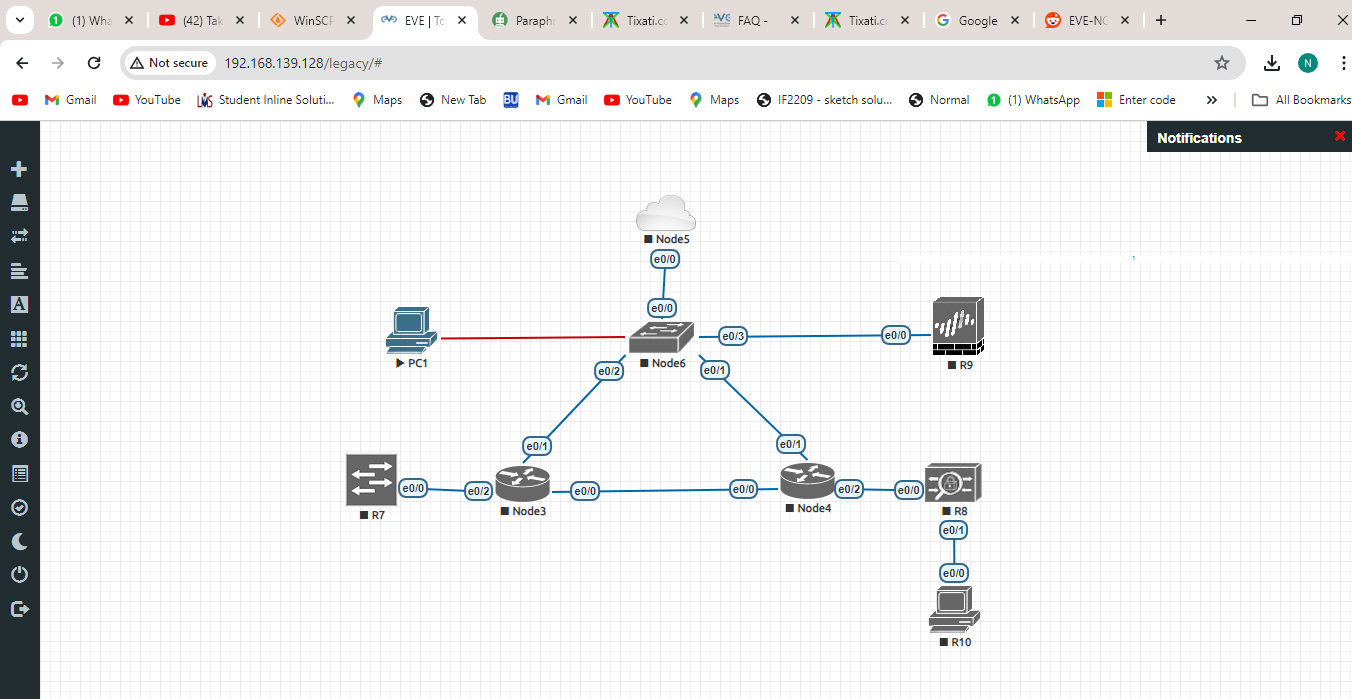






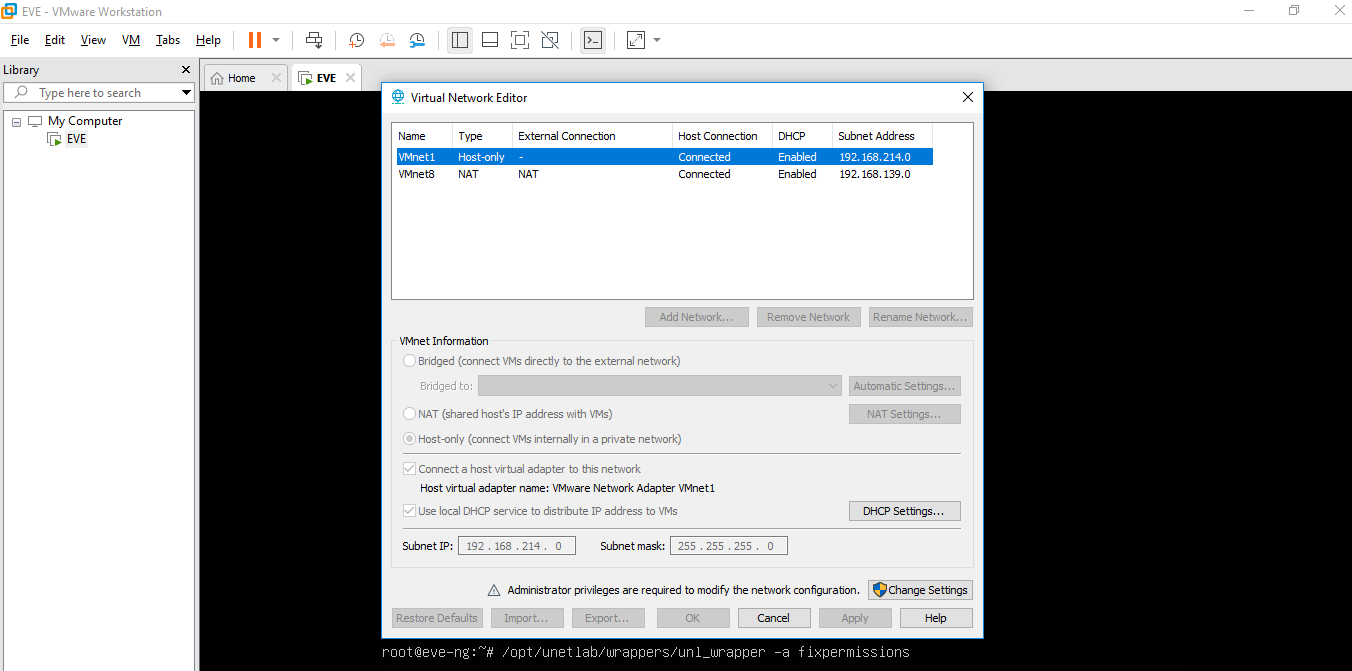
* 1. Your proof of concept should have the following base structure, you are free to provide any recommendation for the blue section of the following diagram:

\*Solution



* 1. **Your implementation must be completed using Ansible**, (you may manually design and connect machines in the eve-ng interface, however all configuration must be implemented using Ansible).

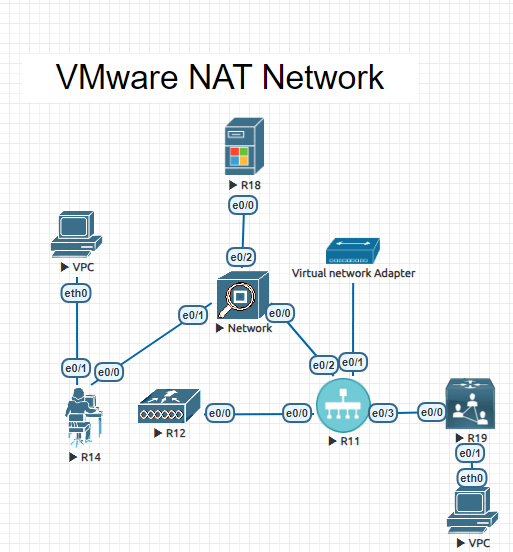
\*Solution



* 1. In this assignment, the VMware NAT network is to be considered as part of the Internet. Anytime you wish to connect devices to the Internet, connect them to the VMware NAT network.

\*Solution

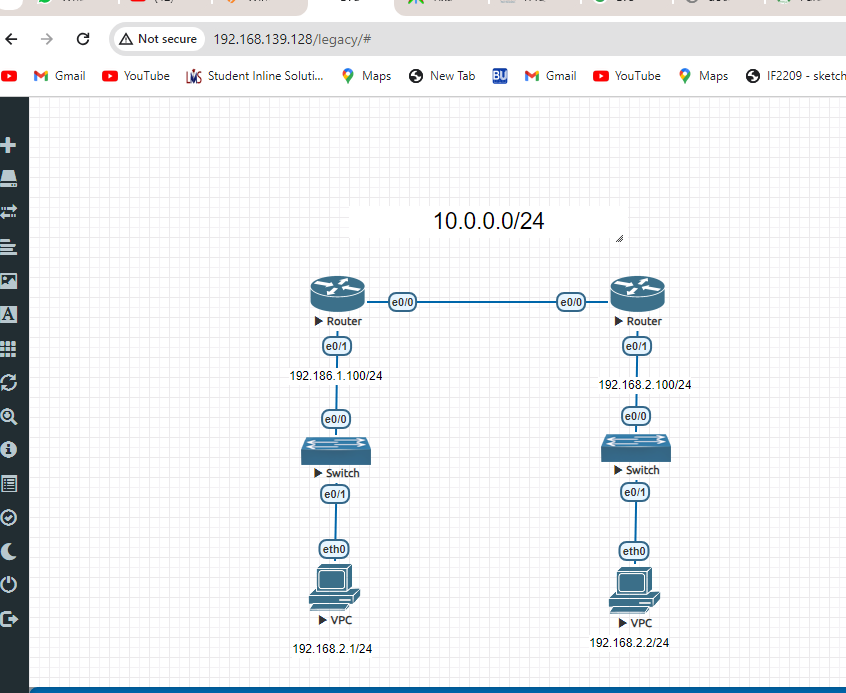
The EVE VMware NAT network templates recommended CPU limit settings set to boot CPU which can uncheck the CPU Limit option. The virtual machine share a hidden network identity, making it invisible to the outside world by using network address translation to tricking network resources into host system. This facilitates data transfer between the two networks. The NAT device must forward the request in order to establish a connection to a server with a source port lower than 1024. For security considerations, some servers do accept connections from source ports lower than 1024. The NAT configuration file contains parameters that regulate the source and destination ports of virtual machines.

