CHAPTER 4

Network Addressing and Services

4.1 NETWORK ADDRESSING AND SERVICES

IP Addressing

Section Skill Overview

- Configure IP addresses on a workstation
- Configure IP addresses on an iPad
- Configure IP addresses on mobile devices

Key Terms

- Octet
- Subnet mask
- Internet Assigned Numbers Authority (IANA)
- Public IP
- Private IP
- Automatic Private IP Addressing (APIPA)
- Loopback address
- Broadcast address
- Network address

Key Terms

- Subnetting
- Fixed-length subnet mask (FLSM)
- Variable-length subnet mask (VLSM)
- Classless Inter-Domain Routing (CIDR)
- ANDing
- Supernetting

Key Definitions

- **Octet:** An 8-bit binary number. An IPv4 address consists of four octets separated by a dot.
- **Subnet mask:** A 32-bit number that defines which portion of an IPv4 address identifies the network address and which portion of the address defines the host address.
- **Internet Assigned Numbers Authority (IANA):** A nonprofit, private American corporation that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System, media types, and other Internet Protocol-related symbols and internet numbers.

Key Definitions

- **Public IP:** An IP address that is used to access the internet.
- **Private IP:** An IP address that is used only on an internal network. These IP addresses do not go out on the internet.
- **Automatic Private IP Addressing (APIPA):** A feature that allows a device to automatically assign itself an IP address on the 169.254.0.0 network when a DHCP server or manual configuration is unavailable.
- **Loopback address:** An address reserved by each network interface card (NIC), which is used for testing purposes. This special address is also known as home or localhost.

Key Definitions

- **Network address:** The first valid IP address on the network. This address is used for routing purposes to identify the network.
- **Broadcast address:** The last valid IP address on a network. It is reserved for broadcast functions. Any packet sent to this address will be sent to all devices on the network.
- **Subnetting:** The process of dividing a large network into smaller networks.
- **Fixed-length subnet mask (FLSM):** A subnetting method in which each created subnet has an equal number of addresses.

Key Definitions

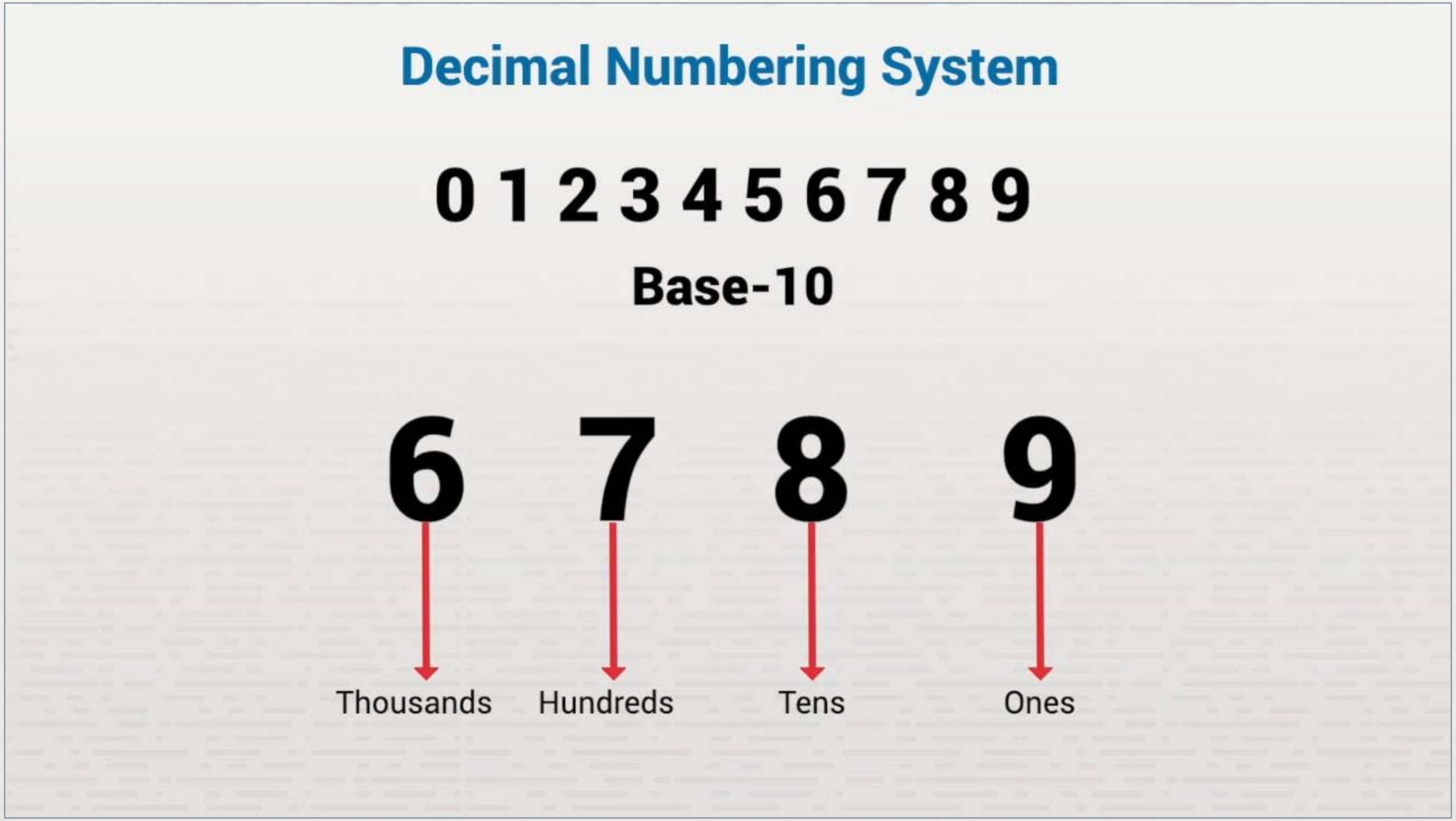
- **Variable-length subnet mask (VLSM):** A subnetting method in which each subnet can be a different size.
- **Classless Inter-Domain Routing (CIDR):** A method for allocating IP addresses and for IP routing. CIDR notation is a simplified method of writing a network address with a slash followed by the number of bits in the network ID.
- **ANDing:** The process used to determine the network address/ID.
- **Supernetting:** The process of combining two or more networks.

Numbering Systems

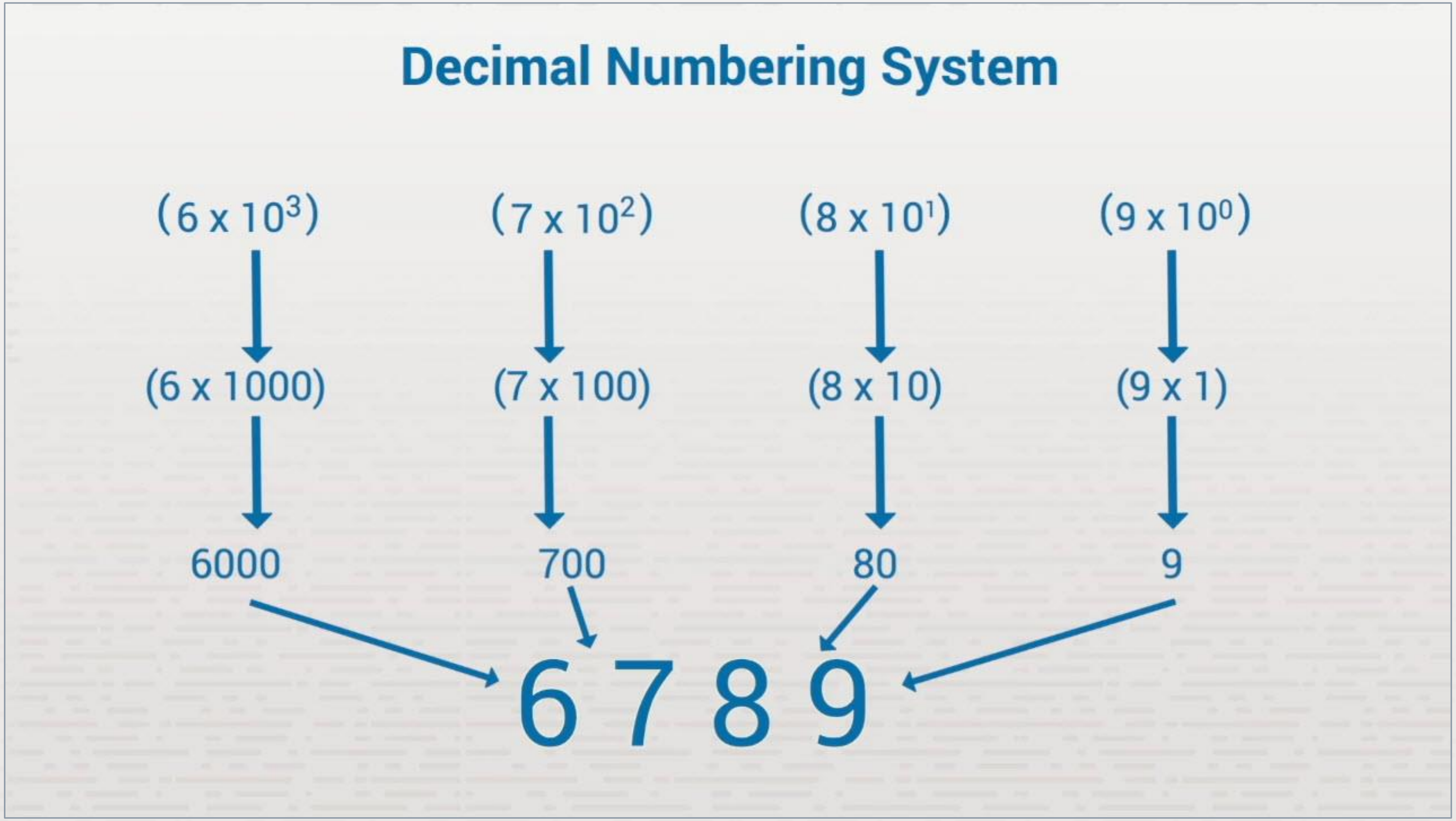
Numbering Systems

- Decimal
- Binary
- Hexadecimal
- Conversion

Numbering Systems



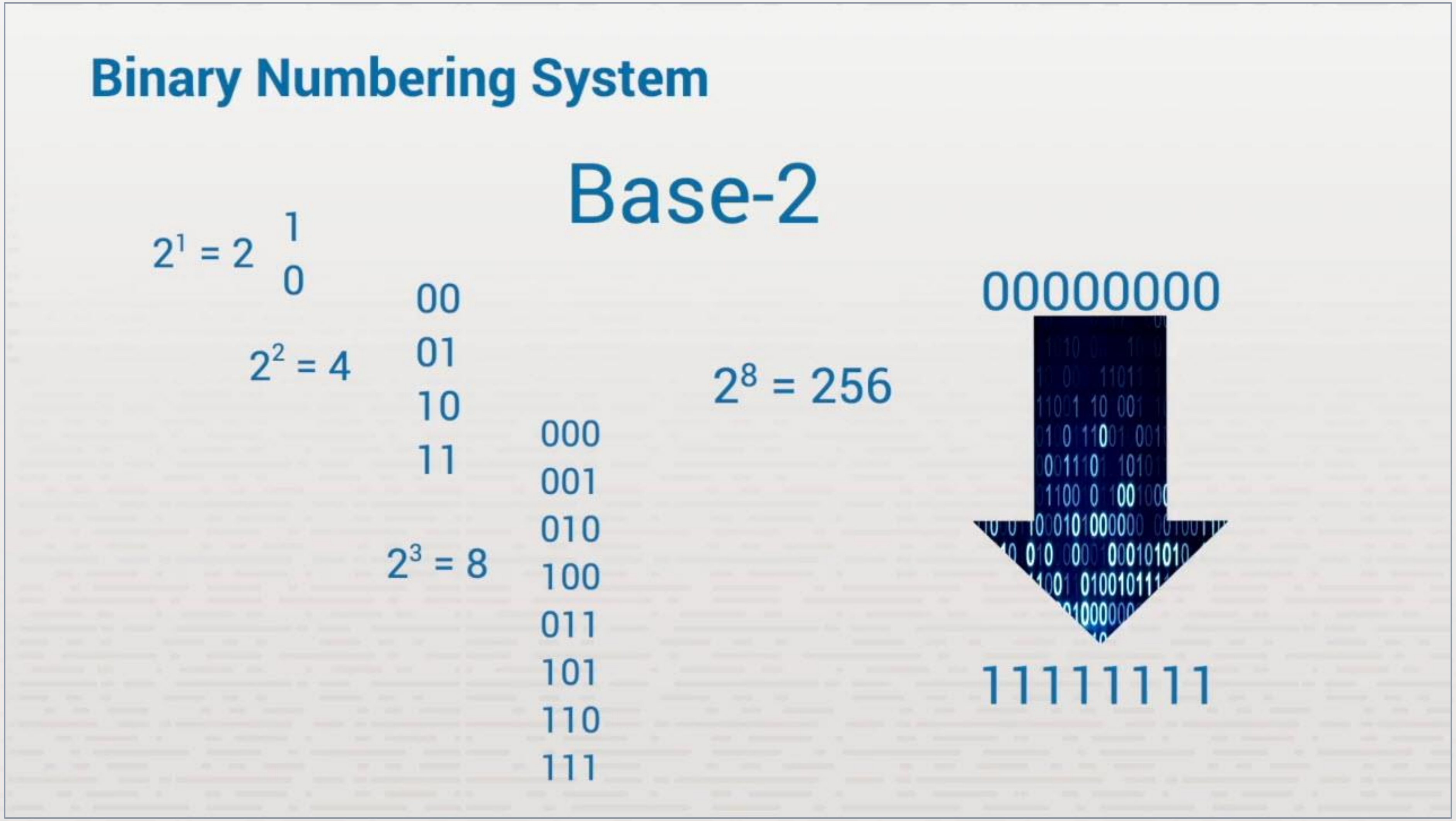
Numbering Systems



Binary Numbering

- States are on/off
- Represented by 1s and 0s
- Base-2 system
- 1s and 0s known as bits

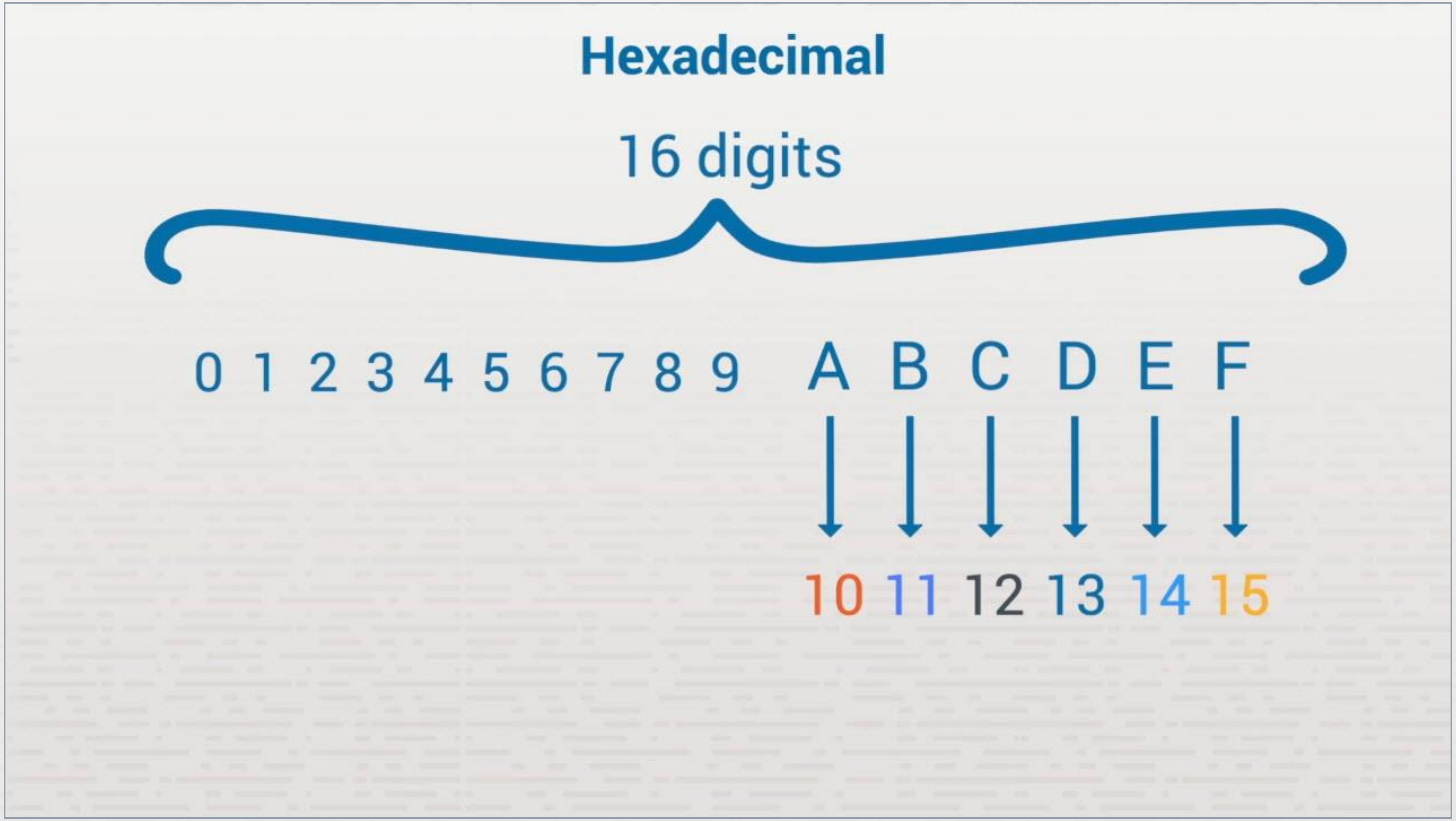
Numbering Systems



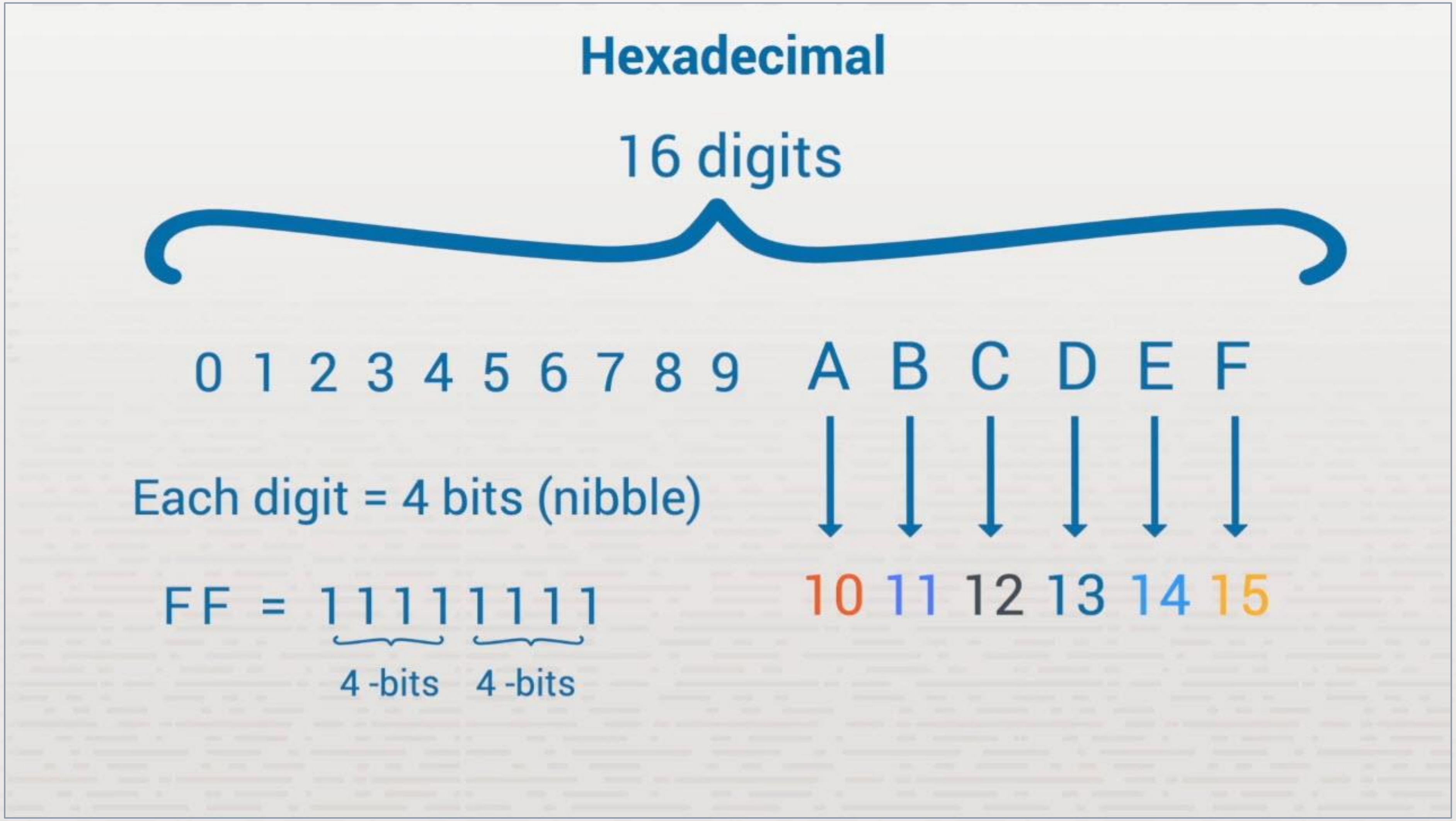
Hexadecimal Numbering

- Hex = 6
- Decim = 10
- A base-16 number system

Numbering Systems



Numbering Systems



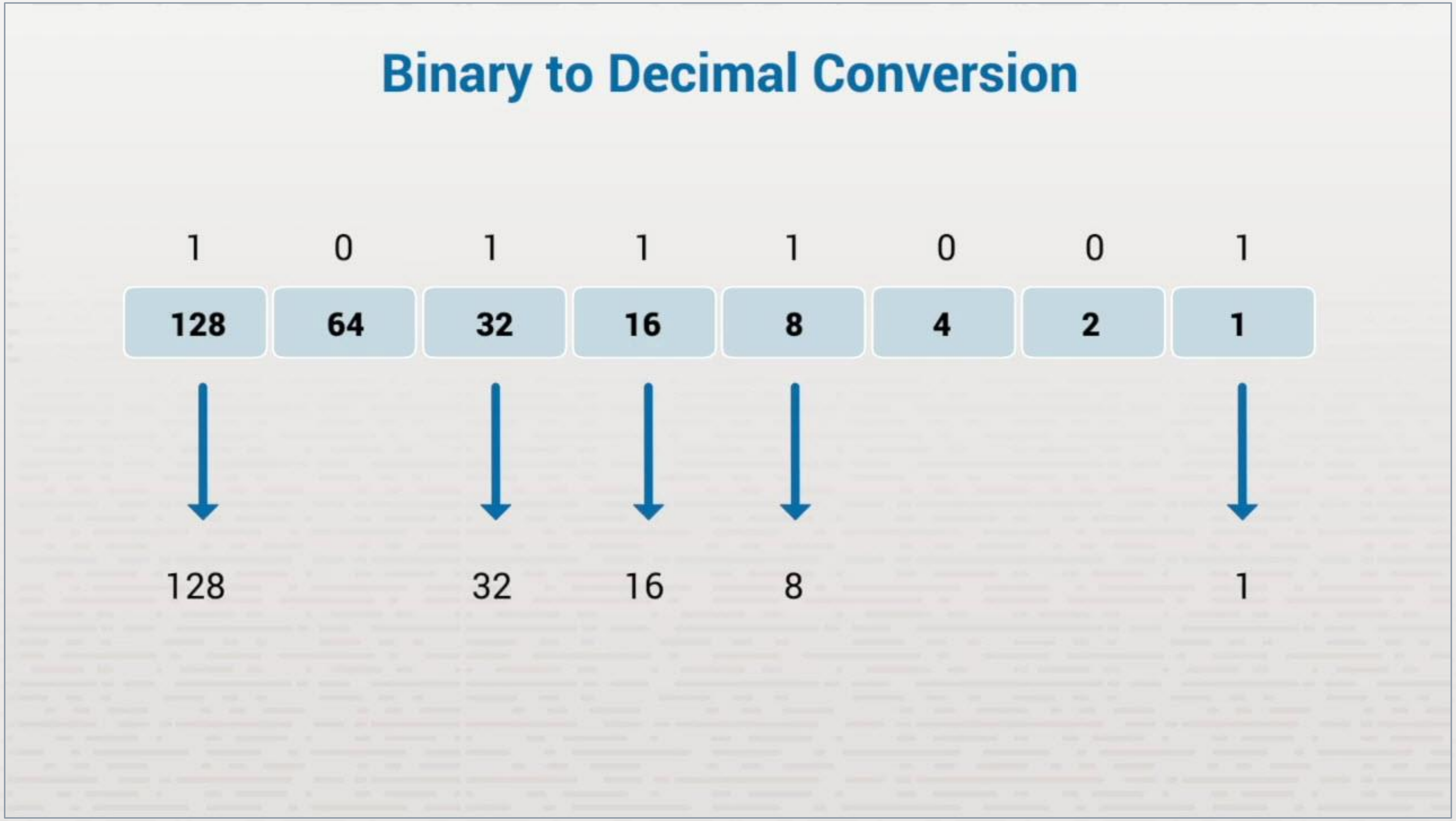
Numbering Systems

Binary to Decimal Conversion

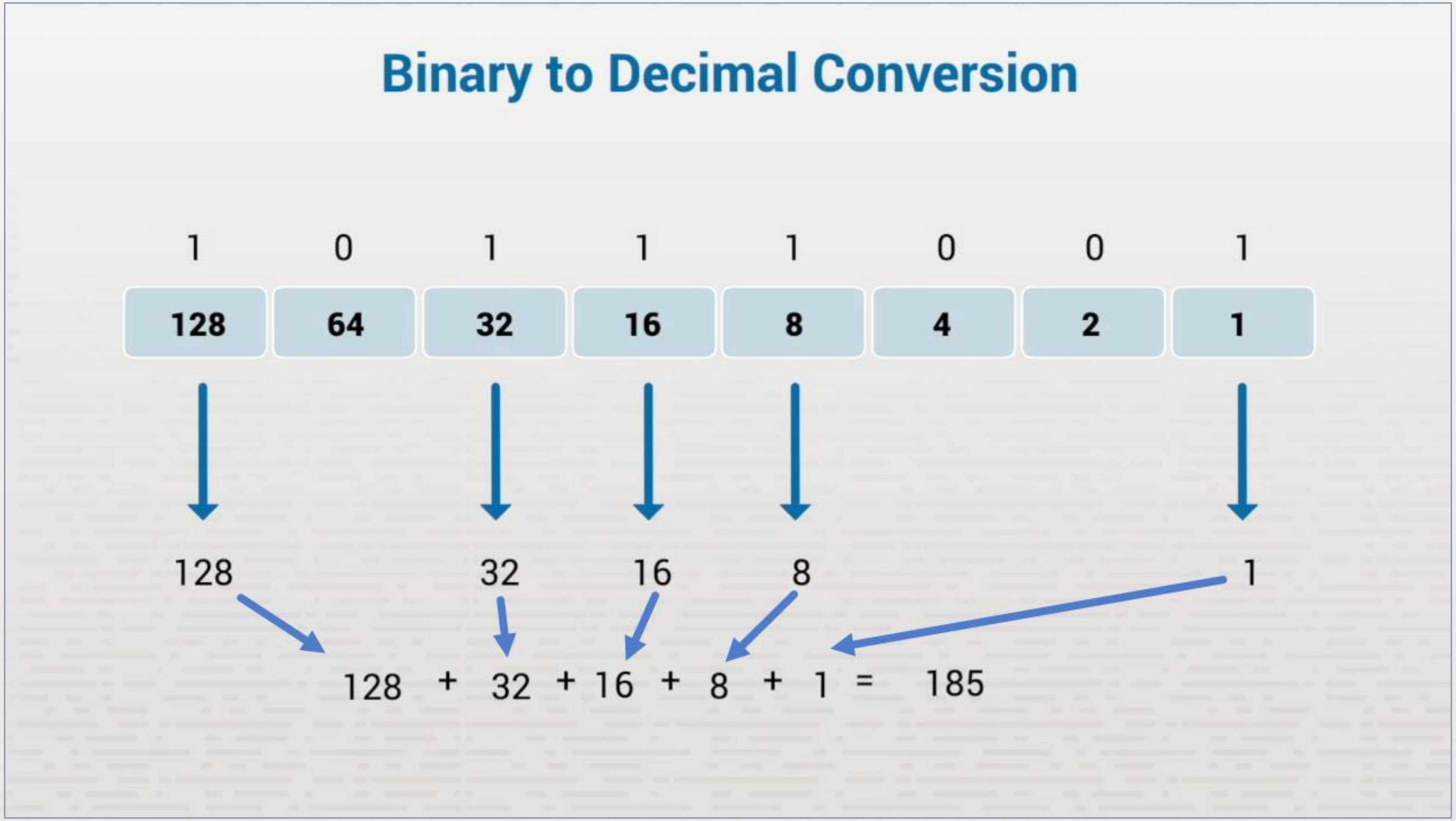
$2^0 = 1$	Anything to the 0 power always equals 1
$2^1 = 2$	$2 \times 1 = 2$
$2^2 = 4$	$2 \times 2 = 4$
$2^3 = 8$	$2 \times 2 \times 2 = 8$
$2^4 = 16$	$2 \times 2 \times 2 \times 2 = 16$
$2^5 = 32$	$2 \times 2 \times 2 \times 2 \times 2 = 32$
$2^5 = 64$	$2 \times 2 \times 2 \times 2 \times 2 \times 2 = 64$
$2^6 = 128$	$2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 128$

