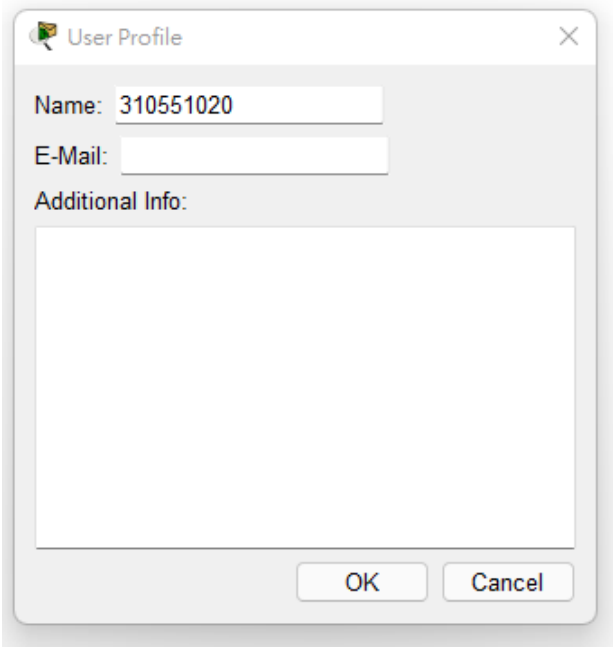
Midterm Exam

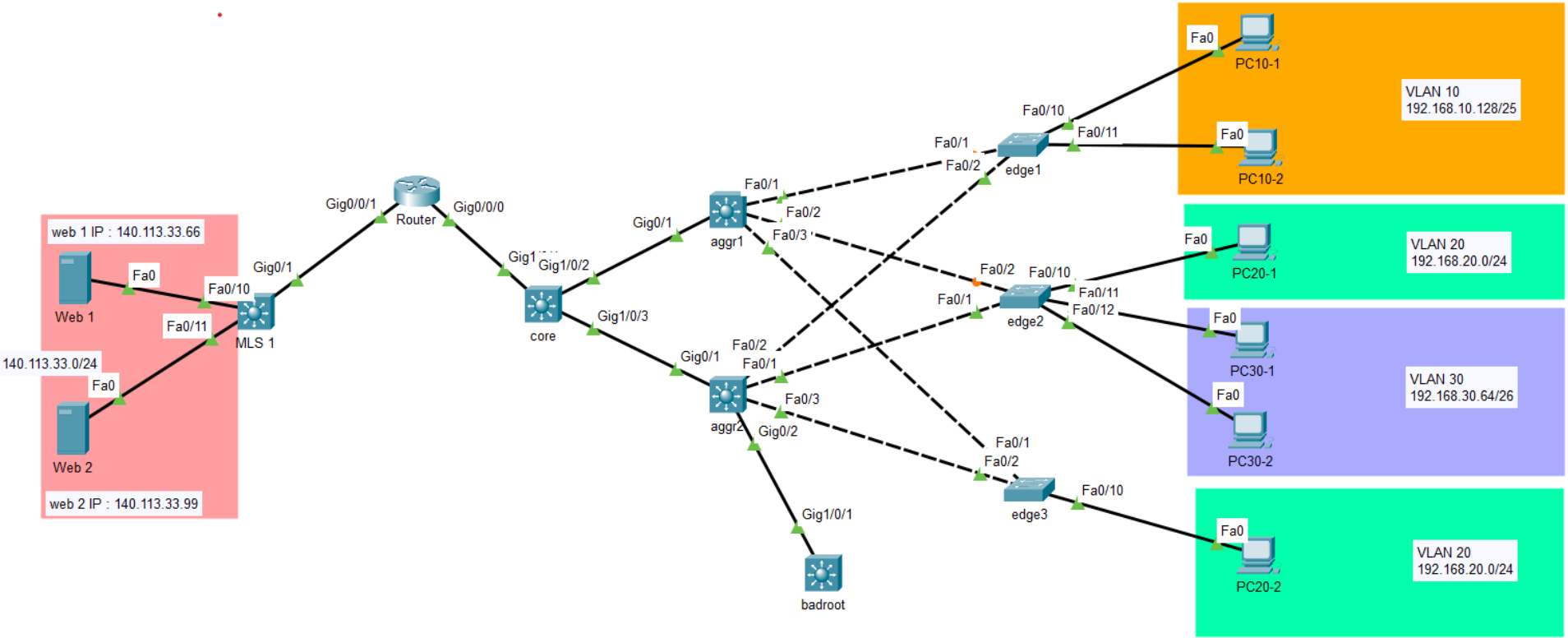
Requirements - Profile

- Fill your student ID to 「Name」 blank of prompt user profile.
  - E-Mail is not needed if you feel shy (?



