WEEKLY JOURNAL 1

Khoi Nguyen Pham

104772183

TNE10005 – Network Administration

Swinburne University of Technology -

I. Table of Contents

I. Table of Contents 2
II. Week 1 (29/07 – 04/08) 2
1. Key Concepts 2
2. Further Study 3
3. Key Configurations and Commands 4
III. Week 2 (05/08 – 11/08) 4
1. Key Concepts 4
2. Further Study 8
3. Key Configurations and Commands 8
IV. Week 3 (12/08 – 18/08) 9
1. Key Concepts 9
2. Further Study 11
3. Key Configurations and Commands 12
V. Week 4 (19/08 – 25/08) 13
1. Key Concepts 13
2. Further Study 16
3. Key Configurations and Commands 16

II. Week 1 (29/07 – 04/08)

1. Key Concepts

The first week of the unit was relatively comfortable, as we were mainly introduced to the unit outline, assessment criteria, expectations, and how we should navigate around the unit's Canvas.

We also began exploring different network devices. Firstly, I got to know some common media types, such as Copper (Unshielded/Shielded Twisted Pair, Coaxial Cable), Glass (Fiber Optic) and Wireless (Infrared, Bluetooth, Wi-Fi). I've also learned that there are two major problems in data transmission, which are attenuation, when signals gradually lose signal strength while traveling through a medium, and interference, when unwanted signals corrupt the original signal. Knowing these media types helps us design efficient and compatible network.

Since I've done Network and Switching before, I was familiar with devices like switches and routers, however this week's contents provide valuable insight on the functionality of these devices and introduced me to new devices as well:

- Repeater: Amplifies and regenerate signals to extend network distance.
- Hub: Broadcasts data to all connected devices.
- Bridge: Connects two network segments.
- Server: Provides services to computers on a network for file sharing, email, or web hosting.

Next, I was also reintroduced to both the OSI and the TCP/IP models. The OSI model has 7 layers with each layer responsible for specific functions that made up a structure framework. Each layer has its own Protocol Data Unit (PDU) and the corresponding devices.

1. Physical: Specifications of cables voltages. The PDU for this layer is Bit and Repeaters/Hubs operate on this layer.
2. Data-link: Reliable transit over physical link. The basic unit of data at this layer is Frame. Devices like bridges and switches function at this layer.
3. Network: Path selection between end hosts. The PDU at this layer is packet and Routers operate at this layer.
4. Transport: Reliable transit of data between end hosts. The PDU at this point is Segment.
5. Session: Establish, manage and terminate sessions between end hosts.
6. Presentation: Translate data formats.
7. Application: Network services to user.

The TCP/IP model is also a framework for understanding network communication. However, it simplifies and combines several OSI layers into fewer layers for more practicality:

1. Network Access: Combination of layer 1 and layer 2 in OSI model.
2. Internet: Layer 3 in OSI model.
3. Transport: Layer 4 in OSI model.
4. Application: Combination of layer 5, 6 and 7 in OSI model.

By mastering the layers of the TCP/IP and OSI models, organizations can effectively pinpoint network problems and successfully solve them.

Lastly, I had the chance to remind myself of some of the number systems, including binary, decimal, and hexadecimal, as well as remembering how to convert numbers between these systems.

E.g.:

- 111010 to decimal: $2^5 + 2^4 + 2^3 + 2^1 = 58$
- 1010 0101 to hexadecimal: (1010) (0101) = A5
- 13 to binary:
  - $13 > 2^3$ => 1 in that corresponding row.
  - $13 – 2^3 = 5 > 2^2$ => 1 in that corresponding row.
  - $5 - 2^2 = 1 < 2^1$ => 0 in that corresponding row.
  - $1 > 2^0$ => 1 in that corresponding row.
  - Therefore, 13 in binary is 1101.

2. Further Study

There’re still some problems in the Revision Quizzes that I have to work on. For instance, I don’t know how media types transfer their data, for example, Shielded Twisted Pair transfers with electrical impulses. Additionally, I haven’t memorized all of the ASCII characters. However, Daniel, my tutor, has a helpful technique for these exercises. He suggested counting the bytes, as each byte represents a character, and then we just have to compare them with the character count in the answer options.

To have a better foundation getting into this unit, I decided to read Chapter 2: The Protocol Suite of "The ABCs of TCP/IP" by Gilbert Held to have more detail function of each layer in both of the OSI and TCP/IP models.

3. Key Configurations and Commands

There was no lab for Week 1, so I proactively prepared and set up the required environments, such as Azure Labs, and carefully read through the Assessment Criteria.

III. Week 2 (05/08 – 11/08)

1. Key Concepts

Getting into Week 2, I have gotten to know some common topologies in networking:

- Bus Topology: A typical CSMA/CD topology. All devices are connected to the backbone. Wi-fi networks also use this.