128	64	32	16	8	4	2	1

Numbering Systems



Numbering Systems



TestOut

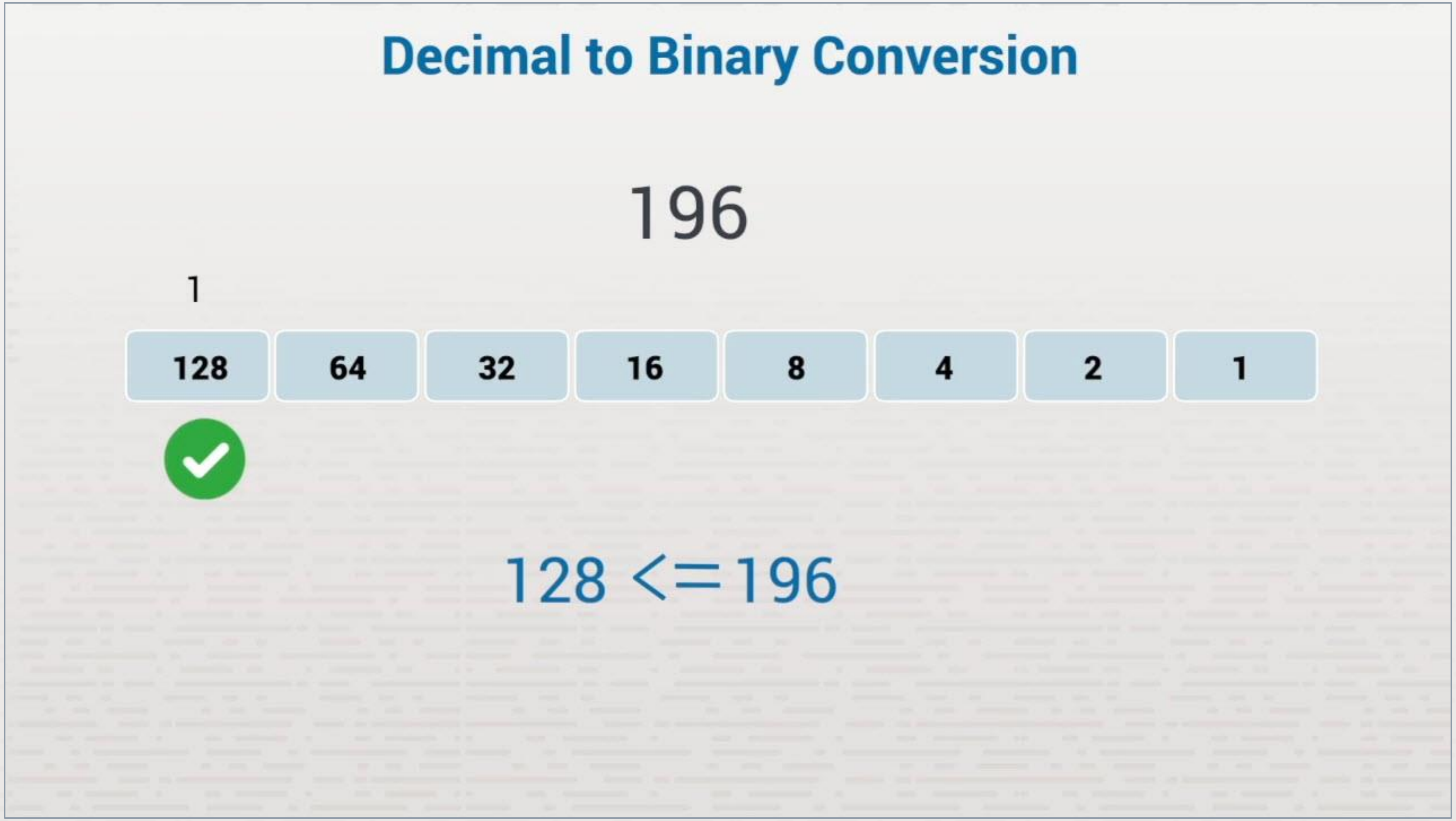
Numbering Systems

Decimal to Binary Conversion

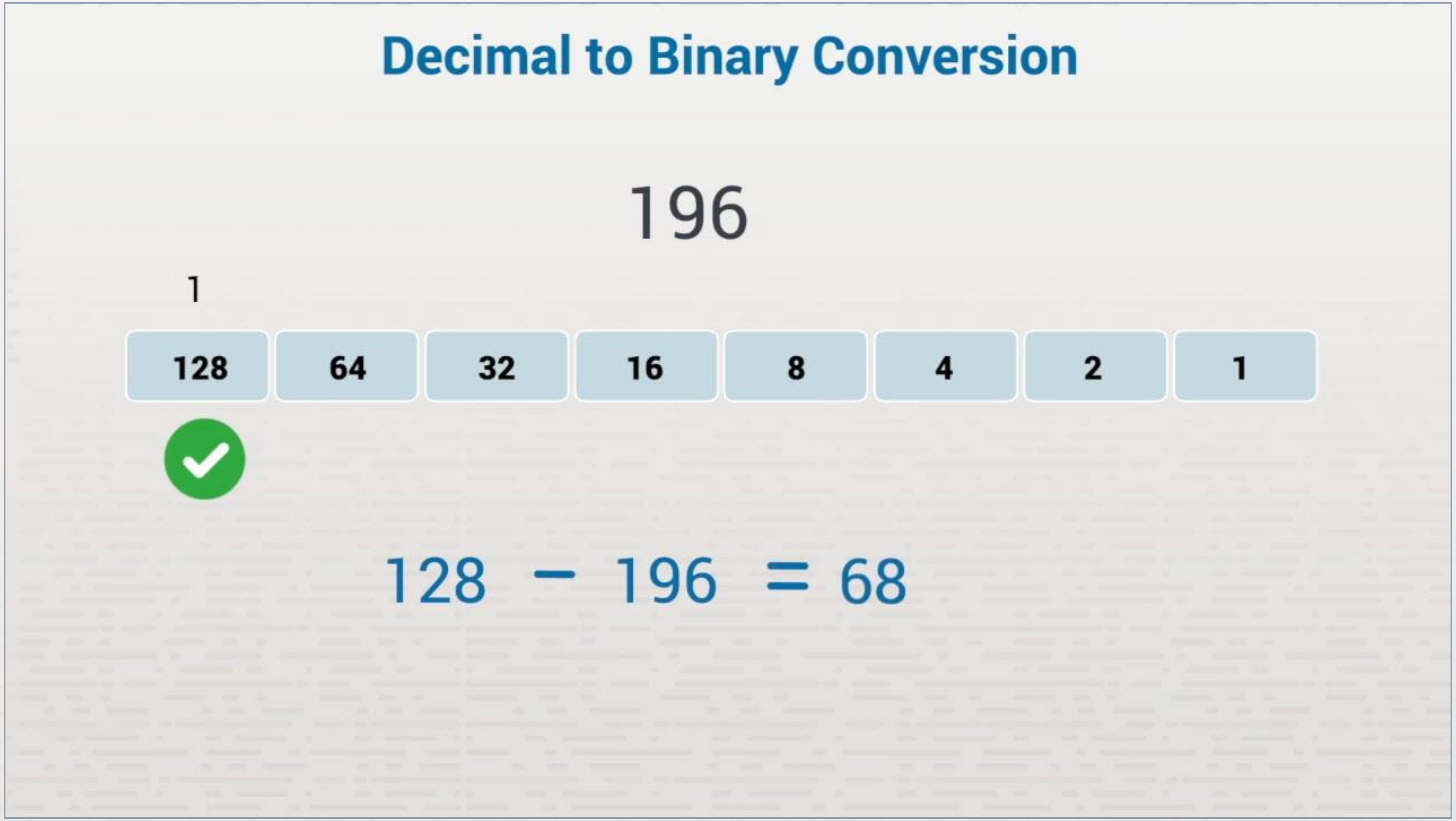
196

128	64	32	16	8	4	2	1

Numbering Systems



Numbering Systems



Numbering Systems

Decimal to Binary Conversion

196

1	1						
128	64	32	16	8	4	2	1

$128 - 196 = 68$

$68 <= 64$

Numbering Systems

Decimal to Binary Conversion

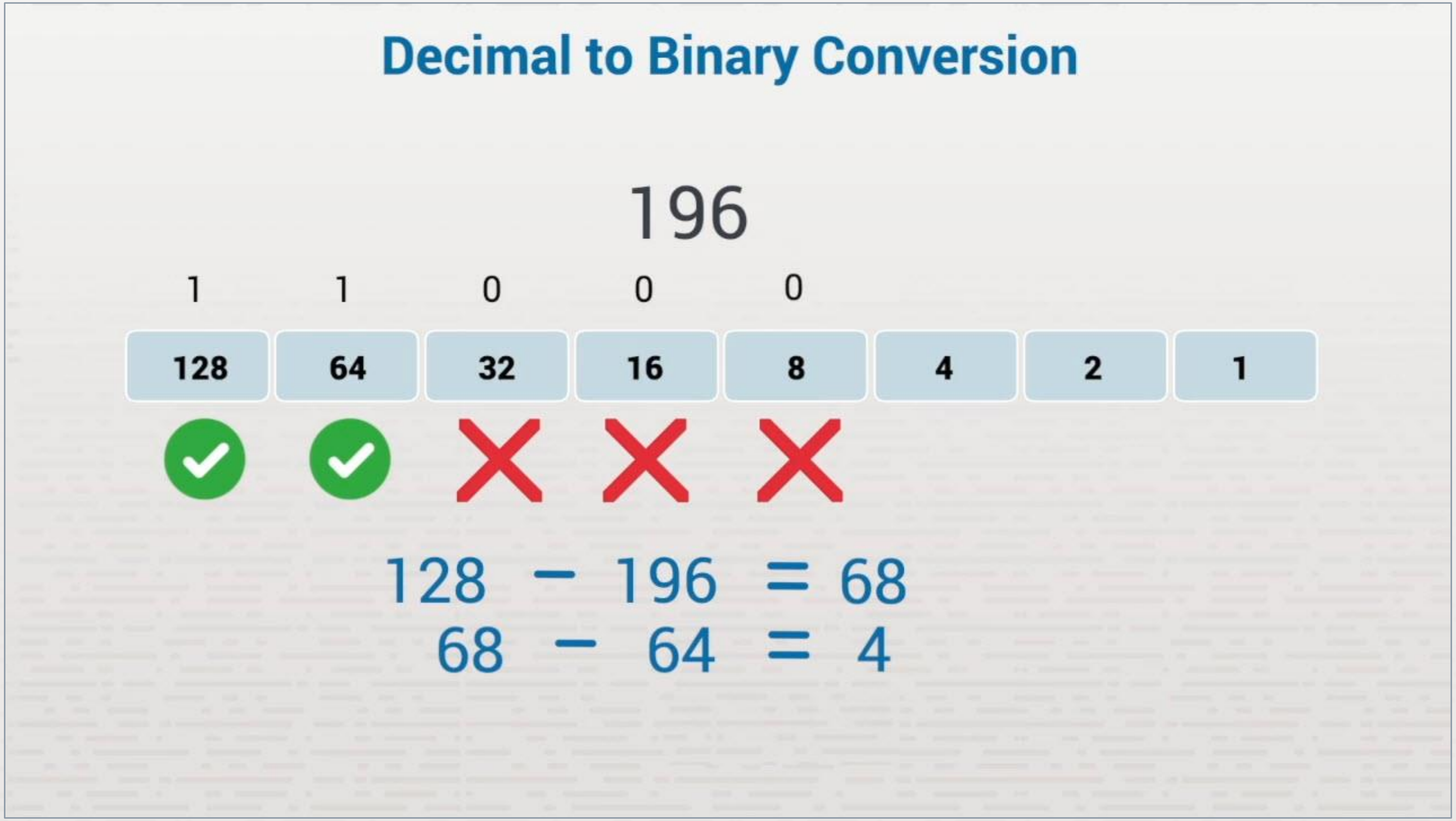
196

1	1	0					
128	64	32	16	8	4	2	1

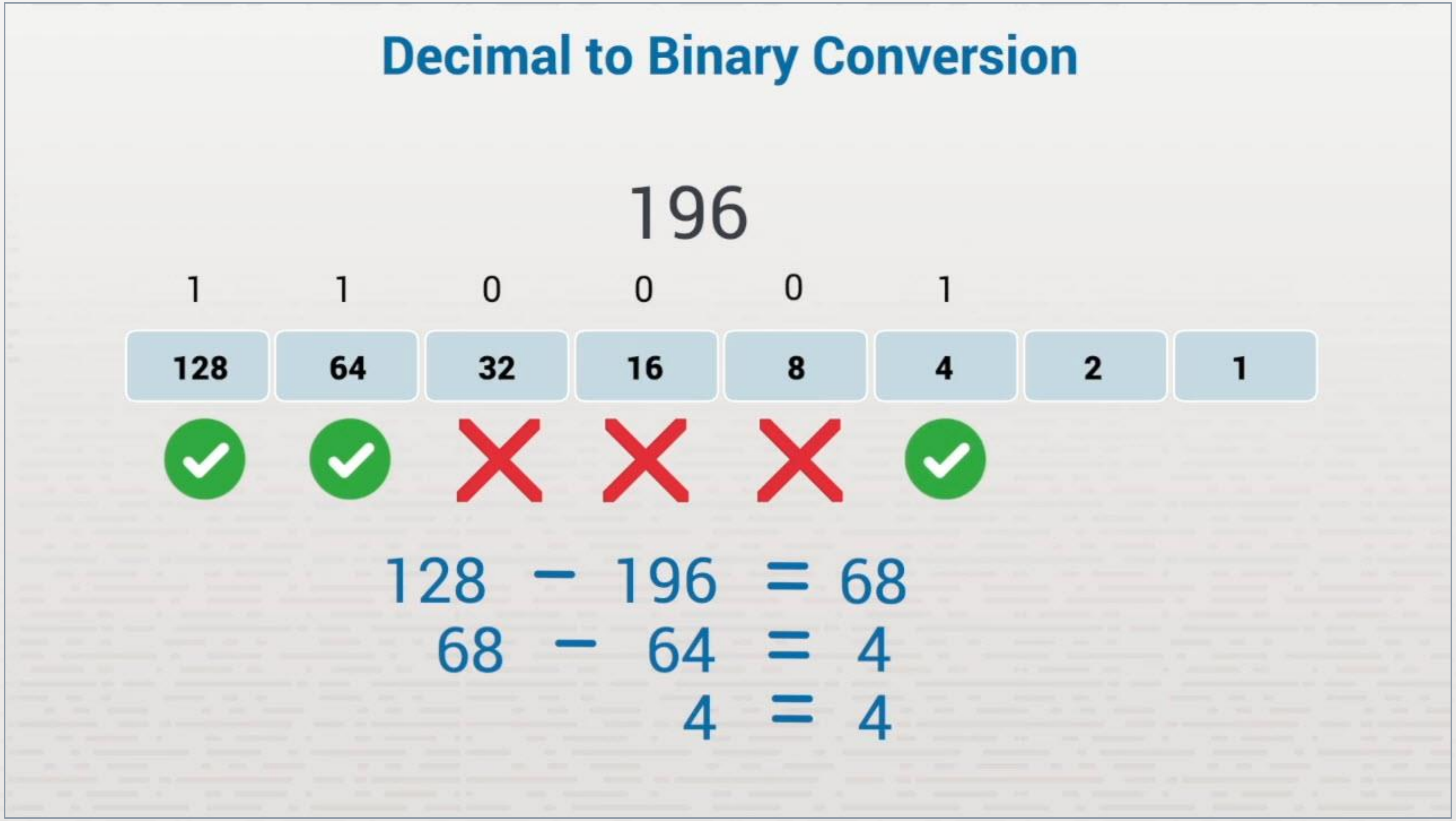
128 − 196 = 68

68 − 64 = 4

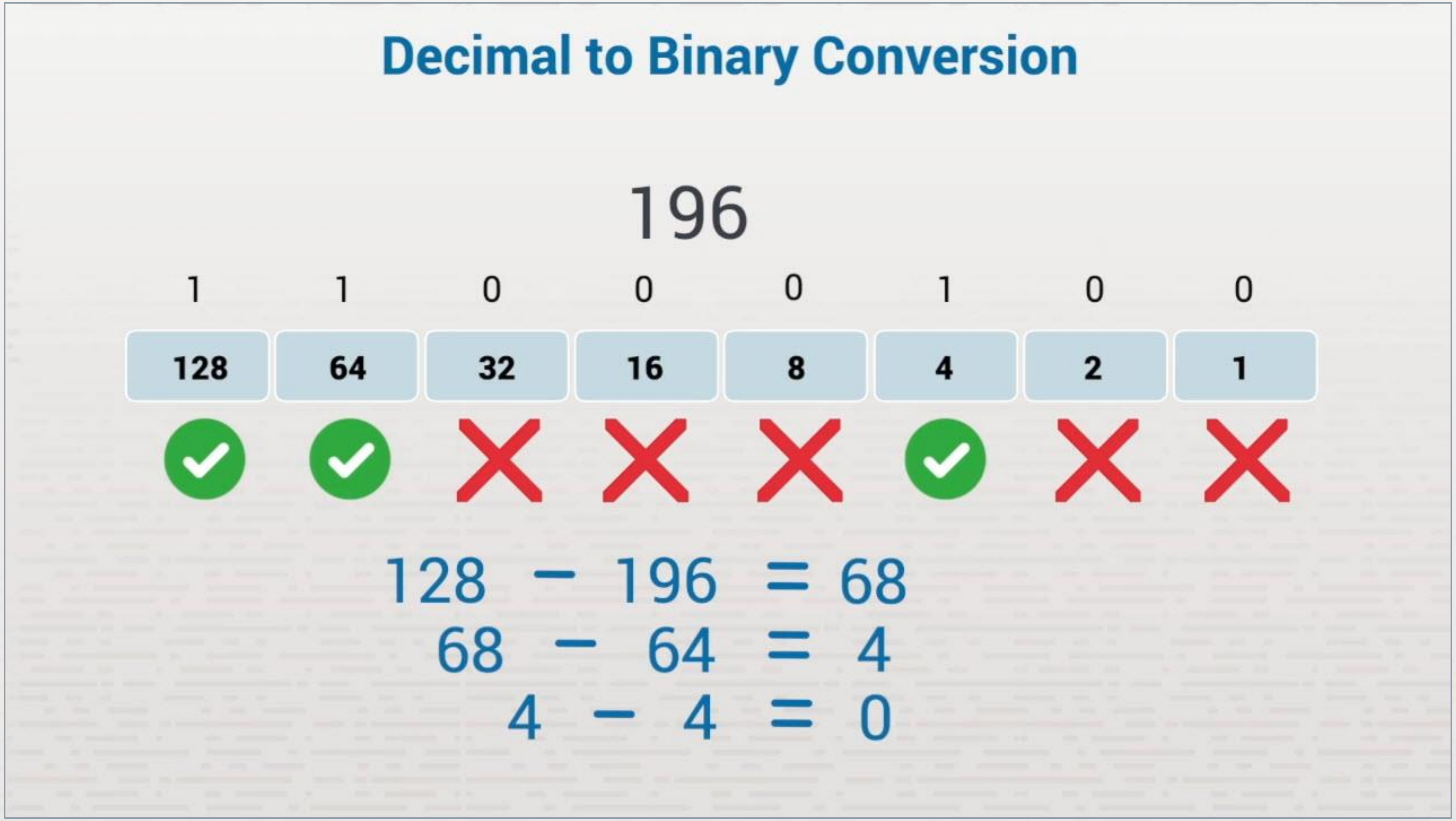
Numbering Systems



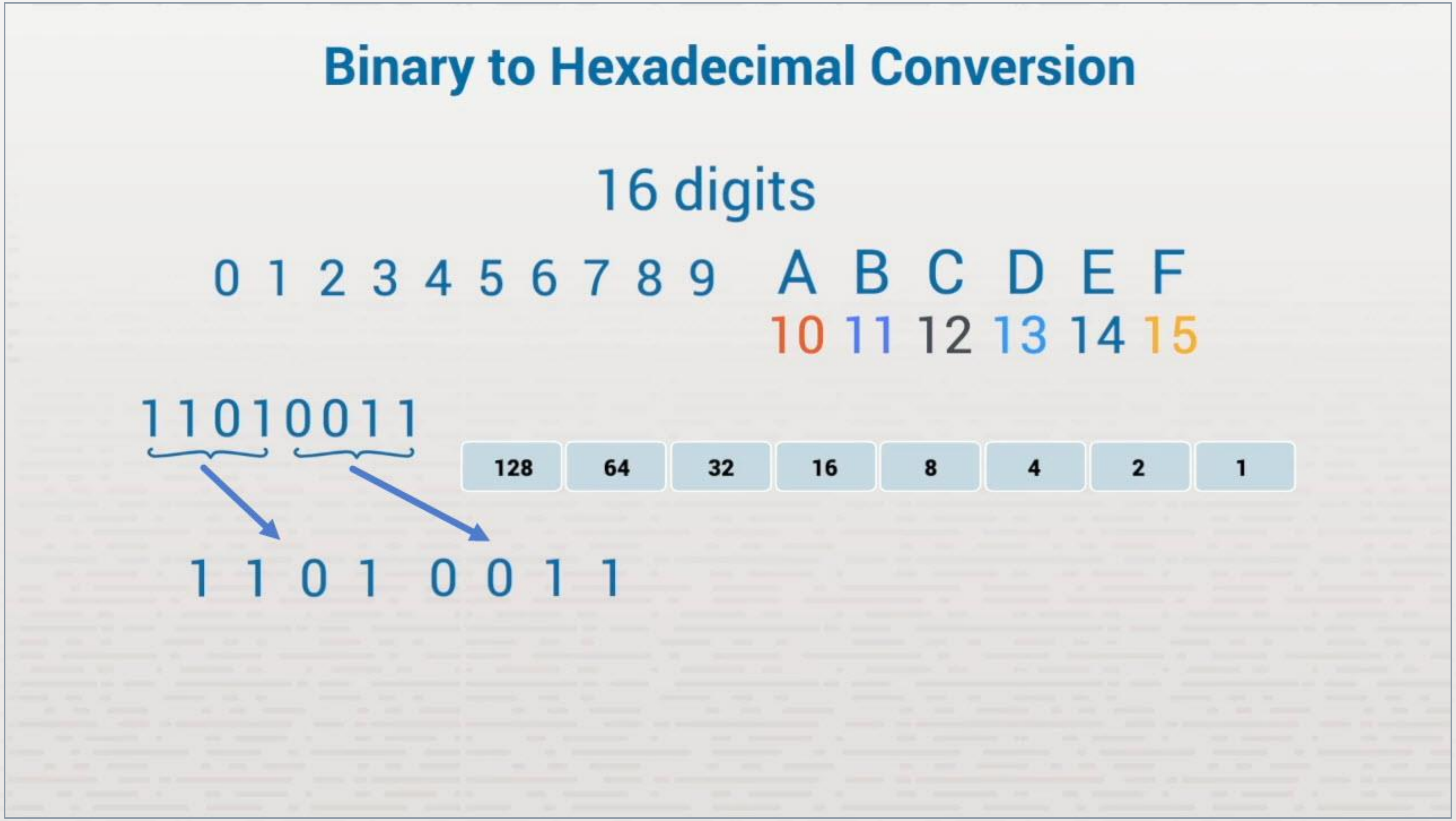
Numbering Systems



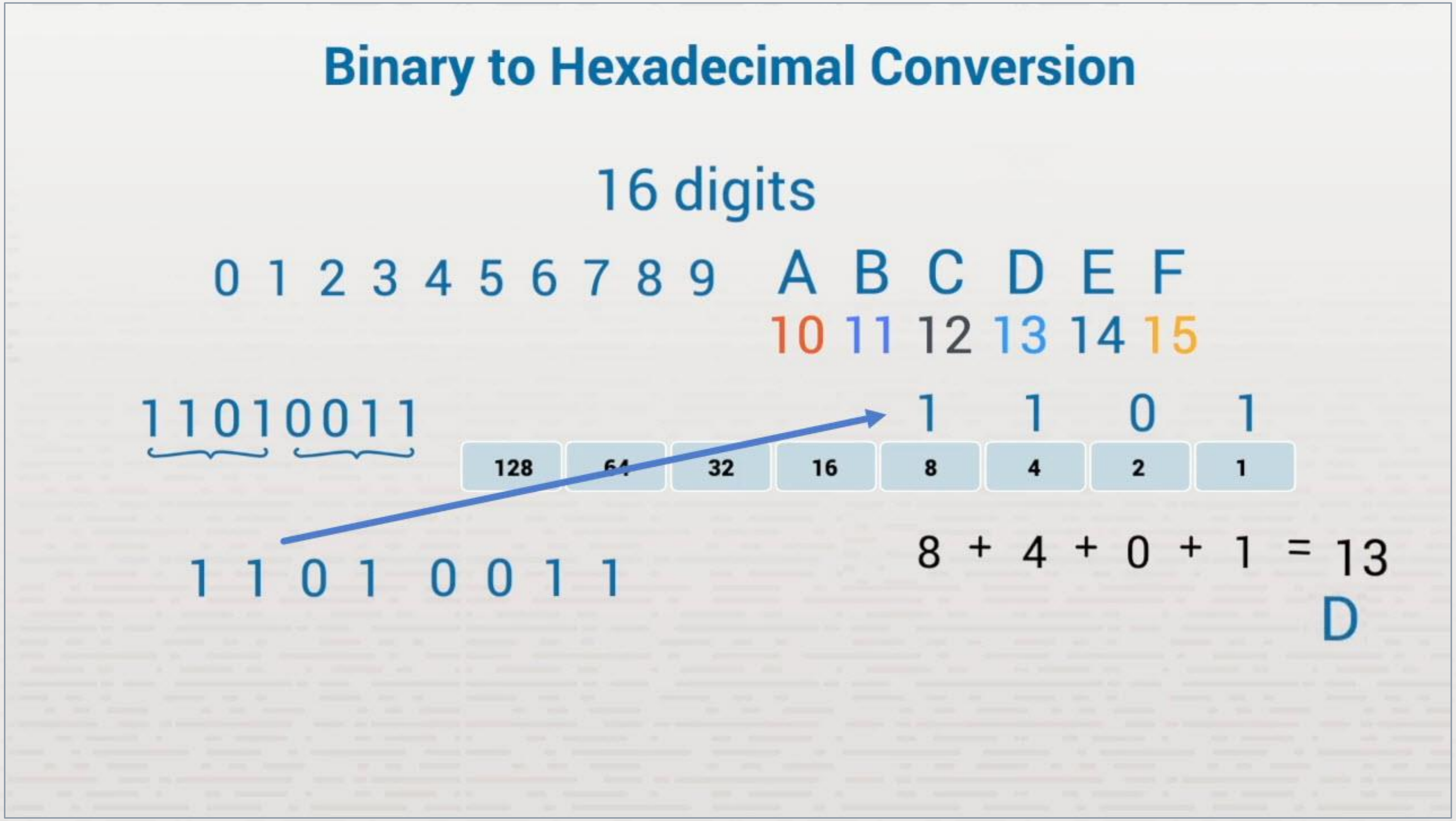
Numbering Systems



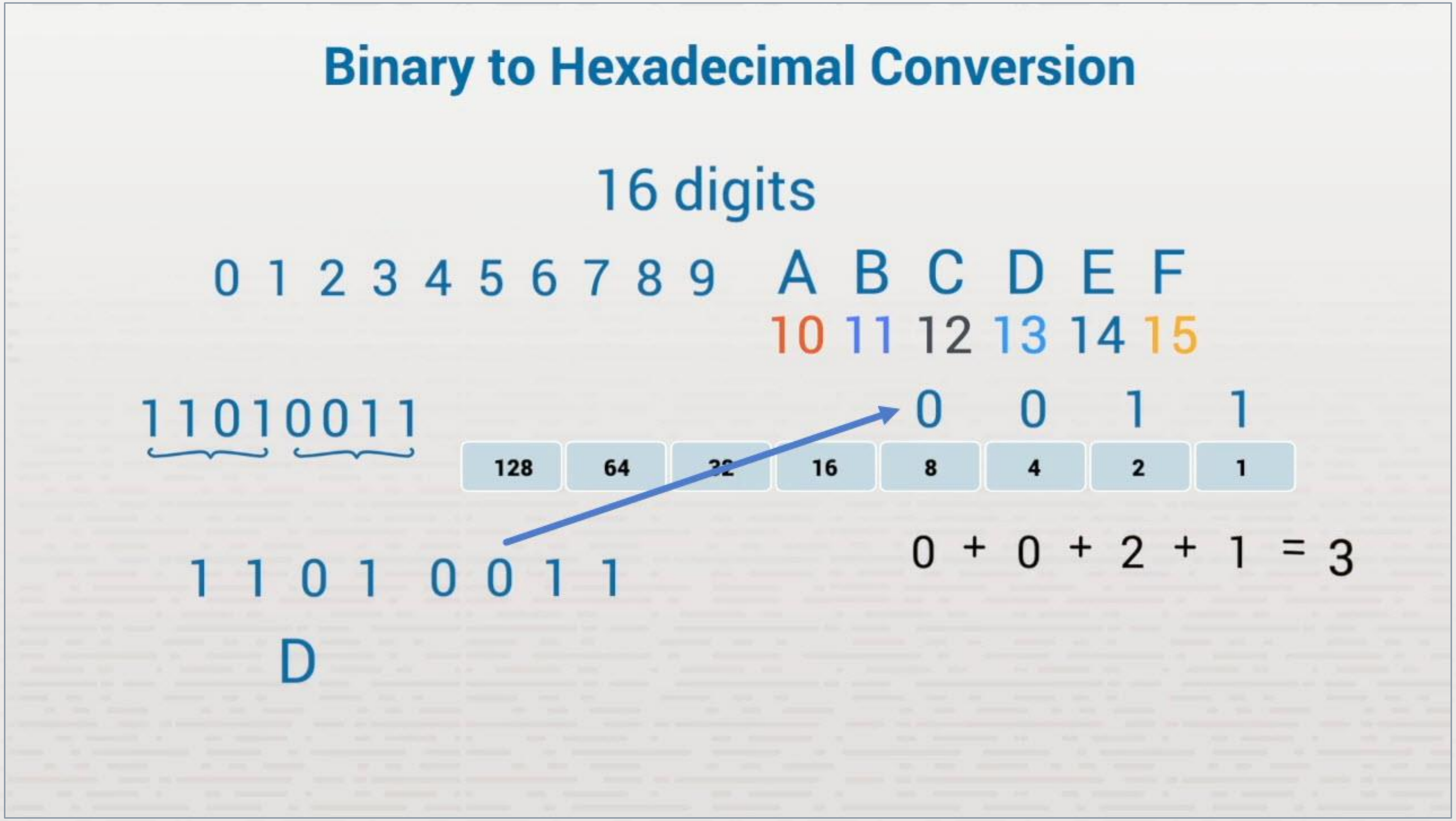
Numbering Systems



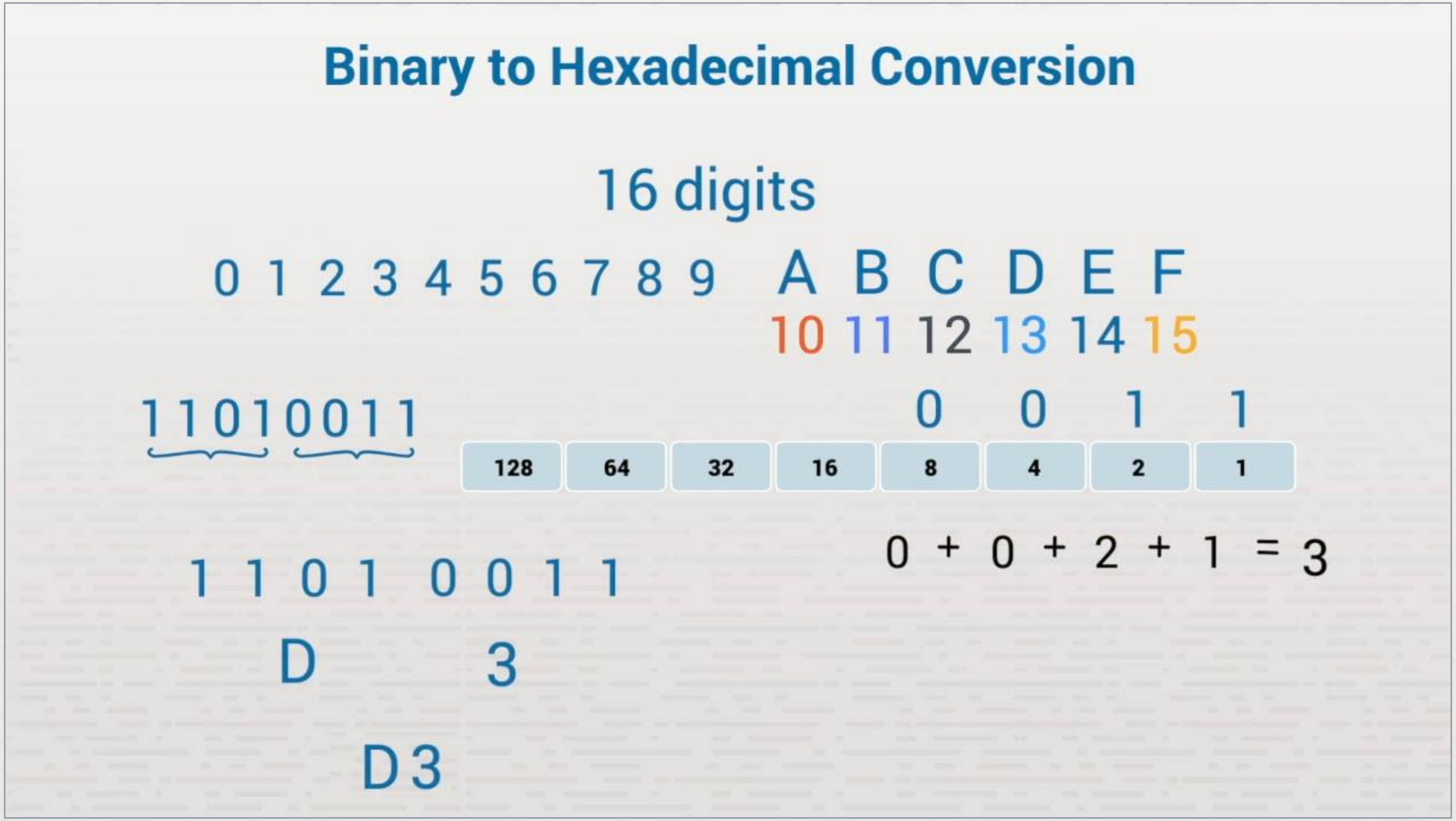
Numbering Systems



Numbering Systems



Numbering Systems



TestOut

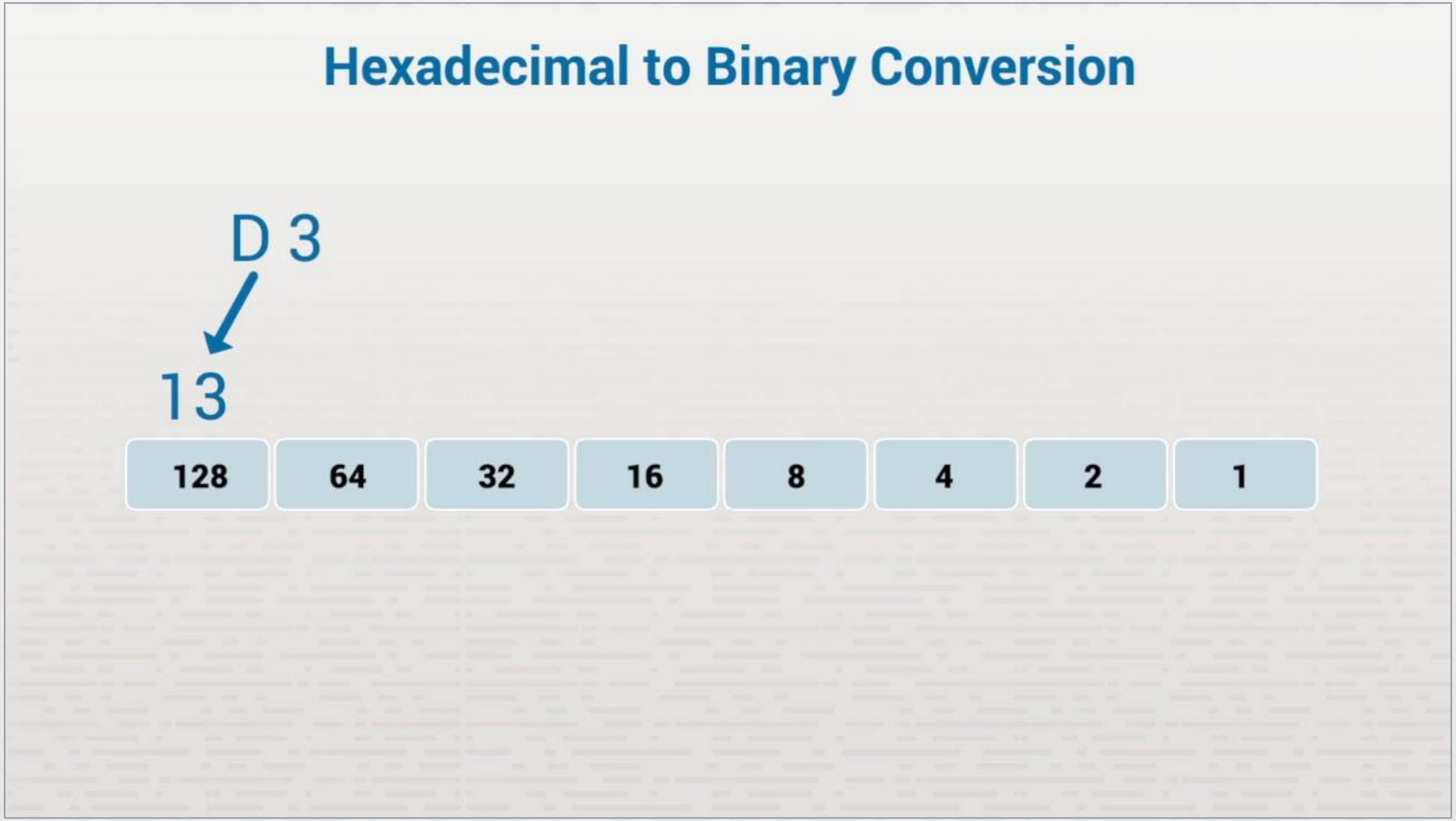
Numbering Systems

Hexadecimal to Binary Conversion

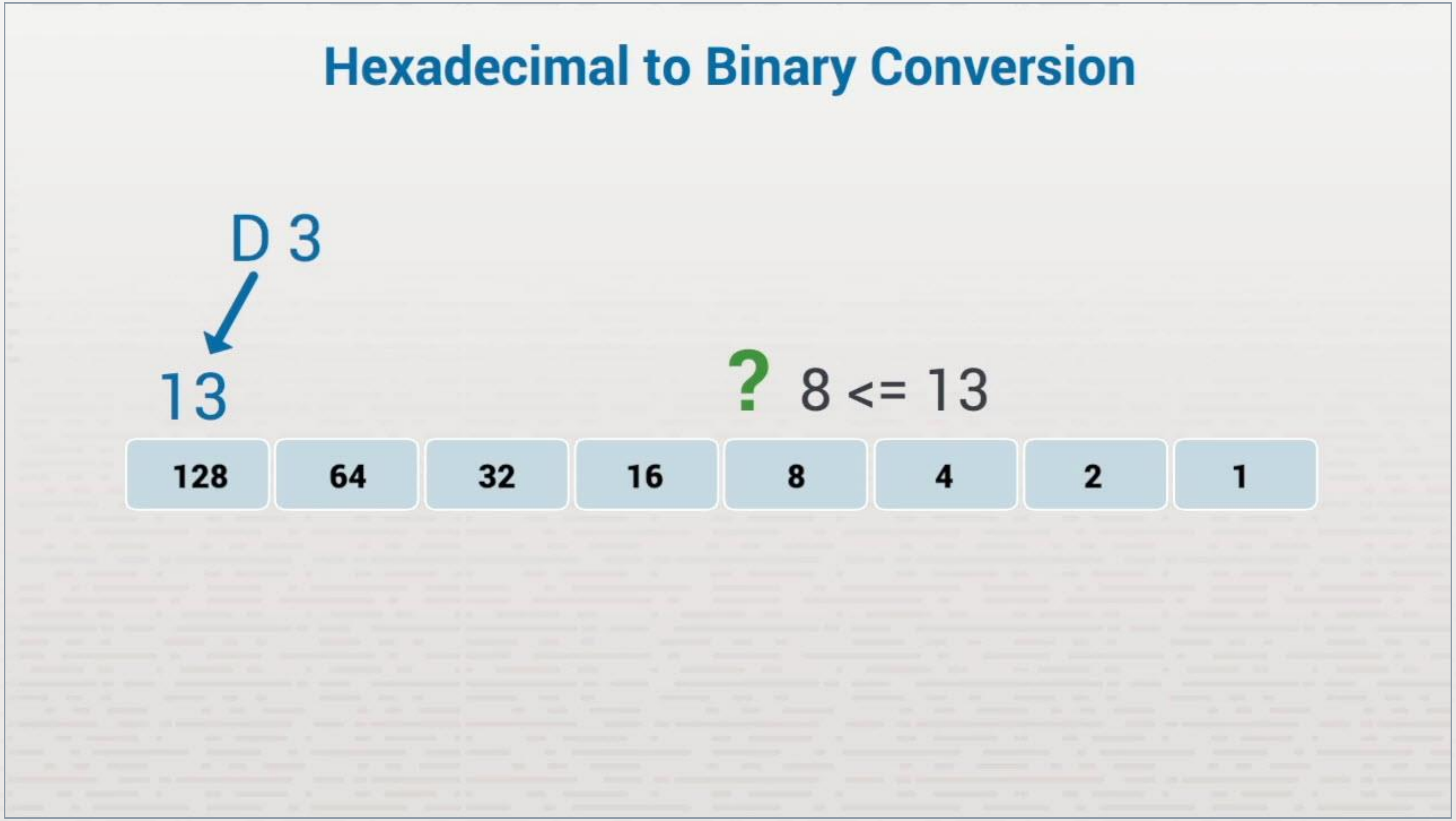
D 3

128	64	32	16	8	4	2	1

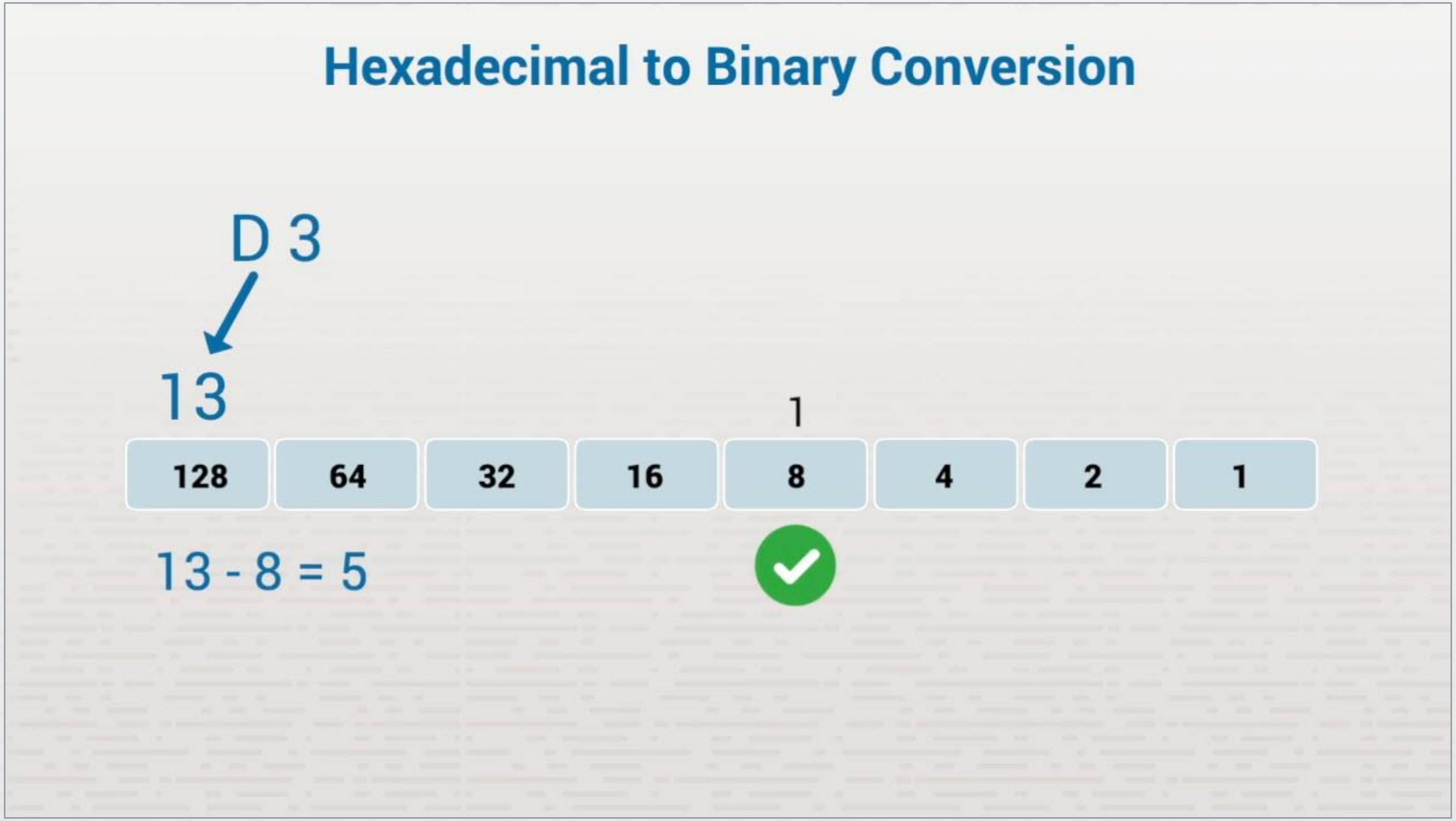
Numbering Systems



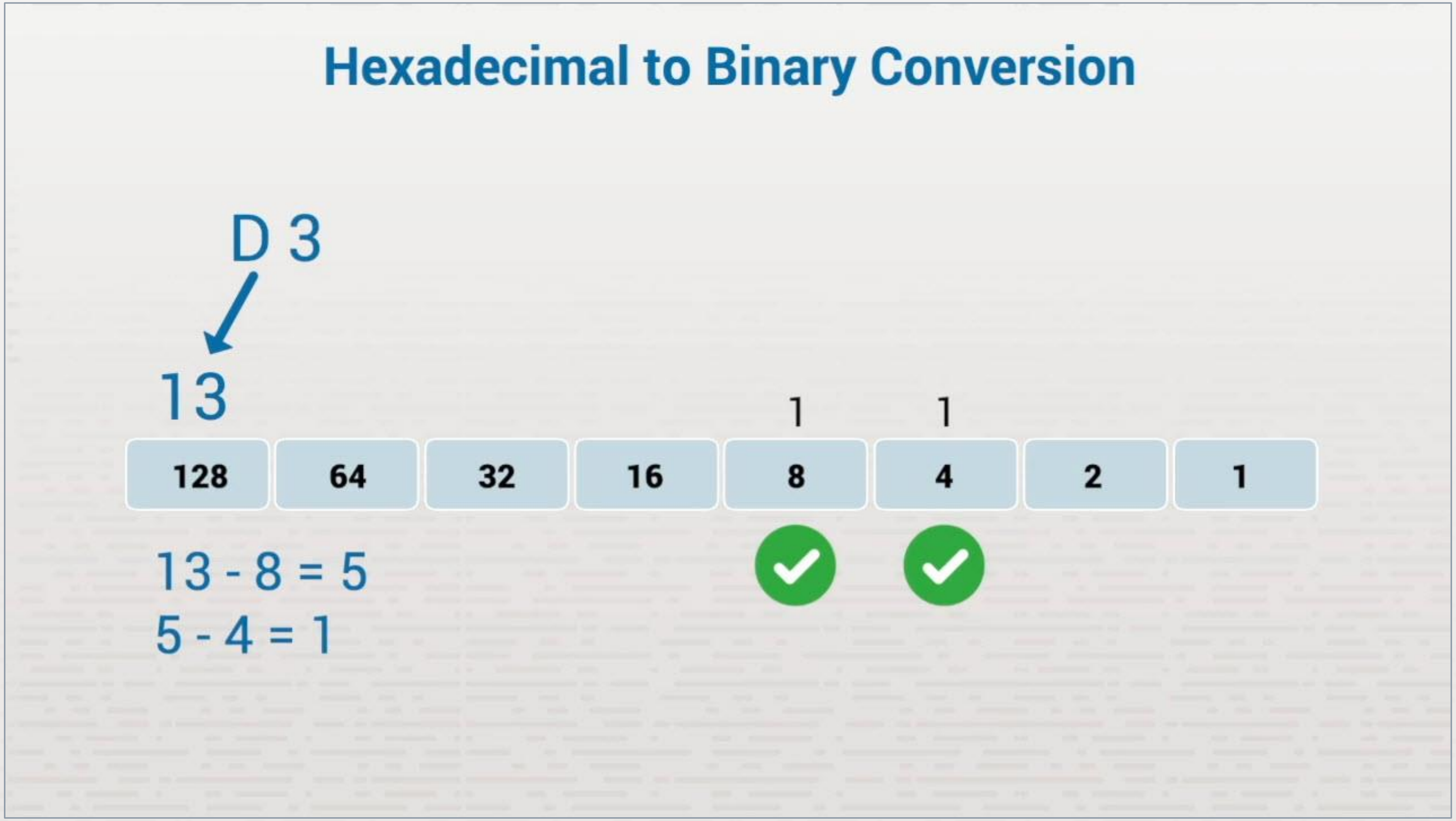
Numbering Systems



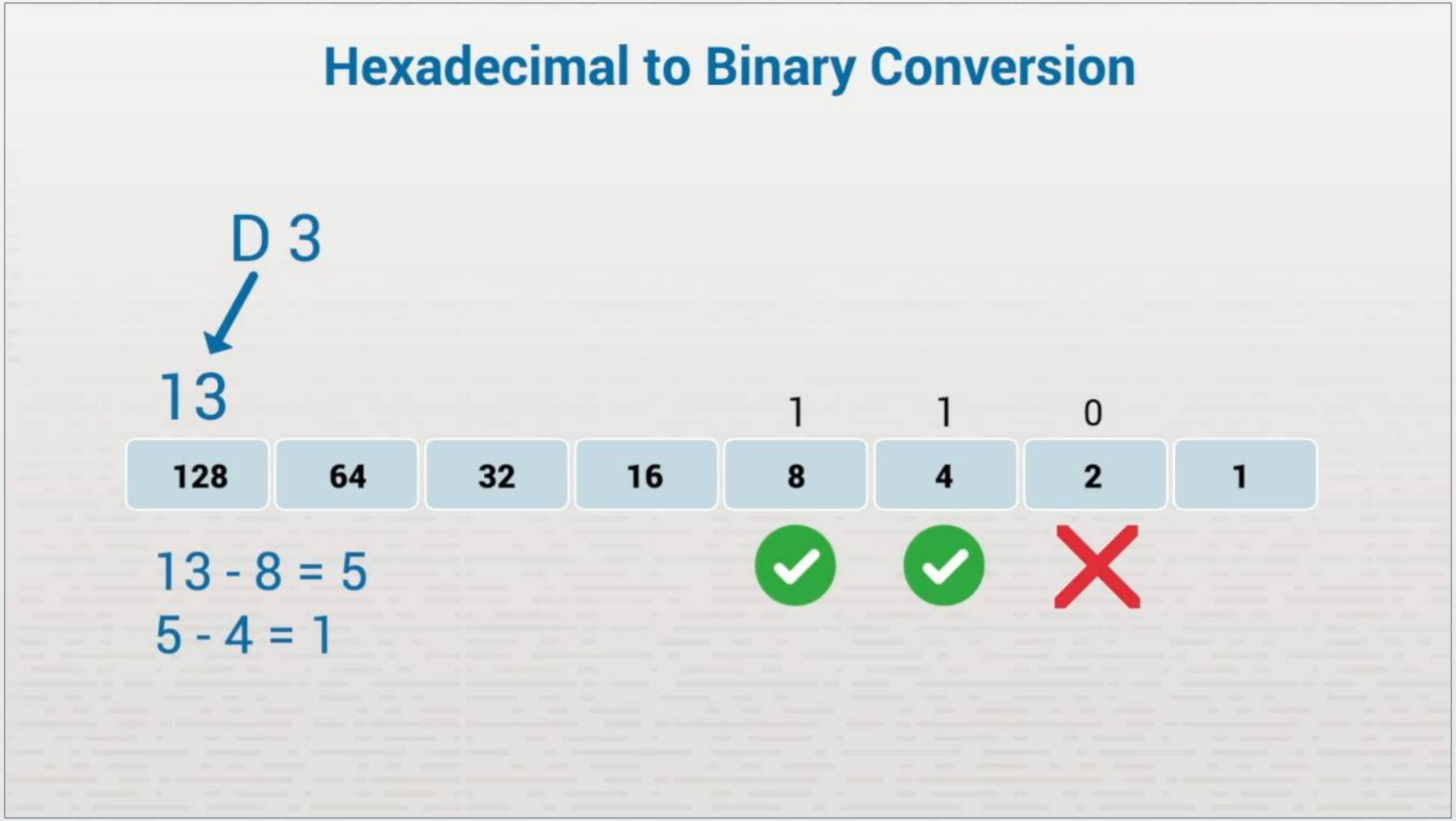
Numbering Systems



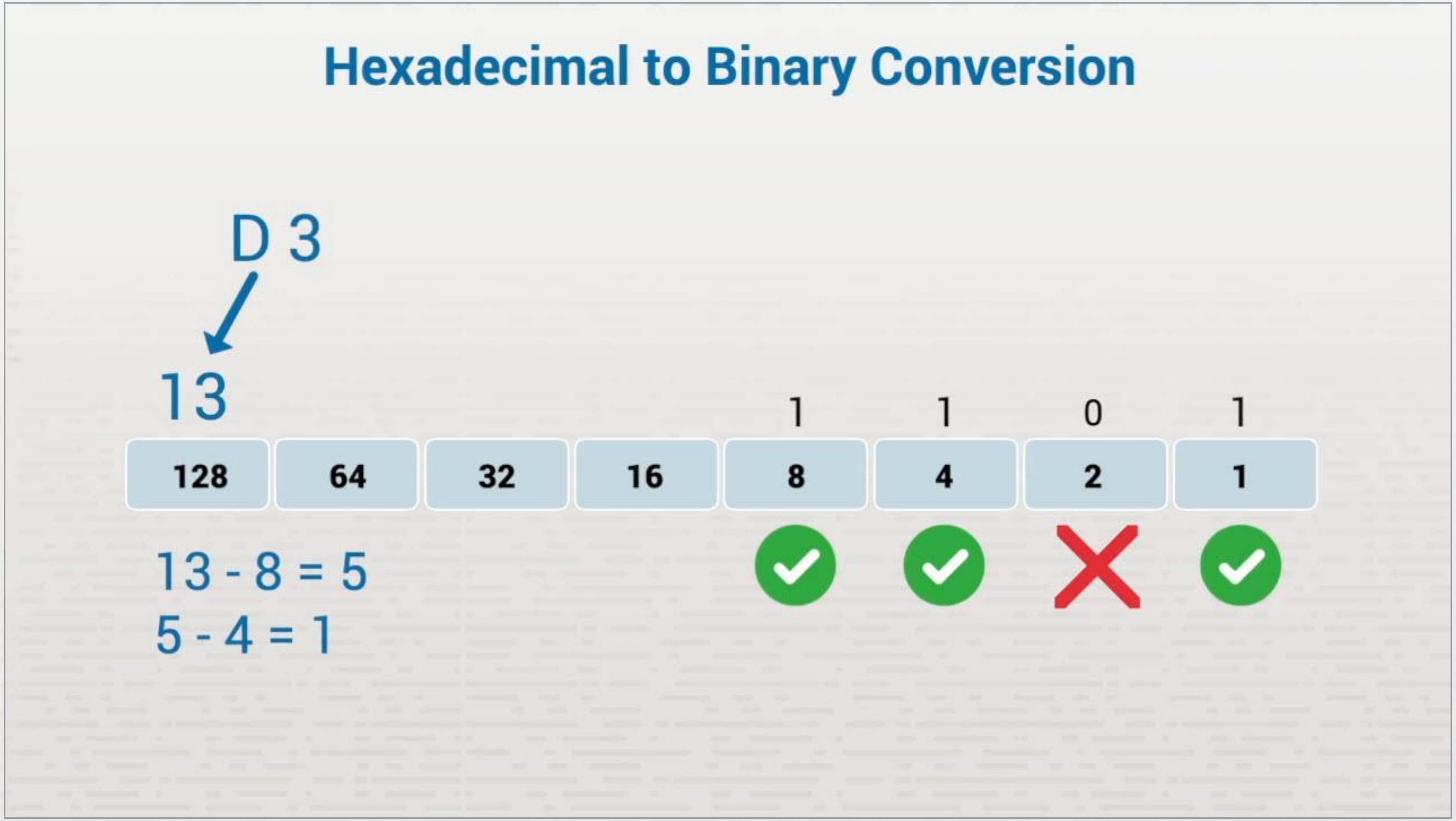
Numbering Systems



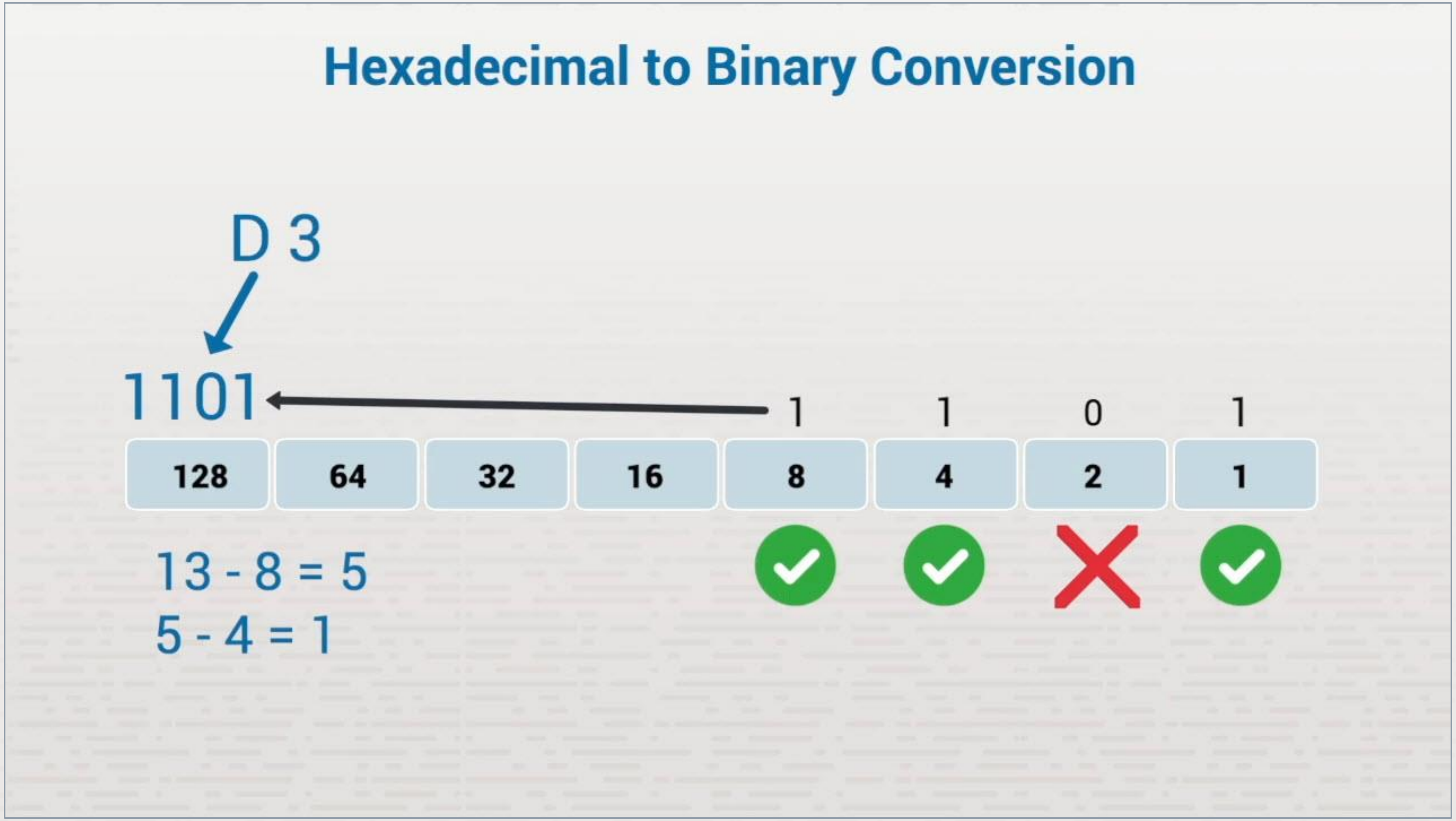
Numbering Systems



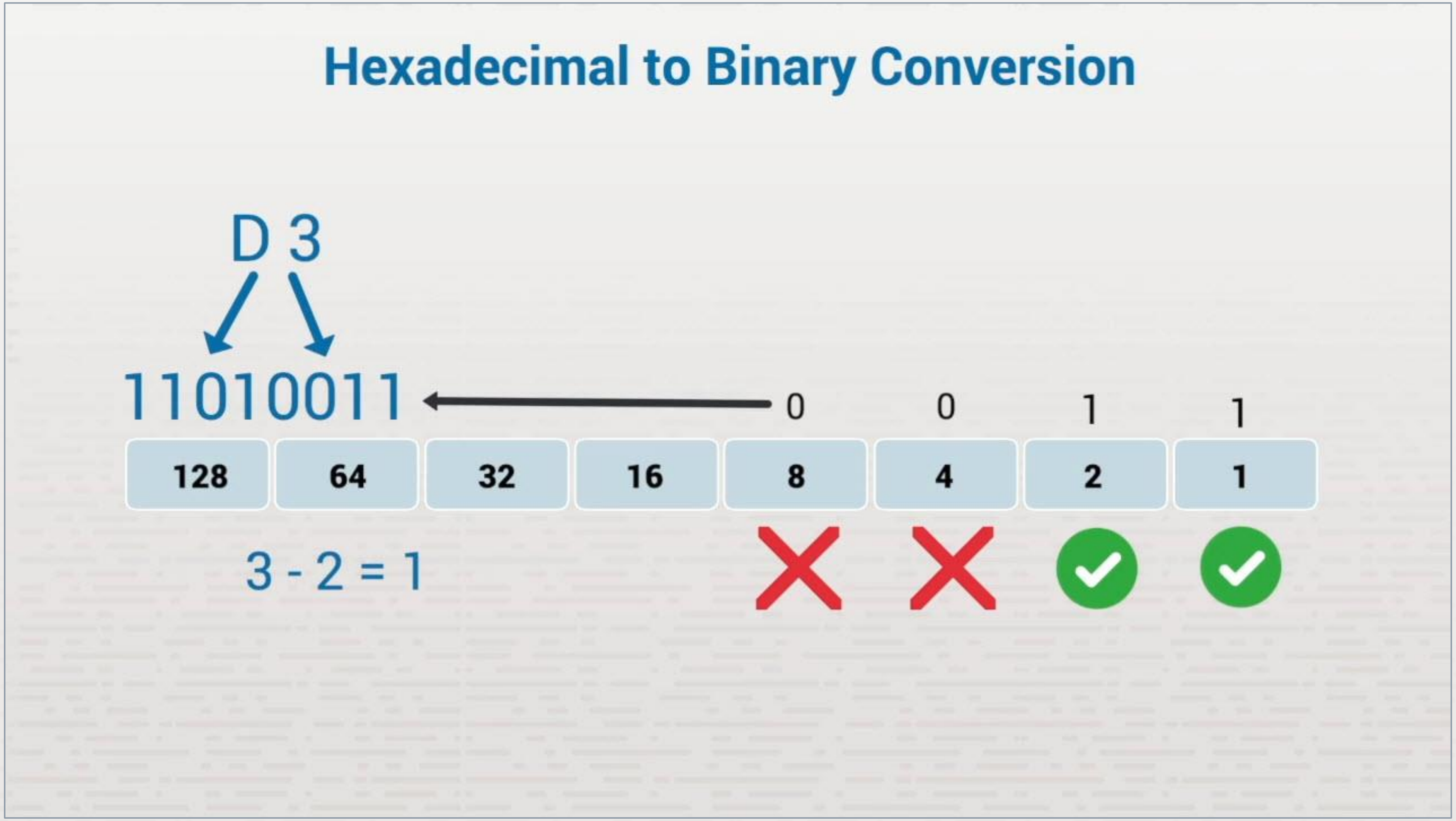
Numbering Systems



Numbering Systems



Numbering Systems



Summary

- Decimal
- Binary
- Hexadecimal
- Conversion

IP Addresses

IPv4 Addresses

- Address format
- Subnet masks
- Address classes
- Special IPv4 addresses

IP Addresses

IP Address Format

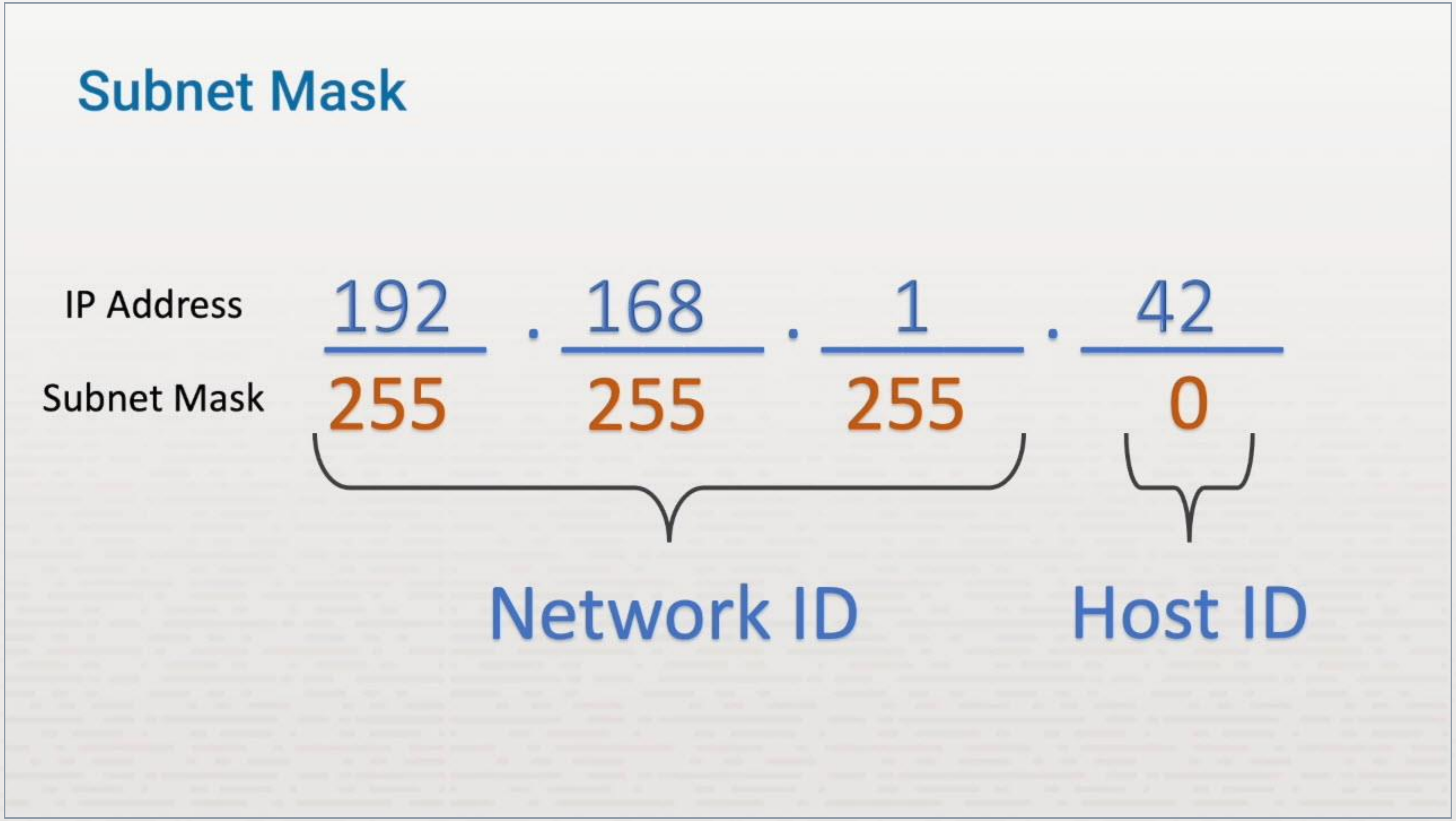
192 . 168 . 5 . 42

Octets

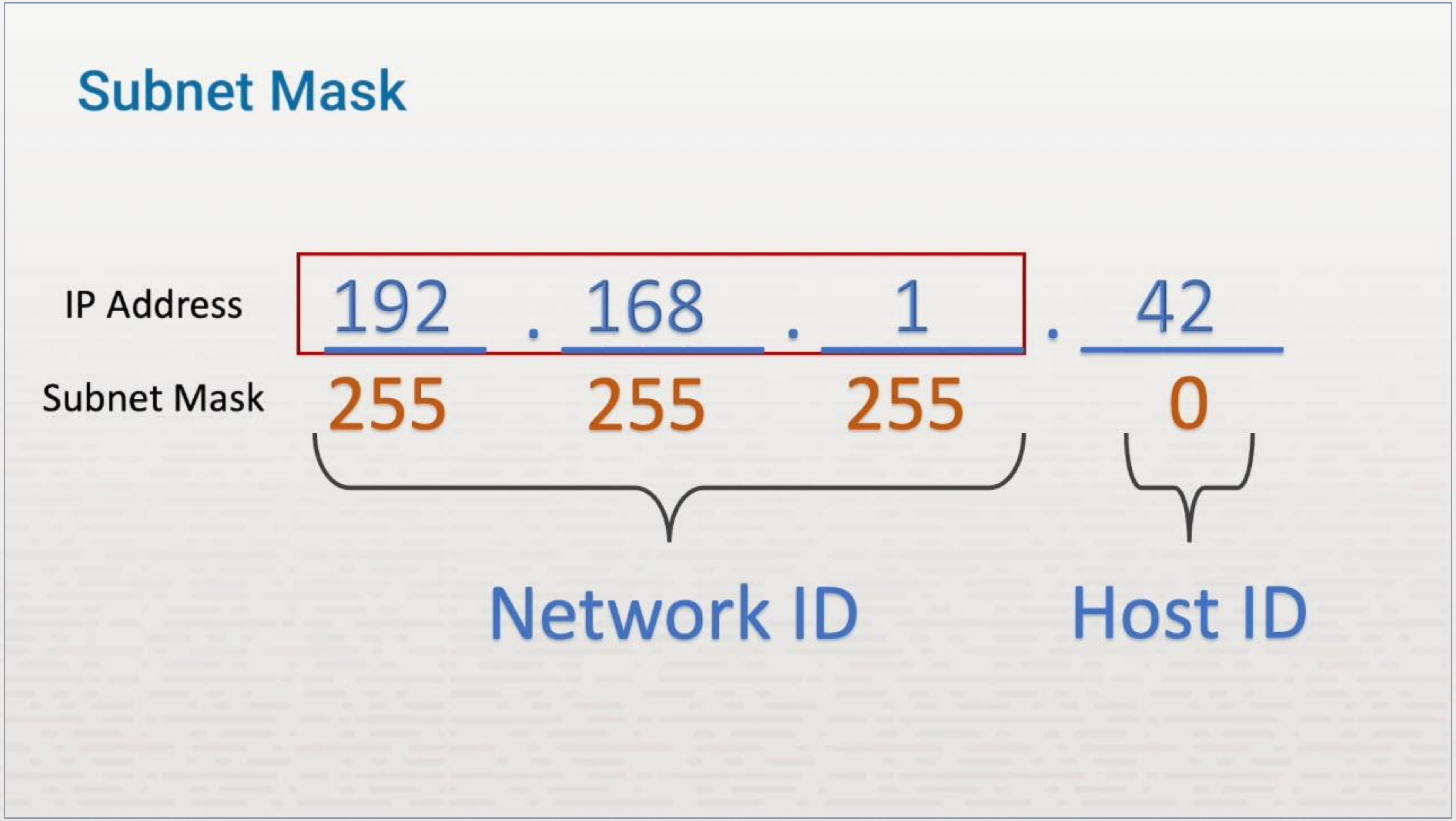
10101000

$2^7 = 256$

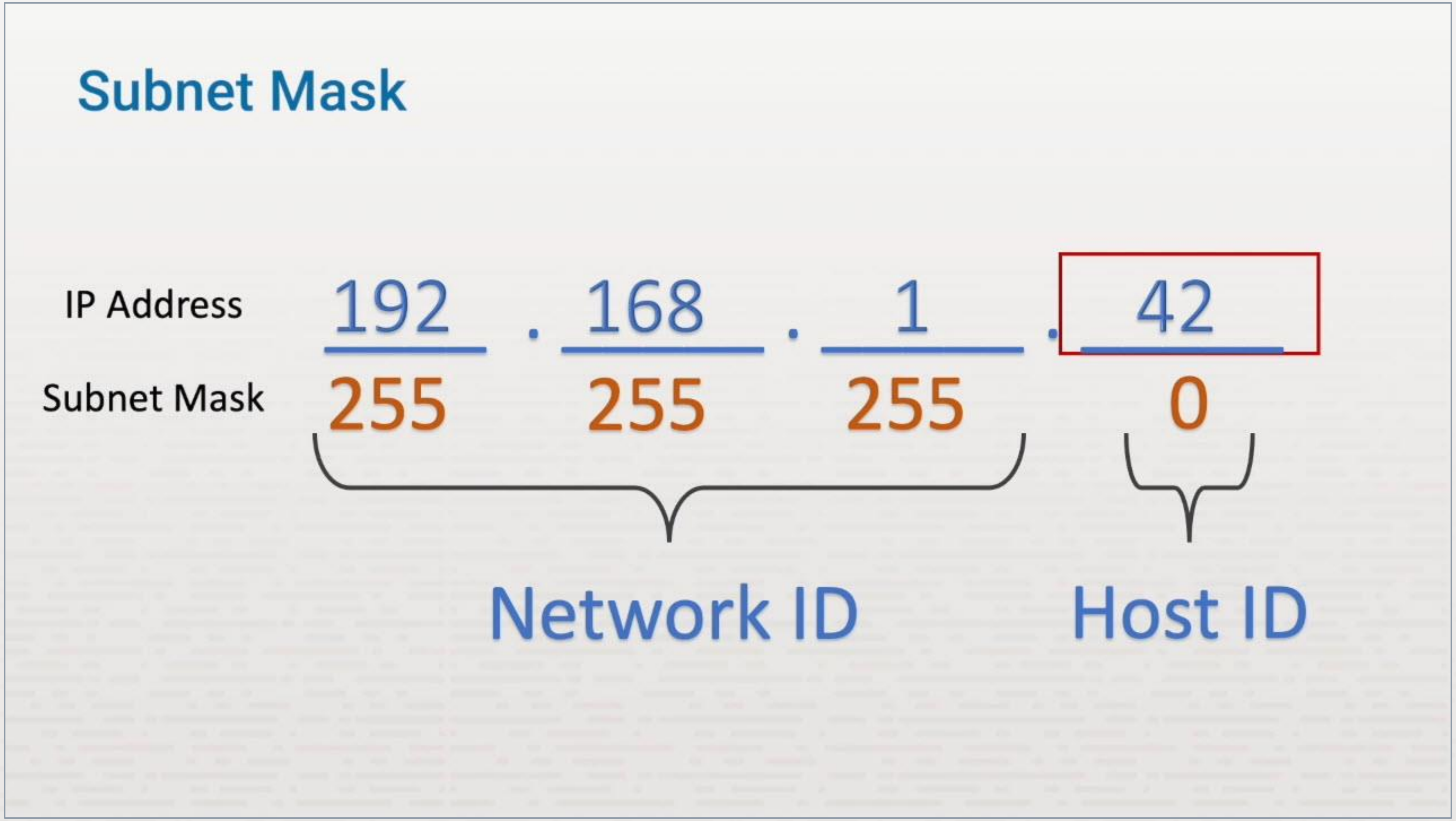
IP Addresses



IP Addresses



IP Addresses

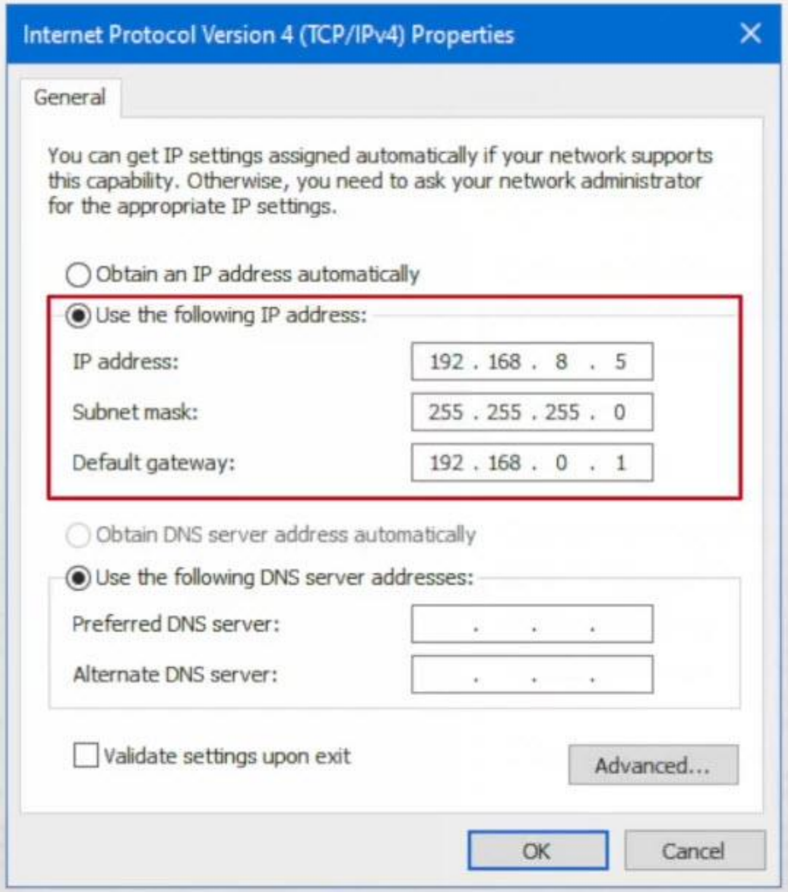


IP Addresses

Subnet Mask

	192	168	8	5
IP Address	192	168	1	42
Subnet Mask	255	255	0	0
	Network ID		Host ID	

IP Addresses



IP Addresses

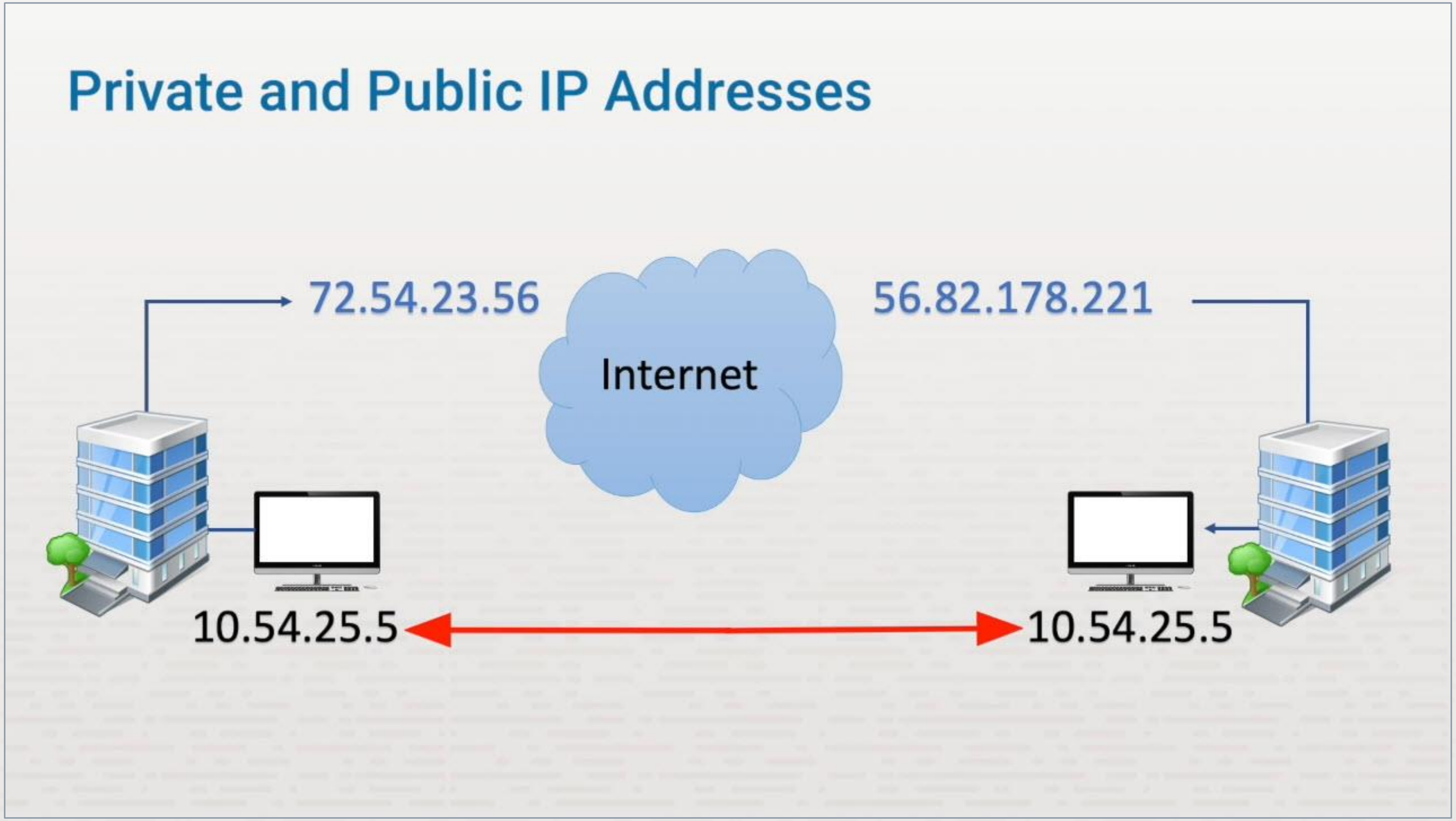
IPv4 Address Classes

Class	First Octet Range	Subnet Mask	Number of Addresses	
A	0 - 127	255.0.0.0	16,777,216 (2^{24})	
B	128 - 191	255.255.0.0	65,536 (2^{16})	
C	192 - 223	255.255.255.0	256 (2^{8})	
D	224 - 239			Used for Multicast
E	240 - 255			Experimental / Research

Assign IPv4 Addresses

- Internet Assigned Numbers Authority
- Internet Service Provider (ISP)
  - Leased IP addresses
  - Public IP addresses

IP Addresses



IP Addresses

IPv4 Address Classes

Class	First Octet Range	Subnet Mask	Number of Addresses	Private IP Range
A	0 - 127	255.0.0.0	16,777,216 (2^{24})	10.0.0.1 –10.255.255.255
B	128 - 191	255.255.0.0	65,536 (2^{16})	172.16.0.0 – 172.32.255.255
C	192 - 223	255.255.255.0	256 (2^{8})	192.168.0.0 – 192.168.255.255
D	224 - 239			Used for Multicast
E	240 - 255			Experimental / Research

IP Addresses

Special IPv4 Addresses

- Automatic Private IP Addressing (APIPA)
  - Starts with 169.x.x.x
- Loopback 127.0.0.1
  - Also known as localhost or home
- Broadcast
  - Largest/last IP address in the network
  - 192.168.1.0 has a broadcast of 192.168.1.225
  - Sent to all hosts on the network
- Network
  - Smallest/first IP address in the network (x.x.x.0)
  - Example: 192.168.1.0
- Host IP addresses cannot end in 0 or 255

Summary

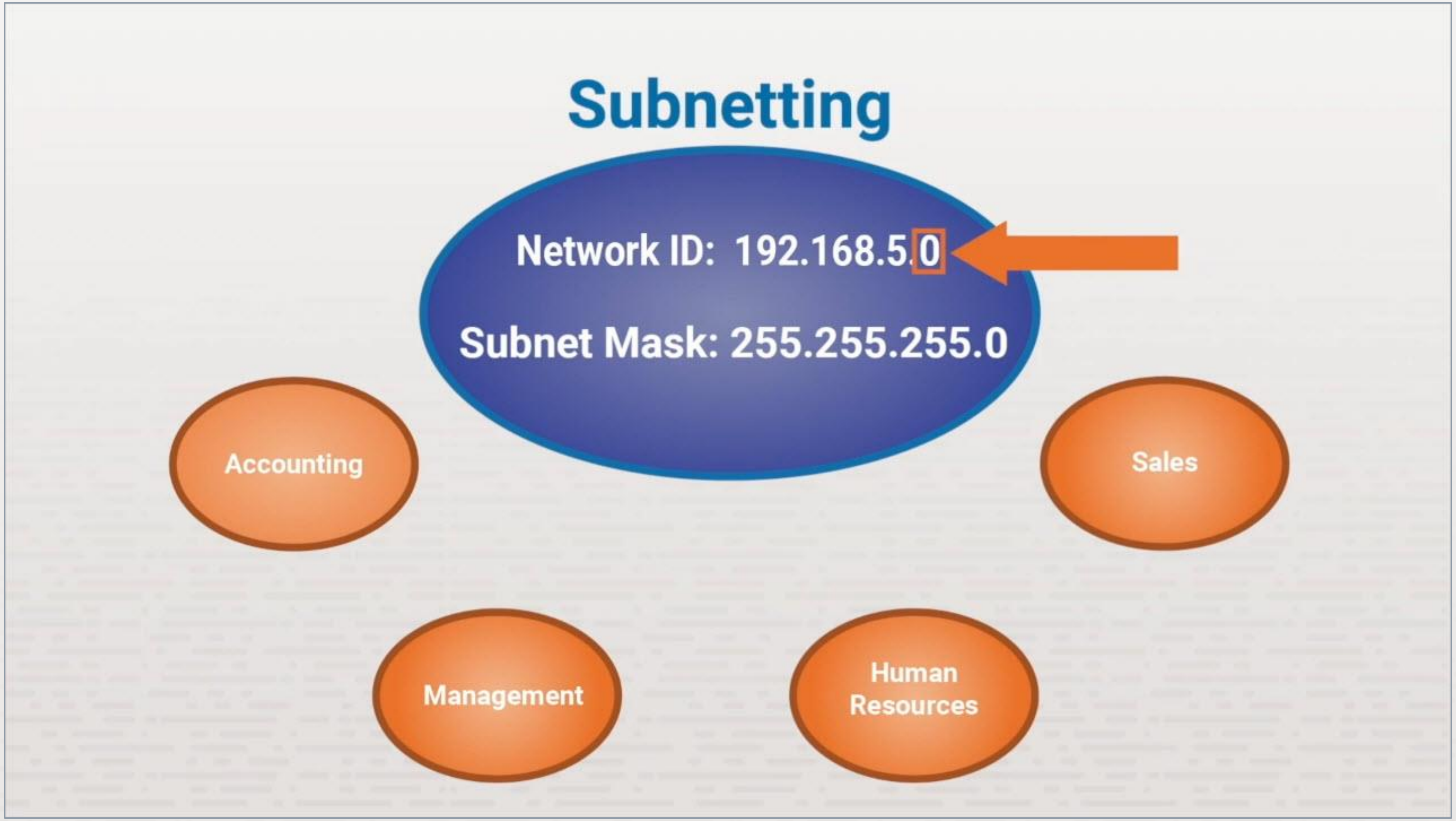
- IPv4 address format
- Subnet masks
- IPv4 address classes
- Special IPv4 addresses

Subnets Part 1

Subnetting Benefits

- Increased security
- Network management
- Network performance
- Separation

Subnets Part 1



Subnets Part 1

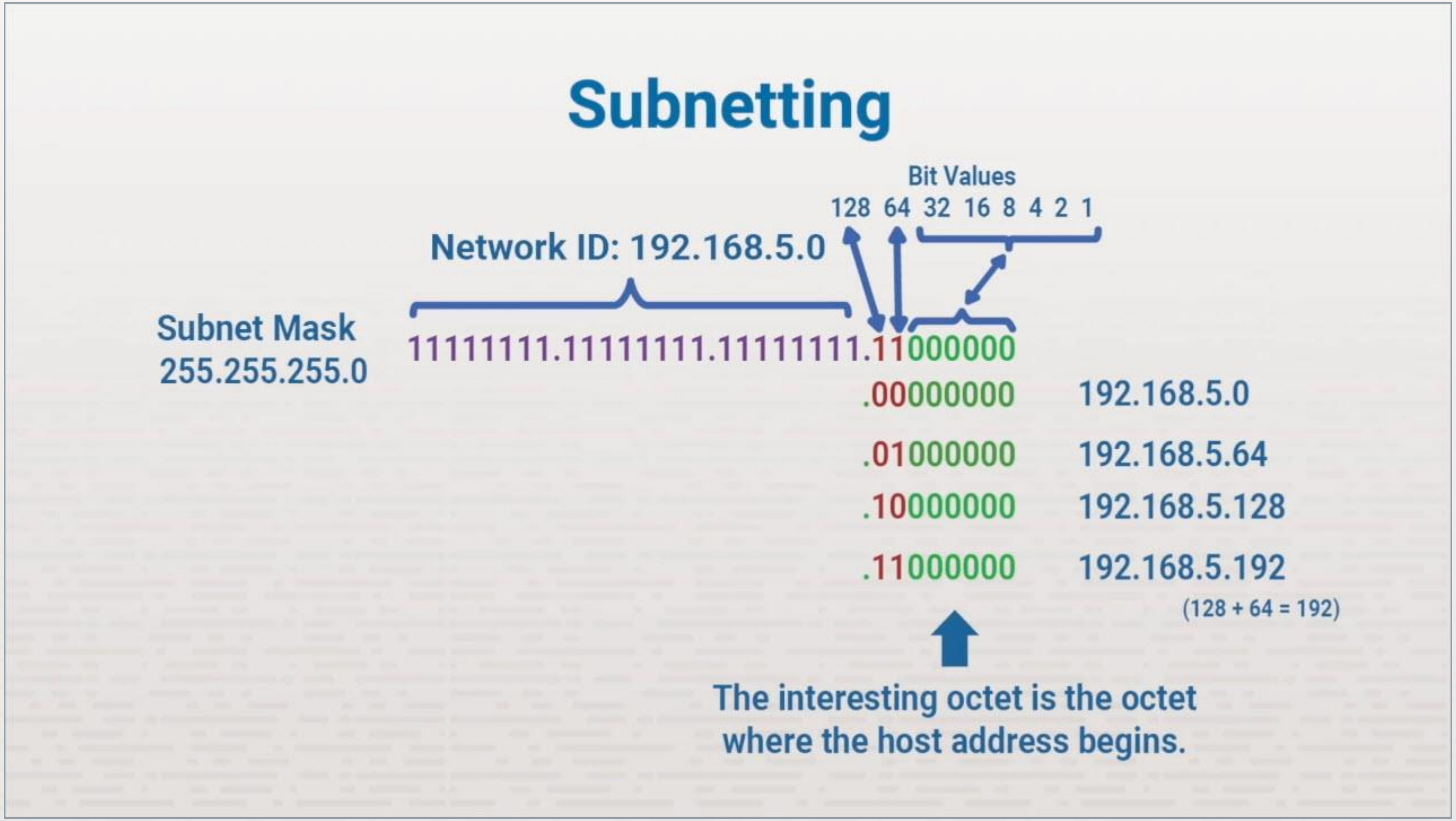
Subnetting

Network ID 192.168.5.0	11000000.10101000.00000101.00000000 (192) . (168) . (5) . (0)
Subnet Mask 255.255.255.0	11111111.11111111.11111111.11000000 (255) . (255) . (255) . (0)

2^x = number of subnets
x = number of bits borrowed

$2^1 = 2$ Two subnets
$2^2 = 4$ Four subnets
$2^3 = 8$ Eight subnets

Subnets Part 1



Subnets Part 1

Calculate Number of Hosts per Subnet

$2^y - 2$ = number of hosts y = number of bits available in host ID

$2^6 = 64$ 11111111.11111111.11111111.00$\boxed{000000}$ 6 bits

$64 - 2 = 62$ 192 168 5 .00000000 Network ID (.0)

Result: four subnets each with 62 usable IPs .00000001 First Usable IP (.1)

First IP = Network ID .00111110 Last Usable IP (.62)

Last IP = Broadcast address .00111111 Broadcast (.63)

Next Subnet .01000000 Network ID (.64)

Network ID	Host Range	Broadcast Address
192.168.5.0	192.168.5.1 – 192.168.5.62	192.168.5.63
192.168.5.64	192.168.5.65 – 192.168.5.126	192.168.5.127
192.168.5.128	192.168.5.129 – 192.168.5.190	192.1685.191
192.168.5.192	192.168.5.193 – 192.168.5.254	192.168.5.255

Classless Inter-Domain Routing (CIDR)

- CIDR uses the number of 1s in the subnet mask to quickly represent the subnet mask.

Subnets Part 1

Classless Inter-Domain Routing (CIDR)

	First Octet Range	Default Subnet Mask	Binary Value	CIDR
Class A	0 - 127	255.0.0.0	11111111.0.0.0	
Class B	128 - 191	255.255.0.0	11111111.11111111.0.0	
Class C	192 - 223	255.255.255.0	11111111.11111111.11111111.0	

Subnets Part 1

Classless Inter-Domain Routing (CIDR)

	First Octet Range	Default Subnet Mask	Binary Value	CIDR
Class A	0 - 127	255.0.0.0	11111111.0.0.0 8	/8
Class B	128 - 191	255.255.0.0	11111111.11111111.0.0 8 + 8	/16
Class C	192 - 223	255.255.255.0	11111111.11111111.11111111.0 8 + 8 + 8	/24

Subnets Part 1

Classless Inter-Domain Routing (CIDR)

Subnet Mask	CIDR
11111111.11111111.11111111.11000000	
8 + 8 + 8 + 2	/26

Subnets Part 1

Classless Inter-Domain Routing (CIDR)

Subnet Mask	CIDR
11111111.11111111.11111111.11000000	
8 + 8 + 8 + 2	/26

Network ID = 192.168.5.0/26

Result: four subnets each with 62 usable IPs

Subnetting Formulas

- The number of subnets = 2^x
  - x = The number of bits borrowed for subnetting
  - Example: 2^x = 8 subnets
- The number of hosts = 2^y-2
  - y = The number of bits in host ID
  - Example: 25 = 32 - 2 = 30 hosts/subnet

Subnets Part 1

Subnetting

Network ID: 172.16.0.0/16

Subnet mask: $\boxed{11111111.11111111}$.0.0

Subnets required: 24

# of subnets ➔ $2^5 = 32$

Network ID: 172.16.0.0/21 ← New CIDR

(16+5=21)

# of hosts ➔ $2^{11} - 2 = 2{,}046$

Network Address	Usable Host Range	Broadcast Address:
172.16.0.0	172.16.0.0 - 172.16.7.254	172.16.7.255
172.16.8.0	172.16.8.1 - 172.16.15.254	172.16.15.255
172.16.16.0	172.16.16.1 - 172.16.23.254	172.16.23.255
172.16.24.0	172.16.24.1 - 172.16.31.254	172.16.31.255
172.16.32.0	172.16.32.1 - 172.16.39.254	172.16.39.255
172.16.40.0	172.16.40.1 - 172.16.47.254	172.16.47.255
172.16.48.0	172.16.48.1 - 172.16.55.254	172.16.55.255
172.16.56.0	172.16.56.1 - 172.16.63.254	172.16.63.255
172.16.64.0	172.16.64.1 - 172.16.71.254	172.16.71.255
172.16.72.0	172.16.72.1 - 172.16.79.254	172.16.79.255
172.16.80.0	172.16.80.1 - 172.16.87.254	172.16.87.255
172.16.88.0	172.16.88.1 - 172.16.95.254	172.16.95.255
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
172.16.184.0	172.16.184.1 - 172.191.31.254	172.16.191.255
172.16.192.0	172.16.192.1 - 172.191.199.254	172.16.199.255
172.16.200.0	172.16.200.1 - 172.191.207.254	172.16.207.255
172.16.208.0	172.16.208.1 - 172.191.215.254	172.16.215.255
172.16.216.0	172.16.216.1 - 172.191.223.254	172.16.223.255
172.16.224.0	172.16.224.1 - 172.191.231.254	172.16.231.255
172.16.232.0	172.16.232.1 - 172.191.239.254	172.16.239.255
172.16.240.0	172.16.240.1 - 172.191.247.254	172.16.247.255
172.16.248.0	172.16.248.1 - 172.191.255.254	172.16.255.255

Summary

- Subnetting
- CIDR notation
- Subnetting formulas
- Subnetting examples

Subnets Part 2

Subnet Masking Types

- Fixed-length subnet mask (FLSM)
  - Same mask and number of addresses
- Variable-length subnet mask (VLSM)
  - Uses different sizes of subnet masks

Subnets Part 2

Variable-Length Subnet Mask (VLSM)

CIDR Notation	Hosts per Subnet
/24	254
/25	126
/26	62
/27	30
/28	14
/29	6
/30	2

Subnets Part 2

Variable-Length Subnet Mask (VLSM)

Network: 192.168.5.0/24

Subnet mask: 255.255.255.0

CIDR Notation	Hosts per Subnet
/24	254
/25	126
/26	62
/27	30
/28	14
/29	6
/30	2

Sales 107 Hosts

Accounting 54 Hosts

Human Resources 25 Hosts

Management 5 Hosts

Subnets Part 2

Variable-Length Subnet Mask (VLSM)

CIDR Notation	Hosts per Subnet
/24	254
/25	126
/26	62
/27	30
/28	14
/29	6
/30	2

Host requirements:

- Sales: 107
- Accounting: 54
- Human resources: 25
- Management: 5

Sales	Subnet	Addresses Available	Hosts Needed
Sales	192.168.5.0/25	126	107
Accounting	192.168.5.128/26	62	54
Human Resources	192.168.5.192/27	30	25
Management	192.168.5.224/29	6	5

Subnets Part 2

Use ANDing to Identify the Network ID

172.16.77.54/21

IP Address	10101100.00010000.01001101.00110110
Subnet Mask	11111111.11111111.11111000.00000000
	8 + 8 + 5 = 21

Subnets Part 2

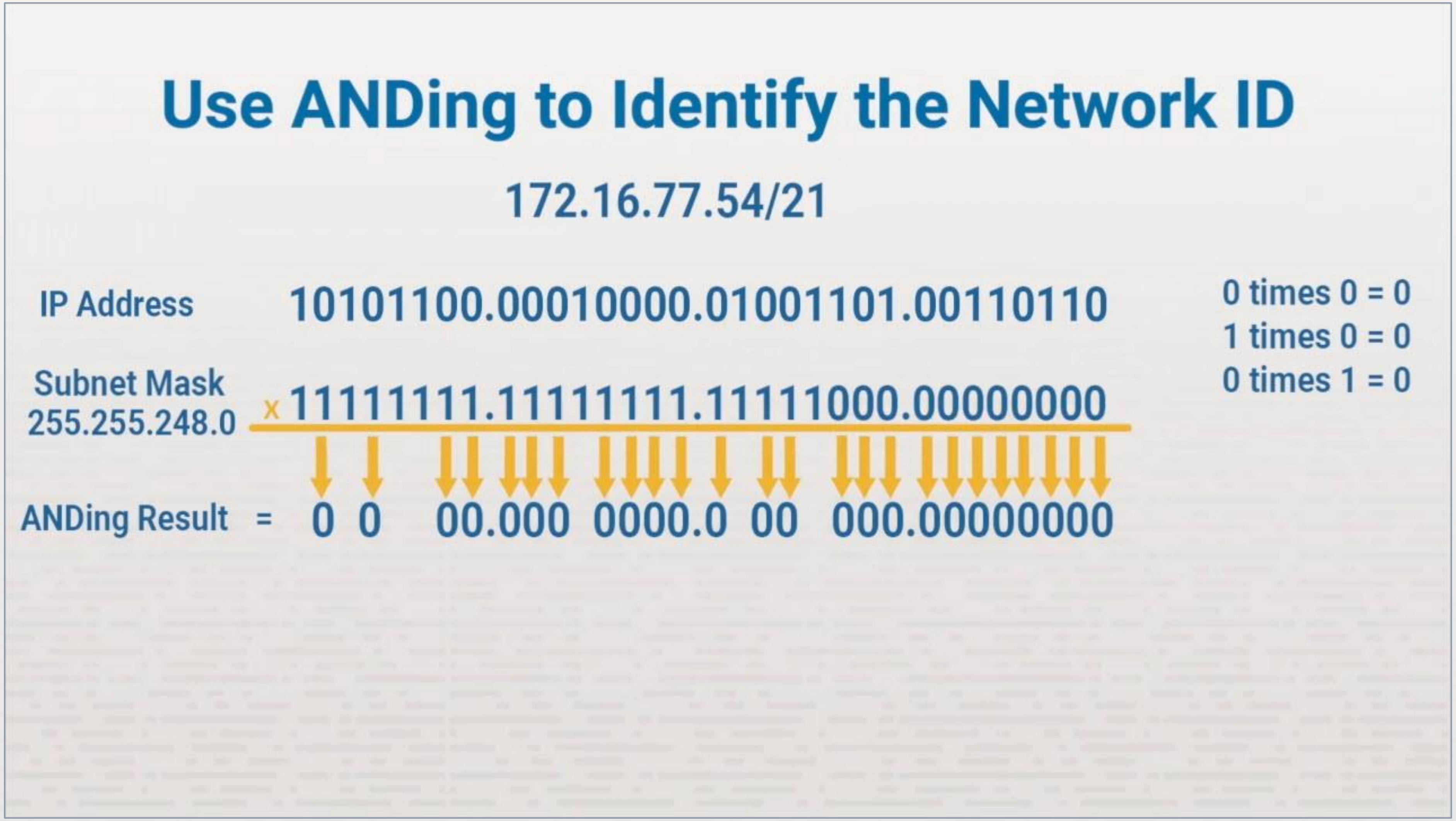
Use ANDing to Identify the Network ID

172.16.77.54/21

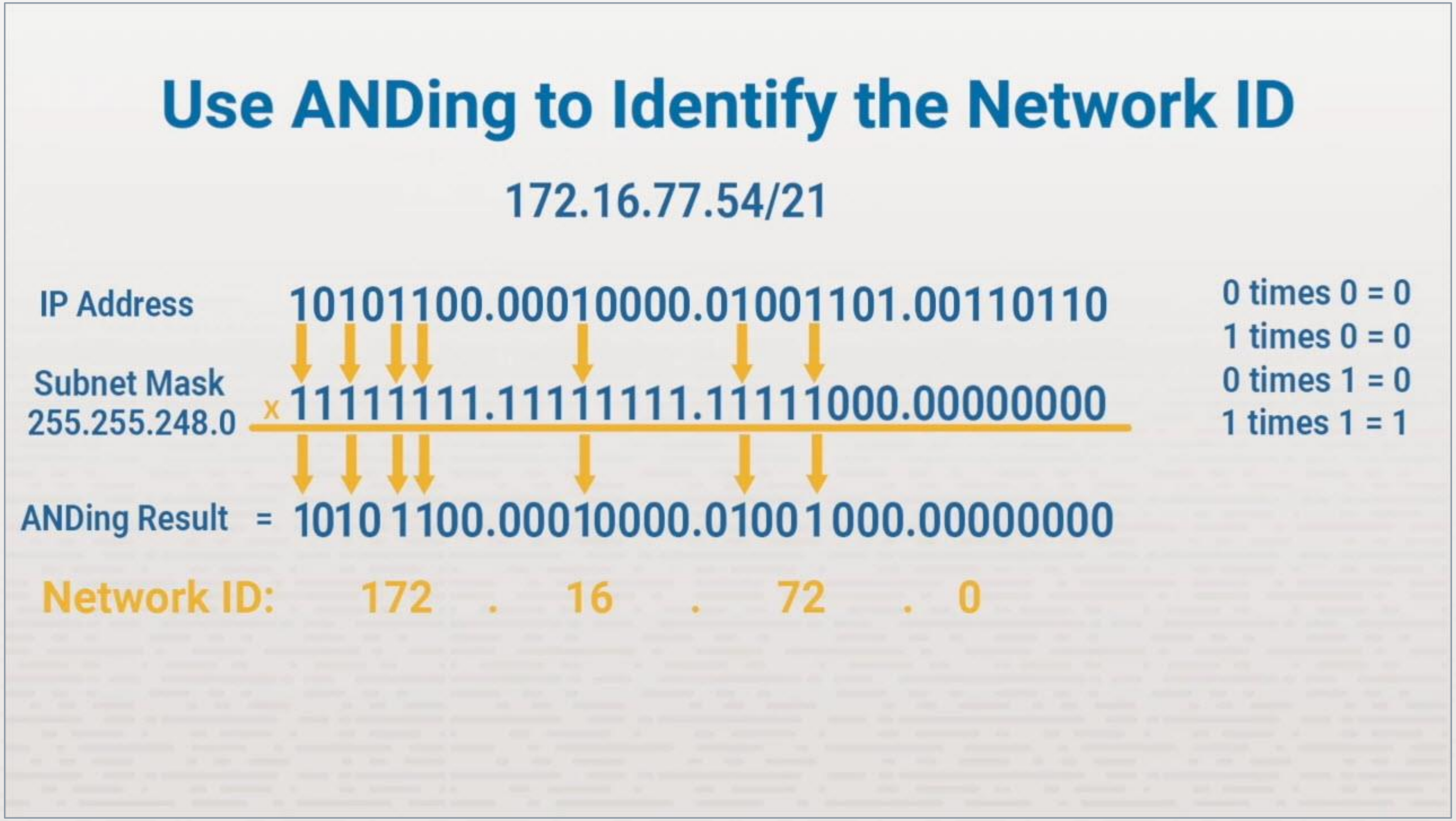
IP Address	10101100.00010000.01001101.00110110
Subnet Mask 255.255.248.0	11111111.11111111.11111000.00000000

128 + 64 + 32 + 16 + 8 = 248

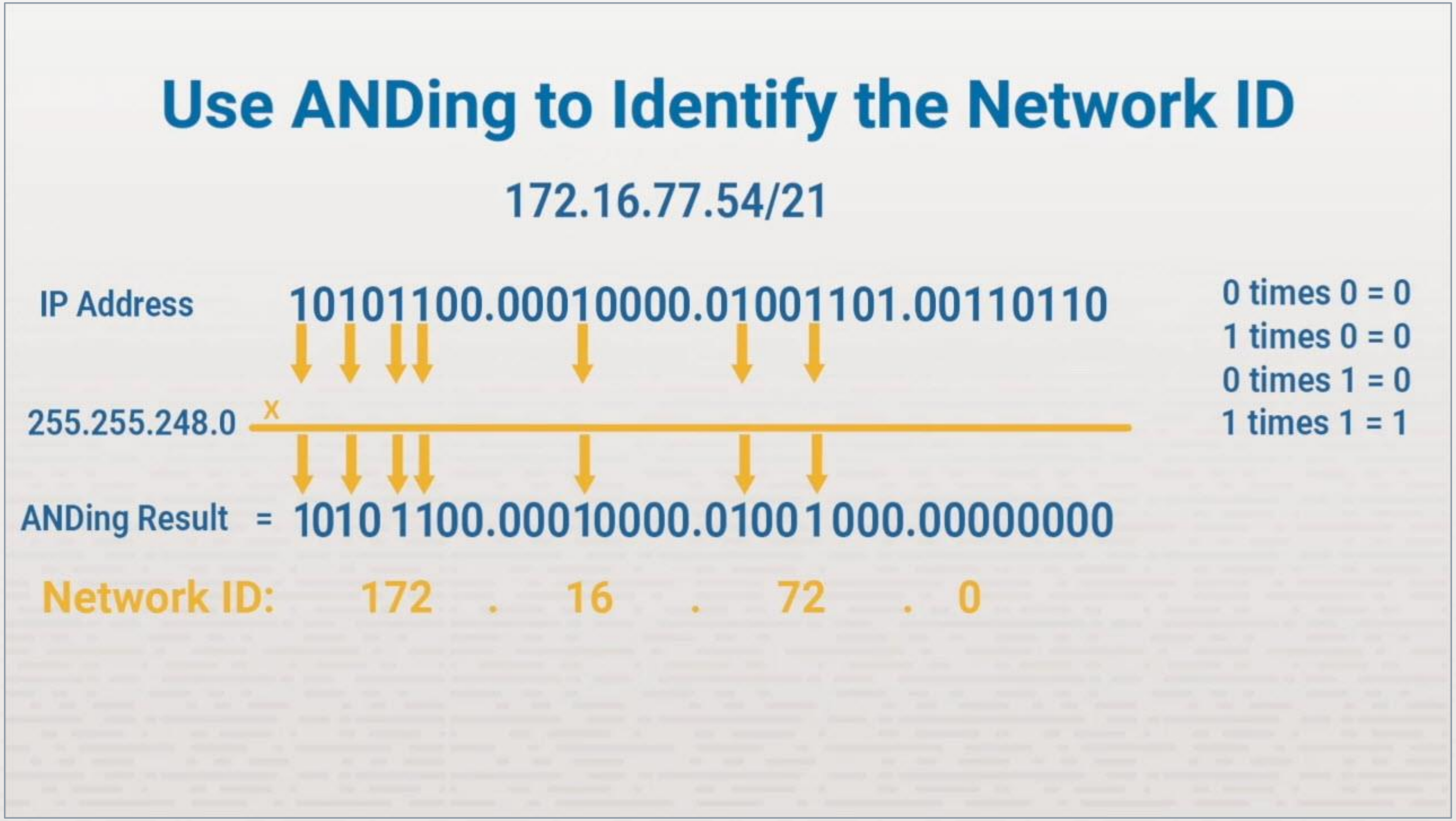
Subnets Part 2



Subnets Part 2



Subnets Part 2



Subnetting Uses

- FLSM used in private networks
- VLSM used in public networks
- Only supported by advanced routing protocols

Subnets Part 2

Supernetting

Supernetting requires contiguous network ID numbers

Can be supernetted	Can't be supernetted
192.168.1.0	192.168.1.0
192.168.2.0	192.168.4.0
192.168.3.0	192.168.5.0

Supernetting Advantages

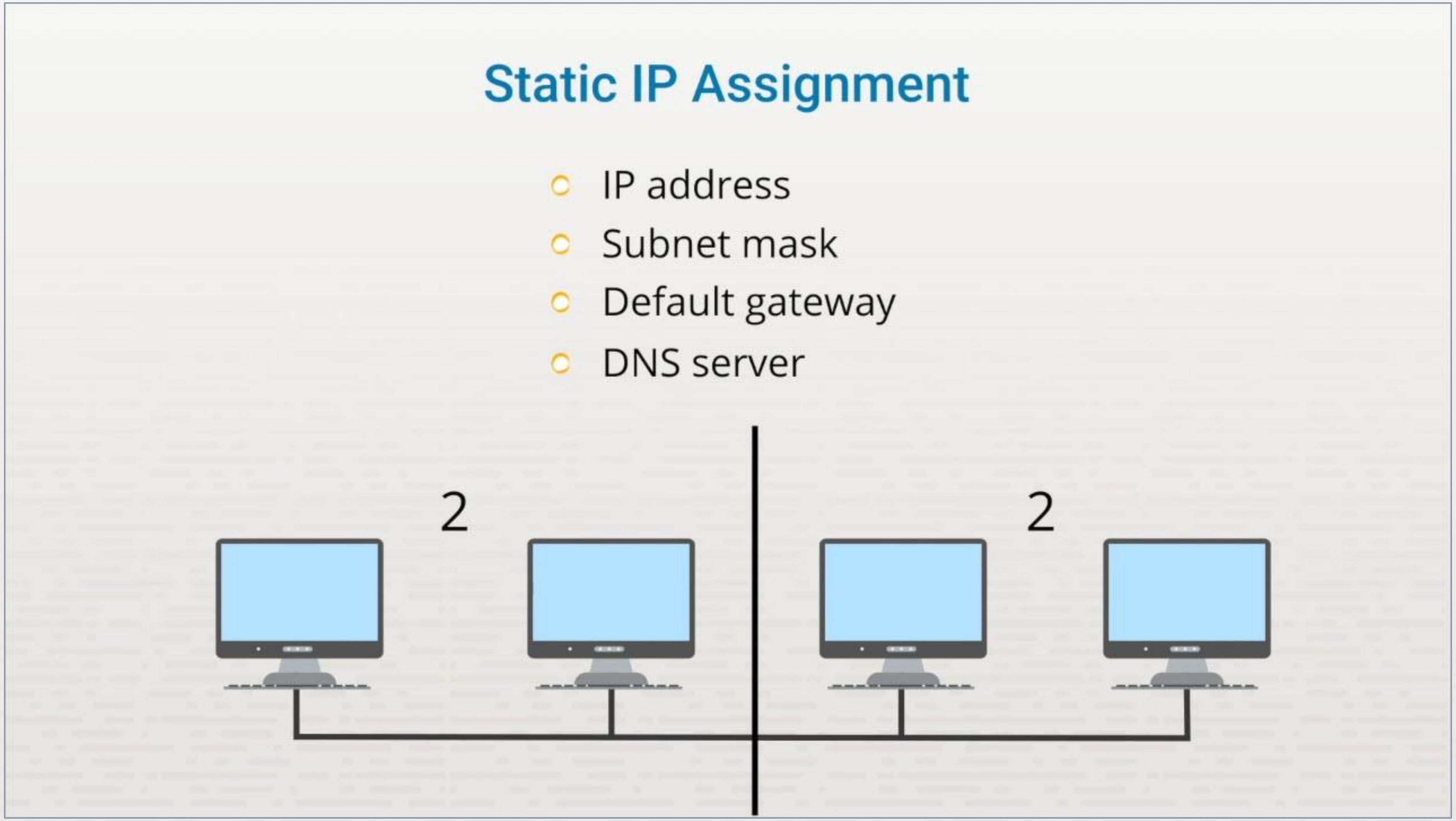
- Reduce routing table size
- Simplify network overview
- Decrease necessary resources
- Improve network performance

