Tag 3

Guten Morgen!

brainymotion

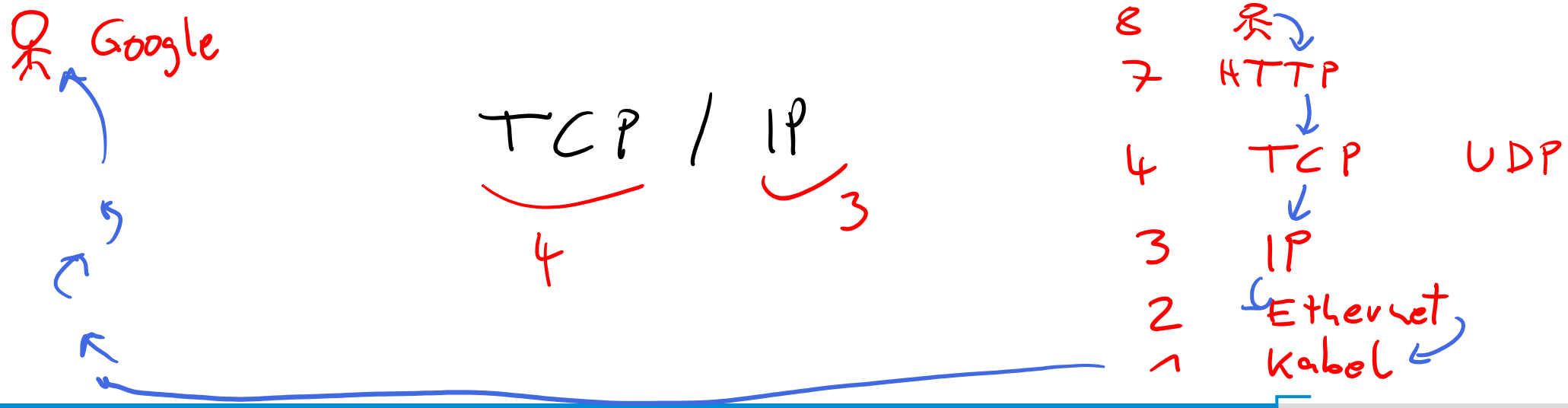
smart trainieren.
sicher können.

Modul 4: Network Infrastructure Fundamenatls

Agenda:

1. Azure Architecture Fundamentals
2. Administration Fundamentals
3. Virtualization Fundamentals
4. Network Infrastructure Fundamentals
5. Storage Management Fundamentals
6. Identity Services Fundamentals

dsa.msc AD Users & Comp.
compmgmt.msc
mmc.exe
WAC | Server Manager | PowerShell
Jeff Snover
Hyper-V
VM
Host1
Host2
Live Migration

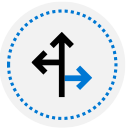


Lesson 1: IPv4 Fundamentals

brainymotion

IPv4 Fundamentals

Overview of IPv4 settings

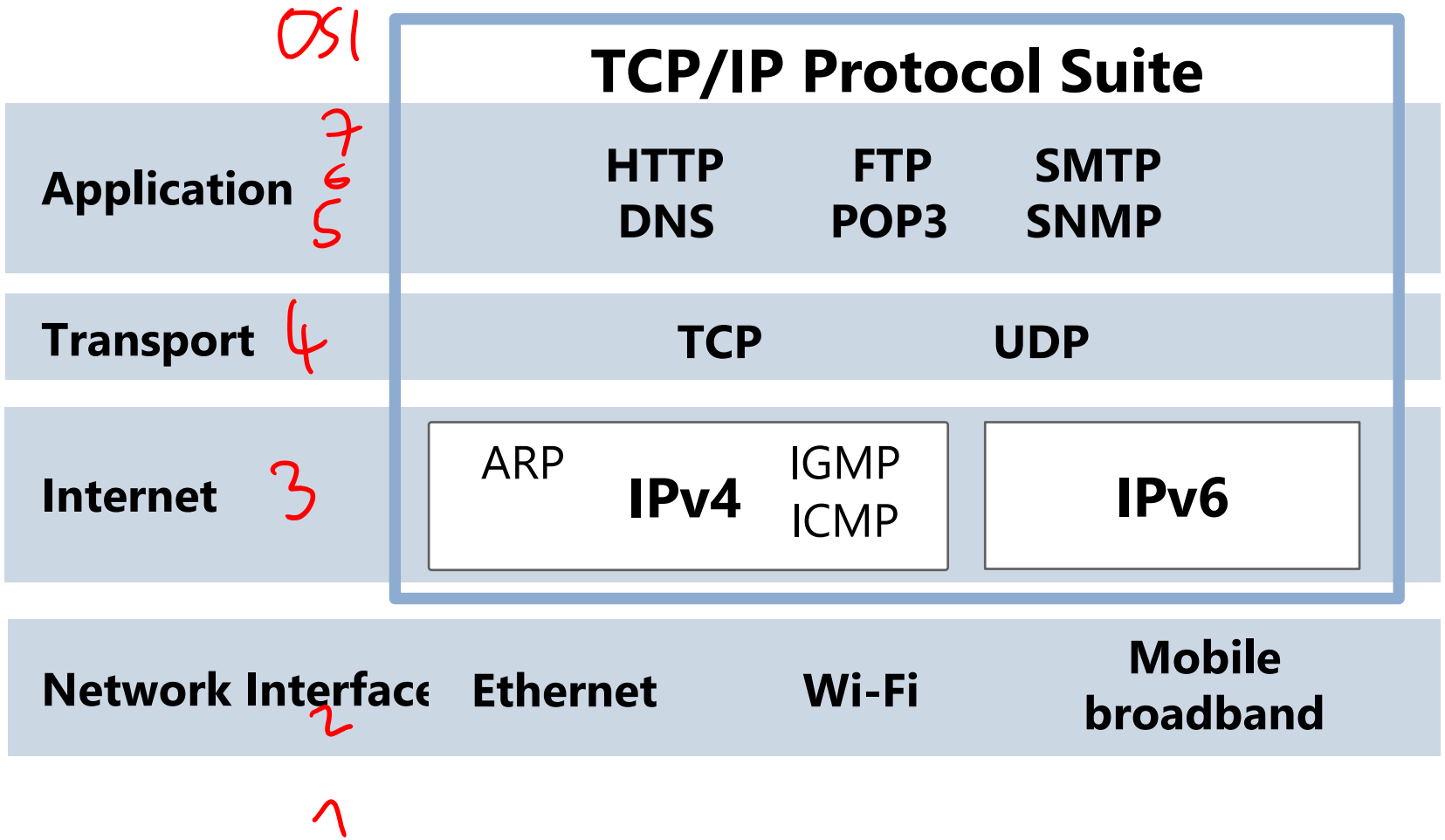


Defining Subnets

Public, private and APIPA addresses

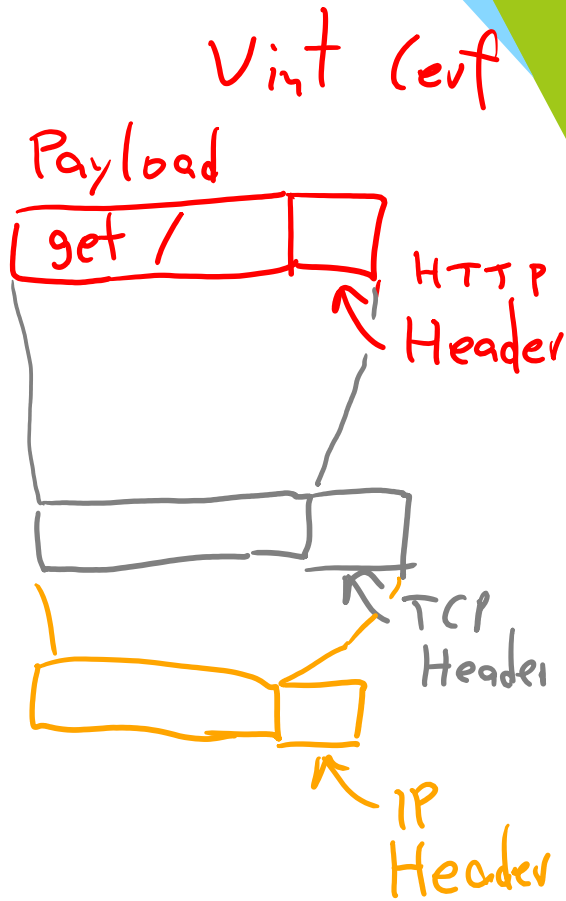
brainymotion

The TCP/IP Protocol Suite



Protocols in the TCP/IP Suite

OSI	TCP/IP	TCP/IP Protocol Suite
Application Presentation Session	Application	HTTP, DNS, FTP, POP3, SMTP, SNMP
Transport	Transport	TCP, UDP
Network	Internet	ARP, IPv4, IGMP, ICMP, IPv6
Data Link Physical	Network Interface	Ethernet, Wi-Fi, Mobile broadband



wireshark capture

TCP/IP Applications

Daemon (Service, Dienst)

Windows FW
NSG

Test-NetConnection -Computername SVR1 -Port 3389

Ziel (Destination) Port

16 Bit
$2^{16} = 65.536$
$2^{10} = 1024$

Some common application layer protocols:

- HTTP 80
- HTTPS 443
- FTP 21
- RDP Remote Desktop 3389
- SMB 445
- SMTP Simple Mail Transfer Proto 25
- POP3 110
- SSH, SFTP 22
- Telnet 23
- Kerberos 88, LDAP 389 } AD

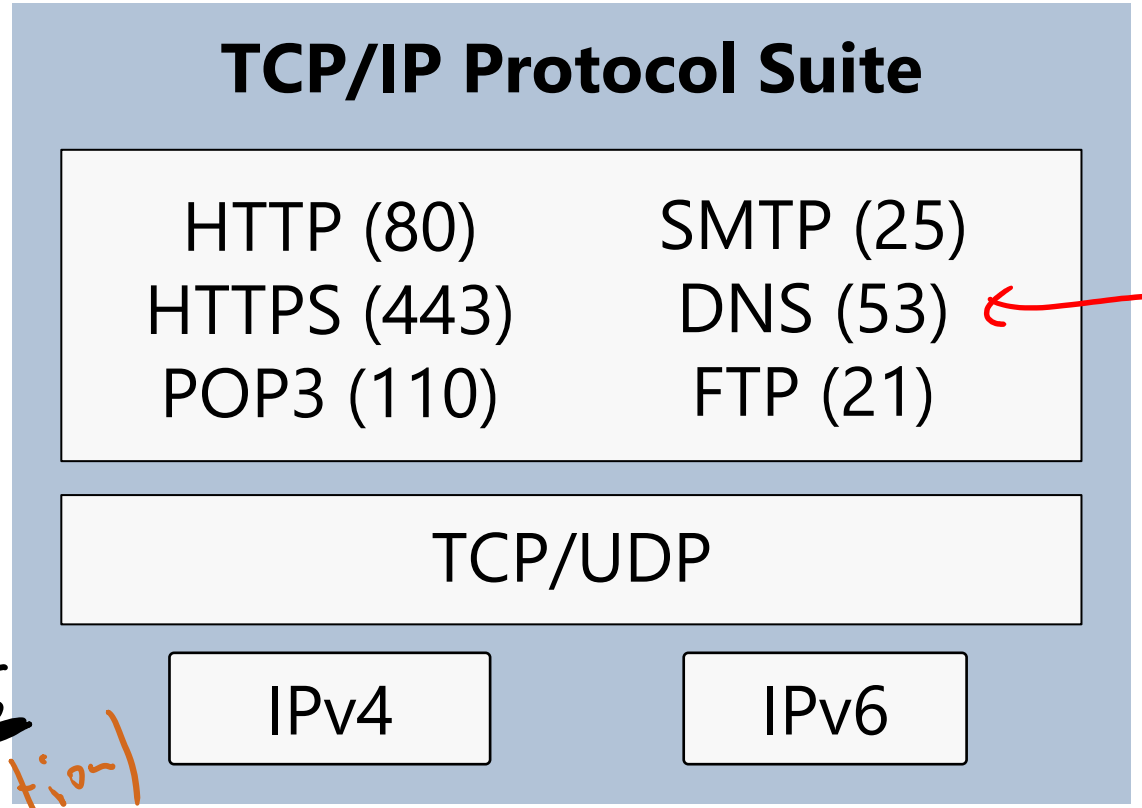
1 Kg = 1000 g

1 KByte = 1024 Byte

What Is a Socket?

AWS
DNS
Route53

A socket is a combination of an IP address, a transport protocol, and a port



Tools
ping
tracert
netstat
route
telnet
traceroute
mail.
25
(Test-Net Connection)

IP

32 Bit

$2^{32} \sim 4 \cdot 10^9$

IPv4 Addressing

IPv6

128 Bit

2^{128}

- Each networked computer must be assigned a unique IPv4 address
- Network communication for a computer is directed to the IPv4 address of the computer
- Each IPv4 address contains:
  - Network ID, identifying the network
  - Host ID, identifying the computer
- The subnet mask identifies which part of the IPv4 address is the network ID (255) and which is the host ID (0)

8 Bit $2^8 = 256$

10 Bit $2^{10} = 1024$

16 Bit $2^{16} = 65536$

32 Bit $2^{32} \approx 4$ Milliarden

IPv4 Addressing

8 Bit = 1 Byte
4 Bit = 1/2 Byte = 1 Nibble

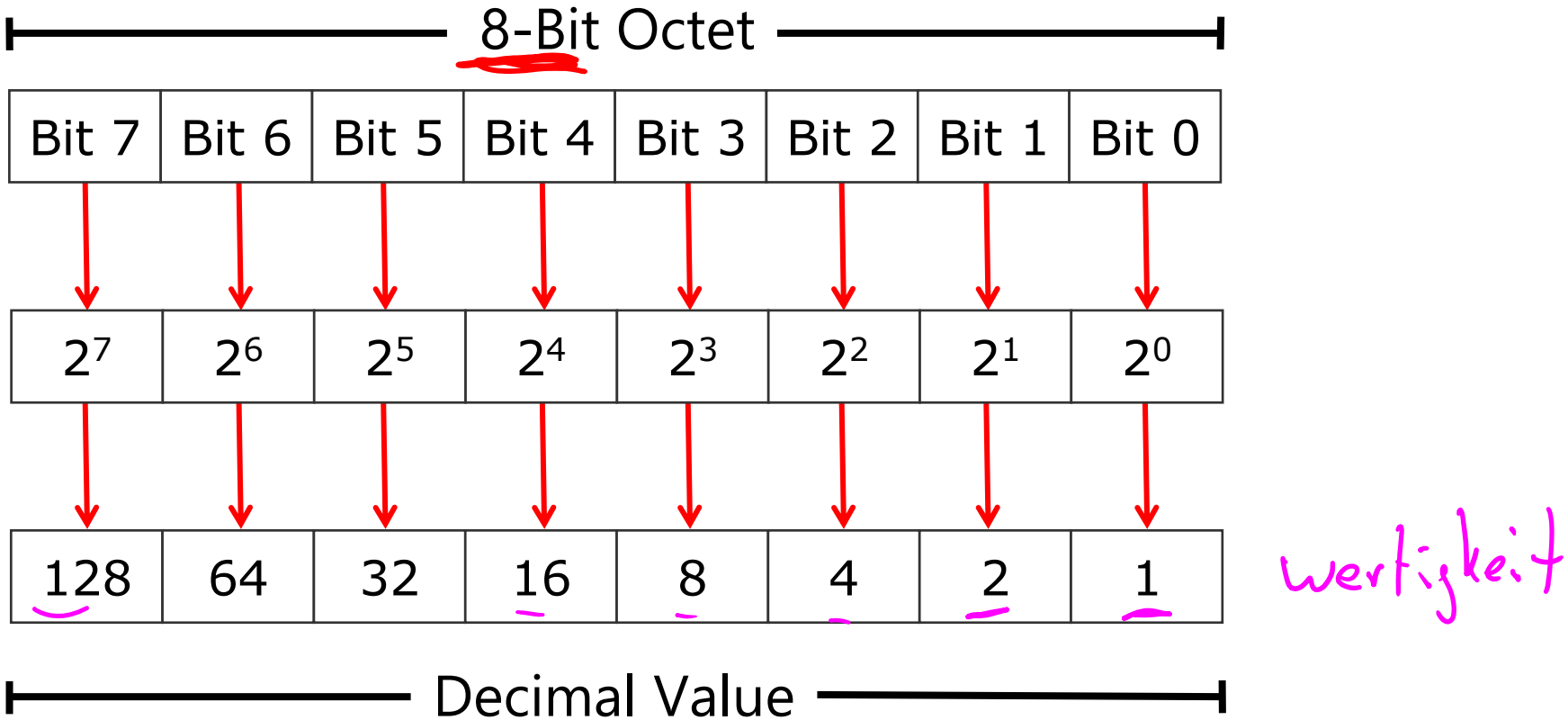
8 Bit

binär	dez
0 0 0 0 0 0 0 0	0
1 1 1 1 1 1 1 1	255

	8 Bit	8 Bit	8 Bit	8 Bit
IP address	**172**	**16**	**0**	**10**
Subnet mask	255	255	0	0
	11111111	11111111	00000000	00000000
Network ID	**172**	**16**	0	0
Host ID	0	0	**0**	**10**

Sitzbuchweg Straße 79 Nr.

IPv4 Addressing



wertigkeit

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

192 224 240 248 252 254 255

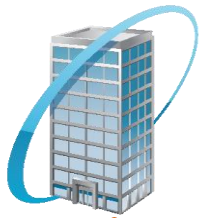
Public, private, and APIPA addresses

Public

- Required by devices and hosts that connect directly to the Internet
- Must be globally unique
- Routable on the Internet
- Must be assigned by IANA/RIR

Private

- Not routable on the Internet
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0./16
- Can be assigned locally by an organization
- Must be translated to access the Internet



RFC

255.255.255.128

125

dec

CIDR

Mask

255.0.0.0

18 — 8 Einser

255.255.255.0

124

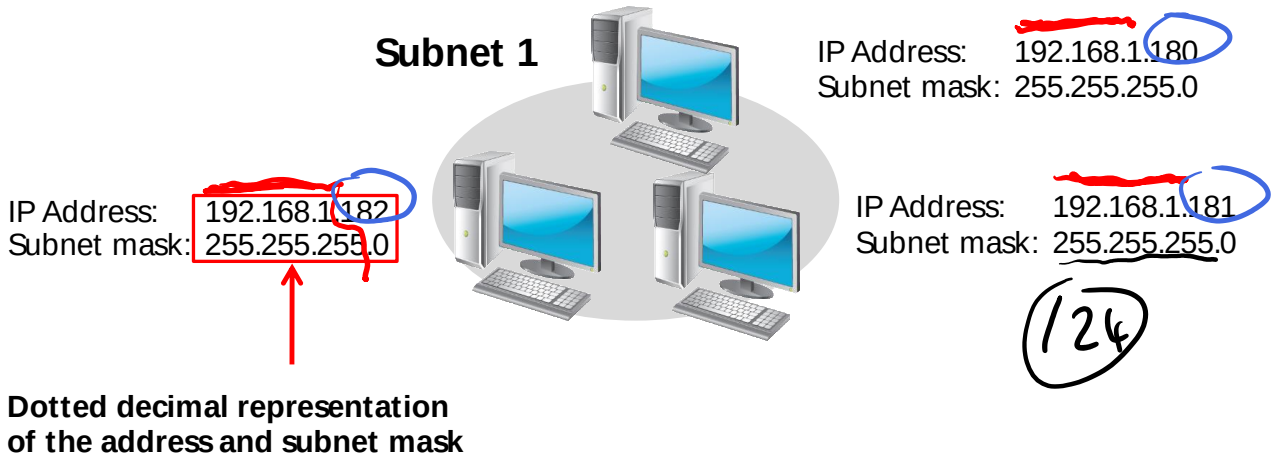
IPv4 Addressing

176.16.0.3/32 Def. dieser Comp

/30

2 Bit → 2 Computer

An IPv4 configuration identifies a computer to other computers on a network



Host

/24

8 Bit für Hosts

$2^8 = 256$

−2 Netz IP Broadcast

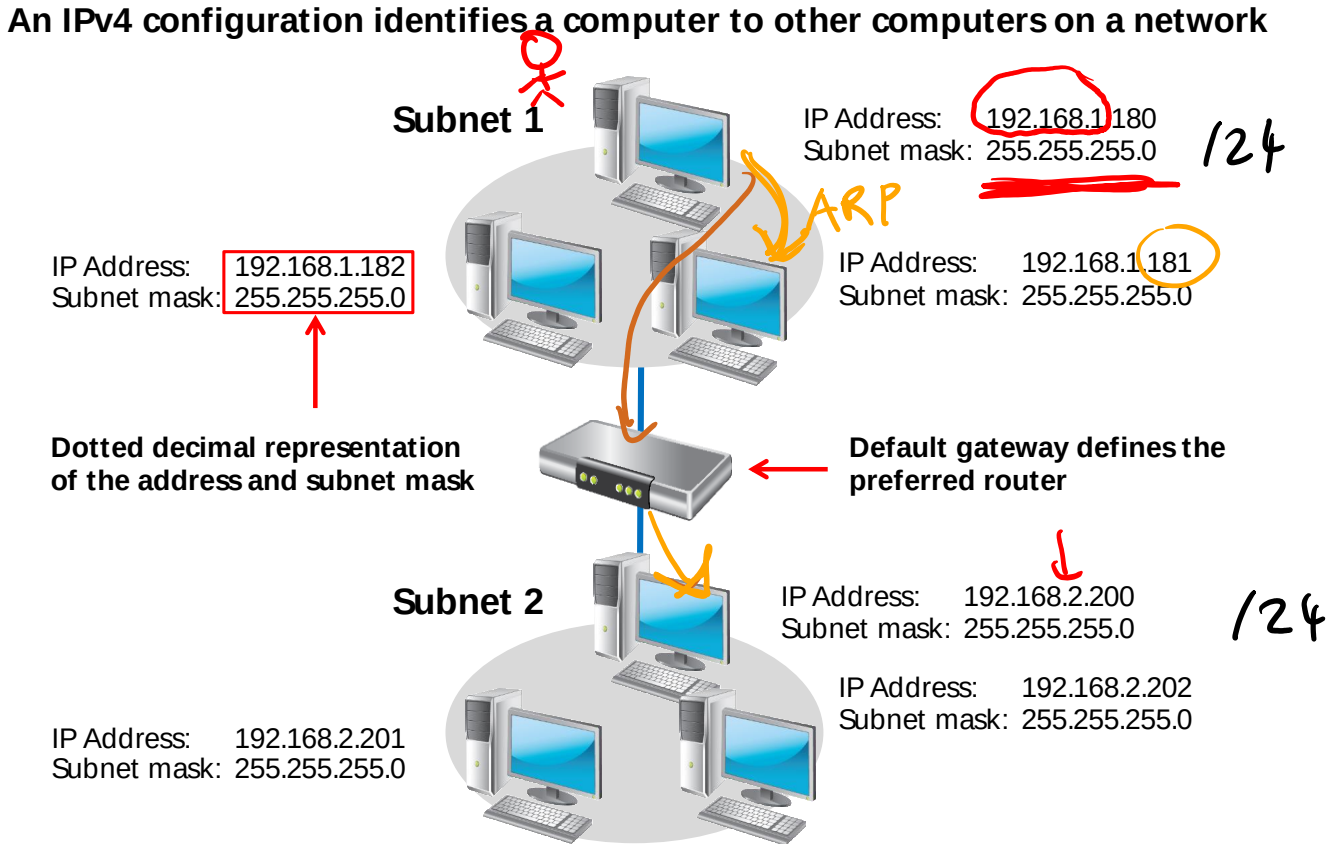
254 Computer

/16

16 Bit Host

65.534 Comp

IPv4 Addressing



Route Table

Default GW

/24

/24

Router = GW

The Benefits of Using Subnetting (1 of 2)