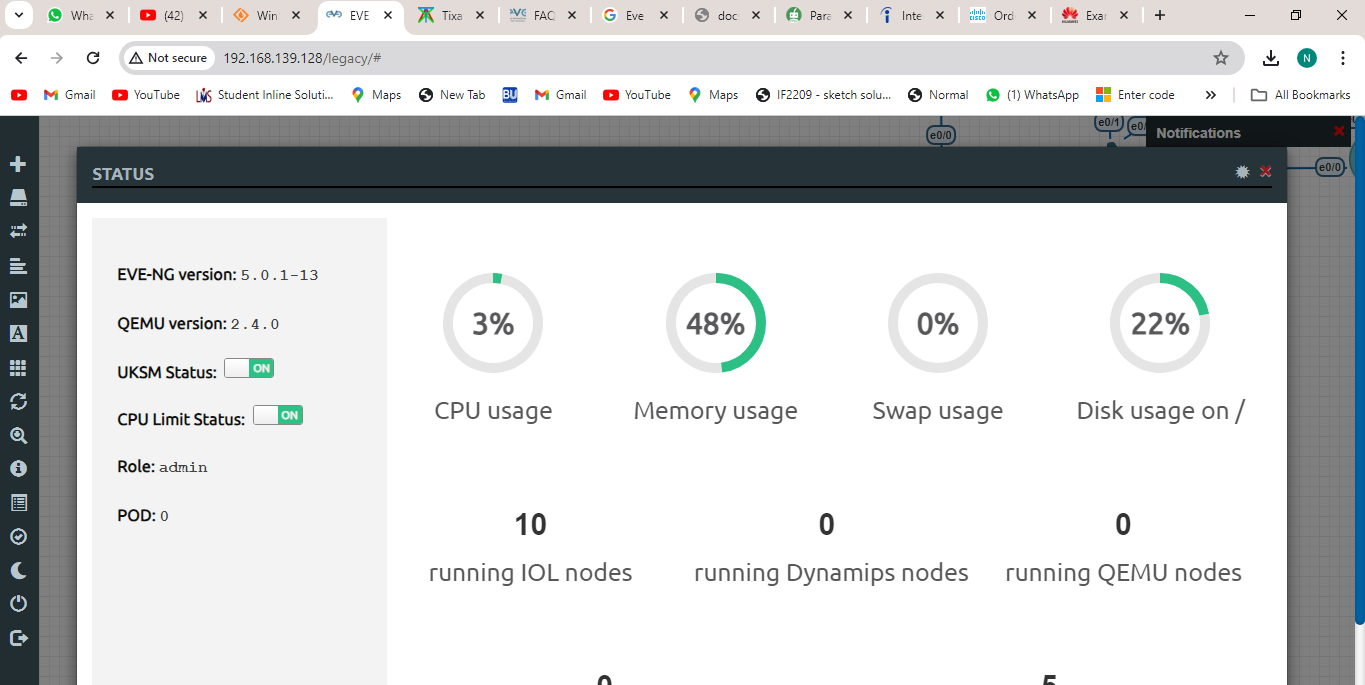


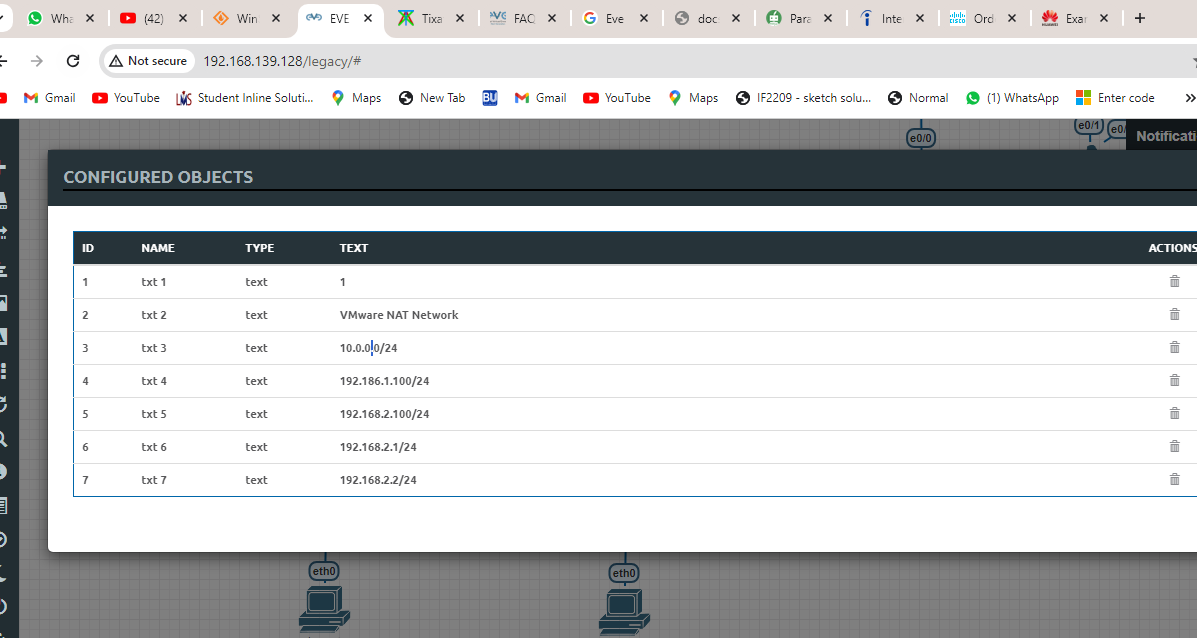
1. Technical Requirements:
   1. External Client/s:
      1. Manually set static routes in your client device/s so they can reach your internal 44 network.

\*Solution

The administrators manually configure static routes for simple networks these routes consume less CPU and bandwidth. They are capable of enhancing the performance of complicated networks and five parameters. The device static route configured peer device which have needs to return route configured in order to enable bidirectional communication. All versions of the S600-E can equal-cost static routes which load balancing and non-equal-cost routes configured for active



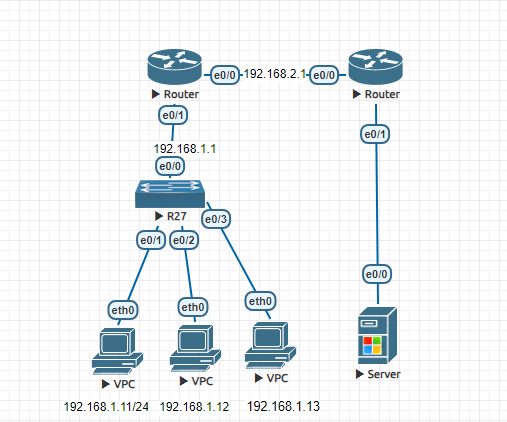


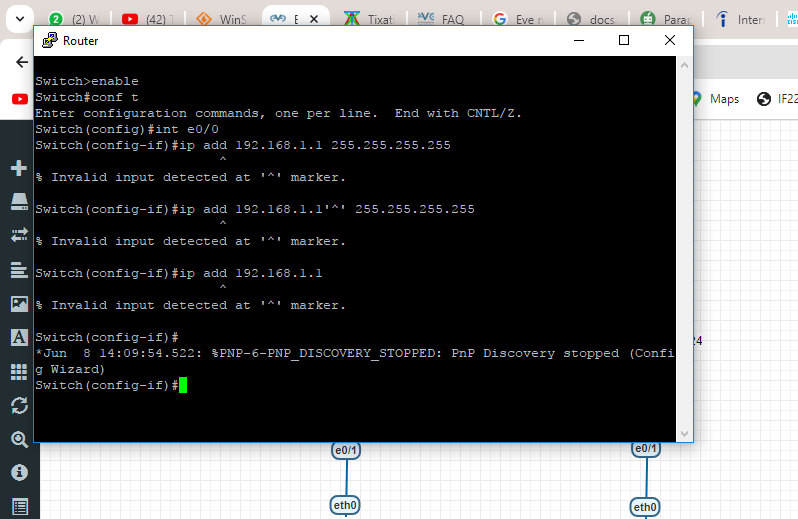


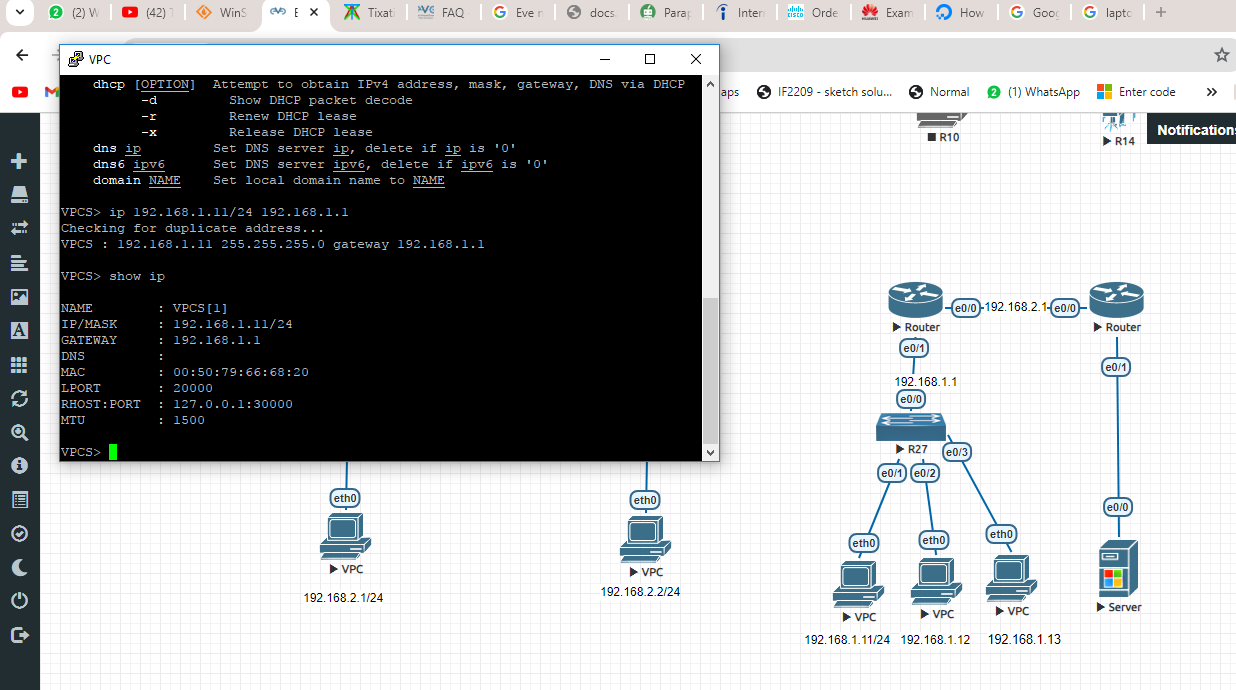
* + 1. Manually configure your clients DNS server/s to point to your Bind DNS server/s.

