WEEKLY JOURNAL 2

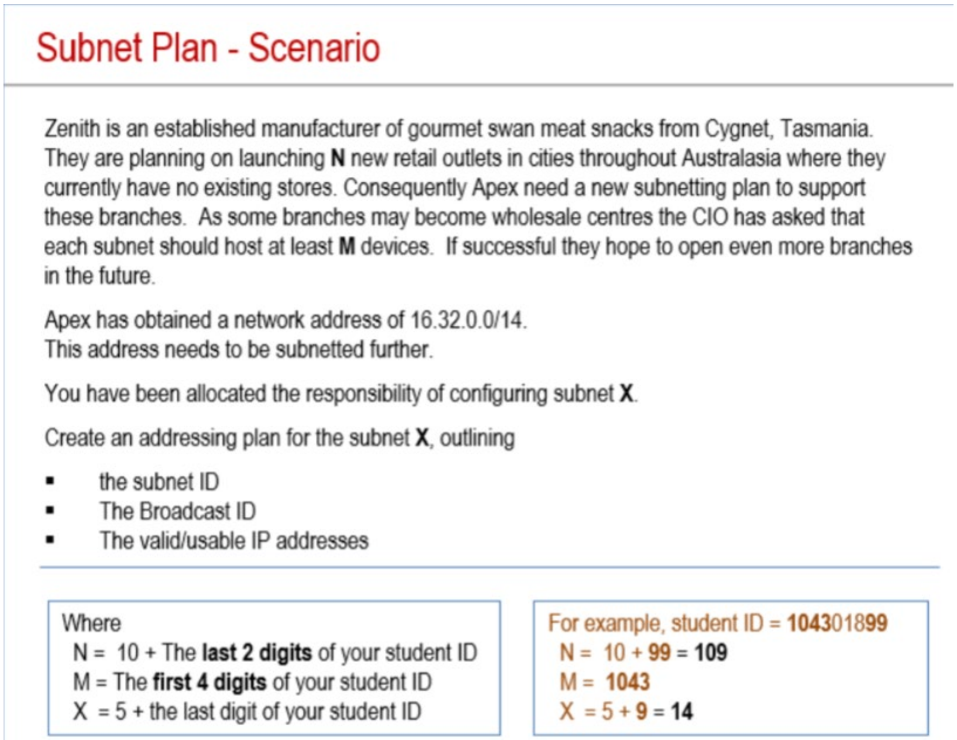
Khoi Nguyen Pham – 104772183

Swinburne University of Technology

I. Table of Contents

II. Subnet Plan

1. Subnet Plan Scenario



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 = **1043**018**99**
N = 10 + **99** = **109**
M = **1043**
X = 5 + **9** = **14**

Figure 1. Subnet Plan Scenario [1]

Since my student ID is 104772183, the values for the scenario are:

- N = 10 + 83= 93 branches
- M = 1047 devices
- X = 5 + 3 = subnet 8

The provided network address is 16.32.0.0/14:

- 93 branches => borrow 7 subnet bits since 2^7 = 128 > 93
- Calculate the subnet bits if borrow 7 bits: 14 + 7 = 21
- 1047 devices => 11 host bits since 2^{11} – 2 = 2046 > 1047
- Calculate the subnet bits for 11 host bits: 32 -11 = 21
- They hope to open more branches, so we have to reserve the subnet bits. However, there're no extra bits => New subnet mask is /21.
- /21 in dotted-decimal notation is 255.255.248.0. Therefore, the subnet gap is in the 3rd octet: 256 – 248 = 8

Having found the subnet gap, now I'm going to create an addressing plan of 16.32.0.0/21 for subnet 8:

Table 1. Subnet Plan made on Word by Khoi Nguyen Pham:

Subnet 0	16.	32.	0.	0.
Subnet 1	16.	32.	8. (0 + 8)	0.
Subnet 2	16.	32.	16. (8 + 8)	0.
Subnet 3	16.	32.	24. (16 + 8)	0.

…	…	…	…	…
Subnet 8	16.	32.	64. (56 + 8)	0.
Subnet 9	16.	32.	72. (64 + 8)	0.

- The subnet ID 8 is 16.32.64.0
- The broadcast address is 16.32.71.255 (one address before subnet ID 9).
- The usable addresses in this subnet are 16.32.64.1 – 16.32.71.254 (subnet ID identifies the network and broadcast address is used to communicate with all devices of the subnet so they can't be used).