When you subdivide a network into subnets, you create a unique ID for each subnet that is derived from the main network ID

The Benefits of Using Subnetting (2 of 2)

- By using subnets, you can:
  - Use a single network address across multiple locations
  - Reduce network congestion by segmenting traffic
  - Increase security by using firewalls
  - Overcome limitations of current technologies

Lesson 2: IPv6 Fundamentals

brainymotion

IPv6 Fundamentals

Overview of IPv4 addressing

brainymotion

Overview of IPv6 addressing

- 128-bit address in binary:

  00100000000000010000110110111000

  00000000000000000010110101001100

  00000001110011000000000011011101

  00010001001000100001001000110100

- 128-bit address divided into 16-bit blocks:

  0010000000000001 0000110110111000

  0000000000000000 0010110101001100

  0000000111001100 0000000011011101

  0001000100100010 0001001000110100

- Each 16-bit block converted to hexadecimal (base 16):

  2001:0DB8:0000:2D4C:01CC:00DD:1122:1234

- Further simplified by removing leading zeros:

  2001:DB8:0:2D4C:1CC:DD:1122:1234

Overview of IPv6 addressing

[0010][1101][0100][1100]

8 4 2 1
[0 0 1 0]
0+0+2+0=2

[1 1 0 1]
8+4+0+1=D

[0 1 0 0]
0+4+0+0=4

[1 1 0 0]
8+4+0+0=C

= 2D4C

IPv6 address structure

- The number of network bits is defined by the prefix
- Each host has 64 bits allocated to the interface identifier

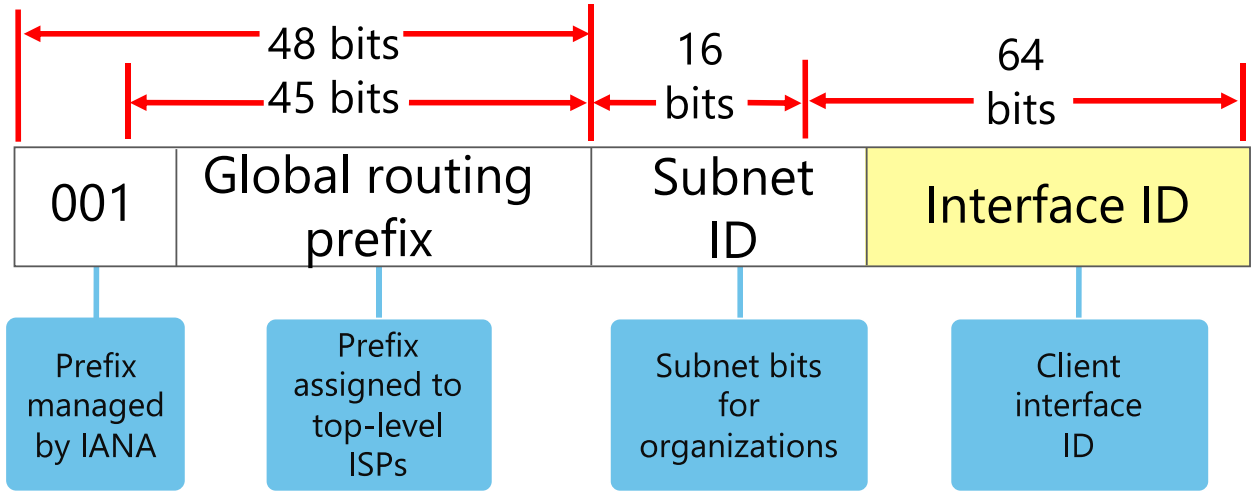
Type of address	**IPv4 address**	**IPv6 address**
Unspecified	0.0.0.0	::
Loopback	127.0.0.1	::1
Autoconfigured	169.254.0.0/16	FE80::/64
Broadcast	255.255.255.255	Uses multicasts instead
Multicast	224.0.0.0/4	FF00::/8

Types of IPv6 addresses

- The following are types of unicast IPv6 addresses:
  - Global unicast addresses
  - Unique local addresses
  - Link-local addresses
  - Site-local addresses:
    - Formerly deprecated in RFC 3879
    - Superseded by unique local addresses
  - Special addresses
  - Compatibility or transition addresses

Types of IPv6 addresses

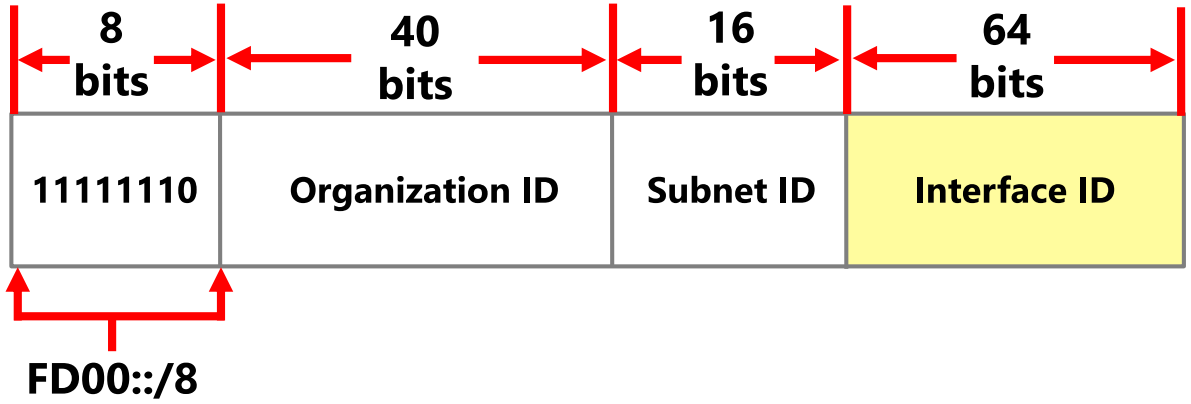
- Global unicast addresses:
  - Are routable on the IPv6 Internet
  - Allocate 16 bits for internal subnetting
  - Begin with 2 or 3 (2000::/3)



brainymotion

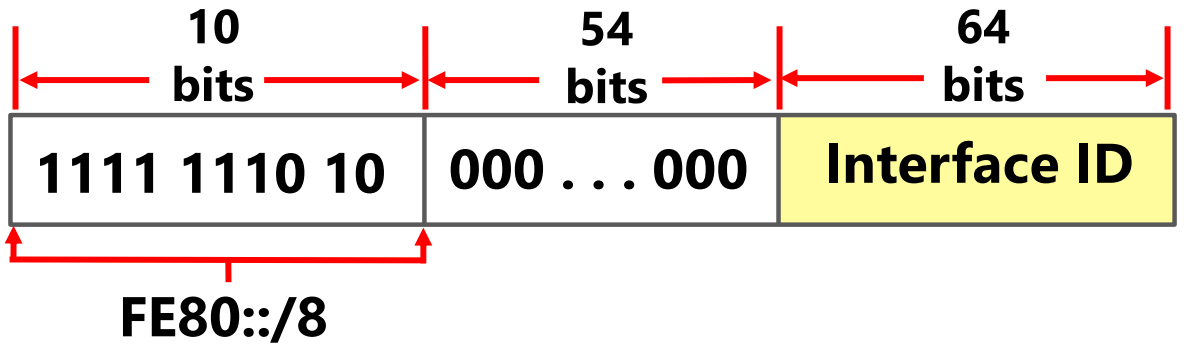
Types of IPv6 addresses

- Unique local addresses:
  - Are equivalent to IPv4 private addresses
  - Require the organization ID to be randomly generated
  - Allocate 16 bits for internal subnetting



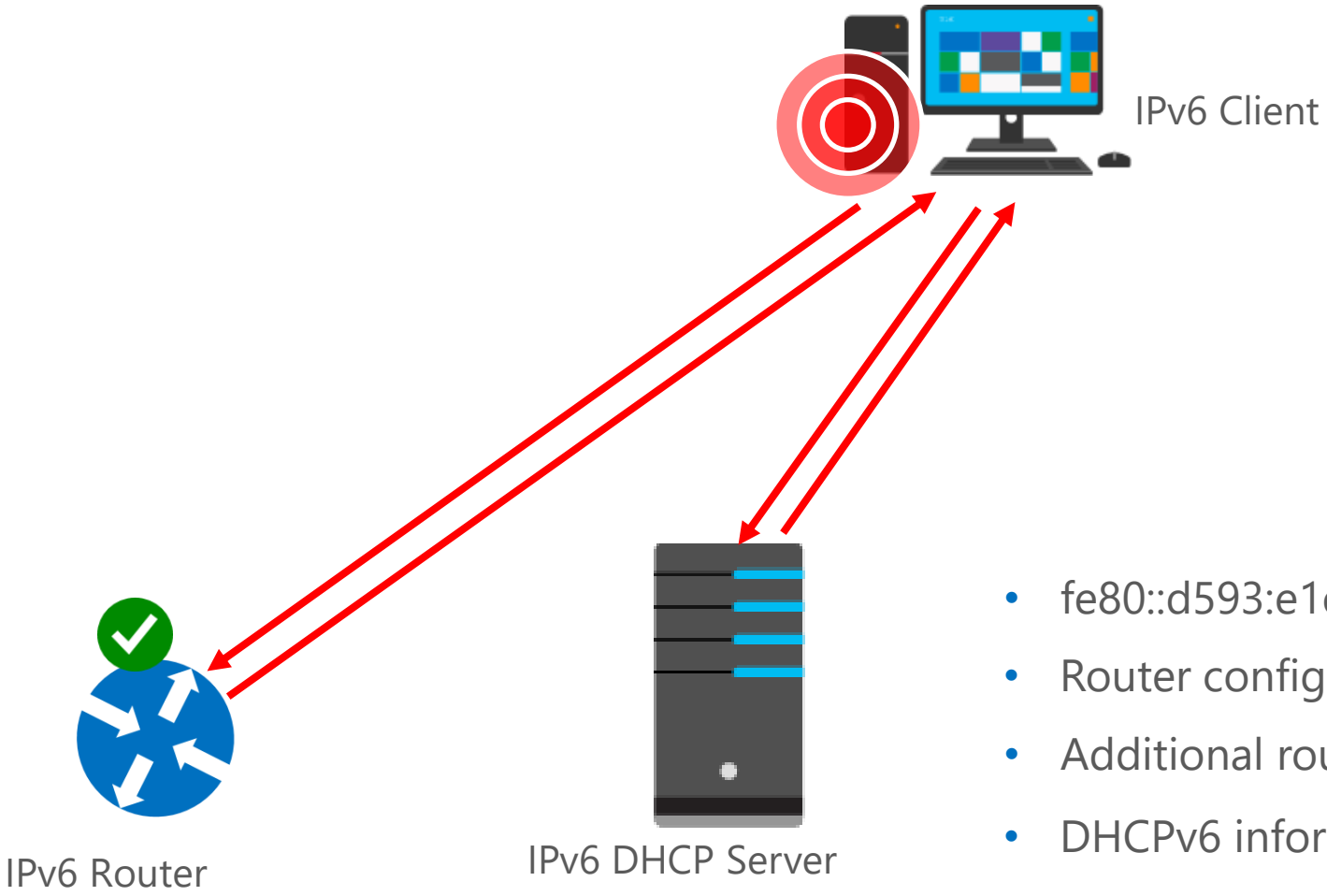
Types of IPv6 addresses

- Link-local addresses:
  - Are automatically generated on all IPv6 hosts
  - Are similar to IPv4 APIPA addresses
  - Are sometimes used in place of broadcast messages
  - Include a zone ID that identifies the interface
  - Examples:
    - fe80::2b0:d0ff:fee9:4143%3
    - fe80::94bd:21cf:4080:e612%2



IPv6 Auto configuration

1 Derive Link-Local Address



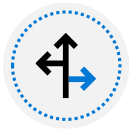
- fe80::d593:e1e:e612:53e4%10
- Router configuration information
- Additional router prefixes
- DHCPv6 information received

Lesson 3: Dynamic Host Configuration Protocol (DHCP)

brainymotion

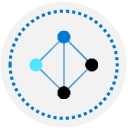
Dynamic Host Configuration Protocol (DHCP)

Benefits of using DHCP



How DHCP allocates addresses

How DHCP lease generation works



How DHCP lease renewal works

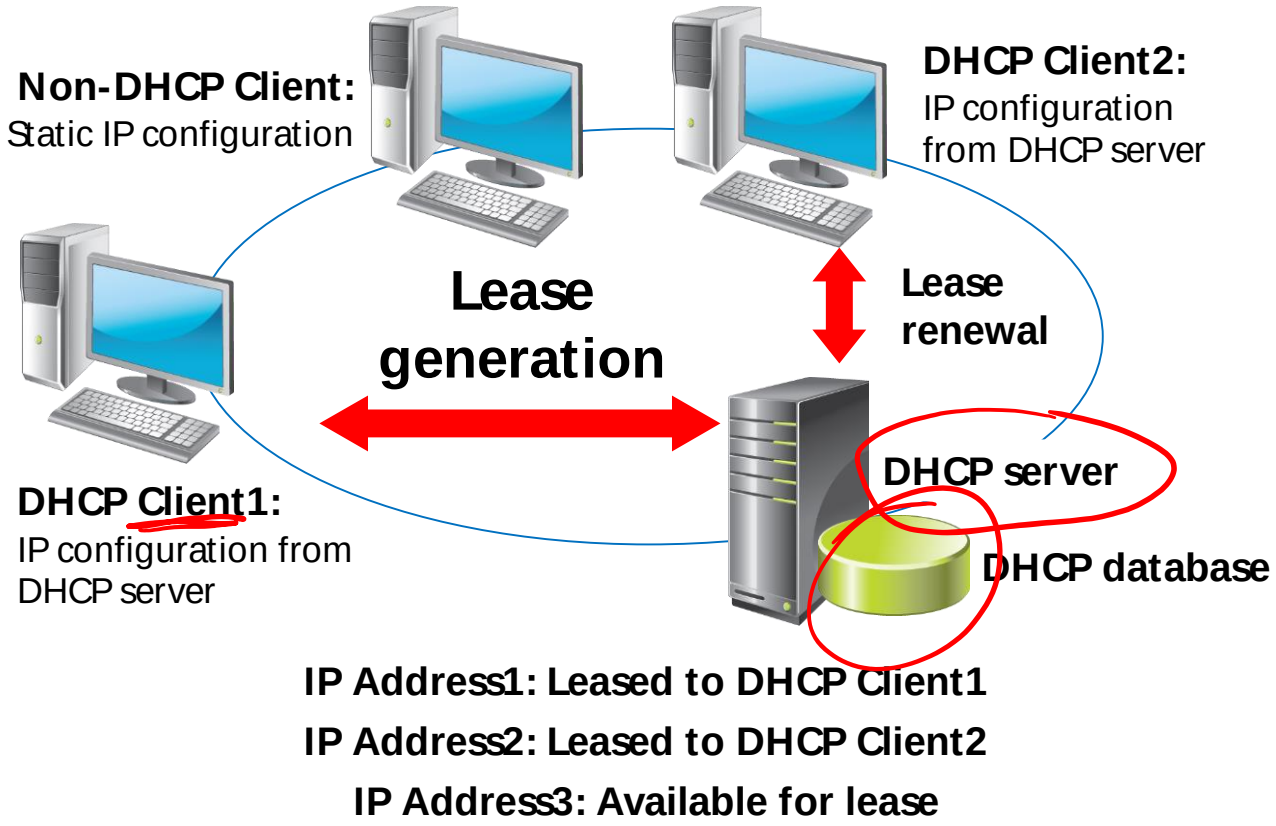
DHCP scope and options

Benefits of Using DHCP

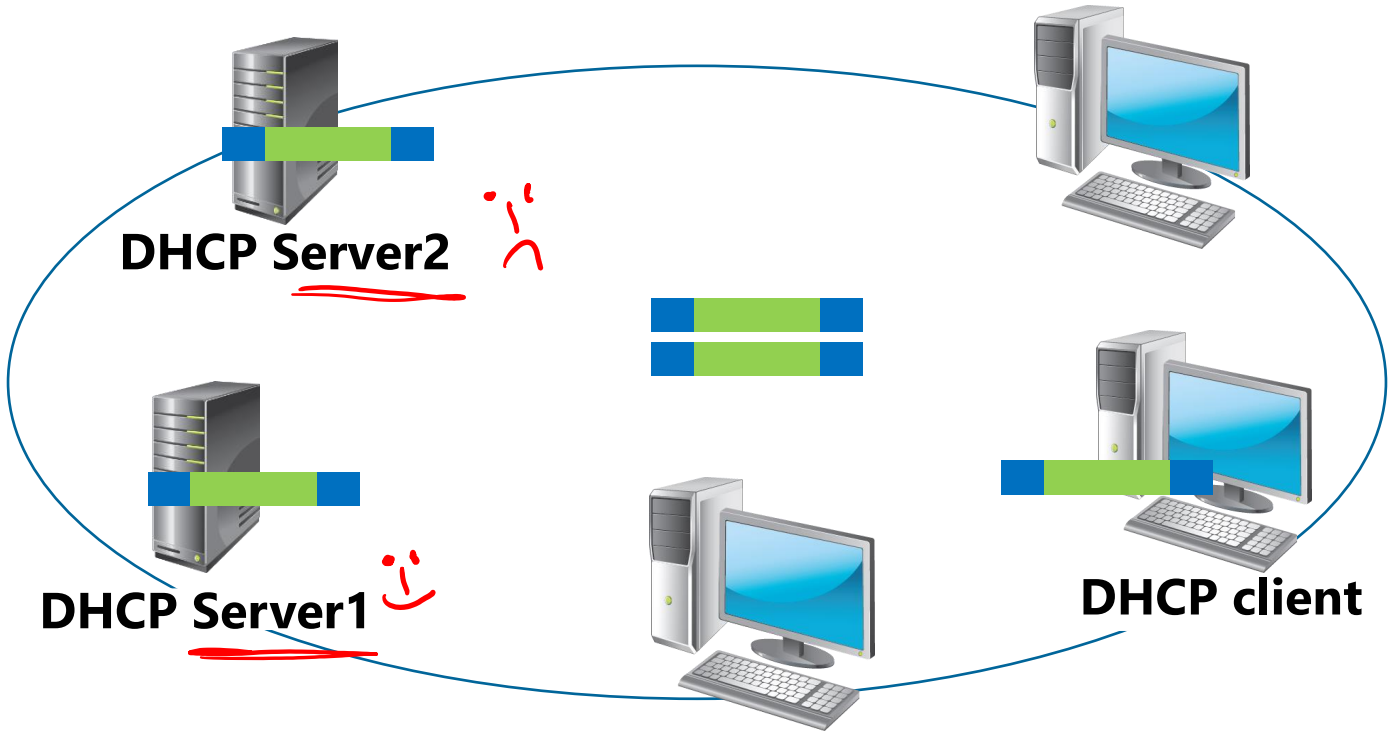
DHCP reduces the complexity and amount of administrative work by using automatic IP configuration

Automatic IP Configuration	Manual IP Configuration
IP addresses are supplied automatically	IP addresses are entered manually
Correct configuration information is ensured	IP address could be entered incorrectly
Client configuration is updated automatically	Communication and network issues can result
A common source of network problems is eliminated	Frequent computer moves increase administrative effort

How DHCP Allocates IP Addresses

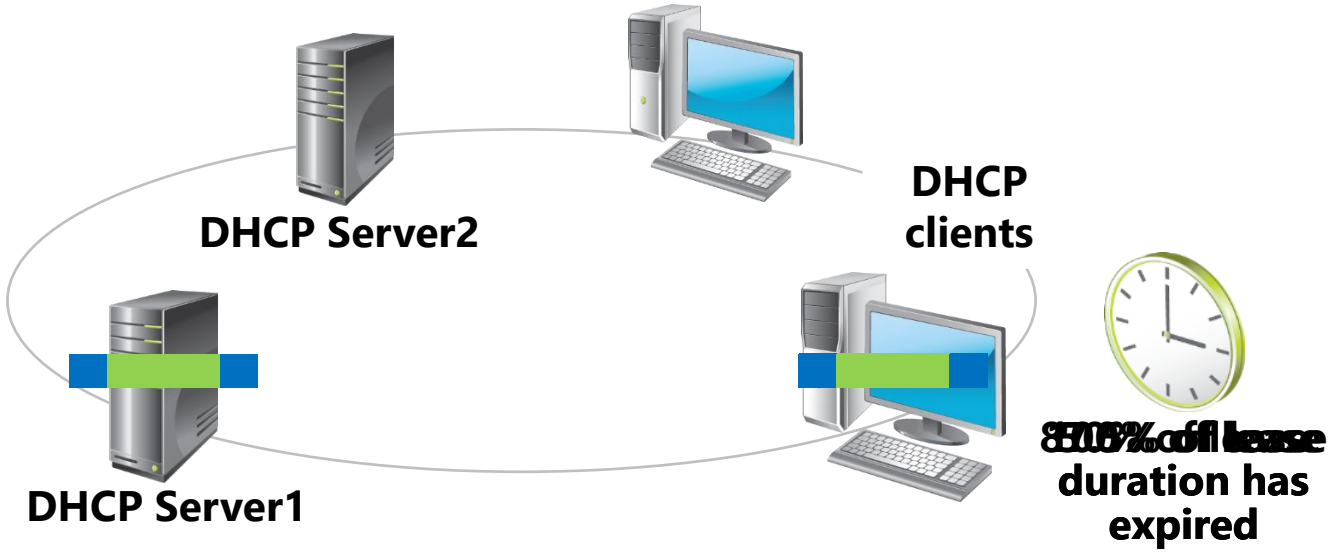


How DHCP Allocates IP Addresses



1. DHCP client broadcasts a DHCPDISCOVER packet
2. DHCP servers broadcast a DHCPOFFER packet
3. DHCP client broadcasts a DHCPREQUEST packet
4. DHCP Server1 broadcasts a DHCPACK packet