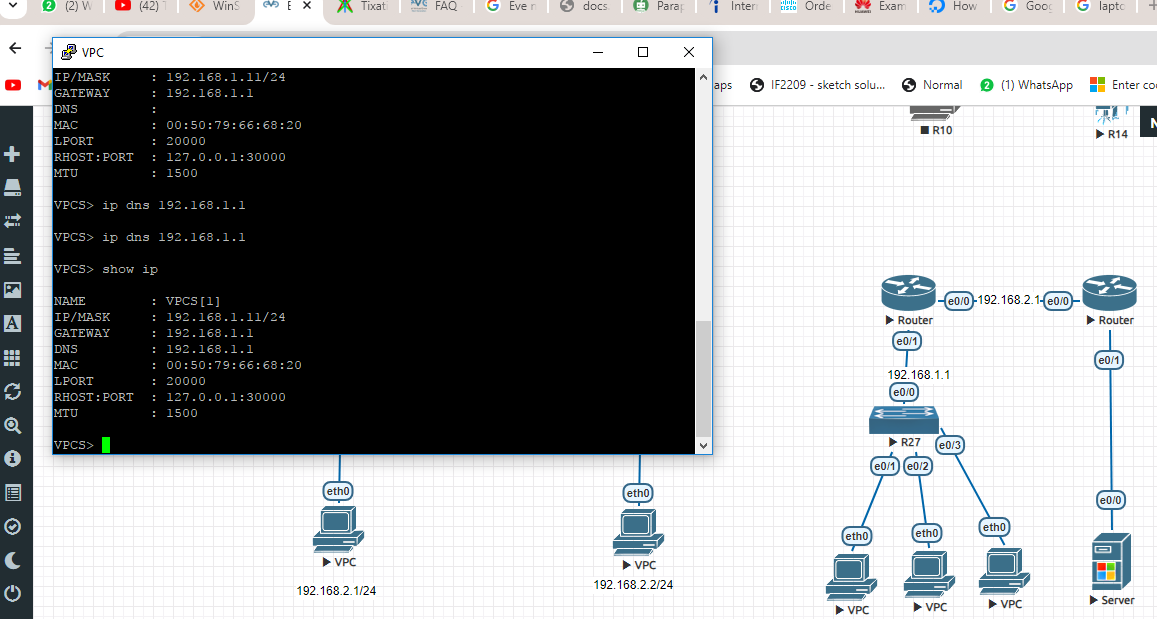
\*Solution

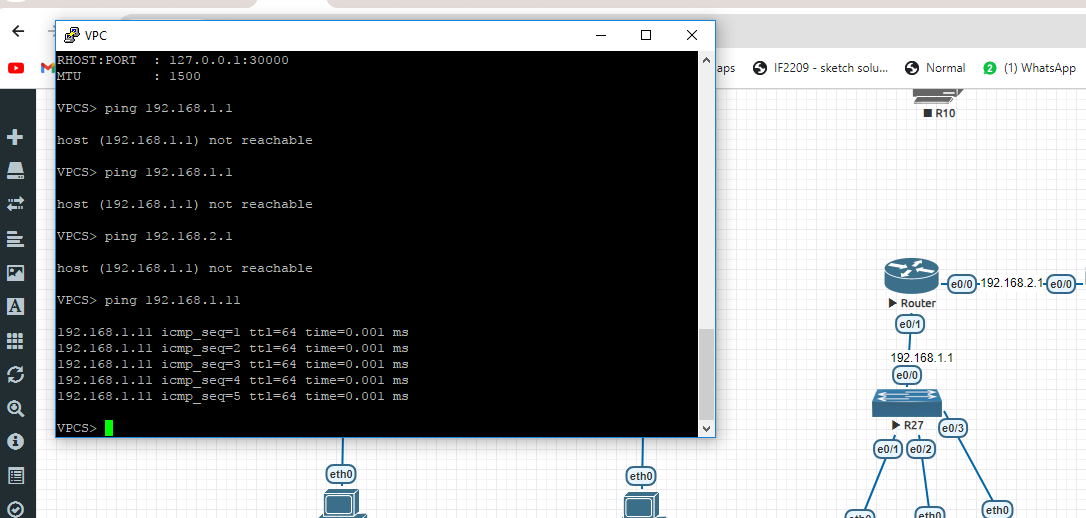
We set up a Router's DNS server access websites on the Internet and the local file server, workstations will be set up to use the eve ng Router DNS Services as follow