Summary

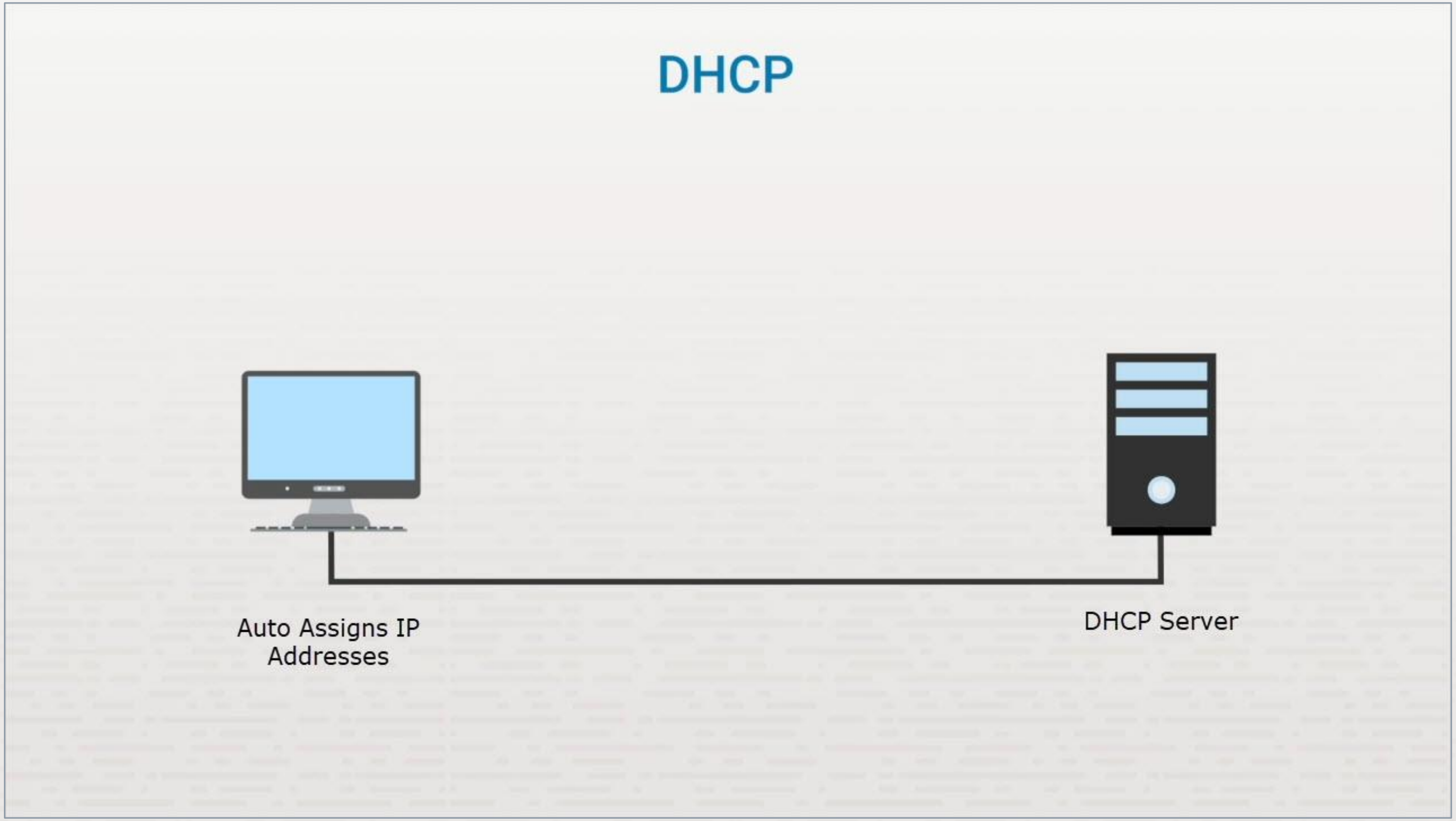
- Fixed-length subnet mask
- Variable-length subnet mask
- ANDing
- Supernetting

IP Address Assignment

IP Address Assignment



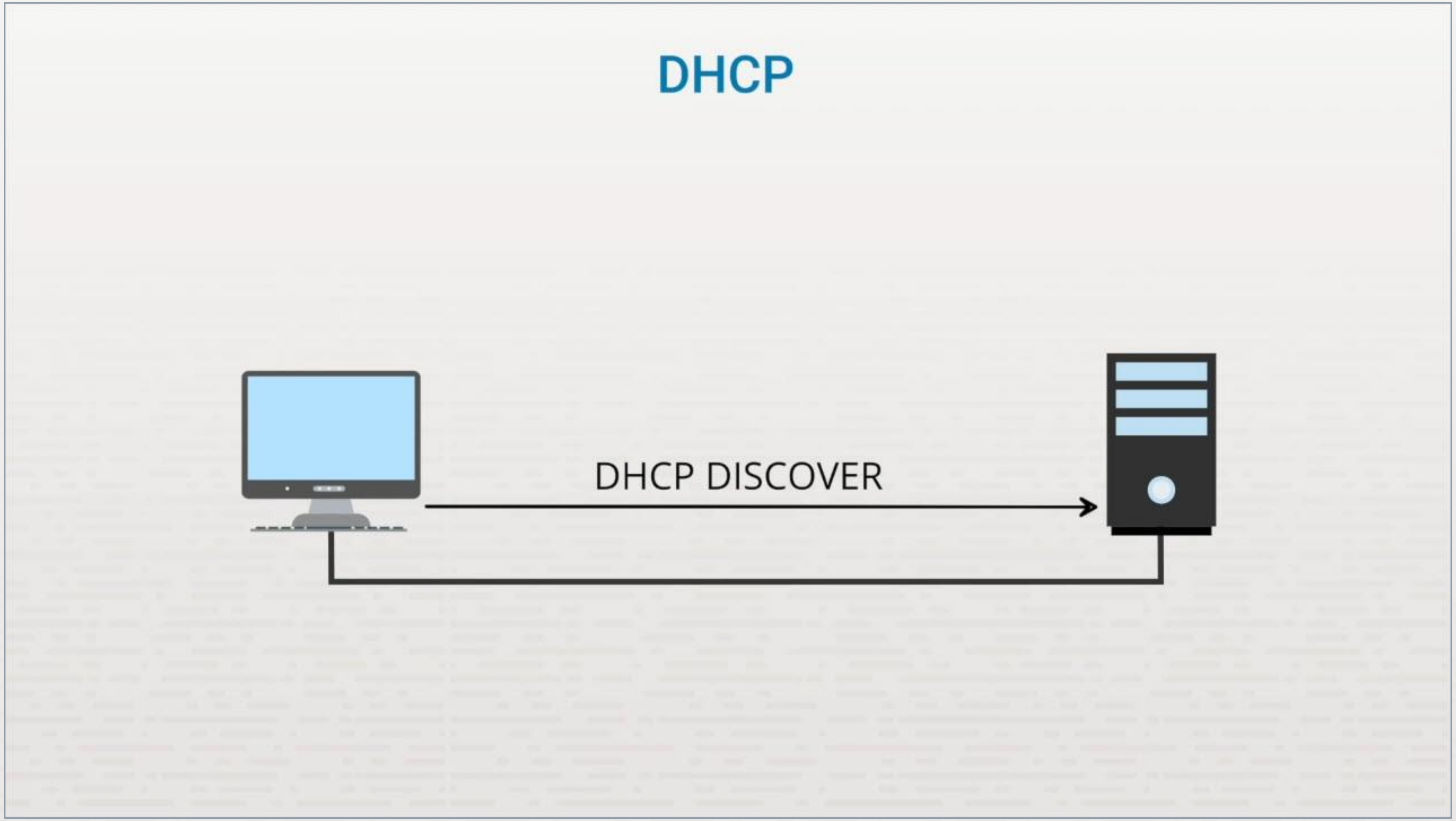
IP Address Assignment



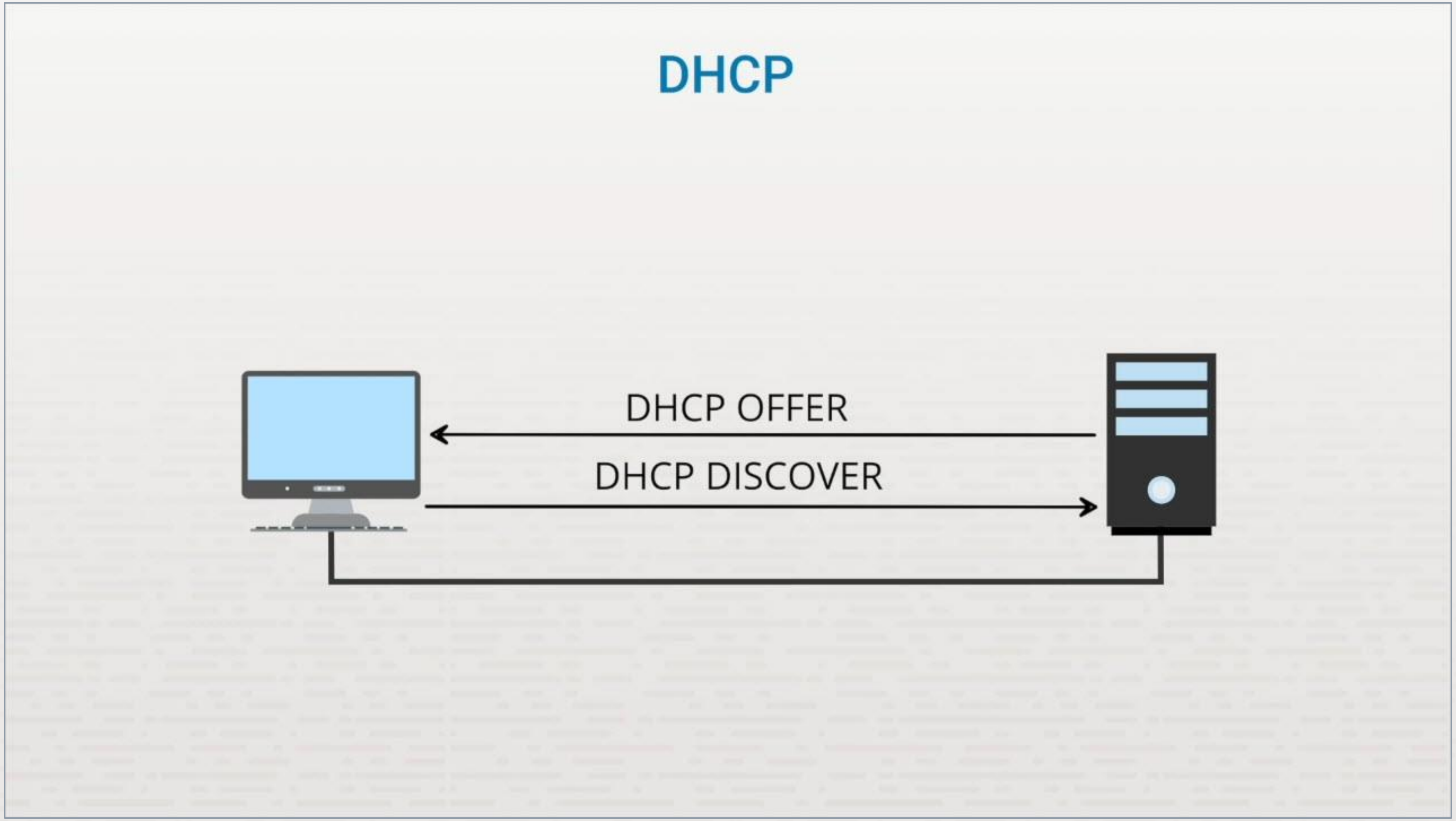
DHCP Scope

- A range of IP addresses
- An appropriate subnet mask
- The address of the DNS server
- The address of the gateway

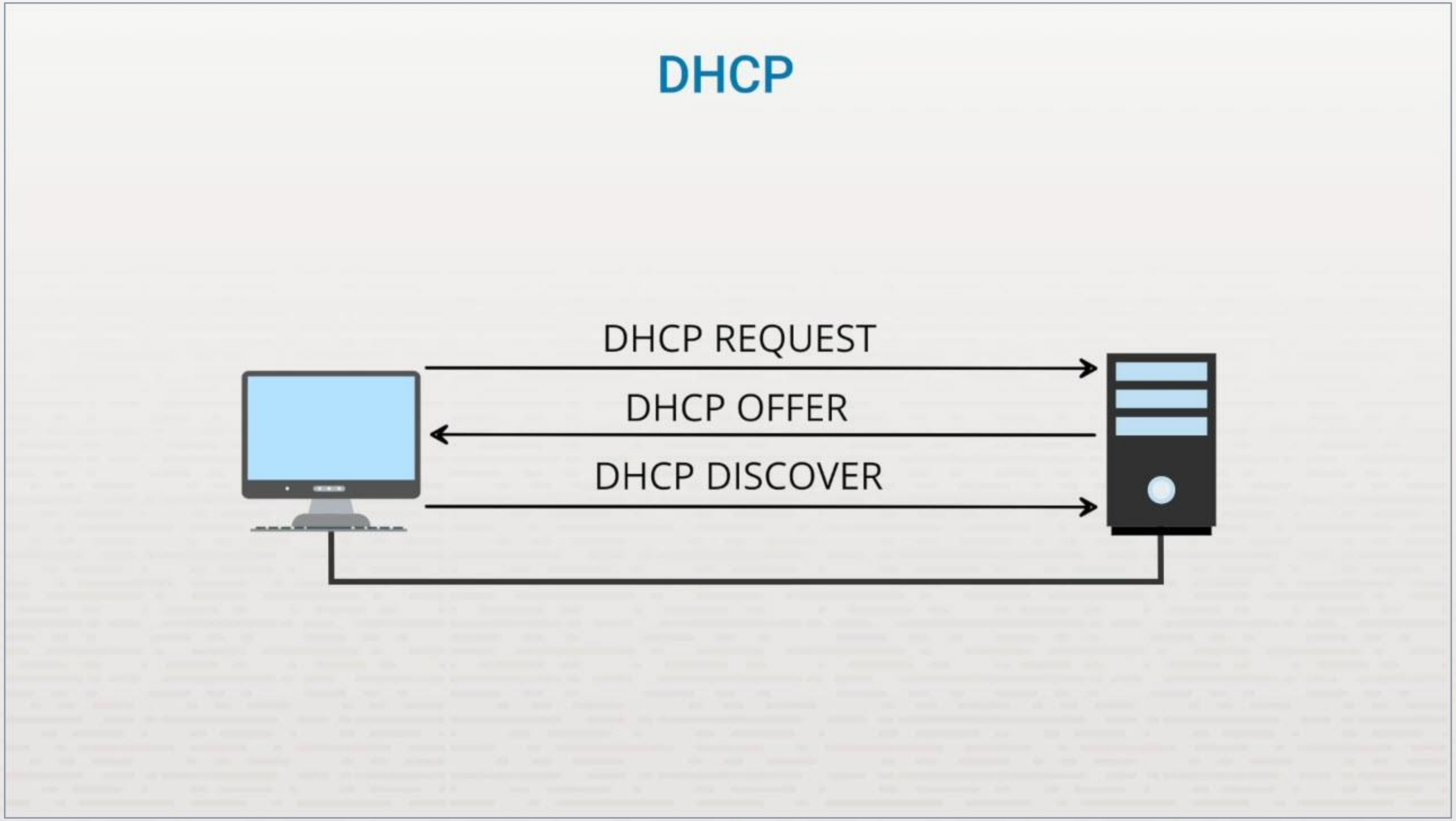
IP Address Assignment



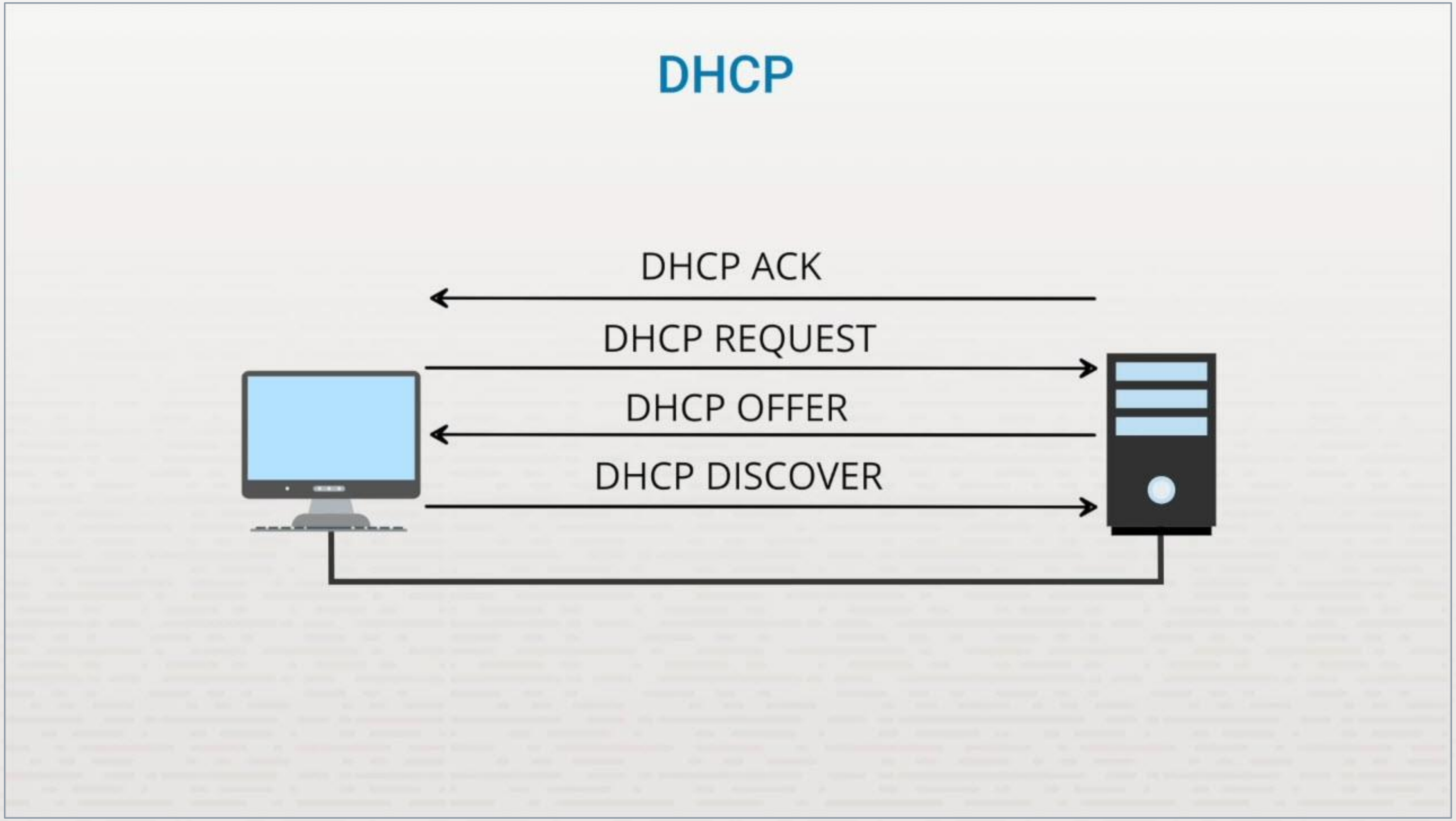
IP Address Assignment



IP Address Assignment



IP Address Assignment



IP Address Assignment

DHCP

Router>enable
Password:
Router#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z
Router (config) #interface fastEthernet 0/1
Router (config-if) #ip helper-address 192.168.0.254
Router (config-if) #exit
Router (config) #exit

Summary

- Benefits and drawbacks of static IP assignments
- Lease assignment process
- Implementing DHCP on switches and routers

In-Class Practice

Do the following labs:

- 4.1.11 Configure IP Addresses
- 4.1.13 Configure IP Addresses on Mobile Devices

Class Discussion

- What is the format of an IPv4 address?
- What is the purpose of a subnet mask?
- What are the different classes of IPv4 addresses?
- What is the purpose of subnetting?
- What formula is used to calculate the number of hosts per subnet?
- What does /14 mean in the following IP address: 199.78.11.12/14?

4.2 NETWORK ADDRESSING AND SERVICES

APIPA and Alternate Addressing

TESTOUT NETWORK PRO

Section Skill Overview

- Set up alternate addressing
- Configure alternate addressing

Key Terms

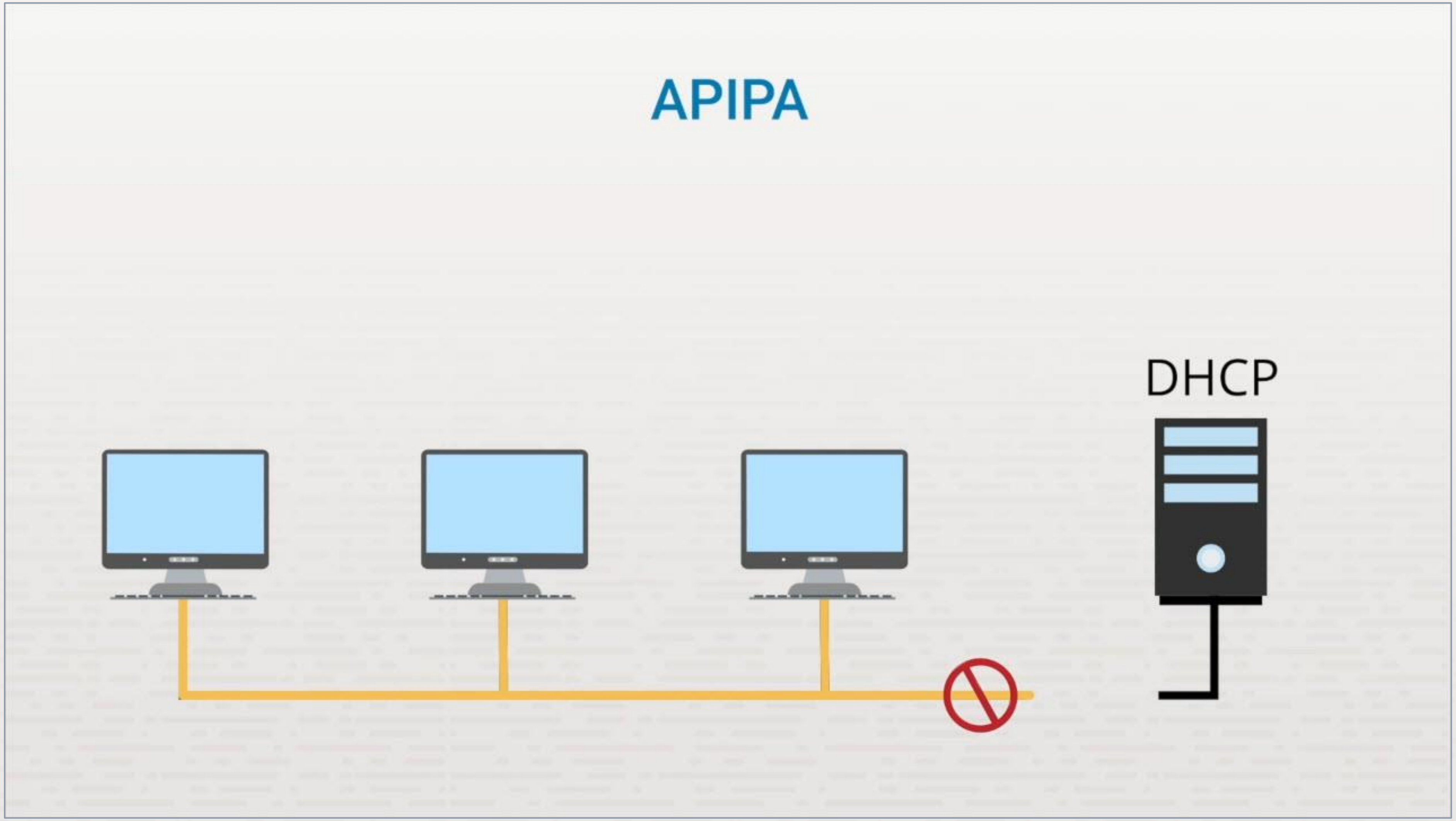
- Automatic Private IP Addressing (APIPA)
- Alternate IP configuration

Key Definitions

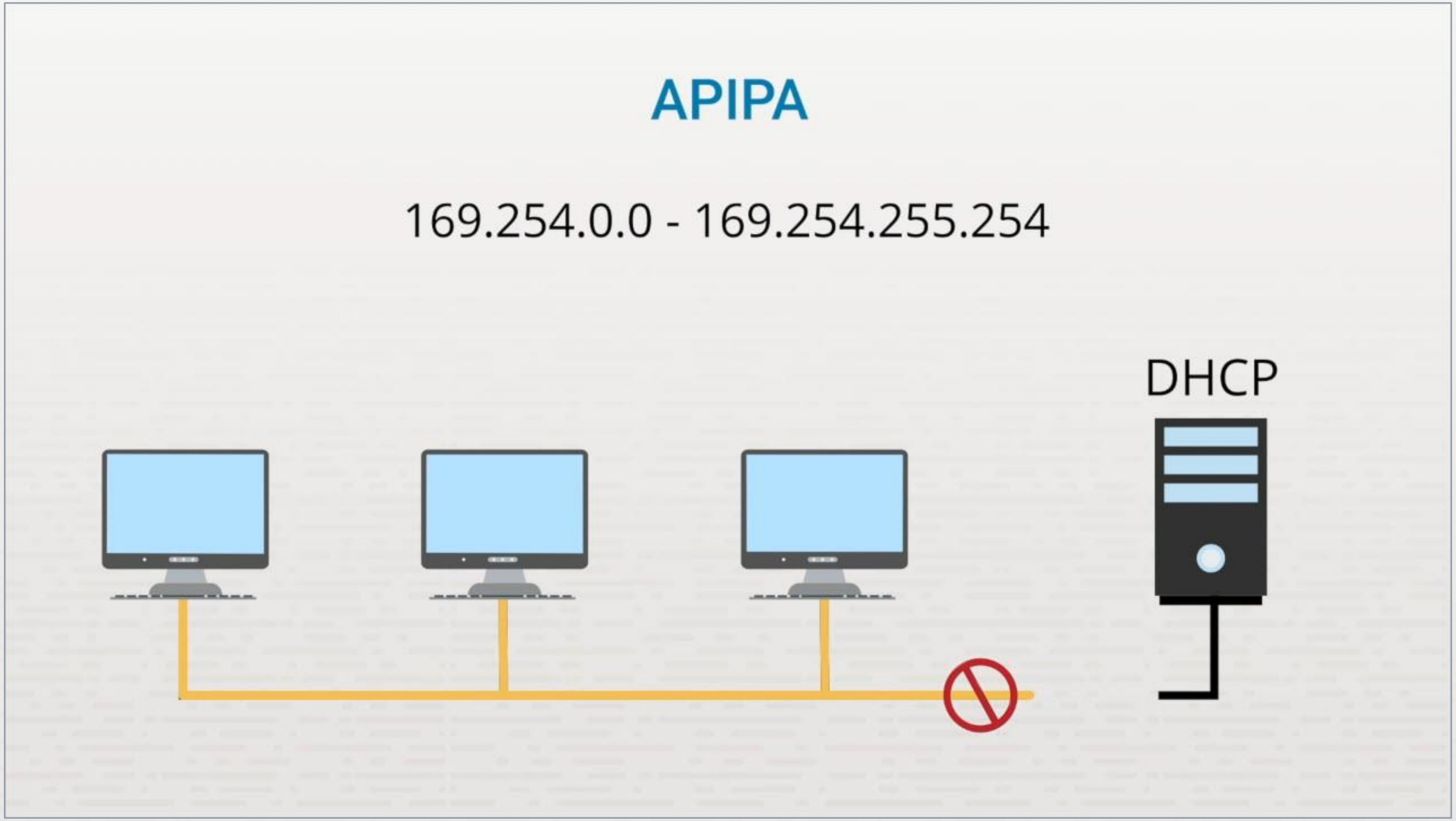
- **Automatic Private IP Addressing (APIPA):** APIPA provides an option for automatic IP address assignment without a DHCP server. APIPA is enabled by default on most modern operating systems, including Windows and Linux.
- **Alternate IP configuration:** A manual configuration of a computer's IP address, default gateway, DNS server address, and WINS address. This configuration is used if the DHCP server fails to provide this similar information.

APIPA

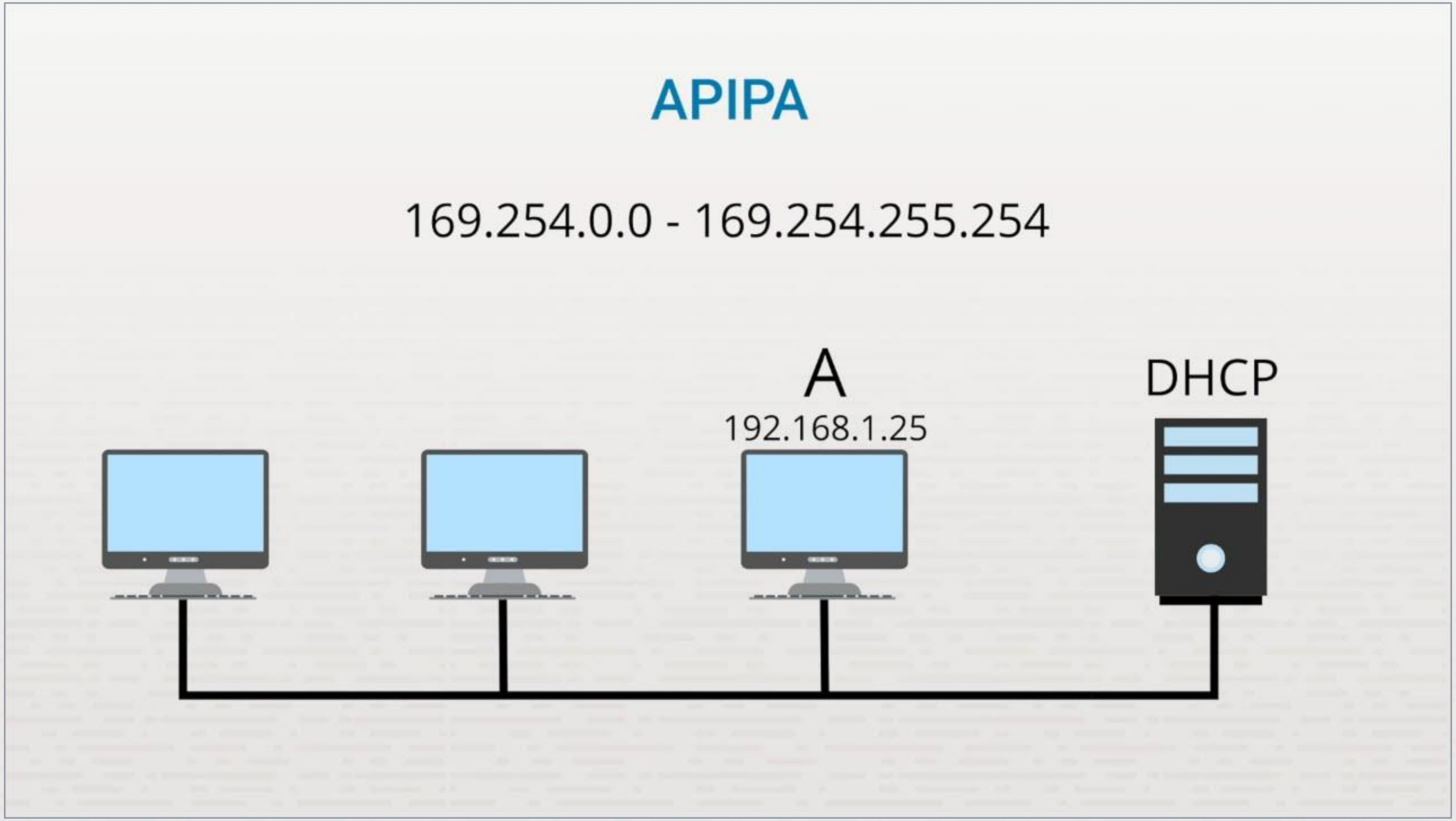
APIPA



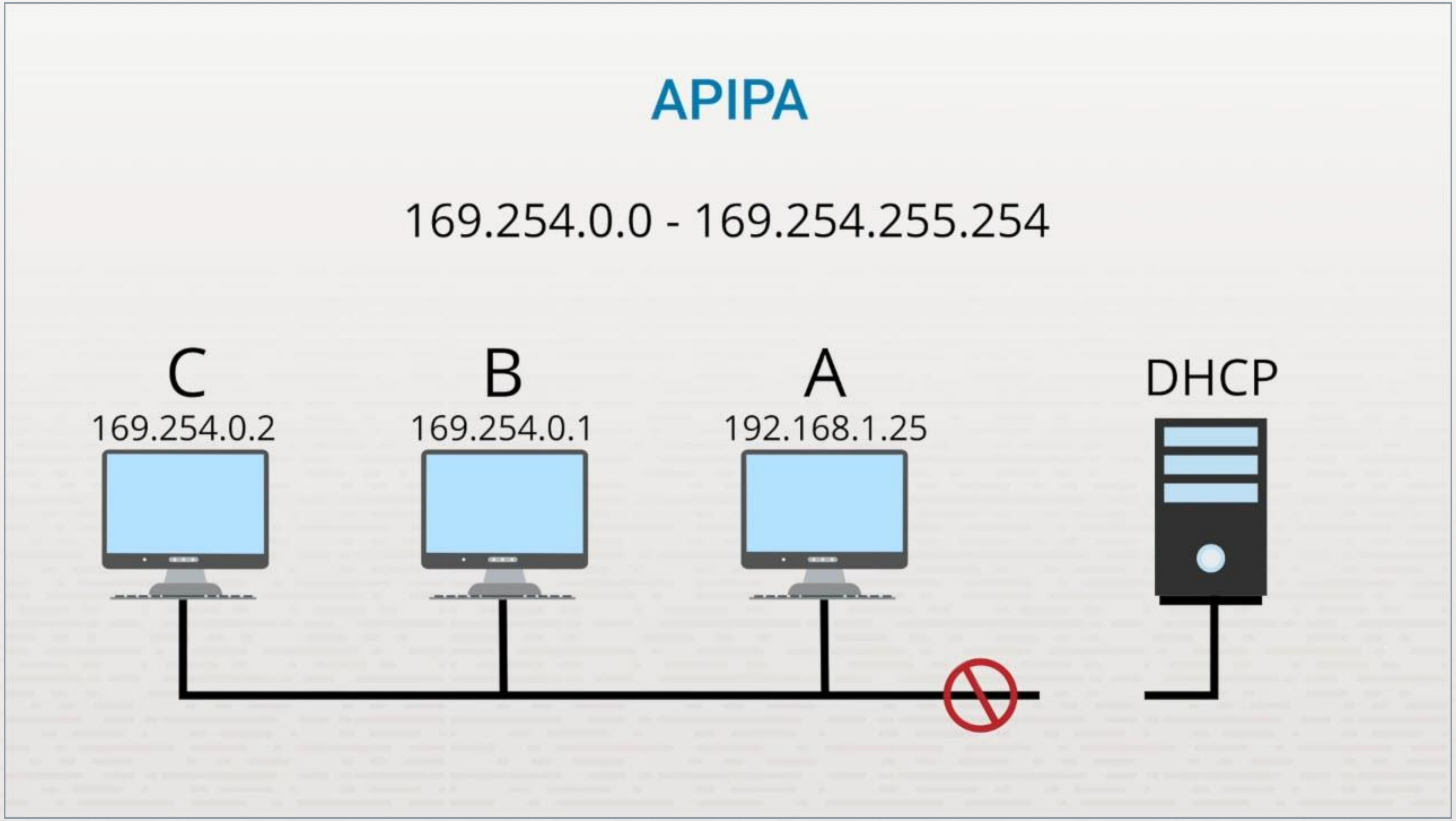
APIPA



APIPA

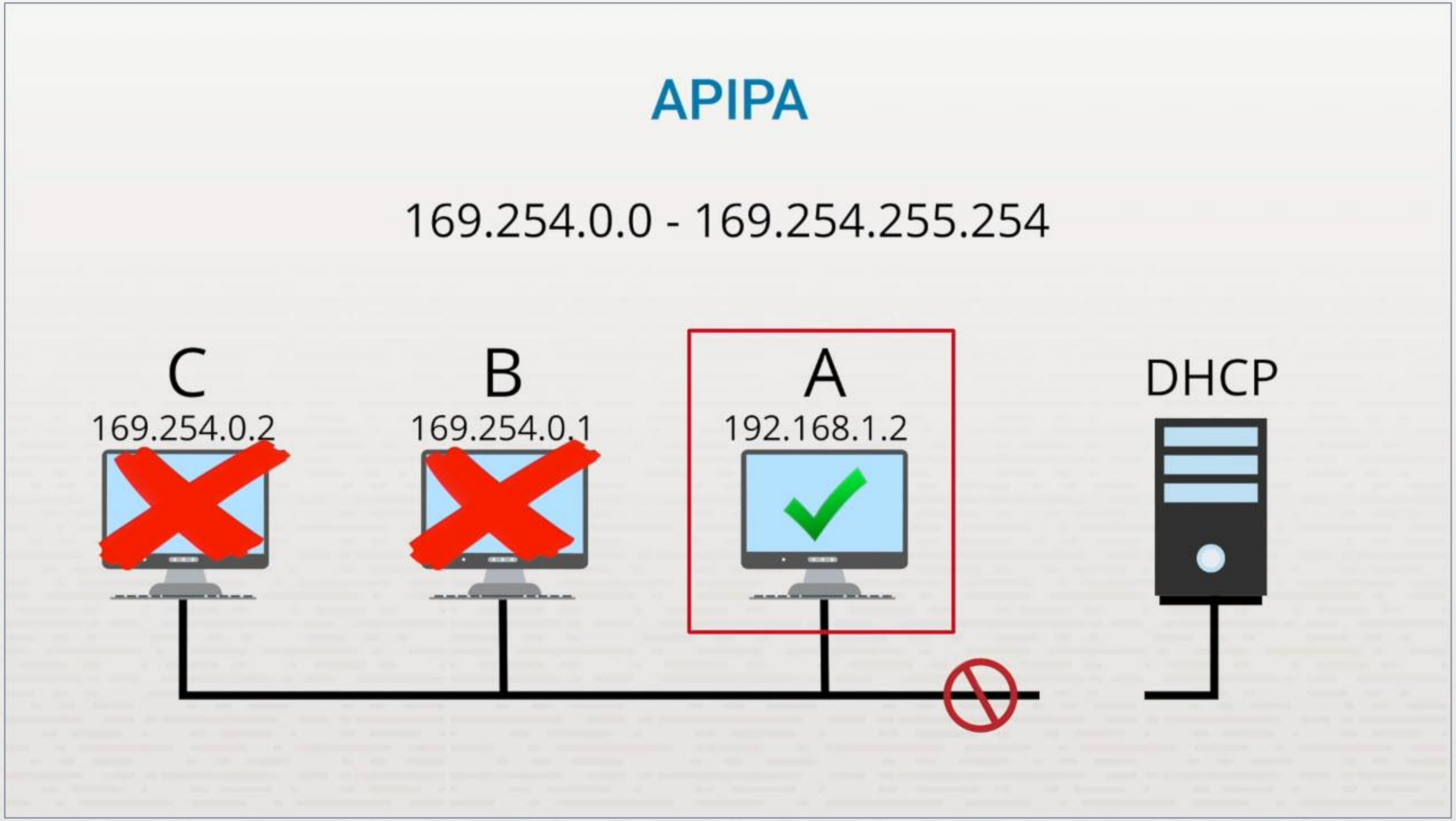


APIPA



APIPA
169.254.0.0 - 169.254.255.254
C
169.254.0.2
B
169.254.0.1
A
192.168.1.25
DHCP

APIPA


APIPA
169.254.0.0 - 169.254.255.254
C
169.254.0.2
B
169.254.0.1
A
192.168.1.2
DHCP

Summary

- APIPA
  - Automatically assigns IP addresses when no DHCP server is available

In-Class Practice

Do the following labs:

- 4.2.4 Configure Alternate Addressing

Class Discussion

- How do you know if a host is using an APIPA address?
- Which IP configuration parameters are set when APIPA is used? Which parameters are not set?
- In which scenarios would an alternate IP configuration simplify IP configuration?

DHCP

Section Skill Overview

- Configure a DHCP server
- Configure DHCP options
- Create DHCP exclusions
- Create DHCP client reservations

Key Terms

- IP range
- Subnet mask
- Exclusions
- Reservations
- DHCP lease time
- Default gateway

Key Definitions

- **IP range:** The IP range defines the range of IP addresses that the DHCP server can assign.
- **Subnet mask:** The subnet mask defines the network ID and host ID.
- **Exclusions:** Exclusions are IP addresses that the DHCP server will not assign.
- **Reservations:** Reservations are static IP addresses that are not dynamically assigned by the DHCP server.

Key Definitions

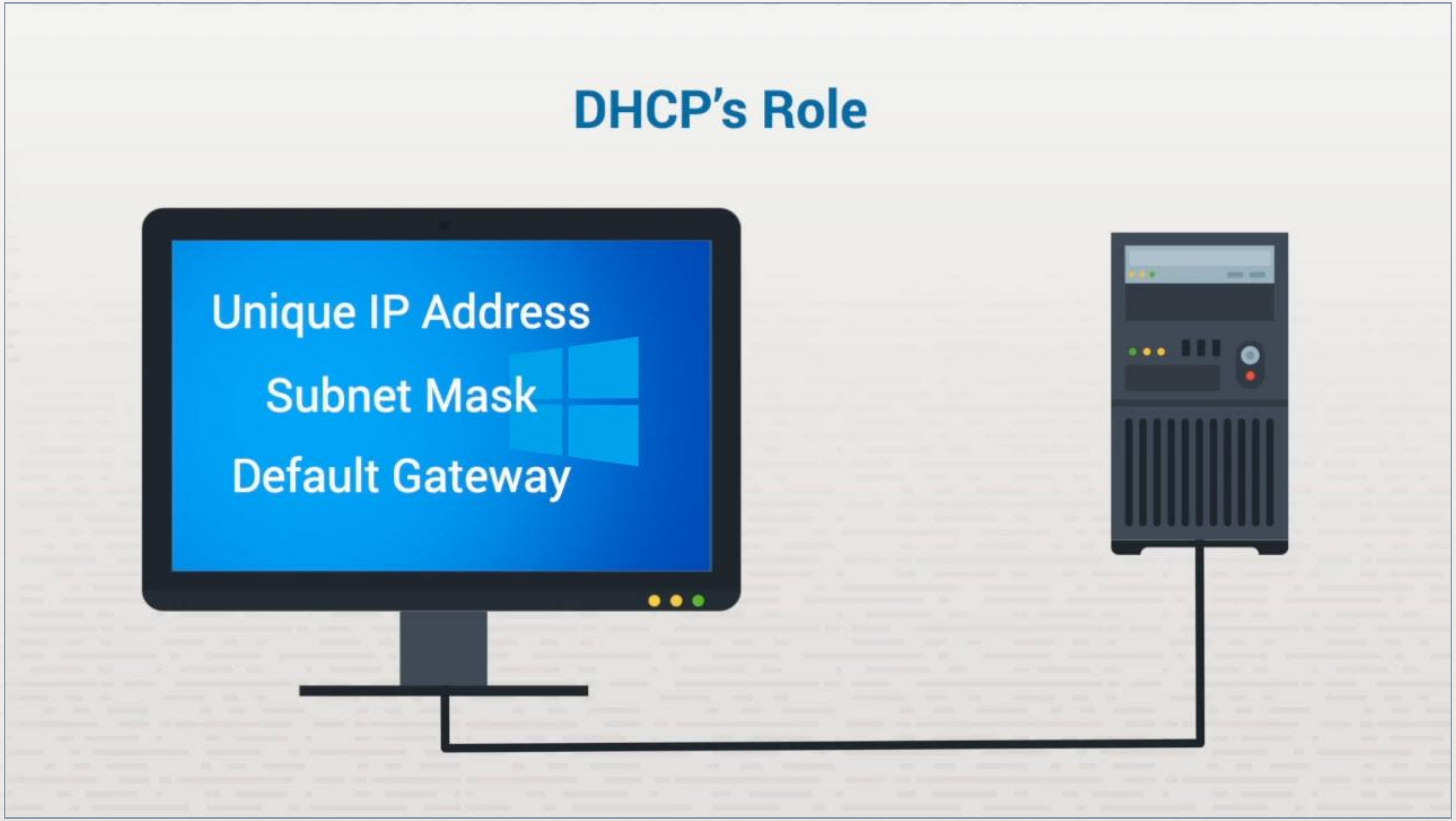
- **DHCP lease time:** When a device is assigned an IP configuration, it is for a specified amount of time. This is the DHCP lease.
- **Default gateway:** The default gateway defines where data packets that are leaving the network should go to be routed.

DHCP

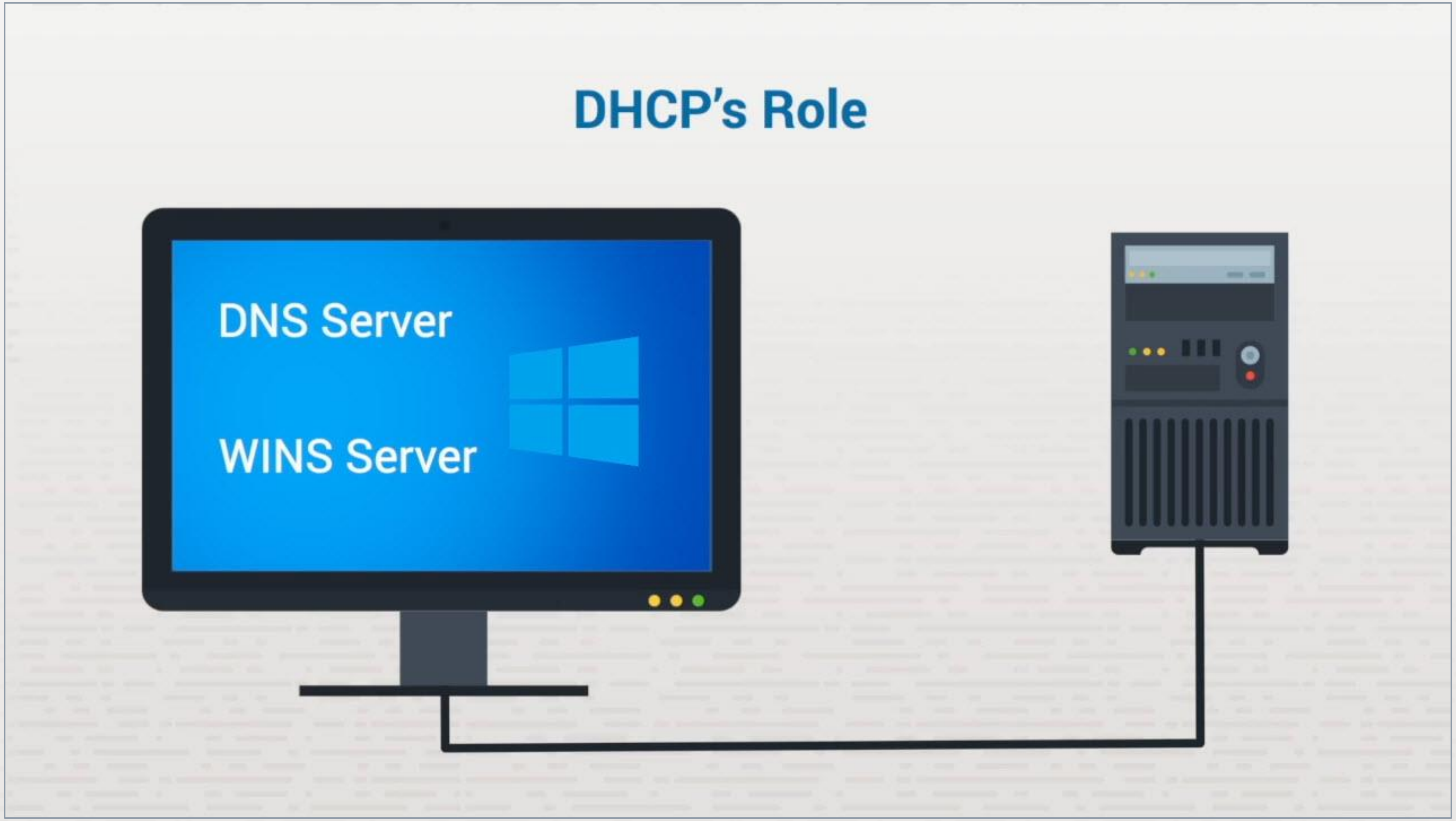
DHCP

- DHCP’s role
- DHCP configuration
- DHCP processes

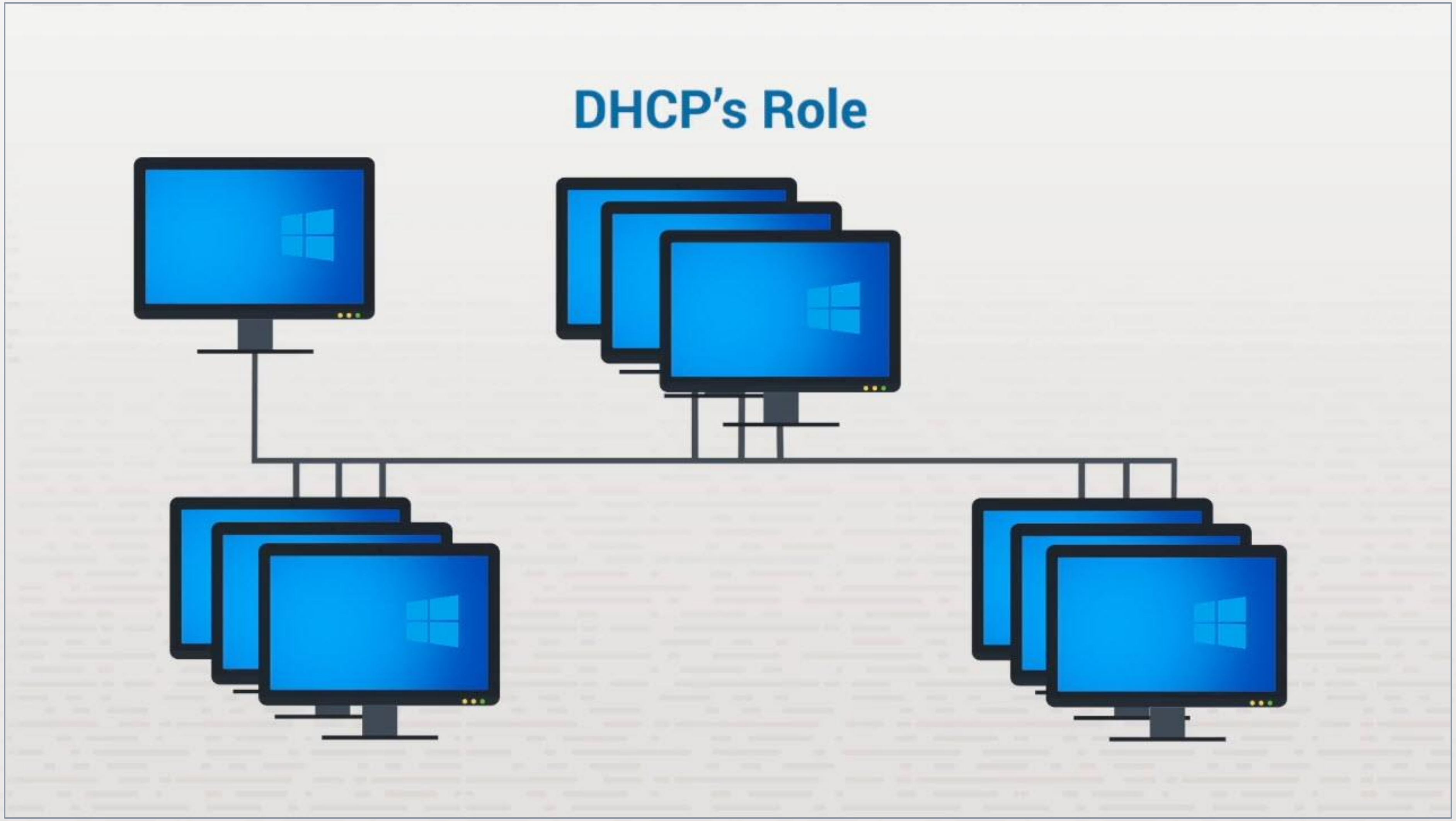
DHCP



DHCP



DHCP



DHCP Scope

- Defines IP configuration
- Wireless router
- Enterprise server

DHCP

Exclusions and Reservations

DHCP Scope	
IP range	192.168.5.50 – 192.168.5.100
Subnet mask	255.255.255.0
Exclusions	192.168.5.50 – 192.168.5.55
Reservations	22-EA-A9-67-51-64 → 192.168.5.56

DHCP

DHCP Lease

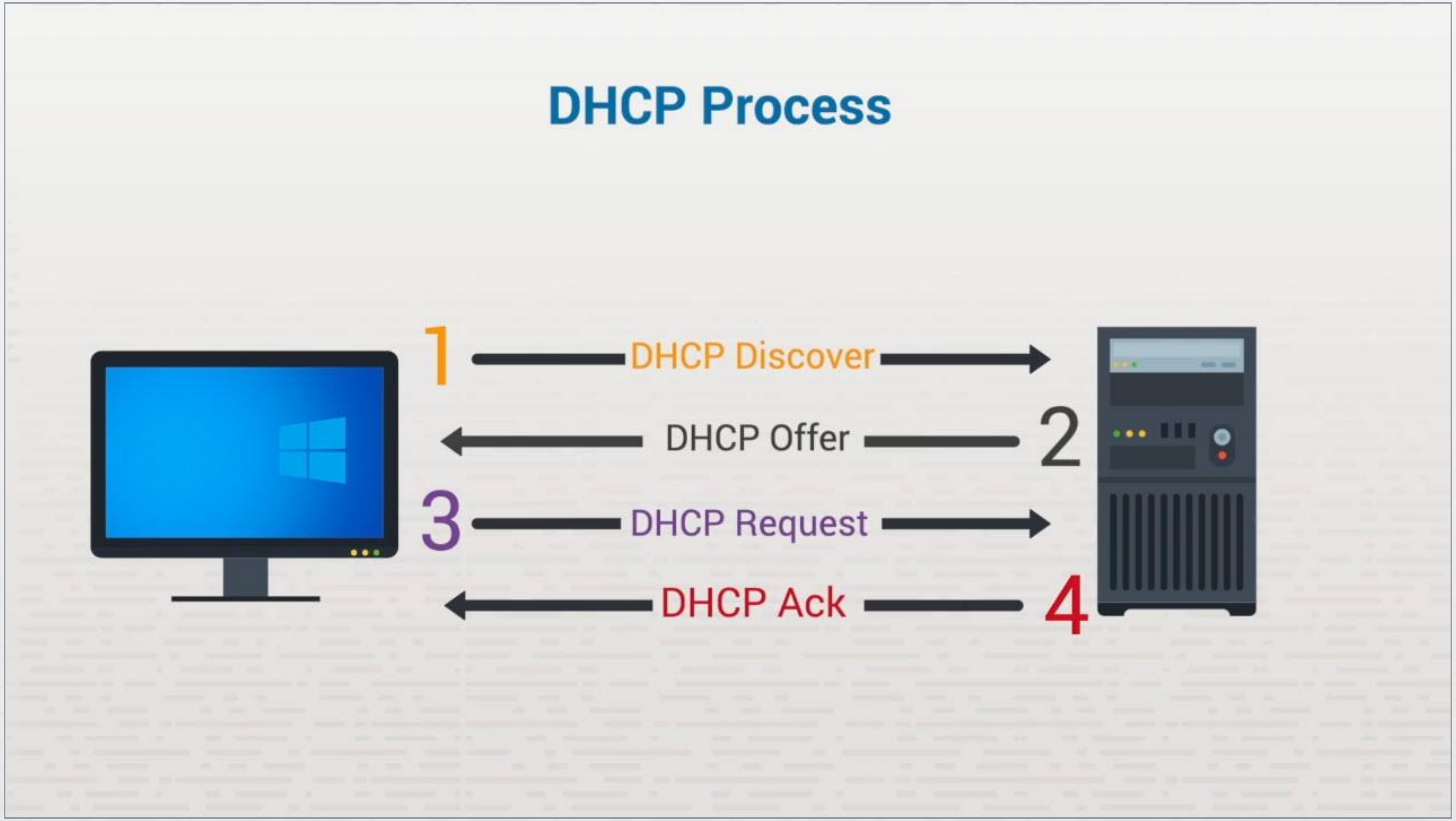
DHCP Scope	
IP range	192.168.5.50 – 192.168.5.100
Subnet mask	255.255.255.0
Exclusions	192.168.5.50 – 192.168.5.55
Reservations	22-EA-A9-67-51-64 → 192.168.5.56
DHCP lease time	4 days 12 hours

DHCP

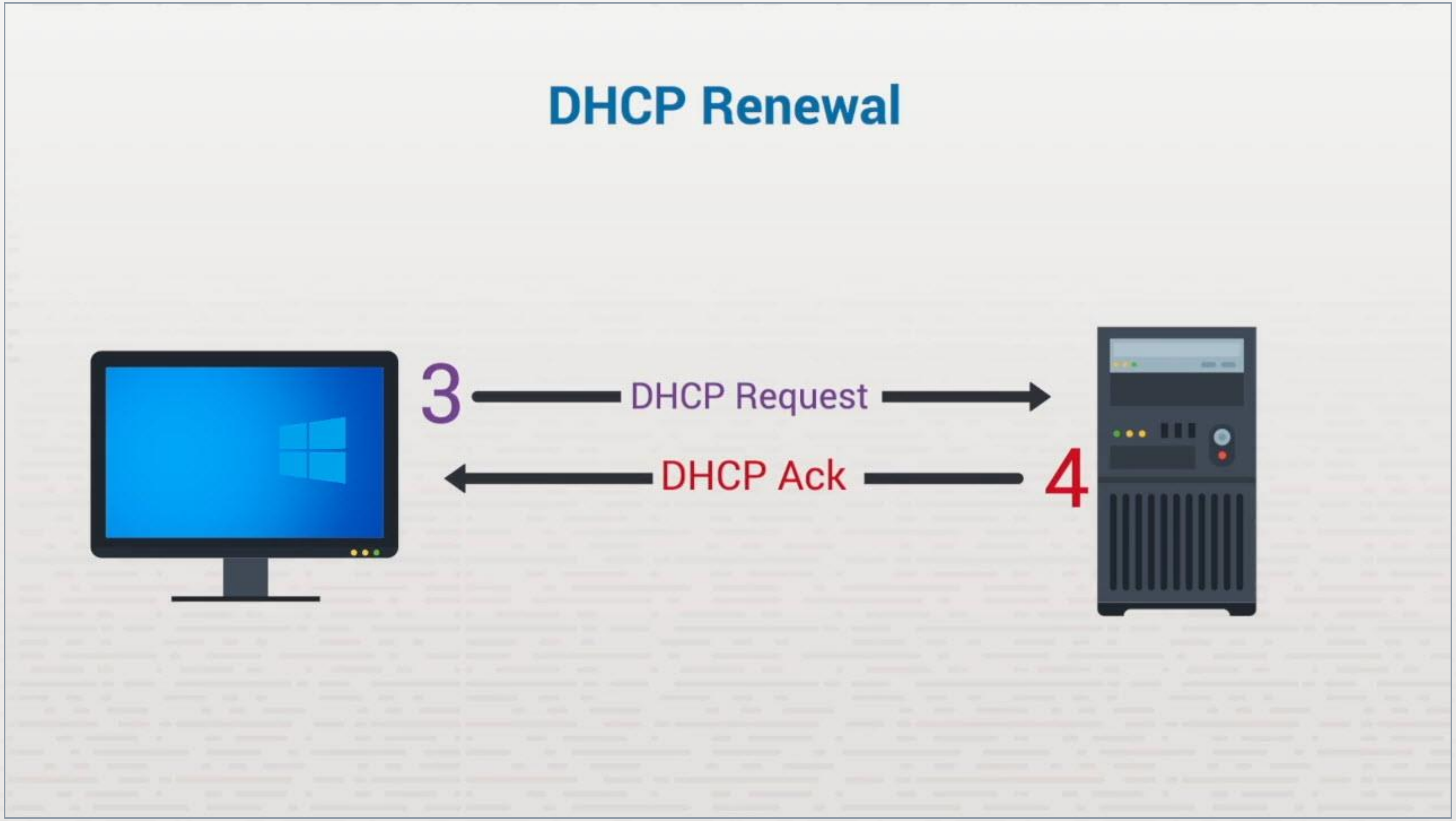
Additional Servers

DHCP Scope	
IP range	192.168.5.50 – 192.168.5.100
Subnet mask	255.255.255.0
Exclusions	192.168.5.50 – 192.168.5.55
Reservations	22-EA-A9-67-51-64 ➞ 192.168.5.56
DHCP lease time	4 days 12 hours
Default gateway	192.168.5.50
DNS server	8.8.8.8 and 8.8.4.4
WINS server	192.168.5.51

DHCP


DHCP Process
1
DHCP Discover
DHCP Offer
2
3
DHCP Request
DHCP Ack
4

DHCP



Summary

- DHCP's role
- DHCP configuration
- DHCP processes

In-Class Practice

Do the following labs:

- 4.3.4 Configure a DHCP Server
- 4.3.6 Configure DHCP Options
- 4.3.7 Create DHCP Exclusions
- 4.3.8 Create DHCP Client Reservations

Class Discussion

- What type of configuration parameters can be delivered using DHCP?
- What is a DHCP scope?
- What type of devices can be used as a DHCP server?
- What are the advantages of static IP address assignments?
- When might you want to use static IP addressing?

DHCP Relay

Key Terms

- DHCP relay agent
- IP helper

Key Definitions

- **DHCP relay agent:** A network device used to forward DHCP requests to a DHCP server located on another network.
- **IP helper:** Performs the same actions as a DHCP relay agent except that it does so for other UDP-based protocols, such as NTP.