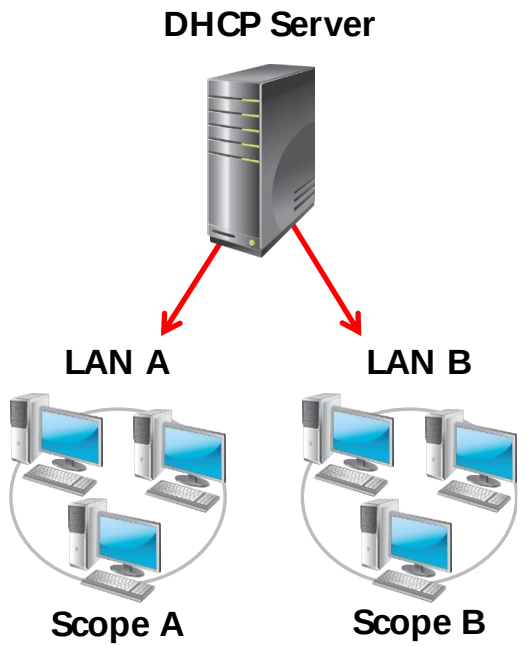
How DHCP Allocates IP Addresses



1. DHCP client sends a DHCPREQUEST packet
2. DHCP Server1 sends a DHCPACK packet
3. If the client fails to renew its lease after 50% of the lease duration has expired, the DHCP lease renewal process begins again after 87.5% of the lease duration has expired
4. If the client fails to renew its lease after 87.5% of the lease has expired, the DHCP lease generation process starts over again with a DHCP client broadcasting a DHCPDISCOVER

DHCP scope and options

- A DHCP scope is a range of IP addresses that are available to be leased
- DHCP scope properties include:
  - Network ID
  - Lease duration
  - Scope name
  - Subnet mask
  - Network IP address range
  - Exclusion range



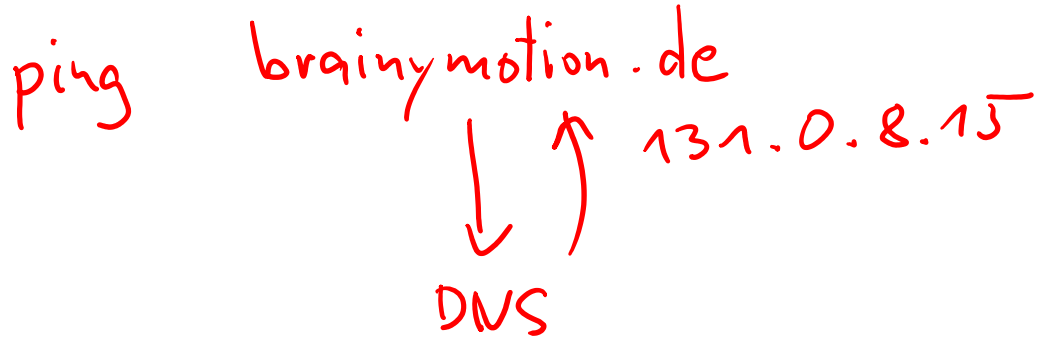
brainymotion

DHCP scope and options

- You must create scopes to define the network information that will be distributed to clients
- A scope must contain:
  - A range of IP addresses
  - A subnet mask
  - A lease duration
- A scope might contain:
  - Default gateway address
  - DNS server and suffix
  - Other network options
- IP addresses can be reserved based on the MAC address of the client network interface

DHCP scope and options

- DHCP options:
  - Are values for common configuration data
  - Can be applied to the server, scope, class, and reservation level
- Common scope options include:
  - Router (Default gateway)
  - DNS domain name
  - DNS servers

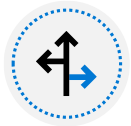


Lesson 4: Domain Name Service (DNS)

brainymotion

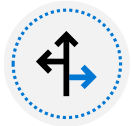
Domain Name Service (DNS)

How does DNS name resolution work?



DNS components

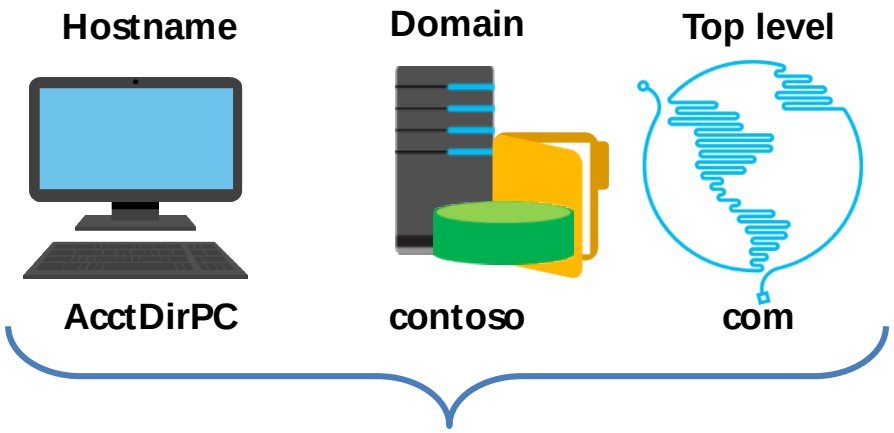
What are DNS zones and records?



Tools and techniques for troubleshooting name resolution

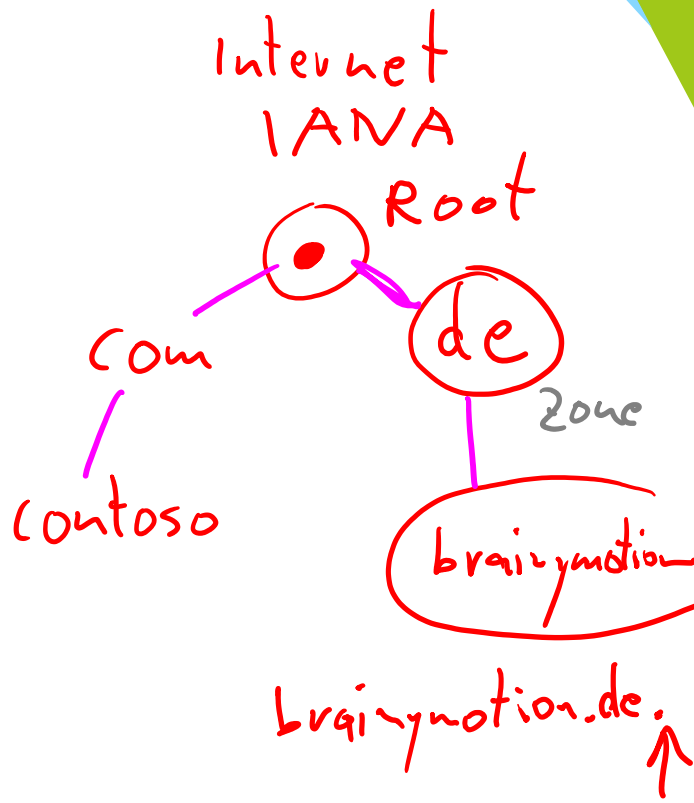
How does DNS name resolution work?

A *hostname* is a computer name that is added to a domain name and top level domain to make a fully qualified domain name (FQDN)

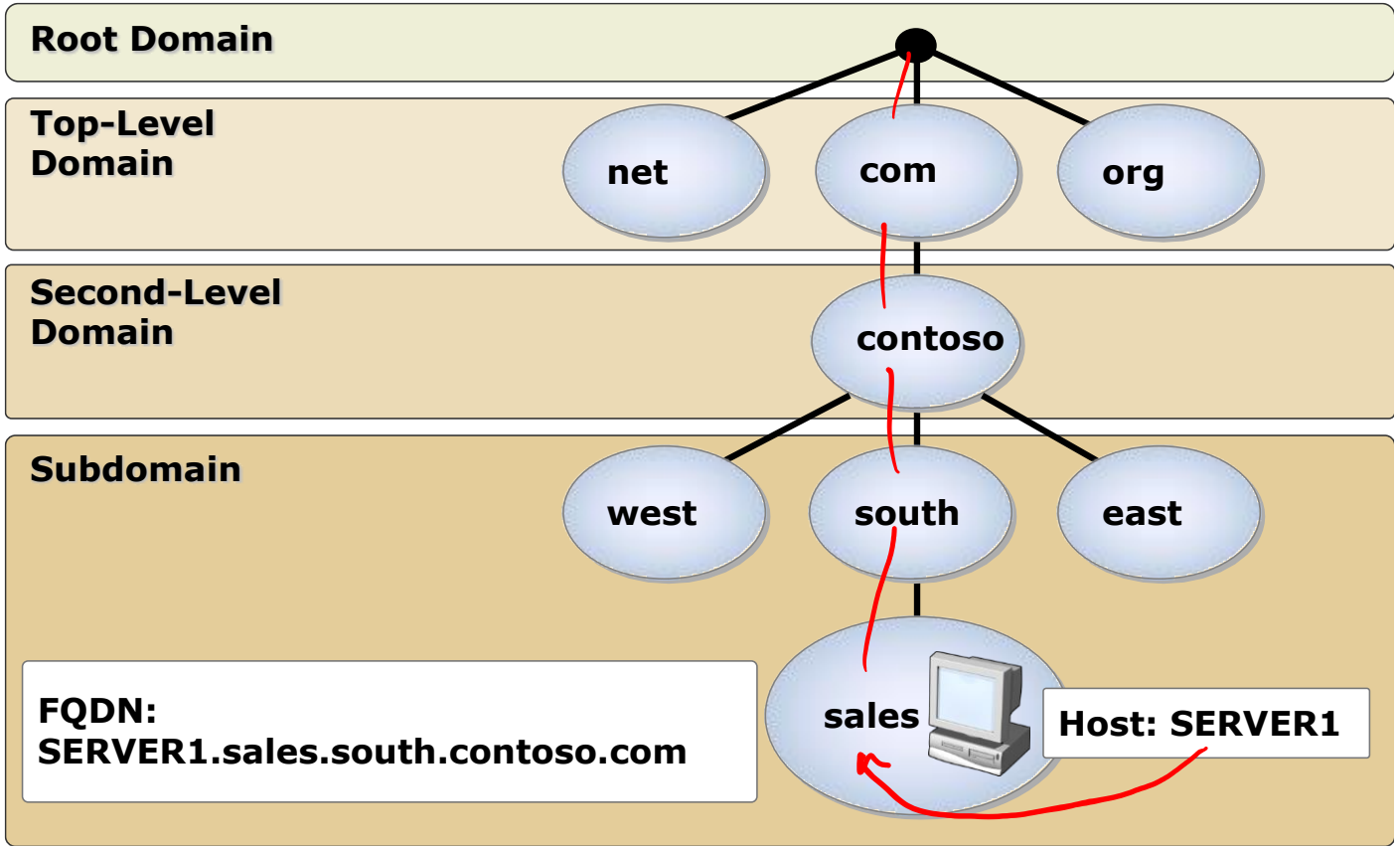


Fully qualified domain name = AcctDirPC.contoso.com

NetBIOS names are rarely used and are being deprecated in Windows operating systems



How does DNS name resolution work?



Zone DB (File)

SOA

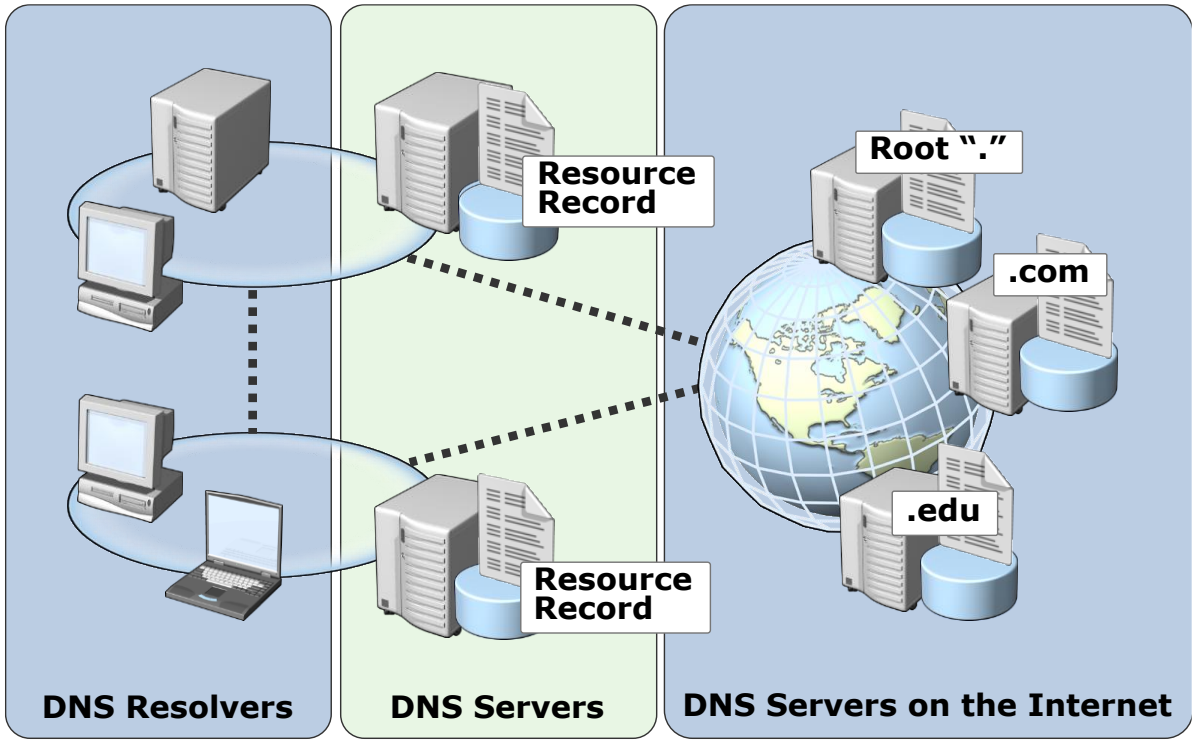
Server1 A 10.0.0.1

AAAA 2001::1

www CNAME Server1 (Alias)

Zone Resource Records z.B. SOA A AAAA NS

DNS components



What are DNS zones and records?

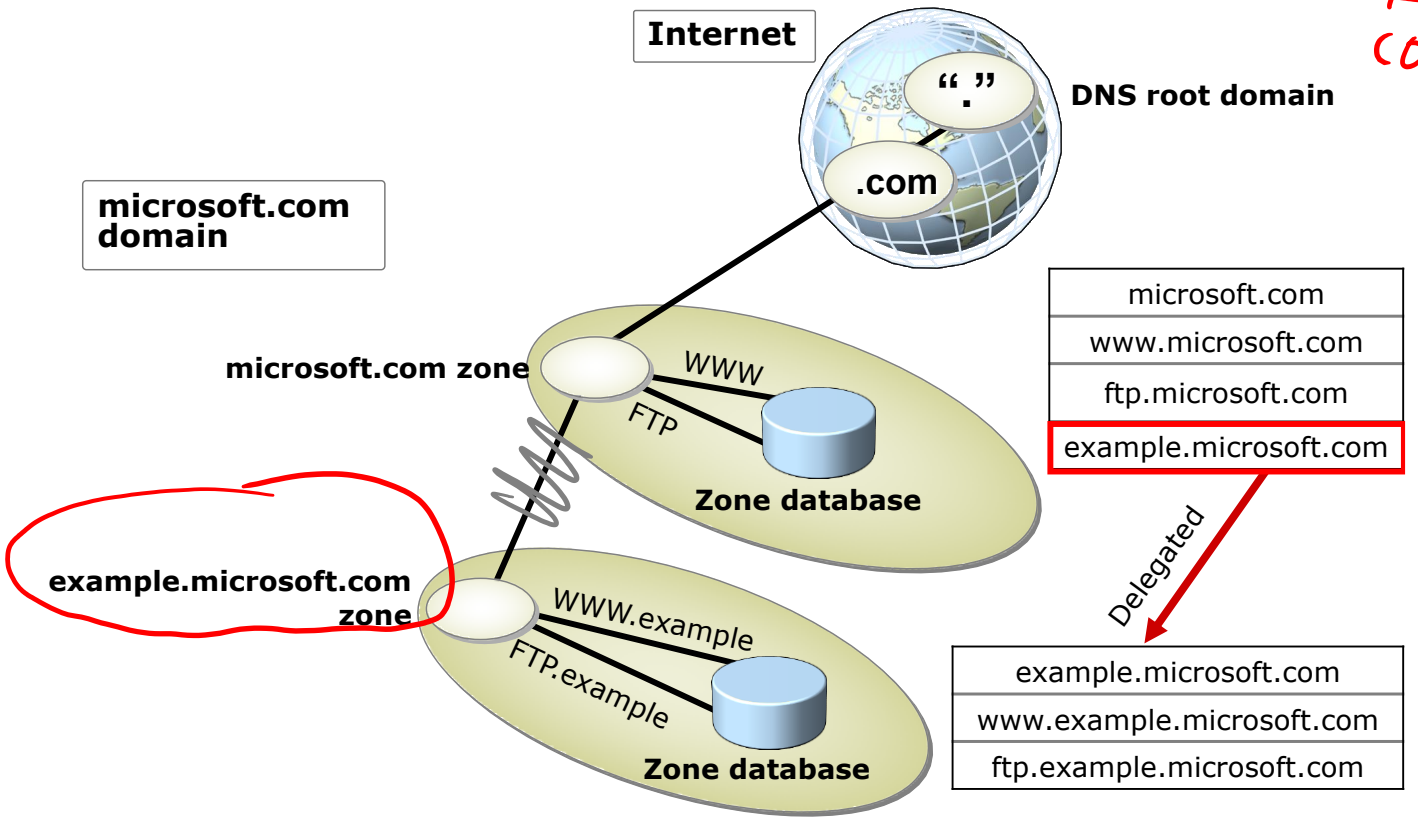
DNS resource records include:

- **SOA: Start of Authority**
- **A: Host Record**
- **CNAME: Alias Record**
- **MX: Mail Exchange Record**
- **SRV: Service Resources**
- **NS: Name Servers**
- **AAAA: IPv6 DNS Record**
- **PTR: Pointer Record**

nslookup

Resolve-DNSName

What are DNS zones and records?



AD braucht DNS

contoso.com

contoso.com

SOA

A

SRV

What are DNS zones and records?

Zones	Description
Primary	Read/write copy of a DNS database
Secondary	Read-only copy of a DNS database
Stub	Copy of a zone that contains only records used to locate name servers
Active Directory–integrated	Zone data is stored in AD DS rather than in zone files

File

File

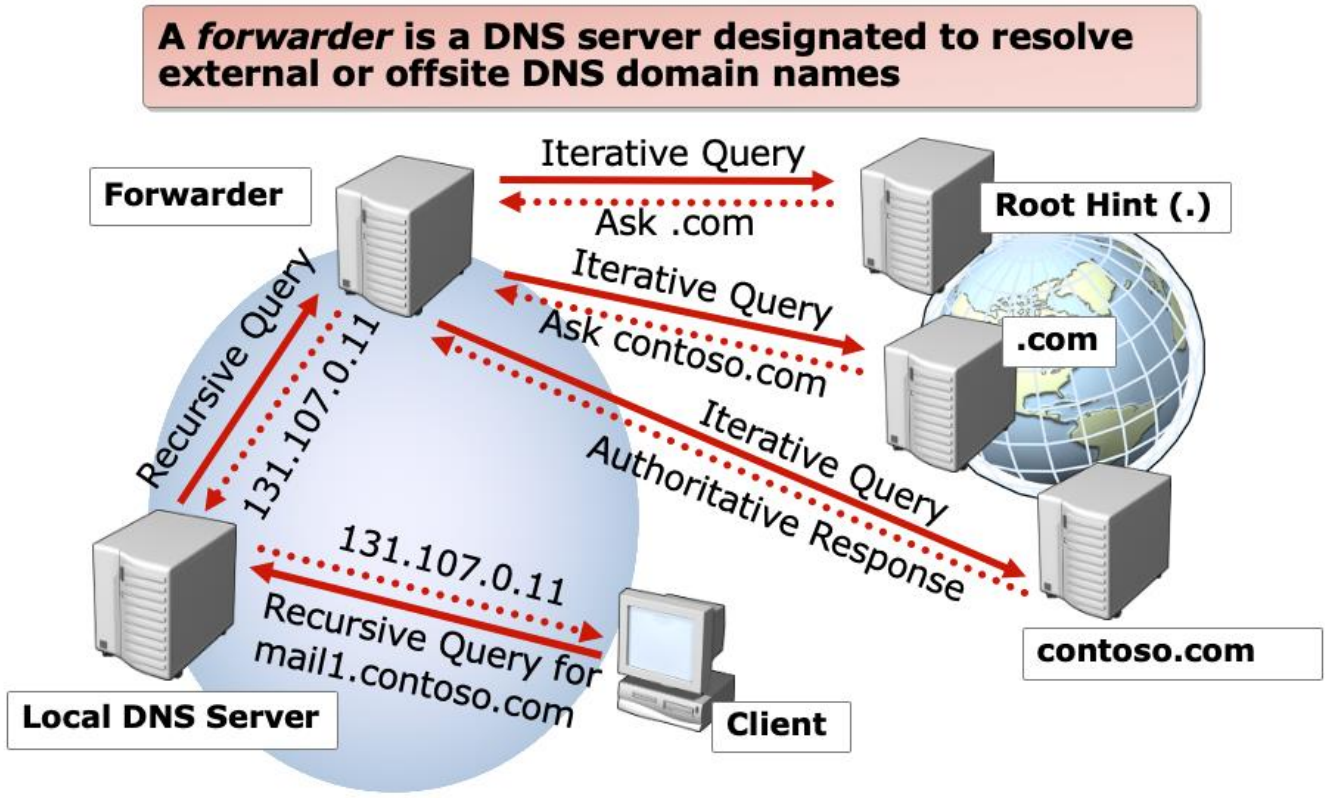
LDAP

A
A
CName

DC1 DC2 DC3

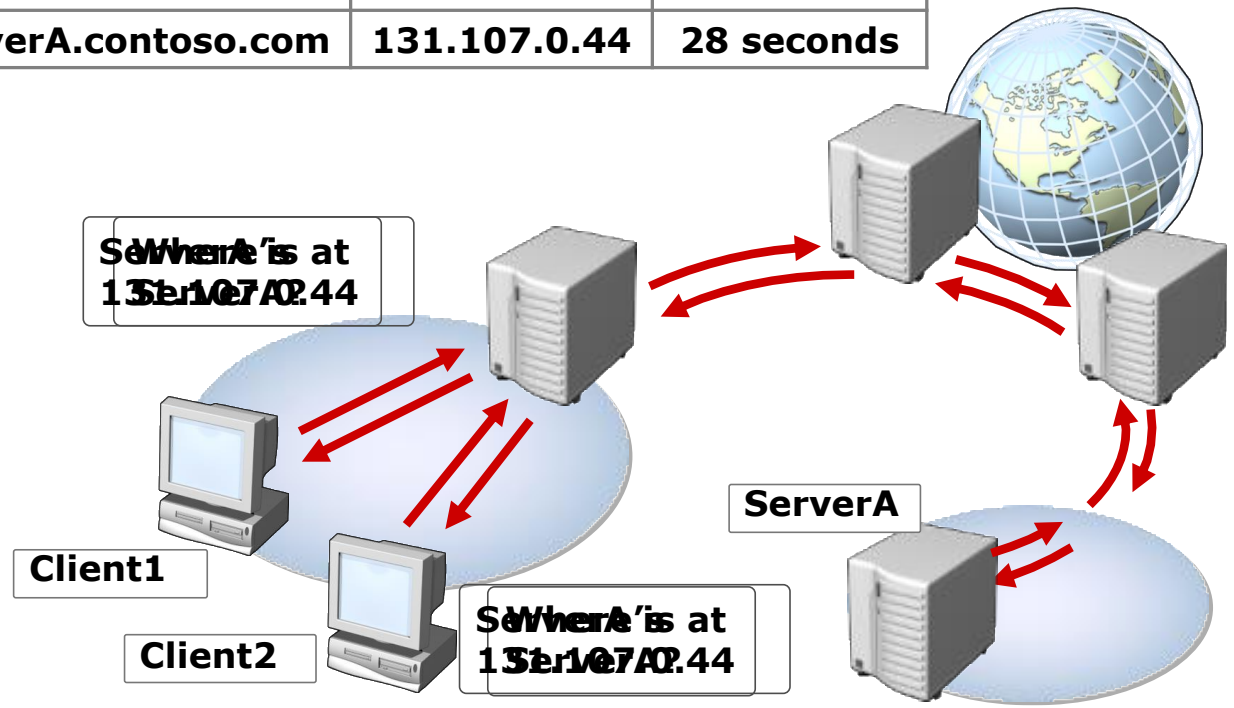
brainymotion

What are DNS zones and records?