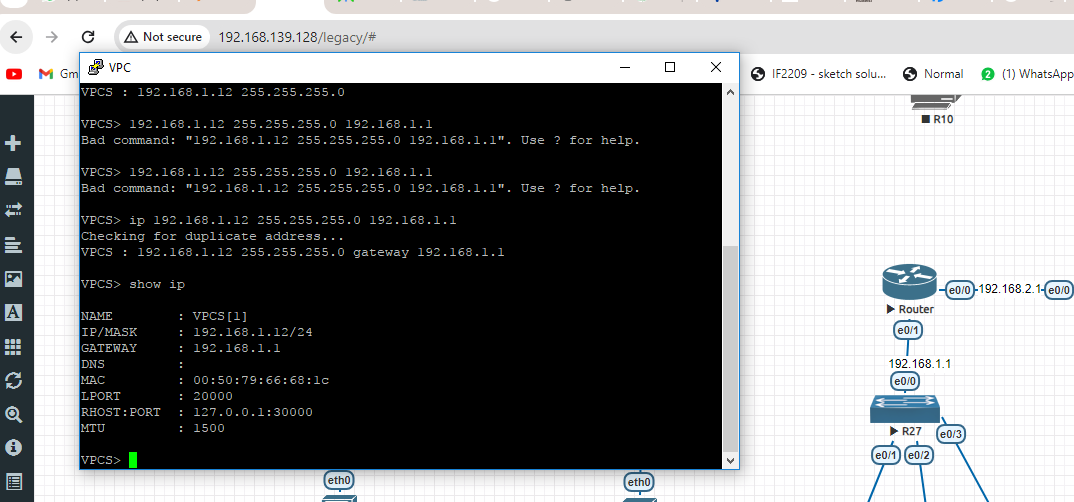


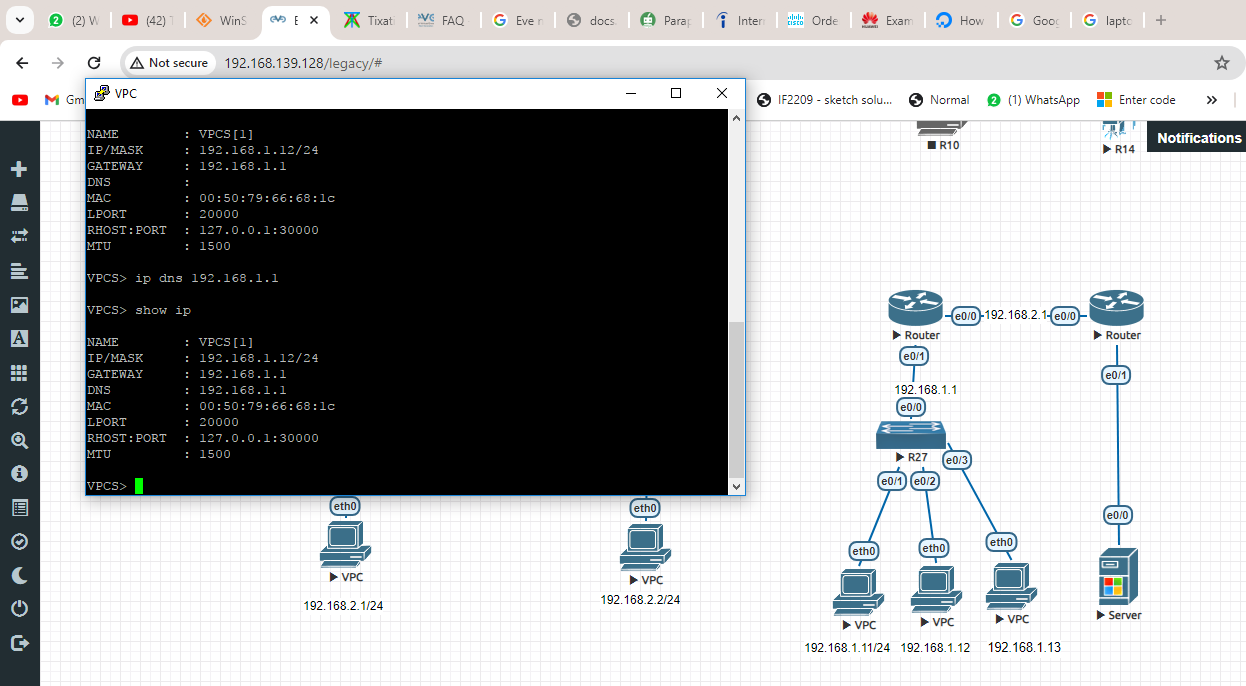


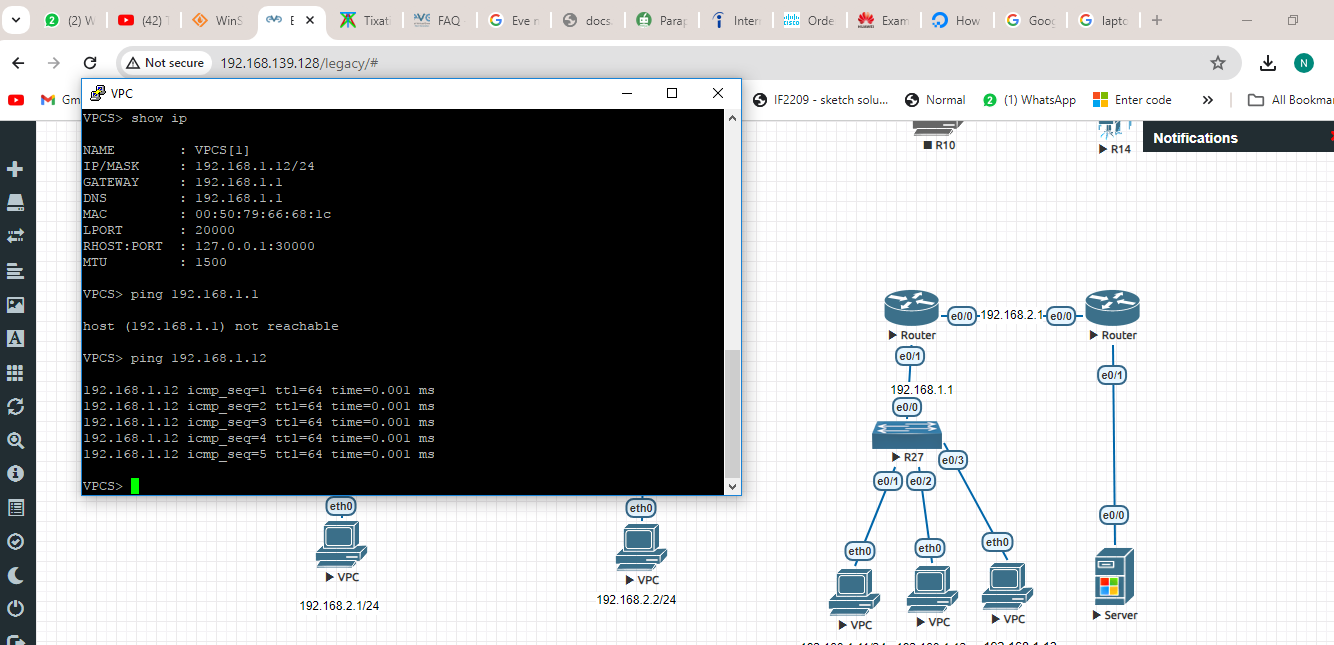






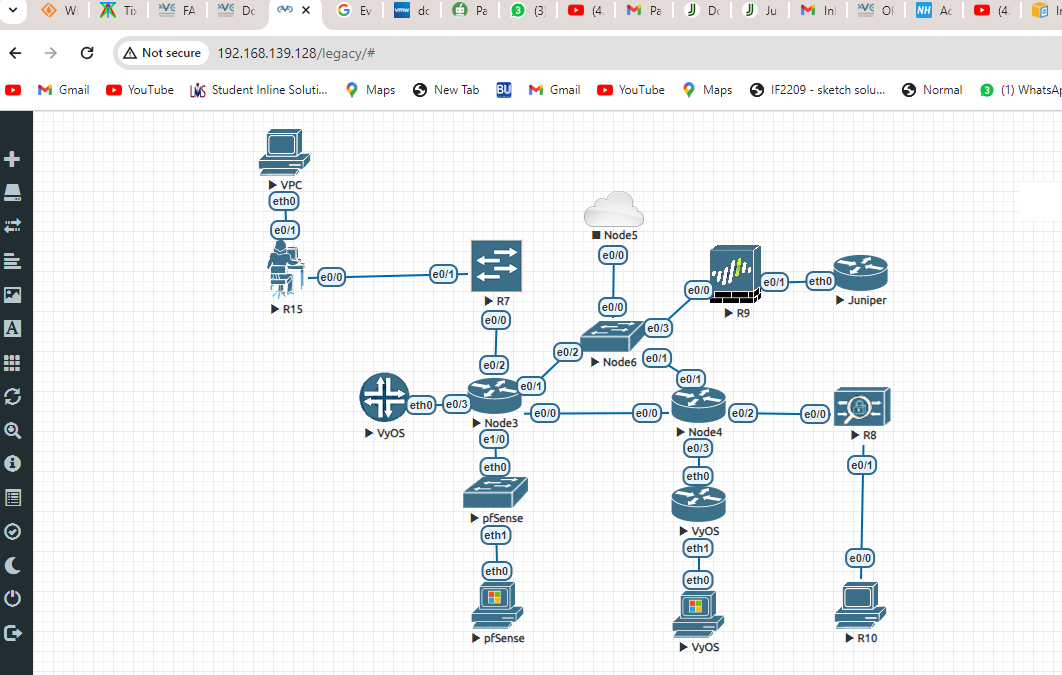






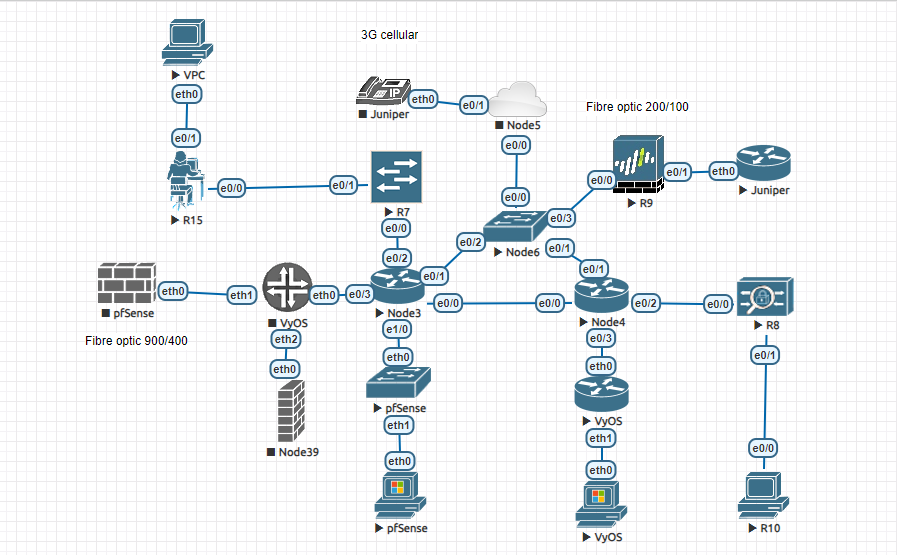
* 1. Network:
     1. Recommend and implement an internal network design that ensures resilient operation, you may use any available network infrastructure image available to you, e.g. (VyOS, Juniper, Cisco, , etc.).

\*Solution



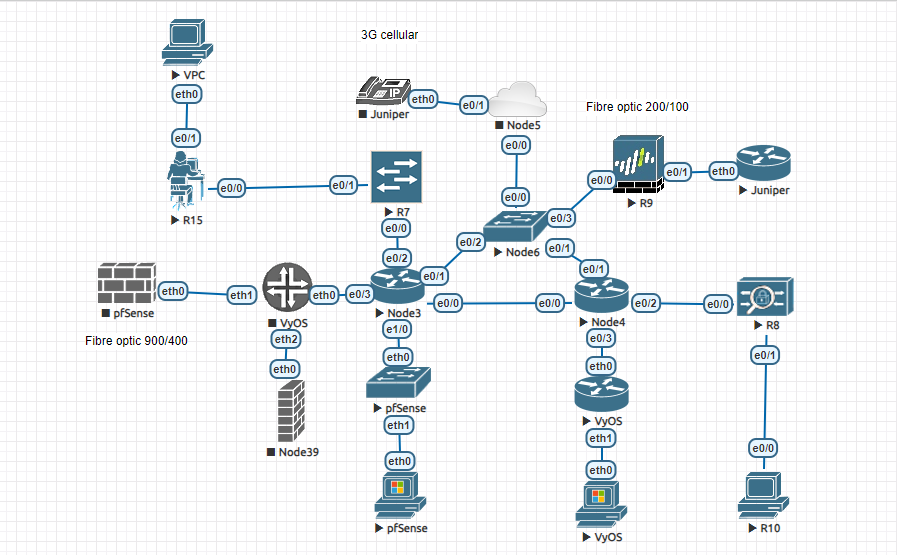
* + 1. Implement multiple Internet gateways to simulate the following internet connections, ensure you specify suitable bandwidth and latency characteristics:
       1. Fibre optic 900/400
       2. Fibre optic 200/100
       3. 3G cellular

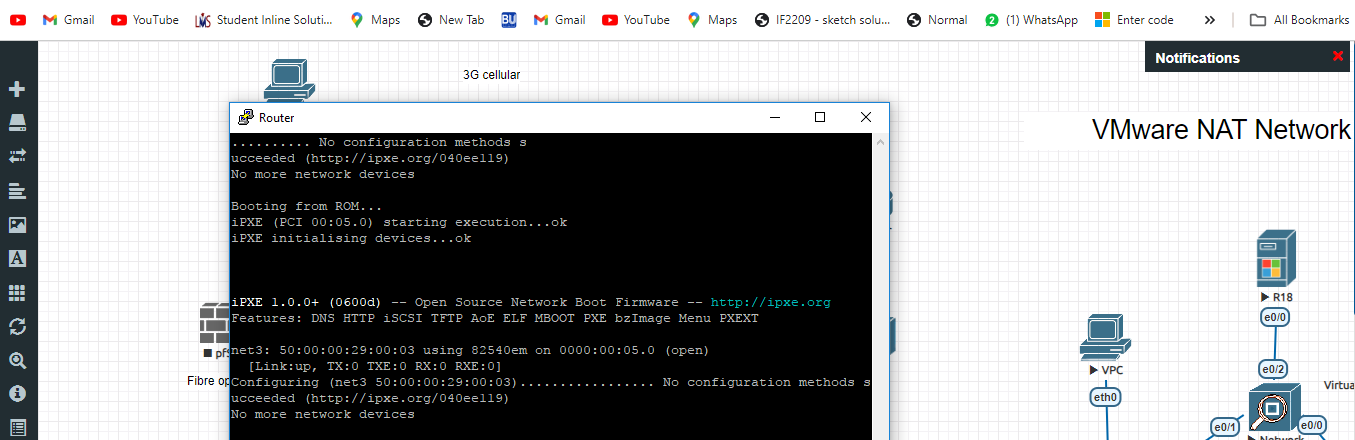
\*Solution



* + 1. Implement a routing solution to use the optimum internet connection.

\*Solution

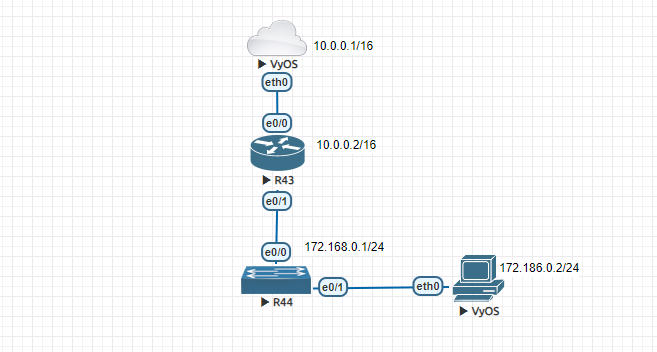
The author connect to a router using a host machine and pnet0, but the interface receives an identical DHCP address as a router which released address, but eve-ng acts as a barrier, preventing ping requests either device disabling eve-ng succeeded. 

