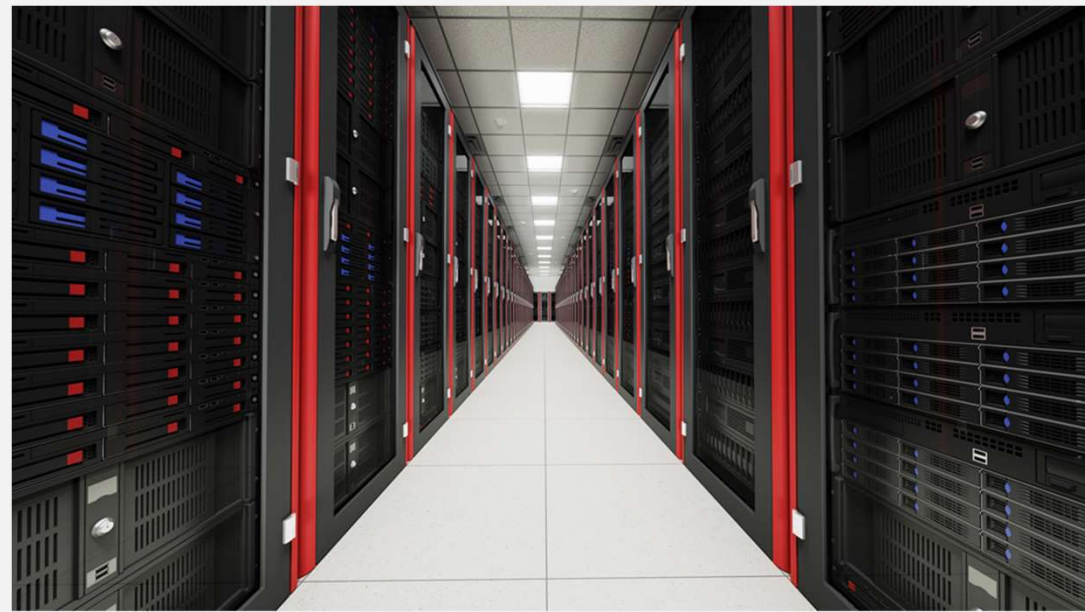


Introduction to Networking

Kevin Brown
MCT (Microsoft Certified Trainer) since 2000,
Azure Security Engineer,
Azure Solutions Architect,
Azure Administrator,
MCSE,
CISSP



Why take this course?

- An understanding of networking is required for?
 - Azure, AWS, GCP or any cloud service
 - Systems Administrator
 - Hyper-V, VMware, Nutanix or any virtualization technology
 - Desktop Support
 - Helpdesk
 - Applications Administrator

Course Outline

- Understanding IPv4 Addressing
- OSI Model
- Subnetting
- Layer 2 and Layer 3 switches
- Routing
- Packet Tracer
- Public and Private IP addresses
- Network Address Translation
- TCP Flow Control
- Client Configuration
- IPv4 Troubleshooting commands and tools
- Wireshark
- DHCP
- Benefits of DHCP
- How DHCP works
- Installation and configuration
- Scope management
- High availability
- Maintaining the DHCP database
- Migrating the DHCP database

Course Outline

- DNS
 - Resolution process
 - DNS components
 - Zones
 - Records
 - Client configuration
 - Root hints
 - Forwarding
 - Troubleshooting DNS related issues
 - Active Directory related networking
- Understanding IPv6 Addressing
 - Why use IPv6
 - Differences between IPv4 and IPv6
 - Overview of IPv6 addressing
 - IPv6 Address Types
 - Autoconfiguration of ipv6 clients
 - IPv6 Client Configurations
 - ipv4 and ipv6 coexistence
 - Considerations for ipv6 implementation
 - Tunneling

Module 1: Understanding, Implementing, and Troubleshooting IPv4



Module Overview

- Planning IPv4 addressing
- Configuring an IPv4 host
- Managing and troubleshooting IPv4 network connectivity



1

End User Computers

2

Servers

3

Telephones
(wired/wireless)

4

Printers

5

Cameras

5

Network Devices

Lesson 1: Planning IPv4 addressing

- Overview of IPv4 settings
- Defining subnets
- Public and private IP addresses

What is an IPv4 Address?

192.168.1.1

10.45.58.97

20.8.49.251

172.16.89.189

An IP address, or Internet Protocol address, is **a series of numbers that identifies any device on a network.**

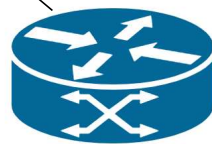
Computers use IP addresses to communicate with each other both over the internet as well as on other networks.





A network **router** connects devices on one network to devices on other networks (internet) by exchanging **packets**

IP Address 20.5.87.94



IP Address 192.168.1.1

A network **switch** connects devices (such as computers, printers, wireless access points) in a network to each other, and allows them to 'talk' by exchanging data **frames**



PC1

IP Address 192.168.1.47
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS: 192.168.1.10



PC2

IP Address 192.168.1.209
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS: 192.168.1.10



File01

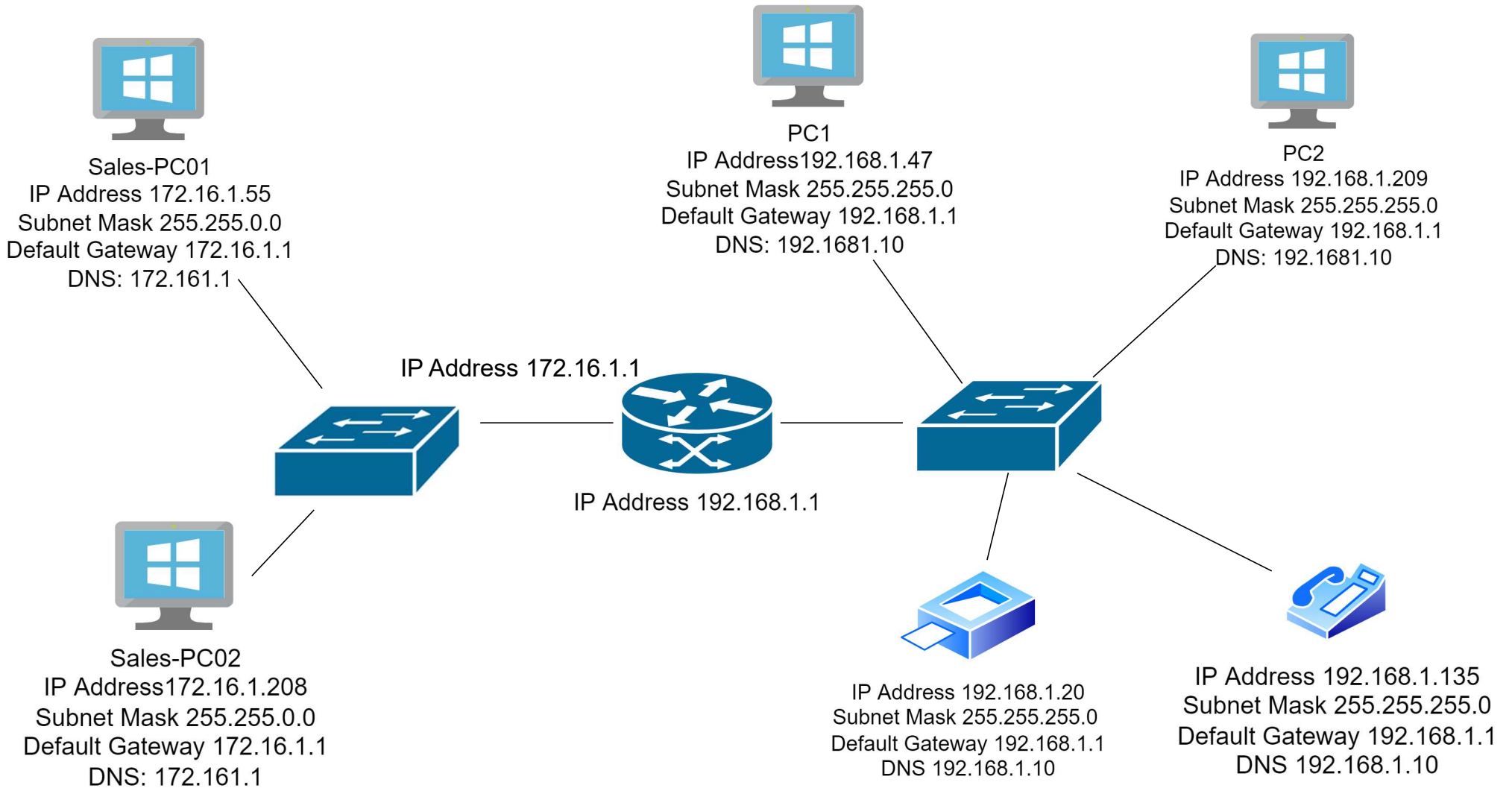
IP Address 192.168.1.17
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS 192.168.1.10



IP Address 192.168.1.20
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS 192.168.1.10



IP Address 192.168.1.135
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS 192.168.1.10





310 Area Code



212 Area Code



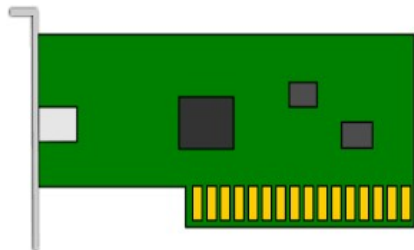
What is a MAC (Media Access Control) Address?

FC-F8-AE-53-6D-8F

A MAC address is assigned to the Network Interface Adapter (NIC).

The NIC can be wired or wireless

Also referred to as 'physical address'



Understanding ARP (address resolution protocol)

For devices on the same IP network:

ARP sends a broadcast directed to the IP address of the destination device

The destination device responds with its MAC address



FC-F8-AE-53-6D-8F
192.168.1.55



A1-5F-AC-16-55-D2
192.168.1.200

Related Commands:

ARP -a

Understanding ARP (address resolution protocol)

For devices on a different IP network:

ARP sends a broadcast directed to the IP address of the default gateway

The default gateway (router) responds with its MAC address

Related Commands:

ARP -a

Route Print

Get-NetRoute



FC-F8-AE-53-6D-8F
192.168.1.55

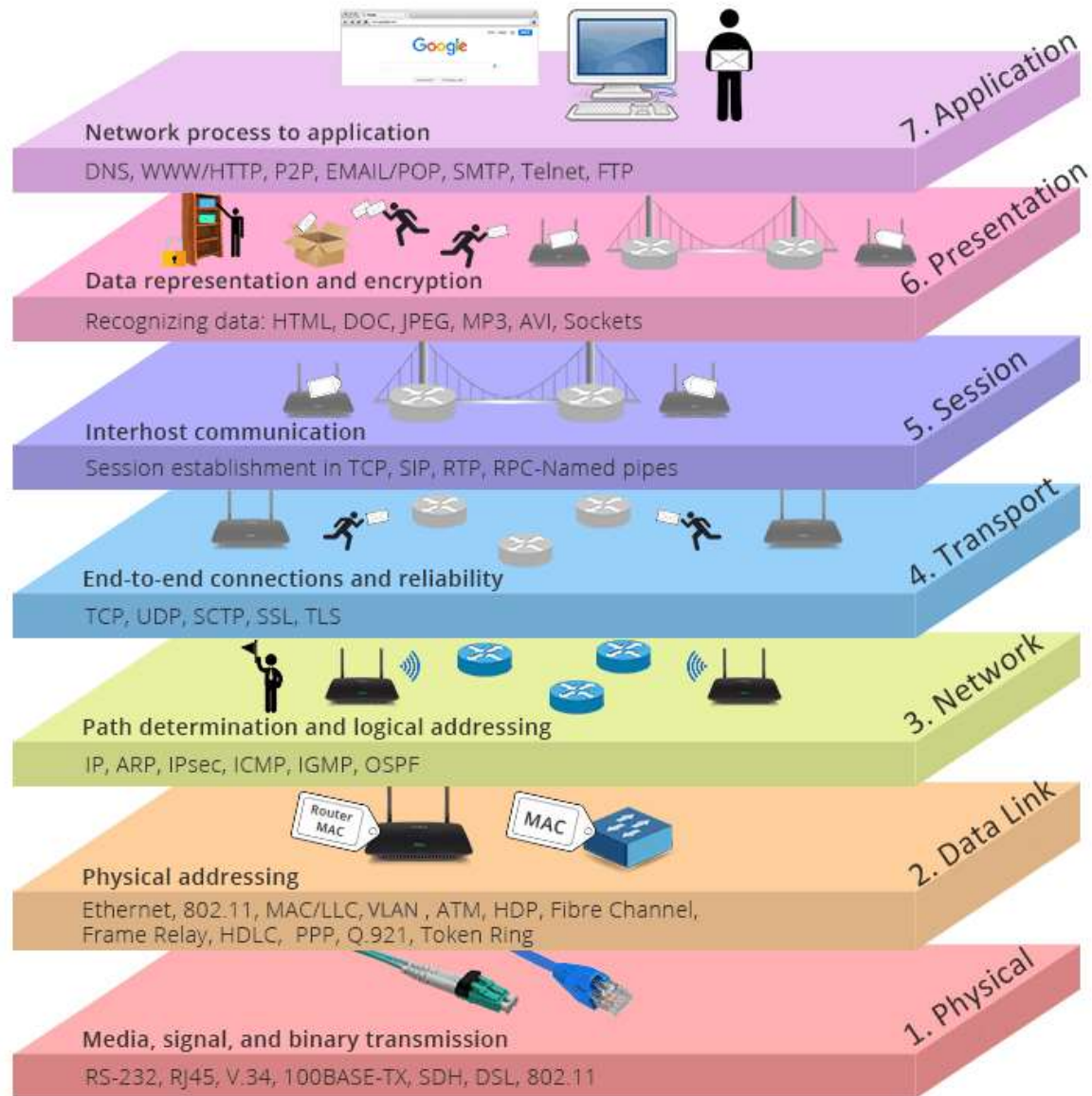


A1-5F-AC-16-55-D2
192.168.1.200



192.168.1.1

OSI Model





PC1

IP Address 192.168.1.47
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS: 192.168.1.10

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data-Link

1 Physical



PC2

IP Address 192.168.1.209
Subnet Mask 255.255.255.0
Default Gateway 192.168.1.1
DNS: 192.168.1.10