2. Reference

[1] Swinburne University of Technology, "TNE10005/TNE60002 - Network Administration Portfolio Task - Weekly Journal 2," 2024.

III. Week 5 (26/08 – 01/09)

1. Key Concepts

1.1. Lectures

a. Topic 1 - DNS

I got introduced to the concept of DNS (Domain Name Server). It's a crucial component that resolves domain names to IP addresses, enabling better internet navigation. The mechanism is helpful not only to organizations, but also for every user to access websites and services quicker and more user-friendly.

DNS used a distributed database structure, which helps with efficient name resolution across the internet. Based on the hierarchy of the structure, root hints, which are a list of servers that host records for all TLD Name Servers, can resolve queries that a DNS server cannot by contacting the root server.

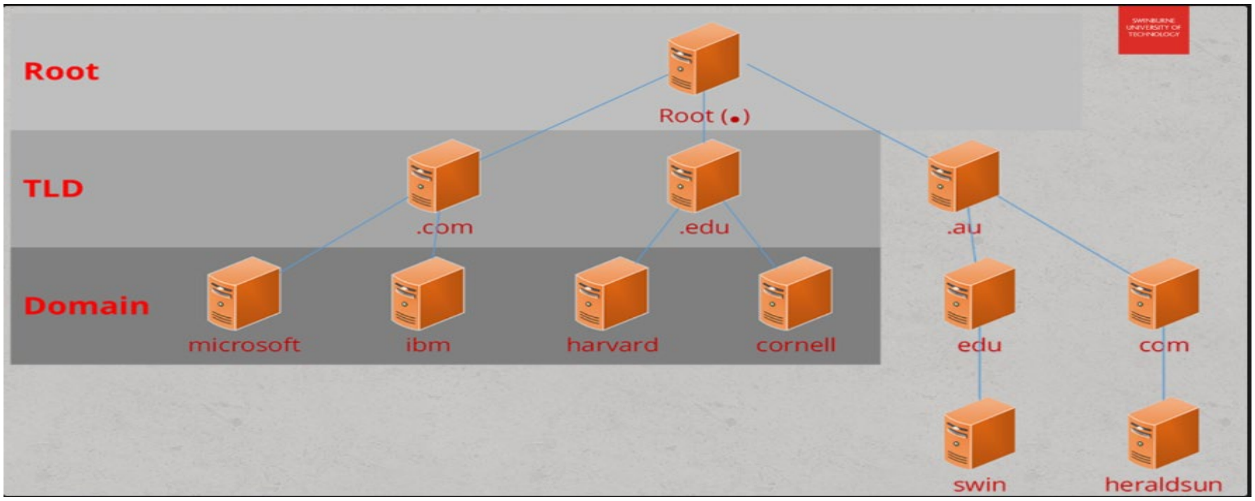


Figure 2. Distributed structure of DNS [2]

For example, a user in Vietnam tries to access a website hosted in Australia. The local DNS server doesn't have the IP address, so it queries the root servers using roots hints. The root servers then direct the query back to the right TLD domain (e.g., .edu) to direct it to the authoritative server for resolving.

Root hints also ensure redundancy and scalability. For instance, if a company is having a regional outage, the queries can still be resolved quickly by other DNS servers thanks to root hints and the hierarchical nature of DNS itself.

Forwarder is another mechanism of DNS server to resolve queries. Small businesses often use this to refer to the ISP's DNS server to resolve external queries for better load balancing and efficiency.