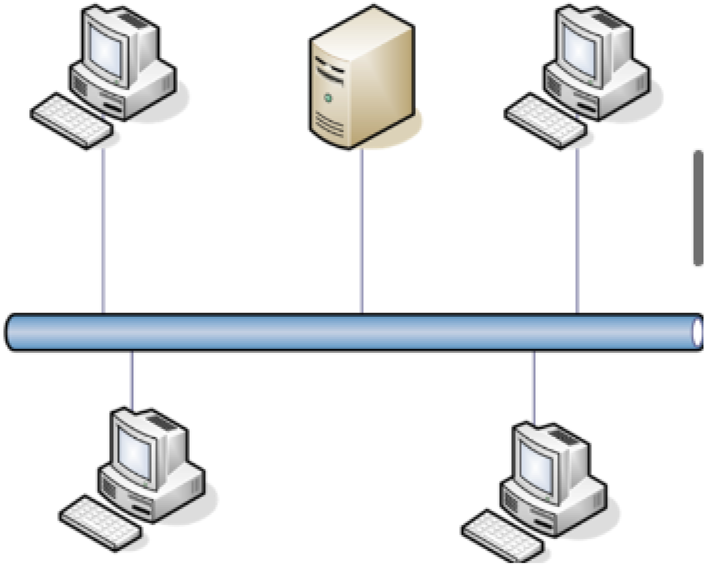


Figure 1. Bus Topology from Topic 1 Lecture 2

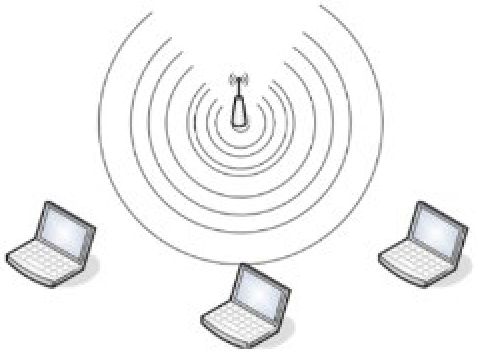


Figure 2. Bus Topology for Wi-Fi from [Topic 1 Lecture 2]

- Star Topology: All devices are connected to a central concentrator.

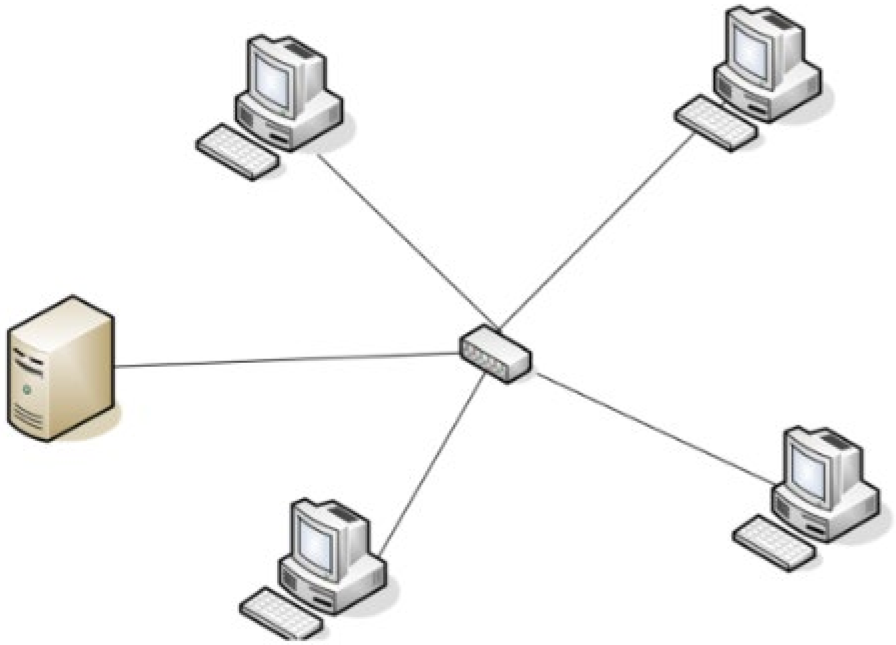
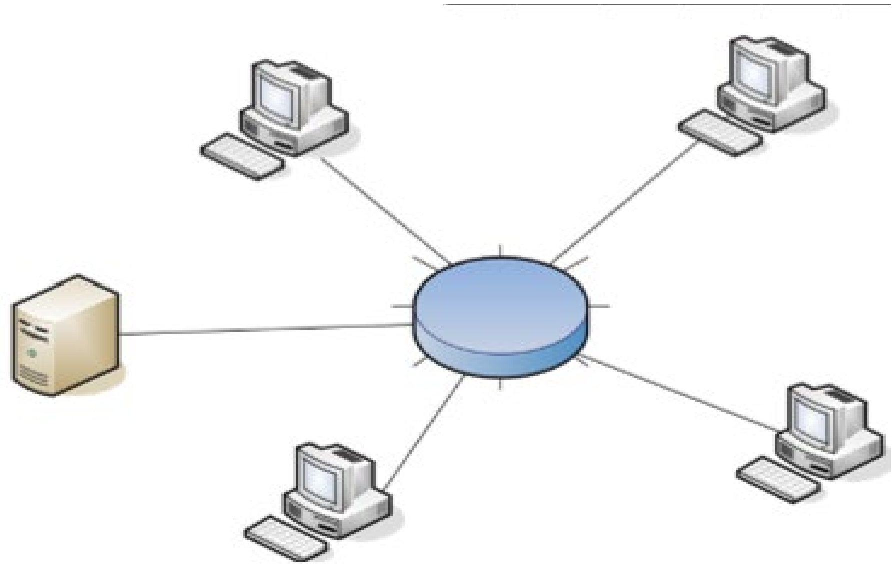


Figure 3. Star Topology from [Topic 1 Lecture 2]

- Ring Topology: All devices are connected to a central MAU or to other devices to form a ring. Used in undersea cables.