7 Application

6 Presentation

5 Session

4 Transport

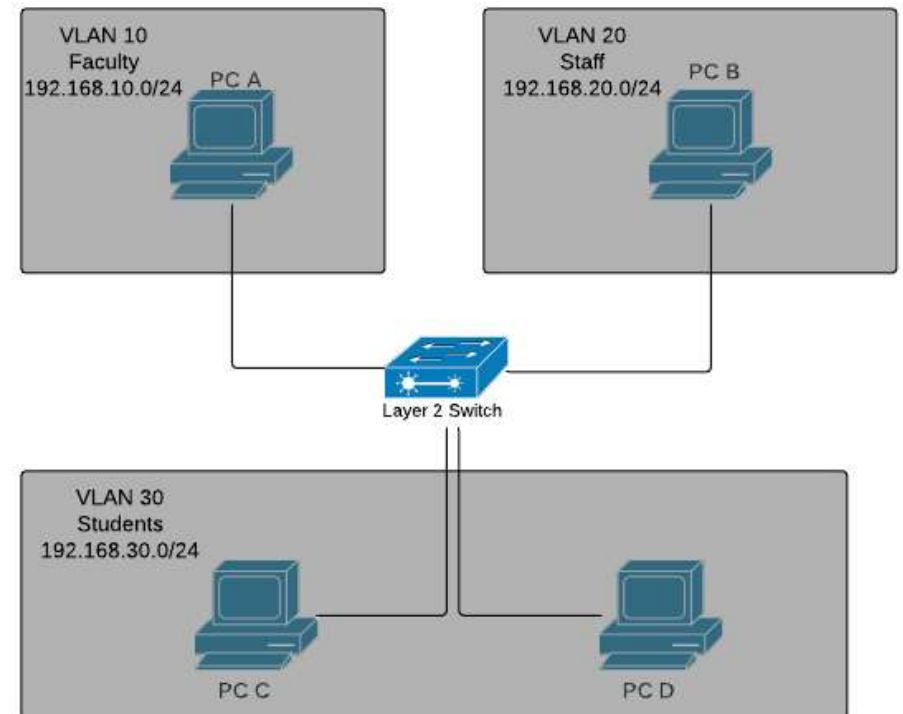
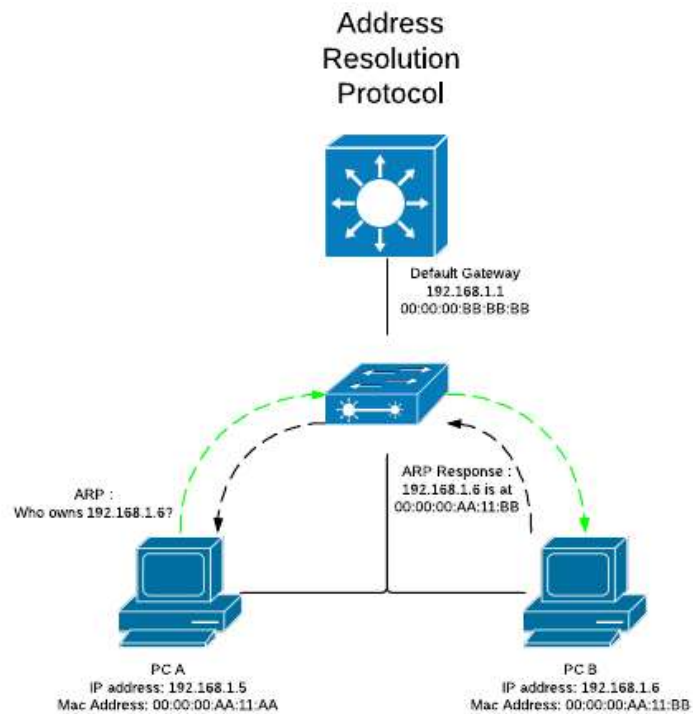
3 Network

2 Data-Link

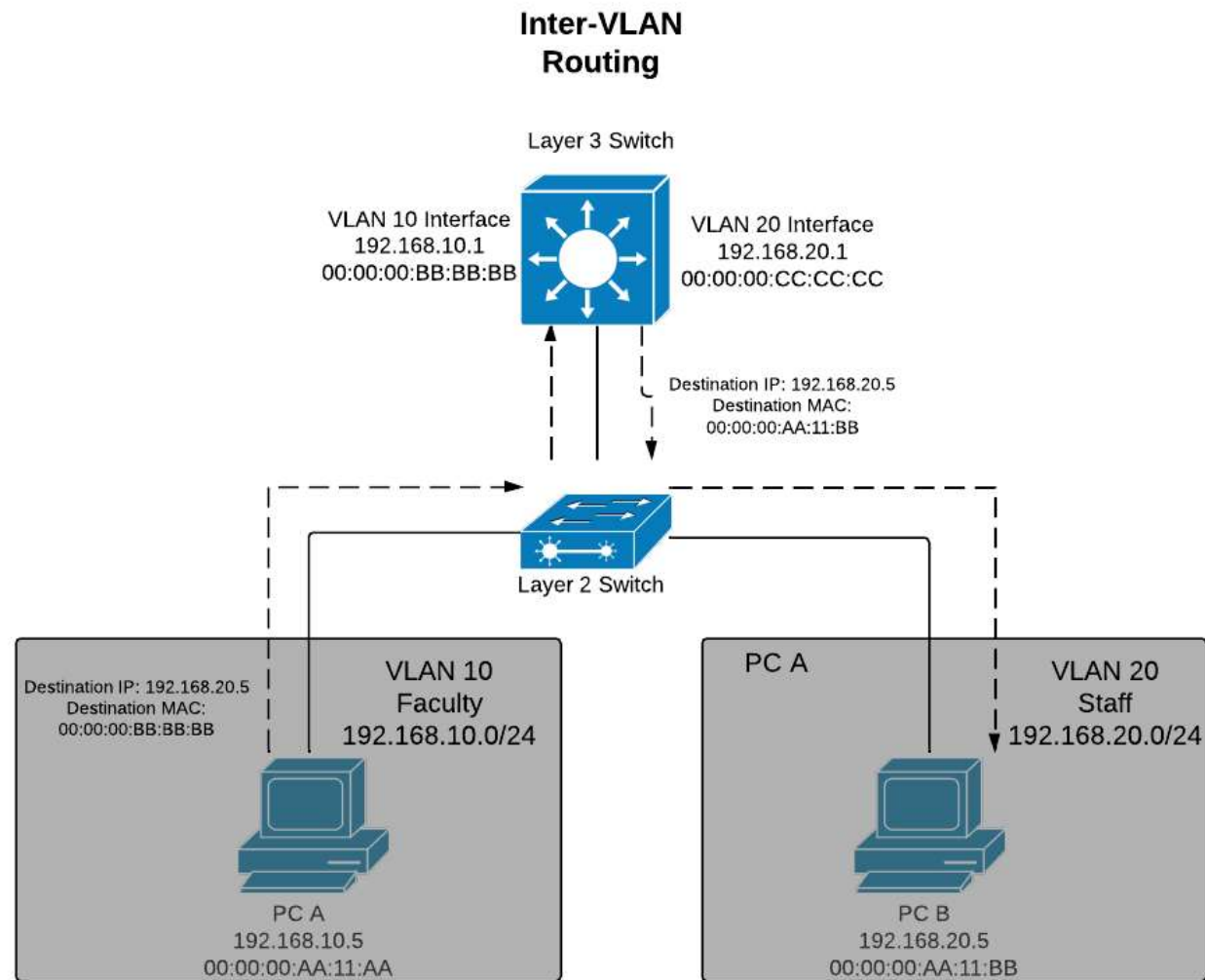
1 Physical



Switches: Layer 2 vs Layer 3



Switches: Layer 2 vs Layer 3



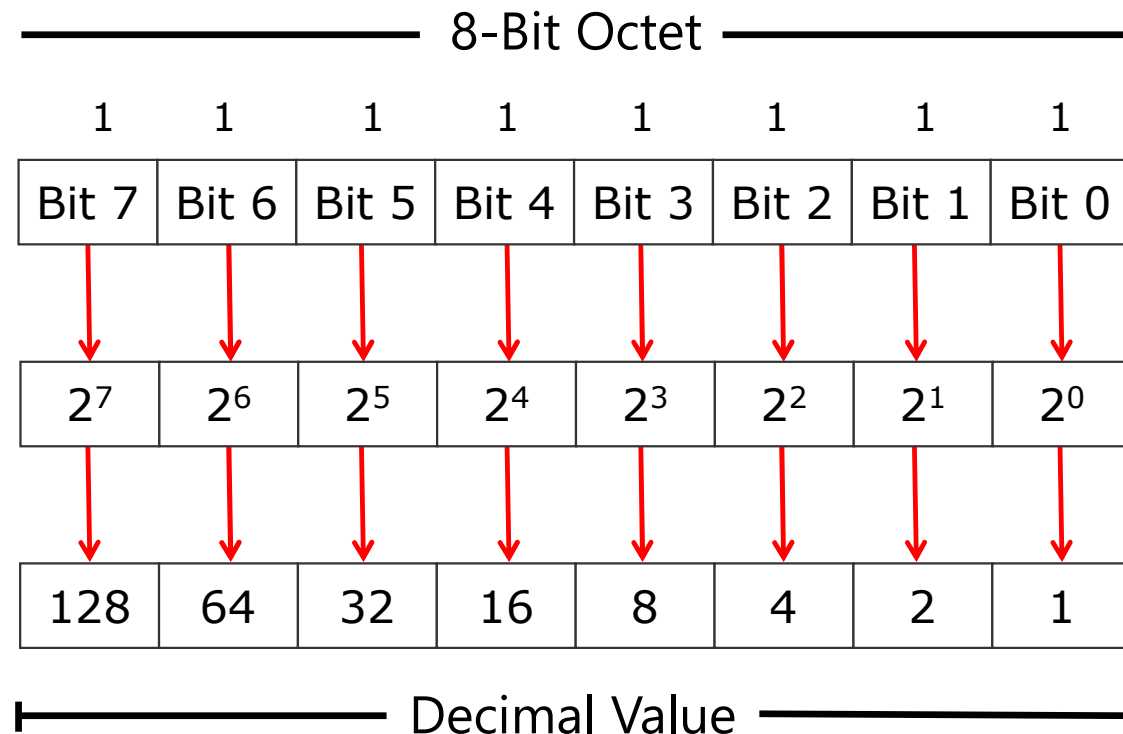
Understanding Binary Code

Dotted decimal notations are based on the decimal number system, but computers use IP addresses in binary

- Within an 8-bit octet, each bit position has a decimal value:
 - A bit that is set to 0 always has a zero value
 - A bit that is set to 1 can be converted to a decimal value
 - The low-order bit represents a decimal value of 1
 - The high-order bit represents a decimal value of 128
- If all bits in an octet are set to 1, then the octet's decimal value is 255, the highest possible value of an octet:
$$128 + 64 + 32 + 16 + 8 + 4 + 2 + 1$$



Overview of IPv4 settings



————— Decimal Value —————

128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

————— Decimal Value —————

128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

- A. 231
- B. 117
- C. 11110111
- D. 010111011

Answer key is under the lecture as a downloadable resource

Overview of IPv4 settings

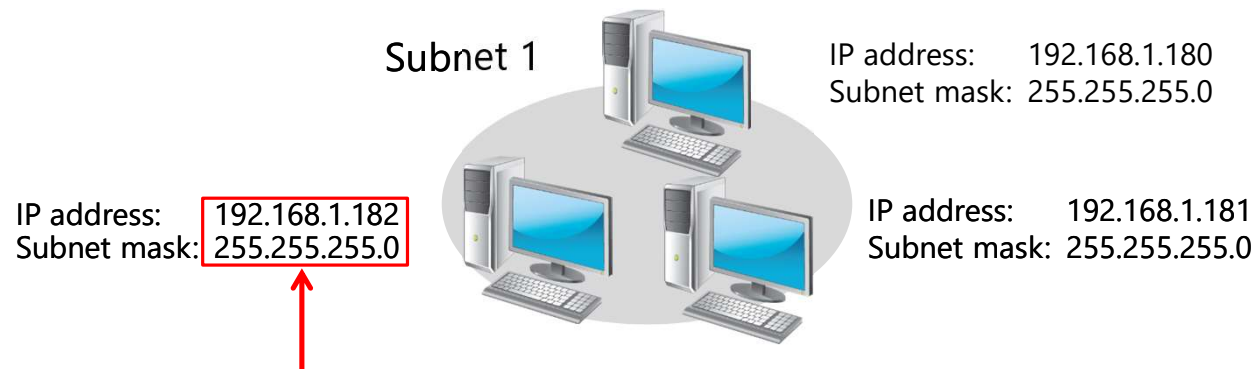
- Each networked computer must be assigned a unique IPv4 address
- Network communication for a computer is directed to the IPv4 address of the computer
- Each IPv4 address contains:
 - ✓ Network ID, identifying the network
 - ✓ Host ID, identifying the computer
- The subnet mask identifies which part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

IP address	172	16	0	10
Subnet mask	255	255	0	0
Network ID	172	16	0	0
Host ID	0	0	0	10



Overview of IPv4 settings

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



Dotted decimal representation
of the address and subnet mask



Classful IP Addressing

CIDR

A = 1 - 126

255.0.0.0 / 8 16⁷⁷⁷, 2¹⁴

1111111 / 00000000 / 00000000 / 00000000

B = 128 - 191

255.255.0.0 / 16 65,534

C = 192 - 223

255.255.255.0 / 24 2⁵⁴

of 1s in mask

Loopback
= 127.0.0.1

$2 - 2 =$
net + 10 & Broadcast

Subnet Mask

Binary	1	1	1	1	1	1	1	1
--------	---	---	---	---	---	---	---	---

Decimal	128	64	32	16	8	4	2	1
---------	-----	----	----	----	---	---	---	---

Subnet Mask	128	192	224	240	248	252	254	255
-------------	-----	-----	-----	-----	-----	-----	-----	-----

Subnetting

Class A example

10.0.0.0
255.0.0.0

Binary	1	1	1	1	1	1	1	1
Decimal	128	64	32	16	8	4	2	1
Subnet Mask	128	192	224	240	248	252	254	255

10.0.0.0
255.255.248.0

Subnetting

Class B example

172.16.0.0

255.255.224.0

Binary	1	1	1	1	1	1	1	1
Decimal	128	64	32	16	8	4	2	1
Subnet Mask	128	192	224	240	248	252	254	255

172.16.244.0
255.255.224.0

Binary	1	1	1	1	1	1	1	1
Decimal	128	64	32	16	8	4	2	1
Subnet Mask	128	192	224	240	248	252	254	255