What are DNS zones and records?

DNS server cache		
Host name	IP address	TTL
ServerA.contoso.com	**131.107.0.44**	**28 seconds**

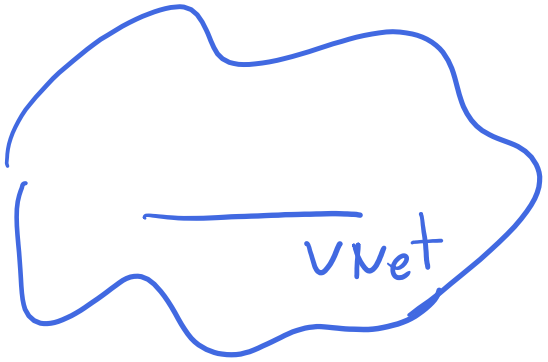


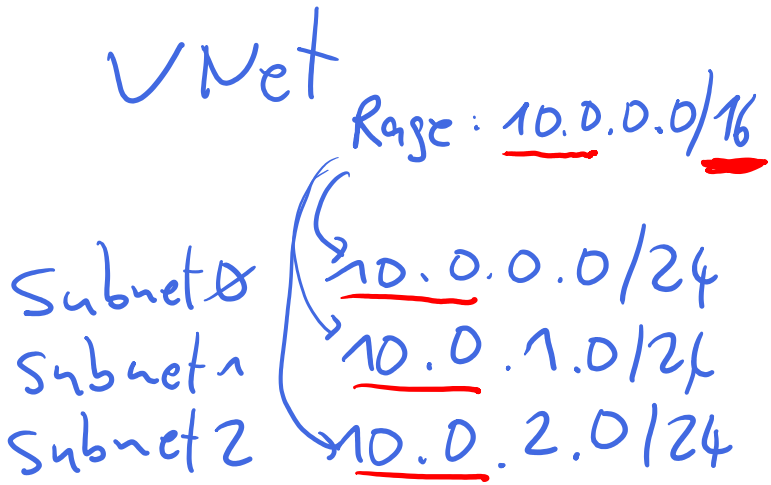
Tools and techniques for troubleshooting name resolution

- Command-line tools to troubleshoot configuration issues:
  - Nslookup
  - DNSCmd
  - DNSlint
  - Ipconfig
- PowerShell:
  - Get-DnsClientServerAddress
  - Clear-DnsClientCache
  - Resolve-DnsName
  - Register-DnsClient

Tools and techniques for troubleshooting name resolution

- The troubleshooting process:
  - Identify client DNS server with nslookup or Resolve-DnsName
  - Communicate via ping
  - Use nslookup to verify records

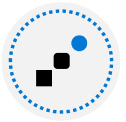




Lesson 4: Azure network Fundamentals

brainymotion

Azure network Fundamentals



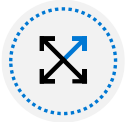
Plan Virtual Networks

Create Subnets

Create Virtual Networks

Plan IP Addressing

Create Public IP Addresses

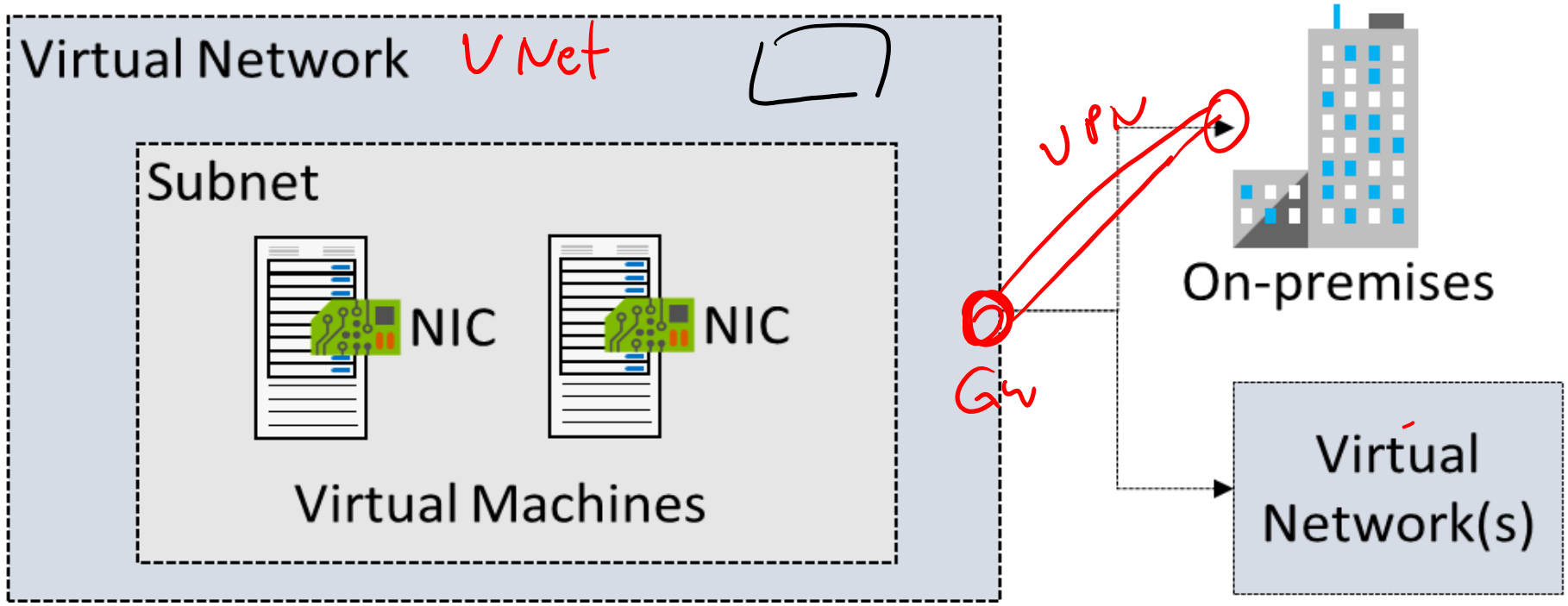


Associate Public IP Addresses

Associate Private IP Addresses

brainymotion

Plan Virtual Networks



Logical representation of your own network

Create a dedicated private cloud-only virtual network

Securely extend your datacenter with virtual networks

Enable hybrid cloud scenarios

brainymotion

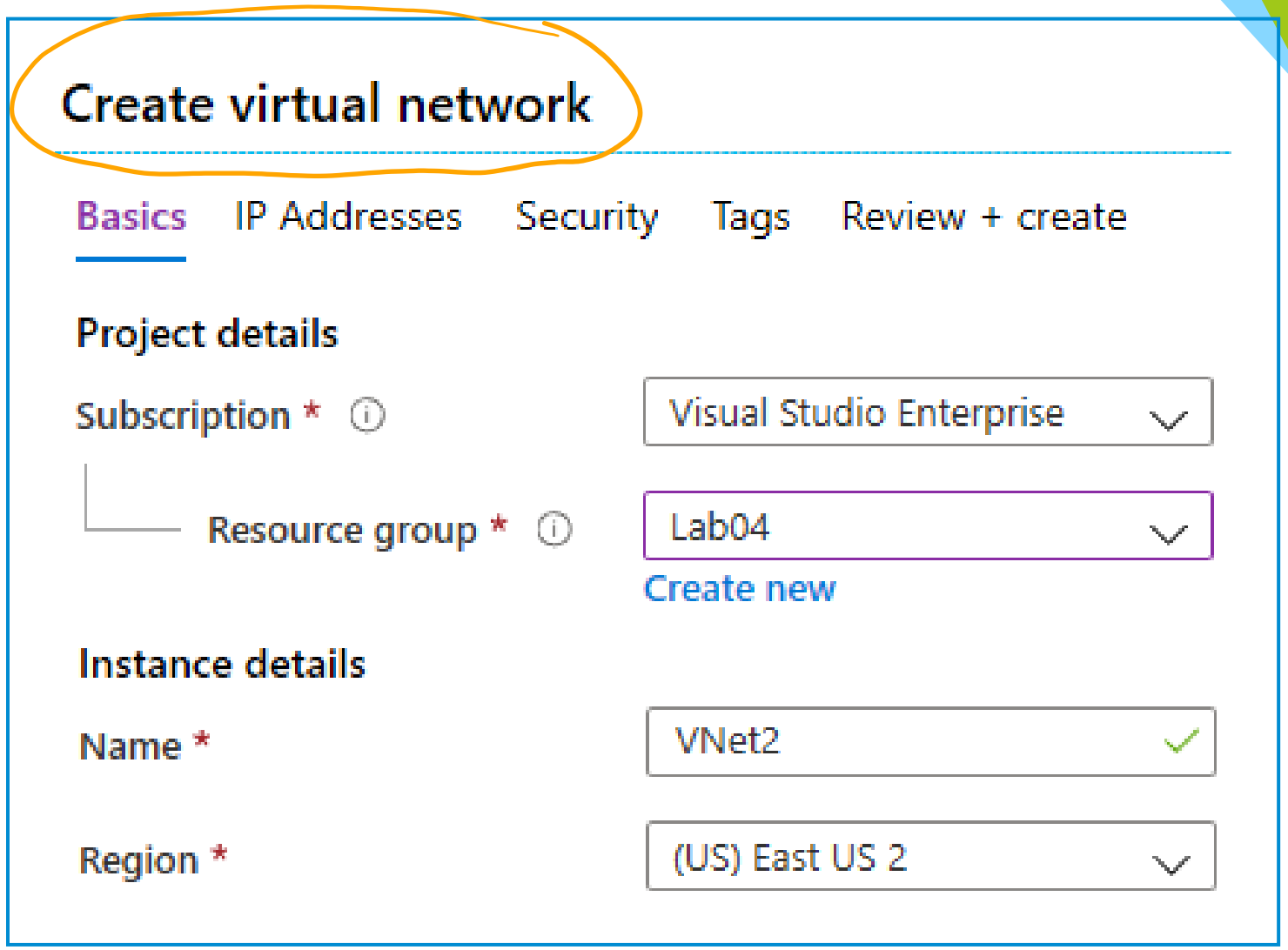
Create Virtual Networks

Create new virtual networks at any time

Add virtual networks when you create a virtual machine

Need to define the address space, and at least one subnet

Be careful with overlapping address spaces

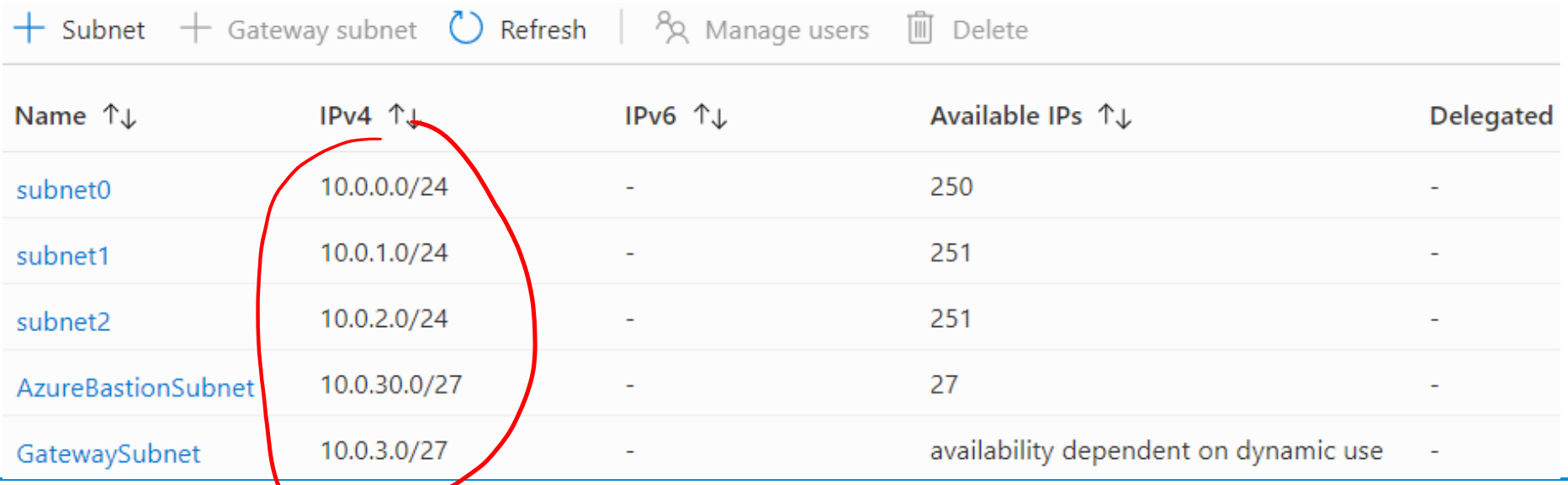


brainymotion

Create Subnets

Private

Public IP Address



10/8
172.16/12
192.168/16

A virtual network can be segmented into one or more subnets

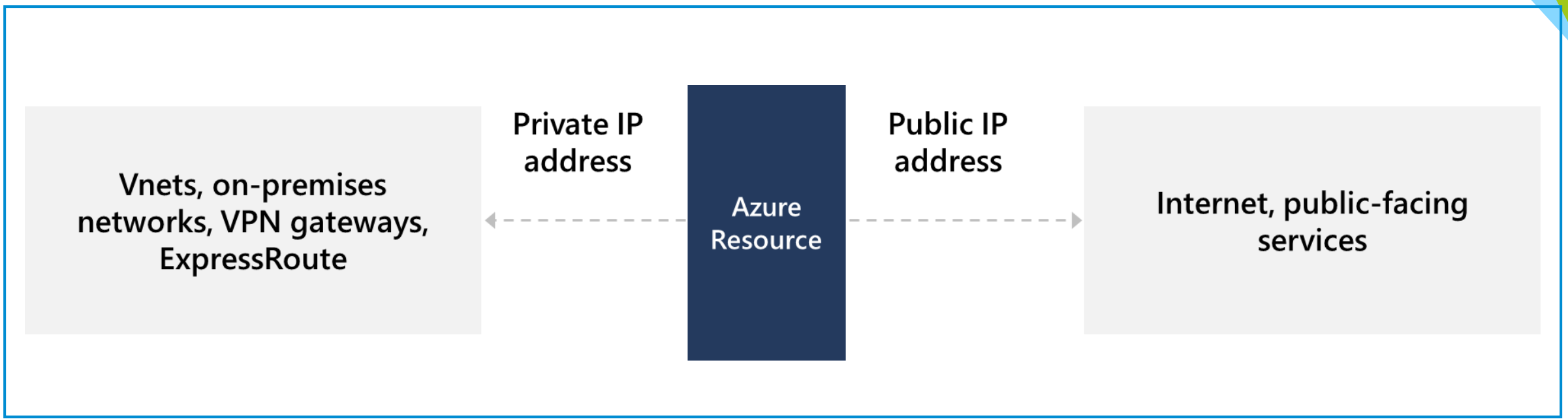
Subnets provide logical divisions within your network

Subnets can help improve security, increase performance, and make it easier to manage the network

Each subnet must have a unique address range – cannot overlap with other subnets in the vnet in the subscription

brainymotion

Plan IP Addressing



Private IP addresses - used within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure

Public IP addresses - used for communication with the Internet, including Azure public-facing services

Associate Public IP Addresses

Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load Balancer	Front-end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	Yes*
Application Gateway	Front-end configuration	Yes	Yes*

A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways

*Static IP addresses only available on certain SKUs.

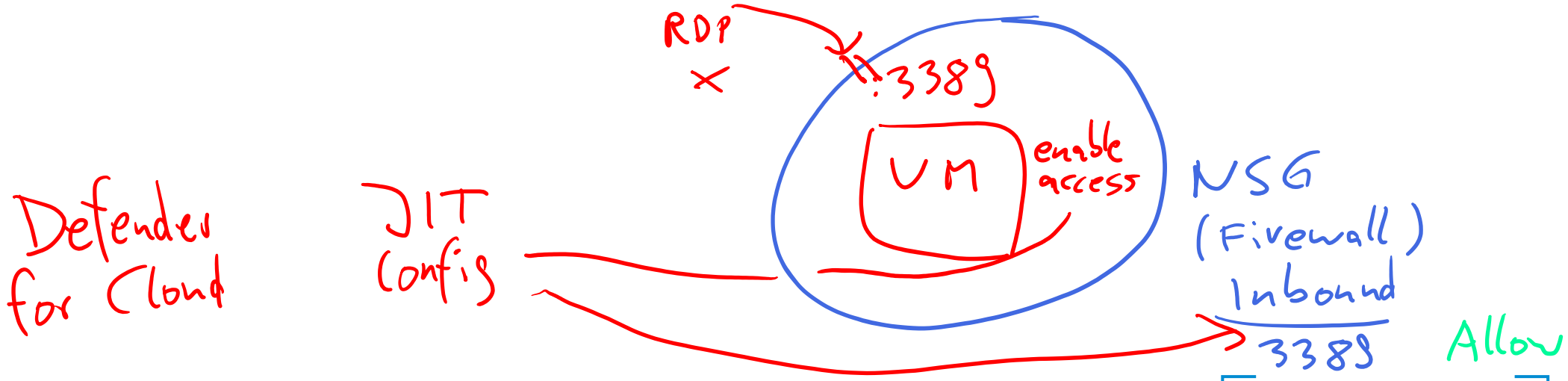
brainymotion

Associate Private IP Addresses

Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Internal Load Balancer	Front-end configuration	Yes	Yes
Application Gateway	Front-end configuration	Yes	Yes

Dynamic (default). Azure assigns the next available unassigned or unreserved IP address in the subnet's address range

Static. You select and assign any unassigned or unreserved IP address in the subnet's address range



Lesson 5: Configure Network Security Groups

brainymotion

Configure Network Security Groups Introduction

Implement Network Security Groups (NSG)

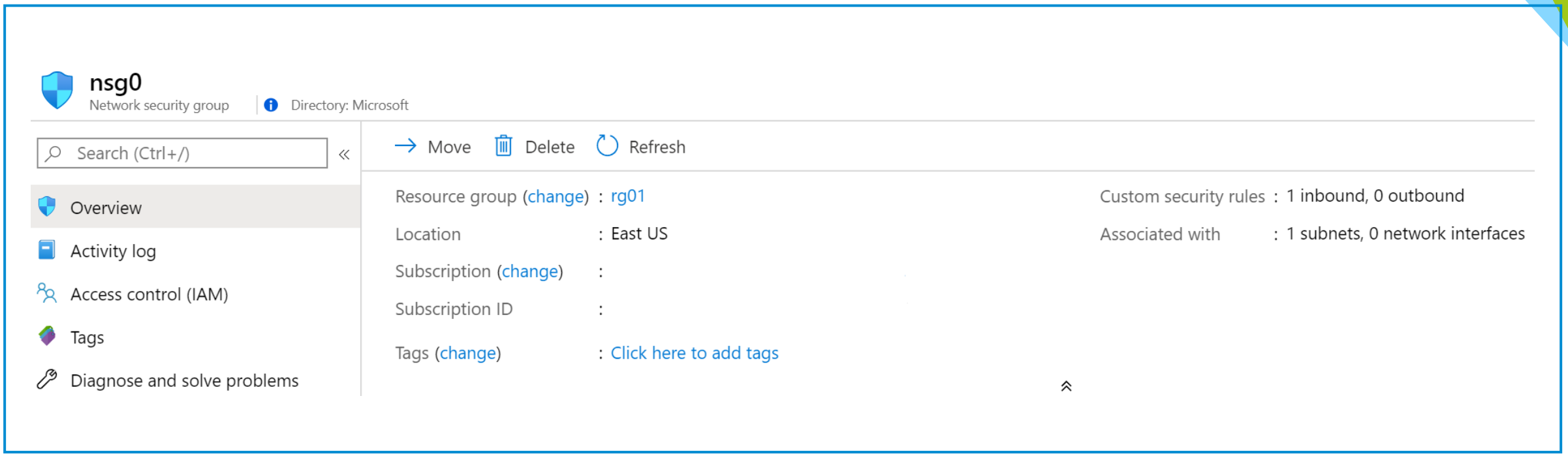
Determine NSG Rules

Determine NSG Effective Rules

Create NSG Rules

brainymotion

Implement Network Security Groups



Limits network traffic to resources in a virtual network

Lists the security rules that allow or deny inbound or outbound network traffic

Associated to a subnet or a network interface

Can be associated multiple times

brainymotion

Determine NSG Rules

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	⚠ RDP_Inbound	3389	Any	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces

