



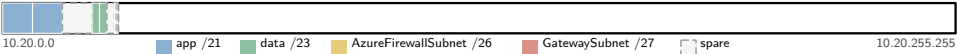
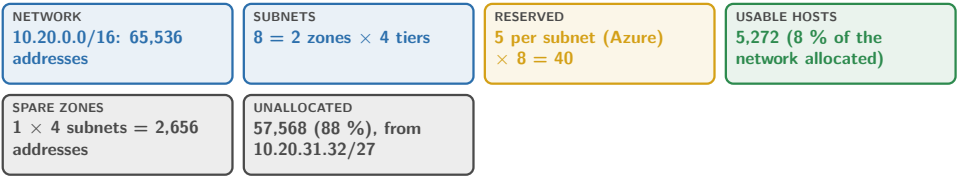
VNets, IP Address Planning, Public IPs and DNS

AZ-700 domain 1, Design and implement core networking infrastructure (part 1) | Address spaces and subnets, reserved addresses, special subnets and delegation, public IP SKUs and prefixes, default outbound access, Azure DNS, Private DNS zones, DNS Private Resolver; az CLI and Bicep

AZ-700 Domain 1 IP planning DNS

Plan the address space

Rule	Detail
Scope	a VNet lives in one region and one subscription; its subnets span all availability zones of the region
Ranges	RFC 1918 (10/8, 172.16/12, 192.168/16) or 100.64/10; public ranges you own are possible but unusual; IPv6 subnets are /64
No overlap	with on-premises, other VNets you peer or connect, and future acquisitions: peering and VPN refuse overlapping prefixes
Reserved	5 per subnet: x.0 network, x.1 gateway, x.2 and x.3 Azure DNS, last = broadcast; smallest subnet /29 (3 usable)
Resize	you can add or resize address spaces of a peered VNet, then sync the peering
Plan per region	one /16 per region is common: hub /22-/24, spokes /20-/24, room for growth



Tier	westeurope	northeurope	spare 1
app /21 2,048 each	10.20.0.0/21 2,043 usable	10.20.8.0/21 2,043 usable	10.20.16.0/21 2,043 usable
data /23 512 each	10.20.24.0/23 507 usable	10.20.26.0/23 507 usable	10.20.28.0/23 507 usable
AzureFirewallSubnet /26 64 each	10.20.30.0/26 59 usable	10.20.30.64/26 59 usable	10.20.30.128/26 59 usable
GatewaySubnet /27 32 each	10.20.30.192/27 27 usable	10.20.30.224/27 27 usable	10.20.31.0/27 27 usable

Azure reserves 5 addresses in every subnet (network address, default gateway, 2 for DNS, broadcast): usable = 2ⁿ(32 - prefix) - 5, where prefix = the subnet's prefix length. Blocks are allocated largest first, so every subnet starts on a multiple of its own size.

One /16 per landing zone split into two regional VNets (columns = regions, because Azure subnets span all zones) plus one spare region

Special subnet	Minimum size	Notes
GatewaySubnet	/29, use /27+	VPN and ExpressRoute gateways; no NSG recommended; UDRs allowed with care
AzureFirewallSubnet	/26	Azure Firewall; plus AzureFirewallManagement Subnet /26 for forced tunnelling or Basic SKU
AzureBastionSubnet	/26	Azure Bastion Basic, Standard, Premium (Developer SKU needs none)
RouteServerSubnet	/27	Azure Route Server
Application Gateway v2	dedicated, /24 recommended	only App Gateways in it; up to 125 instances need addresses
DNS Private Resolver endpoints	/28 each	delegated to Microsoft.Network/dnsResolvers; one inbound, one outbound subnet

10.20.0.0/21	
IPv4 subnet	
NETWORK	10.20.0.0/21
MASK	255.255.248.0 (/21)
WILDCARD	0.0.7.255
BROADCAST	10.20.7.255
HOSTS	10.20.0.1 → 10.20.7.254
COUNT	2,048 addresses = 2^{11} ; usable hosts = $2^{11} - 2 = 2,046$
WHERE	11 = host bits = 32 — prefix length 21; the two removed addresses are the network and the broadcast

ADDRESS	0 0 0 0 1 0 1 0
MASK	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	network bits (21) host bits (11)