[illegible]

www.subnet-calculator.com

Public and private 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

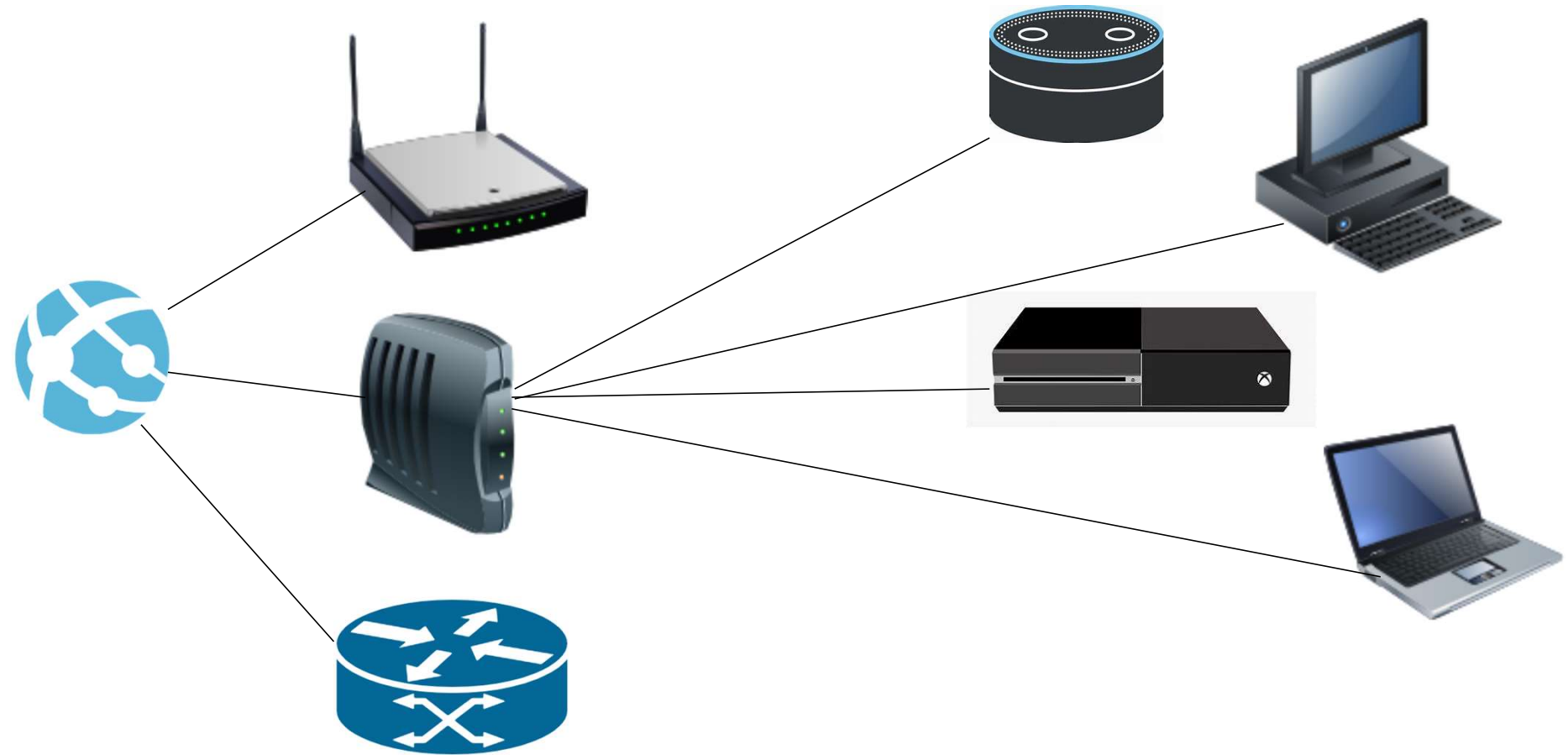


Private

- 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



Network Address Translation (NAT)



TCP Windowing



5 4 3 2 1



1 Ack

Configurable IPv4 settings

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 172 . 16 . 0 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 172 . 16 . 0 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 172 . 16 . 0 . 10

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel



Configurable IPv4 settings

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☒ Obtain DNS server address automatically

☐ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

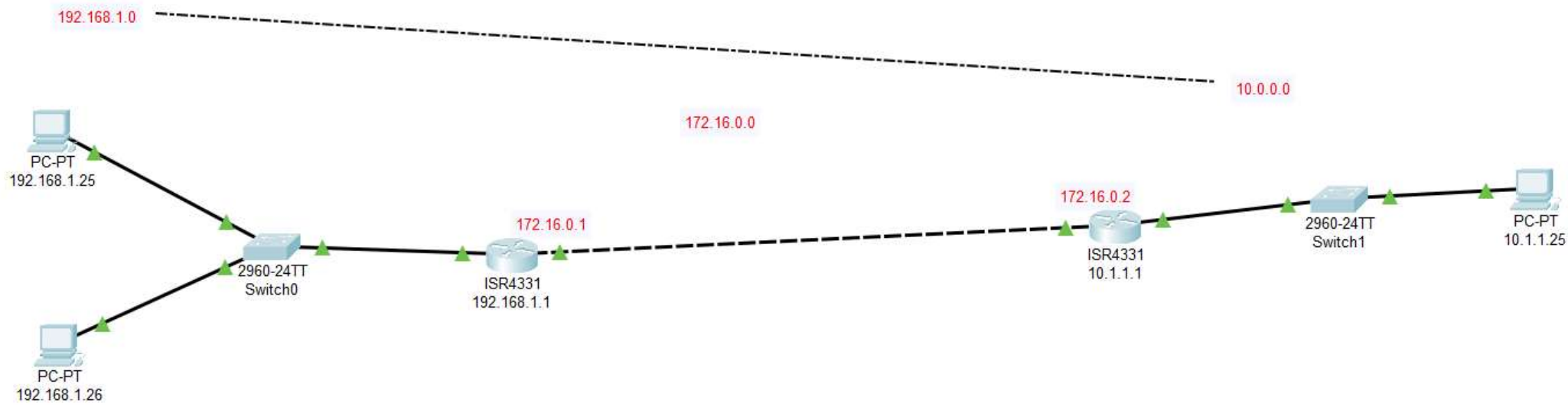
Advanced...

OK Cancel



Cisco Packet Tracer

- Cisco Packet Tracer is a network simulation tool developed by Cisco Systems. It allows users to design, configure, and troubleshoot computer networks using virtual equipment and simulated network devices, including routers, switches, and servers. With Packet Tracer, users can create and test network topologies, experiment with different network configurations, and simulate the behavior of various network protocols.
- Packet Tracer is widely used in educational settings to teach networking concepts, and it is often used by students studying for Cisco networking certifications. It can also be used by network professionals to test and prototype network designs before deploying them in a production environment. The software provides a user-friendly interface that makes it easy to visualize and interact with network topologies, and it supports a variety of network protocols and technologies, including IPv4 and IPv6, VLANs, NAT, DHCP, and VPNs.



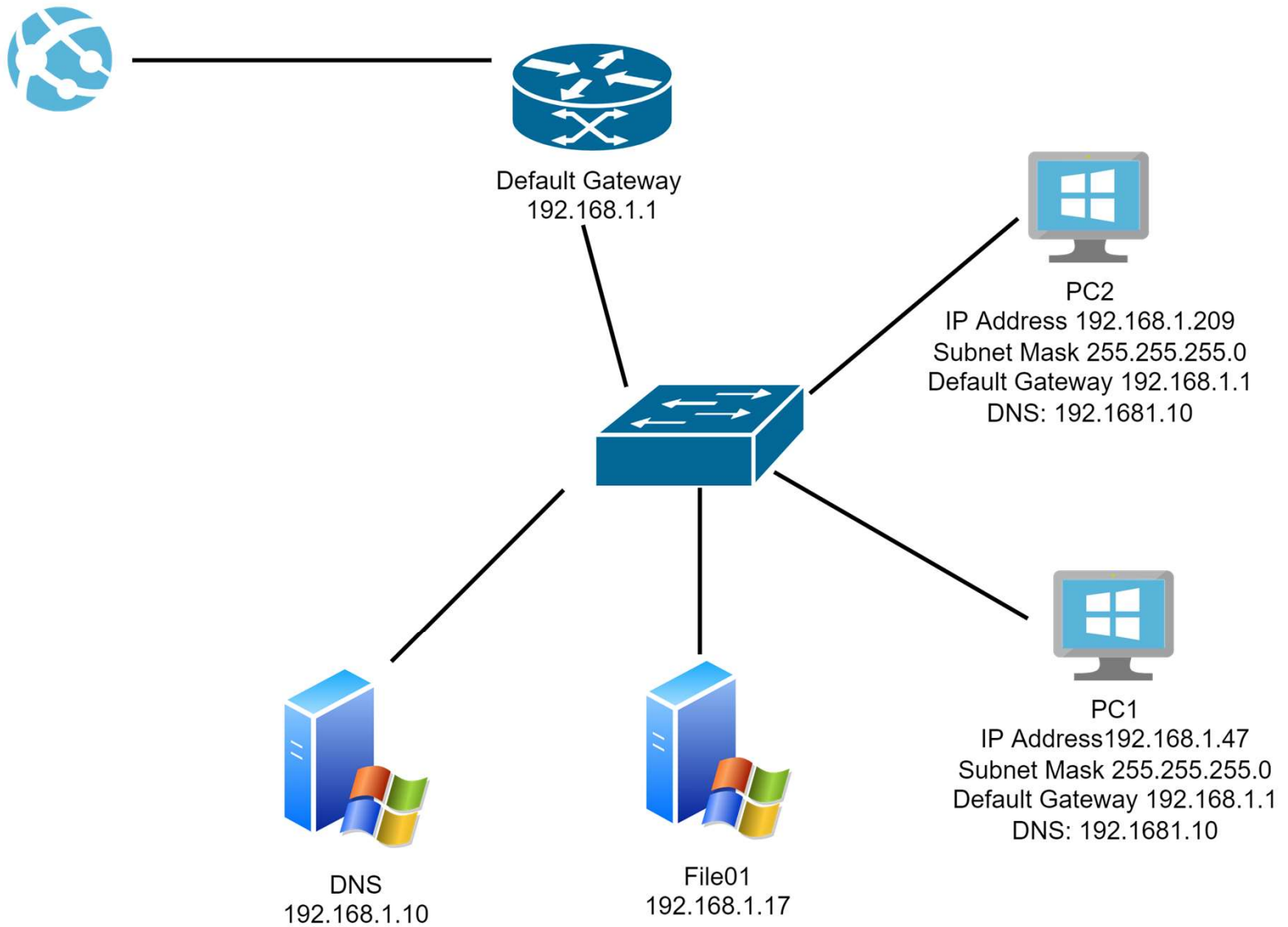
Lesson 2: Managing and troubleshooting IPv4 network connectivity

- IPv4 troubleshooting methodology
- Tools for troubleshooting IPv4
- What is Wireshark?

IPv4 troubleshooting methodology

One methodology is to ask a series of questions about the nature of the issue:

- Can you duplicate the issue?
- What is working?
- What does not work?
- How are the things that work and do not work related?
- Does it work for other systems on the network?
- Has it worked in the past?
- What has changed since it last worked?



Tools for troubleshooting IPv4

Use the following tools to troubleshoot IPv4:

- **Ipconfig**
 - **/?** Displays Help at the command prompt
 - **/all** Displays the full TCP/IP configuration for all adapters
 - **/renew /renew6** Renews a DHCP assigned IP address
 - **/release /release6** Releases a DHCP assigned IP address
 - **/displaydns** Displays the contents of the DNS client resolver cache
 - **/flushdns** Flushes and resets the contents of the DNS client resolver cache.

Tools for troubleshooting IPv4

Use the following tools to troubleshoot IPv4:

- Ping
 - **-t** Ping the specified host until stopped
 - **-a** Resolve addresses to hostnames
 - **-n** <count> Number of echo requests to send
 - **-i** <TTL> Time To Live
 - **-4** Force using IPv4
 - **-6** Force using IPv6

Tools for troubleshooting IPv4

Use the following tools to troubleshoot IPv4:

- Tracert
 - **-d** Stops attempts to resolve the IP addresses of intermediate routers to their names. This can speed up the return of results
 - **-h <Maximum hops>** Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops
 - **-w <timeout>** Specifies the amount of time in milliseconds to wait for the ICMP time Exceeded or echo Reply message corresponding to a given echo Request message to be received. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds)
 - **-4** Specifies that tracert.exe can use only IPv4 for this trace
 - **-6** Specifies that tracert.exe can use only IPv6 for this trace

Tools for troubleshooting IPv4

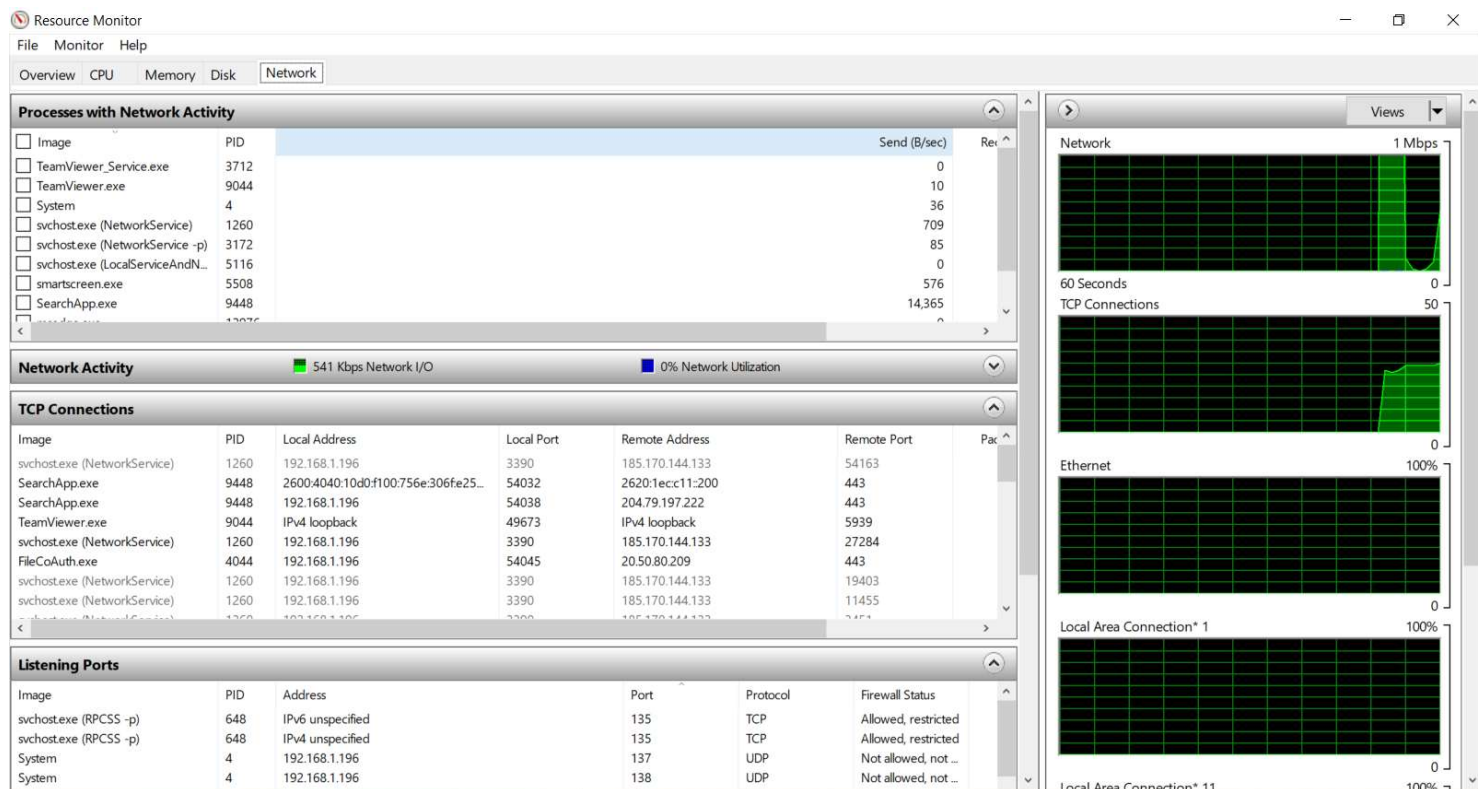
Use the following tools to troubleshoot IPv4:

- Pathping
 - **-n** Prevents **pathping** from attempting to resolve the IP addresses of intermediate routers to their names. This might expedite the display of **pathping** results
 - **-h** Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops
 - **-w <timeout>** Specifies the number of milliseconds to wait for each reply. The default is 3000 milliseconds (3 seconds). This parameter sends multiple pings in parallel. Because of this, the amount of time specified in the *timeout* parameter isn't bounded by the amount of time specified in the *period* parameter for waiting between pings
 - **-4** Specifies that pathping uses IPv4 only
 - **-6** Specifies that pathping uses IPv6 only

Tools for troubleshooting IPv4

Use the following tools to troubleshoot IPv4:

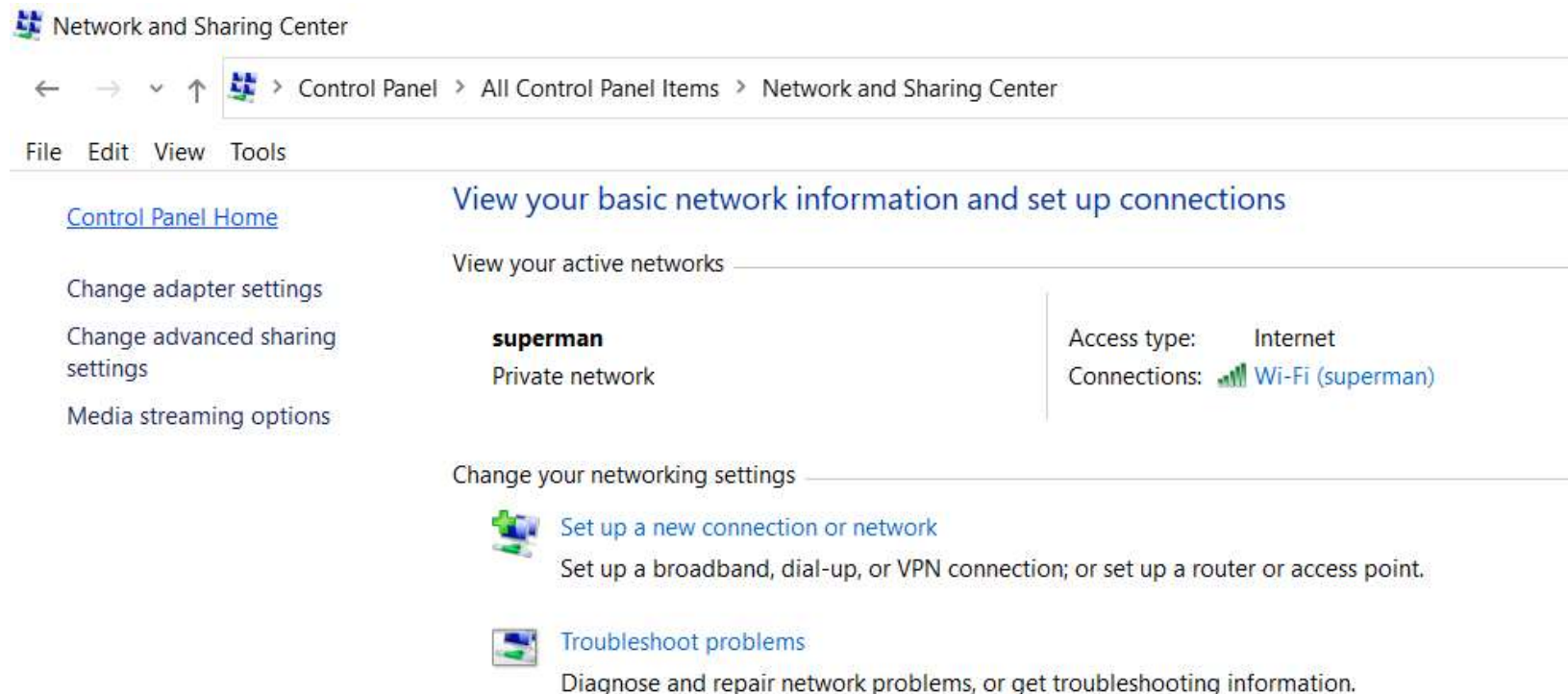
- Resource Monitor



Tools for troubleshooting IPv4

Use the following tools to troubleshoot IPv4:

- Windows Network Diagnostics



Tools for troubleshooting IPv4

New Windows PowerShell cmdlets include:

- Get-NetAdapter
- Restart-NetAdapter
- Get-NetIPInterface
- Get-NetIPAddress
- Get-DNSClientCache
- Get-DNSClientServerAddress
- Set-DnsClient
- Set-DnsClientServerAddress
- Set-NetIPAddress
- Test-Connection (legacy)
- Test-NetConnection
- Resolve-Dnsname

Tools for troubleshooting IPv4

Many Windows PowerShell commands are similar to traditional command-line tools

- To check the network configuration:
 - Windows PowerShell: **Get-NetIPAddress**
 - Command-line: **ipconfig**
- To check routing:
 - Windows PowerShell: **Test-NetConnection -TraceRoute**
 - Command-line: **tracert**
- To check for a response:
 - Windows PowerShell: **Test-NetConnection**
 - Command-line: **ping**

Wireshark

Wireshark is a free and open-source network protocol analyzer. It allows users to capture and examine the traffic passing through a computer network, including both wired and wireless networks.

With Wireshark, you can inspect individual packets to see detailed information about each one, including source and destination addresses, packet sizes, and the type of data being transmitted. This information can be useful for troubleshooting network issues, detecting security threats, and optimizing network performance.

Wireshark supports a wide range of network protocols, including TCP/IP, DNS, HTTP, and many others. It can be used on multiple platforms, including Windows, macOS, and Linux. The user interface of Wireshark is intuitive and provides various tools for filtering and searching network traffic, making it easier to find specific information.

In summary, Wireshark is a powerful and widely used tool for network analysis, providing valuable insights into network traffic and behavior.

Module 2: Dynamic Host Configuration Protocol (DHCP)



Module Overview

- Overview of the DHCP server role
- Deploying DHCP
- Managing and troubleshooting DHCP

Lesson 1: Overview of the DHCP server role

- Benefits of using DHCP
- How DHCP allocates addresses
- How DHCP lease generation works
- How DHCP lease renewal works

How DHCP works

Switch



Router



Server



IP range Start: 192.168.1.11

IP range End: 192.168.1.254

Default Gateway: 192.168.1.1

DNS: 192.168.1.5, 192.168.1.6

DHCP clients

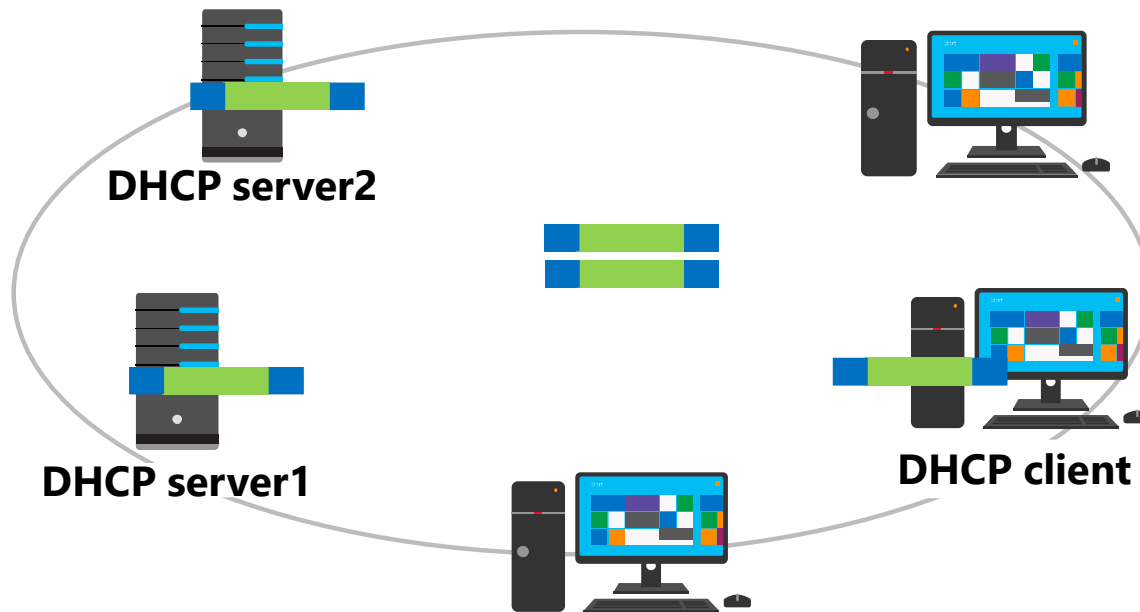


Benefits of using DHCP

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

Automatic IP configuration	Manual IP configuration
Supplies IP addresses automatically	Type IP addresses manually
Ensures correct configuration information	Typing incorrect IP address is a possibility
Updates client configuration automatically	Can result in possible communication and network issues
Eliminates a common source of network problems	Frequent computer moves increase administrative effort

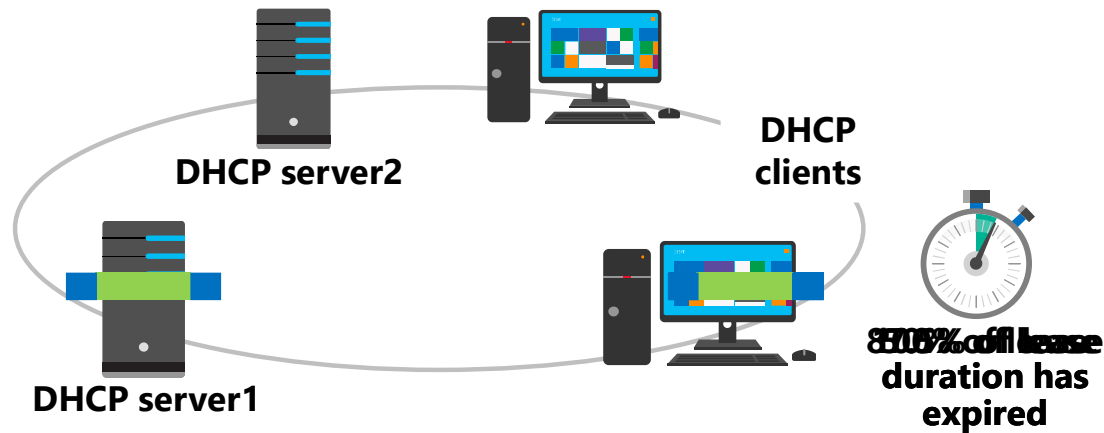
How DHCP lease generation works



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 lease renewal works



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



Automatic Private IP Addressing (APIPA)

- APIPA will automatically assign an IP address to the local computer when DHCP is unavailable.
- APIPA IP addresses are:
 - 169.254.x.x
 - 255.255.0.0
- If a computer has an APIPA IP address it will send a DHCPDISCOVER message every 5 minutes.

