CCNA Foundations – Day 1

with

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

Your Instructor

- Kevin Wallace
- CCIEx2 #7945 (Collaboration and R/S)
- Working with Cisco gear since 1989
- Taught courses with a CLP for nearly 14 years
- Network Design Specialist at Walt Disney World
- Written a bunch of books & made a ton of video courses for Cisco Press

Module 1
Protocols and Reference Models

Ports and Protocols

Client

10.1.1.1

Source IP: 10.1.1.1
Source Port: 49158
Destination IP: 172.16.1.2
Destination Port: 80

Source IP: 172.16.1.2
Source Port: 80
Destination IP: 10.1.1.1
Destination Port: 49158

Web Server

172.16.1.2

Protocol	Description	TCP Port	UDP Port
FTP	**File Transfer Protocol:** Transfers files with a remote host (typically requires authentication of user credentials).	20 and 21	
SSH	**Secure Shell:** Securely connect to a remote host (typically via a terminal emulator).	22	
SFTP	**Secure FTP:** Provides FTP file-transfer service over an SSH connection.	22	
SCP	**Secure Copy:** Provides a secure file-transfer service over an SSH connection and offers a file's original date and time information, which is not available with SFTP.	22	
Telnet	**Telnet:** Used to connect to a remote host (typically via a terminal emulator).	23	
SMTP	**Simple Mail Transfer Protocol:** Used for sending e-mail.	25	
DNS	**Domain Name System:** Resolves domain names to corresponding IP addresses.	53	53
TFTP	**Trivial File Transfer Protocol:** Transfers files with a remote host (does not require authentication of user credentials).		69
DHCP	**Dynamic Host Configuration Protocol:** Dynamically assigns IP address information (for example, IP address, subnet mask, DNS server's IP address, and default gateway's IP address) to a network device.		67
HTTP	**Hypertext Transfer Protocol:** Retrieves content from a web server.	80	
POP3	**Post Office Protocol version 3:** Retrieves e-mail from an e-mail server.	110	
NNTP	**Network News Transport Protocol:** Supports the posting and reading of articles on Usenet news servers.	119	
NTP	**Network Time Protocol:** Used by a network device to synchronize its clock with a time server (NTP server).		123
SNTP	**Simple Network Time Protocol:** Supports time synchronization among network devices, similar to Network Time Protocol (NTP), although SNTP uses a less complex algorithm in its calculation and is slightly less accurate than NTP.		123

Protocol	Description	TCP Port	UDP Port
IMAP4	**Internet Message Access Protocol version 4:** Retrieves e-mail from an e-mail server.	143	
SNMP	**Simple Network Management Protocol:** Used to monitor, manage, and configure network devices. An SNMP agent receives requests on port 161, and an SNMP agent sends traps on port 162.	161 and 162	161 and 162
LDAP	**Lightweight Directory Access Protocol:** Provides directory services (for example, a user directory—including username, password, e-mail, and phone number information) to network clients.	389	
HTTPS	**Hypertext Transfer Protocol Secure:** Used to securely retrieve content from a web server.	443	
SMB	**Server Message Block:** Used primarily in Microsoft networks for sharing resources (e.g. file resources) between devices.		445
rsh	**Remote Shell:** Allows commands to be executed on a computer from a remote user.	514	
RTSP	**Real Time Streaming Protocol:** Communicates with a media server (for example, a video server) and controls the playback of the server's media files.	554	554
LDAPS	**LDAP over SSL:** Securely sends LDAP messages over a Secure Sockets Layer (SSL) connection.	636	636
H.323	An ITU-T recommendation that can setup and teardown multimedia calls (e.g. voice and video calls).	1720	
RDP	**Remote Desktop Protocol:** A Microsoft protocol that allows a user to view and control the desktop of a remote computer.	3389	
SIP	**Session Initiation Protocol:** A signaling protocol used to setup, monitor, and teardown multimedia calls (e.g. voice and video calls). Port 5060 is commonly used for unencrypteypted calls, and port 5061 is commonly used to setup encrypted calls.	5060 and 5061	5060 and 5061

The OSI Model

“Switches live at Layer 2.”

“Routers live at Layer 3.”

The OSI Model's Seven Layers

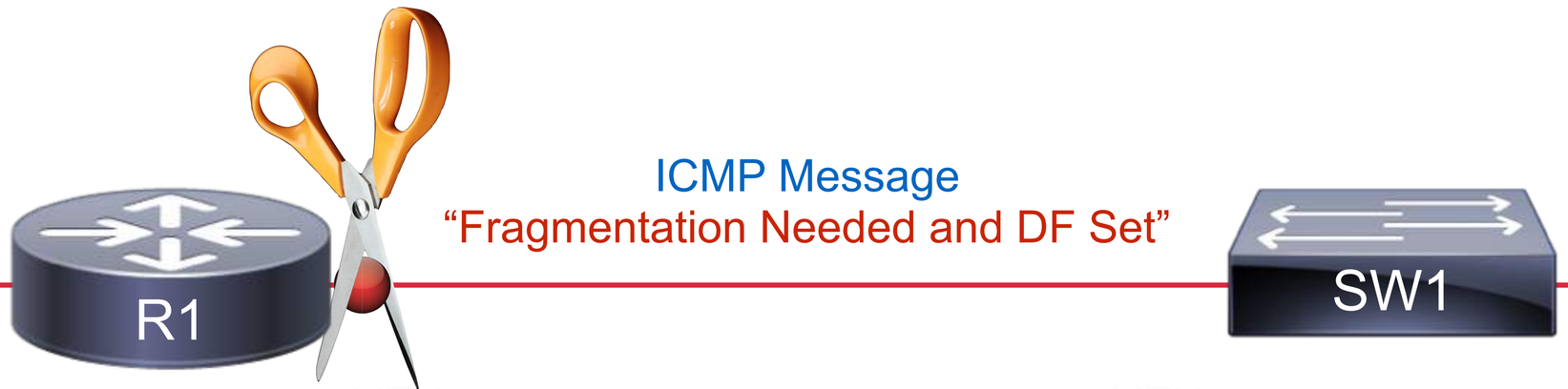
Floor 1

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

Maximum Transmission Unit (MTU)

The largest frame or packet that can be transmitted or received on an interface.

Don't Fragment (DF) Bit: A bit in an IPv4 header that prevents a packet from being fragmented.

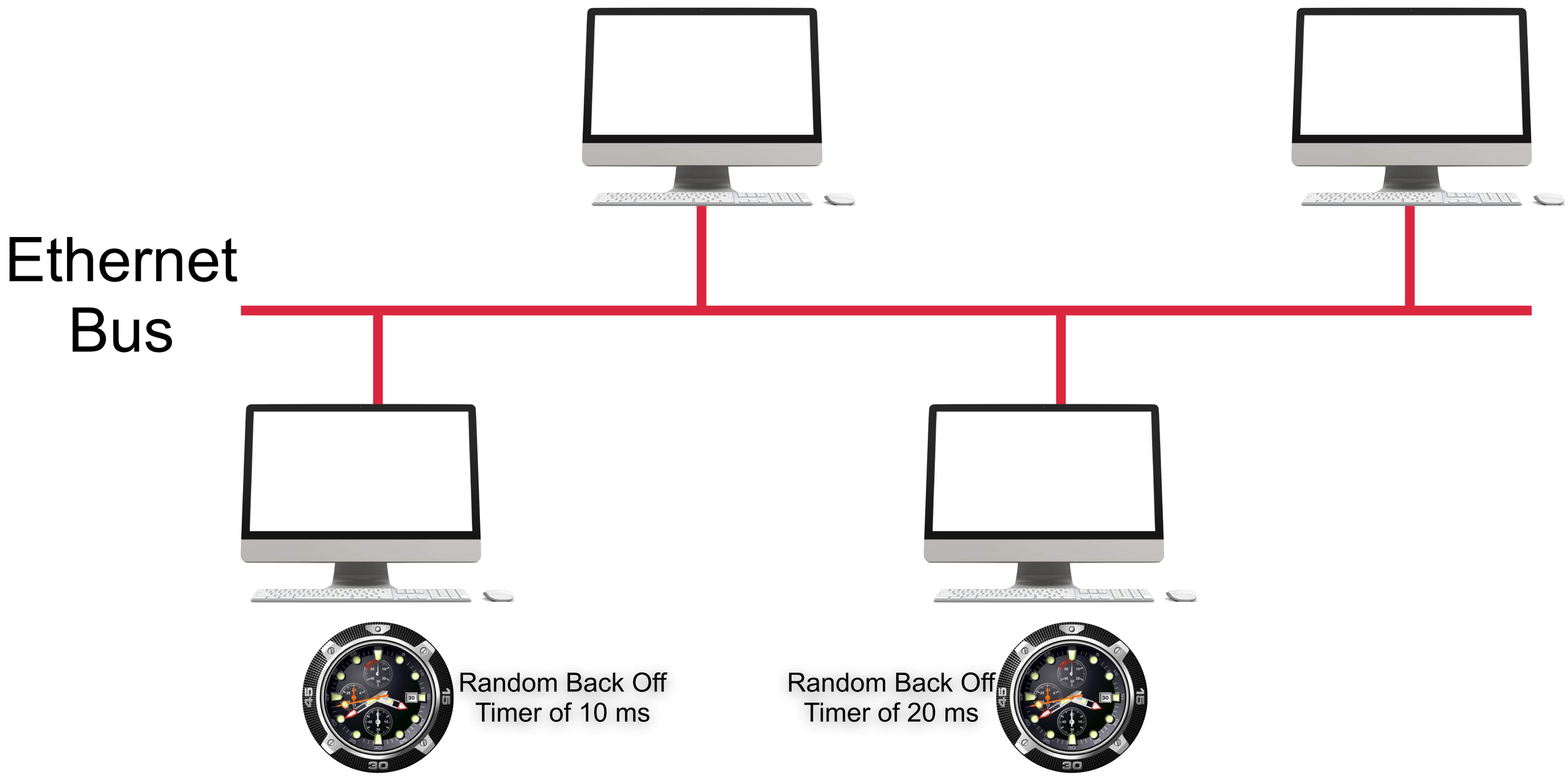


NOTE: IPv6 does not have a DF bit, and it uses a "Packet Too Big" ICMPv6 message.

Module 1
Protocols and Reference Models

Module 2
Network Devices

CSMA/CD vs CSMA/CA



CSMA/CD vs CSMA/CA

“Hidden Node” Problem

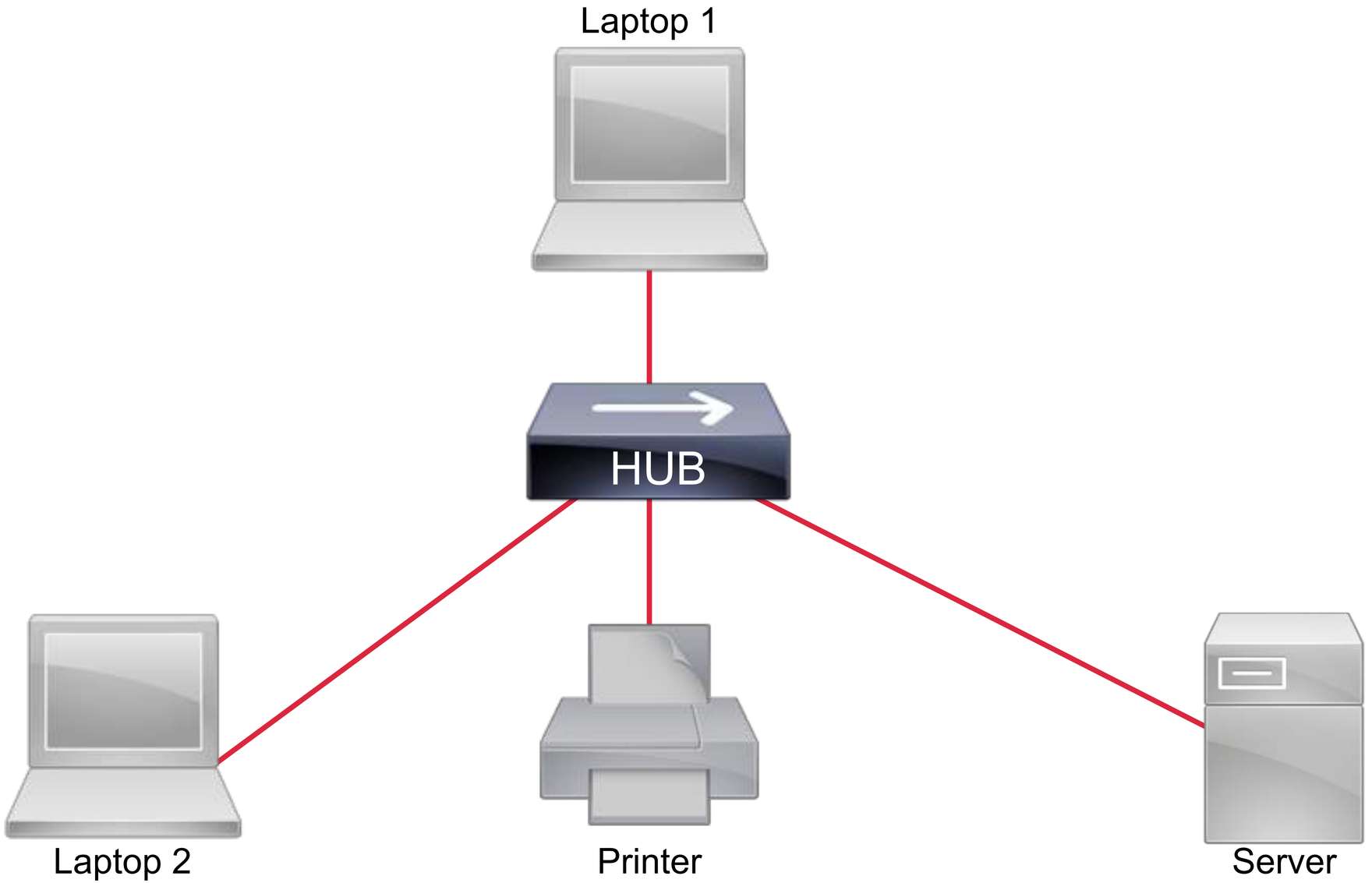
Client 1

Wireless Access Point

Client 2

Random Back Off
Timer of 10 ms

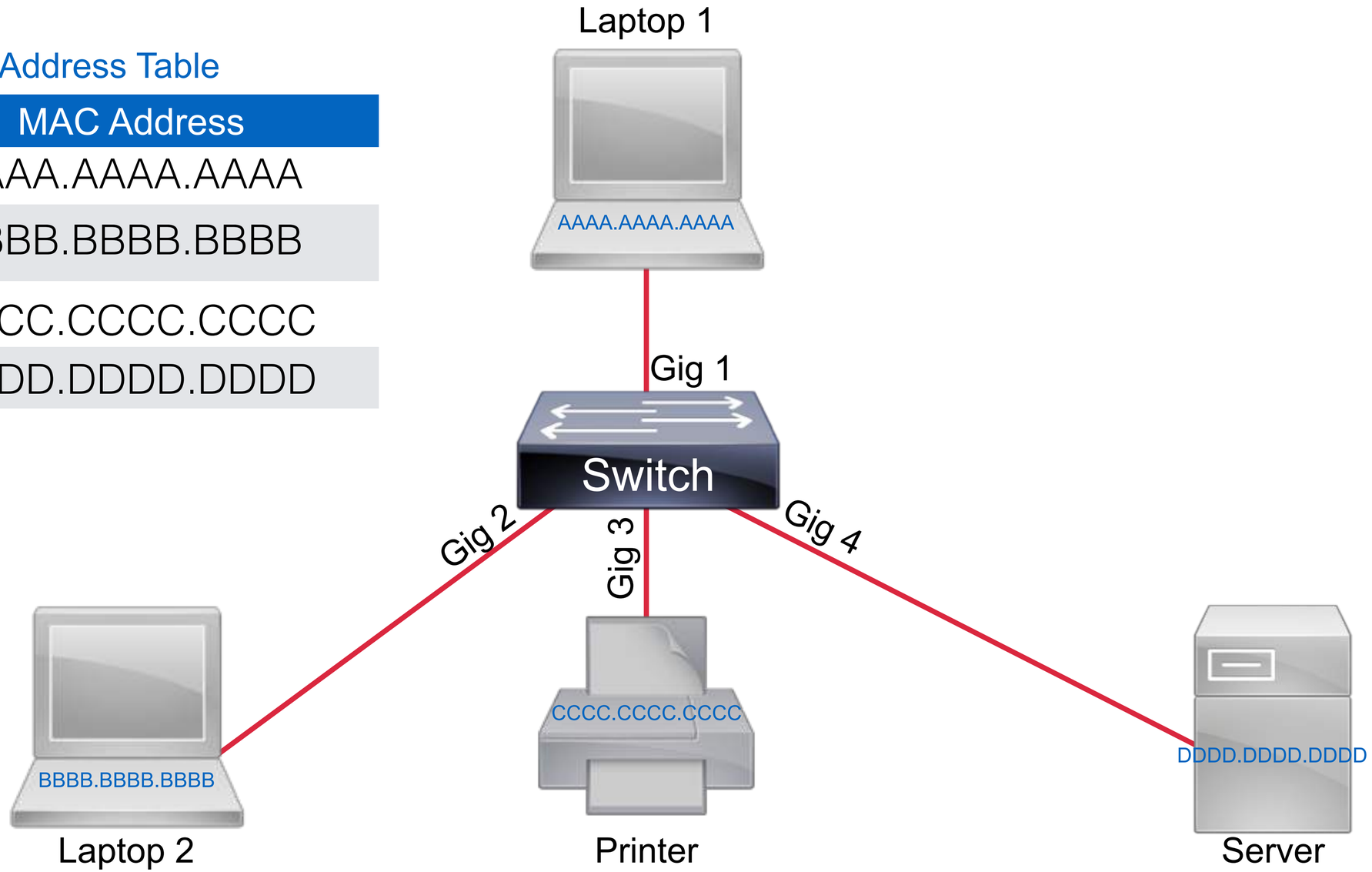
Hub



Switch

MAC Address Table

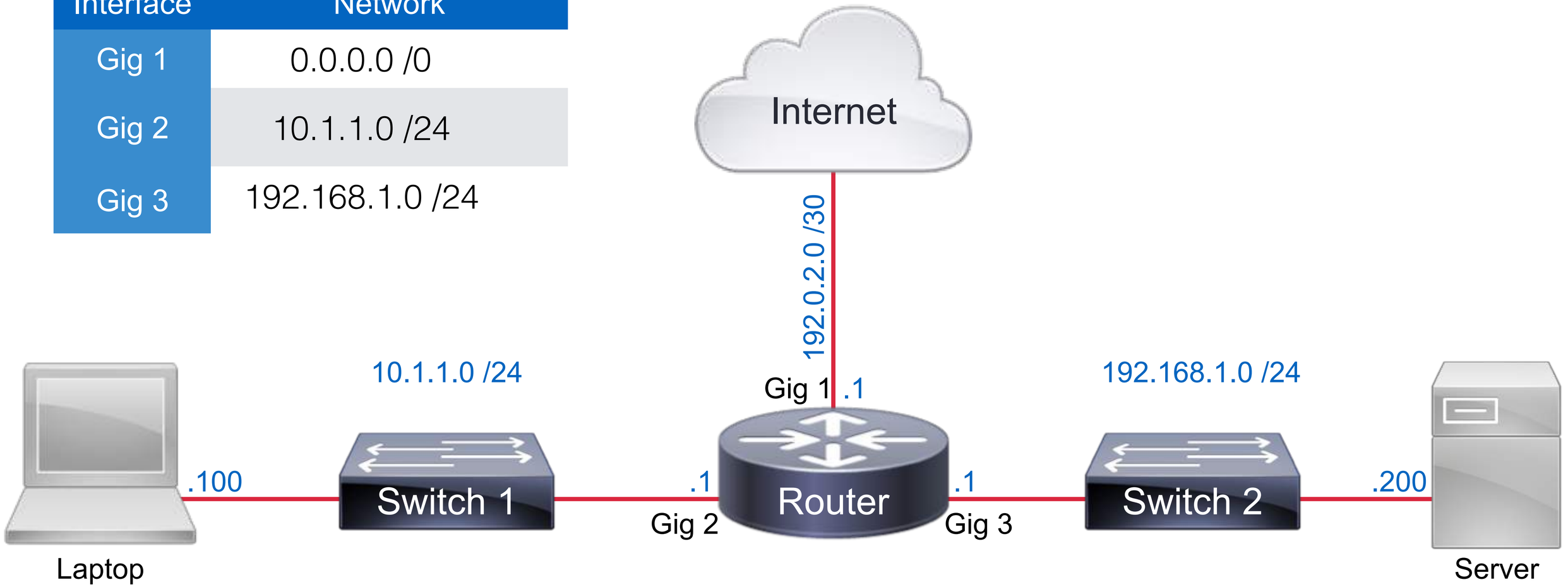
Port	MAC Address
Gig 1	AAAA.AAAA.AAAA
Gig 2	BBBB.BBBB.BBBB
Gig 3	CCCC.CCCC.CCCC
Gig 4	DDDD.DDDD.DDDD