Split into /24: 8 subnets = $2^{(24 - 21)}$, each 256 addresses

1.	10.20.0.0/24	hosts	10.20.0.1	→	10.20.0.254
2.	10.20.1.0/24	hosts	10.20.1.1	→	10.20.1.254
3.	10.20.2.0/24	hosts	10.20.2.1	→	10.20.2.254
4.	10.20.3.0/24	hosts	10.20.3.1	→	10.20.3.254
5.	10.20.4.0/24	hosts	10.20.4.1	→	10.20.4.254
6.	10.20.5.0/24	hosts	10.20.5.1	→	10.20.5.254
7.	10.20.6.0/24	hosts	10.20.6.1	→	10.20.6.254
8.	10.20.7.0/24	hosts	10.20.7.1	→	10.20.7.254

The 10.20.0.0/21 app subnet computed (Azure then removes 5 addresses per subnet)

Public IPs and outbound

- Standard SKU only** Basic public IPs and Basic Load Balancer were retired on 30 September 2025; Standard is static, secure by default (inbound closed until an NSG allows it) and zone-redundant where the region has zones
- Public IP prefix** contiguous block for allow-lists at partners; attach to NAT gateway or allocate IPs from it
- Custom IP prefix (BYOIP)** bring your own public range, provisioned and commissioned in Azure
- Routing preference** Microsoft network (default, cold-potato) or Internet (ISP network, cheaper egress)
- Outbound methods, best first** NAT gateway, then load balancer outbound rules, then instance-level public IP; new VNets have no default outbound access

```

az CLI: VNet, delegated subnet, Standard public IP
az network vnet create -g rg-net -n vnet-hub-weu \
  --address-prefixes 10.20.0.0/22 \
  --subnet-name GatewaySubnet --subnet-prefixes 10.20.0.0/27
az network vnet subnet create -g rg-net --vnet-name vnet-hub-weu \
  -n snet-dns-in --address-prefixes 10.20.1.0/28 \
  --delegations Microsoft.Network/dnsResolvers
az network public-ip create -g rg-net -n pip-vpn-1 \
  --sku Standard --zone 1 2 3

```

spoke.bicep

```

1 resource vnet 'Microsoft.Network/virtualNetworks@20
24-05-01' = {
2   name: 'vnet-app-weu'
3   location: 'westeurope'
4   properties: {
5     addressSpace: { addressPrefixes: [
6       '10.20.8.0/21' ] }
7     subnets: [
8       { name: 'snet-app', properties: {
9         addressPrefix: '10.20.8.0/24'
10        defaultOutboundAccess: false
11        natGateway: { id: natGw.id }
12        networkSecurityGroup: { id: nsg.id } } }
13       { name: 'snet-web', properties: {
14         addressPrefix: '10.20.9.0/24'
15         delegations: [ { name: 'web',
16           properties: {
17             serviceName: 'Microsoft.Web/serverFarms
18             } } ] } } ] }
19   }
20 }