DHCP Relay

DHCP Relay

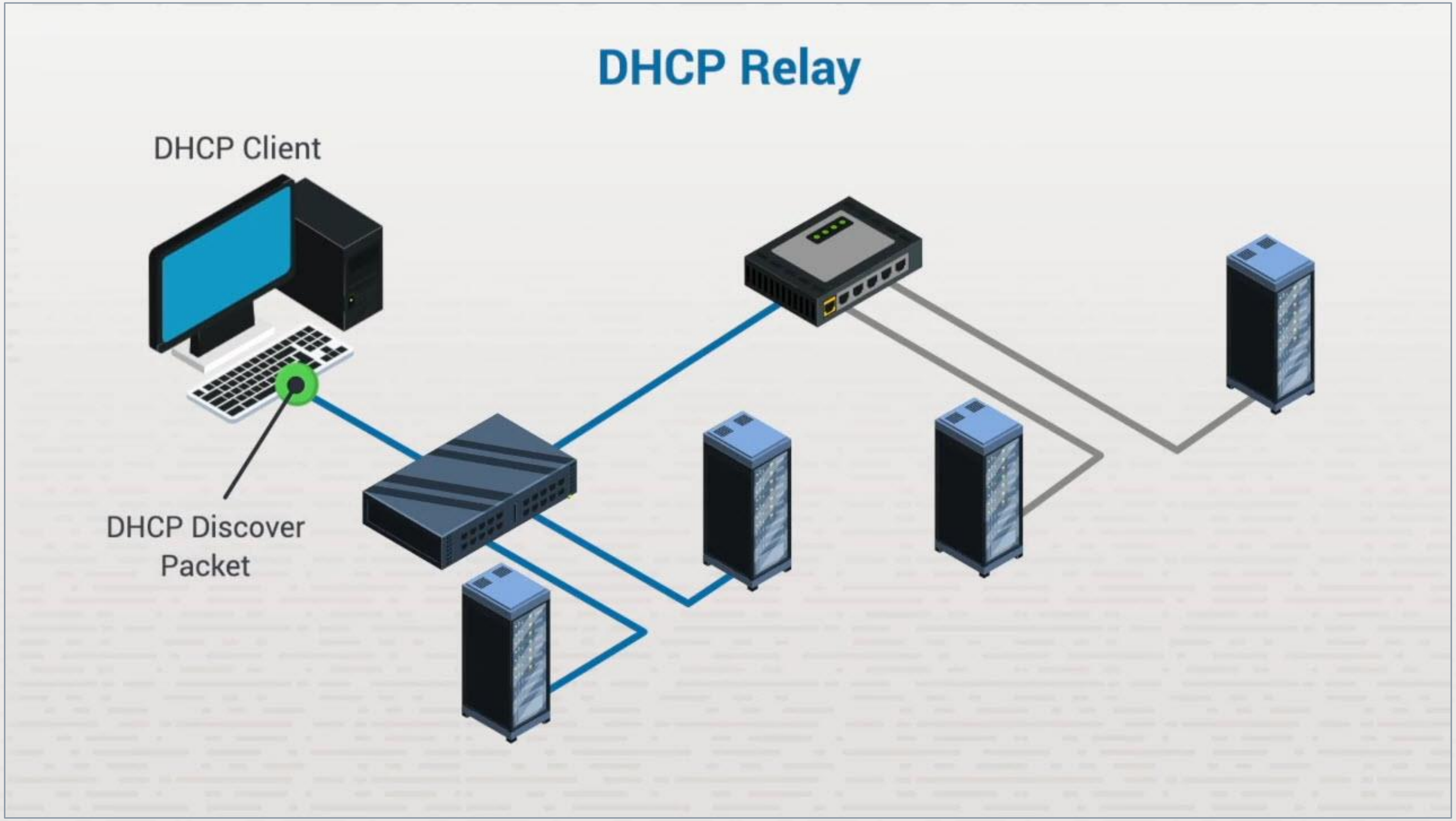
DHCP Servers
Office 1
Office1
Hardware
Office 2
Office2
Hardware
IT Administration
IT-Laptop
ITAdmin
Hardware
Executive Office
Exec
Exec-Laptop
Hardware
Lobby
Gst-Lap
Hardware
Support Office
Support
Hardware

DHCP Relay

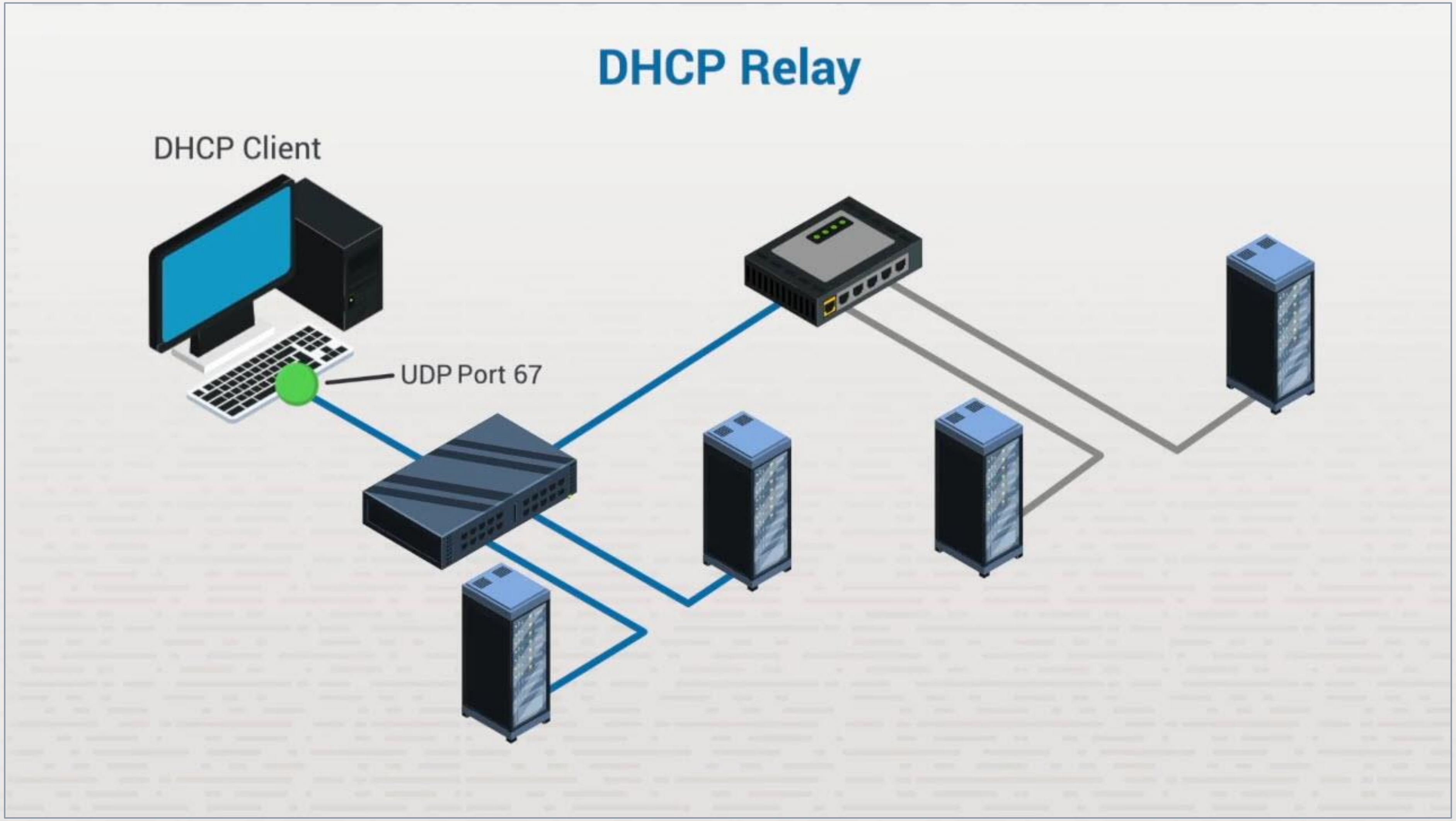
DHCP Relay

- DHCP relay agent
- IP helper

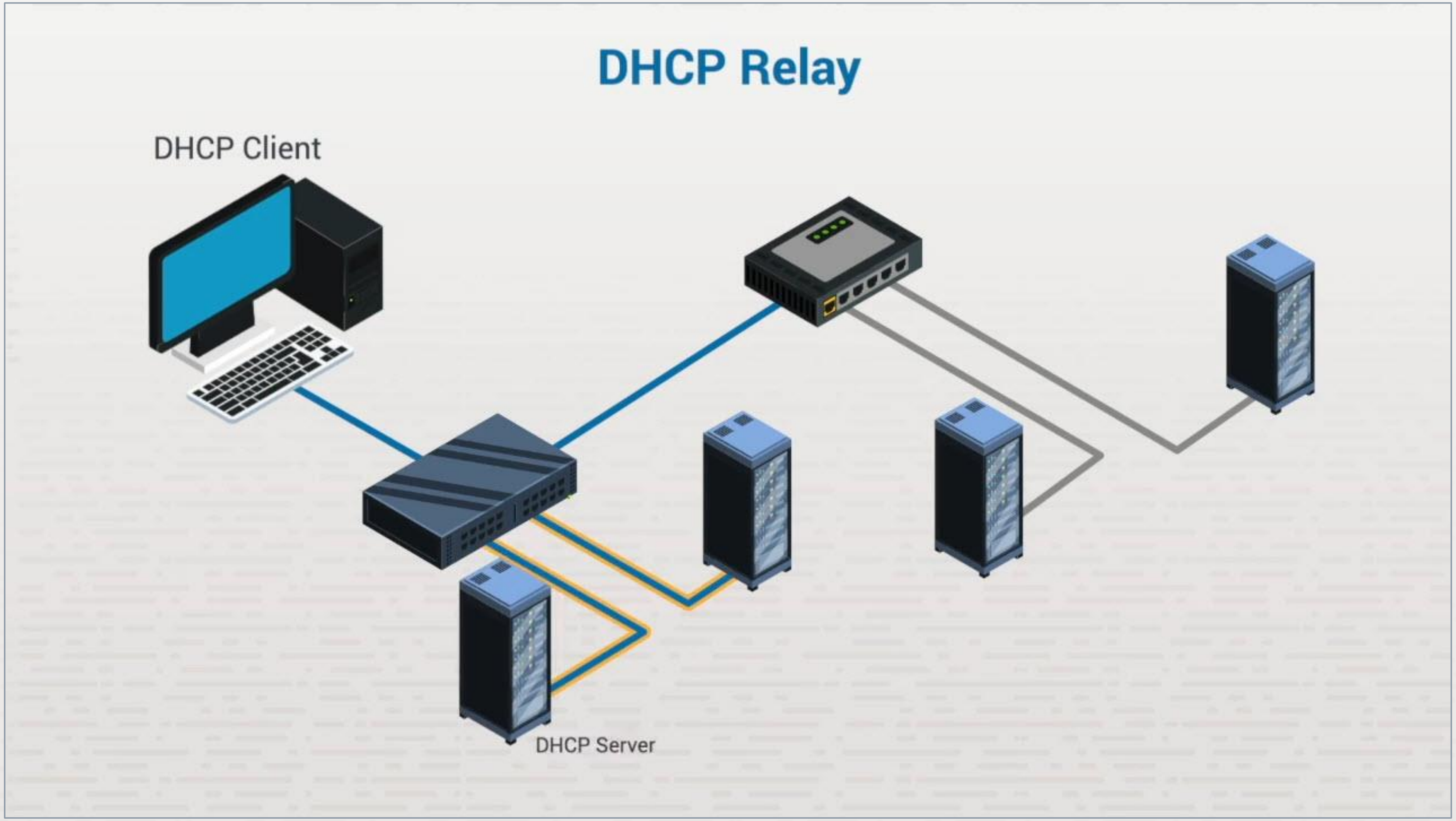
DHCP Relay



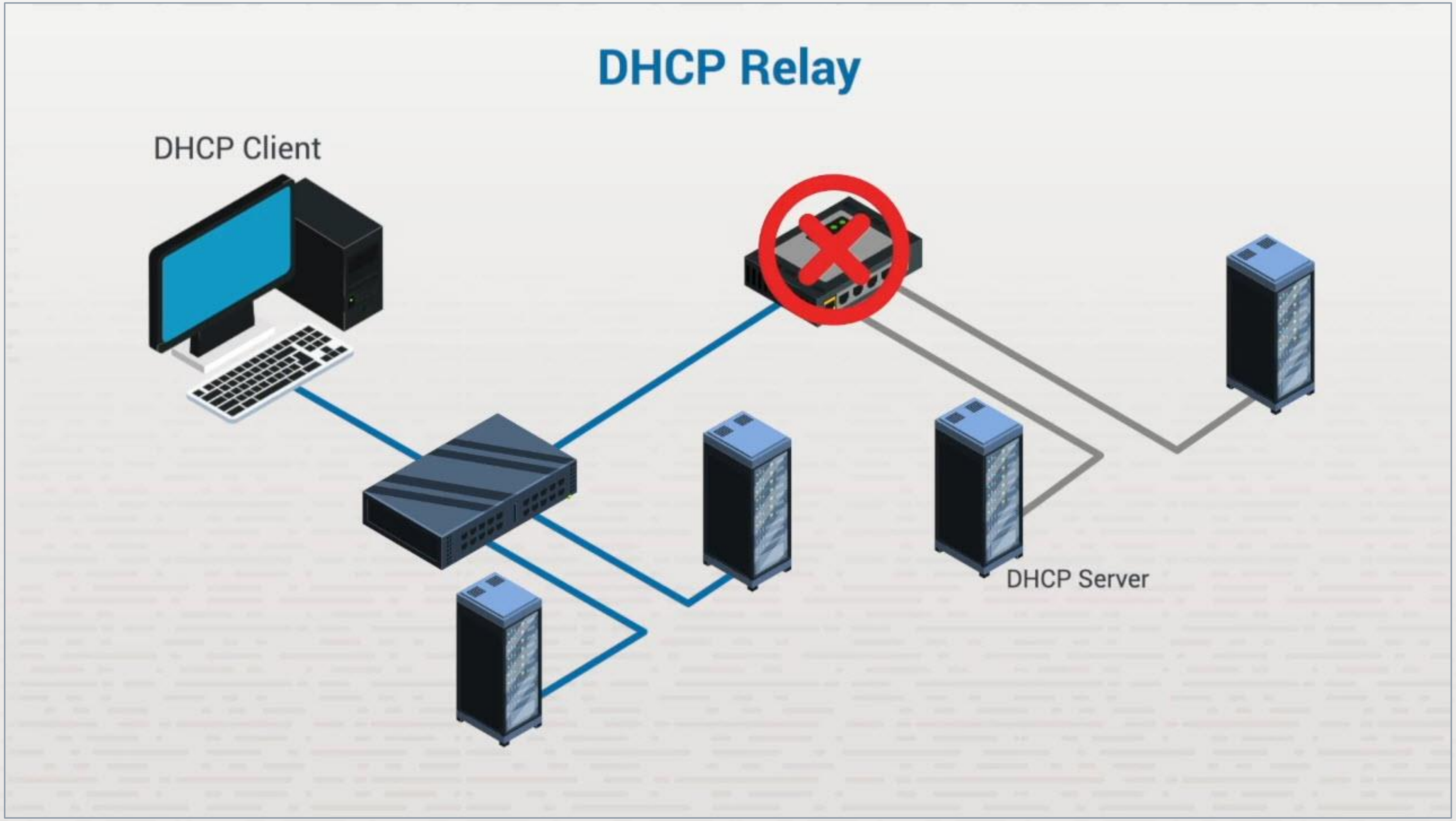
DHCP Relay



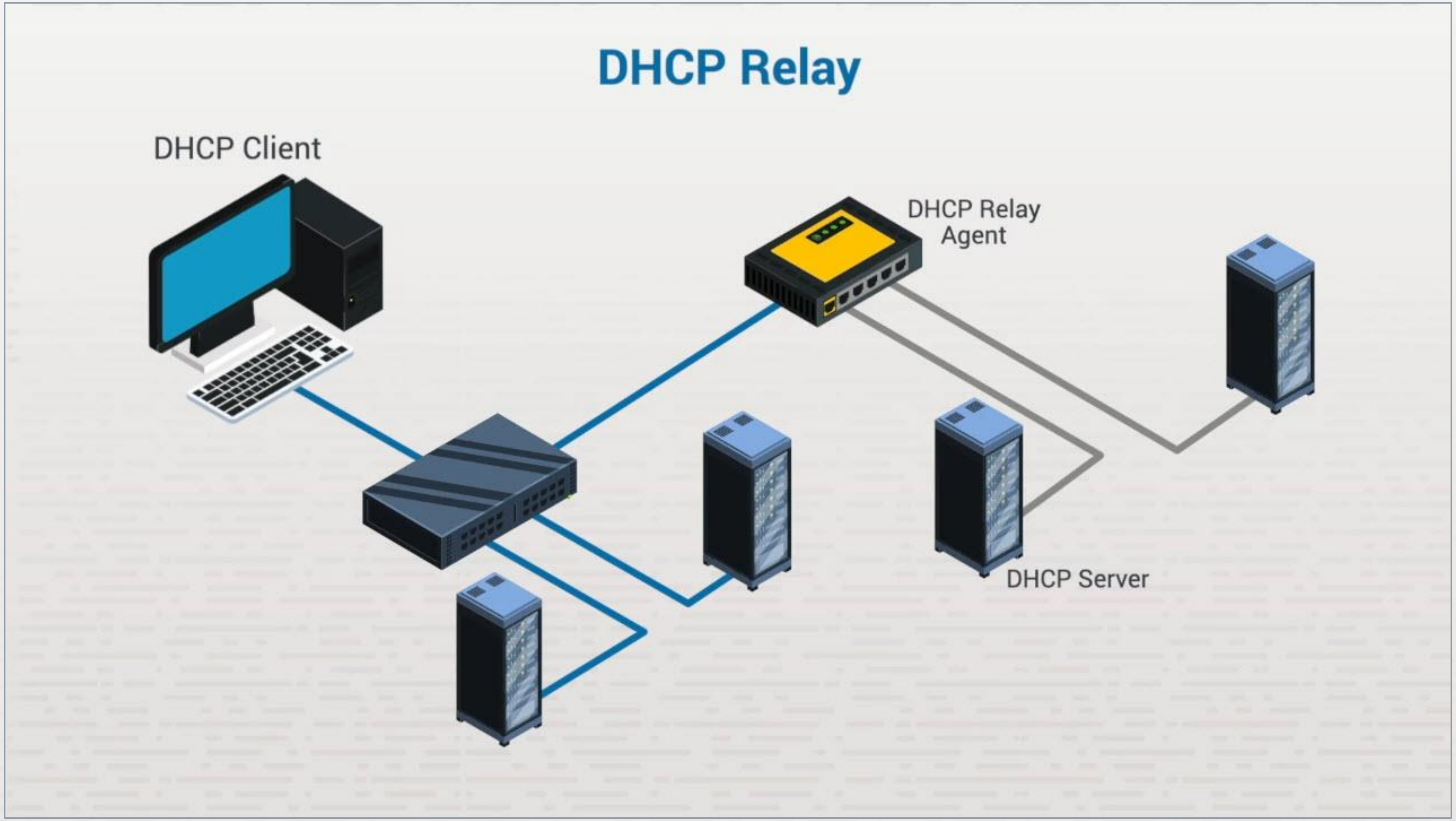
DHCP Relay



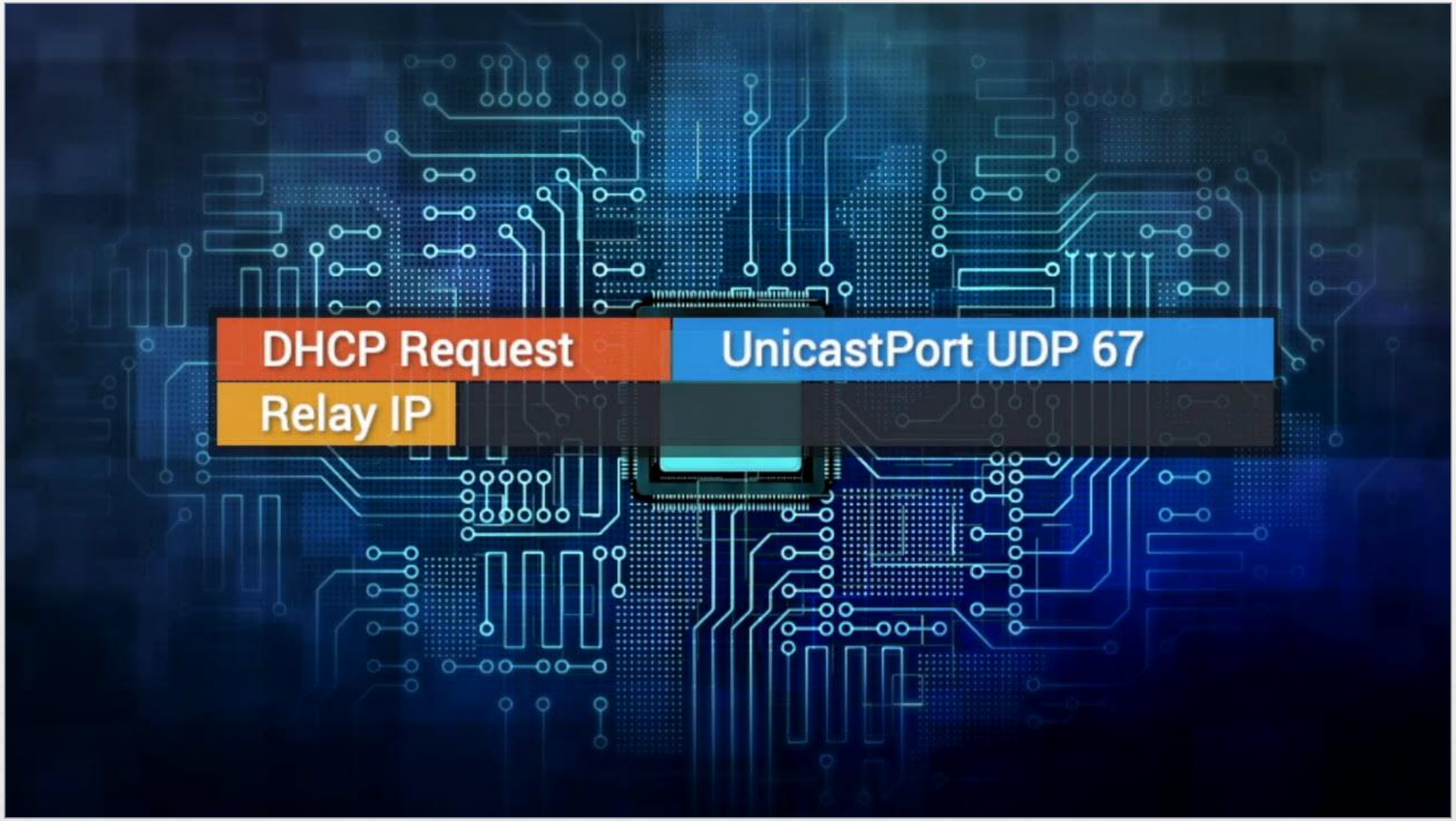
DHCP Relay



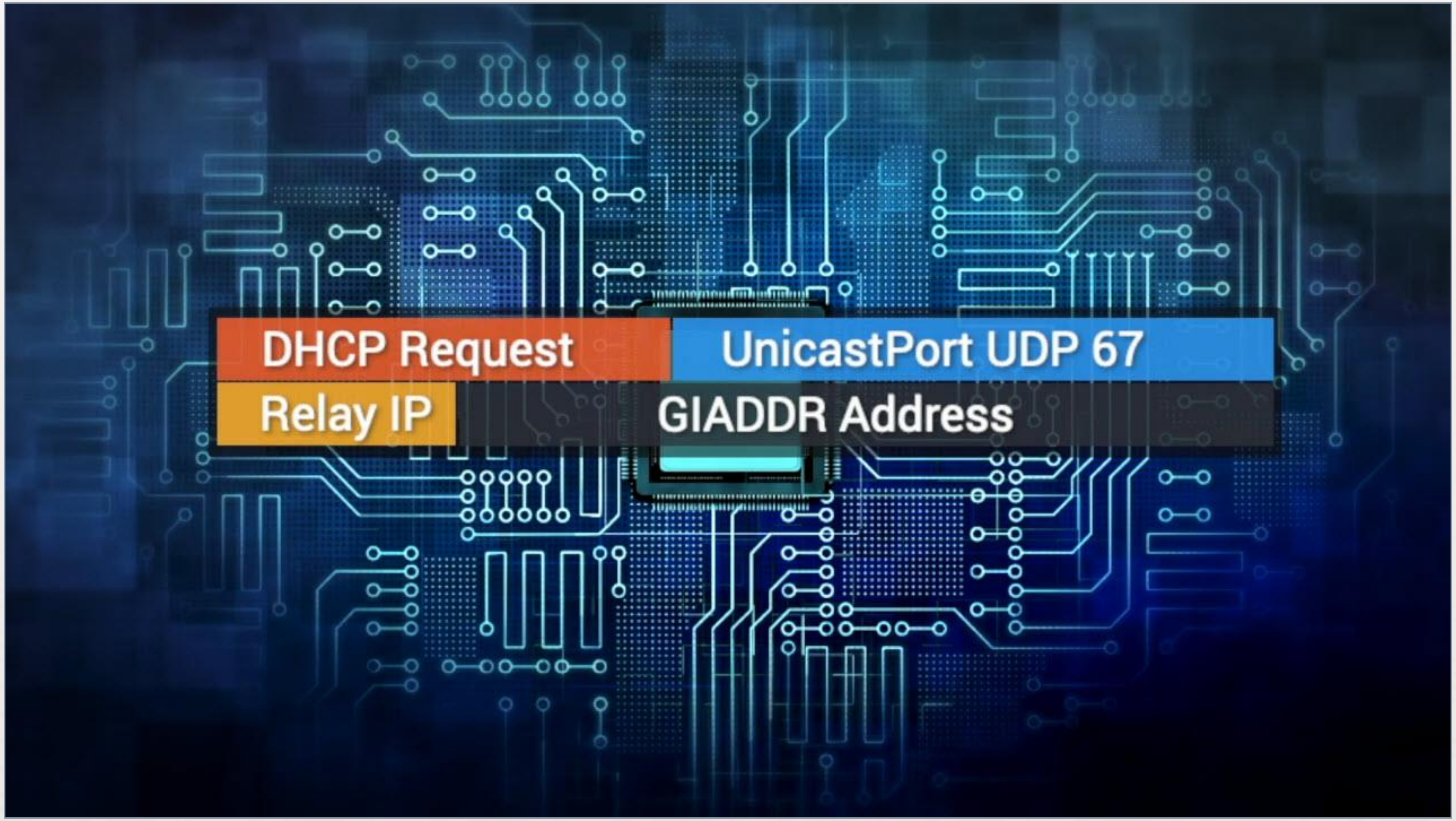
DHCP Relay



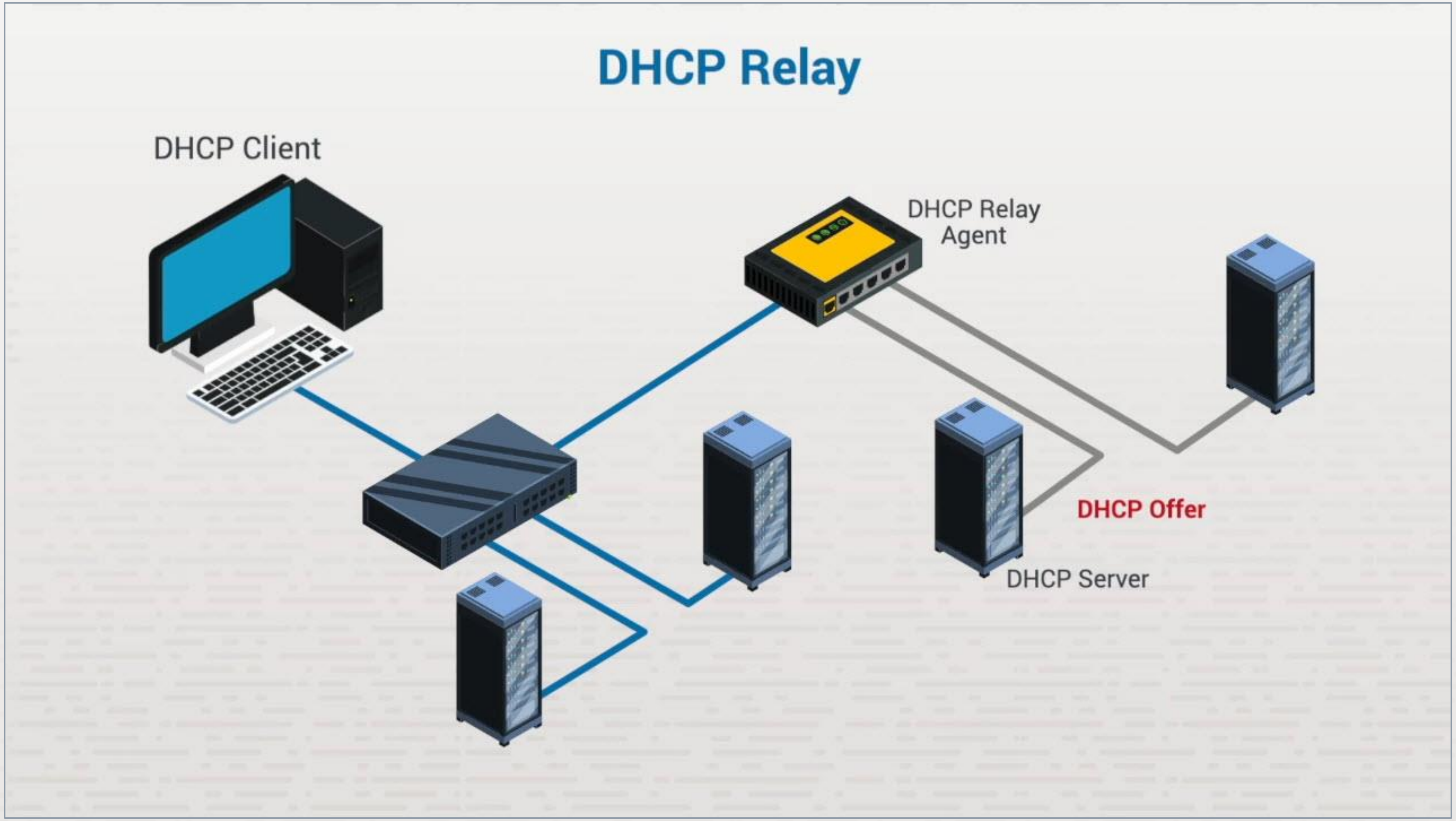
DHCP Relay



DHCP Relay

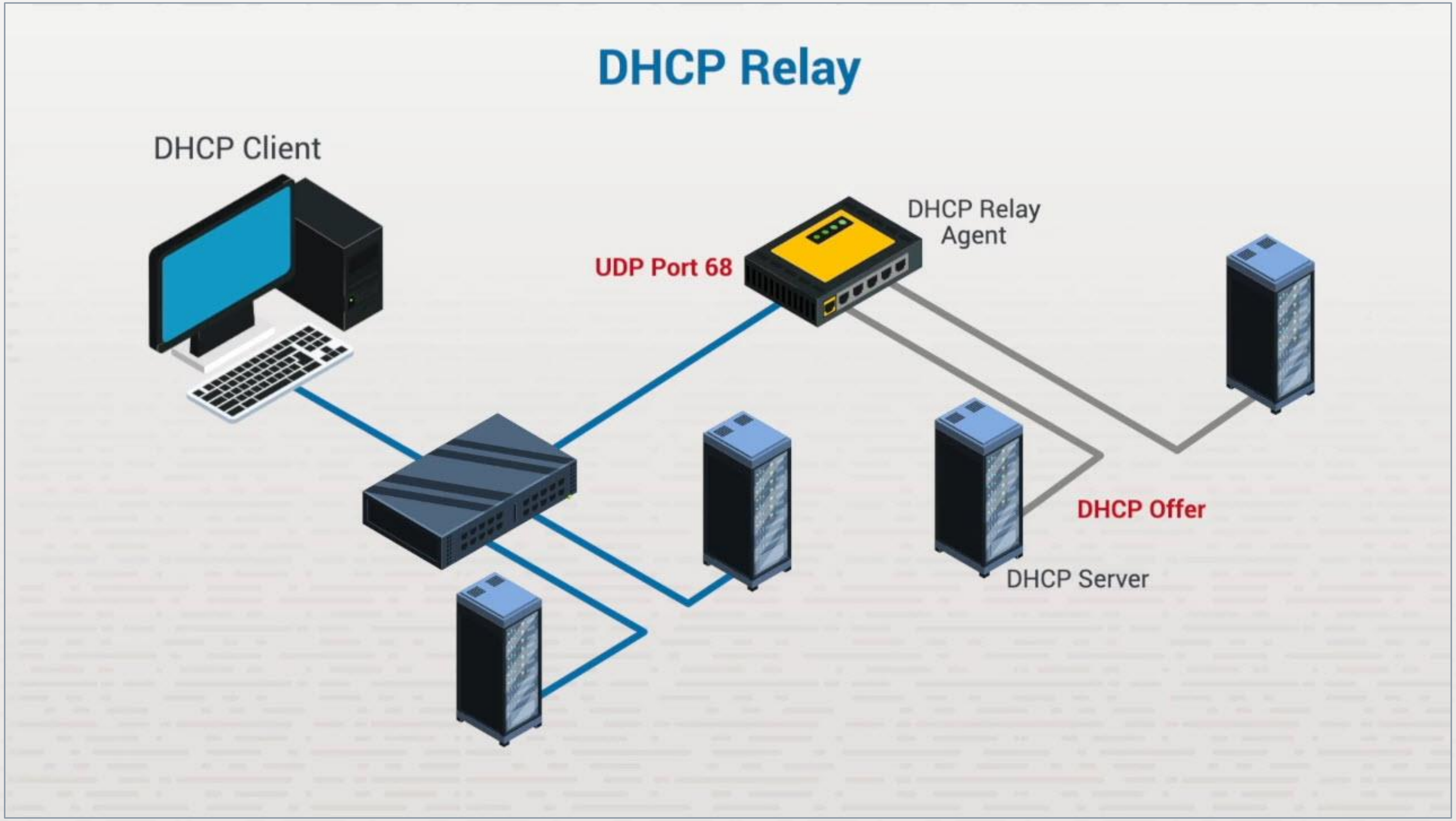


DHCP Relay

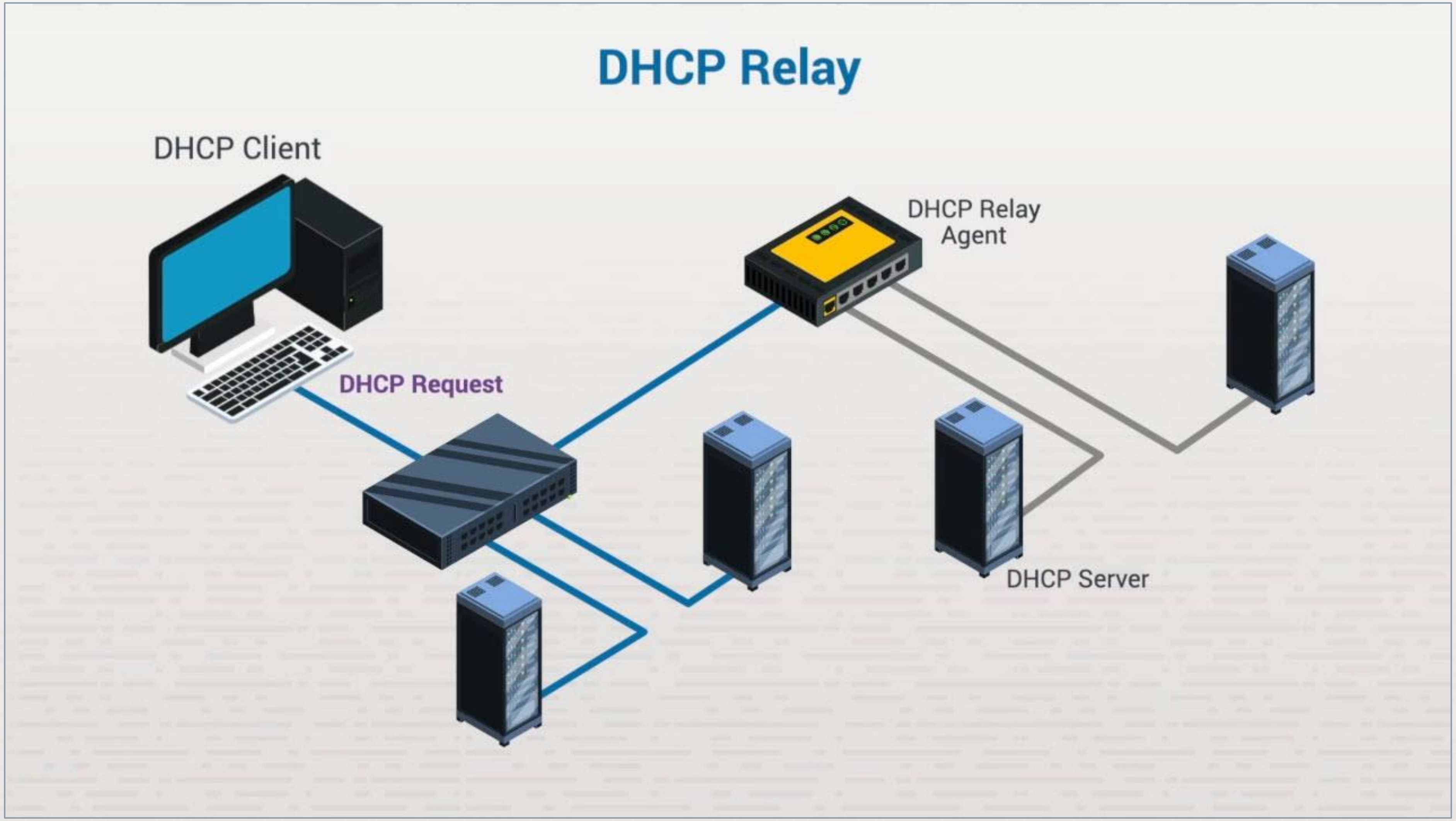


DHCP Relay
DHCP Client
DHCP Relay Agent
DHCP Offer
DHCP Server

DHCP Relay

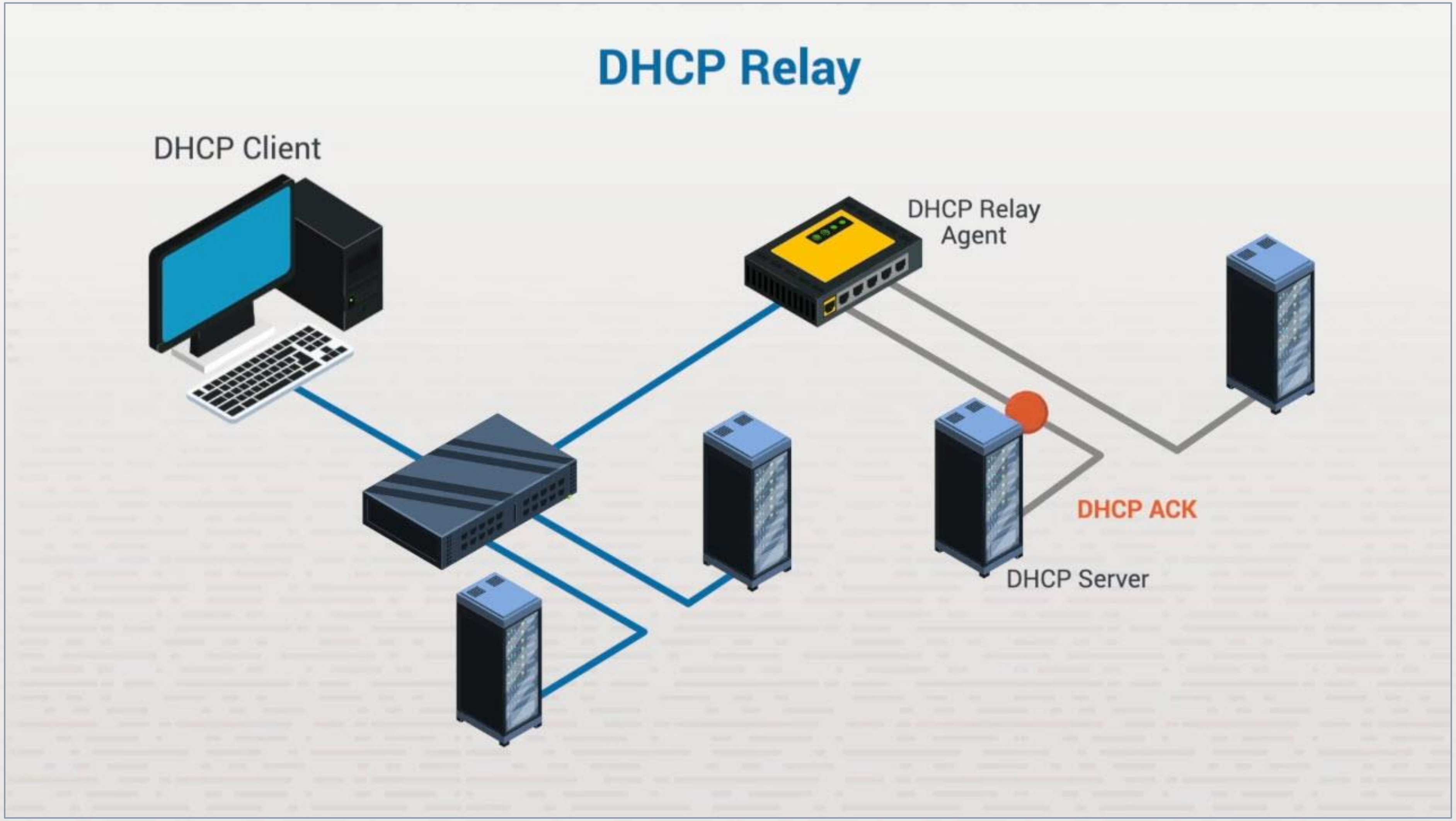

DHCP Relay
DHCP Client
UDP Port 68
DHCP Relay Agent
DHCP Offer
DHCP Server

DHCP Relay

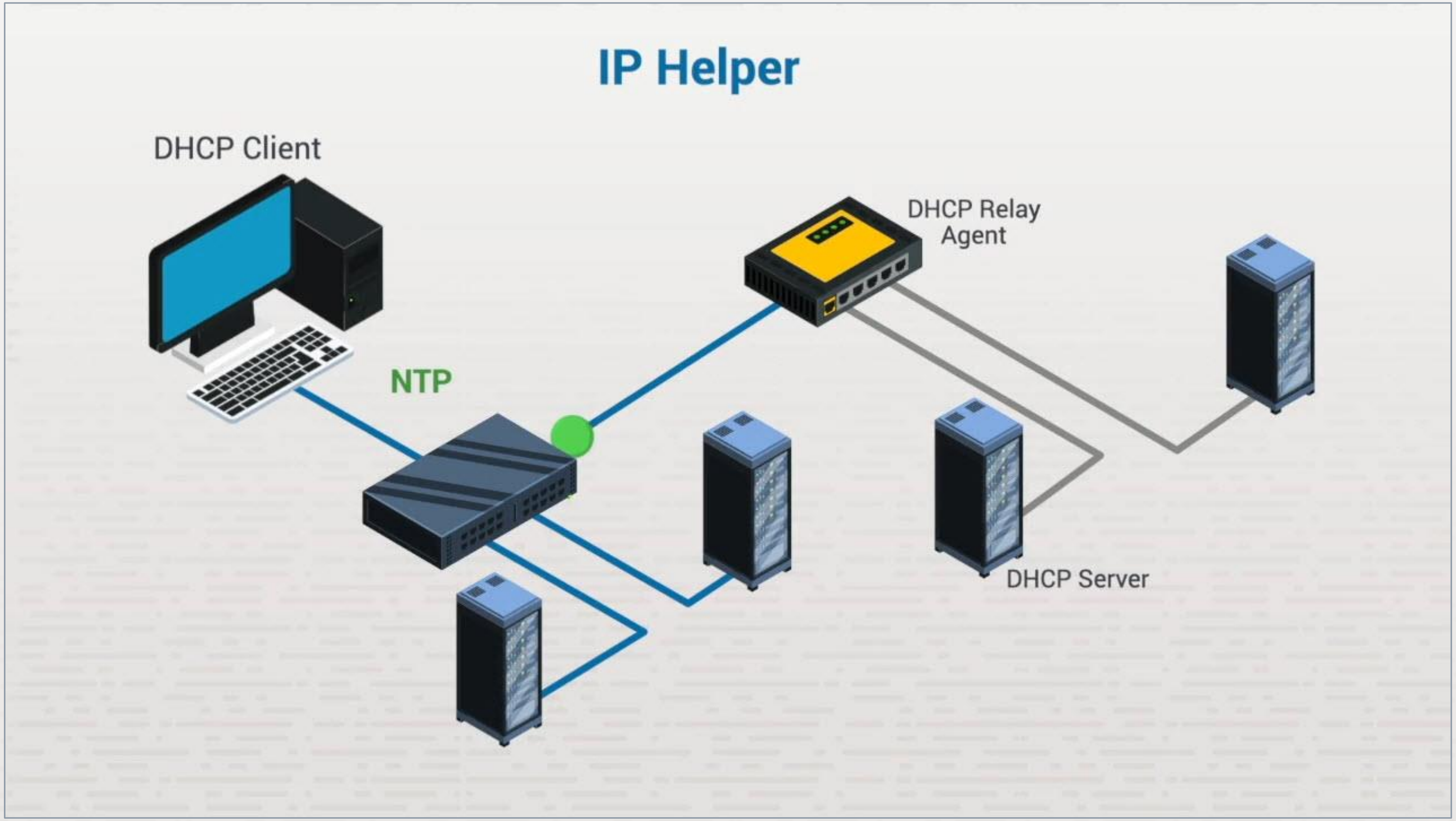


DHCP Relay
DHCP Client
DHCP Relay
Agent
DHCP Request
DHCP Server

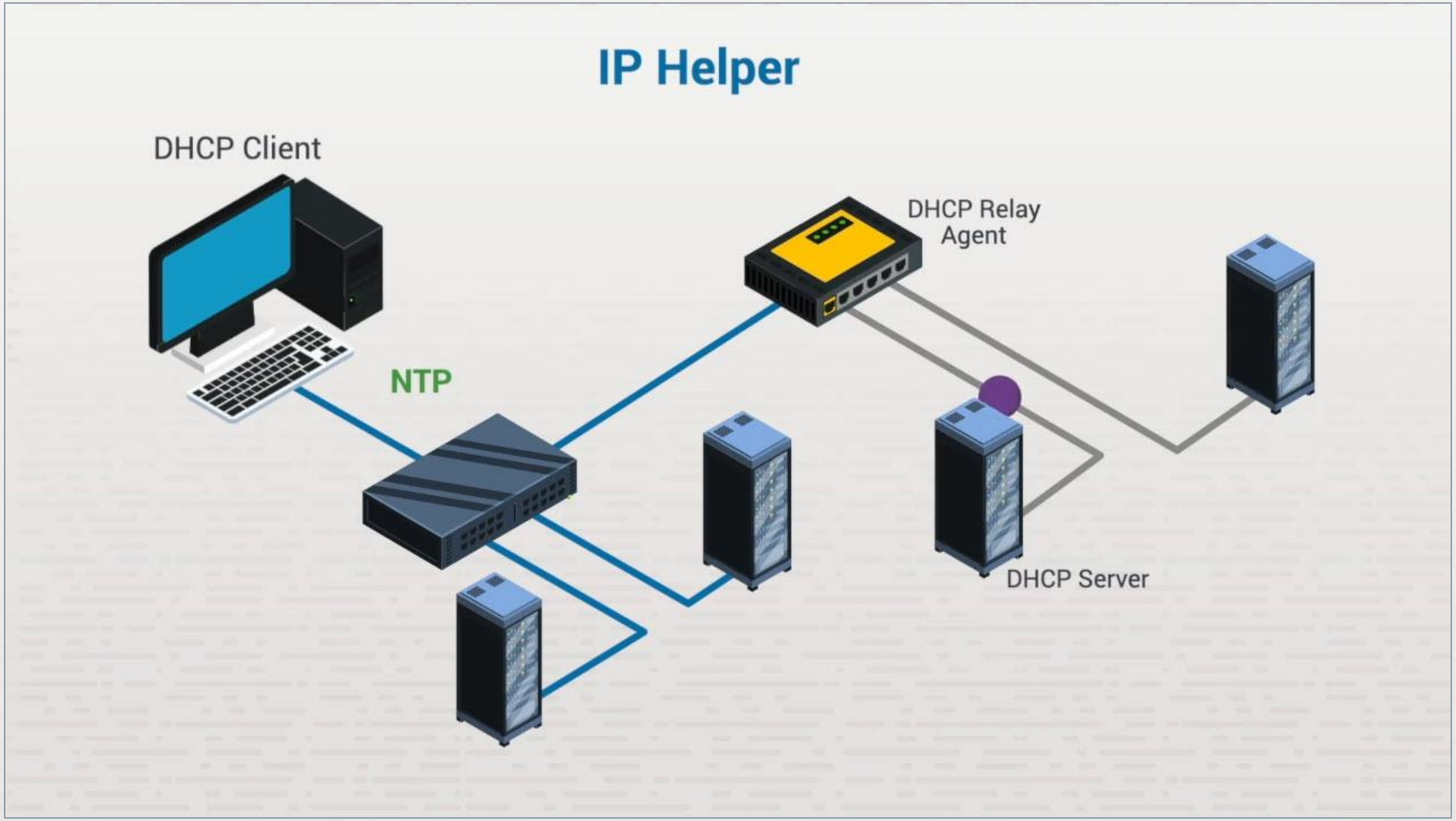
DHCP Relay


DHCP Relay
DHCP Client
DHCP Relay
Agent
DHCP ACK
DHCP Server

DHCP Relay



DHCP Relay



TestOut

Summary

- DHCP relay agent
- IP helper

In-Class Practice

Do the following labs:

- 4.4.4 Configure a DHCP Relay Agent
- 4.4.5 Add a DHCP Server on Another Subnet

Class Discussion

- What is the purpose of a DHCP relay agent?
- What is the purpose of an IP helper? How does it differ from a DHCP relay agent?
- What is a DHCP Discover packet?
- How do you configure a DHCP relay agent?
- How do you add a DHCP server on another subnet?

DNS

Section Skill Overview

- Configure DNS addresses
- Create standard DNS zones
- Create host records
- Create CNAME records
- Troubleshoot DNS records

Key Terms

- Fully qualified domain name (FQDN)
- DNS zone
- Forward lookup zone
- Reverse lookup zone
- Records
- Root server

Key Terms

- Top-level domain (TLD) server
- Authoritative name server
- Recursive server
- HOSTS file
- Dynamic DNS (DDNS)

Key Definitions

- **Fully qualified domain name (FQDN):** A domain name that spells out each level of the hierarchy separated by periods. The final period (which is for the root domain) is often omitted and only implied.
- **DNS zone:** The administrative portion of the DNS namespace used to maintain and define the domain namespace.
- **Forward lookup zone:** The portion of the DNS namespace that resolves the hostname to the IP address.
- **Reverse lookup zone:** The portion of the DNS namespace that resolves the IP address to the hostname.

Key Definitions

- **Records:** Database entries that store information. For DNS, the records store hostnames, IP addresses, etc. in the zone database. Each host has at least one record in the DNS database that maps the hostname to the IP address.
- **Root server:** Servers that hold information for the root zone (.). Root servers answer name resolution requests by supplying the address of the corresponding top-level DNS server.
- **Top-level domain (TLD) server:** Servers that contain the information for all websites that share a common domain extension, such as .com or .org.

Key Definitions

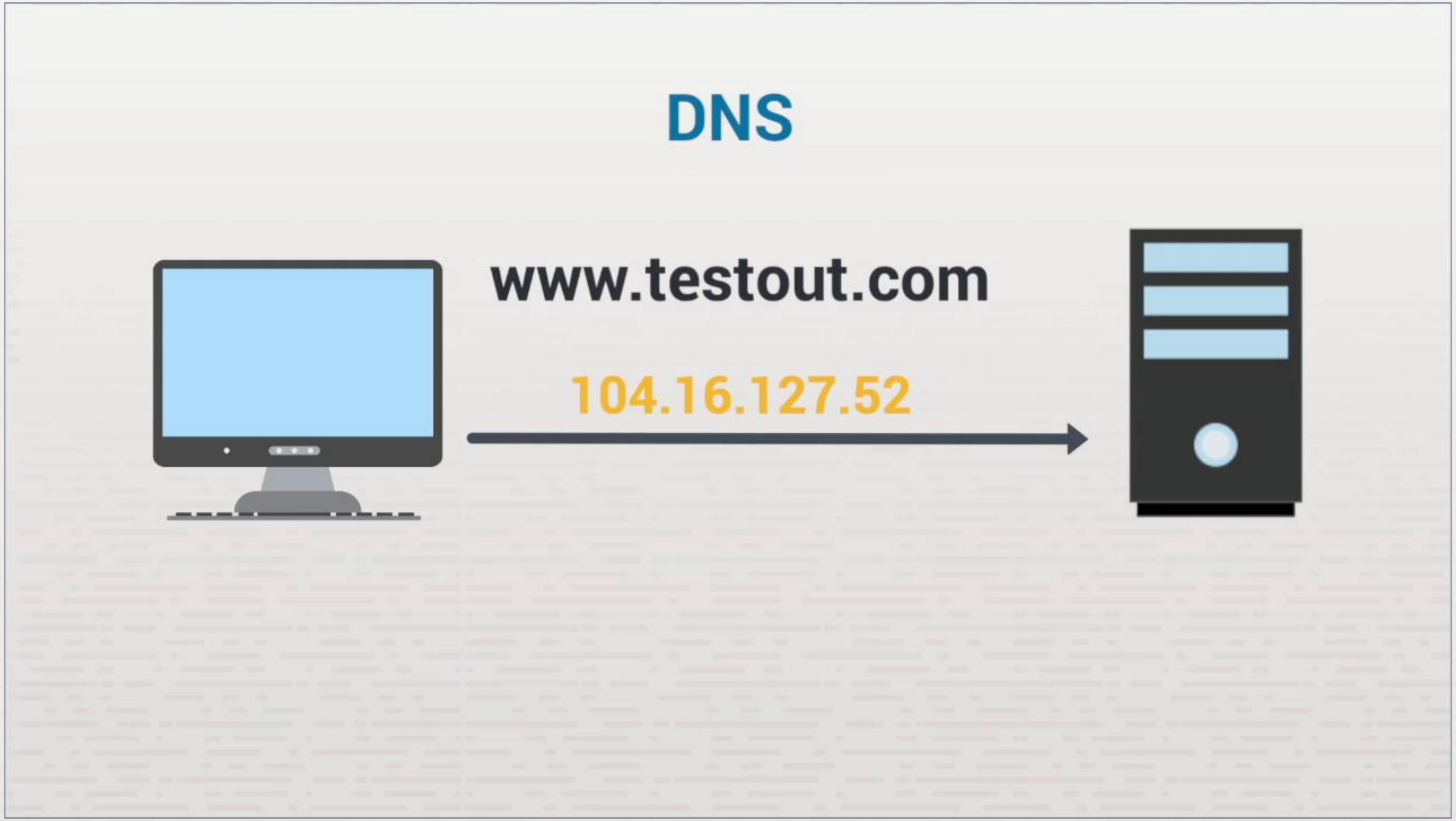
- **Authoritative name server:** A server that contains the DNS information for a site. The server is authoritative because it doesn't have to ask any other DNS server for help because it holds the information already.
- **Recursive server:** A server that handles the DNS name resolution process.
- **HOSTS file:** A local text file on each computer that maps hostnames to IP addresses.

Key Definitions

- **Dynamic DNS (DDNS):** A method that enables clients or the DHCP server to update records in the zone database. Without dynamic updates, all A (host) and PTR (pointer) records must be configured manually. With dynamic updates, host records are created and deleted automatically whenever the DHCP server creates or releases an IP address lease.

DNS - Record Types

DNS - Record Types

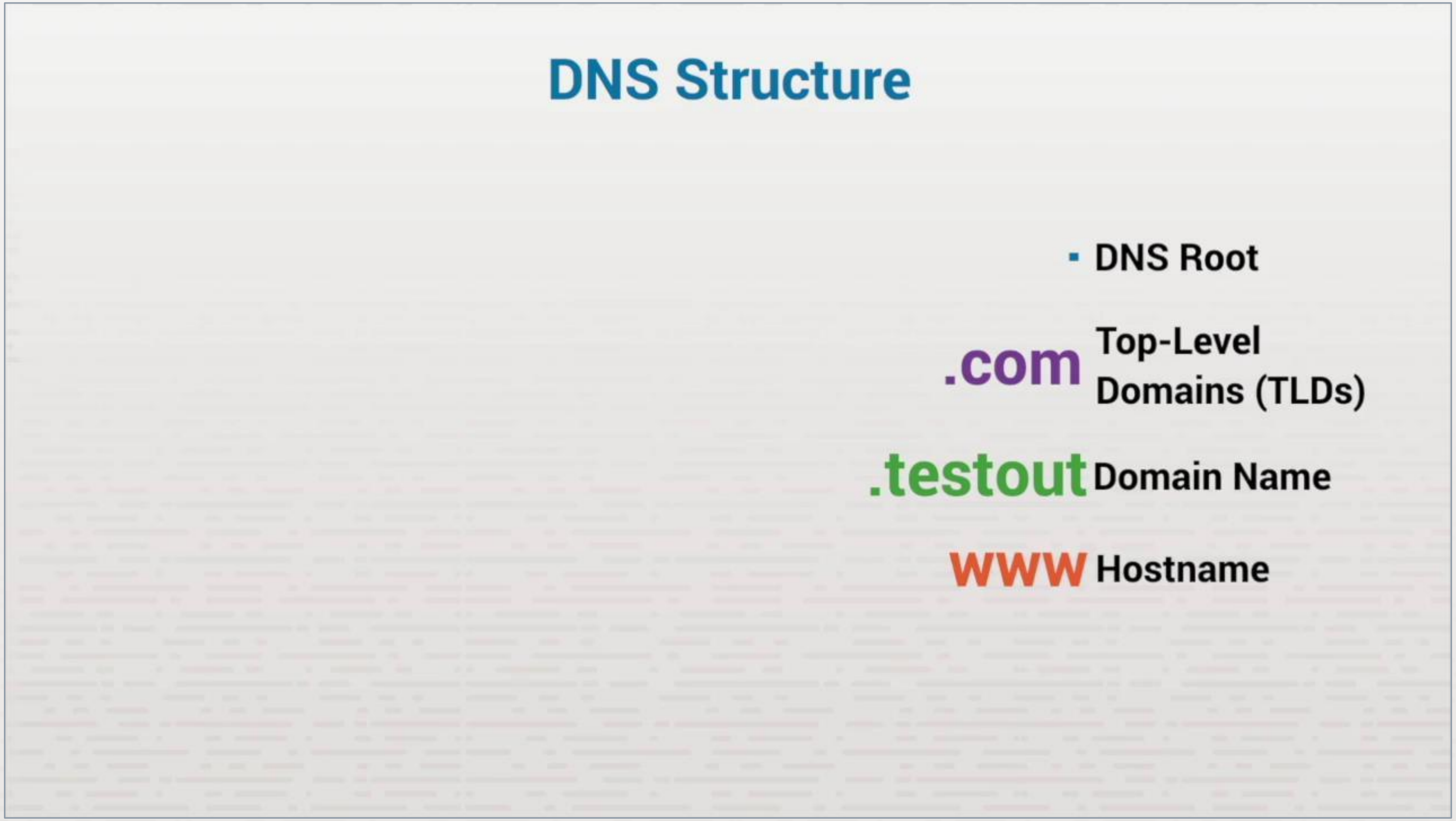


DNS

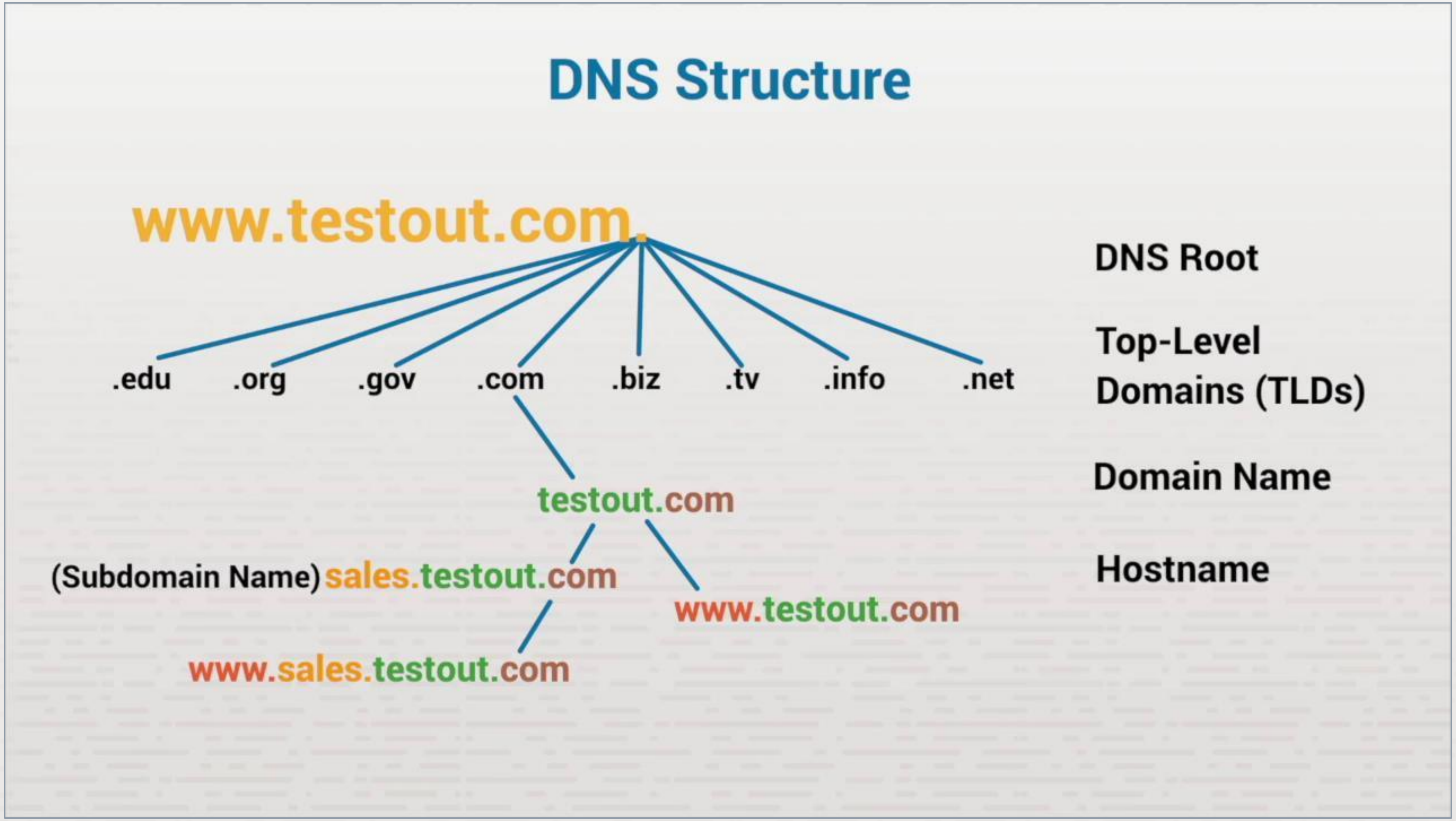
- DNS structure
- DNS process
- DNS records