Lesson 2: Deploying DHCP

- Installing and configuring the DHCP server role
- DHCP server authorization
- Allocating and managing IPv4 addresses with DHCP
- Configuring DHCP options

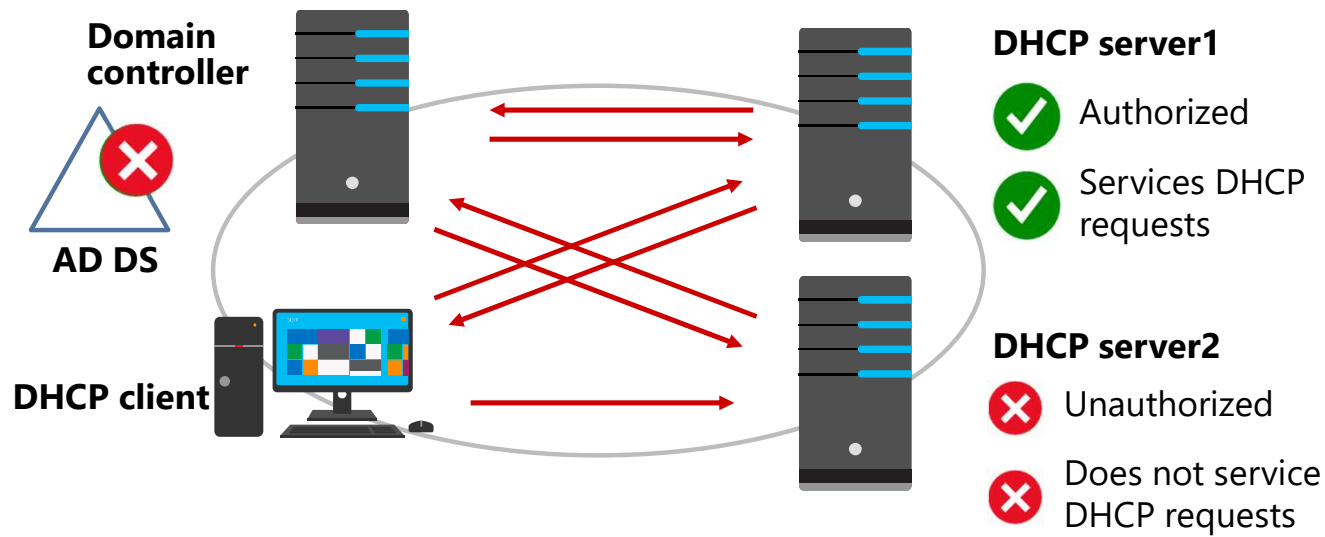
Installing and configuring the DHCP server role

- You can install the DHCP server role by using:
 - The Add Roles and Features Wizard in Server Manager
 - Windows PowerShell:
 - **Install-WindowsFeature DHCP -IncludeManagementTools**
- The server hosting DHCP requires a static IP address
- Post-installation tasks include:
 - Creating DHCP security groups
 - Restarting the DHCP Server service
 - Authorizing the DHCP server in AD DS

DHCP server authorization

DHCP authorization registers the DHCP Server service in the Active Directory domain to support DHCP clients

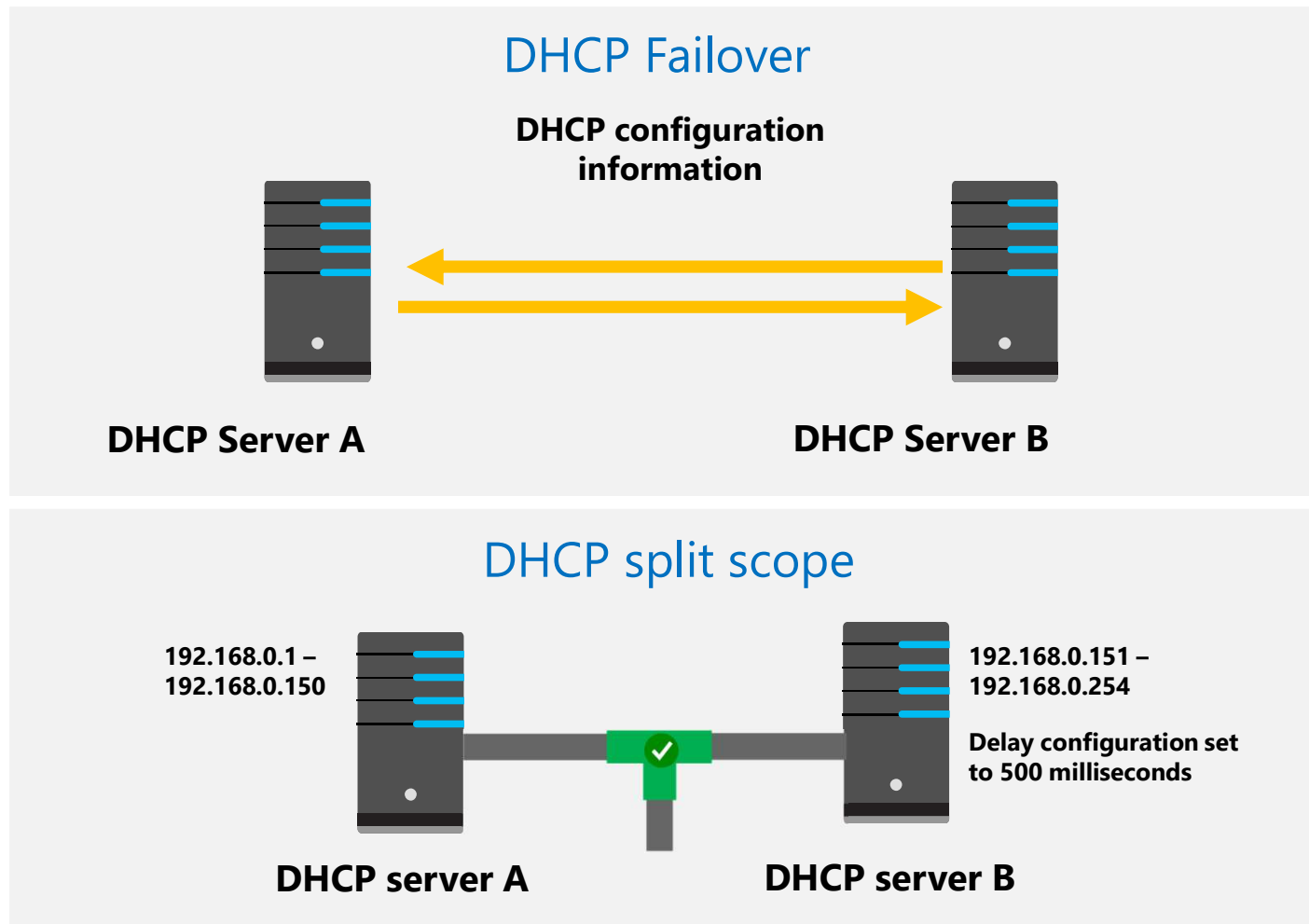
If DHCP Server1 finds its IP address on the list, the service starts and supports DHCP clients



Allocating and managing IPv4 addresses with DHCP

- 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

High availability options for DHCP



What is DHCP Split Scope and Failover?

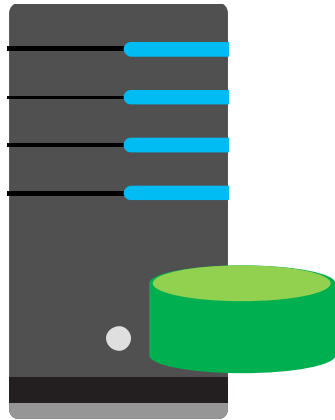
- DHCP Split Scope:
 - Enables two DHCP servers to provide IP addresses and optional configurations to the same subnets
- When you use DHCP failover:
 - The auto state switchover interval determines when a failover partner is considered to be down
 - Firewall rules are auto-configured during DHCP installation
 - Enables two DHCP servers to provide IP addresses and optional configurations to the same subnets or scopes
 - Requires failover relationships to have unique names
 - Supports the hot standby mode and the load sharing mode

Maintaining the DHCP database

- The DHCP database (Dhcp.mdb) contains information relating to scopes, leases, reservations, and all other configuration information
- The default location of DHCP database files is **%systemroot%\system32\DHCP**
- The DHCP database is automatically backed up every 60 minutes. You can also perform a manual backup
- You can reconcile the DHCP database to repair inconsistencies
- You can move the DHCP database to a new DHCP server when the DHCP Server service is moved

Migrating the DHCP server

- You can migrate the DHCP server by exporting the DHCP data from the old server, and then importing it to the new server



Export data from
current server to a file



Import data to new
server from the file



Module 3: Understanding and Implementing Domain Name Service (DNS)



Module Overview

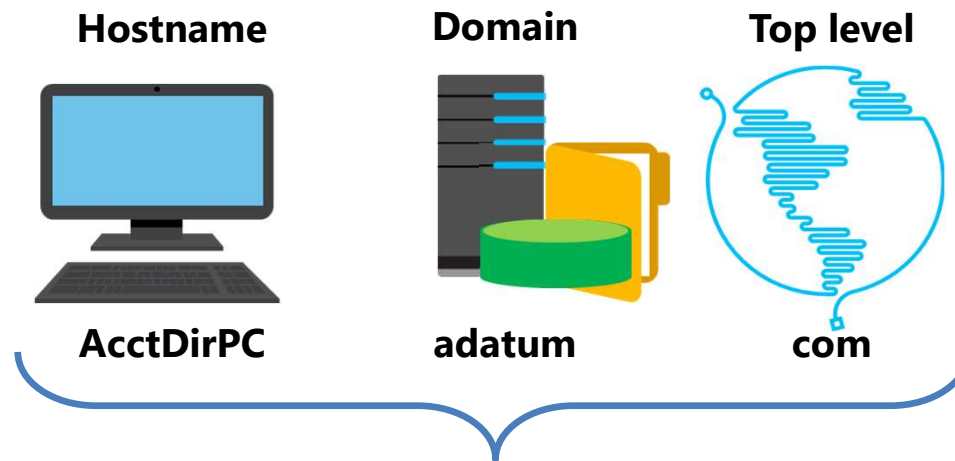
- Implementing DNS servers
- Configuring zones in DNS
- Configuring name resolution between DNS zones
- Configuring DNS integration with AD DS
- Configuring advanced DNS settings

Lesson 1: Implementing DNS servers

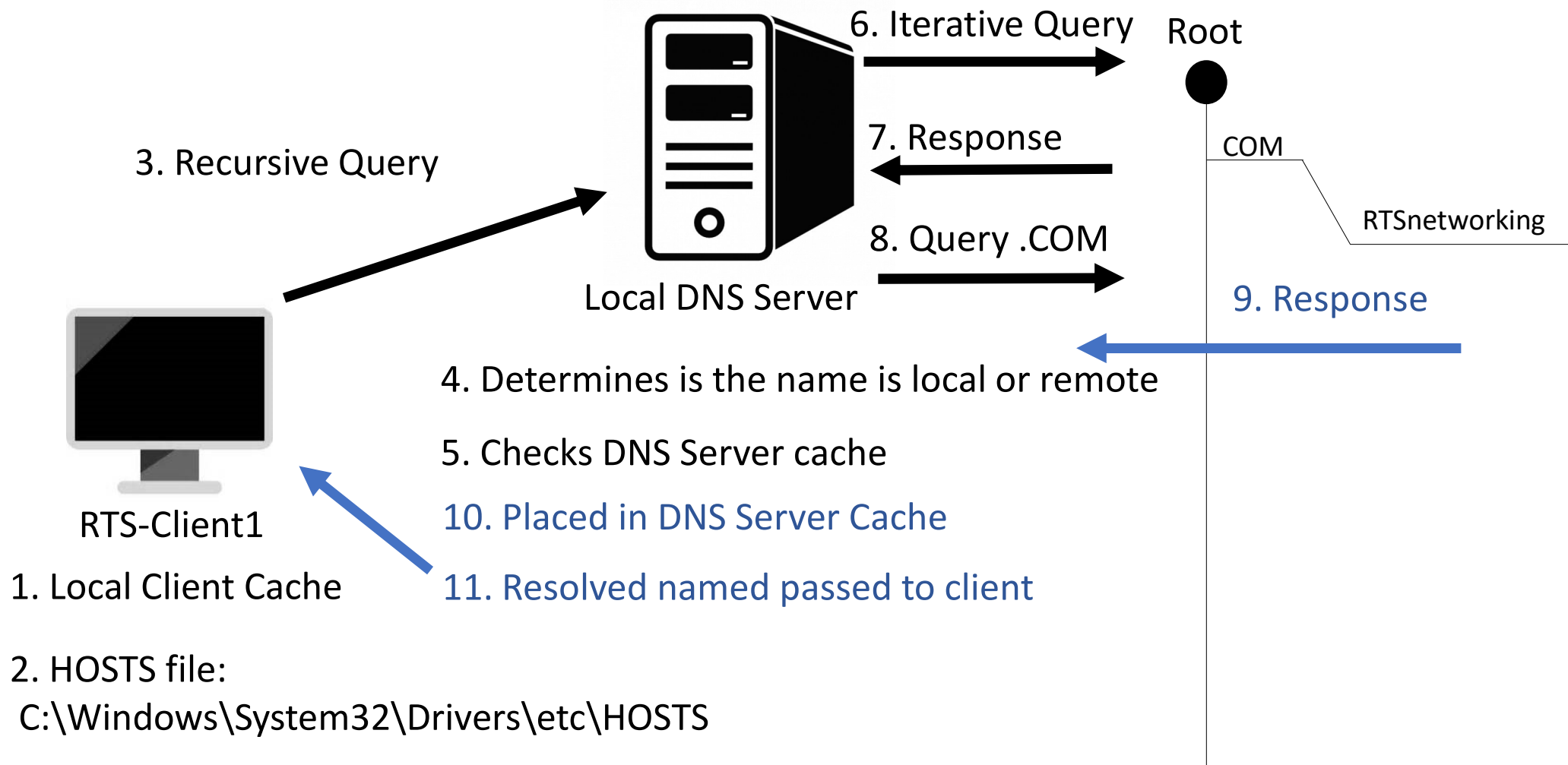
- How does DNS name resolution work?
- DNS components
- What are DNS zones and records?
- Configuring DNS clients
- Tools and techniques for troubleshooting name resolution
- Managing DNS services
- Testing DNS servers

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.adatum.com



DNS components

DNS infrastructure components include:

- DNS server
- DNS zone
- Resource records
- DNS resolvers

What are DNS zones and records?