There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

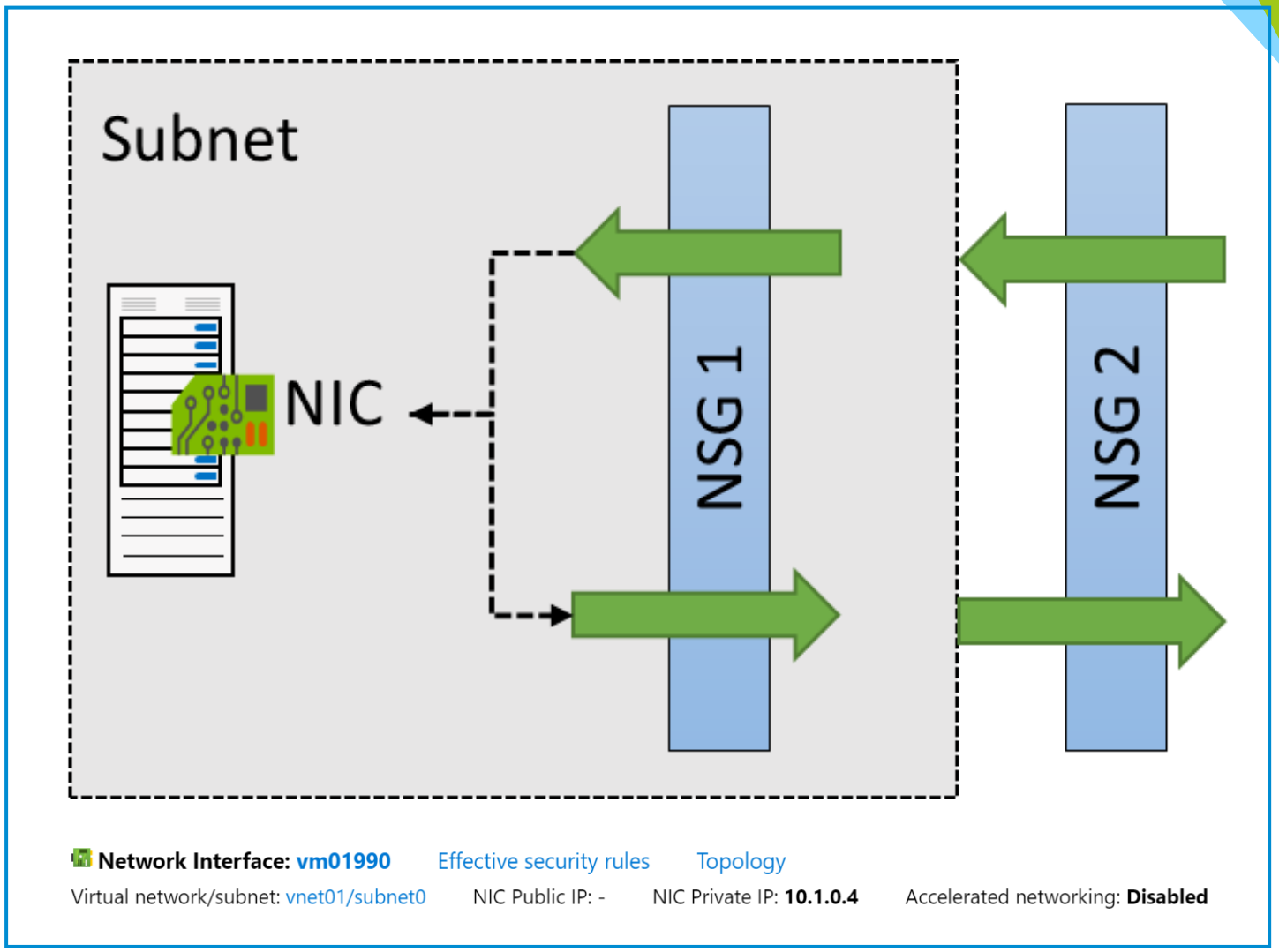
brainymotion

Determine NSG Effective Rules

NSGs are evaluated independently for the subnet and NIC

An “allow” rule must exist at both levels for traffic to be admitted

Use the Effective Rules link if you are not sure which security rules are being applied



brainymotion

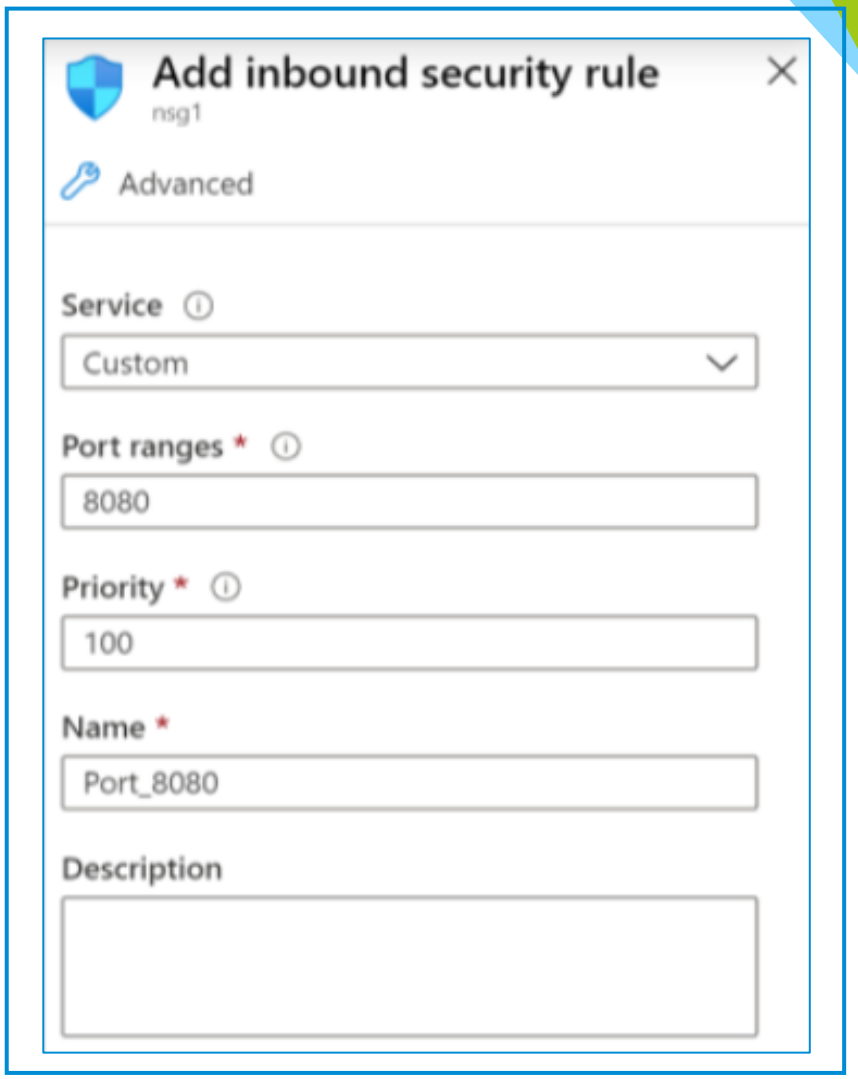
Create NSG rules

Select from a large variety of services

Service – The destination protocol and port range for this rule

Port ranges – Single port or multiple ports

Priority – The lower the number, the higher the priority



brainymotion

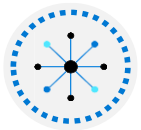
Lesson 6: Configure Azure DNS

brainymotion

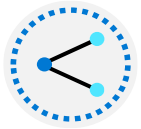
Configure Azure DNS

Identify Domains and Custom Domains

Verify Custom Domain Names



Create Azure DNS Zones



Delegate DNS Domains

Add DNS Record Sets

brainymotion

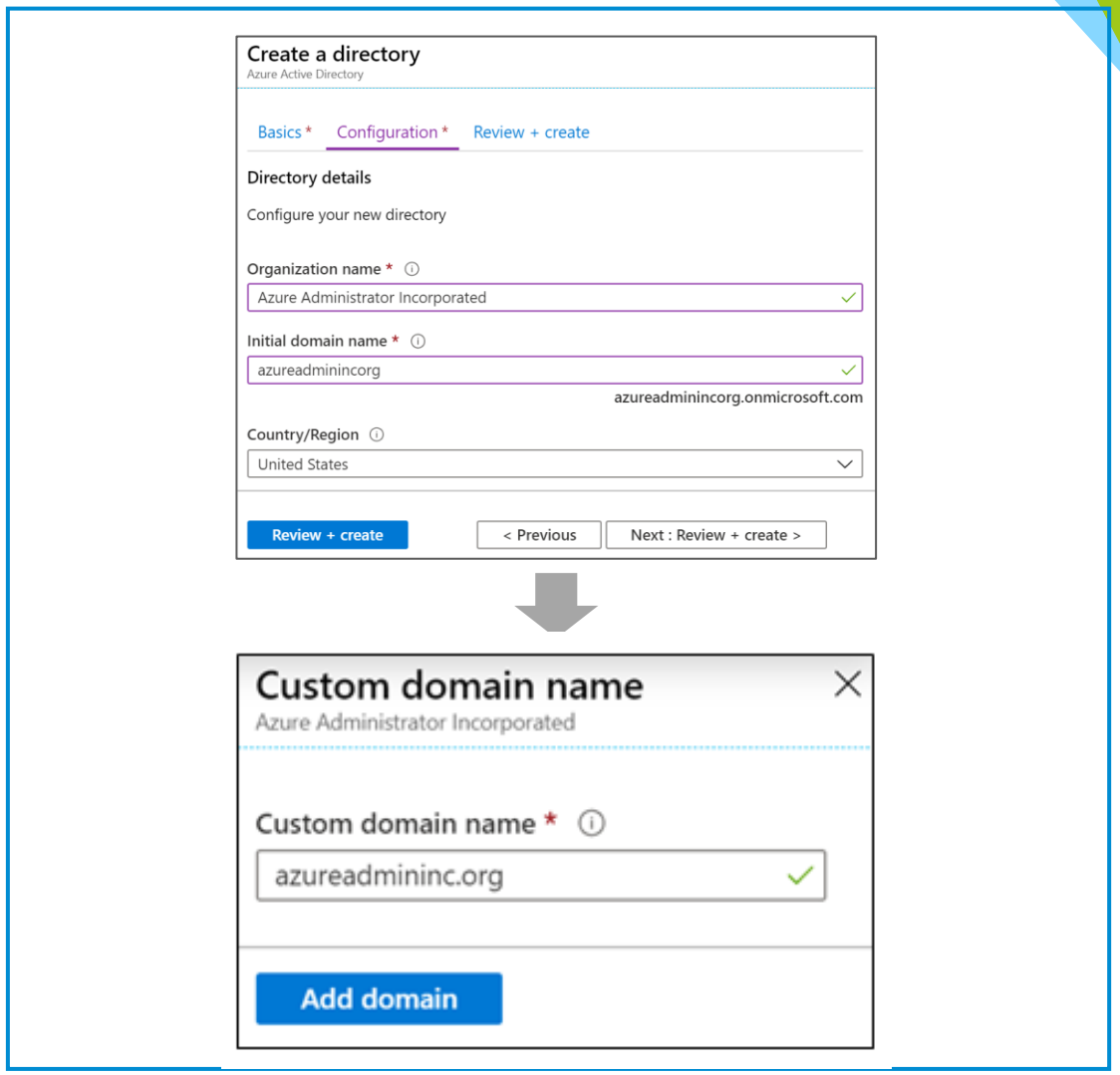
Identity Domains and Custom Domains

When you create an Azure subscription an Azure AD domain is created for you

The domain has initial domain name in the form *domainname.onmicrosoft.com*

You can customize/change the name

After the custom name is added it must be verified (next topic)



brainymotion

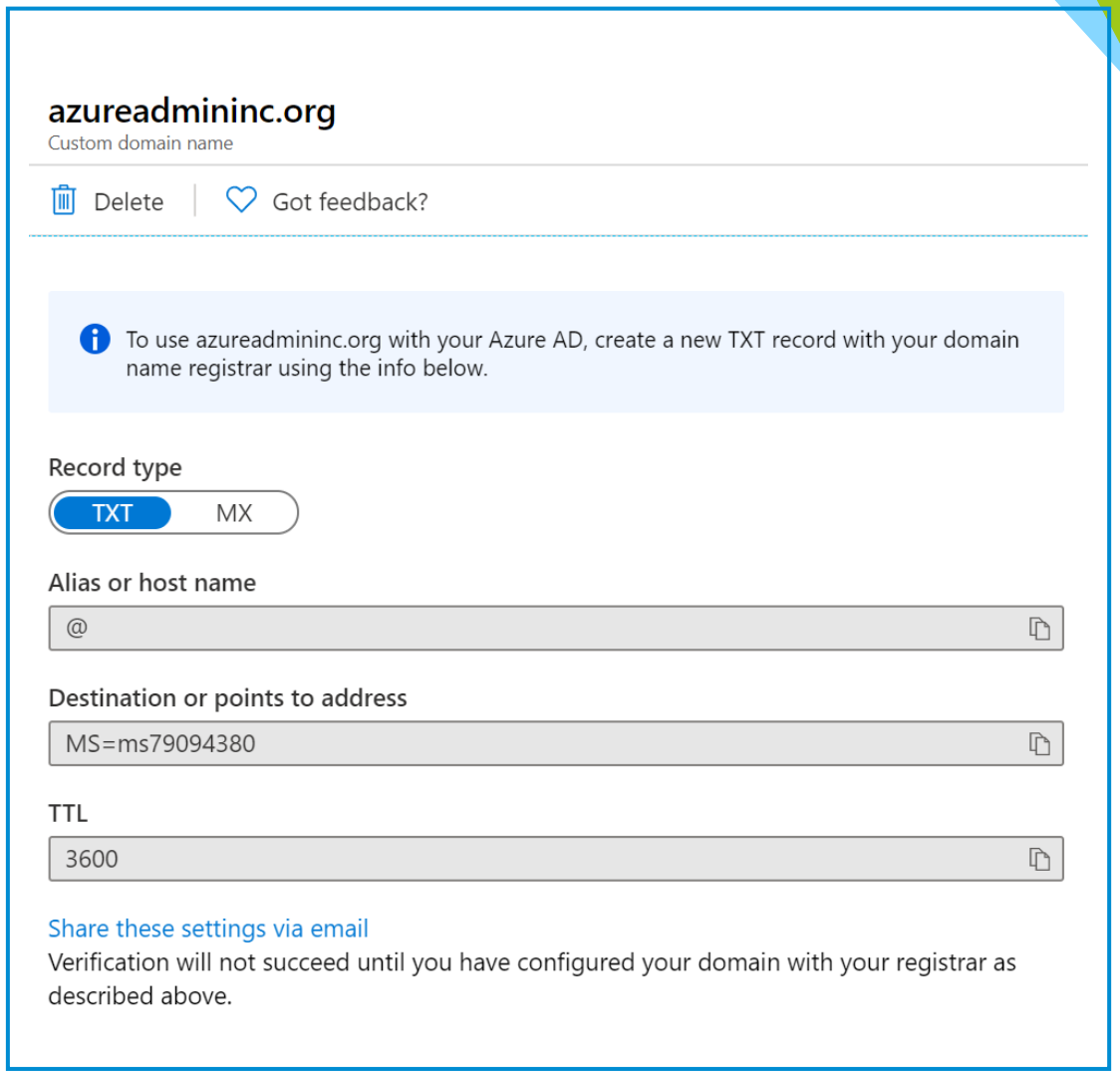
Verify Custom Domain Names

Verification demonstrates ownership of the domain name

Add a DNS record (MX or TXT) that is provided by Azure into your company's DNS zone

Azure will query the DNS domain for the presence of the record

This could take several minutes or several hours



brainymotion

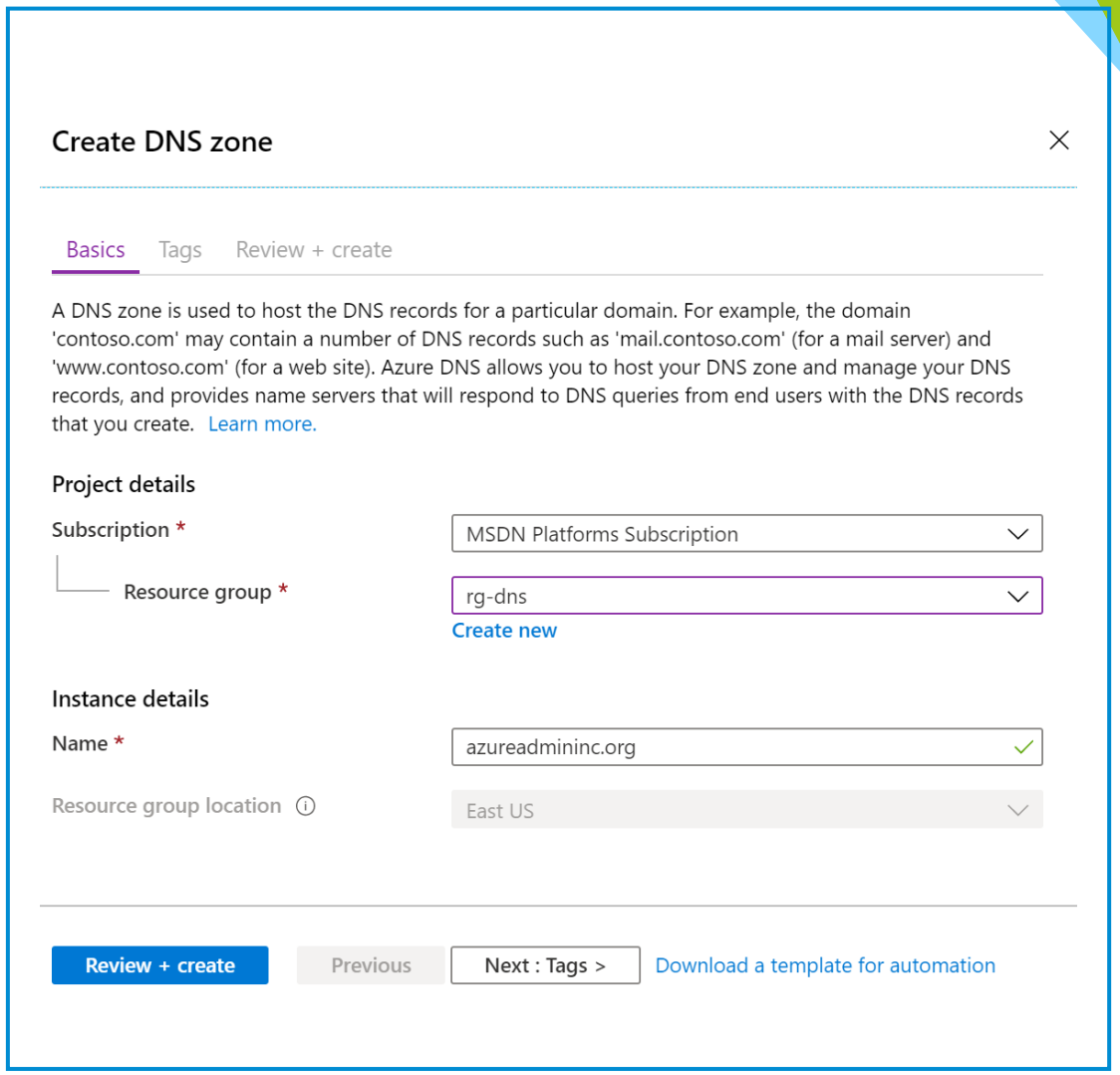
Create Azure DNS Zones

A DNS zone hosts the DNS records for a domain

The name of the zone must be unique within the resource group

Where multiple zones share the same name, each instance is assigned different name server addresses