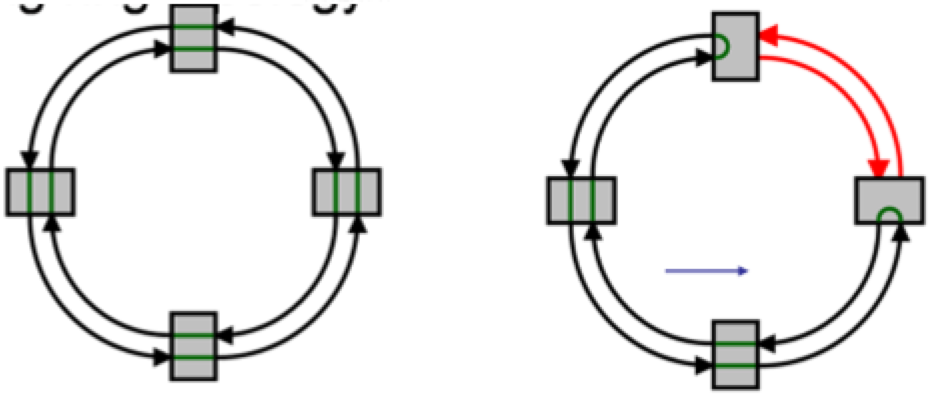


Figure 4. Ring Topology from Topic 1 Lecture 2

- Fully Meshed Topology: Has the best redundancy, however difficult and expensive to maintain. Therefore, organization tend to go for a hybrid approach.

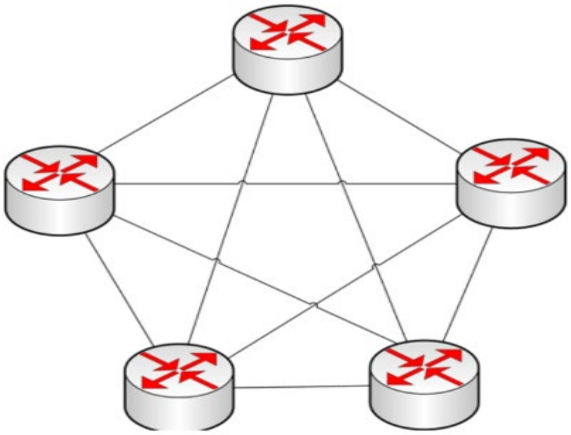


Figure 5. Fully Meshed Topology from Topic 1 Lecture 2

Understanding these network topologies can help organizations to improve performance while maintaining costs effectively.

I’ve also dived deeper into how the first three layers of the OSI model handle network addressing. For example, layer 2 employs physical addresses, which is basically MAC Address, and it is manufactured into devices, whereas layer 3 utilizes IP address, which is configured by the Network Administrator, and is used to group devices into sub-networks. The Address Resolution Protocol (ARP) enables the two layers to resolve each other.

Additionally, I’ve gained a deeper understanding of how the OSI model facilitates network communication. Specifically, I’ve known that encapsulation occurs at Layer 2, as it adds a header containing the MAC Address of communicating devices. Crucially, devices must be in the same subnet to communicate in the same LAN, hence an IP address and a subnet mask must be configured. However, in order to communicate with other subnets, a router must be utilized, and a default gateway must be configured. If communicating using a URL, a DNS server is also required.

I’ve also gotten reintroduced again to the components of an IP address, such as its 32-bit structure and the concepts of octets. I’ve also familiarized myself with the subnet mask, as it is used to enable the hierarchy and determine the network, sub-network and host portions of the IP address. It uses a combination of 1’s and 0’s to differentiate between network and host bits. The subnet mask can be written in dotted decimal notation (e.g., 255.255.255.0) or slash notation (e.g., /24).

E.g.:

- 192.168.1.0/16
    - Subnet Mask is 255.255.0.0
    - Network Address/Subnet ID is 192.168.0.0 by setting all host portion to 0.
    - Broadcast Address is 192.168.255.255 by setting all host portion to 1.
- 172.16.32.1/17
    - Subnet Mask is 255.255.128.0
    - Network Address is 172.16.0.0
    - Broadcast Address is 172.16.127.255

Understanding IP structures is crucial for effective network configuration, management, and troubleshooting.

Lastly, I’ve learned that there are specific ranges of IP addresses which are not available for general public use:

- Multicast: 224.0.0.0 – 239.255.255.255
- IETF research: 240.0.0.0 – 255.255.255.224
- Loopback Address: 127.0.0.1 – 127.255.255.255
- Universal Broadcast Address: 255.255.255.255
- Private IP Addresses:
    - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0 – 172.31.255.255
    - 192.168.0.0 – 192.168.255.255

This week’s lab content focused on introducing students to Network Administration using Hyper-V. I’ve got to know how to navigate and manage VMs’ properties, including RAM allocation, attaching hard disks to controllers, and connecting VMs to virtual networks. These are especially useful since they help us to identify and troubleshoot issues during practical scenarios.

Checkpoint was also introduced, as it allows us to save and restore VM states. Therefore, it is vital for efficient error recovery and troubleshooting. This means that without setting a checkpoint, all of my previous configuring will be lost and set back to default. Checkpoint can also be used as snapshots, as we can create multiple versions of a VM for testing or backing up data.

Finally, the lab also covered the functionality of routers, such as providing DHCP services and routing traffic. Routers are implemented everywhere in network infrastructure, since they enable communication between devices in various networks and locations.

