CSCI 7000-010 – Network Management and Automation

Lab 10

Network Design Group Project

University of Colorado Boulder

Department of Computer Science

Noohu Nufais Sulaiman

My Contributions:

IP Addressing Scheme:

I assumed we got 1.0.0.0/16 from the Tier 3 ISP (Layer 4). I am using starting ranges for the larger Tier 3 ISPs (like /17 to /24) and ending ranges for the internal network connections and the smaller Tier 3 ISPs (like above /24). By doing this, we efficiently subnet the /16 network to the Tier 3 IPSs and have proper IP spaces for future expansion. For the ISPs 8 to 10, I didn't go beyond /24 because the professor said it is not a best practice to go beyond /24.

Version 1:

Subnets for the Tier 3 ISPs:

IPS	No. of expected hosts (from larger to smaller)	CIDR	No. of usable hosts	Network Range (including network address and broadcast address)
1	6498	/19	8190	1.0.0.0 - 1.0.31.255
2	5989	/19	8190	1.0.32.0 - 1.0.63.255
3	2078	/20	4094	1.0.64.0 - 1.0.79.255
4	1027	/21	2046	1.0.80.0 - 1.0.87.255
5	876	/22	1022	1.0.88.0 - 1.0.91.255
6	654	/22	1022	1.0.92.0 - 1.0.95.255
7	196	/24	254	1.0.96.0 - 1.0.96.255
8	76	/24	254	1.0.97.0 - 1.0.97.255
9	63	/24	254	1.0.98.0 - 1.0.98.255
10	46	/24	254	1.0.99.0 - 1.0.99.255

Summarization:

Network to advertise	Network range
1.0.0.0/18	1.0.0.0 - 1.0.63.255
1.0.64.0/19	1.0.64.0 - 1.0.95.255
1.0.96.0/22	1.0.96.0 - 1.0.99.255

In version 1, we are wasting a lot of IP addresses for the larger Tier 3 ISPs. To overcome this, we are giving multiple network ranges to a single Tier 3 ISP (if necessary), instead of giving them one huge block of IPs.

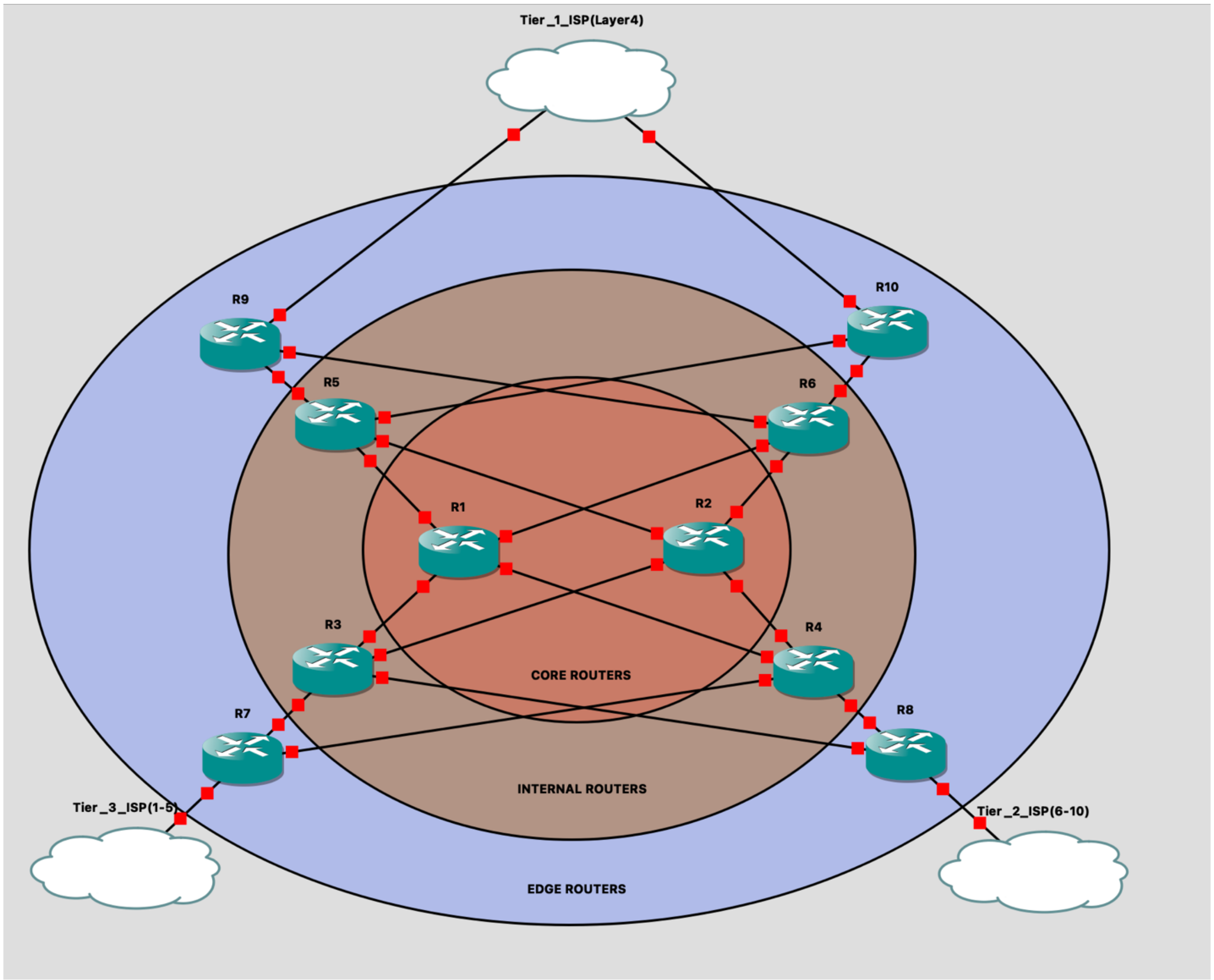
Version 2:

