**Capstone Implementation Design**

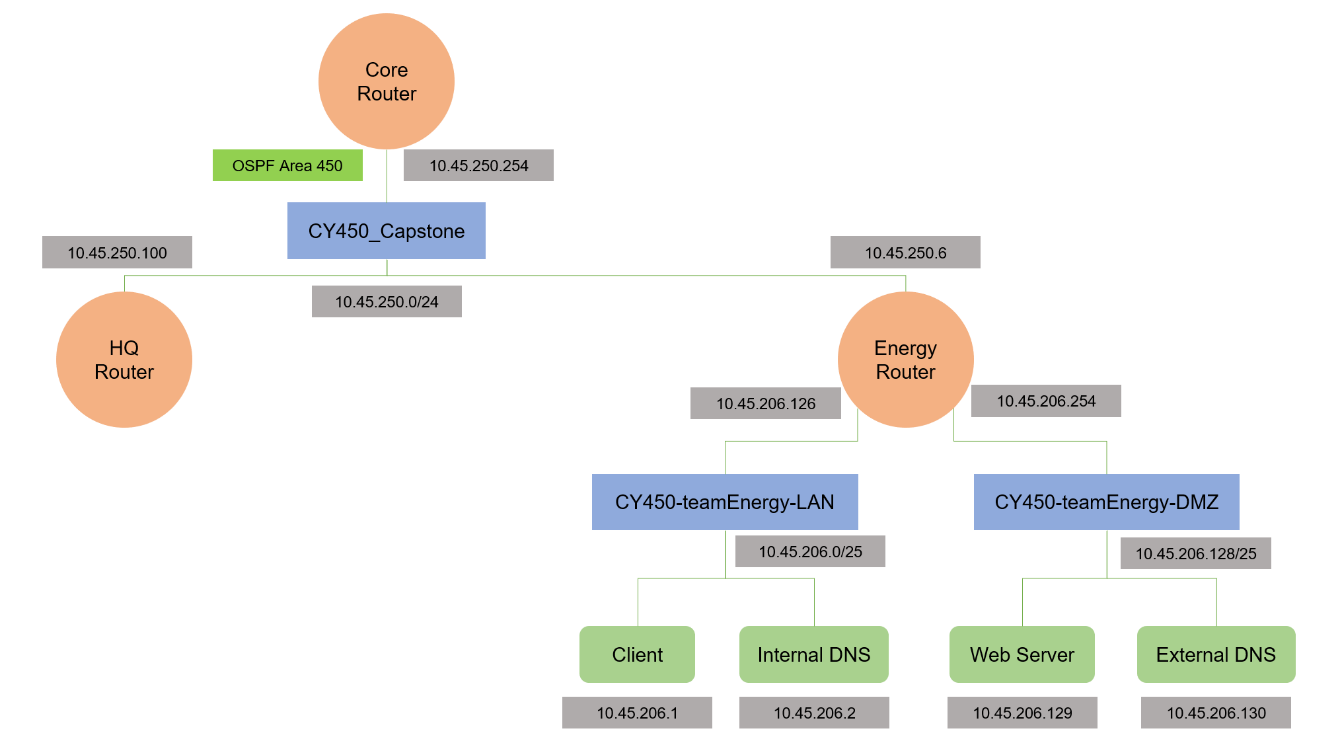


**30 Points**

The following major sections must be included for full credit. Include all details necessary for your team to implement the capstone network in a distributed and asynchronous fashion. You may use this document as a template for this task. It is strongly encouraged that you schedule a review with your instructor prior to beginning to implement your design plan.

1. **Network Diagram**

Include all devices requested in the service implementation plan and all connections among those devices up to the capstone core router and HQ.





1. **Subnet Chart**

Include all explicit requirements from the design specification and any implied requirements in order to successfully execute the design. A table with the following headers should be included.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device/ Network** | **Network Address / Subnet Mask** | **Broadcast Address / GW** | **Host  Range** | **Num. Hosts Possible** | **Num. Hosts Required** |
| Internal (LAN) | 10.45.206.0/25 | 10.45.206.127 | .1 - .126 | 126 | 60 |
| Internal Router | 10.45.206.126/25 |  |  |  |  |
| Internal Client | 10.45.206.1/25 | 10.45.206.126 |  |  |  |
| Internal DNS | 10.45.206.2/25 | 10.45.206.126 |  |  |  |
| External (DMZ) | 10.45.206.128/25 | 10.45.206.255 | .129 - .254 | 126 | 70 |
| External Router | 10.45.206.254/25 |  |  |  |  |
| Web Server | 10.45.206.129/25 | 10.64.206.254 |  |  |  |
| External DNS | 10.45.206.130/25 | 10.64.206.254 |  |  |  |
| WAN Access | 10.45.250.6/24 |  |  |  |  |

