

CCNA Foundations – Day 3

with

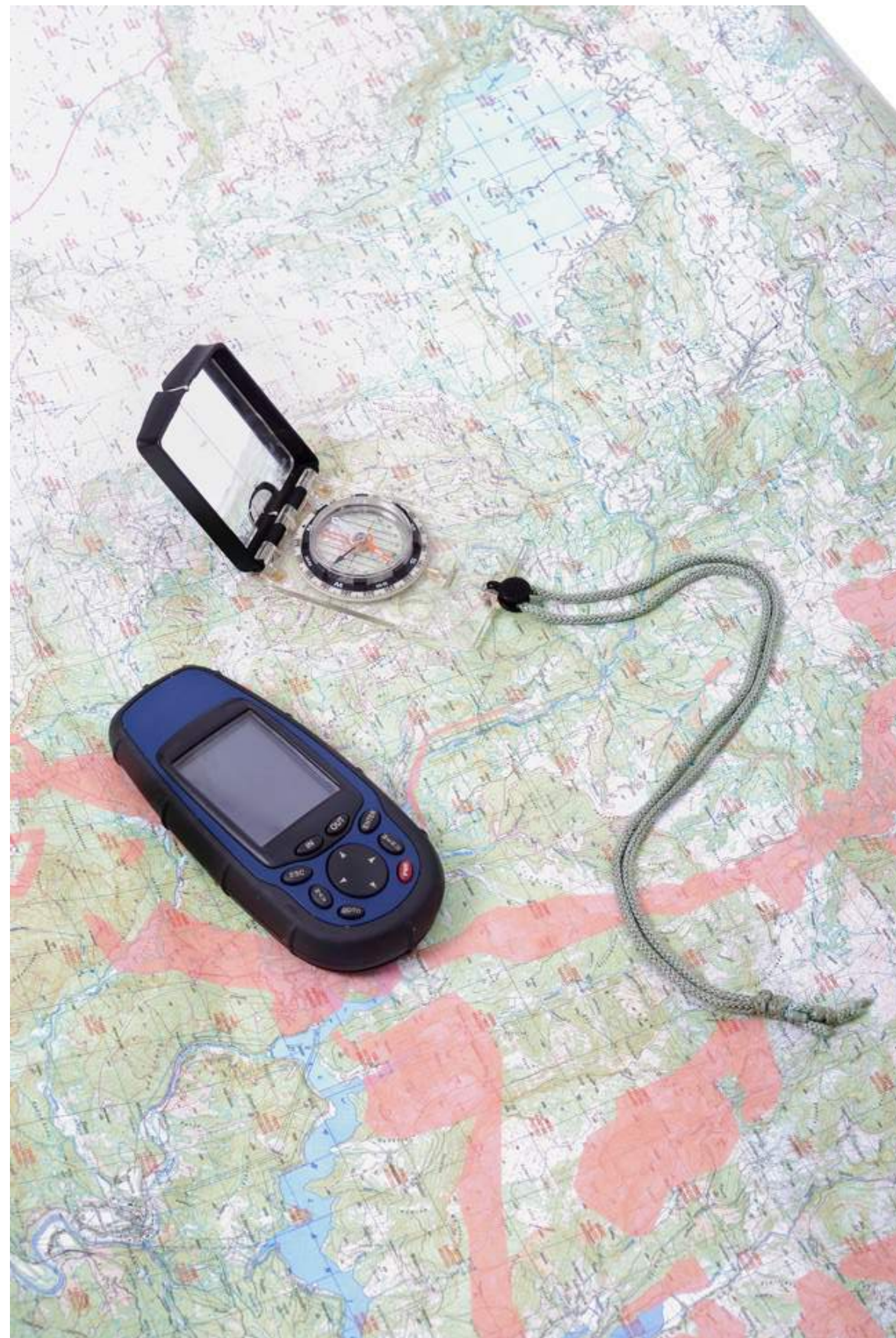
**Kevin Wallace, CCIEx2
(R/S & Collaboration) #7945**

Module 10

Routing (cont.)

Link State Routing Protocols

Every router has a map of the network.



OSPF's Link State Database Compared to a Puzzle



OSPF Fundamentals

- Open standard
- Establishes adjacencies with other routers
- Sends Link State Advertisements (LSAs) to other routers in an area
- Constructs a link state database from received LSAs
- Runs the Dijkstra Shortest Path First (SPF) algorithm to determine the shortest path to a network
- Attempts to inject the best path for each network into a router's IP routing table



Some OSPF Terminology

- **Hello:** A protocol used to discover OSPF neighbors and confirm reachability to those neighbors (also used in the election of a Designated Router)
- **Link State Advertisement (LSA):** Information a router sends and receives about network reachability (used to construct a router's Link State Database)
- **Link State Update (LSU):** A packet that carries LSAs
- **Link State Request (LSR):** Used by a router to request specific LSA information from a neighbor
- **Link State Acknowledgement (LSAck):** Used by a router to confirm it received an LSU



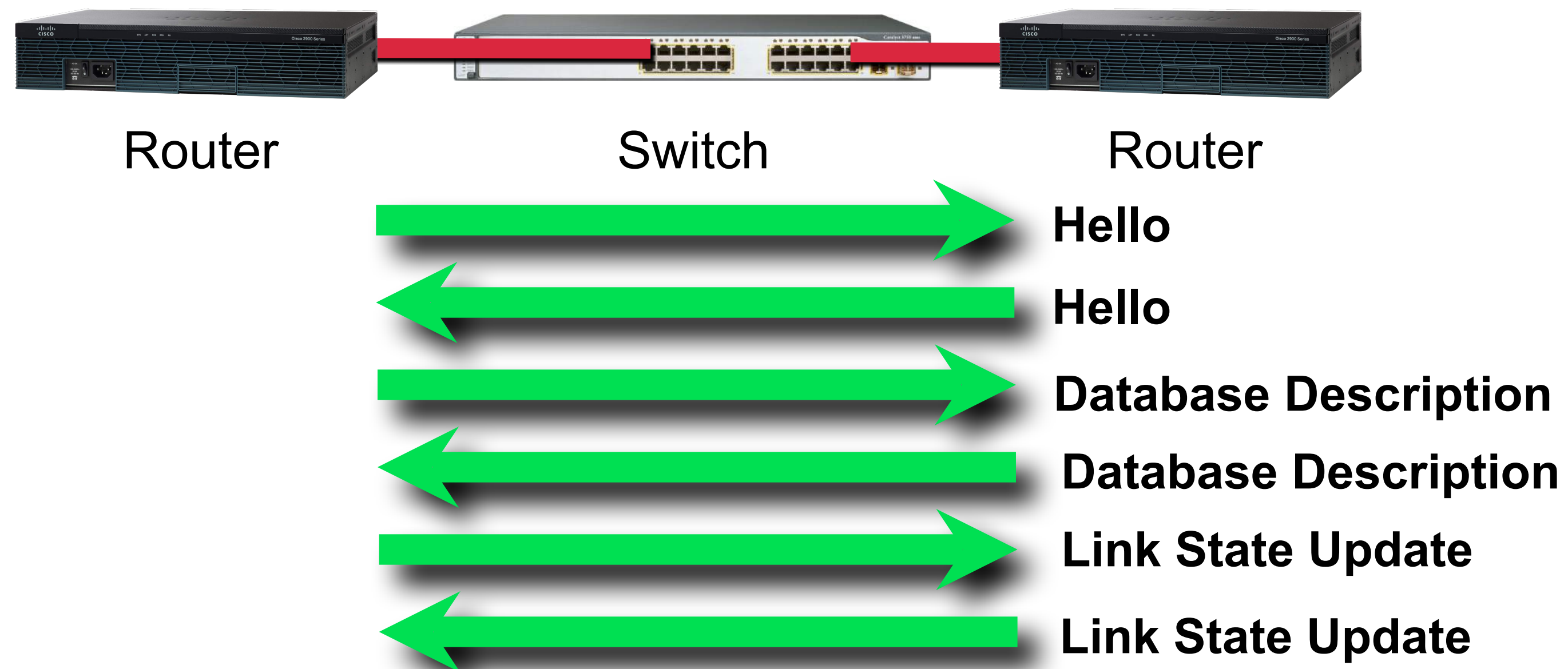
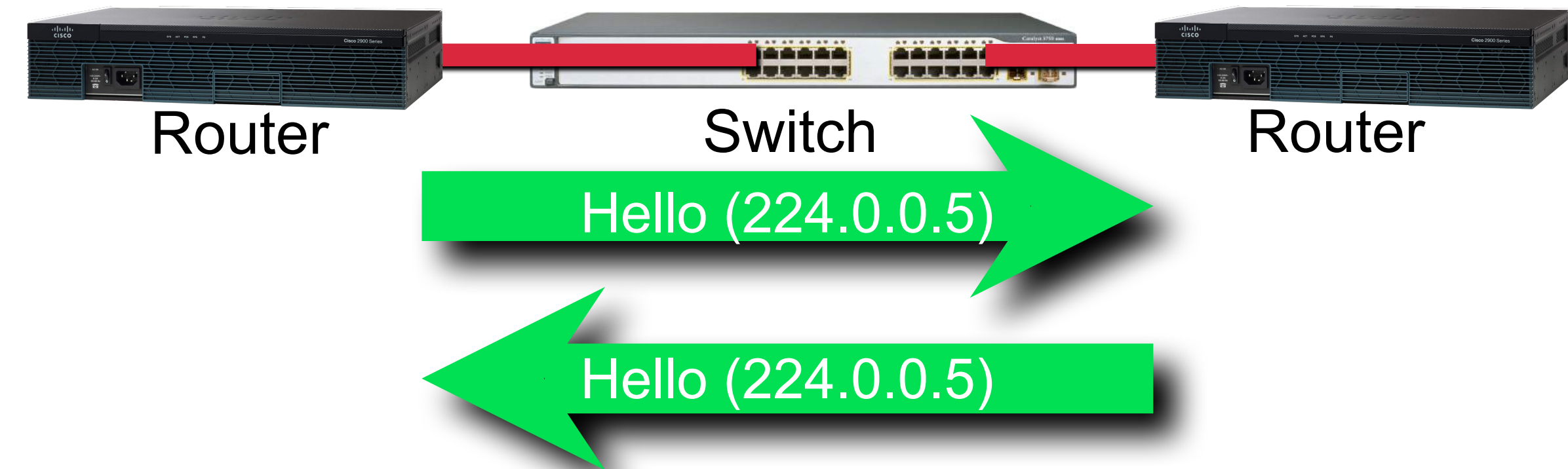
Neighborship vs. Adjacency

Neighbors are routers that:

- Reside on the same network link
- Exchange Hello messages

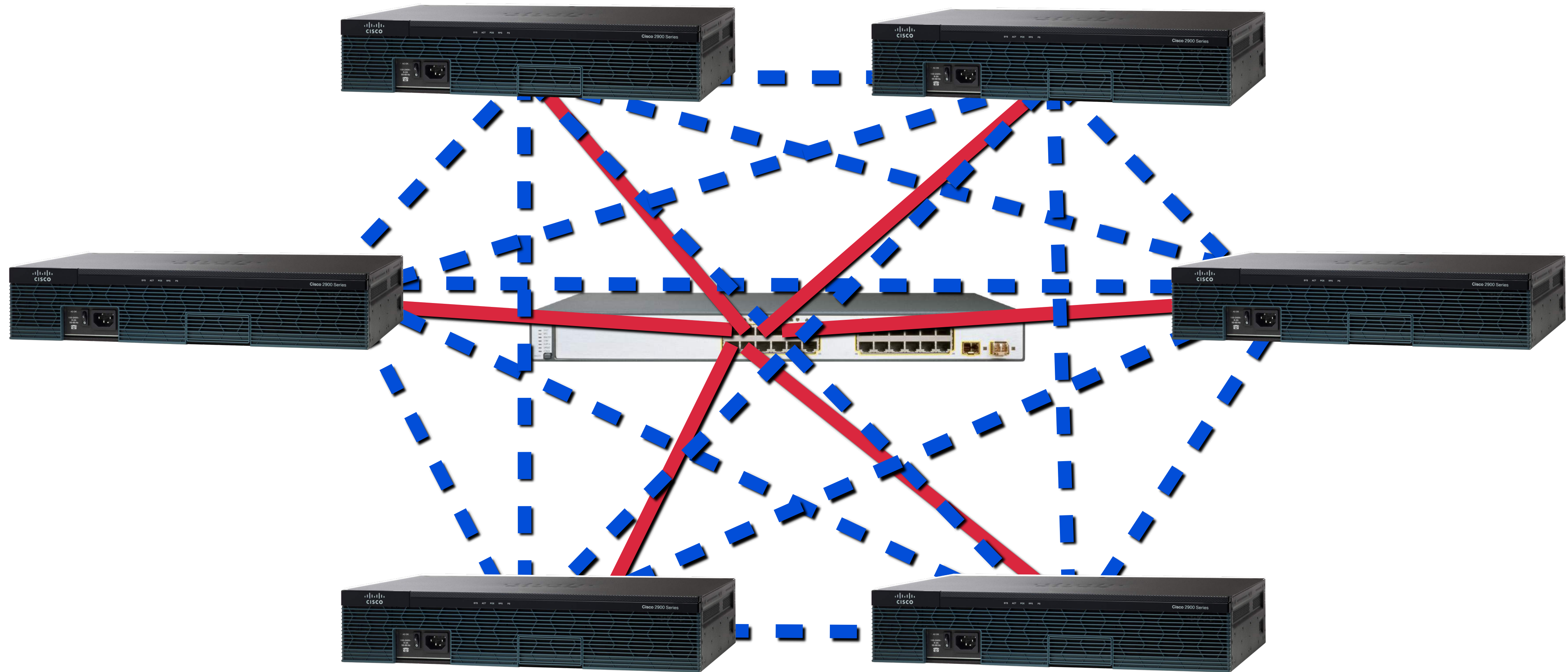
Adjacencies are routers that:

- Are neighbors
- Have exchanged Link State Updates (LSUs) and Database Description (DD) packets



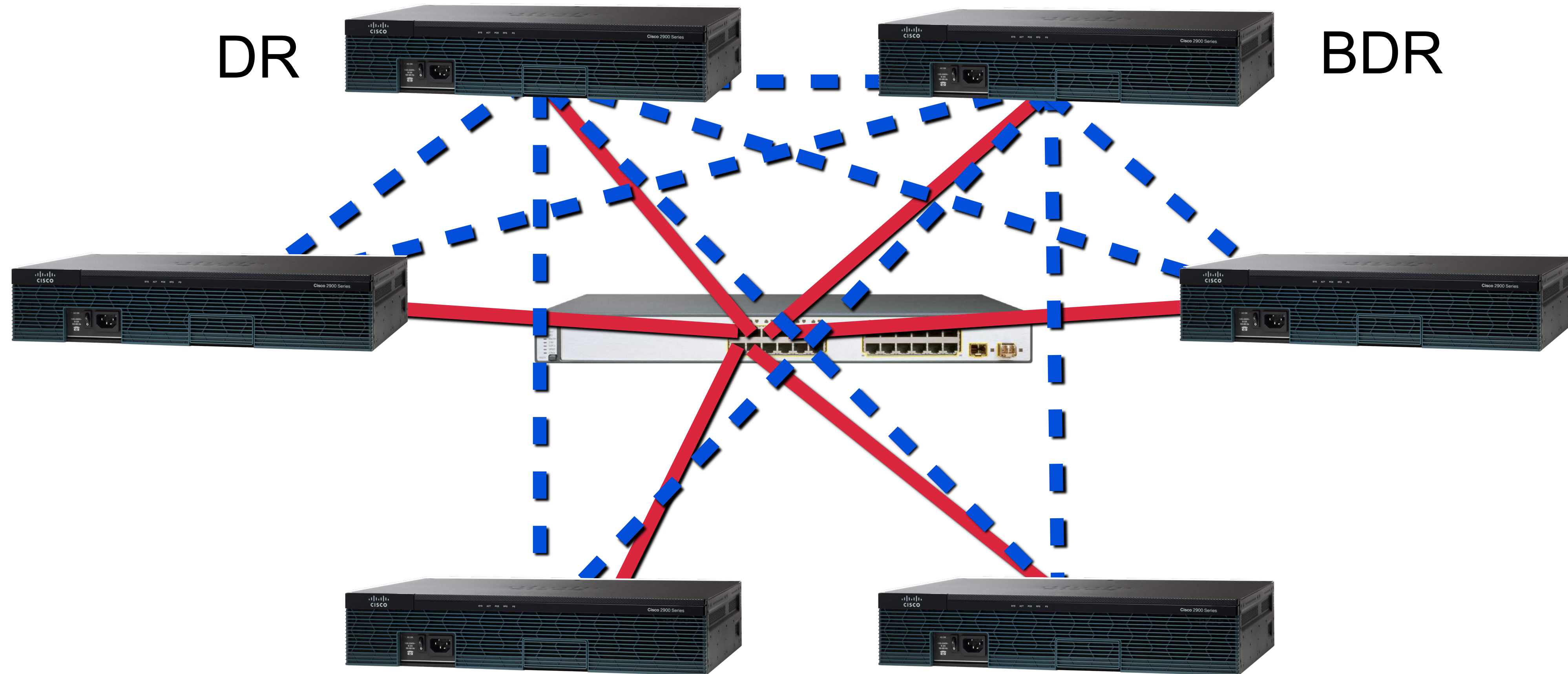
DR and BDR

of Adjacencies = $[n * (n - 1)] / 2$, where n is the number of routers.



DR and BDR

Adjacencies only need to be formed with the DR and BDR.

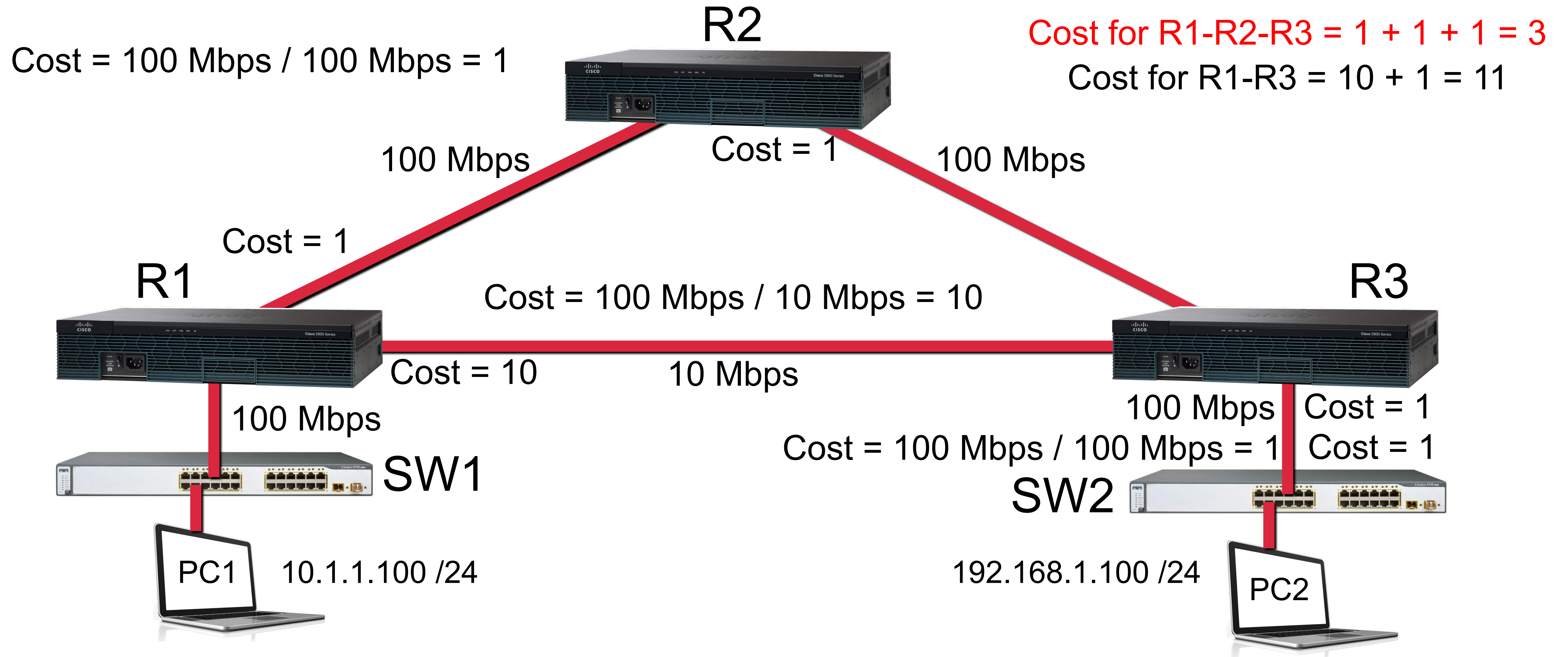


224.0.0.5 - All OSPF routers
224.0.0.6 - All designated routers

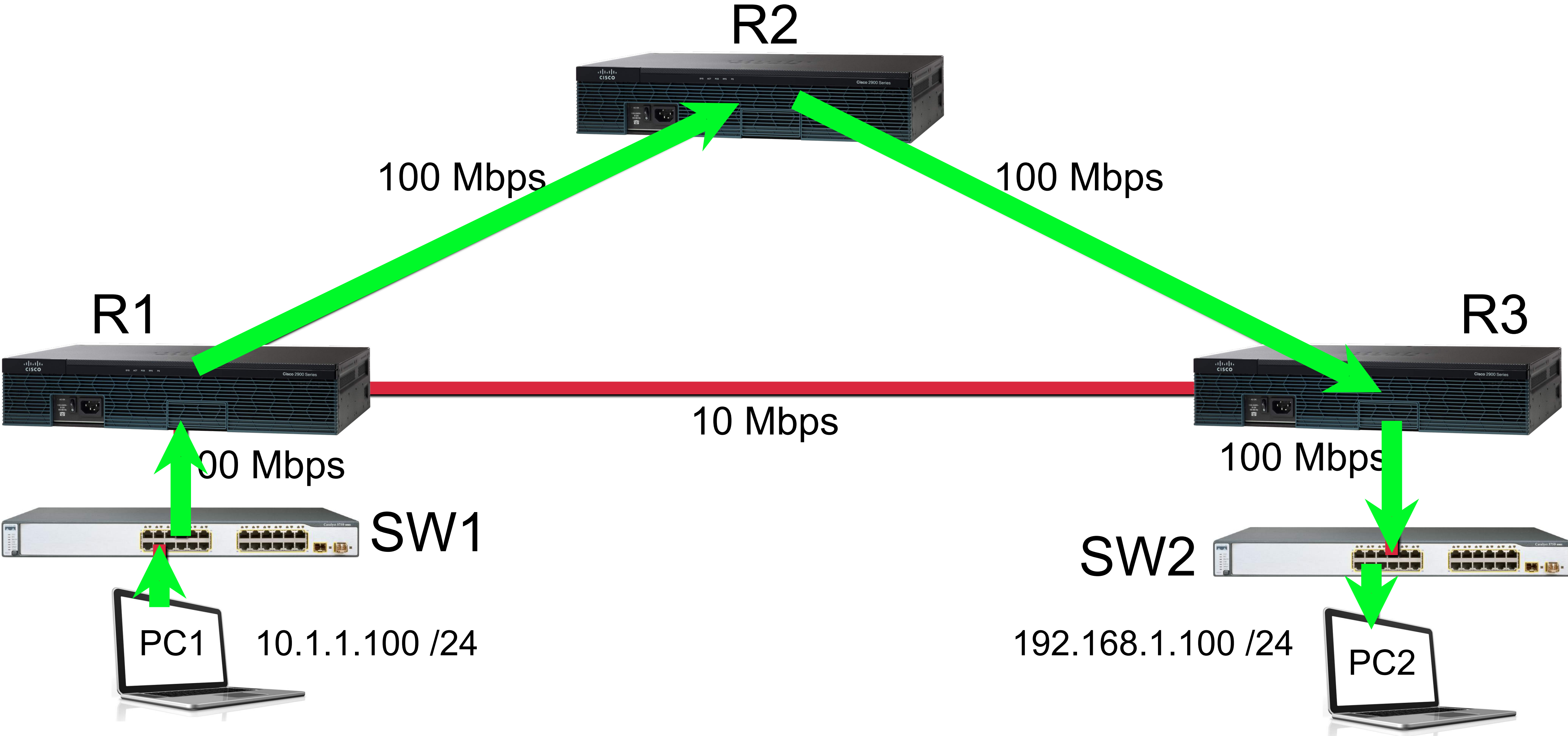
OSPF Cost

The default reference bandwidth is 100,000,000 bits per second (100 Mbps).

$$\text{Cost} = \text{Reference BW} / \text{Interface BW}$$

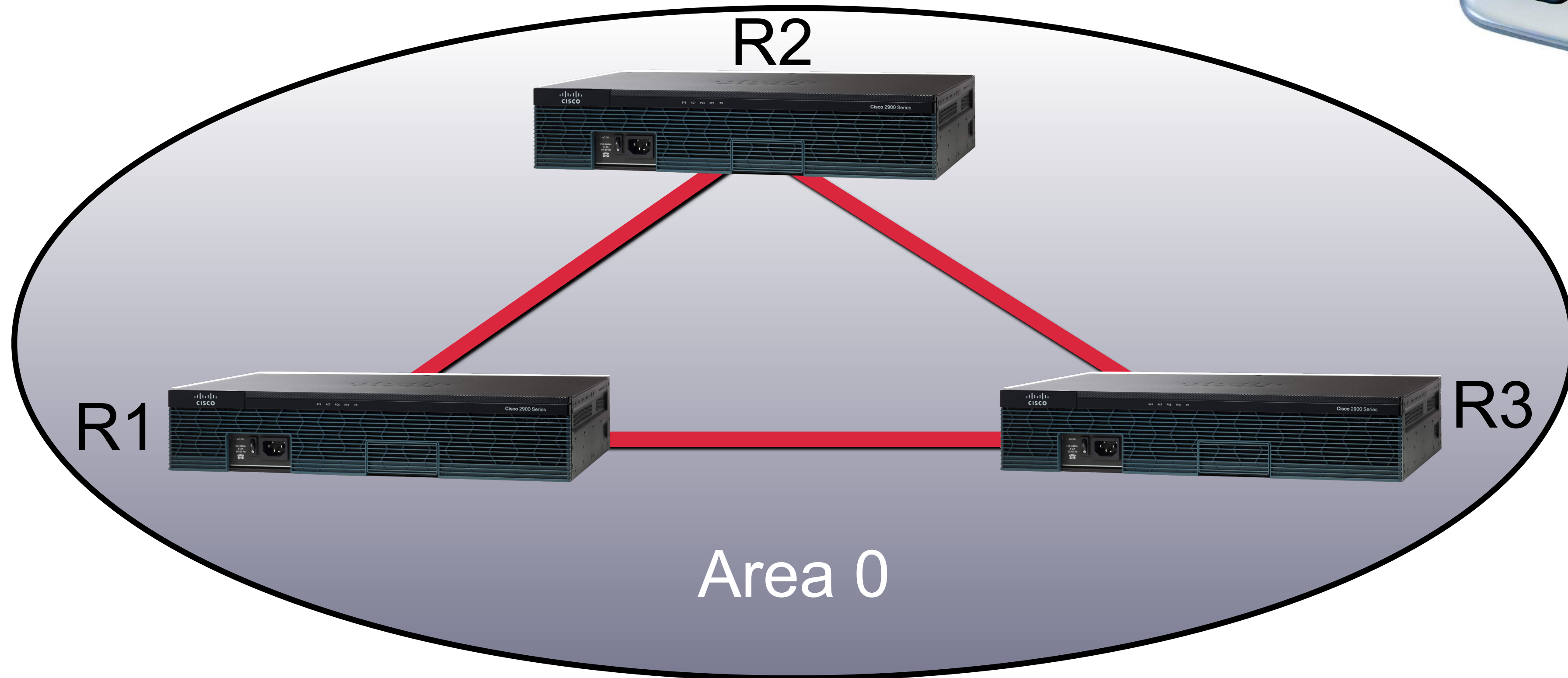


OSPF Cost

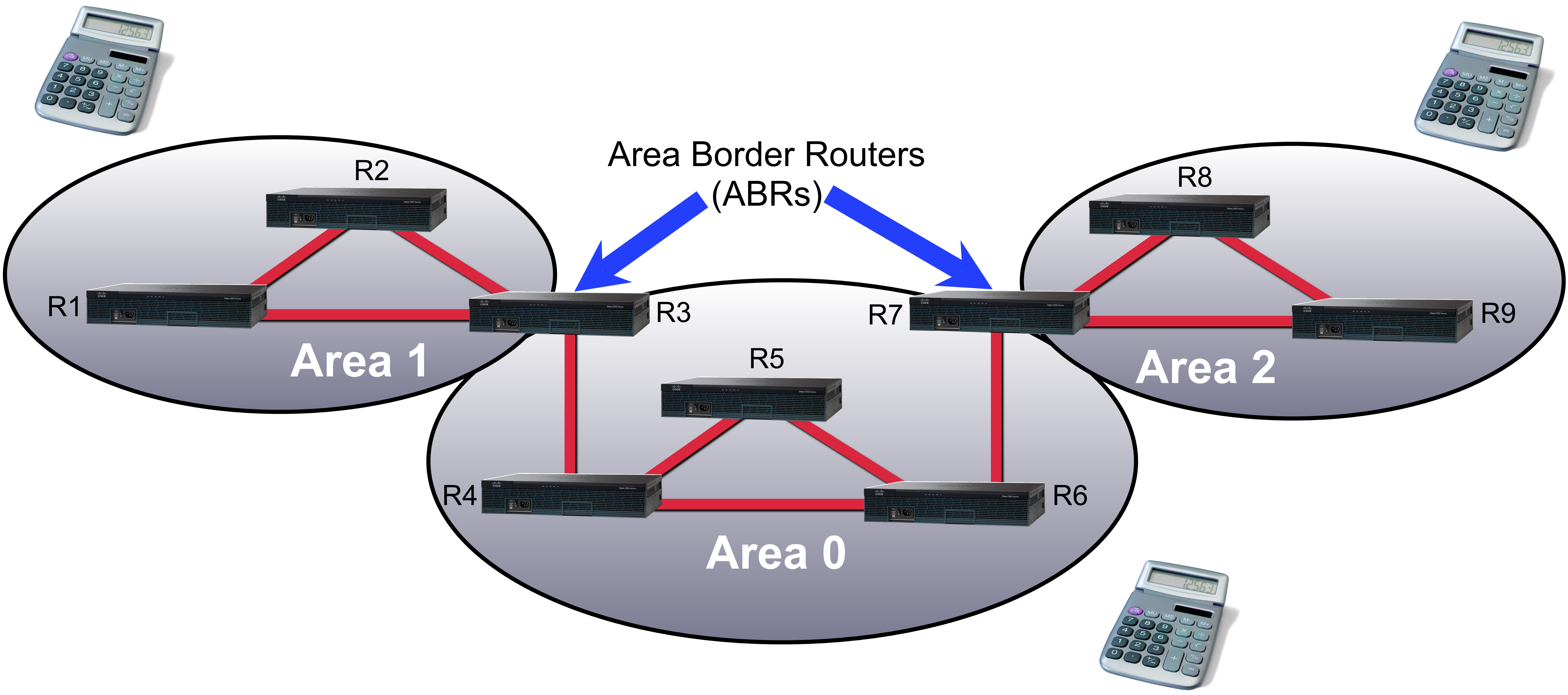


OSPF Areas

We always have a backbone area.



