1. **Azure Virtual Networks (VNets)**

* **Definition & Purpose**
  + Logical isolation of the Azure cloud dedicated to your subscription.
  + Enables Azure resources (VMs, databases, etc.) to securely communicate with each other, the internet, and on-premises networks.
  + Supports hybrid cloud and cloud-only scenarios.
* **Key Concepts**
  + **Address Space:** Defined using private IP address ranges (RFC 1918).
  + **Subnets:** Logical subdivisions of a VNet, used for organizing and securing resources.
  + **Network Interface Cards (NICs):** Attach VMs to subnets within a VNet.
  + **Endpoints:** Allow secure connectivity to Azure services (service endpoints) or private endpoints for private access.
  + **Naming Guidelines:** Use clear, consistent naming for VNets and subnets for easier management.
* **Planning & Creation**
  + Plan address spaces to avoid overlaps with on-premises or other VNets (important for future peering or VPN).
  + VNets can be created independently or during VM creation.
  + Each subnet must have a unique, non-overlapping address range within the VNet.
  + Azure reserves 5 IP addresses per subnet for protocol and platform use.
* **Connectivity**
  + VNets can be connected to on-premises networks via VPN Gateway or ExpressRoute.
  + VNet peering allows direct, low-latency connectivity between VNets (even across regions).
  + Supports both public and private IP addressing.

**2. IP Addressing in Azure**

* **Private IP Addresses**
  + Used for internal communication within a VNet or between peered VNets.
  + Assigned dynamically (default) or statically to resources like VMs, load balancers, and application gateways.
  + Never managed from within the VM; always managed at the Azure resource level.
* **Public IP Addresses**
  + Used for communication with the internet or Azure public-facing services.
  + Can be IPv4 or IPv6, Standard or Basic SKU, and assigned dynamically or statically.
  + Associated with resources such as VM NICs, load balancers, VPN gateways, and application gateways.
  + Standard SKU offers enhanced security and features (e.g., zone redundancy).
* **Best Practices**
  + Separate dynamic and static IP resources into different subnets if needed.
  + Avoid exposing resources directly to the internet unless necessary; use NAT, firewalls, or load balancers for protection.

**3. Subnets**

* **Purpose**
  + Segment a VNet into smaller, manageable sections.
  + Improve security, performance, and management.
  + Assign network security groups (NSGs) and route tables at the subnet level.
* **Azure Reserved IPs in Each Subnet**
  + .0: Network address
  + .1: Azure default gateway
  + .2 & .3: Reserved for Azure services
  + .255: Broadcast address

**4. Network Security Groups (NSGs) & Application Security Groups (ASGs)**

* **Network Security Groups (NSGs)**
  + Act as virtual firewalls to control inbound and outbound traffic at subnet or NIC level.
  + Consist of security rules with priority, source/destination, port, protocol, and action (allow/deny).
  + Default rules exist; custom rules can override with higher priority (lower number).
  + NSGs can be associated with multiple subnets or NICs.
  + Effective security rules are the combination of rules applied at both subnet and NIC levels; both must allow traffic for it to pass.
* **Application Security Groups (ASGs)**
  + Logical grouping of VMs for simplified management of security rules.
  + Useful for micro-segmentation (e.g., group web servers, app servers, DB servers).
  + NSG rules can reference ASGs as source or destination, enabling scalable and dynamic security management.
* **Best Practices**
  + Prefer associating NSGs at the subnet level for easier management.
  + Use ASGs to reduce the number of NSG rules and simplify security for large deployments.
  + Regularly review effective security rules to ensure compliance and minimize exposure.

**5. Azure DNS**

* **Azure DNS Overview**
  + Provides ultra-high availability and performance for domain name system hosting.
  + Supports both public and private DNS zones.
  + When a new Azure tenant is created, a default domain (e.g., contoso.onmicrosoft.com) is assigned.
  + Custom domains can be added and must be verified (proves ownership).
* **DNS Zones**
  + A DNS zone hosts the DNS records for a domain.
  + Multiple zones with the same name can exist in Azure, each with unique name server addresses.
  + Delegation requires updating the registrar with Azure-provided name servers.
* **DNS Records**
  + Record sets are collections of records with the same name and type.
  + Alias records allow dynamic resolution to Azure resources (e.g., public IP, Traffic Manager).
  + Up to 20 records per record set; no duplicate records allowed.
* **Private DNS Zones**
  + Provide name resolution for VMs within a VNet and across peered VNets.
  + Automatic hostname record management for Azure resources.
  + Removes the need for custom DNS solutions or on-premises DNS servers.
  + Supports all common DNS record types and is available in all Azure regions.
* **Domain Verification**
  + Ownership is verified by adding a TXT or MX record to your DNS zone.
  + Azure checks for the presence of this record before allowing domain use.
* **Best Practices**
  + Use private DNS zones for internal name resolution to avoid exposing internal names to the internet.
  + Use alias records for dynamic Azure resource resolution.
  + Regularly audit DNS records and zones for accuracy and security.

**6. Traffic Routing & Security**

* **Traffic Routing**
  + Azure routes traffic within VNets and between subnets automatically.
  + Custom route tables can be used for advanced scenarios (e.g., forced tunneling, firewalls).
  + Azure Firewall provides centralized, stateful firewall protection for VNets.
* **Service Endpoints & Private Endpoints**
  + Service endpoints extend VNet identity to Azure services, securing traffic over the Azure backbone.
  + Private endpoints provide private IP addresses for Azure services, enabling private connectivity.
* **Best Practices**
  + Use NSGs and ASGs to tightly control traffic flow.
  + Use Azure Firewall or third-party appliances for advanced security needs.
  + Monitor network traffic and security rules regularly.

**7. Additional Best Practices & Insights**

* **Naming Conventions**
  + Use clear, descriptive names for VNets, subnets, NSGs, and DNS zones for easier management and automation.
* **Monitoring & Diagnostics**
  + Use Network Watcher for monitoring, diagnostics, and logging of network traffic and security events.
  + Enable diagnostic logs on NSGs and Azure Firewall for auditing and troubleshooting.
* **Scalability & High Availability**
  + Design VNets and subnets with future growth in mind.
  + Use availability zones and redundant resources for critical workloads.
* **Automation**
  + Use ARM templates, Bicep, or Terraform for repeatable, automated network deployments.
  + Leverage Azure Policy to enforce network configuration standards.