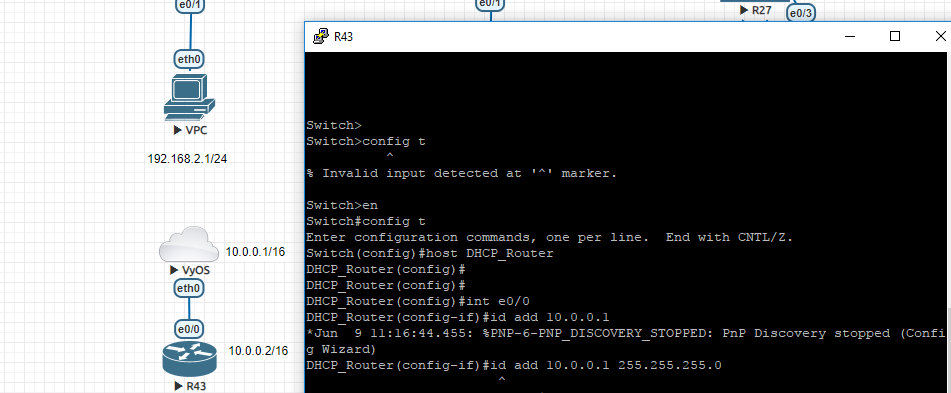


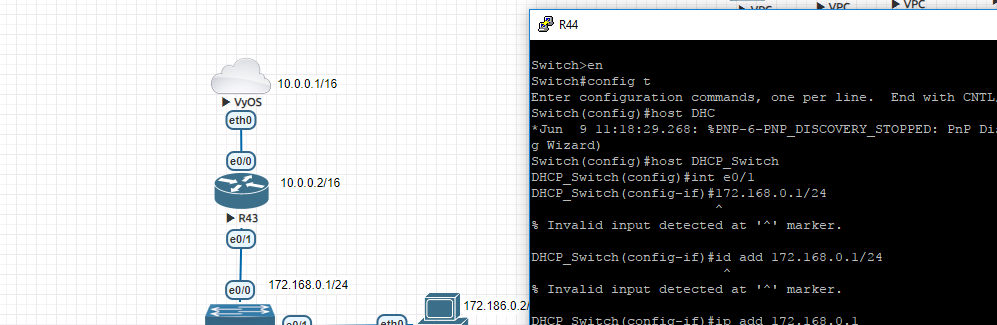
* 1. Firewalls:
     1. Configure host based firewalls within each device on your network
        1. Ensure that only permitted traffic (only the services identified within these specifications) is allowed

\*Solution

The With NAT configured and pnet1 set to 10.0.0.1/16, the user simulates a basic network in VMWare Workstation Pro using EVE-NG. We want to know if there's a way to block their personal network devices in the lab connect to the internet.

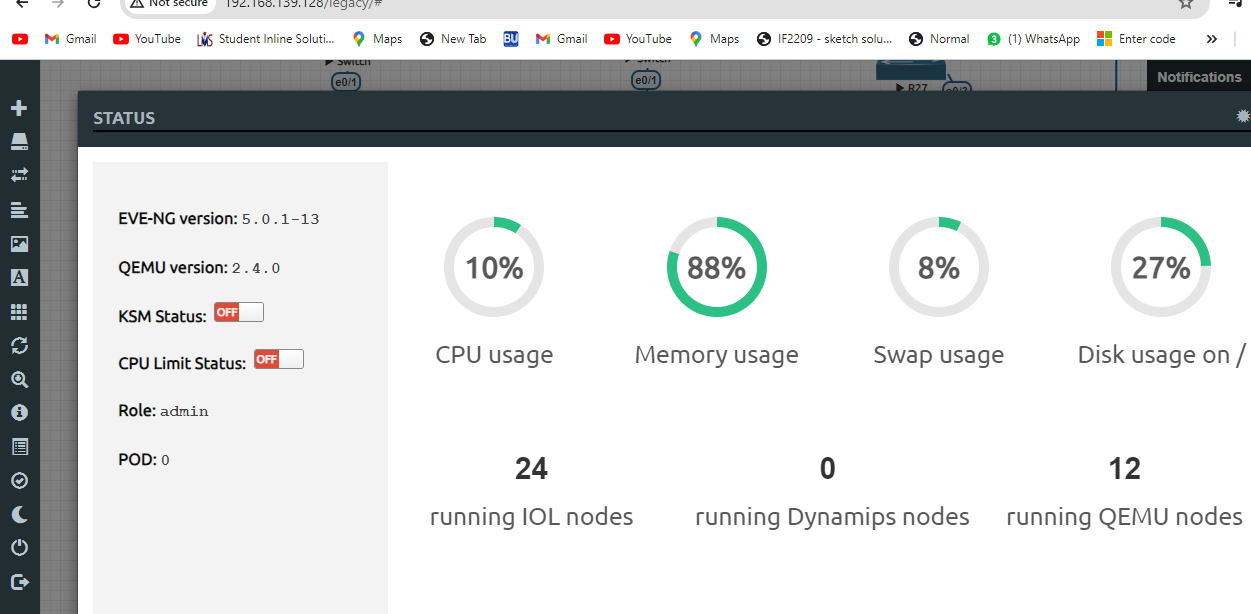




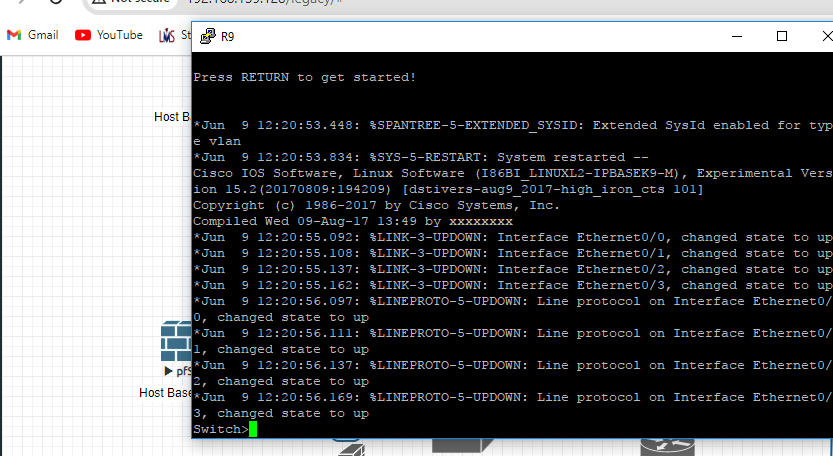


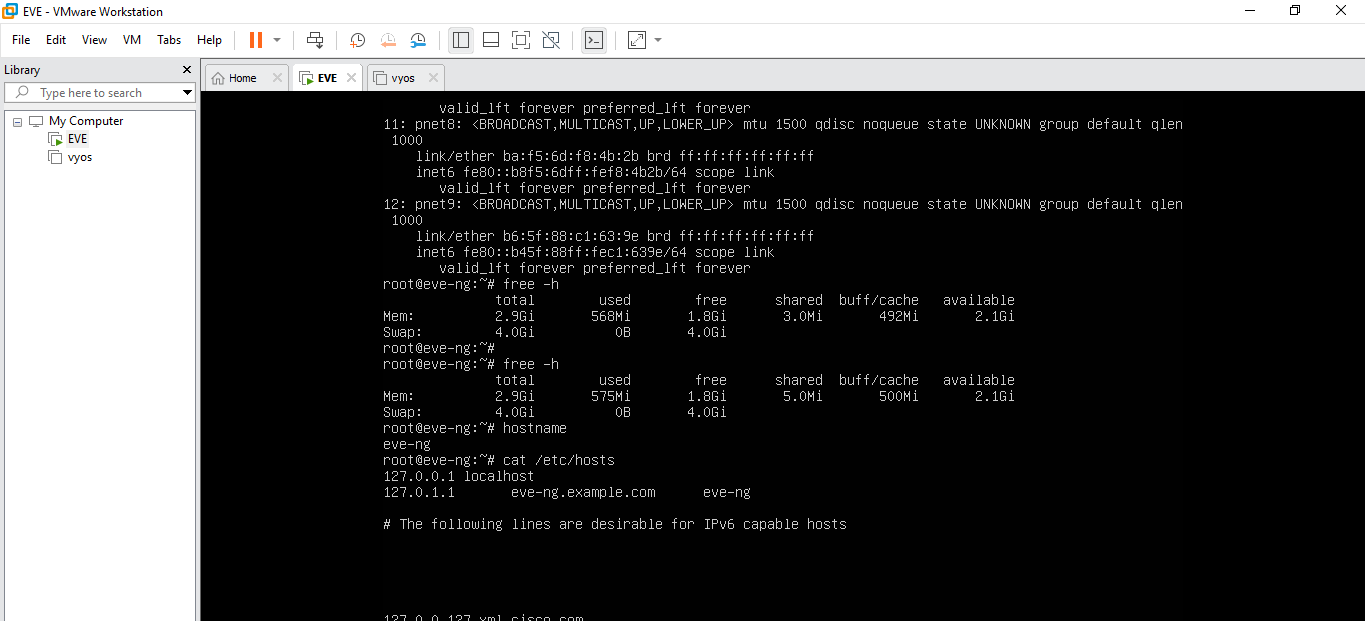
* + - 1. All other traffic should be dropped by default