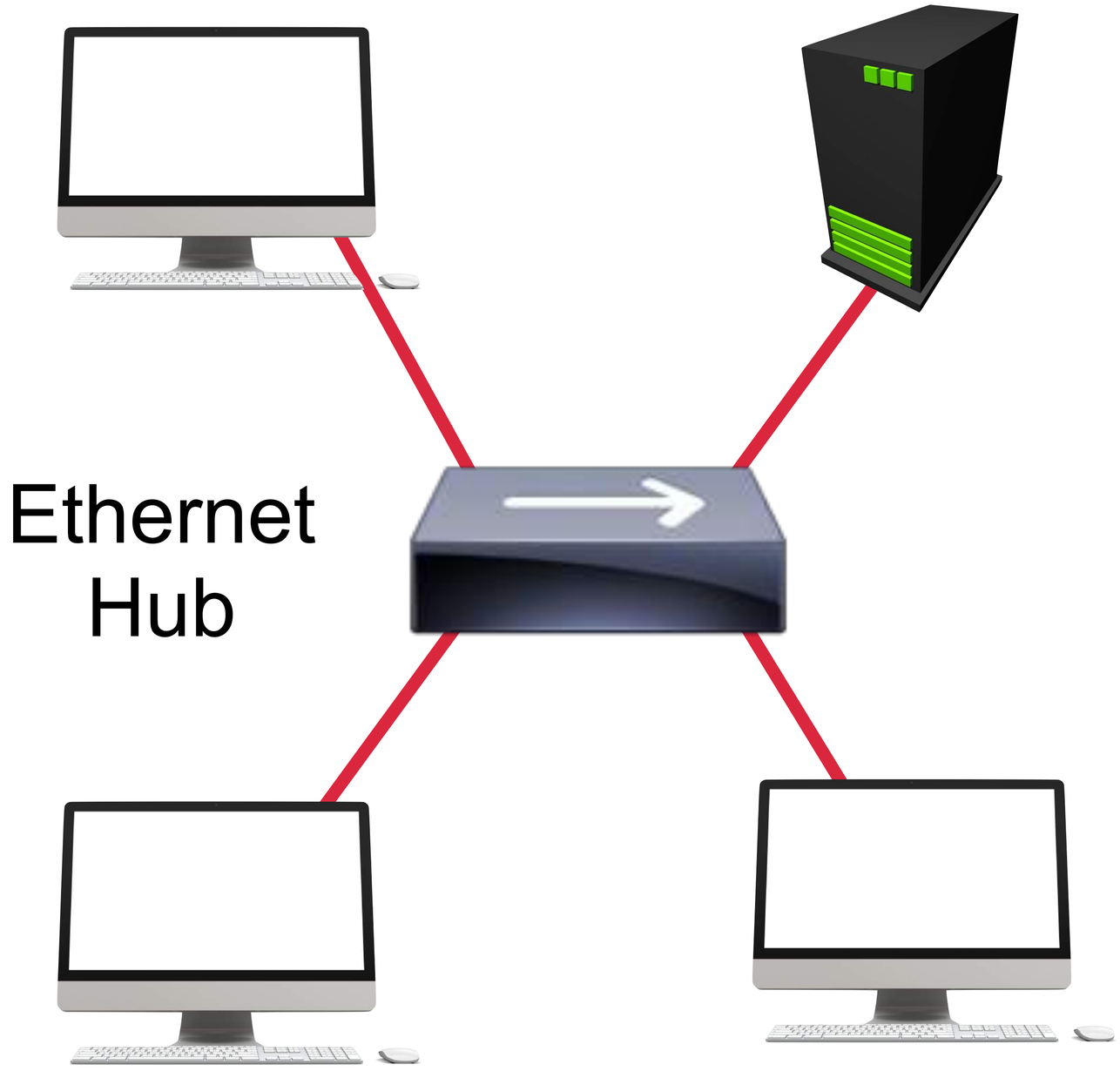


Router

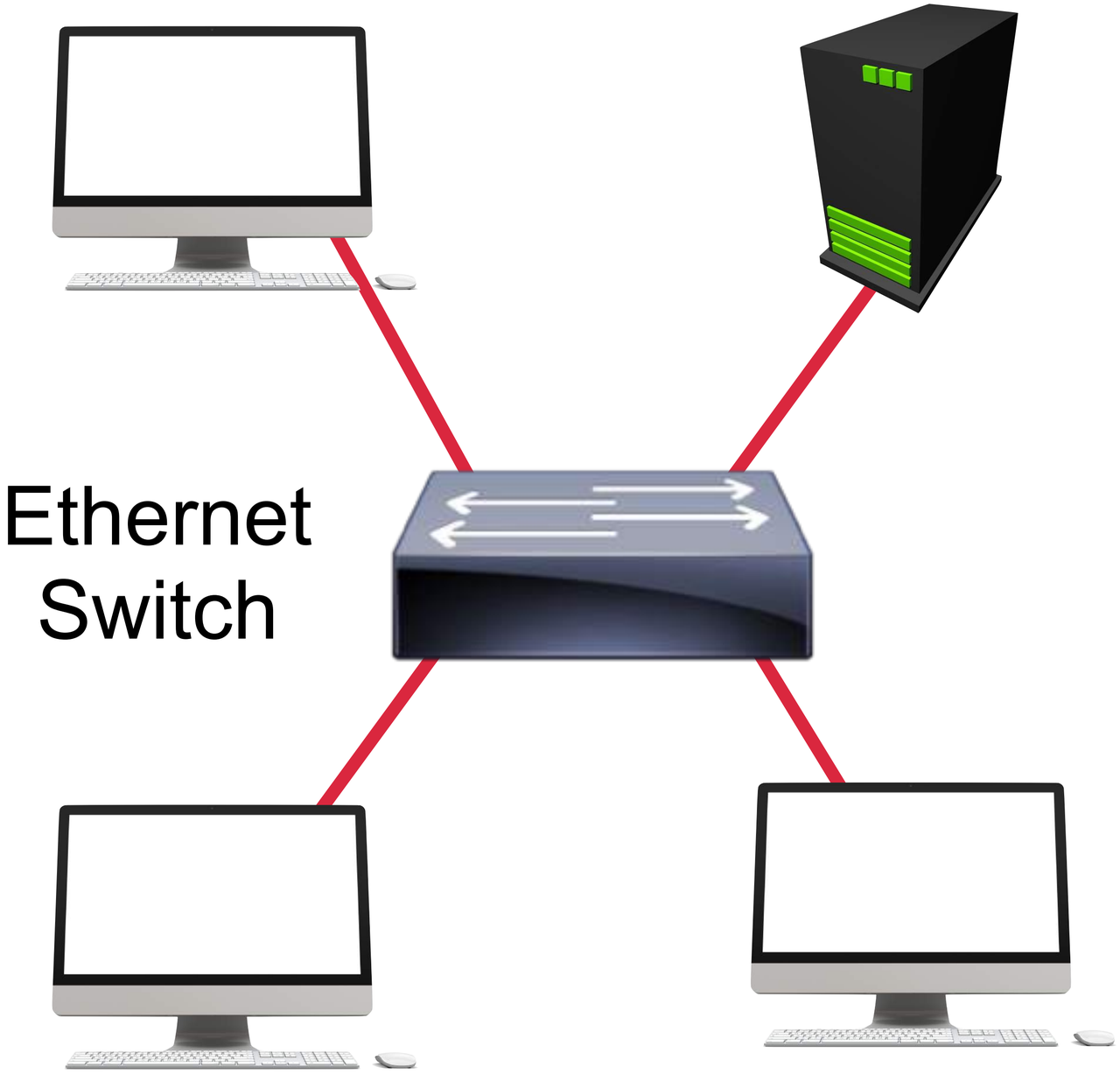
IPv4 Routing Table

Interface	Network
Gig 1	0.0.0.0 /0
Gig 2	10.1.1.0 /24
Gig 3	192.168.1.0 /24

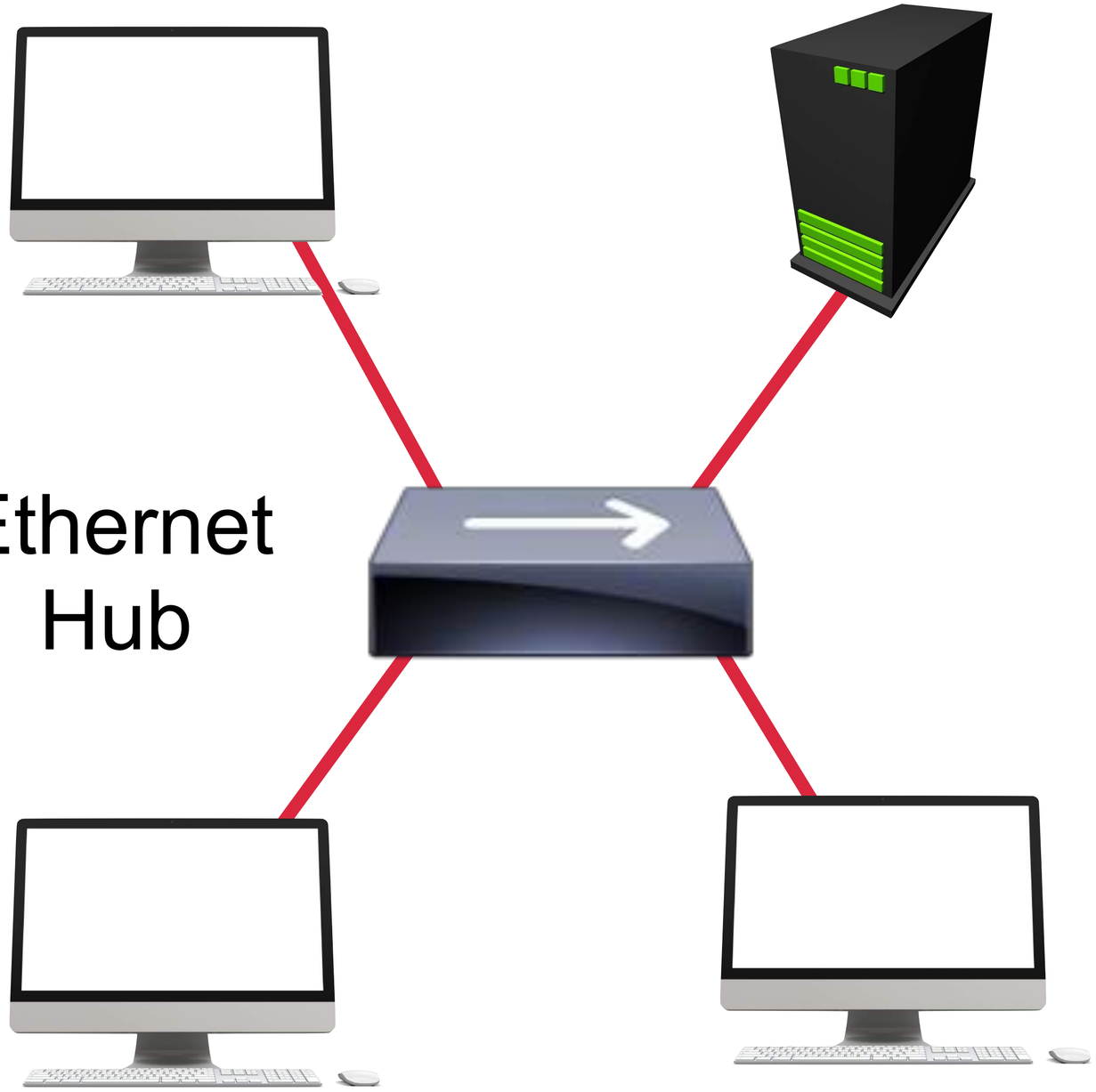




One Collision Domain

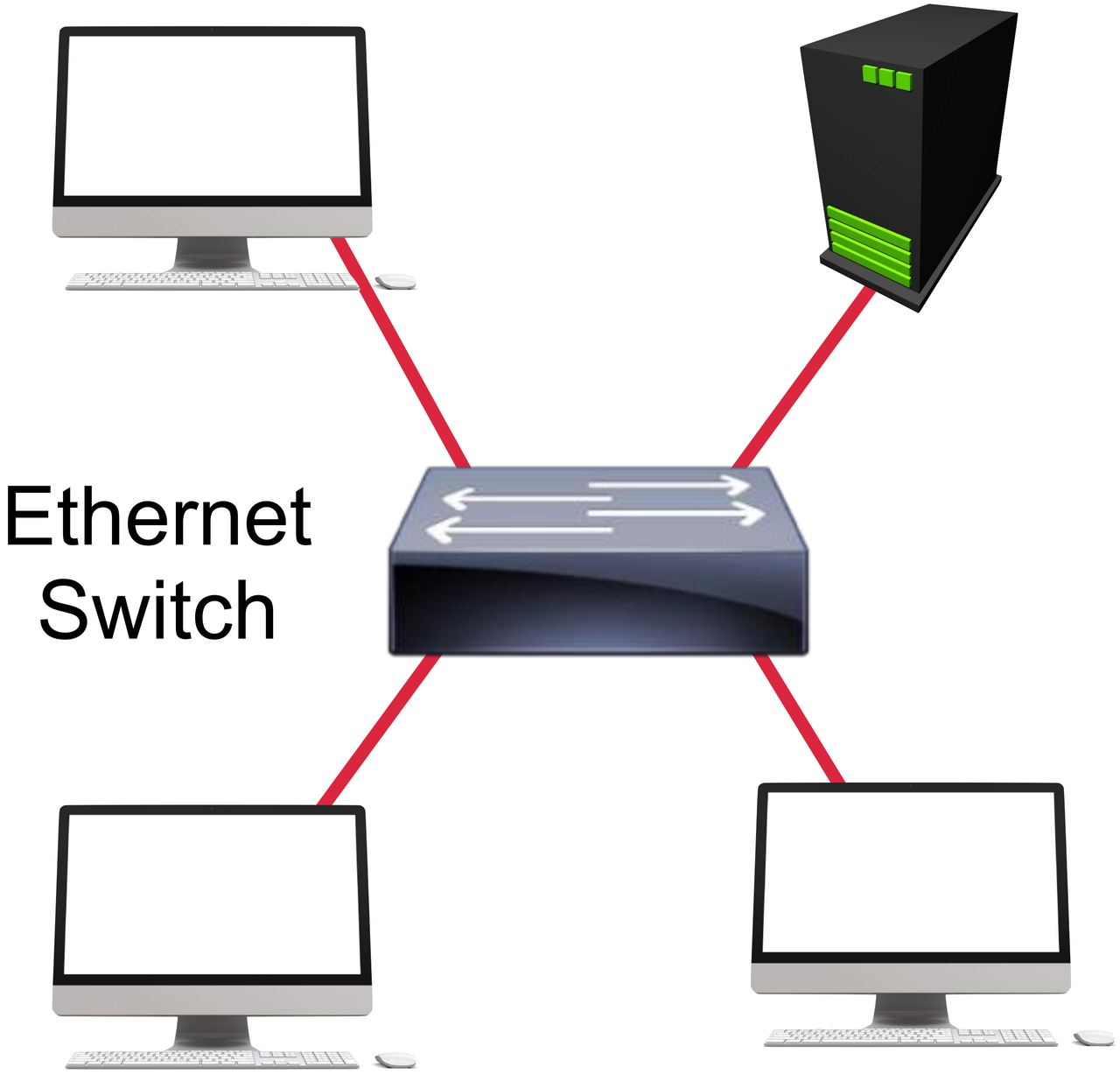


Four Collision Domains

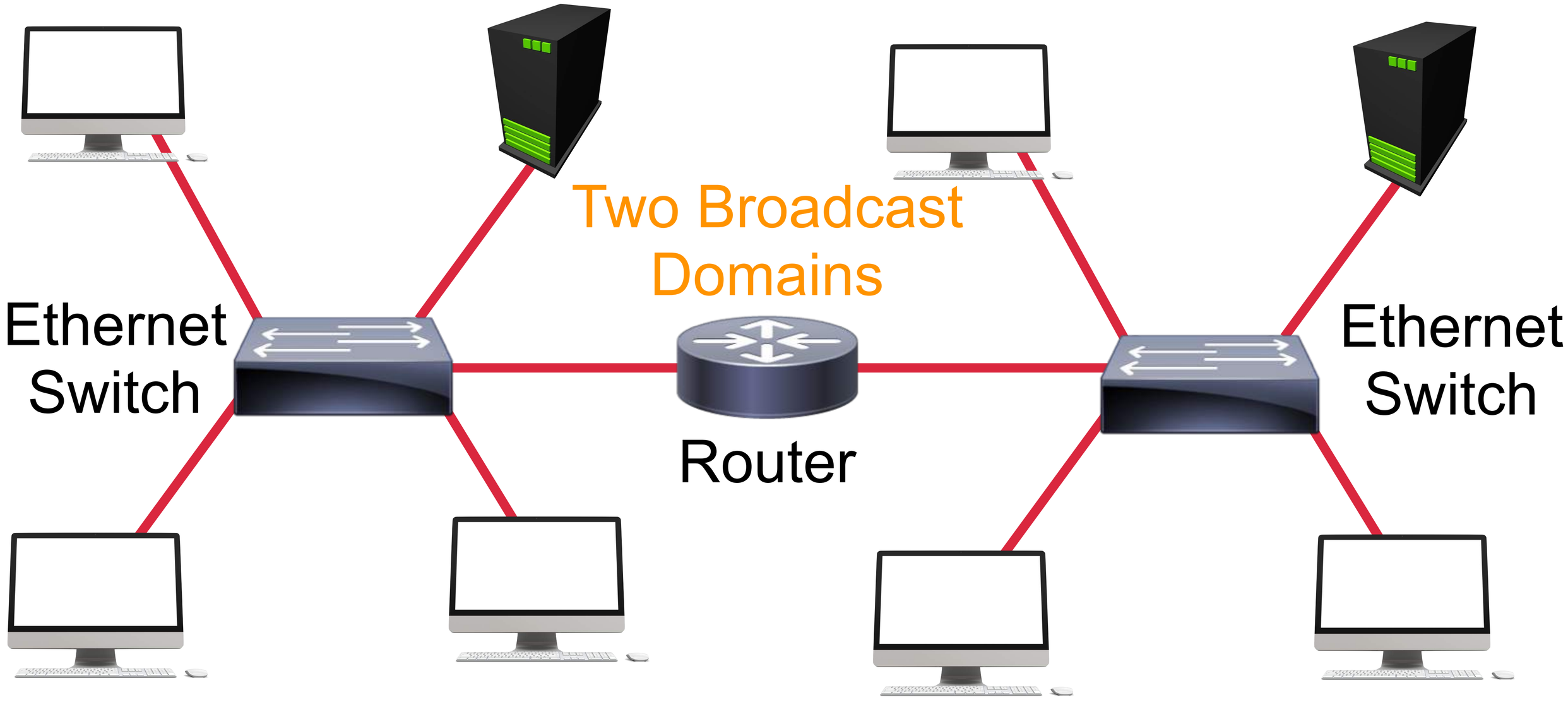


Ethernet Hub

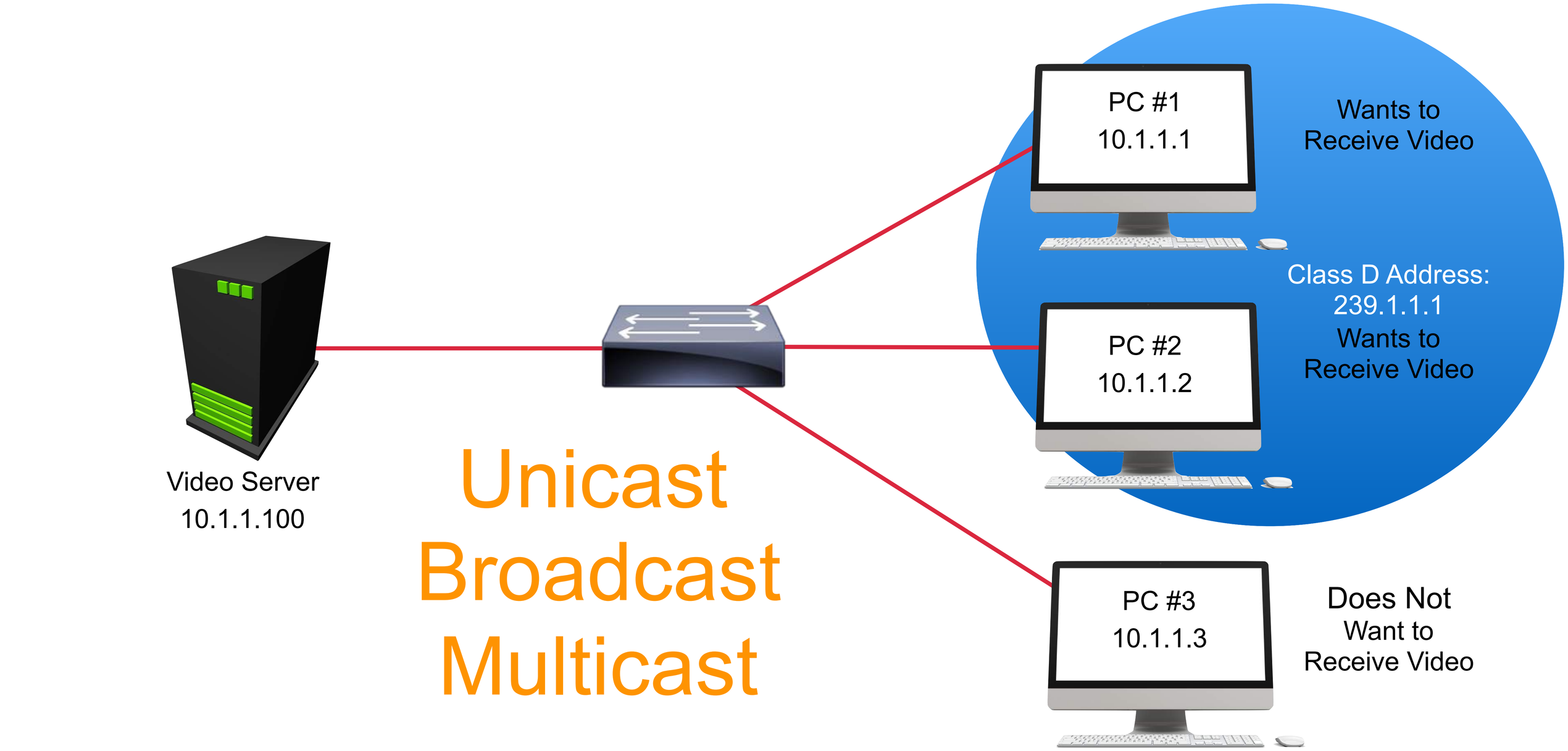
One Broadcast Domain



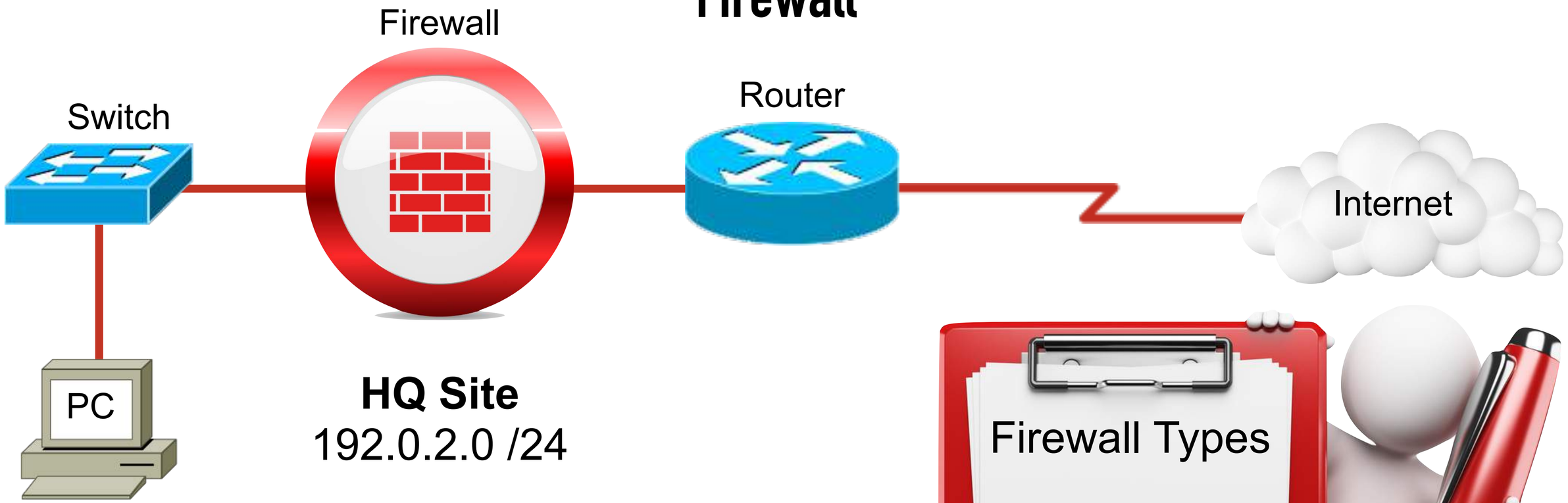
One Broadcast Domain


Two Broadcast Domains
Ethernet Switch
Router
Ethernet Switch

IPv4 Traffic Flows



Firewall

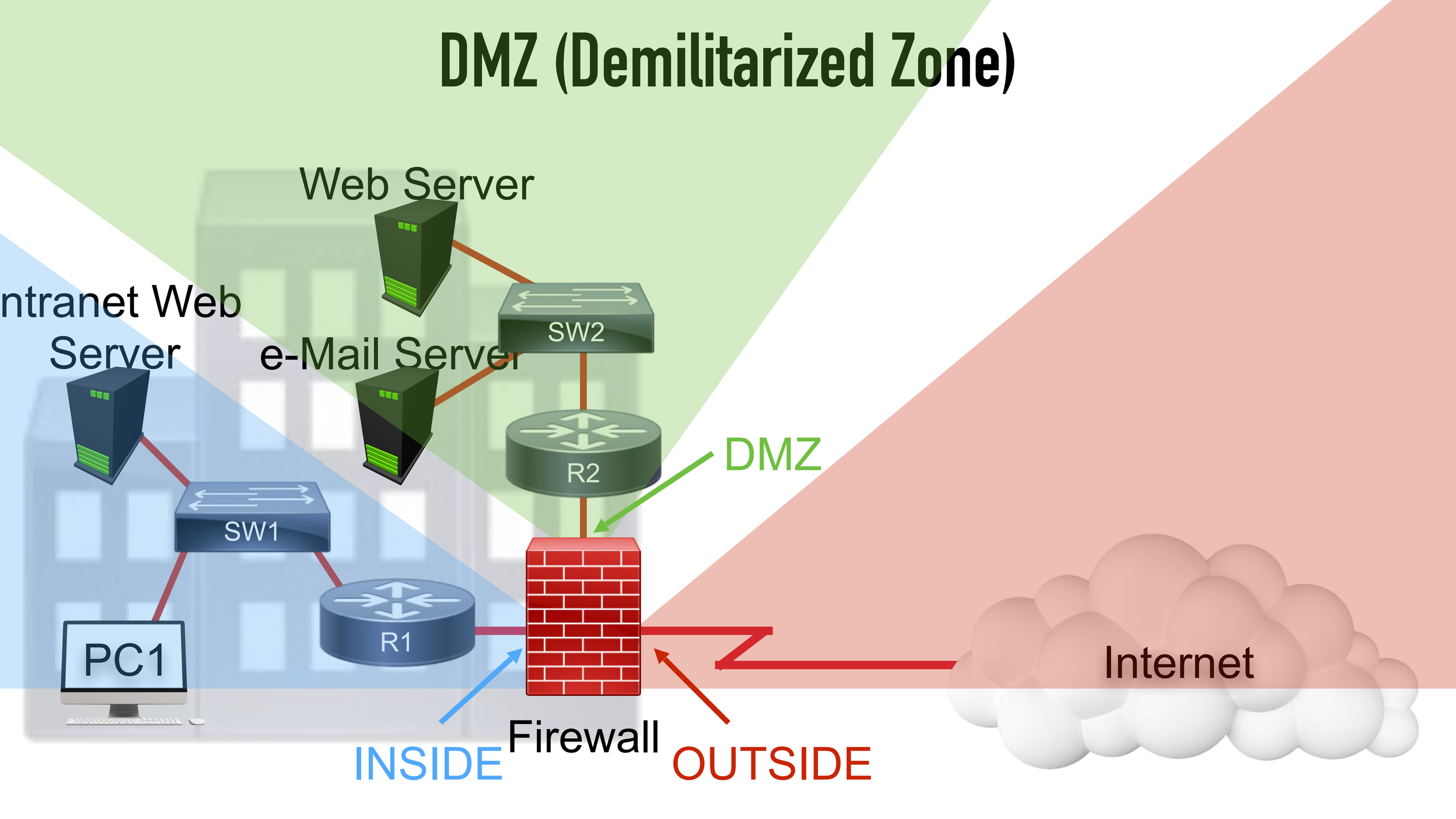


HQ Site
192.0.2.0 /24

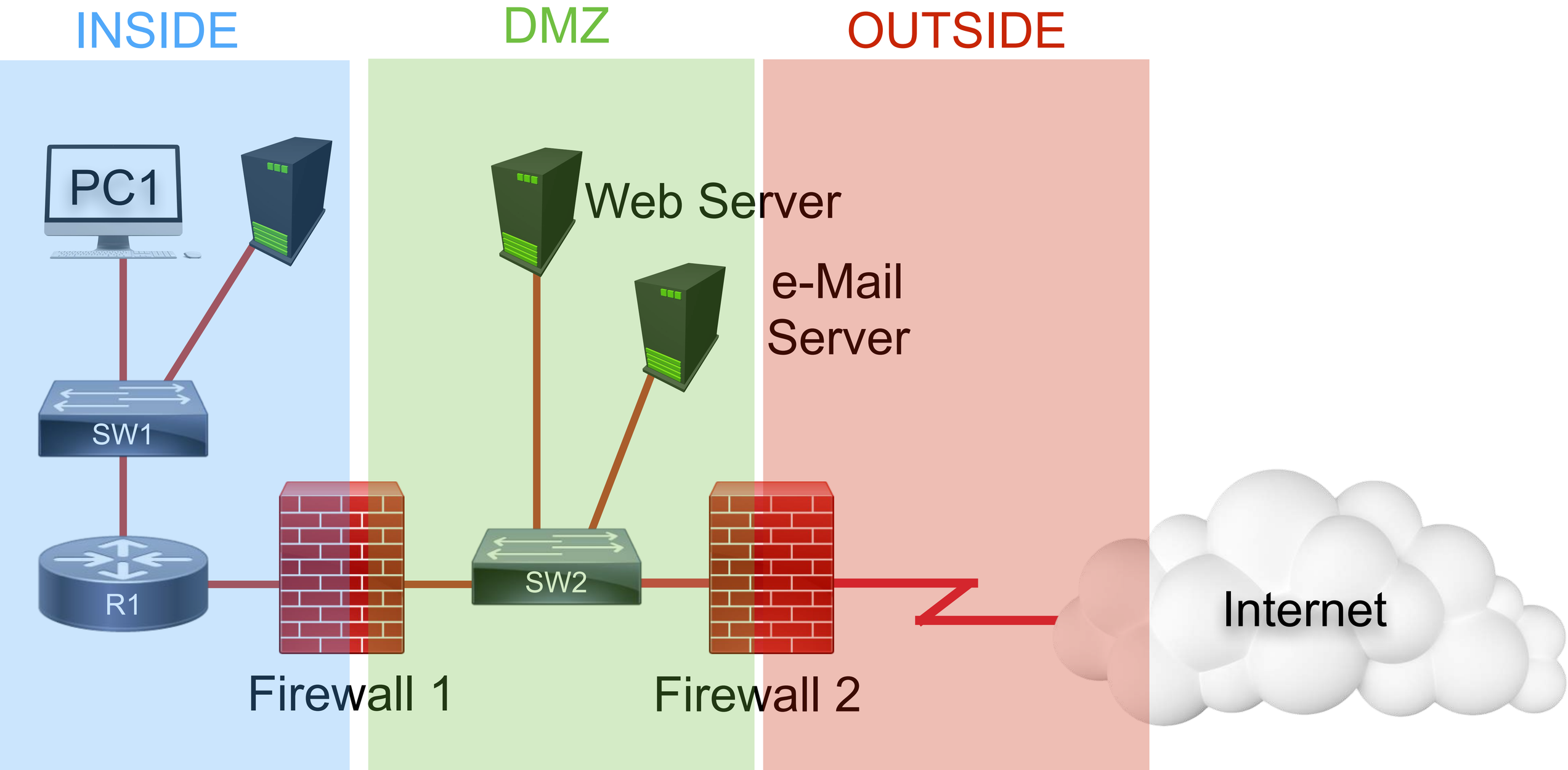
Rules

Source	Destination	Action
192.0.2.0 /24	Any - VoIP	Permit
Any	Any	Deny

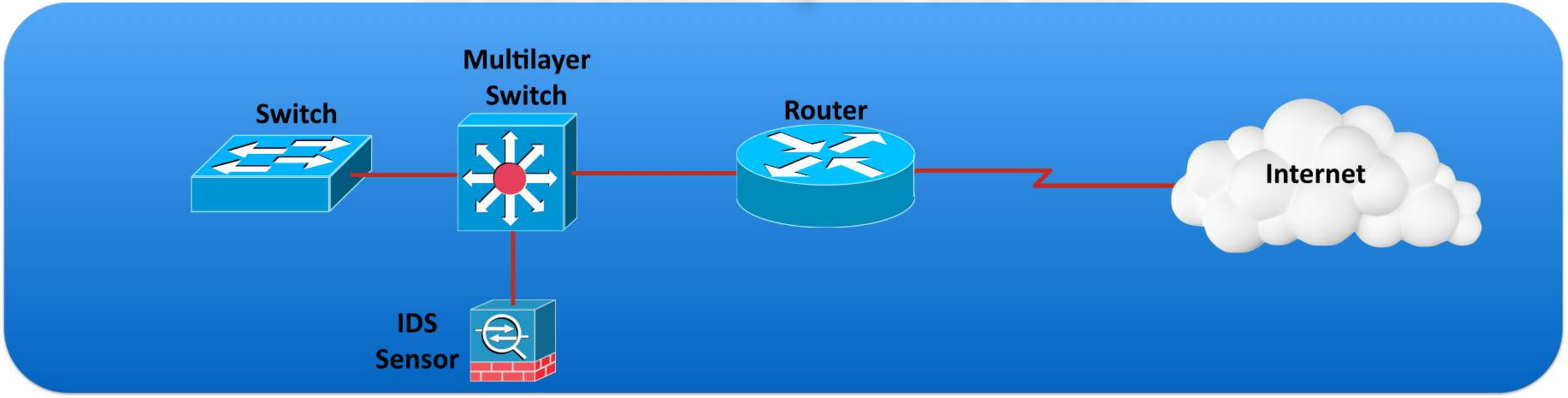
DMZ (Demilitarized Zone)



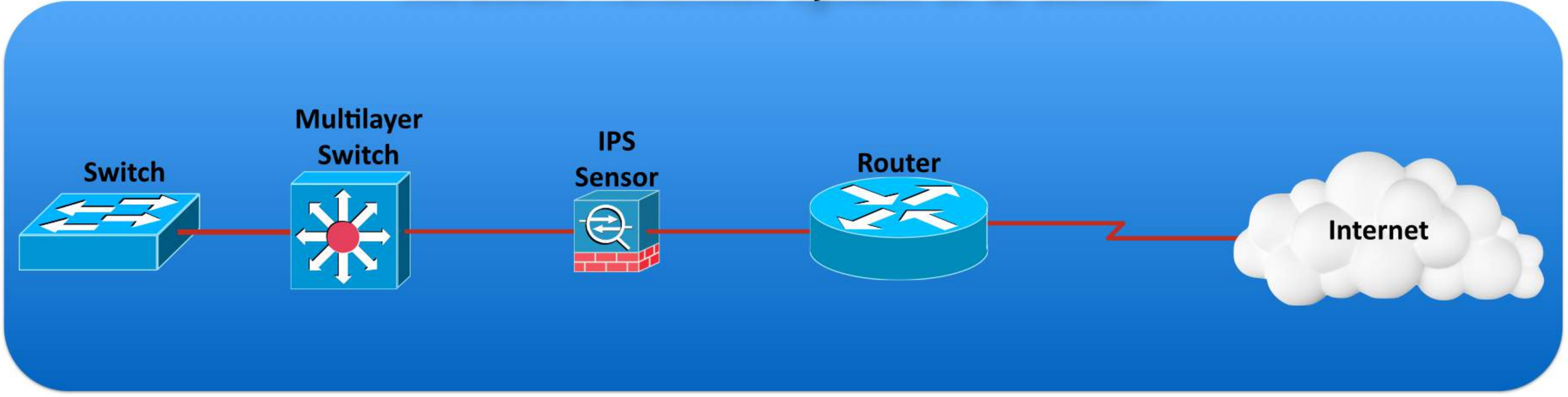
DMZ (Demilitarized Zone)



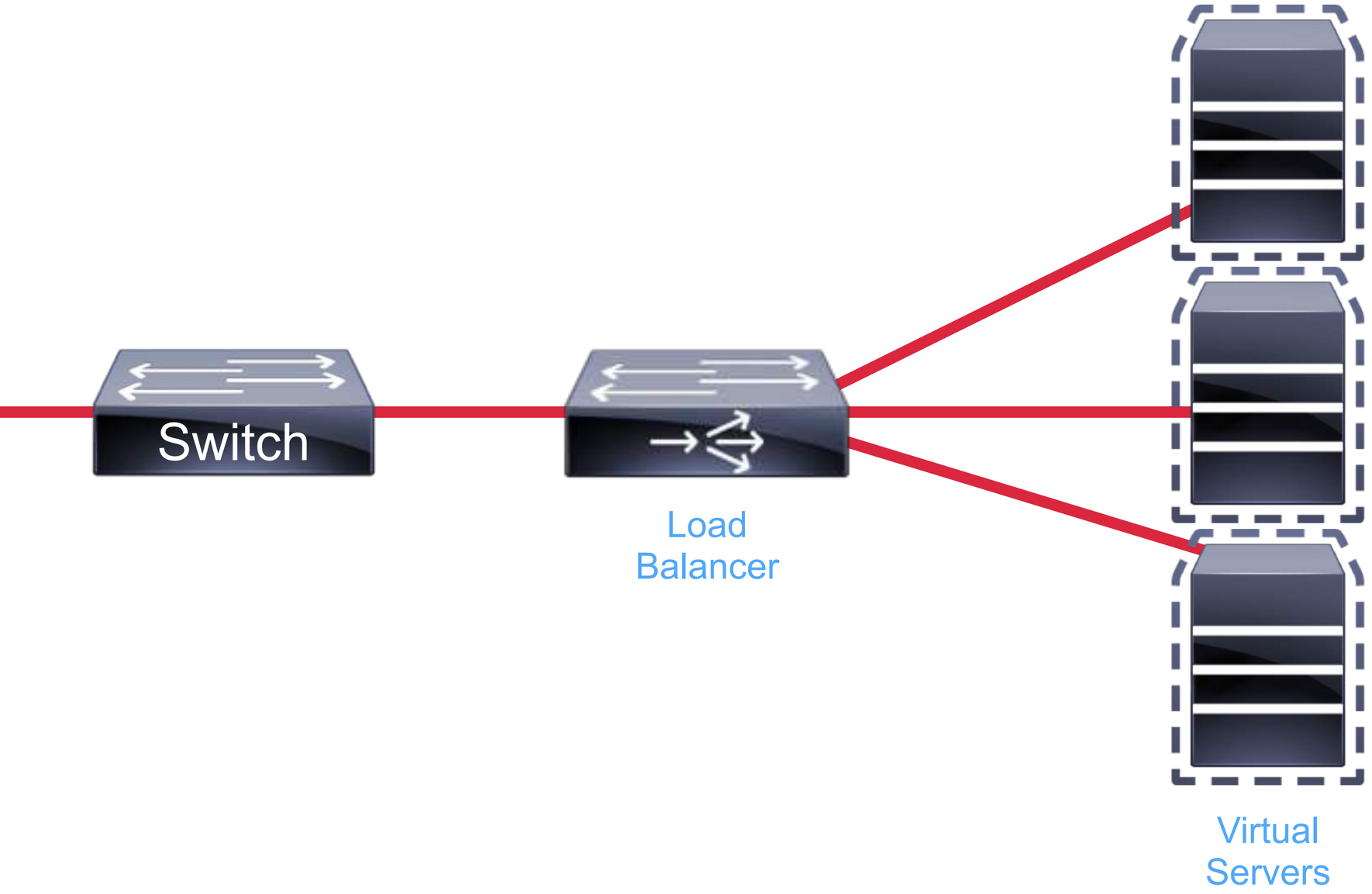
Intrusion Detection System (IDS) Sensor



Intrusion Prevention System (IPS) Sensor

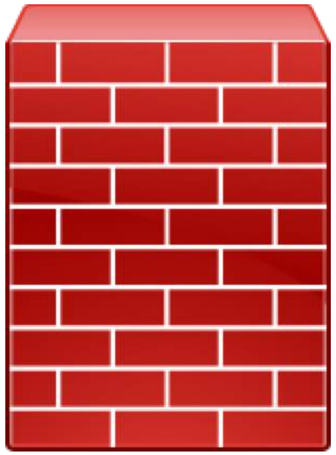


Load Balancer



- Servers with identical content
- Eases the processor/hard drive demand on a single server
- Allows individual servers to be removed from the load balancer's pool of servers (e.g. for maintenance)
- Allows "elastic" server capacity when used with virtual servers
- Could be a dedicated appliance or a router that supports load balancing

Advanced Filtering Appliances



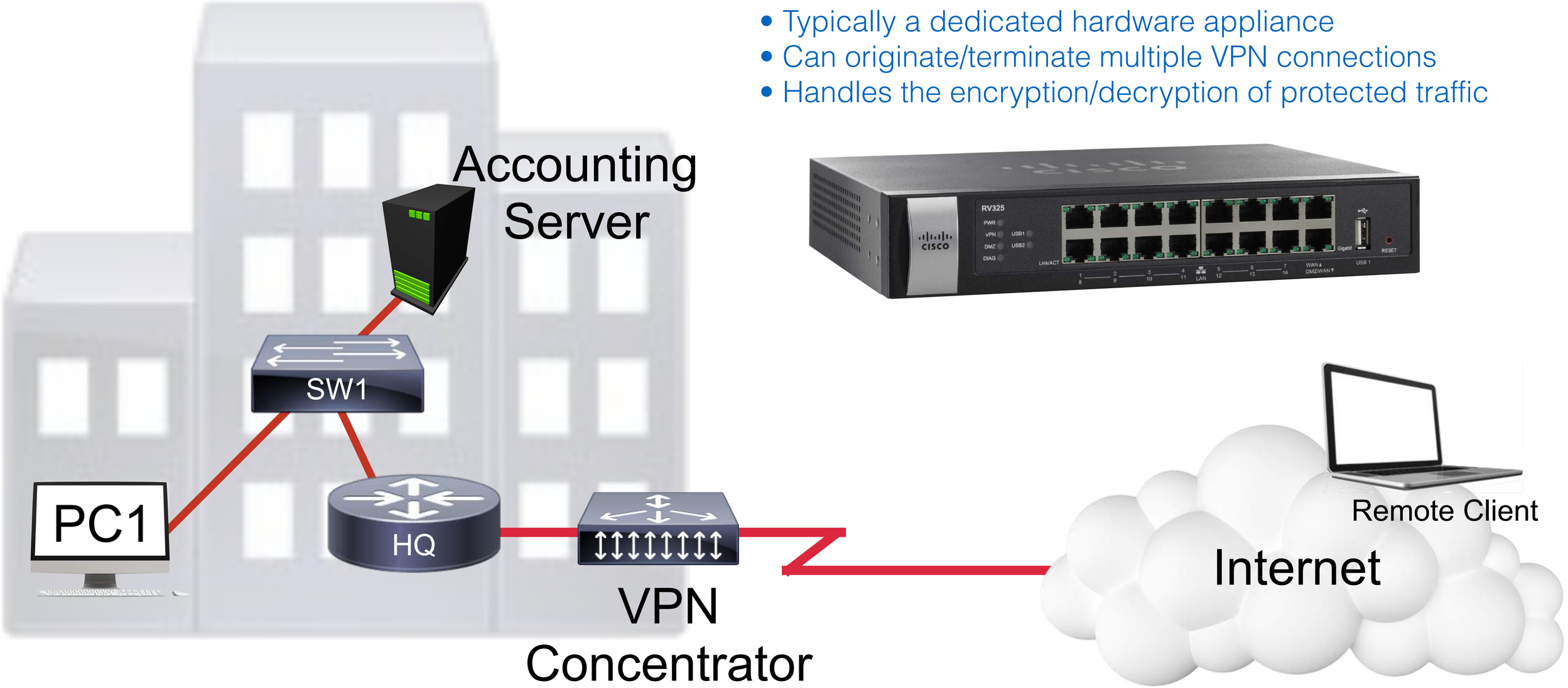
Next Generation Firewall (NGFW/Layer 7 Firewall): An Application Layer firewall with additional features, such as: Deep-Packet Inspection (DPI), Intrusion Prevention System (IPS), and encrypted traffic inspection.

Content Filter: Could be software (e.g. used by parents) or an appliance (e.g. used by enterprises) used to filter traffic thought to be objectionable.

Unified Threat Management (UTM) Appliance: A dedicated appliance that combines multiple filtering functions, such as: Firewall, IPS, Anti-Malware, VPN, and Content Filter.

VPN Concentrator

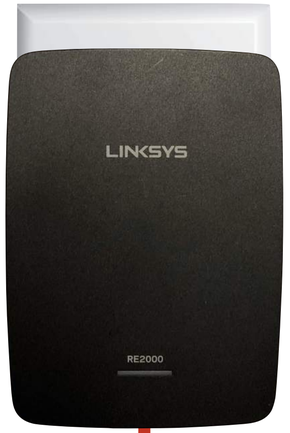
- Typically a dedicated hardware appliance
- Can originate/terminate multiple VPN connections
- Handles the encryption/decryption of protected traffic



Wireless Range Extender

Wireless Access Point

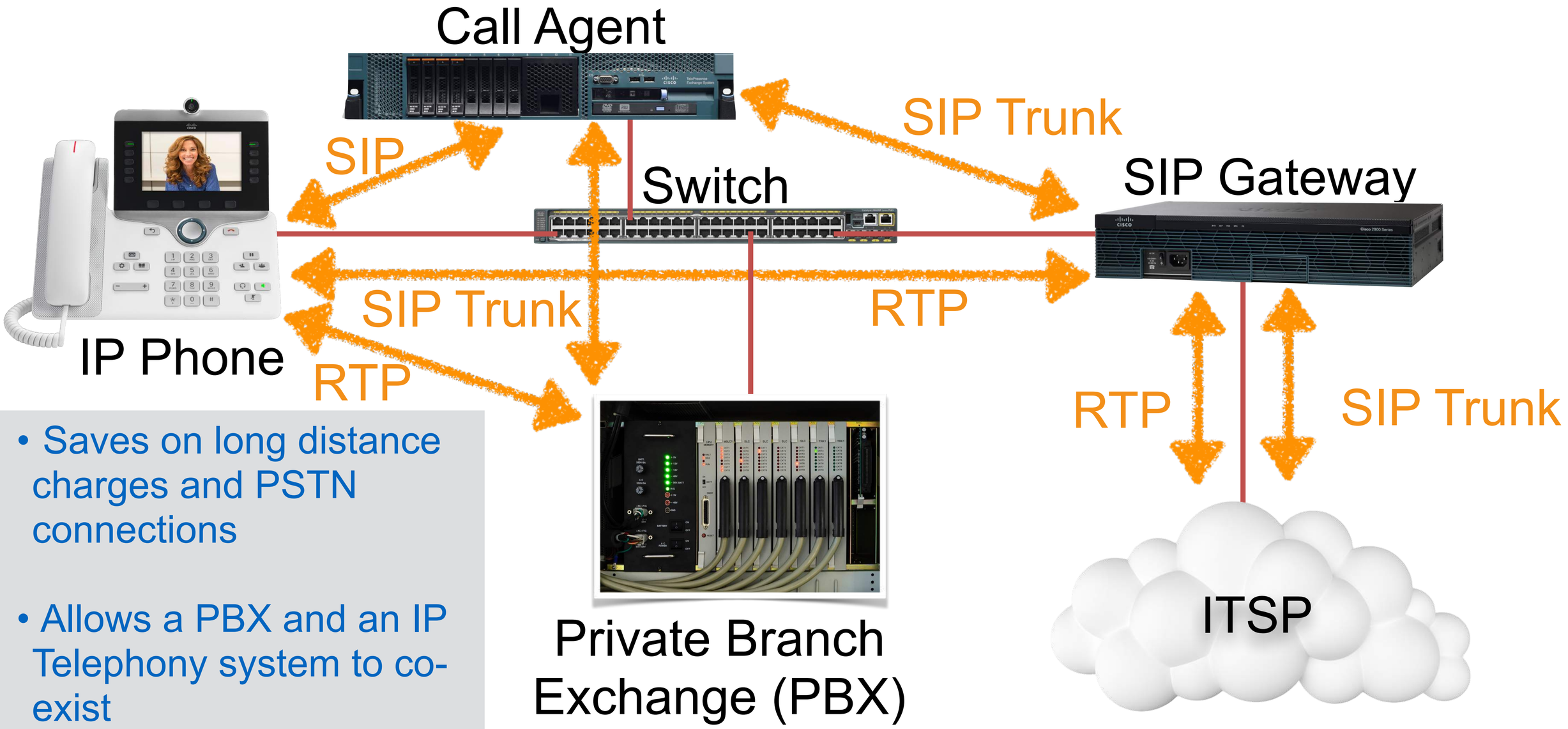
Wireless Range Extender



Printer

Client

SIP Trunks

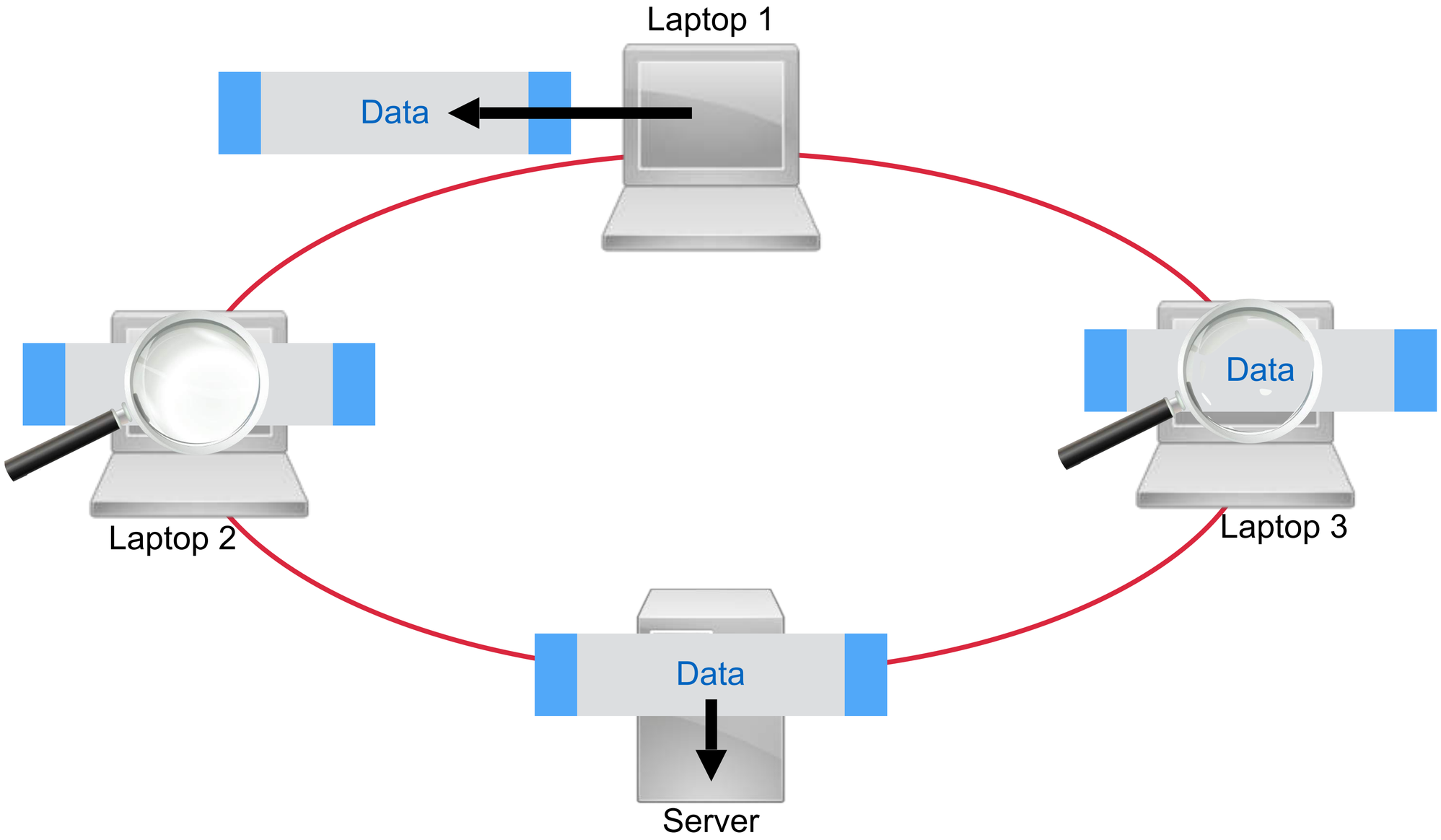


- Saves on long distance charges and PSTN connections
- Allows a PBX and an IP Telephony system to co-exist

