

## IP Addressing Scheme – Azure Enterprise Landing Zone

Enterprise Address Space: 10.0.0.0/8 (supernet)

### Hub VNet – 10.0.0.0/16 (65,536 addresses)

Subnet	CIDR	Usable IPs	Purpose
AzureFirewallSubnet	10.0.1.0/24	251	Azure Firewall Premium
GatewaySubnet	10.0.2.0/24	251	VPN / ExpressRoute GW
ManagementSubnet	10.0.3.0/24	251	Bastion, jump boxes
DNSResolverSubnet	10.0.4.0/24	251	Private DNS Resolver
Available	10.0.5-255.0/24	~63K	Future hub services
<b>Total Allocated</b>	<b>4 x /24</b>	<b>1,004</b>	<b>~1.5% of /16 used 98.5% available for growth</b>

#### Design Decisions:

1. /16 per VNet — provides 65K addresses and room for future subnets
2. /24 per subnet — 251 usable IPs (Azure reserves 5 per subnet)
3. Consistent subnet numbering — .1=web, .2=app, .3=data, .4=PE across all spokes
4. Hub uses .0.x for infrastructure subnets (firewall, gateway, mgmt, DNS)
5. Non-overlapping ranges prevent routing conflicts across peered VNets

### Production Spoke – 10.1.0.0/16

- web: 10.1.1.0/24 (251 IPs)
- app: 10.1.2.0/24 (251 IPs)
- data: 10.1.3.0/24 (251 IPs)
- private-endpoints: 10.1.4.0/24

### Staging Spoke – 10.2.0.0/16

- web: 10.2.1.0/24 (251 IPs)
- app: 10.2.2.0/24 (251 IPs)
- data: 10.2.3.0/24 (251 IPs)
- private-endpoints: 10.2.4.0/24

### Shared Services Spoke – 10.3.0.0/16

- tools: 10.3.1.0/24 (251 IPs)
- infrastructure: 10.3.2.0/24 (251 IPs)
- private-endpoints: 10.3.3.0/24

### On-Premises (via VPN/ER) – 10.100.0.0/16

Configured via `local_network_gateway_config`  
Only active when `deploy_vpn_gateway = true`

### Available for Future Spokes

10.4.0.0/16      10.5.0.0/16      10.6.0.0/16      ...      10.99.0.0/16

Each new spoke gets a /16 block = 65,536 addresses  
Consistent subnet pattern: web, app, data, private-endpoints (/24 each)  
Total capacity: ~96 additional spokes (10.4 through 10.99)