DNS - Record Types

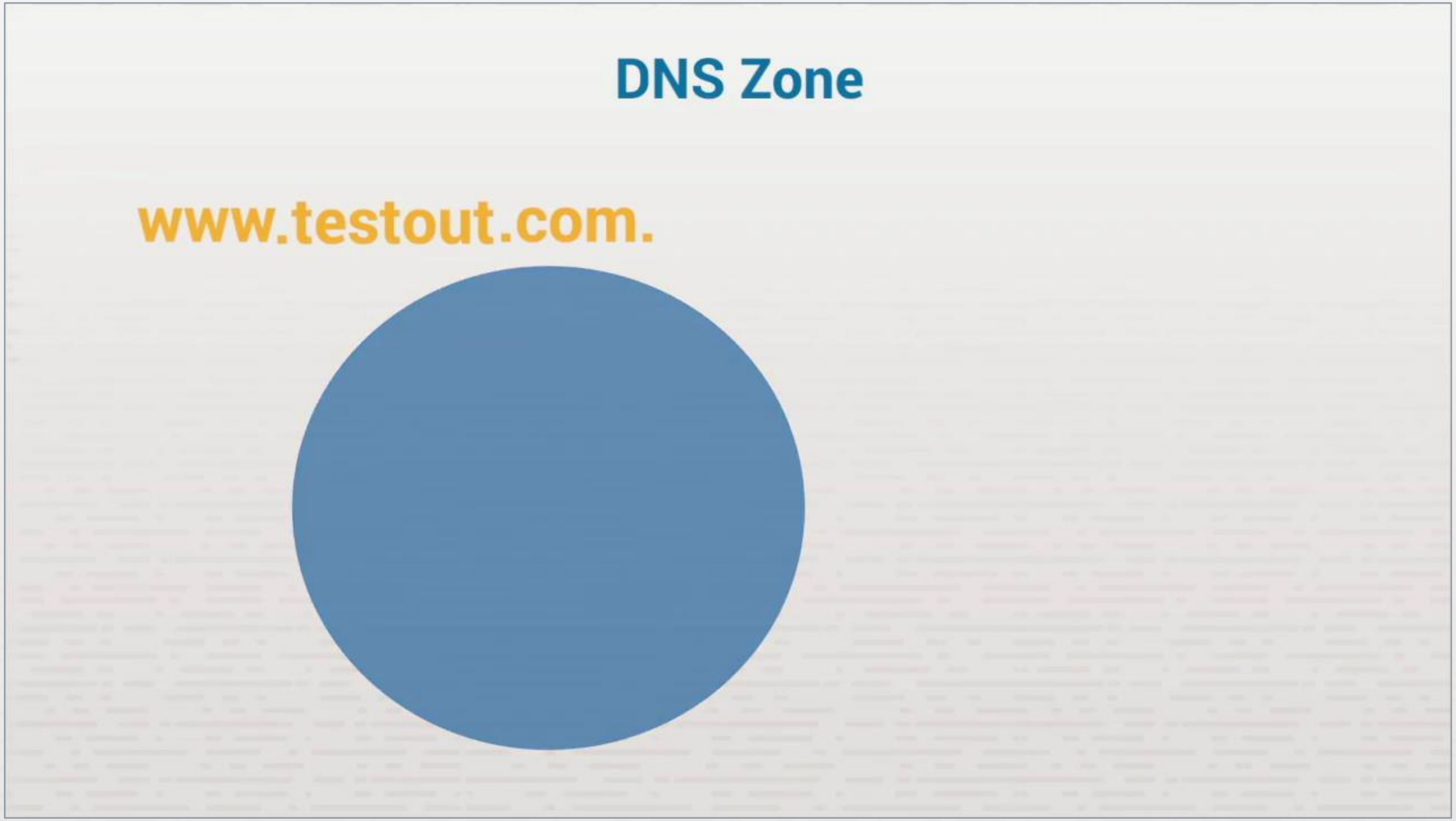
DNS - Record Types



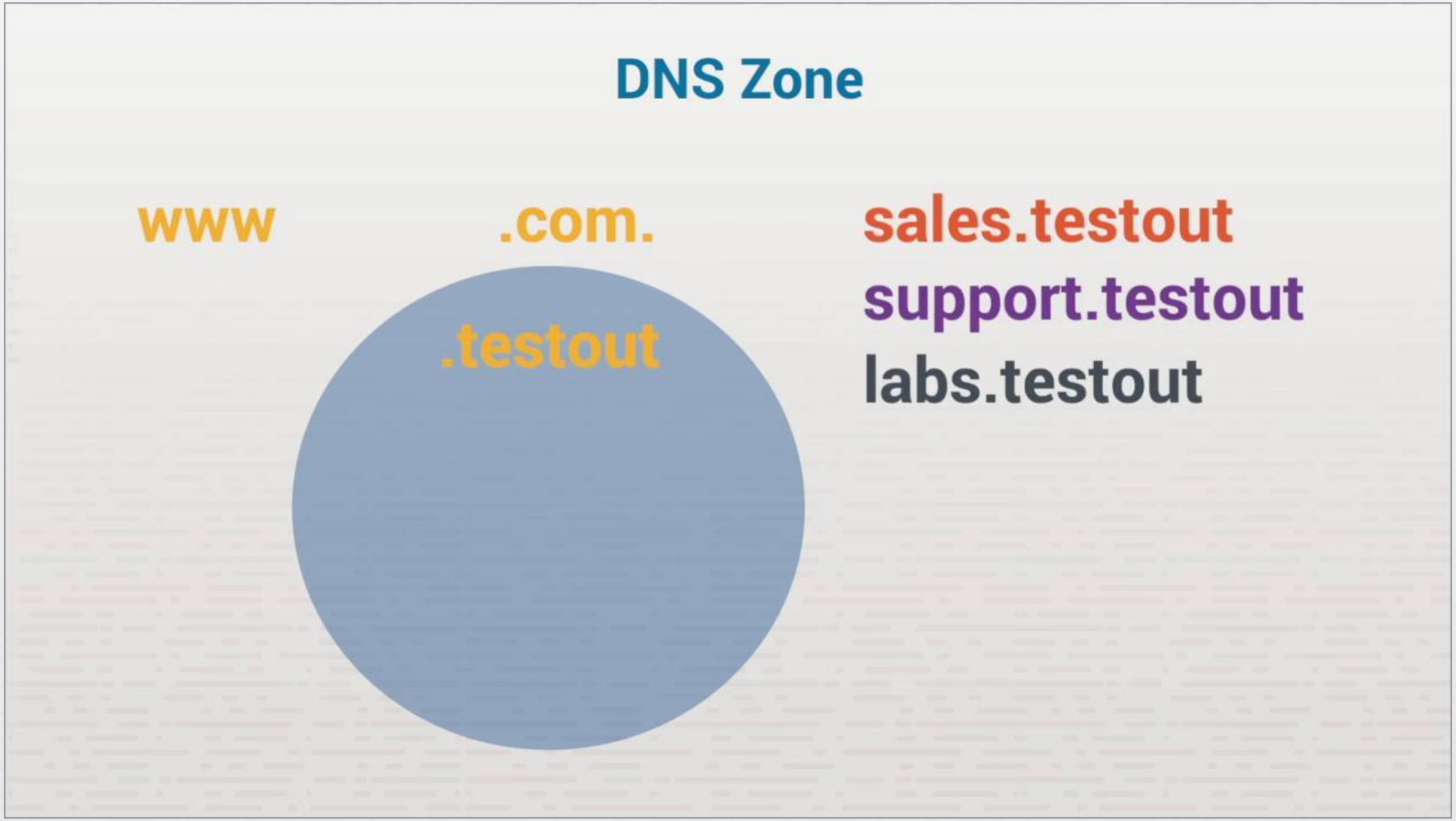
DNS - Record Types



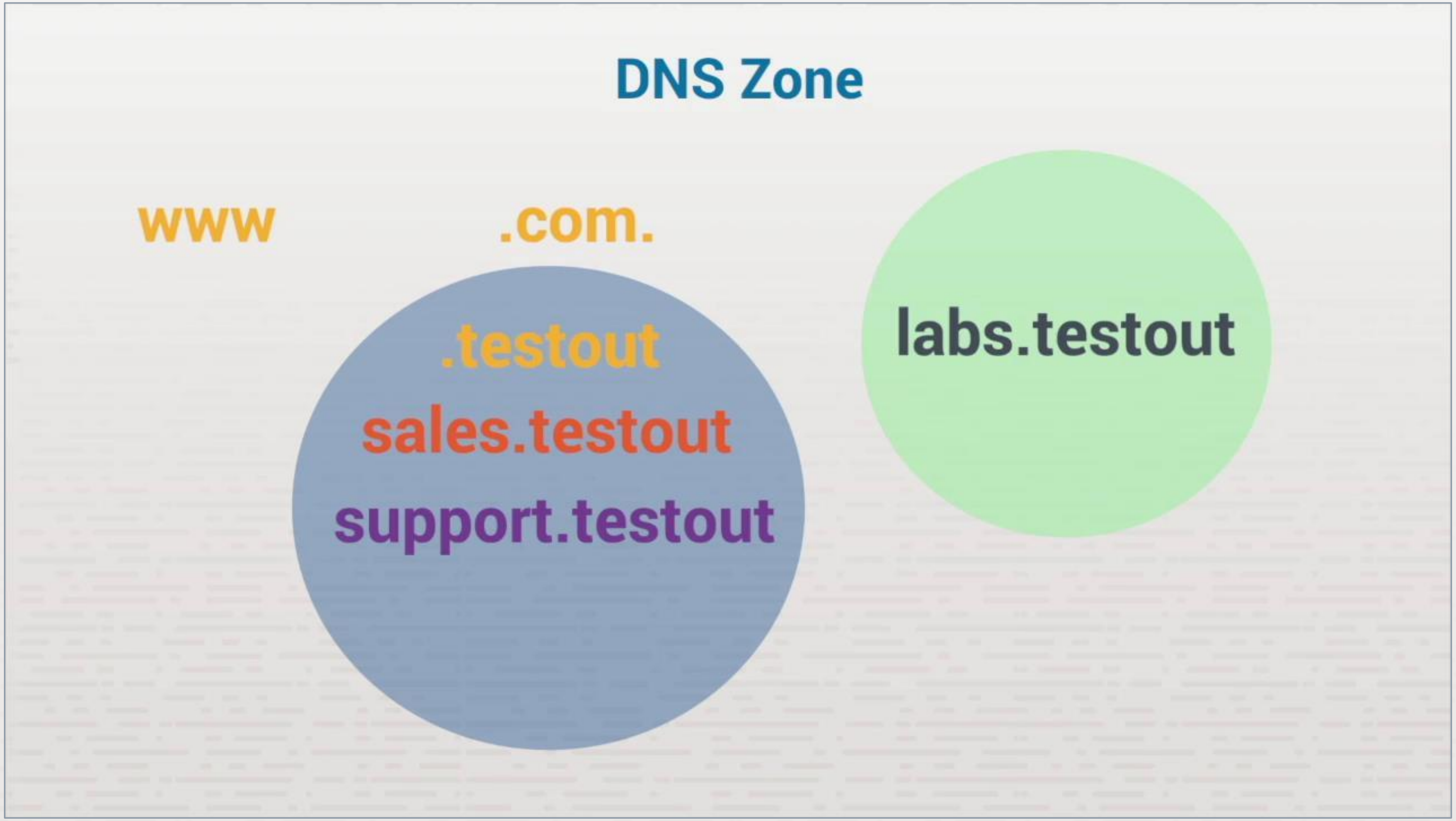
DNS - Record Types



DNS - Record Types



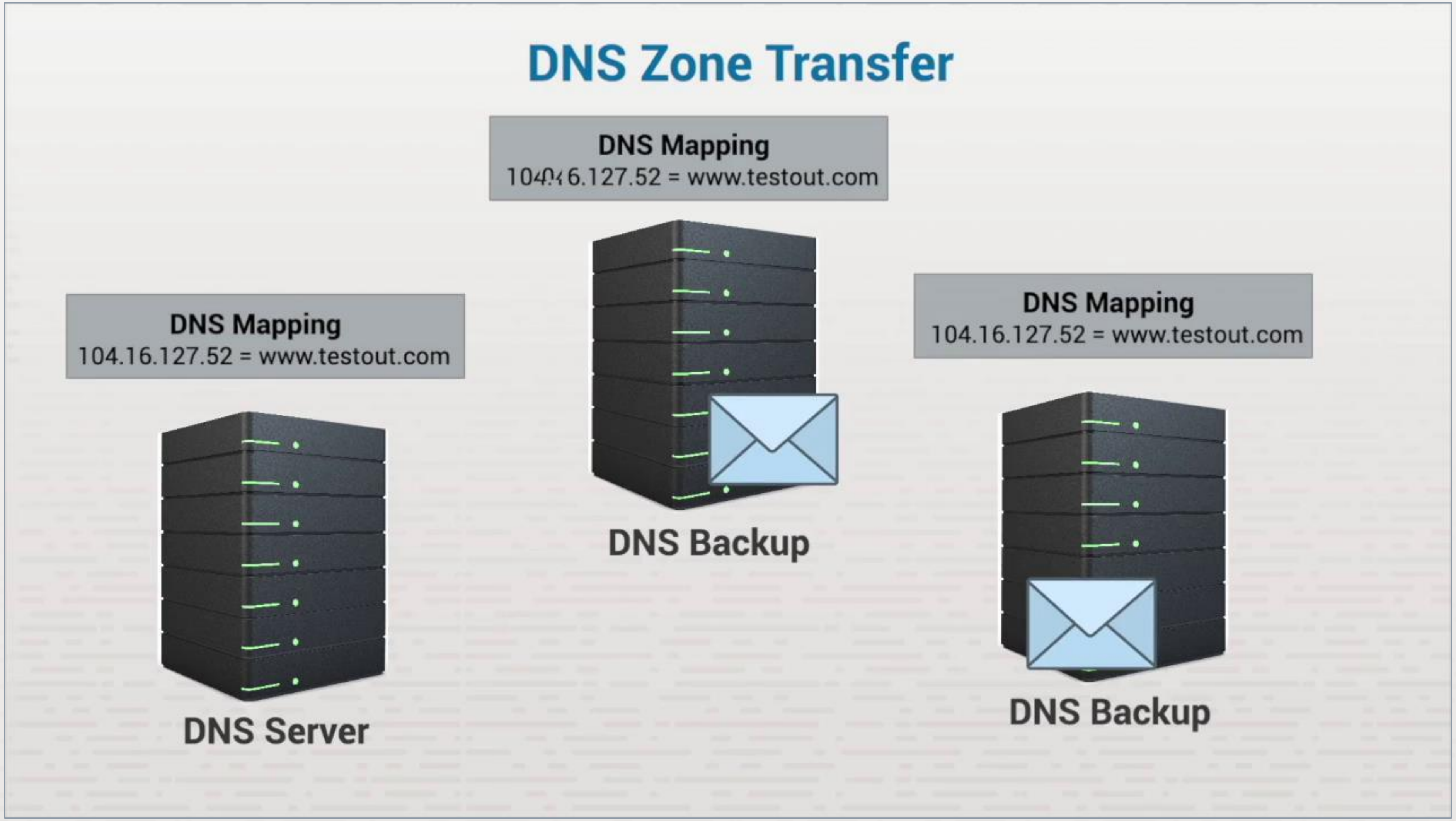
DNS - Record Types



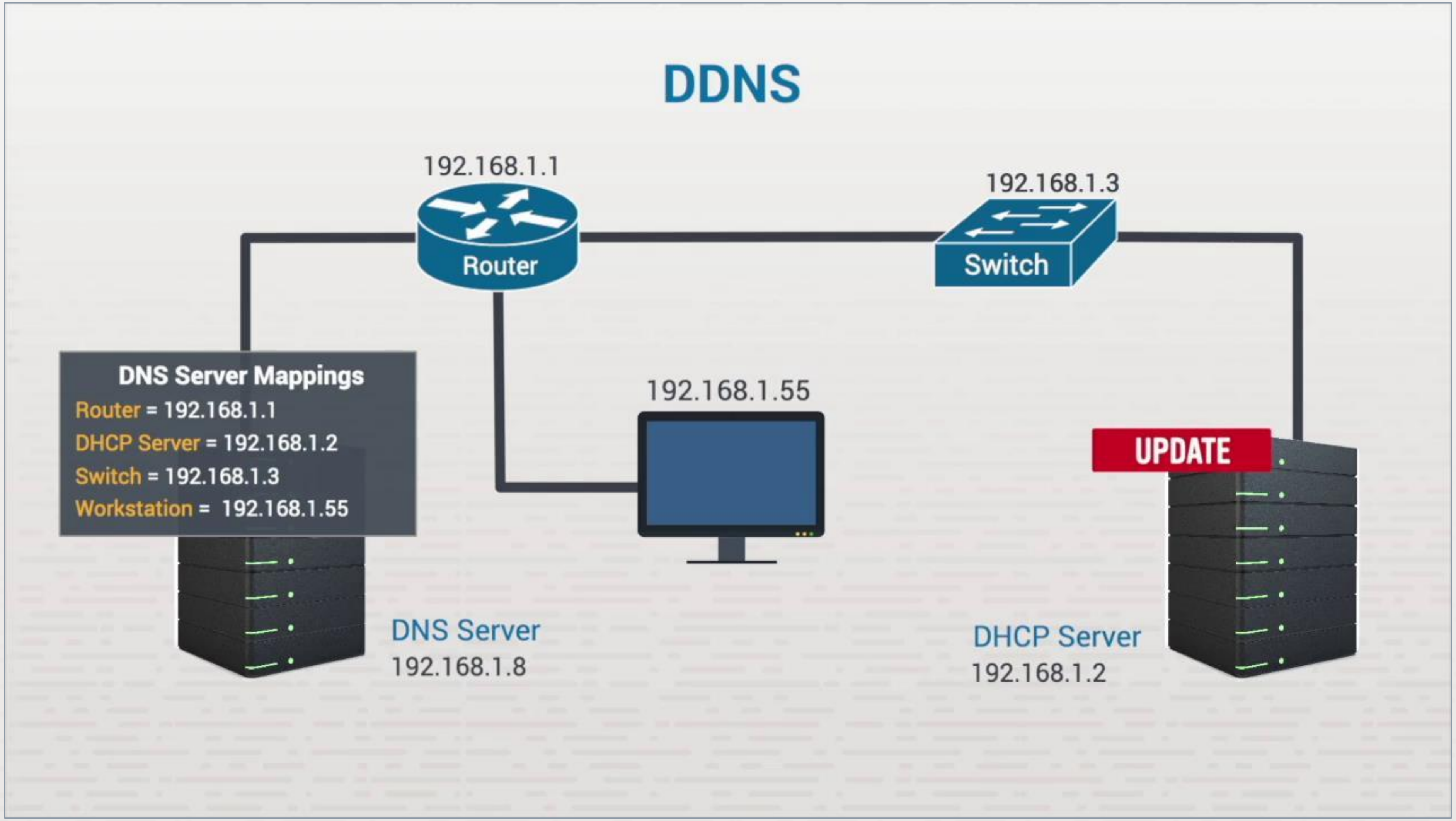
DNS Zones

- Zone file defines DNS
- Forward = hostname to IP
- Reverse = IP to hostname

DNS - Record Types



DNS - Record Types

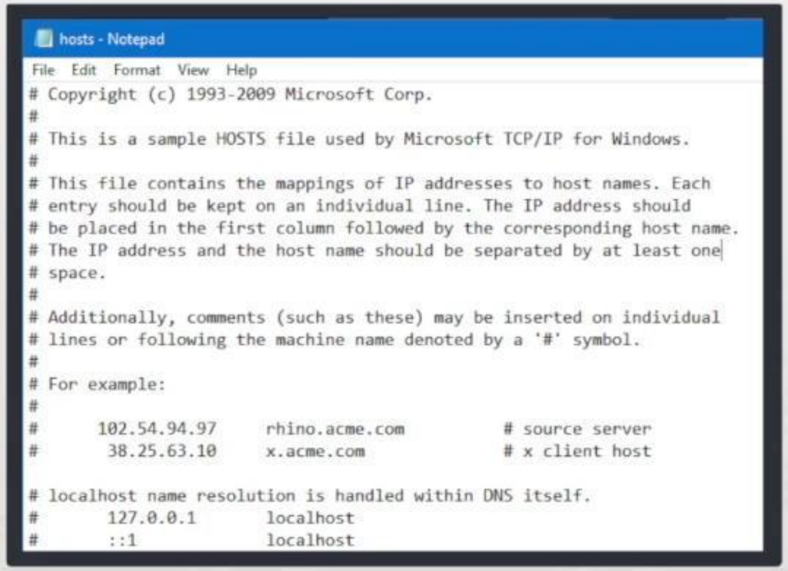


DNS Process

- Recursive
- Authoritative name server
- Top-level domain (TLD)
- Root servers

DNS - Record Types

HOSTS File

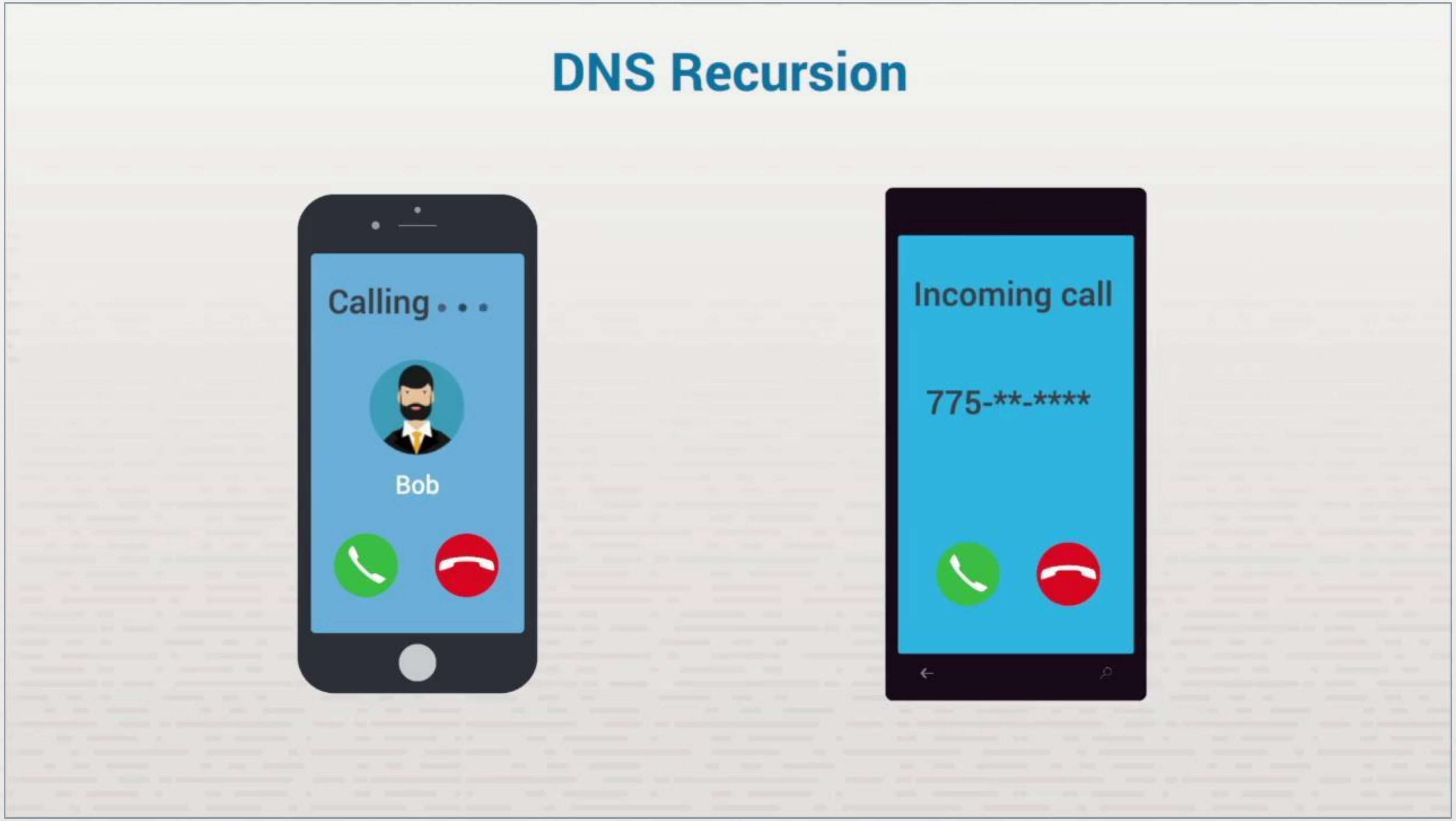


hosts - Notepad

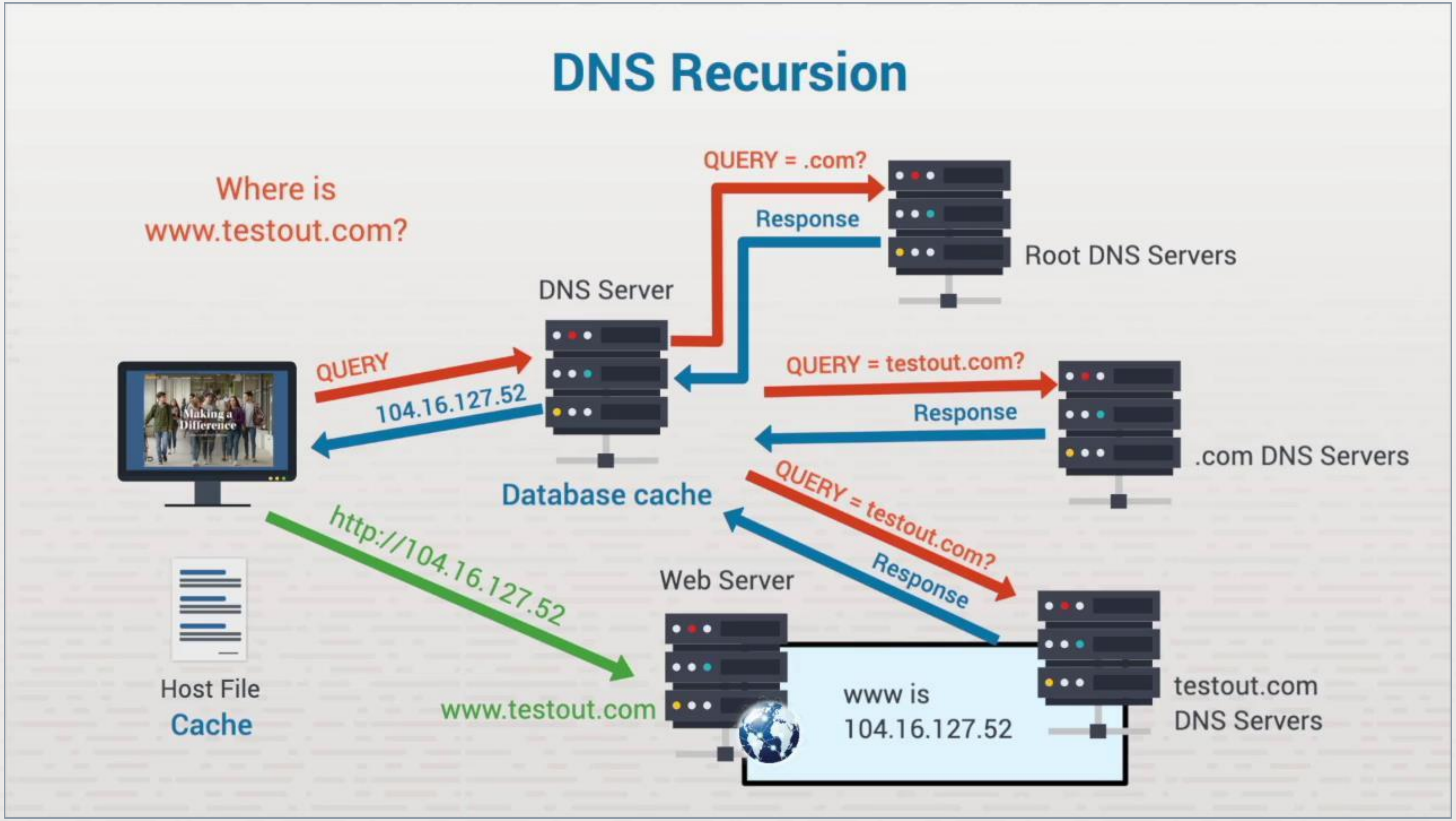
File Edit Format View Help

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

DNS - Record Types



DNS - Record Types



DNS Cache

- Stores known IP mappings
- DNS mappings can change
- DNS time to live (TTL)

DNS - Record Types

DNS Records

DNS Record Type	Description
A	Maps hostname to IPv4 address (ex. www.testout.com → 104.16.32.53)
AAAA	Maps hostname to IPv6 address
Pointer (PTR)	Maps IP address to hostname (ex. 104.16.32.53 → www.testout.com)
Canonical Name (CNAME)	Maps alias name to a domain name (ex. Sales.testout → testout.com)
Mail Exchange (MX)	Identifies servers used for handling email
TXT	Stores plaintext notes in a DNS zone
Start of Authority (SOA)	Stores administration information on DNS zone
Name Server (NS)	Defines the authoritative server for a specific domain
DNS Service (SRV)	Defines host and port for a specific service

Summary

- DNS structure
- DNS process
- DNS records

In-Class Practice

Do the following labs:

- 4.5.4 Configure DNS Addresses
- 4.5.5 Create Standard DNS Zones
- 4.5.6 Create Host Records
- 4.5.7 Create CNAME Records
- 4.5.8 Troubleshoot DNS Records

Class Discussion

- How are hostnames organized in Domain Name Service (DNS)?
- What is the difference between a forward lookup zone and a reverse lookup zone?
- What is the role of the root servers in DNS?
- In DNS, what is the difference between a zone and a domain?
- What is the difference between an A record and a PTR record?

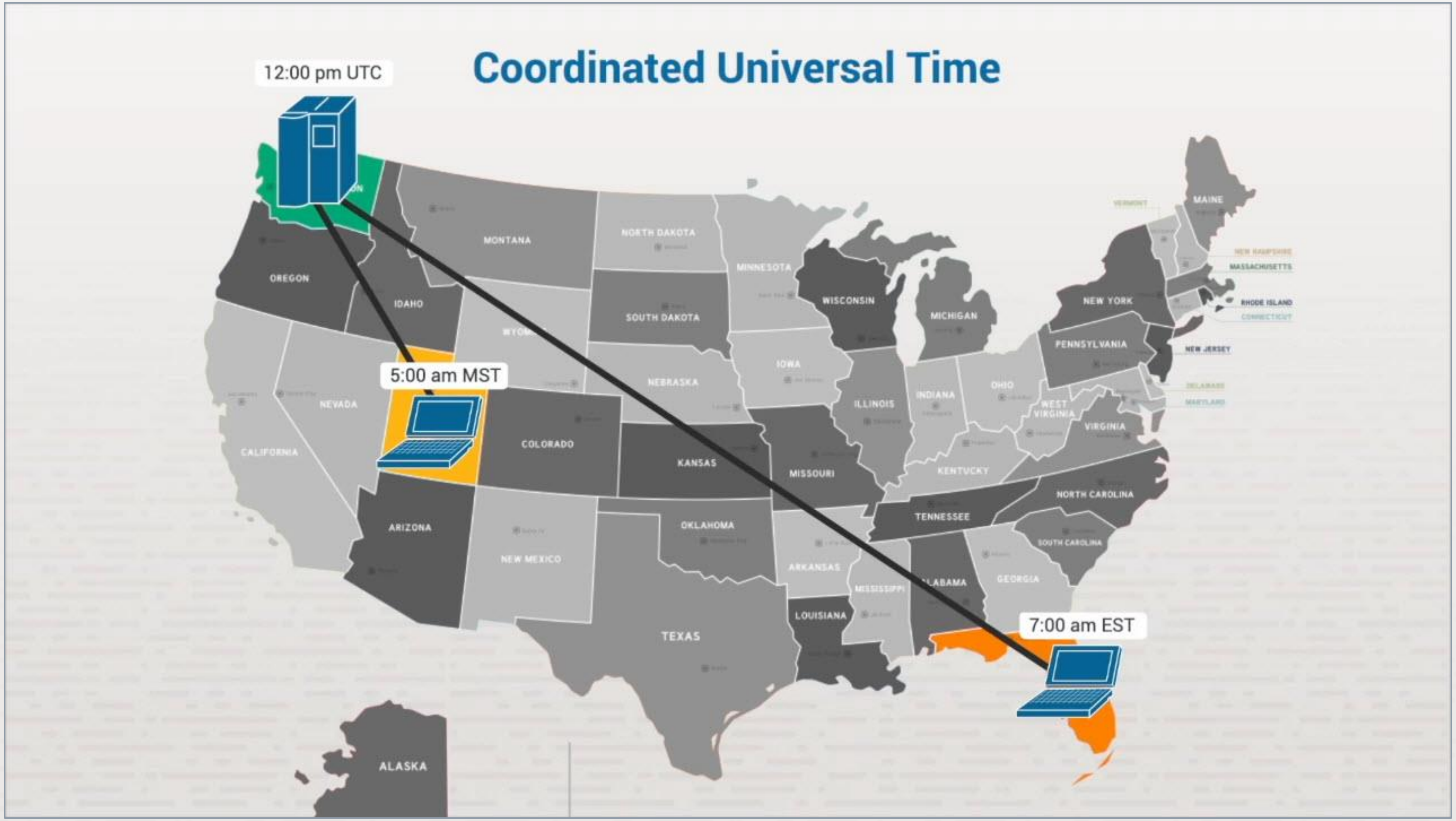
NTP

NTP

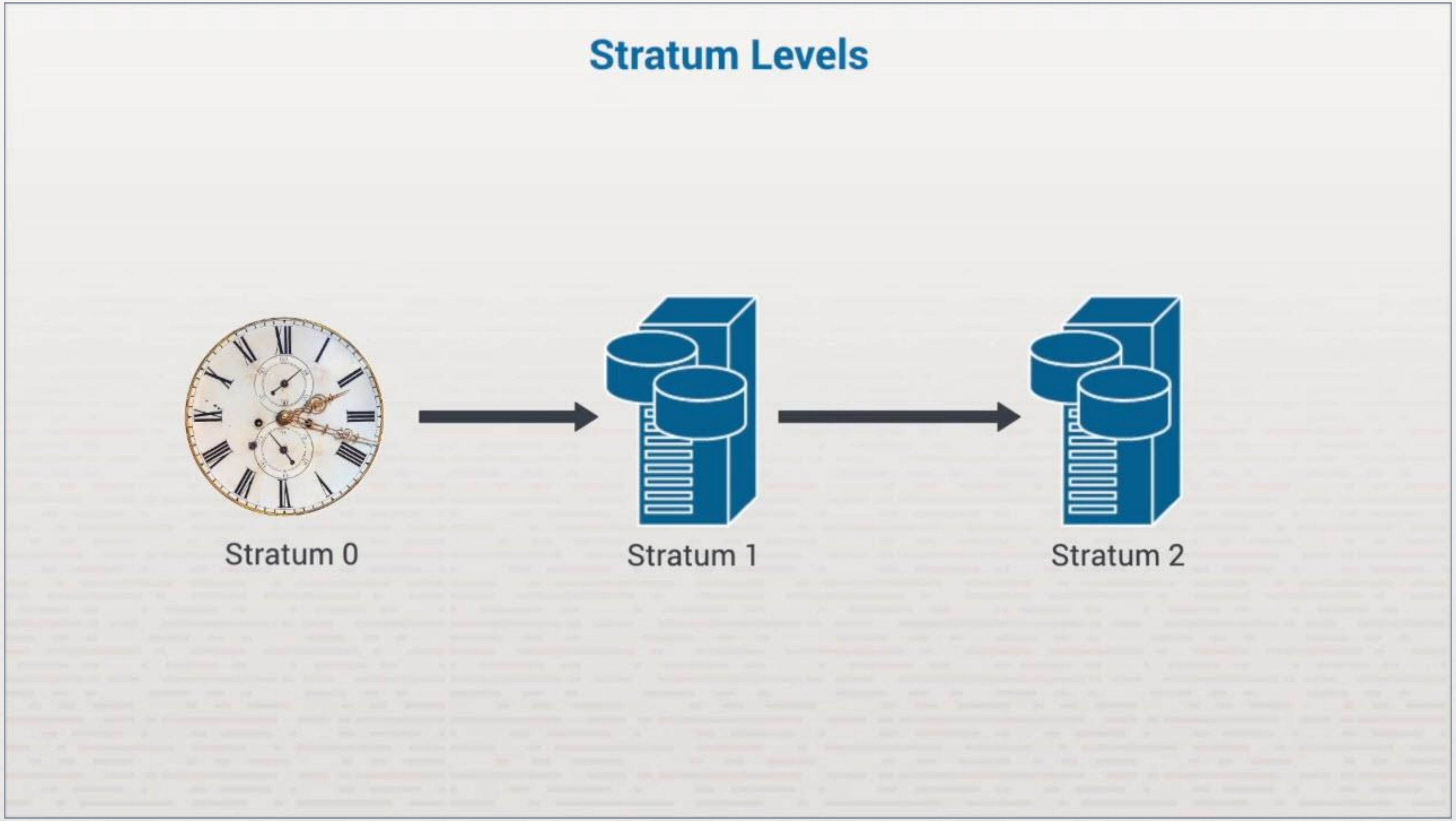
Network Time Protocol

- NTP basics
- NTP uses

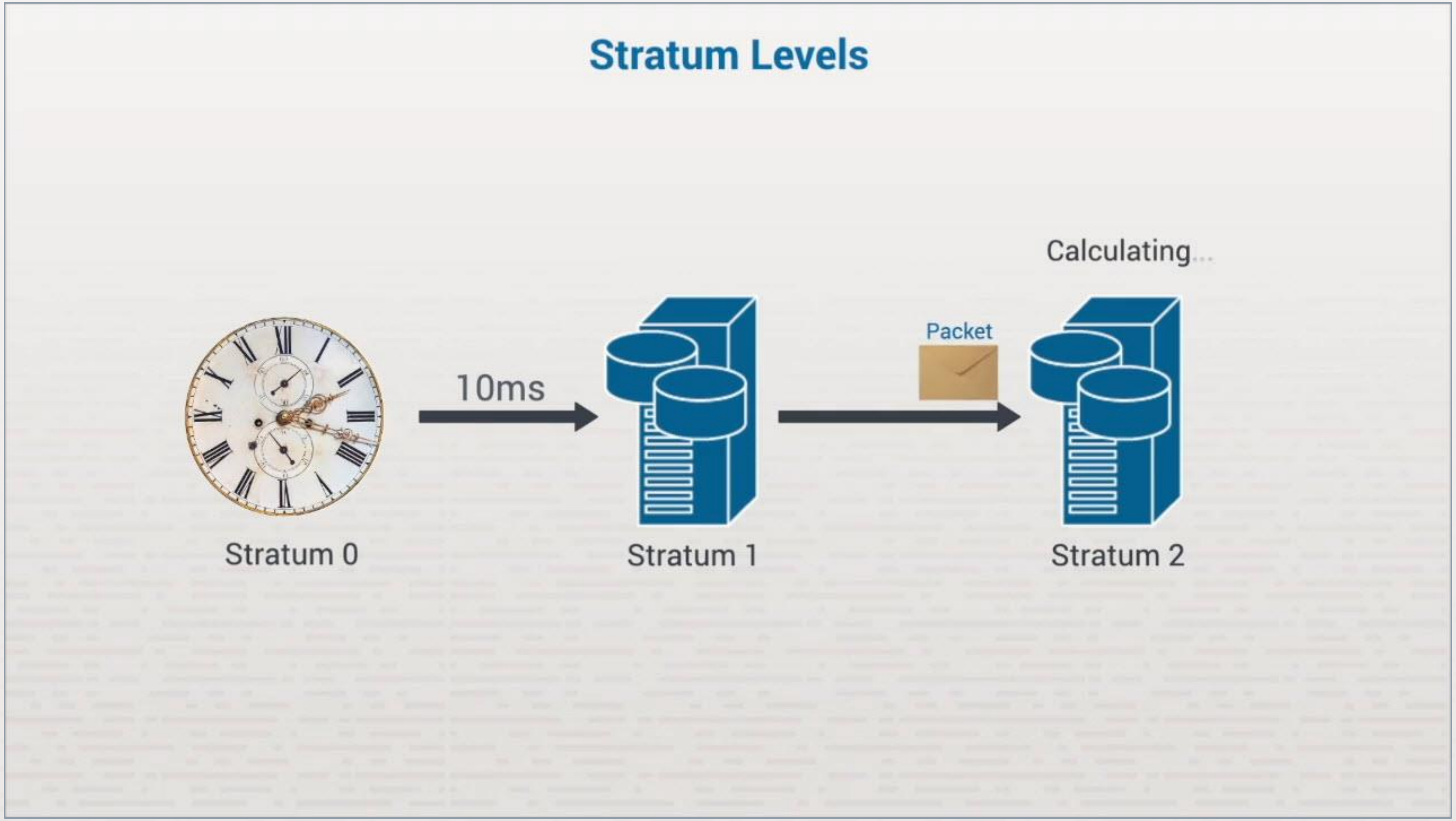
NTP



NTP

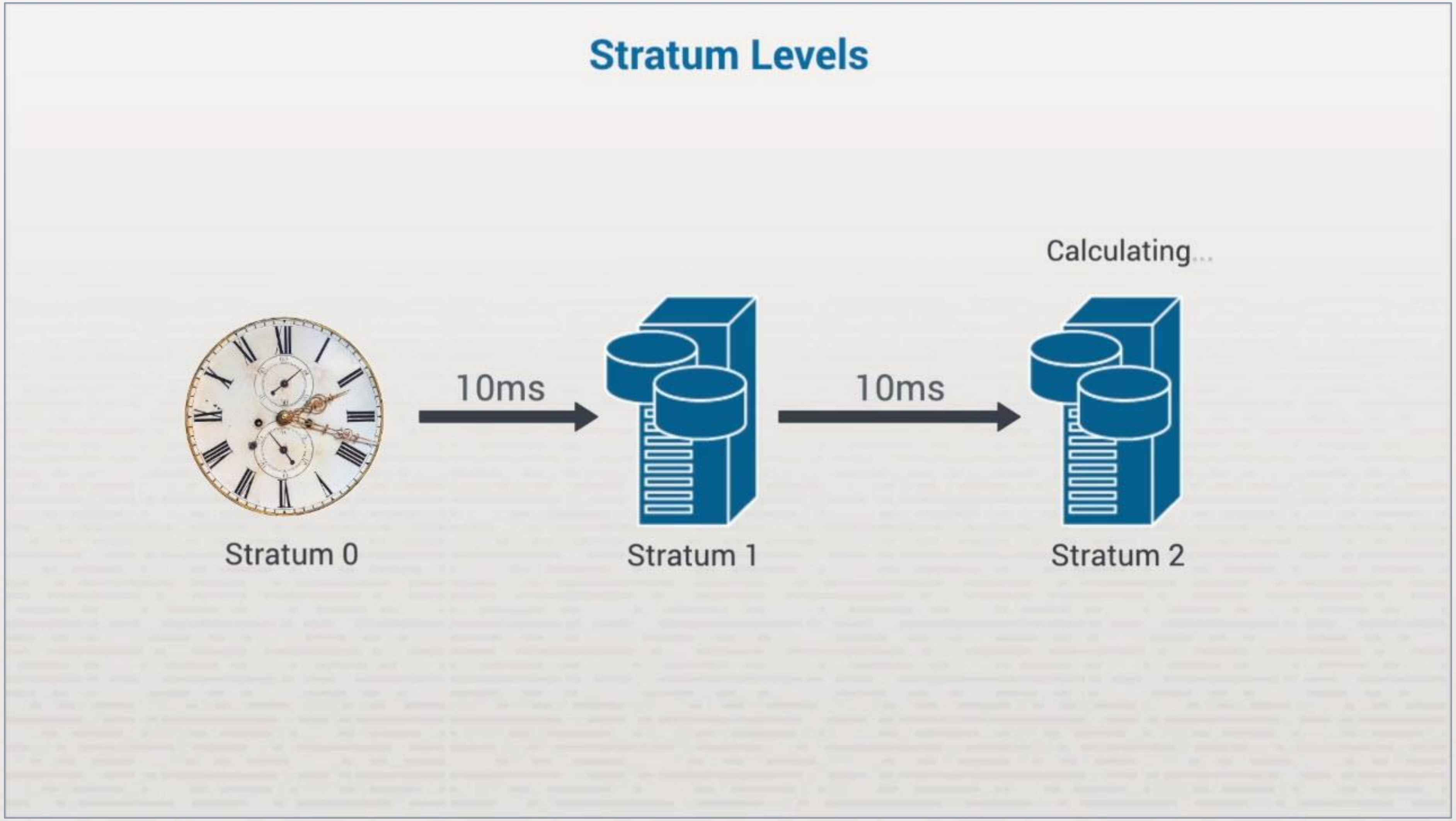


NTP

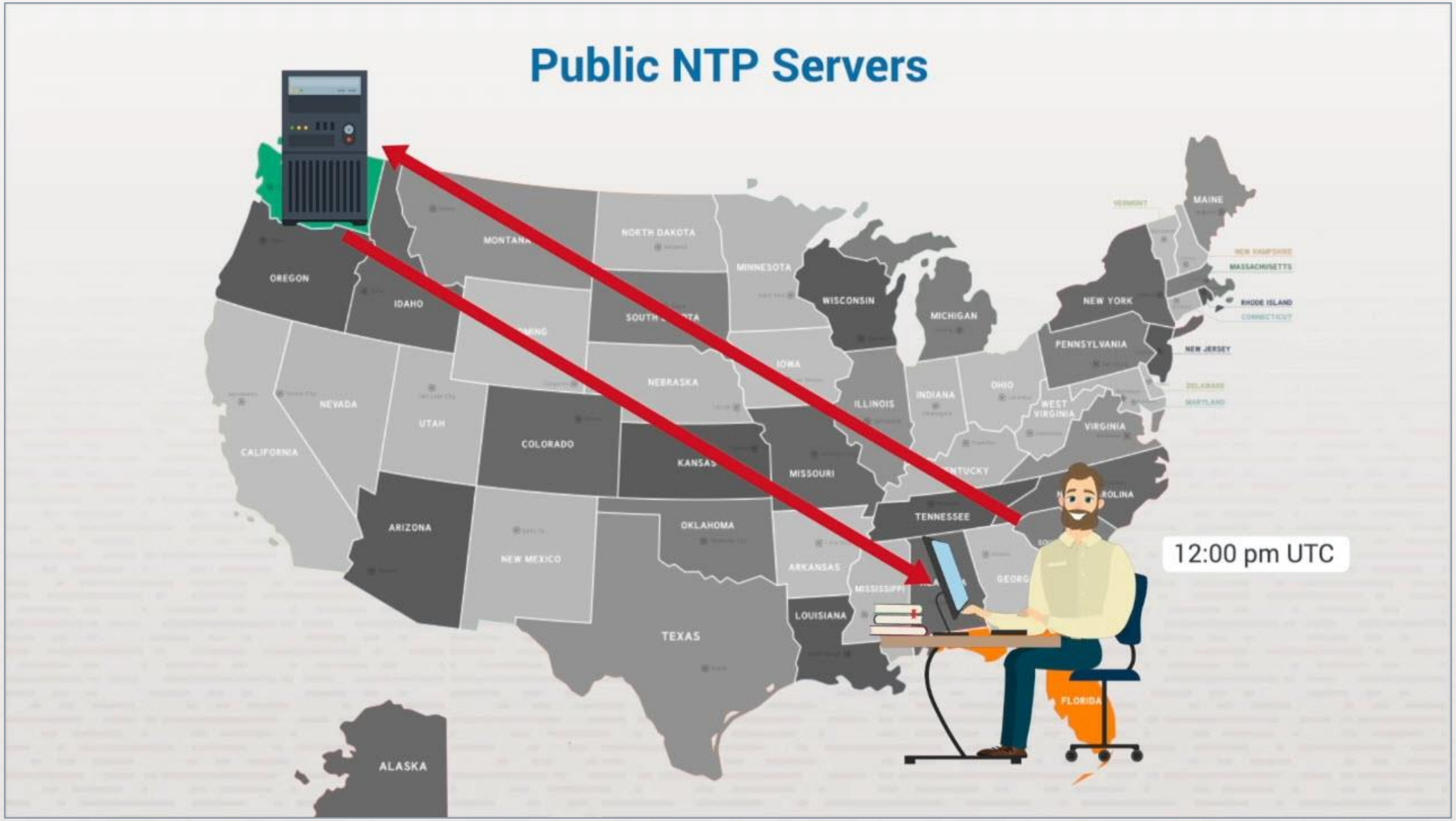


Stratum Levels
Calculating...
10ms
Packet
Stratum 0
Stratum 1
Stratum 2

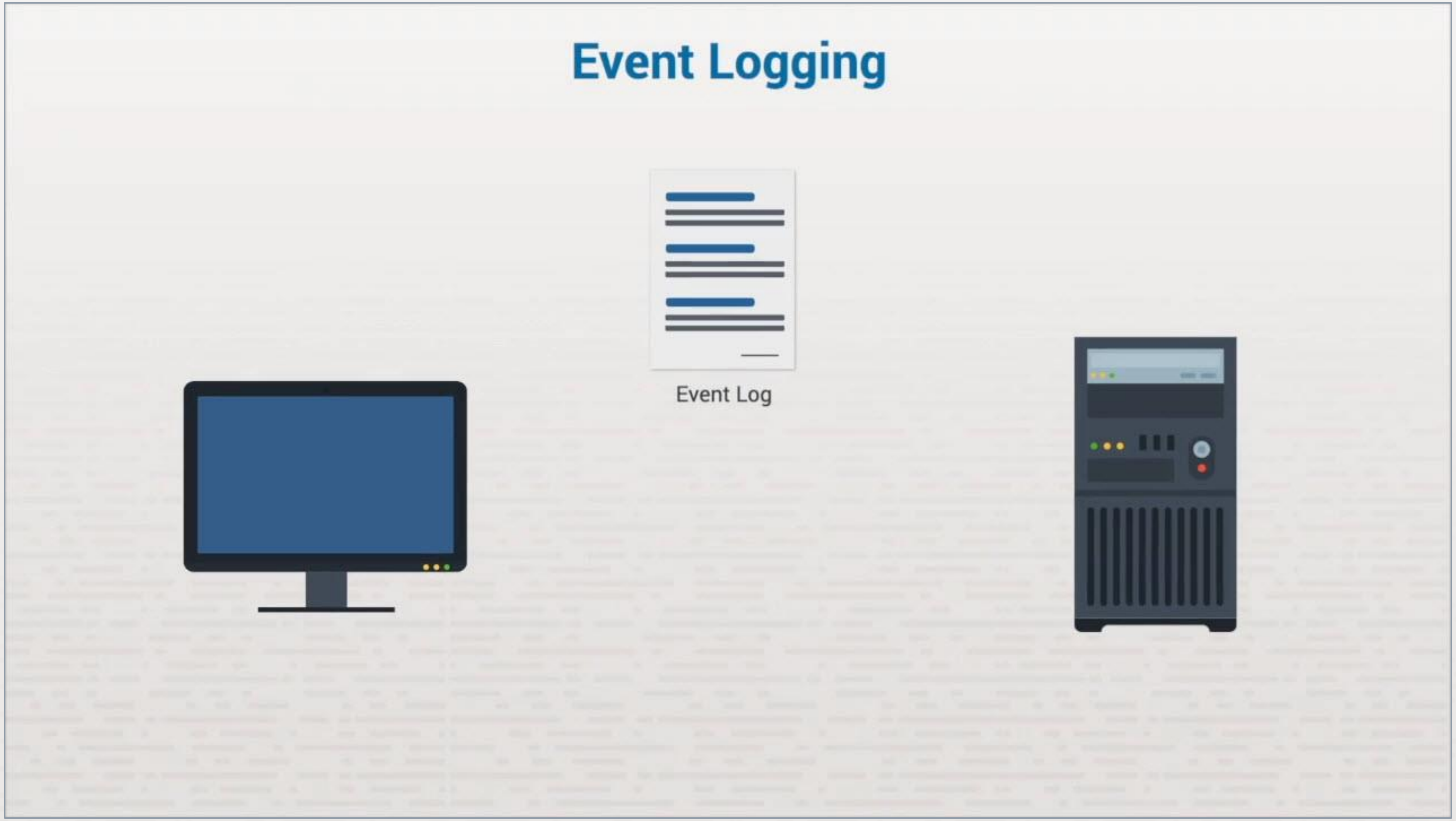
NTP


Stratum Levels
Calculating...
10ms
10ms
Stratum 0
Stratum 1
Stratum 2

NTP



NTP



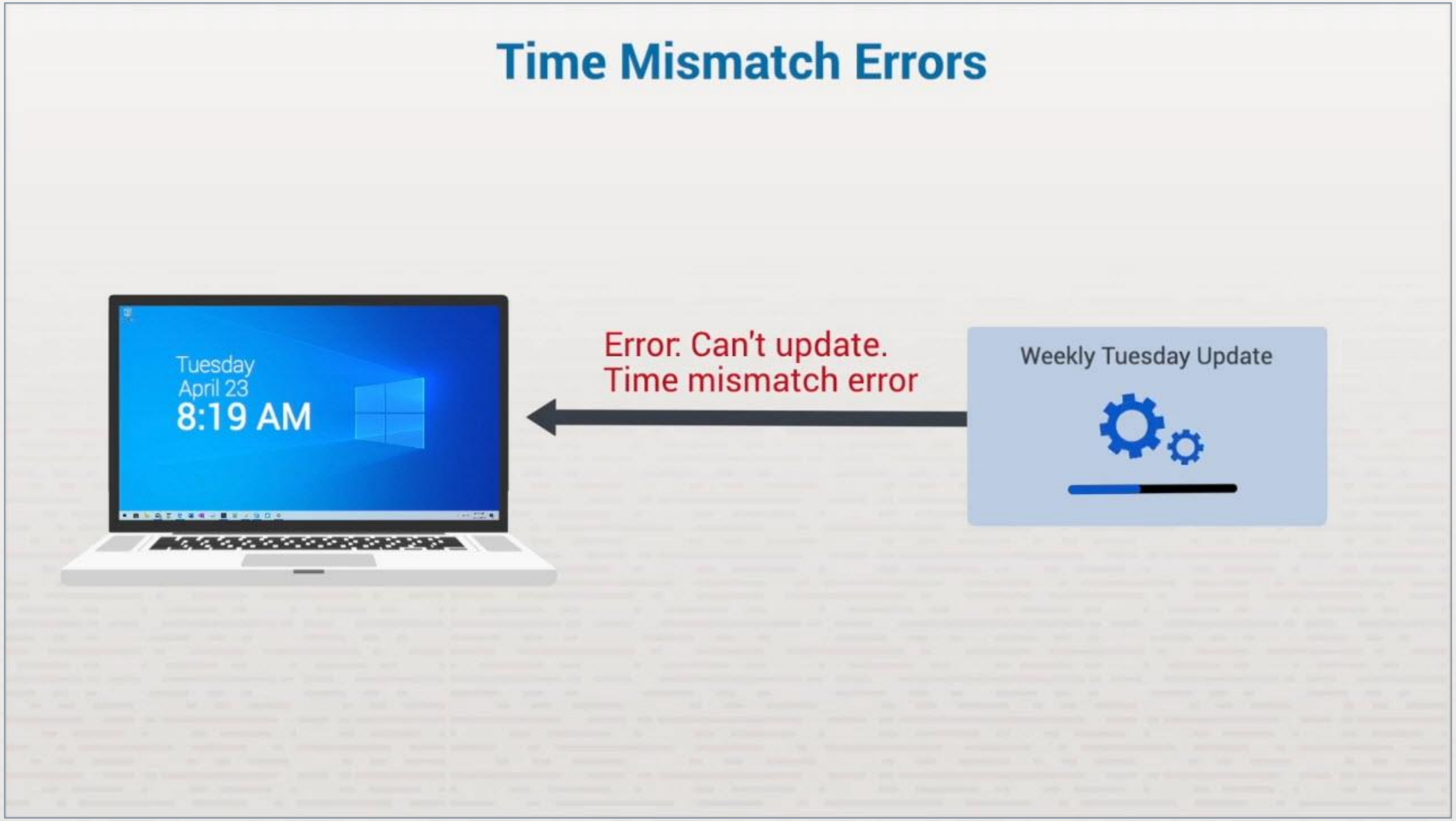
NTP


Event Logging
12:00 pm UTC
5:00 am MST
Event Happened
7:00 am EST
7:00 am EST
OREGON
IDAHO
MONTANA
NORTH DAKOTA
SOUTH DAKOTA
MINNESOTA
WISCONSIN
MICHIGAN
NEW YORK
MAINE
PENNSYLVANIA
NEBRASKA
IOWA
ILLINOIS
INDIANA
OHIO
WEST VIRGINIA
VIRGINIA
NEVADA
CALIFORNIA
COLORADO
MISSOURI
KENTUCKY
NORTH CAROLINA
TENNESSEE
SOUTH CAROLINA
ARIZONA
NEW MEXICO
OKLAHOMA
ARKANSAS
MISSISSIPPI
GEORGIA
LOUISIANA
TEXAS
ALASKA

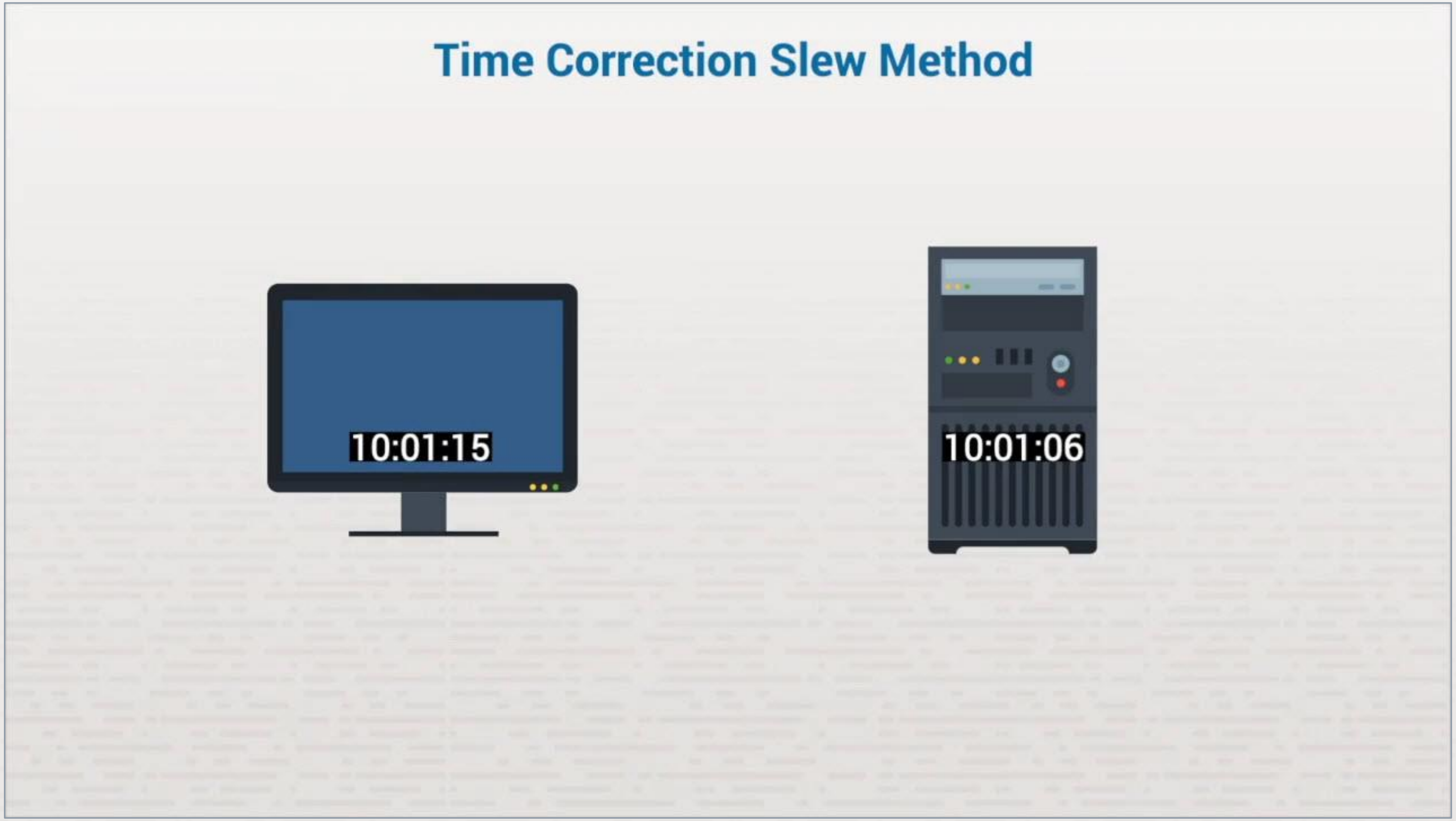
NTP

Event Logging
12:00 pm UTC
Event Happened
5:00 am MST
5:00 am MST
7:00 am EST

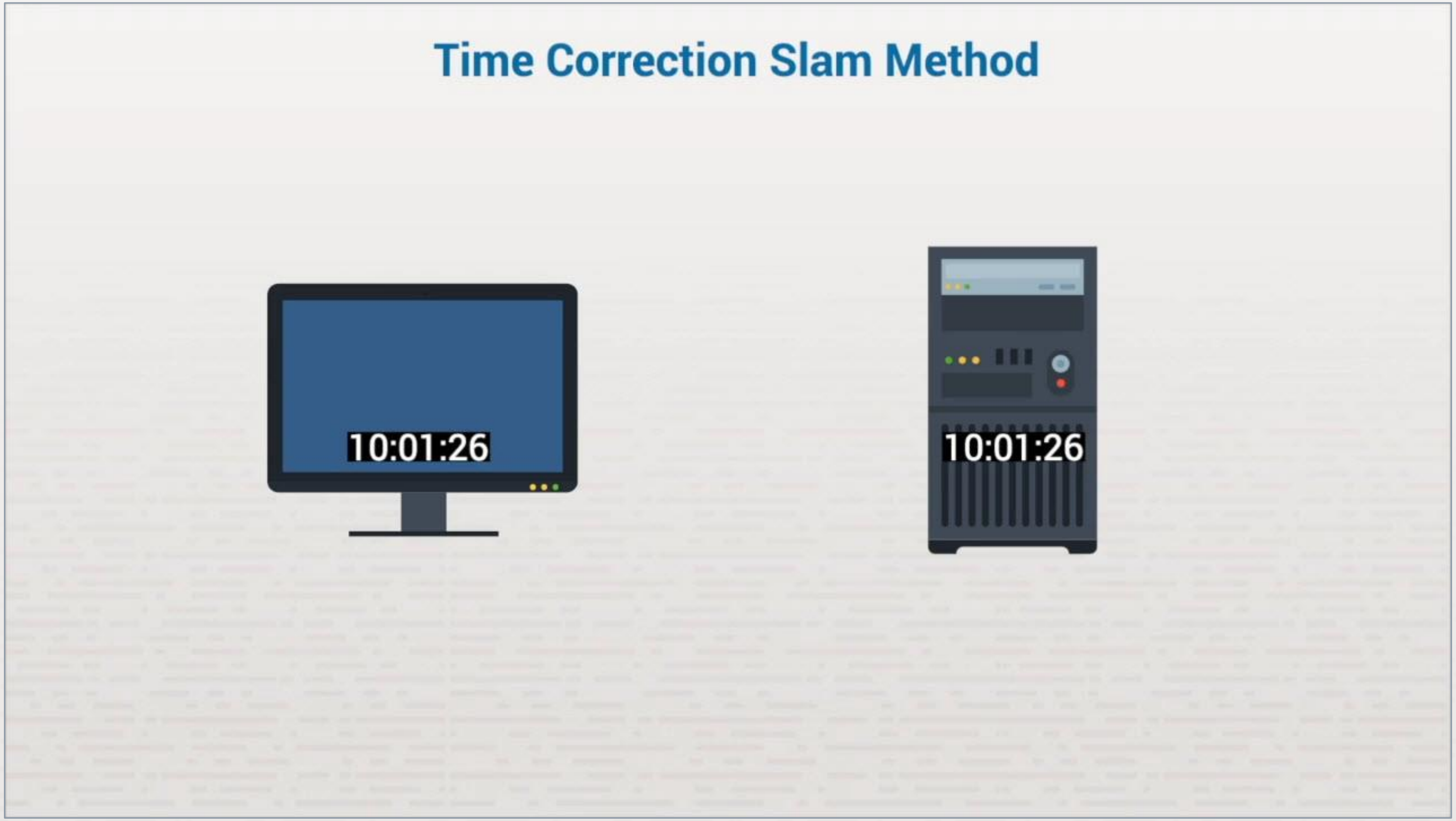
NTP


Time Mismatch Errors
Tuesday
April 23
8:19 AM
Error. Can't update.
Time mismatch error
Weekly Tuesday Update

NTP



NTP



Summary

- NTP basics
- NTP uses

4.7 NETWORK ADDRESSING AND SERVICES

IP Version 6

Section Skill Overview

- Configure IPv6 addresses
- Configure a DHCPv6 server

Key Terms

- Prefix ID
- Interface ID
- Tunneling
- Unicast address
- Multicast address
- Anycast address
- Loopback address

Key Definitions

- **Prefix ID:** The first 64 bits of the IPv6 address. The prefix can be divided into various parts that identify things such as geographic region, ISP, network, and subnet.
- **Interface ID:** The last 64 bits of the IPv6 address. This is a unique identifier for each device, similar to a MAC address.
- **Tunneling:** Allows IPv6 hosts or sites to communicate over the existing IPv4 infrastructure.
- **Unicast address:** An address assigned to a single interface for the purpose of allowing one host to send and receive data. Packets sent to a unicast address are delivered to the interface identified by that address.

Key Definitions

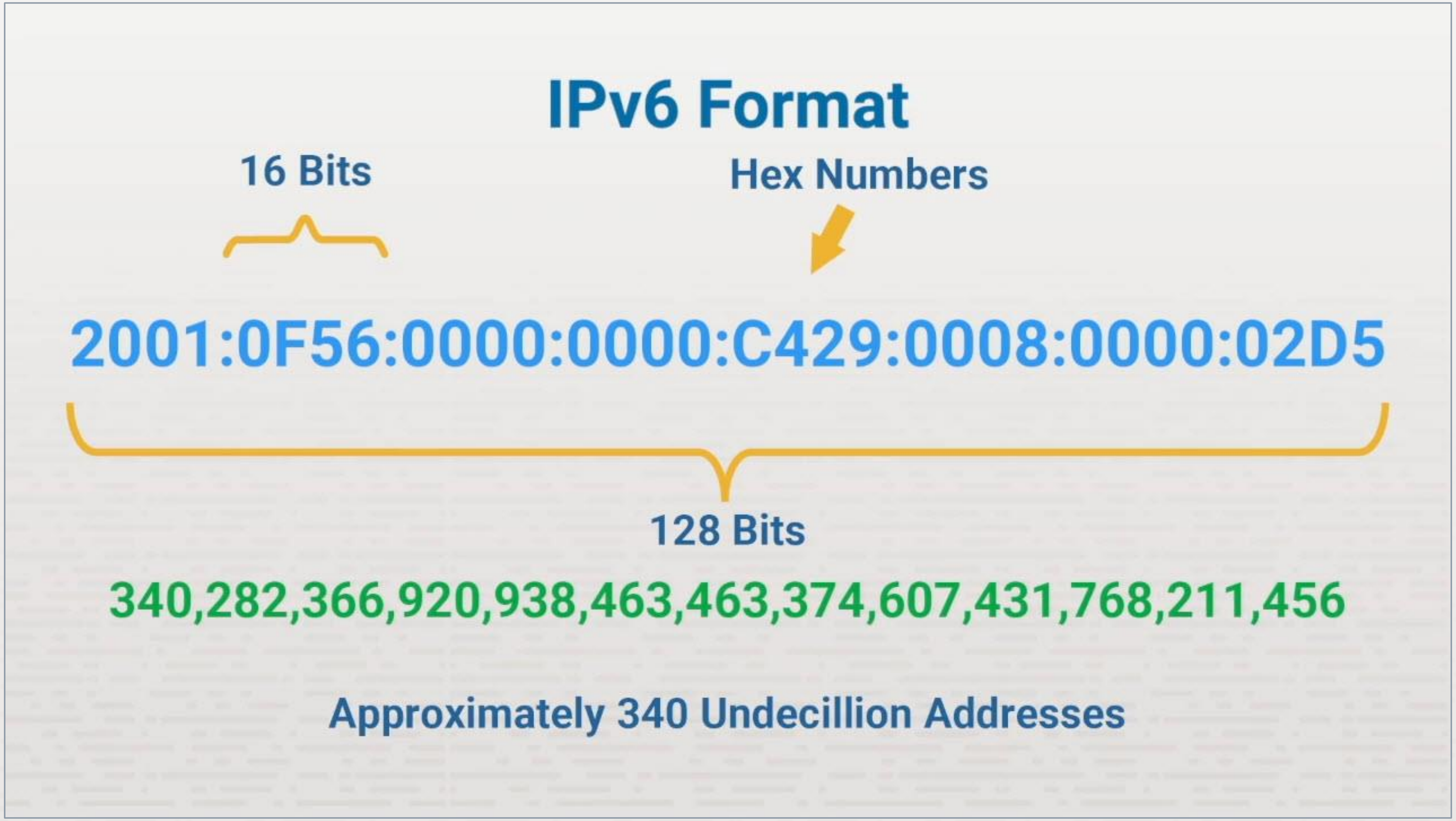
- **Multicast address:** An address that represents a dynamic group of hosts.
- **Anycast address:** A unicast address assigned to more than one interface, typically belonging to different hosts.
- **Loopback address:** A special IP address that can be used to verify that the TCP/IP protocol stack is properly installed on the host. The local loopback address is not assigned to an interface.

IP Version 6

IPv6

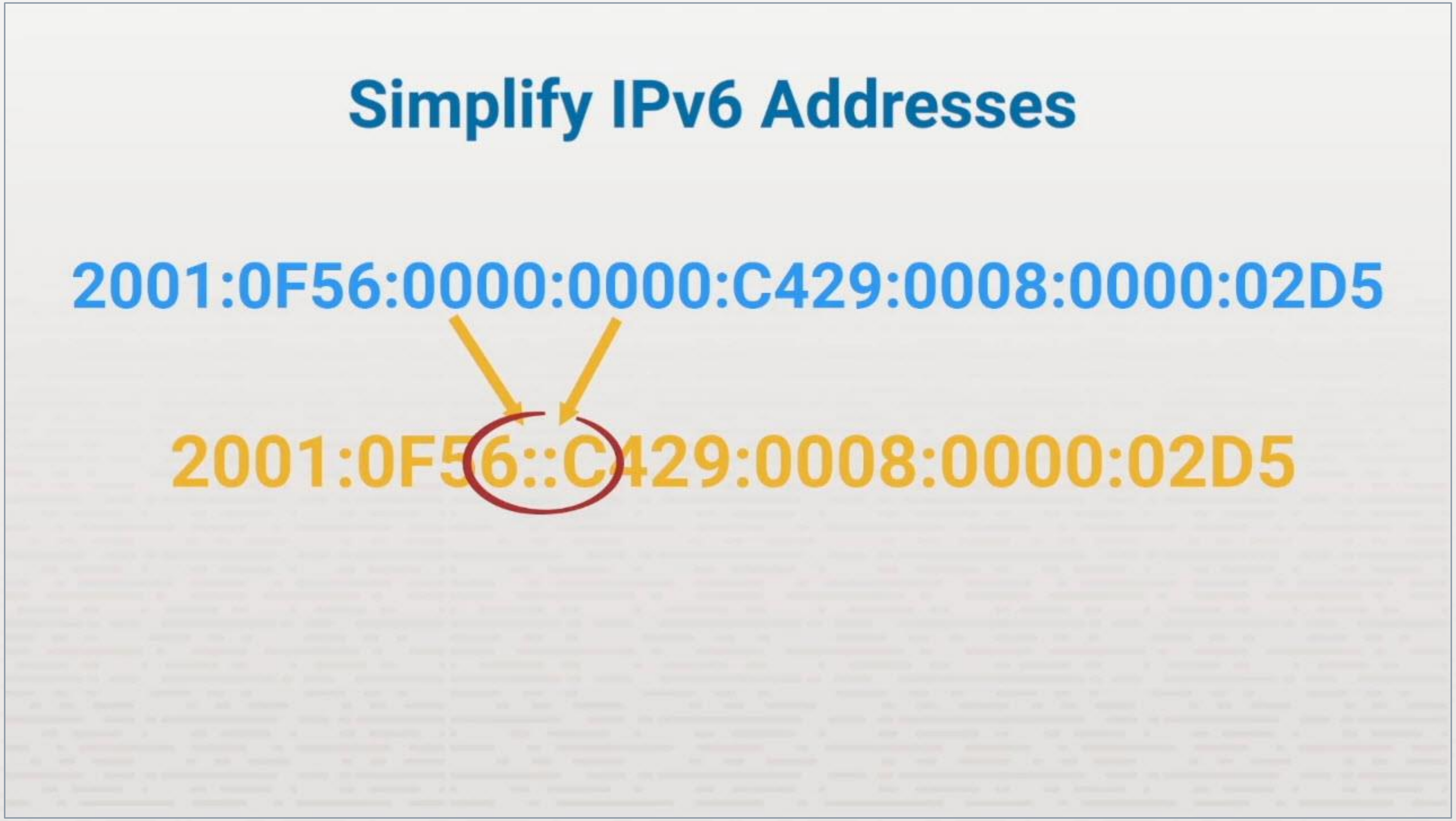
- IPv6 format
- IPv6 components
- IPv6 features

IP Version 6



IPv6 Format
16 Bits
Hex Numbers
2001:0F56:0000:0000:C429:0008:0000:02D5
128 Bits
340,282,366,920,938,463,463,374,607,431,768,211,456
Approximately 340 Undecillion Addresses

IP Version 6


Simplify IPv6 Addresses
2001:0F56:0000:0000:C429:0008:0000:02D5
2001:0F56::C429:0008:0000:02D5

IP Version 6

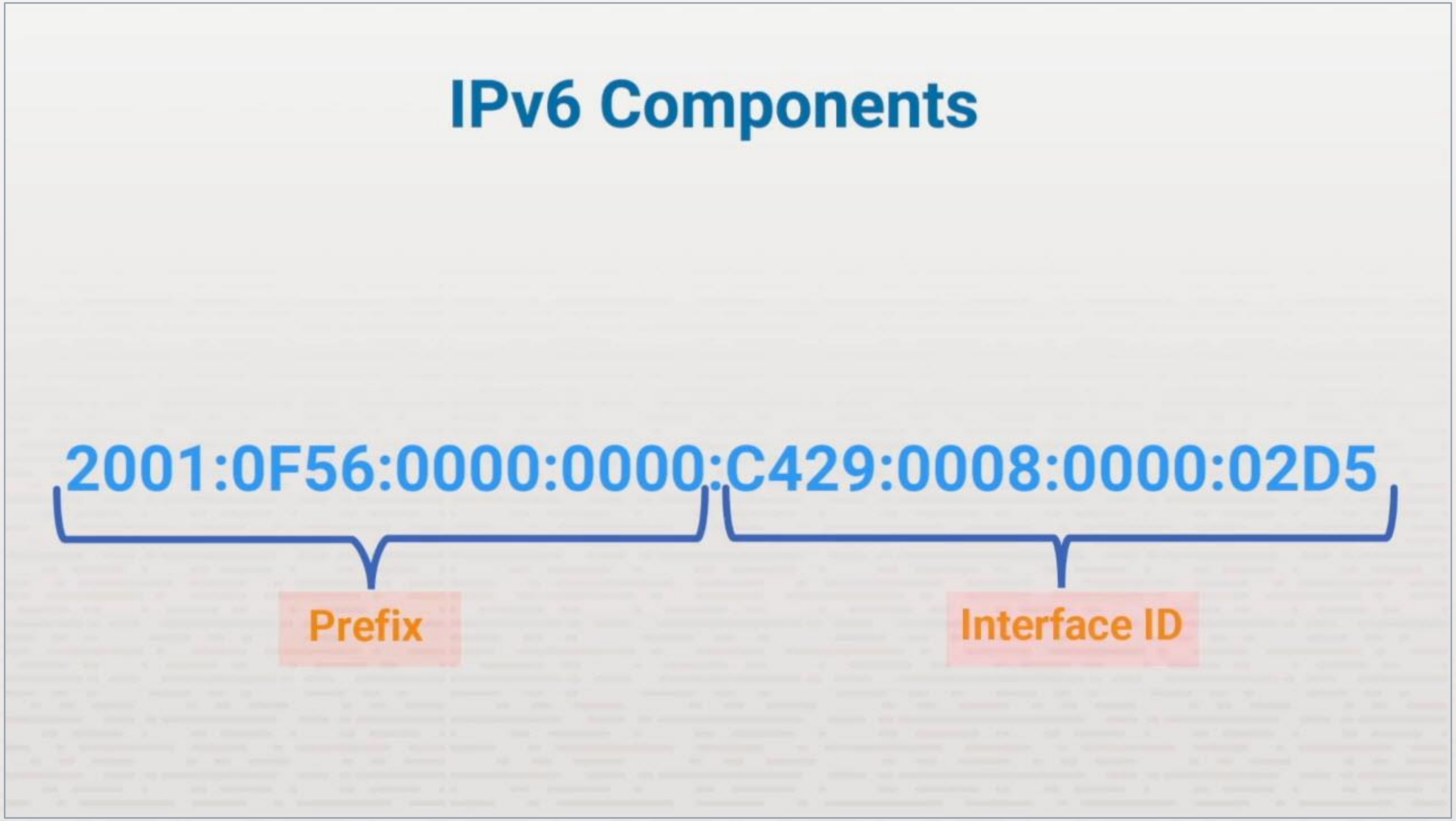
Simplify IPv6 Addresses

2001:0F56:0000:0000:C429:0008:0000:02D5

2001:~~0~~F56::C429:~~000~~8:~~000~~0:~~0~~2D5

2001:F56::C429:8:0:2D5

IP Version 6


IPv6 Components
2001:0F56:0000:0000:C429:0008:0000:02D5
Prefix
Interface ID

IP Version 6

IPv6 Prefix

$$\underbrace{\texttt{2001:0F56:0000}}_{\text{Site Prefix}}\texttt{:}\underbrace{\texttt{0000}}_{\text{Subnet ID}}\texttt{:C429:0008:0000:02D5}$$

Site Prefix
- Defines the location
- Assigned by ISP

Subnet ID
- Like a subnet address
- Network ID

IP Version 6

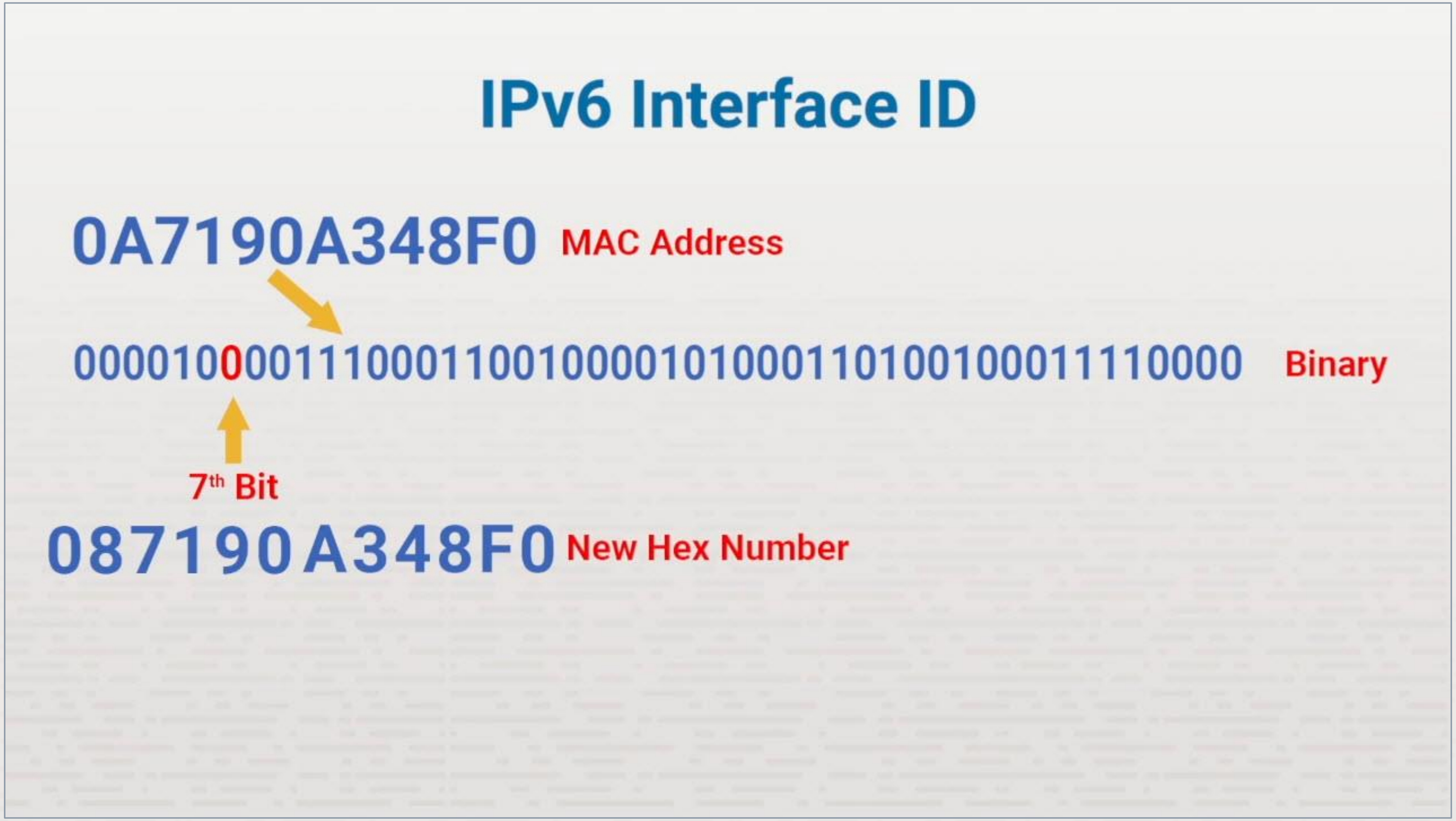
IPv6 Prefix

2001:0F56:0000:0000:C429:0008:0000:02D5

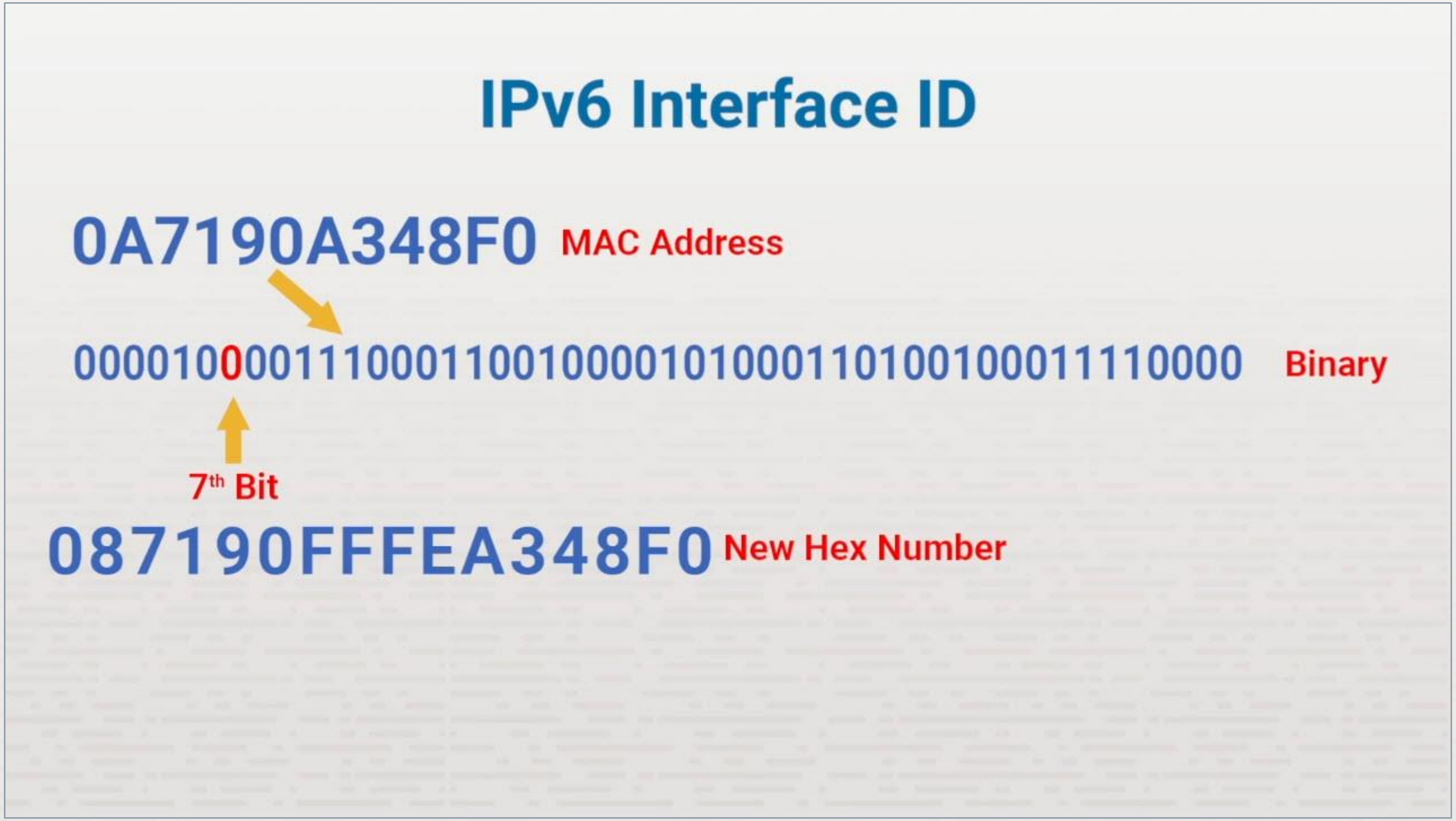
Unique Identifier

Modified EUI-64 Interface ID

IP Version 6

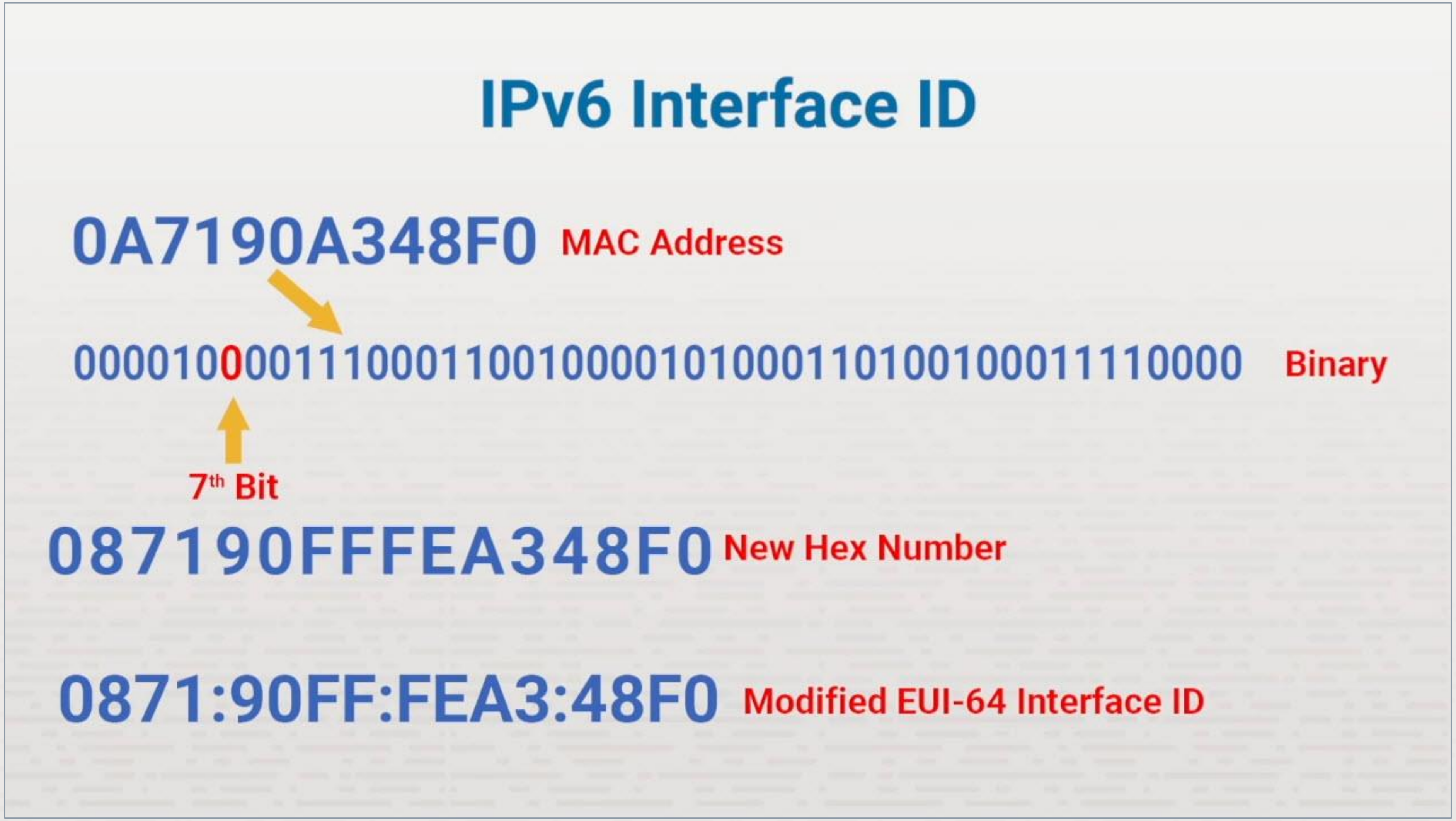

IPv6 Interface ID
0A7190A348F0
MAC Address
000010000011100011001000010100011010010001111 0000
Binary
7th Bit
087190A348F0
New Hex Number