\*Solution

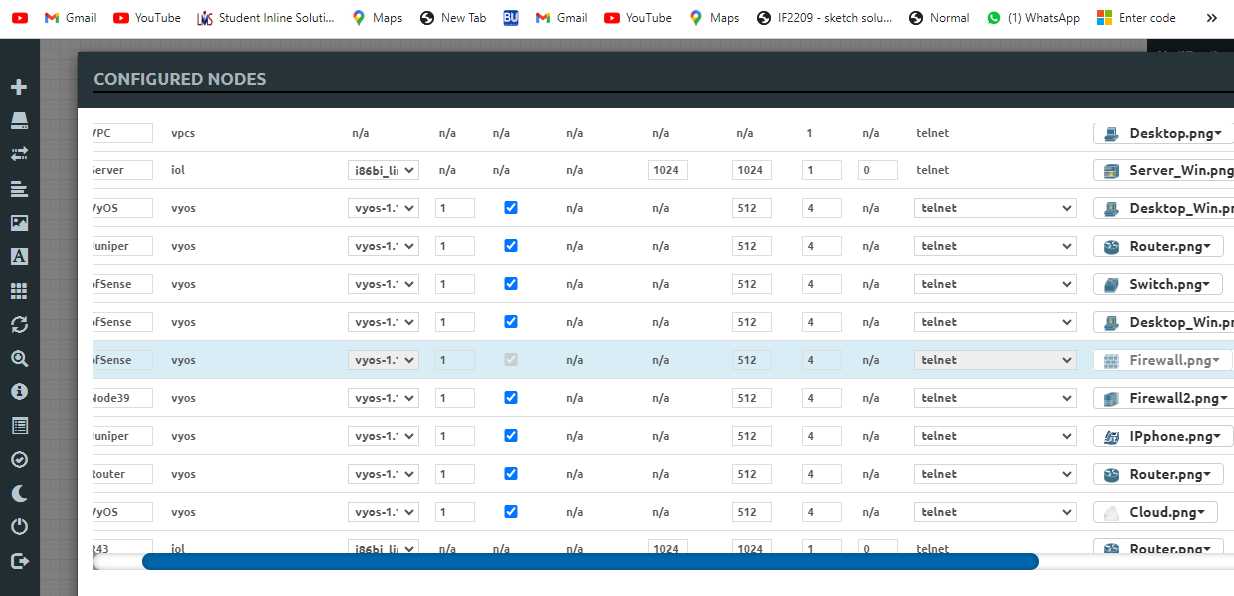


* + 1. Ensure Ansible is able to connect to each host
    2. Configure your choice of gateway firewall, e.g. Vyos, PFSense, etc. between the internal network and the VMware NAT network (Internet)
       1. Ensure that only permitted traffic (only the services identified within these specifications) is allowed



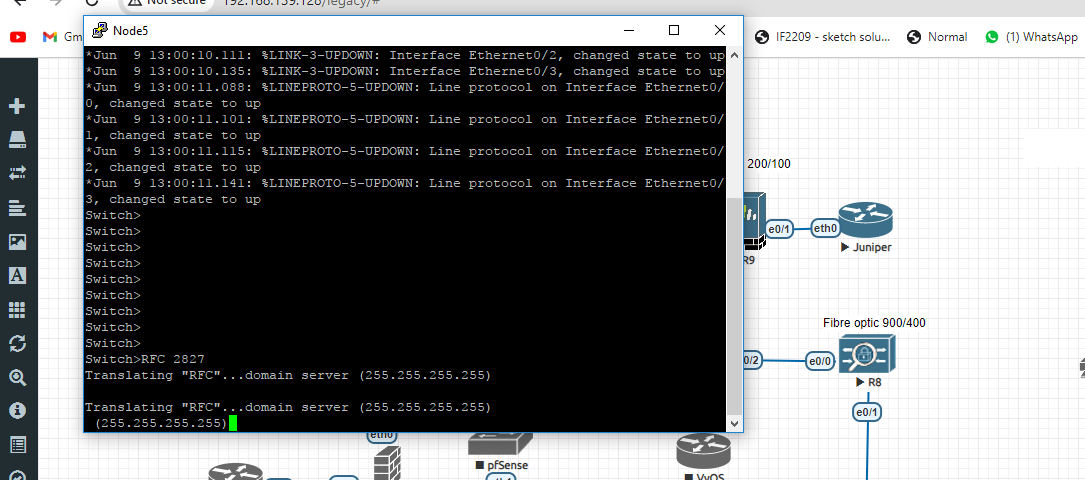


* + - 1. All other traffic should be dropped by default

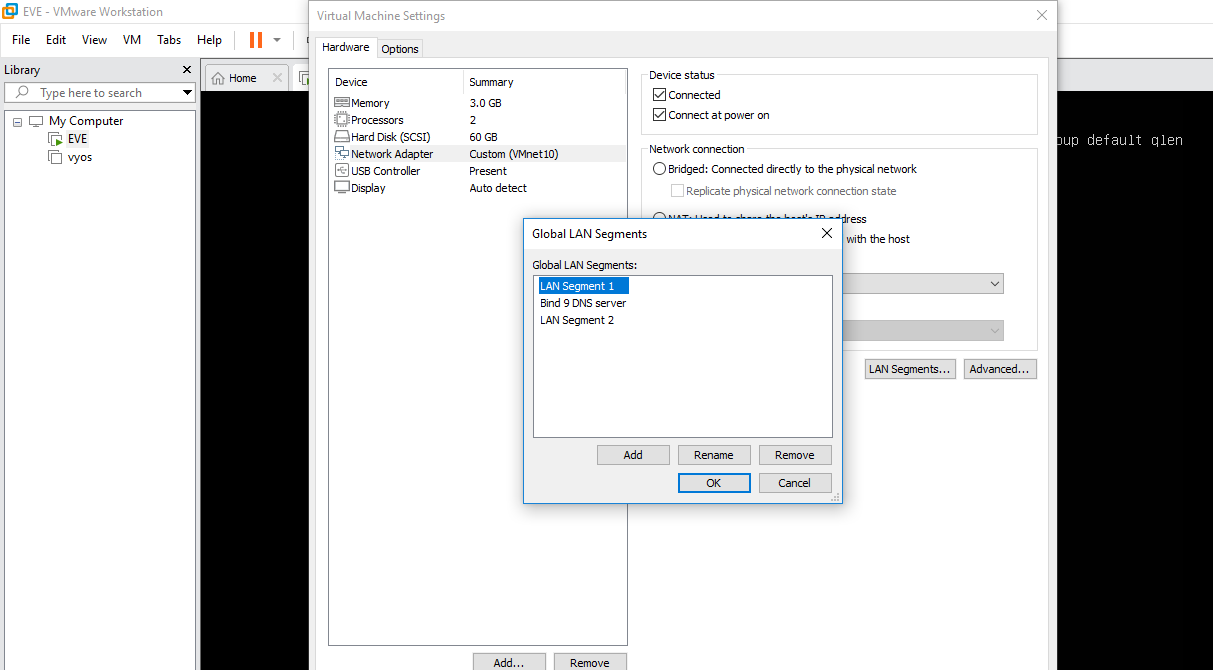


* + 1. Apply gateway filtering in compliance with RFC 2827 to prevent spoofed source addresses from passing your gateway routers. Ensure you filter ingress and egress packets.

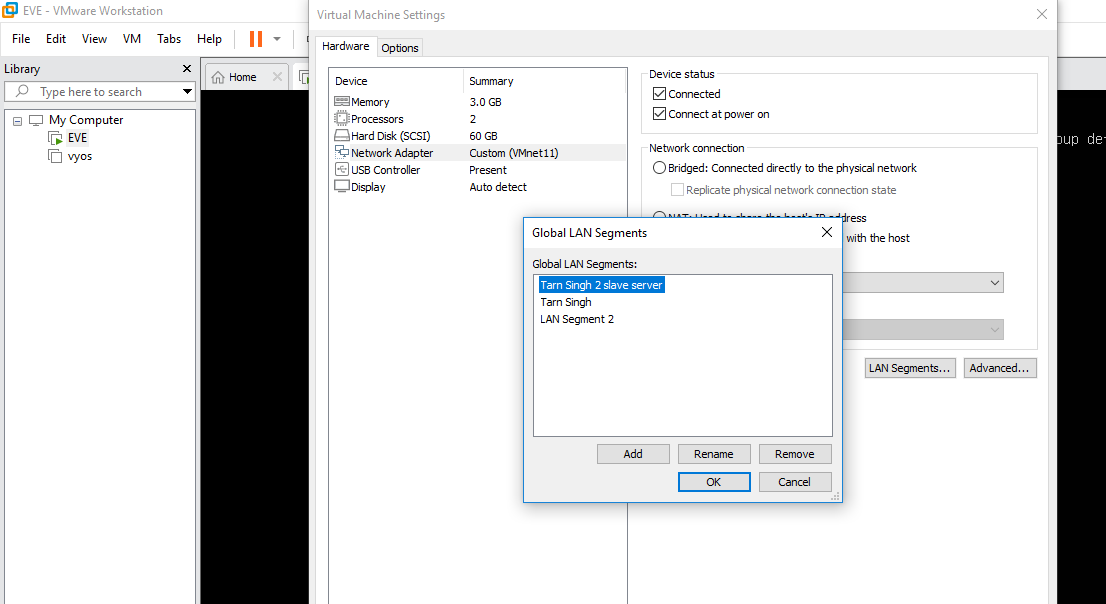
\*Solution



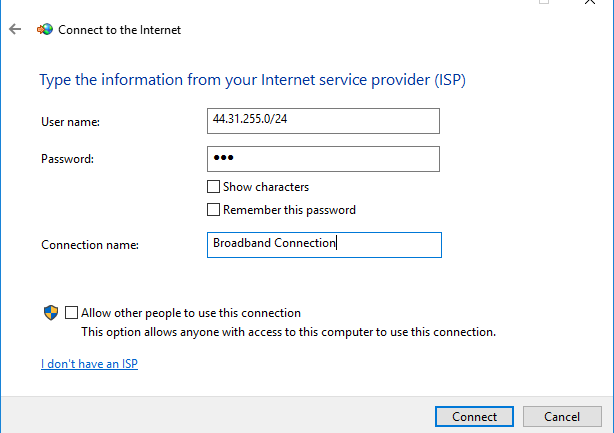
* 1. Bind9 DNS Server
     1. Create a Bind9 DNS master server that is authoritive for **YourName.t301**