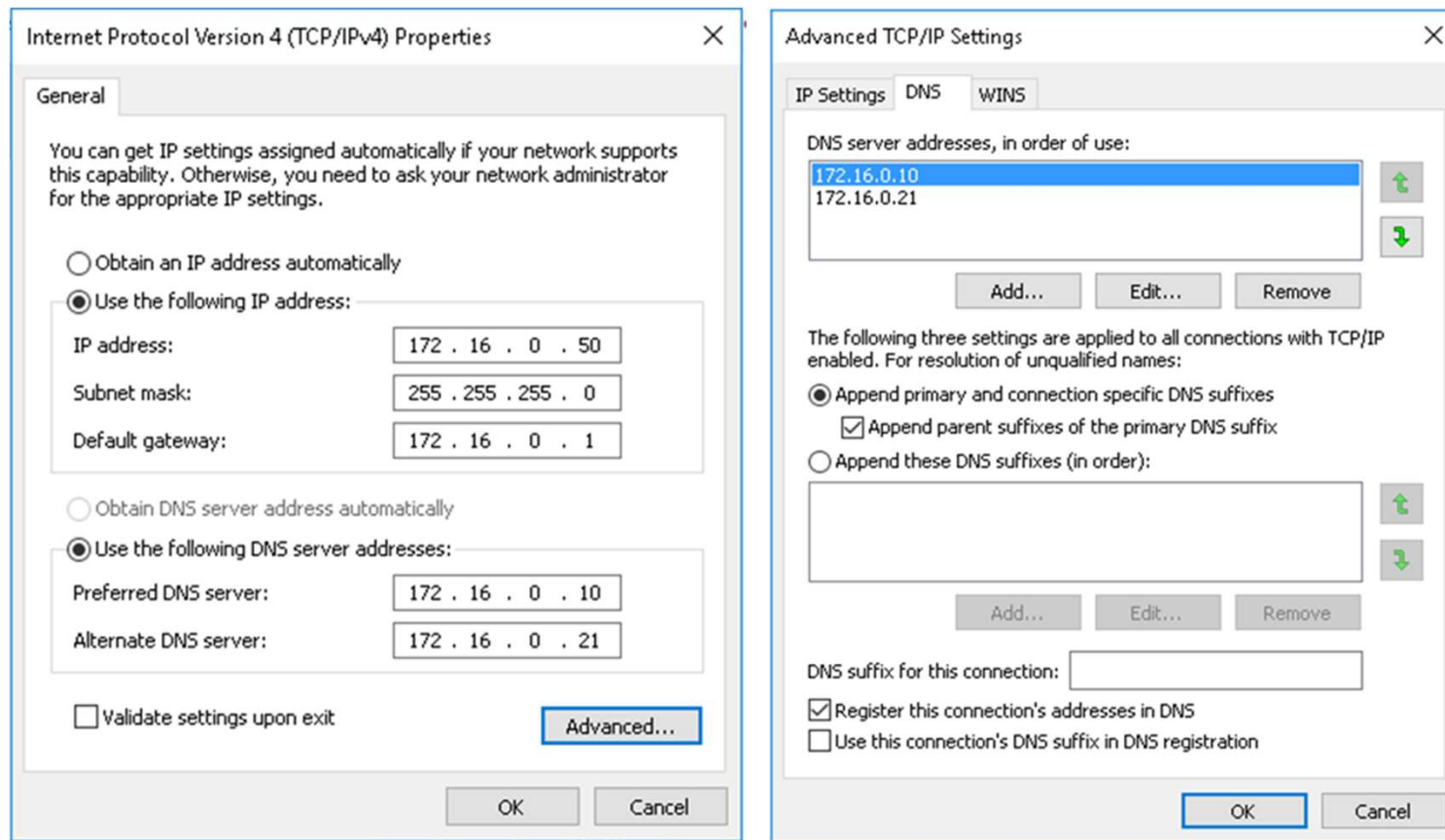
- A DNS zone is a specific portion of DNS namespace that contains DNS records
- Zone types:
 - Forward lookup zone
 - Reverse lookup zone
- Resource records in forward lookup zones include: A, MX, SRV, NS, and CNAME
- Resource records in reverse lookup zones include: PTR

DNS resource record types

DNS resource records include:

- A: IPv4 host address resource record
- CNAME: Alias resource record
- MX: Mail exchange resource record
- SRV: Service locator resource record
- NS: Name server resource record
- AAAA: IPv6 host address resource record
- PTR: Pointer resource record

Configuring DNS clients



```
Set-DnsClientServerAddress -InterfaceIndex 12 -ServerAddresses  
("172.16.0.10","172.16.0.21")
```

Tools and techniques for troubleshooting name resolution

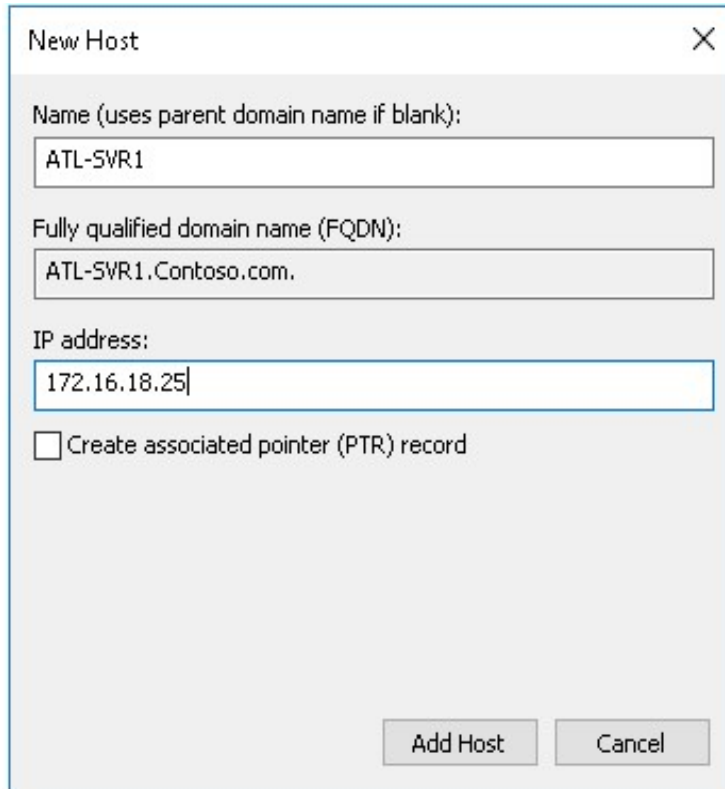
Command-line tools to troubleshoot configuration issues:

- Ping
- Test-NetConnection
- Test-NetConnection –ComputerName ***name*** –Port ***port_number***
- TraceRoute
- Test-NetConnection –traceroute ***name***
- Pathping
- Ipconfig
- Get-NetIpAddress
- Nslookup
- Resolve-DnsName
- Ipconfig /displayDNS
- Ipconfig /flushDNS
- Get-DnsClientCache
- Clear-DncClientCache

Lesson 2: Configuring zones in DNS

- Creating records in DNS
- Configuring DNS zones
- What are primary and secondary zones?
- Configuring zone replication

Creating records in DNS



The 'New Host' dialog box is used to create a new host record. It contains three text input fields: 'Name (uses parent domain name if blank):' with the value 'ATL-SVR1', 'Fully qualified domain name (FQDN):' with the value 'ATL-SVR1.Contoso.com.', and 'IP address:' with the value '172.16.18.25'. There is an unchecked checkbox labeled 'Create associated pointer (PTR) record'. At the bottom right are 'Add Host' and 'Cancel' buttons.

New Host

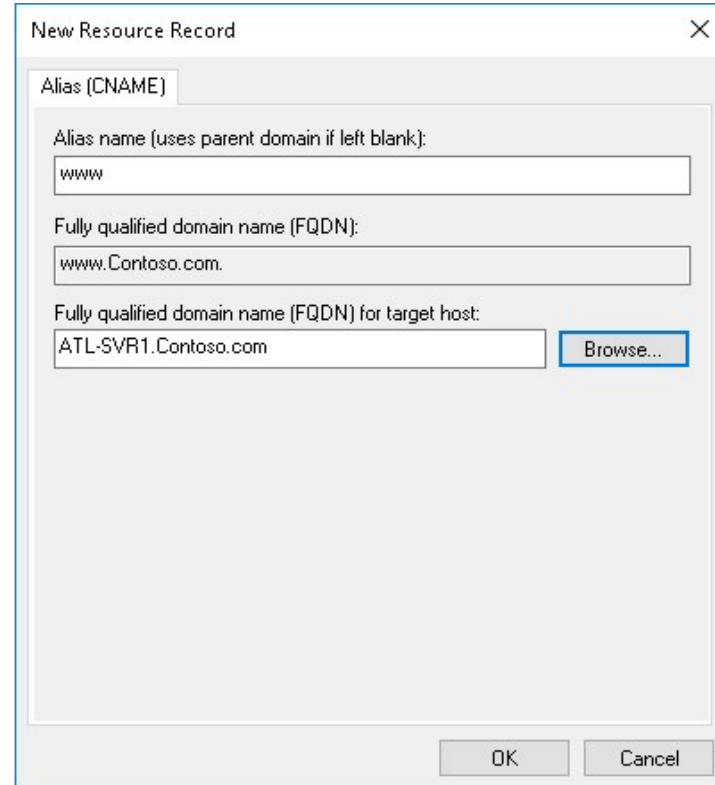
Name (uses parent domain name if blank):
ATL-SVR1

Fully qualified domain name (FQDN):
ATL-SVR1.Contoso.com.

IP address:
172.16.18.25

☐ Create associated pointer (PTR) record

Add Host Cancel



The 'New Resource Record' dialog box is used to create a new resource record. It has a tab labeled 'Alias (CNAME)'. It contains three text input fields: 'Alias name (uses parent domain if left blank):' with the value 'www', 'Fully qualified domain name (FQDN):' with the value 'www.Contoso.com.', and 'Fully qualified domain name (FQDN) for target host:' with the value 'ATL-SVR1.Contoso.com'. There is a 'Browse...' button next to the target host field. At the bottom right are 'OK' and 'Cancel' buttons.

New Resource Record

Alias (CNAME)

Alias name (uses parent domain if left blank):
www

Fully qualified domain name (FQDN):
www.Contoso.com.

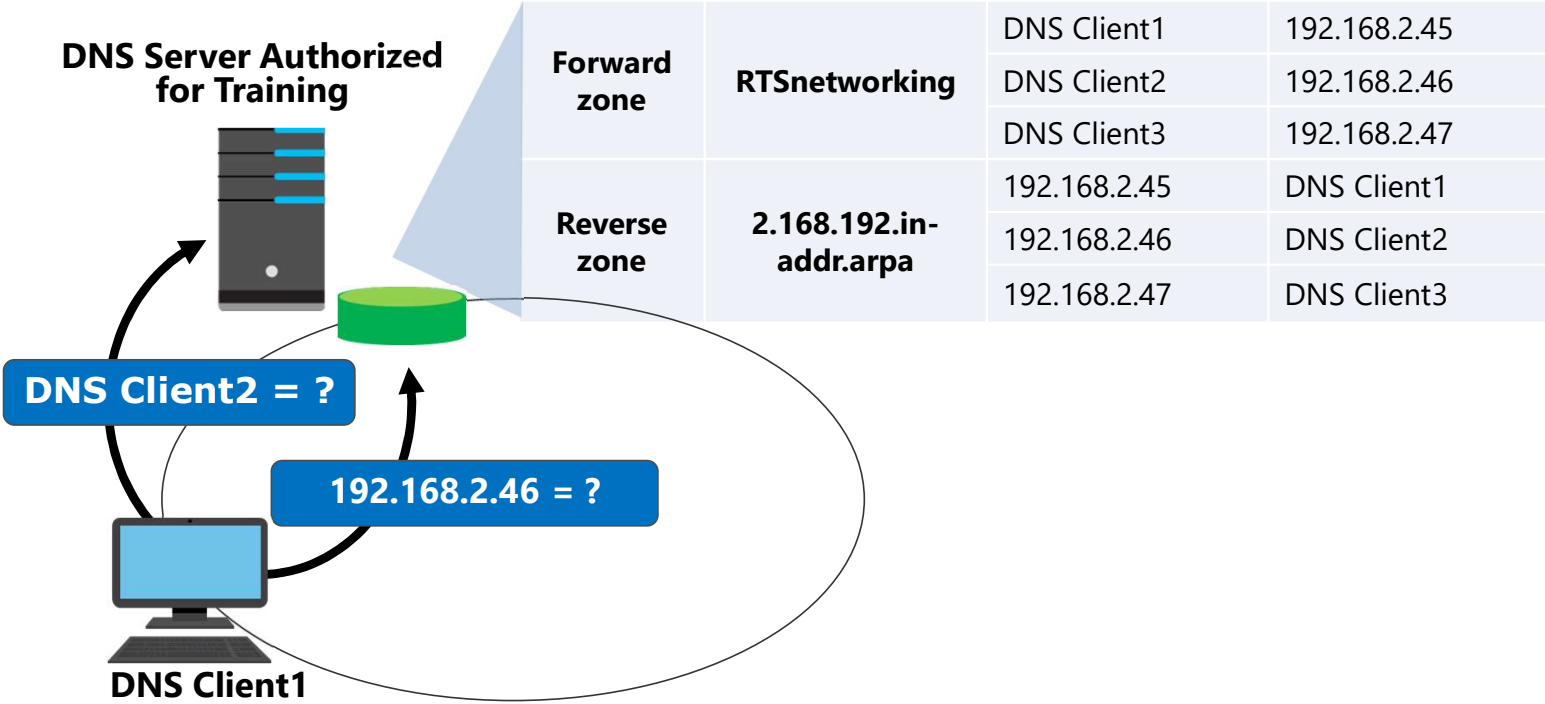
Fully qualified domain name (FQDN) for target host:
ATL-SVR1.Contoso.com Browse...

OK Cancel

**Add-DnsServerResourceRecordA -ZoneName Contoso.com -Name ATL-SVR1
-IpAddress 172.16.18.25**

Configuring DNS zones

Namespace: rtsnetworking.com



What are primary and secondary zones?

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

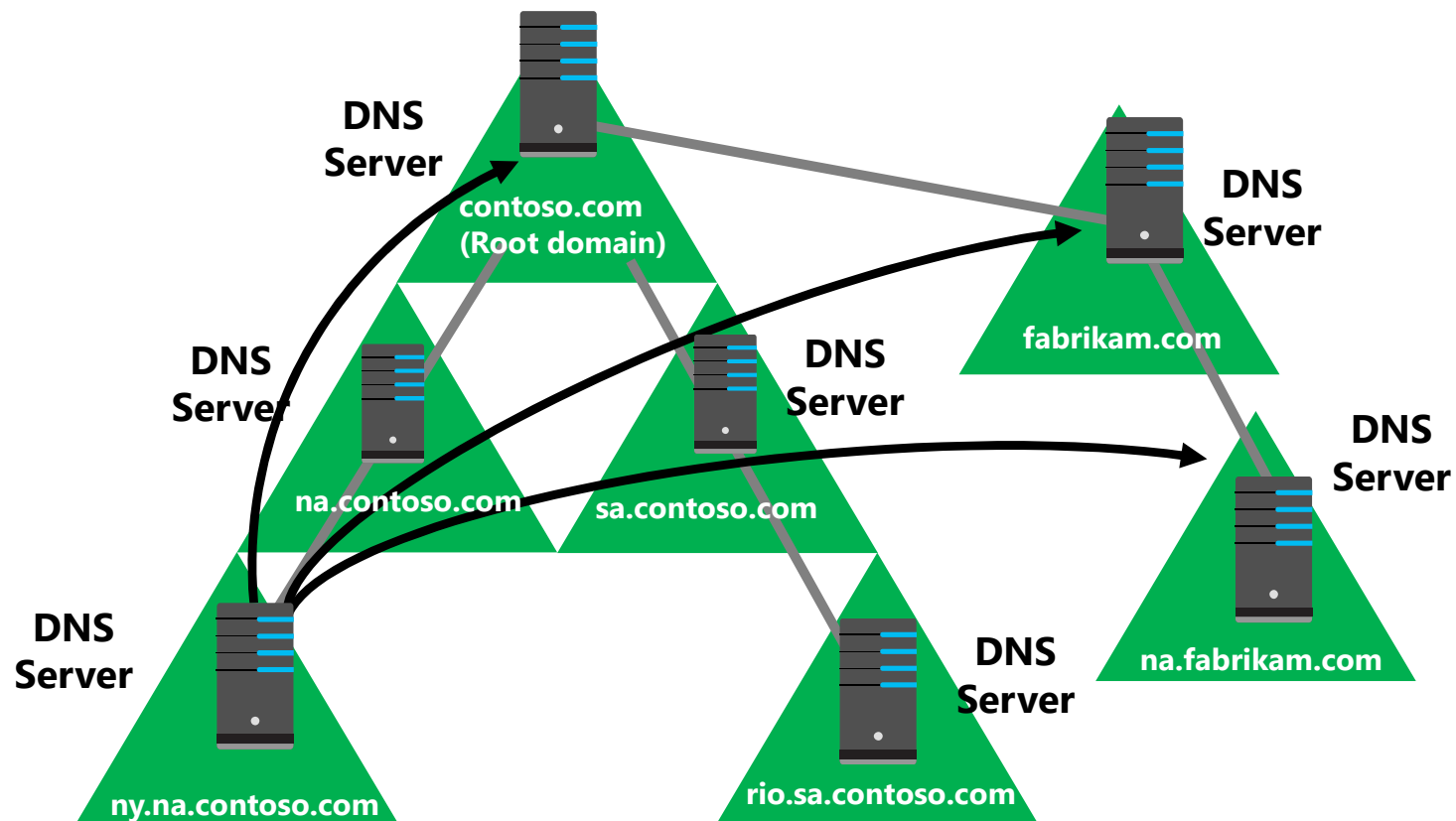
What are Active Directory–integrated zones?