IP Version 6



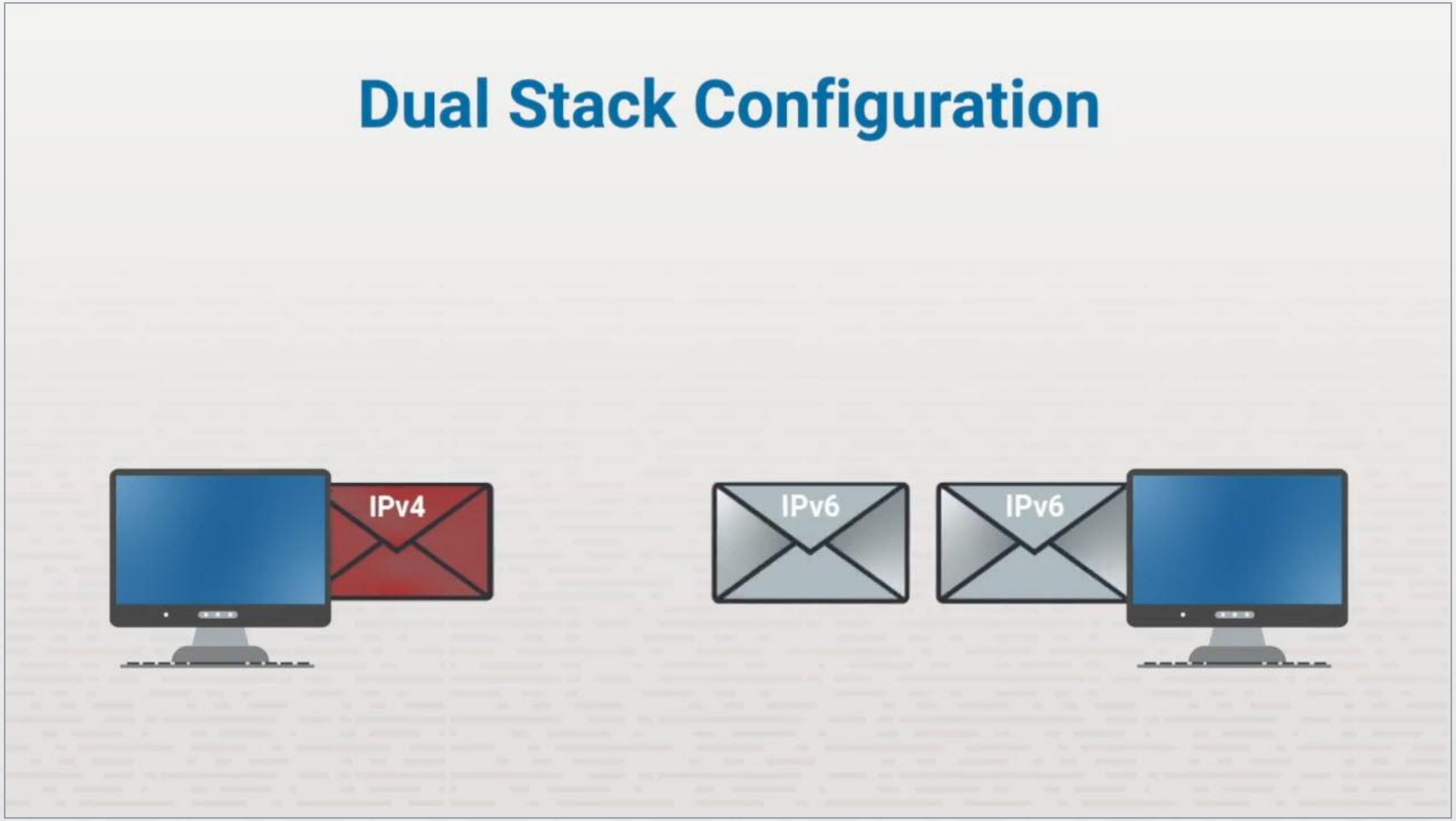
IPv6 Interface ID
0A7190A348F0
MAC Address
000010000111000110010000101000110100100011110000
Binary
7th Bit
087190FFFEA348F0
New Hex Number

IP Version 6



IPv6 Interface ID
0A7190A348F0 MAC Address
000010000111000110010000101000110100100011110000 Binary
7th Bit
087190FFFEA348F0 New Hex Number
0871:90FF:FEA3:48F0 Modified EUI-64 Interface ID

IP Version 6



Tunneling

- One packet inside another

IP Version 6

Teredo Tunneling

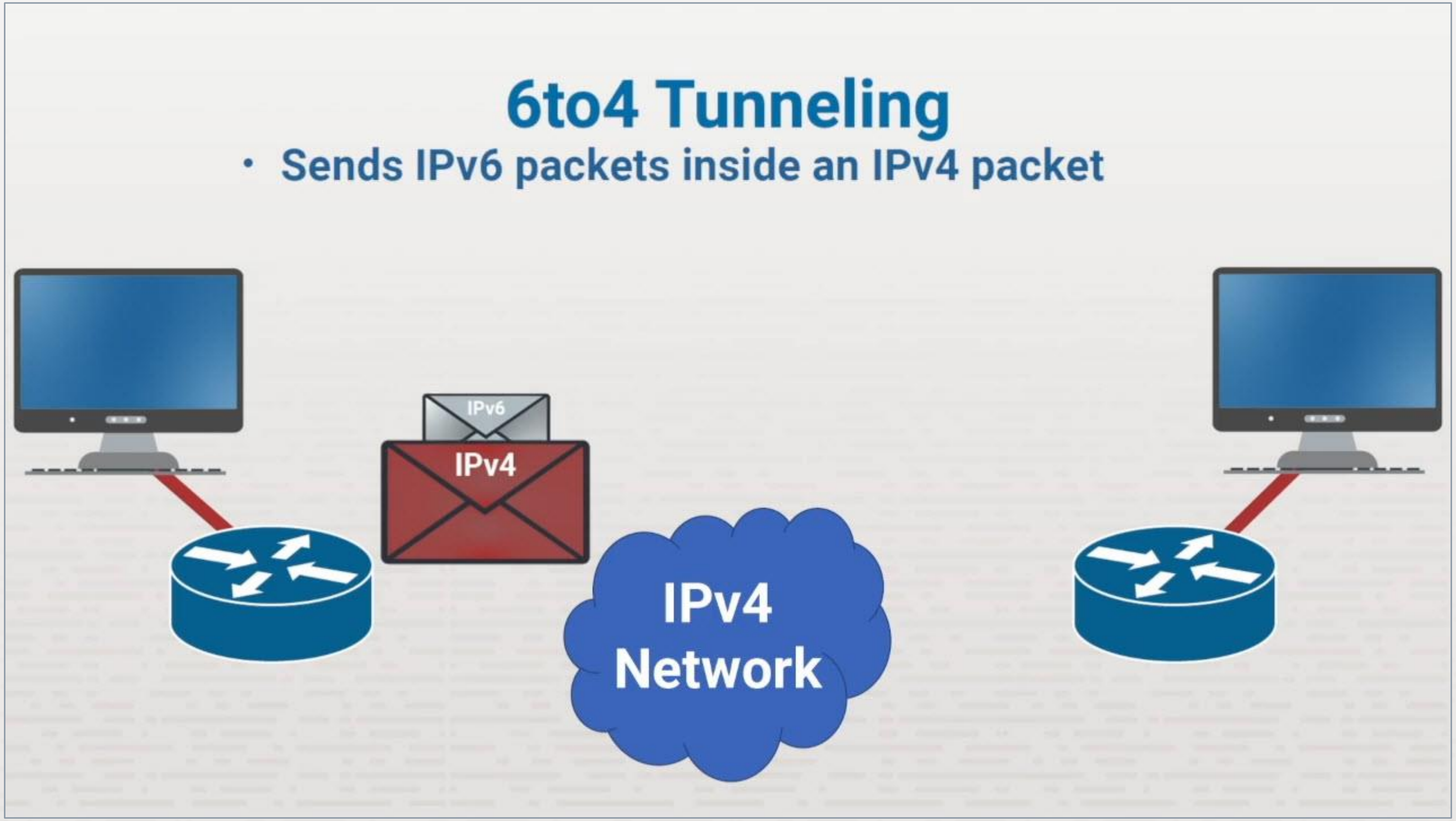
- Sends IPv6 packets inside an IPv4 packet
- Encapsulation/decapsulation completed by each host

IP Version 6

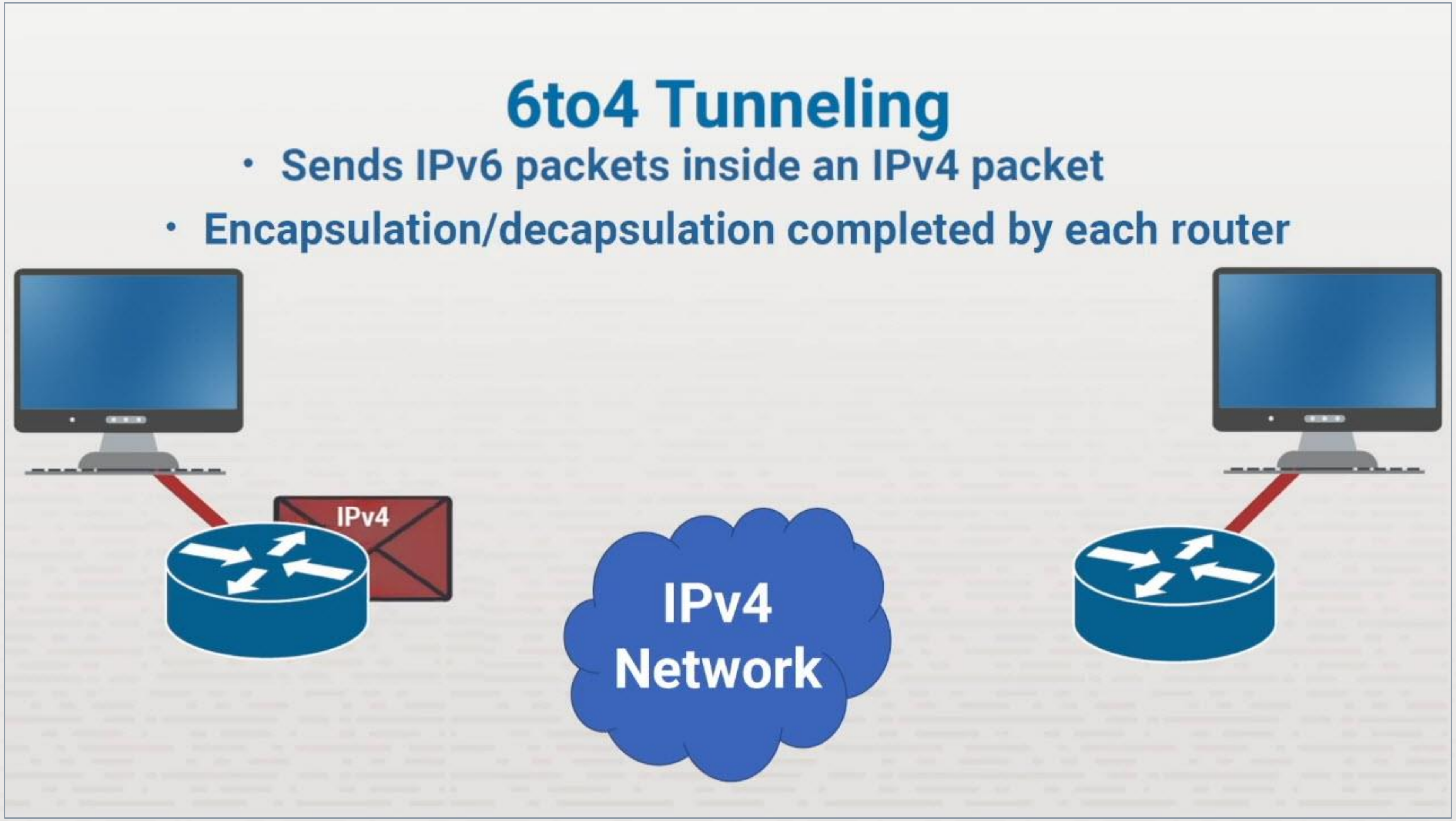
Teredo Tunneling

- Sends IPv6 packets inside an IPv4 packet
- Encapsulation/decapsulation completed by each host

IP Version 6

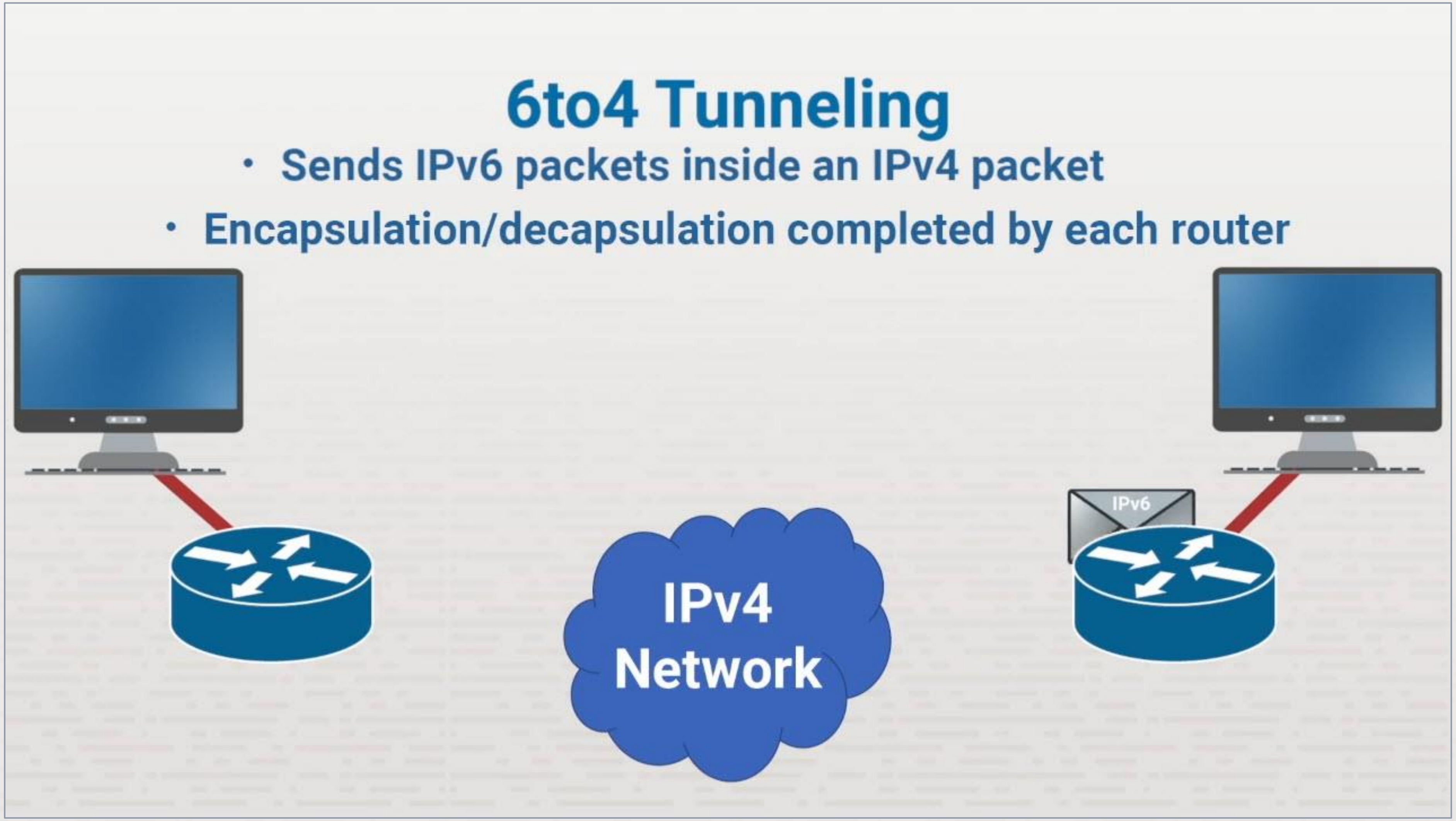

6to4 Tunneling
• Sends IPv6 packets inside an IPv4 packet
IPv6
IPv4
IPv4
Network

IP Version 6



6to4 Tunneling
• Sends IPv6 packets inside an IPv4 packet
• Encapsulation/decapsulation completed by each router
IPv4
IPv4 Network

IP Version 6

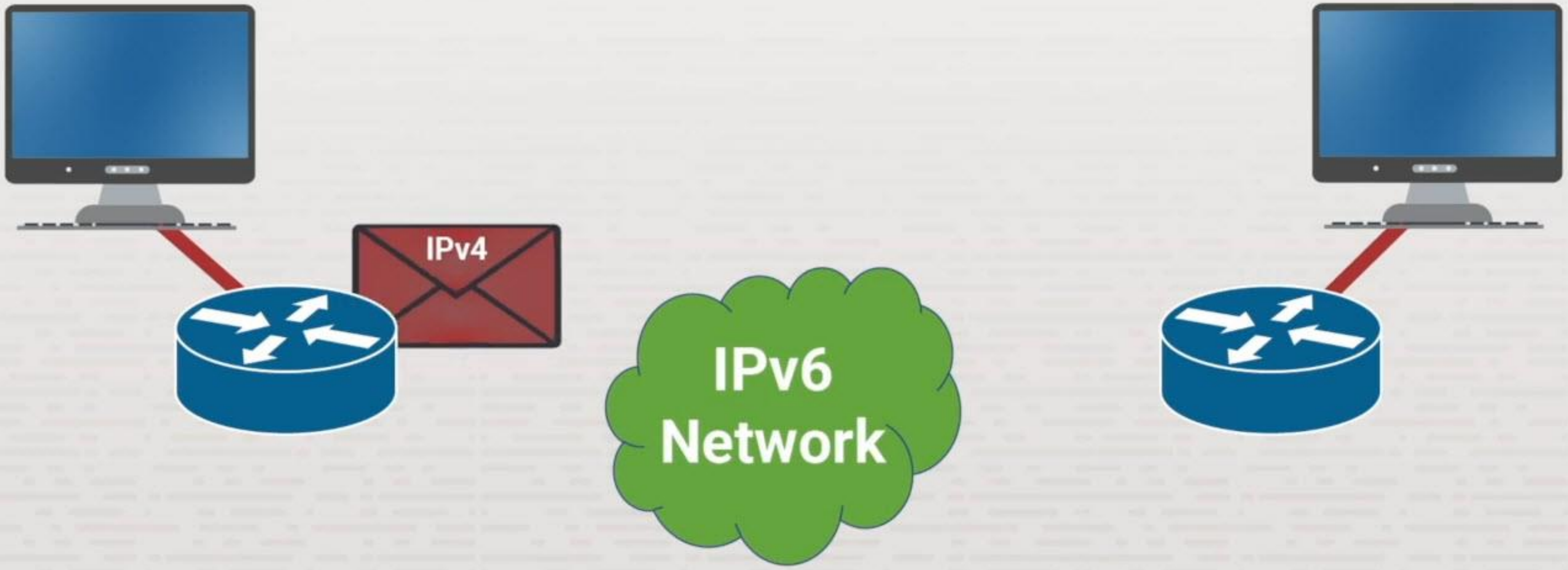


6to4 Tunneling
• Sends IPv6 packets inside an IPv4 packet
• Encapsulation/decapsulation completed by each router
IPv6
IPv4
Network

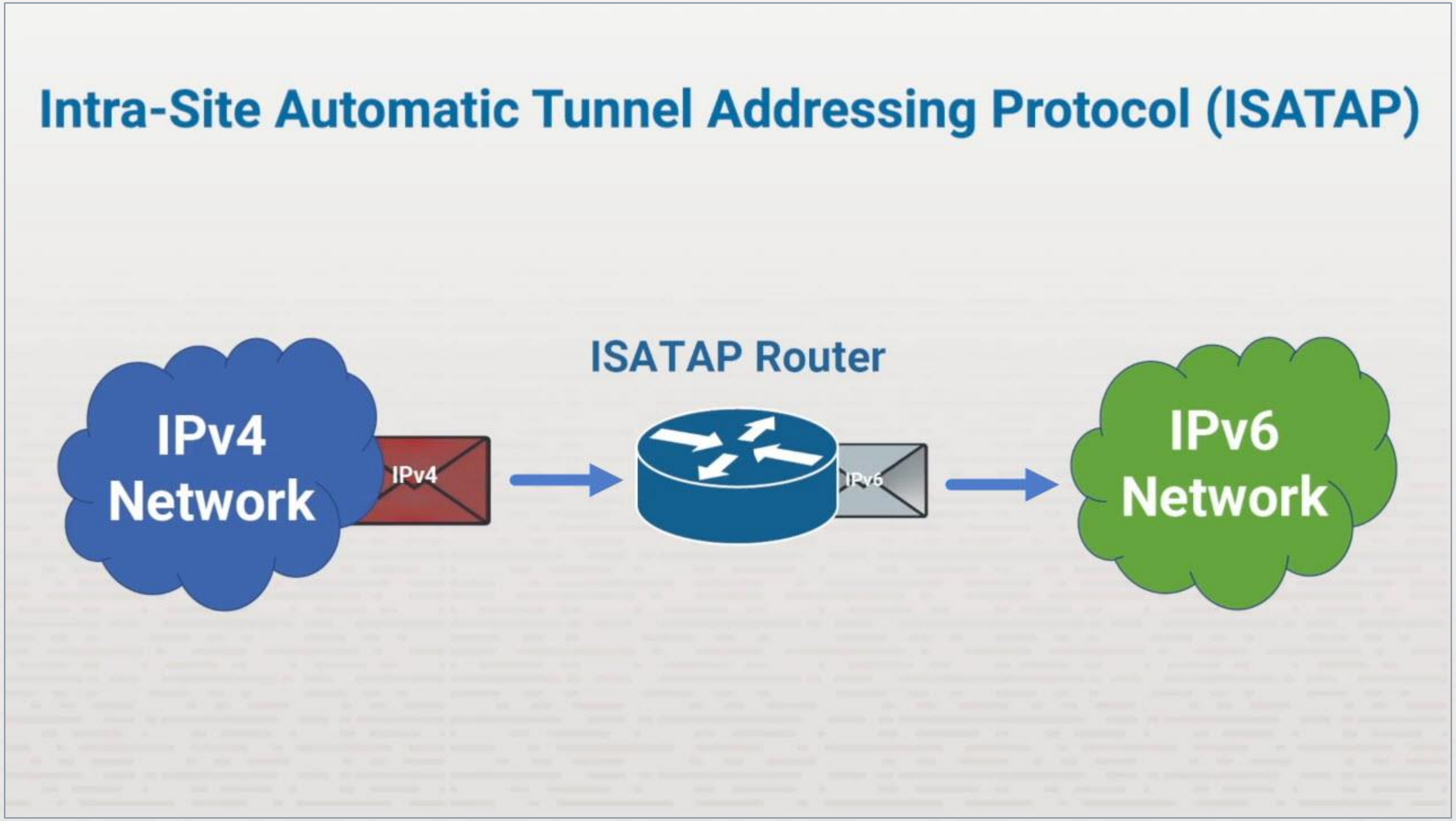
IP Version 6

4to6 Tunneling

- Sends IPv6 packets inside an IPv4 packet
- Encapsulation/decapsulation completed by each router



IP Version 6



TestOut

Summary

- IPv6 format
- IPv6 components
- IPv6 features

IPv6 Address Assignment

IPv6 Address Assignment

- IPv6 address types
- IPv6 address assignment

Link-Local IPv6 Addresses

- Valid only on local subnet
- Talk to host on same subnet
- Not forwarded by routers
- One will always be assigned
- Used for:
  - Automatic address configuration
  - Neighbor discover

IPv6 Address Assignment

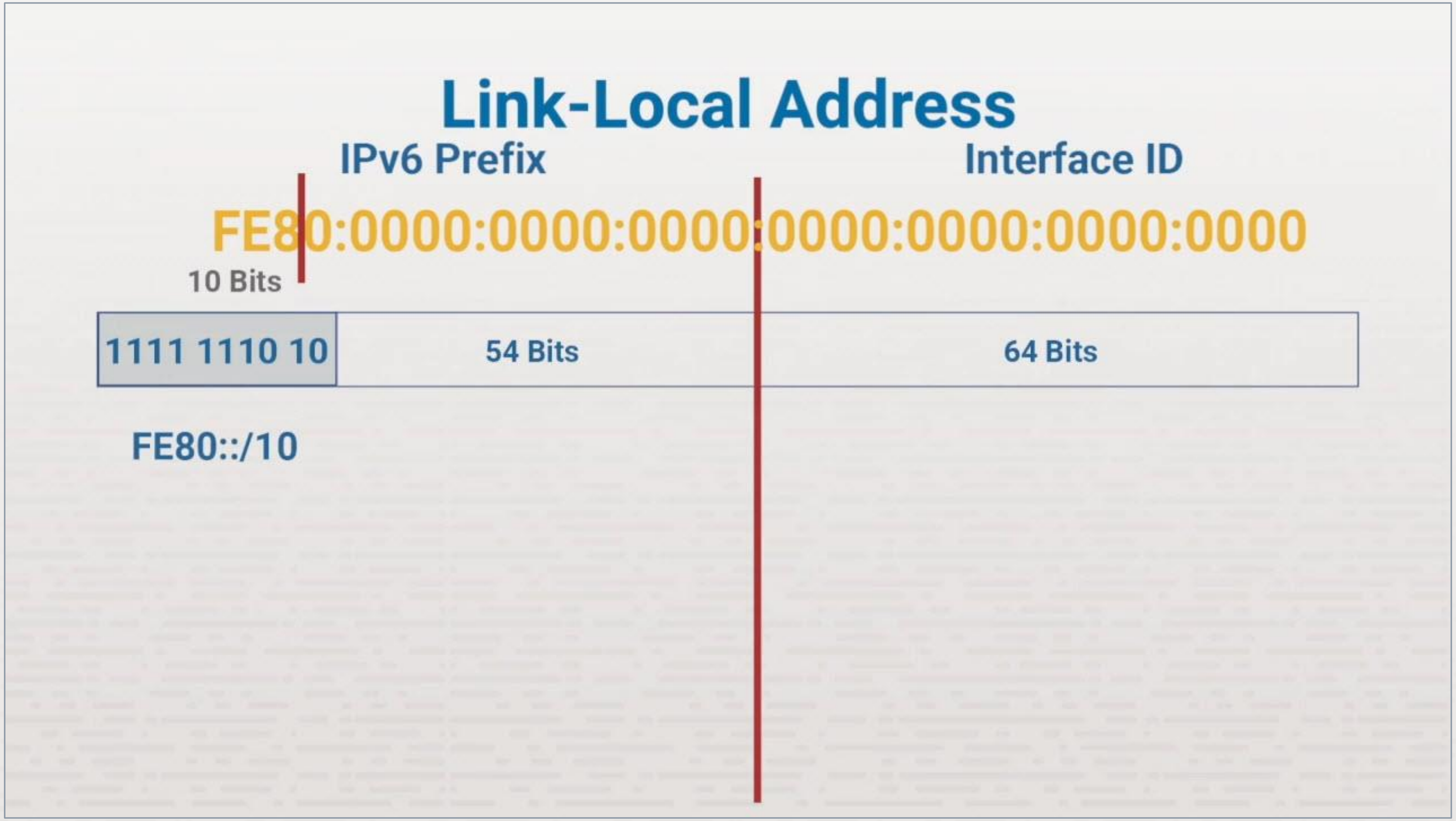
Link-Local IPv6 Address

- Starts with a hex value of FE
- The 10th bit must be 0
- Possible addresses can be:
  - FE8
  - FE9
  - FEA
  - FEB

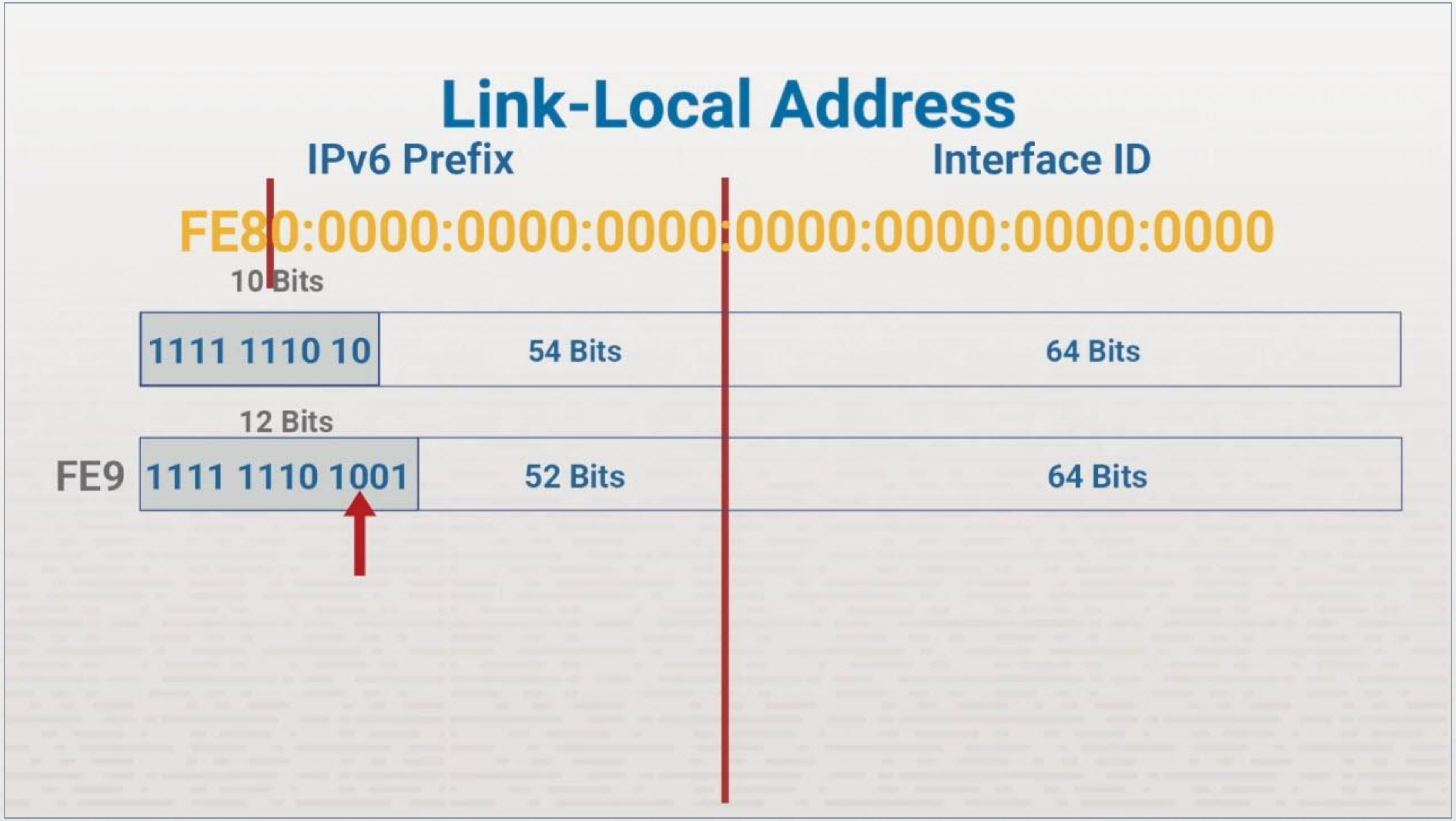
1111 1110 1000

10th Bit

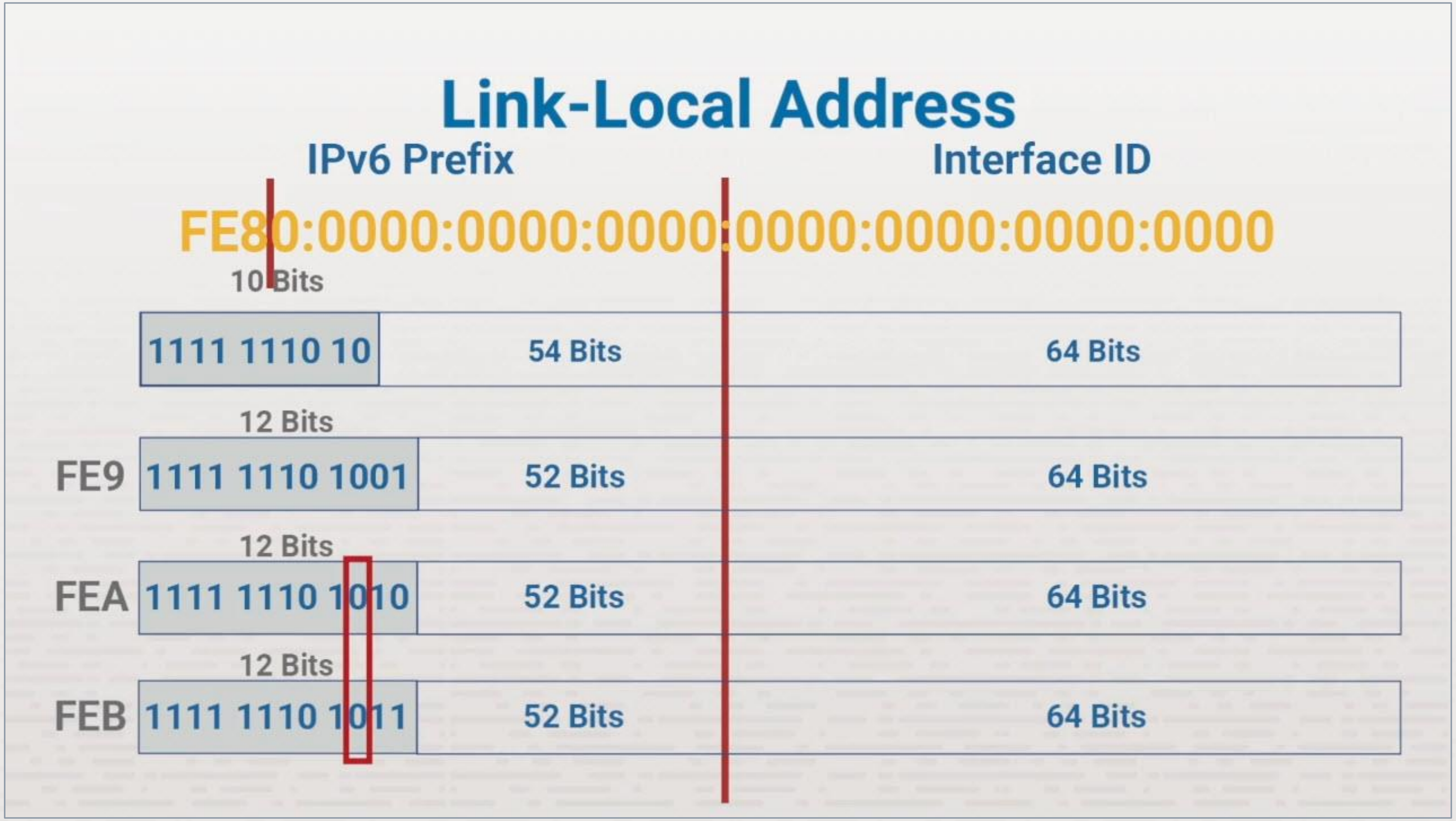
IPv6 Address Assignment



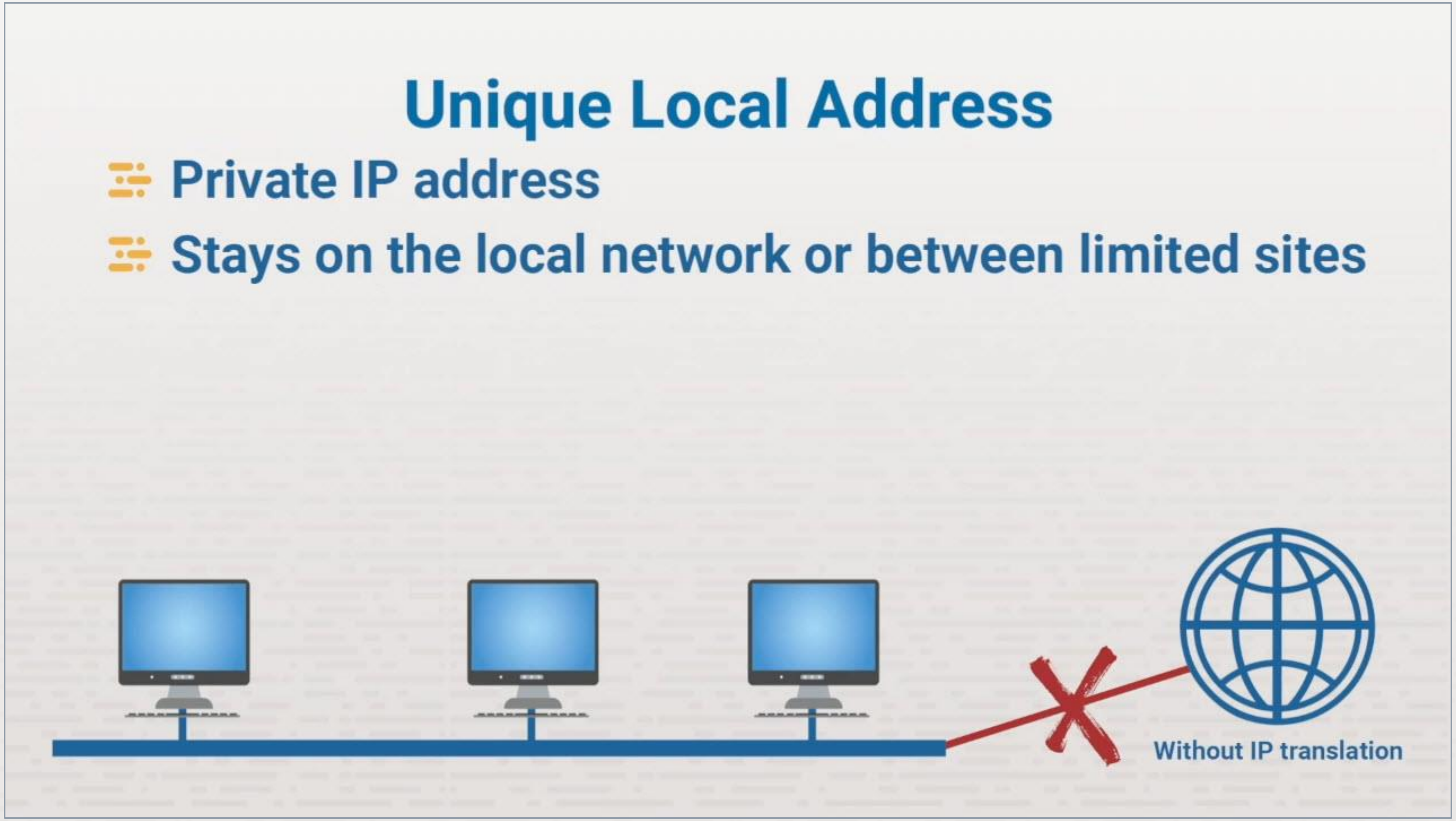
IPv6 Address Assignment



IPv6 Address Assignment



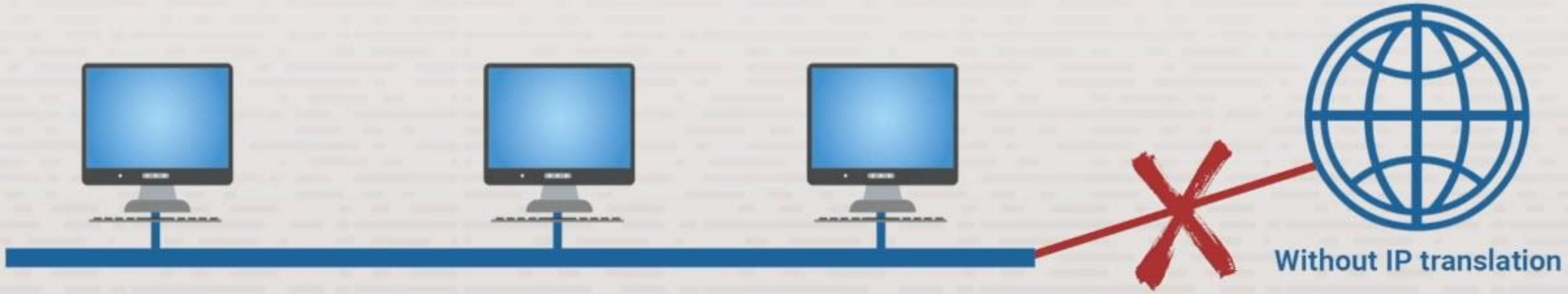
IPv6 Address Assignment



IPv6 Address Assignment

Unique Local Address

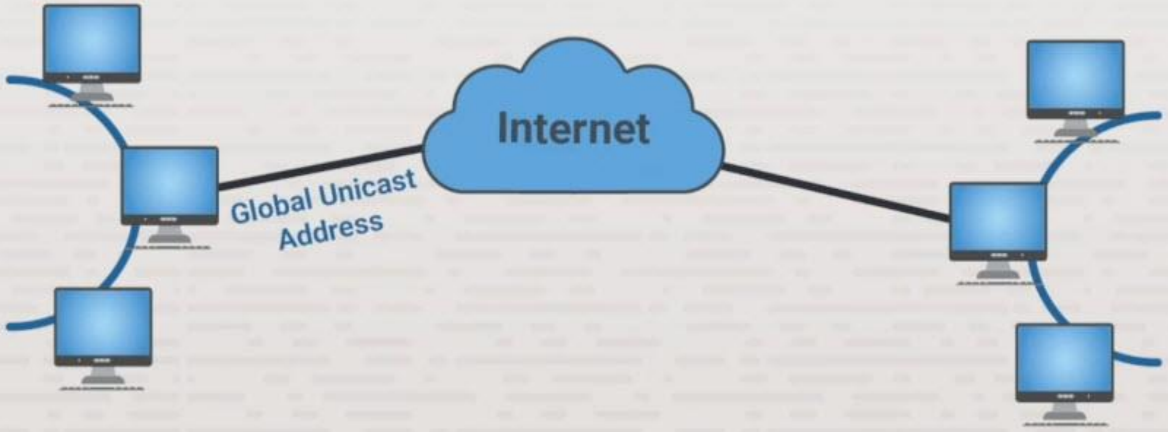
- Private IP address
- Stays on the local network or between limited sites
- Uses an FC00::/7 prefix
- Starts with either FC or FD
- Followed by the global ID



IPv6 Address Assignment

Global Unicast Address

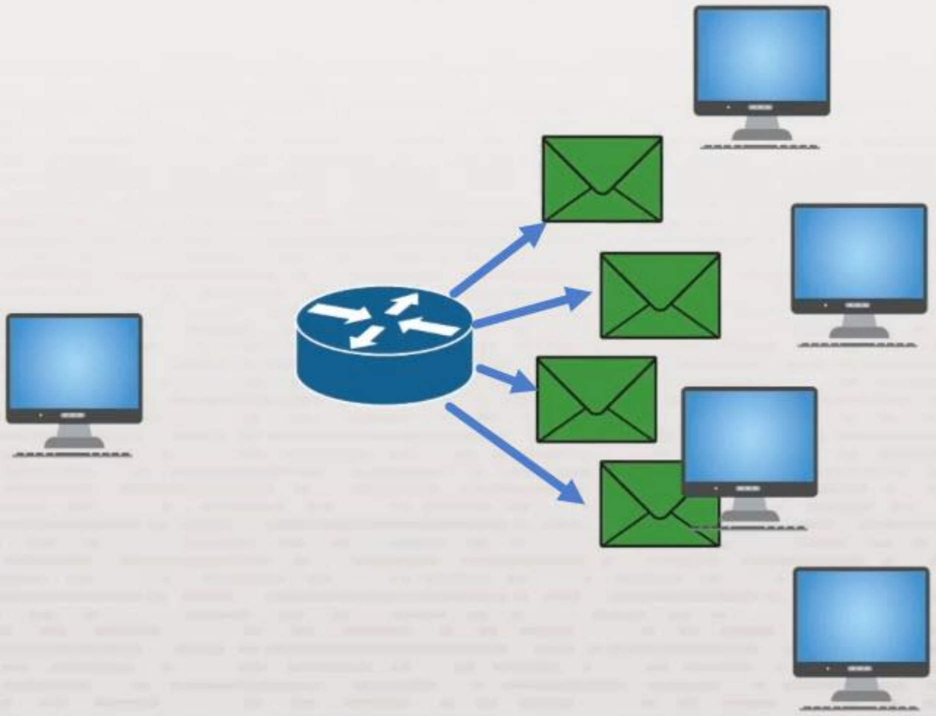
- Unique registered IPv6 address
- Global routing prefix assigned by ISP
- Used on public networks, such as the internet
- Uses a prefix of 2000::/3



IPv6 Address Assignment

Multicast Address

- One to many



IPv6 Address Assignment

Multicast Address

- One to many
- Unique for a set of devices
- FF00::/8 prefix
- Local multicast FF02::/16 prefix
- Examples:
  - FF02::1 identifies all nodes on the local network
  - FF02::2 identifies all nodes on the local network
  - FF02::1:2 identifies all DHCP servers or DHCP relay agents on the local network

IPv6 Address Assignment

IPv6 Address Assignment

IPv6 Address Assignment

Loopback Address

0000:0000:0000:0000:0000:0000:0000:0001/128

IPv6 Address Assignment

Loopback Address

- 0000:0000:0000:0000:0000:0000:0000:0001/128
  OR
  ::1/128

IPv6 Address Assignment

Loopback Address

- 0000:0000:0000:0000:0000:0000:0000:0001/128
  OR
  ::1/128
- Not assigned to an interface
- Used for testing and troubleshooting

IPv6 Address Assignment

IPv6 Address Assignment

Static Full Assignment

All configuration is manually assigned

Each device must be configured and maintained individually

IPv6 Address Assignment

IPv6 Address Assignment

Static Full Assignment	Static Partial Assignment
All configuration is manually assigned	Prefix is assigned manually
Each device must be configured and maintained individually	Interface ID uses modified EUI-64 format

IPv6 Address Assignment

IPv6 Address Assignment

Static Full Assignment	Static Partial Assignment	DHCPv6
All configuration is manually assigned Each device must be configured and maintained individually	Prefix is assigned manually Interface ID uses modified EUI-64 format	Stateful autoconfiguration →IP configuration is assigned using a DHCPv6 server Stateless autoconfiguration → uses SLAAC to obtain IPv6 address, but gets other needed information from DHCPv6 server

IPv6 Address Assignment

IPv6 Address Assignment

Static Full Assignment	Static Partial Assignment	DHCPv6	Stateless Address Autoconfiguration (SLAAC)
All configuration is manually assigned Each device must be configured and maintained individually	Prefix is assigned manually Interface ID uses modified EUI-64 format	Stateful autoconfiguration →IP configuration is assigned using a DHCPv6 server Stateless autoconfiguration → uses SLAAC to obtain IPv6 address, but gets other needed information from DHCPv6 server	Device generates a link-local address DAD process checks that address is unique Device sends RS message to multicast Router responds with global unicast address prefix Combines this with interface ID for address

Summary

- IPv6 address types:
  - Link-local
  - Unique local
  - Multicast
  - Anycast
  - Loopback
- Assignment methods:
  - Static full/partial
  - Stateful autoconfiguation
- SLACC

In-Class Practice

Do the following labs:

- 4.7.8 Configure an IPv6 Address

Class Discussion

- Why is IPv6 needed?
- What is the format of a IPv6 address?
- How can an IPv6 address be simplified?
- What are the two parts of an IPv6 address?
- What allows IPv6 hosts to communicate over an IPv4 network?
- What is the difference between stateful autoconfiguration and stateless autoconfiguration?

Multicast

Key Terms

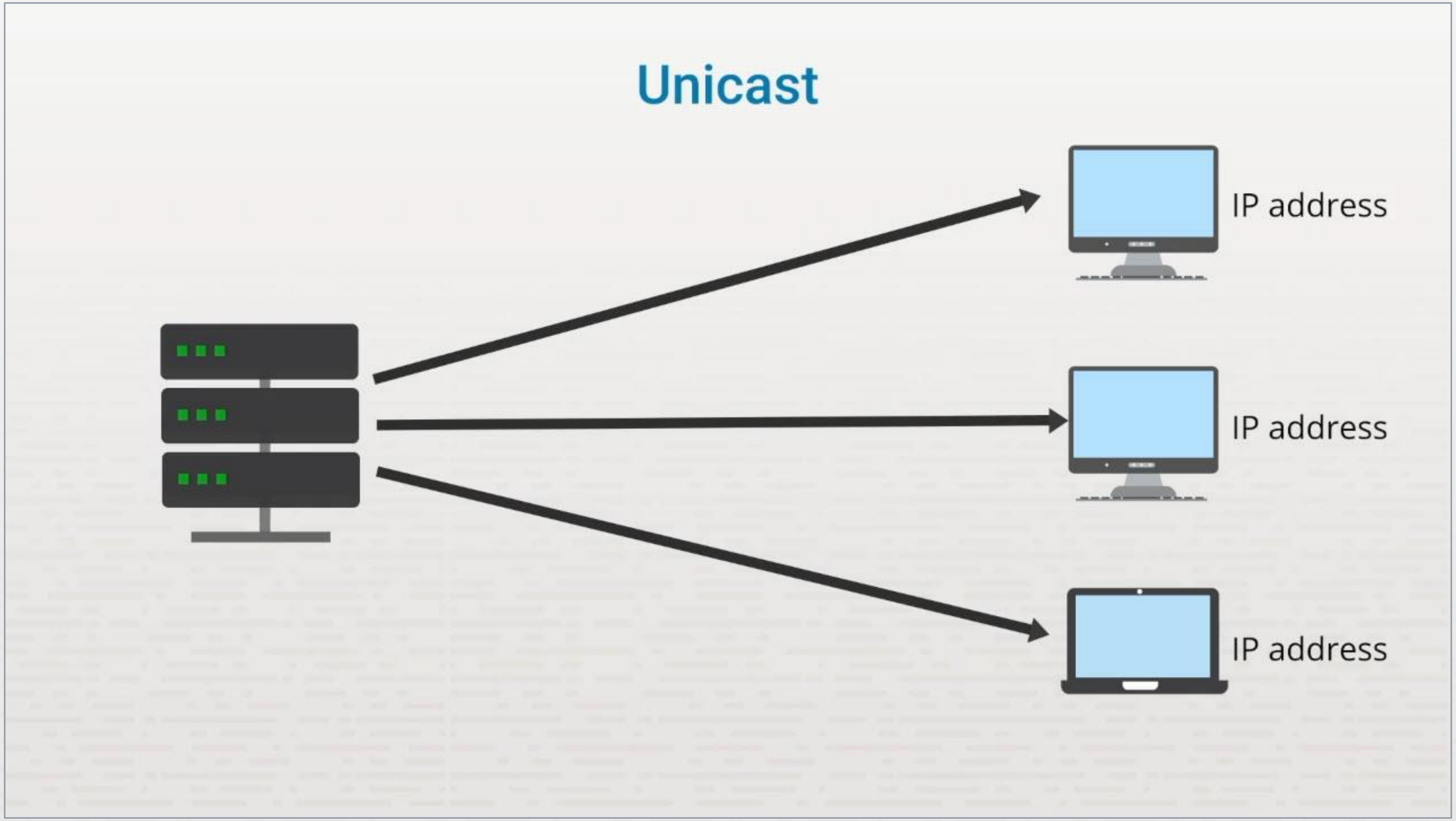
- Unicast
- Broadcast
- IGMP

Key Definitions

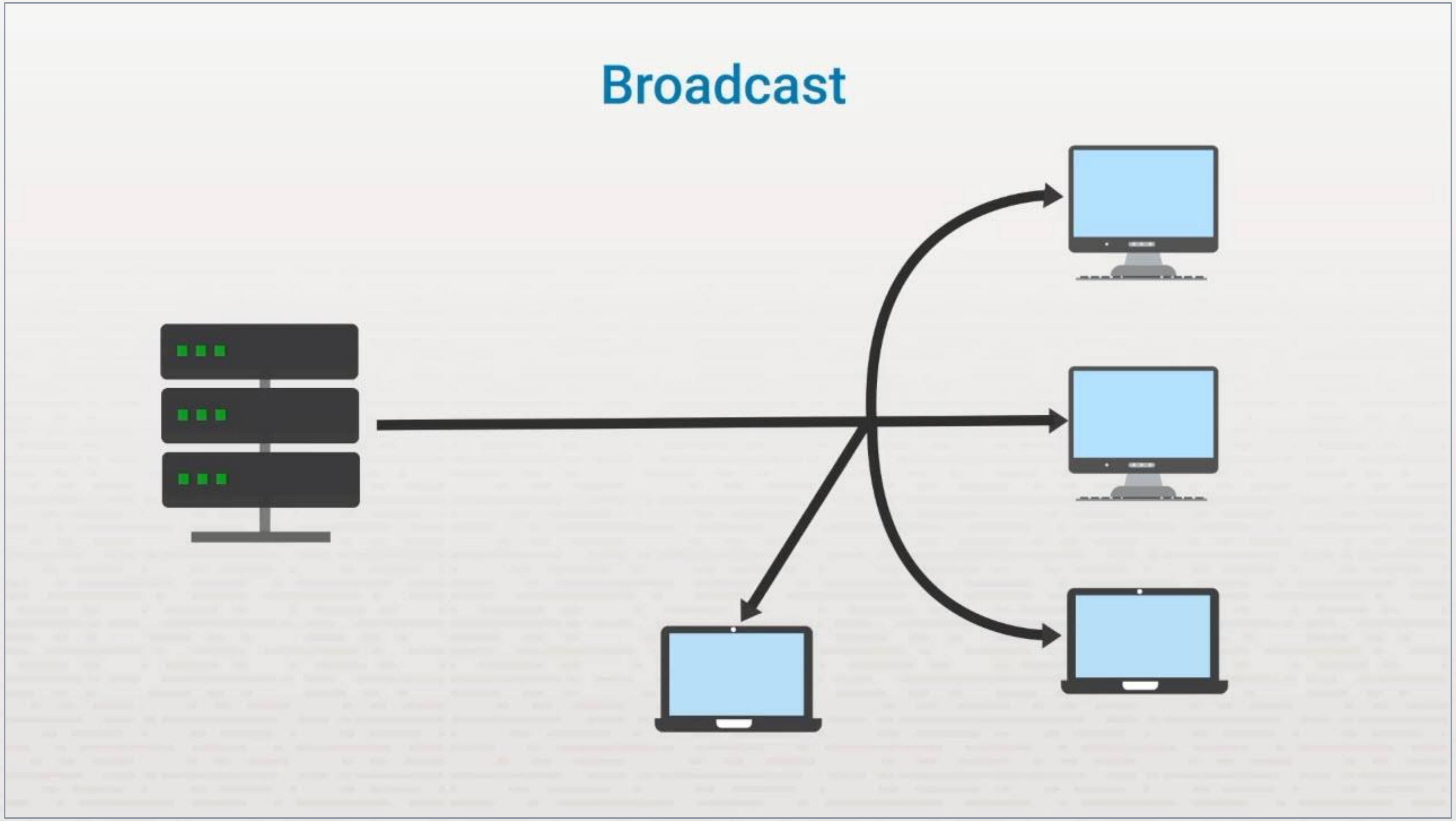
- **Unicast:** Messages that are sent to a specific host address. The sending device must know the IP address of all recipients and must create a separate packet for each destination device.
- **Broadcast:** A single packet that, when sent, is processed by all hosts. Broadcast packets are not typically forwarded by routers, so broadcast traffic is limited to within a single subnet.
- **IGMP:** The Internet Group Management Protocol (IGMP) is used to identify group members and to forward multicast packets on to the segments where group members reside.

Multicast

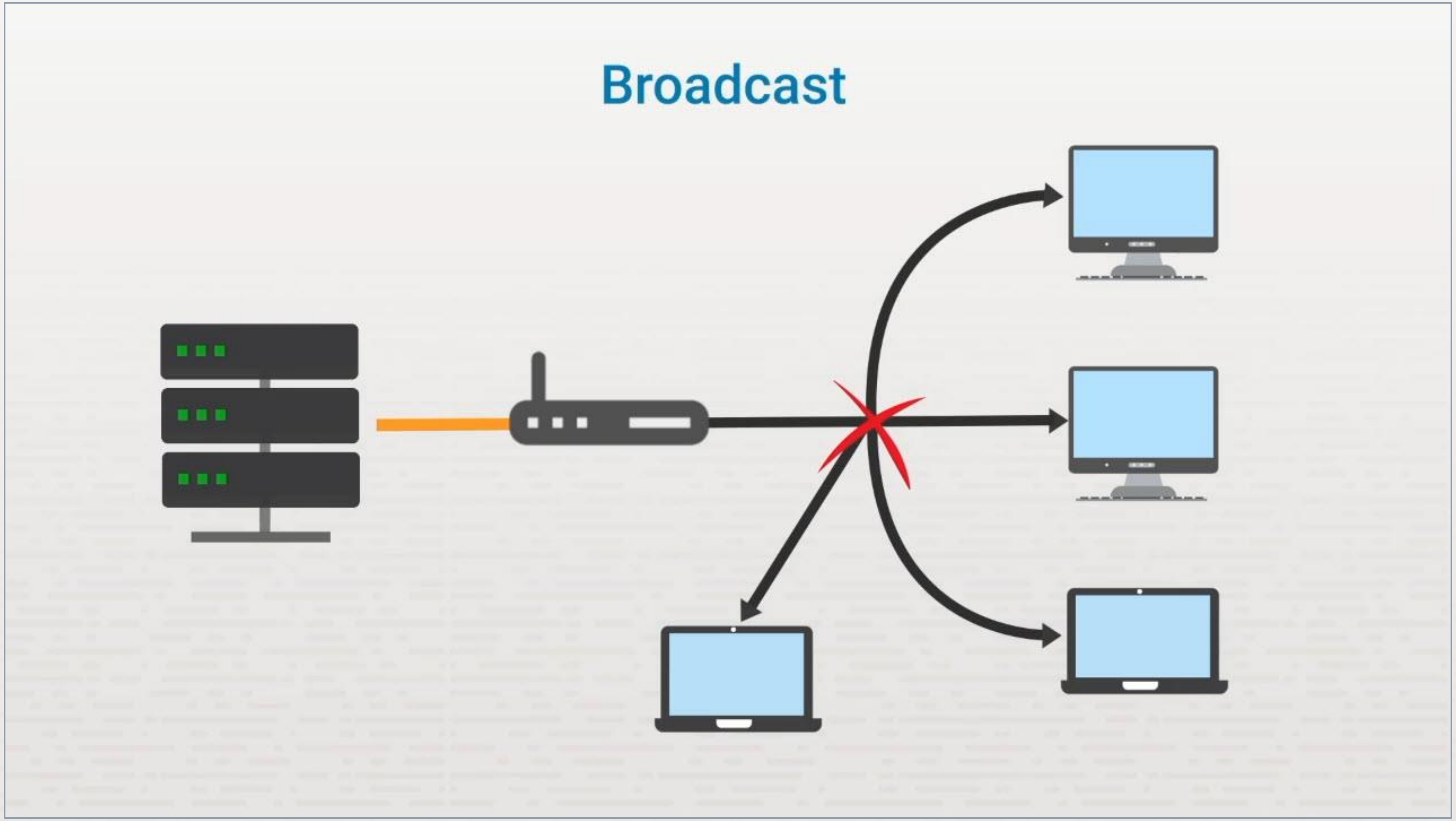
Multicast



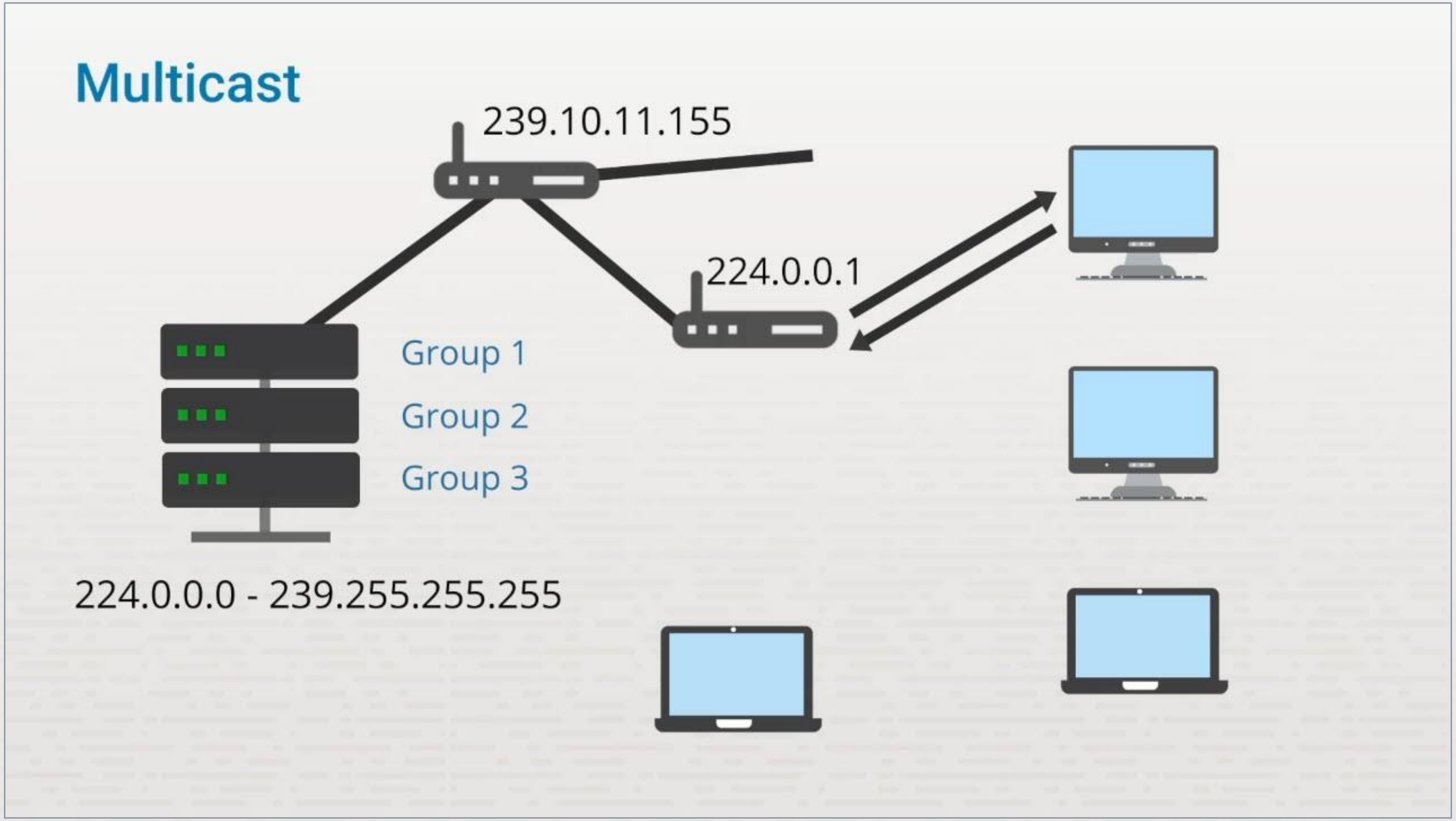
Multicast



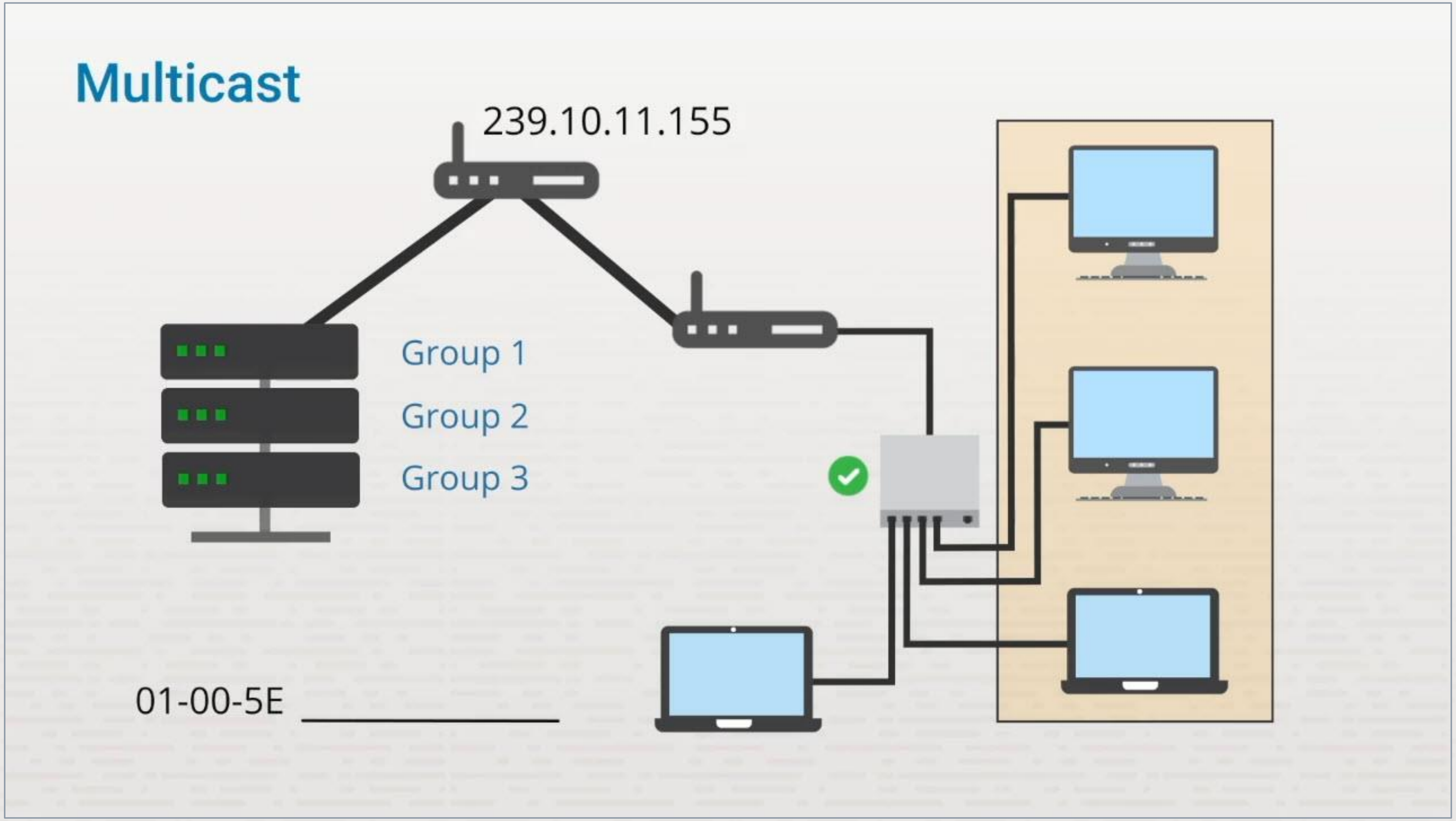
Multicast



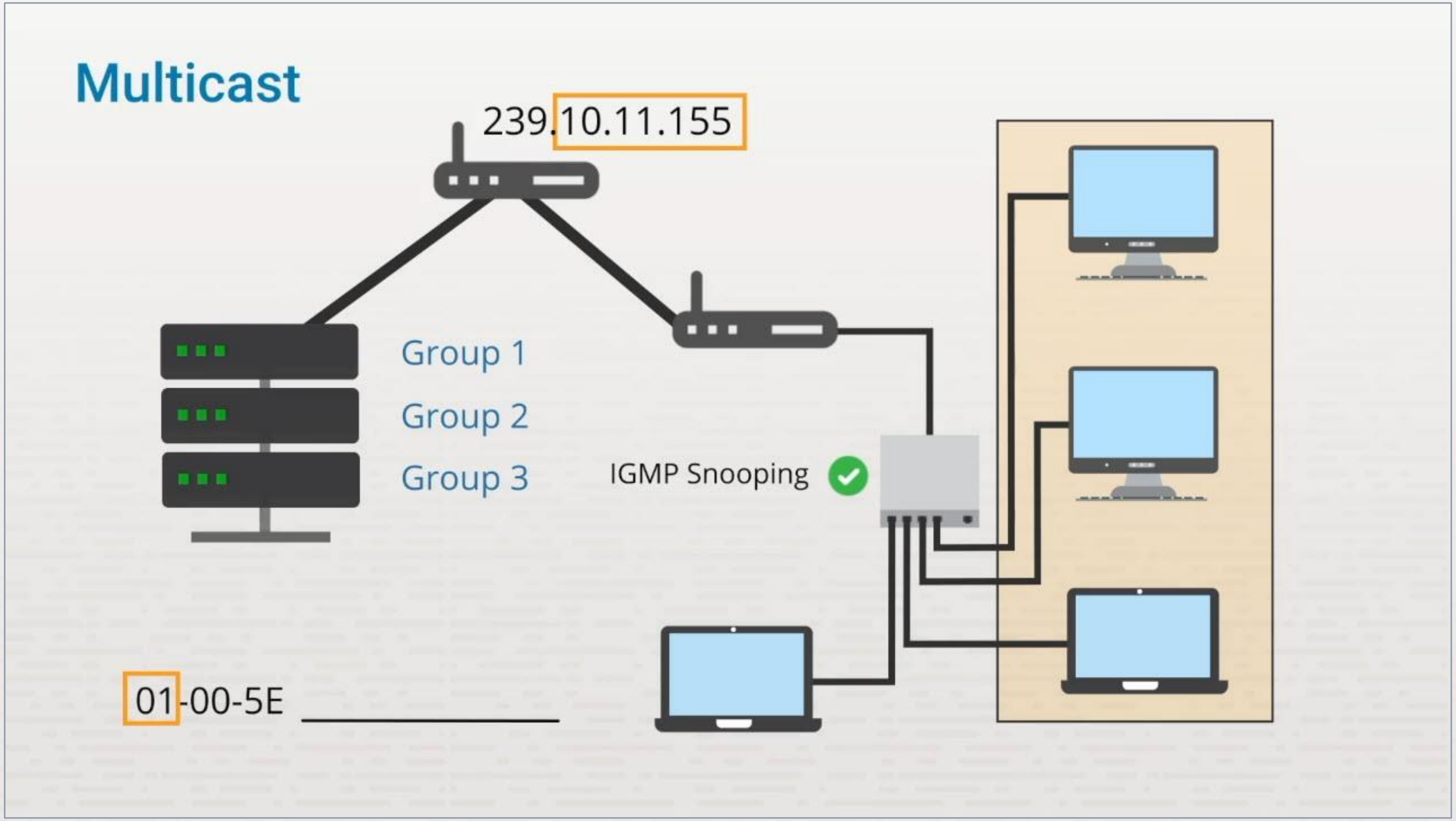
Multicast


Multicast
239.10.11.155
224.0.0.1
Group 1
Group 2
Group 3
224.0.0.0 - 239.255.255.255

Multicast



Multicast

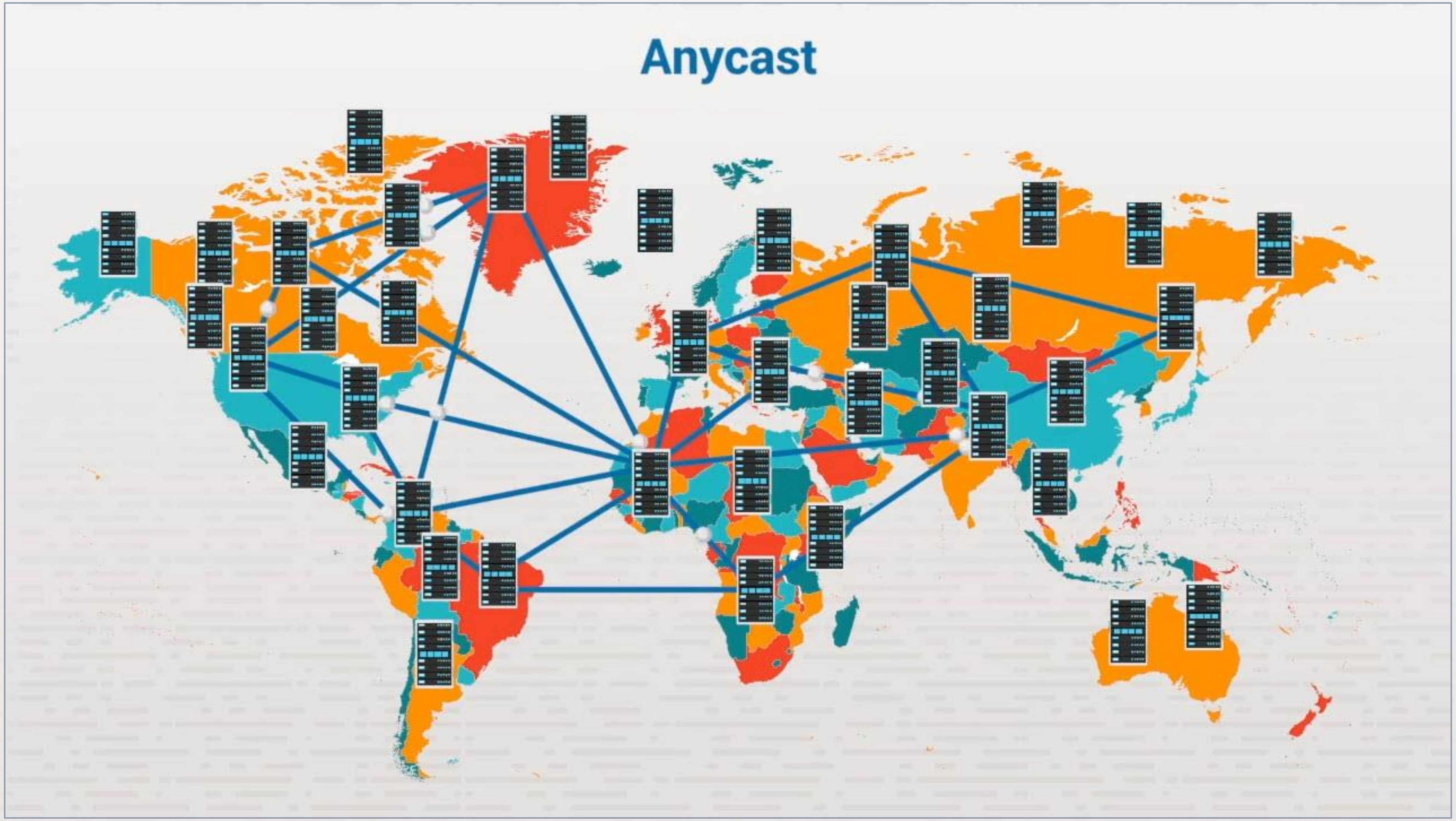


Multicast
239.10.11.155
Group 1
Group 2
Group 3
IGMP Snooping
01-00-5E

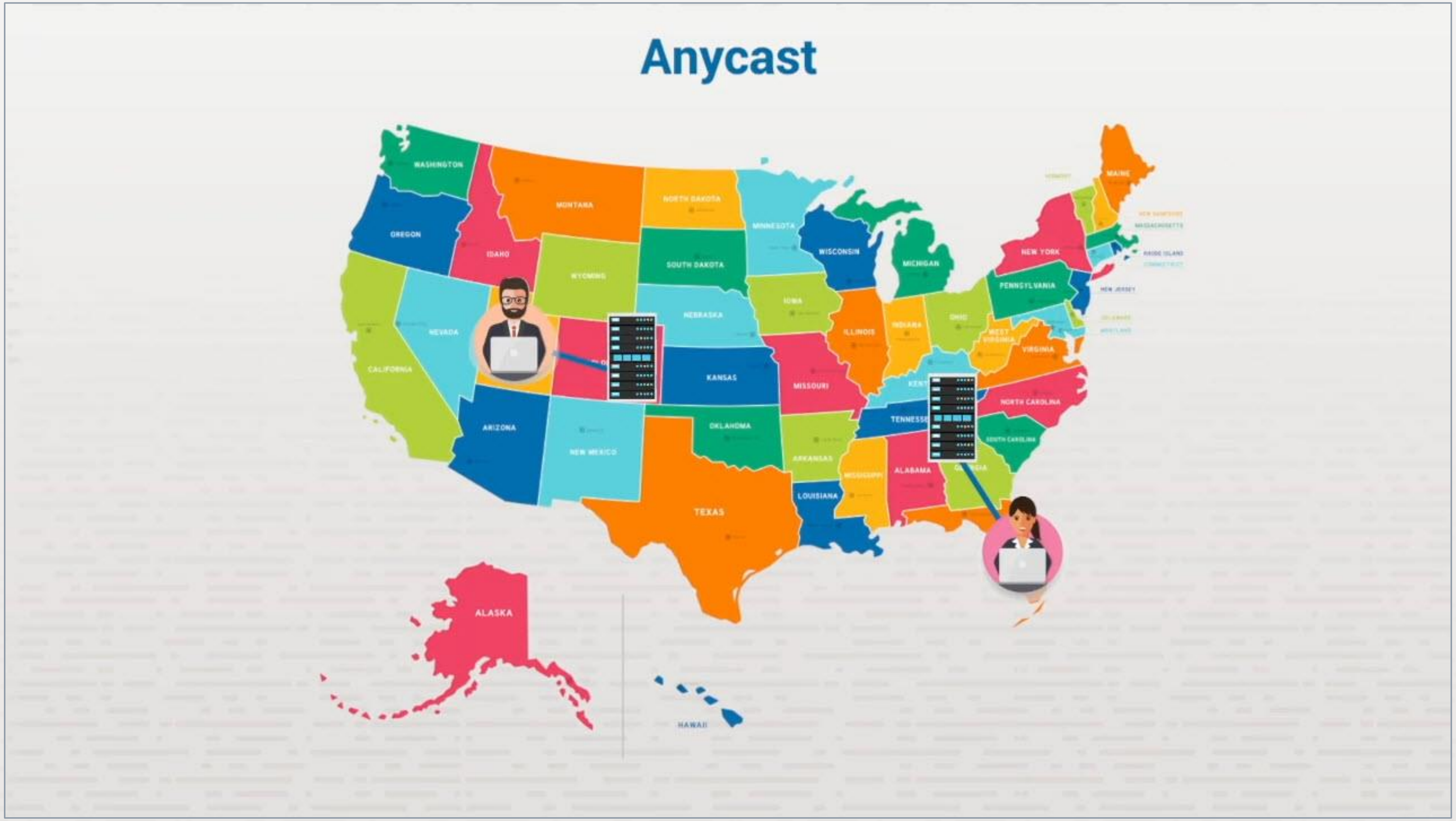
Anycast

- For IPv6 only
- Servers share IP address
- Data routed to nearest server
- Advantages:
  - Speed
  - Redundancy
  - DDoS mitigation
- Disadvantages:
  - Difficult to implement

Multicast



Multicast


Anycast
WASHINGTON
OREGON
IDAHO
MONTANA
NORTH DAKOTA
SOUTH DAKOTA
MINNESOTA
WISCONSIN
MICHIGAN
NEW YORK
PENNSYLVANIA
WYOMING
NEBRASKA
IOWA
ILLINOIS
INDIANA
OHIO
NEVADA
CALIFORNIA
KANSAS
MISSOURI
VIRGINIA
NORTH CAROLINA
ARIZONA
NEW MEXICO
OKLAHOMA
ARKANSAS
TENNESSEE
SOUTH CAROLINA
ALABAMA
LOUISIANA
TEXAS
ALASKA
HAWAII

Border Gateway Protocol (BGP)

- Same address to multiple servers
- Defines different routes

Summary

- Unicast
- Broadcast
- Multicast
- Anycast

Class Discussion

- How does multicast differ from unicast and broadcast?
- What is the IP address range reserved for multicast groups?
- What does a regular switch do when it receives a multicast frame?
- Which device would you configure to prevent multicast traffic from being sent to non-group members?