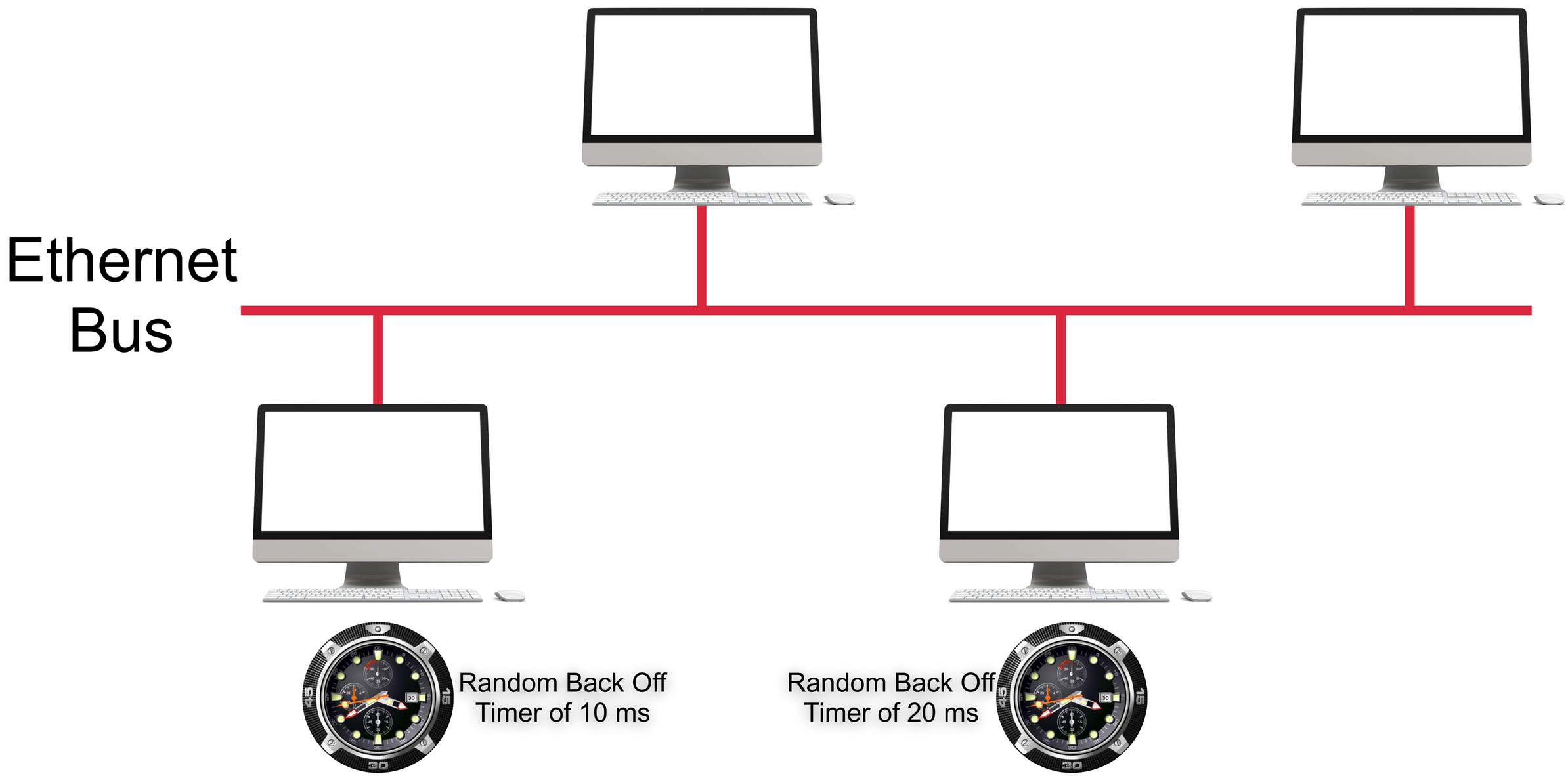
Module 2
Network Devices

Module 3
Network Topologies and Categories

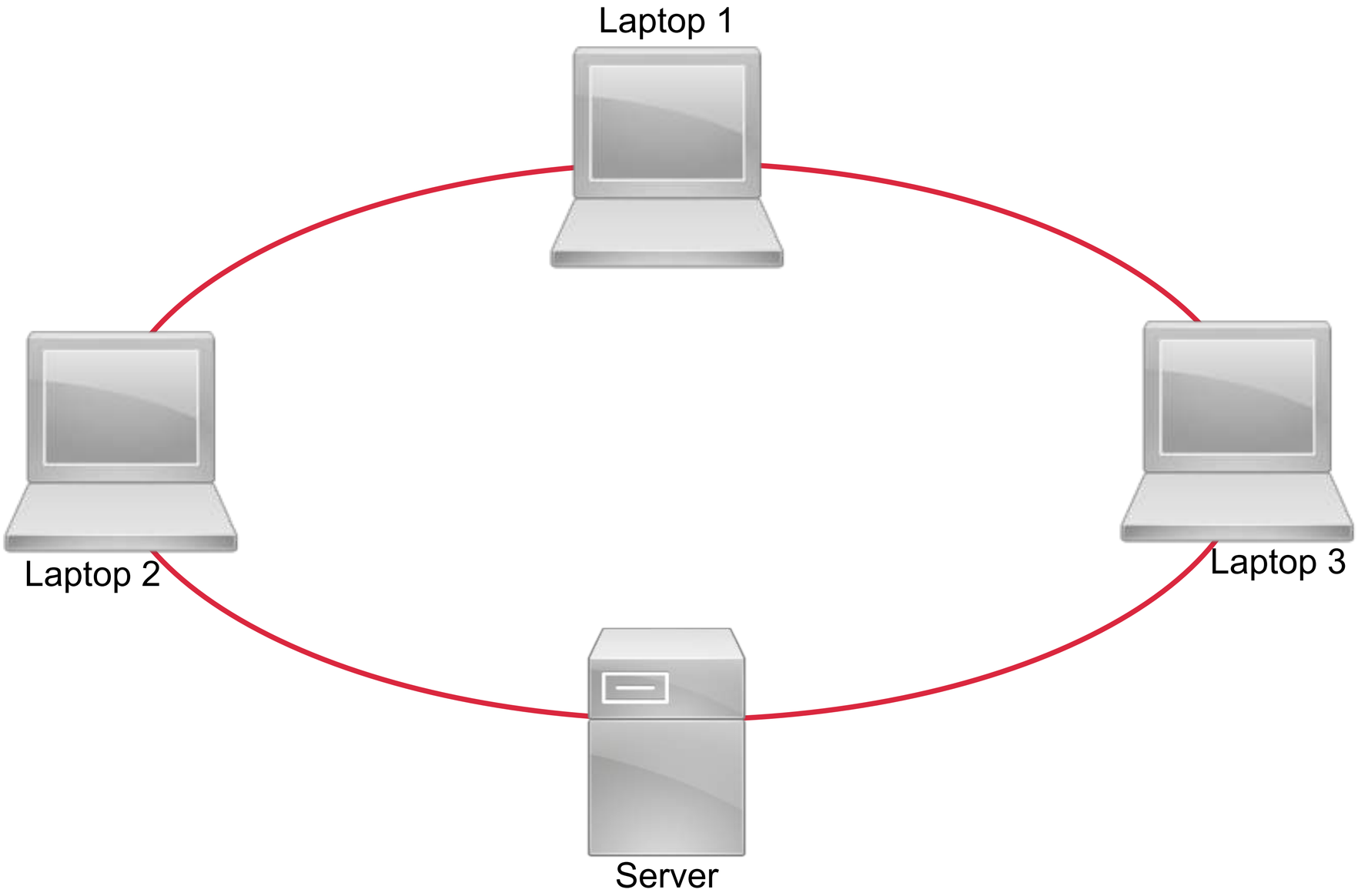
Ring Topology



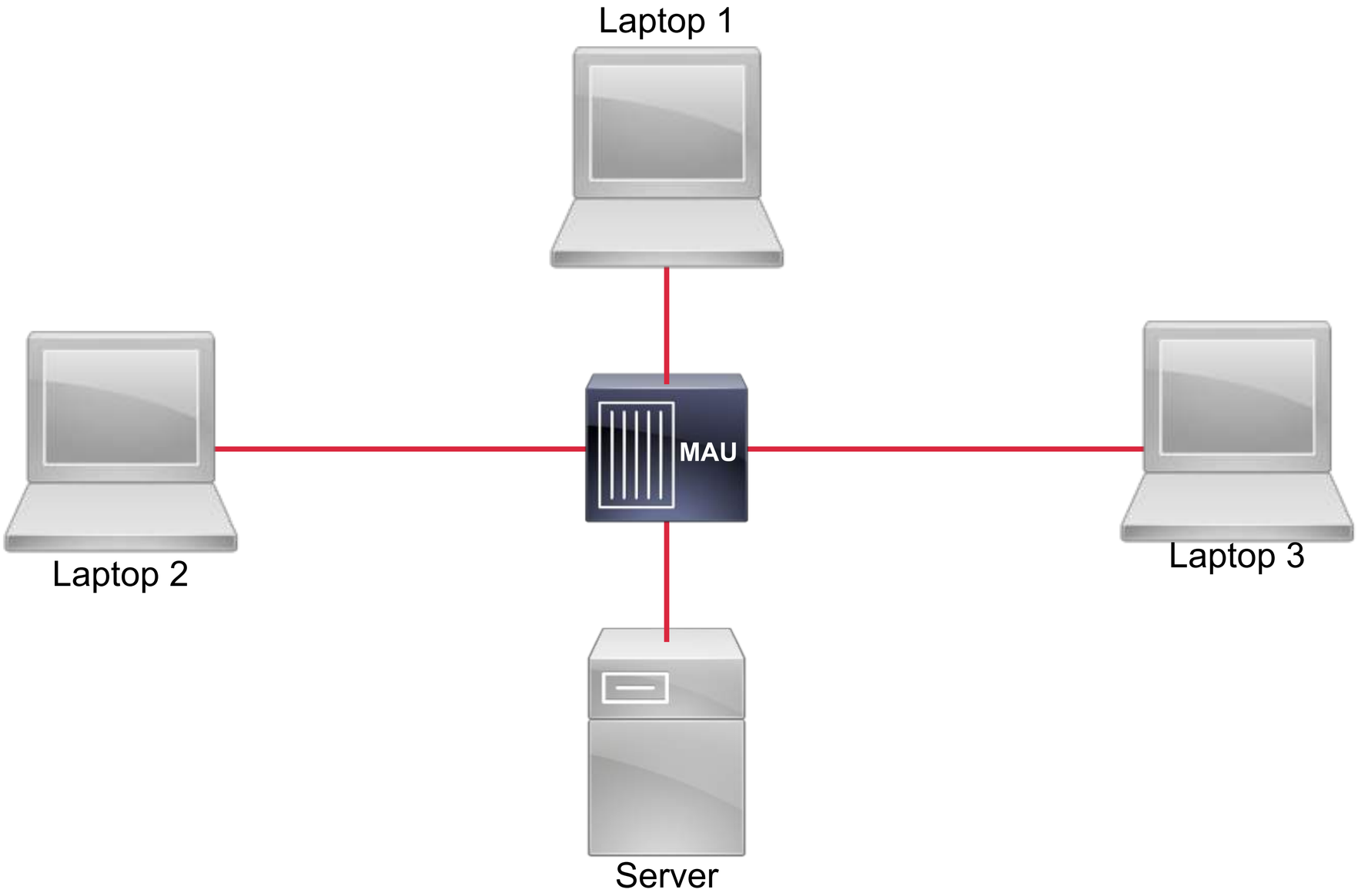
Bus Topology



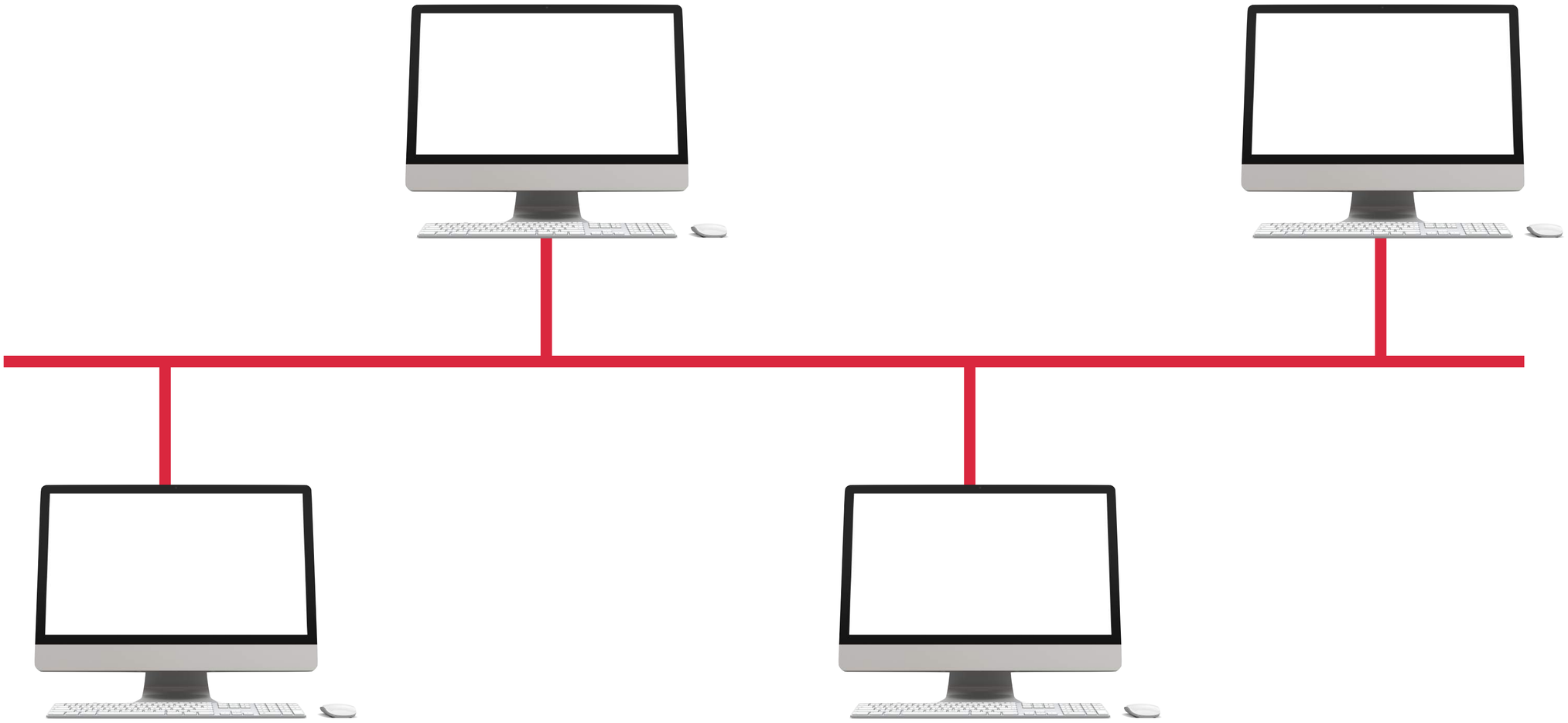
Logical vs. Physical Topologies



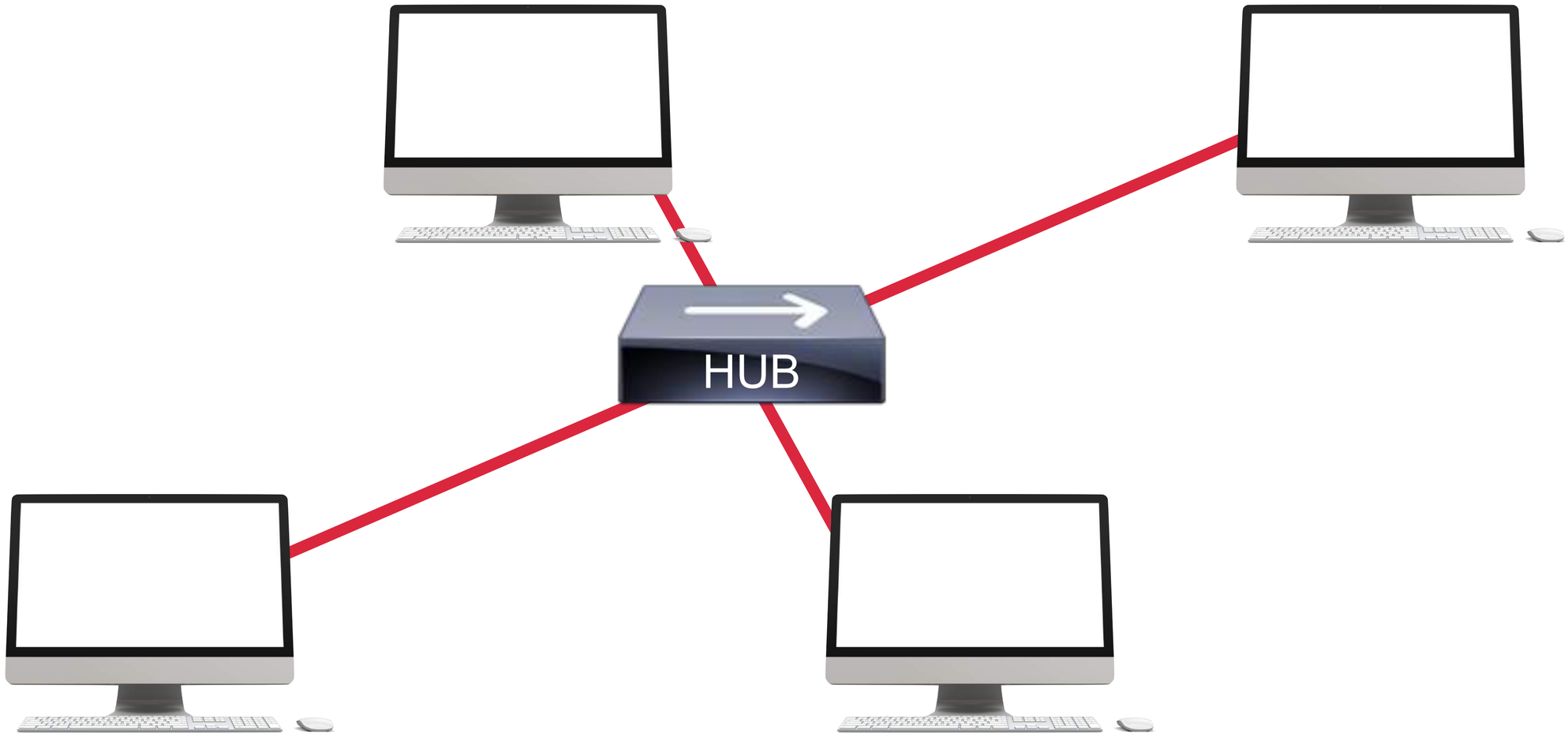
Logical vs. Physical Topologies



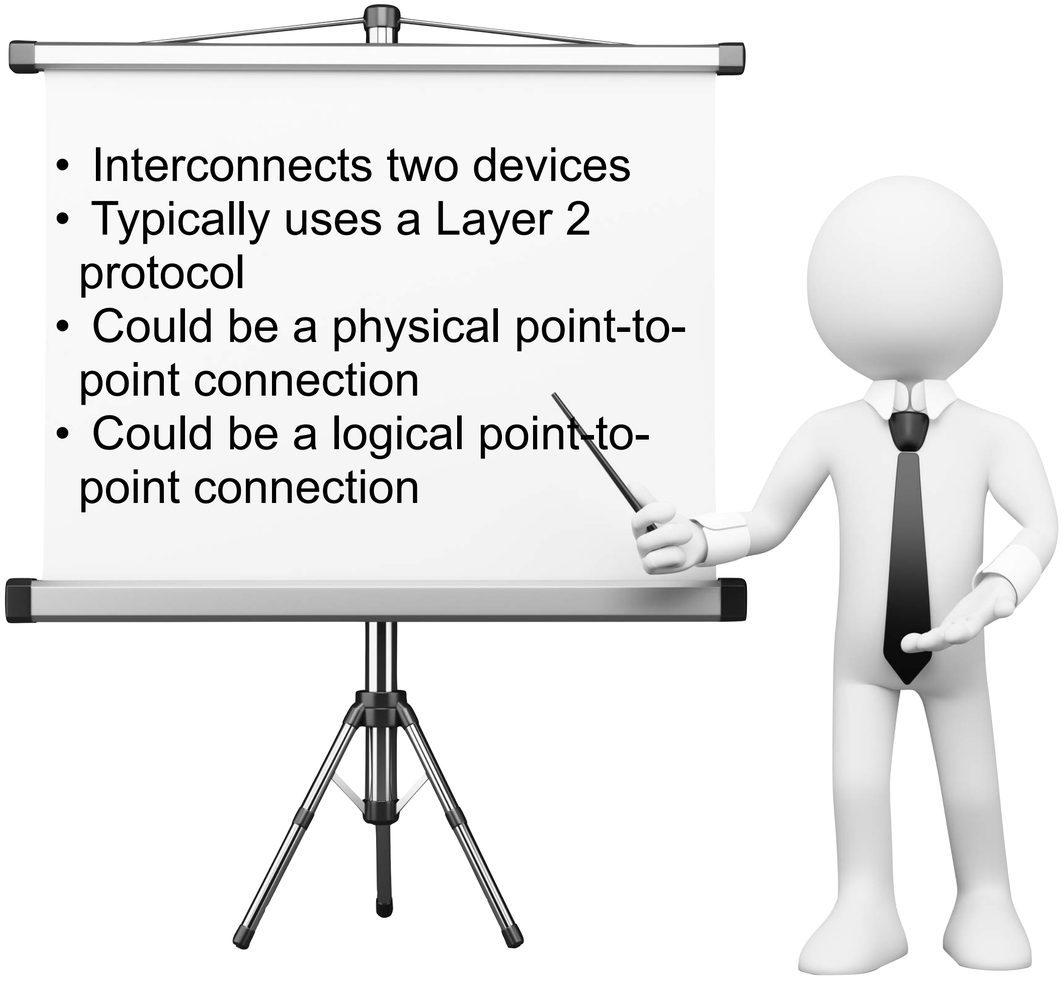
Logical vs. Physical Topologies



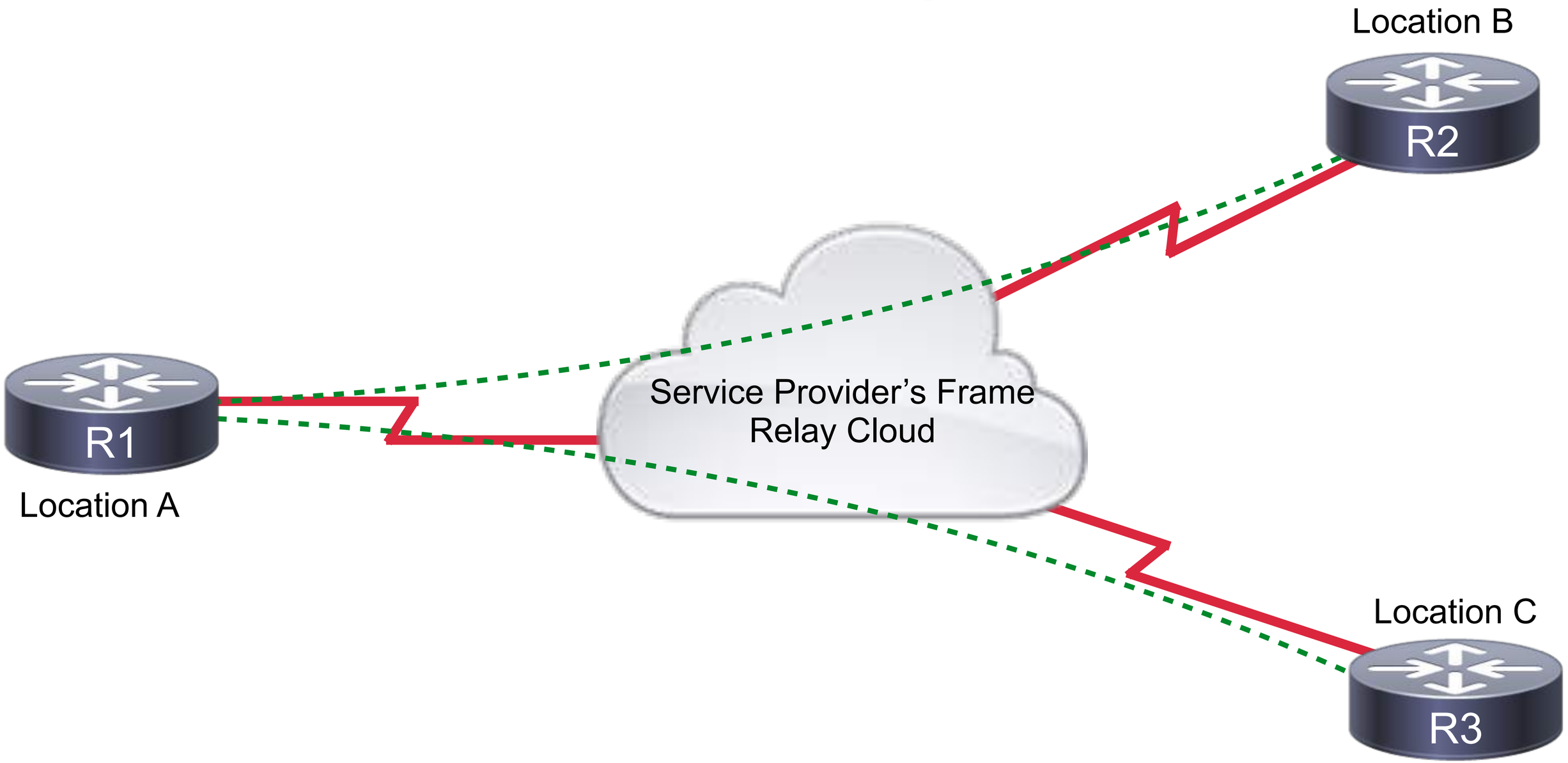
Logical vs. Physical Topologies



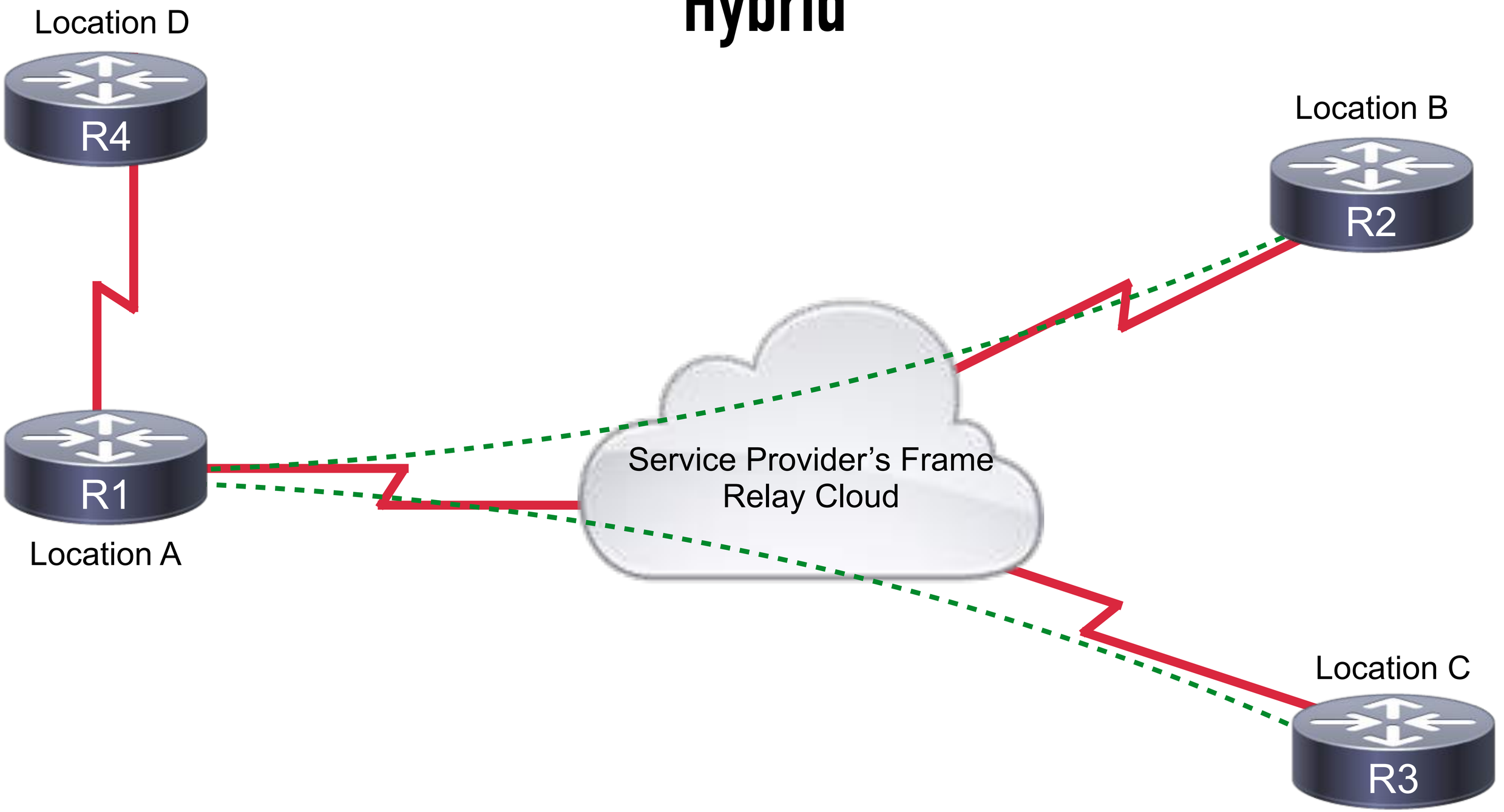
Point-to-Point



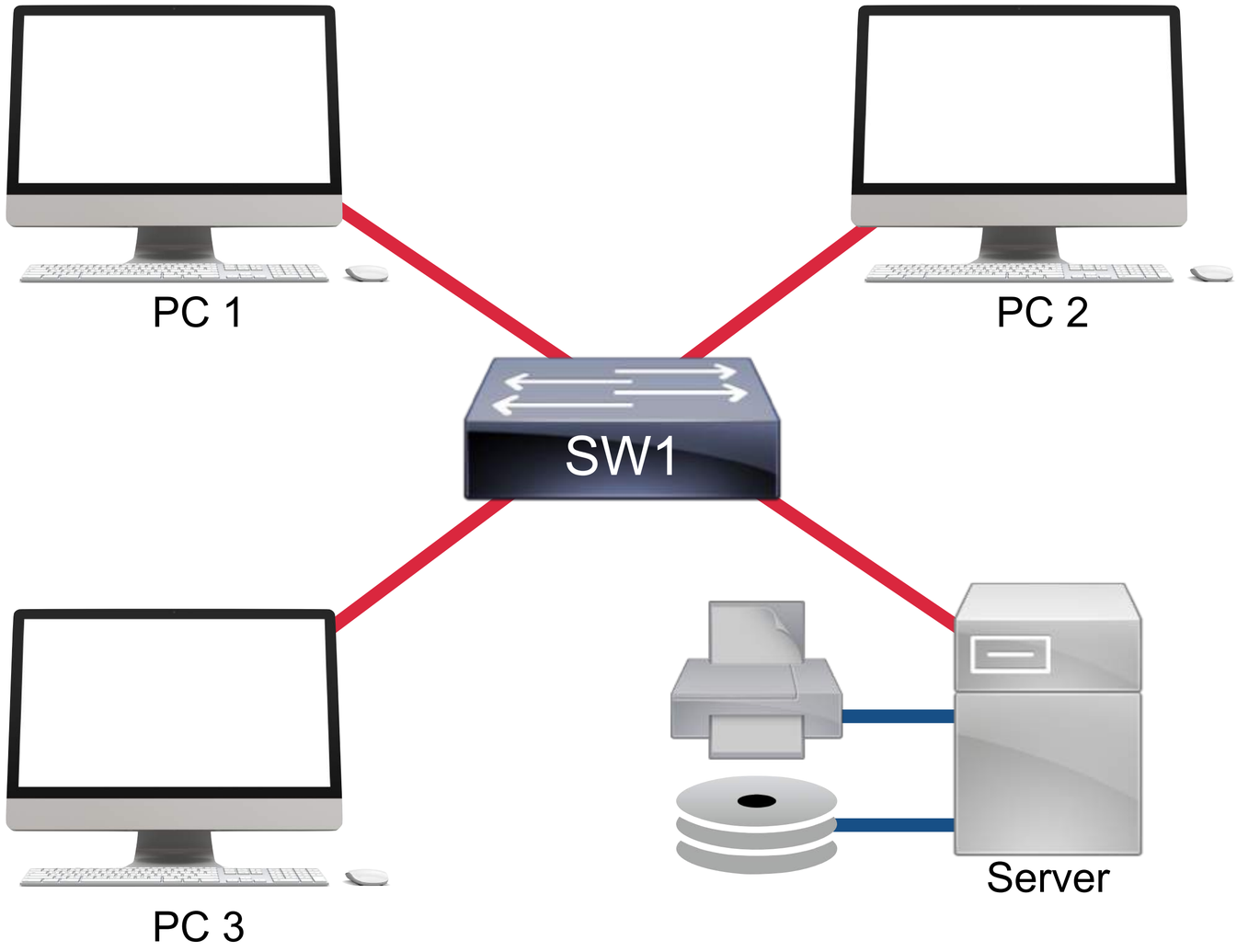
Point-to-Multipoint



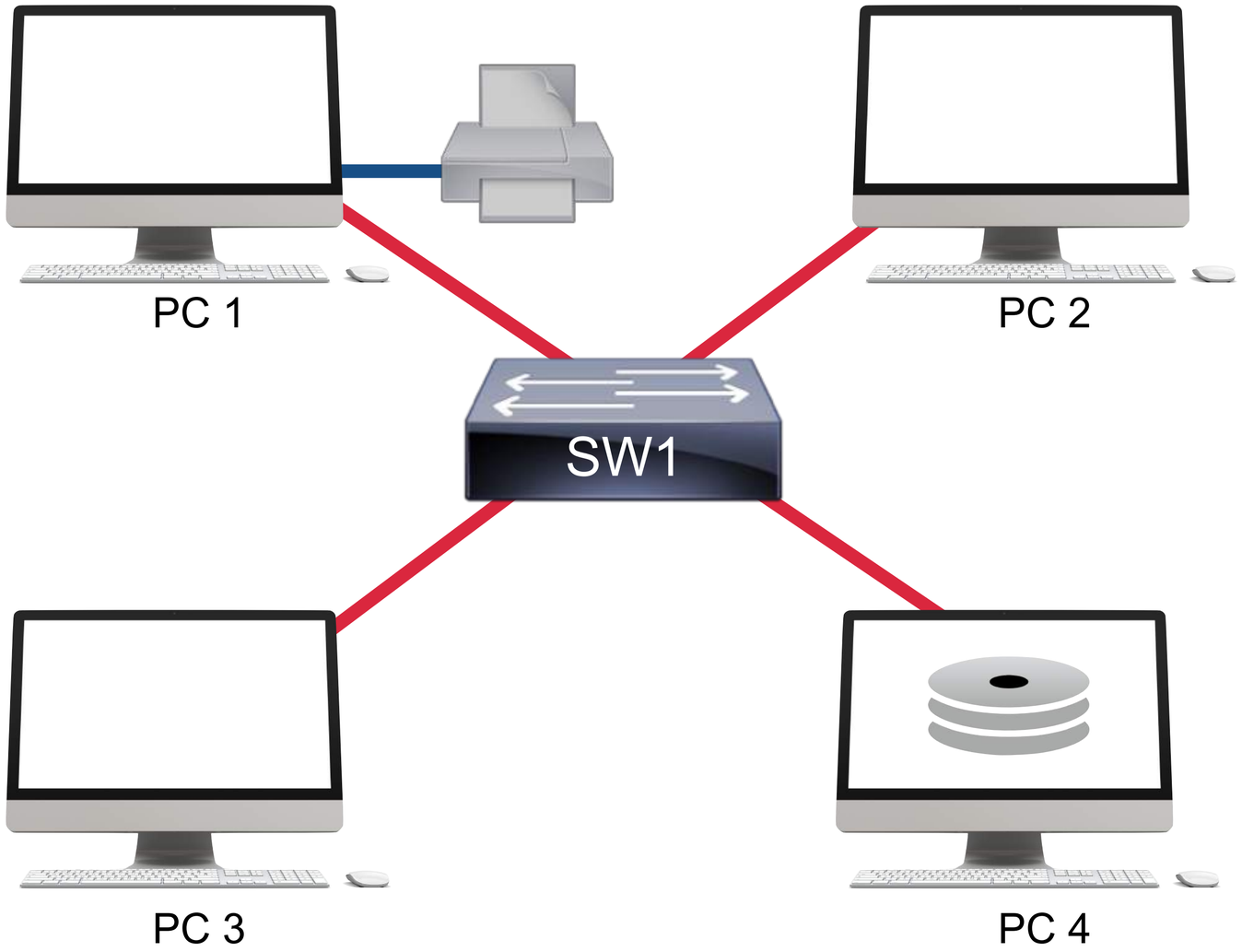
Hybrid

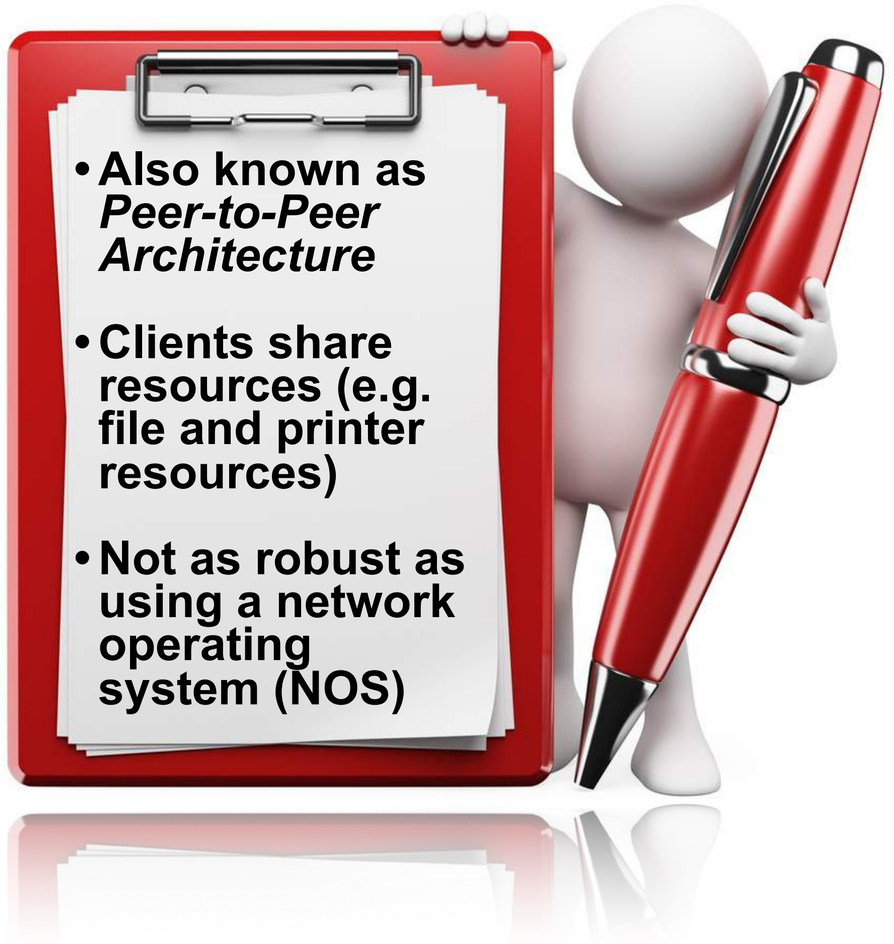

Location D
R4
Location B
R2
R1
Location A
Service Provider's Frame Relay Cloud
Location C
R3

