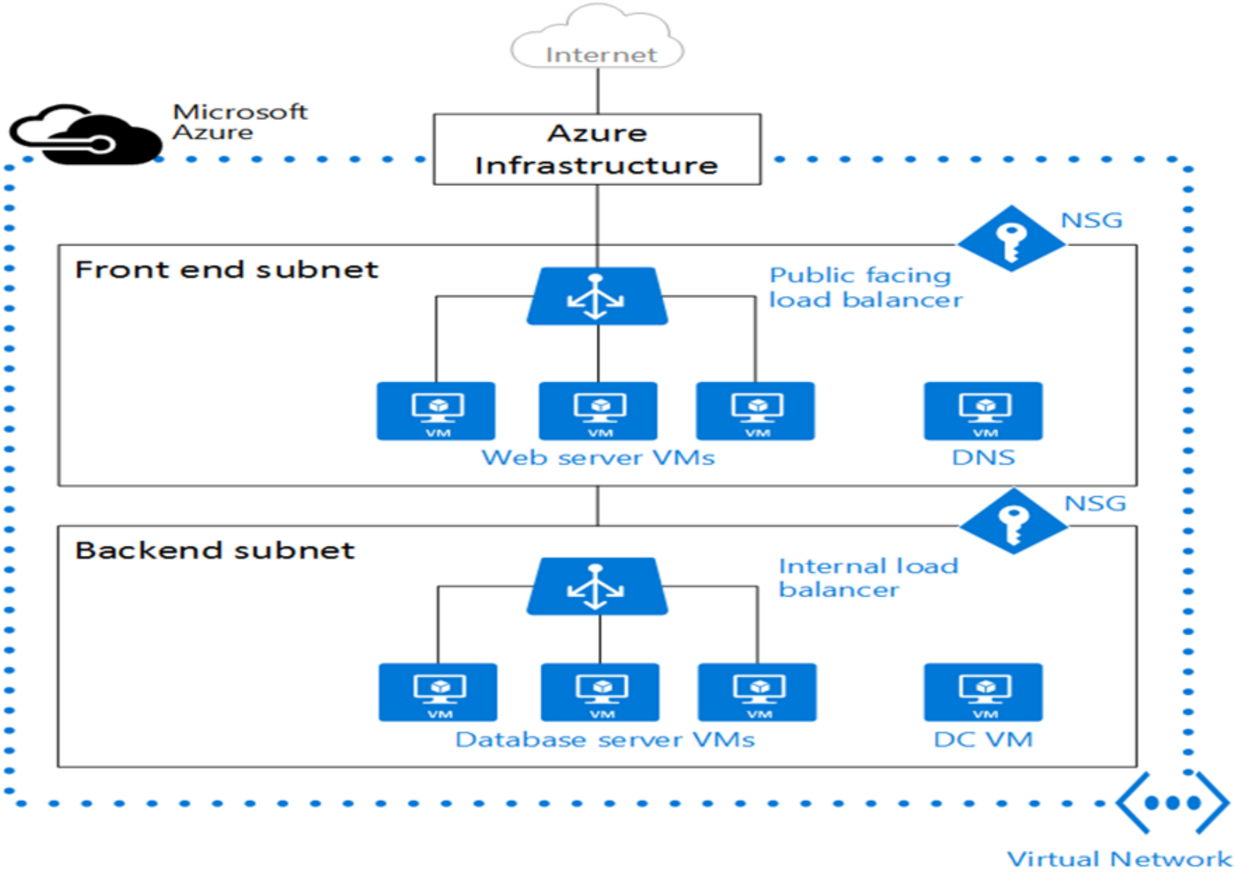
Stories 6 : Create a VNet with two subnet nets one public and another Private subnet.

Vnet: VNet" typically refers to "Virtual Network" in the context of cloud computing and networking. Specifically, it is a term commonly associated with Microsoft Azure, which is a cloud computing platform provided by Microsoft.



features and functionalities of Azure VNets include:

1. **Isolation:** VNets provide network isolation and segmentation, allowing you to group and isolate resources based on your requirements.
2. **Connectivity:** You can establish connections between VNets, between VNets and on-premises networks, and to the internet. This is often done using VPNs (Virtual Private Networks) or Azure ExpressRoute.
3. **Subnetting:** VNets can be divided into subnets to further organize and manage resources within the network.
4. **Security:** Network security groups (NSGs) can be used to control inbound and outbound traffic to and from resources within the VNet.
5. **DNS Configuration:** VNets come with built-in Domain Name System (DNS) resolution, allowing you to use custom DNS settings.

Subnet:

A subnet, short for "subnetwork," is a logical subdivision of an IP network. It is created by taking a larger network and dividing it into smaller, more manageable segments. Subnetting is a technique used to improve the efficiency of IP address utilization, enhance network security, and optimize network performance.

