LAB SESSION WEEK 2 – TUTORIAL NOTES

GENERAL INFO

1. You should have received your NetAcademy registration link on your student email
2. You are advised to read the CCNA material as per the weekly planner

REVISION

Role of Switches and Routers

1. Switches: Layer 2 communication devices
2. Routers: Layer 3 communication devices
3. Switches interconnect many hosts to be in the same L2 segment ← high port density
4. Switches forward frames from one port to another based on the **MAC address**
5. Routers interconnect Networks

ATC Cisco Labs

1. Five enclosures in ATC328 and five enclosures in ATC329
2. Five Kits per enclosure, and 8 devices per Kit: 4 Routers and 4 Switches

   4 x Cisco 4321 Routers

   2 x Cisco Catalyst 2960

   2 x Cisco Catalyst 3650
3. We use the **SmartRack** system to remotely access the network devices console

4. We can access the Smart rack system from home using our Swinburne VPN
5. Establish 1 SSH session to SmartRack server per each device ← unique username/pwd per device
6. In this Unit we will be using Router1, Switch3, Switch4 and Switch1.
7. **Always keep unused devices powered off**

Wiring Scheme

1. Devices in the lab are pre-cabled
2. Even if we go back to campus, we will not be cabling the devices ourselves
3. You must familiarize yourself with the existing cabling scheme
4. You used the **show ip interface brief** command to validate the cabling scheme
5. Let's review the answer to those questions ← go to Lab SU – 1a

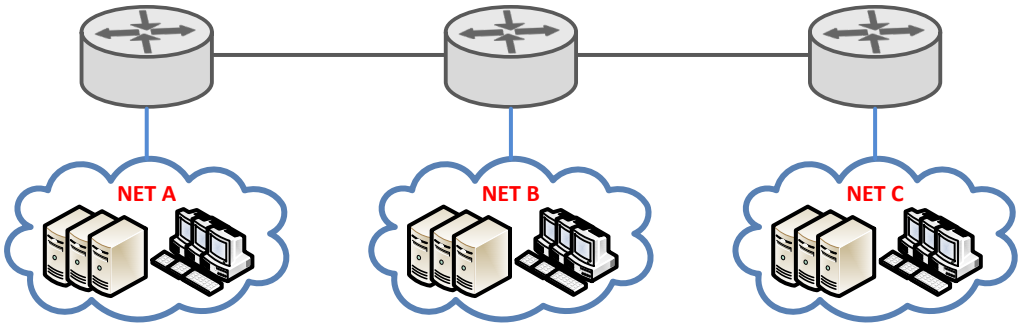
TUTORIAL

IPv4 addressing

1. One of the main functions at layer 3 is addressing the hosts – Unique ID
2. An IPv4 address is a unique combination of 32 0s and 1s (what we call bits)
3. Dotted decimal notation:
    - Break the 32 bits into 4 groups of 8 – What we call byte or octets
    - Translate each octet from binary to decimal numbers
    - How? Calculate powers of 2 of '1' bits (as per position) then add these powers of 2

7 6 5 4 3 2 1 0		7 6 5 4 3 2 1 0		7 6 5 4 3 2 1 0		7 6 5 4 3 2 1 0	
11000000	.	10101000	.	00000101	.	00100110	
2^7 + 2^6	.	2^7 + 2^5 + 2^3	.	2^2 + 2^0	.	2^5 + 2^2 + 2^1	
128 + 64	.	128 + 32 + 8	.	4 + 1		32 + 4 + 2	
192	.	168	.	5	.	38	/24

4. Network and Host portions:



- Computers and communication devices cannot learn every single host address
- Instead, they know about Networks and how to find them

  Note: again, household example (someone in charge knows unique names)
- The INTERNET is nothing but many interconnected IP networks
- Yet applications will typically send data to a host address, not a network address
- A computer/router needs to know the network a host belongs to from its address
- The Network portion, a few of those 32 bits, define the Network – leftmost bits
- Hosts in the same Network share the same 0s and 1s Network bits combination
- Then, the rest of the IP address uniquely identifies the host within the Network

  Note: give family name and given name example

5. Network mask:
    - Defines where the Network portion ends, and the Host portion begins
    - CIDR value, mask length or slash notation: /*n* - *n* is the number of mask bits
    - Dotted decimal notation: Network bits set to 1 and Host bits set to 0
    - Note that the Network mask will define the size of the Network
    - Shorter Network portion → Longer Host portion → More unique Host combinations

CIDR: /24

11000000	.	10101000	.	00000101	.	00100110
11111111	.	11111111	.	11111111	.	00000000
2^7+2^6+2^5+ 2^4+2^3+2^2+2^1+2^0	.	2^7+2^6+2^5+ 2^4+2^3+2^2+2^1+2^0	.	2^7+2^6+2^5+ 2^4+2^3+2^2+2^1+2^0	.	0
128+64+32+16+8+4+2+1	.	128+64+32+16+8+4+2+1	.	128+64+32+16+8+4+2+1	.	0
255	.	255	.	255	.	0