Client-Server Network

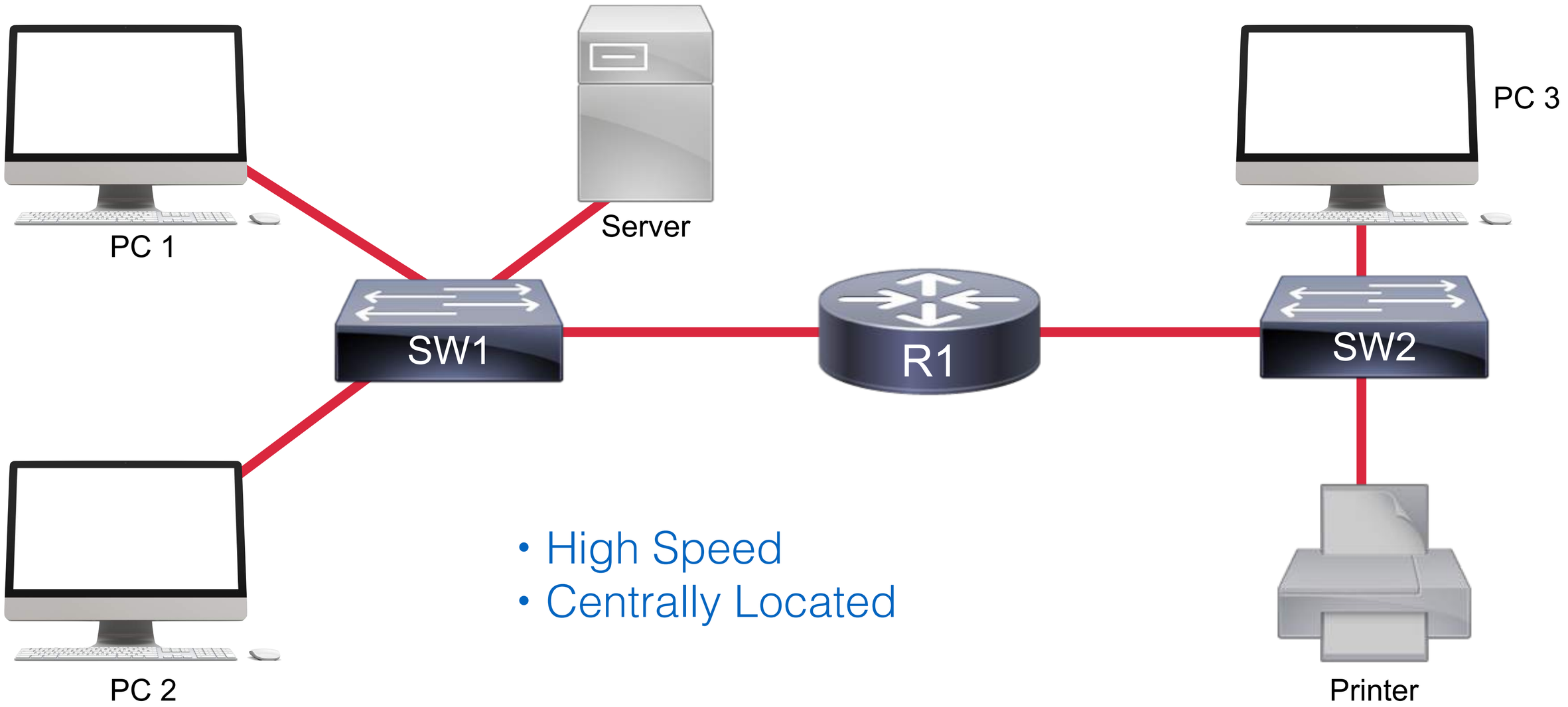


Peer-to-Peer Network



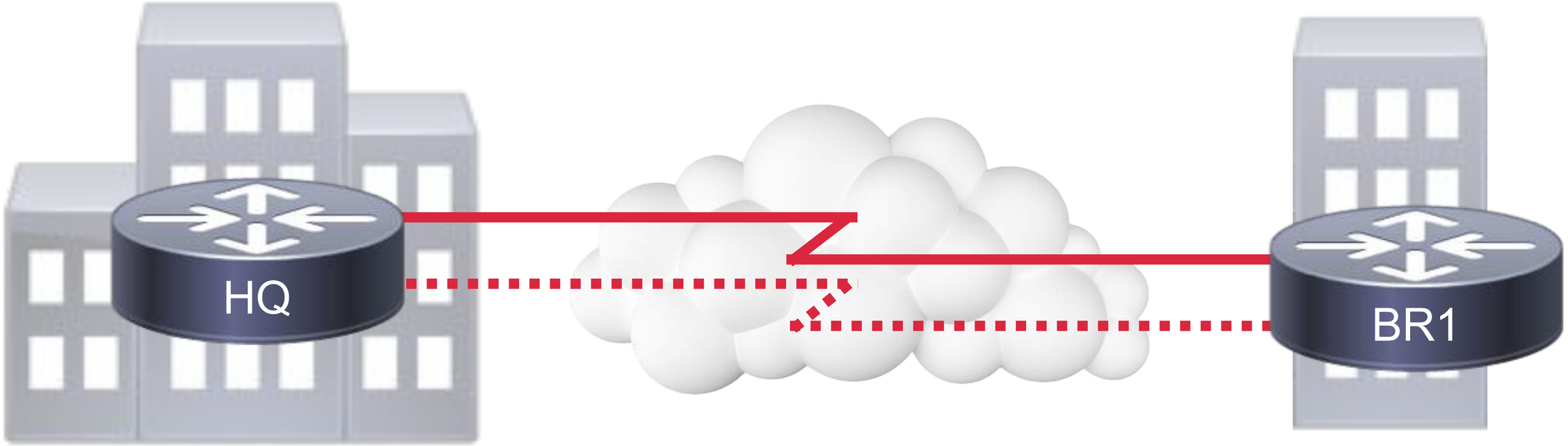


Local Area Network (LAN)



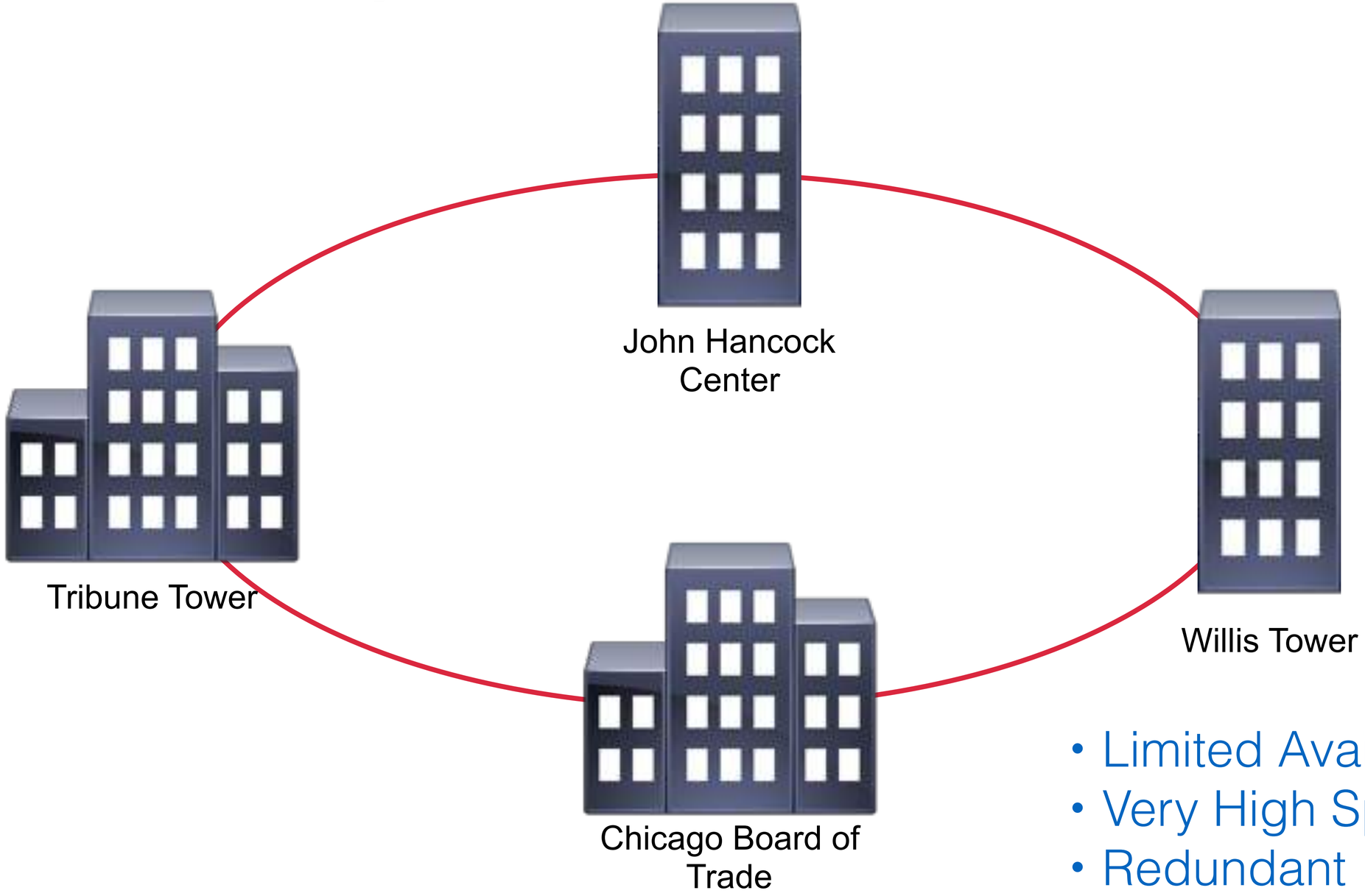
- High Speed
- Centrally Located

Wide Area Network (WAN)



- Typically Slower Speed than LANs
- Geographically Dispersed Sites
- Sites Connect to Service Provider

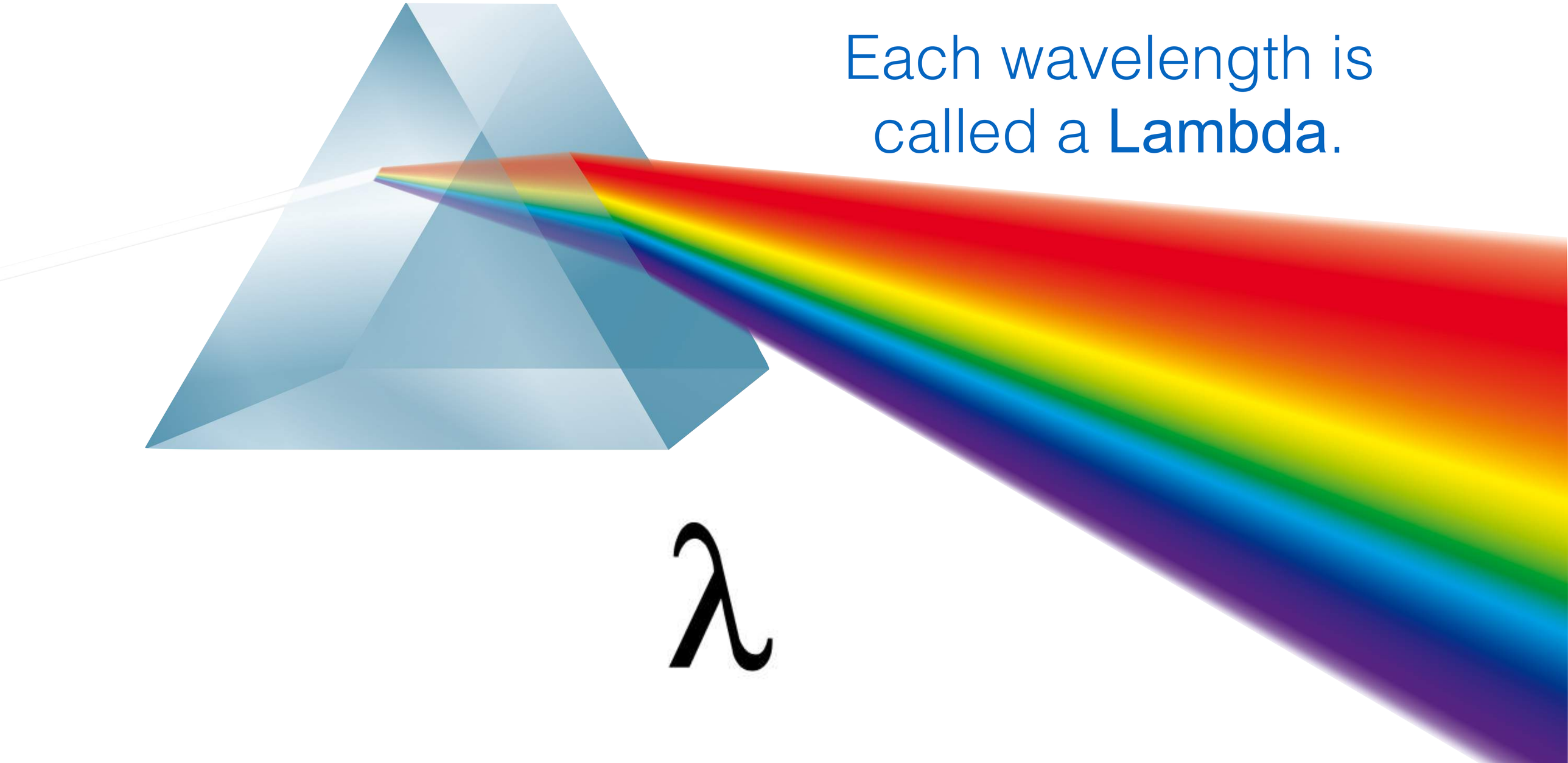
Metropolitan Area Network (MAN)



- Limited Availability
- Very High Speed
- Redundant

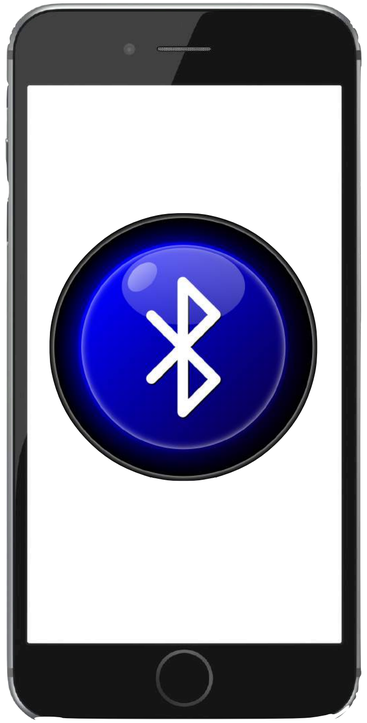
Metropolitan Area Network (MAN)

Each wavelength is called a **Lambda**.



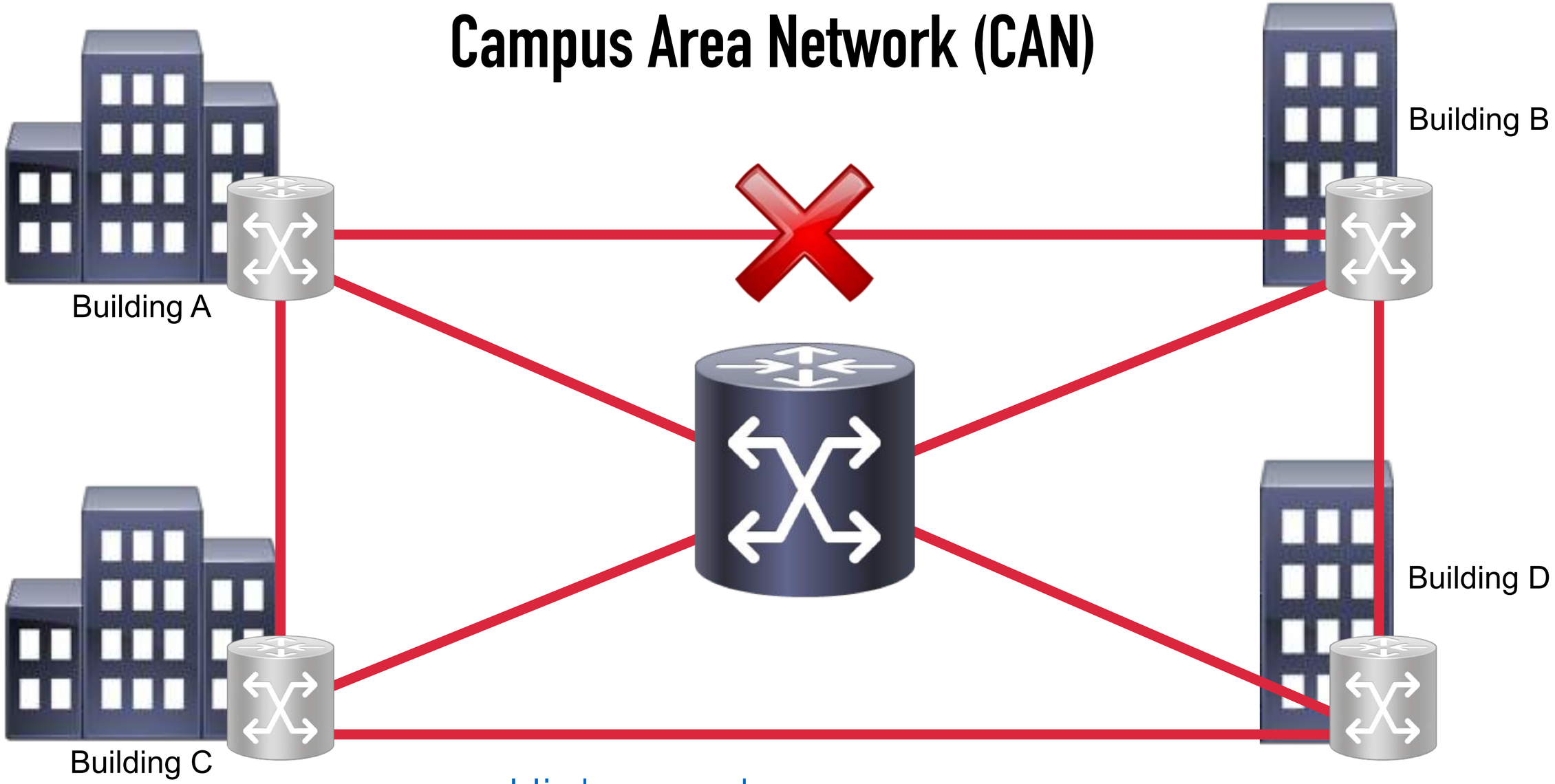
λ

Personal Area Network (PAN)



- Interconnects Two Devices
- Limited Distance
- Limited Throughput

Campus Area Network (CAN)

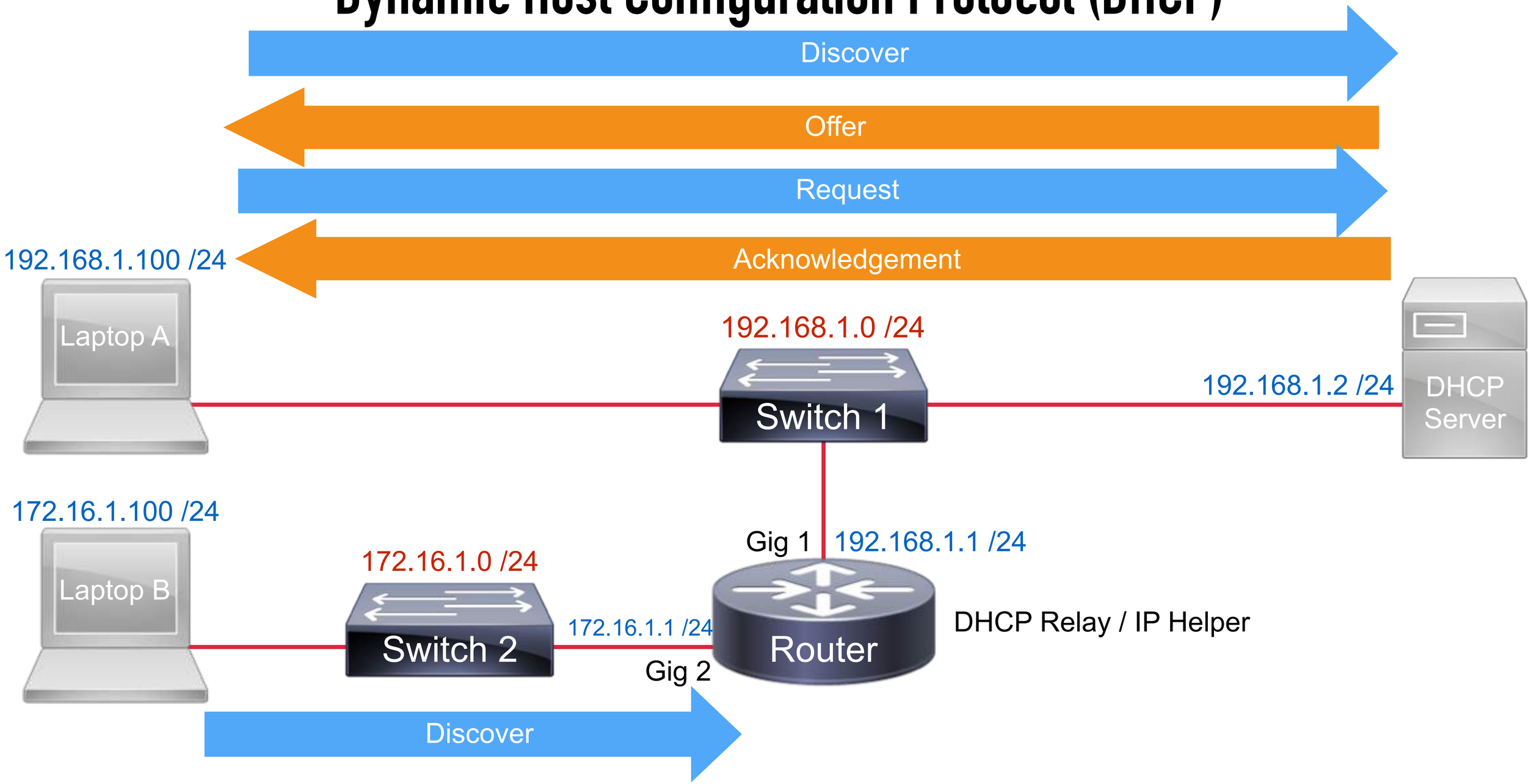


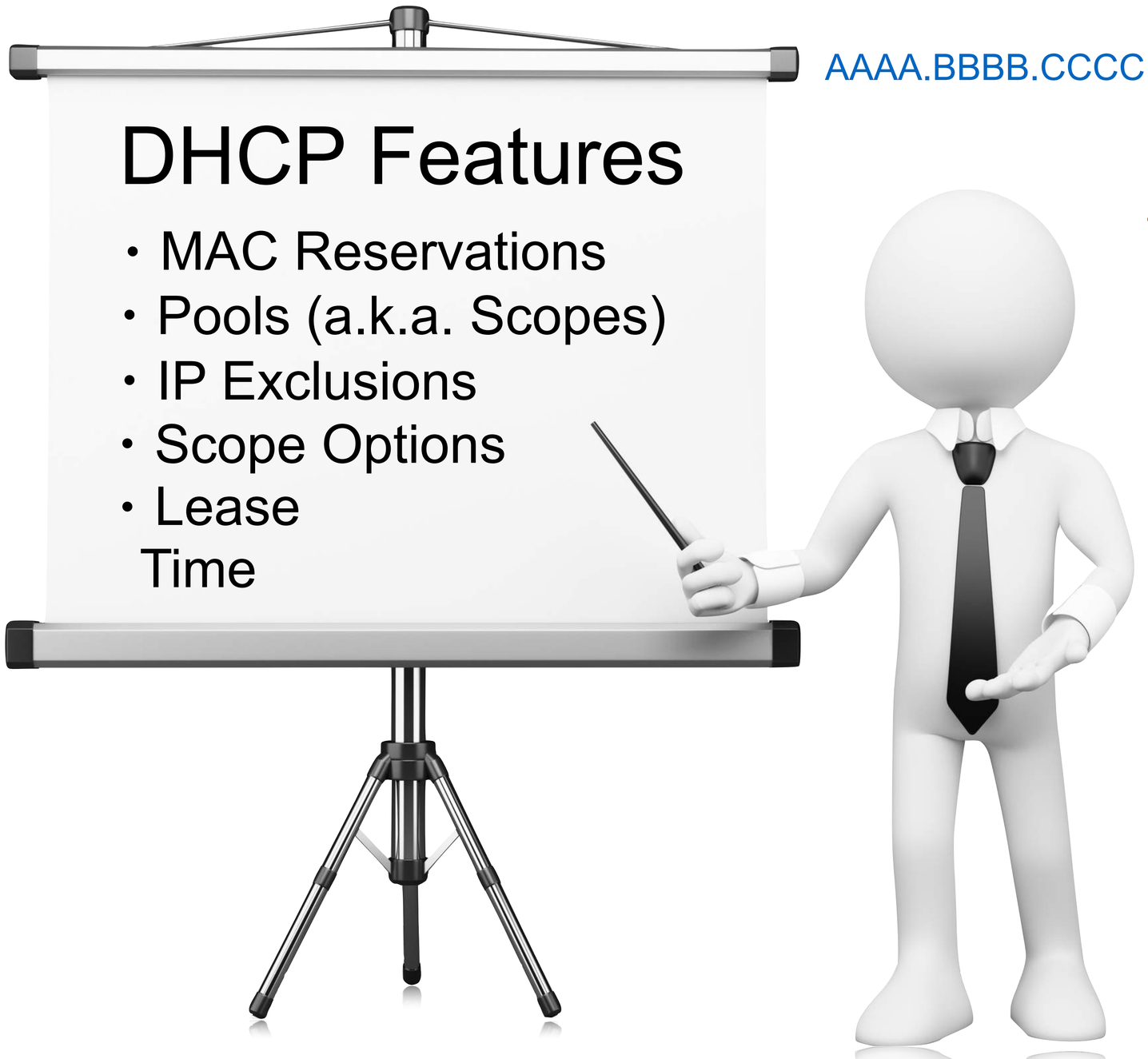
- High speed
- Interconnects Nearby Buildings
- Easy to Add Redundancy

Module 3
Network Topologies and Categories

Module 4
Network Services

Dynamic Host Configuration Protocol (DHCP)





AAAA.BBBB.CCCC.1234 → 192.168.1.125

POOL1	POOL2
192.168.1.100-199	172.16.1.100-199

Excluded

192.168.1.1-99

192.168.1.200-254

172.16.1.1-99

172.16.1.200-254

Scope Options (Examples)

Default Gateway

DNS Server

TTL

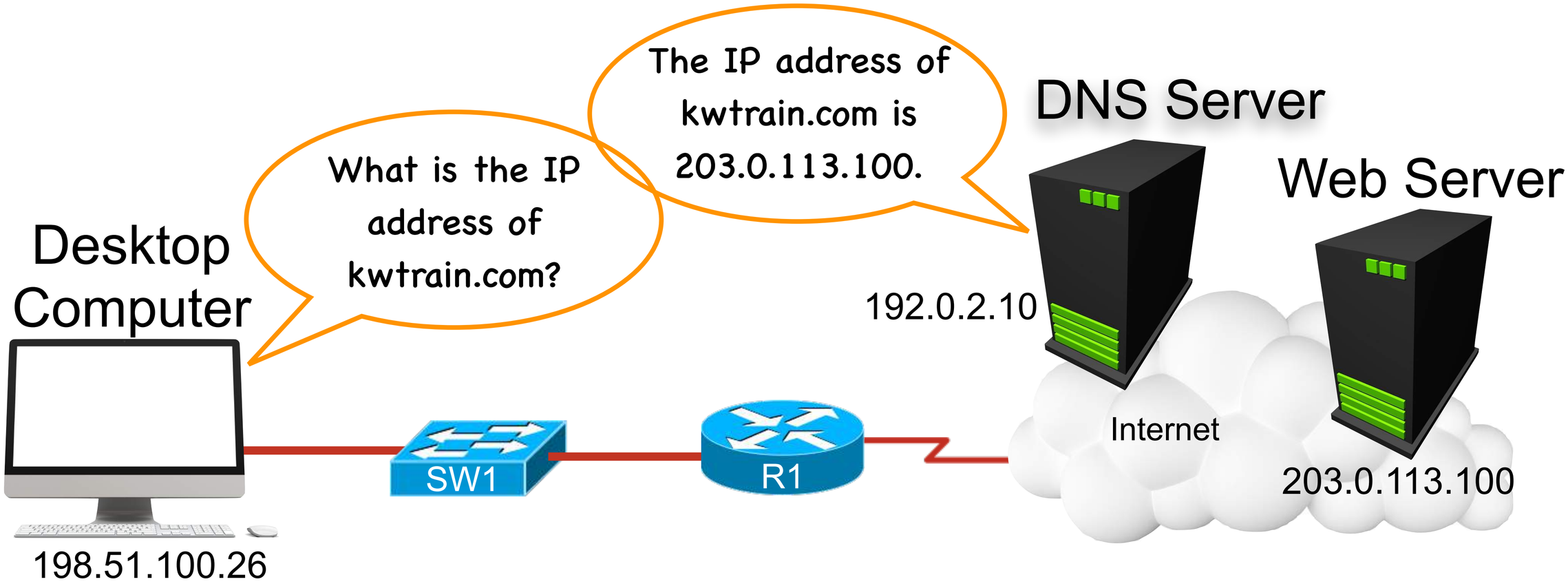
Option 150

Lease Time Timers

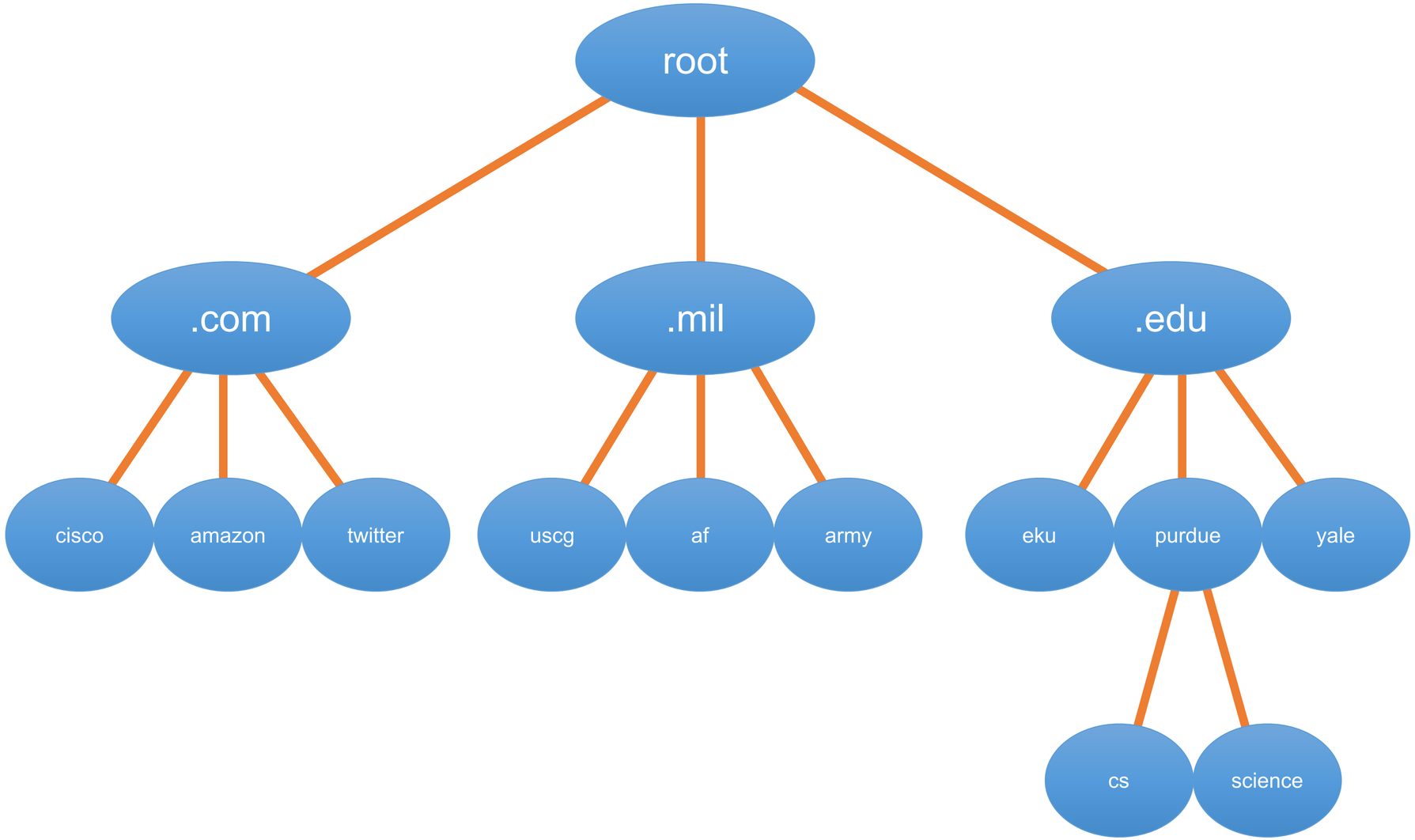
T1 = 1/2 of the Lease Time

T2 = 7/8 of the Lease Time

DNS Services



Hierarchical DNS Structure



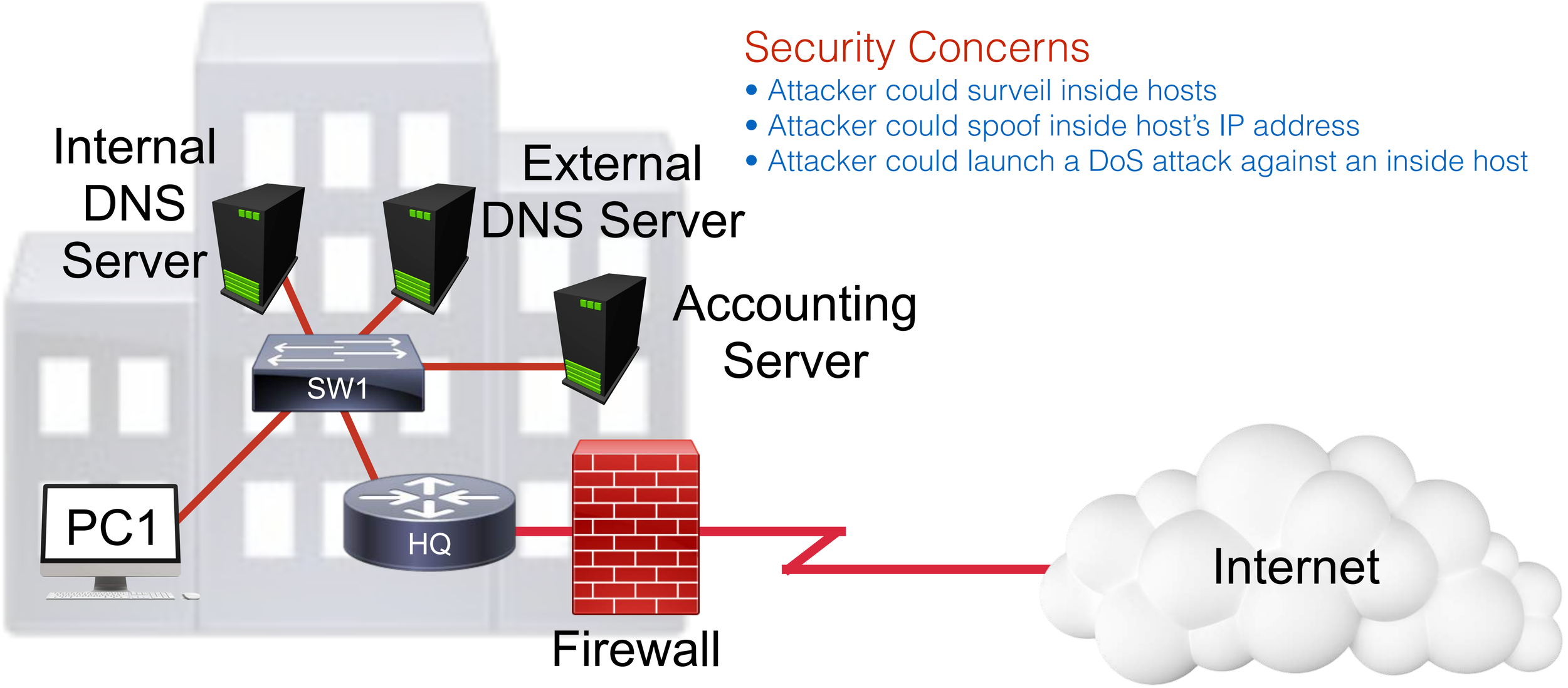
DNS Record Types

Record Type	Description
A	An **address** record is used to map a hostname to an IPv4 address.
AAAA	An **IPv6 address** record is used to main a hostname to an IPv6 address.
CNAME	A **canonical name** record is an alias of an existing record, thus allowing multiple DNS records to map to the same IP address.
MX	A **mail exchange** record maps a domain name to an e-mail (or message transfer agent) server for that domain.
PTR	A **pointer** record points to a canonical name. A PTR record is commonly used when performing a reverse DNS lookup, which is a process used to determine what domain name is associated with a known IP address.
SOA	A **start of authority** record provides authoritative information about a DNS zone, such as: e-mail contact information for the zone's administrator, the zone's primary name server, and various refresh timers.