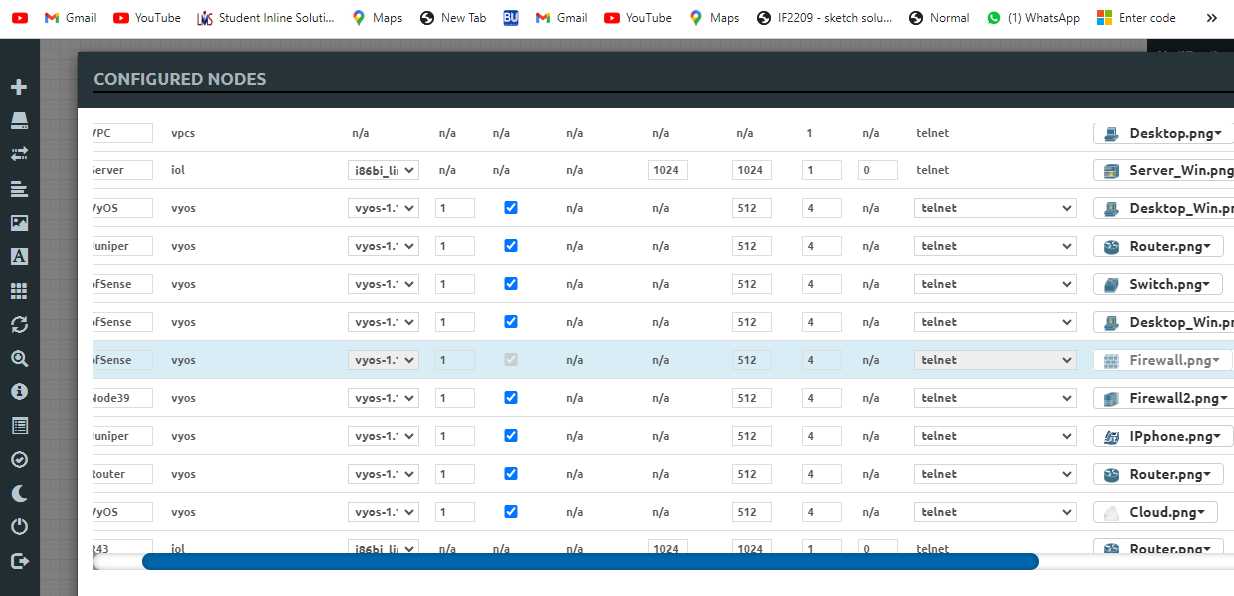
* + 1. Create a Bind9 DNS slave server that is authoritive for **YourName.t301**



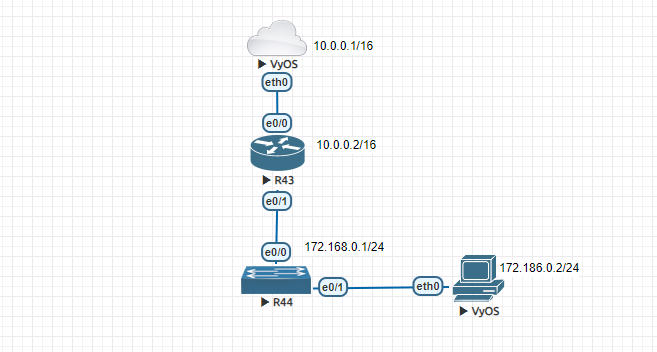
* + 1. Ensure your Bind9 DNS servers will only answer queries from your VMWare NAT network and the 44.31.255.0/24 supernet.



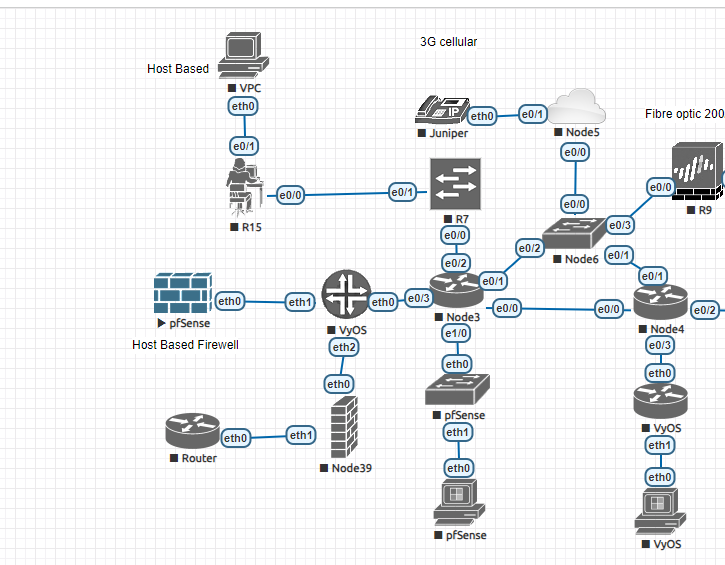
* + - 1. Complete this restriction in both bind9 and iptables
    1. Ensure resource records created in the master server are accessible from the slave server



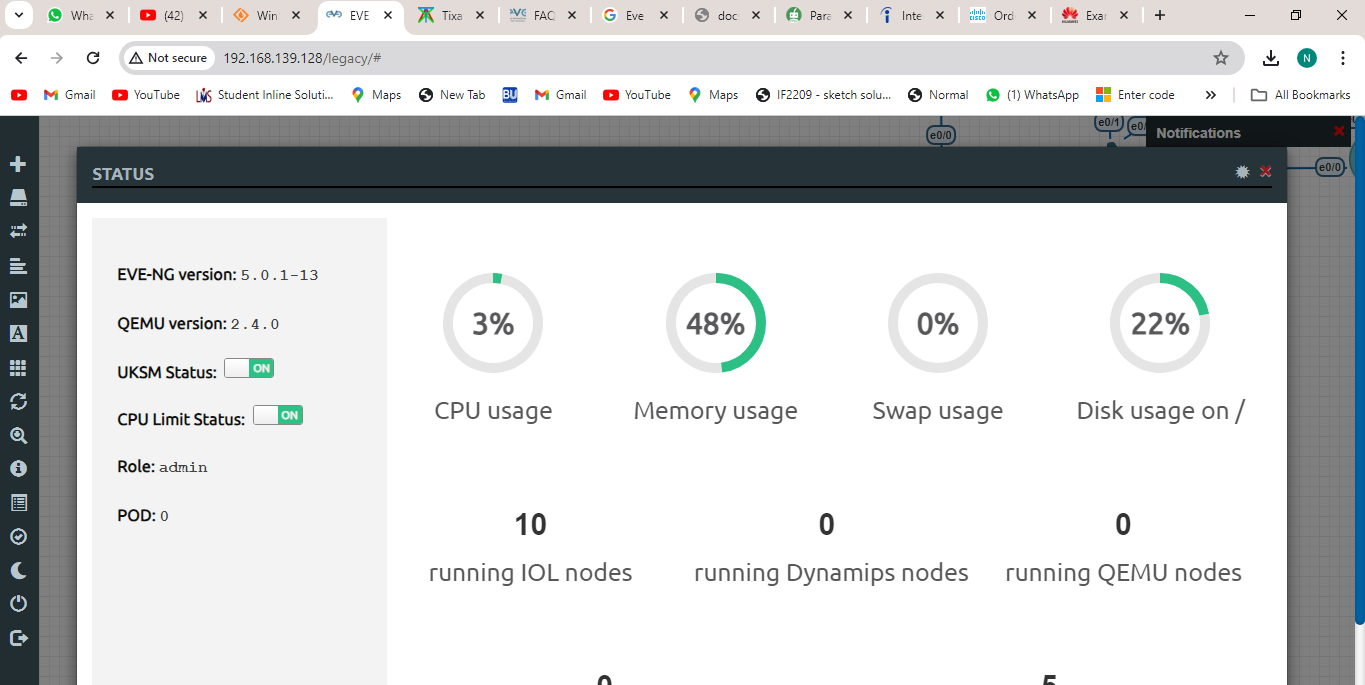
* + 1. Forward requests for any non-authoritive domain/s to 8.8.8.8
  1. Device Hardening
     1. Ensure you use SSH host keys on all Debian servers and any other device that supports them.



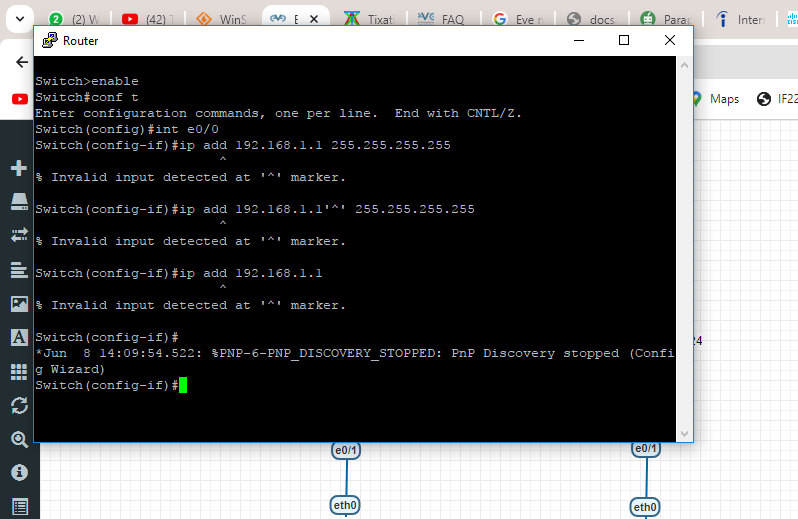
* 1. Apply QoS to all applicable devices, providing the following priority (high to low):
     1. Ensure Ansible SSH traffic has the highest priority



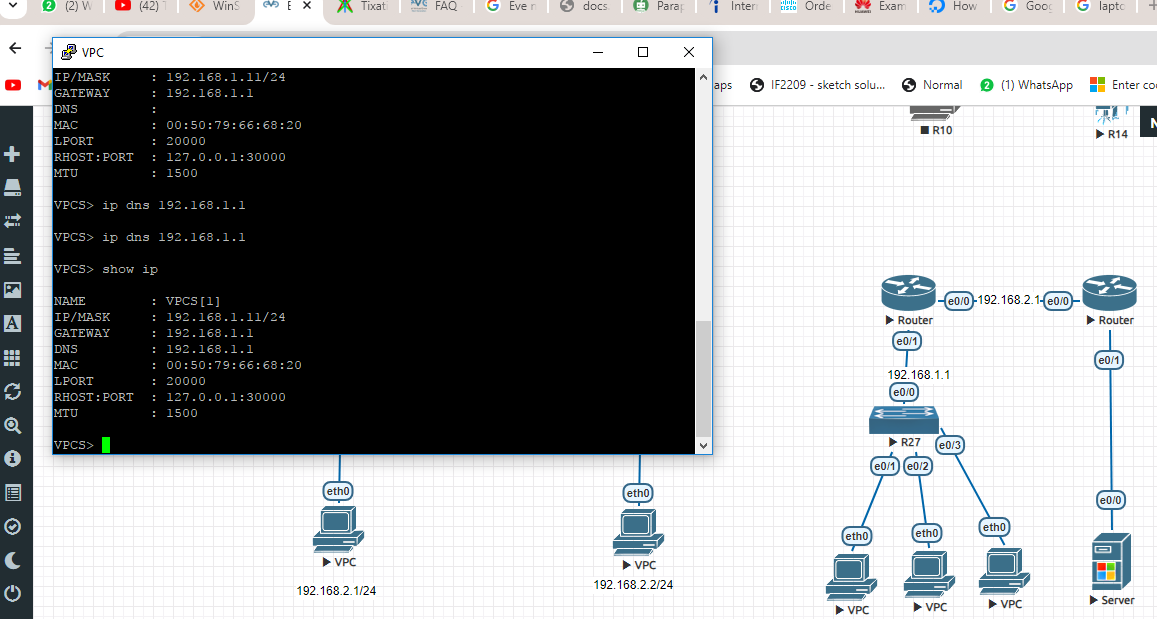
* + 1. Syslog traffic being sent to the Greylog server



