WEEKLY REPORT

Network Administration

APRIL 27, 2024

SWINBURNE UNIVERSITY OF TECHNOLOGY

Tran Anh Thu Pham
103818400

WEEKLY JOURNAL 2

(week 5 and week 6)

Table of Contents

Week 5

➢ Key concepts

DNS (Domain Name System) resolves domain names to IP addresses. For example, www.swin.edu.au will be resolved to 136.186.1.10 by DNS. **DNS** is a global distributed database and one of its main functionalities is resolving FQDNs to IP addresses and resolving IP addresses to host names. Additionally, DNS locates domain controller, global catalogue server and email server during email delivery.

FQDN (Fully Qualified Domain Name) is formed: <Host Name>.<Domain Name>.<Top-level Domain>. E.g. mymail.swin.edu.

DNS zone is a specific portion of DNS namespace that contains **DNS records**. Here are the main characteristics of DNS Zone:

Zone focus: Forward lookup zone or Reverse lookup zone
Zone type: Primary zone, Secondary zone and Stub zone
Zone Storage: Text and Active Directory Integrated.

Records can only be created in the Primary zone. Resource records in **forward lookup zones** include: SOA, A, AAAA, NS, CNAME, MX, SVR
In **reverse lookup zone** include**:** PTR

Here are DNS record types and their description:

Record	Description
SOA	Identifies the **start of a zone** of authority
A	Maps an FQDN to an **IPv4** address
AAAA	Maps an FQDN to an **IPv6** address
NS	Indicates the **name server** that is authoritative for a zone
PTR	Maps an IP address to an FQDN for **reverse** lookups
CNAME	Specifies an **alias**
MX	Specifies a **mail exchange** server for a DNS domain name
SRV	Specifies the IP addresses of servers for a specific **service**

DNS Queries are initiated by DNS servers and DNS clients and they can be recursive or iterative. To differentiate these 2 queries, these 2 situations can be referred.

When the client tells the DNS resolver: “Hey, I need the IP address for this domain, please look for it and do not get back to me until you can find it.” → **Recursive.**

When the client tells the DNS resolver: “Hey, I need the IP address for this domain, please give me the address of the DNS server in the lookup route so I can look up it by myself.” → **Iterative.**

The query specification is in Fig. 1 below.

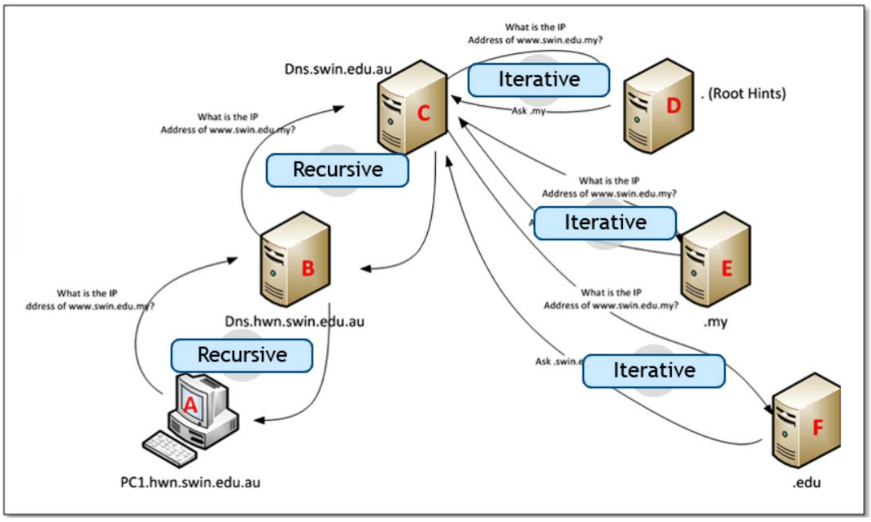


Fig. 1 DNS query types specifications

The process of a DNS resolution follows these steps:

- Step 1: When the domain name is entered into a browser, the browser sends recursive DNS query to find out which IP address the domain corresponds to.
- Step 2: If the recursive resolver has the address, it will return that IP address to the client.
- Step 3: If it can not find the IP address, it will send out the queries to other servers in the order: DNS root name server → top-level domain (TLD) name server and authoritative name servers. These server types will work together to find the IP address.
- Step 4: If it still can not find the IP address, it will return an error message.