An Active Directory–integrated zone:

- Allows multi-master writes to zone
- Replicates DNS zone information by using AD DS replication:
 - Leverages efficient replication topology
 - Uses efficient incremental updates for Active Directory replication processes
- Enables secure dynamic updates

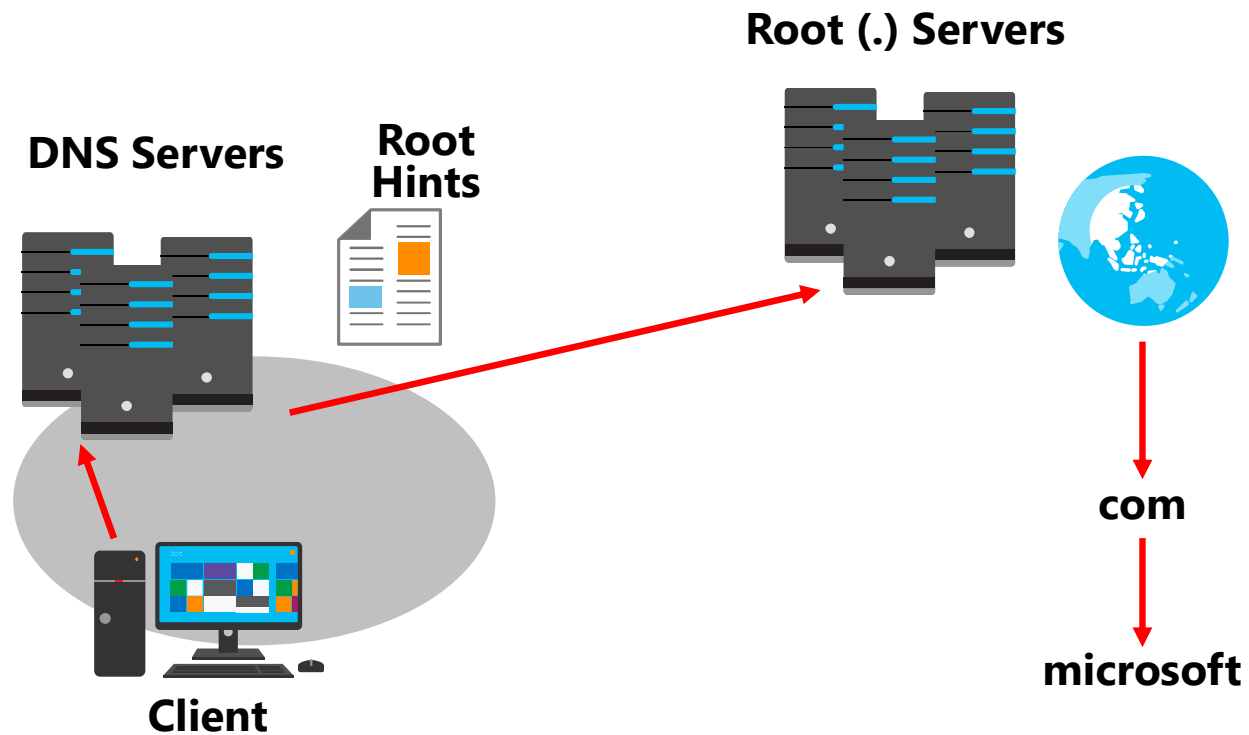
What is a stub zone?

Without stub zones, the ny.na.contoso.com server must query several servers to find the server that hosts the na.fabrikam.com zone

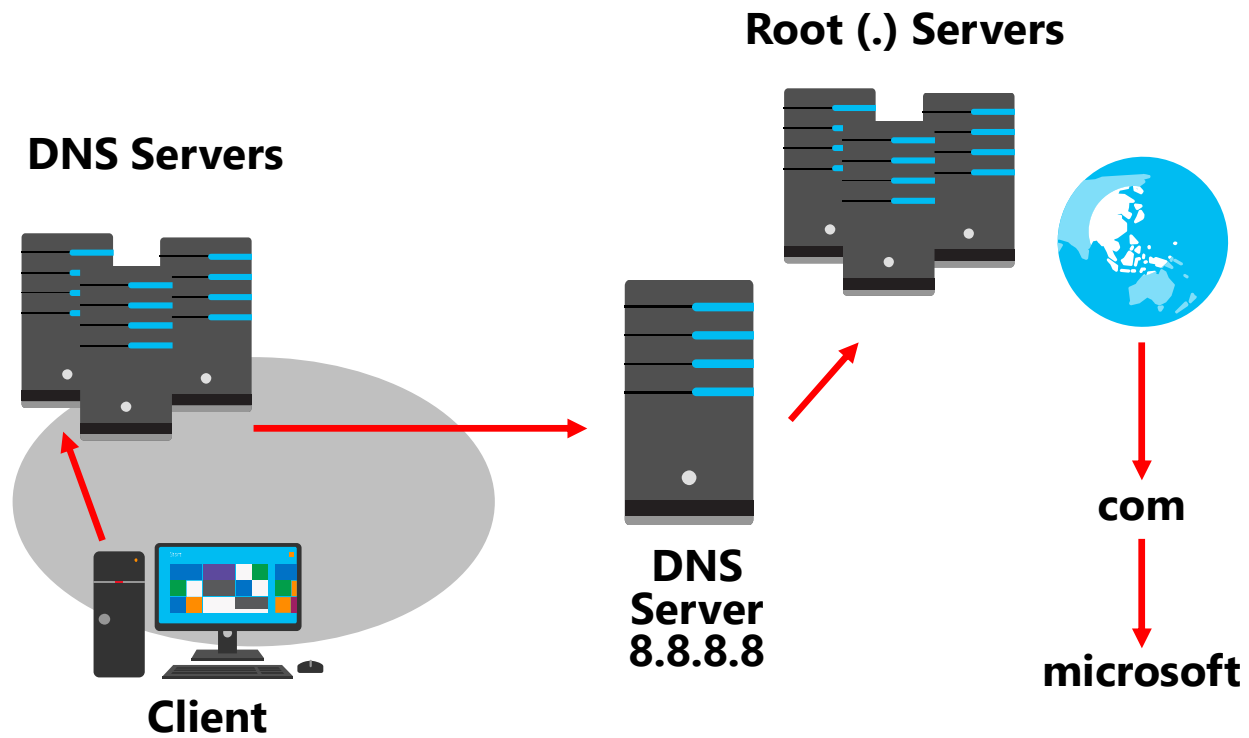


Configuring root hints

**Root hints contain the IP addresses for
DNS root servers**



Configuring DNS Forwarding



Module 4: Understanding IPv6



Module Overview

- Overview of IPv6 addressing
- Configuring an IPv6 host
- Implementing IPv6 and IPv4 coexistence
- Transitioning from IPv4 to IPv6

Lesson 1: Overview of IPv6 addressing

- Why use IPv6?
- Differences between IPv4 and IPv6
- Overview of IPv6 addressing
- IPv6 address structure
- Types of IPv6 addresses
- Autoconfiguration options for IPv6

Why use IPv6?

Organizations should consider using IPv6 because of:

- The exponential growth of the Internet and the impending exhaustion of the IPv4 address space
- The need for simpler configuration
- The requirement for security at the IP layer
- The need for better support for real-time delivery of data (also known as Quality of Service)

Differences between IPv4 and IPv6

Feature	IPv4	IPv6
Address length	32 bits	128 bits
DNS host records	A records	AAAA records
IP Addresses	4,294,967,296	340 undecillion (trillion trillion trillion)

340,000,000,000,000,000,000,000,000,000,000,000

Overview of IPv6 addressing

- 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):

FD00:0DB8:0000:0000:2D4C:0000:00DD:1122

- Further simplified by removing leading zeros:

FD00:DB8::2D4C:0:DD:1122

IPv6 address structure

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

Types of IPv6 addresses

The following are types of unicast IPv6 addresses:

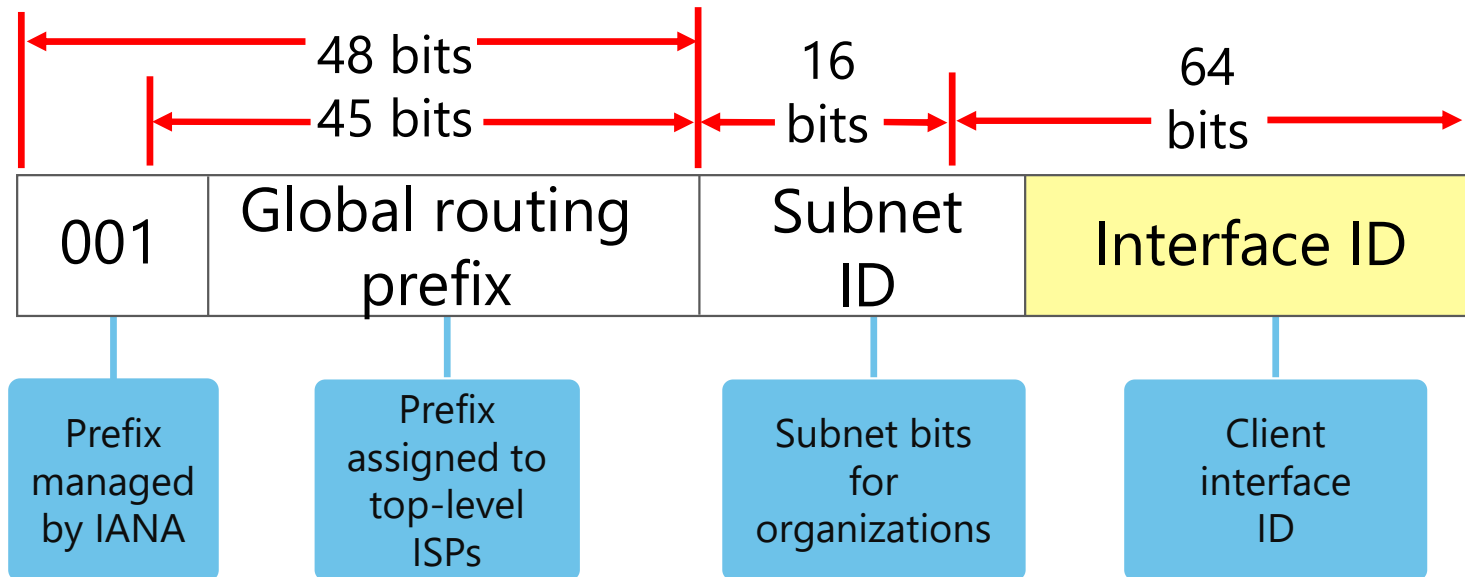
- Global unicast addresses
- Unique local addresses
- Link-local addresses



Types of IPv6 addresses

Global unicast addresses:

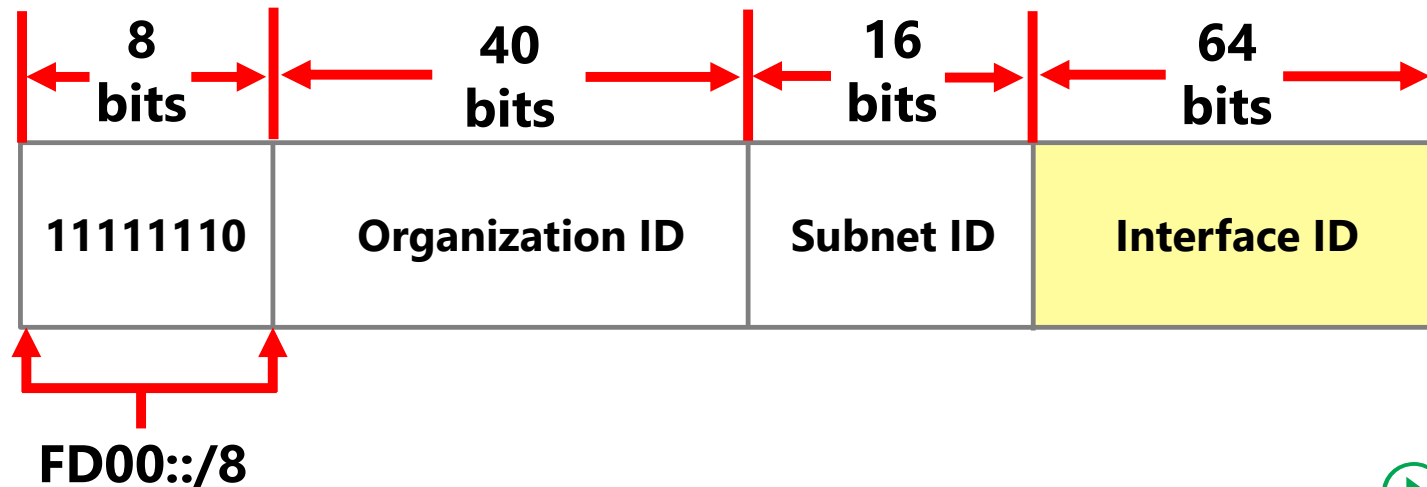
- Are routable on the IPv6 Internet
- Allocate 16 bits for internal subnetting
- Begin with 2 or 3 (2000::/3)