Root/Parent domain is registered at the registrar and pointed to Azure NS



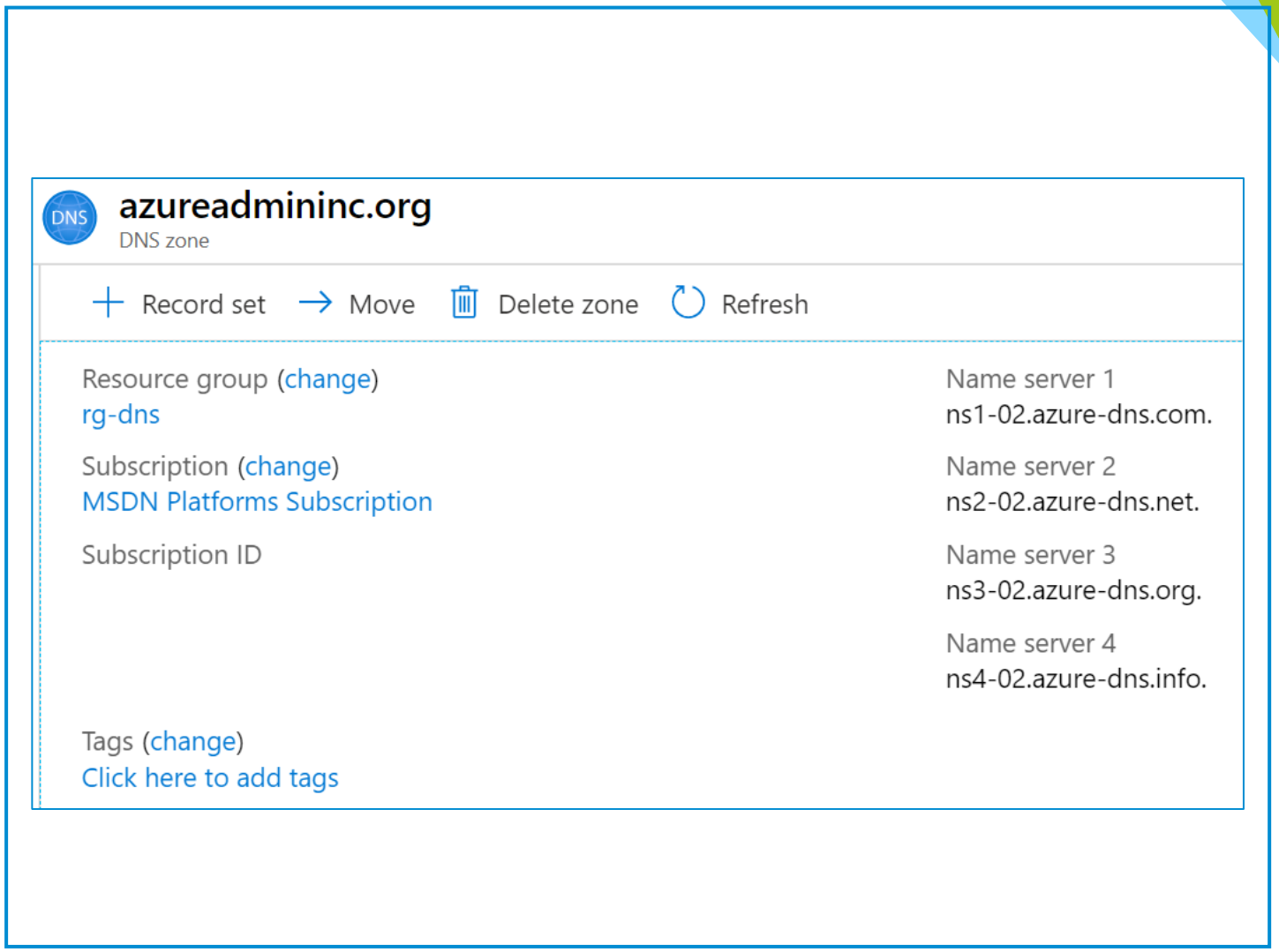
brainymotion

Delegate DNS Domains

When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS – use all four

Once the DNS zone is created, update the parent registrar

For child zones, register the NS records in the parent domain



brainymotion

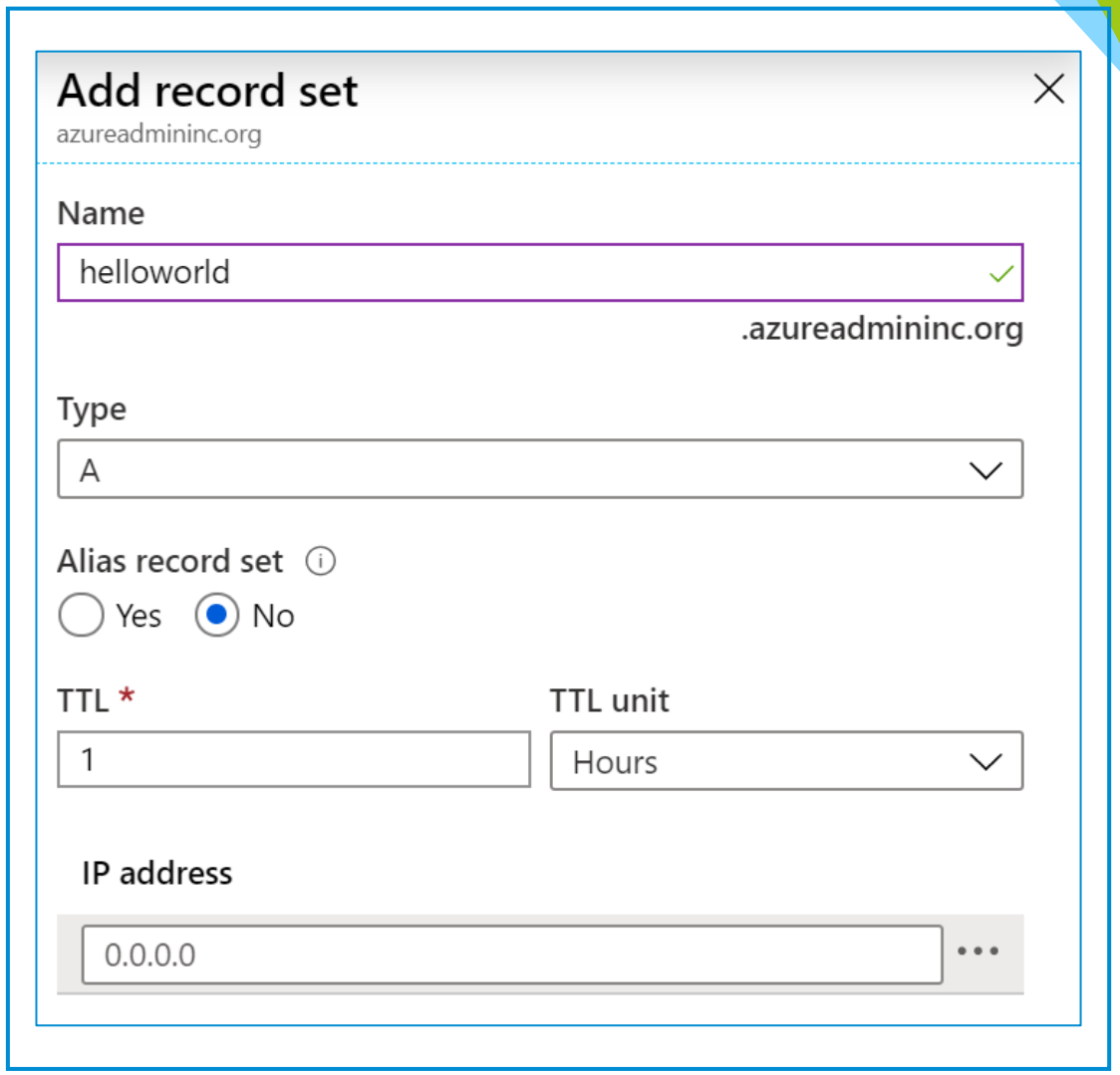
Add DNS Record Sets

A record set is a collection of records in a zone that have the same name and are the same type

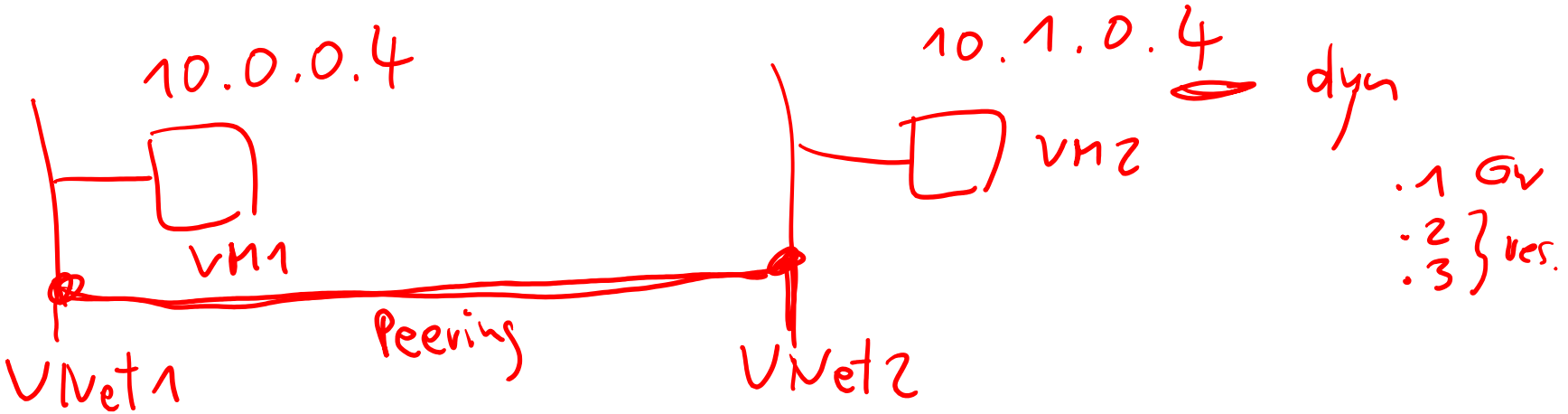
You can add up to 20 records to any record set

A record set cannot contain two identical records

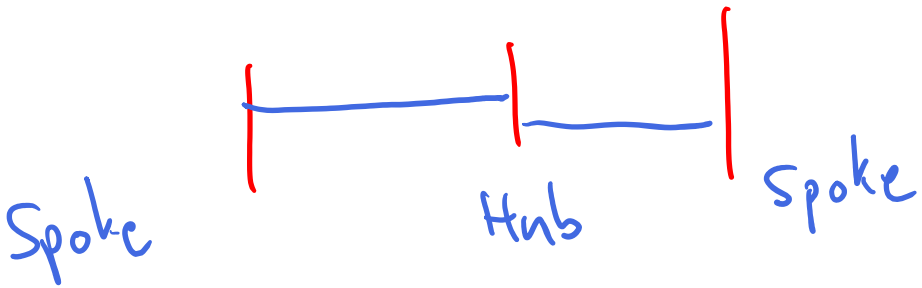
Changing the drop-down Type, changes the information required



brainymotion



Lesson 7: Configure VNet Peering



brainymotion

Configure VNet Peering Introduction

Determine VNet Peering Uses

Determine Gateway Transit and Connectivity Needs

Create VNet Peering

Determine Service Chaining Uses

Demonstration – VNet Peering

Summary and Resources

brainymotion

Determine VNet Peering Uses

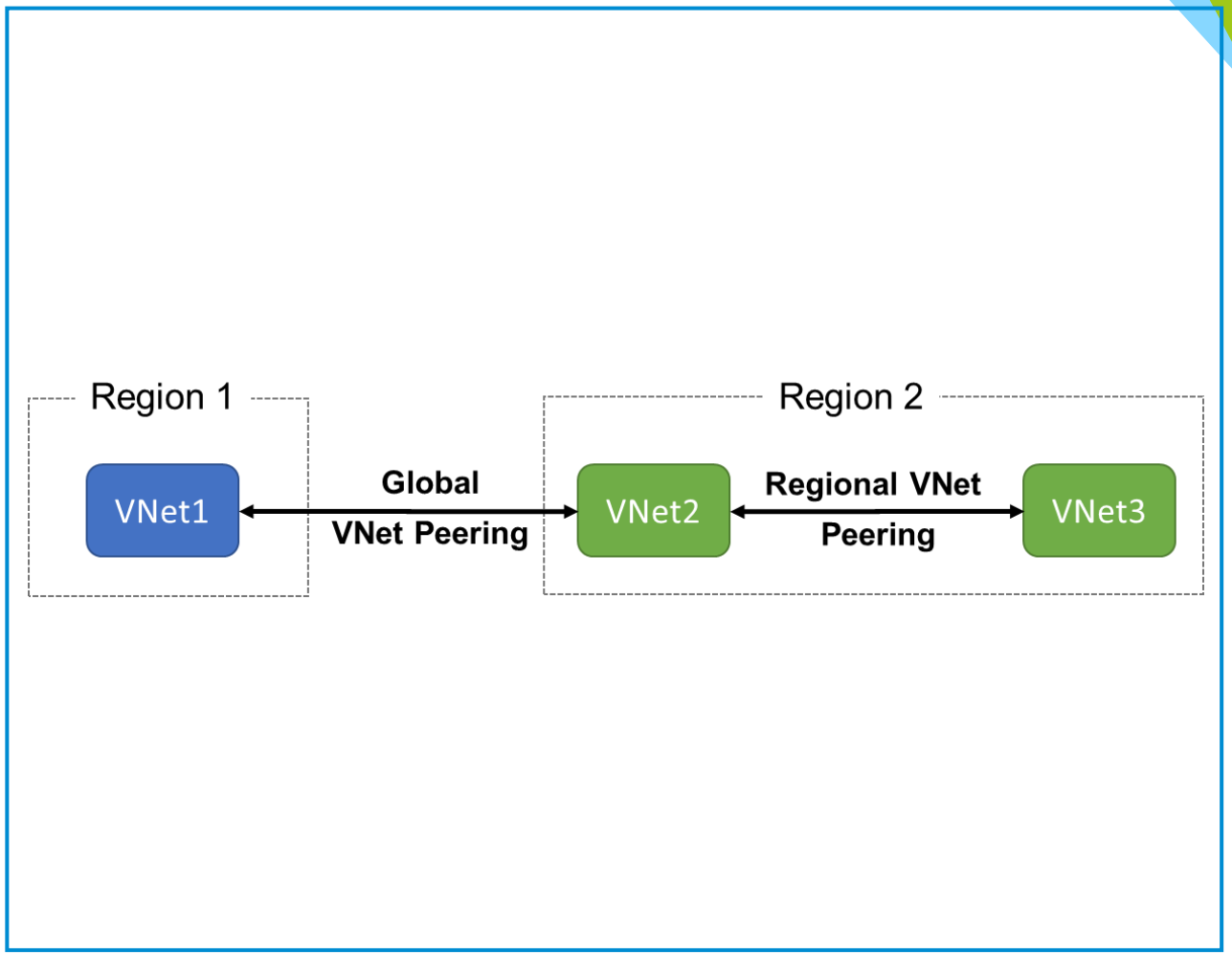
VNet peering connects two Azure virtual networks

Two types of peering: Regional and Global

Peered networks use the Azure backbone for privacy and isolation

You can peer across subscriptions and tenants

Easy to setup, seamless data transfer, and great performance



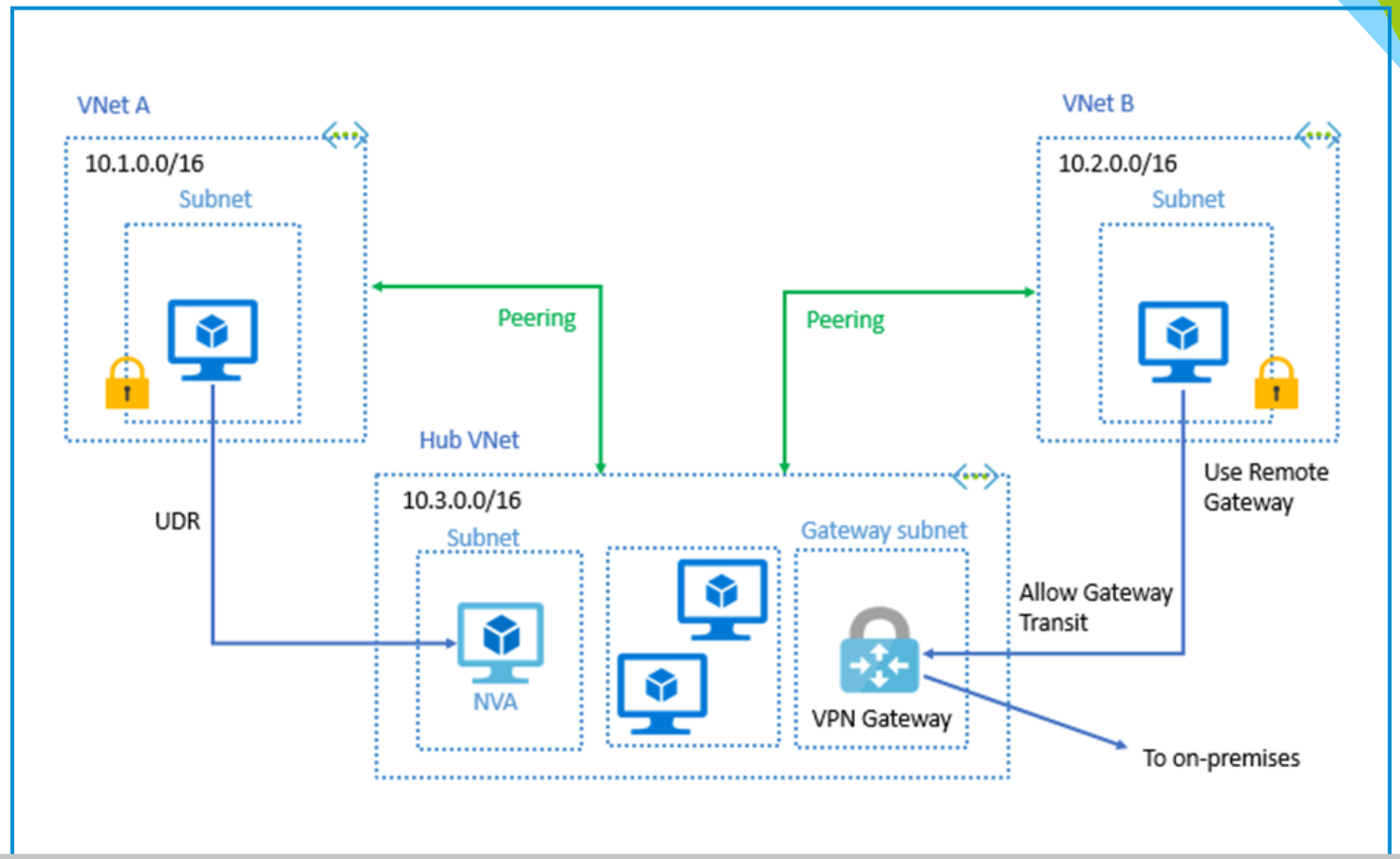
brainymotion

Determine Gateway Transit and Connectivity Needs

Gateway transit allows peered virtual networks to share the gateway and get access to resources

No VPN gateway is required in the peered virtual network

Default VNet peering provides full connectivity



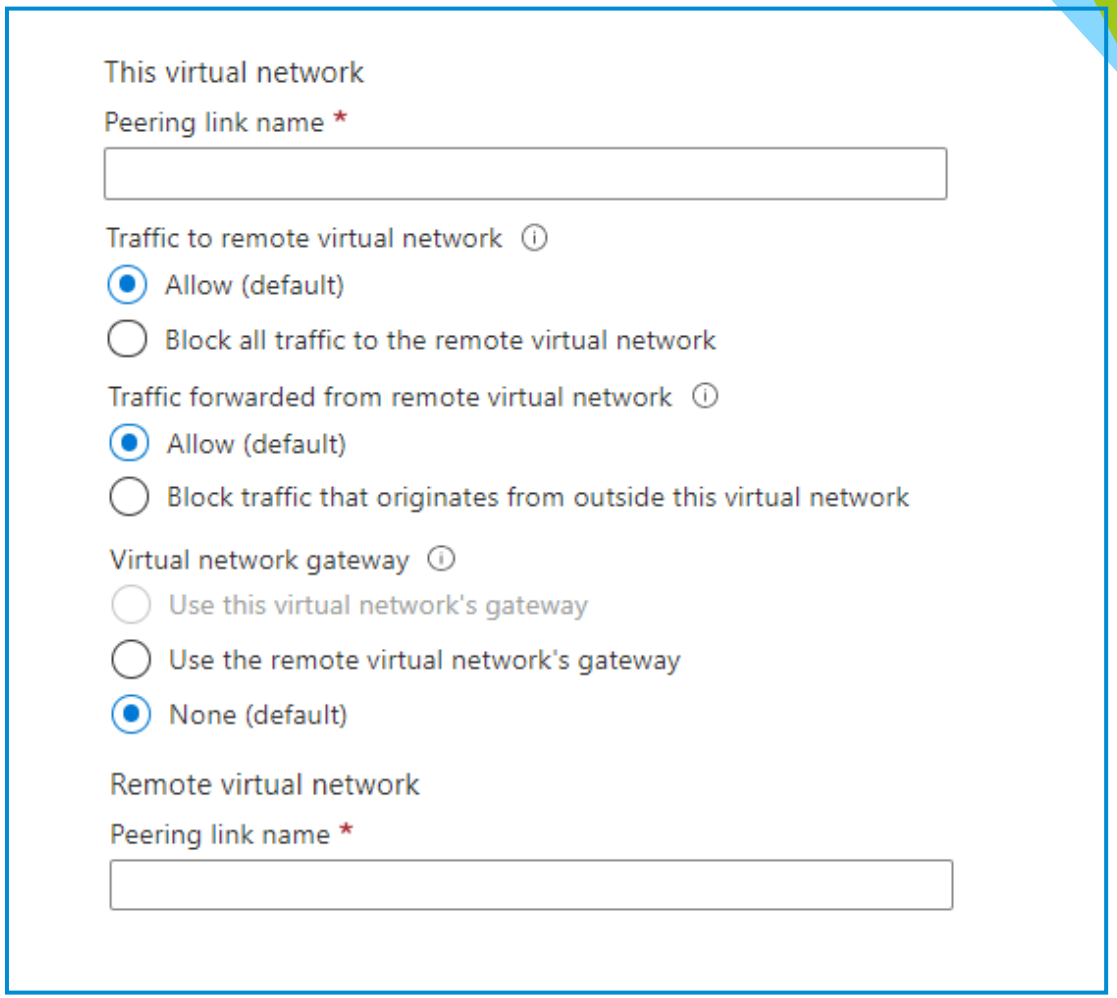
✓ IP address spaces of connected networks can't overlap

brainymotion

Create VNet Peering

Allow virtual network access settings

Configure forwarded traffic settings



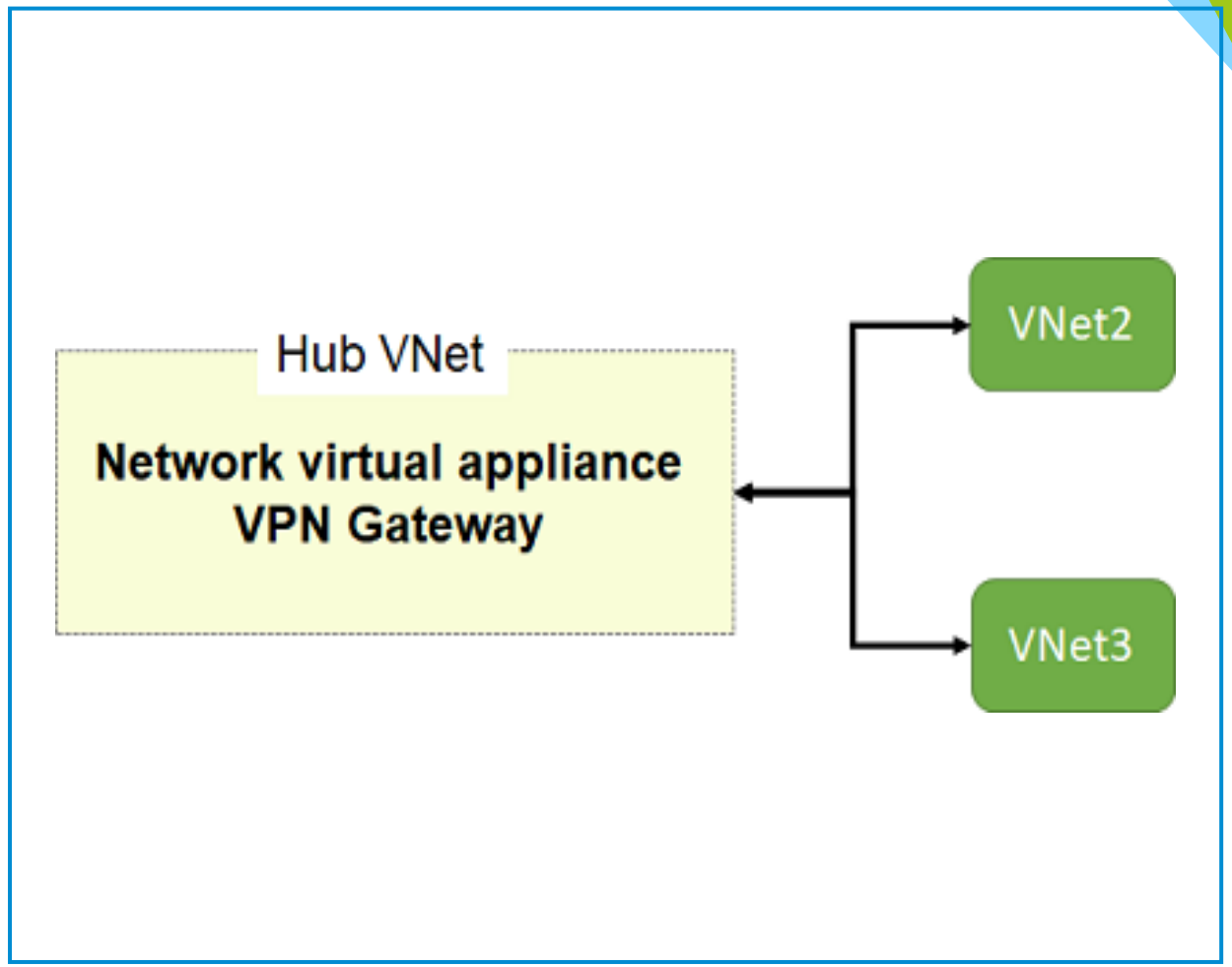
brainymotion

Determine Service Chaining Uses

Leverage user-defined routes and service chaining to implement custom routing

Implement a VNet hub with a network virtual appliance or a VPN gateway

Service chaining enables you to direct traffic from one virtual network to a virtual appliance, or virtual network gateway,
in a peered virtual network, through
user-defined routes