OSPF Areas



Characteristics of EIGRP

- Fast convergence



Characteristics of EIGRP

- Fast convergence
- Scalable



Characteristics of EIGRP

- Fast convergence
- Scalable
- Load balancing over unequal cost links



Characteristics of EIGRP

- Fast convergence
- Scalable
- Load balancing over unequal cost links
- Classless (VLSM support)

10.1.1.0 /24

10.2.2.0 /24

10.5.5.0 /24

Characteristics of EIGRP

- Fast convergence
- Scalable
- Load balancing over unequal cost links
- Classless (VLSM support)
- Communicates via multicast

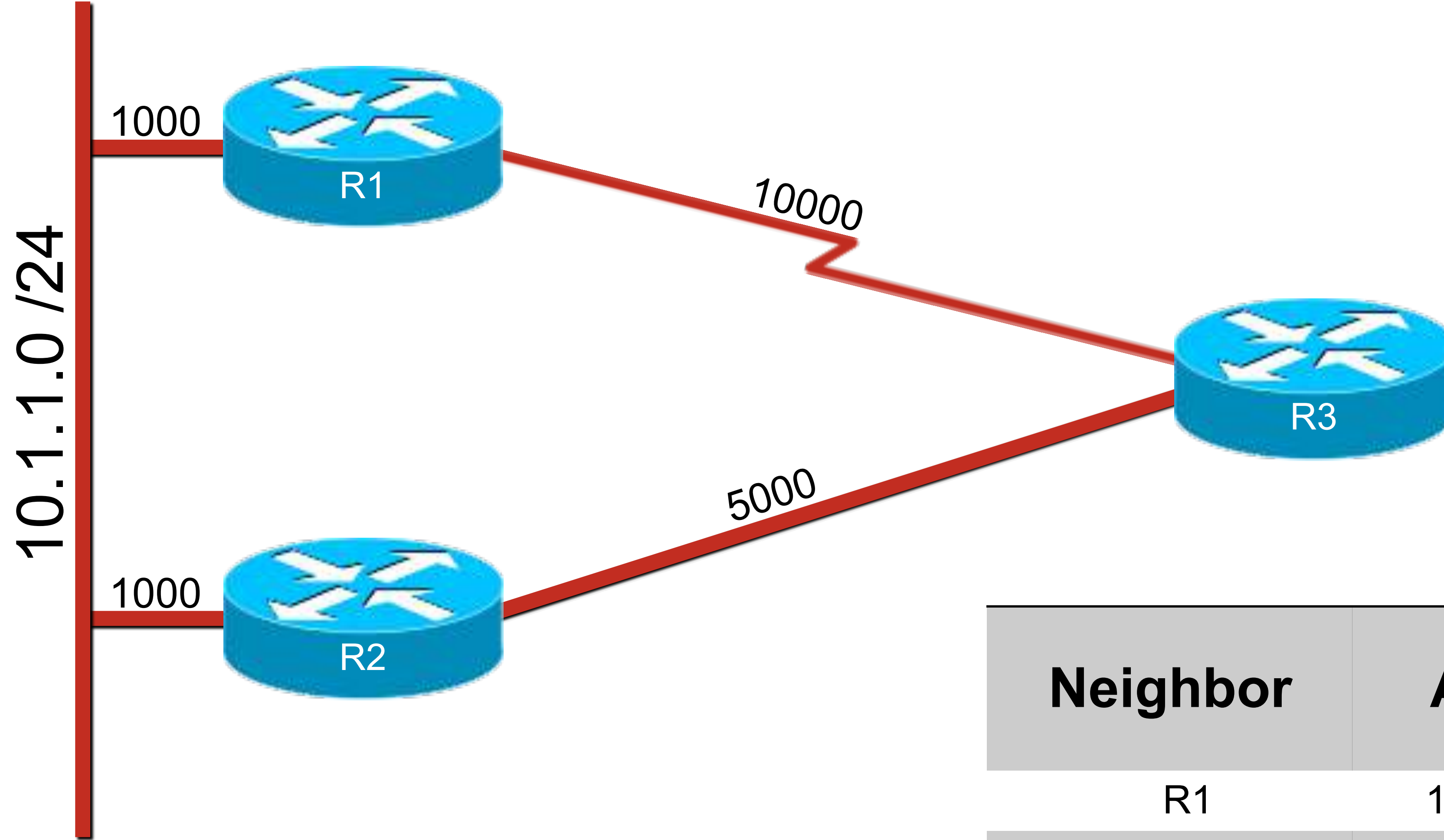
224.0.0.10

Characteristics of EIGRP

- Fast convergence
- Scalable
- Load balancing over unequal cost links
- Classless (VLSM support)
- Communicates via multicast
- Was Cisco-proprietary



Path Selection



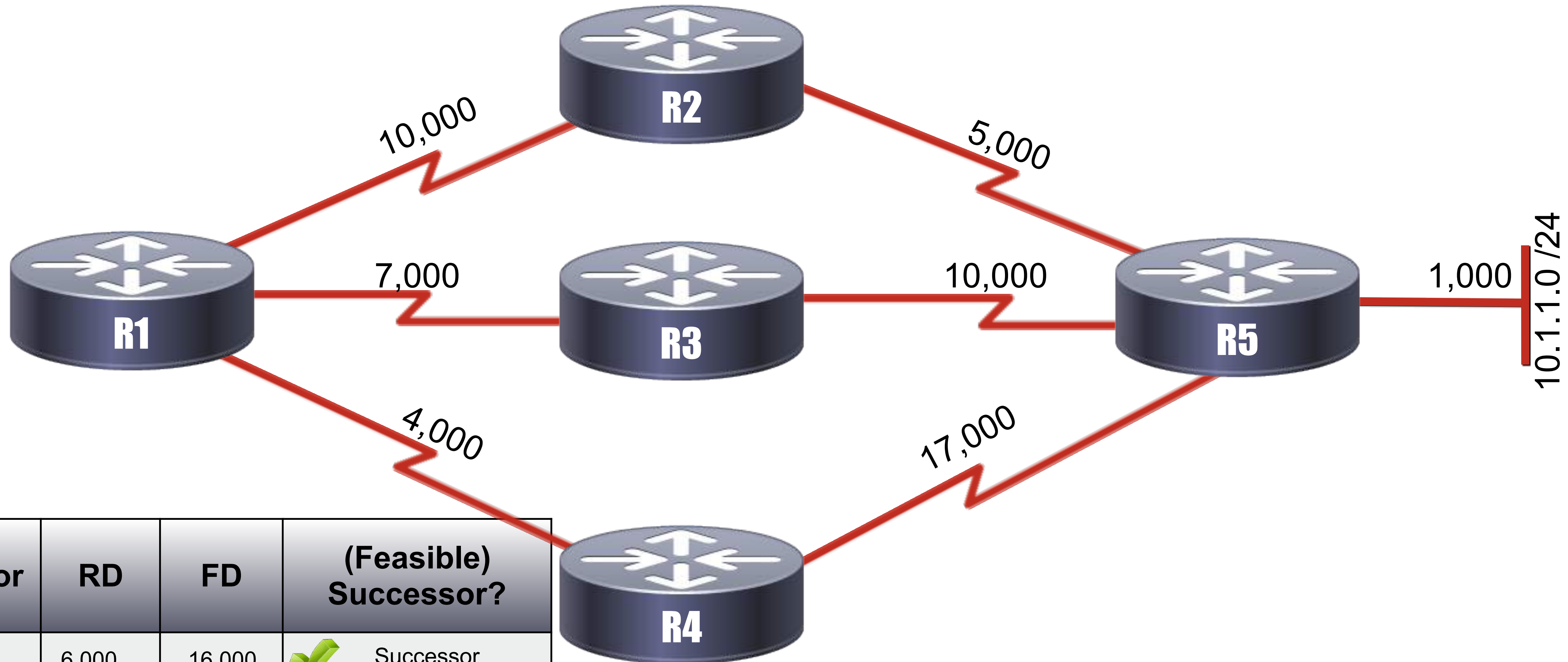
Neighbor	AD	FD
R1	1000	11000
R2	1000	6000

The Feasibility Condition

An EIGRP route is a feasible successor route if its reported distance (RD) from our neighbor is less than the feasible distance (FD) of the successor route.



The Feasibility Condition



Neighbor	RD	FD	(Feasible) Successor?
R2	6,000	16,000	✓ Successor
R3	11,000	18,000	✓ Feasible Successor
R4	18,000	22,000	✗

Metric Calculation

B _____

D _____

R _____

L _____

M _____

Default K Values:

$$K1 = 1$$

$$K2 = 0$$

$$K3 = 1$$

$$K4 = 0$$

$$K5 = 0$$



$$\text{Metric} = \left[\left(K1 * BW_{\min} + \frac{K2 * BW_{\min}}{256 - \text{load}} + K3 * \text{delay} \right) * \frac{K5}{K4 + \text{reliability}} \right] * 256$$

$$BW_{\min} = \frac{10^7}{\text{least-bandwidth}}$$

BGP Characteristics



BGP

- Forms Neighbor-ships
- Neighbor's IP Address is Explicitly Configured
- A TCP Session is Established Between Neighbors
- Advertises Address Prefix and Length
- Advertises Path Attributes
- Path Vector Routing Protocol

Module 10

Routing

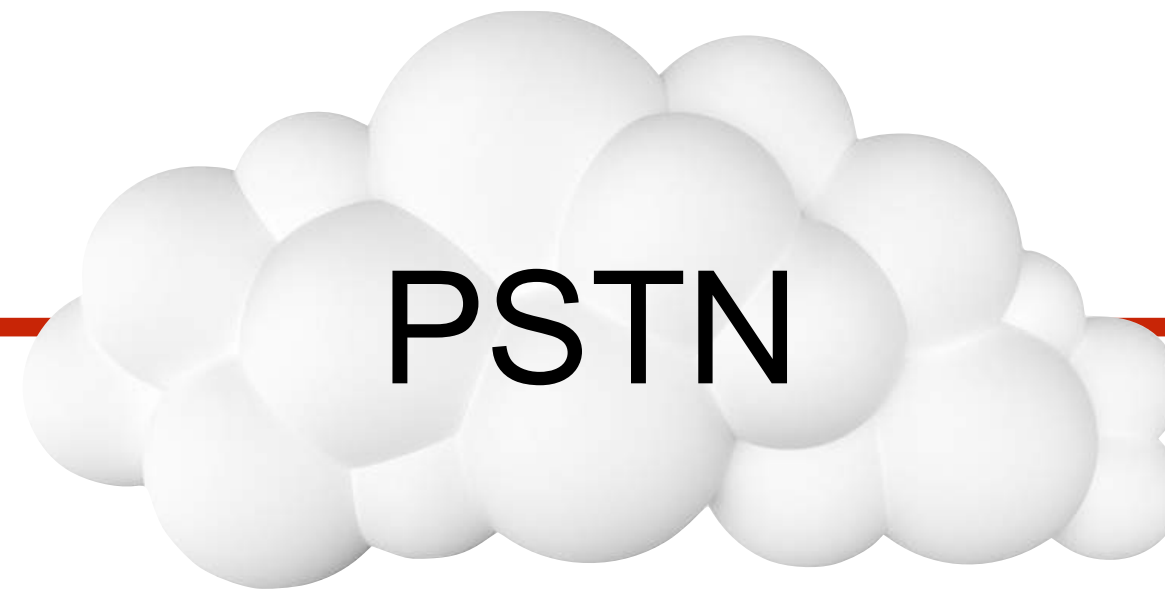
Module 11

Unified Communications

Analog Phone

Voice over IP (VoIP)

Analog Phone



Analog Phone

Voice over IP (VoIP)

Analog Phone



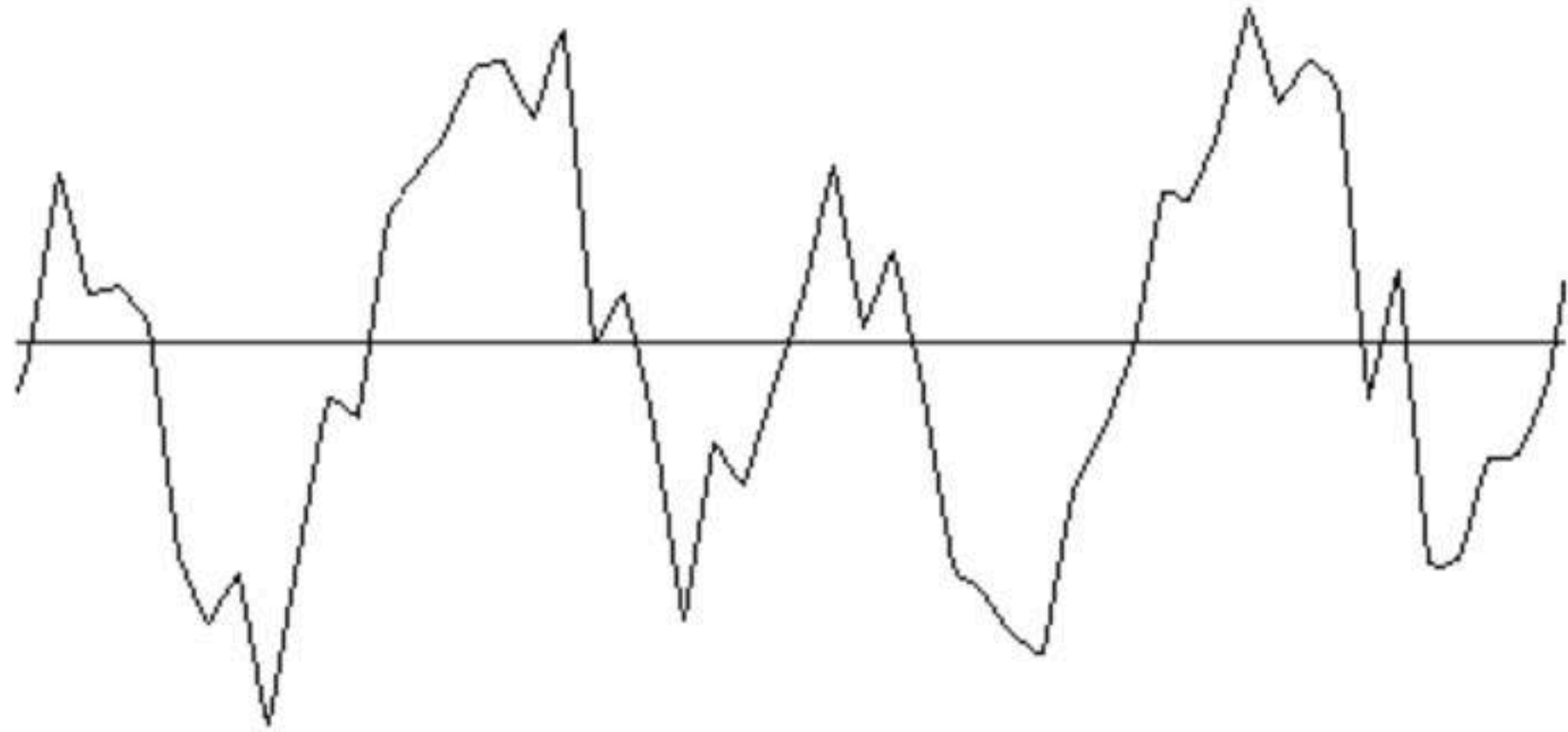
Router

Router

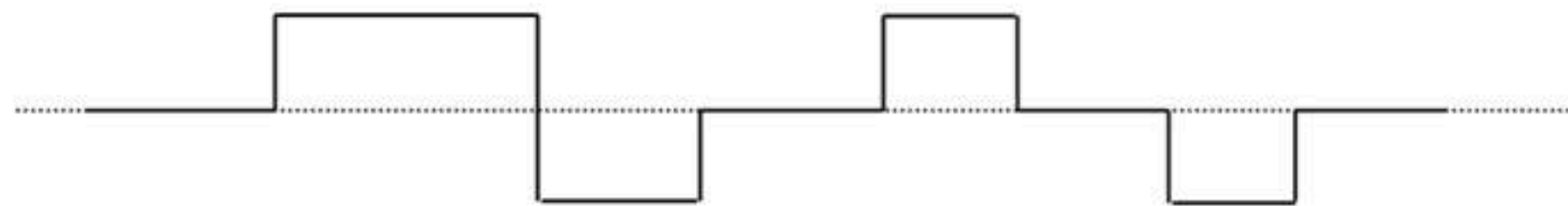


Digitizing Voice

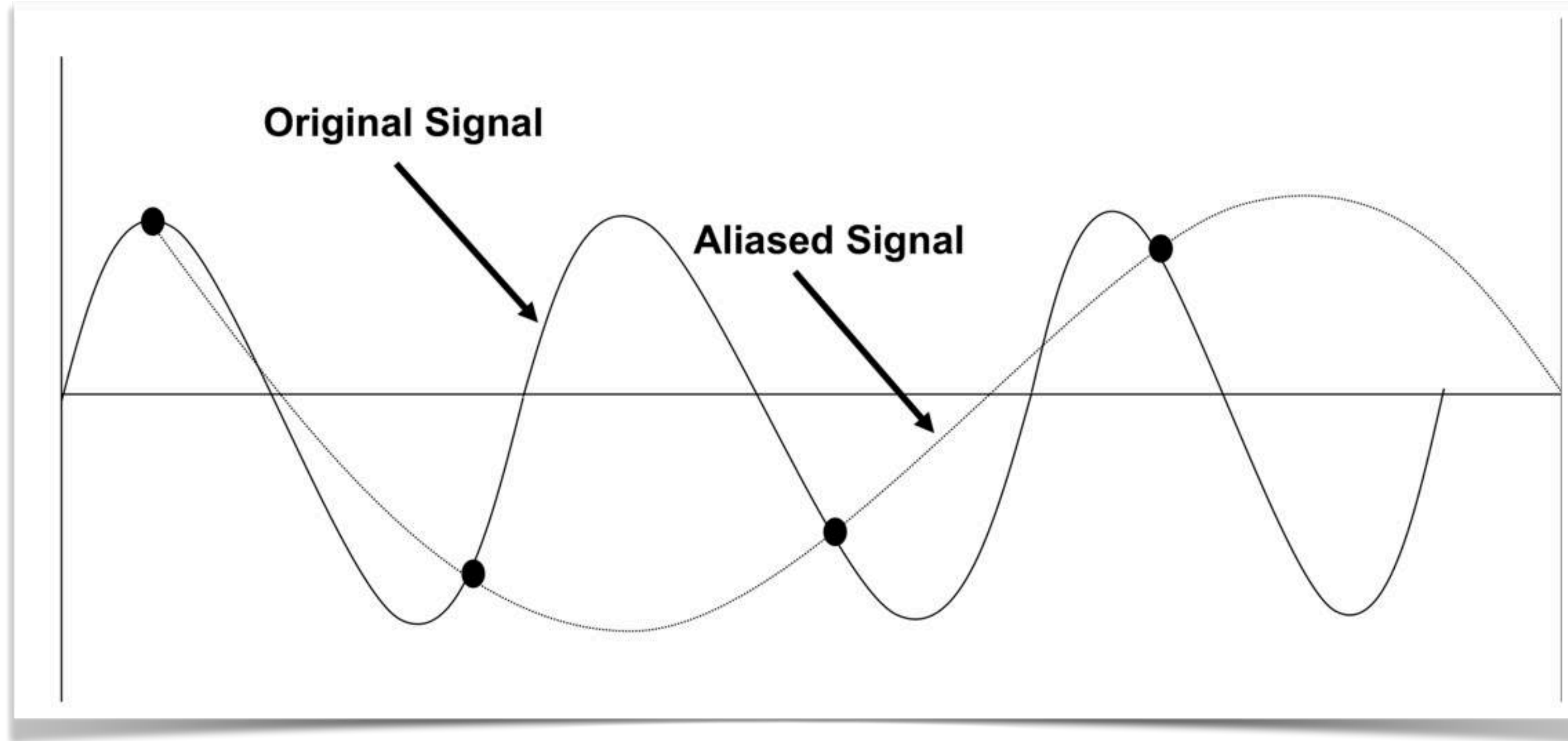
Analog Waveform



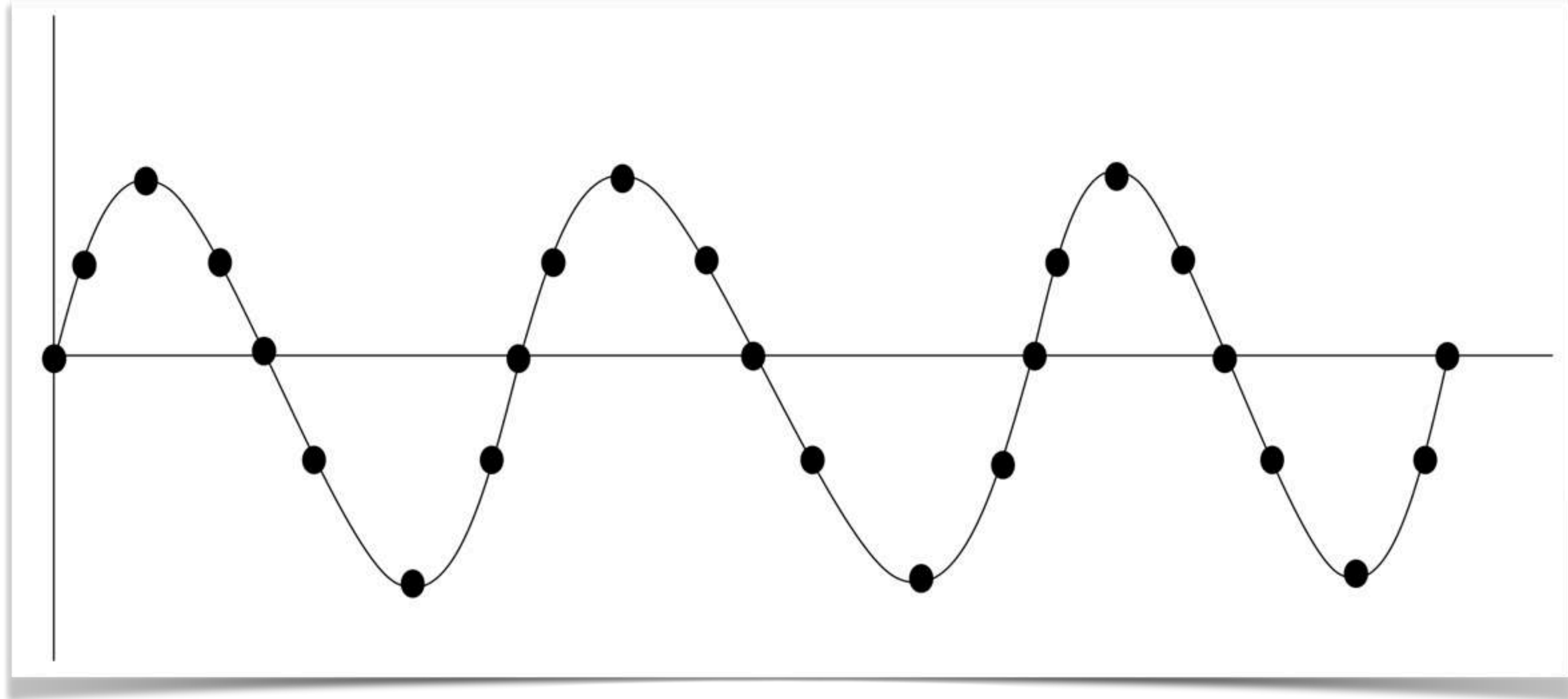
Digital Waveform



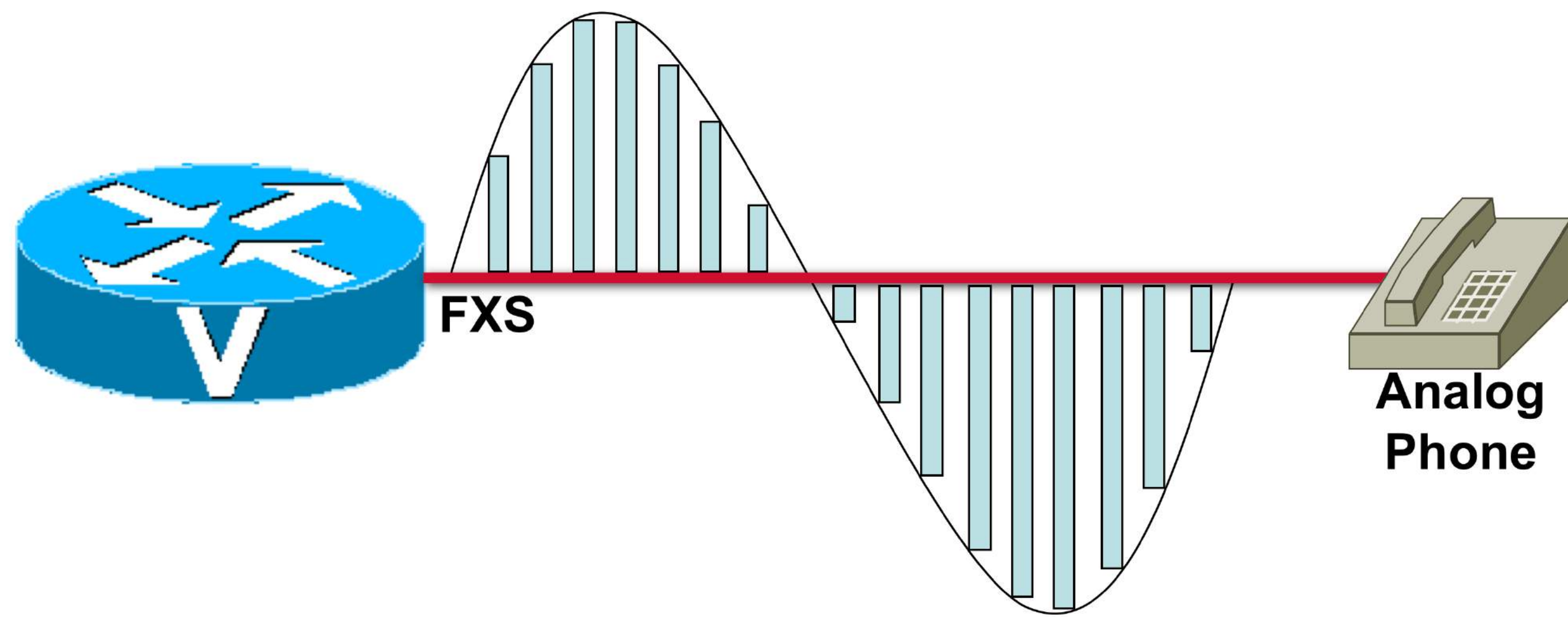
Digitizing Voice



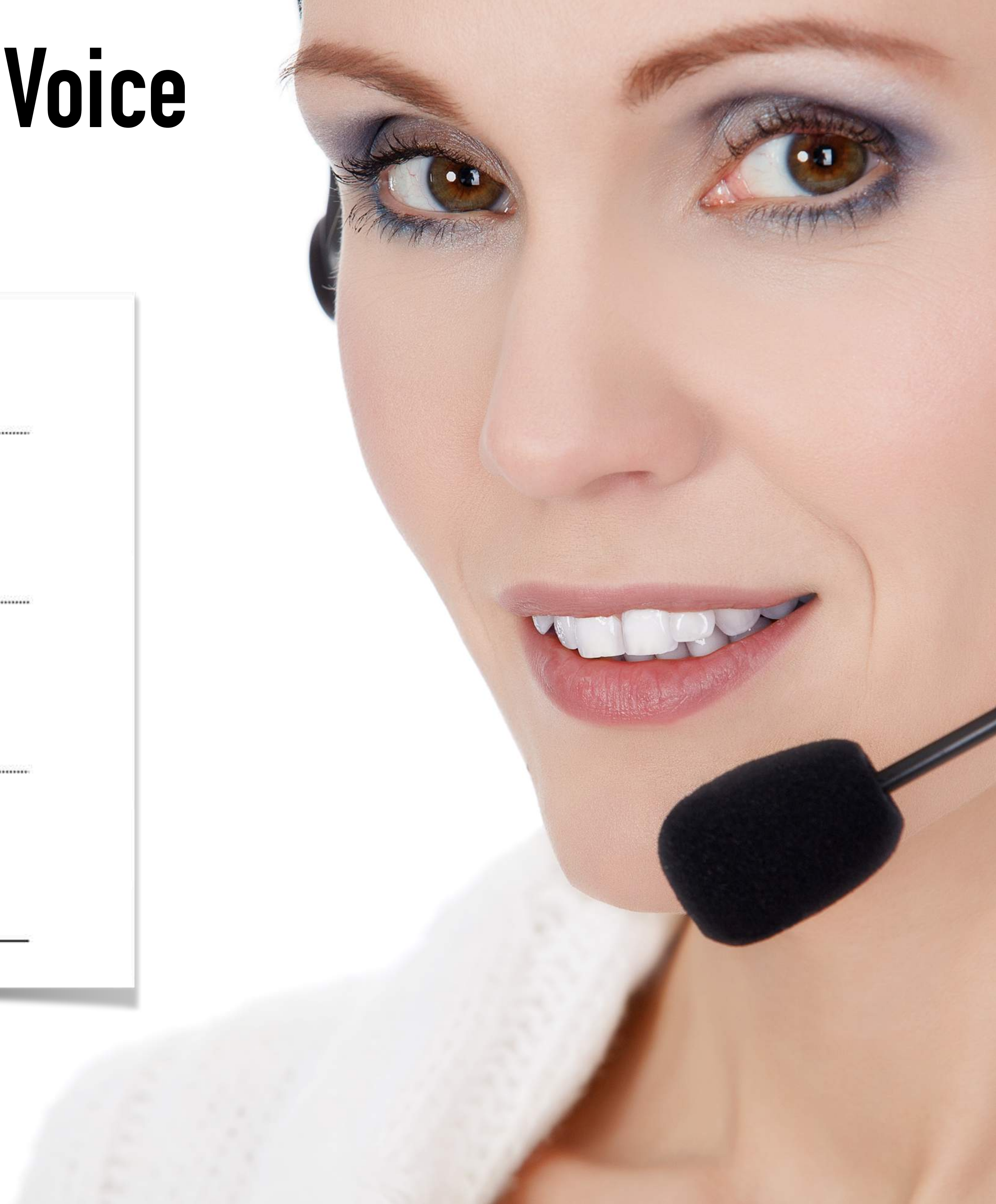
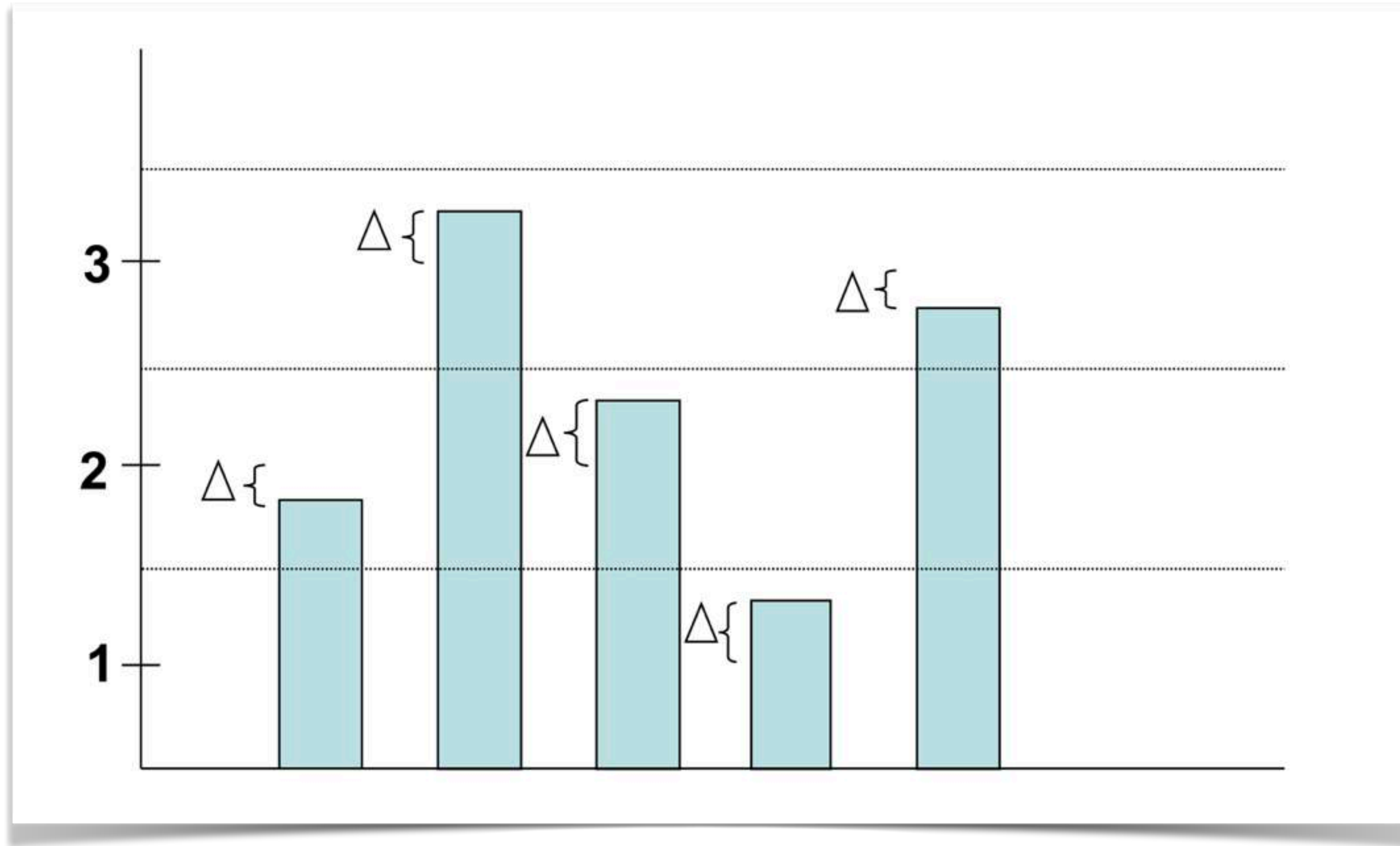
Digitizing Voice