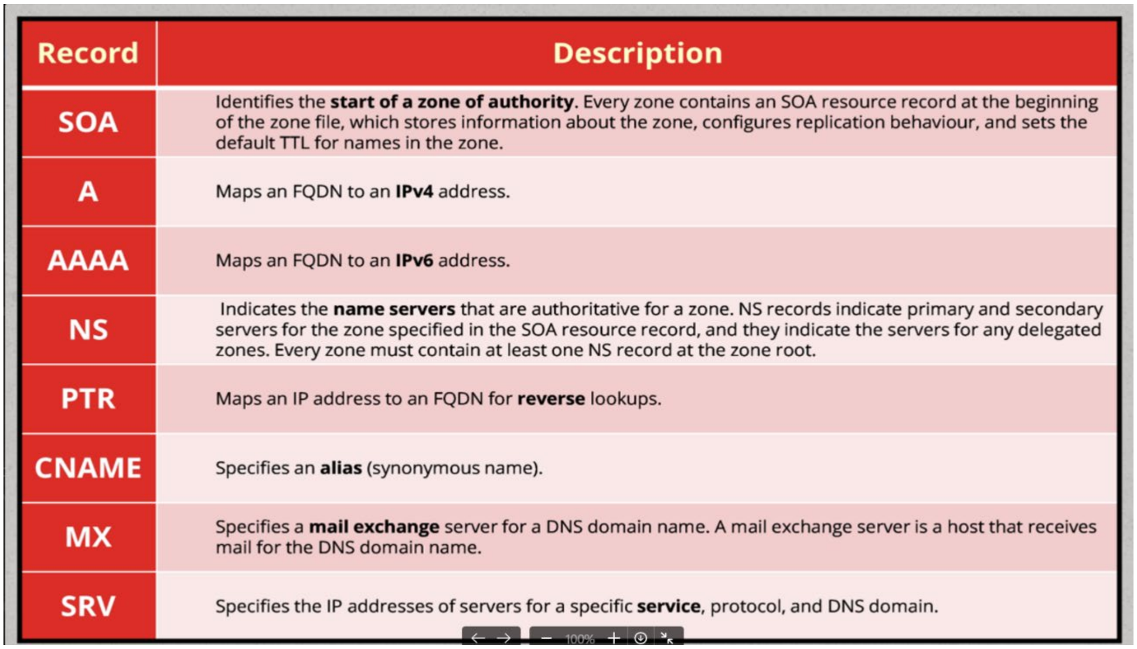
DNS zones are specific portions of DNS namespace that contains DNS records. Organizations can utilize zones to manage their DNS infrastructure. For example, a primary zone contains the original information of the DNS database, whereas a secondary zone receives the data from the primary zone through data transfer as a read-only copy. This is crucial in managing DNS database since if the primary zone goes down, the secondary zone can still resolve DNS queries.

Both of these zones provide authoritative responses to DNS queries, meaning that the information they provide comes directly from the source or its read-only copy zone, as opposed to having to check its cache or to use forwarders and root hints.

A stub zone can also help with redundancy and load balancing, as it partially stores the records from the primary zone. Let's say an online service provider wants to direct user queries to the nearest data center, they can use stub zone to find the server since it only contains the NS records, therefore the process is quicker.

As opposed to zone types (primary/secondary) in which they define the role in term of data management, forward/reverse lookup zones define the direction of the DNS query. For instance, forward lookup zones resolve www.google.com to 172.217.164.110, whereas reverse lookup zones do the opposite. Both of these zones are useful for network services to control network activity through logging/monitoring or help in locating services.

We've also learned DNS records, which are individual entries within a DNS zone that specified how domain names should be resolved.



Record	Description
SOA	Identifies the **start of a zone of authority**. Every zone contains an SOA resource record at the beginning of the zone file, which stores information about the zone, configures replication behaviour, and sets the default TTL for names in the zone.
A	Maps an FQDN to an **IPv4** address.
AAAA	Maps an FQDN to an **IPv6** address.
NS	Indicates the **name servers** that are authoritative for a zone. NS records indicate primary and secondary servers for the zone specified in the SOA resource record, and they indicate the servers for any delegated zones. Every zone must contain at least one NS record at the zone root.
PTR	Maps an IP address to an FQDN for **reverse** lookups.
CNAME	Specifies an **alias** (synonymous name).
MX	Specifies a **mail exchange** server for a DNS domain name. A mail exchange server is a host that receives mail for the DNS domain name.
SRV	Specifies the IP addresses of servers for a specific **service**, protocol, and DNS domain.

Figure 3. DNS Records [2]

I've looked up online to find some real-life scenarios on how each record is used:

- A: www.google.com => 172.217.164.110 [3]
- AAAA: www.google.com => 2607:f8b0:4006:81f::2004 [3]
- CNAME: www.example.com => example.com
- MX:gmail.com => alt1.gmail-smtp-in.l.google.com [4]
- NS: google.com => ns1.google.com [5]
- PTR: 8.8.8.8 => dns.google [6]
- SOA: Provide information about DNS zone, like primary name server, email, serial number, etc.
- SRV: _sip._tcp.microsoft.com => sipdir.online.lync.com [7]

Next, I was introduced to 2 types of queries:

- Recursive: Returns the required result or errors. Due to its simplicity, small/medium businesses often prefer recursive query since clients don't handle multiple queries, resulting in faster response.
- Iterative: Returns the required result or referrals to servers that might be authoritative for the requested record. It's preferred by large enterprise since querying multiple servers can reduce dependency on a single DNS server, hence improving resilience and resource usage. Since clients handle part of the query process, lower cost is needed.