4.9 NETWORK ADDRESSING AND SERVICES

Troubleshoot IP Configuration Issues

Section Skill Overview

- Use ipconfig
- Use the ip command
- Explore IP configuration
- Troubleshoot IP configuration

Key Terms

- APIPA
- DHCP
- DNS
- Rogue DHCP server

Key Definitions

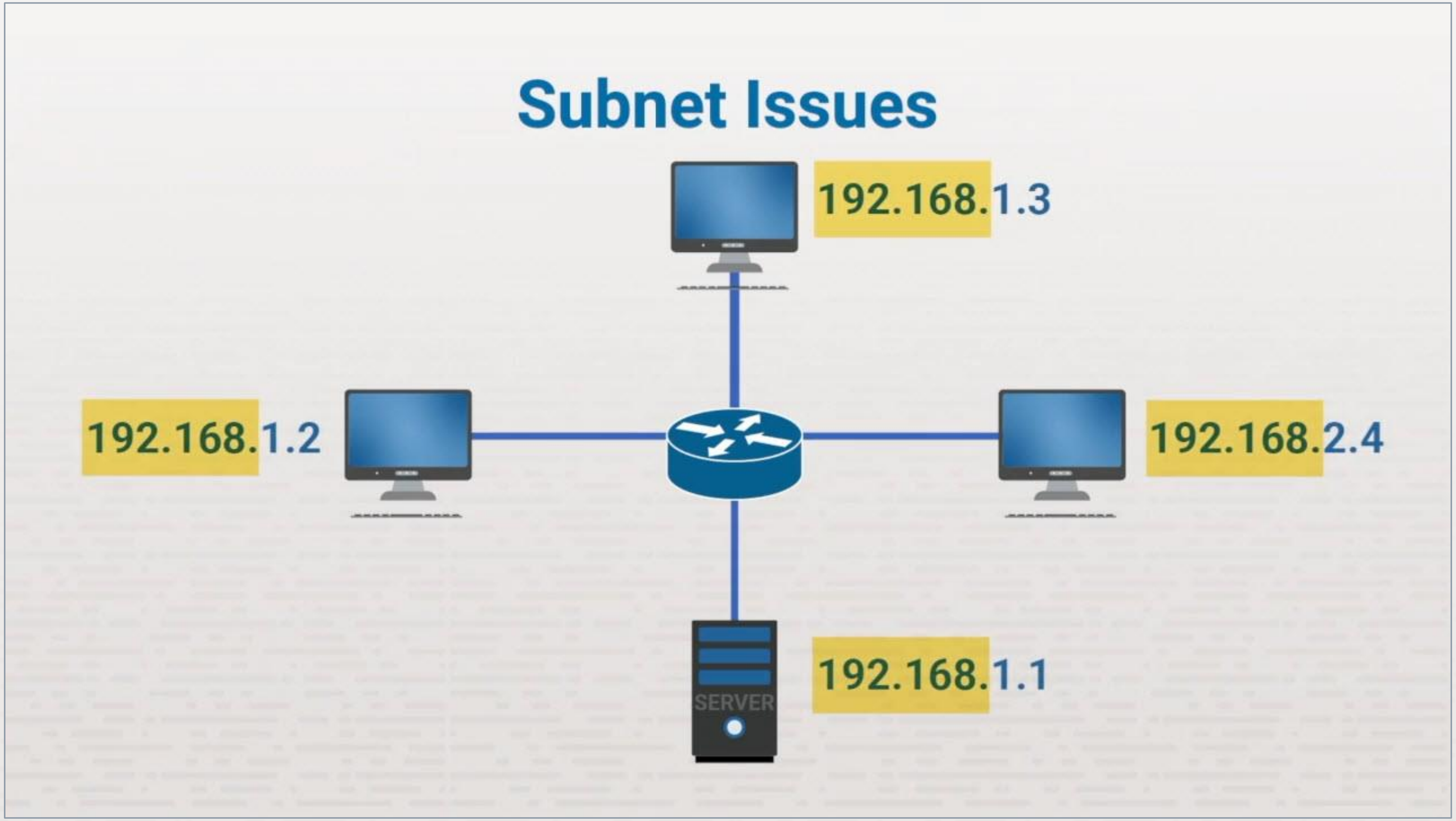
- **APIPA:** Automatic Private IP Addressing (APIPA) is the Windows function that provides DHCP autoconfiguration addressing.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a protocol used to centrally manage the distribution of IP addresses within a network.
- **DNS:** DNS stands for Domain Name System. The main function of DNS is to translate domain names into IP addresses, which computers can understand.
- **Rogue DHCP server:** A rogue DHCP server is an unauthorized DHCP server on the network.

IP Configuration Troubleshooting

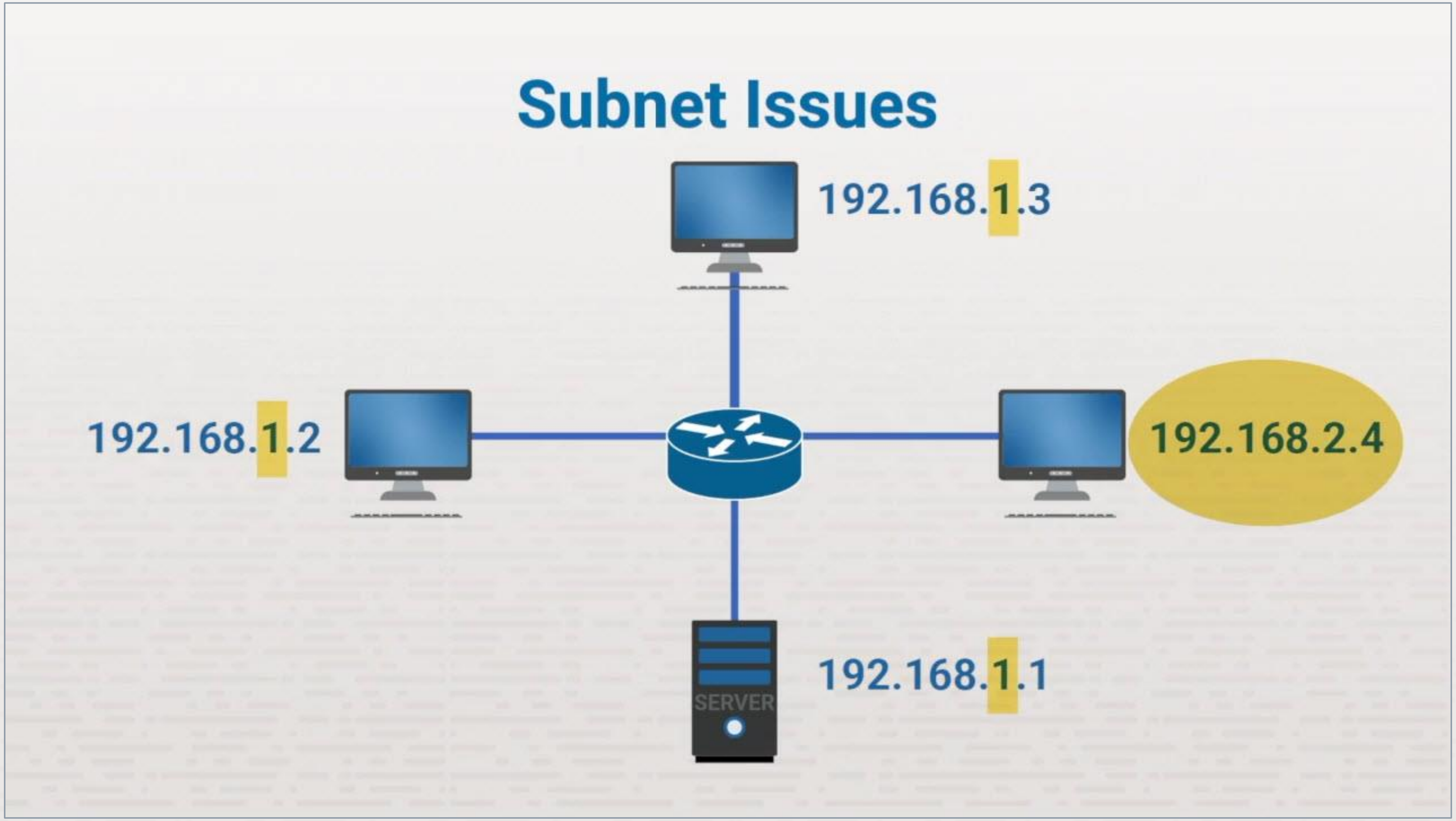
IP Configuration Troubleshooting

- Improper IP configuration
- DHCP issues

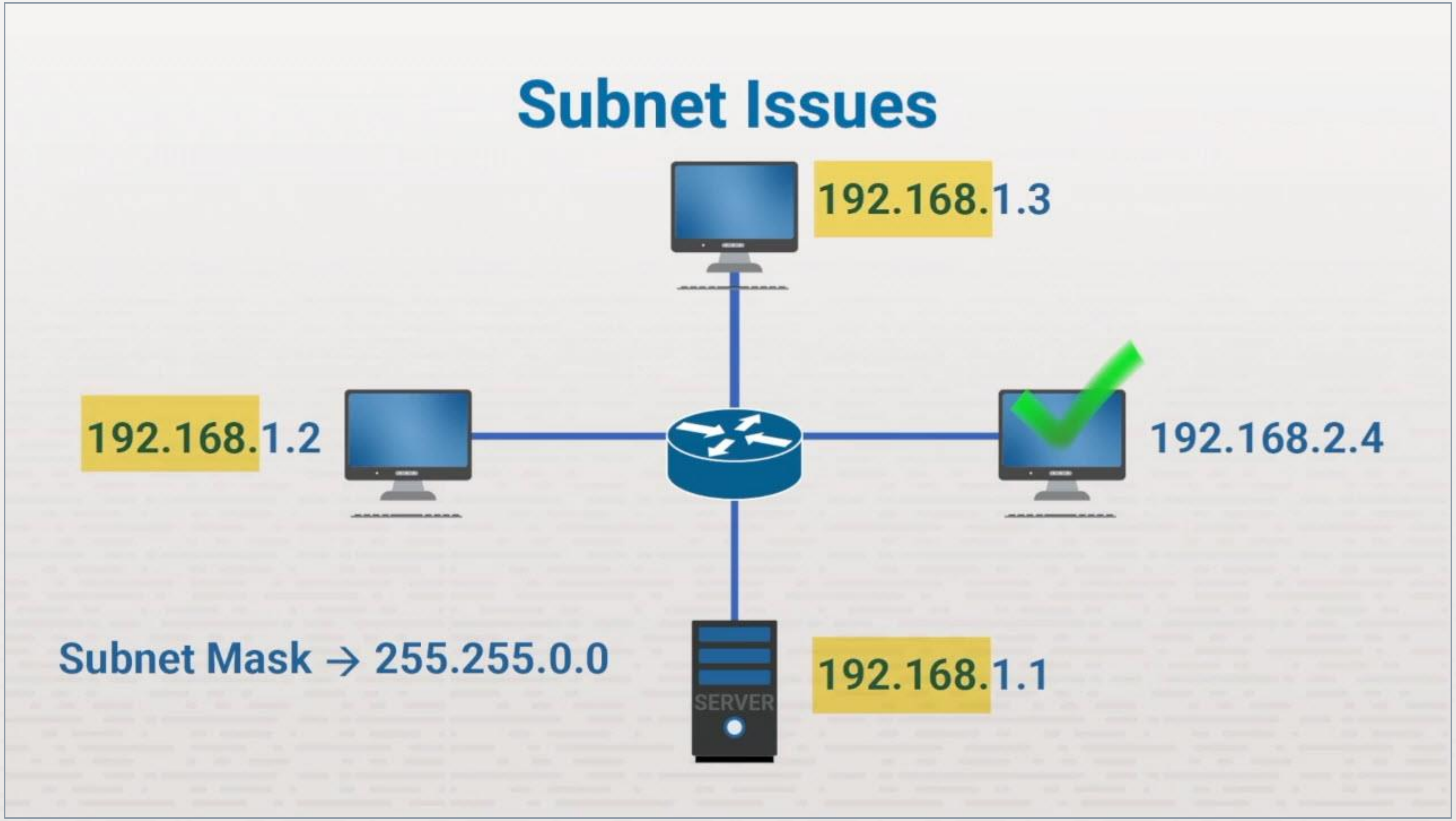
IP Configuration Troubleshooting



IP Configuration Troubleshooting

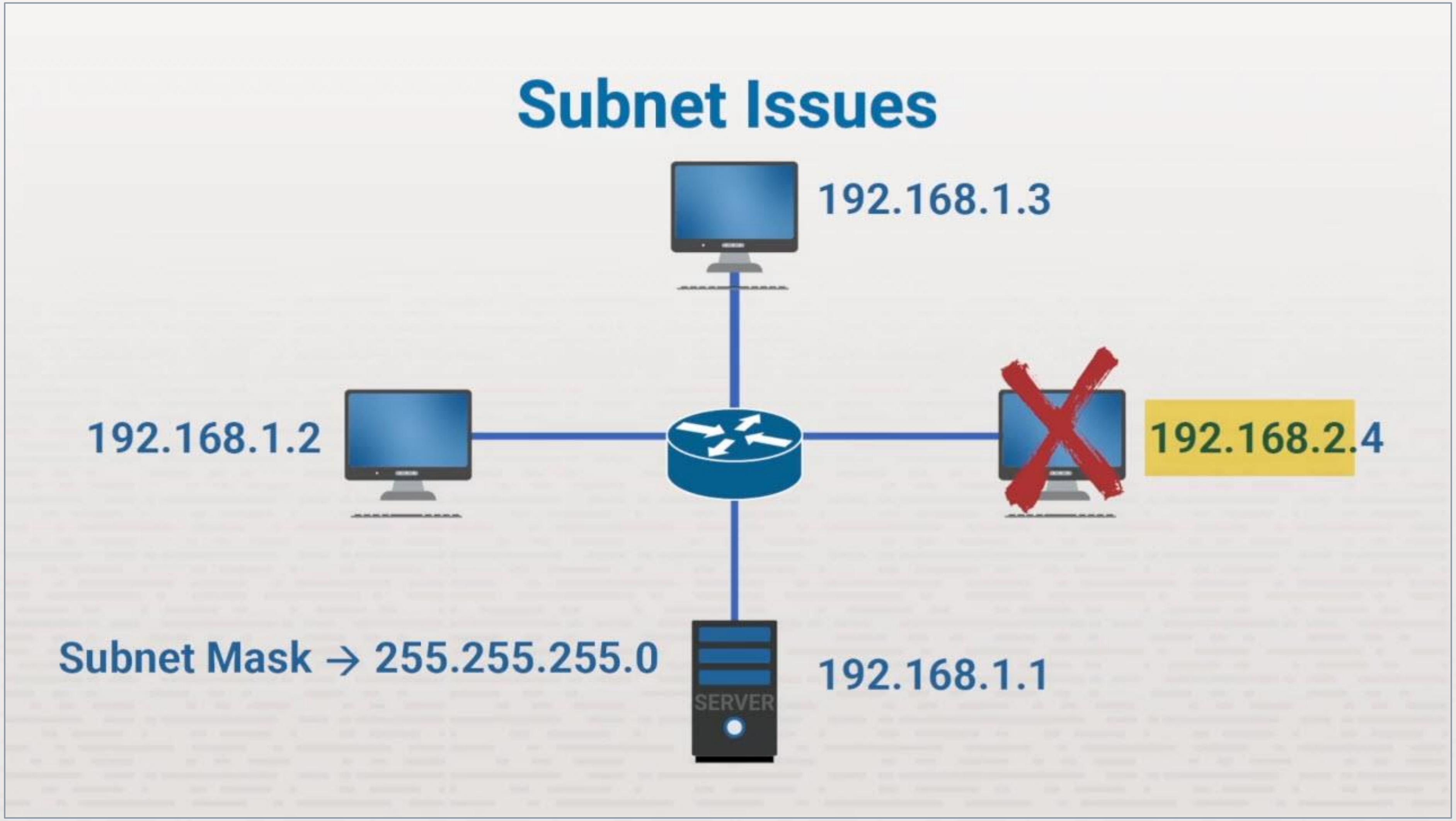


IP Configuration Troubleshooting



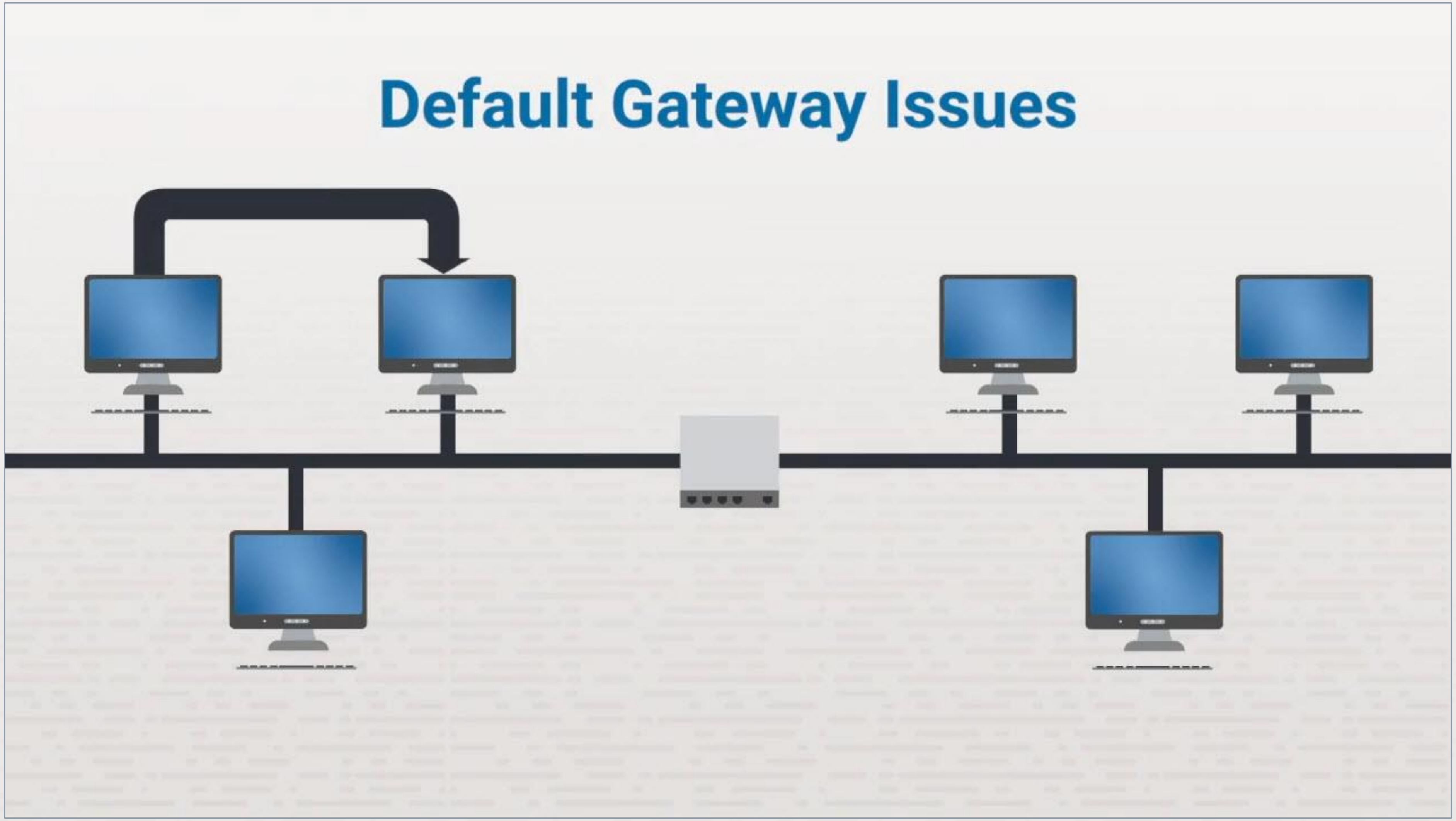
TestOut

IP Configuration Troubleshooting



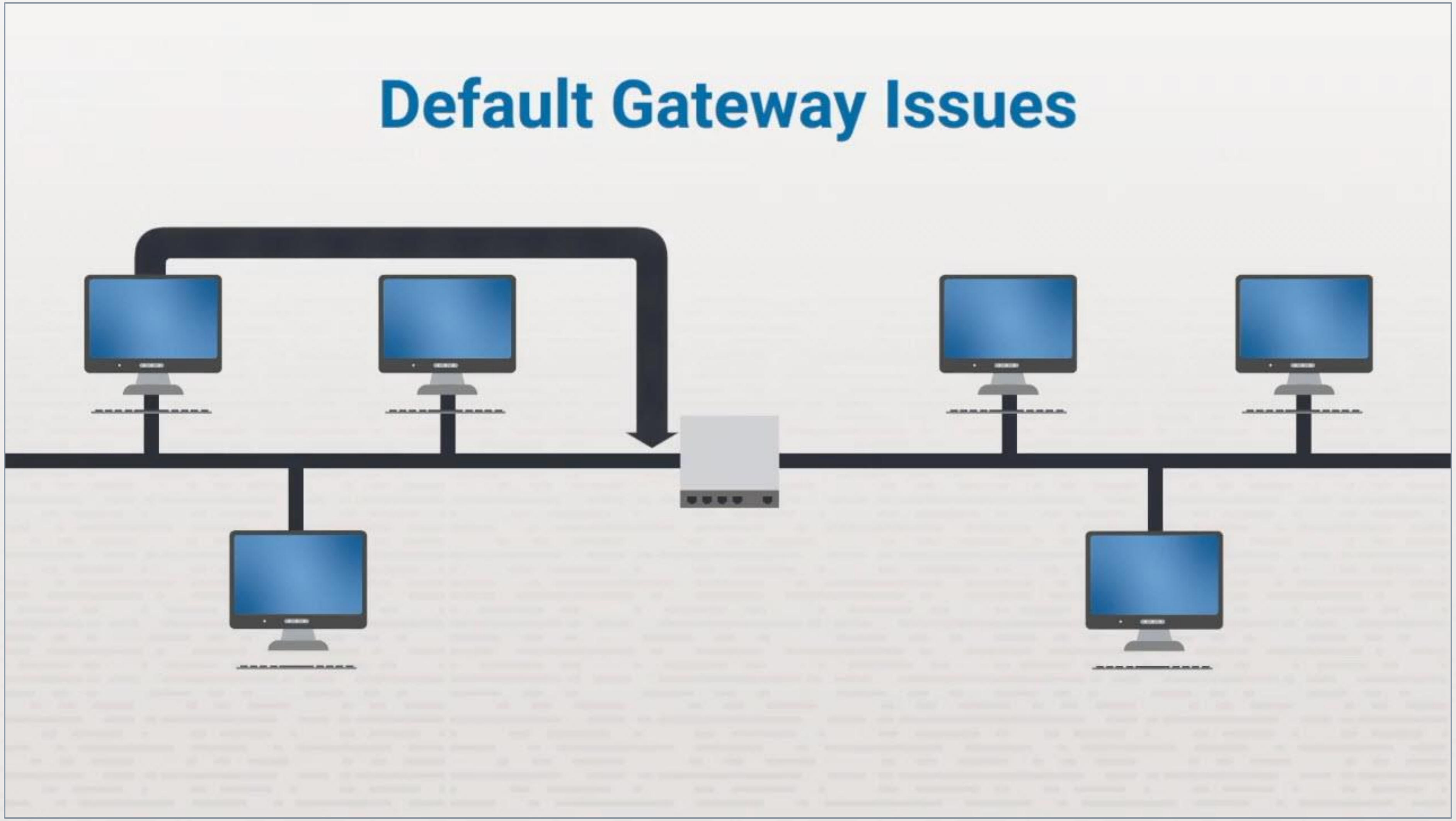
TestOut

IP Configuration Troubleshooting

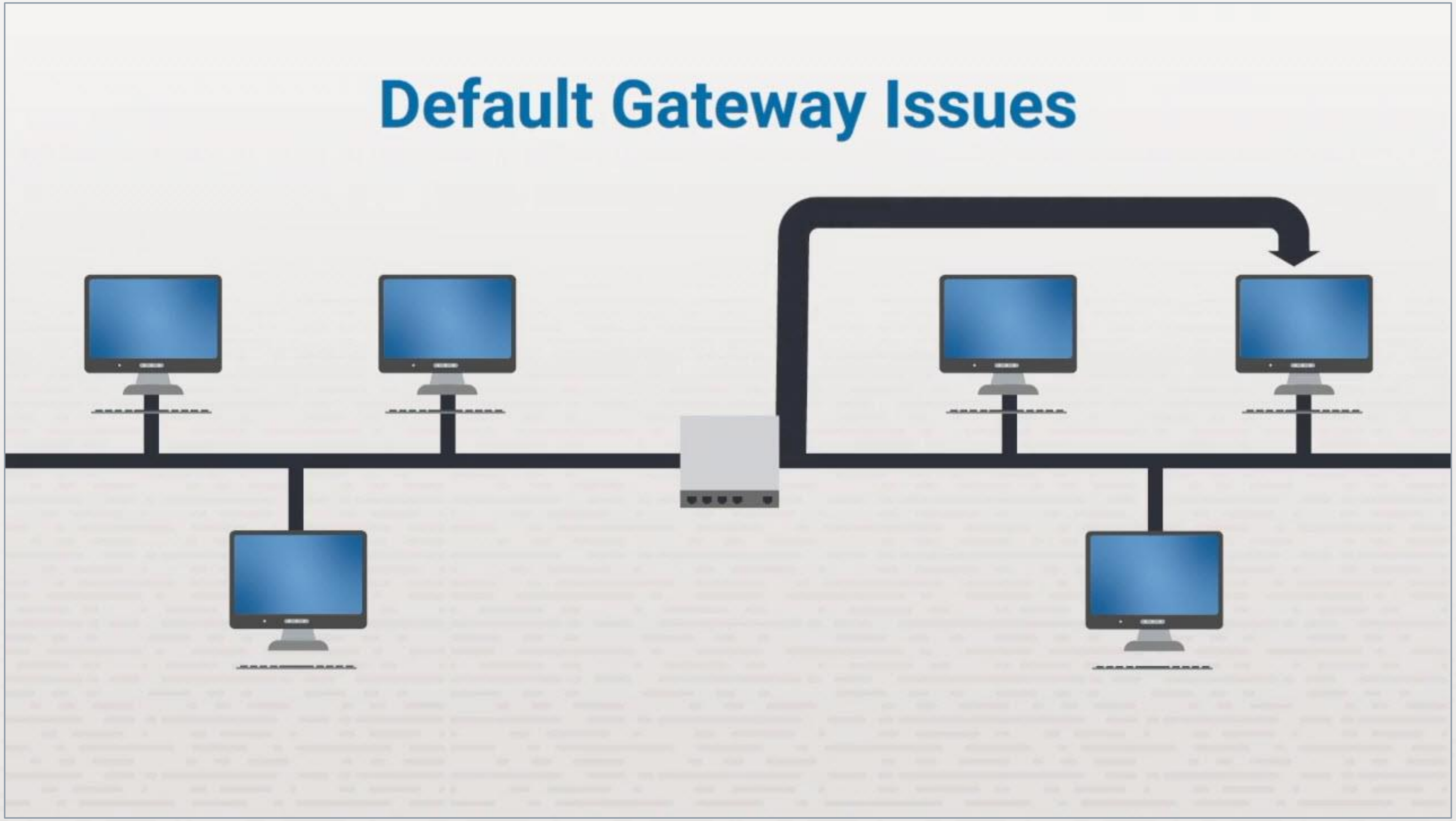


TestOut

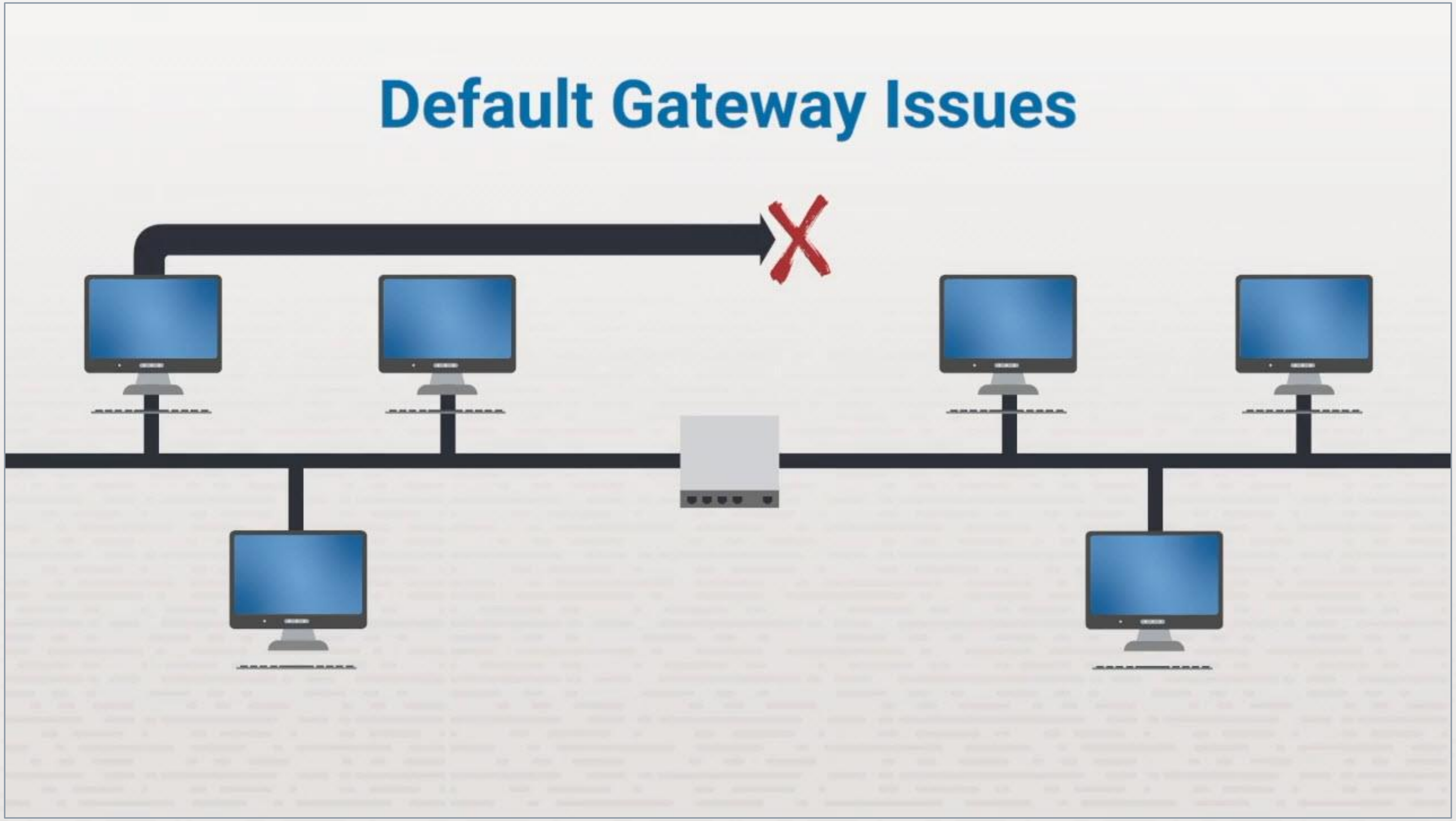
IP Configuration Troubleshooting



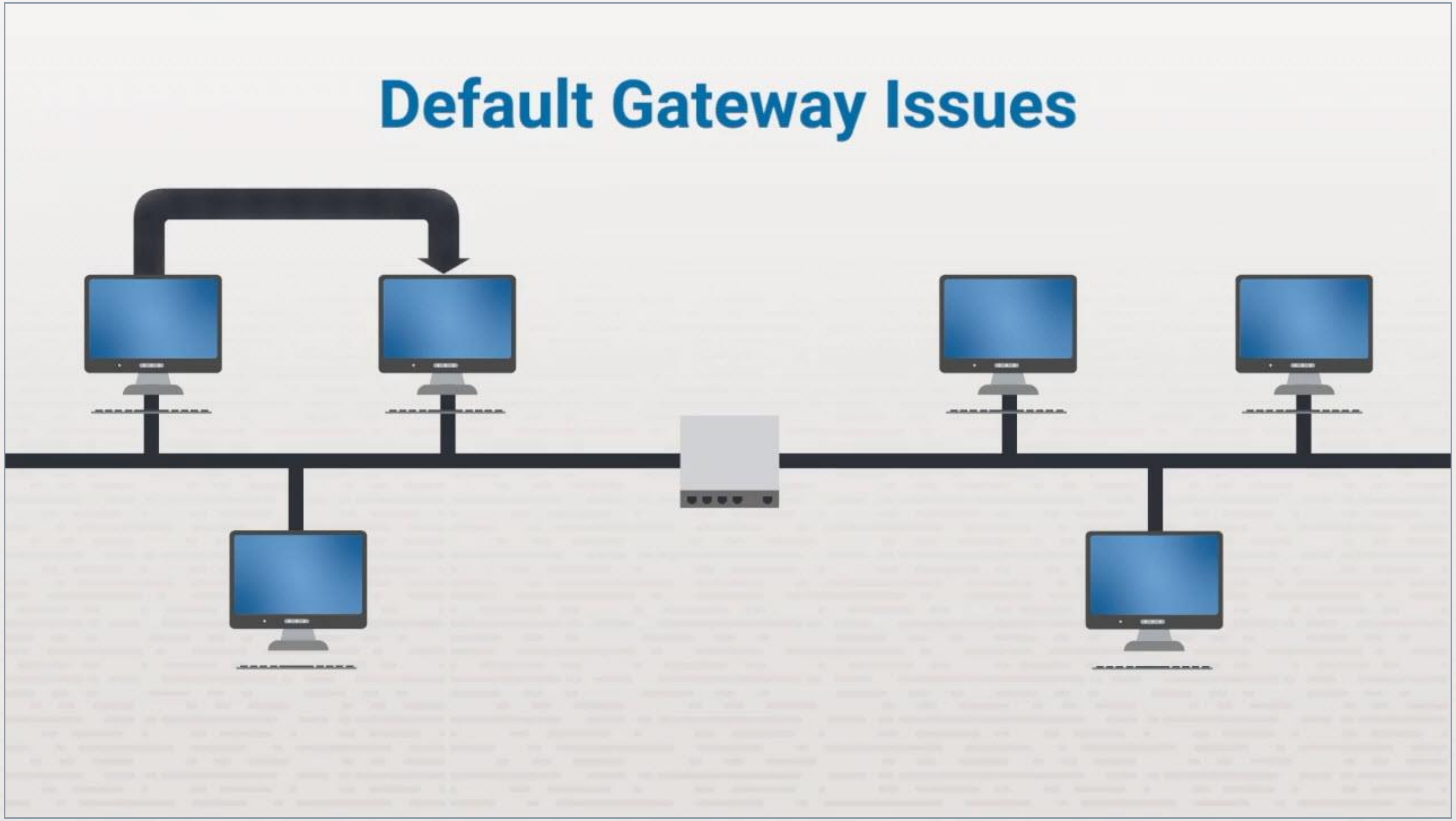
IP Configuration Troubleshooting



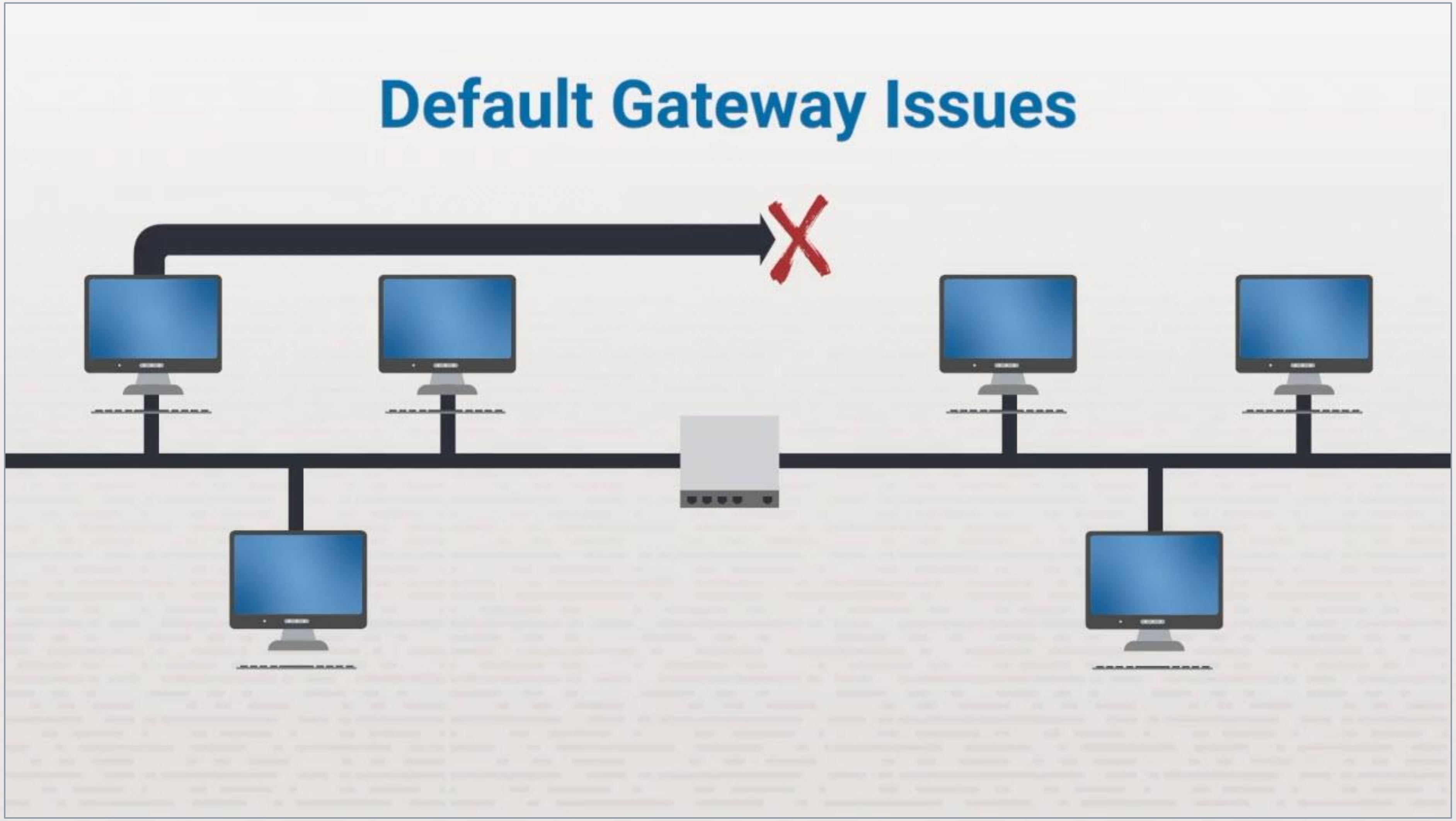
IP Configuration Troubleshooting



IP Configuration Troubleshooting



IP Configuration Troubleshooting

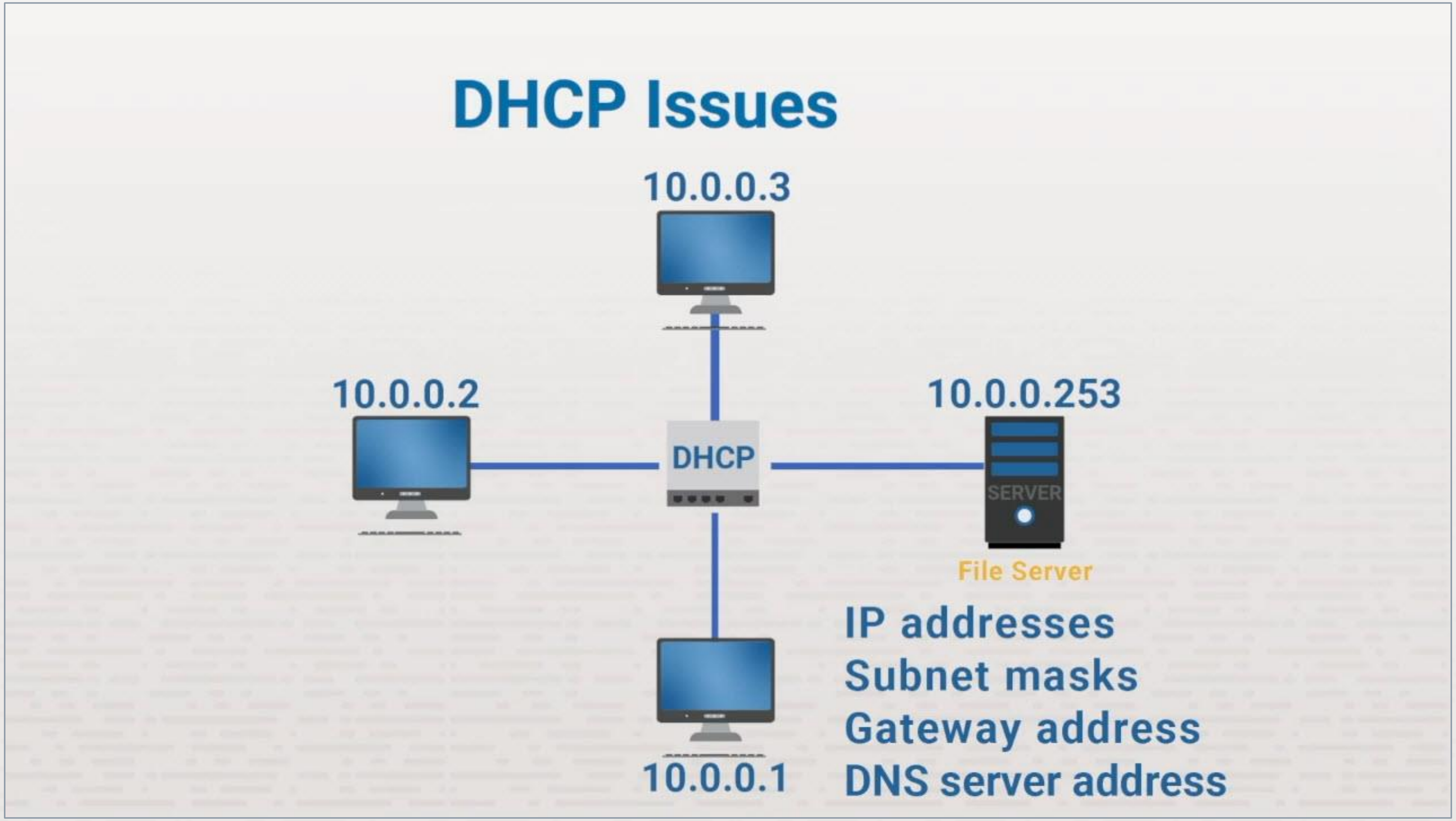


IP Configuration Troubleshooting

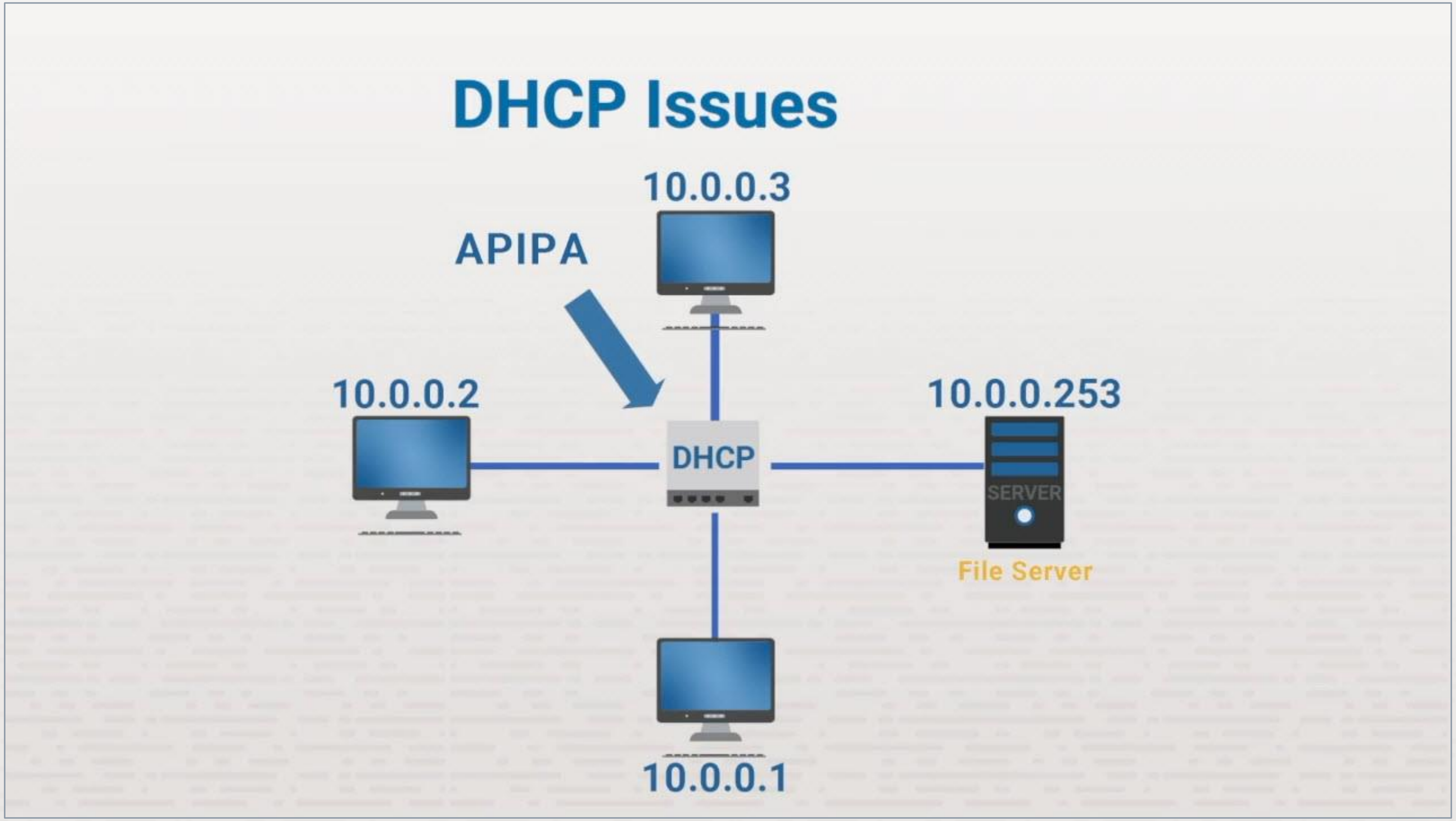
IP Tools

- ipconfig
- ipconfig /all
- ip
- ifconfig (Linux)

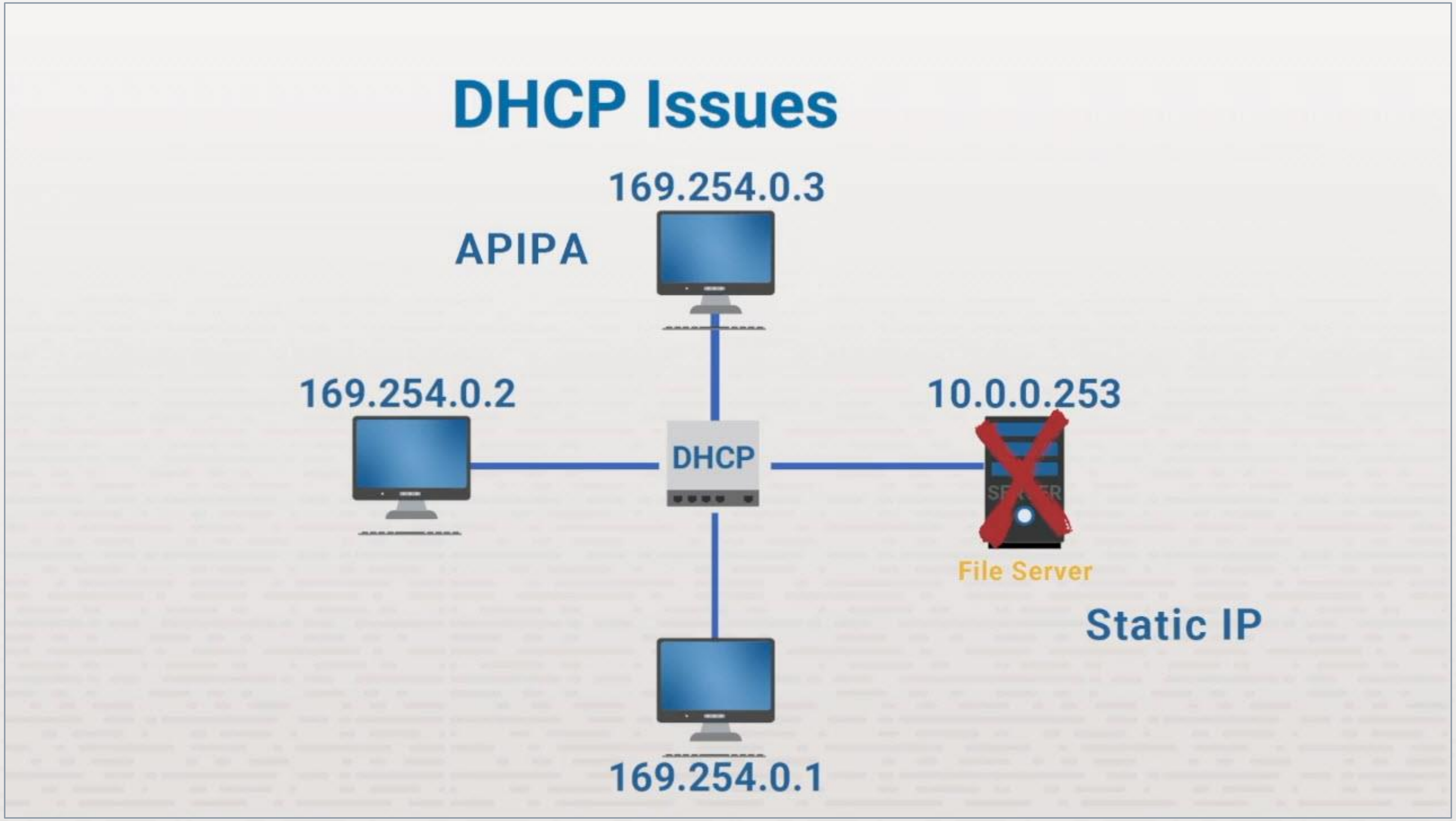
IP Configuration Troubleshooting



IP Configuration Troubleshooting



IP Configuration Troubleshooting



APIPA

- APIPA = DHCP issue
- Issue ipconfig /release
- Follow with ipconfig /renew
- Escalate issue if APIPA is reassigned
- Check DHCP scope

Summary

- Improper IP configuration
- DHCP issues

In-Class Practice

Do the following labs:

- 4.9.5 Explore IP Configuration
- 4.9.6 Troubleshoot IP Configuration 1
- 4.9.7 Troubleshoot IP Configuration 2
- 4.9.8 Troubleshoot IP Configuration 3

Class Discussion

- Which IP configuration issues should you be aware of?
- How can an incorrect subnet mask cause IP communication issues?
- Which issues may prevent a DHCP server from properly issuing an IP address to a host?
- What does the /release switch do when used with ipconfig?
- How can you tell if a rogue DHCP server is active on your network?
- How do you know if a host is using APIPA?

4.10 NETWORK ADDRESSING AND SERVICES

Troubleshoot IP Communications

Section Skill Overview

- Use ping and tracert
- Use arp and netstat
- Use tcpdump
- Explore network communications

Key Terms

- ping
- Address Resolution Protocol (ARP)
- tcpdump

Key Definitions

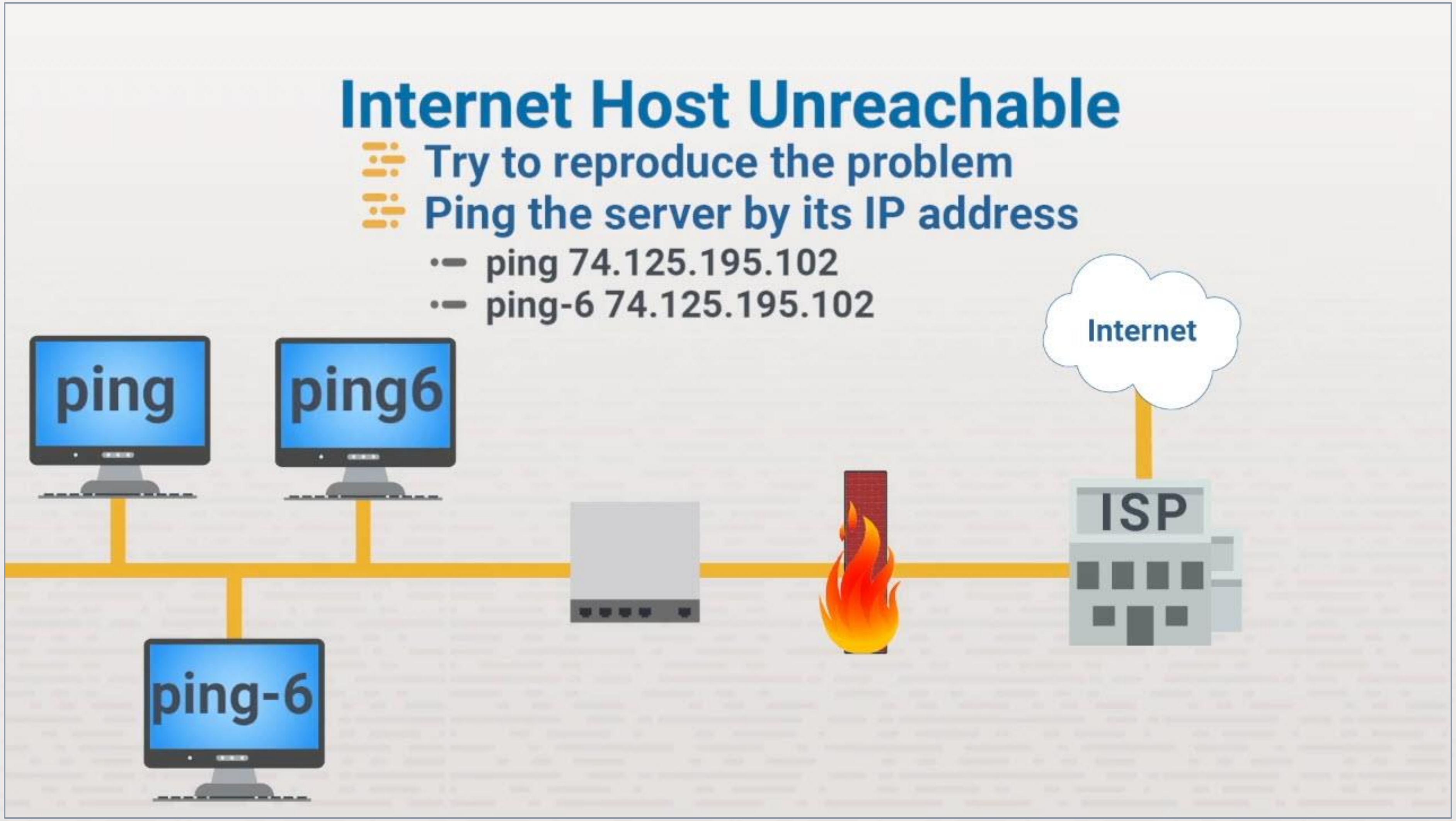
- **ping:** ping sends an ICMP echo request/reply packet to a remote host. A response from the remote host indicates that both hosts are correctly configured and a connection exists between them.
- **Address Resolution Protocol (ARP):** Hosts use ARP to discover the MAC address of a device from its IP address.
- **tcpdump:** tcpdump is a packet analyzer that runs in a command line utility. It allows the user to view TCP/IP and other packets as they are transmitted and received over a computer network.

Network Communication Troubleshooting

Identify the Scope

- Is it happening to many systems?
- Is it isolated to one system?