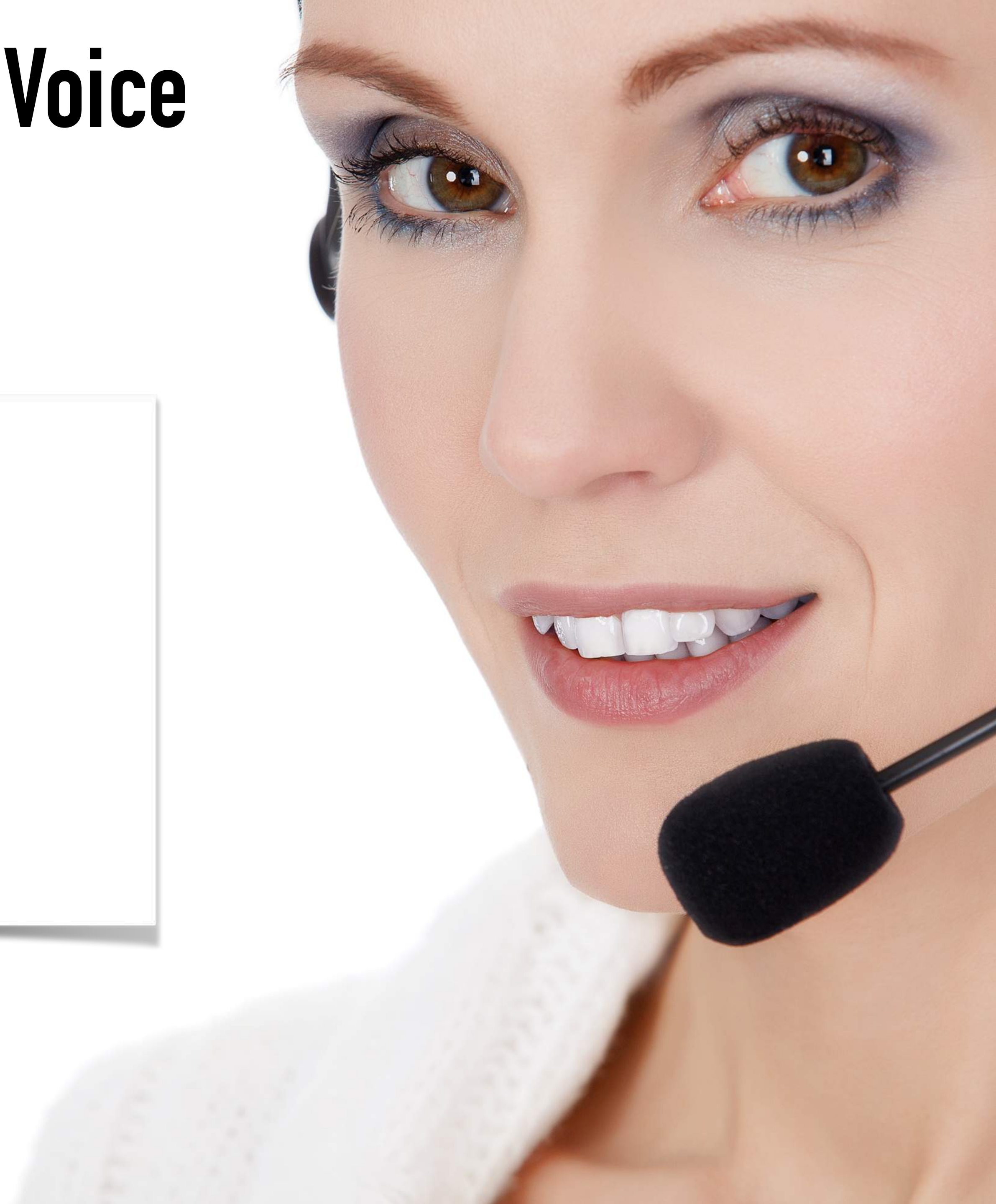
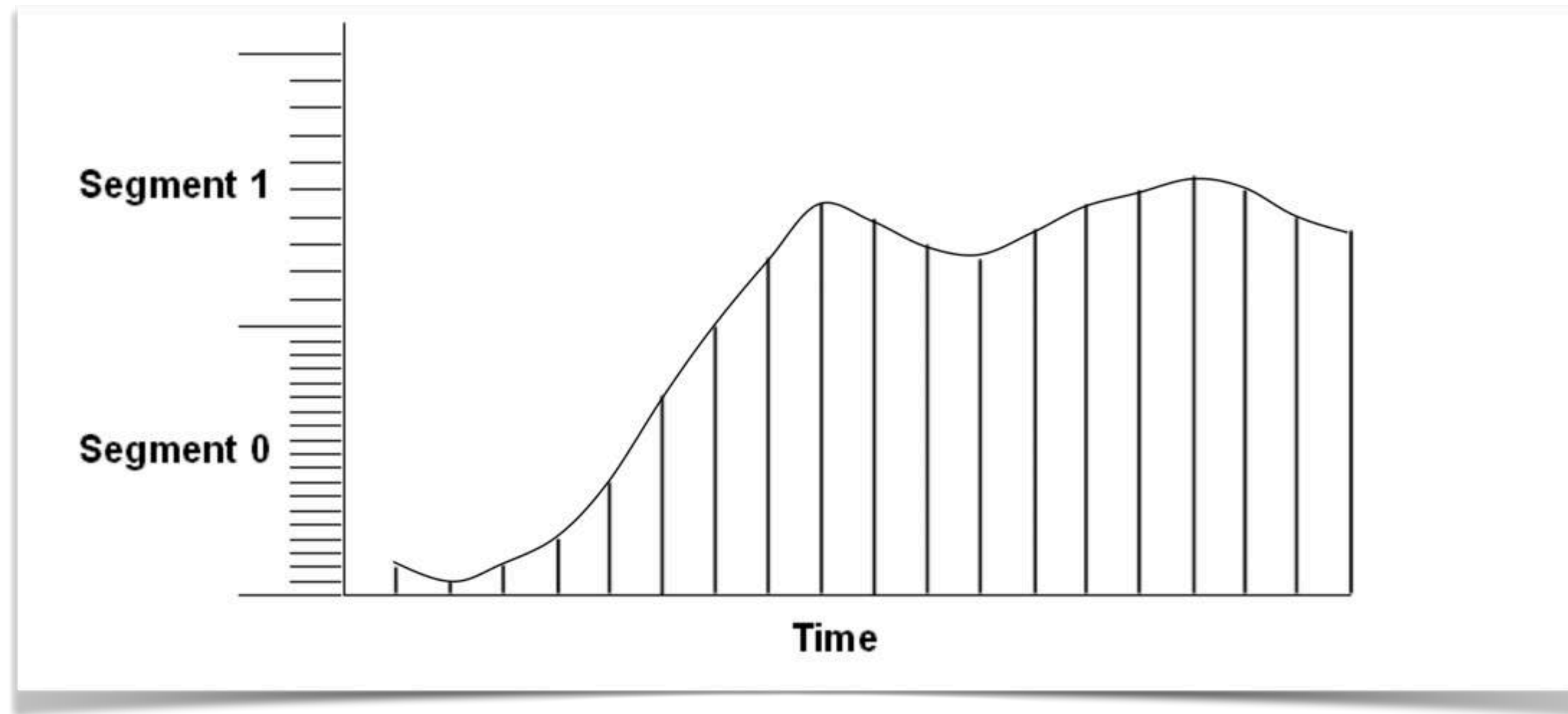
Digitizing Voice



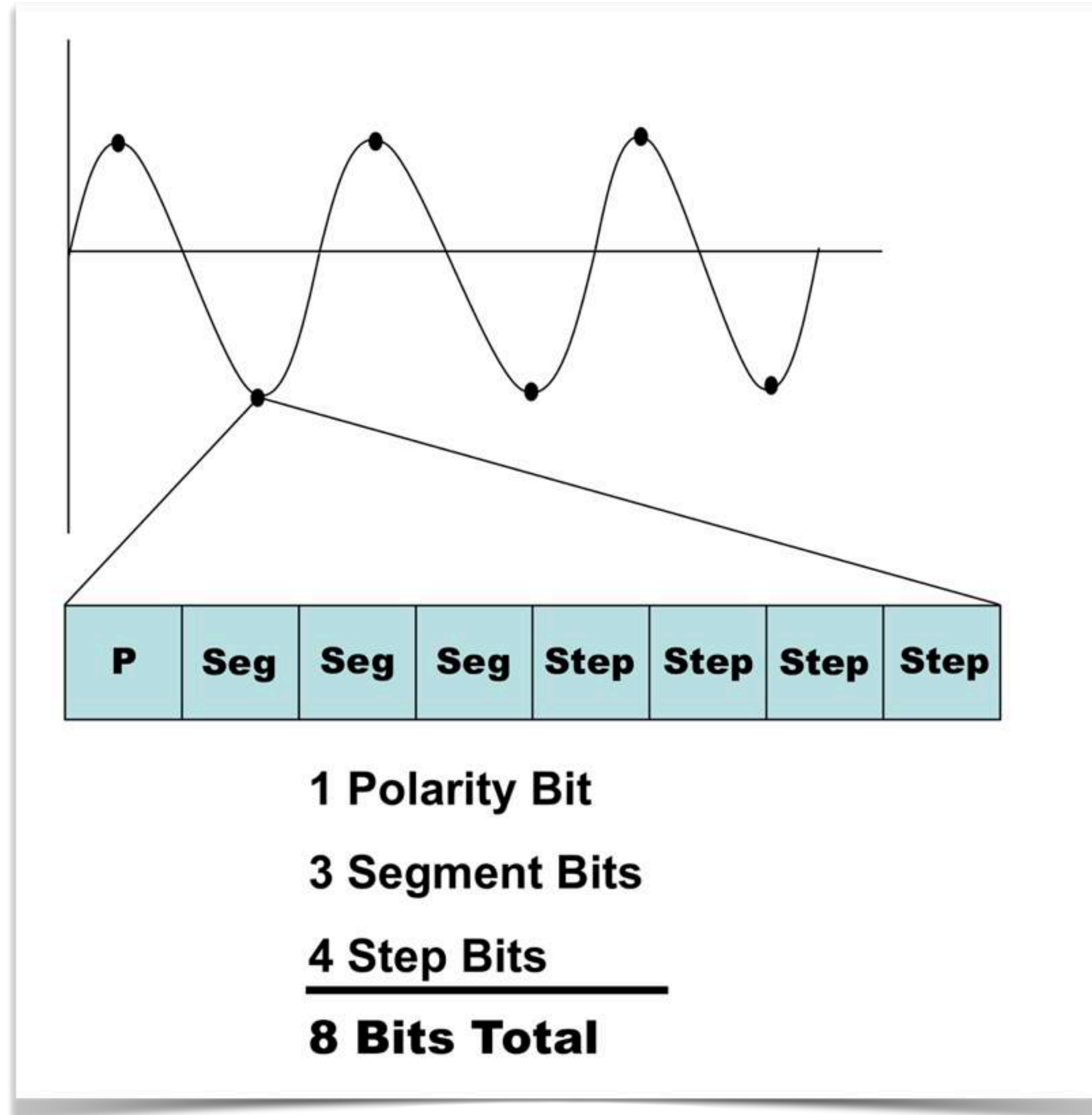
Digitizing Voice



Digitizing Voice

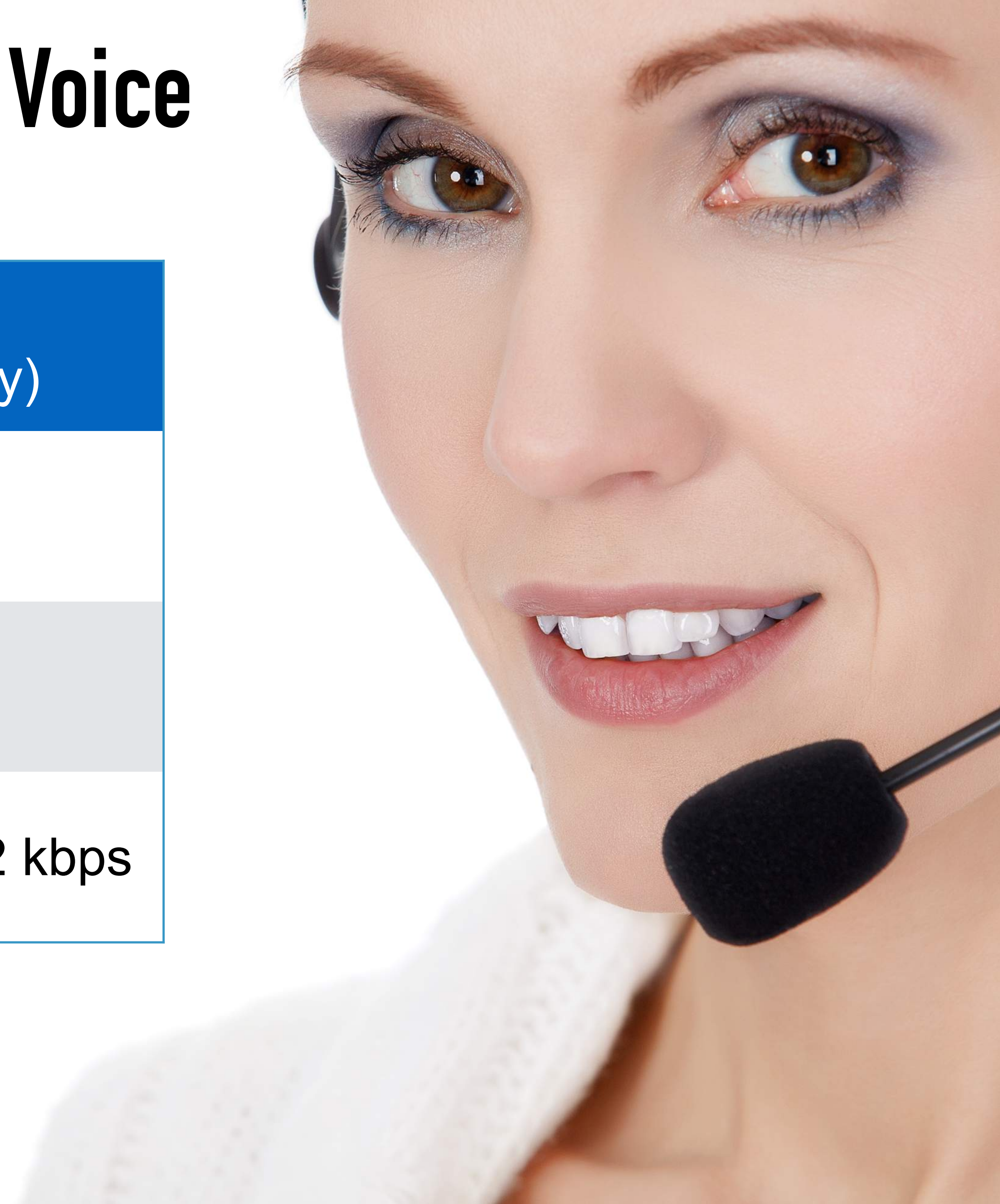


Digitizing Voice

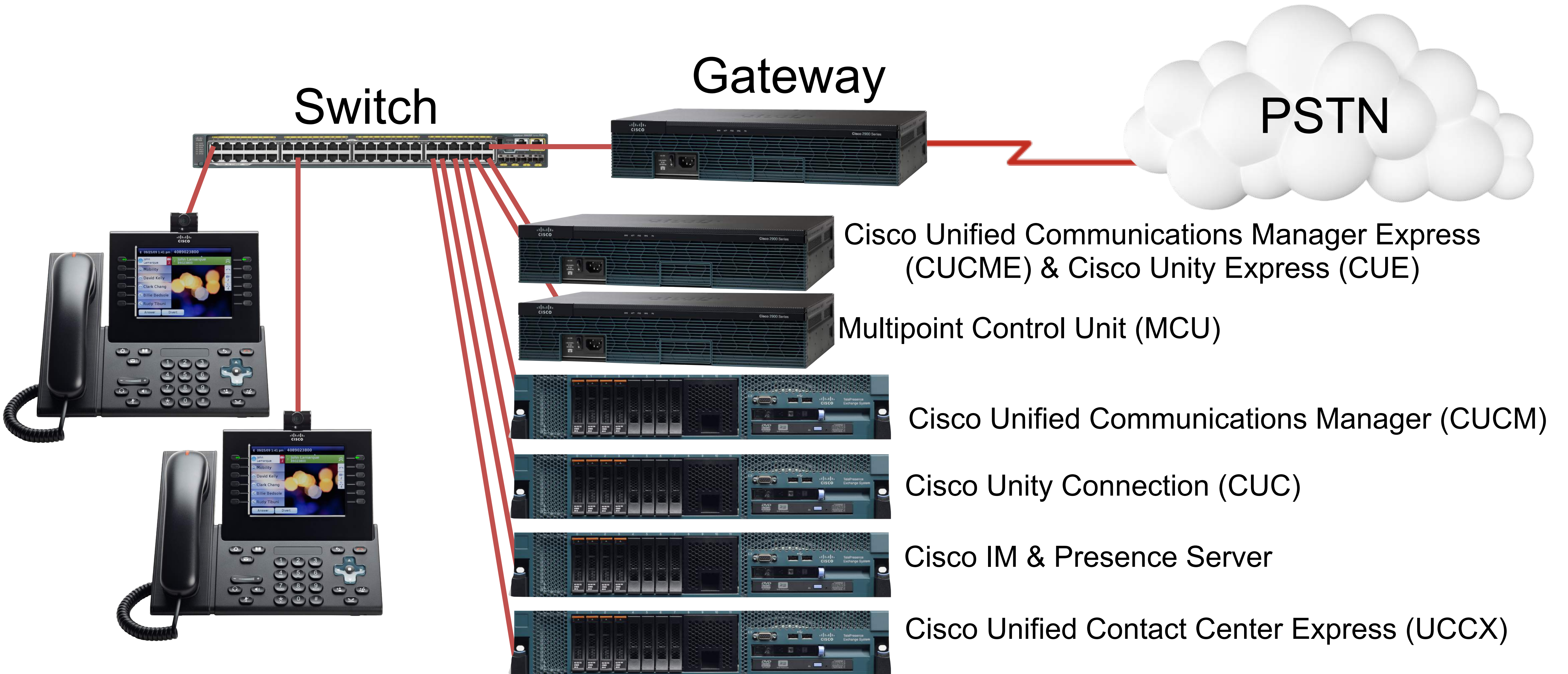


Digitizing Voice

Codec	Bandwidth (Payload Only)
G.711	64 kbps
G.729	8 kbps
iLBC	13.3 kbps or 15.2 kbps



Unified Communications



Examples of Video Applications



Audio and Video IP Phone

Audio and Video



Audio and Video IP Phone

Video
Calls

Examples of Video Applications



Video Conference Calls

Examples of Video Applications

Video Contact
Center

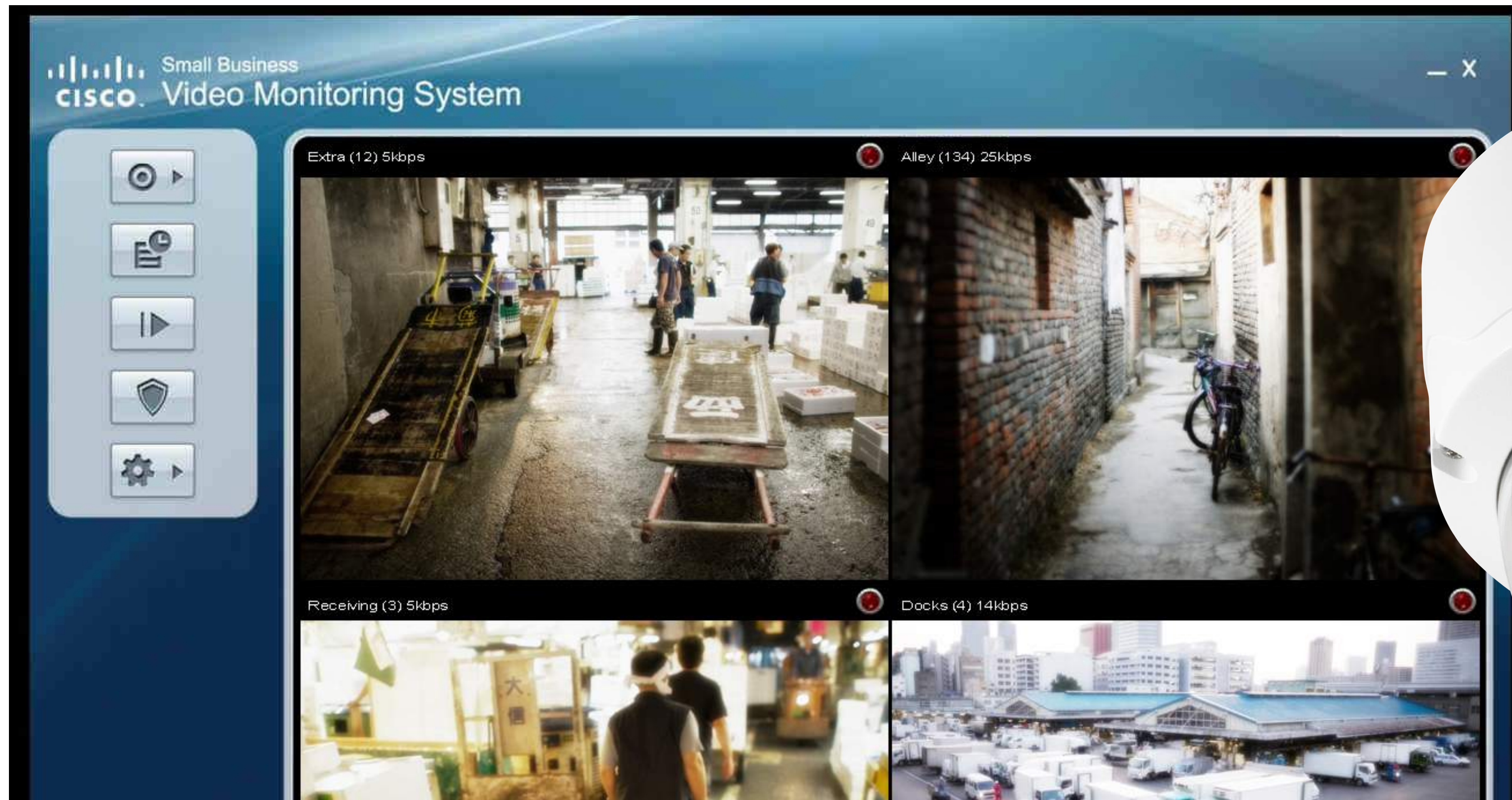


Examples of Video Applications



Video Communication with
Business Partners

Examples of Video Applications

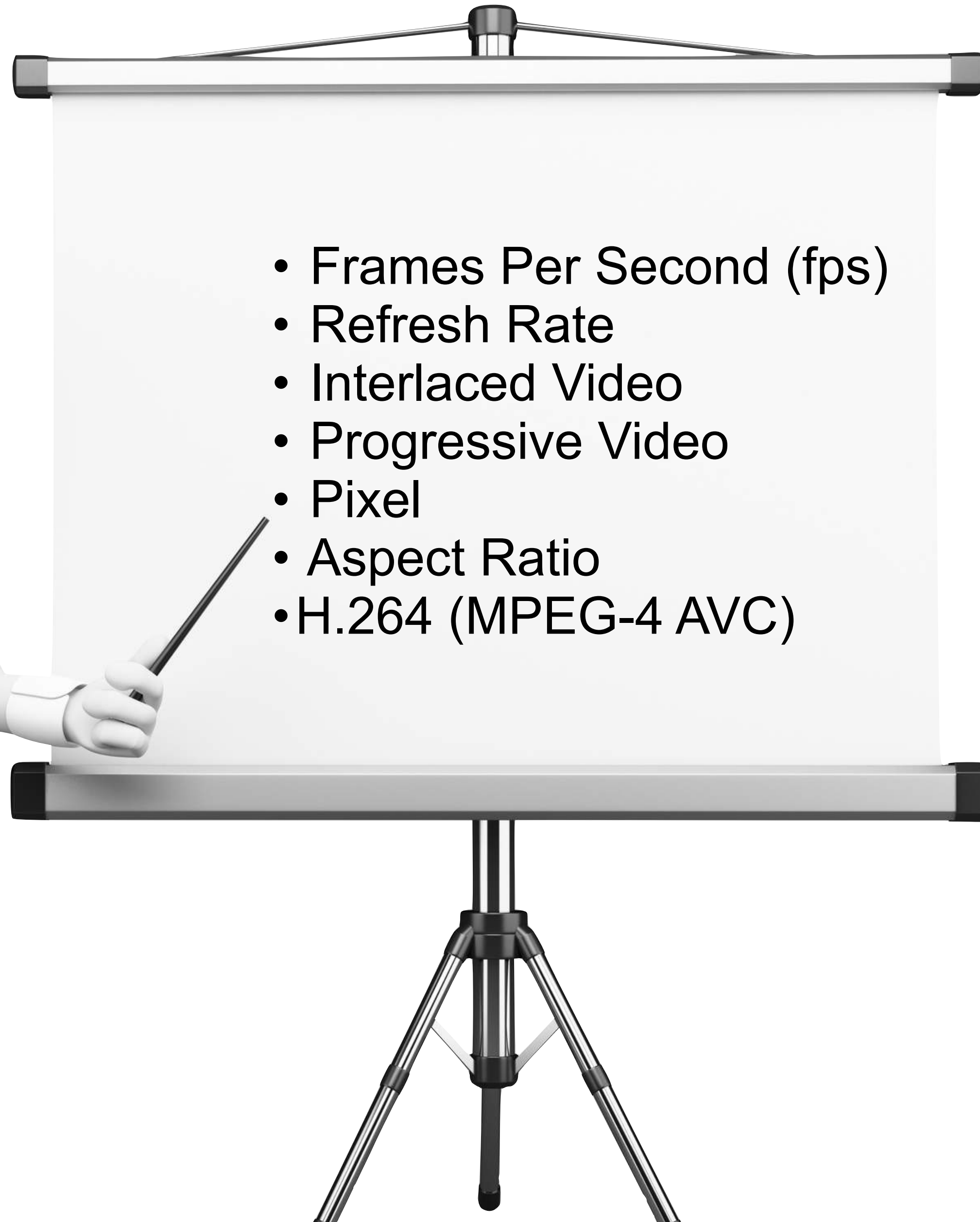


Video Surveillance



Terms to Know

- Frames Per Second (fps)
- Refresh Rate
- Interlaced Video
- Progressive Video
- Pixel
- Aspect Ratio
- H.264 (MPEG-4 AVC)



Terms to Know

- Frames Per Second (fps)
- Refresh Rate
- Interlaced Video
- Progressive Video
- Pixel
- Aspect Ratio
- H.264 (MPEG-4 AVC)



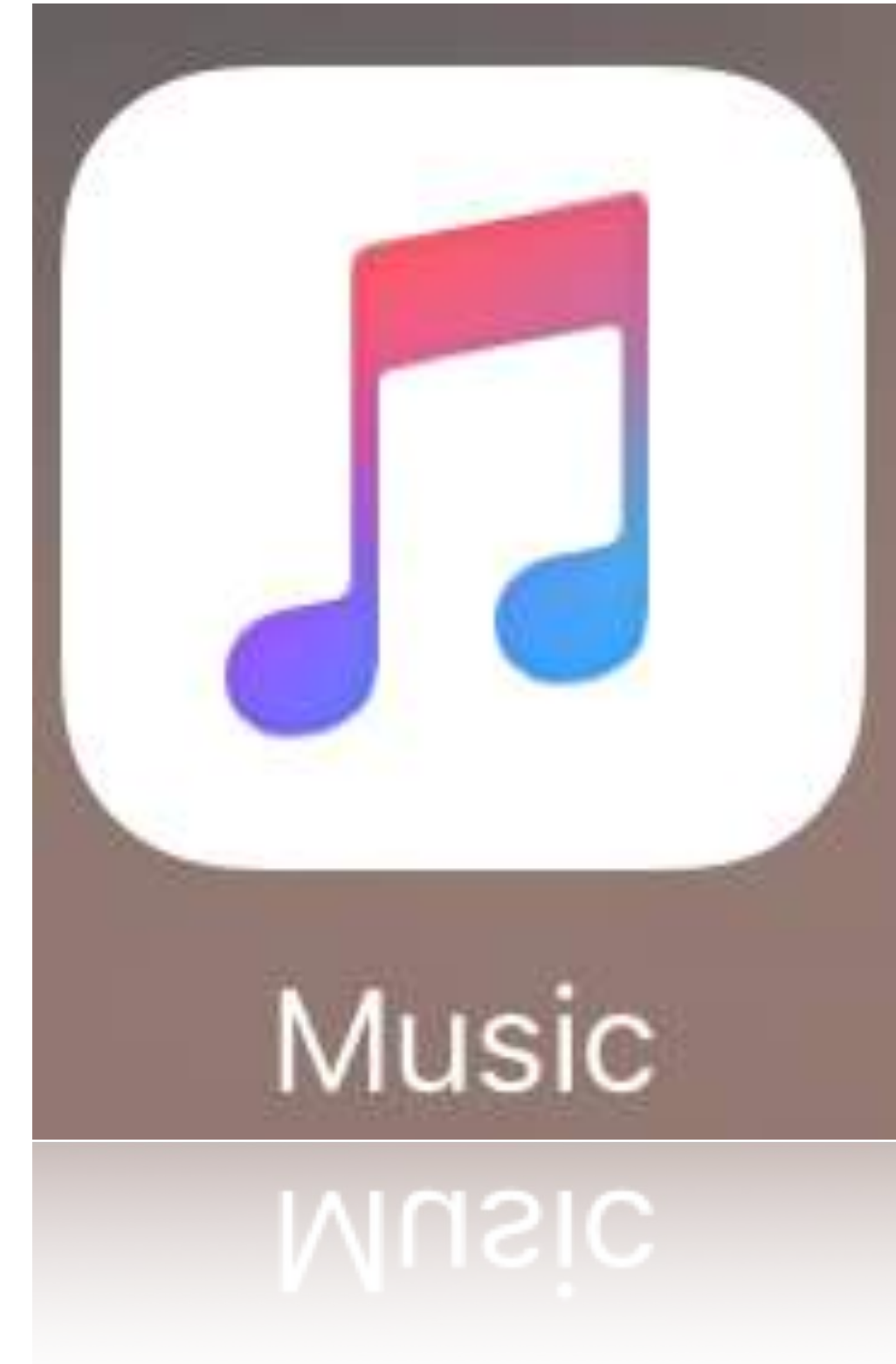
Terms to Know

- Frames Per Second (fps)
- Refresh Rate
- Interlaced Video
- Progressive Video
- Pixel
- Aspect Ratio
- H.264 (MPEG-4 AVC)



Terms to Know

- Frames Per Second (fps)
- Refresh Rate
- Interlaced Video
- Progressive Video
- Pixel
- Aspect Ratio
- H.264 (MPEG-4 AVC)

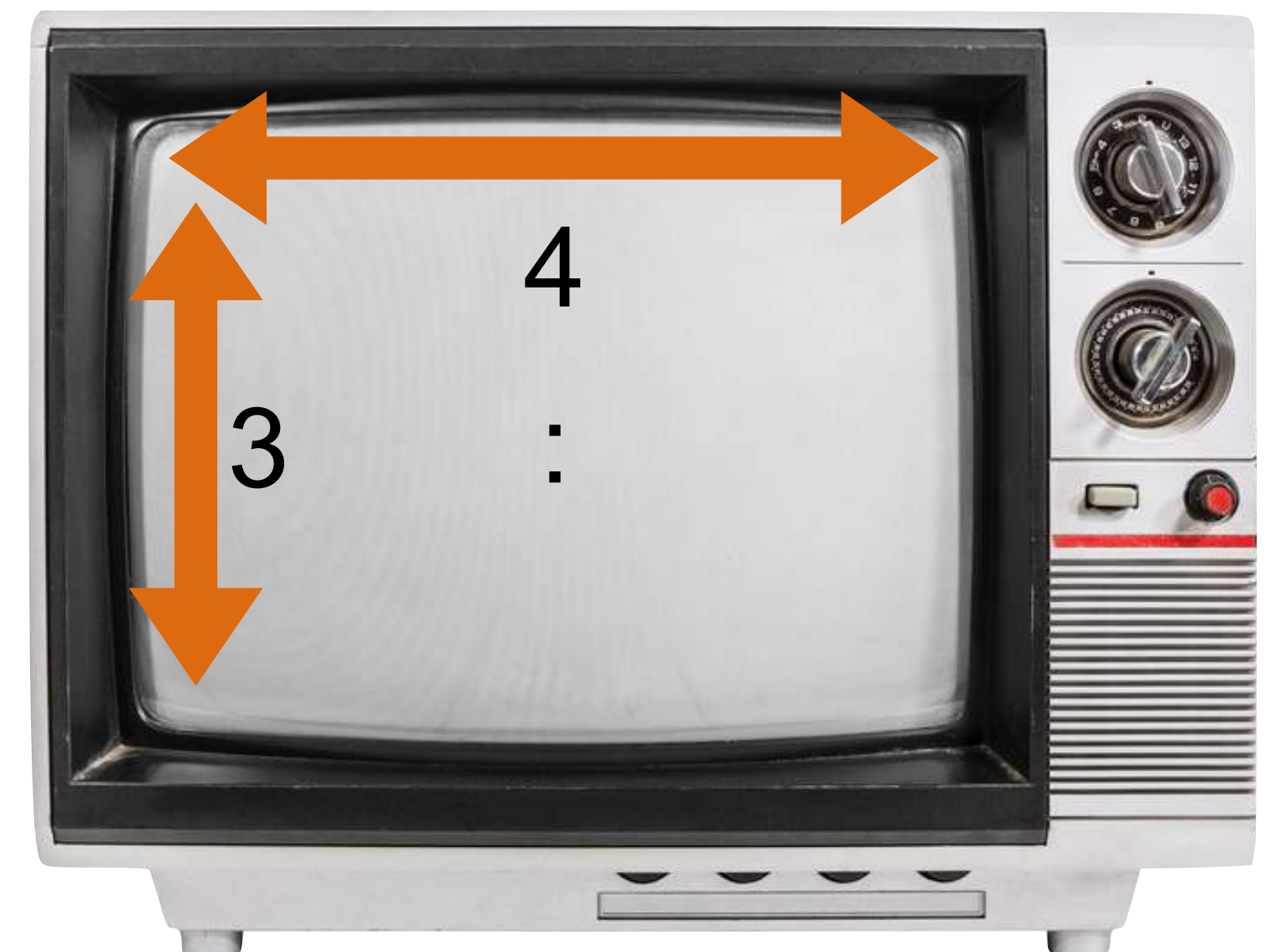
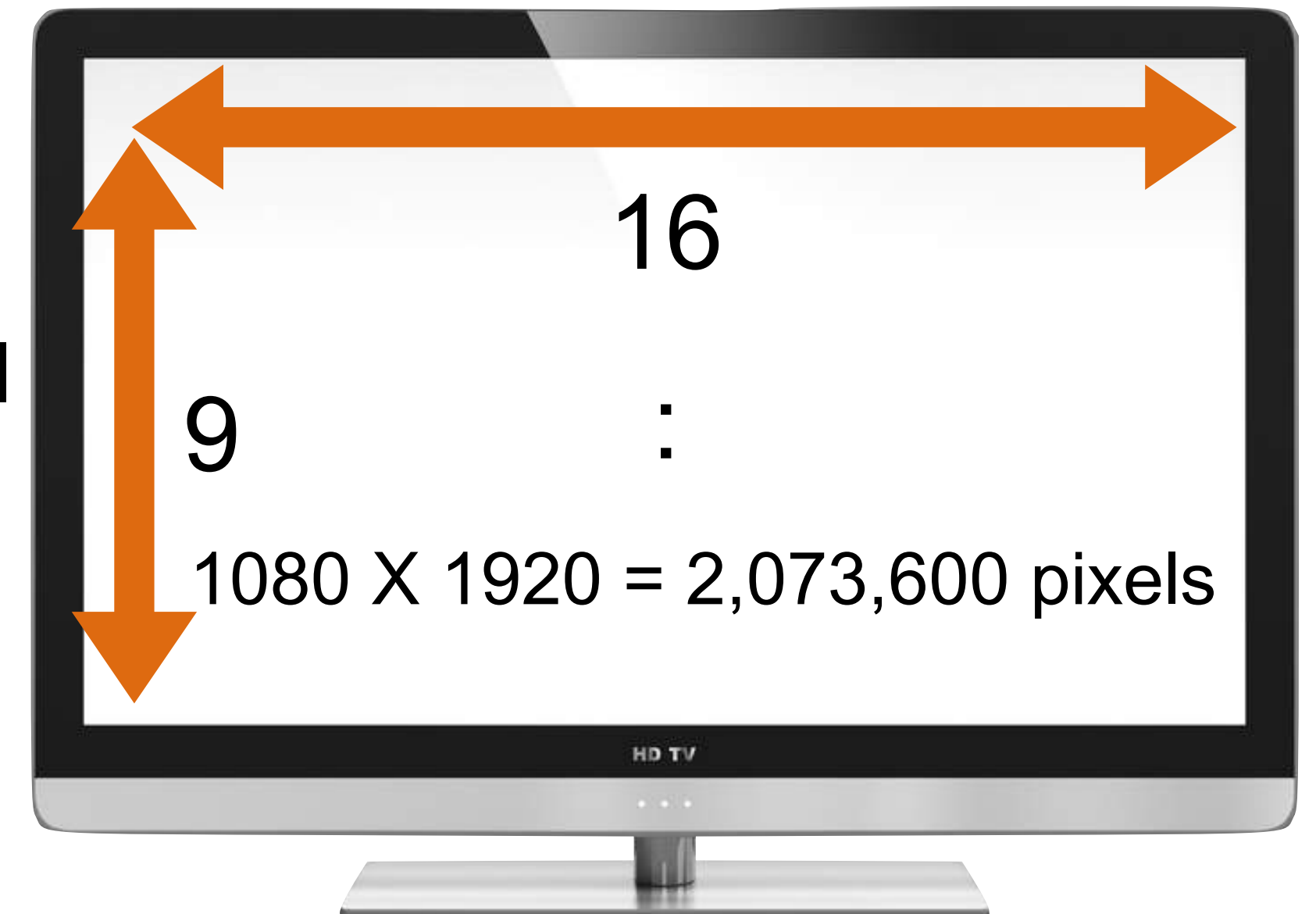