2. Further Study

Since I've relatively familiarized myself with the contents of this week from Network and Switching, there's nothing particularly noticeable about the Revision Quizzes. However, I still want to strengthen my practical skills in IP addressing rules, so I've decided to do the Practice Questions provided on Canvas.

Besides, I want to extend my knowledge on Networking Protocol, so I decided to read Chapter 4: The Internet Protocol and Related Protocols of "The ABCs of TCP/IP" by Gilbert Held

3. Key Configurations and Commands

There's a crucial configuration that I need to remember is how to change the IP address and the subnet mask of the VM:

In the ***Server Manager Window*** of the VM, click ***Local Server*** in the left pane. Below the ***Properties*** section, click the hyperlink next to ***Ethernet***. This will open the ***Network Connections*** window. There I need to right click ***Ethernet*** and select ***Properties***. Finally, click on ***Internet Protocol Version 4 (TCP/IPv4)***, select the ***Properties*** button, and now I can configure the addresses.

There are some commands which are essential to effectively navigate and manage the system:

- ***ipconfig***: Displays network configuration information such as IP address, subnet mask, default gateway, and DNS server addresses.
- ***ipconfig /all***: Displays all network configurations including MAC address, DHCP server information, and DNS suffix.
- ***arp -d***: Deletes all entries from the ARP cache.
- ***arp -a***: Displays the current contents of the ARP cache, showing IP addresses and their corresponding MAC addresses.

IV. Week 3 (12/08 – 18/08)

1. Key Concepts

Coming into week 3, I've gained a solid foundation for the TCP/IP Model and how each layer functions. This week's content specifically gave us a broader view of each layer's protocols.

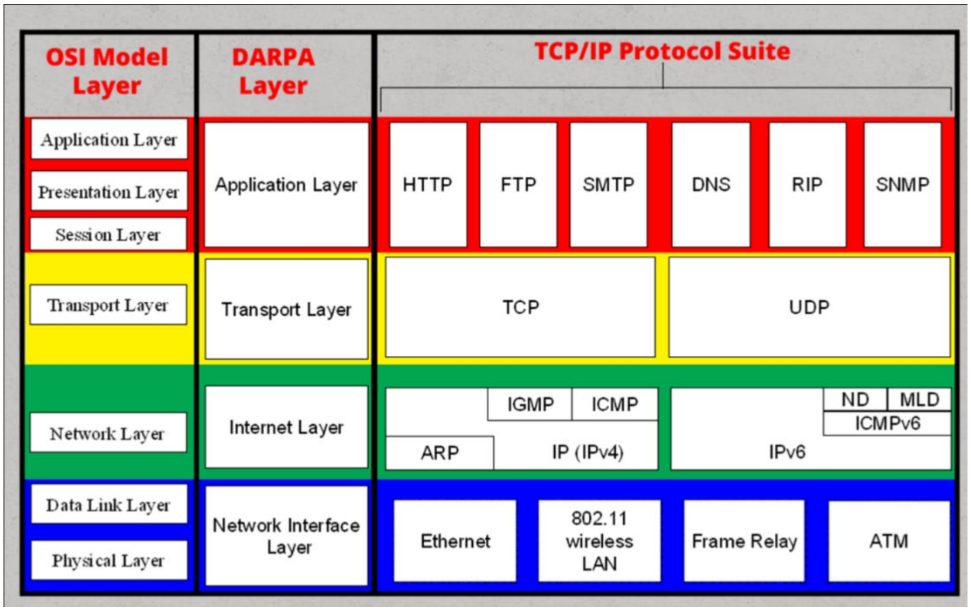


Figure 6. Each layer's protocols from Topic 1 Lecture 3

There are some familiar protocols that I've already encountered either in previous lectures, such as IPv4, IPv6, and ARP, or in Network and Switching, like, TCP, UDP, Ethernet and 802.11. However, there are additional protocols that I need to remember as well:

- IMCP: Reports error and control messages.
- Frame Relay and ATM: Legacy protocols.

Especially, I have to memorize the port numbers of the Application Layer's protocols:

- HTTP: TCP port 80
- FTP: TCP port 21
- SMTP: TCP port 25
- DNS: UDP port number 63
- RIP: UDP port 520
- SNMP: UDP port 161

Remembering these port numbers can benefit network administrators as they can effectively configure firewalls and develop better network applications.

I've always wondered how each independent layer determines the appropriate protocol to deliver to, and the week's material answered it perfectly by introducing us to the definition of a socket. A socket is a combination of an IP address, a transport protocol, and a port number. These configurations with the port numbers ensure security for the network.

I've also reintroduced how Network and Host portion contribute to IP addressing. Specifically, the Network portion represents the specific network that all devices belong to, whereas Host portion identifies a specific device in that network, and it must be unique.

Furthermore, I've learn that IP addresses are divided into classes of different sizes:

- Class A: Used for large networks since it has up to 2^{24} host bits.
- Class B: Used for medium-sized networks and it has 2^{16} host bits.
- Class C: Used for small networks as it only has 2^{8} host bits.
- Class D and E are reserved for specific purposes and are not available to use.

Nowadays, we no longer use Classful Addressing since we ran out of them decades ago, hence we use CIDR. However, understanding them can still be beneficial for network design and troubleshooting.