```

1

address space must not overlap hub, peers or on-premises

2

private subnet: no implicit internet IP

3

explicit outbound through NAT gateway

4

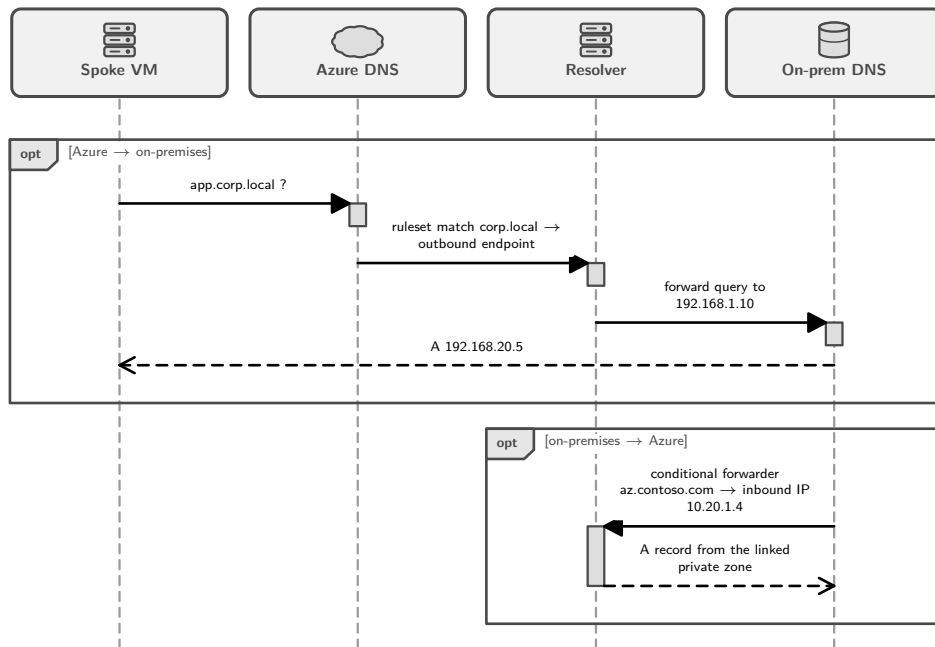
NSG on the subnet, stateful

5

delegation for App Service VNet integration

DNS in Azure

Option	Resolves	Use when
Azure-provided DNS (168.63.129.16)	public names, VM names inside one VNet (internal.cloudapp.net)	simple single-VNet labs
Azure DNS public zone	your internet domain, hosted on Azure name servers; alias records to Azure re-sources	public DNS hosting
Private DNS zone + links	custom private names in all linked VNets; auto-registration of VM records (one registration zone per VNet)	multi-VNet name resolution, privatelink zones
DNS Private Resolver	hybrid: inbound endpoint for on-premises, outbound endpoint + ruleset to on-premises	replaces DNS forwarder VMs
Custom DNS servers on the VNet	whatever your servers resolve (AD DS DNS)	domain controllers in Azure; forward to 168.63.129.16



A spoke VM resolves an on-premises name and on-premises resolves a private zone

Worked example: usable addresses for an App Gateway subnet

Application Gateway v2 can scale to $N = 125$ instances and each needs one private IP, plus a private frontend IP. Required $R = 125 + 1 = 126$. A $/25$ has $2^{(32-25)} = 128$ addresses, minus 5 reserved = 123 usable $< 126 \rightarrow$ too small. A $/24$ has $256 - 5 = 251$ usable $\geq 126 \rightarrow$ fits with room for a second gateway. That is why Microsoft recommends $/24$.

MYTH

✗ Subnets are created per availability zone

✗ A $/29$ gives 6 usable addresses in Azure

✗ One private DNS zone can auto-register VMs from many VNets, and a VNet from many zones

✗ Blocking 168.63.129.16 is a good hardening step

FACT

✓ **Azure subnets are regional**
Zones are chosen per resource (VM, IP, gateway), not per subnet.

✓ **Only 3**
 $8 - 5 \text{ reserved} = 3$.

✓ **A VNet has at most one registration zone**
It can be linked to other zones for resolution only.

✓ **It breaks DNS, DHCP, health probes and the VM agent**
NSGs do not filter it by default; leave it reachable.

Q1 Five reserved addresses in 10.1.2.0/24?

A 10.1.2.0, .1, .2, .3 and .255.

Q2 Minimum size of AzureFirewallSubnet and AzureBastionSubnet?

A $/26$ each.

Q3 Subnet size for DNS Private Resolver endpoints?

A $/28$ minimum each, delegated to Microsoft.Network/dnsResolvers.

Q4 On-premises must resolve names in an Azure private DNS zone: what do you deploy?

A DNS Private Resolver inbound endpoint; on-premises conditional forwarder to its IP.

Q5 Azure VMs must resolve corp.local: what do you deploy?

A Outbound endpoint + forwarding ruleset (`corp.local → on-prem DNS`) linked to the VNets.

Q6 Which public IP SKU remains after September 2025?

A Standard (Basic retired).

Q7 How many VNets can a VNet register its VMs into?

A One private DNS zone with auto-registration per VNet.

Q8 What is 168.63.129.16?

A Azure platform virtual IP for DNS, DHCP, health probes and VM agent.

Key takeaways

01

No overlaps, ever

plan a $/16$ per region and keep a spare

02

Minus five per subnet

and special subnets have fixed names and sizes

03

Standard public IPs, explicit outbound

NAT gateway first

04

Private Resolver for hybrid DNS

inbound for on-prem, outbound + ruleset for Azure

05

One registration zone per VNet

many resolution links allowed