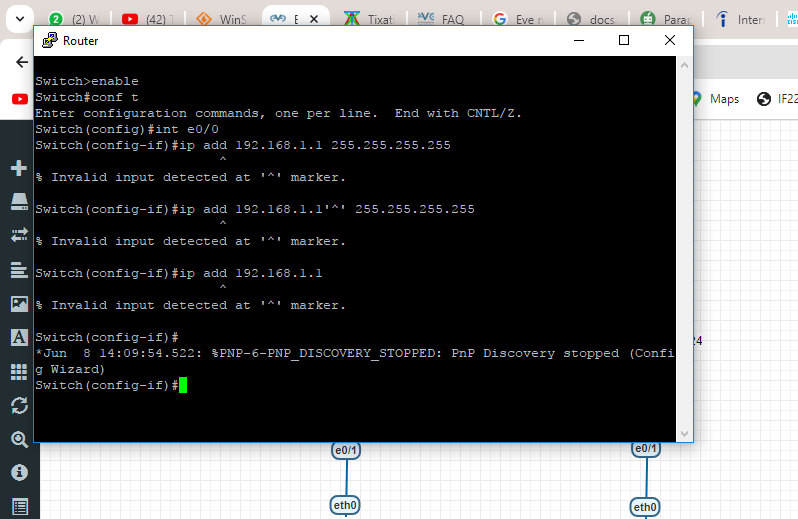
* + 1. DNS



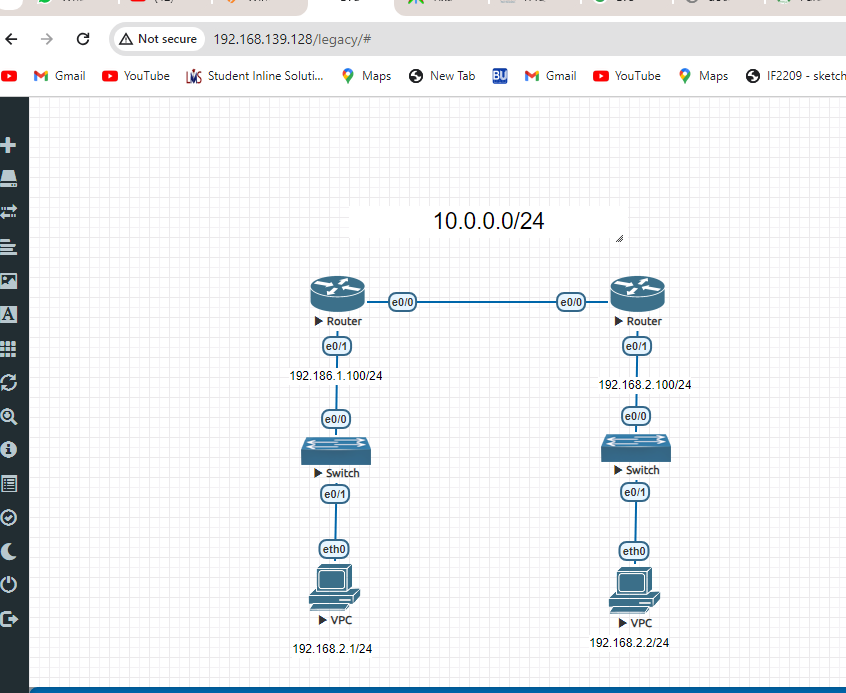
* 1. Your choice of either Greylog or Nagios:
     1. Greylog:
        1. Install one Greylog server.



* + - 1. Configure all Debian servers and any other device that supports syslog to send their logs to the Greylog server



* 1. Docker:
     1. Use Docker when implementing at least one of the other services.



## Infrastructure Requirement Change:

There will be a requirement change point within this assignment that will be completed on an individual basis under limited open book exam conditions in exam week. Further details will be available in Moodle closer to the time.

## Deliverables

1. A single Git repository displaying progress, containing the Ansible playbooks and associated files needed to configure servers as described in the assignment tasks.
2. A ZIP export of the GitHub repository is to be uploaded to Moodle.
3. An .mp4 video presentation using a webcam, microphone and desktop/screen sharing showing your project how you have configured your Ansible roles and tasks to complete the assignment tasks. The video must show evidence of each marking criteria being operational.  
   To verify authenticity your video must utilise a webcam and discussion in your natural voice. OBS (<https://obsproject.com/>) is a good option if you are looking for some software to make a recording.

## submission

1. Invite the “labconf” GitHub user as a collaborator on your private GitHub repository.
2. Export a copy of your repository to a Zip file, upload this to the Assignment 2 Submission link in Moodle.
3. Upload an .mp4 video presentation to SharePoint, see your email for a SharePoint link.

## Marking Grid

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Criteria** | **Improvement Needed** | **Pass** | **Good** | **Excellent** | **Marks** |
| Usage of GitHub to manage assignment | GitHub was not used to manage the assignment or used in a minor way | GitHub was used periodically to manage the assignment | GitHub was used commonly to manage the assignment | Extensive usage of GitHub was evident |  |
| **0** | **1** | **2** | **3** |
| Independence | Instructor advice was needed commonly | Instructor advice was needed however independent progress was clear | Instructor advice was needed periodically however independent progress was clear | Minimal to no additional instructor advice was needed |  |
| **0** | **1** | **2** | **3** |
| Ansible | Ansible was not used, or used in a minimal way over all allocated hosts.  Best practice structure and guidelines were not followed.  Configuration was of poor quality. | Ansible was used to achieve the specified requirements.  Playbooks and roles showed good consideration of best practice structure and guidelines with appropriate naming and commenting. | Ansible was used commonly to achieve the specified requirements.  Playbooks and roles were usually created following best practice structure and are easy to follow. Appropriate naming, commenting, templates and variables were generally used well. | Ansible was used extensively to achieve the specified requirements.  Playbooks and roles were created following best practice structure and are easy to follow. Appropriate naming, commenting, templates and variables were used effectively to facilitate efficient ongoing maintenance.  Roles were created in a clear coordinated manor that would facilitate future reuse. |  |
| **0-12** | **13-15** | **16-19** | **20-25** |
| Network | No network, or a network with no resilience is recommended and implemented. Internet access is not configured. | A network recommendation with some resilience is implemented. Basic traffic routing is performed to enable Internet access. | A network recommendation with considerable resilience is implemented. The routing within the recommendation attempts to optimally route traffic through available network gateways. | A resilient network recommendation is implemented. The routing within the recommendation will optimally route traffic through available network gateways. |  |
| **0-3** | **4-5** | **6-7** | **8-9** |
| Network Gateway Simulation | Minimal or no Internet gateway simulations were implemented. | Internet gateway simulation provides Internet connectivity and correctly simulates at least one of the required gateways. | Internet gateway simulation provides Internet connectivity and correctly simulates at least two of the required gateways. | All internet gateways are implemented as required and have realistic simulation configurations. |  |
| **0** | **1** | **2** | **3** |
| External clients | External clients are not configured correctly to access internal devices. |  |  | External client/s have correct static route and DNS settings allowing access to internal devices. |  |
| **0** |  |  | **1** |
| Gateway Firewalls | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is installed using Ansible and meets most requirements | Is installed using Ansible and meets all requirements |  |
| **0** | **1** | **2** | **3** |
| Bind master server | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is installed using Ansible and meets most requirements | Is installed using Ansible and meets all requirements |  |
| **0** | **1** | **2** | **3** |
| Bind slave server | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is installed using Ansible and meets most requirements | Is installed using Ansible and meets all requirements |  |
| **0** | **1** | **2** | **3** |
| QoS | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is installed using Ansible and meets most requirements | Is installed using Ansible and meets all requirements |  |
| **0** | **1-2** | **3-4** | **5** |
| CameraA | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is installed using Ansible and meets most requirements | Is installed using Ansible and meets all requirements |  |
| **0** | **1** | **2** | **3** |
| CameraB | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is installed using Ansible and meets most requirements | Is installed using Ansible and meets all requirements |  |
| **0** | **1** | **2** | **3** |
| MosaicA | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is installed using Ansible and meets most requirements | Is installed using Ansible and meets all requirements |  |
| **0** | **1** | **2** | **3** |
| MosaicB | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is installed using Ansible and meets most requirements | Is installed using Ansible and meets all requirements |  |
| **0** | **1** | **2** | **3** |
| Greylog | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is installed using Ansible and meets most requirements | Is installed using Ansible and meets all requirements |  |
| **0** | **1-2** | **3-4** | **5** |
| Nagios | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is installed using Ansible and meets most requirements | Is installed using Ansible and meets all requirements |  |
| **0** | **1-2** | **3-4** | **5** |
| Docker | Not implemented or major additional configuration needed | Is installed and meets some requirements | Is correctly configured using Ansible to implement 2 or more services | Is correctly configured using Ansible to implement 3 or more services |  |
| **0** | **1** | **2** | **3** |
| Configuration change | Configuration change was not completed or show sufficient progression towards meeting the requirement/s | Configuration change was undertaken that showed reasonable progression towards meeting the requirement/s | Configuration change was undertaken that showed good progression towards meeting the requirement/s | Configuration change was completed that met the requirement/s |  |
| **0** | **1-2** | **3-4** | **5** |
| **Total /83** | | | | | |