In computer networks, there are some primary **Server Roles**: File Server, Print Server, Web Server, Application Server, Database Server Server and Domain Controller.

➢ Innovative ways to address business needs

DNS Spoofing is an attack to manipulate the DNS resolution process. In the DNS spoofing process. The attacker modifies the DNS response to direct the users to the malicious website instead of the legitimate To do this, the attacker finds the vulnerabilities in the DNS server and injects the false DNS records into the DNS cache.

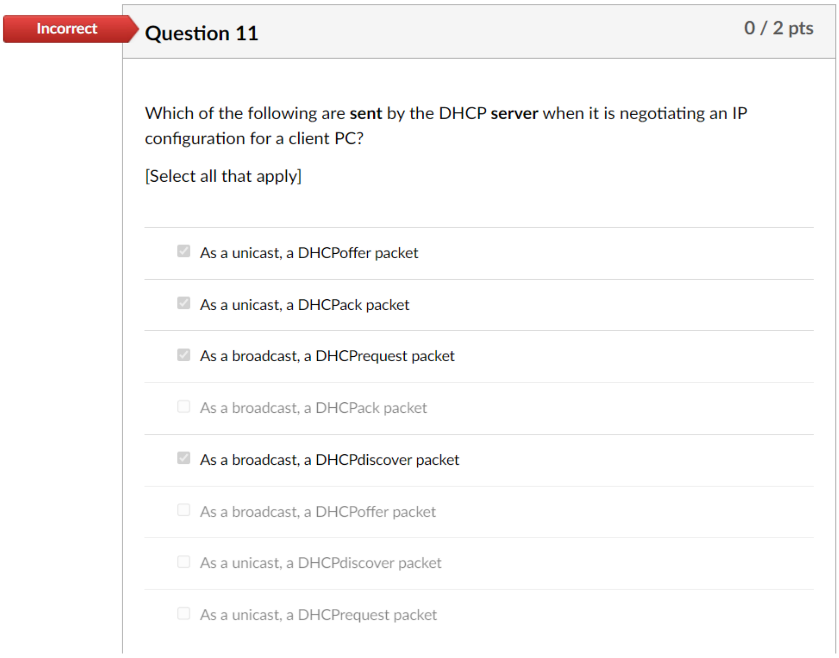
There are some solutions to address this attack:

Randomized source ports used in DNS queries can be implemented to make it more difficult for the attacker to guess and inject the malicious response.

An Intrusion Detection System (IDS) should be employed to identify any unusual DNS traffic patterns or abnormal DNS responses which can lead to DNS spoofing process.

Reflection and plan for further study

Remember the 4 steps of DHCP connection is important; however, it is even more important to be mindful of the type of transmission. In this case, I forgot that in DHCP progress, all the transmissions are broadcast.



Incorrect

Question 11

0 / 2 pts

Which of the following are **sent** by the DHCP **server** when it is negotiating an IP configuration for a client PC?

[Select all that apply]

☑ As a unicast, a DHCPoffer packet

☑ As a unicast, a DHCPack packet

☑ As a broadcast, a DHCPrequest packet

□ As a broadcast, a DHCPack packet

☑ As a broadcast, a DHCPdiscover packet

□ As a broadcast, a DHCPoffer packet

□ As a unicast, a DHCPdiscover packet

□ As a unicast, a DHCPrequest packet

Fig. 2 question related to the DHCP server process

To not answer this question incorrectly next time, I view the theories of the weekly pre-recorded lecture again and DHCP lecture notes.
Up to this week, there are more and more theories so I need to review all the Slides quizzes and Revision quizzes once a week.

Key configurations and commands

In this week's lab, the installation and configuration of **DHCP** are completed for multiple aspects such as **Scopes**, **Exclusions**, **Reservations** and **Options**.