The primary purposes of subnetting include:

1. **IP Address Management:** Subnetting allows organizations to efficiently allocate and manage IP addresses. Instead of having a single, large network with a potentially wasteful allocation of IP addresses, subnetting enables a more granular distribution of addresses.
2. **Network Performance:** Smaller subnets can reduce broadcast domains, which can help improve network performance. In a large network, broadcasts can become a significant source of network traffic. By dividing the network into subnets, broadcast traffic is confined to the local subnet, minimizing its impact on the overall network.

3. **Security:** Subnetting provides a level of security by isolating different parts of a network. Access controls and security policies can be applied at the subnet level, restricting communication between subnets and enhancing network security.
4. **Routing Efficiency:** Subnetting facilitates more efficient routing within a network. Routers use subnet information to determine the best path for forwarding packets, reducing the load on the overall network.

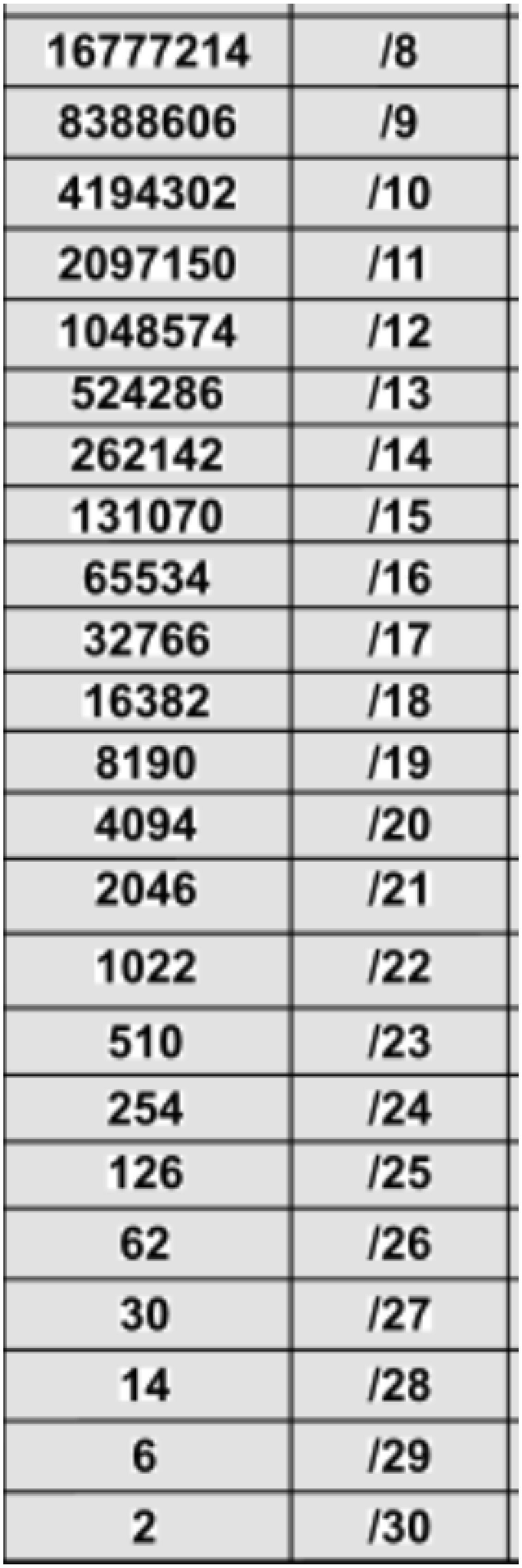
CIDR:

CIDR stands for "Classless Inter-Domain Routing," and it is a method for efficiently allocating and specifying IP addresses and their routing on the Internet. CIDR allows for more flexible allocation of IP addresses than the traditional class-based addressing scheme.

In the traditional IPv4 addressing scheme, IP addresses were divided into classes (Class A, B, and C) with fixed ranges of addresses. CIDR was introduced to address the limitations of the class-based system and to provide a more scalable and efficient way of managing IP addresses.

ADDRESS SPACE

- An IP is **32 bit number** & **4 Octets**, 1 octet being 8 Bits
- An IP Address looks like 10.0.0.0
- Total Bits - 32
- Netmask - X
- Result = Total Bits - Netmask
- Number Of Devices/IP’s = 2 ^ Result
- /8 (Netmask) - 16 Million IP’s / Devices
- 8 - Result = Total Bits - Netmask → 32 - 8 = 24 → Number Of Devices/IP’s = 2 ^ Result → 2 ^ 24 = 16 Million IP’s / Devices



16777214	/8
8388606	/9
4194302	/10
2097150	/11
1048574	/12
524286	/13
262142	/14
131070	/15
65534	/16
32766	/17
16382	/18
8190	/19
4094	/20
2046	/21
1022	/22
510	/23
254	/24
126	/25
62	/26
30	/27
14	/28
6	/29
2	/30

Azure Reservation

- Azure reserves the first four and last IP addresses for a total of **5 IP addresses within each subnet**.
- For example, the IP address range of 10.0.1.0/24 has the following reserved addresses:

10.0.1.0 : Network address

10.0.1.1 : Reserved by Azure for the default gateway

10.0.1.2, 10.0.1.3 : Reserved by Azure to map the Azure DNS IPs to the VNet space

10.0.1.255 : Network broadcast address.