Network Communication Troubleshooting



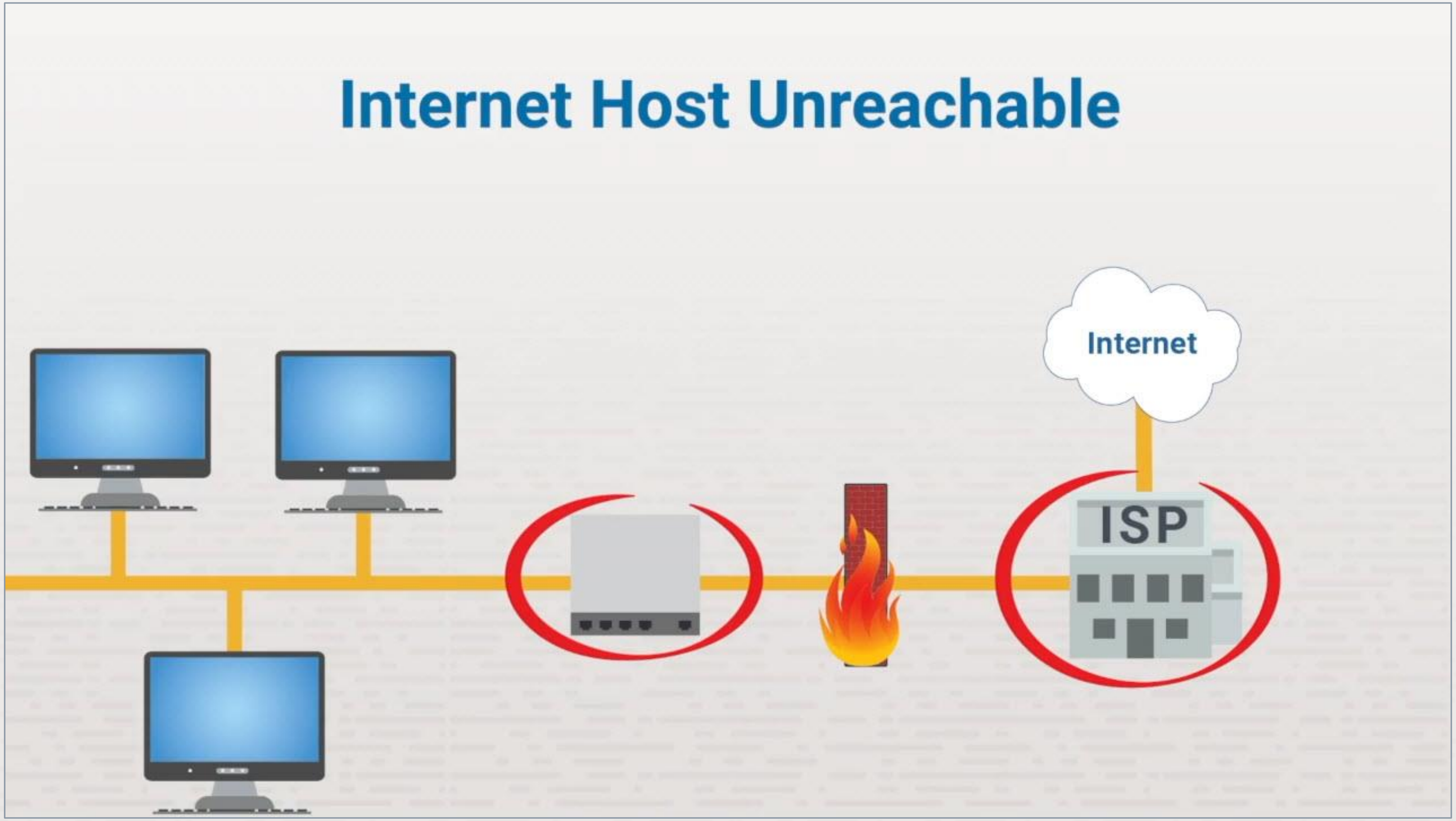
Ping Results

- If ping to IP address works
  - All hardware is functioning
- If ping to DNS fails
  - A name resolution problem exists
- If ping to IP address fails
  - Server may be down
  - Routers malfunctioning
  - Other issues

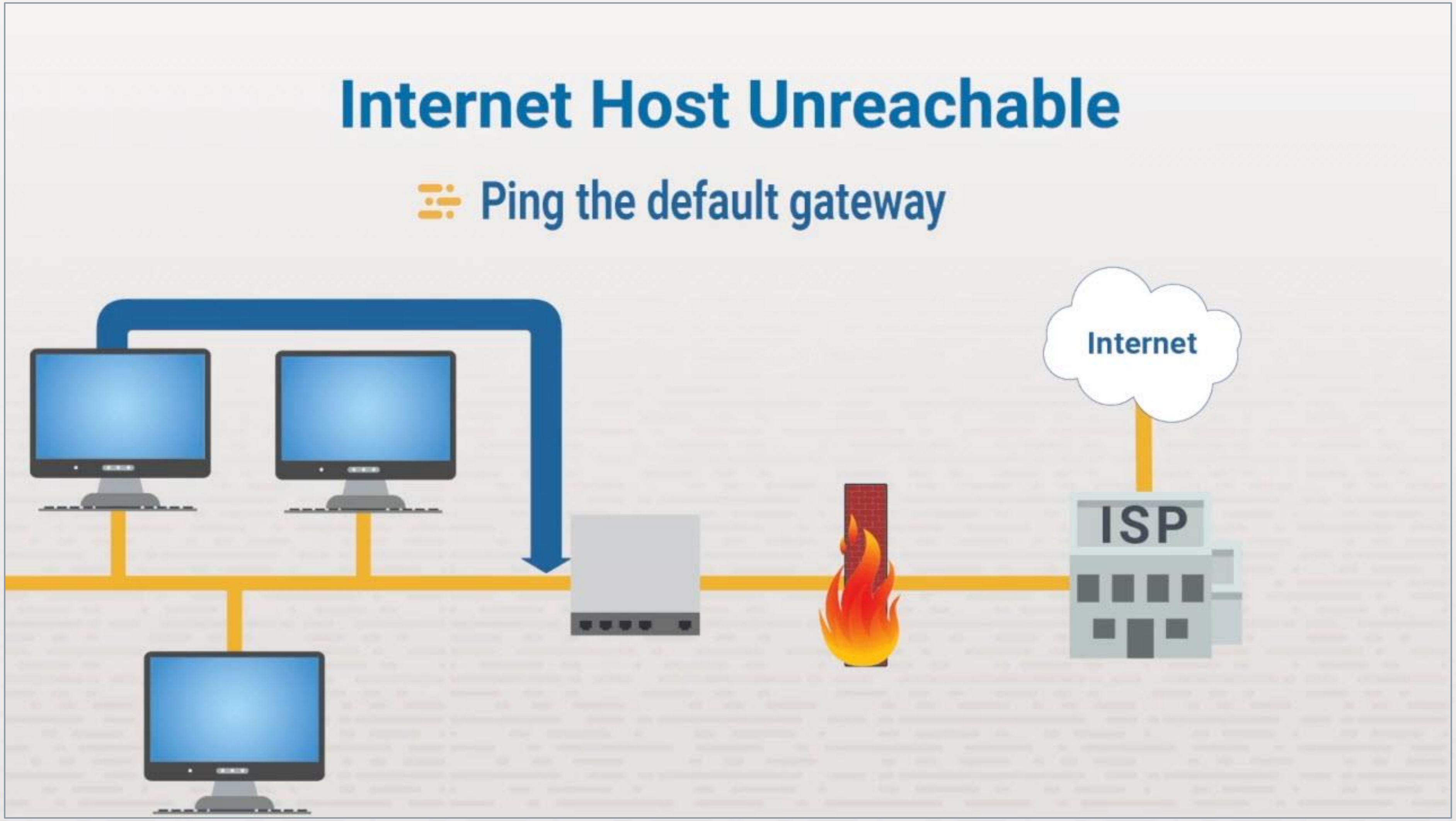
Failed Ping to IP Address

- Firewall blocking ping
- Misconfigured IP information
- Access a different website
- Ping other hosts on the internet

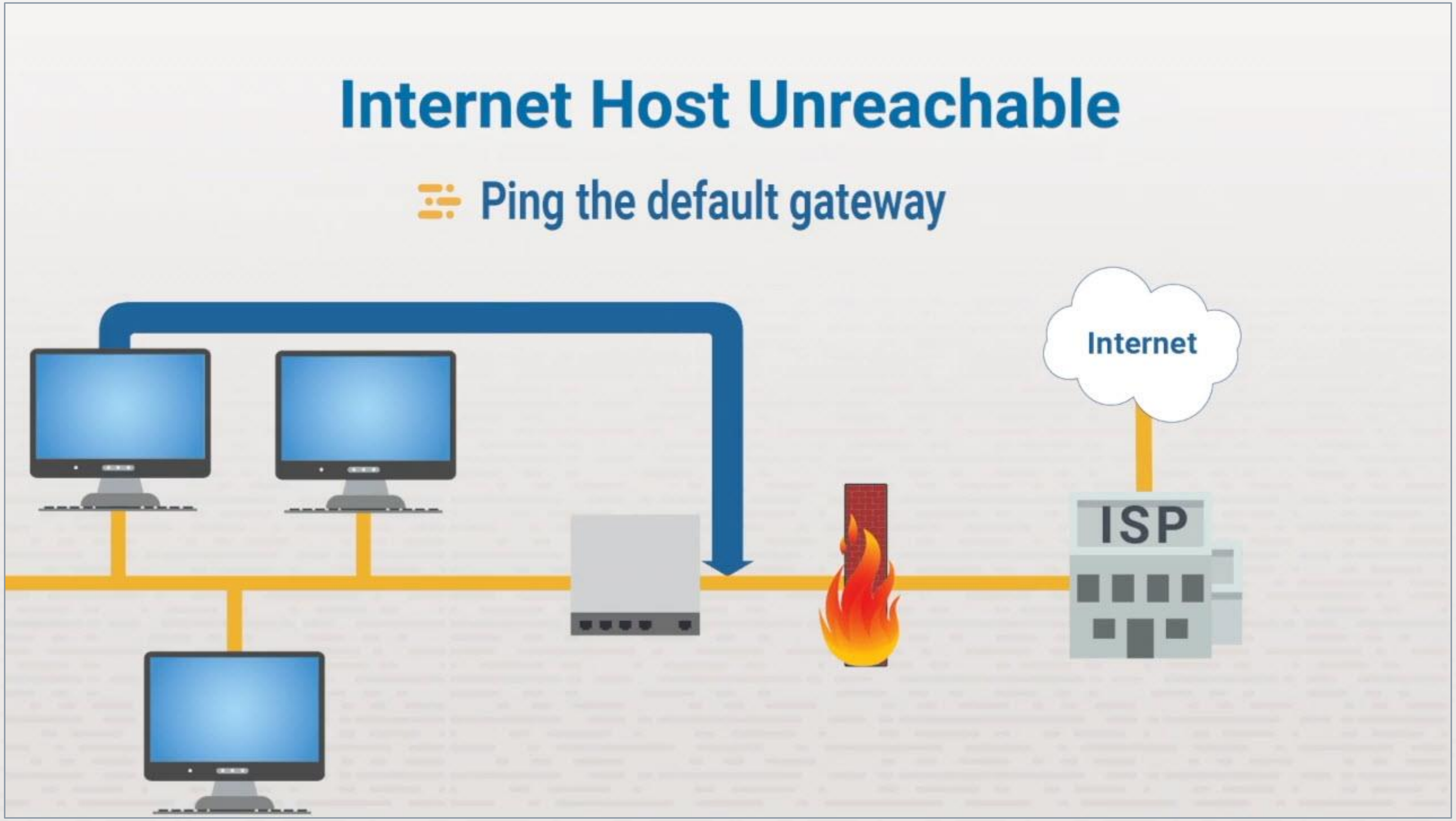
Network Communication Troubleshooting



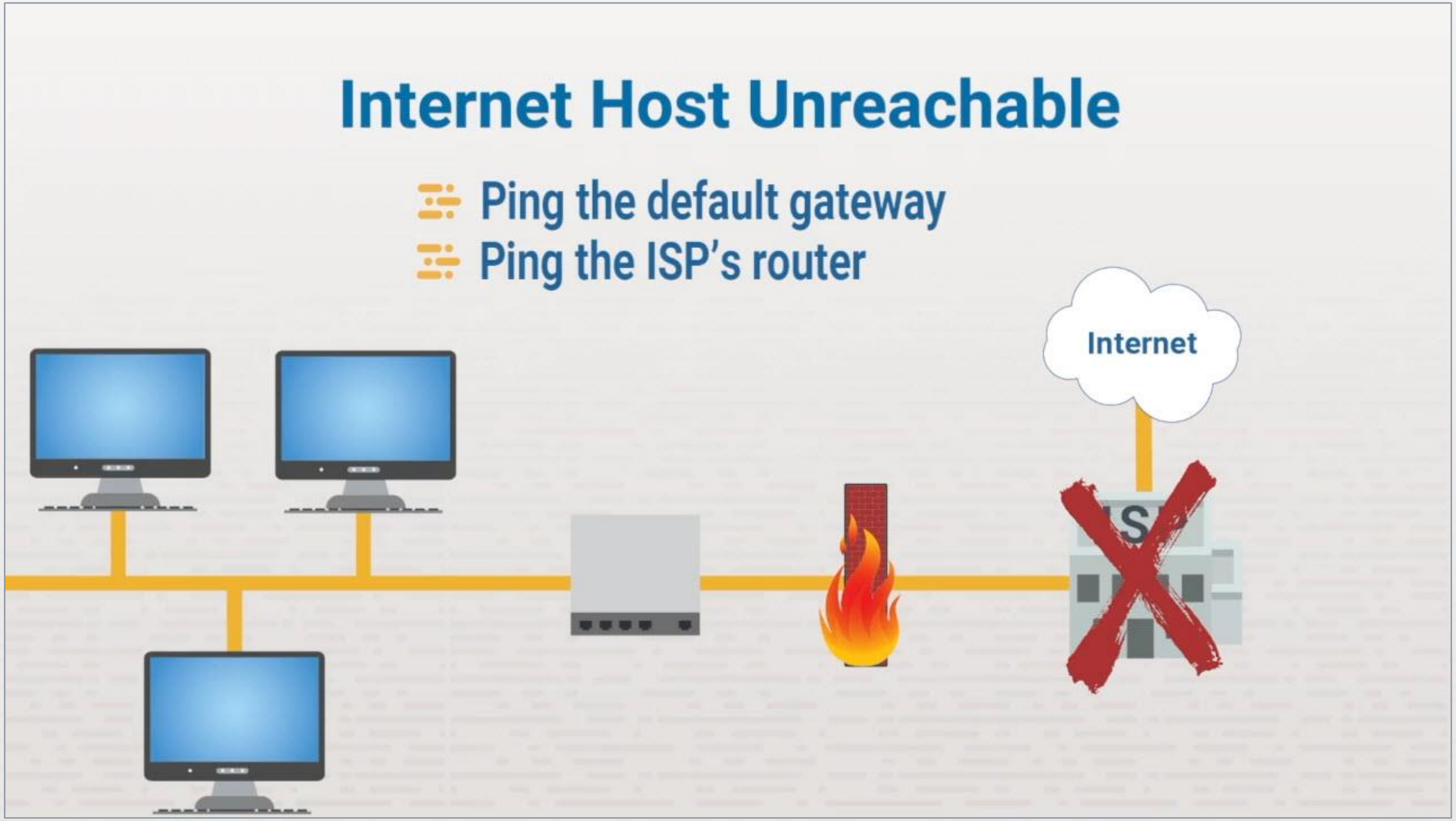
Network Communication Troubleshooting



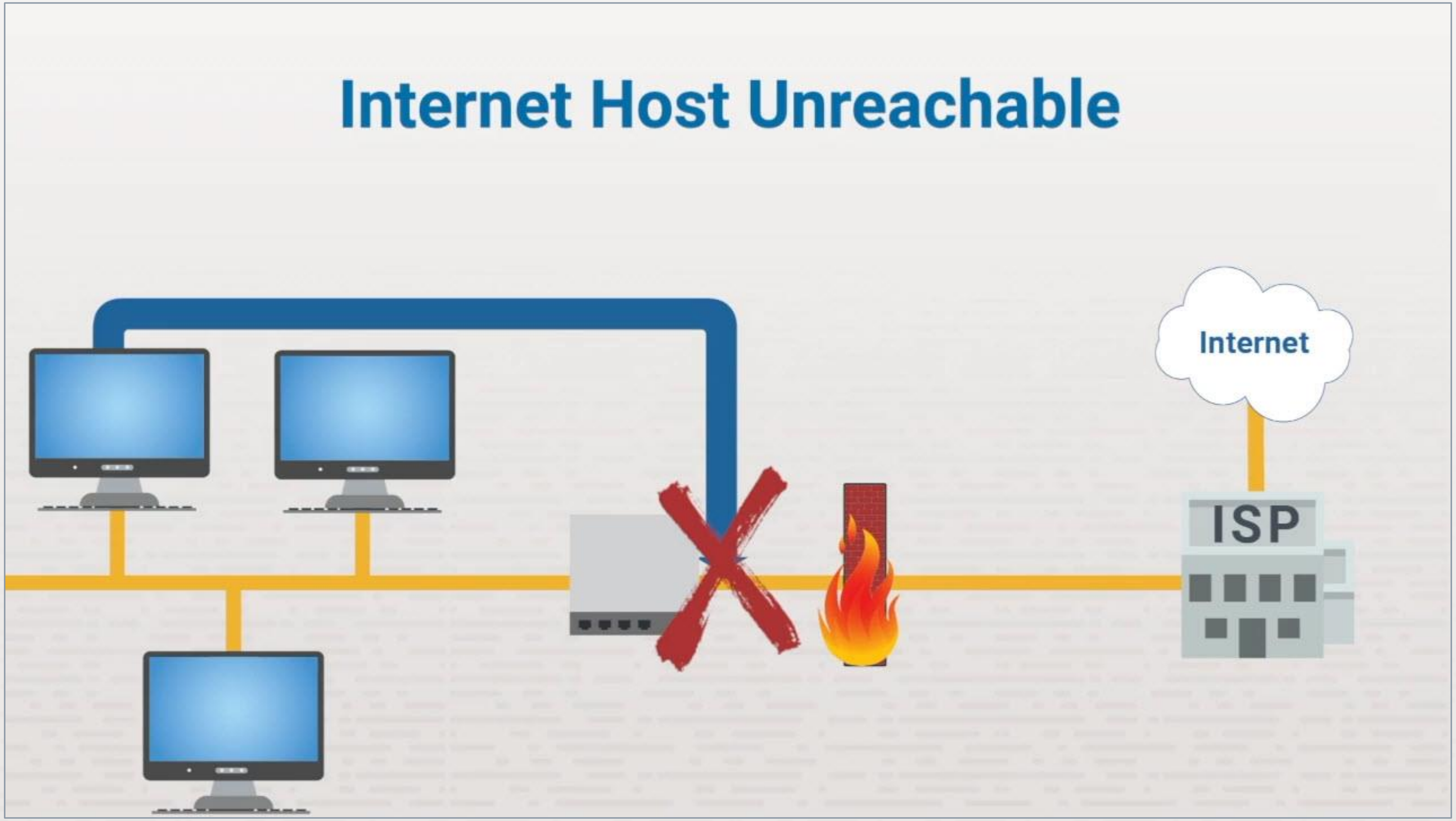
Network Communication Troubleshooting



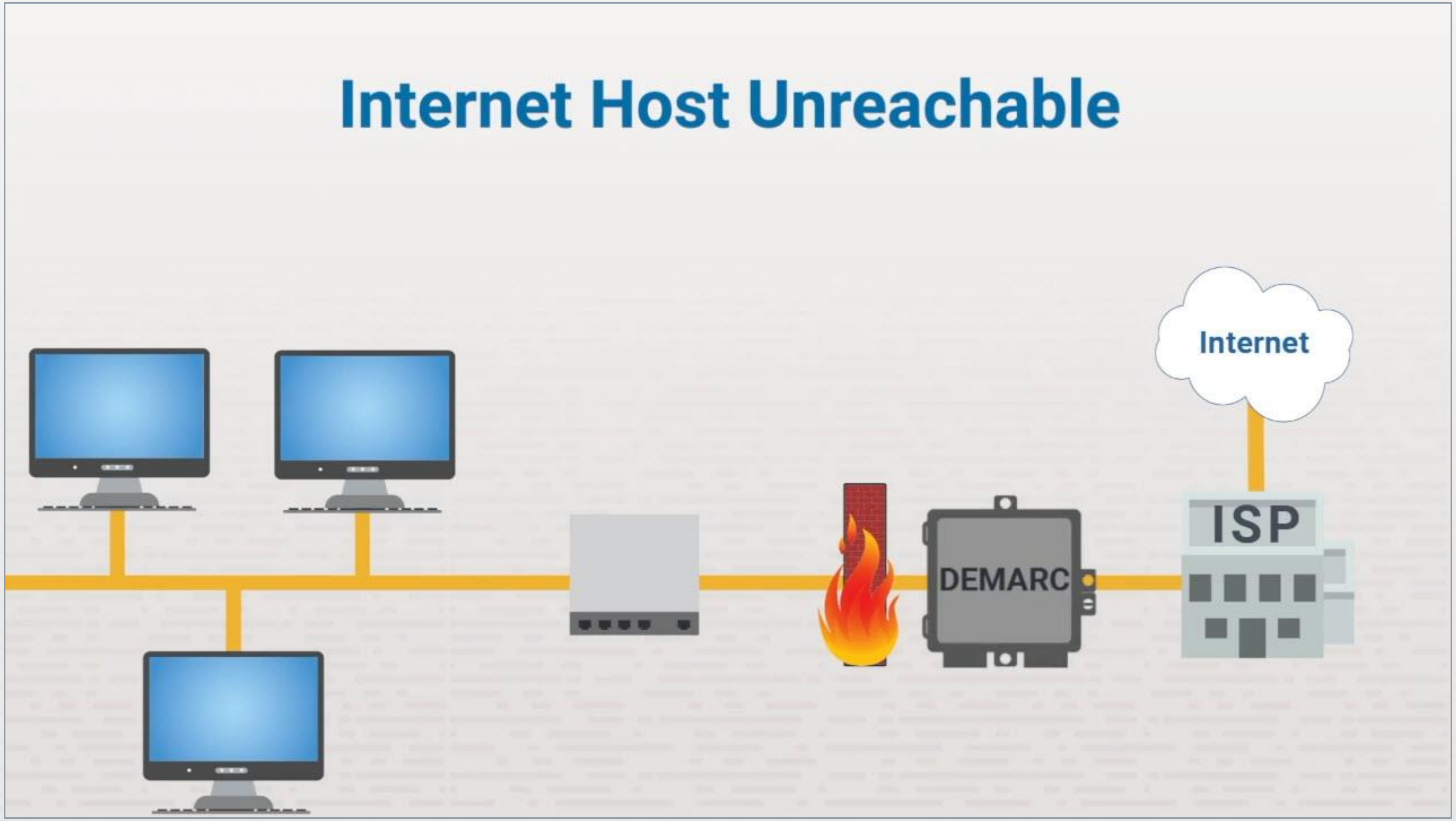
Network Communication Troubleshooting



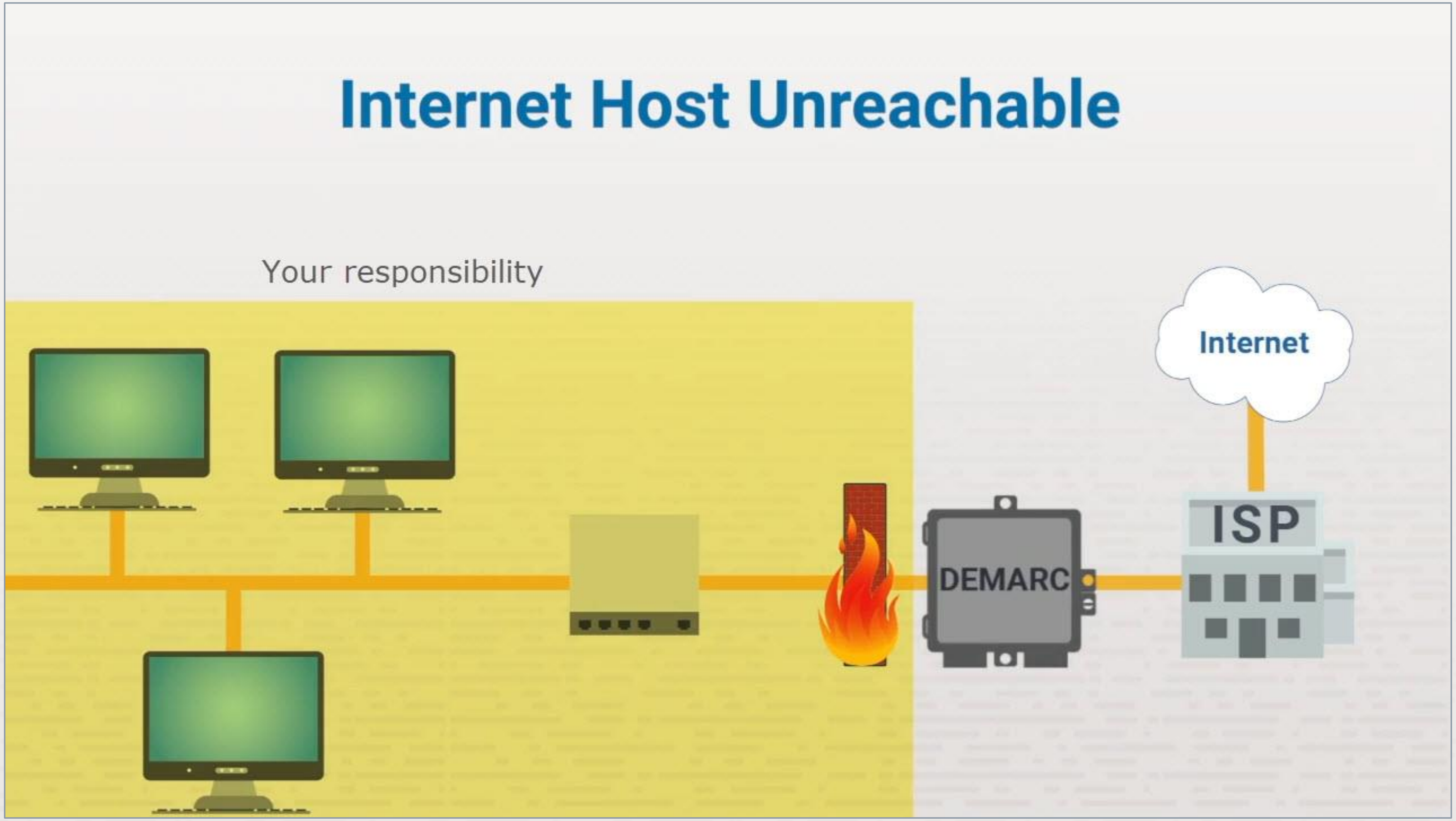
Network Communication Troubleshooting



Network Communication Troubleshooting

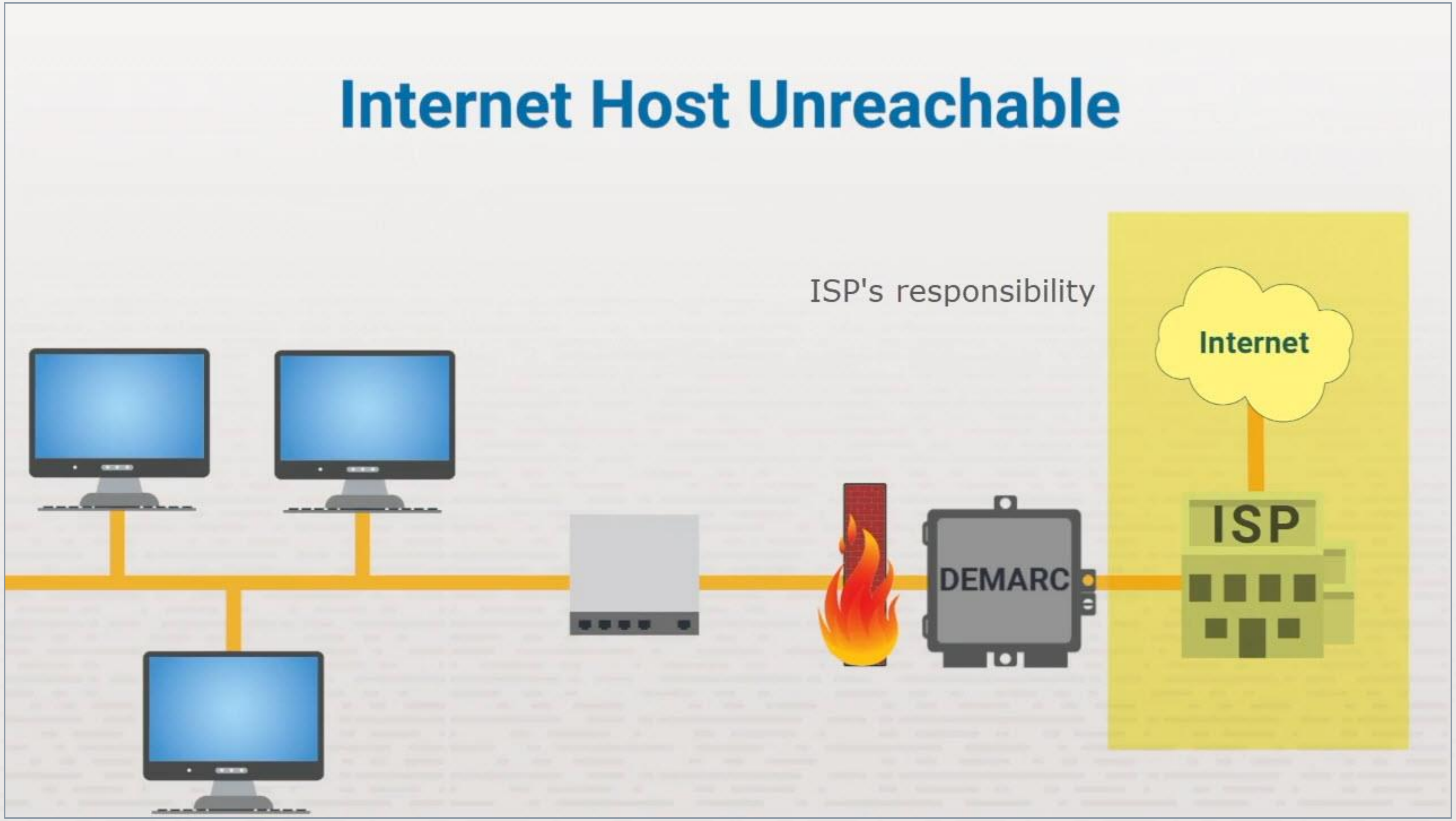


Network Communication Troubleshooting

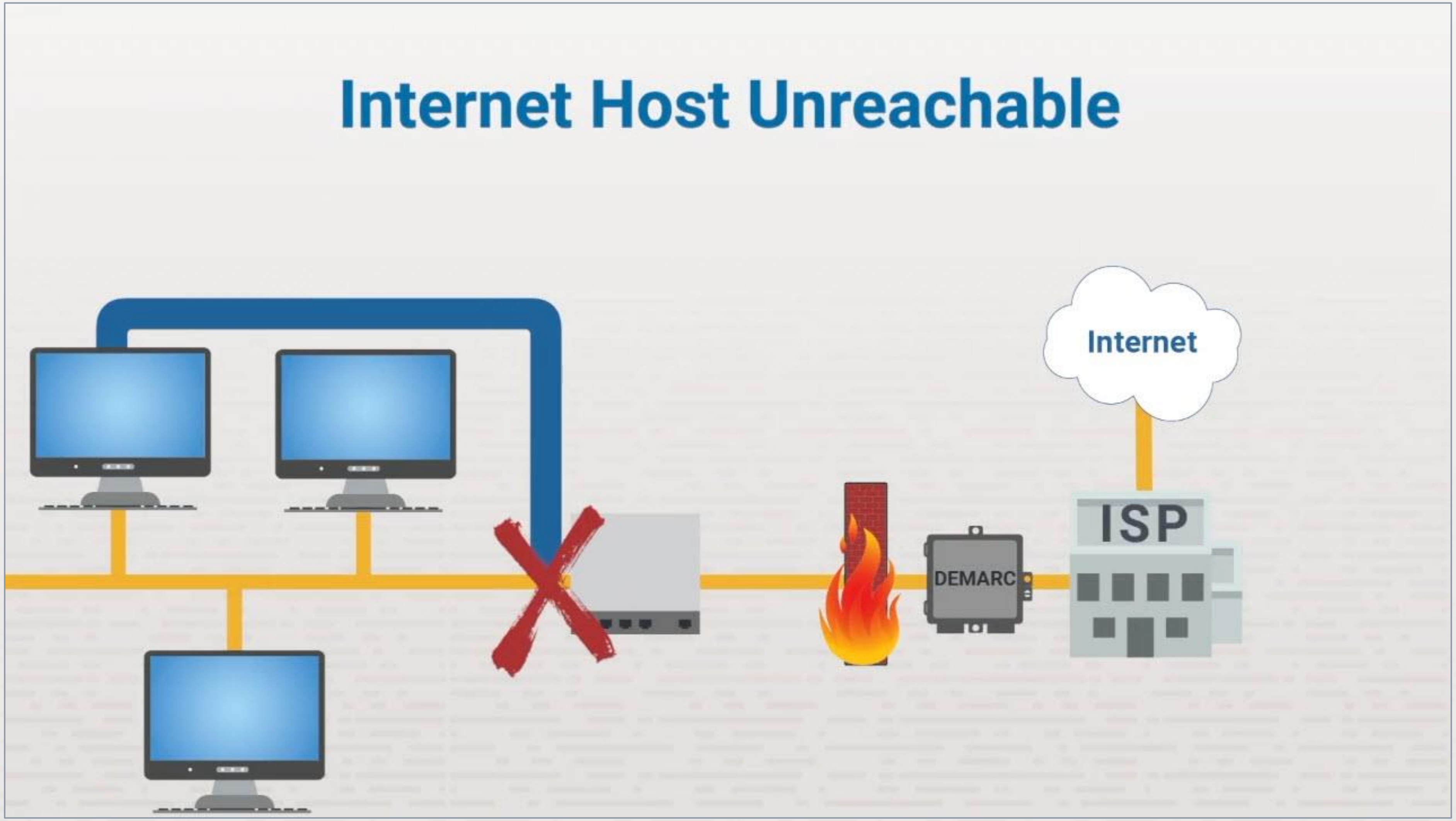


TestOut

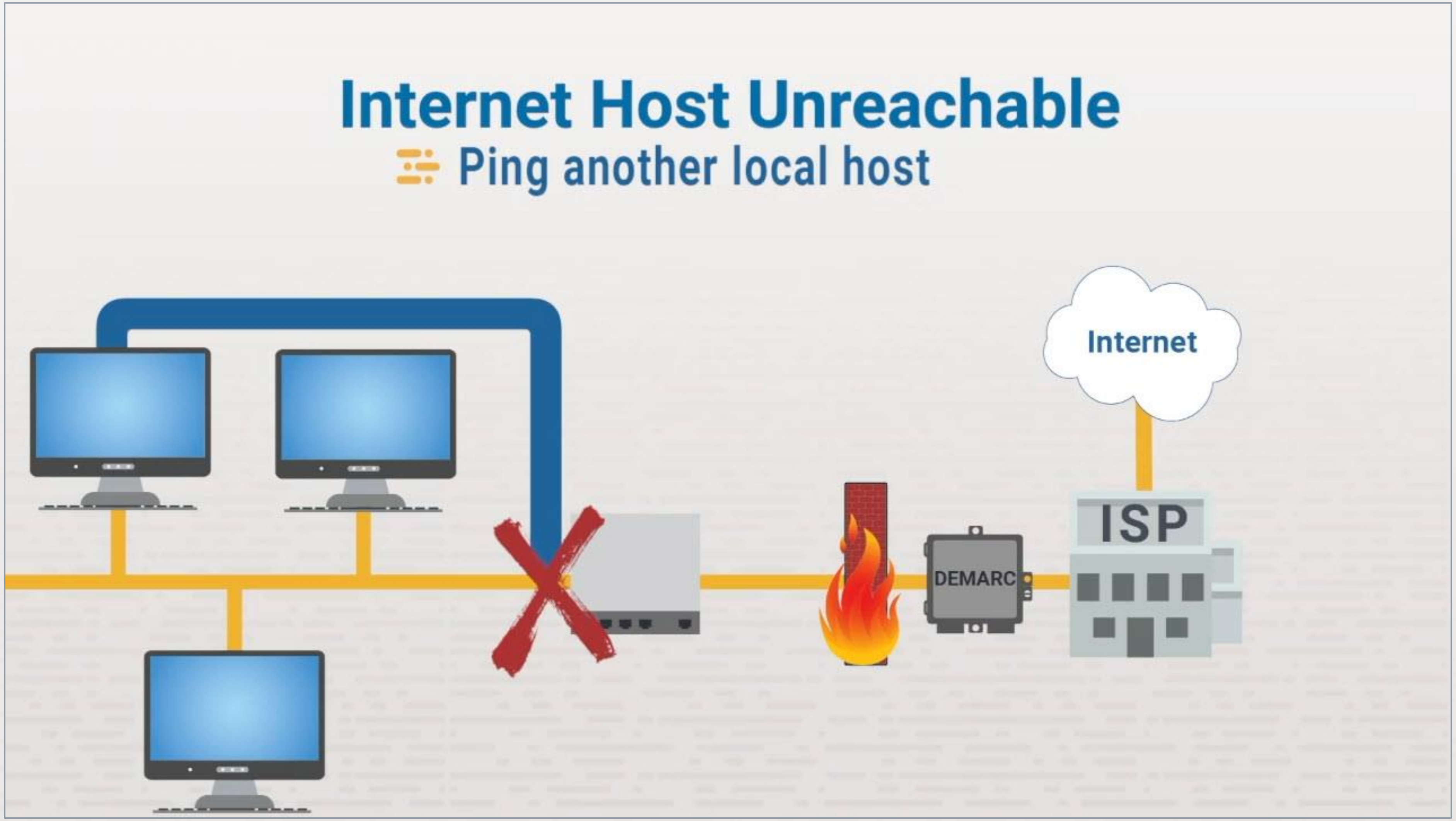
Network Communication Troubleshooting



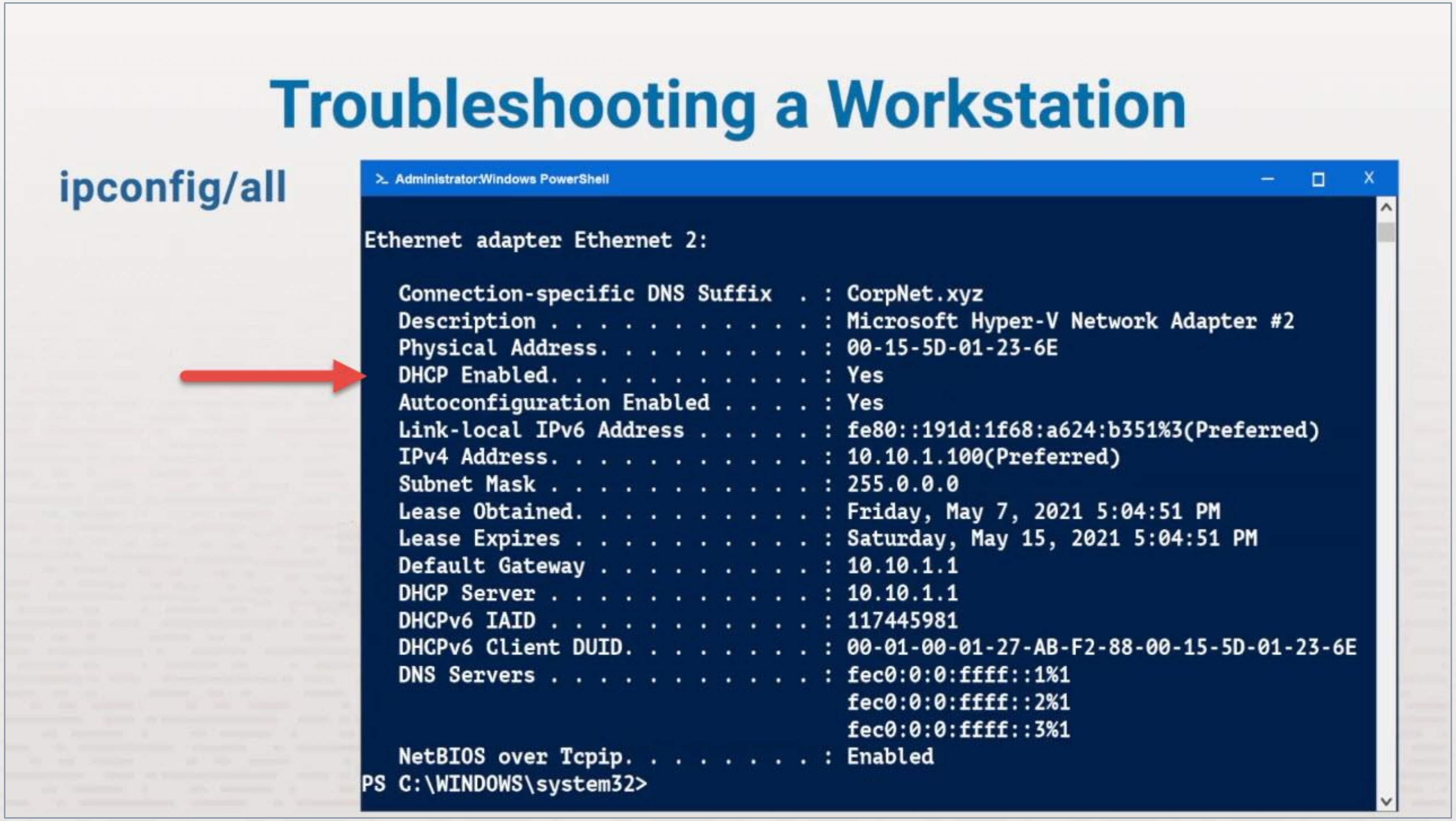
Network Communication Troubleshooting



Network Communication Troubleshooting



Network Communication Troubleshooting



Troubleshooting a Workstation

ipconfig/all

Administrator:Windows PowerShell

```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : CorpNet.xyz
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter #2
   Physical Address. . . . . . . . . : 00-15-5D-01-23-6E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::191d:1f68:a624:b351%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.1.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Lease Obtained. . . . . . . . . . : Friday, May 7, 2021 5:04:51 PM
   Lease Expires . . . . . . . . . . : Saturday, May 15, 2021 5:04:51 PM
   Default Gateway . . . . . . . . . : 10.10.1.1
   DHCP Server . . . . . . . . . . . : 10.10.1.1
   DHCPv6 IAID . . . . . . . . . . . : 117445981
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-AB-F2-88-00-15-5D-01-23-6E
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\WINDOWS\system32>
```

Network Communication Troubleshooting

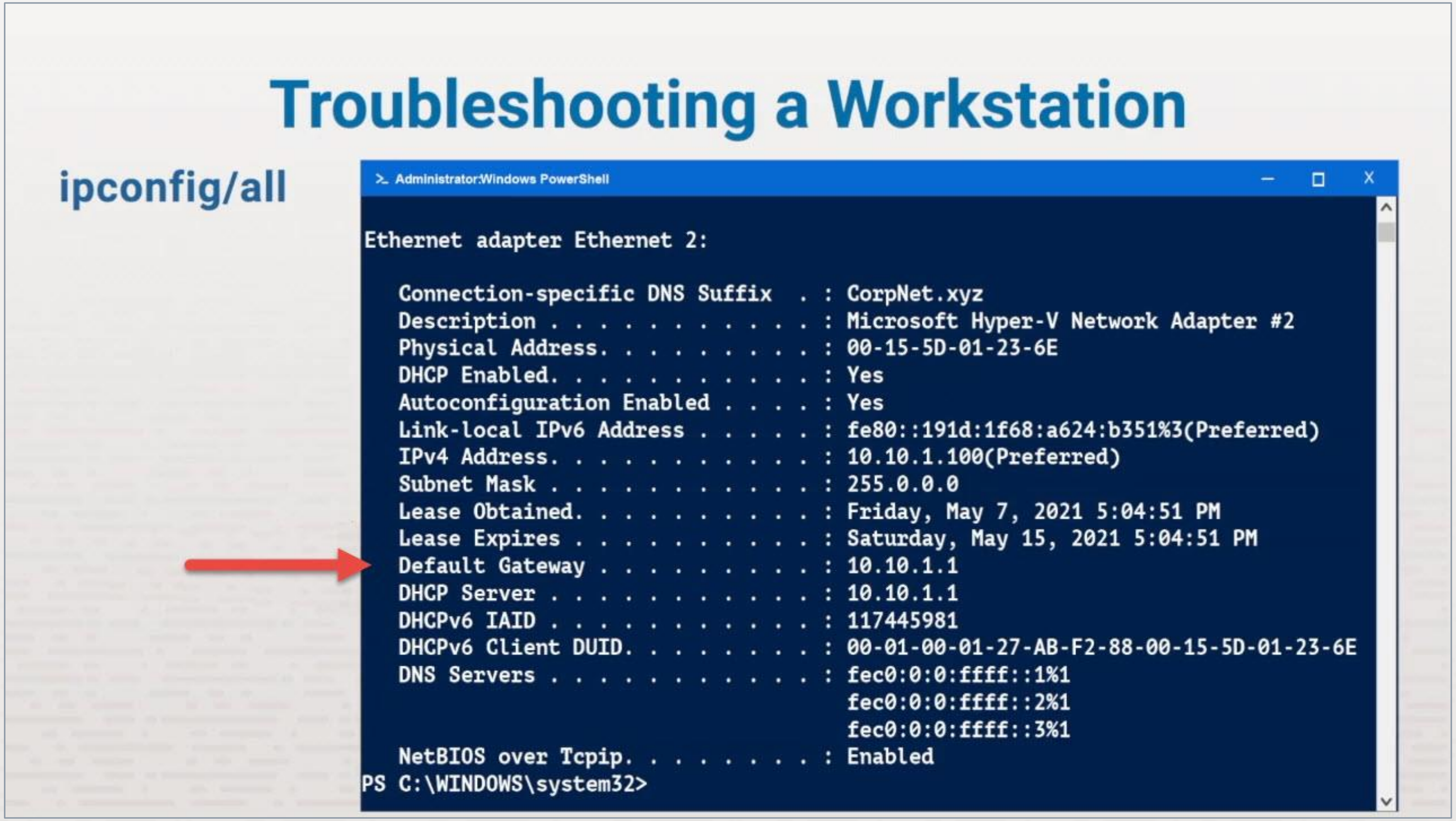
Troubleshooting a Workstation

ipconfig/all

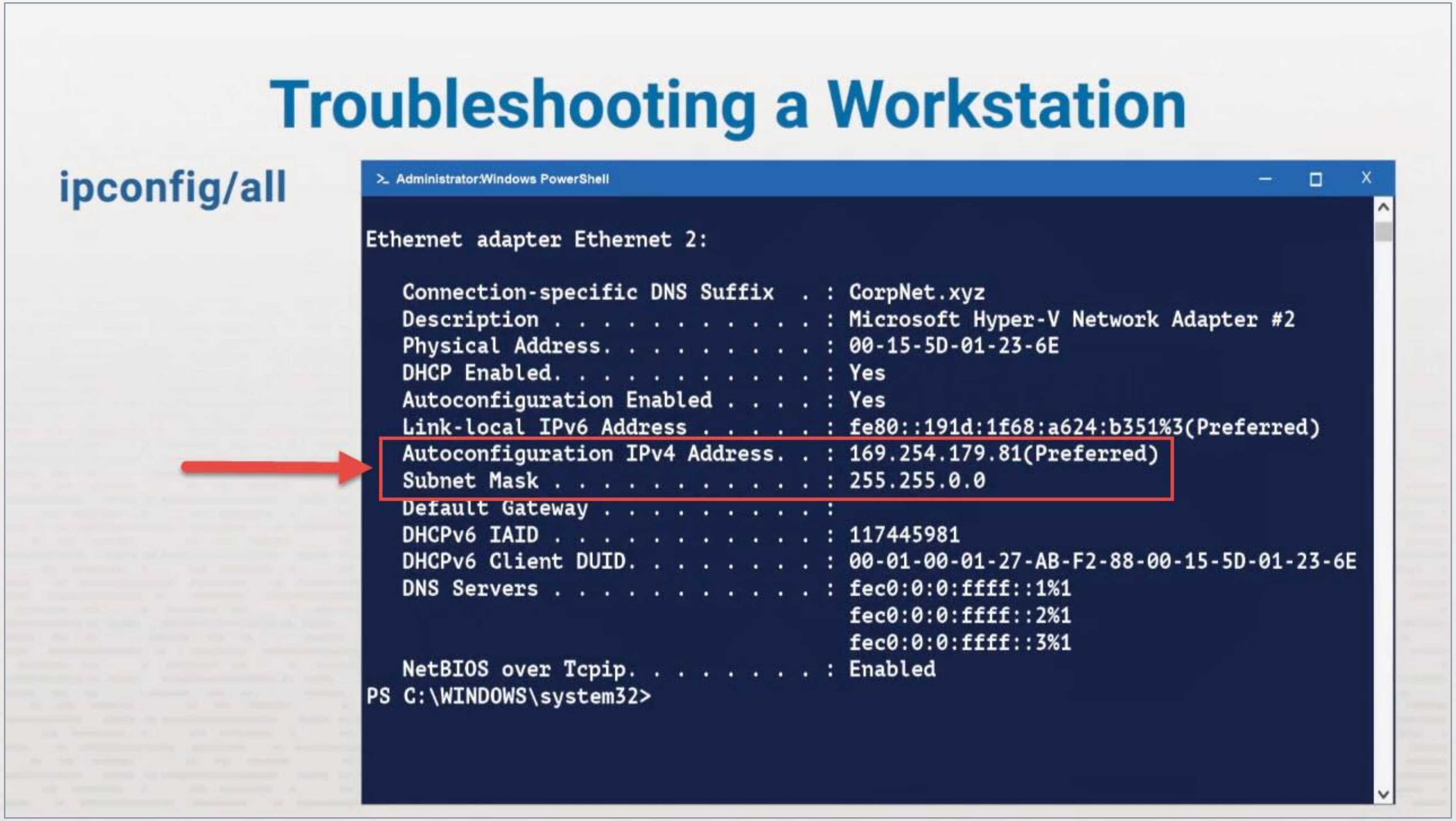
Administrator:Windows PowerShell

```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : CorpNet.xyz
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter #2
   Physical Address. . . . . . . . . : 00-15-5D-01-23-6E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::191d:1f68:a624:b351%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.1.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Lease Obtained. . . . . . . . . . : Friday, May 7, 2021 5:04:51 PM
   Lease Expires . . . . . . . . . . : Saturday, May 15, 2021 5:04:51 PM
   Default Gateway . . . . . . . . . : 10.10.1.1
   DHCP Server . . . . . . . . . . . : 10.10.1.1
   DHCPv6 IAID . . . . . . . . . . . : 117445981
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-AB-F2-88-00-15-5D-01-23-6E
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\WINDOWS\system32>
```

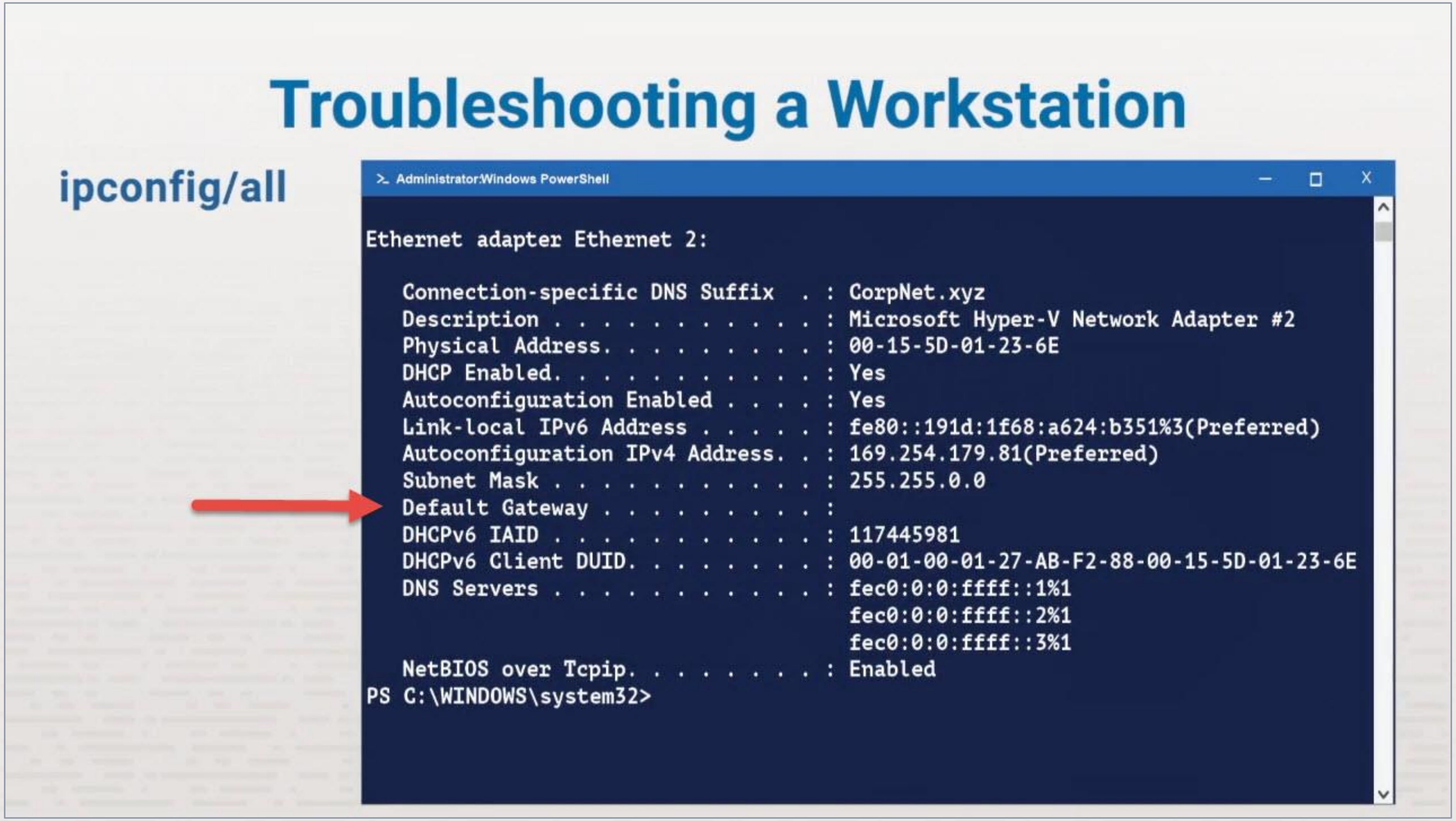
Network Communication Troubleshooting



Network Communication Troubleshooting



Network Communication Troubleshooting



In-Class Practice

Do the following labs:

- 4.10.6 Explore Network Communications

Class Discussion

- What is the difference between netstat and arp?
- If a ping test fails, what should you do?
- What information does tracert provide?
- What does TCPdump do?

Troubleshoot DNS

Section Skill Overview

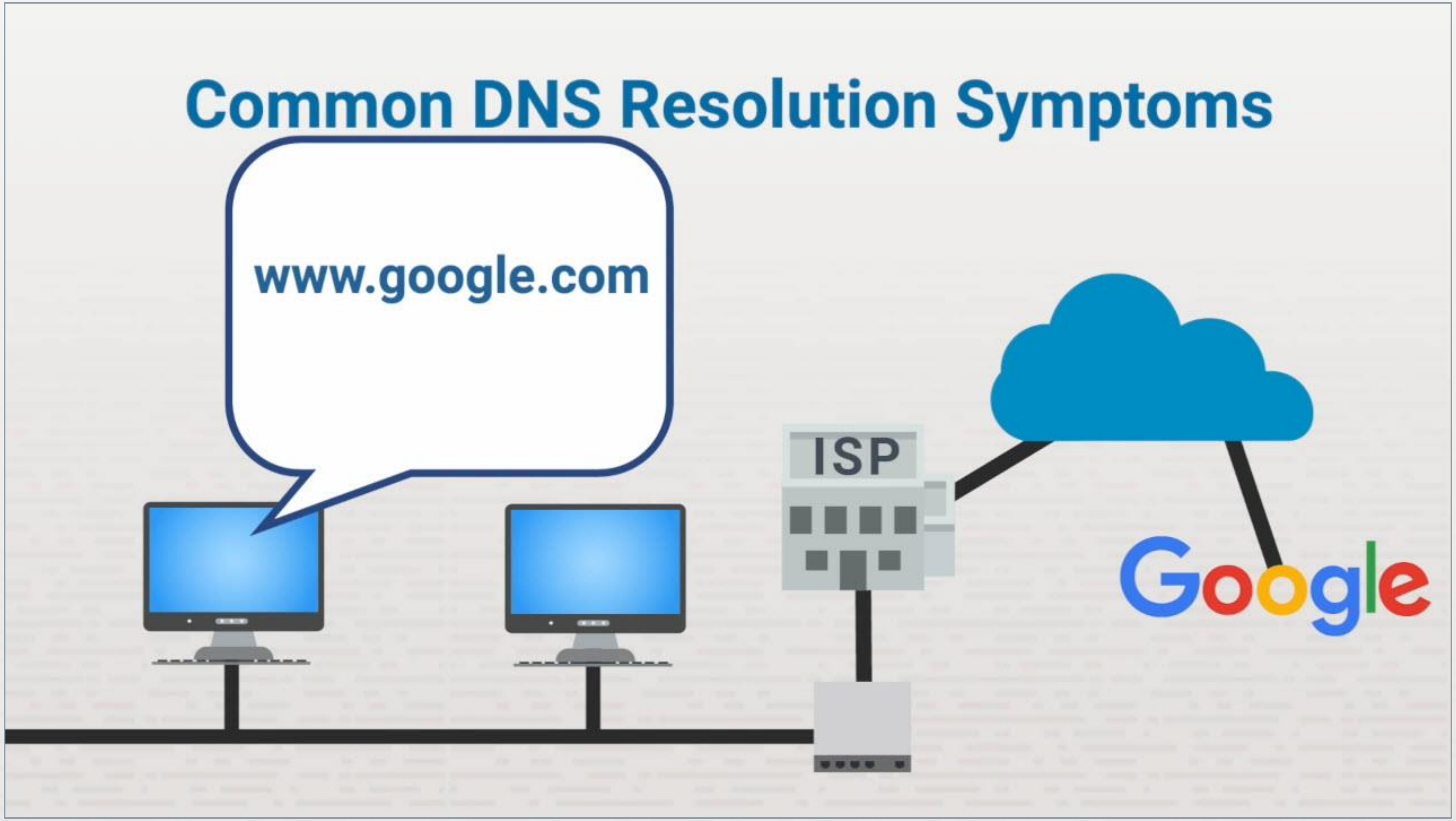
- Examine DNS attacks
- Use nslookup
- Use dig

DNS Troubleshooting

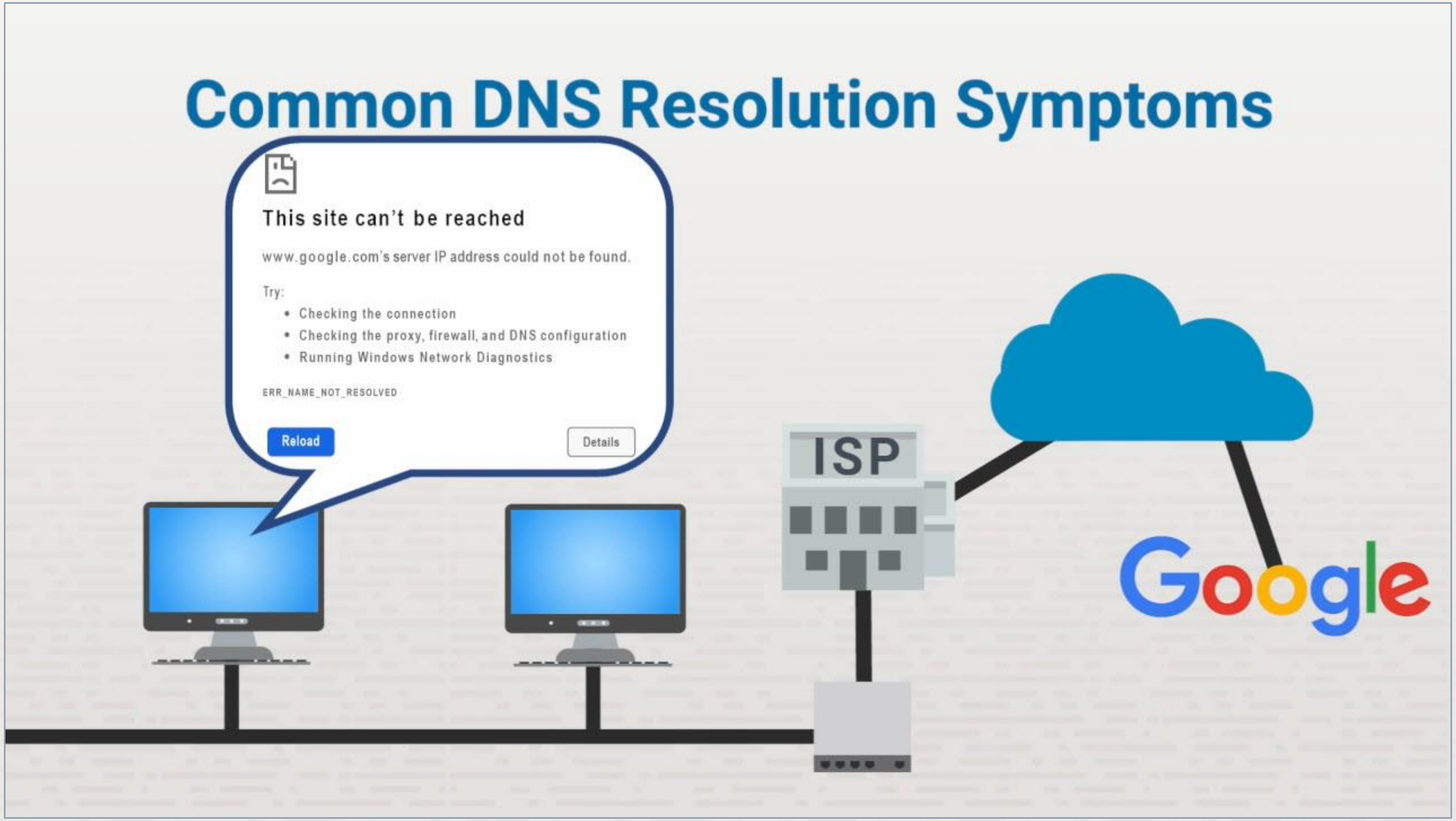
Domain Name System

- Resolves hostname to IP address
- Resolves IP address to hostname

DNS Troubleshooting



DNS Troubleshooting



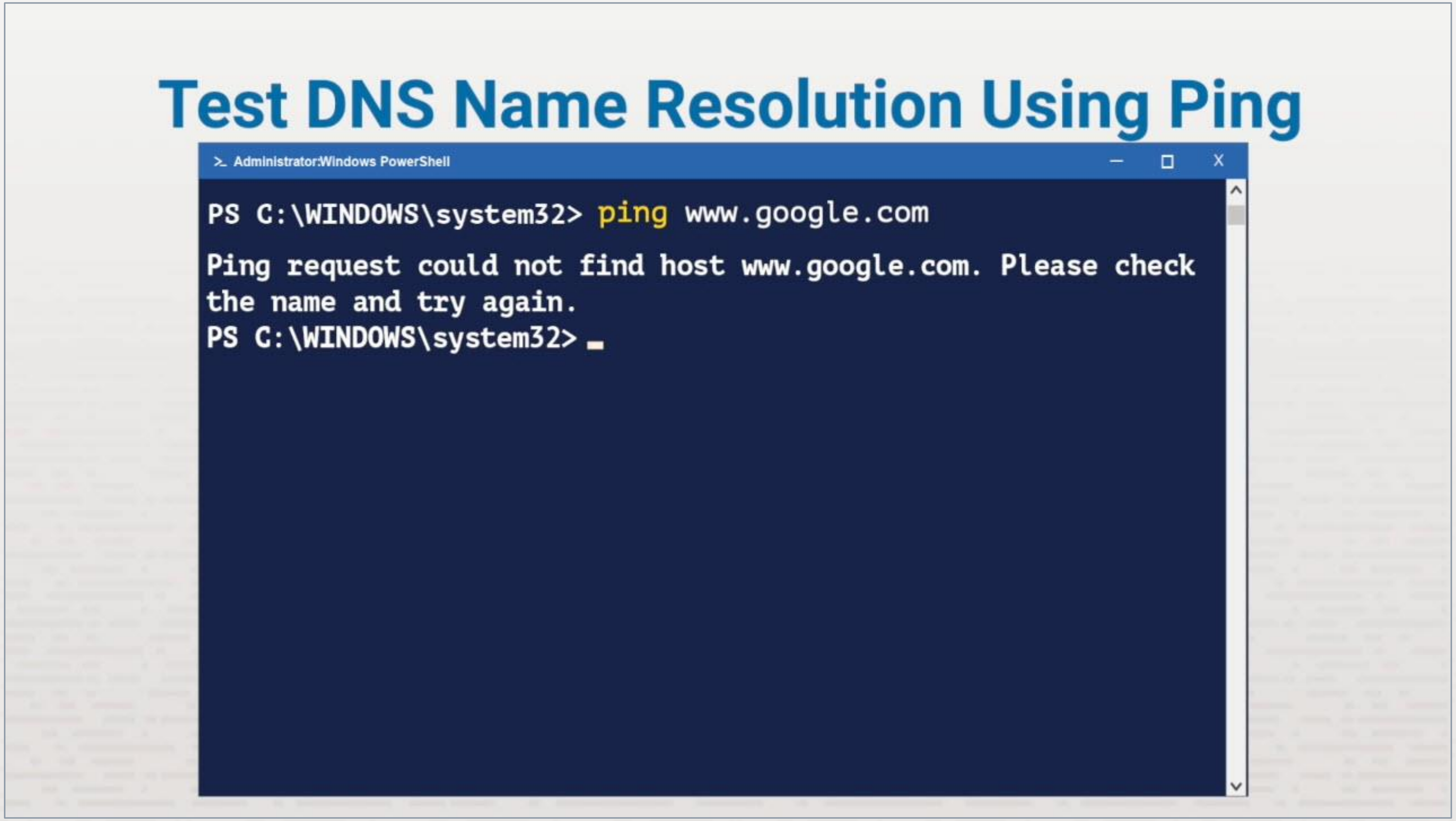
DNS Troubleshooting

Test DNS Name Resolution Using Ping

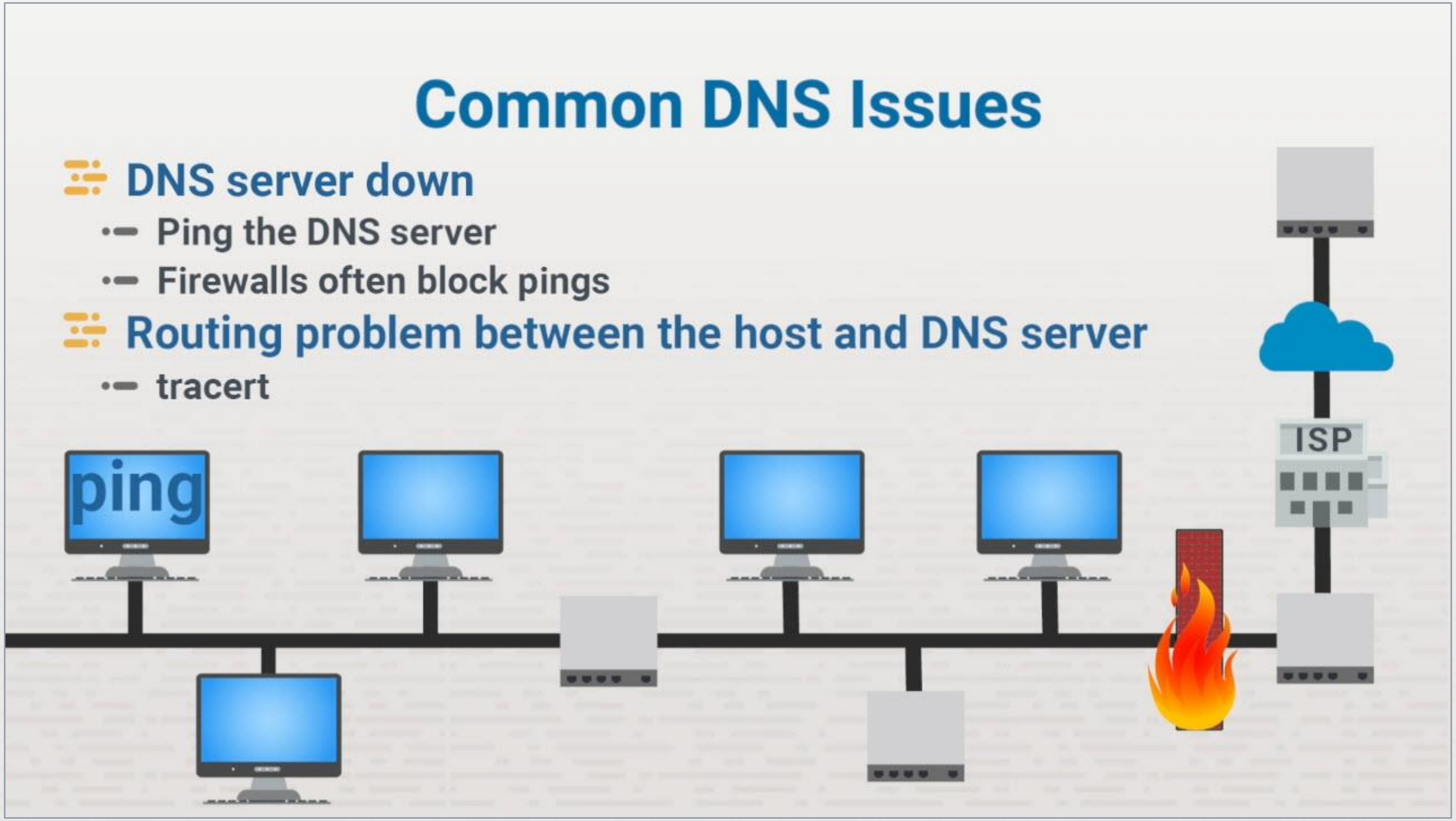
Administrator:Windows PowerShell

```
PS C:\WINDOWS\system32> ping 74.125.195.139

Pinging 74.125.195.139 with 32 bytes of data:
Reply from 74.125.195.139: bytes=32 time=72ms TTL=103
Reply from 74.125.195.139: bytes=32 time=72ms TTL=103
Reply from 74.125.195.139: bytes=32 time=72ms TTL=103
Reply from 74.125.195.139: bytes=32 time=72ms TTL=103

Ping statistics for 74.125.195.139:
    Packets: Sent = 4, Received = 4, :ost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 52ms, maximum = 96ms, Average = 68ms
PS C:\WINDOWS\system32> _
```

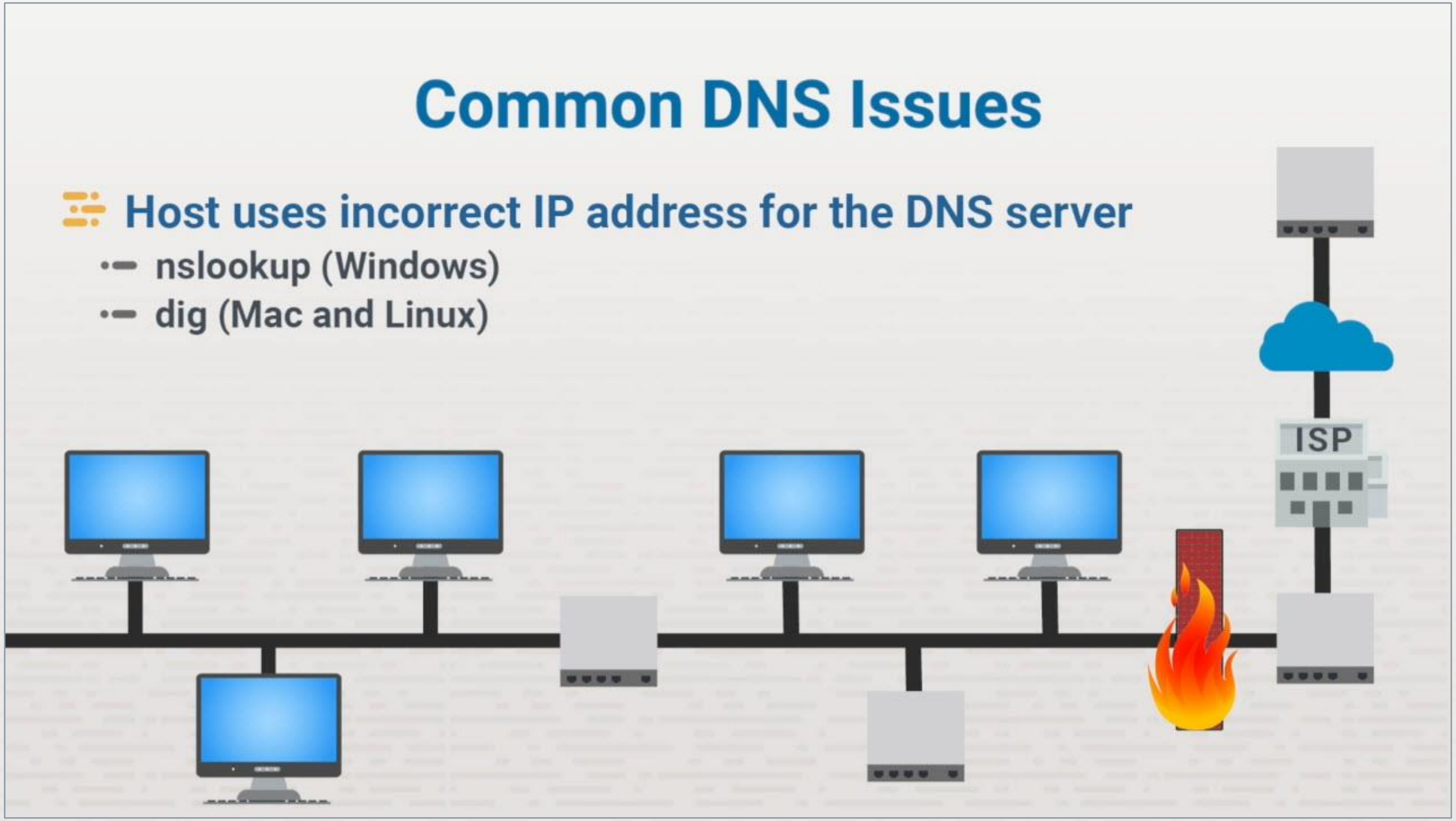
DNS Troubleshooting



DNS Troubleshooting



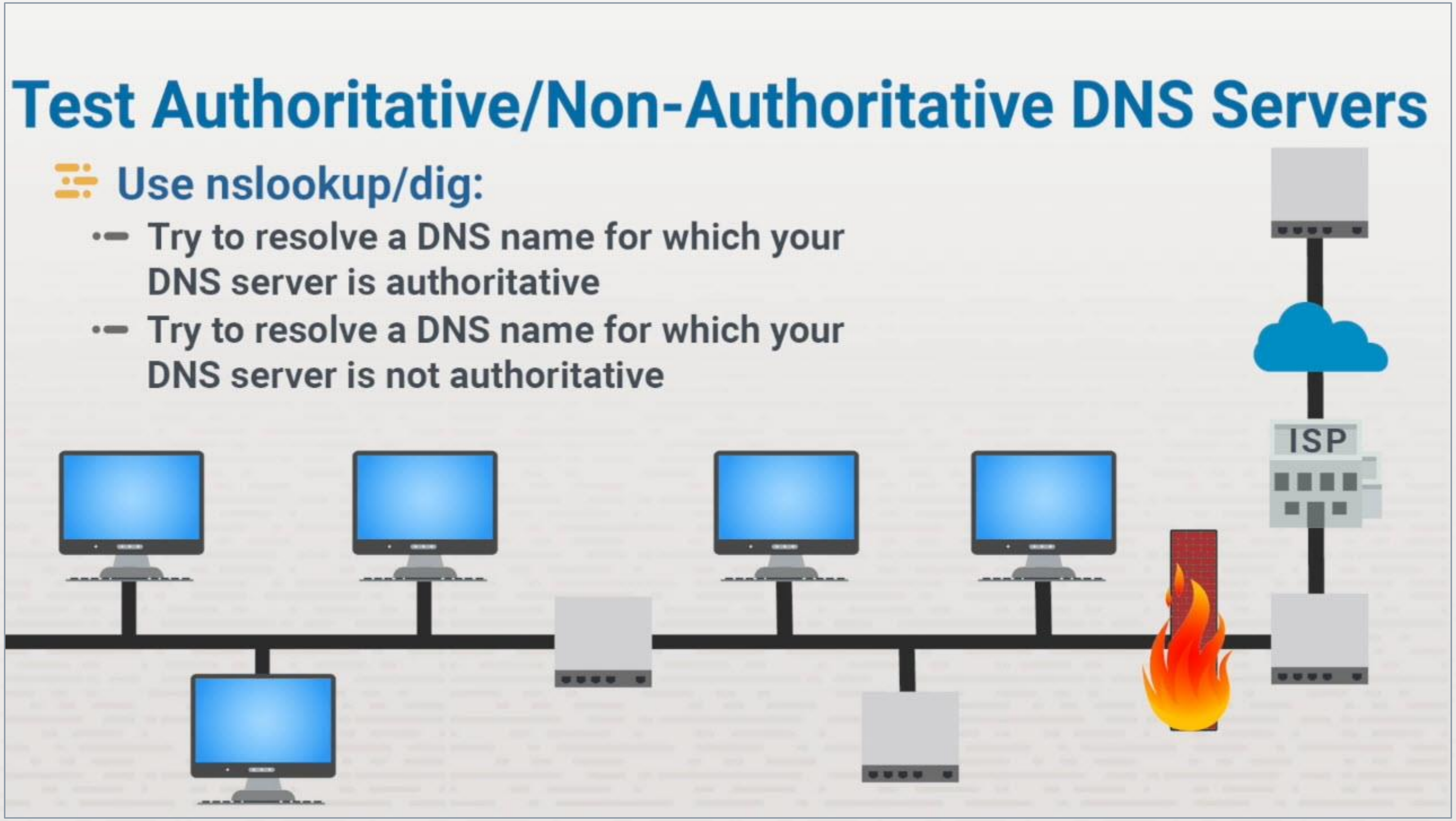
DNS Troubleshooting



Other Possible DNS Issues

- Unable to contact root-level DNS
  - Routing issues
  - Connectivity issues
  - WAN link issues

DNS Troubleshooting



Summary

- Troubleshooting DNS
- Commons DNS issues
  - Unreachable name servers
  - Routing problems
  - Misconfigured host DNS IP addressing
- Root-level DNS communications

In-Class Practice

Do the following labs:

- 4.11.6 Explore nslookup

Class Discussion

- What are the symptoms of name resolution problems?
- What is the difference between nslookup and dig?