Terms to Know

- Frames Per Second (fps)
- Refresh Rate
- Interlaced Video
- Progressive Video
- Pixel
- Aspect Ratio
- H.264 (MPEG-4 AVC)

1080
Horizontal
Rows

1920 Vertical Columns



Terms to Know

- 
- Frames Per Second (fps)
 - Refresh Rate
 - Interlaced Video
 - Progressive Video
 - Pixel
 - Aspect Ratio
 - H.264 (MPEG-4 AVC)

Approx. 4000 Vertical
Columns



Terms to Know

- Frames Per Second (fps)
- Refresh Rate
- Interlaced Video
- Progressive Video
- Pixel
- Aspect Ratio
- H.264 (MPEG-4 AVC)

STANDARD



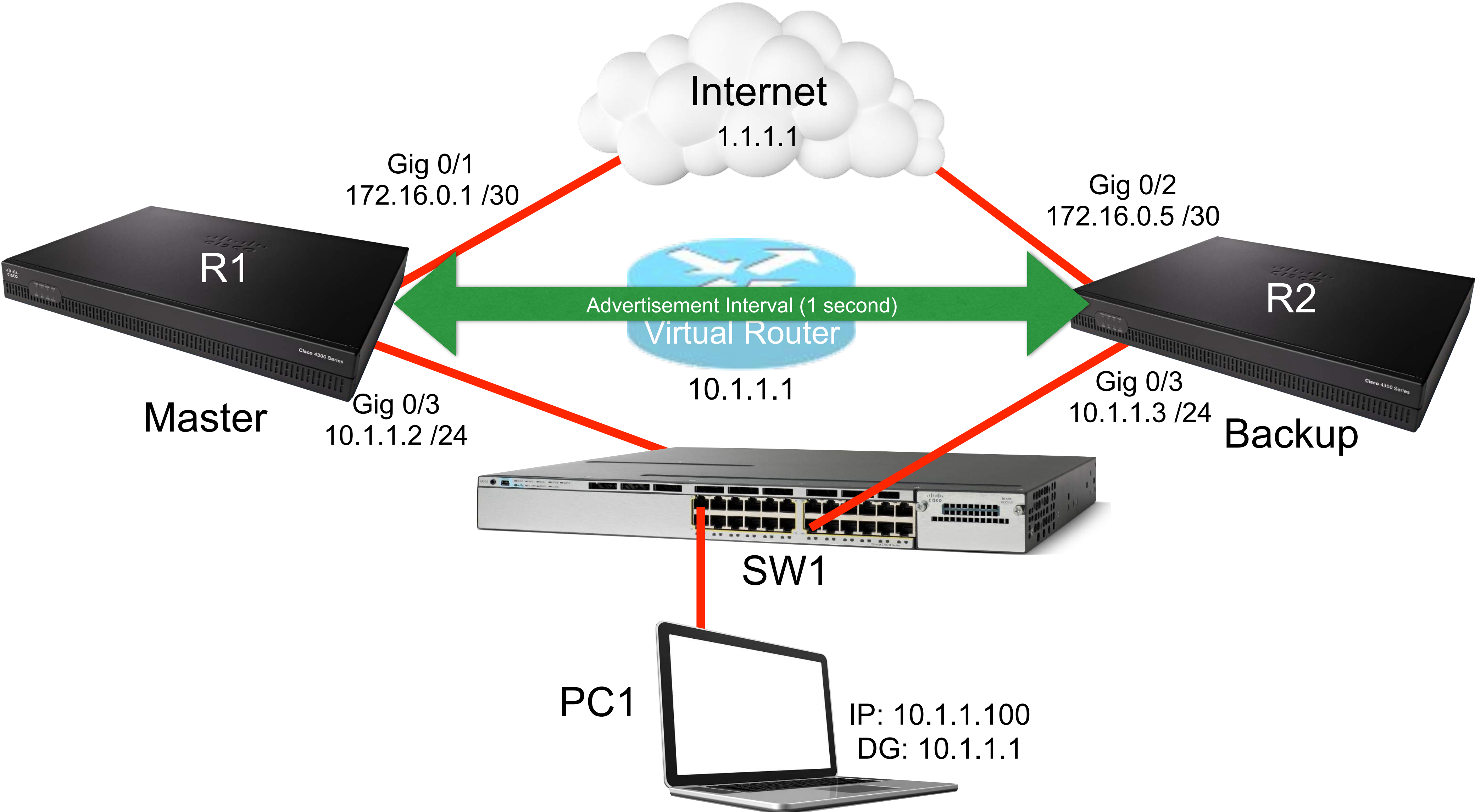
Module 11

Unified Communications

Module 12

Cloud and Virtualization

Virtual IP



Virtual Server

Microsoft
Windows
Server



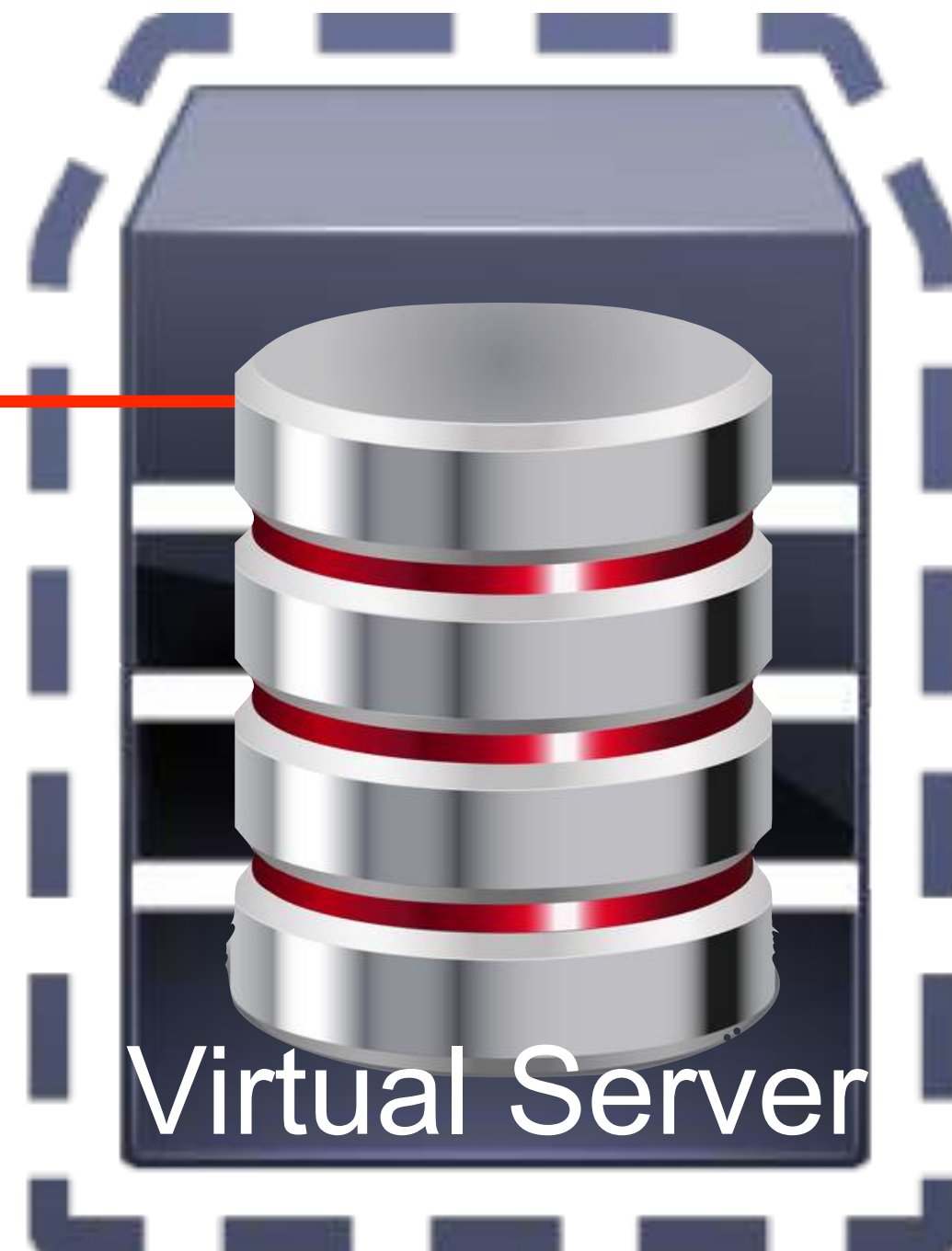
Linux
Server



Oracle
Solaris
Server

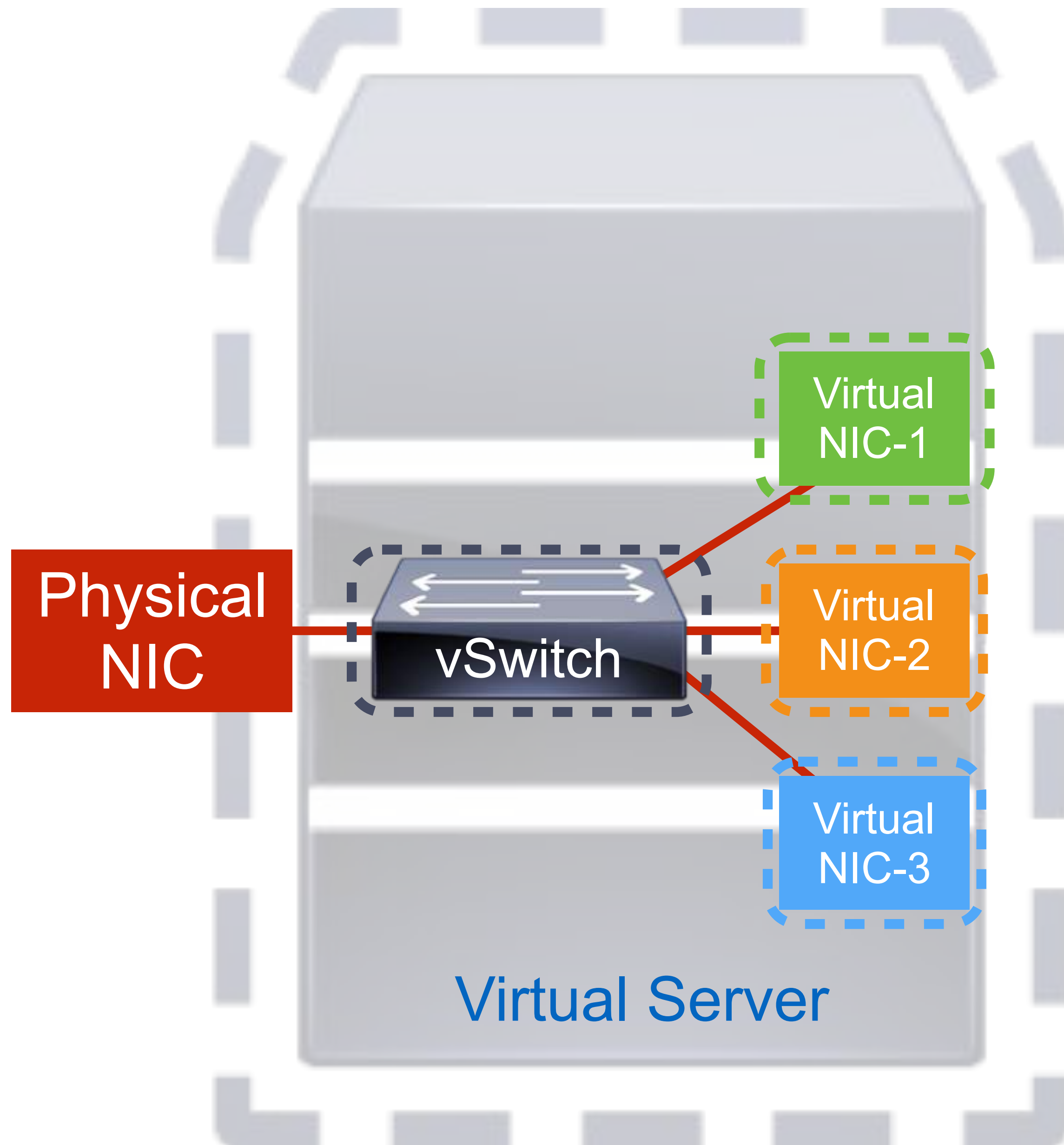


Switch



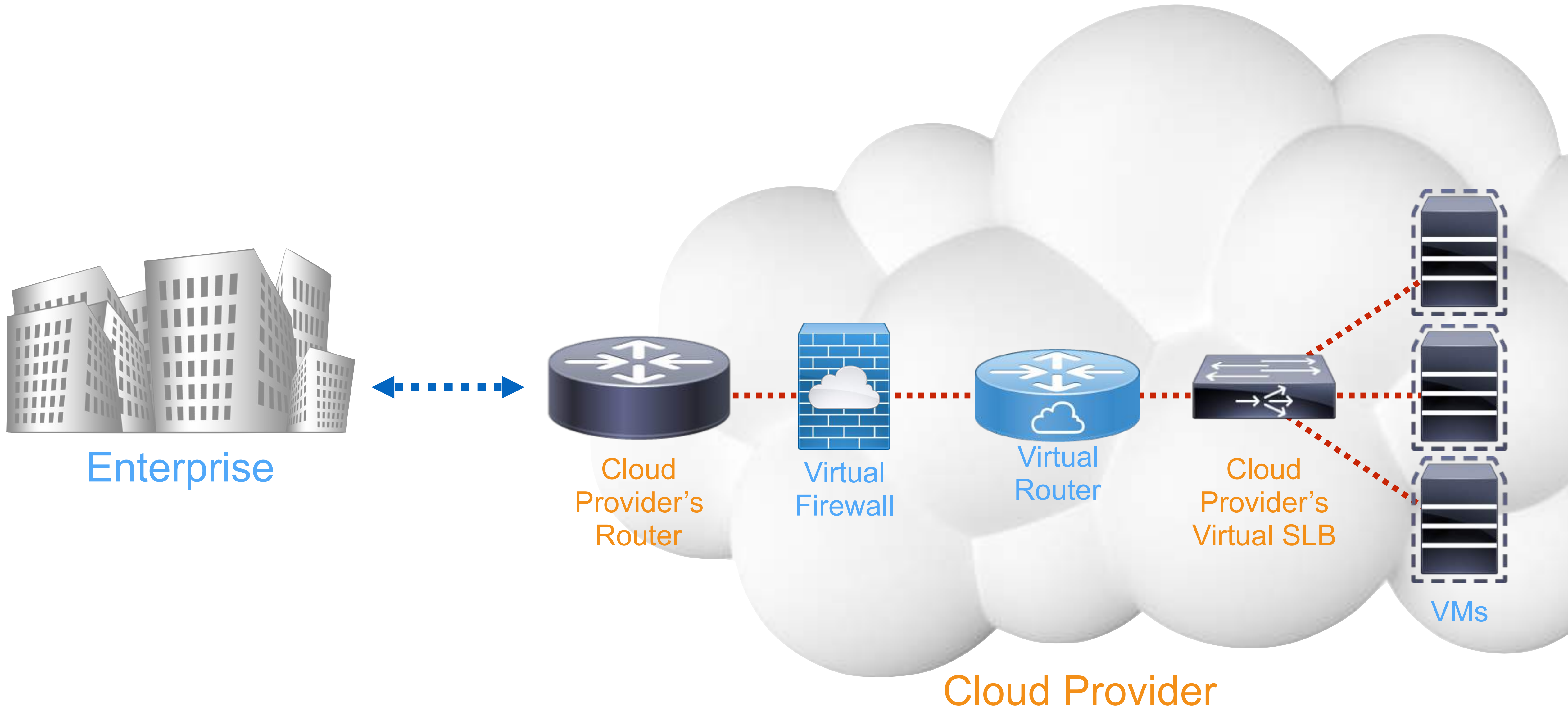
- **Hypervisor:** Software that can create, start, stop, and monitor multiple virtual machines.

Virtualization

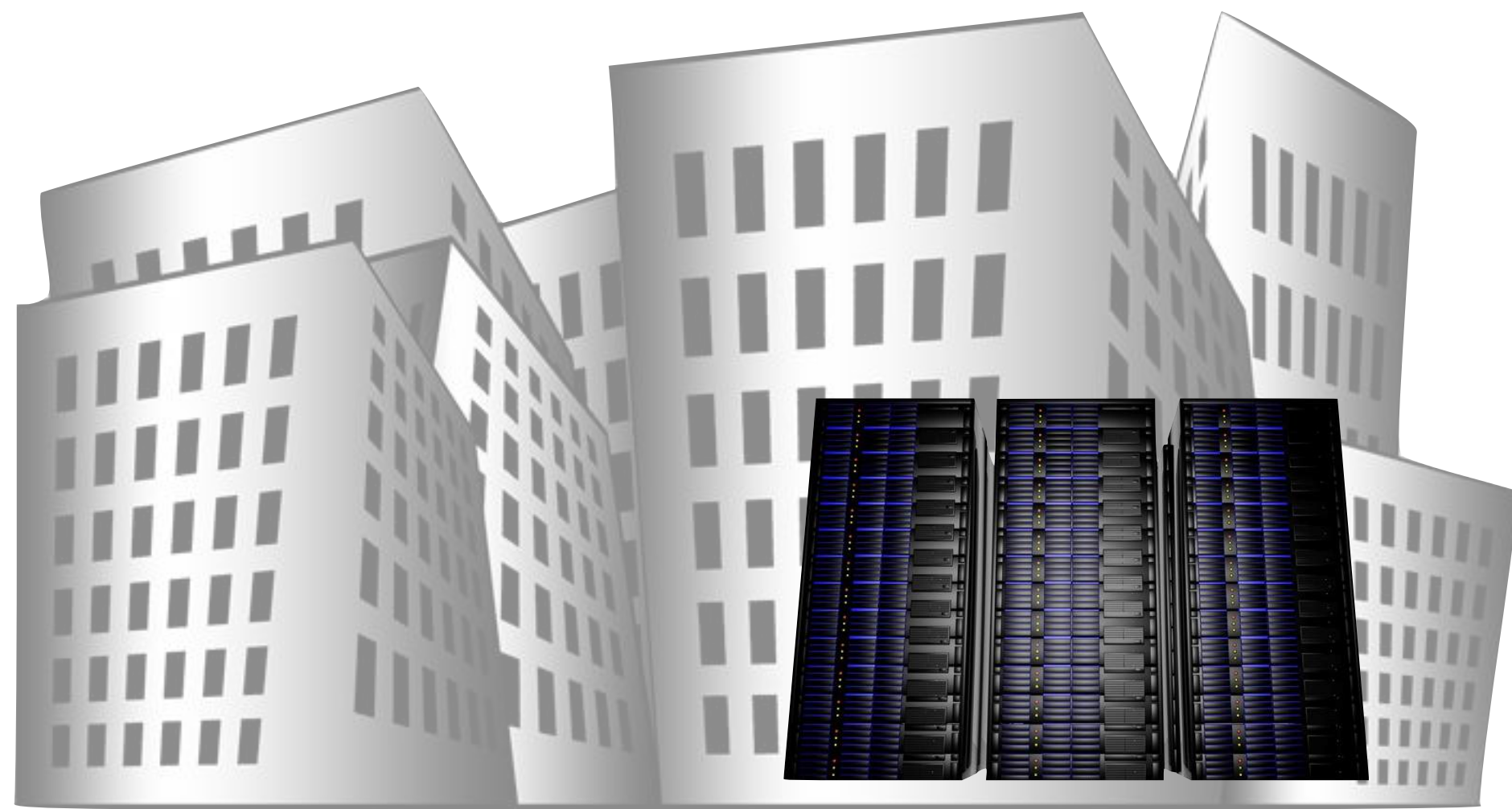


- **Virtual NIC:** Software associated with a unique MAC address, which can be used by a VM to send and receive packets.
- **Virtual Switch:** Software that can connect to other virtual switches, virtual NICs and to a physical NIC.