Besides, I've gained basic understanding of basic subnetting, and the concept of "borrowing" bits and it is called "Multiple Subnet Network". For example, if there are 4 subnets, then I have to borrow 2 bits since 2 bits can create up to 4 subnets.

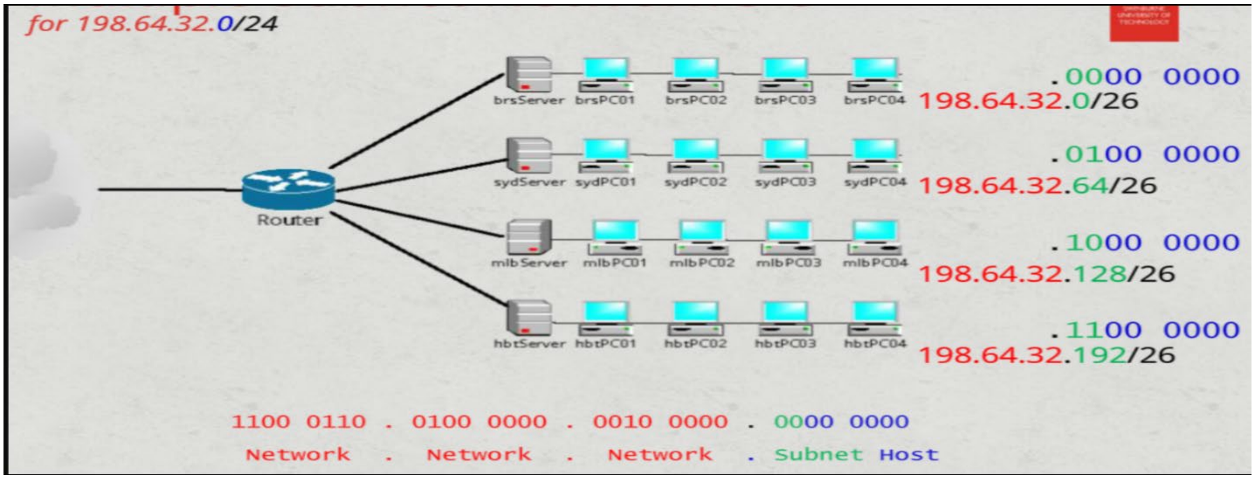


Figure 7. Multiple network subnetting from Topic 1 Lecture 3

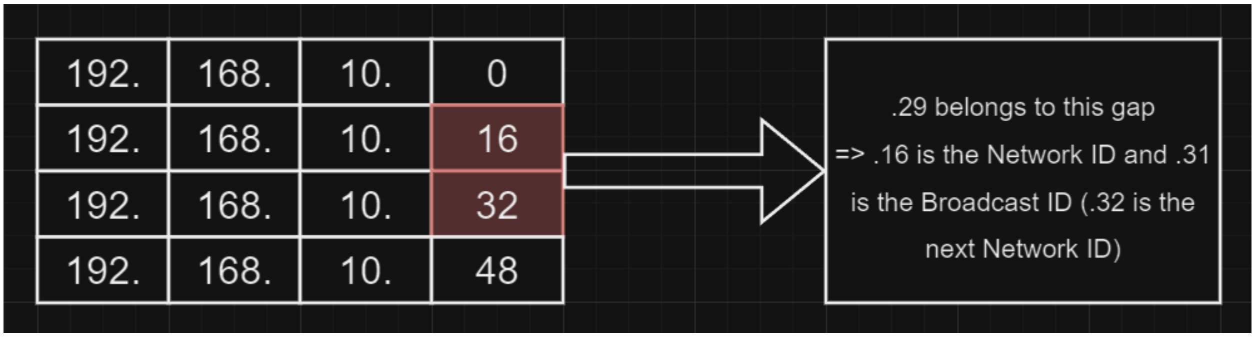
There are several benefits to Multiple Subnet Network compared to Single Subnet. Firstly, we can use a single network address for multiple locations. Besides, network congestion is reduced by segmenting traffic. And lastly, we can apply better security by using firewalls to separate subnets.

Lastly, I got introduced to a new method of finding the Network/Broadcast Address, by finding the gap between the networks.

E.g.: 192.168.10.29/28

- The dotted-decimal value of /28 is 255.255.255.240

- If the octet is not 255, take 256 – 240 = 16 => this is the gap between the networks.



192.	168.	10.	0
192.	168.	10.	16
192.	168.	10.	32
192.	168.	10.	48

.29 belongs to this gap => .16 is the Network ID and .31 is the Broadcast ID (.32 is the next Network ID)

Figure 8. Drawn in draw.io

This is definitely a quicker and easier way to find the Subnet/Broadcast Address, and it is especially helpful when it comes to determining whether two addresses are in the same subnet or not.