At the PowerShell terminal of the DHCP client, run the command below to allow the assignment of DHCP:

```
Set -NetIPInterface -InterfaceAlias Ethernet -dhcp enabled
```

To verify the assignment, type: **ipconfig /all**
In it appears: *DHCP: enabled* → successful configuration.

To install DHCP in **Server Manager,** the steps below should be followed:

- Step 1: Select **Add Roles** in **Manage** menu.

- Step 2: To install the local server, click **Next** three times and stop at **Select server roles** section
- Step 3: Tick the check box of **DHCP Server.** Click **Add Features** button. Then click **Next** three times.
- Step 4: Click **Install** to install DHCP.

After installing DHCP server role, it is mandatory to configure the new role (notice the yellow triangle alert appears). The next step is clicking on Complete DHCP configuration and what the server is authorized based on the network environment. On the **DHCP Post-install configuration wizard → Next → Commit → Close.**

To **create a Scope**, some steps need to be followed:

- Step 1: In **Server Manager** → **Tools menu** → **DHCP**
- Step 2: Click on the server name to expand the sub-containers → **IPv4 →**
- Step 3: Click **Next** → enter the name for the scope.
- Step 4: Click **Next** → enter the values on the **IP Address Range page**.
- Step 5: Click on the **Scope** icon → right click the **Scope** icon → **Activate →** The red arrow and blue exclamation mark should have now disappeared.
- Step 6: Click on the server name to expand the sub-containers → **IPv4 →**
- Step 7: Click **Next** → enter the name for the scope and stop the service of any other server by clicking on the name of that server in DHCP console → **All Tasks → Stop.**

To **test the DHCP server**, go to one of the PCs in the network. In Powershell and do the following steps:

- Step 1: Release the existing leased IP address. Type: **ipconfig /release** → enter
- Step 2: Obtain a new IP address. Type: **ipconfig /renew** → enter

To **Configure Exclusions**, some steps need to be followed:

- Step 1: In the **DHCP management console** of the server → expand the scope → right click on the **Address Pool** container → **New Exclusion Range**
- Step 2: Enter the **Start IP address** value and **End IP address** value → **Add**

To test the Exclusive range, do the same steps with **Test the DHCP server** section above.

To **Configure a Reservation**, some steps need to be followed:

- Step 1: In the **DHCP management console** of the server → expand the IPv4 and Scope containers → right click on **Reservations → New Reservation**.
- Step 2: Enter the name of the PC is required to be reserved with the IP address for it and also remember to enter the MAC address value of that PC (

to find the MAC address of the PC, type: **ipconfig /all** in the Powershell terminal of the PC required to be reserved.

To test the Reservation, do the same steps with **Test the DHCP server** section above.

DHCP Options can be applied at multiple levels: **Server**, **Scope** and **Reservation.** Do the same steps in configuring Reservation above → Select **Configure Options** → Choose the appropriate options in the **Options dialog box:**

Option code	**Name**
003	Router
004	Time Server
005	Name Servers
006	DNS Servers
12	Hostname
015	DNS Domain Name
031	Perform Router Discovery

Here are some commands to troubleshoot configuration issues: **nslookup, ipconfig, resolve-DnsName, nslookup, DNSCmd.**

Week 6

➢ Key Concepts

In a network, all resources are shared on the server and controlled by the server. In a **Workgroup**, a PC sharing a resource acts as a client and a PC that accesses to the shared resource acts as a client.

Domain Controller is responsible for authenticating users, computer accounts and authorizing access to the resource.

There are three options for **installing a Domain Controller: Add a DC to an existing domain**, **Add a new Domain to an existing Forest** and **Add a new Forest**.

All objects and records in one Domain Controller in the **Active Directory Domain** are backed up automatically because they are replicated to the other Domain Controller. This is called **Multi-master Replication**.

User account is the one for user to logs on to a Windows network and **computer account** is the one for a computer to connect to a Windows domain. To be more specific, **User account** is used for control access to the computer and objects on a computer such as files, folders, printers, etc.

> If someone want to log onto the computer using a user account, they must enter the password which is used for user **authentication**.
> **Authorisation** is the process of allowing access control of the specific user to specific objects.
>
> Every user account has a **Security Identifier** (SID) which is used every time a user accesses an object. **SID** is contained in the **access token** which is generated when a user logs onto a system.