Virtual Services



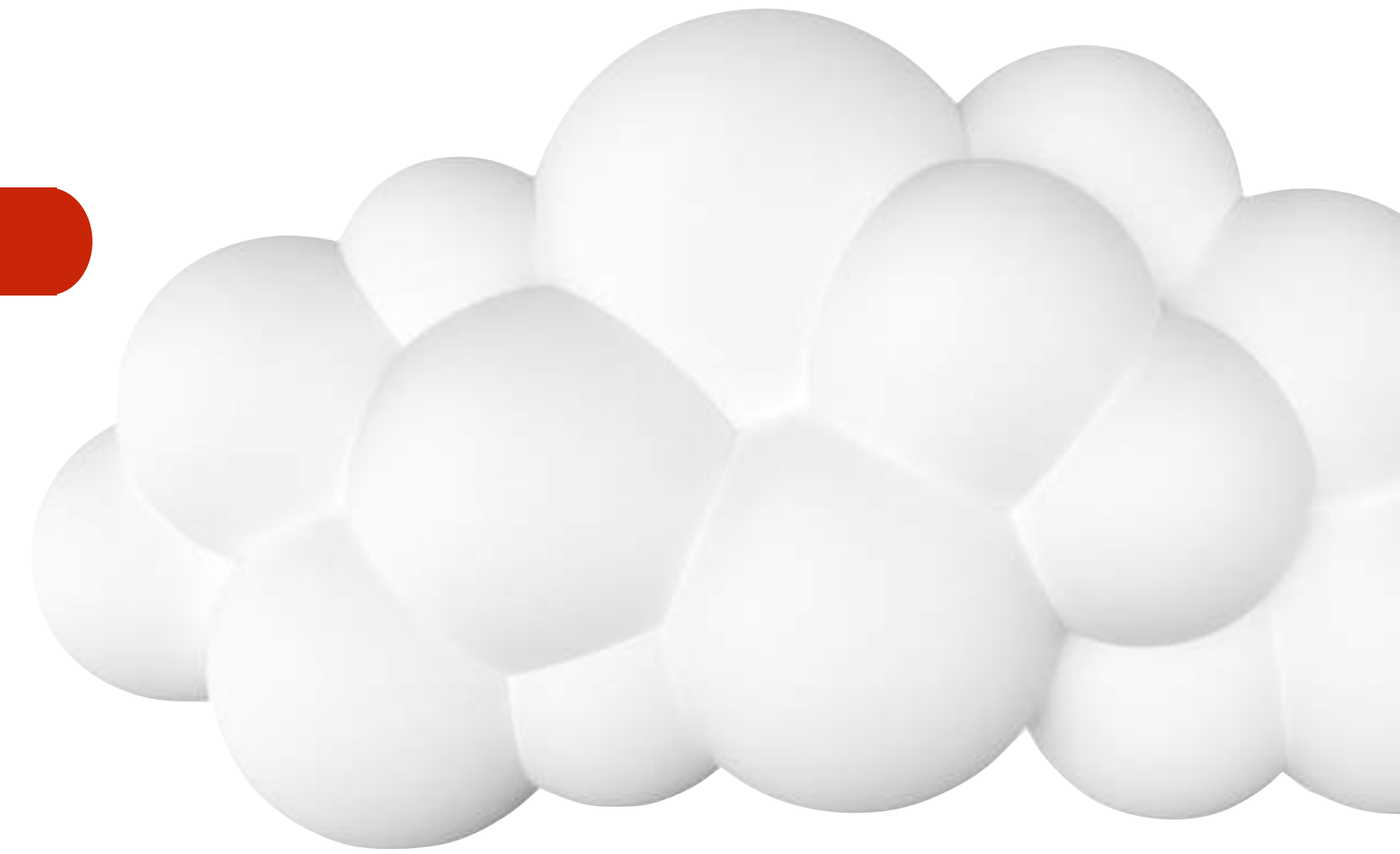
Accessing Cloud Services



Enterprise

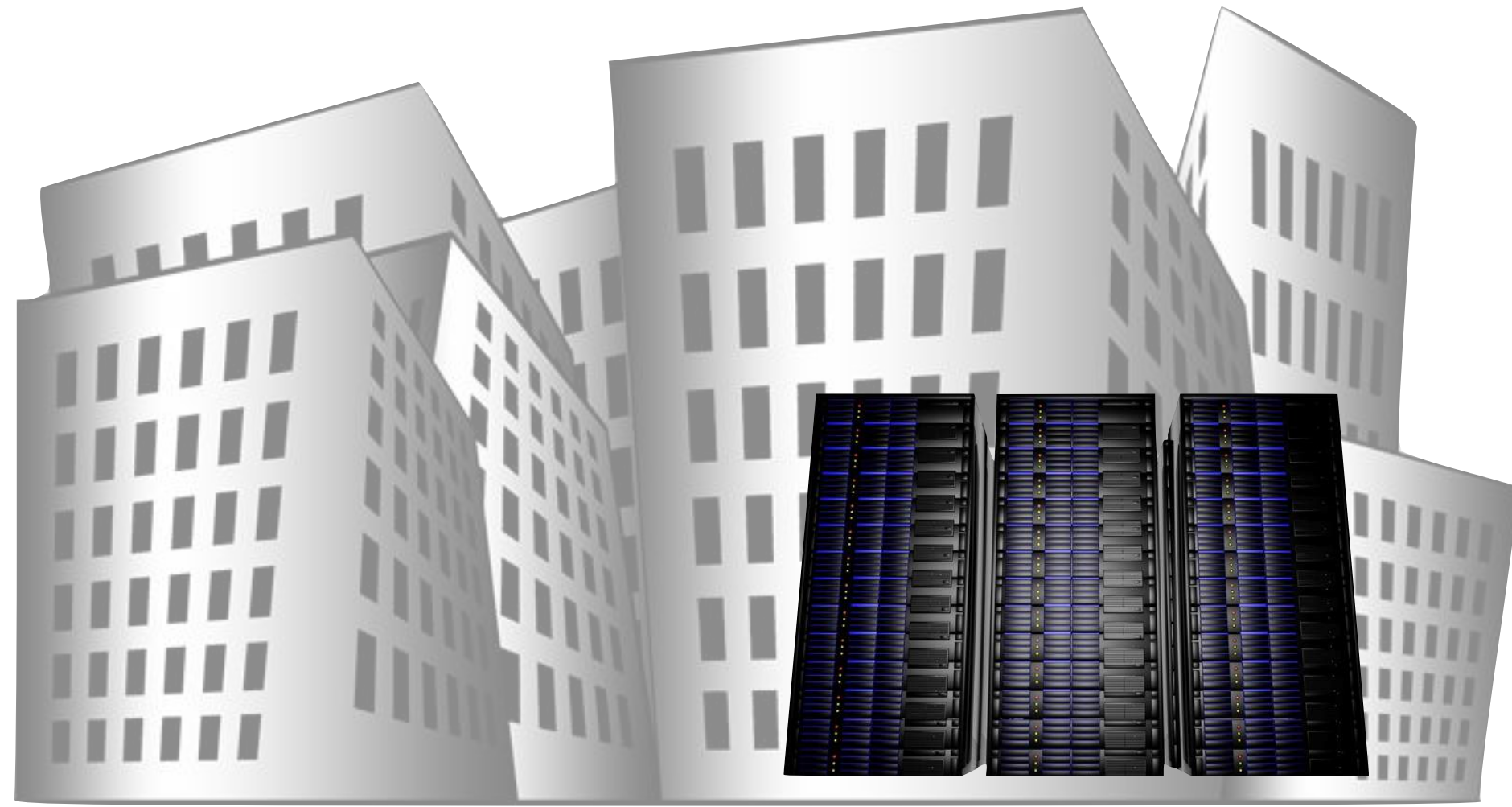


Internet

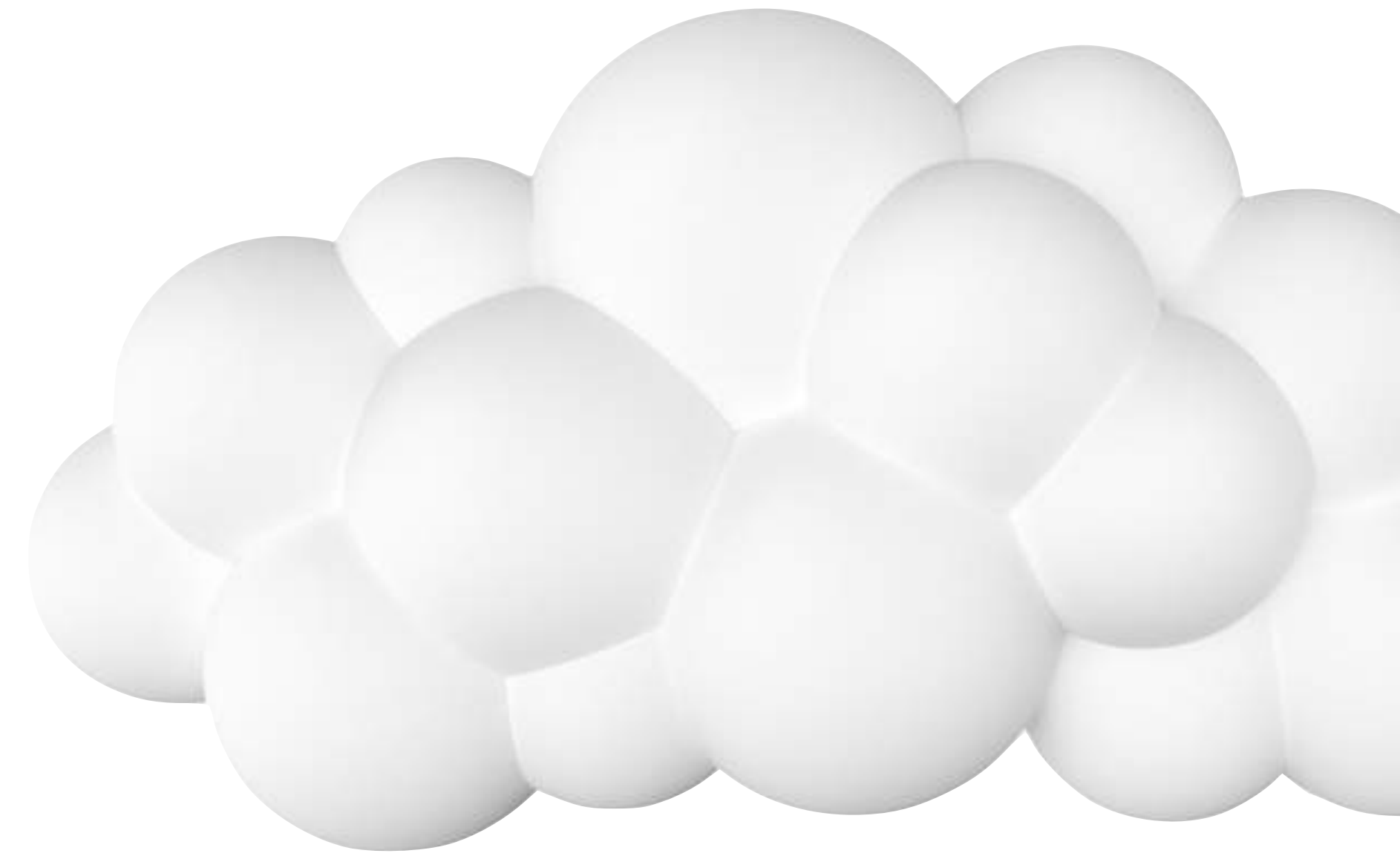


Cloud Provider

Accessing Cloud Services

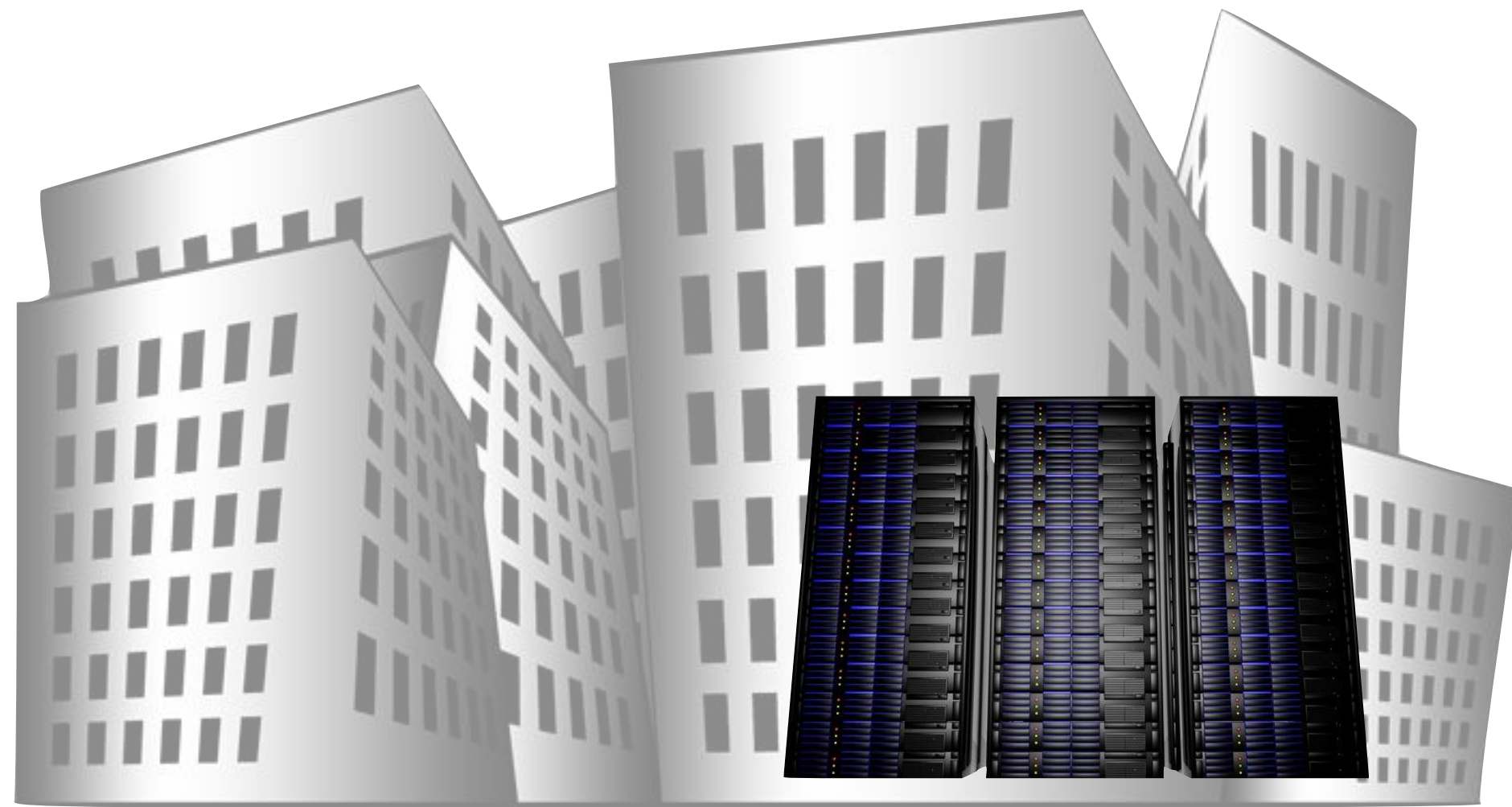


Enterprise

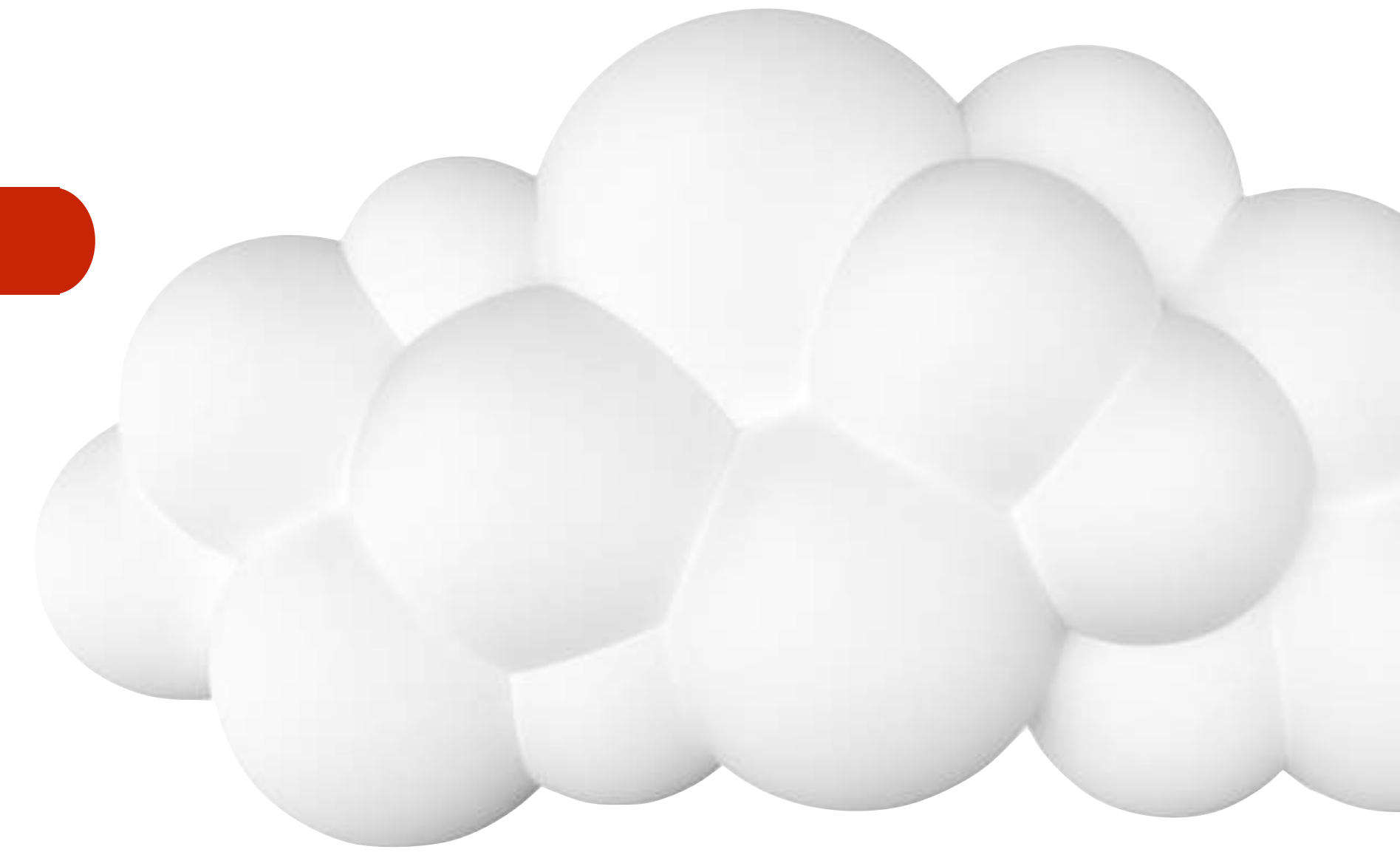


Cloud Provider

Accessing Cloud Services

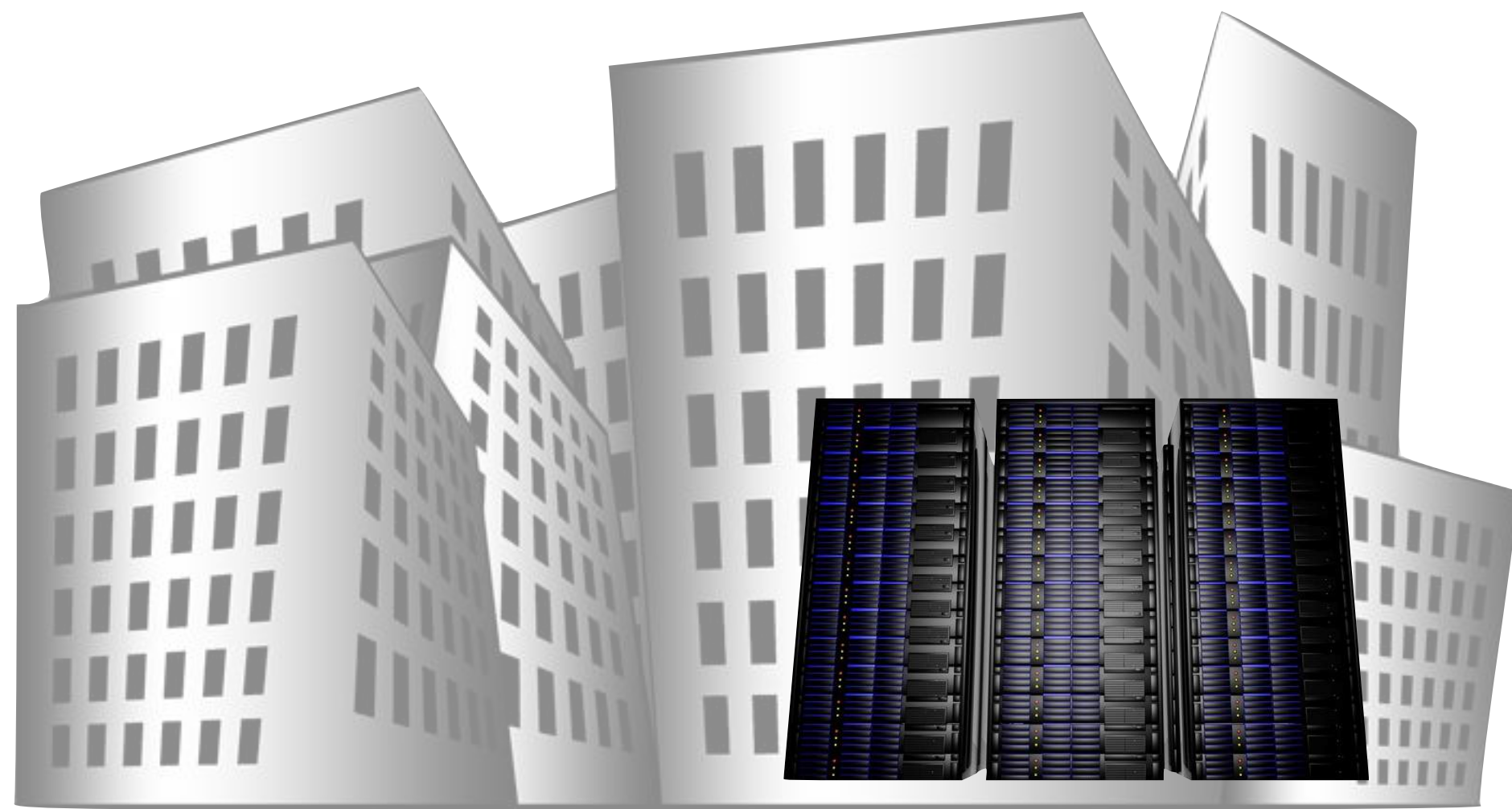


Enterprise



Cloud Provider

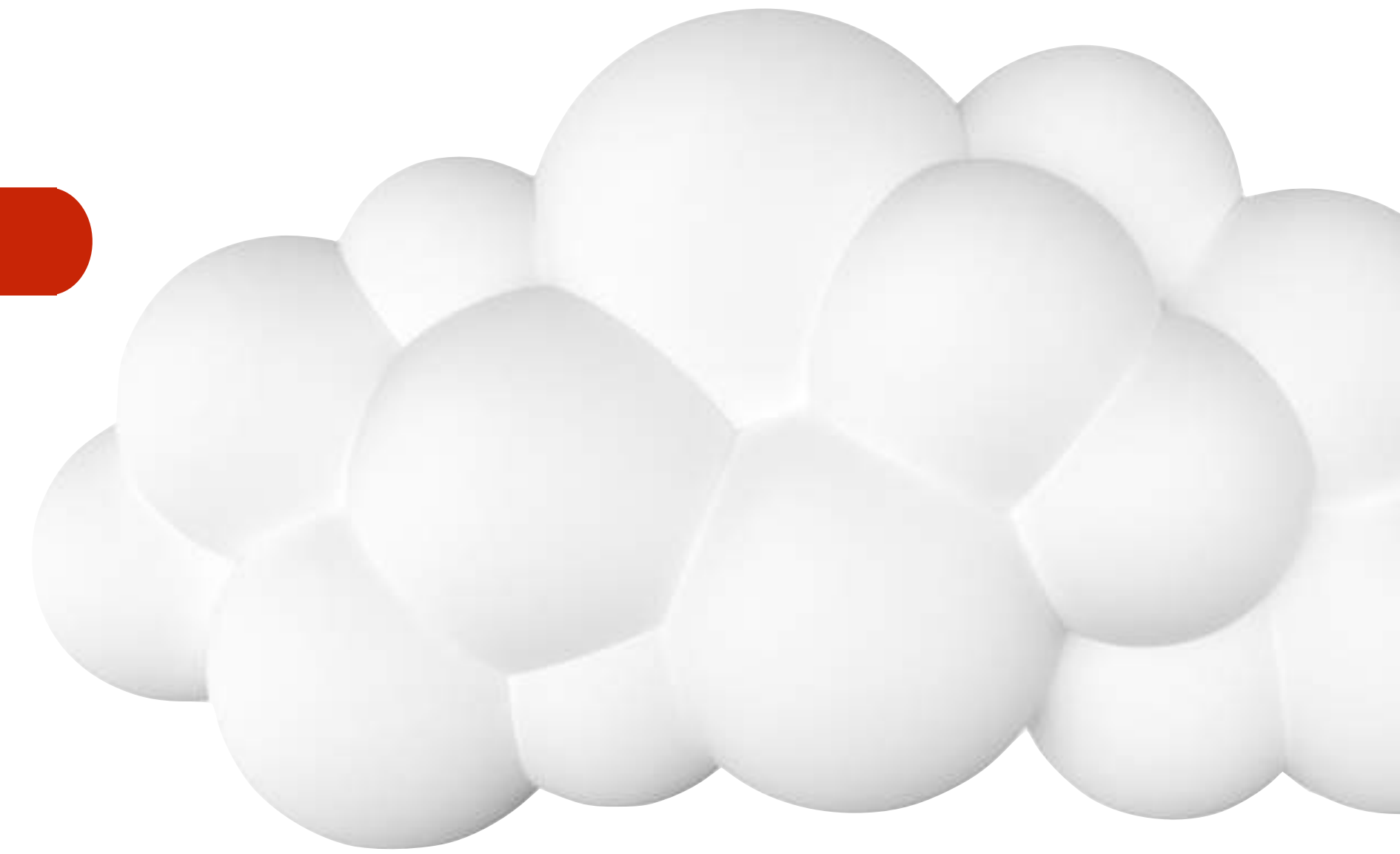
Accessing Cloud Services



Enterprise

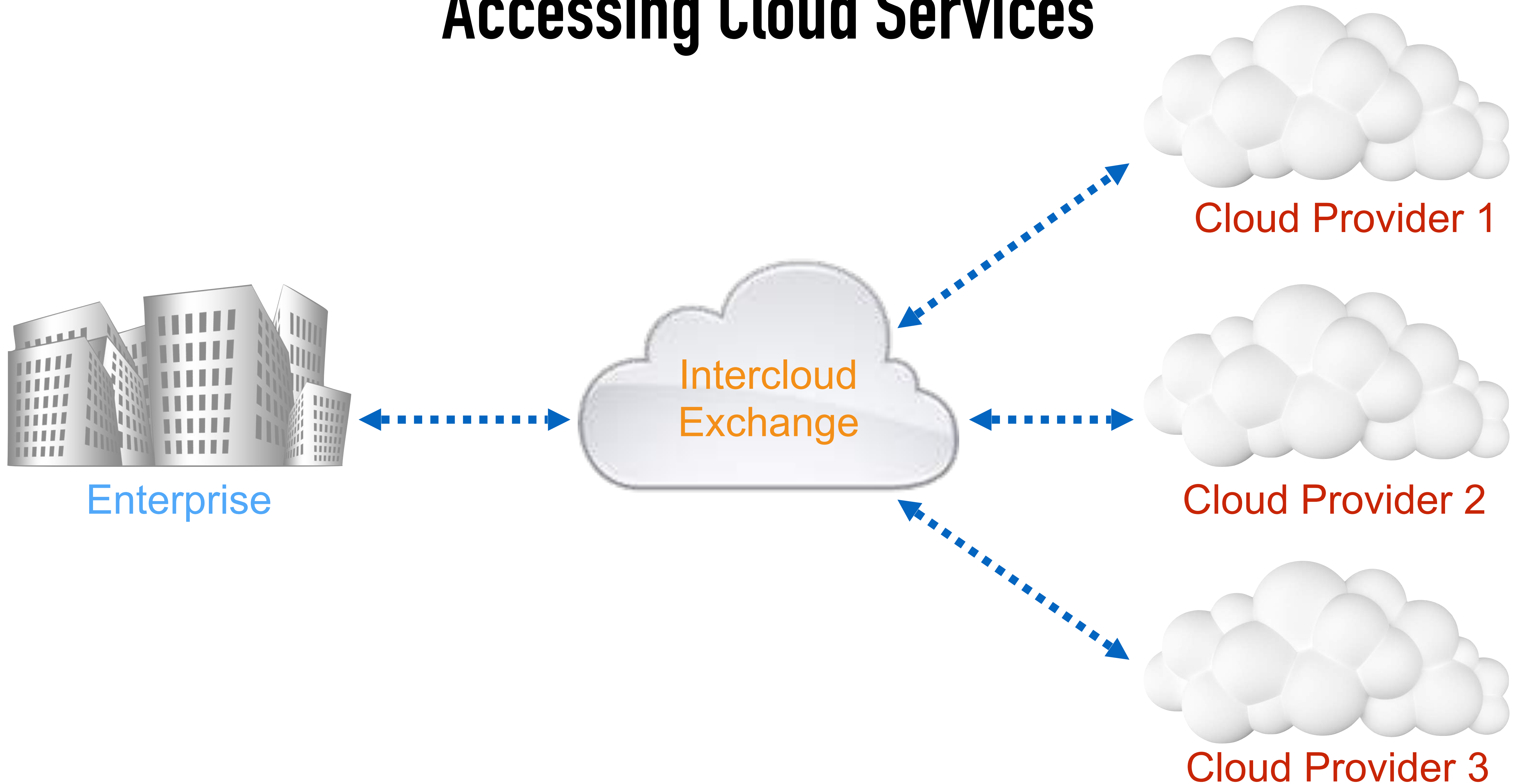
Internet
VPN

Private WAN
MPLS
Metro Ethernet



Cloud Provider

Accessing Cloud Services



Module 12

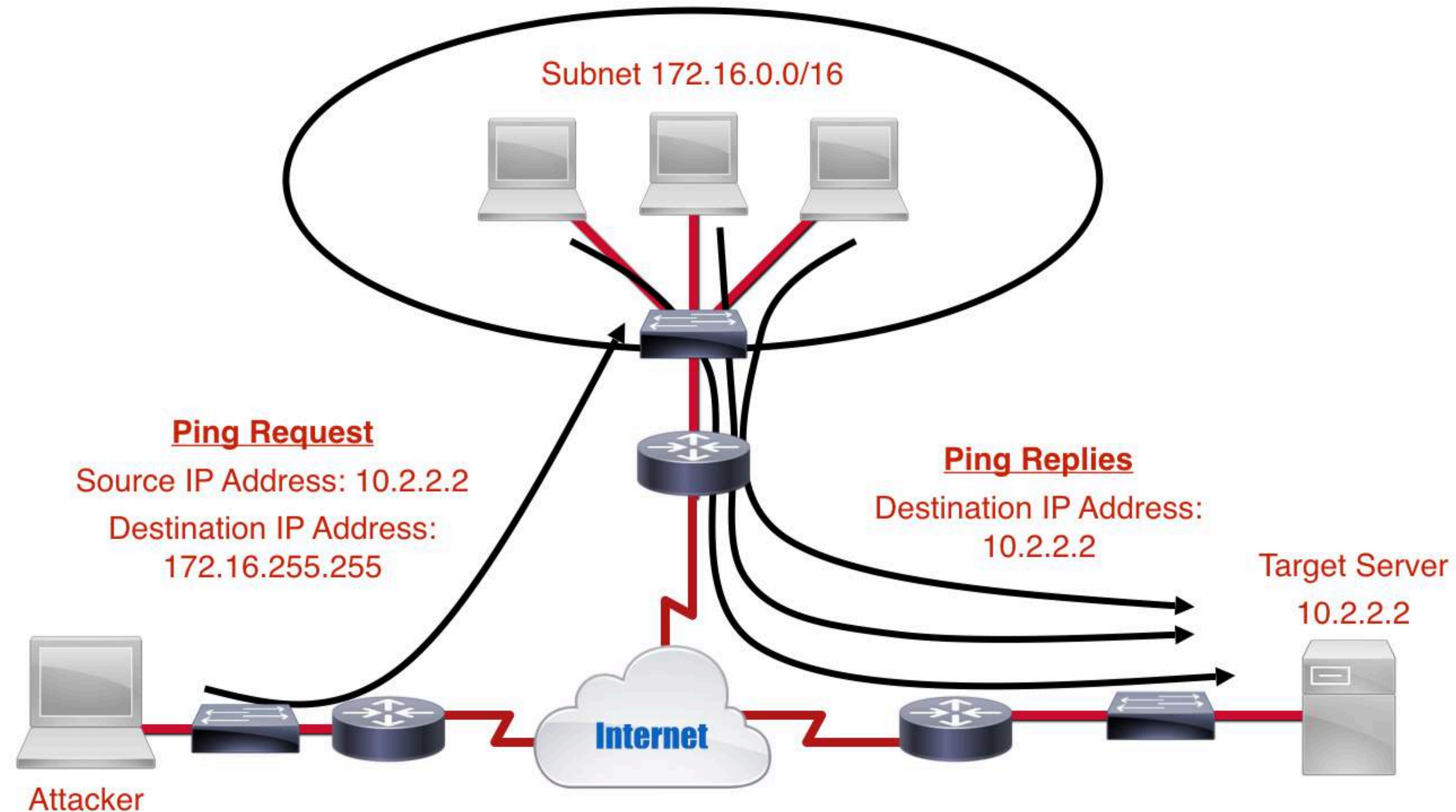
Cloud and Virtualization

Module 13

Network Security

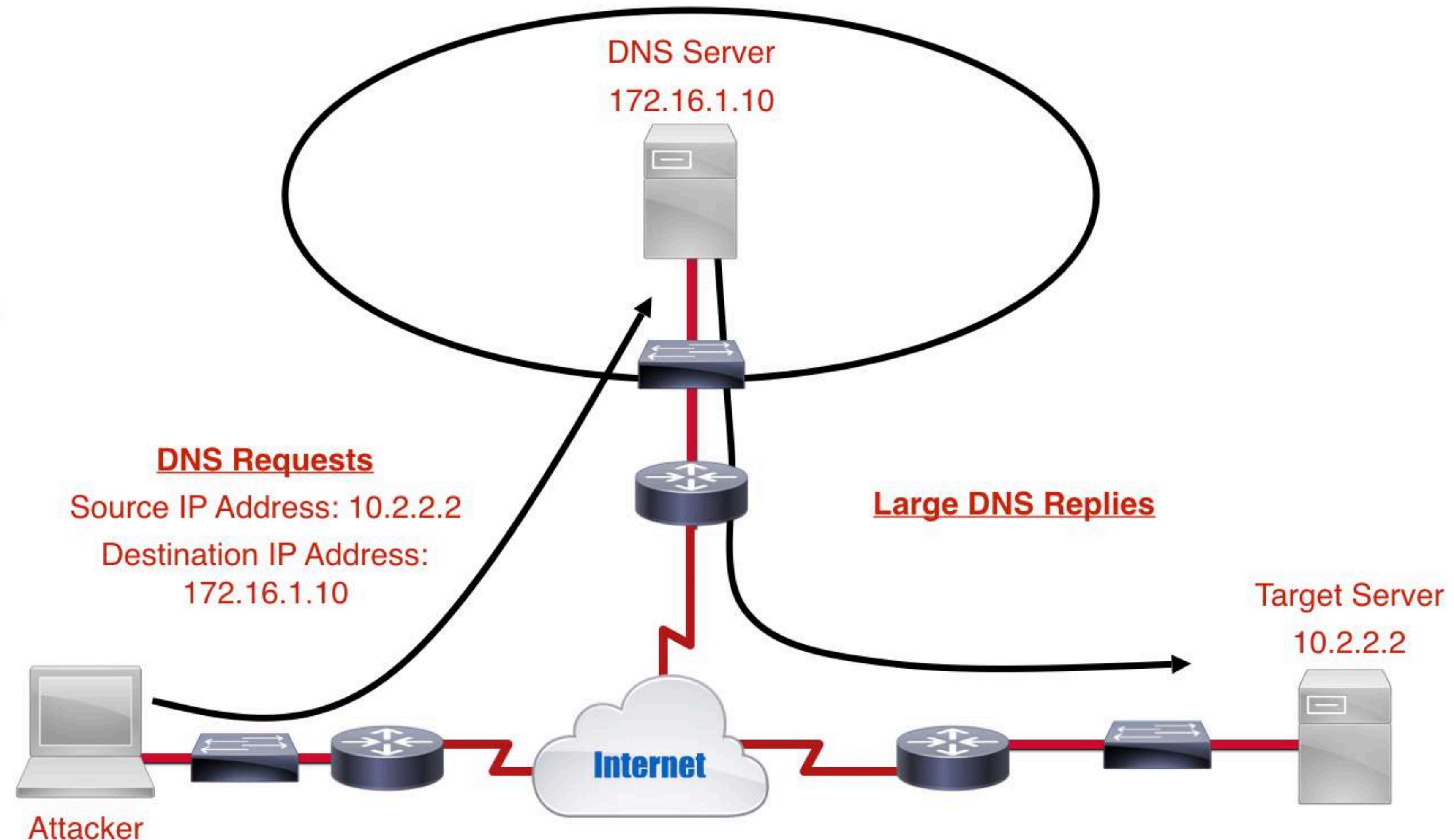
Common Network Attacks

- **Denial of Service (DoS):** An attack where a targeted system is overwhelmed with a large volume of requests, causing it to consume its resources to the point where it can't perform its intended function
 - **Reflective:** Used by an attacker to hide their identity by spoofing their IP address (i.e. the IP address of the intended victim) for a flood of requests sent to third-party devices, causing those devices to respond to the target system



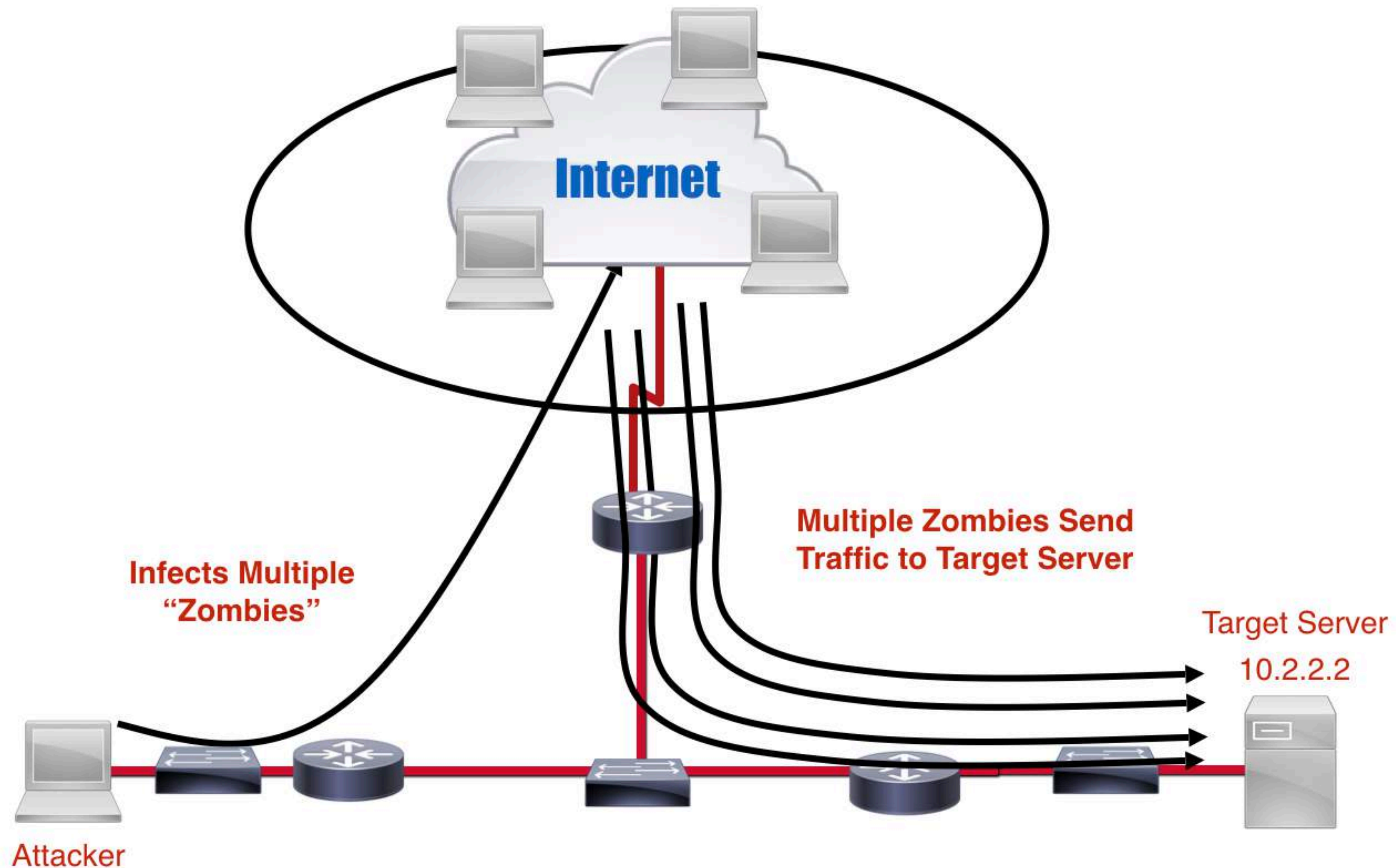
Common Network Attacks

- **Denial of Service (DoS):** An attack where a targeted system is overwhelmed with a large volume of requests, causing it to consume its resources to the point where it can't perform its intended function
 - **Reflective:** Used by an attacker to hide their identity by spoofing their IP address (i.e. the IP address of the intended victim) for a flood of requests sent to third-party devices, causing those devices to respond to the target system
 - **Amplified:** Commonly uses DNS servers to send a large amount of DNS record information to the target system



Common Network Attacks

- **Denial of Service (DoS):** An attack where a targeted system is overwhelmed with a large volume of requests, causing it to consume its resources to the point where it can't perform its intended function
 - **Reflective:** Used by an attacker to hide their identity by spoofing their IP address (i.e. the IP address of the intended victim) for a flood of requests sent to third-party devices, causing those devices to respond to the target system
 - **Amplified:** Commonly uses DNS servers to send a large amount of DNS record information to the target system
 - **Distributed (DDoS):** Traffic overwhelming the target system is sourced from multiple locations



Common Network Attacks (cont.)

- **Social Engineering:** Influencing others to reveal confidential information



Common Network Attacks (cont.)

- **Social Engineering:** Influencing others to reveal confidential information
- **Insider Threat:** A malicious user that is part of (or claims to be part of) an organization



Common Network Attacks (cont.)

- **Social Engineering:** Influencing others to reveal confidential information
- **Insider Threat:** A malicious user that is part of (or claims to be part of) an organization
- **Logic Bomb:** A malicious piece of code that can perform some destructive action based on a time or an event that occurs



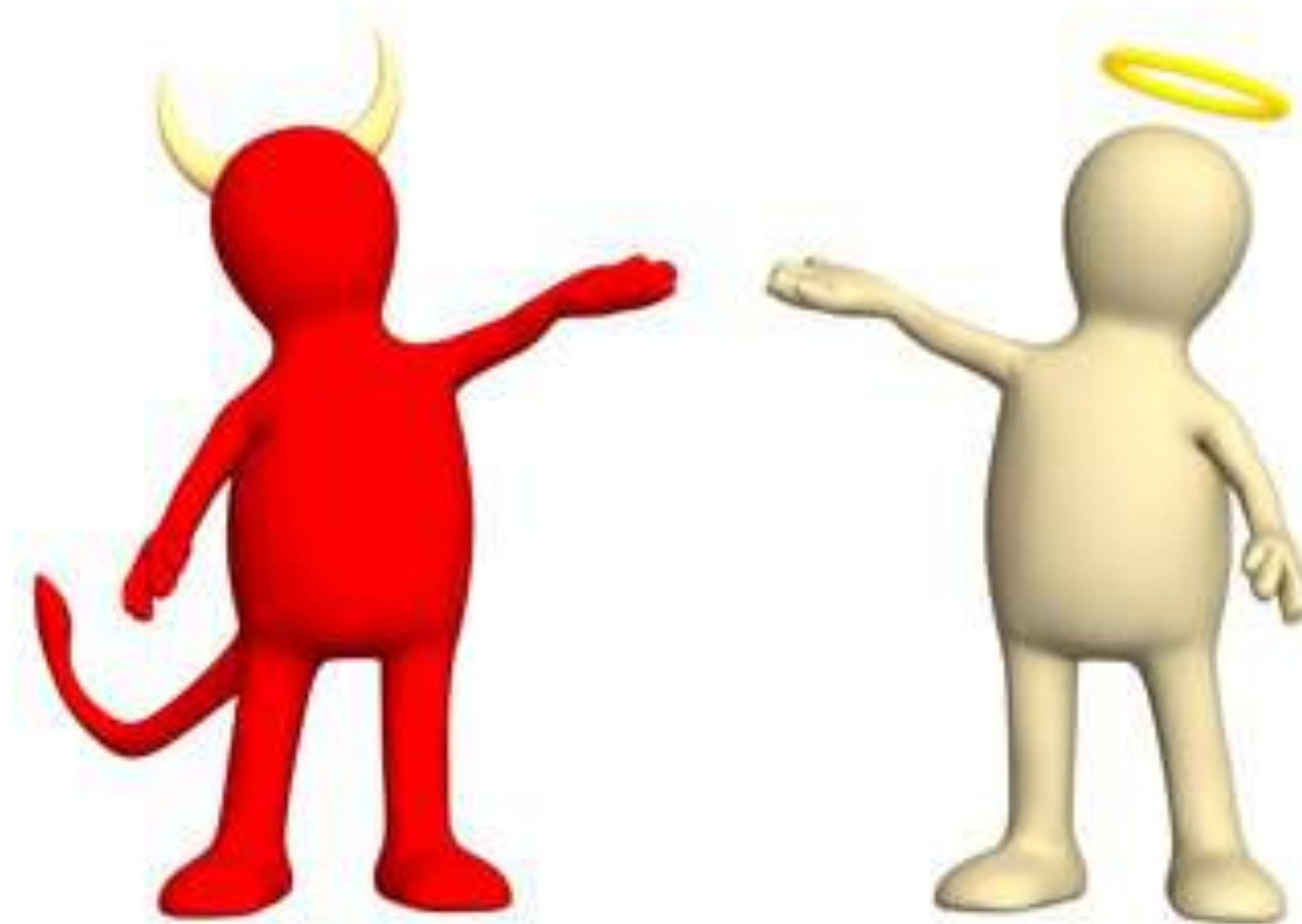
Common Network Attacks (cont.)