Types of IPv6 addresses

Unique local addresses:

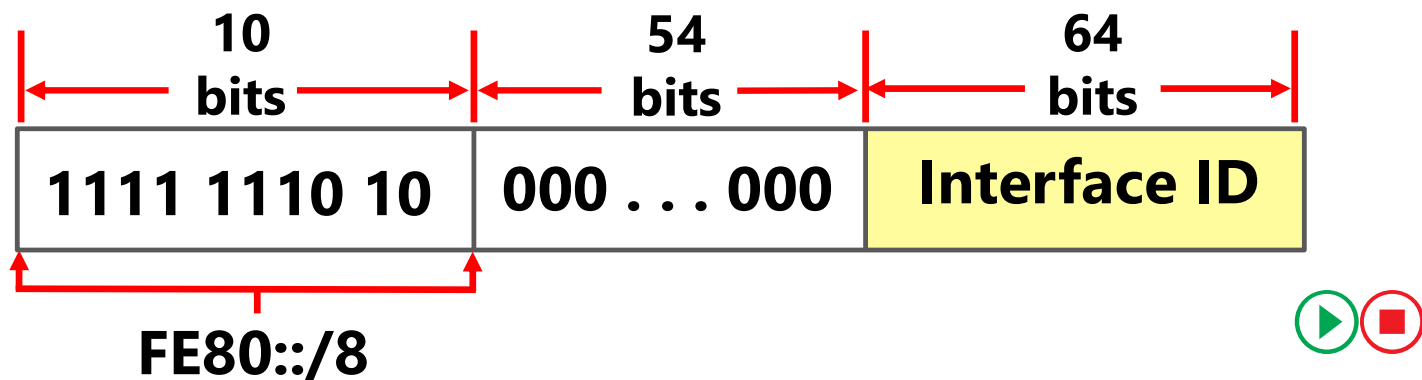
- Are equivalent to IPv4 private addresses
- Require the organization ID to be randomly generated
- Allocate 16 bits for internal subnetting



Types of IPv6 addresses

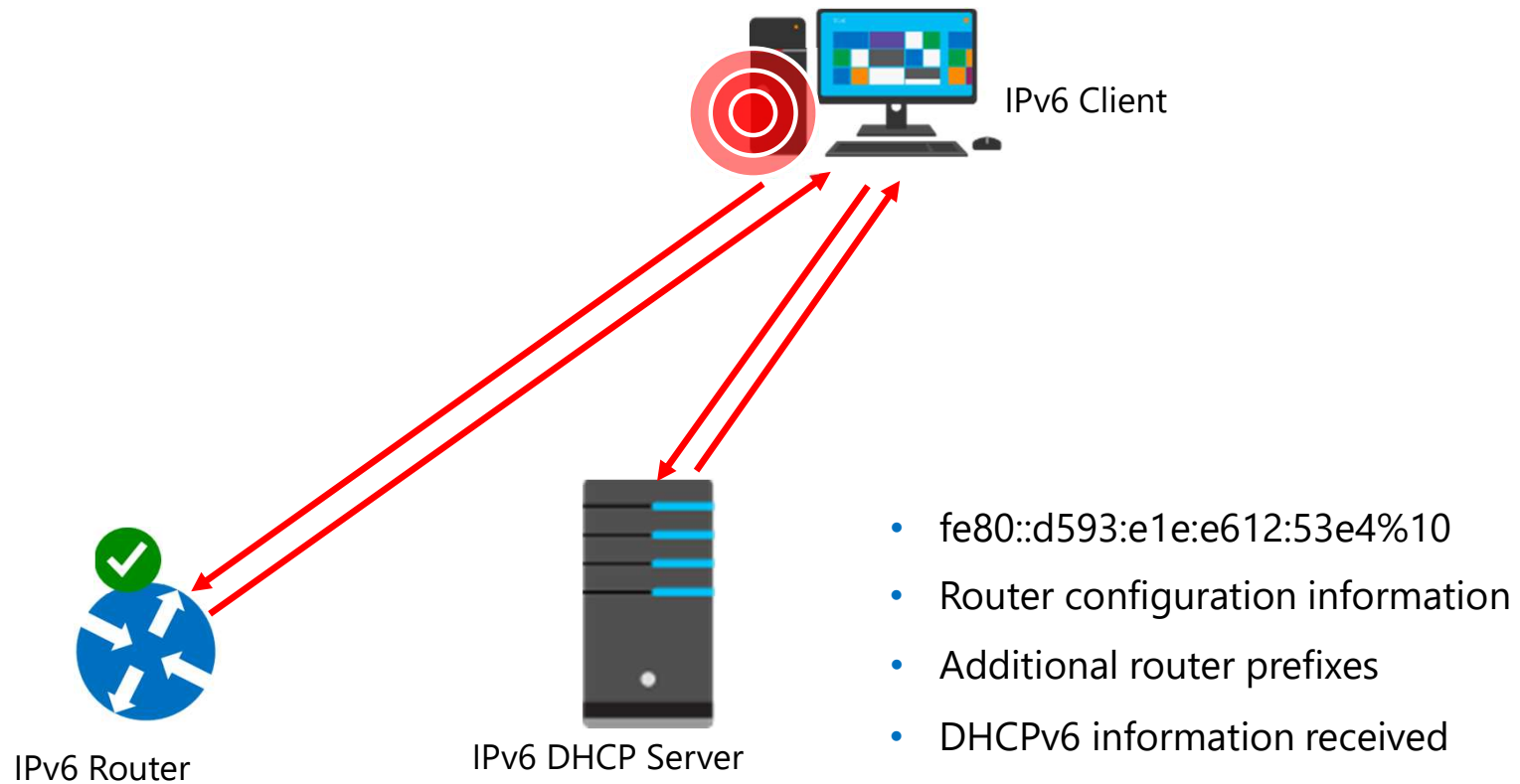
Link-local addresses:

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

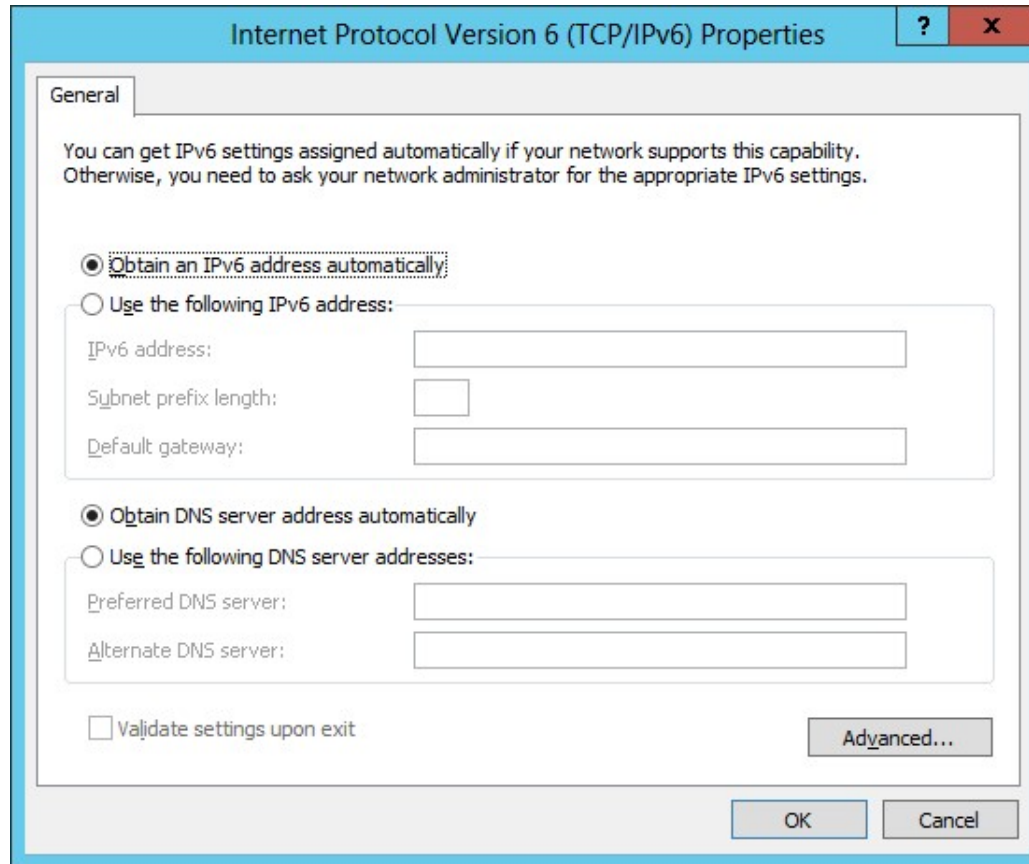


Autoconfiguration options for IPv6

1 Derive Link-Local Address



Configurable IPv6 settings



The image shows a Windows dialog box titled "Internet Protocol Version 6 (TCP/IPv6) Properties". The "General" tab is selected. The dialog contains instructions: "You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings." There are two main sections for configuration. The first section is for the IPv6 address, with the option "Obtain an IPv6 address automatically" selected. The second section is for DNS server addresses, with the option "Obtain DNS server address automatically" selected. At the bottom, there is a checkbox for "Validate settings upon exit" and an "Advanced..." button. The "OK" and "Cancel" buttons are at the bottom right.

Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

☒ Obtain an IPv6 address automatically:

☐ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

☒ Obtain DNS server address automatically:

☐ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel



Configurable IPv6 settings

Advanced TCP/IP Settings

IP Settings DNS

DNS server addresses, in order of use:

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

☒ Append primary and connection specific DNS suffixes
☒ Append parent suffixes of the primary DNS suffix

☐ Append these DNS suffixes (in order):

DNS suffix for this connection:

☒ Register this connection's addresses in DNS
☐ Use this connection's DNS suffix in DNS registration



Using DHCPv6

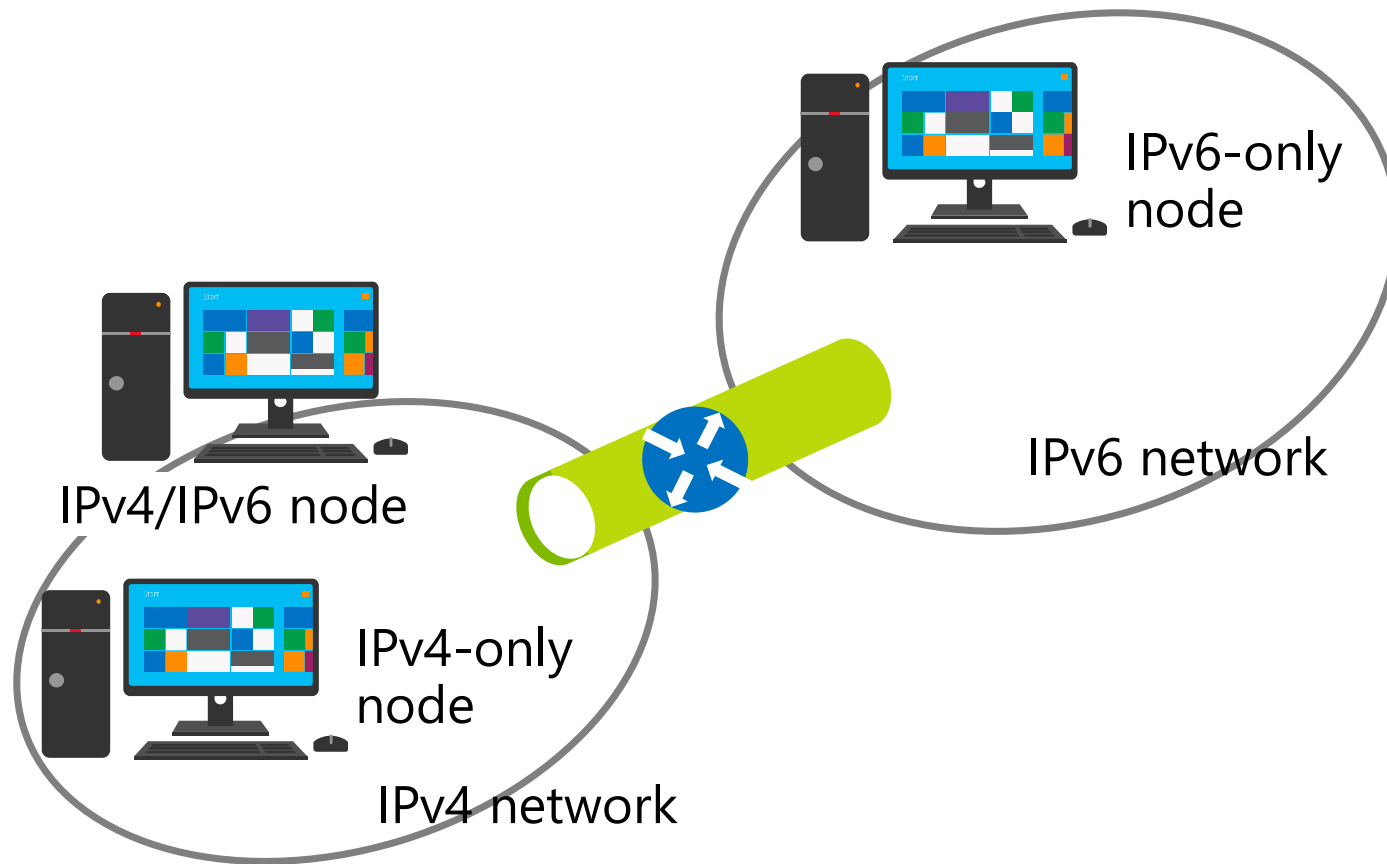
DHCP for IPv6 in Windows Server 2016 and newer

- Supports IPv6 by default
- You can configure DHCP by creating and configuring IPv6 scopes and options

DNS for IPv6 in Windows Server 2016 and newer

- Supports IPv6 by default
- Computers or DHCP can register AAAA records in DNS
- You can manually create AAAA records in DNS
- You need to create and configure reverse lookup zones for IPv4 and IPv6

What are node types?



Options for IPv4 and IPv6 coexistence

- Windows Server 2016 uses a dual IP layer architecture that supports IPv4 and IPv6 in a single protocol stack
- DNS records required for coexistence:
 - Host (A) resource records for IPv4 nodes
 - IPv6 host (AAAA) resource records
 - Reverse lookup pointer resource records for IPv4 and IPv6 nodes

Considerations for planning a native IPv6 environment

When planning for a native IPv6 environment, organizations should consider the support for:

- Operating system
- Routers and firewalls
- Network devices
- Application products
- Custom applications

What is IPv6 over IPv4 tunneling?