Lesson 8: Configure Network Routing

brainymotion

Configure Network Routing and Endpoints Introduction

Review System Routes

Identify User-Defined Routes

Examine a Routing Example

Determine Service Endpoint Uses

Determine Service Endpoint Services

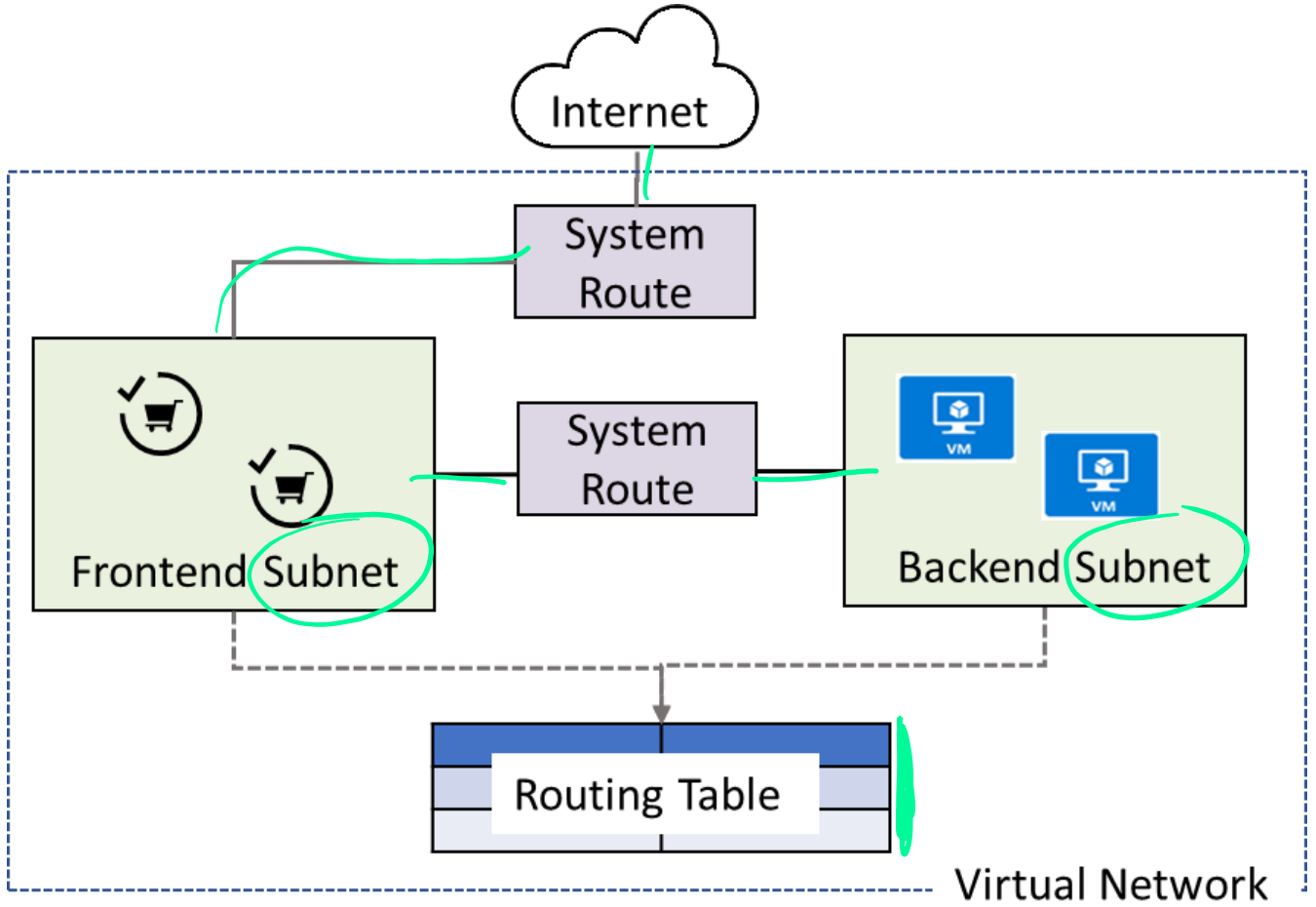
Identify Private Link Uses

brainymotion

Review System Routes

System routes direct network traffic between virtual machines, on-premises networks, and the Internet:

- Traffic between VMs in the same subnet
- Between VMs in different subnets in the same virtual network
- Data flow from VMs to the Internet
- Communication between VMs using a VNet-to-VNet VPN
- Site-to-Site and ExpressRoute communication through the VPN gateway



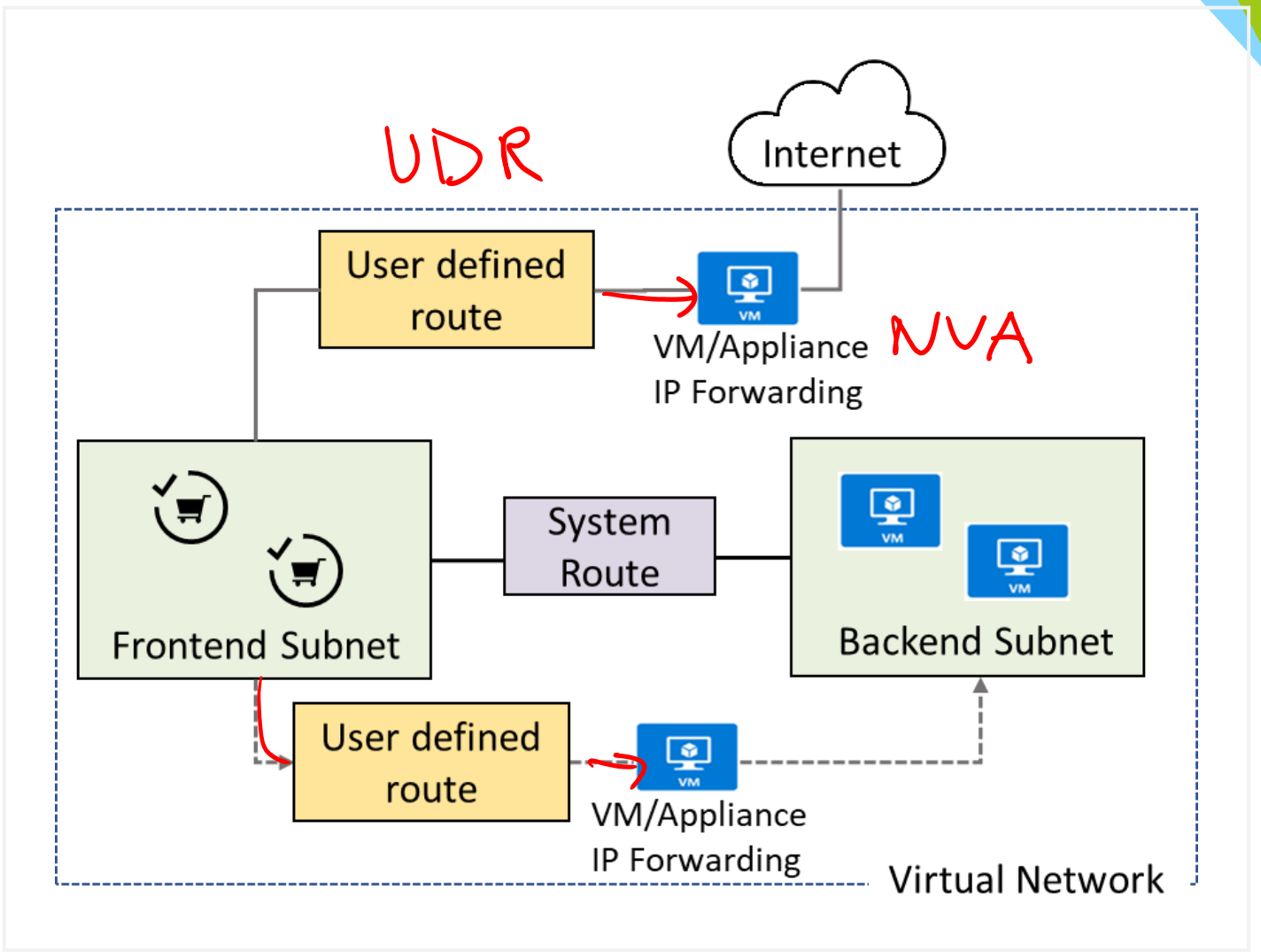
brainymotion

Identify User-Defined Routes

A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network

User-defined routes are custom routes that control network traffic by defining routes that specify the next hop of the traffic flow

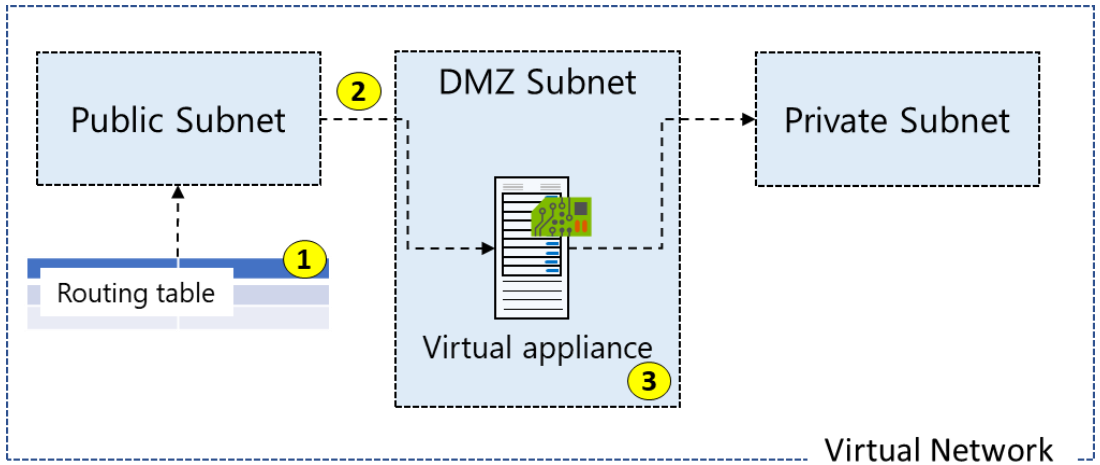
The next hop can be a virtual network gateway, virtual network, internet, or virtual appliance

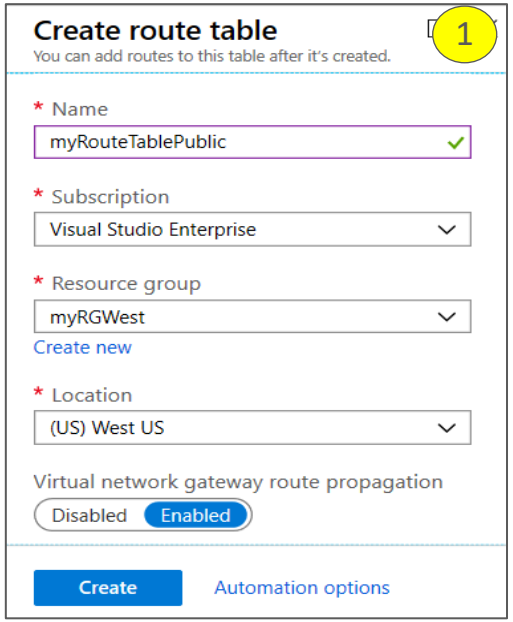


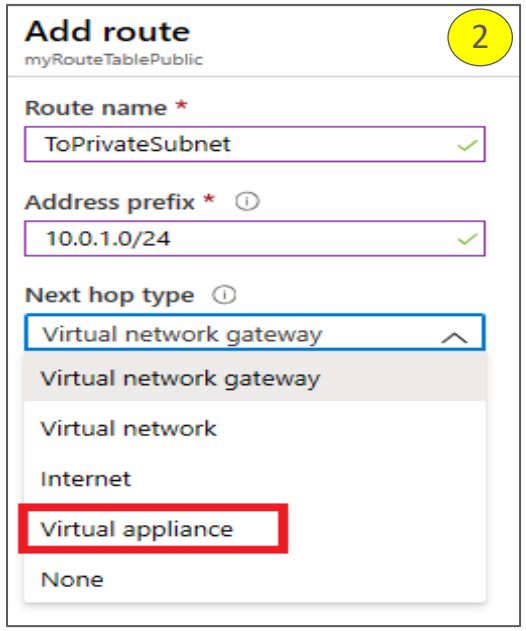
brainymotion

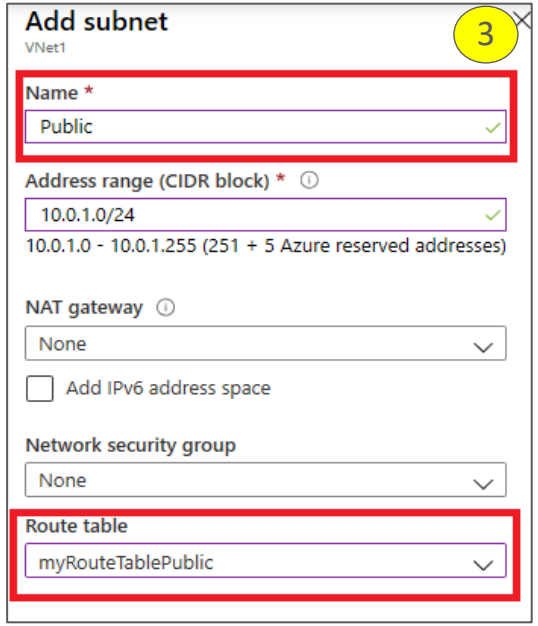
Examine a Routing Example

All traffic coming into the public subnet and headed for the private subnet must go through the virtual network appliance









brainymotion

Lesson 9: Configure Azure Load Balancer

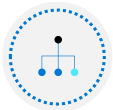
brainymotion

Configure Azure Load Balancer Introduction

Determine Azure Load Balancer Uses

Implement a Public Load Balancer

Implement an Internal Load Balancer



Determine Load Balancer SKUs

Create Backend Pools

Create Load Balancer Rules

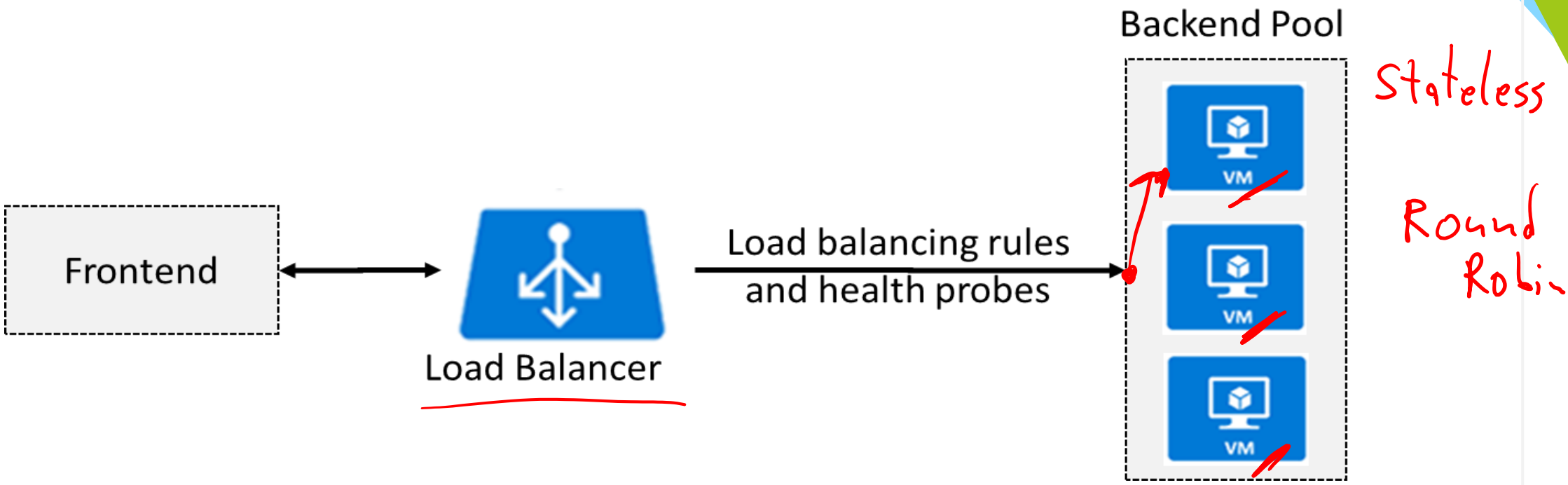
Configure Session Persistence

Create Health Probes

Summary and Resources

brainymotion

Determine Azure Load Balancer Uses



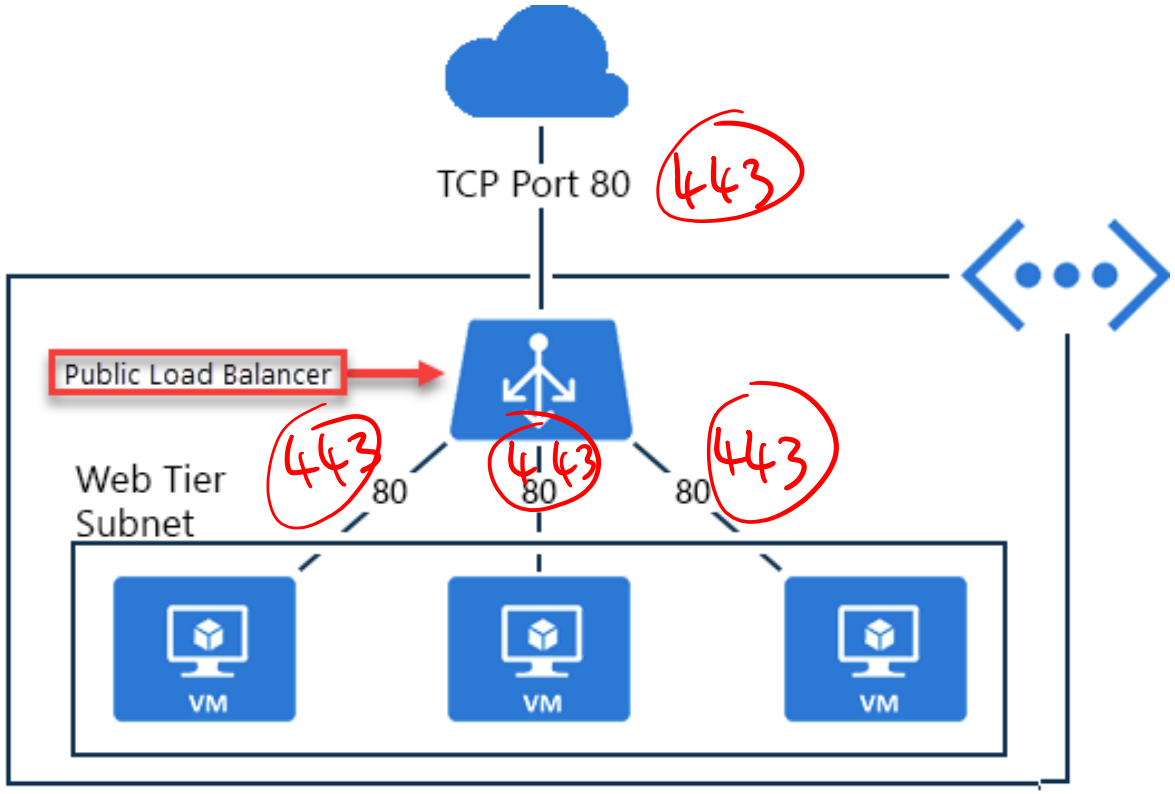
Distributes inbound traffic to backend resources using load-balancing rules and health probes