DNS Record Types

Record Type	Description
TXT	A **text** record was originally intended to contain descriptive text (for humans to read). However, it's most often used to carry various attributes and their values, readable by the requesting computer.
SRV	A **Service Locator** record can be used to specify the IP address of a host providing a specific service, which is more generic than using an MX record, which points just to an e-mail service.
NS	A **Name Server** record tells a DNS zone to use specific name servers, for security reasons.

Internal vs. External DNS Servers



Security Concerns

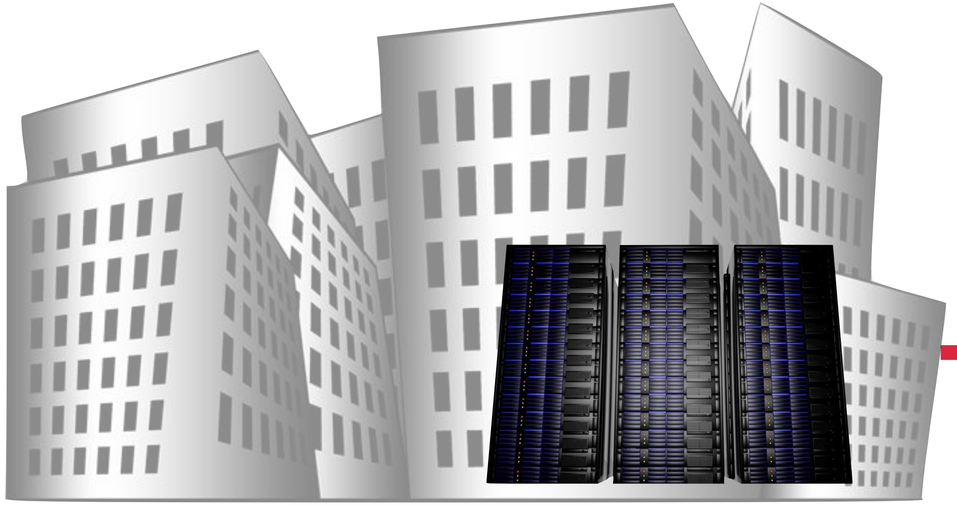
- Attacker could surveil inside hosts
- Attacker could spoof inside host's IP address
- Attacker could launch a DoS attack against an inside host

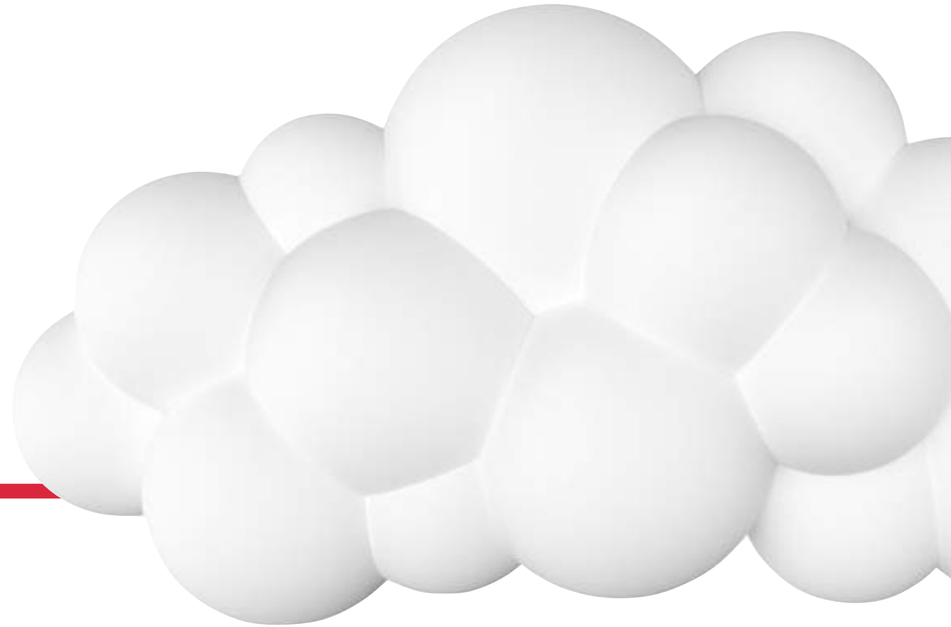
DNS in the Cloud

Google Public DNS

- 8.8.8.8
- 8.8.4.4

Google Cloud DNS

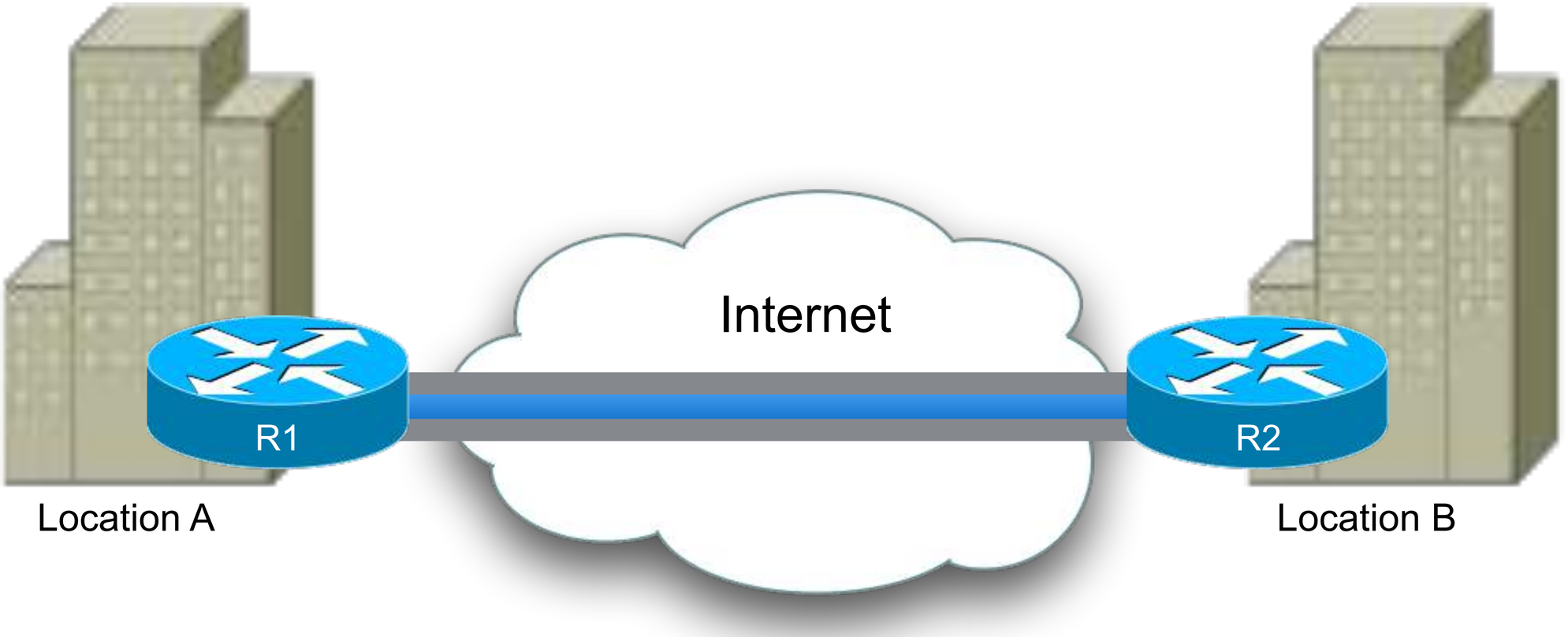




Enterprise

Cloud Provider

Virtual Private Networks (VPNs)

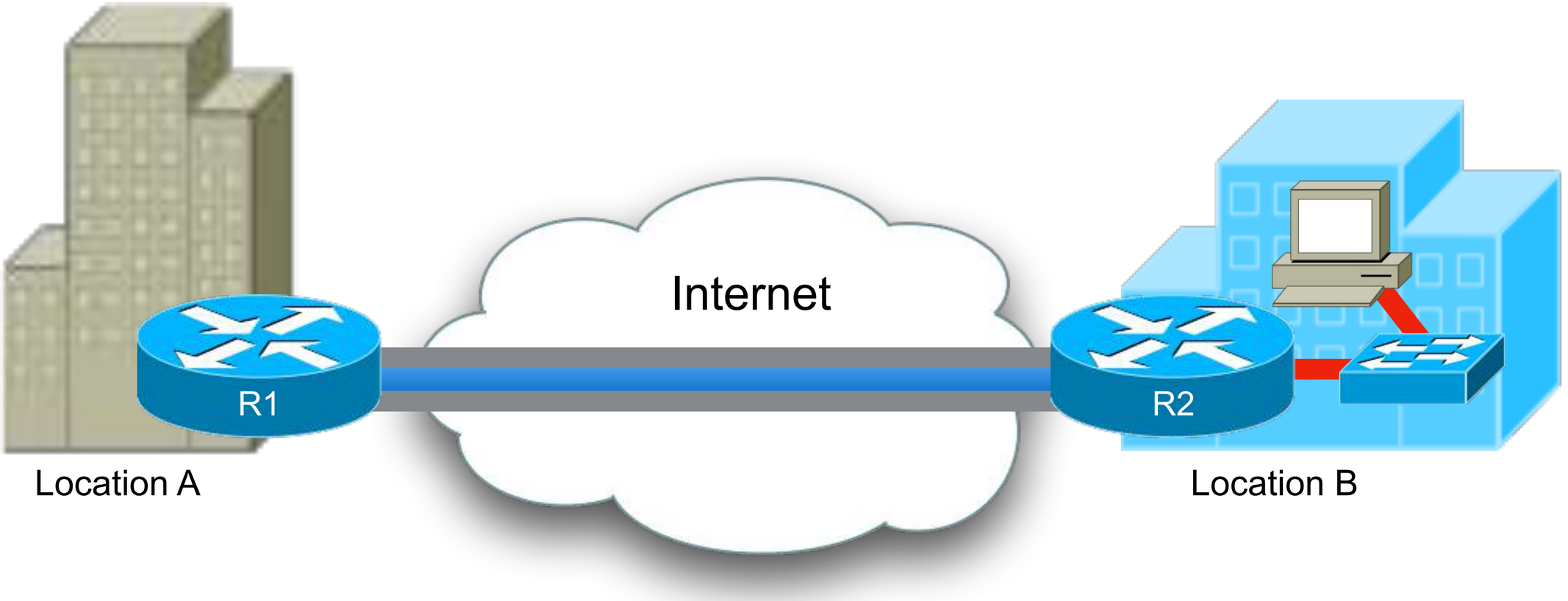


Site-to-Site VPN

Benefits

1. Can use common broadband technologies (e.g. DSL and cable)
2. Can scale to many connections (i.e. new connections just need Internet access)
3. Can securely transmit data over an untrusted network (e.g. the Internet)

Virtual Private Networks (VPNs)

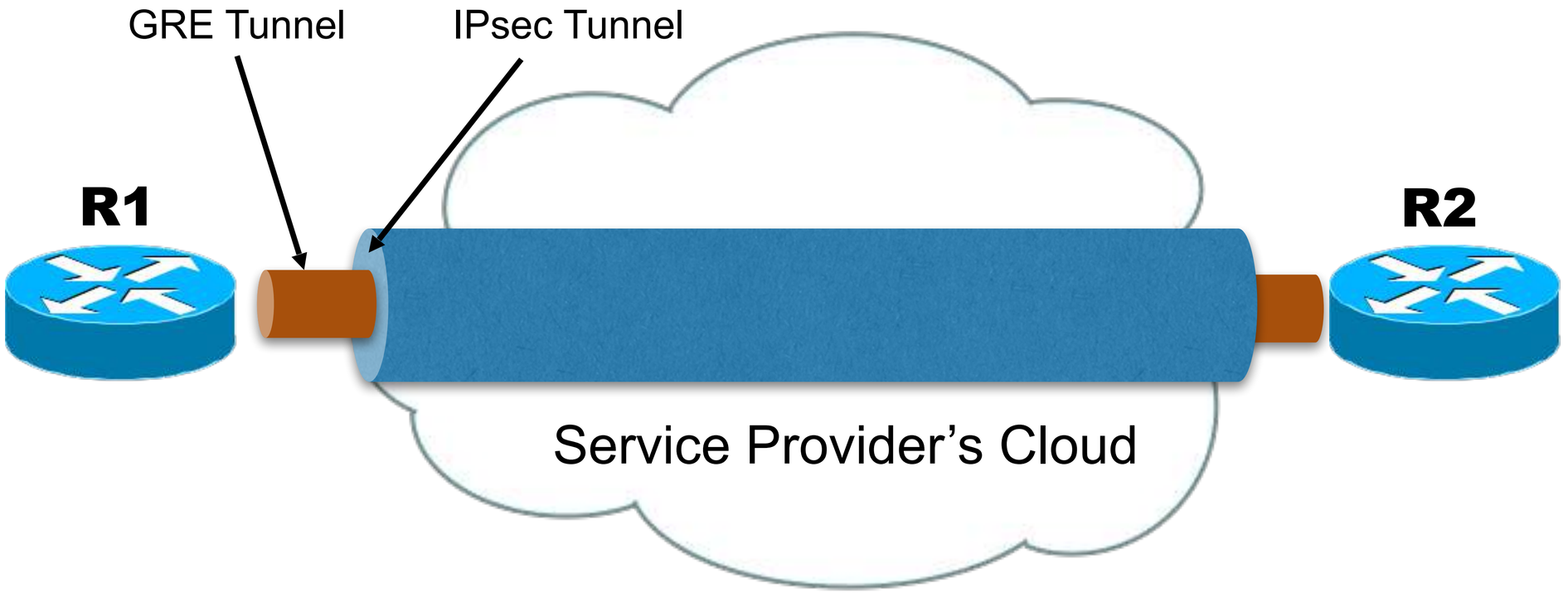


Remote-Access VPN

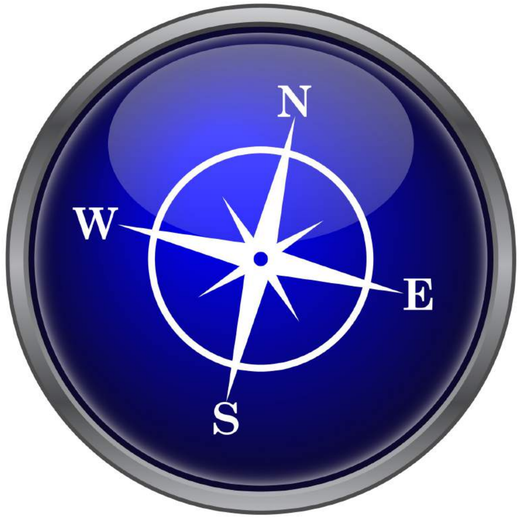
SSL VPN Options

1. Securely use a web browser (e.g. Clientless Cisco SSL VPN)
2. Install a software client (e.g. Cisco AnyConnect SSL VPN)

IPsec and GRE Tunnels



Software Defined Networking (SDN)

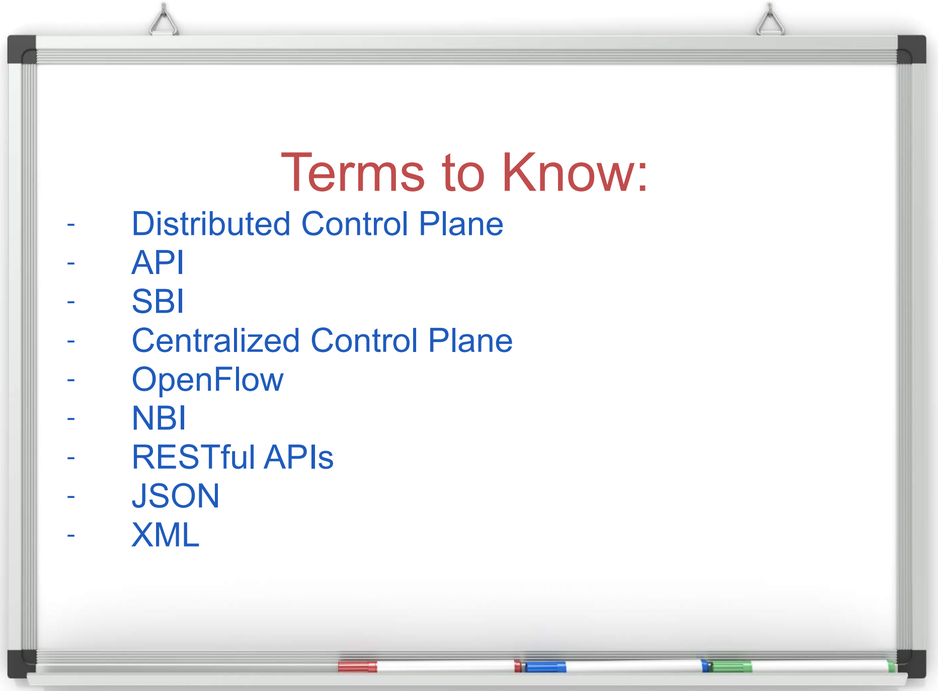


Applications

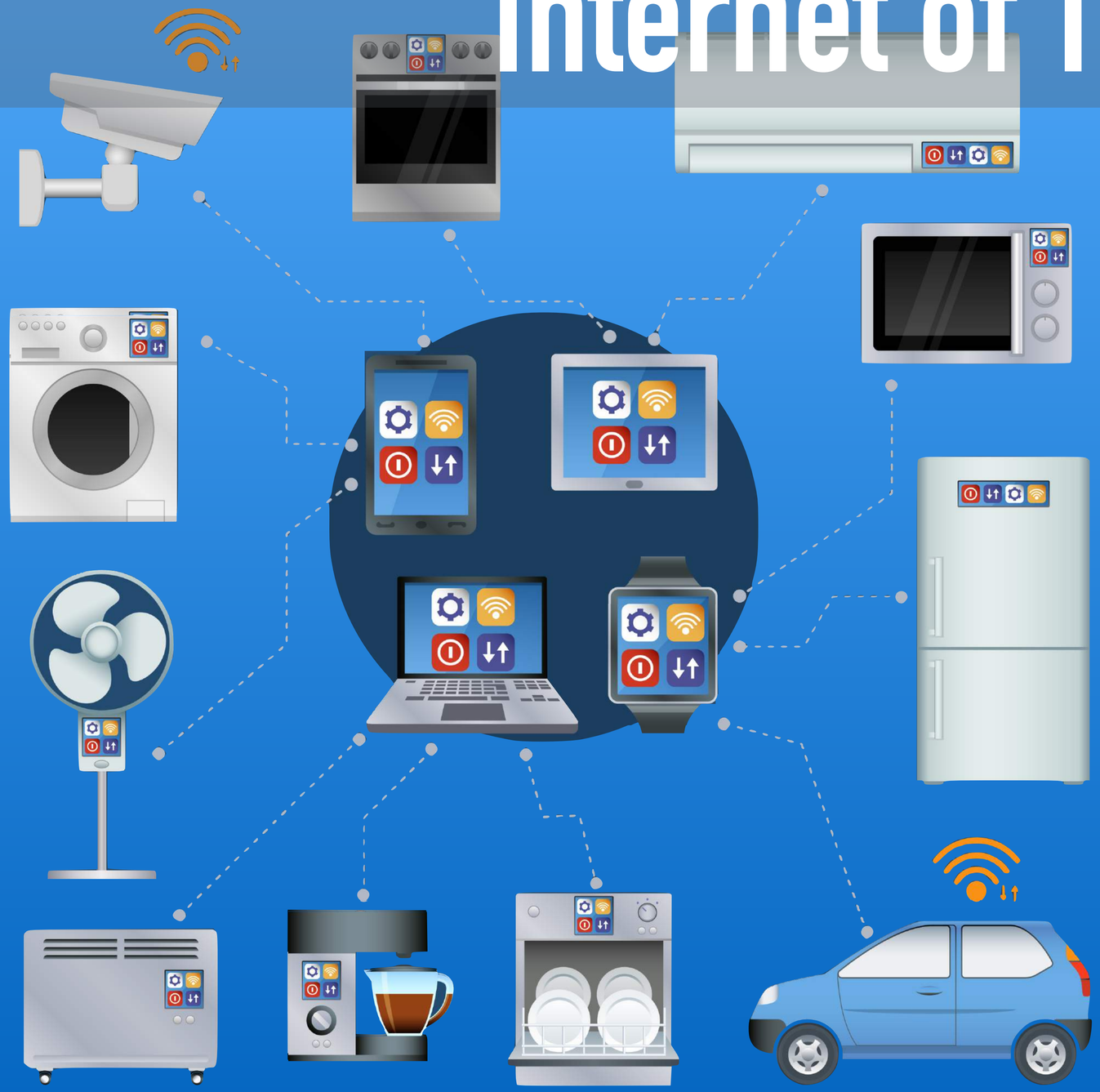
Northbound Interfaces

Network Controller

Southbound Interfaces



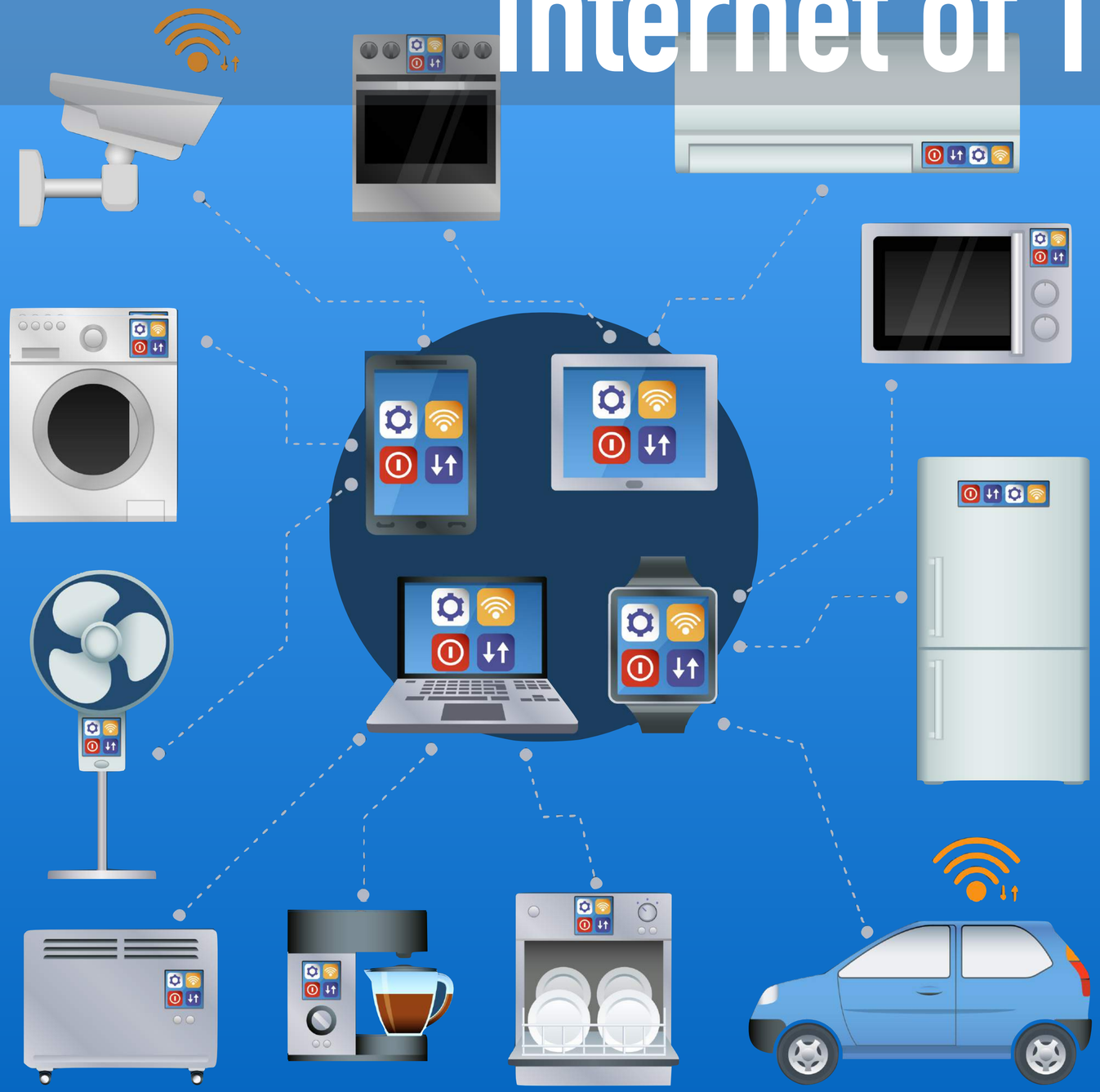
Internet of Things (IoT)



Drivers

- High speed Internet widely available
- Wi-Fi built into more devices
- Growing smartphone adoption

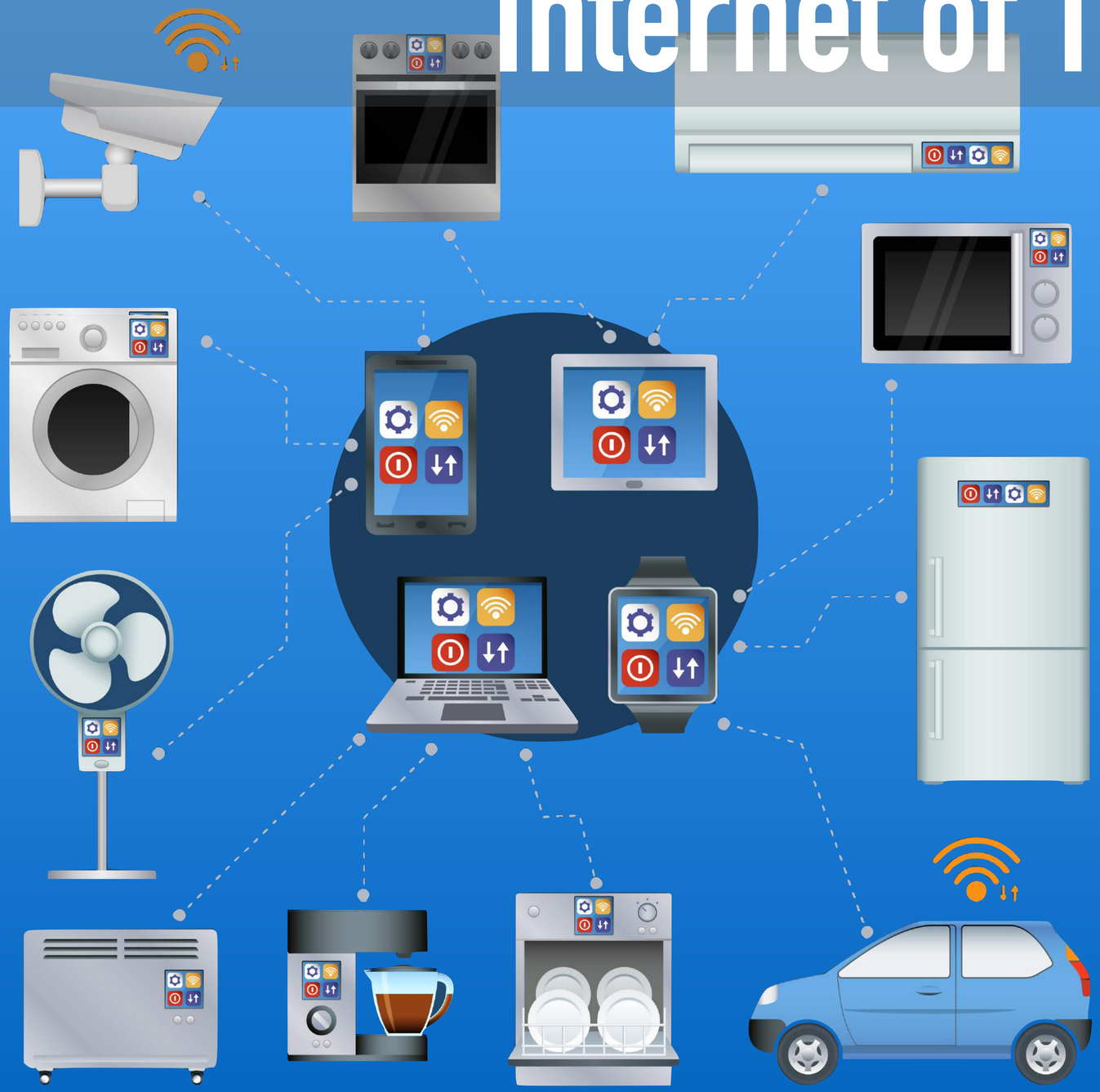
Internet of Things (IoT)



Growth

- 26 billion connected devices by 2020
- IoT market - $267B by 2020

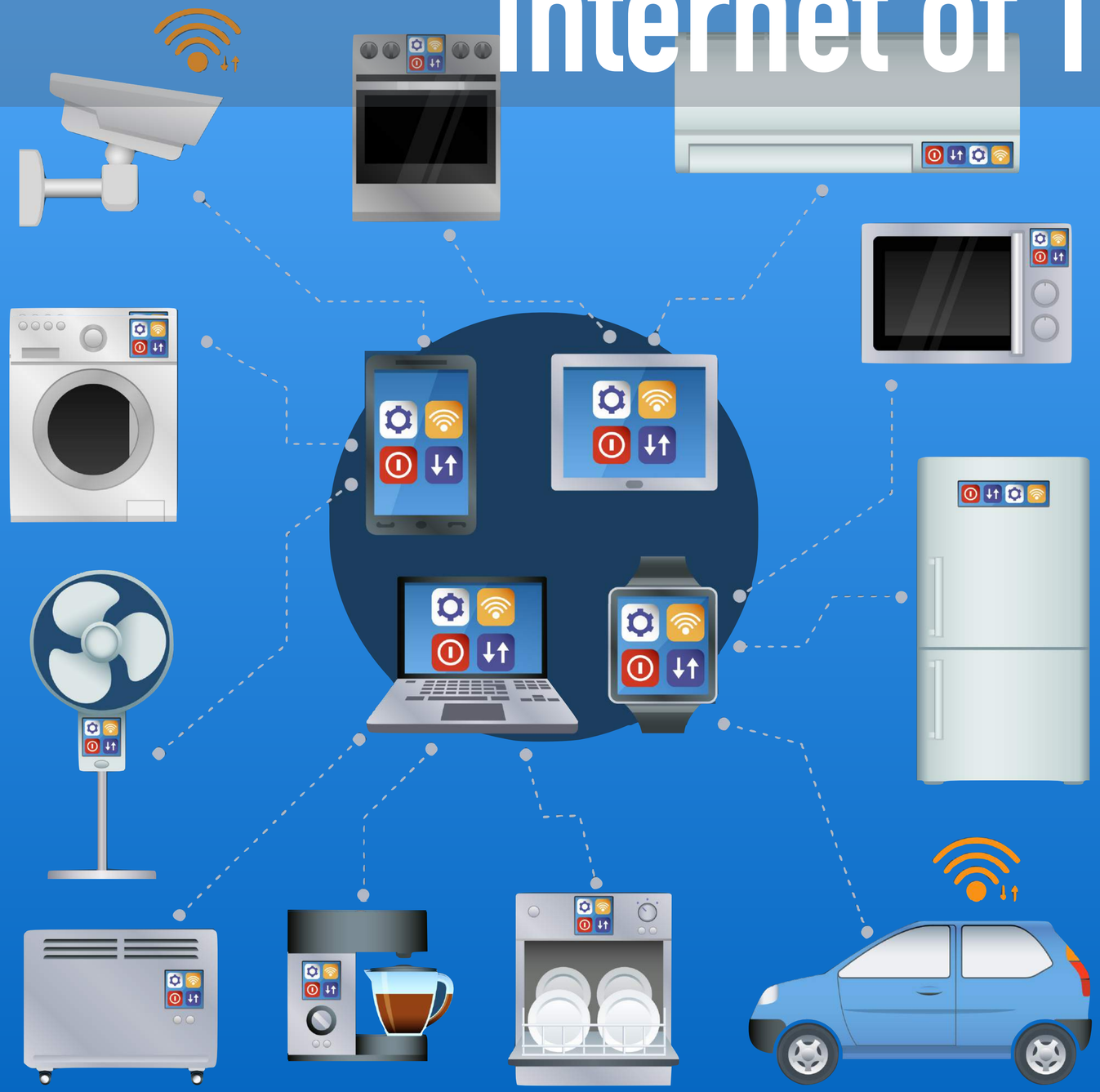
Internet of Things (IoT)