Notice

- No need to configure **badroot** switch
- Do not remove static route on **MLS**, **Router** and **Core**
- Do not forget to save what you have done at all times to running-config
  - Make sure you save your configuration to both switches and PacketTracer
- Raise your hand if you meet any questions


web 1 IP : 140.113.33.66
Web 1
Fa0
Fa0/10
Fa0/11
MLS 1
Gig0/1
140.113.33.0/24
Fa0
Web 2
web 2 IP : 140.113.33.99
Gig0/0/1
Router
Gig0/0/0
Gig1
Gig1/0/2
core
Gig1/0/3
Gig0/1
aggr1
Fa0/1
Fa0/2
Fa0/3
Gig0/1
aggr2
Fa0/1
Fa0/2
Fa0/3
Gig0/2
Gig1/0/1
badroot
Fa0/1
Fa0/2
edge1
Fa0/10
Fa0/11
Fa0
PC10-1
Fa0
PC10-2
VLAN 10
192.168.10.128/25
Fa0/2
Fa0/1
edge2
Fa0/10
Fa0/11
Fa0/12
Fa0
PC20-1
VLAN 20
192.168.20.0/24
Fa0
PC30-1
Fa0
PC30-2
VLAN 30
192.168.30.64/26
Fa0/1
Fa0/2
edge3
Fa0/10
Fa0
PC20-2
VLAN 20
192.168.20.0/24

VLAN	Use for	Subnet
10	pc	192.168.10.128/25
20	pc	192.168.20.0/24
30	pc	192.168.30.64/26
87	mgmt	192.168.87.0/27
333	server farm	140.113.33.0/24

Requirements - VLAN

- Only trunk needed VLAN between two switches
  - VLAN 87 should also trunk between core to aggr1 and aggr1 to edge1
- Core to aggr* and aggr* to edge* should configure in trunk mode

Device	Interface	IP	Gateway
PC10-1	fa0	192.168.10.129/**25**	The third to last usable (exclude broadcast and subnet ID) IP address in the LAN
PC10-2	fa0	192.168.10.130/**25**	
PC20-1	fa0	192.168.20.1/**24**	
PC20-2	fa0	192.168.20.2/**24**	
PC30-1	fa0	192.168.30.65/**26**	
PC30-2	fa0	192.168.30.66/**26**	
Web 1	fa0	140.113.33.66/**24**	Already set
Web 2	fa0	140.113.33.99/**24**	

- Set Gateway IP of each VLAN as SVI on「**core**」

MGMT Setting

Device	IP
core	192.168.87.1/27
aggr1	192.168.87.2/27
edge1	192.168.87.3/27

- Set the above management IPs on Vlan 87 (SVI)

- Set hostname for every switch.
  - The hostname is shown on the topology under every device (lowercase)
- Add user **ccna-exam** on **core, aggr1, edge1**
  - Use **midterm** as password and encrypt it with **MD5**
- Set up ssh vty connection on **core, aggr1, edge1**
  - Use **cs.nycu.edu.tw** as domain name
  - ssh setting should be configured on all vtys
  - Modulus Bits: 2048
  - Use ssh version 2

Requirements - STP

- Please use **Rapid PVST** as STP mode
- Set vlan1, 10, 20, 30, 87 STP priority of **"core"** to **4096**
- Avoid the role of root switch (core) being robbed by badroot switch
  - Root guard configuration shouldn’t effect other switches except badroot
- Set portfast on the interfaces connected to end devices
- Prevent BPDU from entering the interfaces configured as portfast
  - Disable the interface if any BPDU enters it
  - Configuration should on interface not global

Before ACL

- Make sure all PCs should ping to each other success
- Make sure all PCs should ping to Web1、Web2 success

Requirements - ACL (1/2)

- Use single ACL to meet the each requirements below, no need for logging
- Configure standard ACL
  - Block **PC30-1** from getting out from vlan30
    - Configure as number **88** ACL on **core** , and finish it with **2** entries
    - Other PCs except PC30-1 shouldn’t be blocking
  - Only permit devices in vlan87 to connect to management IP of all switches with ssh
    - Configure as number **9** ACL on **all the vty** of switches, and finish with only 1 entry

Requirements - ACL (2/2)

- Use single ACL to meet the each requirements below, no need for logging
- Don not configure extended ACL on gi1/0/1
- Configure extended ACL
  - Block all devices in vlan10 to connect to **Web2** port 80 (www)
    - Configure as named ACL on **core**, name it with block-to-Web2 and finish with **2** entries
  - Block all devices in vlan20 to connect to **Web1** port 80 (www)
    - Configure as named ACL on **core**, name it with block-to-Web1 and finish with **2** entries

Hint

- Note: If you want to apply ACL on the interface with switchport function enabled, you need to apply ACL to the VLAN.
  - In packet tracer, interface with switchport function enabled can't be applied ACL directly

Submission (1/2)

- Open FileZilla
- Connect to sftp://140.113.168.201
    - Use username/password we gave

Submission (2/2)

- Make sure your remote path is /<username>
- Double click your local .pka file to upload
  - Filename: midterm_<student ID>.pka
  - Don’t upload other files