ISP	No. of hosts	CIDR	Subnetting order	Network Range	No. of usable hosts	Total number of usable hosts
1	6498	/20	1	1.0.0.0 - 1.0.15.255	4094	6650
		/21	3	1.0.32.0 - 1.0.39.255	2046	
		/23	8	1.0.64.0 - 1.0.65.255	510	
2	5989	/20	2	1.0.16.0 - 1.0.31.255	4094	6140
		/21	4	1.0.40.0 - 1.0.47.255	2046	
3	2078	/21	5	1.0.48.0 - 1.0.55.255	2046	2300
		/24	10	1.0.68.0 -1.0.68.255	254	
4	1027	/22	6	1.0.56.0 - 1.0.59.255	1022	1276
		/24	11	1.0.69.0 -1.0.69.255	254	
5	876	/22	7	1.0.60.0 - 1.0.63.255	1022	1022
6	654	/23	9	1.0.66.0 - 1.0.67.255	510	764
		/24	12	1.0.70.0 -1.0.70.255	254	
7	196	/24	13	1.0.71.0 -1.0.71.255	254	254
8	76	/24	14	1.0.72.0 -1.0.72.255	254	254
9	63	/24	15	1.0.73.0 -1.0.73.255	254	254
10	46	/24	16	1.0.74.0 -1.0.74.255	254	254