1. **Service Implementation Plan**

Enumerate all virtual machines requested by type and describe function. Include network configuration and DNS entries needed for each host requested. Enumerate all ports that each VM is offering services on. Differentiate between services that should be accessible to internal users vs. external users.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Virtual Machines** | | | | | |
| Type | Description | Host Name | Zone | Network Configuration | DNS Entries | Ports |
| *Client* | This VM will be used by many user workstations within our organization. We will secure these hosts while preserving the legitimate user accounts that are on them. | Client.int-ENERGY.cy450 | Internal | IP: 10.45.206.1  SNM: 255.255.255.128  GW: 10.45.206.126  DNS Server: 10.45.206.2 (P) 10.45.206.130 (A) | N/A | 22 (SSH) |
| *Internal DNS (PRIMARY)* | Internal DNS will be configured such that only our internal users have access. | ns2.int-ENERGY.cy450 | Internal | IP: 10.45.206.2  SNM: 255.255.255.128  GW: 10.45.206.126 | Master Server  Composed of internal, forward, and reverse zones  Forwards requests to the HQ DNS  All external zone names will be authoritatively resolved by the Internal DNS | 22 (SSH)  53 (DNS) |
| *External DNS (SECONDARY)* | External DNS will be configured such that both our internal and external users can access. | ns1.ENERGY.cy450 | Internal/  External | IP: 10.45.206.130  SNM: 255.255.255.128  GW: 10.64.206.254 | Slave Server  Composed of forward and reverse zones  Forwards requests to the HQ DNS | 22 (SSH)  53 (DNS) |
| *Web Server* | Our sector’s web server will include several components. The home page (<http://www.energy.cy450/>) will be descriptive and professional. It will include two pages: team\_info.html and sector\_info.html. The homepage will link to these two pages and the Collabtive project management web application. Our web server will primarily use HTTPs and will redirect any HTTP requests to HTTPS. Our certificate will also be signed by HQ to prevent users from receiving a certificate warning. | www.ENERGY.cy450 | Internal/  External | IP: 10.45.206.129  SNM: 255.255.255.128  GW: 10.64.206.254  DNS Server: 10.45.206.2 (P) 10.45.206.130 (A) | N/A | 80 (HTTP) 443 (HTTPS) |
| *Router* | Network traffic will flow between the energy local network and the greater CY450\_Capstone network. Our external network will be accessible from both our internal network and the greater CY450\_Capstone network. We will advertise our networks to the CY450\_Capstone network via OSPF area 450. | router.ENERGY.cy450 | Internal/  External | IP: 10.45.206.126 (internal)  SNM: 255.255.255.128  IP: 10.45.206.254 (external)  SNM: 255.255.255.128  DNS Server: 10.45.206.2 (P) 10.45.206.130 (A) | N/A | 22 (SSH) |

1. **Initial Security Considerations**

List specific mechanisms from **four** **principles of defensible systems** that you plan to execute based on the requirements. This component of your plan should include where you will apply security **controls**, the tentative details of those controls (such as firewall rules on your router), a password plan for the administrative (sector) accounts, how you plan on becoming and staying **current**, etc. Try to include all four principles of defensible systems not limited to the above examples.

We plan to ensure the system is controlled by making all admin accounts have unique login credentials, so an attacker cannot take advantage of a default password. We will make the system minimized by using ACLs to limit access to the system from any unauthorized processes or individuals. We will get the system current by ensuring all services and applications are up to date and we will continue to check for updates on a regular basis. Our system will be monitored through the logging of all user account, security, and software changes.



1. **Team Roles**

Clearly identify, at a minimum, team leader, network lead, DNS lead, service lead, and security lead. You should plan on having redundancy among areas of responsibility. You should synchronize the timeline and everyone’s roles (i.e. the network lead is not done helping the team after the network is set up).

Team Leader: Kendyl McFarland

Network Lead: Taylor Schorlemmer

* Security Lead provides secondary help as network is being constructed

Service Lead: Joseph Zuccarelli

* Team Leader provides secondary help as services are being implemented

DNS Lead: Benjamin Siegel

* Service Lead works with the DNS Lead to ensure proper implementation

Security Lead: Greyson Olep

* Network Lead and Team Leader provide secondary help as security is being implemented

1. **Timeline**

Detail the schedule of all major events remaining in capstone and any personally disruptive events for any team members (besides CoVID). Describe what functionality should be expected at each stage of execution, e.g. router interface configuration, external routing with HQ, internal DNS, etc. Include a sync plan (how and how often the group plans to synchronize their efforts).

**Timeline**

4/1/2021: Project Start

* Organize team, gain understanding of the project, delegate roles to team members

4/6/2021 – 4/7/2021

* Construct design plan
  + Network Design
  + Subnet Chart
  + Service Implementation Plan
  + Initial Security Considerations
* Organize team details
  + Roles of team members
  + General Timeline

**4/8/2021: Implementation Design (30)**

* Turn in Implementation Design

4/9/2021

* Assess implementation design feedback and make necessary corrections

4/10/2021 – 4/19/2021

* Implement subnet chart into network
* Set up Router configuration
* Set up DNS

4/14/2021: Implementation Assessment (IPR)

**4/20/2021: Implementation Assessment**

4/21/2021

* Review implementation assessment feedback

4/22/2021 – 5/4/2021

* Implement ACLs
* Check system logs
* Ensure password protection is enabled
* Make any necessary changes to firewalls

4/28/2021: Security Assessment (IPR)

**5/5/2021: Security Assessment**

5/6/2021

* Review security assessment feedback

**5/11/2021: Project Completion (180)**

**Incident Response Report (30)**

**Group Final Report (50)**

**Individual Security Reflections (100)**

Synchronization: Meet on drops to sync work together.

1. **Change Requests**

List any change requests you may already have. Enumerate all change requests directed in the specification.

We will need two additional VMs (Internal DNS, External DNS).