DNS also implements security by using DNSSEC and Split Brain DNS. DNSEC can prevent DNS spoofing (attackers providing false DNS responses) by ensuring that the responses are authenticated, whereas Split-Brain DNS helps organizations to keep internal network details hidden from external customers, hence reducing attack surface.

b. Topic 2 - Windows Server File & Print Services

There're many server roles which define the services that they provide within a network. To access and control these services, we need to have accounts, specifically a user and computer account, to connect to the Window network and domain.

User accounts are fundamental to business IT's infrastructure, especially in security. For example, passwords are always required to prevent unauthorized access. On top of that, Access Control Lists (ACLs) add a second layer of authorization, determining what users are allowed to do once they have access to the system. Let's say I somehow know the password of Daniel's computer, and I want to find the answers folder for test 2. However, I can't access the folder if the ACLs are configured to only allow access from Utami's account.

Every user account has a Security Identifier (SID). It's used to uniquely identify users, groups, and permissions in ACLs. Access token is created every time the user log onto the system. It includes the user's SID, others SID, user's privileges, and other information.

These mechanisms are beneficial in management, since they help organizations to have a clear audit trail of user activities and track network access. They also provide better security as the system compares the ACLs of resources to the SIDs in the access token to grant permission. There're multiple share permissions ranking from read, change, to full control, and by integrating these permissions, administrators can manage the network more efficiently.

We've also dived deeper to some common usage of some servers:

- File Server: File management over network. Companies can use a file server to store all documents so employees can collaborate from their workstations.
- Web Server: Hosts websites by handling HTTTP requests. E-commerce companies can utilize it to host online stores.
- Application Server: Hosts applications. For instance, a game company can implement this to handle logic and interact with the game database server to retrieve and update accounts information.
- Print Server: Manages printer within network by allowing multiple users to share printer. For example, printer pooling is combining multiple physical printers into a single logical unit, hence increasing availability and load balancing within a business.

1.2. Labs

Lab 4 guided us through the process of setting up and managing DHCP. This includes setting up DHCP scopes, exclusions, reservations, and automating the process of assigning IPs. We've also got to know how configurations with the same setting are set in different options, the reservation will "rule them all". Understanding the priority of options helps network administrators to manage IPs more efficiently without conflict. The automatic IP allocation can benefit businesses that work with multiple branches and want to reduce manual configurations and errors.

DHCP server needs to be configured with redundancy, as if the main one goes down, the backup server can still obtain IP addresses. With multiple servers, we also have to keep in mind that overlapping scopes can be complex and cause connectivity issues.

2. Further Study

One of the challenges for me is to memorize the DNS records. To resolve this, I actively looked up online to find real-life scenarios where these records are applied, as well as created handwritten flashcards to help me learn by heart.

I also have to prepare for Test 1, and to achieve my goal of getting an HD, I've dedicated significant time to study the course material by writing down key definitions that I've learned and note my mistakes from previous quizzes to identify the areas I need to focus on.

3. Key Configurations and Commands

- ***Resolve-DnsName***: Resolves domain names to IPs .
- ***DNSCmd***: Queries servers, tests resolutions, and manages zones.
- Authorize DHCP Server: ***DHCP Post-install configuration wizard => Next*** => accept default section => ***Commit.***
- Scopes: ***DHCP*** console, right-click ***IPv4*** => ***New Scope =>*** Right-click ***Scope*** icon => ***Activate.***
- Exclusion: **…**, right-click ***Address Pool*** => ***New Exclusion Range.***
- Reservation: **…**=> ***New Reservation.***
- Options: **…**=> right-click ***Server Options.***

4. Reference

[2] Swinburne University of Technology, "TNE10005/TNE60002 - Network Administration Lecture 05 Slide Presentation - DNS, File & Print Servers," Aug. 2024.

[3] DNS Checker, "DNS Checker - DNS Check Propagation Tool," [Online]. Available: https://dnschecker.org [Accessed: Aug. 28, 2024].