Public Subnet:

A public subnet is a portion of an IP network that is configured to allow direct access to the Internet. In the context of cloud computing, such as platforms like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP), public subnets are typically associated with resources that need to communicate directly with the Internet or external networks.

Key characteristics of public subnets include:

1. **Internet Connectivity:** Resources deployed in a public subnet can have a public IP address and can communicate directly with the Internet. This is useful for services that need to be accessible from the Internet, such as web servers, load balancers, or other publicly facing applications.
2. **Routing:** Public subnets are often configured with a routing table that includes a route to the Internet through a network address translation (NAT) gateway or NAT instance. This allows outbound traffic from resources in the public subnet to reach the Internet.
3. **Security Group Configuration:** Security groups or network security rules are typically configured to control inbound and outbound traffic to and from resources in the public subnet. This helps enforce security policies and protect the resources from unauthorized access.

4. **Public IP Addresses:** Resources in a public subnet may be assigned public IP addresses, allowing them to have direct communication with the Internet. This is in contrast to private subnets, where resources typically have private IP addresses and require a NAT gateway to access the Internet.

Private Subnet:

A private subnet is a segment of an IP network that is typically configured to restrict direct access from the public Internet. In cloud computing environments, such as those provided by Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP), private subnets are often used for resources that do not need to be directly accessible from the Internet but still require network connectivity within the cloud environment or with on-premises networks.

Key characteristics of private subnets include:

1. **Limited Internet Connectivity:** Resources in a private subnet usually do not have direct access to the Internet. If these resources need to access the Internet for updates or other purposes, they typically do so via a Network Address Translation (NAT) gateway or a NAT instance located in a public subnet.
2. **Routing Configuration:** Private subnets are configured with routing tables that may include routes for internal network communication or routes to reach specific services in other parts of the network. However, there is no default route to the Internet.
3. **Security Group Configuration:** Security groups or network security rules are configured to control inbound and outbound traffic for resources within the private subnet. Access controls are often tightened to restrict communication to specific resources within the same network.
4. **Private IP Addresses:** Resources in a private subnet are assigned private IP addresses, typically from non-routable address ranges. This adds an additional layer of security by preventing direct access from the public Internet.

5. **Backend Services:** Backend databases, application servers, or other components that do not require direct exposure to the Internet are often placed in private subnets. These resources can still communicate with other resources in the same network or with on-premises data centers through secure connections.

Azure Network Security Group (NSG)

- You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

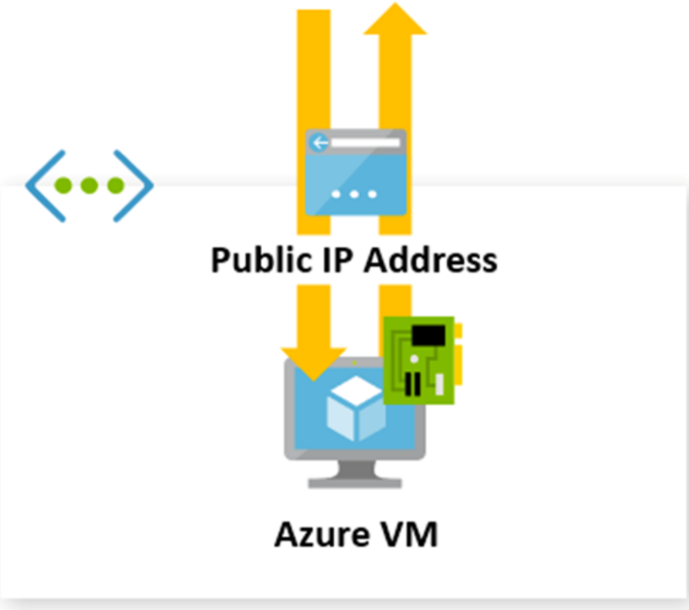
Azure Public IP

- Public IP addresses allow Internet resources to communicate inbound to Azure resources. Public IP addresses enable Azure resources to communicate to Internet and public-facing Azure services.

Azure NIC

- A network interface enables an Azure Virtual Machine to communicate with internet, Azure, and on-premises resources. A virtual machine created with the Azure portal, has one network interface with default settings. You may instead choose to create network interfaces with custom settings and **add one or more network interfaces t**o a virtual machine when you create it.

Azure Public IP



- Public IP addresses allow Internet resources to communicate inbound to Azure resources. Public IP addresses enable Azure resources to communicate to the Internet.