Can be used for both inbound/outbound scenarios

Two types: Public and Internal

brainymotion

Implement a Public Load Balancer



Maps public IP addresses and port number of incoming traffic to the VM's private IP address and port number, and vice versa

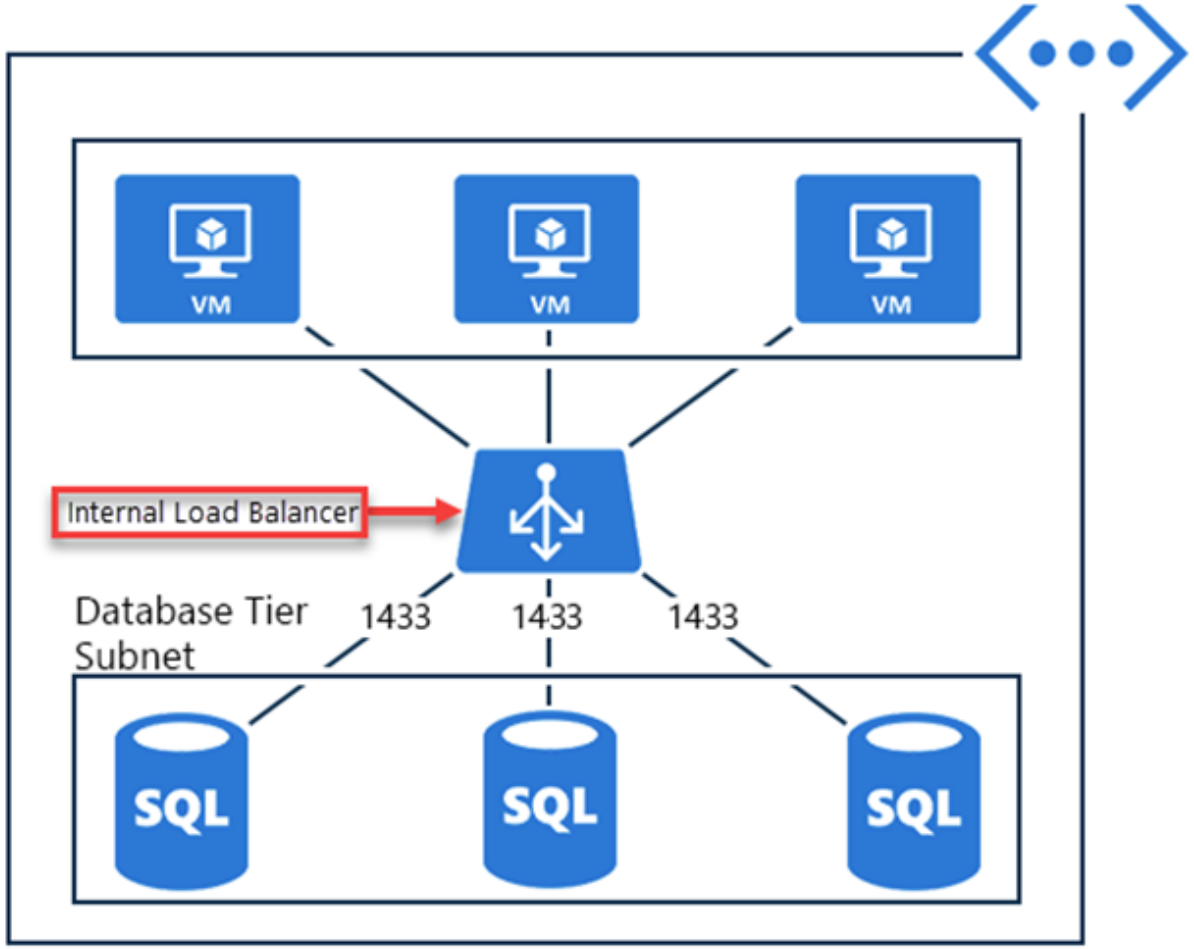
Apply load balancing rules to distribute traffic across VMs or services

Implement an Internal Load Balancer

Directs traffic only to resources inside a virtual network or that use a VPN to access Azure infrastructure

Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint

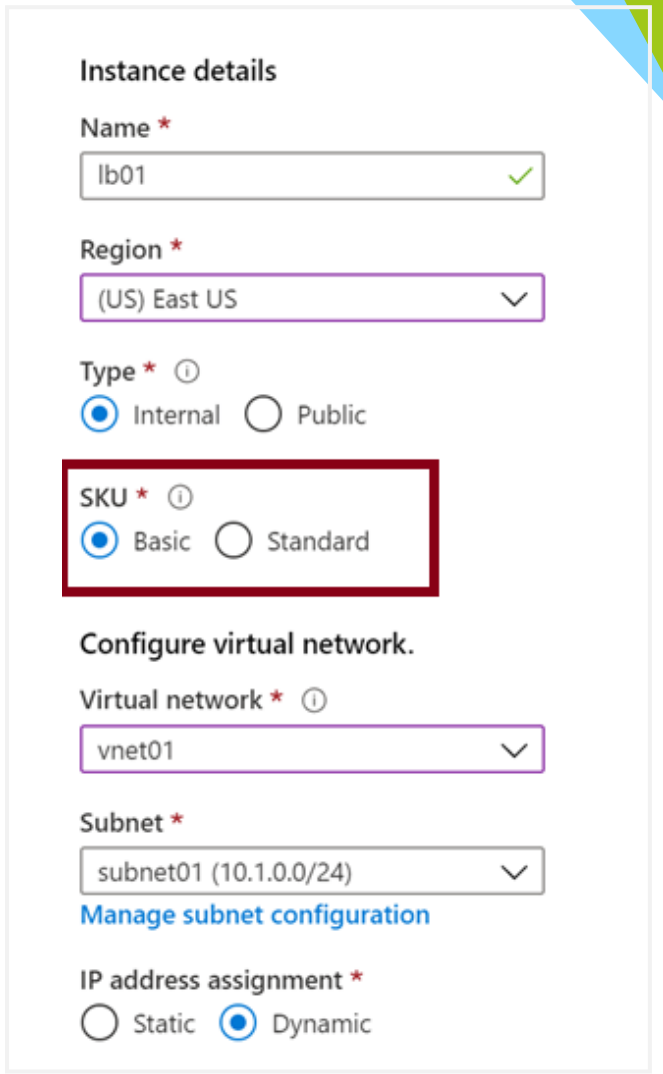
Enables load balancing within a virtual network, for cross-premises virtual networks, for multi-tier applications, and for line-of-business applications



brainymotion

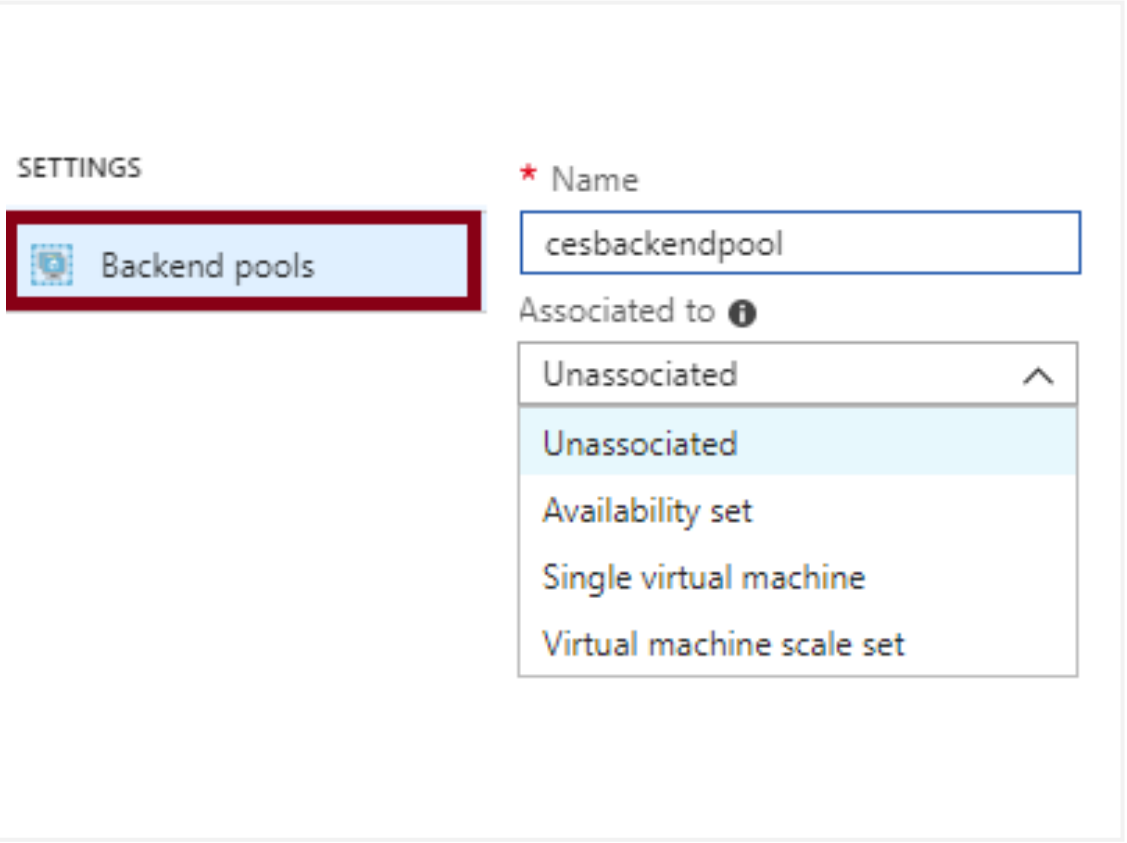
Determine Load Balancer SKUs

Feature	Basic SKU	Standard SKU
Backend pool	Up to 300 instances	Up to 1000 instances
Health probes	TCP, HTTP	TCP, HTTP, HTTPS
Availability zones	Not available	Zone-redundant and zonal frontends for inbound and outbound traffic
Multiple frontends	Inbound only	Inbound and outbound
Secure by default	Open by default. NSG optional.	Closed to inbound flows unless allowed by a NSG. Internal traffic from the virtual network to the internal load balancer is allowed.
SLA	Not available	99.99%



brainymotion

Create Backend Pools



SKU	Backend pool endpoints
Basic SKU	VMs in a single availability set or VM scale set
Standard SKU	Any VM in a single virtual network, including a blend of VMs, availability sets, and VM scale sets

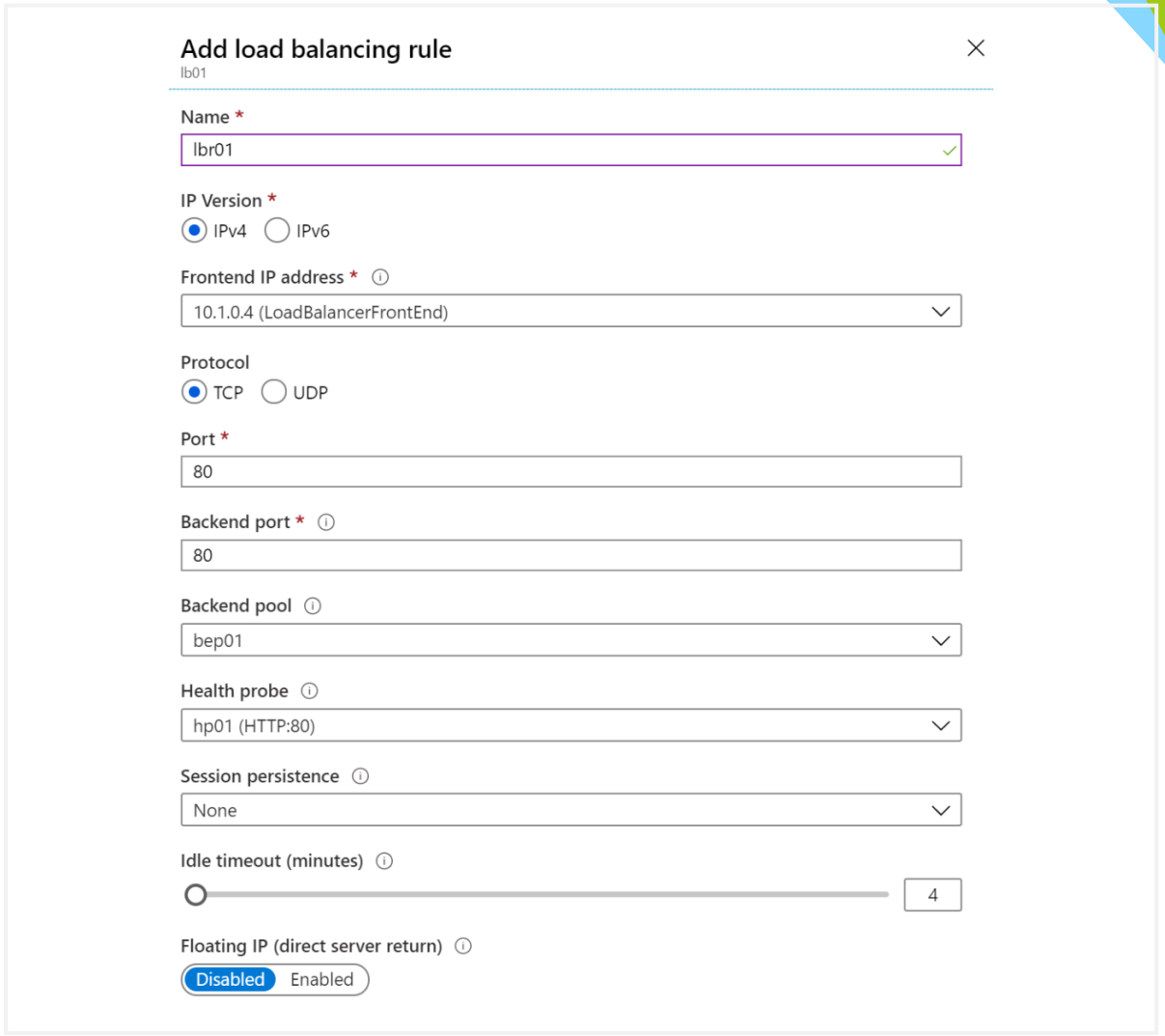
To distribute traffic, a back-end address pool contains the
IP addresses of the virtual NICs that are connected to the load balancer

Create Load Balancer Rules

Maps a frontend IP and port combination to a set of backend pool and port combination

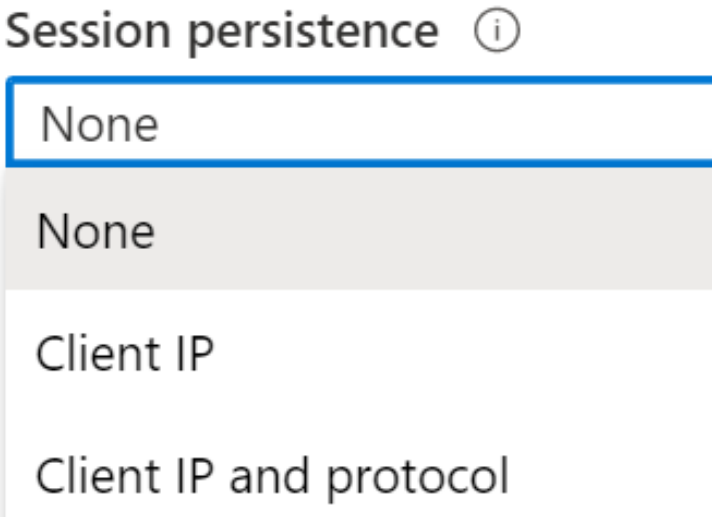
Rules can be combined with NAT rules

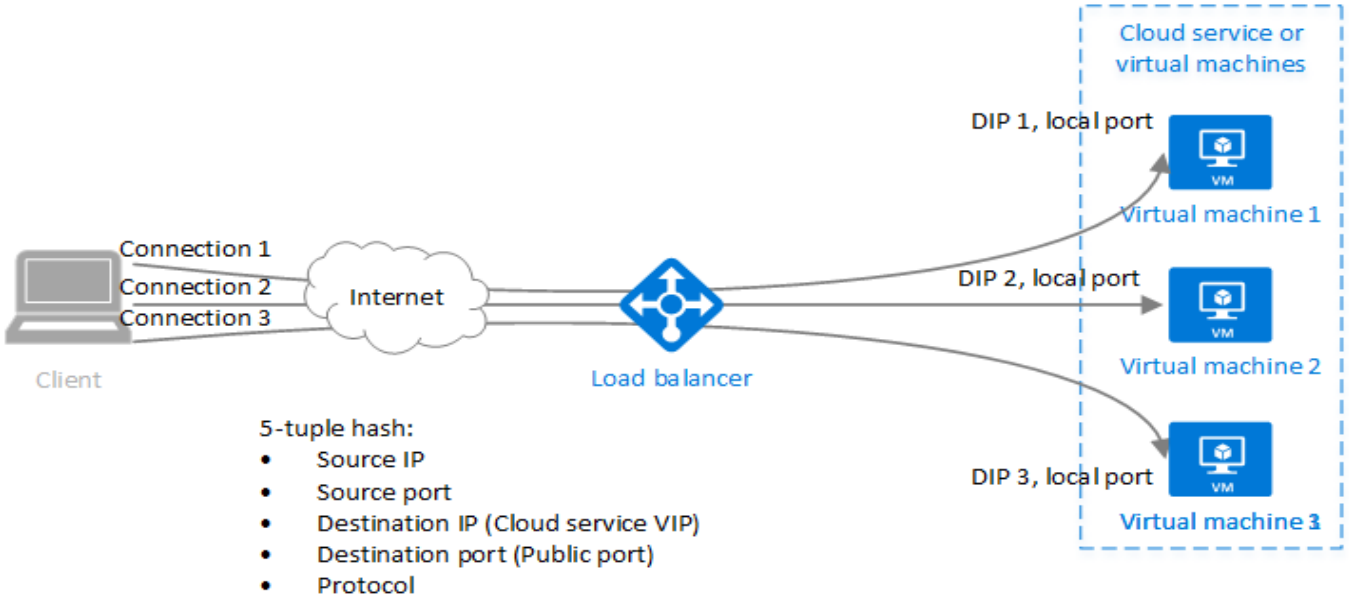
A NAT rule is explicitly attached to a VM (or network interface) to complete the path to the target



brainymotion

Configure Session Persistence





Session persistence specifies how client traffic is handled

None (default) requests can be handled by any virtual machine

Client IP requests will be handled by the same virtual machine

Client IP and protocol specifies that successive requests from the same address and protocol will be handled by the same virtual machine

brainymotion

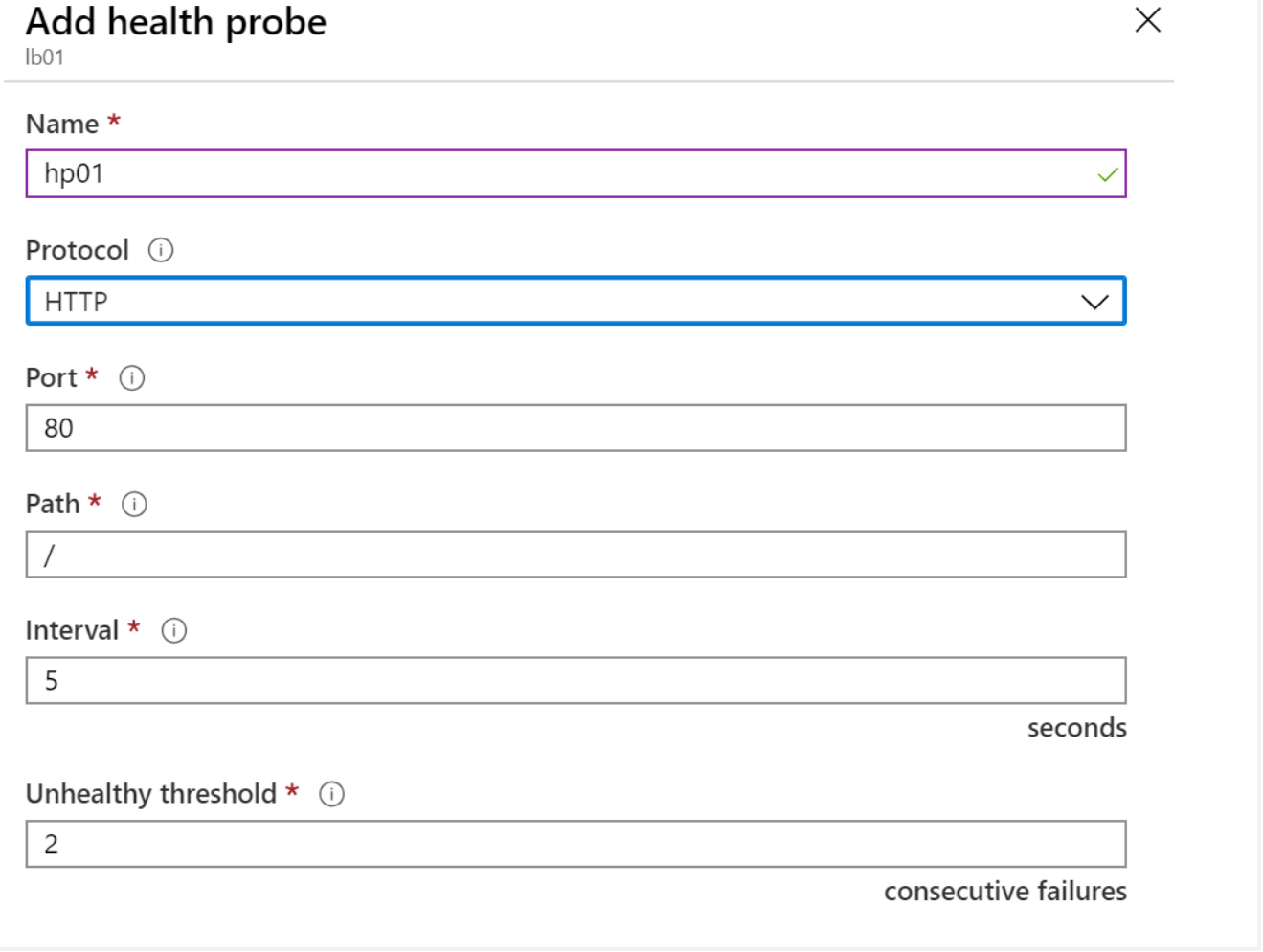
Create Health Probes

Allows the load balancer to monitor the status of an app

Dynamically adds or removes VMs from the load balancer rotation based on their response to health checks

HTTP custom probe (preferred) pings every 15 seconds

TCP custom probe tries to establish a successful TCP session



brainymotion

brainymotion

The End