When a user tries to access an object, the SID in the Access Token is compared against the ACE's in the **Discretionary Access Control List** (DACL). If there is a match, the decision to permit the user access to the object is made. If no match is made, the user is denied.

It is not good to let the **Everyone group be automatically assigned to the Read permission** and it should set the maximum number of users who have permission to access the shared resource. NTFS has access control to set specific users' permission.

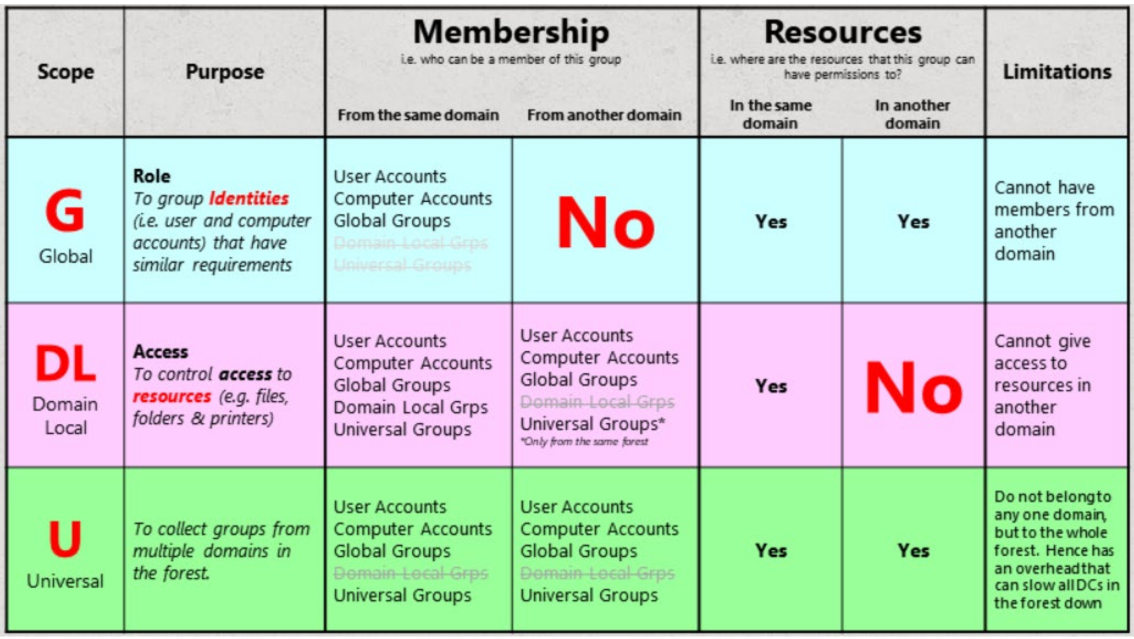
The table below identifies the basic NTFS permission:

Permission	Folder permission	File permission
Full control	• Modify the folder permission and take ownership of the folder • Delete everything in the folder • Perform all actions associated with all other NTFS folder permissions	• Modify the file permission and take ownership of the file • Perform all actions associated with all other NTFS file permissions
Modify	• Delete the folder • Perform all actions associated with the Write and the Read & Execute permissions	• Modify the file and delete the file • Perform all actions associated with the Write and the Read & Execute permissions
Read and Execute	• Navigate through restricted folders to reach other files and folders • Perform all actions associated with the Read and List Folder Contents permission	• Perform all actions associated with the Read permission • Run applications
List Folder Contents	• View the names of the files and sub-folders in the folder	
Read	• See the files and sub-folders in the folder • View the folder's ownership, permission, and attributes	• Read the file's contents • View the file's ownership, permission, and attributes
Write	• Create new files and subfolders inside the folder • Modify the folder attributes • View the folder's ownership and permission	• Overwrite the files • Modify the file attributes • View the file's ownsership and permissions

There are some network terminologies:

- **Forest**: a collection of AD DS domains that are bound by automatically created **two-way trust** relationships.
- **Domain**: a logical **administrative unit** that is the home for users, computers, and other objects.
- **Tree**: a collection of AD DS domains that share a **common root** domain and have a **contiguous namespace**.
- **Organisational Unit**: a container within a domain that organizes users, computers and other OUs.

