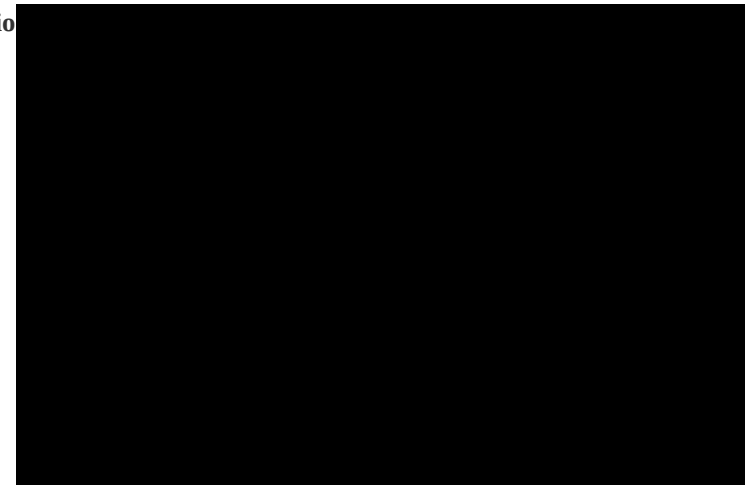
CCNP SWITCH(642-813) Lab – AAA dot1x(New)

[Scenario Acme is a small shipping company that has an existing enterprise network comprised of 2 switches;DSW1 and ASW2. The topology diagram indicates their layer 2 mapping. VLAN 40 is a new VLAN that will be used to provide the shipping personnel access to the server. For security reasons, it is necessary to restrict access to VLAN 20 in the following manner: - Users connecting to ASW1's port must be authenticate before they are given access to the network. Authentication is to be done via a Radius server: - Radius server host: 172.120.39.46 - Radius key: rad123 - Authentication should be implemented as close to the host device possible. - Devices on VLAN 20 are restricted to in the address range of 172.120.40.0/24. - Packets from devices in the address range of 172.120.40.0/24 should be passed on VLAN 20. - Packets from devices in any other address range should be dropped on VLAN 20. - Filtering should be implemented as close to the server farm as possible. The Radius server and application servers will be installed at a future date. You have been tasked with implementing the above access control as a pre-condition to installing the servers. You must use the available IOS switch features. **[Scenario**



[Solution 1. Verification of Pre-configuration: a. Check that the denoted vlan [vlan20] is created in both switches and ports [fa0/1 of ASW1] are assigned. b. Take down the radius-server ip [172.120.39.46] and the key [rad123]. c. Take down the IP range [172.120.40.0/24] to be allowed the given vlan [vlan20] **2. Configure the Port based authentication on ASW1:** aaa new-model radius-server host 172.120.39.46 key rad123 aaa authentication dot1Q default group radius dot1Q system-auth-control int fa 0/1 switchport mode access switchport access vlan 20 dot1x port-control auto copy running-config startup-config **3. Filter the traffic and create vlan access-map to restrict the traffic only for a range on DSW1** ip access-list standard allow permit 172.120.40.0 0.0.0.255 vlan access-map vamap 5 match ip address allow action forward vlan acces-map vamap 10 action drop vlan filter vamap vlan-list 20 copy running-config startup-config **4. Note:** It is not possible to verify the configuration in this lab. All we have do the correct configurations. Most of the exam takers report that ? copy running-config startup-config? is not working. It does not a matter. Do not try unwanted/wrong commands in the consoles. They are not real switches. Packet tracer is not supporting this LAB.