Layer 2 Addressing – Ethernet

1. A 'segment' is what we called a group of hosts physically connected to each other
2. Hosts within a segment share the same transmission media – wire or wirelessly
3. Within a segment, hosts address each other not by their IP address but by their L2 address
4. In an Ethernet segment (Ethernet as L2 protocol): MAC addresses
    - 48 bits represented as 12 hexadecimal numbers ← 6 groups of 2 or 3 groups of 4
    - Every NIC in the world has a unique MAC address
    - The first 3 bytes (6 hexadecimal digits) identify the NIC manufacturer: OUI

Encapsulation overview

1. Frames ← Layer 2 data unit
2. Packet ← Layer 3 data unit
3. Ethernet frame header: source and destination MAC address
4. IP packet header: source and destination IP address
5. For a host to send a message, it uses both a L2 and a L3 destination to form the frame
6. If the destination host is in the same IP Network/L2 segment as the sender:
    - Destination IP address is that of the destination host
    - Destination MAC address is that of the destination host
7. If not:
    - Destination IP address is that of the destination host
    - Destination MAC address is that of the local ***Default Gateway***

ARP Process

1. Packets need to be encapsulated in a L2 frame for transmission
2. Hosts then need to know the dest. MAC address to be used for a particular dest. IP address
3. How do they know: The ARP (Address Resolution Protocol) process?
4. When first need to send a message to a particular IP address:
    - If in the same Network → L2 broadcast ARP request: who is 'destination IP address'
    - If NOT → L2 broadcast ARP request: who is 'default GW address'

Packet Tracer – Show and Tell

We will through the rest of the Tutorial using Packet Tracer for demonstration purposes

More about Switches

1. Purpose-built Operating System → Internetworking Operating System (IOS)
2. Storage: RAM, NVRAM and Flash
3. CPU
4. Multiple Network Interfaces
5. No terminal (not keyboard/display)
6. Terminal emulation:
    - Console (RJ45 – DB9 console cable)
    - Remote access (Telnet or SSH)

Modes of Operation

1. Execution mode ← as you access the CLI
2. Privileged Execution (or enable) mode ← type ***enable*** to go to this mode
3. Global Configuration mode ← type ***configuration terminal*** to go to this mode
4. Specific Configuration modes ← e.g. interface configuration mode
5. Note the characters following the router name will change from one mode to the other

Important files

1. running-config – stored in the RAM → sh run
2. startup-config – stored in the NVRAM → sh start
3. IOS image file – stored in the Flash → sh flash
4. vlan.dat – stored in the Flash or NVRAM
5. config-reg – 16-bit value stored in the NVRAM. →

   Some possible values:

   0x2102 → load startup-config

   0x2142 → bypass startup-config

The Switch Name

1. We need to give the switch a name to differentiate it from other switches for management purposes.
2. NOT to be confused with their IP address.
3. The Switch name is only for reference purposes and does not take any part in the switching tasks for the device.

Passwords

1. Altering a switch's configuration could bring serious consequences
2. We need to protect switches' CLI from unauthorized access
3. To protect access to the Execution mode:
   - Console password
   - Line VTY password: for remote access (need ***login*** keyword and enable password)

4. To protect access to the Privilege Execution mode:
    - Enable password: plain text in configuration file
    - Enable secret password: encrypted in configuration file
    - Secret takes precedence if both are configured

Banner – Message of the Day

1. Displayed on terminal when accessing the Execution mode
2. Start with a special character (usually $ or &). This character will not show on the banner
3. End with the same character. This character will not show on the banner
4. The purpose of this message should be to display a security warning
5. DO NOT welcome the user in. This could be used as a justification to enter the CLI

Enable/disable switchports

In a Cisco switch, all switchports are enabled by default. It's good practice to shut down all unused ports (we won't be doing this on ALL lab sessions)

1. Go to interface configuration mode

   You can also configure a range of interfaces at once using the "range" command word
2. Disable → shutdown
3. Enable → no shutdown

Configuring VLAN Interfaces

NOTE: In this lab we will assume VLAN 1 is always the management VLAN. VLAN 1 is the default VLAN on Cisco switches, meaning all switchports belong to VLAN 1 by default.

1. Go to interface vlan configuration mode
2. IP address and network mask
3. Description

Validate Interface Status → the "sh ip int brief" command

1. Interface status

   Administratively down → disabled

   Down → enabled but not receiving electrical signal

   Up → enabled and receiving electrical signal
2. Protocol status

   Checks that Layer 2 specifications are correct on both ends of the connection. For Ethernet interfaces, all that's needed for the protocol to be in the UP status is that the interfaces on both ends are enabled, and that the UTP cable is in working order.

Switch console logging

Relevant activity in the switch is logged to a memory space that can be revisit for troubleshooting. However, when connected directly via console, these messages pop up on your screen as they are logged. The switch is "talking to you" and is useful to "listen" to it; it can help you identify potential issues earlier on.