LAB SESSION WEEK 3 – TUTORIAL NOTES

GENERAL INFORMATION

1. Labs will continue to run online in Weeks 4 and 5
2. Remember to skip the “on-campus” steps of the Lab practice

REVISION

Packet Tracer

1. Drag and drop devices and interconnect them to build the lab topology
2. Power supply must be installed on Catalyst 3650 switches
3. Free training module in NetAcademy
4. If you are an offshore student → Mid Sem Skills Exam is PT based.

IP address, MAC address and ARP process

1. Layer 3 addressing
    - IPv4 address structure ← 32 bits expressed in 4 dotted decimal numbers
    - Network portion/Host portion and the subnet mask

2. Layer 2 addressing
    - MAC address ← 48 bits expressed in 12 hexadecimal digits
    - Unique for each NIC
    - Assigned by manufacturer
3. ARP process
    - Devices must know both the destination IP and destination MAC ← for encapsulation
    - Applications know the IP address
    - ARP request/reply to determine the destination MAC address for a destination IP
    - Binding entries saved to the ARP table

Basic Switch configuration

1. Parts of the switch → IOS, RAM, NVRAM, Flash, CPU and Network Interfaces
2. Terminal emulation required → console or remote access via telnet/ssh
3. Important files: running-config, startup-config, IOS image (.bin), vlan.dat, config-reg
4. Basic global configuration → hostname, console and remote access password, enable password, MOTD
5. Basic interface configuration → management VLAN IP, disable/enable Ethernet interfaces, interface description
6. How to save the configuration → copy run start
7. How to remove the configuration → write erase & reload (say no when asked if want to save the changes)
8. How to remove the VLAN configuration on a switch → delete vlan.dat

9. Some show commands:
    - show ip interface brief → very important to know how to read the output
    - show run → displays the running configuration file (check running settings)
    - show start → displays the startup config file (check the settings that will take effect after a reboot)
    - show version → IOS version, image file name, last rebooted, config-reg value, etc.

Answer to the questions in the lab handout

Go to LAB-SU2 handout.

TUTORIAL

VLANs

1. Virtual Local Area Networks → divides a switch into multiple L2 domains (or virtual switches)
2. Devices connected to the same VLAN can communicate with each other without the aid of a layer 3 devices
3. Devices in the same VLAN should be configured in the same IP network (i.e. same network portion)
4. Devices in different VLANs cannot communicate directly via the switch ← a router is needed
5. VLAN configuration is saved to the vlan.dat file NOT the running config
6. We can **delete the vlan.dat** file to remove all VLANs.
7. **no vlan command** removes 1 VLAN

Management VLAN

8. The management VLAN carries management traffic
9. We configure the switch management IP on the corresponding VLAN interface
10. Is not a good practice to use the switch's default VLAN (VLAN 1) → by default, all ports belong to VLAN 1
11. We configure a dedicated VLAN for management
12. It is not a good practice to place end hosts to the management VLAN (in today's lab we will, but not in the future)

Remote Access (Telnet or SSH)

1. Switch must have a management IP → configure on the interface VLAN for the management VLAN
2. If you want to access the switch from a different network as the mgmt. IP, the switch must also have a default gateway
3. We access the CLI using a terminal emulation application
4. Telnet
    - Clear text communication between server (switch) and client (admin's PC)
    - Windows telnet client can be used from a **cmd** window
    - We can telnet into a switch from another switch or from a router
5. SSH
    - Encrypted communication between server and client
    - To enable SSH on a switch, you first need to configure a hostname, define the switch's FQDM and generate RSA keys
    - There is no SSH client built-in on Windows, you need to use an application such as Putty, SecureCRT, etc.
    - We can SSH into a switch from another switch or another router

6. The switch can authenticate Remote Access against a local user database (stored in the running and startup config files)
7. The local user database needs to be populated → need to create user and passwords

Switch security

13. Remove management from the default VLAN
14. Disable unused ports
    - Unauthorized access to the network
    - MAC address flooding attacks
    - MAC address spoofing attacks
15. Switchport security ← how many and which MAC addresses can connect to a port