[4] "How to update your MX records to work with Gmail," Google Workspace Knowledge Center. [Online]. Available: https://knowledge.workspace.google.com/kb/how-to-update-your-mx-records-to-work-with-gmail-000005563 [Accessed: Aug. 28, 2024].

[5] Google, "Google Workspace MX record values," Google Workspace Admin Help. [Online]. Available: https://support.google.com/a/answer/174125?hl=en [Accessed: Aug. 28, 2024].

[6] Google, "Hover: Set up MX records," Google Workspace Admin Help. [Online]. Available: https://support.google.com/a/answer/6151047?hl=en [Accessed: Aug. 28, 2024].

[7] Microsoft, "Add DNS records to connect your domain," Microsoft 365 admin. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider?view=o365-worldwide [Accessed: Aug. 28, 2024].

IV. Week 6 (02/09 – 08/09)

1. Key Concepts

1.1. Lectures

a. Topic 1 - Introduction to AD DS

This topic introduced us to some network models:

- Client-Server: A central server manages resources. It suits small businesses since centralized storage ensures easy backup and retrieval. Also, security is enhanced because one server is in charge of controlling access.

However, this reliance on a single server only works in small locations and a server failure can disrupt operations.

- Workgroups: Peer-to-peer networks where each computer manages its own resources. Small businesses can utilize this since it's simple to use and doesn't require any server. Because of that, this model isn't very scalable, as it becomes problematic when maintaining accounts.
- Domains: Centralized and managed by domain controllers. Resources can be located anywhere on the network by implementing trust relationships in Domain Central TrustStore, therefore requiring extensive setups and configurations. Hence, large enterprise can implement this model to handle authentication and authorization from many users. For example, an employee in the Sydney office can access shared resources in the Melbourne office because each domain controller has its own TrustStore to verify user's identity and permissions.

I got introduced to New Technology File System (NTFS) permissions and their implementation. Compared to share permissions, they're more flexible and are attached to objects like files and folders, not the user accounts. NTFS are set on a parent folder can be inherited by all subfolders and files, simplifying management. On the other hand, share permissions are easier to configure, and offer more specific application. Here are the standard NTFS permissions:

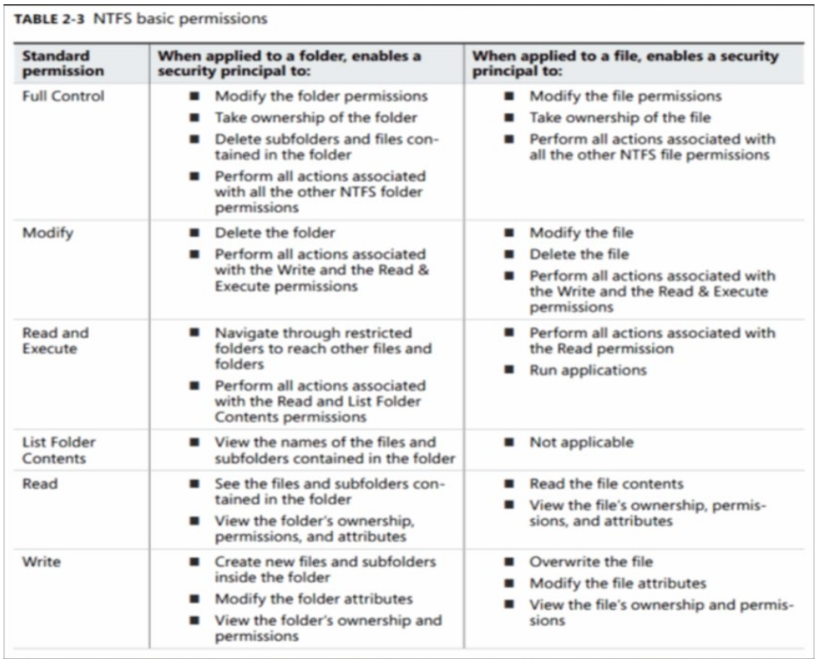


TABLE 2-3 NTFS basic permissions

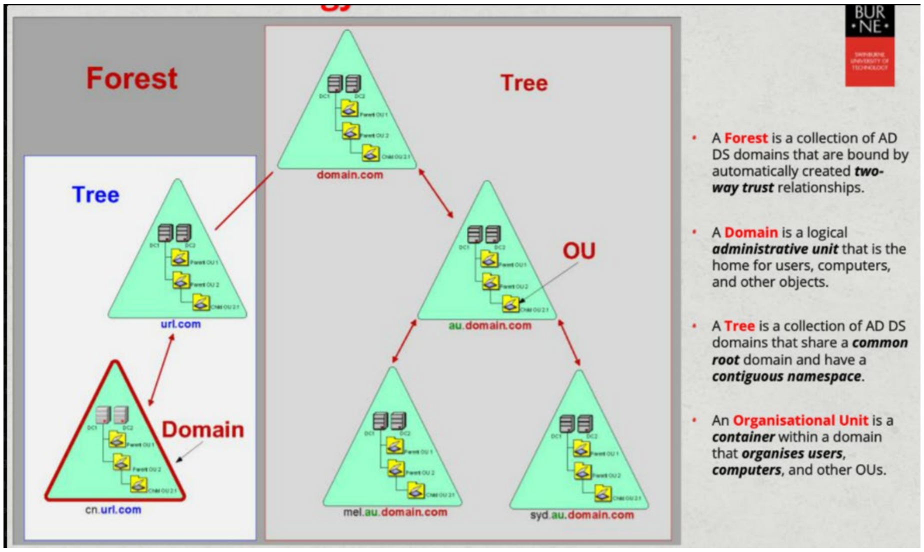
Standard permission	When applied to a folder, enables a security principal to:	When applied to a file, enables a security principal to:
Full Control	■ Modify the folder permissions ■ Take ownership of the folder ■ Delete subfolders and files contained in the folder ■ Perform all actions associated with all the other NTFS folder permissions	■ Modify the file permissions ■ Take ownership of the file ■ Perform all actions associated with all the other NTFS file permissions
Modify	■ Delete the folder ■ Perform all actions associated with the Write and the Read & Execute permissions	■ Modify the file ■ 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 permissions	■ Perform all actions associated with the Read permission ■ Run applications
List Folder Contents	■ View the names of the files and subfolders contained in the folder	■ Not applicable
Read	■ See the files and subfolders contained in the folder ■ View the folder's ownership, permissions, and attributes	■ Read the file contents ■ View the file's ownership, permissions, and attributes
Write	■ Create new files and subfolders inside the folder ■ Modify the folder attributes ■ View the folder's ownership and permissions	■ Overwrite the file ■ Modify the file attributes ■ View the file's ownership and permissions

Figure 4. NTFS basic permissions [8]

NTFS permissions are often used in IT infrastructure that works with multiple roles and departments. For example, a company can assign NTFS permissions to control access for roles including managers, staffs, and interns:

- Managers: Full control (manage ownerships).
- Staff: Modify (add/edit/delete files).
- Interns: Read (view only).

I've also learned about Active Directory, as it's an Object-Oriented Database that helps manage domains. We can use AD to control who can manage and access objects like users, computers, printers, etc. The hierarchical structure of the domain terminology allows AD to centralize management better.



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

Figure 5. Domain Terminology and its components [8]

Let’s say a game corporation operates in multiple countries and has several departments, including marketing, design, program and visual. To manage IT infrastructure efficiently, the company can apply this AD structure:

- Forest: Top-level structure. Allows centralized management of entire organization while providing flexibility for individual departments.
- Trees: Allows for some independence and policy enforcement within its own departments. For example, the design department can decide on the game’s storyline, characters, and their skillsets.
- Domain: Within each department, there are domains for different regions. For example, the marketing division might have domains for Europe, Asia and Oceania.
- OU: Within each domain, there’re OUs to organize users, computers and resources. For instance, the design domain will have OUs for design managers, design staffs, and design interns.

b. Topic 2 - Installing AD DS

In order to install a domain, the Window Server must be the OS. Also, we must have DNS before. After installing ADDS role, the server needs to be promoted to become a Domain Controller.