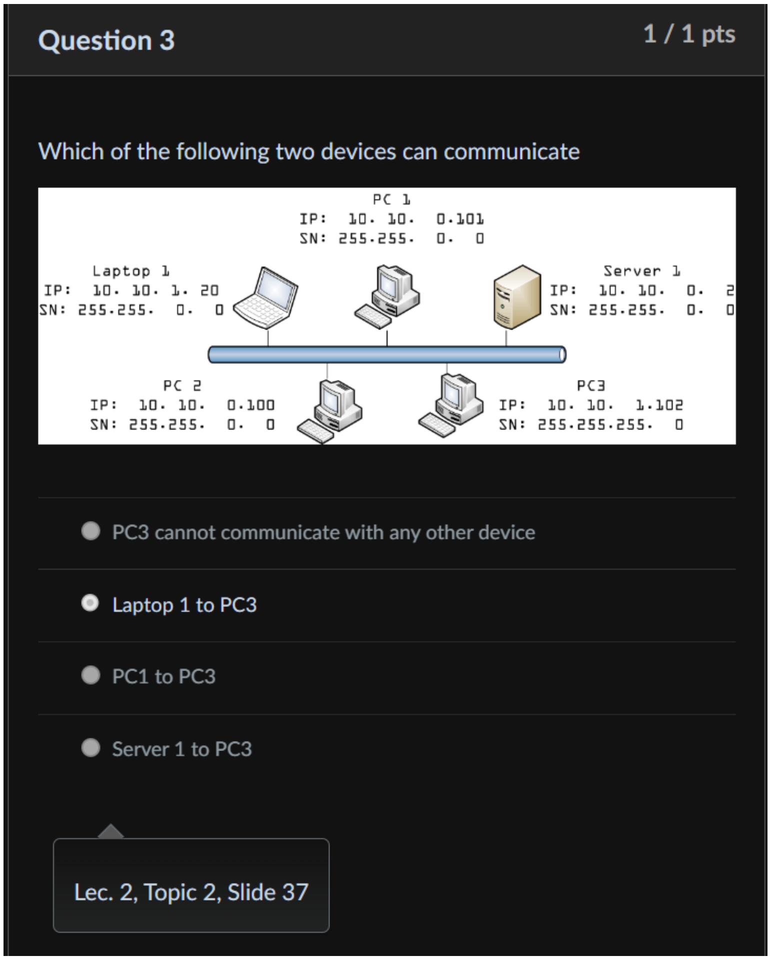
This week’s lab focused on helping us practice and understand network communication among VMs connected to the same and different switches. Specifically, we were instructed to ping around devices from the same switch first, then change it to another switch and try again. This time, a software-based router (sWin22RTR) is needed for layer 3 communication. Pinging is an effective way to determine if the devices can communicate with each other, hence there are no errors during configuration.

I’ve also learned to configure a VM to obtain IP settings from the deployed DHCP servers in the unit labs. To do that, we have to use Windows Powershell in administrators mode. DHCP automatically assigns IP addresses, therefore eliminating the need for manual configuration as well as reducing human errors.

2. Further Study

The concept of subnetting is nothing new for me, since I’ve done VLSM (Variable Length Subnet Mask) in Network and Switching before. However, I still want to further solidify this skill in order to get ahead of this unit. Therefore, I’ve looked back again the method of VLSM in the previous unit and strengthen my knowledge by reading and doing exercises in Chapter 3: Subnetting and VLSM of 1,001 CCNA Routing and Switching Practice Questions for Dummies by Glen E. Clarke.

There are some challenging questions related to communication between devices in this week’s Revision Quizzes. The first question focused on frame source and destination addresses. Specifically, during intra-device communication, the source/destination IPs remain the same, whereas the source/destination MACs change based on the receiving device’s network interface. The second question related to communication between devices in a Bus topology:



Question 3 1 / 1 pts

Which of the following two devices can communicate

○ PC3 cannot communicate with any other device

◉ Laptop 1 to PC3

○ PC1 to PC3

○ Server 1 to PC3

Lec. 2, Topic 2, Slide 37

Figure 9. Question from Lecture 02 Revision Quiz

In this topology, laptop 1 is able to communicate with PC3 even though it looks like that they are not in the same subnet. However, to determine this, we have to check if the device's network mask can see other devices in the same subnet.

- Laptop 1's Network ID when compared to its own subnet mask is 10.10.0.0
- PC3 "sees" laptop 1 by comparing its IP address with laptop 1's subnet mask, therefore PC3's network ID is also 10.10.0.0
- It's the same the other way around, where both of their network ID when compared to PC3's subnet mask is 10.10.1.0

3. Key Configurations and Commands

I've learned some common command-line tools used for troubleshooting network connections on Window systems.

- ***Arp***: Allows to view and modify ARP cache, as well as mapping IPv4 addresses to their corresponding MAC addresses.
- ***Hostname***: Displays the hostname of the computer

- ***Netsh***: Allows you to manage network interfaces, routing tables, DNS clients, and other network components.
- ***Netstat***: Displays active TCP, UDP, information about listening ports, established connections, and connection states.
- ***Nslookup***: Queries a DNS server to resolve domain names to IP addresses as well as helps verify DNS configurations and troubleshoot DNS-related issues.
- ***Ping***: Test connectivity.
- ***Route***: Displays and modifies the IPv4 routing table.
- ***Tracert***: Traces the route a packet takes to reach a destination host and its IP addresses.
- ***Pathping***: Combines the functionality of ping and tracert and display network latency and packet loss for each hop in the path.
- ***netsh interface ip set address Ethernet dhcp:*** Obtain IP address from DHCP Server.

V. Week 4 (19/08 – 25/08)

1. Key Concepts

In this week's lecture, I've dived deeper into the concept of calculating Subnet Addresses. I've learned that there are key differences between determining subnet addresses and host addresses.