Top Applications

- Predictive maintenance
- Self-optimizing production
- Automated inventory management

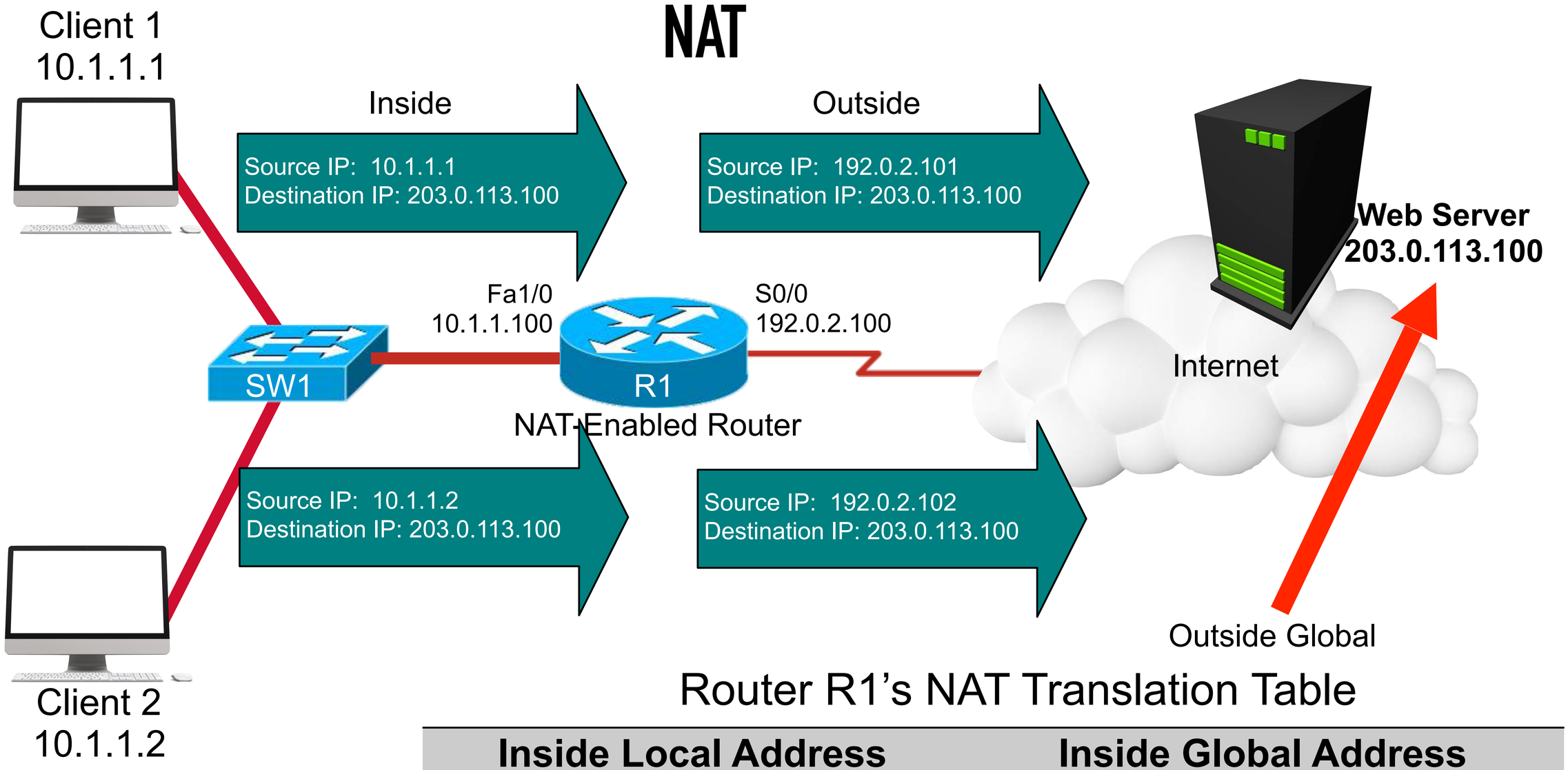
Internet of Things (IoT)



Supporting Technologies

- Z-Wave
- Ant+
- Bluetooth
- Near-Field Communication (NFC)
- Infrared (IR)
- Radio Frequency Identification (RFID)
- IEEE 802.11

NAT

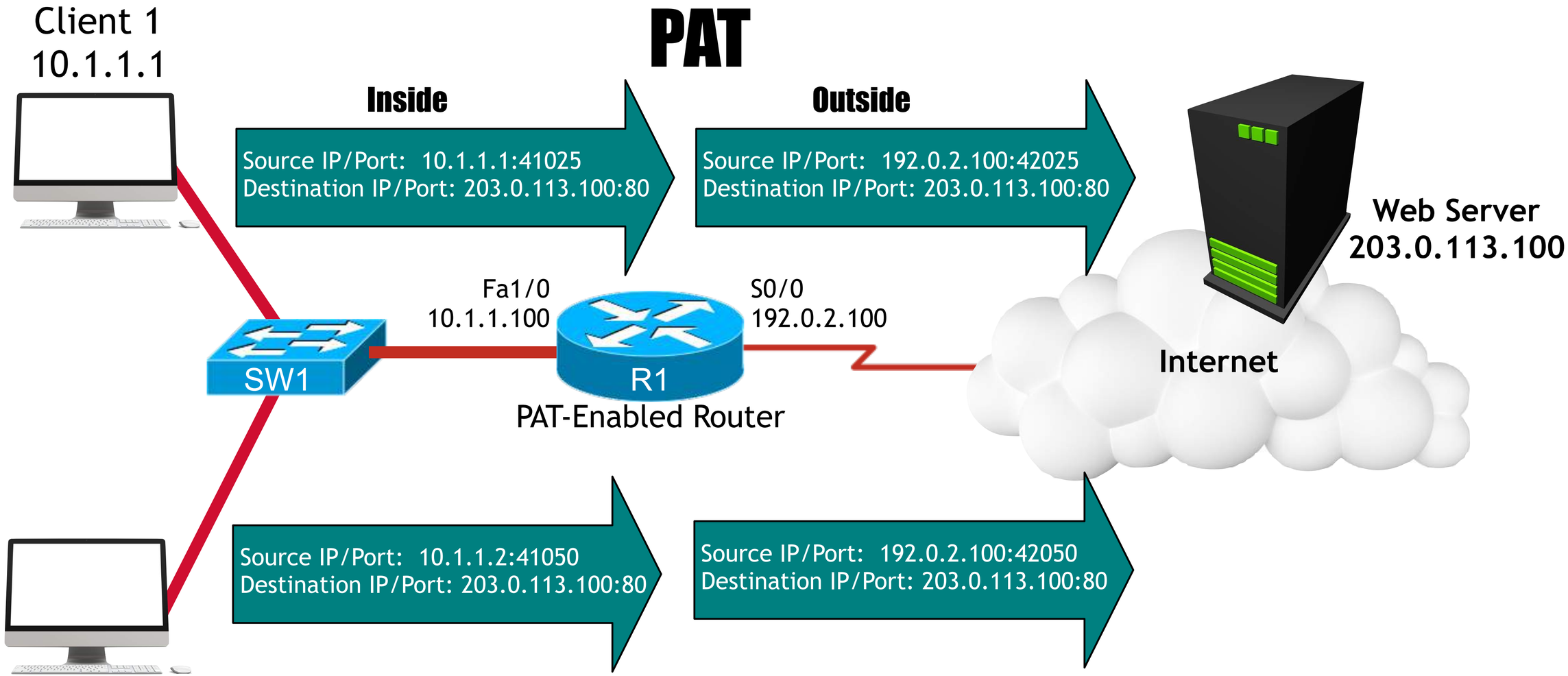


Pool of Addresses:
192.0.2.101-192.0.2.199

Router R1's NAT Translation Table

Inside Local Address	Inside Global Address
10.1.1.1	192.0.2.101
10.1.1.2	192.0.2.102

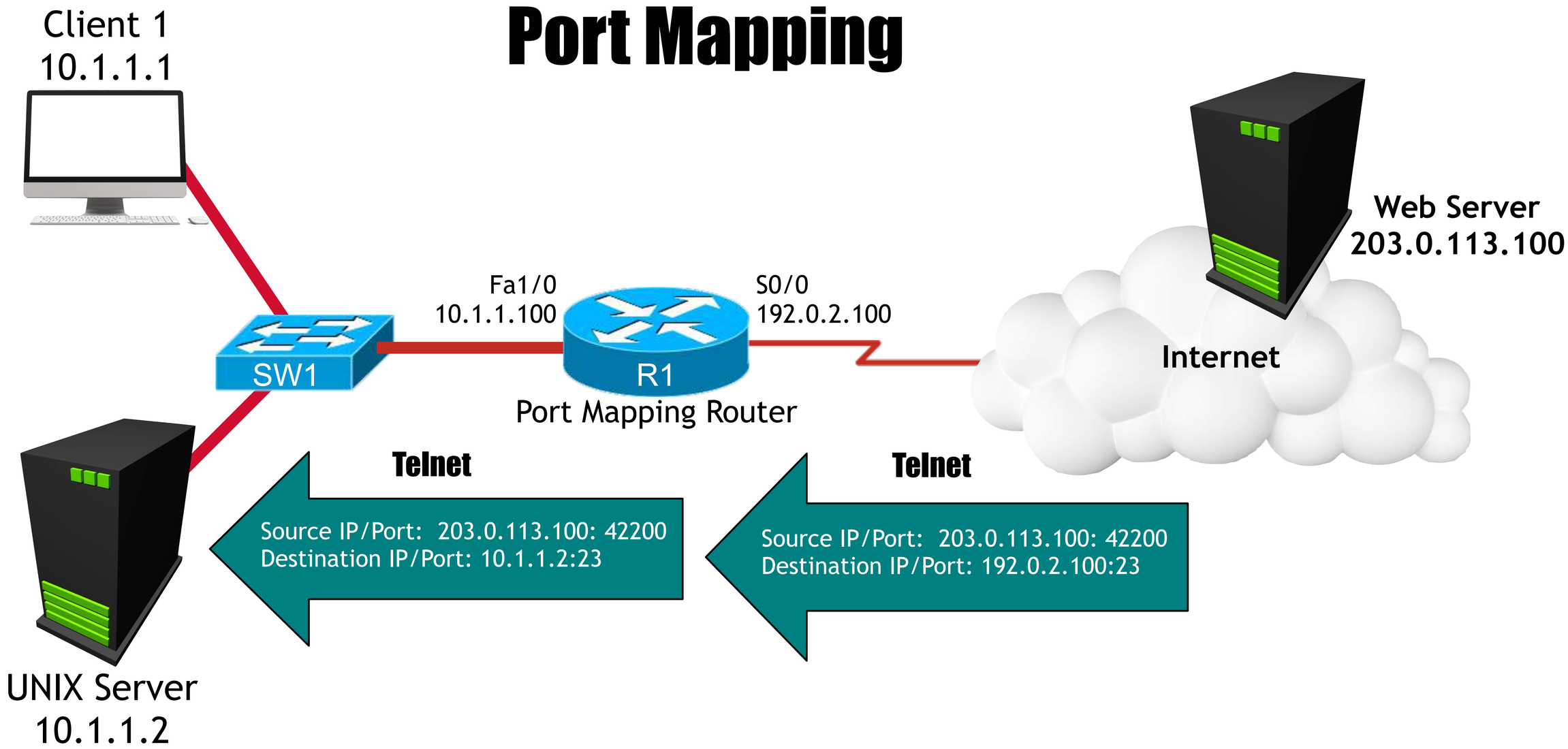
PAT



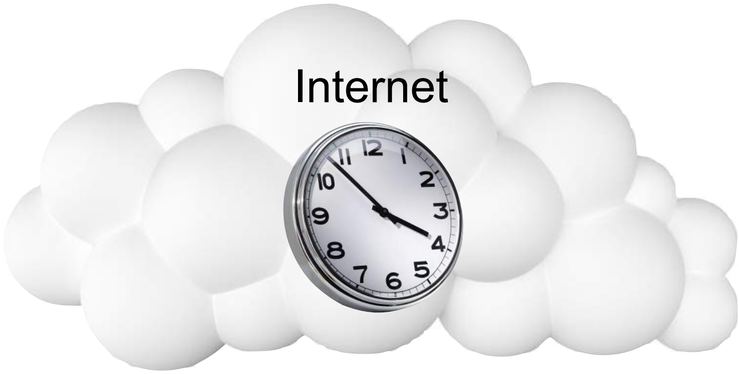
Router R1's NAT Translation Table

Inside Local Address	Inside Global Address
10.1.1.1:41025	192.0.2.100:42025
10.1.1.2:41050	192.0.2.100:42050

Port Mapping



Network Time Protocol (NTP)



- Uses UDP Port 123
- Uses a *stratum number* to measure the believability of a time source

Module 4
Network Services

Module 5
WAN Technologies

Packet Switched vs. Circuit Switched Networks

Circuit Switched

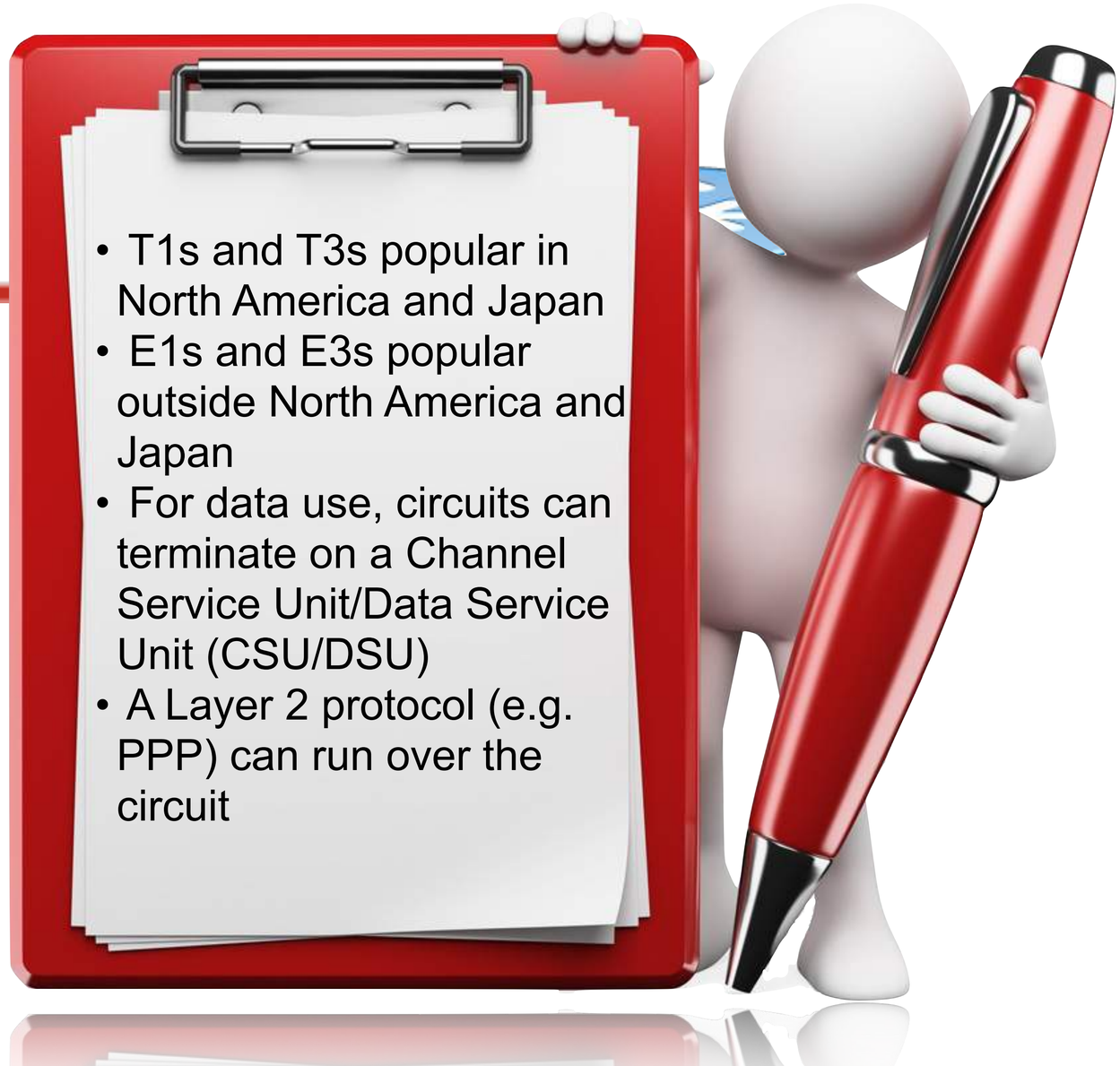
- A circuit (or a “call”) is setup before transmitting
- Voice, data, and/or video is sent over the circuit
- Examples include:
  - Telephone calls
  - ISDN
- Dedicated bandwidth

Packet Switched

- A connection is “always-on”
- Voice, data, and/or video is encapsulated in packets and sent through a network
- Examples include:
  - Cable modems
  - Wireless networks
  - LANs
- Shared bandwidth

Digital Circuits

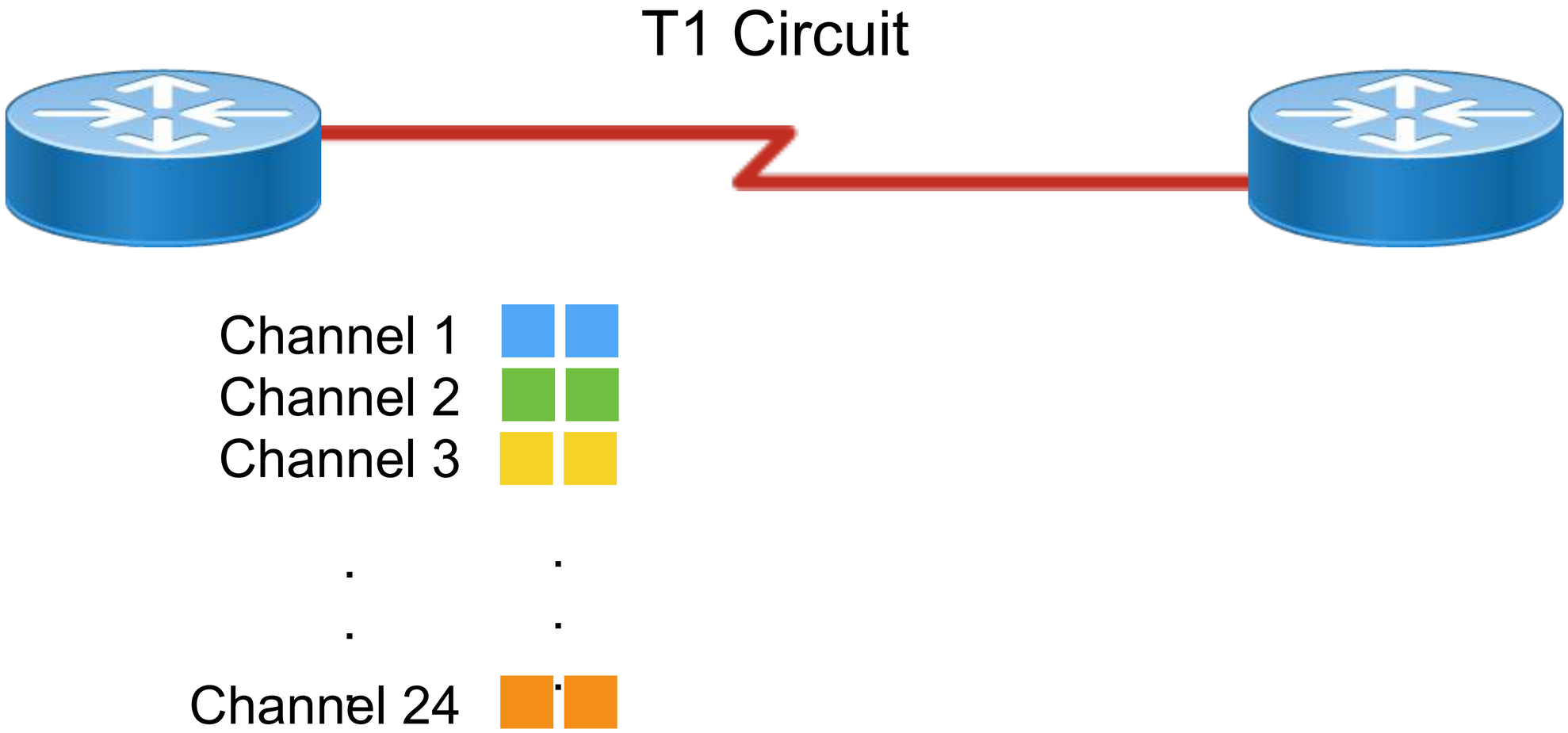
T1 or E1 Circuit



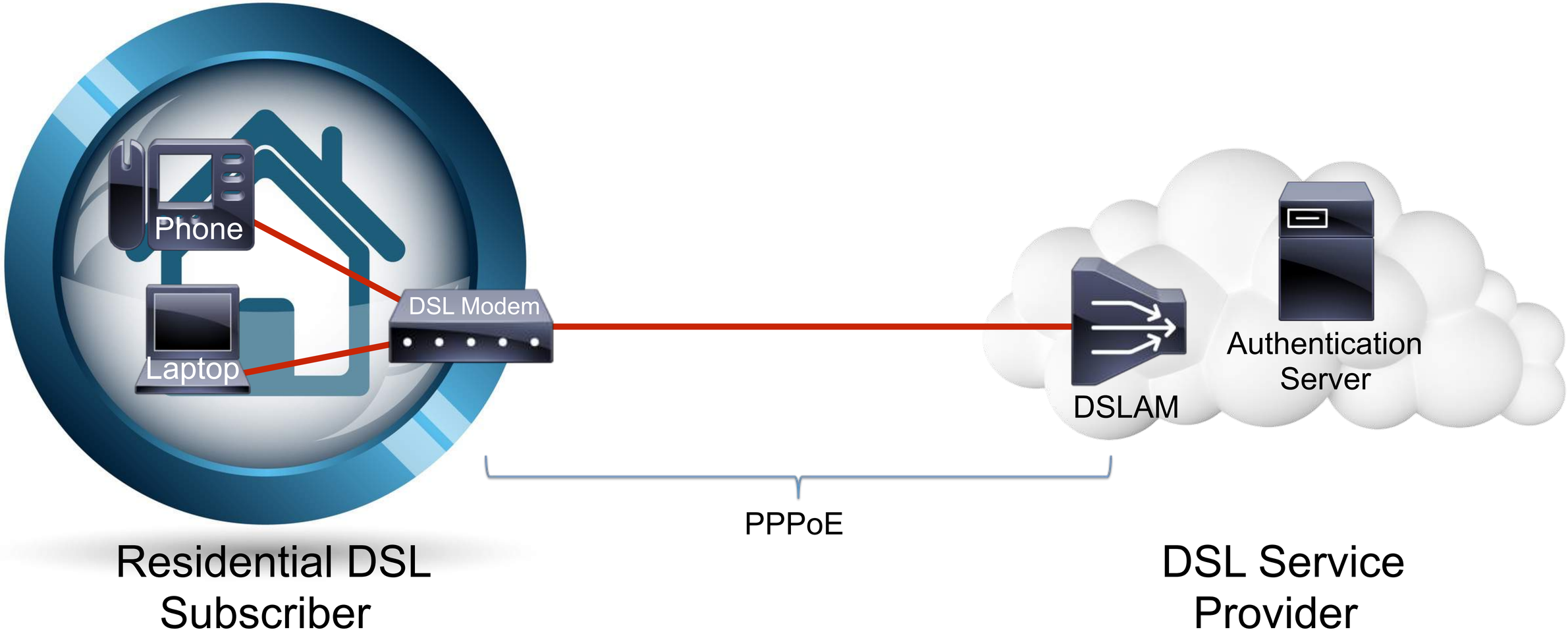
- T1s and T3s popular in North America and Japan
- E1s and E3s popular outside North America and Japan
- For data use, circuits can terminate on a Channel Service Unit/Data Service Unit (CSU/DSU)
- A Layer 2 protocol (e.g. PPP) can run over the circuit

	T1	E1	T3	E3
Bandwidth	1.544 Mbps	2.048 Mbps	44.7 Mbps	34.4 Mbps

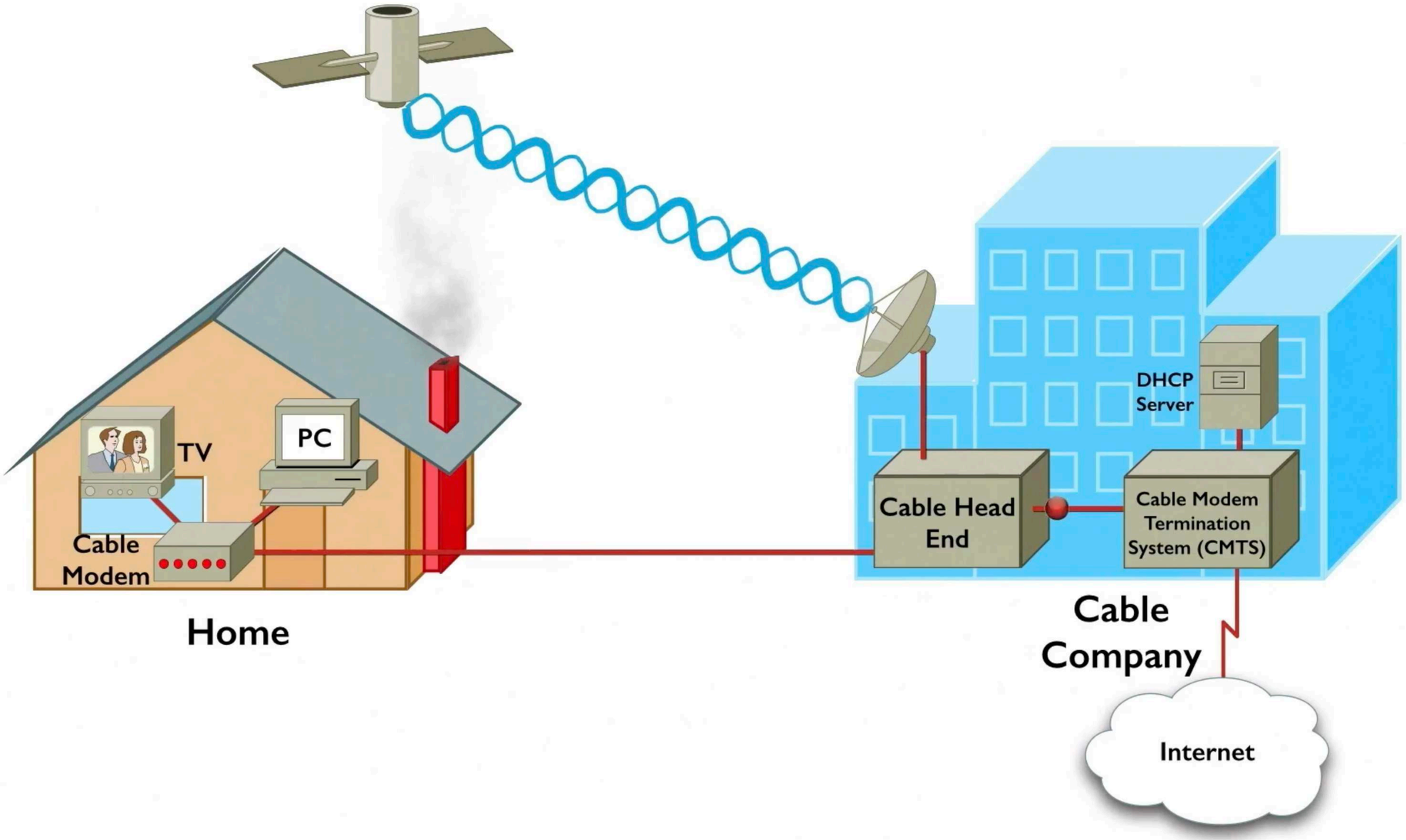
Time-Division Multiplexing (TDM)



Digital Subscriber Line (DSL) with PPP over Ethernet (PPPoE)



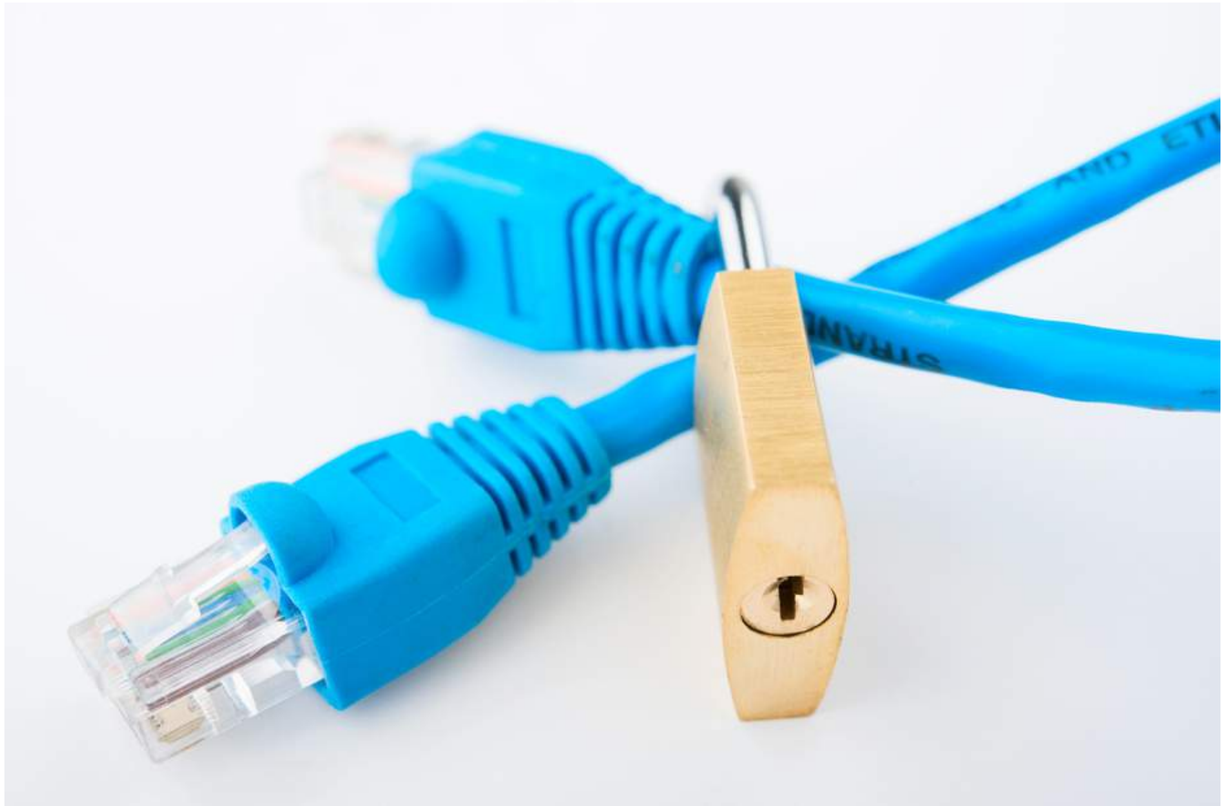
Cable Modem


TV
PC
Cable
Modem
Home
DHCP
Server
Cable Head
End
Cable Modem
Termination
System (CMTS)
Cable
Company
Internet

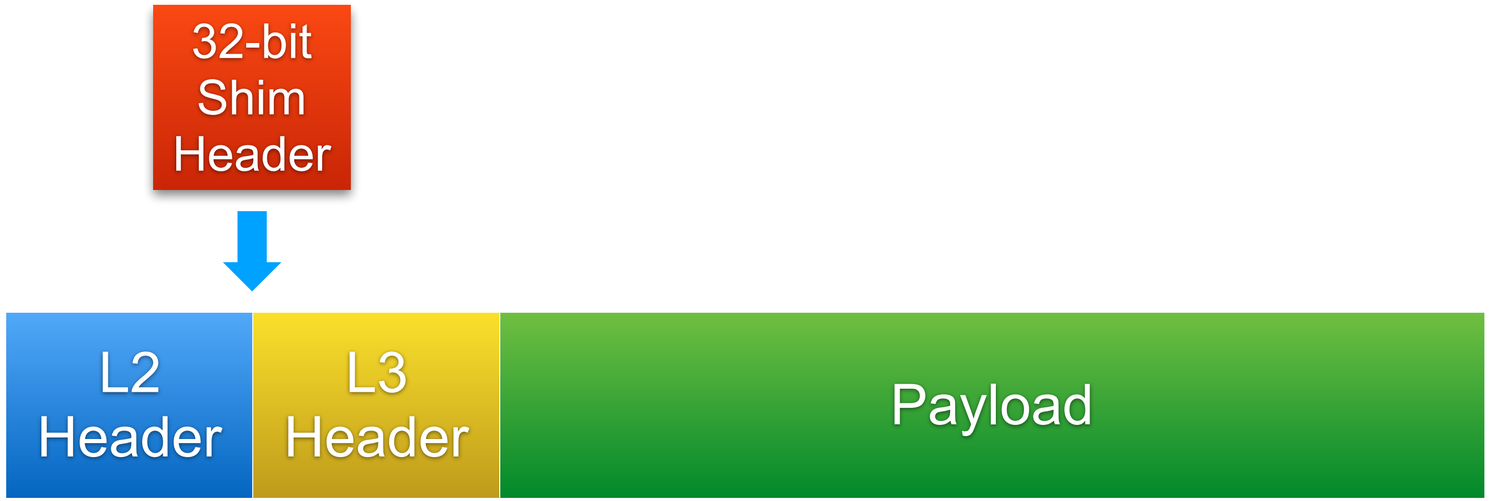
Point-to-Point Protocol (PPP)