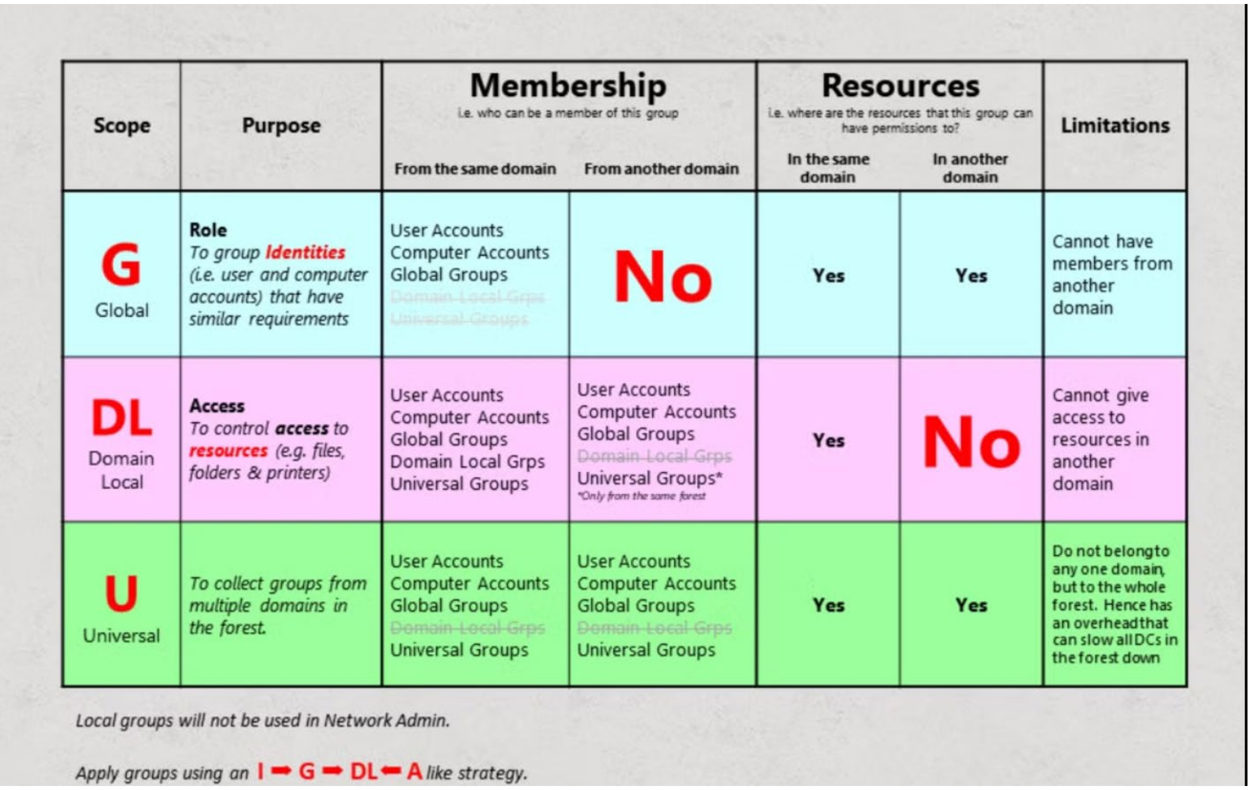
There’re 3 options for installing a Domain Controller:

- Add a DC to an existing Domain: If one domain fails, others can take over.
- Add a new Domain in an existing Forest: Useful for large businesses wanting to separate units while maintaining a single forest.
- Add a new Forest: Suitable for organizations requiring separate directory service environments.

There’s another feature of AD called Multi-Master Replication. It automatically backs up all objects, hence beneficial for organizations that require high availability, scalability, and better performance.

c. Topic 3 - Role Based Access Control using AD i.e. Group Strategy

In AD, there’re 3 main group scopes for Network Administration:



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

Local groups will not be used in Network Admin.

Apply groups using an I ➡ G ➡ DL ⬅ A like strategy.

Figure 6. Group Scopes [8]

The I=>G=>DL<=A strategy is a common measure to manage permissions effectively. To solidify my understanding, I've come up with an example to apply that strategy as well as the group scopes.

Let's say a group of engineers and builders are working with an online blueprint for a building:

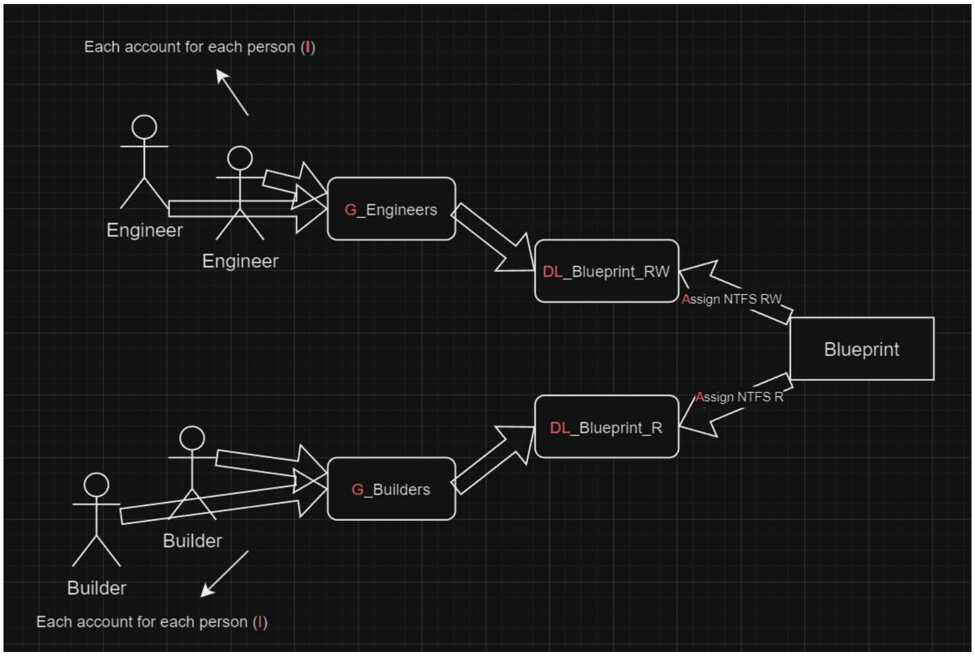


Figure 7. Drawn in diagrams.net [9]

With this structure, I’ve applied my knowledge of the I=>G=>DL<=A strategy as well as group scopes to ensure that permissions are managed effectively to both the engineers and builders.

1.2. Labs

This lab helps us in understanding DNS and how to configure it. I’ve also learned how to configure zones, records, and server roles. Specifically, I’ve learned how to create a zone and add server roles such as File/Web server. The File Server allows us to share and access file over network easily, while the Web Server enables the hosting of websites and web applications. Then, I’ve created DNS records, so users can use that instead of the IP address. Finally, I’ve tested the record on a different VM, and I successfully accessed the website.

2. Further Study

As I dived deeper into NTFS permissions, I’ve learned that they can be combined with shared permissions to enhance security [10]. When both are combined, the most restrictive permission takes precedence. For example, if “Full Control” Share Permission and “Read” NTFS Permission are applied for the “G_Engineers” groups, the engineers will only have Read access since it’s the more restrictive permission.

There aren’t particularly any challenges in the quizzes of this week, and since I’ve just received feedback for Weekly Journal 1, I’ve decided to read a Reference Guide [11] provided on Canva to improve my citations and implemented the techniques into this journal.

3. Key Configurations and Commands

- Primary Forward Lookup Zone: In ***DNS Manager*** => right-click ***Forward Lookup Zones*** => ***New Zones*** => ***Zone Type*** => ***Primary Zone.***
- Add IIS: In ***Server Manager*** => ***Add Roles and Features*** => ***Select server roles*** => add ***IIS.***
- DNS Records: ***Forward Lookup Zones*** => right-click ***burne.edu*** => ***New Host*** => enter www and IP => ***Add Host.***
- Secondary Zone and transfer: right-click ***Forward Lookup Zones*** => ***New Zones*** => enter primary’s IP => on primary, right-click ***burne.edu*** => Properties **=>** ***Zone Transfers*** => ***Name Servers*** => add and resolve. ***Zone Transfers*** tab => ***Allow zone transfers, Only to servers listed on the name servers tab*** => ***Transfer from Master.***
- ***ipconfig /flushdns:*** Clears DNS cache.

4. References

[8] Swinburne University of Technology, “TNE10005/TNE60002 - Network Administration Lecture 06 Slide Presentation - ADDS,” Sep. 2024.

[9] "diagrams.net," JGraph Ltd. [Online]. Available: https://app.diagrams.net [Accessed: Sep. 9, 2024].

[10] "Combining Shared Folder Permissions and NTFS Permissions," NTFS.com. [Online]. Available: https://www.ntfs.com/ntfs-permissions-combined.htm [Accessed: Sep. 9, 2024].

[11] IEEE, "IEEE Reference Guide," IEEE Author Center. [Online]. Available: https://journals.ieeeauthorcenter.ieee.org/wp-content/uploads/sites/7/IEEE_Reference_Guide.pdf [Accessed: Sep. 9, 2024].