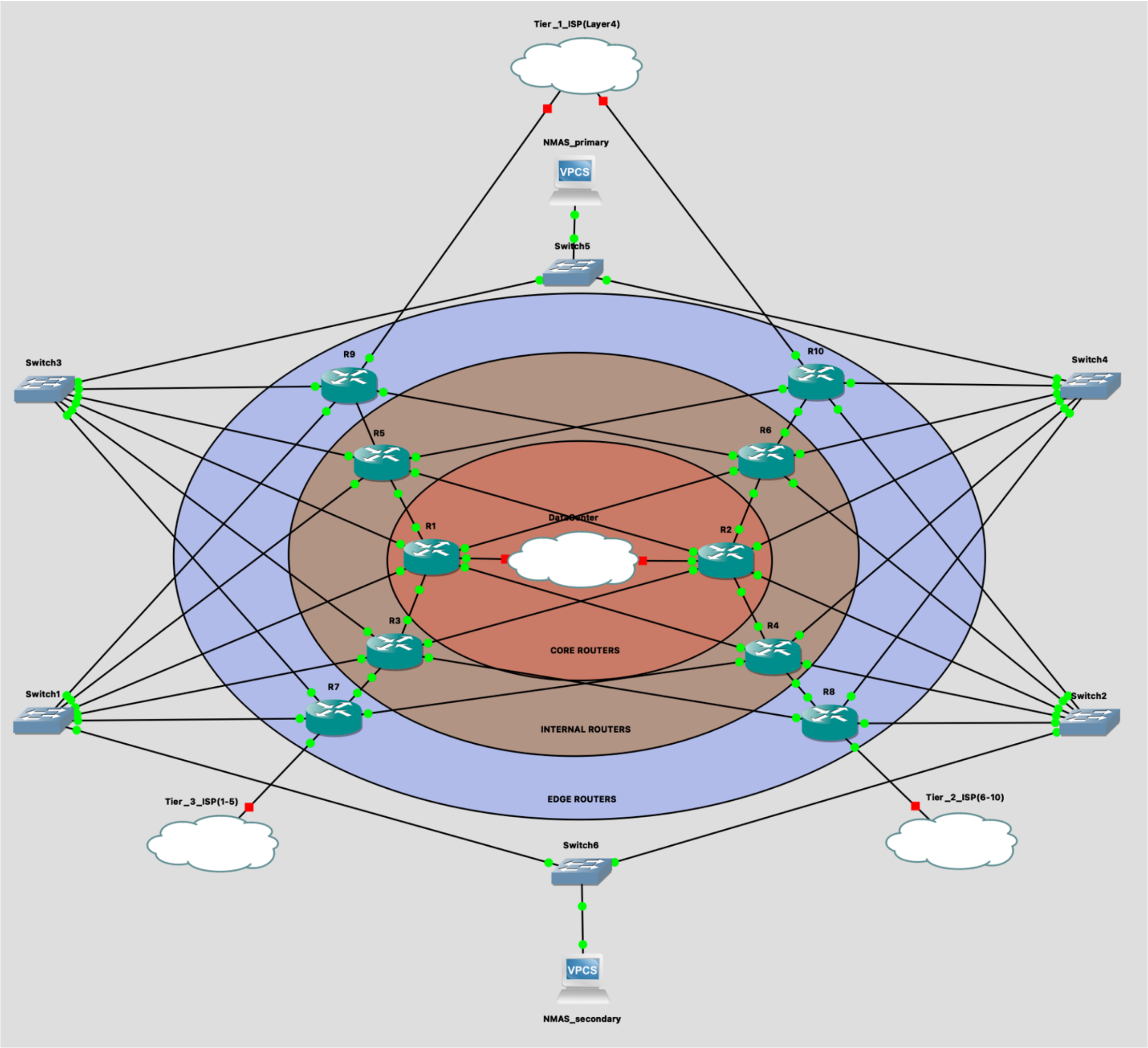
Summarization:

Network to advertise	Network range
1.0.0.0/18	1.0.0.0 - 1.0.63.255
1.0.64.0/21	1.0.64.0 - 1.0.71.255
1.0.72.0/23	1.0.72.0 - 1.0.73.255
1.0.74.0/24	1.0.74.0 - 1.0.74.255

Backbone Network Design:



- Two Edge Routers to connect to the Tier 1 ISP for redundancy.
- Two Edge Routers to connect to the Tier 3 ISPs.
- Each router in each layer is connected to two other routers in the adjacent/next layer for load balancing and redundancy.



- There are 2 NMASs (Primary and Secondary), and each NMAS is connected to all the routers via the management network.
- If the Primary NMAS fails or the management connection to any of the routers fails, we have Backup/Secondary NMAS to connect to the routers.
- Connected the Data Center to the Core routers, so that it could be accessible from anywhere with an equal amount of time.

Network Security Solution:

Firewall:

To fortify network security against potential DDoS attacks, the Cisco ASR 9904 Router functions as an edge router for firewalls, providing robust protection for the data center, internal infrastructure, and core routers against unauthorized access, malicious attacks, data breaches, and DDoS assaults.

Load Balancing:

Each router within the network is intricately interconnected with two neighboring routers in the subsequent layer, ensuring redundancy and high availability. With each router equipped to manage substantial traffic loads, load balancing automatically activates once a router nears its capacity threshold, efficiently distributing incoming traffic across available paths to maintain optimal performance and network resilience.

Securing Management Network:

1. **Implementation of VRF on Router Interfaces:**
   - Virtual Routing and Forwarding (VRF) is applied to each router's management interface, ensuring isolation and segregation of management traffic, and safeguarding critical functions from security threats.

2. **Configuration of ACLs on Router Interfaces:**
   - Access Control Lists (ACLs) are configured on the router's management interfaces, permitting only traffic originating from the designated network management system (NMS), thus tightly controlling access, and mitigating unauthorized intrusion risks.

3. **Enforcement of Port Security on Switches:**
   - Port security measures are enforced on management switches, allowing only authorized network management system (NMS) devices to connect. This restricts access to designated NMS devices by binding connections to specific MAC addresses, bolstering overall security.