- **Social Engineering:** Influencing others to reveal confidential information
- **Insider Threat:** A malicious user that is part of (or claims to be part of) an organization
- **Logic Bomb:** A malicious piece of code that can perform some destructive action based on a time or an event that occurs
- **Rogue Access Point:** A wireless access point installed on a network without proper authorization



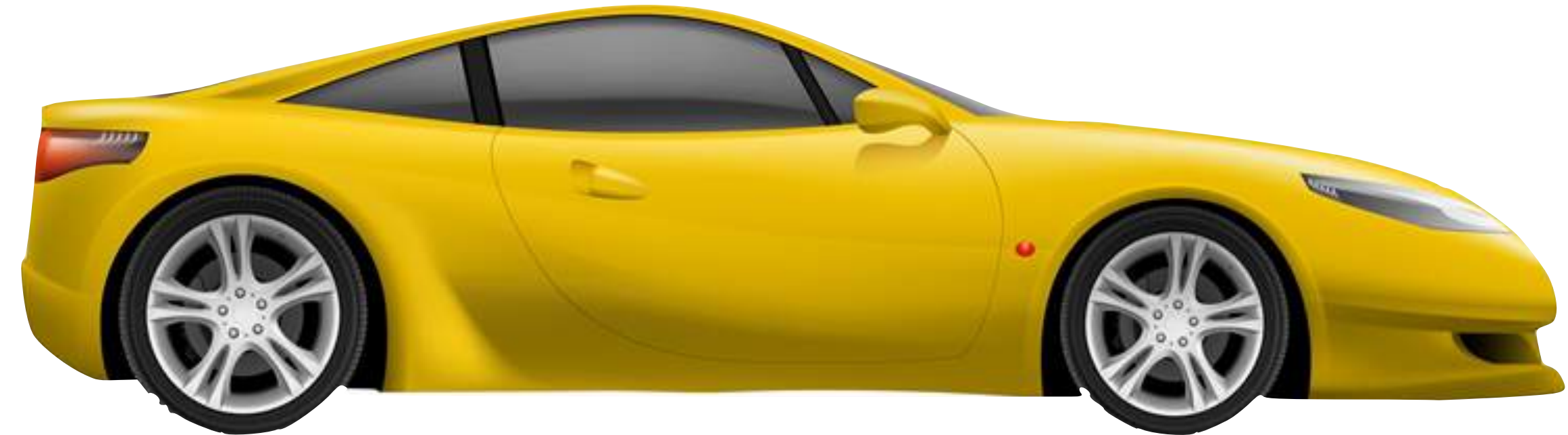
Common Network Attacks (cont.)

- **Social Engineering:** Influencing others to reveal confidential information
- **Insider Threat:** A malicious user that is part of (or claims to be part of) an organization
- **Logic Bomb:** A malicious piece of code that can perform some destructive action based on a time or an event that occurs
- **Rogue Access Point:** A wireless access point installed on a network without proper authorization
- **Evil Twin:** A rogue access point appearing to be a legitimate wireless access point (e.g. has a matching SSID)



Common Network Attacks (cont.)

- **Social Engineering:** Influencing others to reveal confidential information
- **Insider Threat:** A malicious user that is part of (or claims to be part of) an organization
- **Logic Bomb:** A malicious piece of code that can perform some destructive action based on a time or an event that occurs
- **Rogue Access Point:** A wireless access point installed on a network without proper authorization
- **Evil Twin:** A rogue access point appearing to be a legitimate wireless access point (e.g. has a matching SSID)
- **War Driving:** Driving around a geographical area in an attempt to find Wi-Fi hotspots that can be accessed



Common Network Attacks (cont.)

- **Phishing:** When malicious users leverage e-mail, webpages, etc. that appear legitimate, in an attempt to obtain confidential information



Common Network Attacks (cont.)



- **Phishing:** When malicious users leverage e-mail, webpages, etc. that appear legitimate, in an attempt to obtain confidential information
- **Ransomware:** Malware that prevent users from accessing their data unless they pay a ransom

Common Network Attacks (cont.)



- **Phishing:** When malicious users leverage e-mail, webpages, etc. that appear legitimate, in an attempt to obtain confidential information
- **Ransomware:** Malware that prevent users from accessing their data unless they pay a ransom
- **DNS Poisoning:** When an attacker advertises incorrect domain name resolution information into a DNS server, causing DNS requests to resolve to the attacker's computer

Common Network Attacks (cont.)

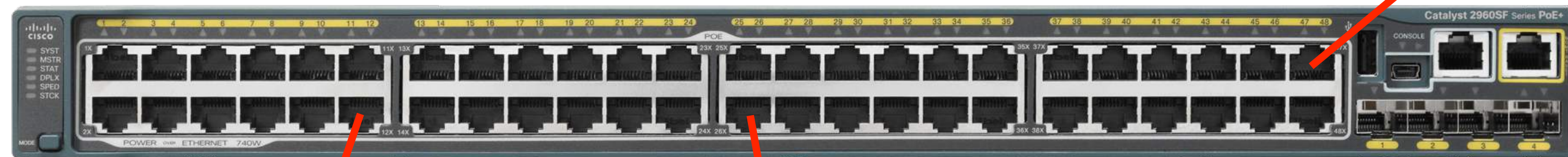


- **Phishing:** When malicious users leverage e-mail, webpages, etc. that appear legitimate, in an attempt to obtain confidential information
- **Ransomware:** Malware that prevent users from accessing their data unless they pay a ransom
- **DNS Poisoning:** When an attacker advertises incorrect domain name resolution information into a DNS server, causing DNS requests to resolve to the attacker's computer
- **ARP Poisoning:** Used in a man-in-the-middle attack, where an attacker sends gratuitous ARP replies to a client system, often convincing the client system to send frames destined for its default gateway to the attacker's computer

Common Network Attacks (cont.)

Man-in-the-Middle: An attack where a malicious user somehow injects themselves inside a communication flow between two systems, enabling them to intercept that flow's traffic

IP Address: 10.1.1.1
MAC Address: AAAA.AAAA.AAAA



Dest. IP: 10.1.1.1
Dest. MAC: AAAA.AAAA.AAAA

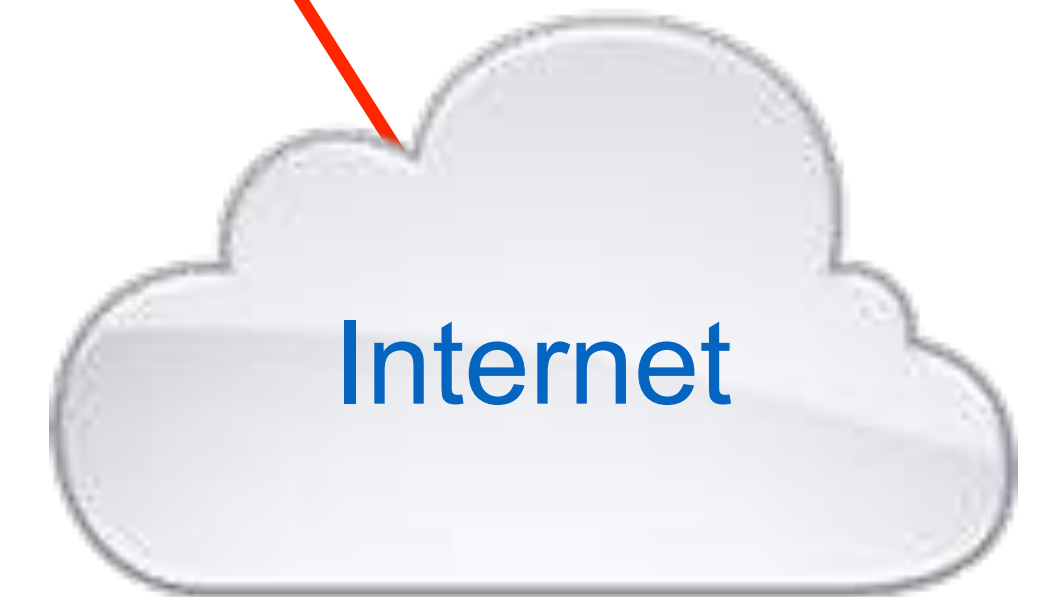
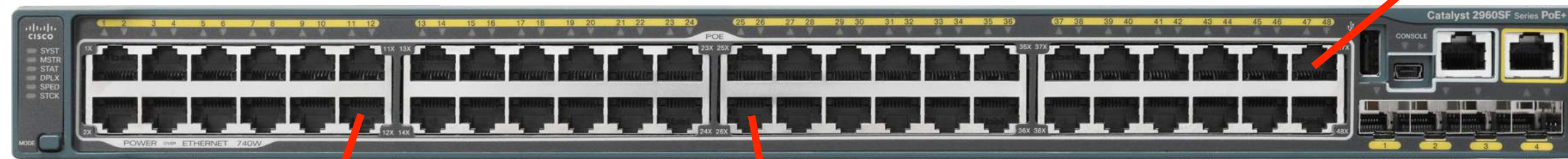


"Man in the Middle"

Common Network Attacks (cont.)

Man-in-the-Middle: An attack where a malicious user somehow injects themselves inside a communication flow between two systems, enabling them to intercept that flow's traffic

IP Address: 10.1.1.1
MAC Address: AAAA.AAAA.AAAA



Gratuitous ARP



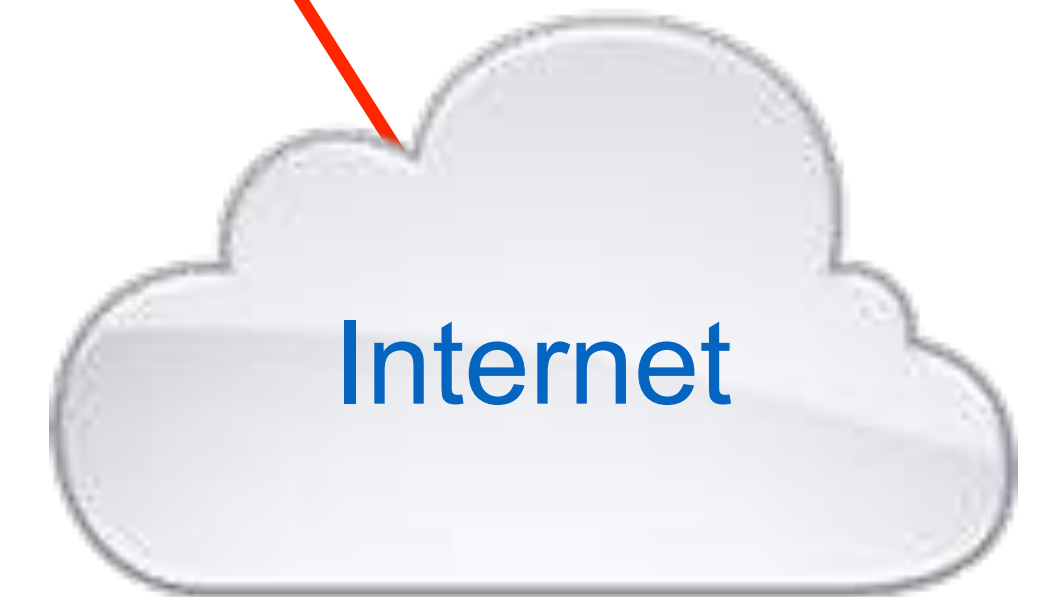
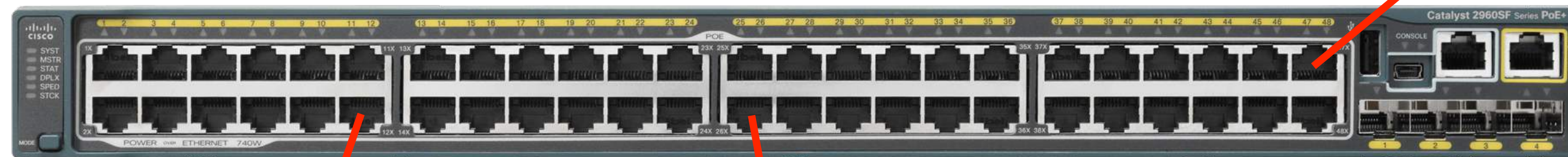
IP Address: 10.1.1.22
MAC Address: BBBB.BBBB.BBBB

"Man in the Middle"

Common Network Attacks (cont.)

Man-in-the-Middle: An attack where a malicious user somehow injects themselves inside a communication flow between two systems, enabling them to intercept that flow's traffic

IP Address: 10.1.1.1
MAC Address: AAAA.AAAA.AAAA



Dest. IP: 10.1.1.1
Dest. MAC: BBBB.BBBB.BBBB



IP Address: 10.1.1.22
MAC Address: BBBB.BBBB.BBBB

"Man in the Middle"

Mitigating Network Threats



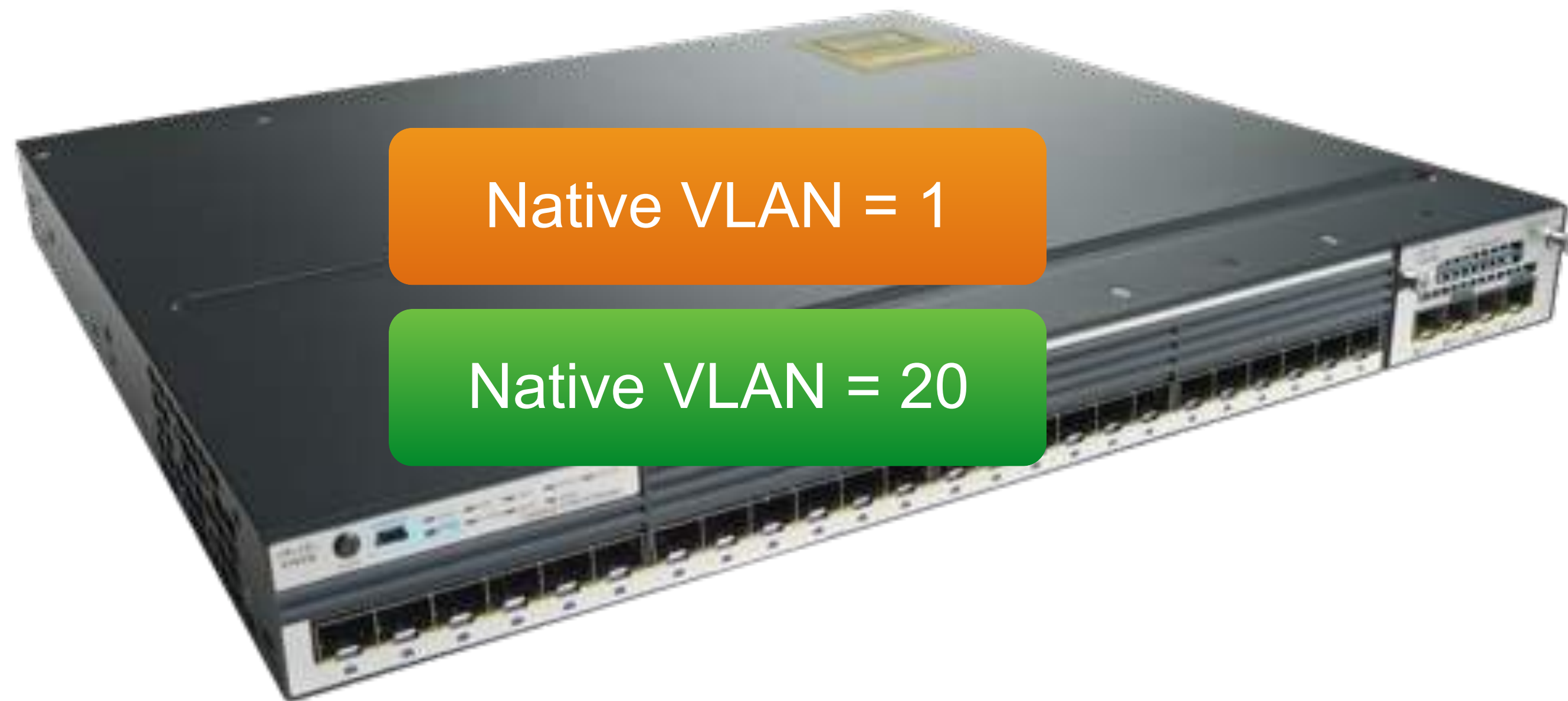
- **Signature Management:** Keep attack signatures current on devices, such as IDS and IPS sensors

Mitigating Network Threats



- **Signature Management:** Keep attack signatures current on devices, such as IDS and IPS sensors
- **Device Hardening:** Apply a collection of best practice procedures to secure network devices (e.g. disabling unnecessary services on a device)

Mitigating Network Threats



- **Signature Management:** Keep attack signatures current on devices, such as IDS and IPS sensors
- **Device Hardening:** Apply a collection of best practice procedures to secure network devices (e.g. disabling unnecessary services on a device)
- **Change the Native VLAN:** Configure a trunk's untagged VLAN to a non-default value, to prevent unconfigured switch ports from automatically belonging to the native VLAN

Mitigating Network Threats



- **Signature Management:** Keep attack signatures current on devices, such as IDS and IPS sensors
- **Device Hardening:** Apply a collection of best practice procedures to secure network devices (e.g. disabling unnecessary services on a device)
- **Change the Native VLAN:** Configure a trunk's untagged VLAN to a non-default value, to prevent unconfigured switch ports from automatically belonging to the native VLAN
- **Define Privileged User Accounts:** Define accounts for administrative users, and add administrative privileges to those accounts, rather than sharing a single "admin" account

Mitigating Network Threats (cont.)

- **File Integrity Monitoring:** Use a service that can detect any change made to defined files (e.g. critical system files or financial records)



Mitigating Network Threats (cont.)

- **File Integrity Monitoring:** Use a service that can detect any change made to defined files (e.g. critical system files or financial records)
- **Role Separation:** Assign different sets of permissions to different categories of users, in an attempt to prevent conflicts of interest



Mitigating Network Threats (cont.)

- **File Integrity Monitoring:** Use a service that can detect any change made to defined files (e.g. critical system files or financial records)
- **Role Separation:** Assign different sets of permissions to different categories of users, in an attempt to prevent conflicts of interest
- **Honeypot (or HoneyNet) Deployment:** Configure a host (or a network) that does not contain sensitive information, and don't properly secure it

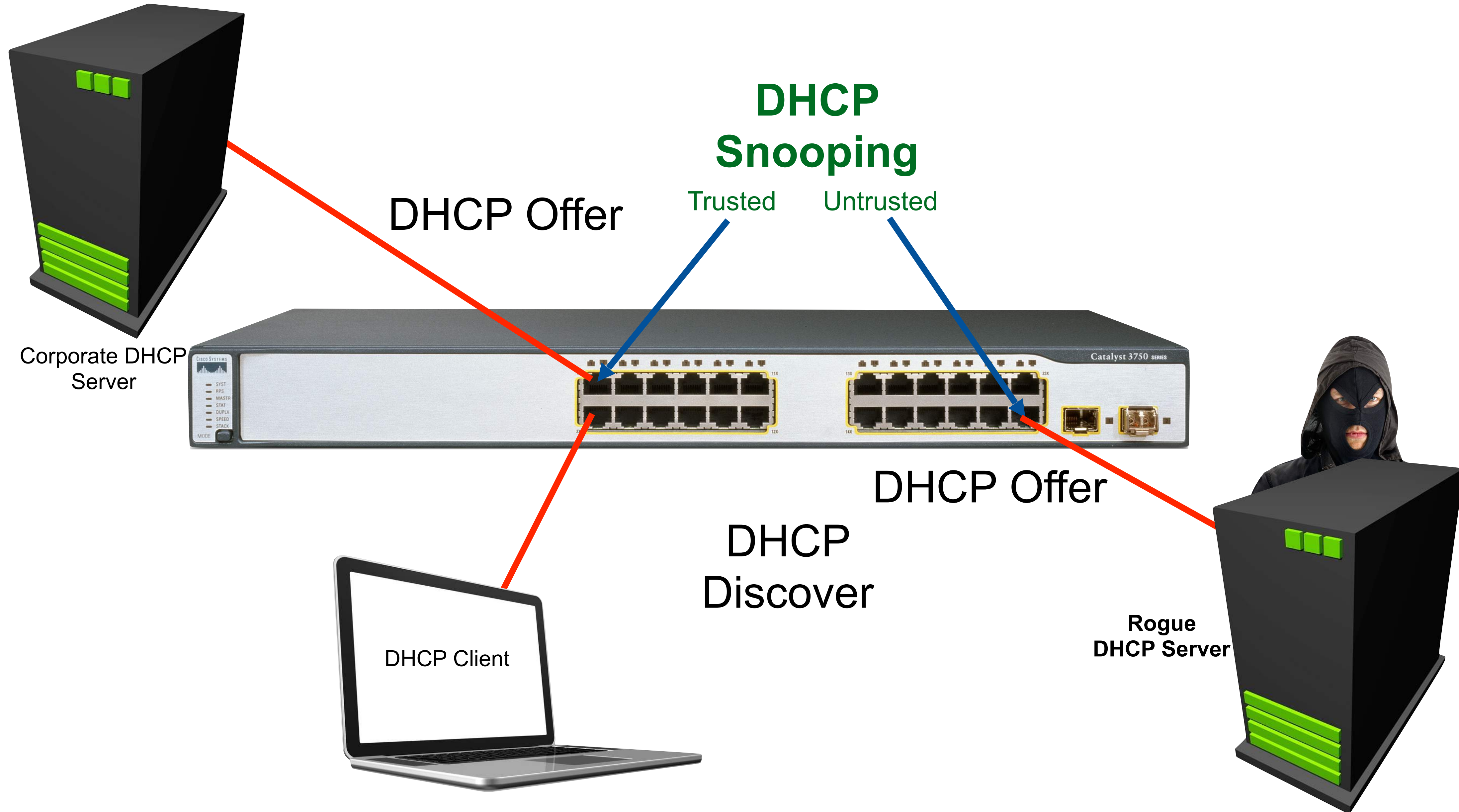


Mitigating Network Threats (cont.)

- **File Integrity Monitoring:** Use a service that can detect any change made to defined files (e.g. critical system files or financial records)
- **Role Separation:** Assign different sets of permissions to different categories of users, in an attempt to prevent conflicts of interest
- **Honeypot (or Honeynet) Deployment:** Configure a host (or a network) that does not contain sensitive information, and don't properly secure it
- **Penetration Testing (a.k.a. "Pen Testing"):** Launch an authorized attack on your network (or network device), in an attempt to evaluate its level of security



Mitigating Network Threats (cont.)



The Need for Wireless Security



- **Authentication:** A user provides credentials, such as a username and a password, to gain access to a network
- **Encryption:** Packets are scrambled such that, if they're intercepted by an attacker, an attacker cannot make sense of them



Tools for Securing a Wireless Network

- **MAC Filtering:** Only allowing a device on a network if its MAC address is an allowed MAC address
- **Geofencing:** Can use a mobile device's GPS location to permit or deny network access, or to grant or revoke specific network permissions
- **Wired Equivalent Privacy (WEP)**
 - The security standard specified by the original IEEE 802.11 wireless standard
 - Uses the RC4 encryption algorithm
 - Two types of authentication
 - **Open:** Does not require a WEP key, but will encrypt traffic if a valid WEP key is specified
 - **Shared:** Wireless clients and wireless access points have a matching pre-shared key



Enhanced Security Protocols



- **Temporal Key Integrity Protocol (TKIP)**
 - Improved encryption, compared to RC4
- **Message Integrity Check (MIC)**
 - Helps protect against man-in-the-middle or replay attacks
- **Advanced Encryption Standard (AES)**
 - Significantly stronger encryption, compared to TKIP, and vastly superior to RC4
- **Counter Mode with Cipher Block Chaining Message Authentication Code (CCMP)**
 - Adds onto AES's powerful encryption by making it challenging for a malicious user to spot repeated sequences
 - Uses hashing to verify messages have not been modified in transit

Enhanced Wireless Security Standards

- **Wi-Fi Protected Access (WPA)**
 - Uses TKIP for enhanced encryption
 - Uses a longer initialization vector (IV) to reduce the number of “collisions”
 - Has a discovered security weakness
- **Wi-Fi Protected Access II (WPA2)**
 - Requires support for AES and CCMP
 - Has a discovered security weakness
- **Wi-Fi Protected Access III (WPA3)**
 - Announced as the replacement for WPA2
 - Uses 192-bit encryption (as opposed to 128-bit encryption)
 - Will help with adoption of IoT devices due to easier setup for devices without displays



Primary Modes of Key Distribution

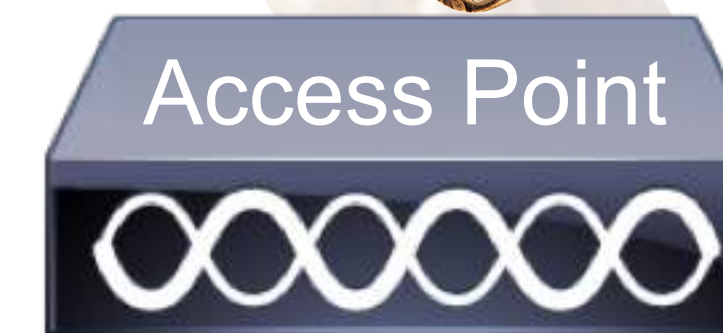
Two Modes of Key Distribution

- **Pre-Shared Key (PSK) Mode (a.k.a. “Personal Mode”)**: Matching keys are preconfigured on wireless clients and access points

Pre-Shared Key



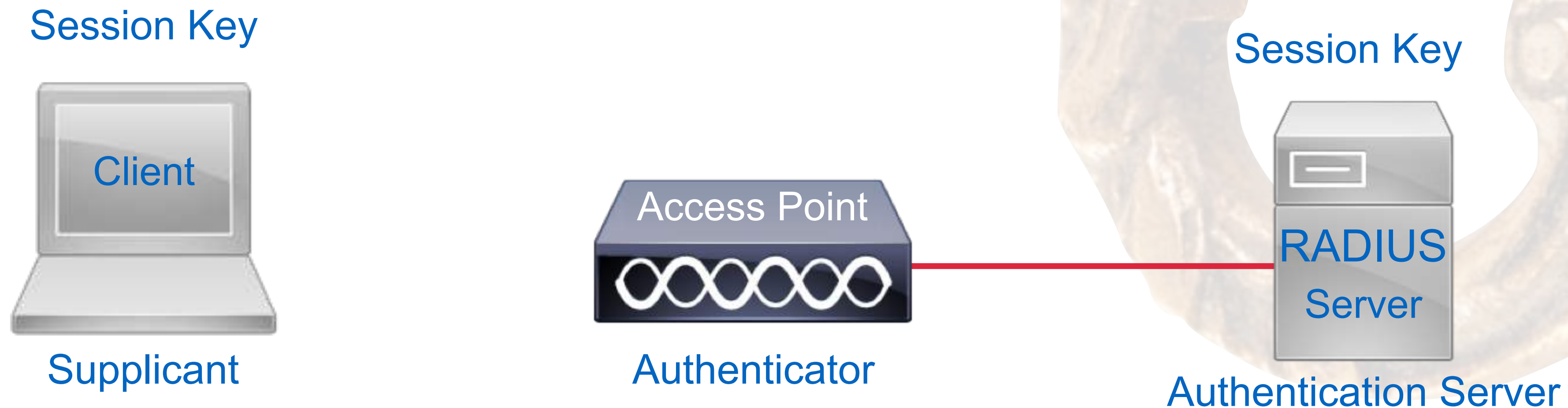
Pre-Shared Key



Primary Modes of Key Distribution

Two Modes of Key Distribution

- **Pre-Shared Key (PSK) Mode (a.k.a. “Personal Mode”)**: Matching keys are preconfigured on wireless clients and access points
- **Enterprise Mode**: Clients provide authentication credentials to an authentication server (e.g. a RADIUS server), which permits or denies network access and provides a session key to use during a permitted session.



Module 13

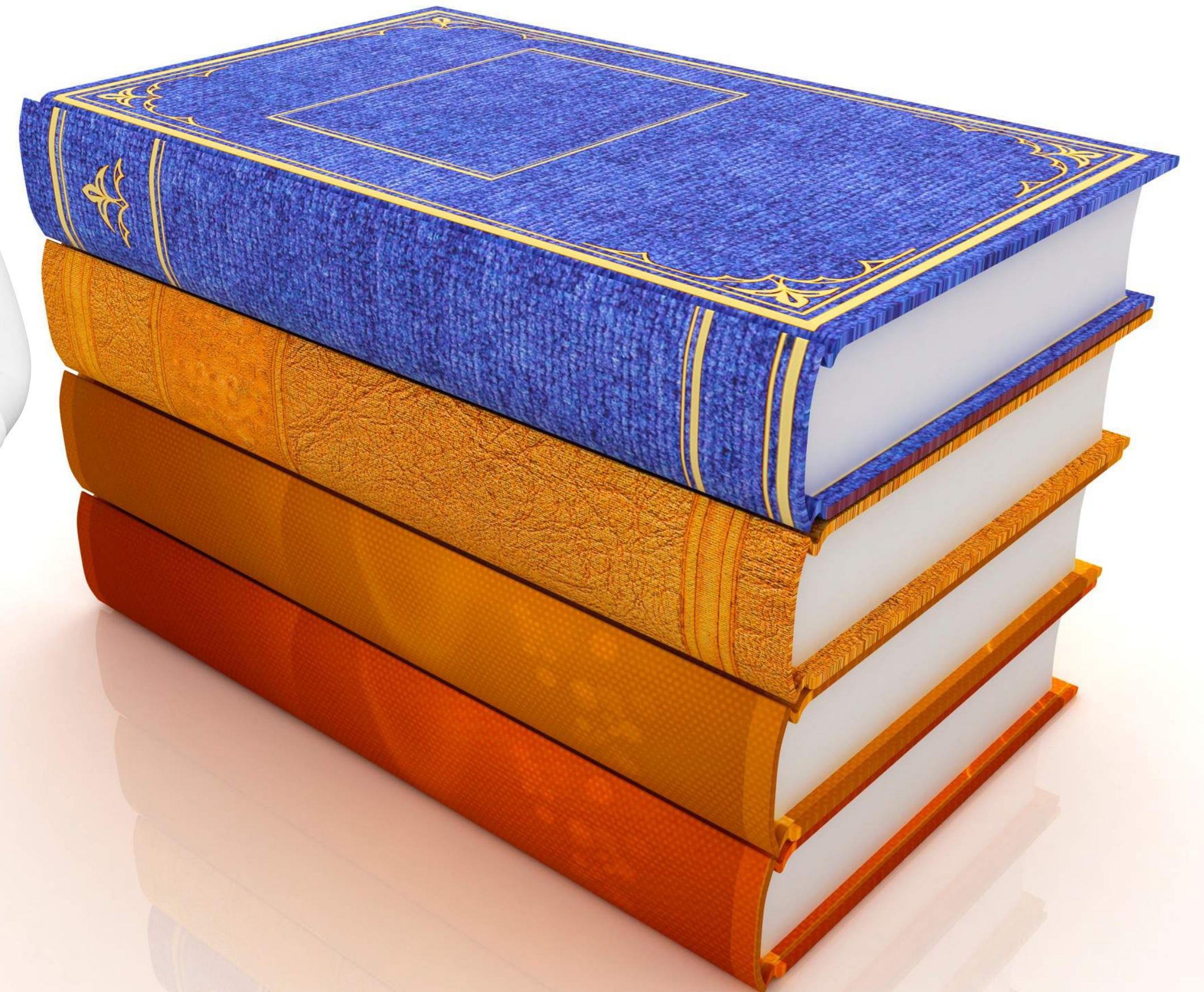
Network Security

Module 14

Network Monitoring and Management

Documentation

- Logical Topology
- Physical Topology
- Updated for New Installs
- Used for:
 - Troubleshooting
 - New Employees
 - Planning New Installations

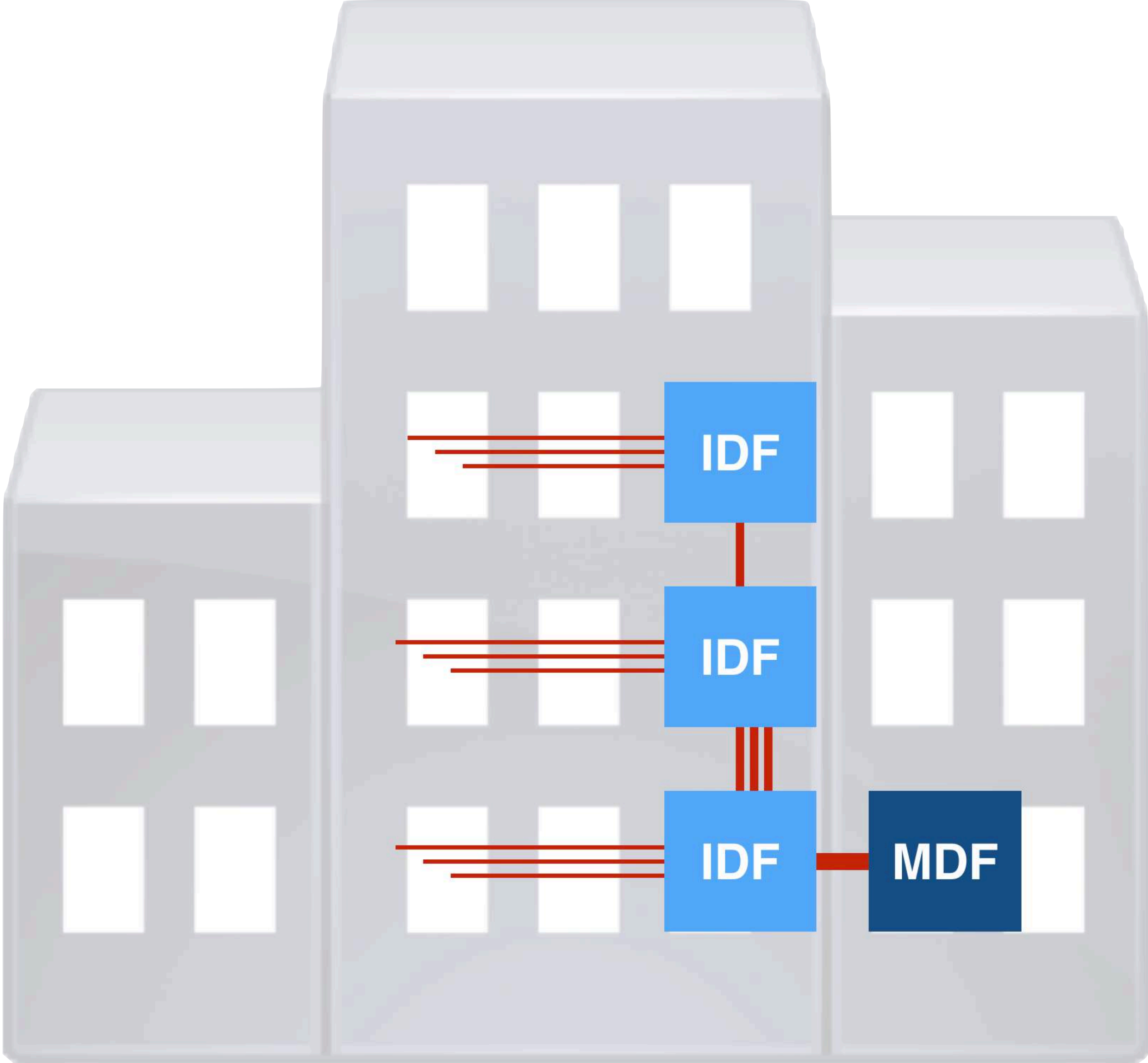


Other Recommended Documentation

CHANGE
MANAGEMENT

Other Recommended Documentation

IDF/MDF



Syslog Example

```
R1#  
R1#  
R1#  
R1#  
R1#conf term  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#int s1/0  
R1(config-if)#shutdown  
R1(config-if)#  
000040: *Nov 20 20:05:08.179: %LINK-5-CHANGED: Interface Serial1/0, changed state to administratively down  
000041: *Nov 20 20:05:09.183: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down  
R1(config-if)#
```



The screenshot shows the Kiwi Syslog Server interface. The window title is "Kiwi Syslog Server (Version 9.2)" and the address bar shows "192.168.1.50". The interface includes a menu bar (File, Edit, View, Help), a toolbar with various icons, and a table displaying received syslog messages. The table has columns for Date, Time, Priority, Hostname, and Message. Two messages are visible: one with priority 44 and one with priority 43, both from host 192.168.1.48.

