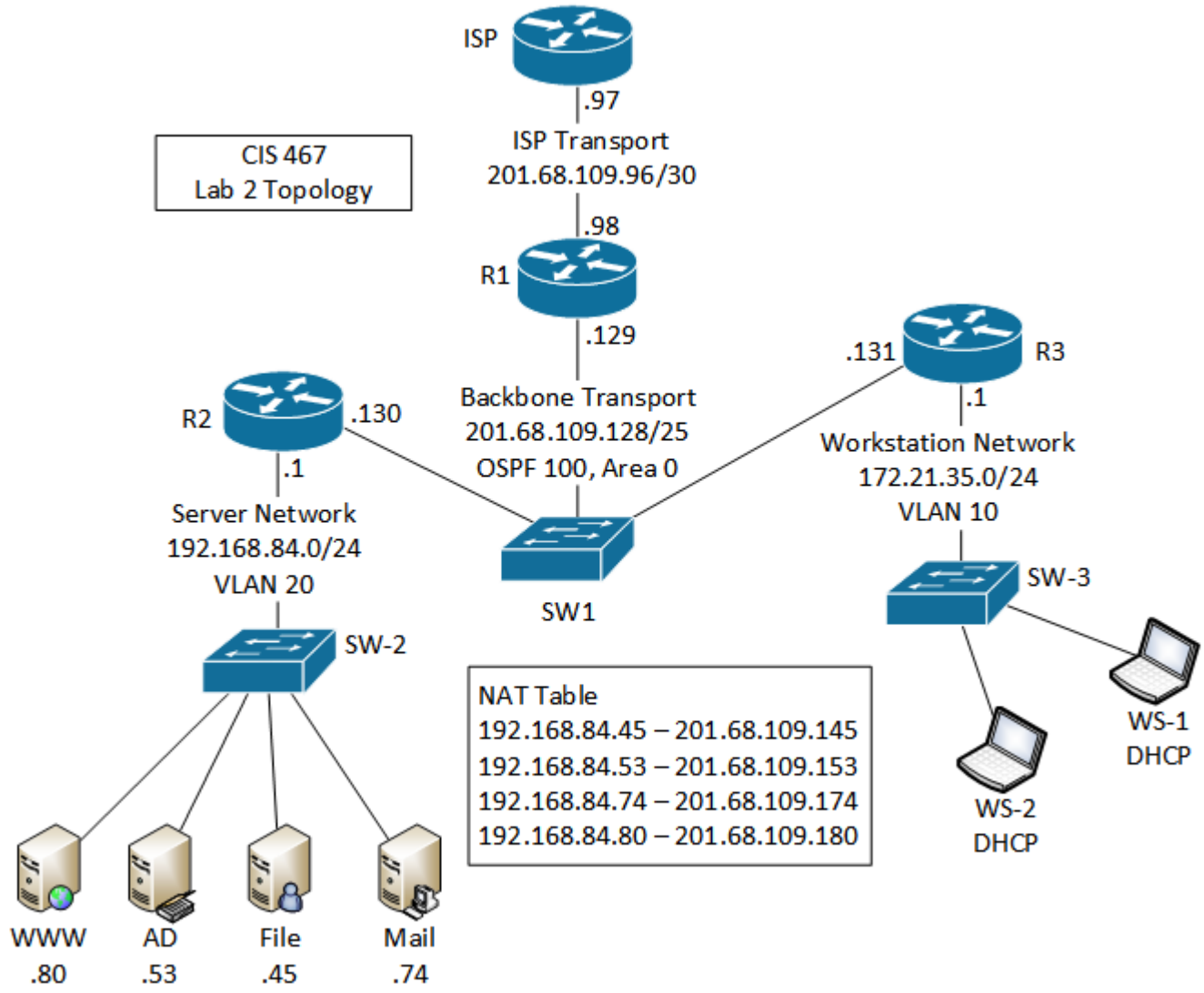
CIS 467 Network Security
James Schneider

LAB #2

Using Cisco routers and switches complete the tasks below. You may use reference materials from the Internet and the resources listed on the Blackboard site. Additionally, you may team up with up to two other students! Each student must submit their own copy of the lab.



Lab Tasks:

1. Configure all routers, switches, and servers with the hostnames, connections, and IP addressing depicted in the diagram.
    a. R2 and R3 will act as the default gateway for the workstation and server segments.
    b. Ensure that VLAN's are used on SW-2 and SW-3 per the diagram.
2. Configure a static default route to the ISP router on R1.
3. Configure a static route for the workstation network on the ISP router.
4. Configure OSPF connectivity between R1, R2, and R3 using the parameters depicted in the topology.

    a. All routed interfaces (except the ISP segment) should be members of Area 0.
    b. R1 should originate a default route for all other routers.
    c. Ensure you have full, 100% connectivity between ALL routed networks. Full connectivity is validated when pings from the ISP router are successful to the following IP addresses:
        i. 201.68.109.130 (R2 Outside)
        ii. 201.68.109.131 (R3 Outside)
        iii. 192.168.84.1 (R2 Inside)
        iv. 172.21.35.1 (R3 Inside)
5. On R1 configure and apply an access control list that will prevent all sources from RFC 1918 networks from being sent out to the Internet.
6. Setup static NAT on R1 with the following translations:
    a. 192.168.84.45 – 201.68.109.145
    b. 192.168.84.53 – 201.68.109.153
    c. 192.168.84.74 – 201.68.109.174
    d. 192.168.84.80 – 201.68.109.180
7. Setup PAT on R1. Create the PAT entry so that the workstation subnet (172.21.35.0/24) is translated out as R1's external interface (201.68.109.98).
8. Configure R3 as a DHCP server with a DHCP pool of 172.21.35.0/24. Ensure clients receive the correct default gateway for the network, and use the AD server for DNS. Exclude addresses 172.21.35.1 – 172.21.35.25 from being assigned by DHCP.
9. Create and apply an access control list on R1 using the information below. (Remember you used NAT previously!!!)
    a. Allow SMTP from the Internet to Mail.
    b. Allow HTTP and HTTPS from the Internet to WWW and File.
    c. Allow DNS requests from the Internet to AD.
    d. Deny and log all other requests from the Internet to every server.
10. Create and apply access control lists on R3 using the information below.
    a. Allow hosts on the workstation network to access LDAP, Kerberos, and RPC services on AD.
    b. Block and log workstation hosts from accessing File and WWW via SSH. Allow and log all other requests from workstations.
    c. Block and log all requests to workstation hosts using the Remote Desktop protocol.
    d. Ensure all other services are allowed into the workstation network.
11. Setup AAA on R1, R2, and R3 so that users are authenticated by the active directory / ACS server (192.168.84.53) for all local and remote management connections. Use Cisco123 as your RADIUS key. Only permit SSH connections from the server network segment on each router. Enable SSH and disable all other remote management services.

Once you have completed the lab, save it in softcopy, (the configuration files OR the packet tracer file). Upload your file(s) to Blackboard.