The Fig. specifies the Group Scopes for Network Admin. The strategy to be more easier to remember: **I → G → DL ← A.**



Scope	Purpose	Membership i.e. who can be a member of this group		Resources i.e. where are the resources that this group can have permissions to?		Limitations
		From the same domain	From another domain	In the same domain	In another domain	
G Global	**Role** *To group **Identities** (i.e. user and computer accounts) that have similar requirements*	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ ~~Universal Groups~~	**No**	**Yes**	**Yes**	Cannot have members from another domain
DL Domain Local	**Access** *To control **access** to **resources** (e.g. files, folders & printers)*	User Accounts Computer Accounts Global Groups Domain Local Grps Universal Groups	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ Universal Groups* **Only from the same forest*	**Yes**	**No**	Cannot give access to resources in another domain
U Universal	*To collect groups from multiple domains in the forest.*	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ Universal Groups	User Accounts Computer Accounts Global Groups ~~Domain Local Grps~~ Universal Groups	**Yes**	**Yes**	Do not belong to any one domain, but to the whole forest. Hence has an overhead that can slow all DCs in the forest down

Fig. 3 Group scopes and its features in active directory

Innovative ways to address business needs

In the real business world, one of the common scenarios is sharing the sensitive documents of the corporation. For instance, the folder on a Windows computer called *FinanceDocs.* This folder needs to be restricted access and only authorize users can view and modify the files within it. Here is how NTFS permission is applied:

- Finance Team: Members of this group must be given **Read and Write permissions**, allowing them to view and modify the documents.
- Managers: Members of this group must be given **Full Control permission**, allowing them not only to view and modify the documents but also to change the permission of other users.
- Other departments are only allowed to view the documents but not make any changes so they must be given **Read permission**.

Reflection and plan for further study

In my point of view, it is quite difficult to remember all the theories such as the DNS record types, shared permission, NTFS permission, and especially the group scopes. It will be easy to make mistakes in the exam due to the time restriction.

For the **shared permission and NTFS permission**, to be more proficient in these scopes, I need to practice these permission applications in the labs.
To be better at **identifying the memberships and limitations of a specified group scope**, I need to read and work on more scenarios in the lectures and on Internet as well.

To remember all the **DNS records** in detail, I need to view the lecture notes of this knowledge frequently.

➢ Key configurations and commands

DSA: Active Directory Users & Computers
ADAC: Active Directory Administrative Center

To **create User Accounts,** in PowerShell, type: **New-AdUser -name "Thu" -Path "cn=users,dc=SWin,dc=local" -accountPassword (ConvertTo-SecureString -AsPlainText "Pa55w.rd" -Force) -enable $True**

To **create Computer Accounts**, DSA and ADAC can be used. In PowerShell, to create a new account, type: **New-ADComputer -name sWin10PC1**

There are some **User Account Properties**: Logon hours, Log On To…, Account expires,…

To **install DNS**, the steps should be followed: Server Manager → Manage → Add Roles and Features → install the **DNS Server role**.
From the **Tools** menu → **DNS** → The **DNS Manager** console will appear.

To create a **Primary Forward Lookup Zone**, in DNS Manager, expand the name of the server→ **Forward Lookup Zone** → **New Zone**
On the welcome screen →**Next**→ **Primary Zone** → **Next** → Enter the zone name → **Next** → **Finish.**

To create the **File Server** for network resources, choose another server rather than the server created in the steps above. In that VM server, create a new folder and a text file in that folder. To share that folder, right-click on that folder → **Properties** → **Sharing** tab → **Advance Sharing** → Check **Share this folder.**