Date	Time	Priority	Hostname	Message
11-20-2013	20:01:19	Local7.Notic	192.168.1.48	44: 000041: *Nov 20 20:05:09.183: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
11-20-2013	20:01:19	Local7.Notic	192.168.1.48	43: 000040: *Nov 20 20:05:08.179: %LINK-5-CHANGED: Interface Serial1/0, changed state to administratively down

Monitoring Processes

- Log Reviewing



Monitoring Processes

- Log Reviewing
- Port Scan

The screenshot displays the 'Pentest-Tools' website interface. The top navigation bar includes links for Pricing, Tools, API Reference, About, Contact, and Login. The sidebar on the left lists tool categories: Information Gathering, Web Application Testing, Infrastructure Testing (with sub-items like Ping Sweep, TCP Port Scan, UDP Port Scan, etc.), Exploit Helpers, and Utils. The main content area is titled 'TCP Port Scan with Nmap' and shows a configuration form. The 'Target' field is set to '192.168.1.1-254'. The 'Ports to scan' section has 'Common' selected, with a sub-option 'Scan the most common 100 TCP ports'. The 'Scan options' section includes four toggle switches: 'Detect service version' (ON), 'Detect operating system' (OFF), 'Do traceroute' (OFF), and 'Don't ping host (-Pn)' (OFF). A checkbox at the bottom indicates 'I am authorized to scan this target and I agree the Terms of Service'. A prominent orange 'Start Scan' button is located at the bottom right of the configuration area. Below the configuration form, there is an 'About this tool' section explaining that the tool discovers open TCP ports on a target host. A 'Parameters' section follows, listing details for Target, Ports to scan (Common, Range, List), and the various scan options.

About this tool

TCP Port Scan with Nmap allows you to discover which TCP ports are open on your target host.

Network ports are the entry points to a machine that is connected to the Internet. A service that listens on a port is able to receive data from a client application, process it and send a response back. Malicious clients can sometimes exploit vulnerabilities in the server code so they gain access to sensitive data or execute malicious code on the machine remotely. That is why testing for all ports is necessary in order to achieve a thorough security verification.

Port scanning is usually done in the initial phase of a penetration test in order to discover all network entry points into the target system. Port scanning is done differently for TCP ports and for UDP ports that's why we have different tools.

Parameters

- **Target:** This is the hostname of IP address(es) to scan
- **Ports to scan - Common:** This option tells Nmap to scan only the top 100 most common TCP ports (Nmap -F).
- **Ports to scan - Range:** You can specify a range of ports to be scanned. Valid ports are between 1 and 65535.
- **Ports to scan - List:** You can specify a comma separated list of ports to be scanned.
- **Detect service version:** In this case Nmap will try to detect the version of the service that is running on each open port. This is done using multiple techniques like banner grabbing, reading server headers and sending specific requests.
- **Detect operating system:** If enabled, Nmap will try to determine the type and version of the operating system that runs on the target host. The result is not always 100% accurate, depending on the way the target responds to probe requests.
- **Do traceroute:** If enabled, Nmap will also do a traceroute to determine the path packets take from our server to the target server, including the ip addresses of all network nodes (routers).
- **Don't ping host:** If enabled, Nmap will not try to see if the host is up before scanning it (which is the default behavior). This option is useful when the target host does not respond to ICMP requests but it is actually up and it has open ports.

Monitoring Processes

- Log Reviewing
- Port Scan
- Vulnerability Scan

The screenshot displays the 'Pentest-Tools' website interface. The top navigation bar includes links for Pricing, Tools, API Reference, About, Contact, and Login. The left sidebar lists tool categories: Information Gathering, Web Application Testing, Infrastructure Testing (selected), Exploit Helpers, and Utils. Under Infrastructure Testing, 'TCP Port Scan' is highlighted. The main content area is titled 'TCP Port Scan with Nmap' and shows a configuration form. The 'Target' field is set to '192.168.1.1-254'. The 'Ports to scan' section has 'Common' selected, with a sub-option 'Scan the most common 100 TCP ports'. The 'Scan options' section includes: 'Detect service version' (ON), 'Detect operating system' (OFF), 'Do traceroute' (OFF), and 'Don't ping host (-Pn)' (OFF). A checkbox at the bottom indicates 'I am authorized to scan this target and I agree the Terms of Service'. A 'Start Scan' button is visible. Below the form, the 'About this tool' section explains that the tool discovers open TCP ports and provides a list of parameters: Target, Ports to scan (Common, Range, List), Detect service version, Detect operating system, Do traceroute, and Don't ping host.

About this tool

TCP Port Scan with Nmap allows you to discover which TCP ports are open on your target host.

Network ports are the entry points to a machine that is connected to the Internet. A service that listens on a port is able to receive data from a client application, process it and send a response back. Malicious clients can sometimes exploit vulnerabilities in the server code so they gain access to sensitive data or execute malicious code on the machine remotely. That is why testing for all ports is necessary in order to achieve a thorough security verification.

Port scanning is usually done in the initial phase of a penetration test in order to discover all network entry points into the target system. Port scanning is done differently for TCP ports and for UDP ports that's why we have different tools.

Parameters

- **Target:** This is the hostname of IP address(es) to scan
- **Ports to scan - Common:** This option tells Nmap to scan only the top 100 most common TCP ports (Nmap -F).
- **Ports to scan - Range:** You can specify a range of ports to be scanned. Valid ports are between 1 and 65535.
- **Ports to scan - List:** You can specify a comma separated list of ports to be scanned.
- **Detect service version:** In this case Nmap will try to detect the version of the service that is running on each open port. This is done using multiple techniques like banner grabbing, reading server headers and sending specific requests.
- **Detect operating system:** If enabled, Nmap will try to determine the type and version of the operating system that runs on the target host. The result is not always 100% accurate, depending on the way the target responds to probe requests.
- **Do traceroute:** If enabled, Nmap will also do a traceroute to determine the path packets take from our server to the target server, including the ip addresses of all network nodes (routers).
- **Don't ping host:** If enabled, Nmap will not try to see if the host is up before scanning it (which is the default behavior). This option is useful when the target host does not respond to ICMP requests but it is actually up and it has open ports.

Monitoring Processes

- Log Reviewing
- Port Scan
- Vulnerability Scan
- Patch Management



Monitoring Processes

- Log Reviewing
- Port Scan
- Vulnerability Scan
- Patch Management
- Compare with Baseline Data



Monitoring Processes

- Log Reviewing
- Port Scan
- Vulnerability Scan
- Patch Management
- Compare with Baseline Data
- Packet Analysis

No.	Time	Source	Destination	Protocol	Length	Info
6433	7.71914700	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6434	7.71928200	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6435	7.71928600	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6436	7.71928800	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6437	7.71943900	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6438	7.71956500	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6439	7.71956900	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6440	7.71971100	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6441	7.71971500	192.168.1.40	71.74.45.136	TCP	60	61694->80 [ACK] Seq=2413 Ack=8192623 win=32722 Len=0
6442	7.71982200	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6443	7.71993200	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6444	7.71994300	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6445	7.71994500	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6446	7.72020200	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6447	7.72030600	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6448	7.72030900	71.74.45.136	192.168.1.40	TCP	1514	[TCP segment of a reassembled PDU]
6449	7.72031000	71.74.45.136	192.168.1.40	HTTP	768	HTTP/1.1 200 OK (video/mp2t)
6450	7.72031200	192.168.1.40	71.74.45.136	TCP	60	61694->80 [ACK] Seq=2413 Ack=8203557 win=32654 Len=0
6451	7.72035700	192.168.1.40	71.74.45.136	TCP	60	[TCP Window Update] 61694->80 [ACK] Seq=2413 Ack=8203557 win=32768 Len=0
6452	7.74772700	192.168.1.40	71.74.45.136	HTTP	470	GET /LIVE/1028/hls/ae/wLEXDT_13088/3400.m3u8?adId=66947d76-a52d-4055-bb59-a14bcc180ebf HTTP/1.
6453	7.78032700	71.74.45.136	192.168.1.40	HTTP	498	HTTP/1.1 304 Not Modified
6454	7.78033500	192.168.1.40	71.74.45.136	TCP	60	61694->80 [ACK] Seq=2829 Ack=8204001 win=32754 Len=0
6455	9.40295700	192.168.1.2	255.255.255.255	UDP	215	Source port: 45606 Destination port: 7437
6456	9.52253600	fe80::9df3:1b31:82f7ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
6457	9.60040900	78:8a:20:40:17:4c	Spanning-tree-(for-tSTP	60	RST. Root = 32768/0/78:8a:20:40:17:4b Cost = 0 Port = 0x8003	
6458	9.80300500	f0:9f:c2:c5:5f:34	Parallel_85:8a:9a	ARP	60	who has 192.168.1.120? Tell 192.168.1.1
6459	9.80302900	Parallel_85:8a:9a	f0:9f:c2:c5:5f:34	ARP	42	192.168.1.120 is at 00:1c:42:85:8a:9a
6460	11.60047700	78:8a:20:40:17:4c	Spanning-tree-(for-tSTP	60	RST. Root = 32768/0/78:8a:20:40:17:4b Cost = 0 Port = 0x8003	

Frame 1: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface 0
Ethernet II, Src: Tp-LinkT_6e:56:ba (c4:e9:84:6e:56:ba), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 239.255.255.250 (239.255.255.250)
User Datagram Protocol, Src Port: 59122 (59122), Dst Port: 1900 (1900)
Hypertext Transfer Protocol

Module 14

Network Monitoring and Management

Module 15

High Availability

High Availability

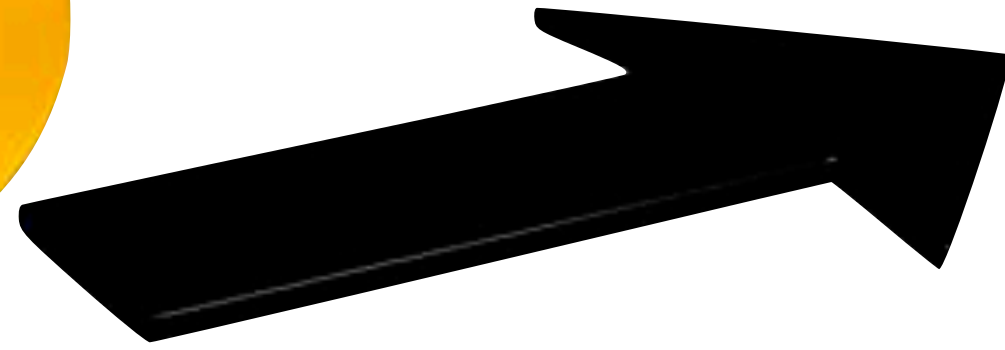


“The 5 Nines of Availability”

99.999 Percent Uptime

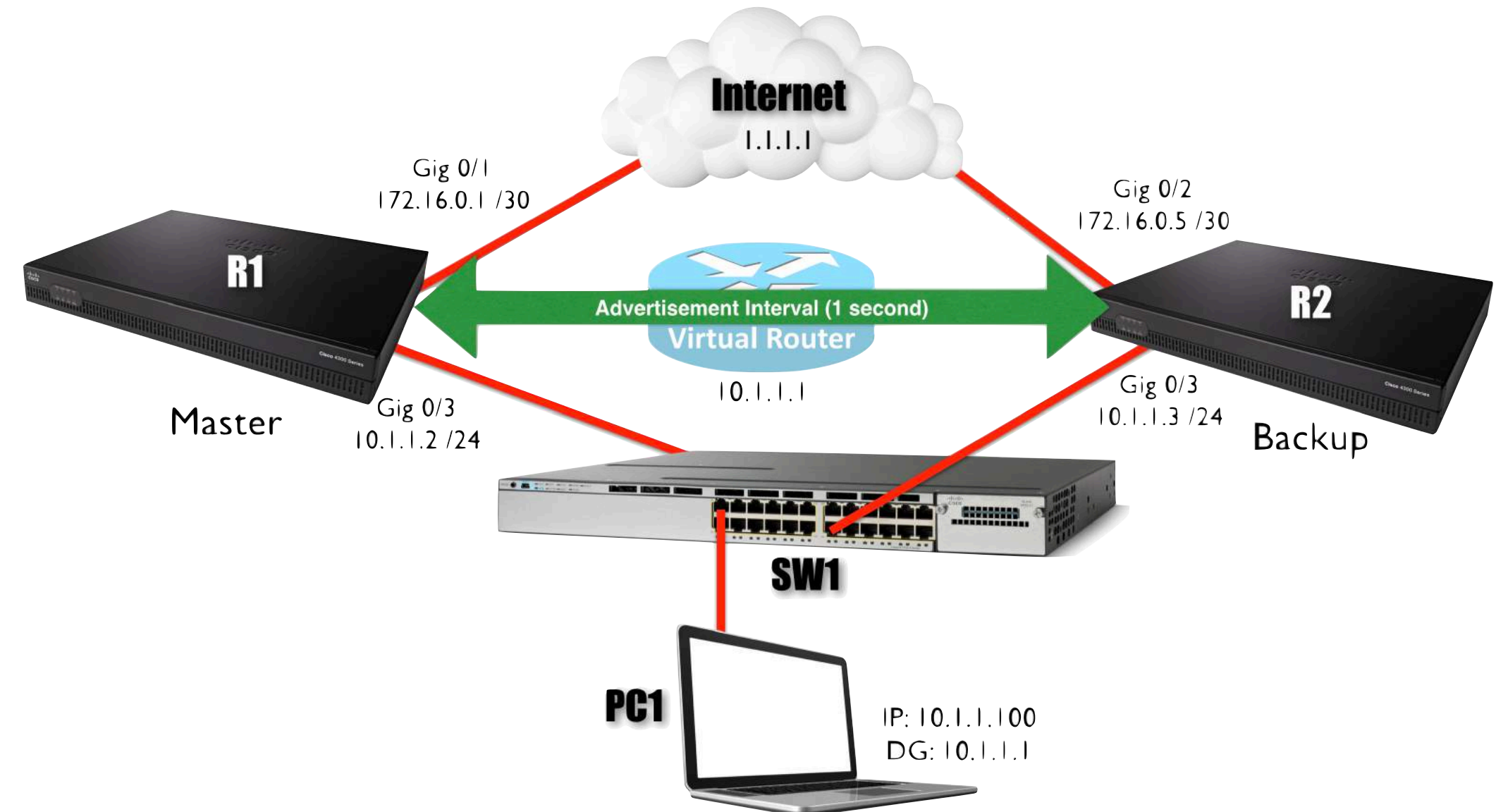
Approx. 5 Min. of Downtime/Year

High Availability



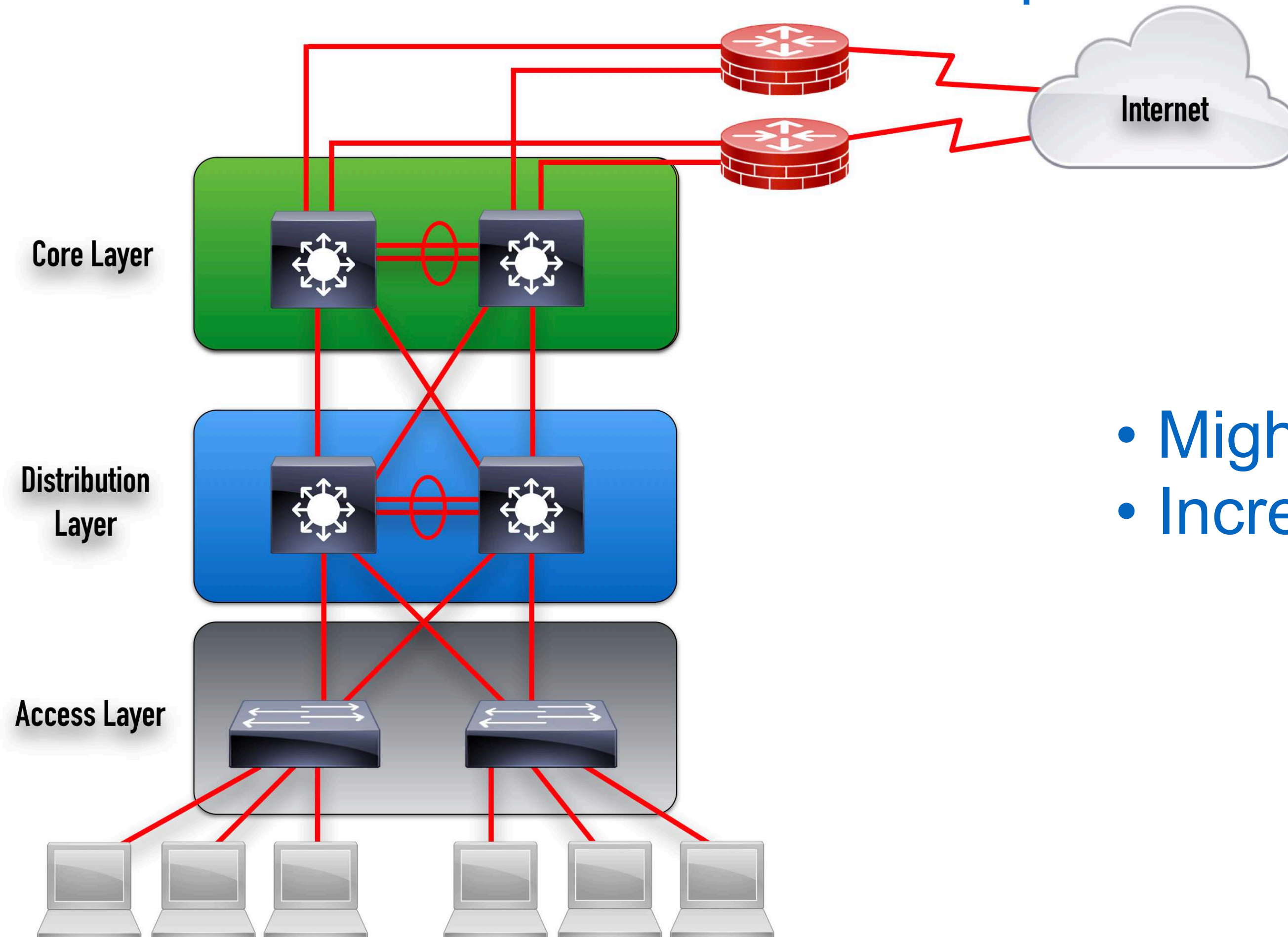
Higher Costs

- Redundant Components
- UPS/Generator
- VRRP



Fault Tolerance

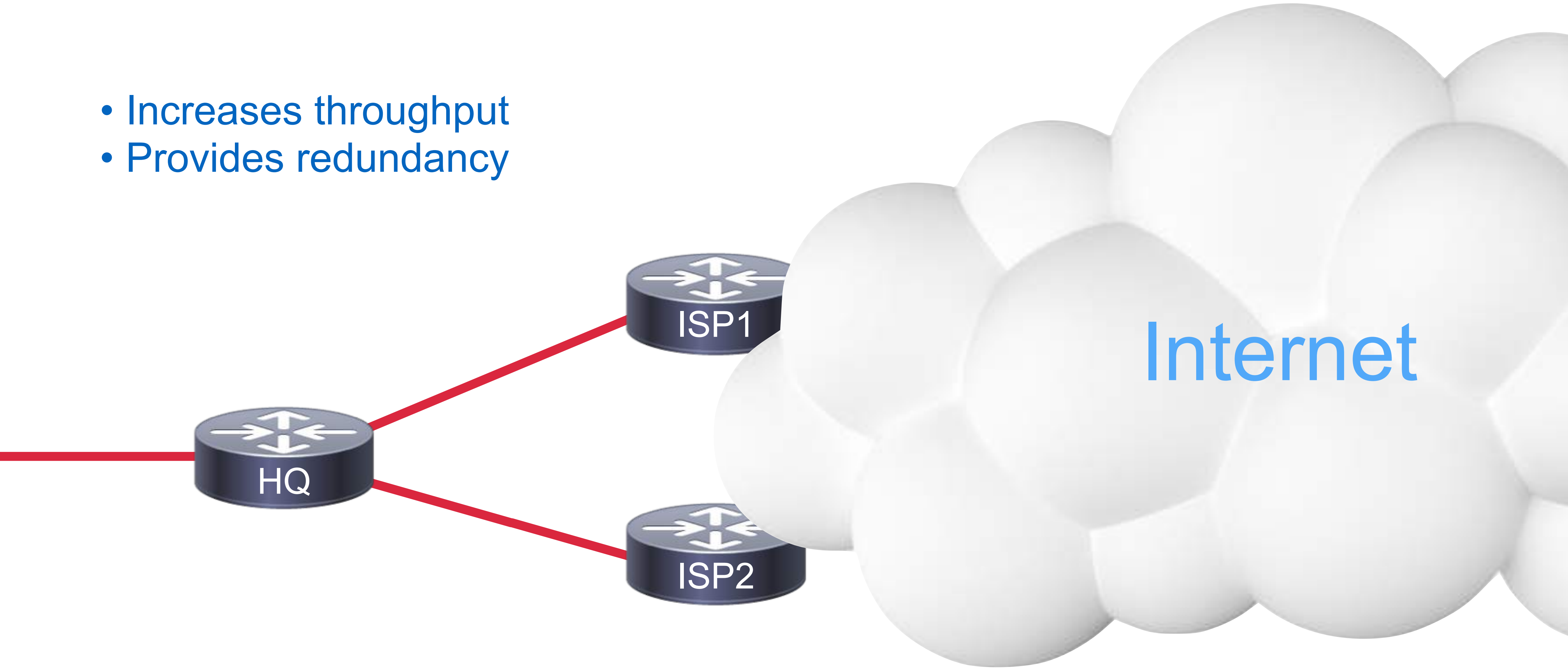
Fault Tolerance: The ability of a device to continue operation if one of its components fails.



- Might impact performance
- Increases complexity

Load Balancing

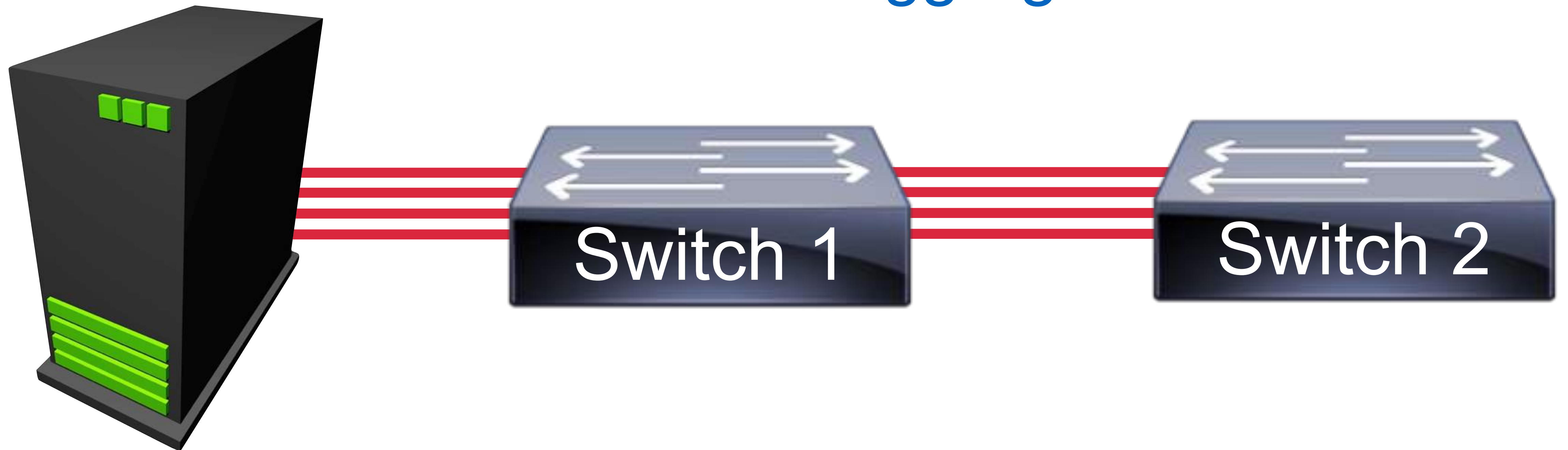
- Increases throughput
- Provides redundancy