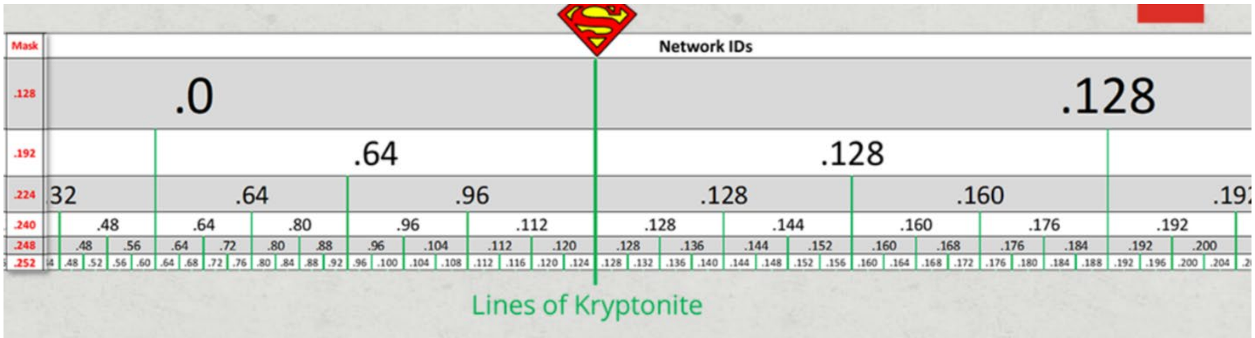
- When determining subnet addresses, I have to use the formula 2^n , where n represents the number of bits reserved for the subnet mask.
  E.g.:
  - 40 locations = 40 subnets required.
  - 2^5 = 32 subnets (not enough).
  - 2^6 = 64 subnets => 6 bits are required.
- When determining host addresses, I have to use the formula 2^n - 2.
  E.g.: For subnets with 64 hosts, we need 7 bits.
  - 2^6 – 2 = 62 hosts (not enough).
  - 2^7 – 2 = 128 hosts => 7 bits are required.

However, the subnetting method we got introduced this week and last week is fixed length, meaning all subnet masks have to be the same. This can lead to inefficient use of IP addresses, especially in networks with varying sizes and densities. For example, a large subnet with few active devices may waste IP addresses, while a small subnet with many active devices may run out of addresses quickly.

Therefore, the concept of Variable-length subnet masking (VLSM) is introduced, as it offers more flexibility by optimizing the number of hosts in different subnet sizes. It also means that the subnet mask will be different during the subnetting process.

I've also understand the concept of Supernetting. Basically, it's a technique used to aggregate multiple class C networks into a single larger network. Since class C networks are in small size, but it's also the cheapest to obtain, people have utilized Supernetting to reduce the number of routing entries required to manage a network.

Subnets chosen for Supernetting must be adjacent and consolidate within upper boundaries:



Mask	Network IDs
.128	.0 .128
.192	.64 .128
.224	32 .64 .96 .128 .160 .19
.240	.48 .64 .80 .96 .112 .128 .144 .160 .176 .192
.248	.48 .56 .64 .72 .80 .88 .96 .104 .112 .120 .128 .136 .144 .152 .160 .168 .176 .184 .192 .200
.252	4 .48 .52 .56 .60 .64 .68 .72 .76 .80 .84 .88 .92 .96 .100 .104 .108 .112 .116 .120 .124 .128 .132 .136 .140 .144 .148 .152 .156 .160 .164 .168 .172 .176 .180 .184 .188 .192 .196 .200 .204 .2

Lines of Kryptonite

Figure 10. Supernetting table from Topic 1 Lecture 4

E.g.:

- 192.168.1.80/28 and 192.168.1.64/28 consolidate to 192.168.1.64/27
- 192.168.3.112/28 and 192.168.3.128/28 do not consolidate to anything, since they are on different sides of the "Lines of Kryptonite".

We've also have a deeper understanding of DHCP's benefits, and some of its configurations. DHCP allows better efficiency and flexibility by automatically obtaining IP addresses, hence it is helpful in eliminating risks and working at numerous branches.

DHCP Authorization is a mechanism used to control and ensure that online authorized devices are allowed to obtain IP addresses from the server. This is one of the implemented features since Window Server 2016 as it helps to reduce security problems and reduce troubleshooting efforts.

I've also gained more insight during the process of DHCP address assignment, and it's called DORA:

1. Discover: A DHCP client broadcasts a DHCP Discover message to request an IP address.
2. Offer: A DHCP server replies with a broadcast DHCP Offer message. The respond also offers the lease time to let the client know when it can use the assigned IP address.
3. Request: If satisfied with the IP address and the lease time, the client broadcasts a DHCP Request message to confirm.
4. Acknowledge: The DHCP server sends a DHCP Acknowledge message to confirm and assign the address to the client.

The clients normally try to renew the lease using a unicast DHCP Request every time it starts up. This is called DHCP Renewal, and it ensures that the device can obtain the same IP address and avoid interruptions in network communication without having to go through the entire DORA process again. Therefore, if there are too many broadcast messages, we have to check whether there's something wrong with the DHCP server. By understanding DORA and the concept of DHCP Renewal, I can be more efficient in troubleshooting DHCP issues, configuring and securing networks.

DHCP scopes are crucial in DHCP configuration. A scope is a range of IP addresses that a DHCP server can assign to clients on a network. All addresses in that range must come from the same subnet, and a server can have many scopes. This helps organizations to organize and manage IP address allocations easier and more efficiently.