R1

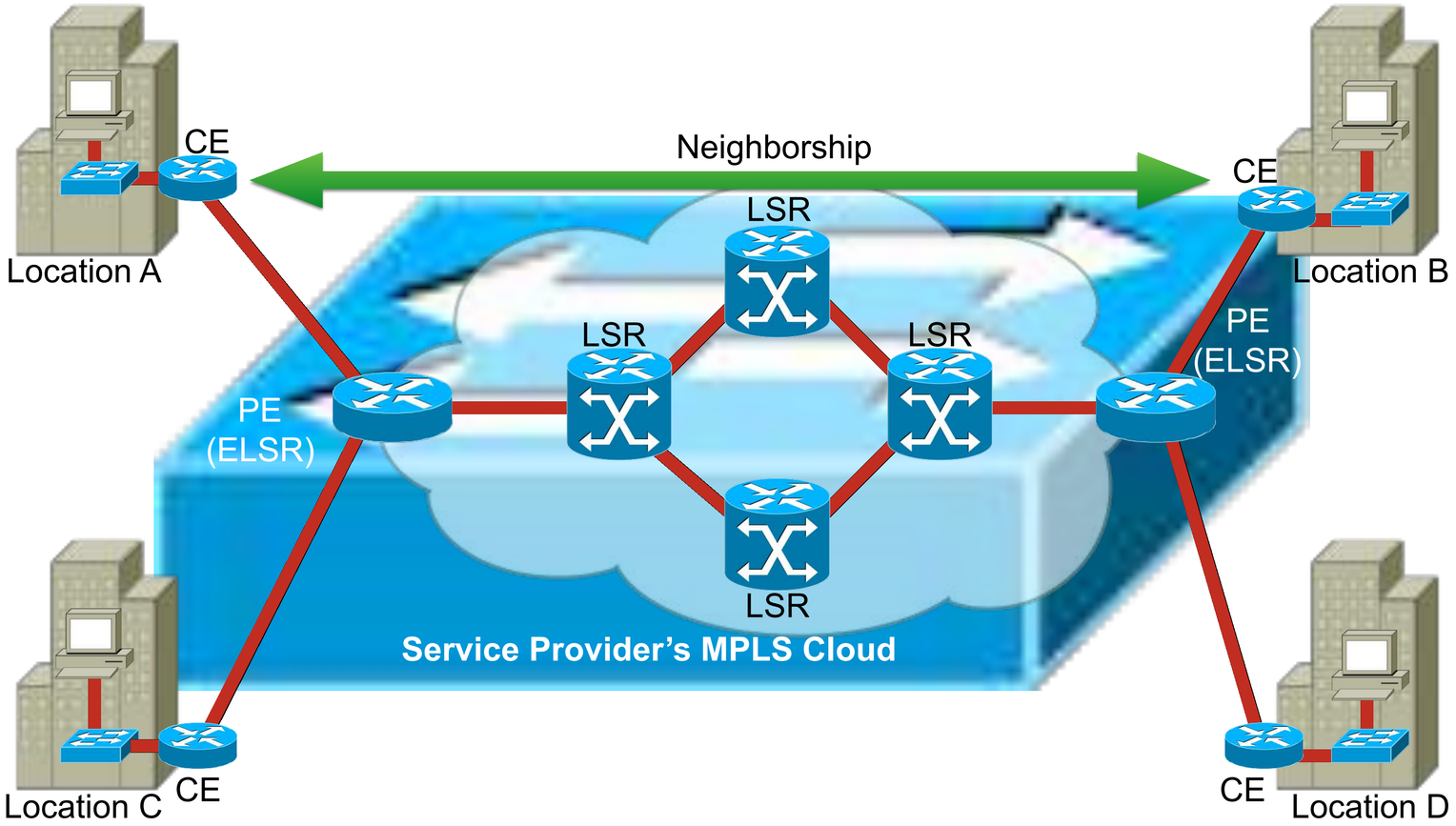
R2



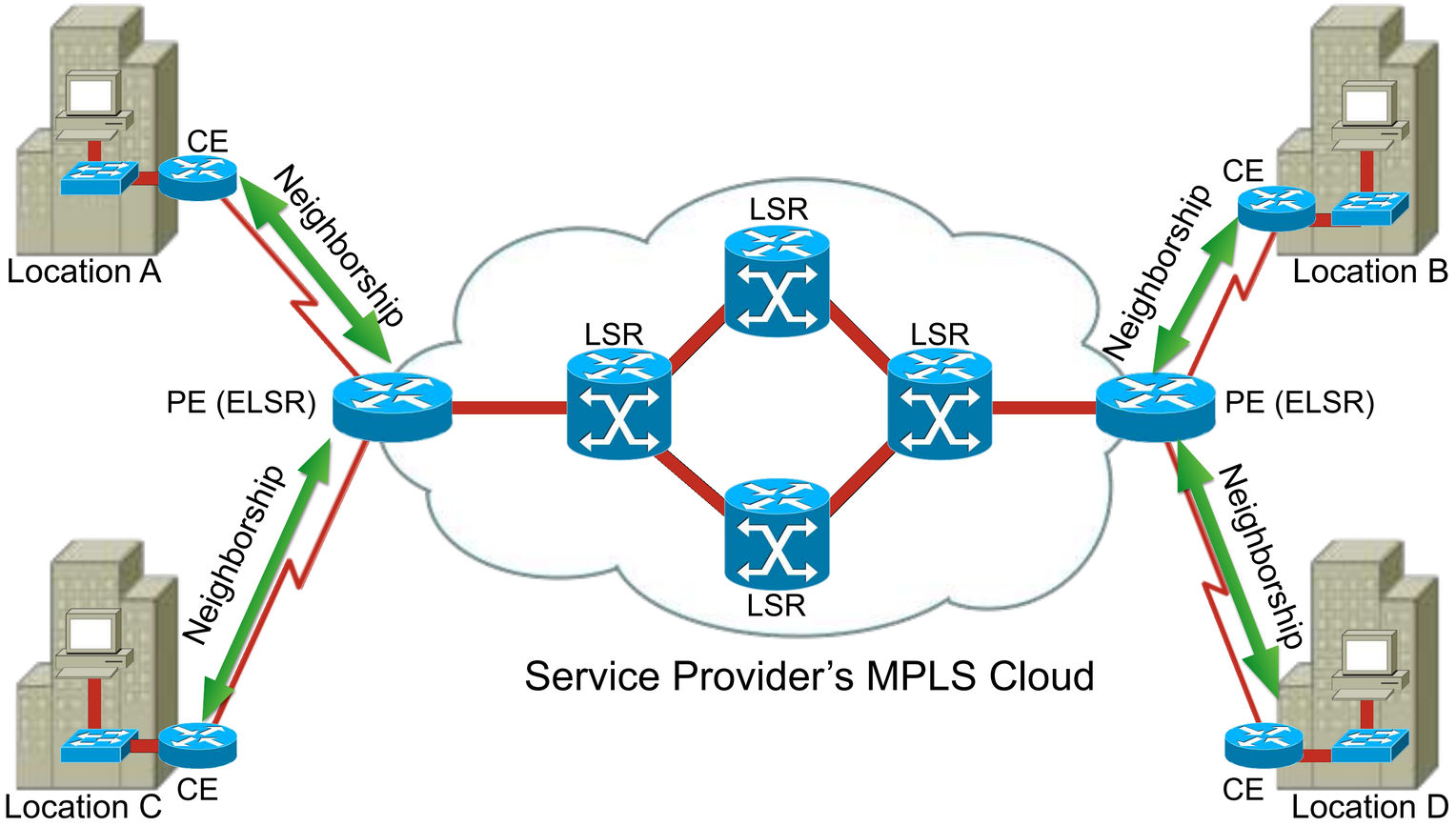
Multiprotocol Label Switching (MPLS) Frame



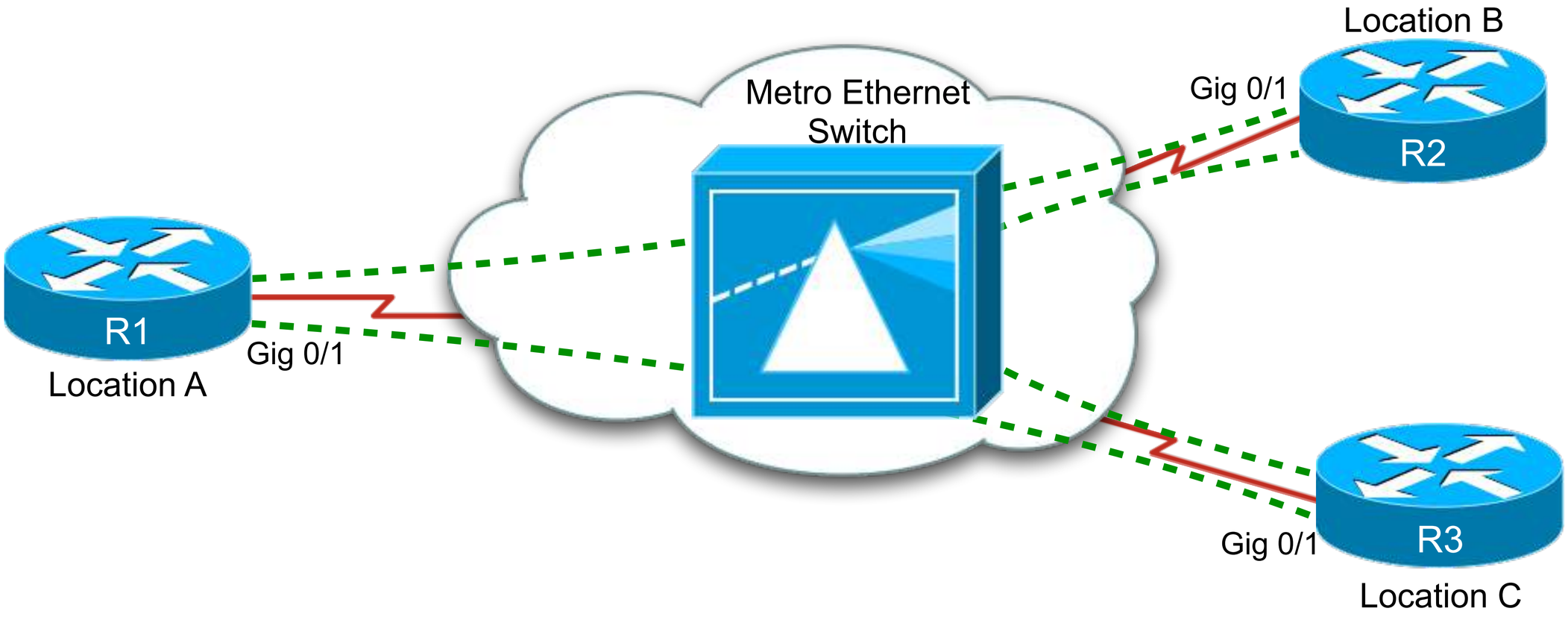
Layer 2 MPLS


CE
Neighborship
CE
Location A
Location B
LSR
LSR
LSR
PE
(ELSR)
PE
(ELSR)
LSR
Service Provider's MPLS Cloud
CE
CE
Location C
Location D

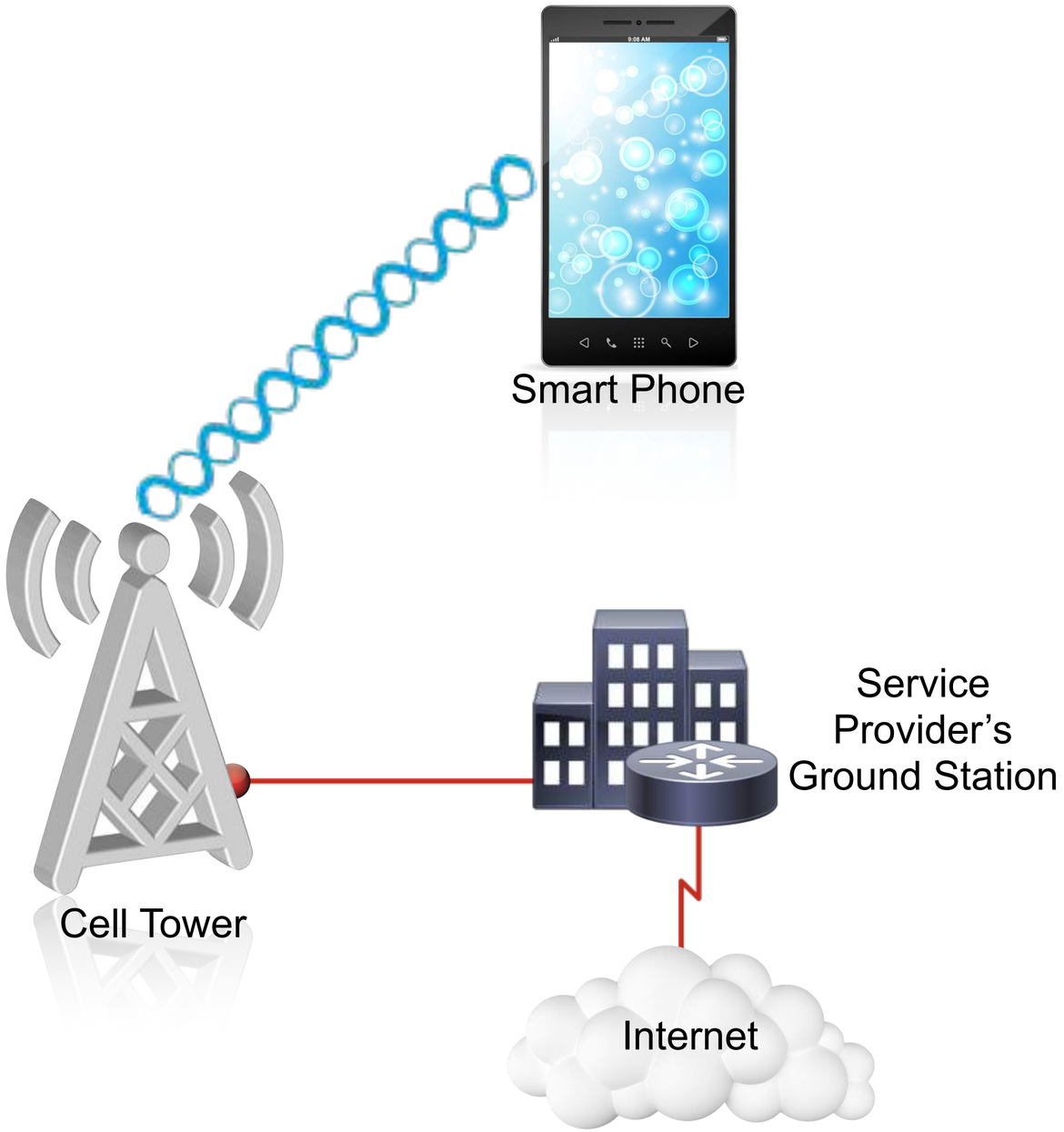
Layer 3 MPLS

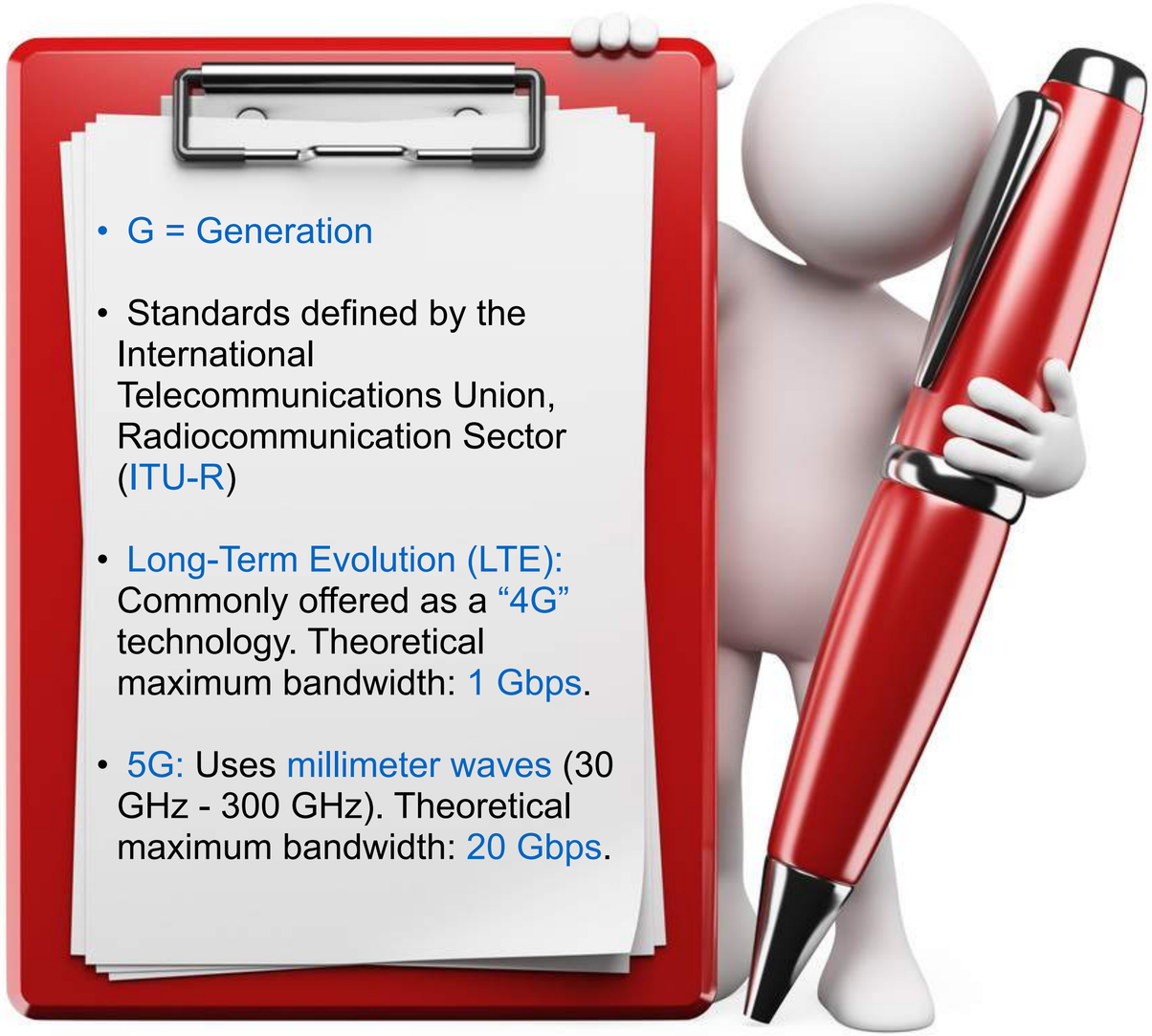

CE
Location A
Neighborship
PE (ELSR)
LSR
LSR
LSR
LSR
Service Provider's MPLS Cloud
Neighborship
CE
Location C
Neighborship
CE
Location B
PE (ELSR)
Neighborship
CE
Location D

Metro Ethernet



Cellular Technologies





- G = Generation
- Standards defined by the International Telecommunications Union, Radiocommunication Sector (ITU-R)
- Long-Term Evolution (LTE): Commonly offered as a "4G" technology. Theoretical maximum bandwidth: 1 Gbps.
- 5G: Uses millimeter waves (30 GHz - 300 GHz). Theoretical maximum bandwidth: 20 Gbps.

Module 5
WAN Technologies

Module 6
Cables and Connectors

Copper Cables

- RG-59
- RG-6
- RG-58
- RG-8/U

Coaxial Cable

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)
- Plenum-Rated

Twisted Pair Cable

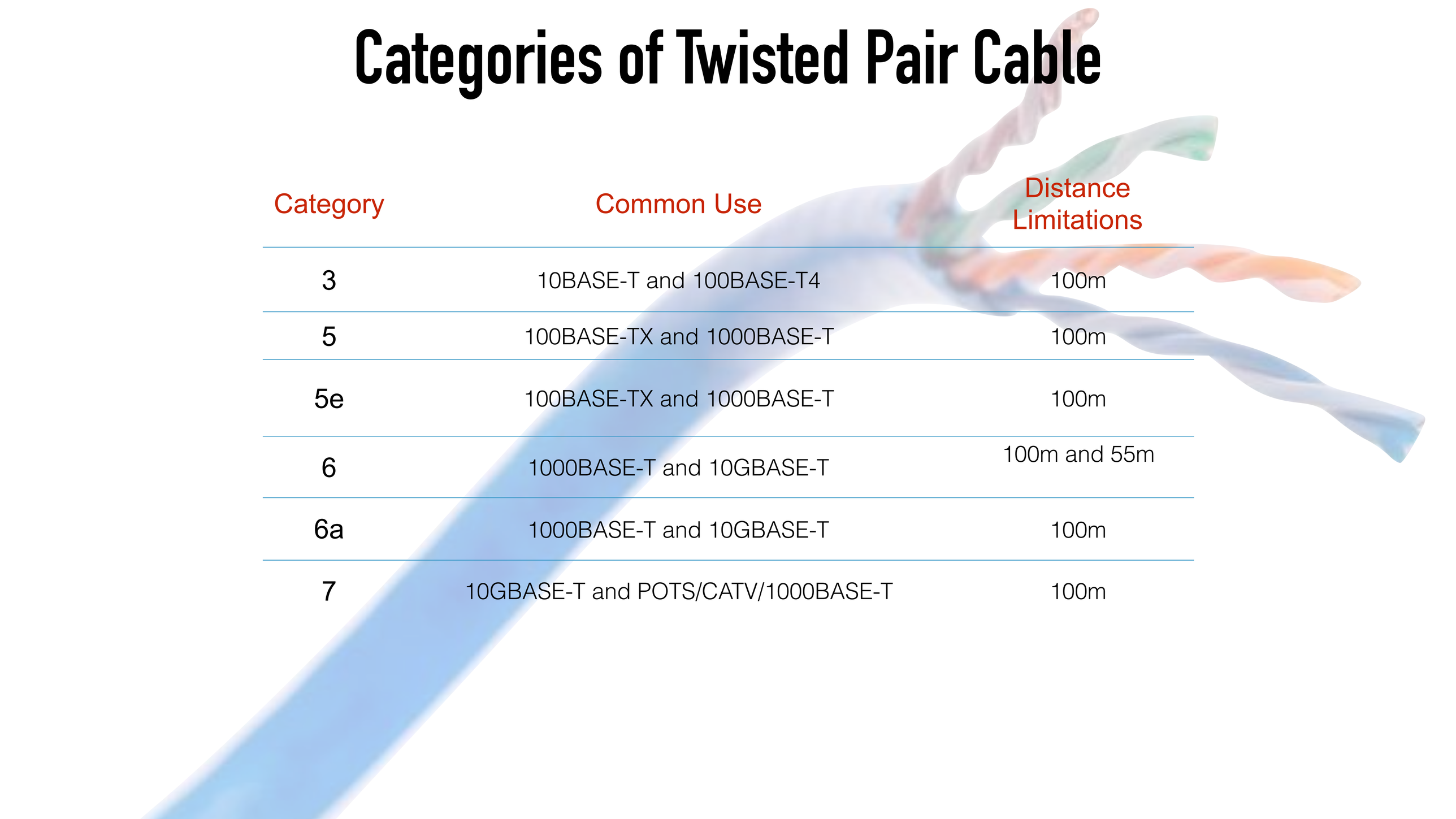
Electromagnetic Interference (EMI): Occurs when radio waves are picked up by or radiated by a cable carrying another signal, resulting in signal degradation

---

Impedance: A circuit's opposition to traffic flow (measured in Ohms), which can have resistive, capacitive, and/or inductive components

Categories of Twisted Pair Cable

Category	Common Use	Distance Limitations
3	10BASE-T and 100BASE-T4	100m
5	100BASE-TX and 1000BASE-T	100m
5e	100BASE-TX and 1000BASE-T	100m
6	1000BASE-T and 10GBASE-T	100m and 55m
6a	1000BASE-T and 10GBASE-T	100m
7	10GBASE-T and POTS/CATV/1000BASE-T	100m



DB-9 and DB-25

DB-9

DB-25

Commonly used with serial connections (e.g. modem, serial printer, console on Unix host, or mouse)

RJ-11 and RJ-45

RJ-45

- Commonly used on Ethernet cables
- 8 positions with 8 conductors

RJ-11

- Commonly used on telephones, modems, and fax machines
- 6 positions with 2 conductors
- (RJ-14: 6 positions with 4 conductors)

F-Type and BNC

F-Type

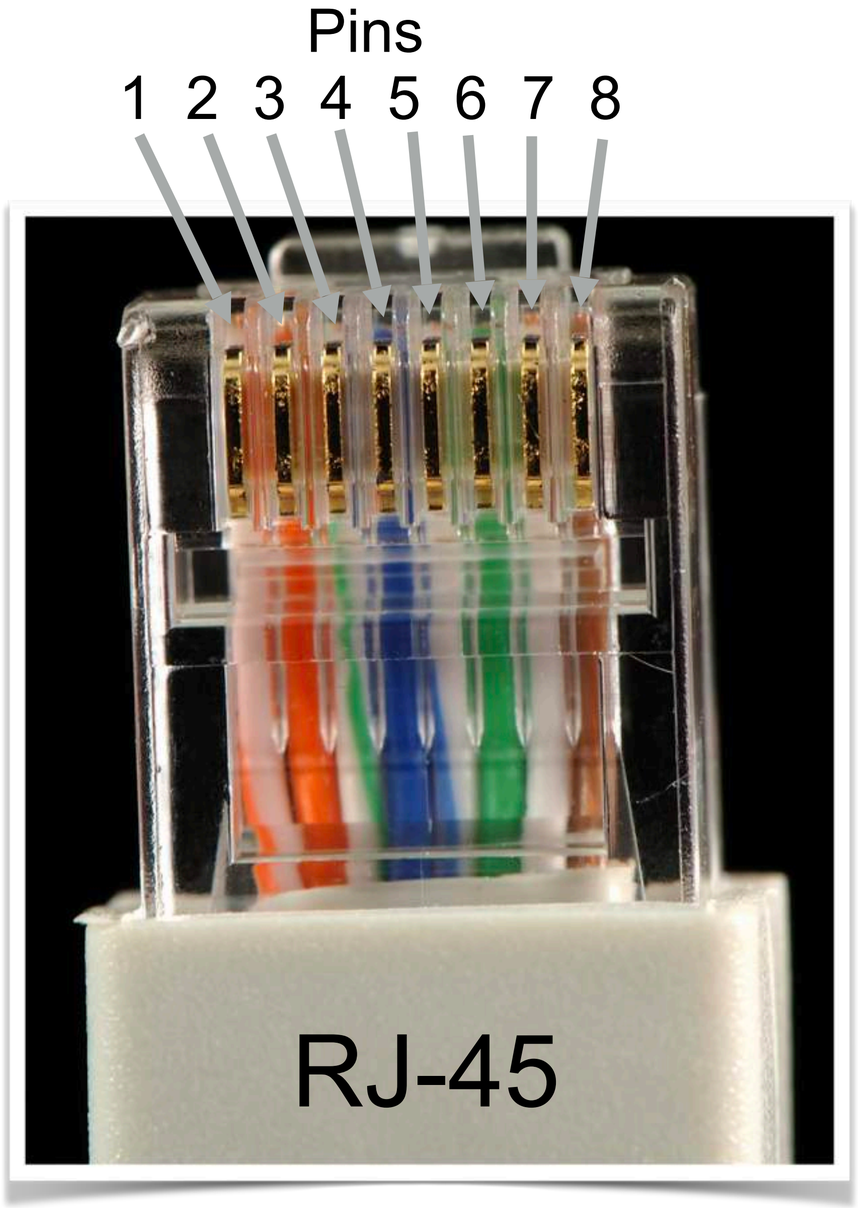
- Commonly connects cable modems
- Commonly used with RG-6 and RG-59 coaxial cable

BNC

- Was used with 10BASE-2 networks
- Carries radio frequencies for a variety of electronic gear
- Usually connects to 50 or 75 Ohm coaxial cable

Straight-Through vs. Crossover Cables

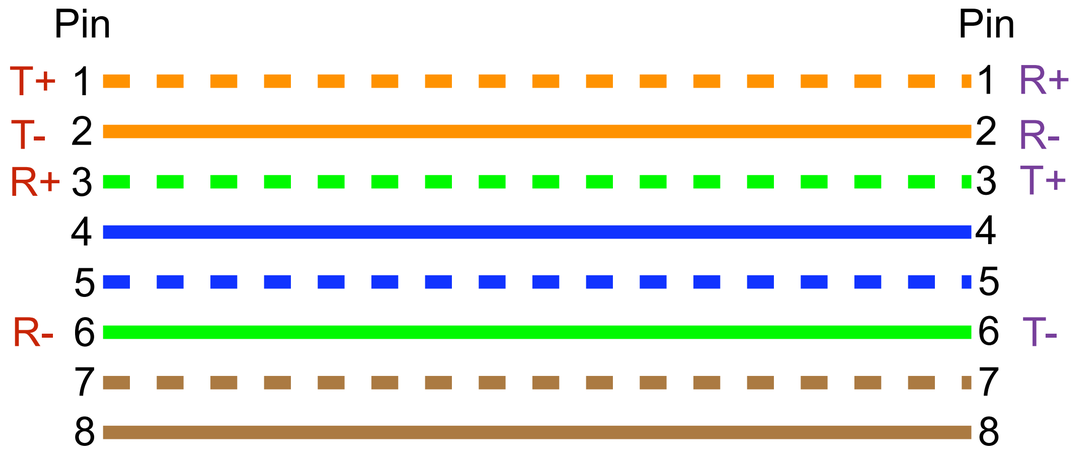
PIN	T568B
1	White/Orange
2	Orange
3	White/Green
4	Blue
5	White/Blue
6	Green
7	White/Brown
8	Brown



Straight-Through Cable

PIN	T568B
1	White/Orange
2	Orange
3	White/Green
4	Blue
5	White/Blue
6	Green
7	White/Brown
8	Brown

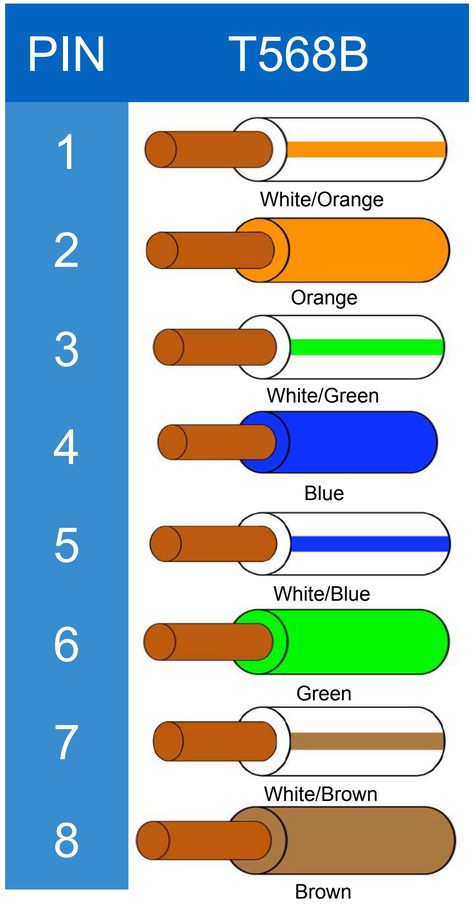
10BASE-T and 100BASE-TX

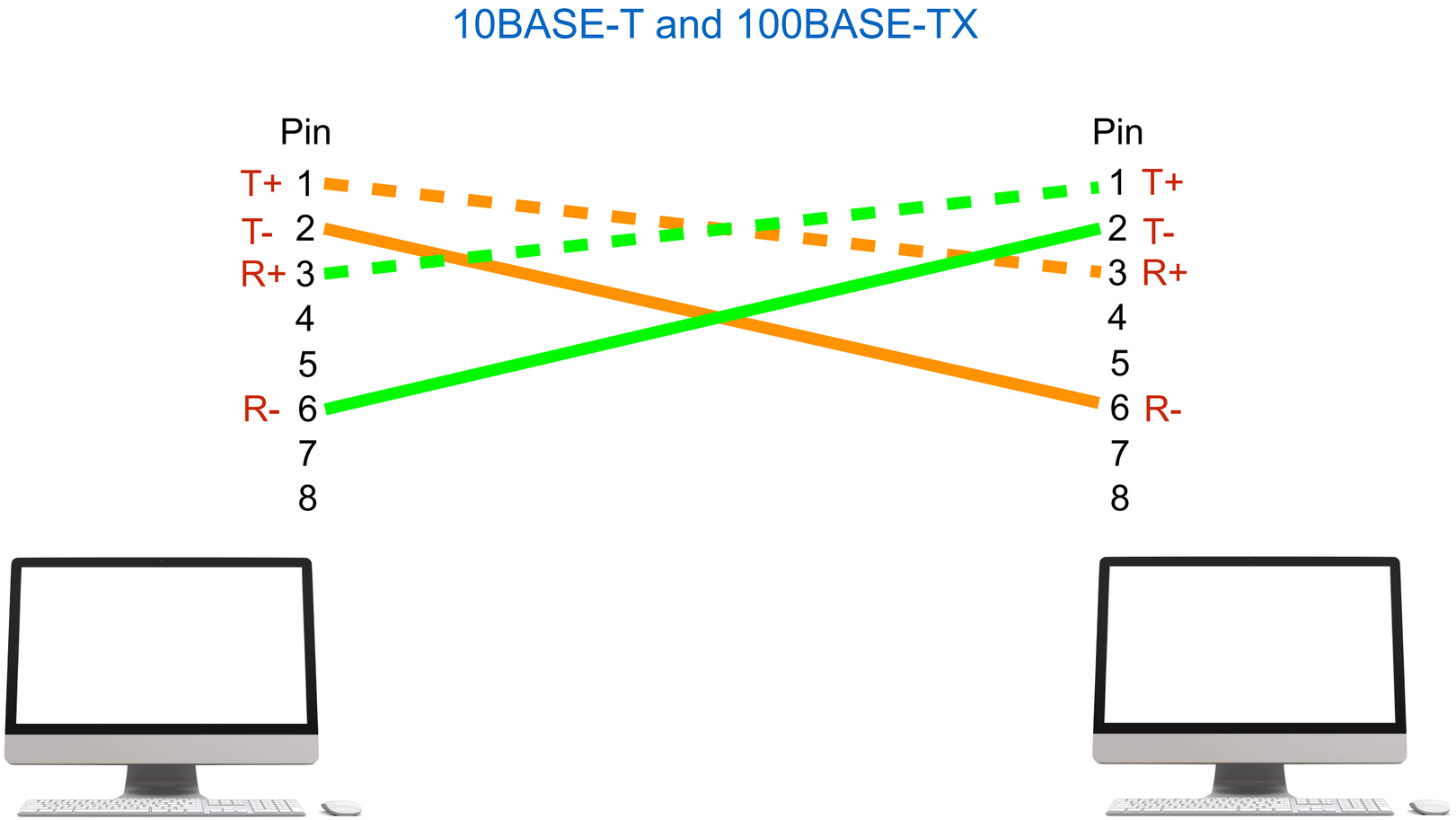


Media Dependent Interface (MDI)

Media Dependent Interface Crossover (MDI-X)

Crossover Cable





Straight-Through Cable

PIN	T568B
1	White/Orange
2	Orange
3	White/Green
4	Blue
5	White/Blue
6	Green
7	White/Brown
8	Brown

1000BASE-T

Pin		Pin
DA+ 1		1 DB+
DA- 2		2 DB-
DB+ 3		3 DA+
DC+ 4		4 DD+
DC- 5		5 DD-
DB- 6		6 DA-
DD+ 7		7 DC+
DD- 8		8 DC-

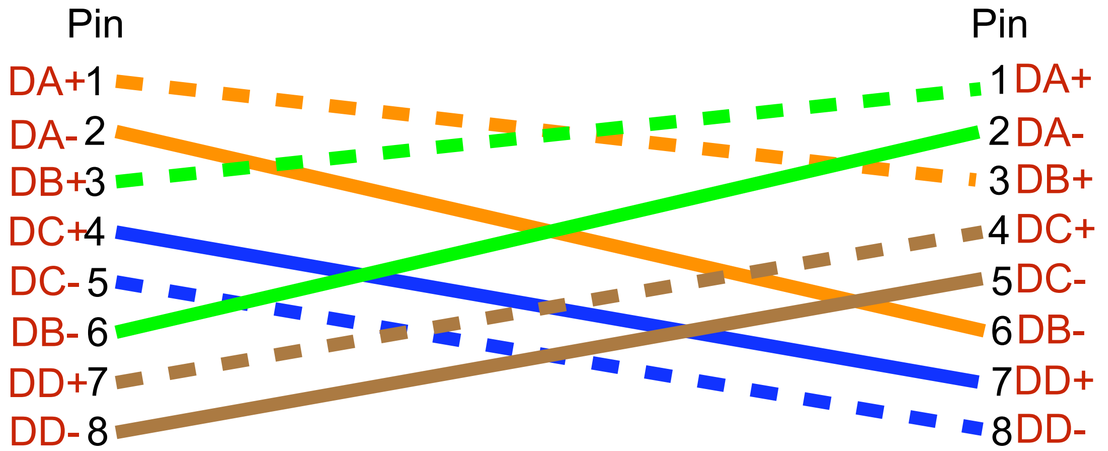
Media Dependent Interface (MDI)

Media Dependent Interface Crossover (MDI-X)

Crossover Cable

PIN	T568B
1	White/Orange
2	Orange
3	White/Green
4	Blue
5	White/Blue
6	Green
7	White/Brown
8	Brown

1000BASE-T



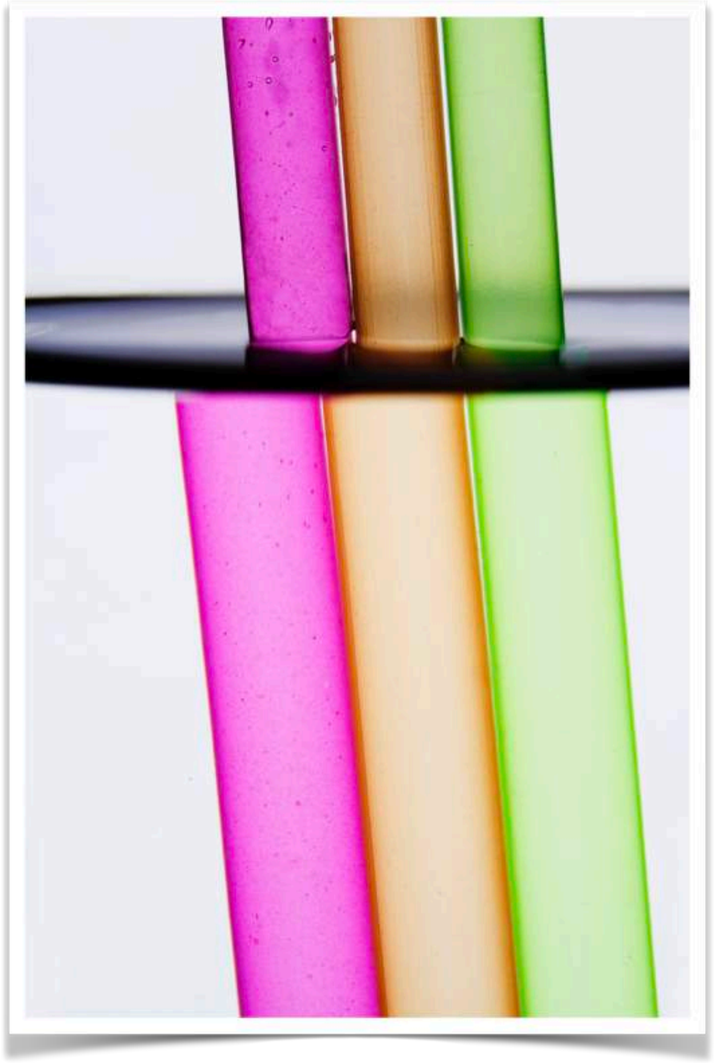
Media Dependent Interface (MDI)