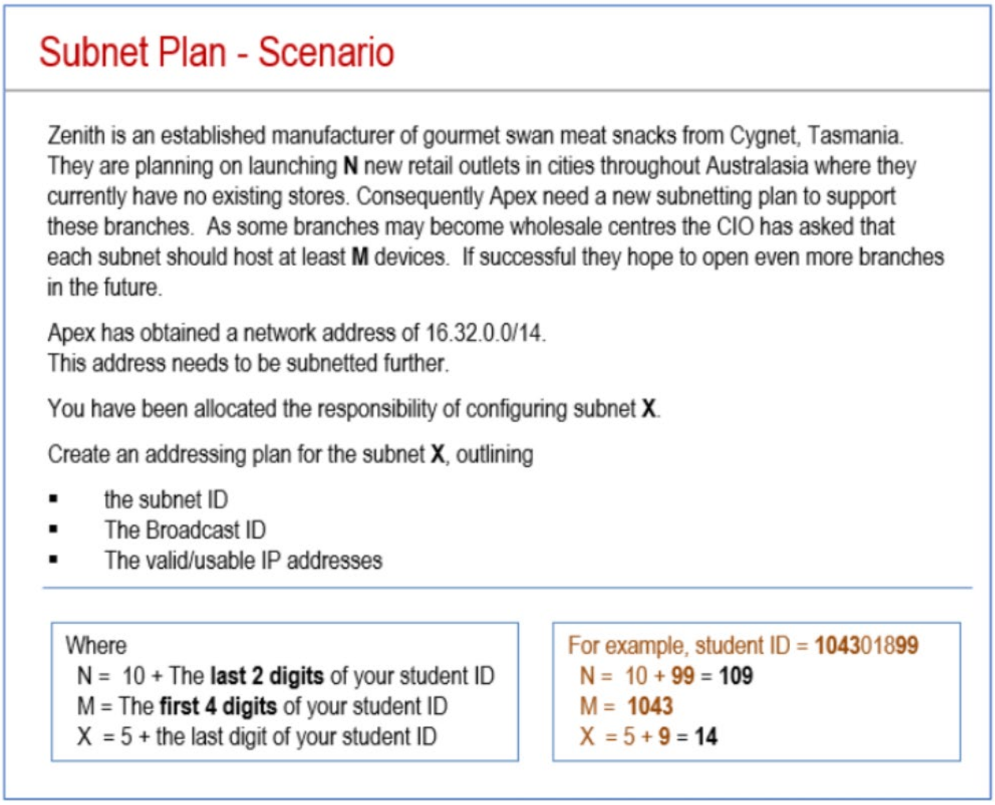
To create **Web Server** for the network resource, in the same server that the File Server was created, in **Server Manger** → **Add Roles and Features** → in **Select server roles** page, add the **Web Server** role. Then right-click on **notepad** icon → **Run as administrator** → write the source code for the website in notepad → Save the text file in the C:\inetpub\wwwroot folder.

To **create DNS records**, in the same server that the **Primary Forward Lookup zone** was created previously → right-click the selected zone and select **New Host** → Type the name, FQDN and IP address → **Add Host**.

If there is a mistake in DNS record configuration, on the client PC, type: **ipconfig /flushdns** to clear the DNS cache.

To test the DNS configuration, log on to the client PC, and type the DNS address in the browser. If the website comes up → successful configuration.

Subnet Plan



Subnet Plan - Scenario

Zenith is an established manufacturer of gourmet swan meat snacks from Cygnet, Tasmania. They are planning on launching **N** new retail outlets in cities throughout Australasia where they currently have no existing stores. Consequently Apex need a new subnetting plan to support these branches. As some branches may become wholesale centres the CIO has asked that each subnet should host at least **M** devices. If successful they hope to open even more branches in the future.

Apex has obtained a network address of 16.32.0.0/14.
This address needs to be subnetted further.

You have been allocated the responsibility of configuring subnet **X**.