Multiple Interconnections

NIC Teaming

Port Aggregation

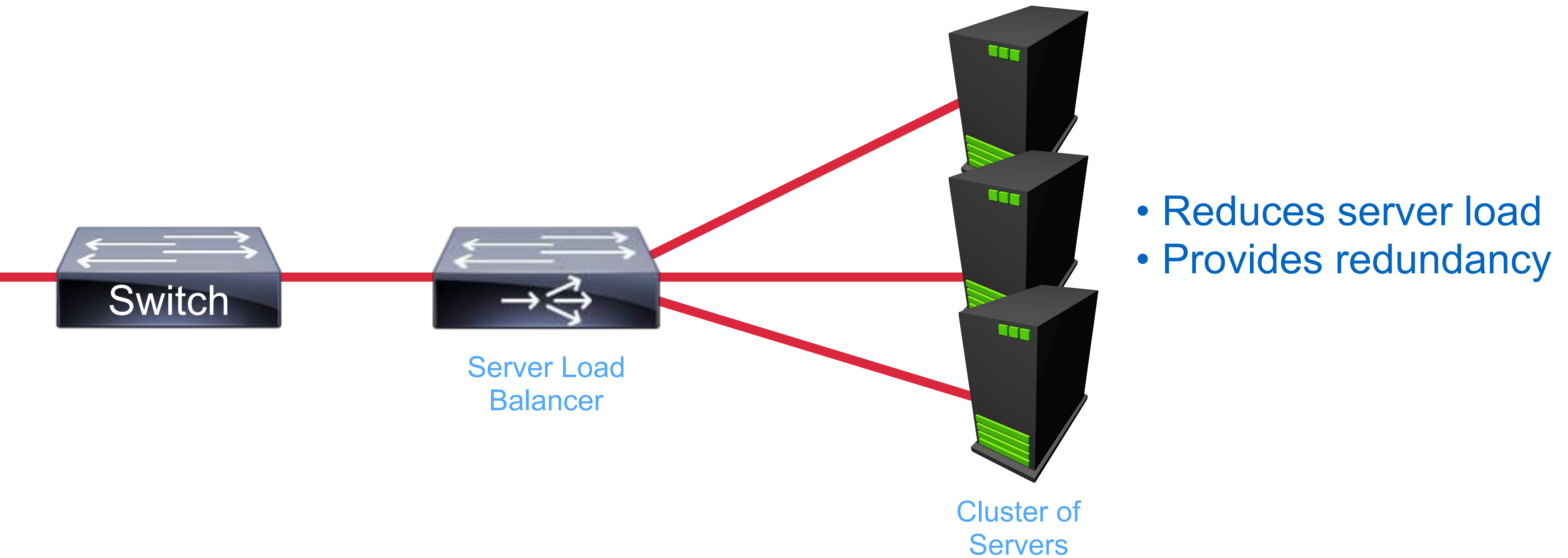


Server

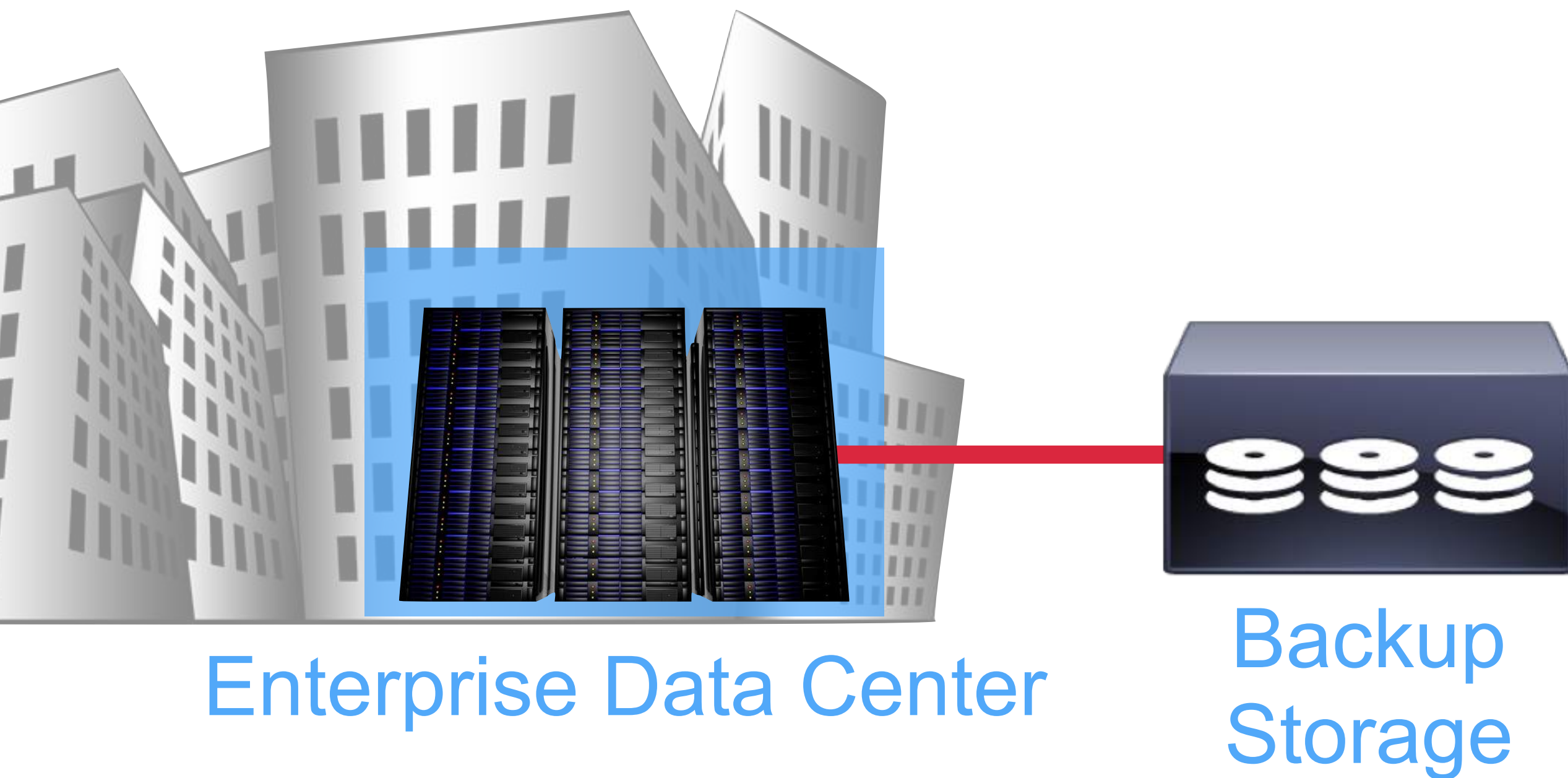
Switch 1

Switch 2

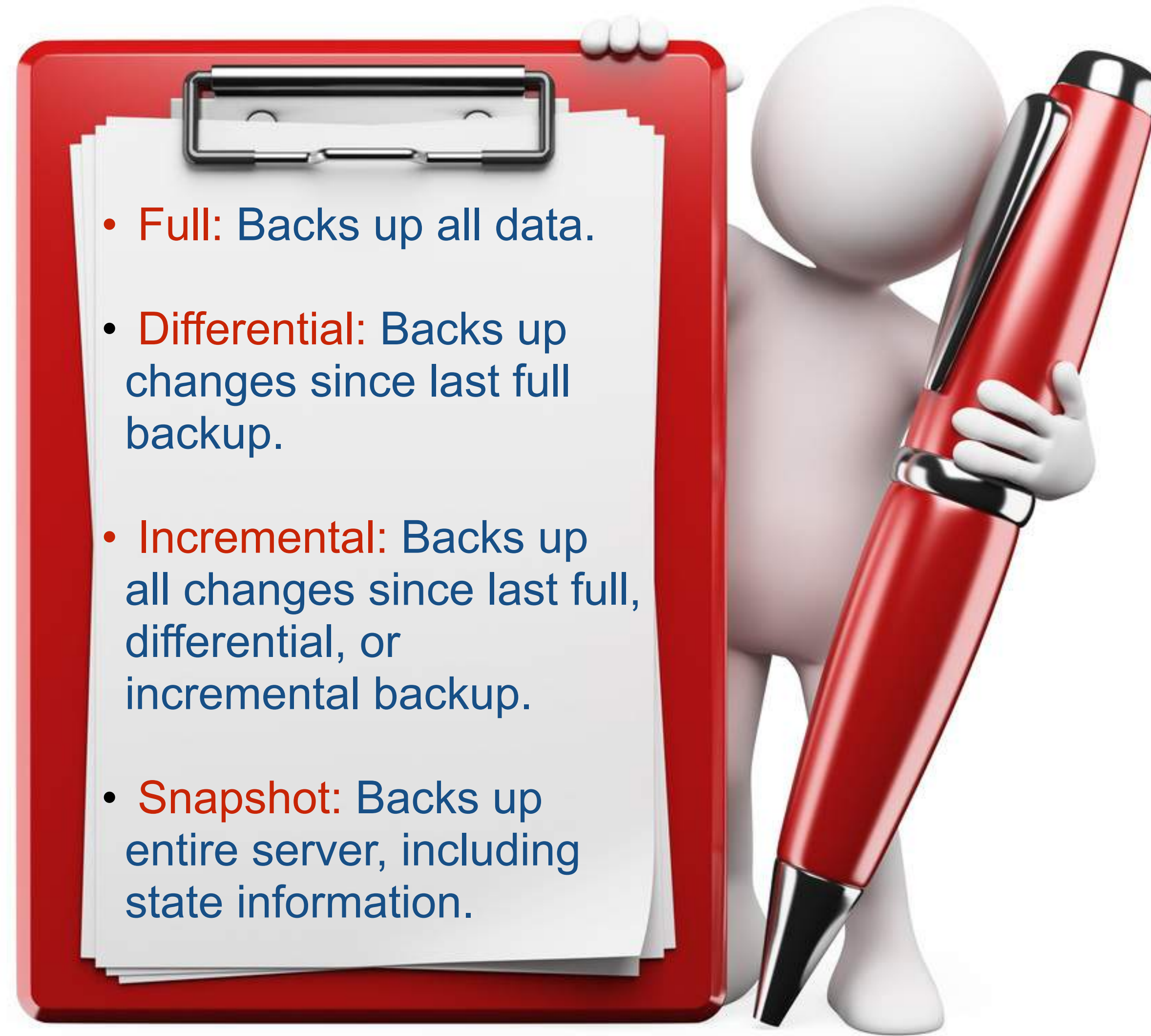
Clustering



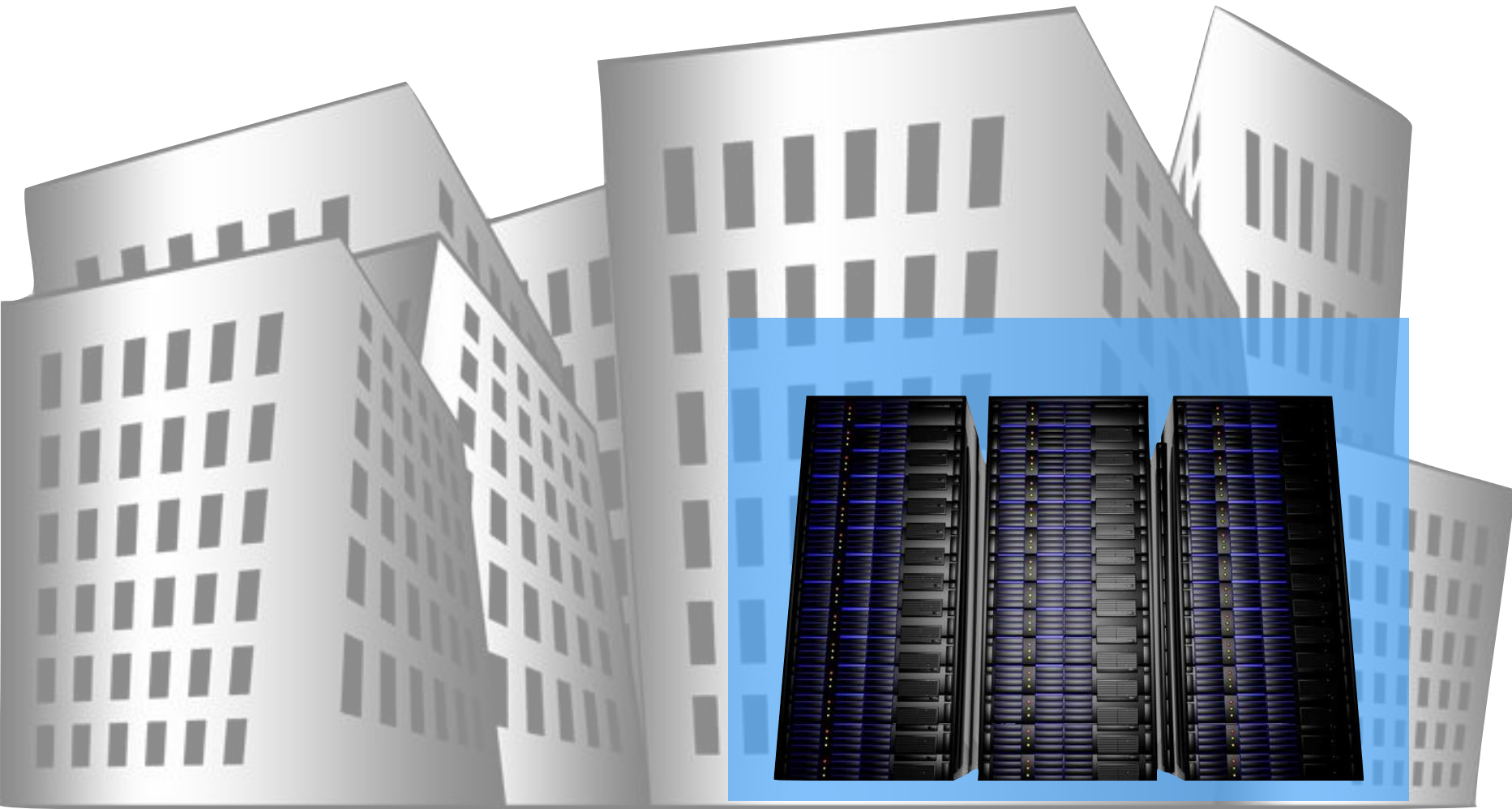
Disaster Recovery



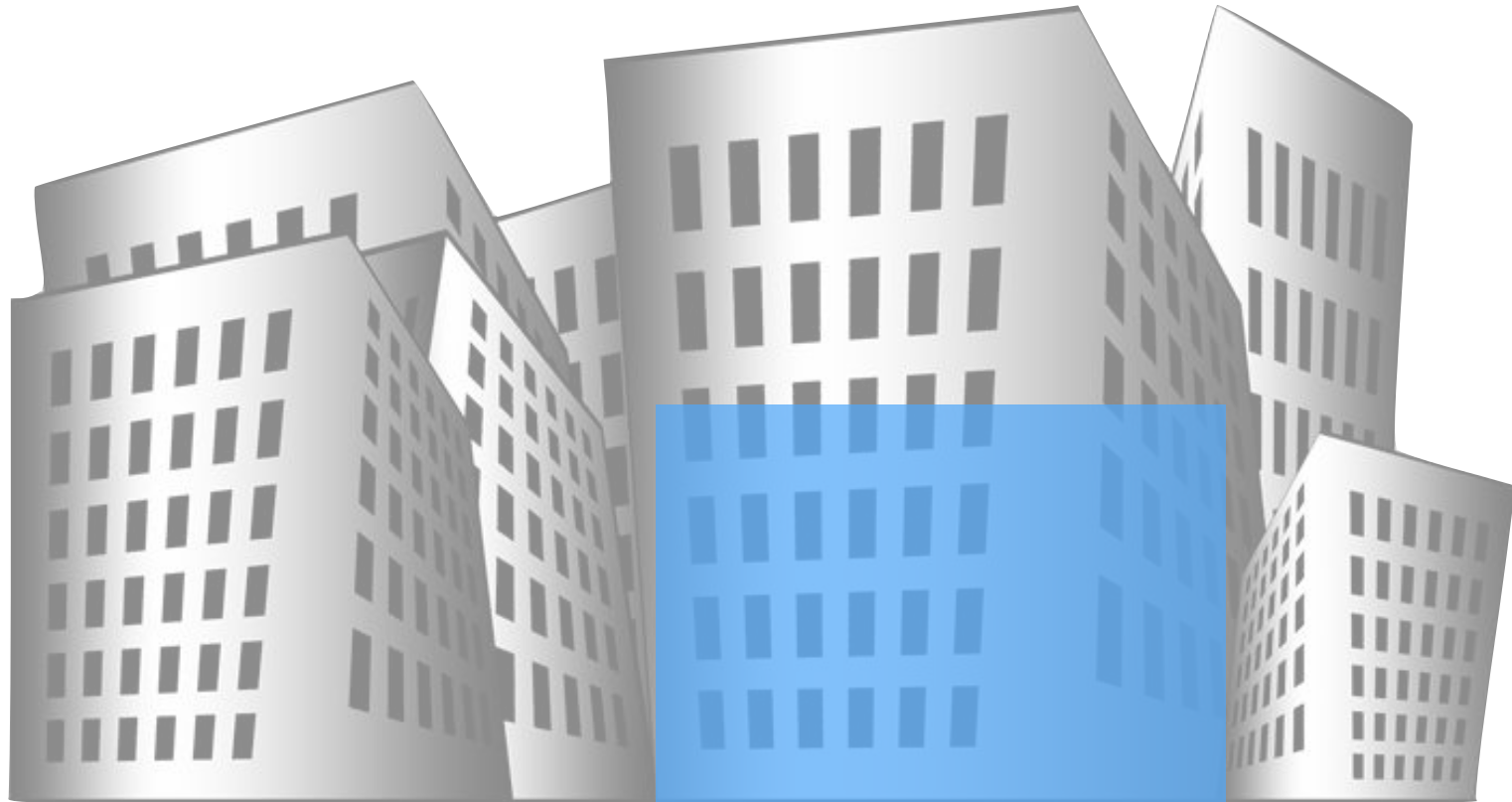
- **Full:** Backs up all data.
- **Differential:** Backs up changes since last full backup.
- **Incremental:** Backs up all changes since last full, differential, or incremental backup.
- **Snapshot:** Backs up entire server, including state information.



Remote Sites



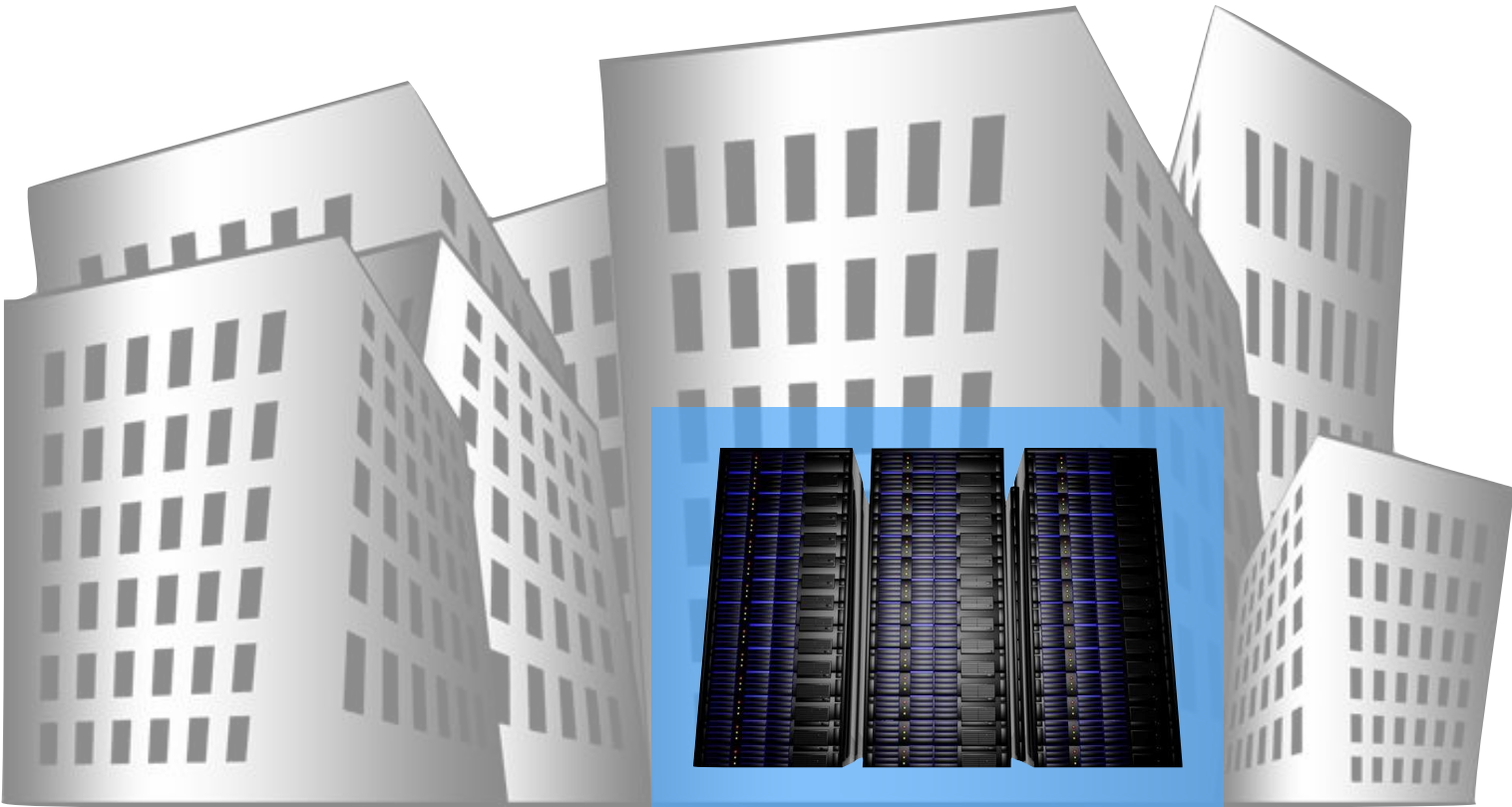
Enterprise Data Center



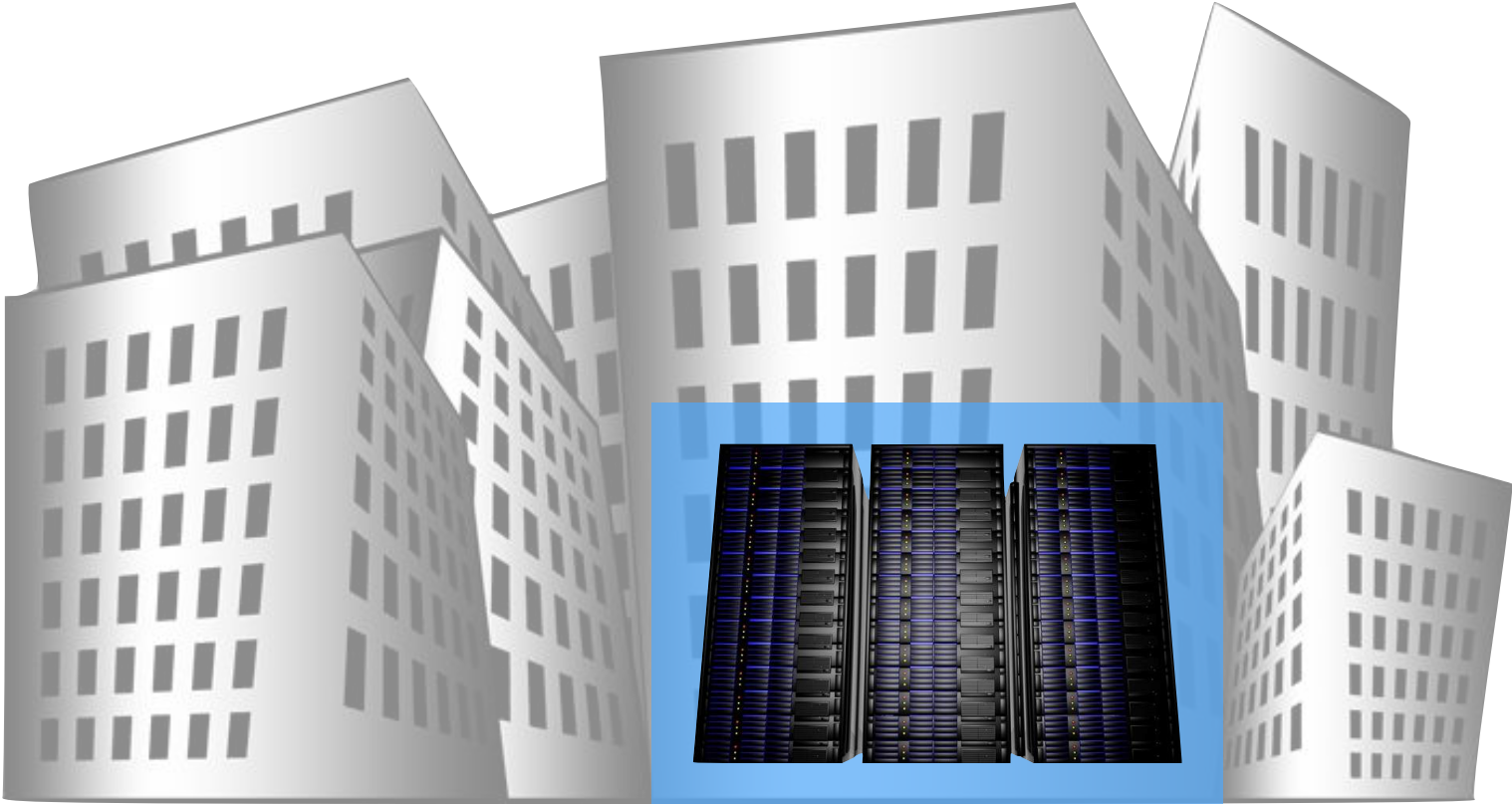
Cold Site

- Power
- HVAC
- Floor Space

- Power
- HVAC
- Floor Space
- Server Hardware
- Synchronized Data



Hot Site



Warm Site

- Power
- HVAC
- Floor Space
- Server Hardware

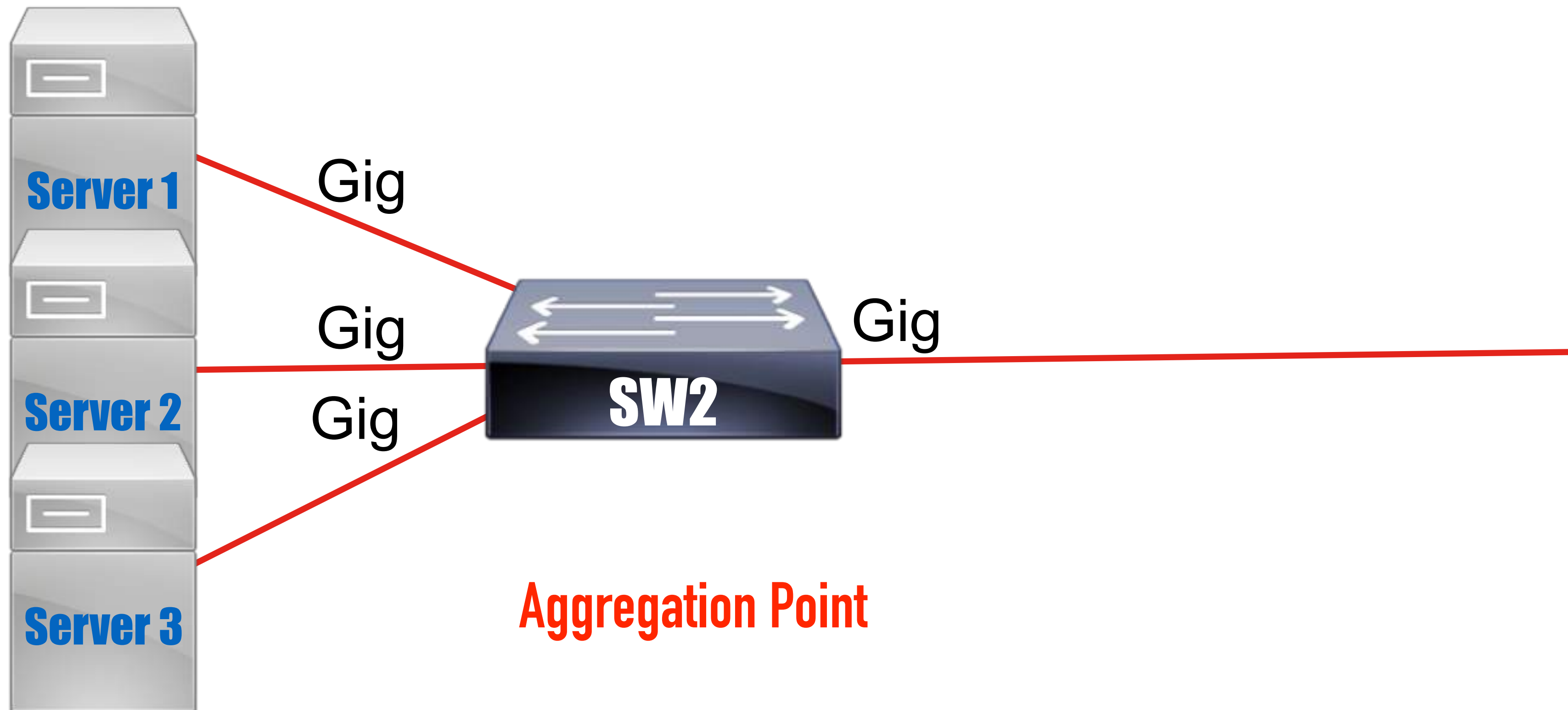
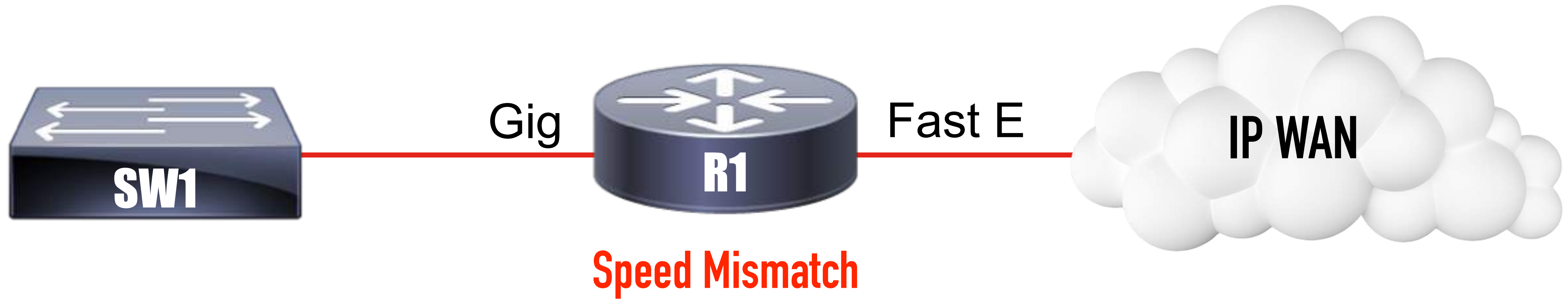
Module 15

High Availability

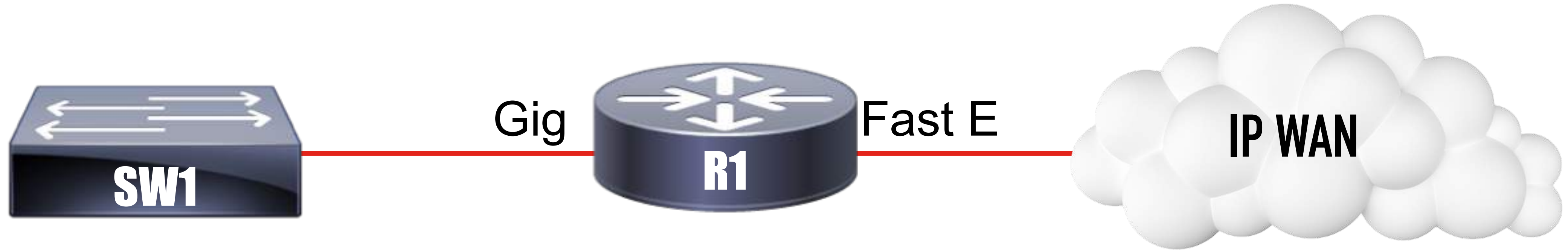
Module 16

Quality of Service

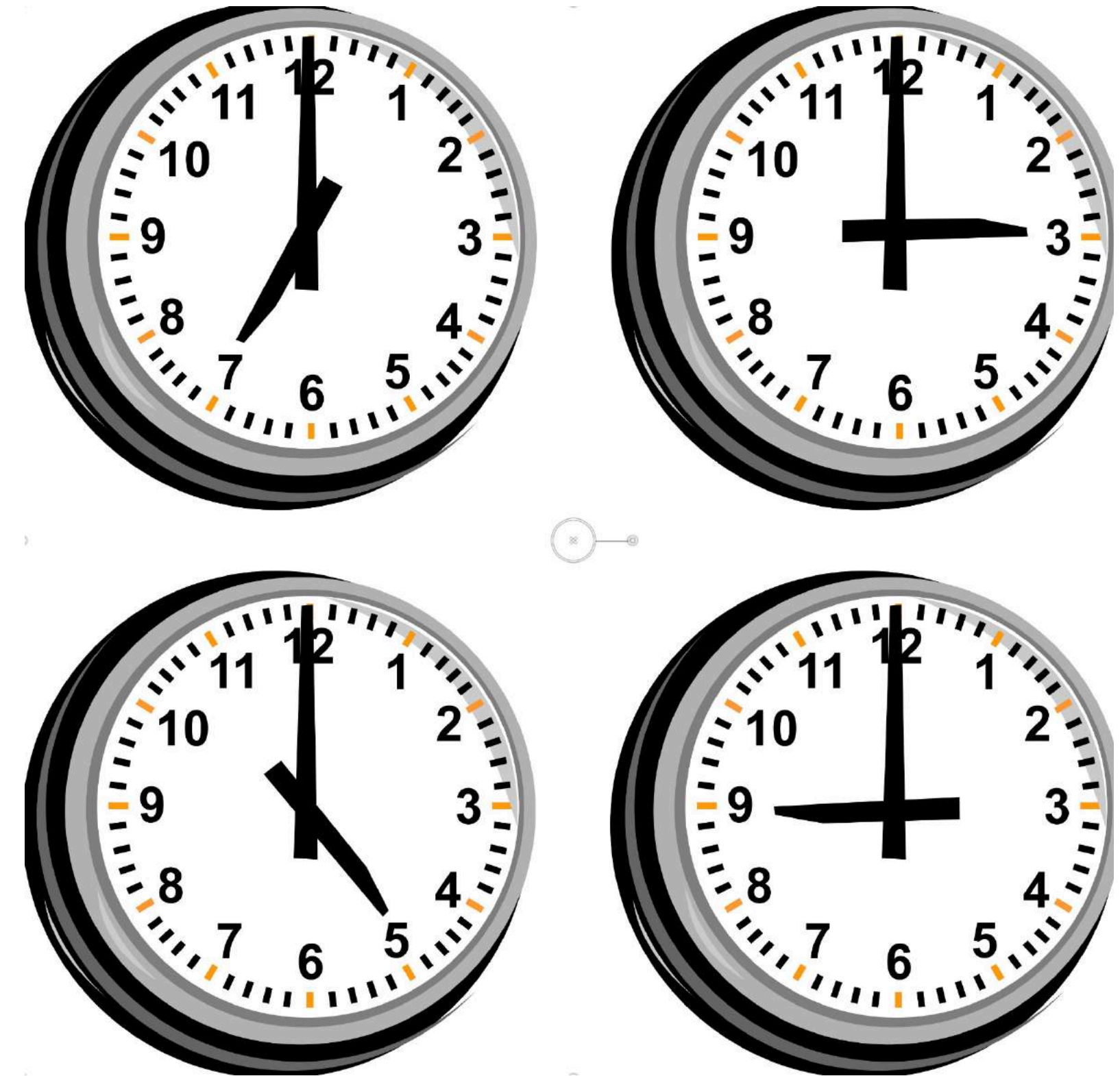
Do You Need QoS?



Do You Need QoS?



**Periodic
Congestion**

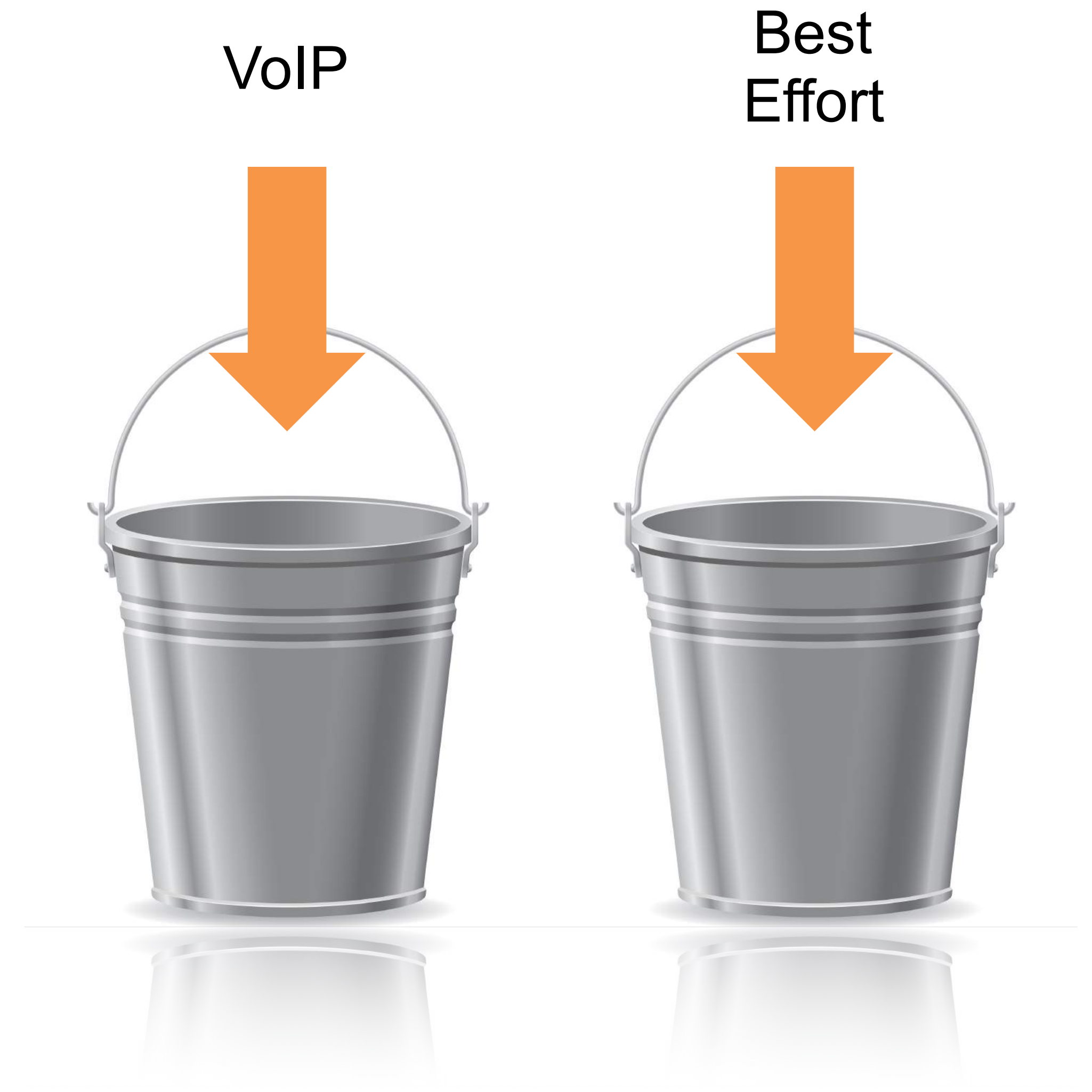
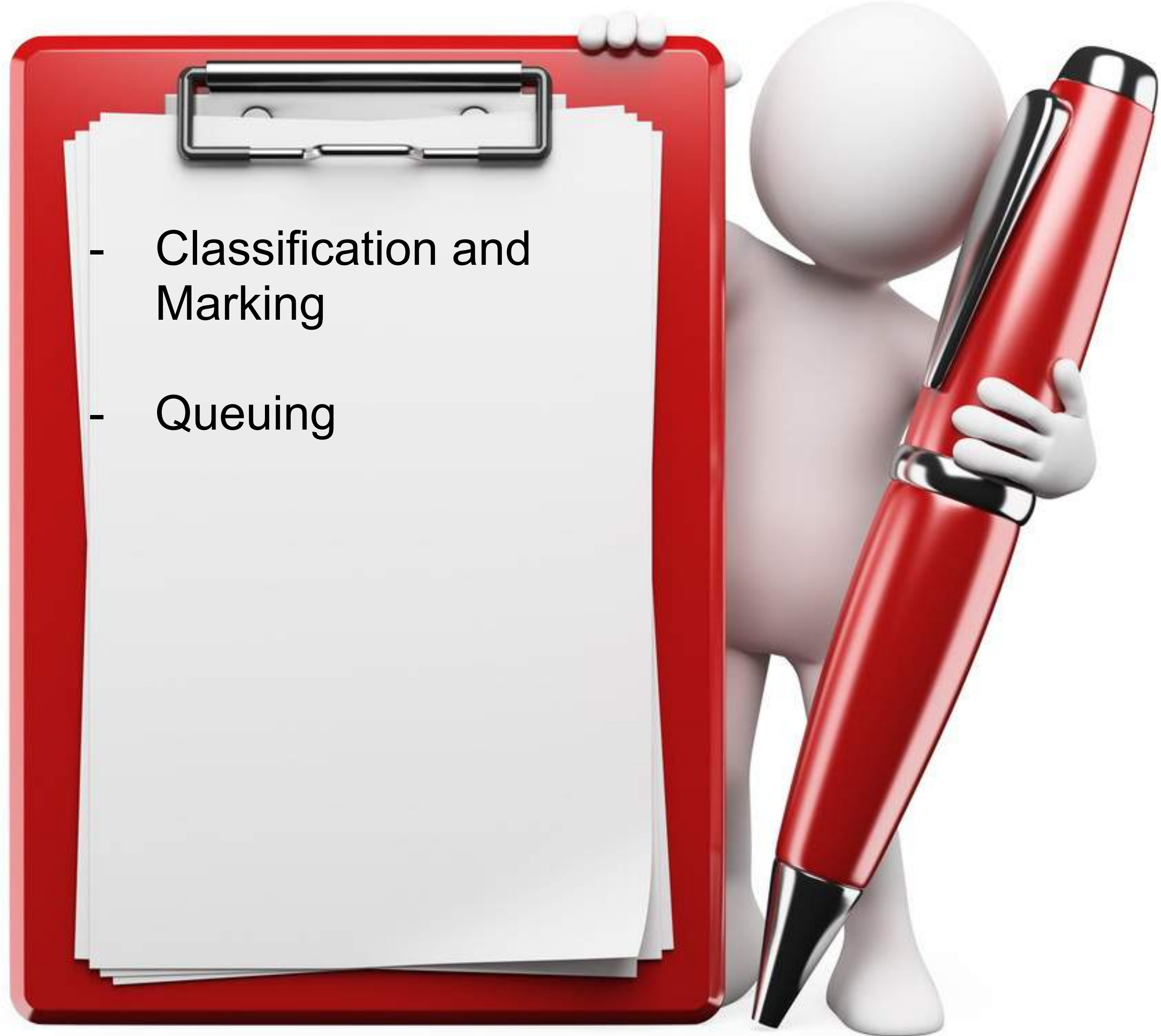


Common QoS Mechanisms

- Classification and Marking



Common QoS Mechanisms




Common QoS Mechanisms



- Classification and Marking
- Queuing
- Congestion Avoidance




Common QoS Mechanisms

- 
- Classification and Marking
 - Queuing
 - Congestion Avoidance
 - Policing and Shaping



Common QoS Mechanisms

- 
- Classification and Marking
 - Queuing
 - Congestion Avoidance
 - Policing and Shaping
 - Link Efficiency



Module 16

Quality of Service