DHCP Relay Agent is a mechanism to support clients in remotely finding the correct DHCP scope to obtain the address and it is normally configured at routers. It acts as a "man in the middle" between clients and servers by capturing the broadcast messages from the client and then unicast them to the DHCP server. After that, the relay agent receives the respond from the server and broadcast back to the DHCP client. DHCP Relay Agent offers many benefits including better management, scalability and security. For example, we can configure relay agents to filter DHCP requests to prevent unauthorized devices from obtaining IP addresses.

DHCP exclusion and reservation are essential features used to control IP addresses within DHCP scopes. Exclusion ranges are reserved for specific purposes and can't be obtained by the DHCP server. This is useful for reserving static IPs used by non-DHCP clients. On the other hand, DHCP reservations are used to allocate the same address to a device based on its Mac Address. By using both features, network administrators can effectively control IP address allocation and prevent conflicts between devices.

DHCP options can be provided for DHCP server to determine the applied range and network setting. We can apply DHCP options at various levels, such as server, scope and reserved client so that network can be customized based on specific requirements.

Lastly, the network normally has 2 DHCP servers to ensure redundancy, hence if one DHCP server fails, the other one can immediately take control. If they are assigned with the same address, the 50/50 rule is applied for DHCP servers on the same network segment, and 80/20 rule is applied for the second server which is DHCP relay.

In this week lab, we had the chance to observe how subnet mask and default gateway work in practical scenarios. For example, sWin10PC201 couldn't ping sWin22SVR3 because they were in different networks, and sWin10PC201 hasn't been assigned a default gateway. In this scenario, the default gateway of sWin10PC201 should be the router's IP, which is sWin22RTR's.

As for the subnet mask, I observed the functionality of it by configuring the setting shown in this topology:

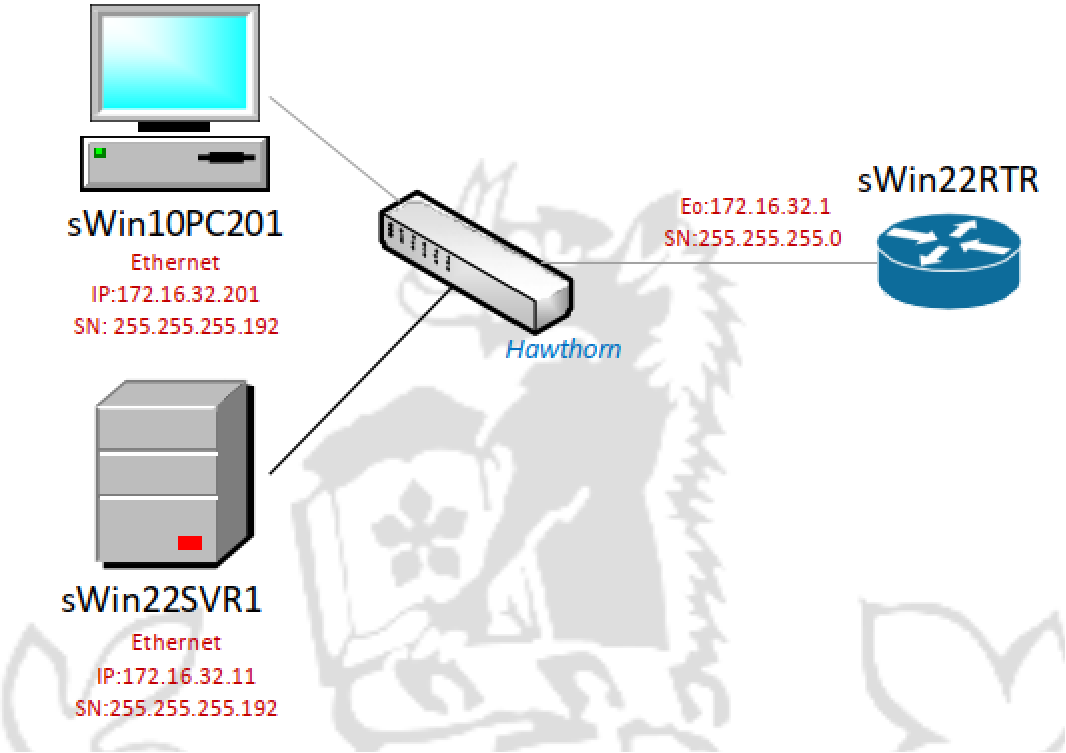


Figure 11. Topology in Lab 3

Even though sWin22SVR1 and sWin22RTR have different subnet masks, they can still ping each other unlike sWin10PC201. This is because both switches “see” each other with the same subnet ID, by comparing its own subnet mask with both IPs, hence communication works.

I also got to observe how an ARP table is constructed. Every time I successfully pinged a new address inside the network, an entry for that address was added to the ARP table, therefore it will resolve the IP address by mapping it to the corresponding MAC address of the device. However, when pinging a device outside the network, we need to access the router, therefore the ARP table contains the MAC address of the default gateway.

2. Further Study

This week’s Revision Quizzes are relatively easy, as I only made mistake on the port numbers of TCP protocols, hence I need to memorize those more thoroughly. I’ve decided to read Appendix C: Port Numbers from “The ABCs of TCP/IP” by Gilbert Hild to know some new protocols and their corresponding port numbers.

3. Key Configurations and Commands

The only noticeable configuration of this week’s lab is to configure the default gateway, which can be accessed in the same way we change the IPs.