Create an addressing plan for the subnet **X**, outlining

- the subnet ID
- The Broadcast ID
- The valid/usable IP addresses

Where
N = 10 + The **last 2 digits** of your student ID
M = The **first 4 digits** of your student ID
X = 5 + the last digit of your student ID

For example, student ID = **104301899**
N = 10 + **99** = **109**
M = **1043**
X = 5 + **9** = **14**

Fig. 4 Subnet Plan Scenario

Student ID: 103818400

According to the instructions in the Fig. above:

N = 10 + 0 = 10

M = 1038

X = 5 + 0 = 5

After applying the change, the scenario problem can be summarised as:

The company: Network Address: 16.32.0.0/14

Need: 10 new branches/subnets

Need: at least 1038 devices/available hosts for each subnet

Administrator: responsible for Subnet 5

Here is the subnet plan for this company:

Referring to the scenario in Fig. 4 above, the demand of the company is opening more branches in the future rather than increasing the devices in each branch.

Currently, the company needs 10 more branches so 4 host bits need to be borrowed (2^3 = 8 < 10 so it must be 2^4 = 16 > 10).

The company needs 1038 devices for each subnet so 11 bits need to be borrowed (2^{10} - 2 = 1022 < 1038 so must be 2^{11} – 2 = 2046 > 1038).

The leftover bits = 32 – 14 – 4 – 11 = 3 bits. These 3 leftover bits should be added to the network portion due to the demand of the company. Therefore the number of network bits after subnetting = 14 + 4 + 3 = 21 bits.

The subnet mask of the subnet address is 255.255.248.0 (slash notation: /21)

The gap size will be 256 – 248 = 8. Every time the gap size is added to the next subnet ID, the gap size will be added to the third octet of the address as 248 is located in the third octet.

To find the first IP address of each subnet, increment the last octet value of that subnet ID by one.

To find the broadcast address of each subnet, decrement the third octet value of the next subnet ID by one and set the last octet value to 255.

To find the last IP address of each subnet, decrement the last octet value of that subnet's broadcast address by one.

After doing the subnetting the subnets information is displayed in the table below:

Subnet	Subnet ID	First Address	Last Address	Broadcast address
0	16.32.0.0/21	16.32.0.1	16.32.7.254	16.32.7.255
1	16.32.8.0/21	16.32.8.1	16.32.15.254	16.32.15.255
2	16.32.16.0/21	16.32.16.1	16.32.23.254	16.32.23.255
3	16.32.24.0/21	16.32.24.1	16.32.31.254	16.32.31.255
4	16.33.32.0/21	16.33.32.1	16.33.39.254	16.33.39.255
5	16.33.40.0/21	16.33.40.1	16.33.47.254	16.33.47.255

Based on the table above, subnet 5 has:

Subnet ID: 16.33.40.0/21

Broadcast address: 16.33.47.255

Subnet range: 16.33.40.1 - 16.33.47.254 → 2046 usable host.

References

Lutkevich, B. and Burke, J. (2021). What is DNS? How Domain Name System works. [online] SearchNetworking. Available at: https://www.techtarget.com/searchnetworking/definition/domain-name-system.

What Is Recursive DNS? | Cloudflare. (n.d.). Cloudflare. [online] Available at: https://www.cloudflare.com/learning/dns/what-is-recursive-dns/.

login.microsoftonline.com. (n.d.). Redirecting. [online] Available at: https://swinburne.instructure.com/courses/57016/pages/lecture-05-slide-presentation-dns-file-and-print-servers?module_item_id=3845566.

login.microsoftonline.com. (n.d.). Redirecting. [online] Available at: https://swinburne.instructure.com/courses/57016/pages/lecture-06-slide-presentation-adds?module_item_id=3845568.

login.microsoftonline.com. (n.d.). Redirecting. [online] Available at: https://swinburne.instructure.com/courses/57016/pages/lab-04-dhcp-and-further-subnetting.

login.microsoftonline.com. (n.d.). Redirecting. [online] Available at: https://swinburne.instructure.com/courses/57016/pages/lab-05-introduction-to-dns.

Alibaba Cloud Community. (n.d.). What Is DNS Spoofing and How to Avoid It? [online] Available at: https://www.alibabacloud.com/blog/what-is-dns-spoofing-and-how-to-avoid-it_600041.

login.microsoftonline.com. (n.d.). Redirecting. [online] Available at: https://swinburne.instructure.com/courses/57016/assignments/619953 [Accessed 20 Apr. 2024].