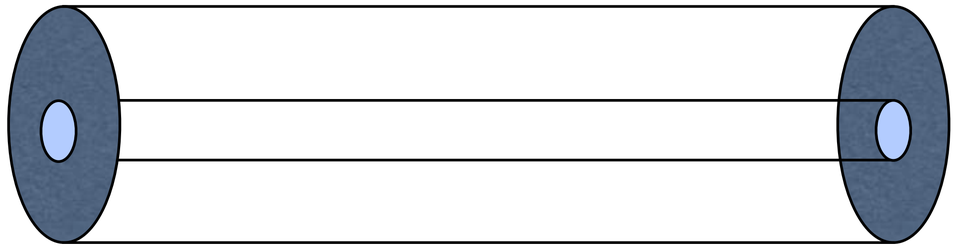
Media Dependent Interface (MDI)

Fiber Cables

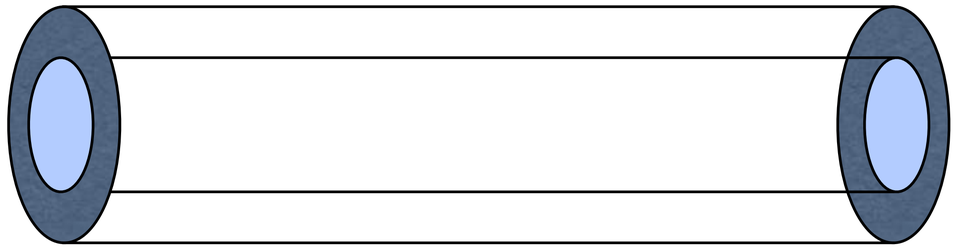
- Single-Mode Fiber (SMF)
- Multimode Fiber (MMF)

Fiber Optic Modes





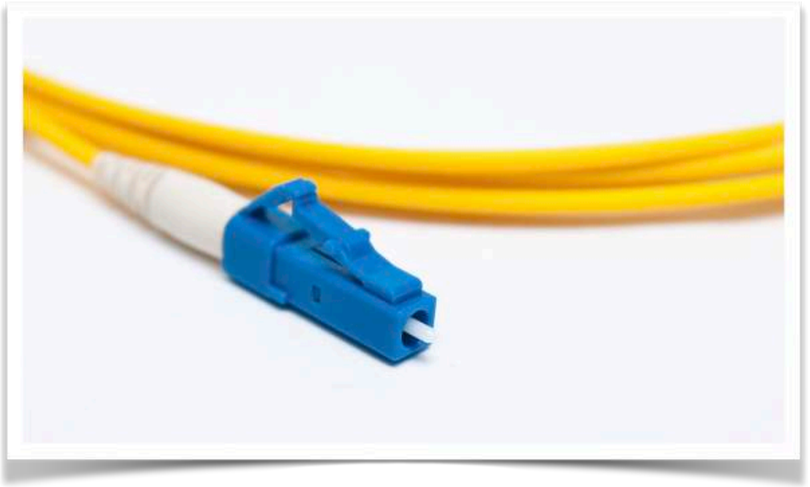
Single-Mode Fiber



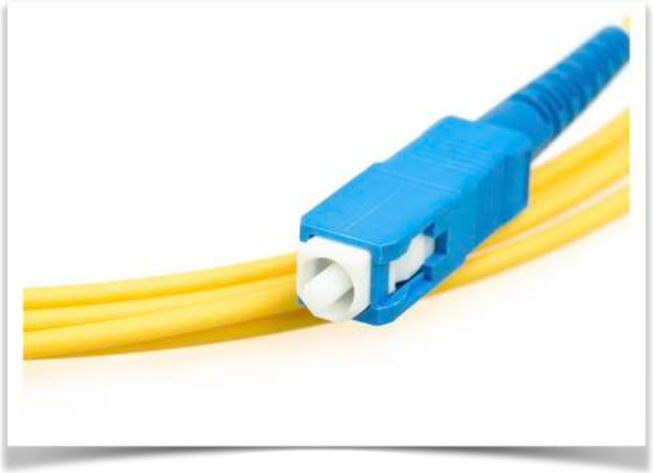
Multimode Fiber

Fiber Connectors

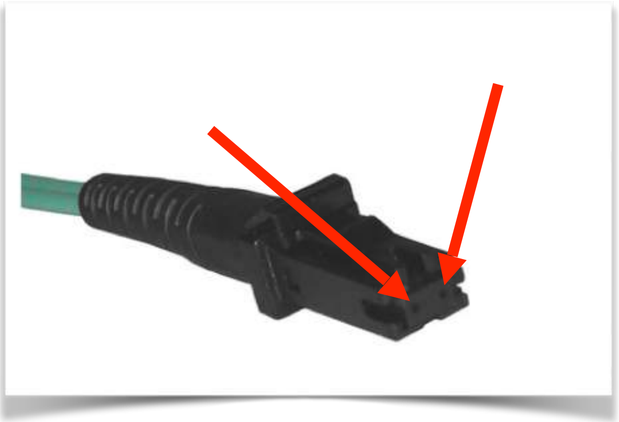
ST



LC

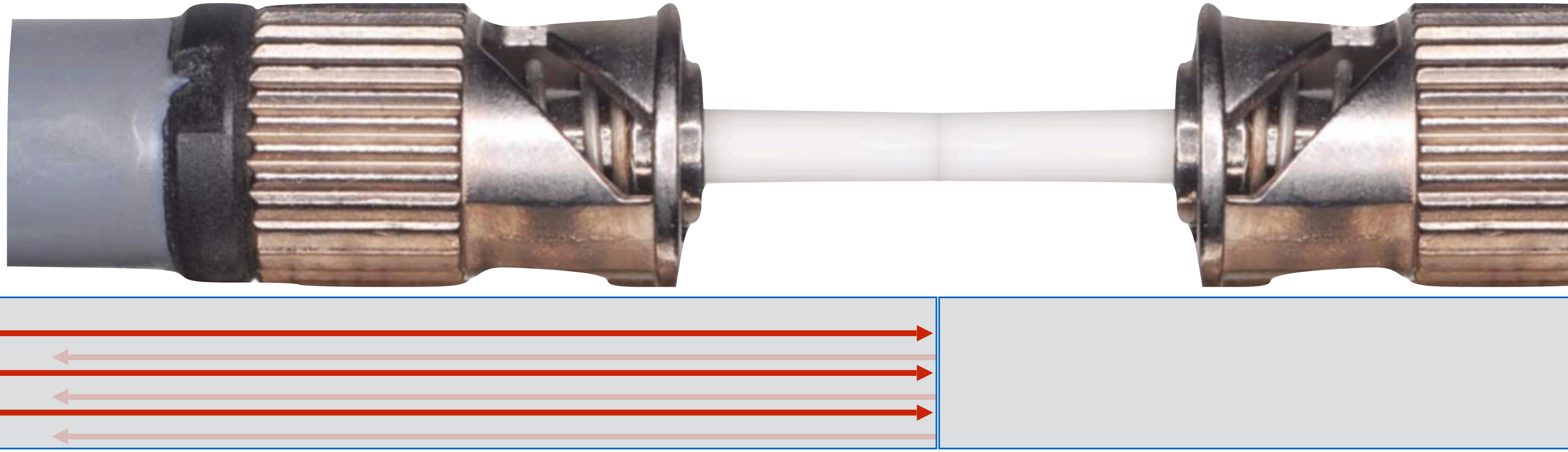


SC



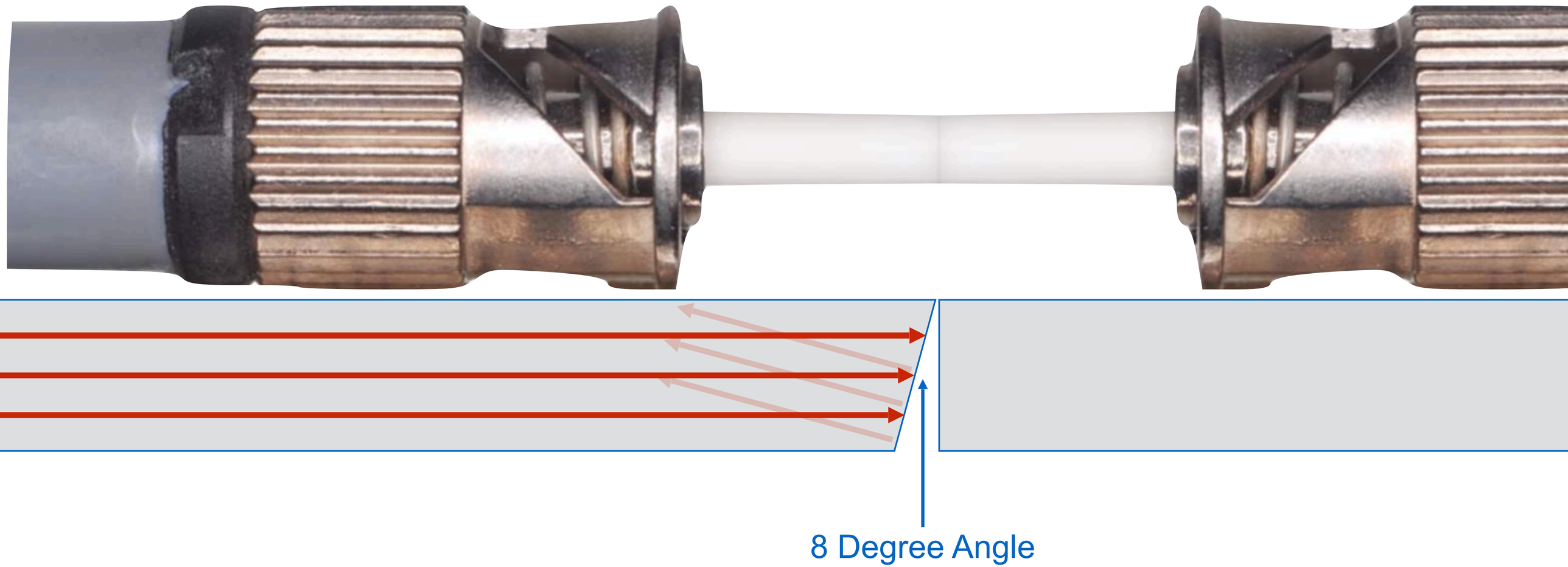
MTRJ

Fiber Connectors



Ultra Physical Contact (UPC)

Fiber Connectors



Angled Physical Contact (APC)

Ethernet Standards

Ethernet Standard	Media Type	Bandwidth Capacity	Distance Limitation
100BASE-TX	Cat 5 (or higher) UTP	100 Mbps	100 m
1000BASE-T	Cat 5 (or higher) UTP	1 Gbps	100 m
1000BASE-LX	MMF/SMF	1 Gbps/1 Gbps	550 m/5 km
1000BASE-SX	MMF	1 Gbps	220 m (62.5mm)/550 m (50mm)
10GBASE-T	Cat 6/Cat 6a (or higher)	10 Gbps	55 m/100 m

Transceivers

GBIC

SFP

SFP+

QSFP

Gigabit Interface Converter (GBIC)

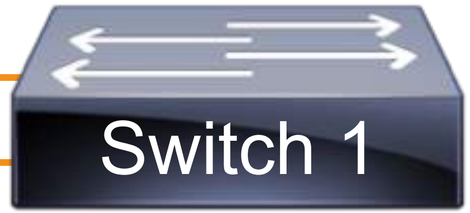
Small Form-factor Pluggable (SFP) Transceiver

SFP+

Quad SFP (QSFP)

BiDi Transceiver

Tx



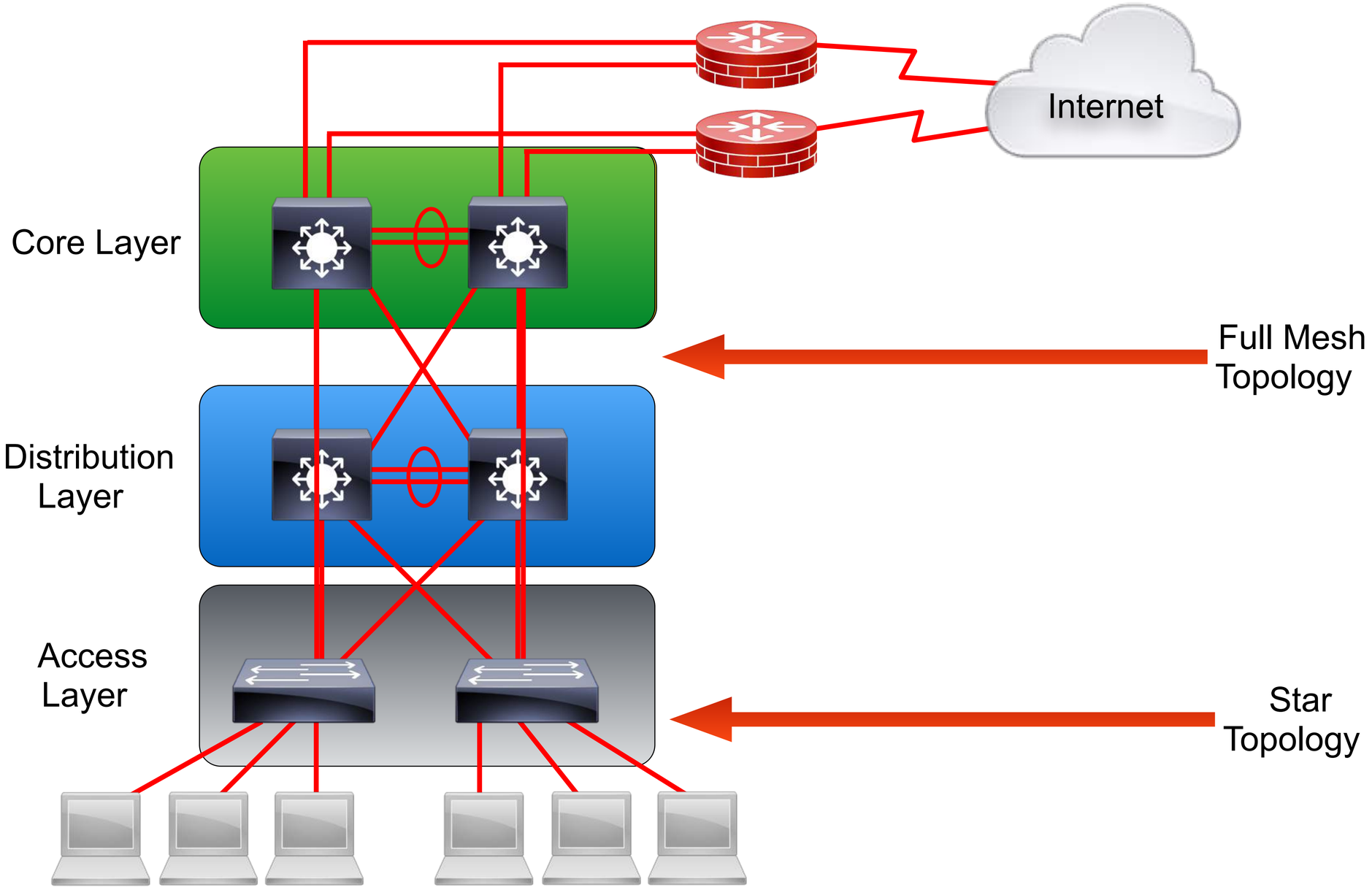
Rx

Full-Duplex

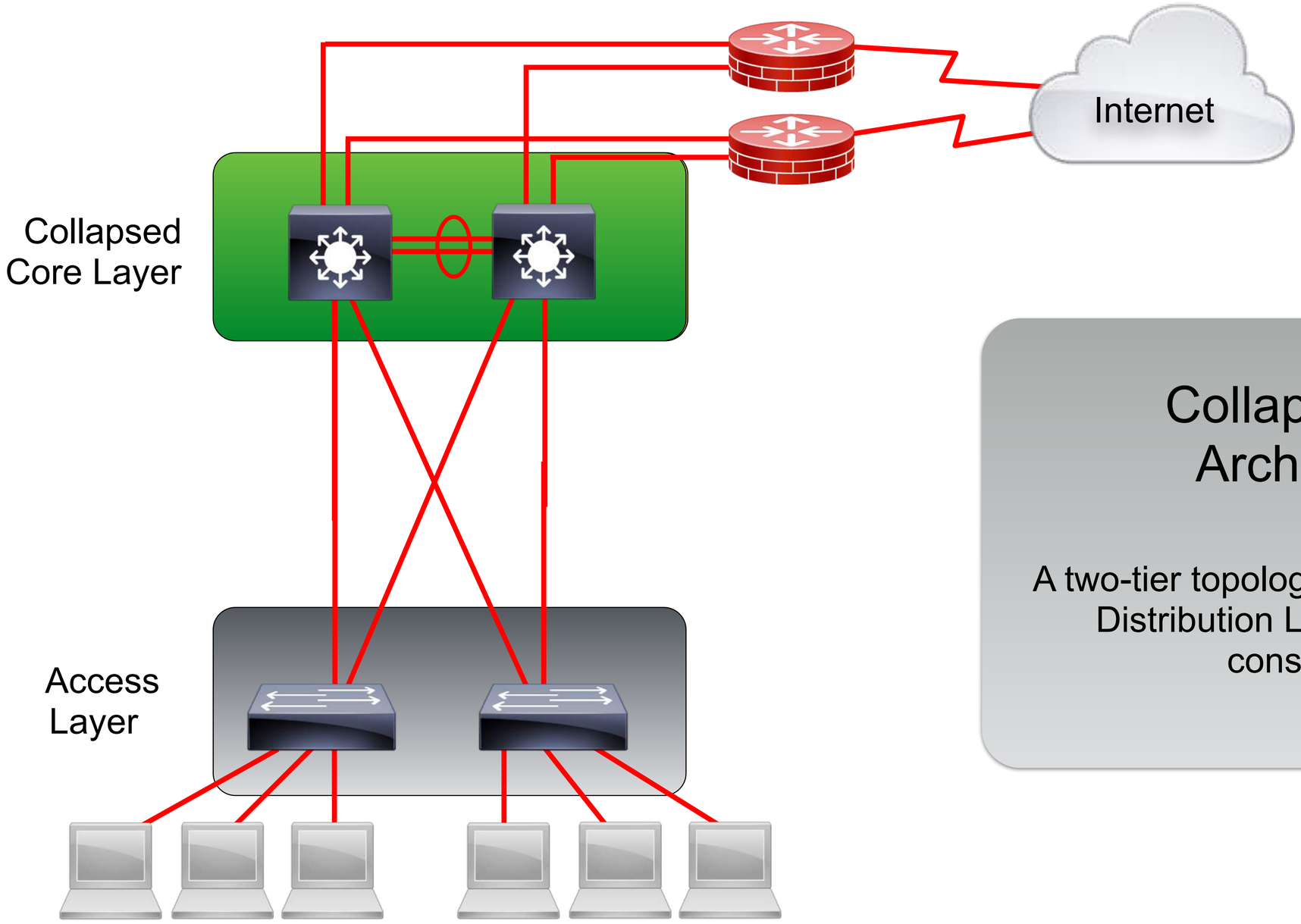
Tx and Rx

Bidirectional Transceiver (BiDi Transceiver)

Collapsed Core vs. Three-Tier Architectures



Collapsed Core vs. Three-Tier Architectures

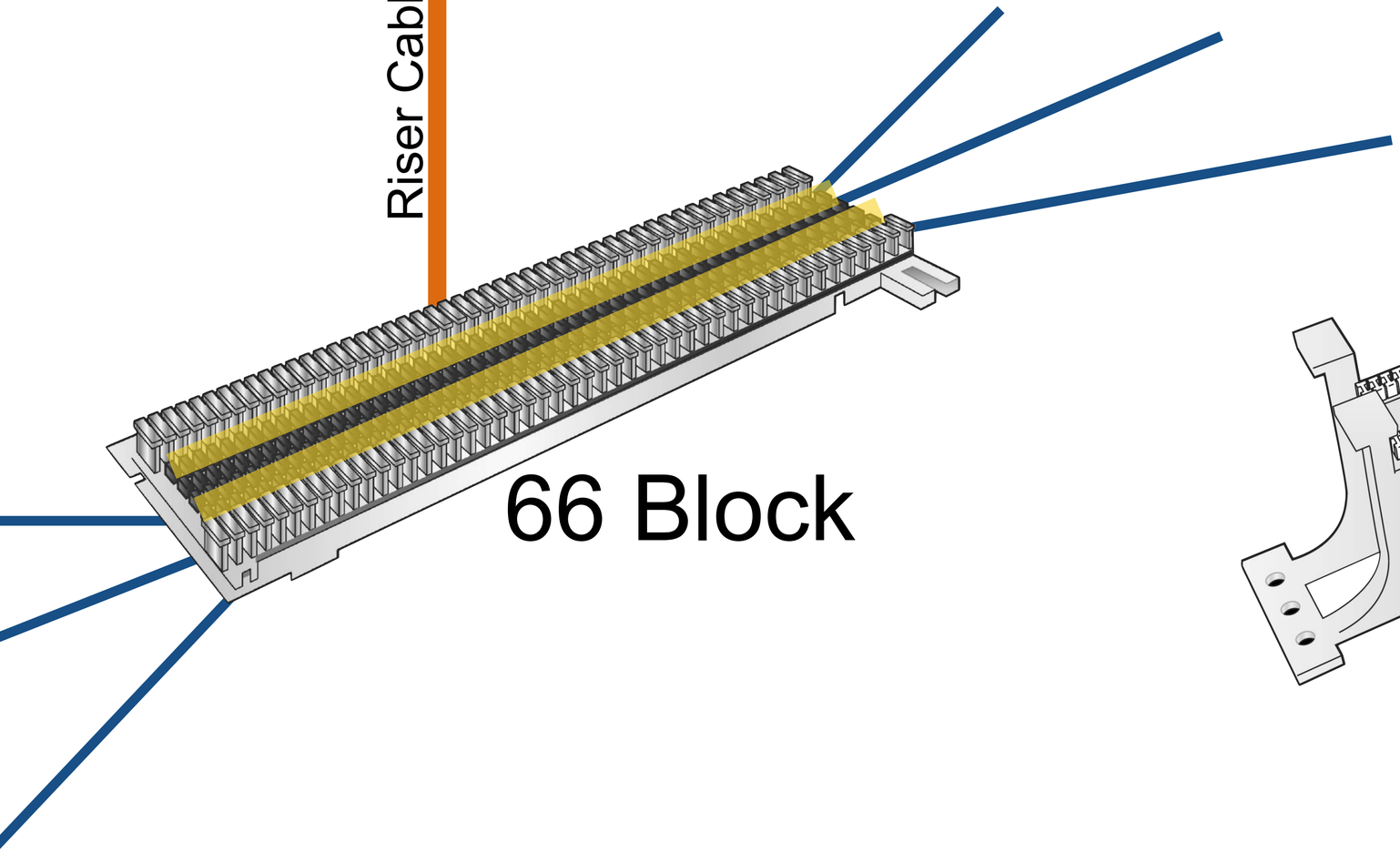


Collapsed Core Architecture

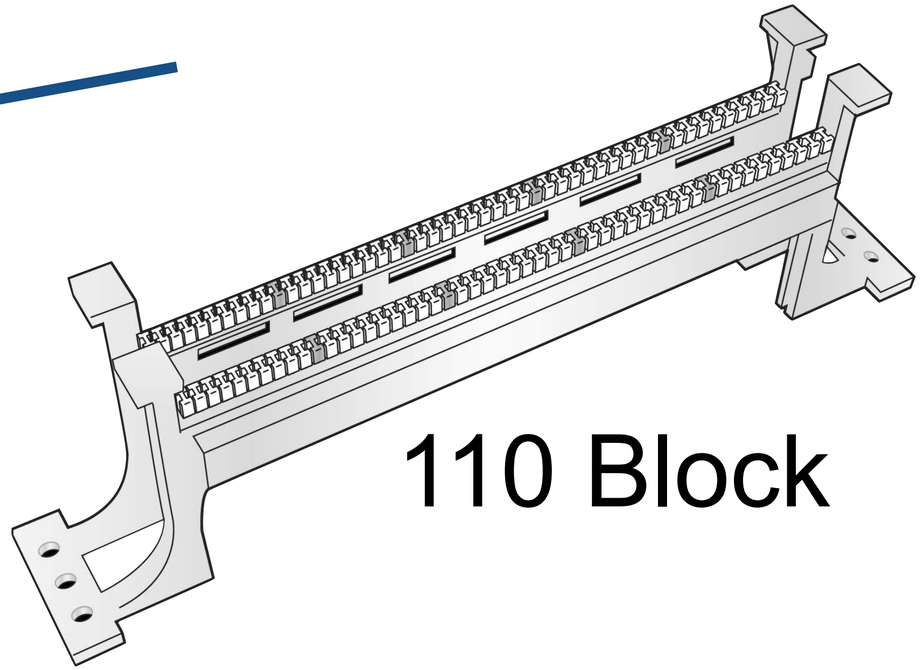
A two-tier topology where the Core and Distribution Layers have been consolidated.

66 and 110 Blocks

Riser Cable



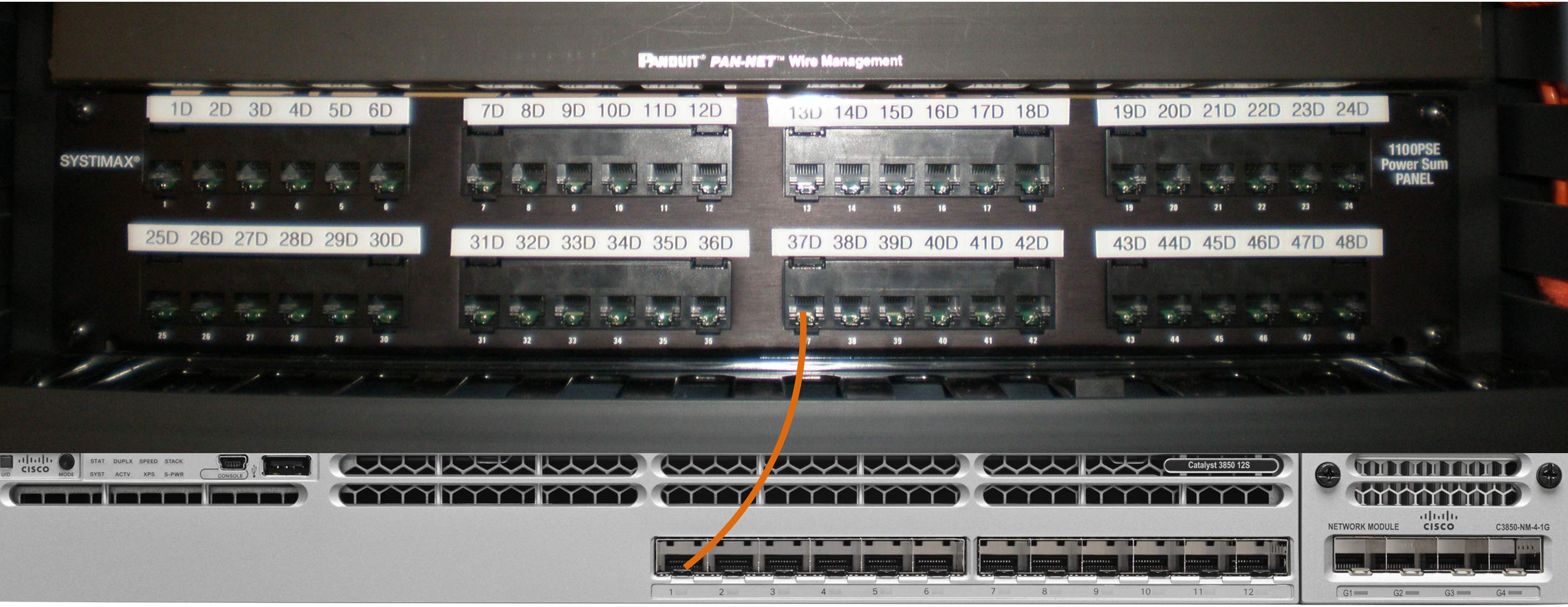
66 Block



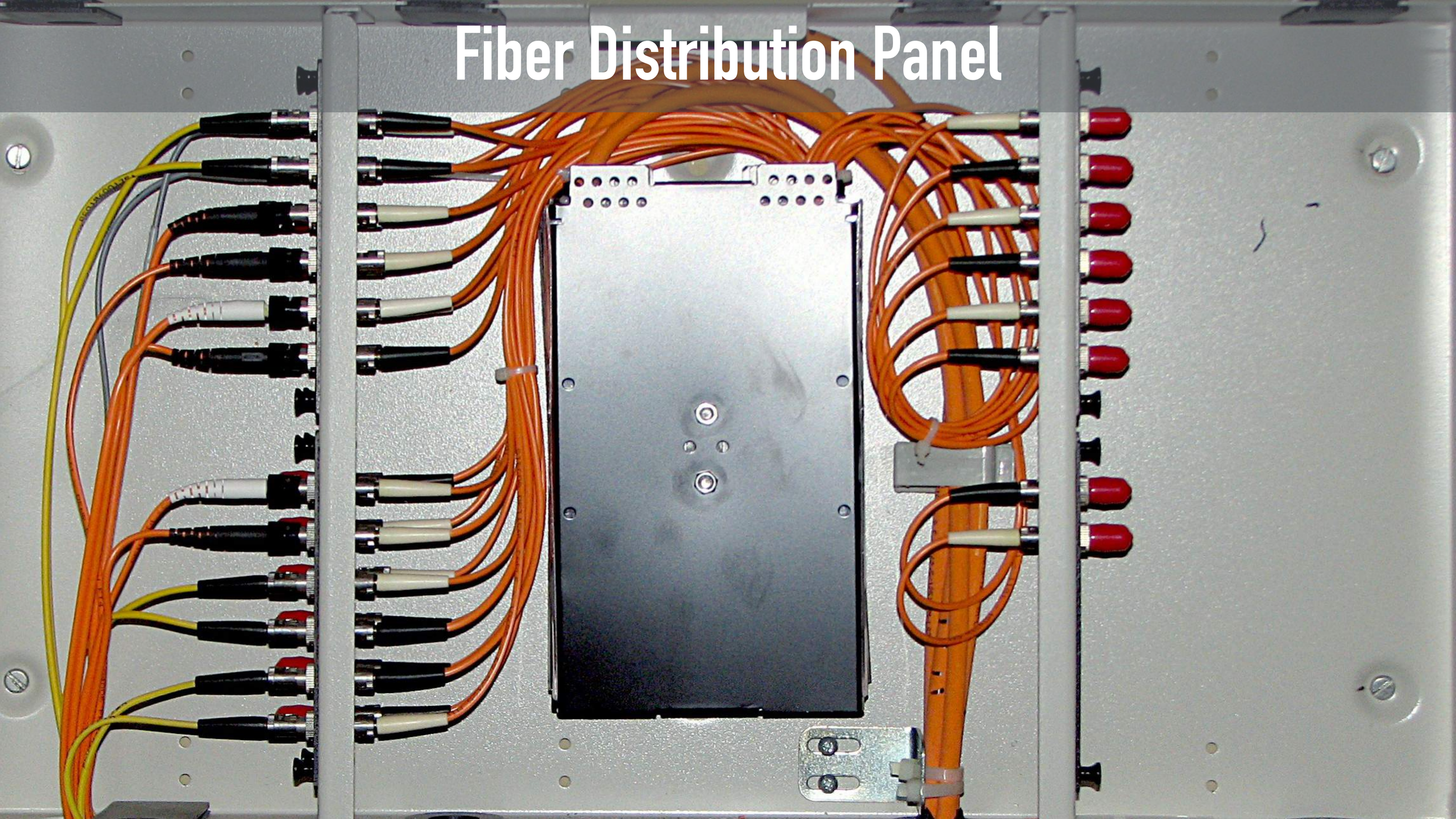
110 Block

Punch Down Tool

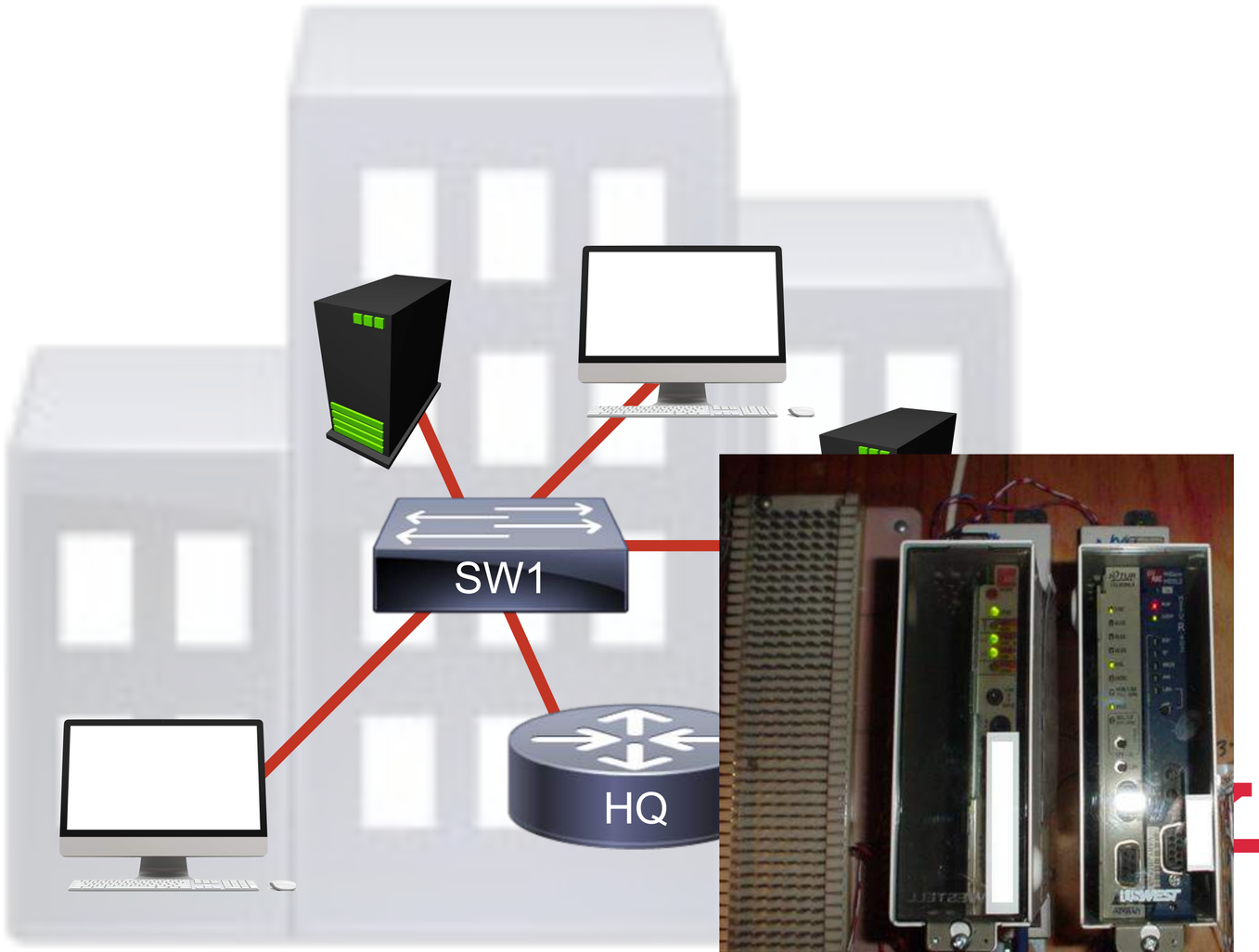
Patch Panel


PANDUIT® PAN-NET™ Wire Management
SYSTIMAX®
1100PSE
Power Sum
PANEL
1D 2D 3D 4D 5D 6D
7D 8D 9D 10D 11D 12D
13D 14D 15D 16D 17D 18D
19D 20D 21D 22D 23D 24D
25D 26D 27D 28D 29D 30D
31D 32D 33D 34D 35D 36D
37D 38D 39D 40D 41D 42D
43D 44D 45D 46D 47D 48D
Catalyst 3850 12S
NETWORK MODULE
C3850-NM-4-1G

Fiber Distribution Panel

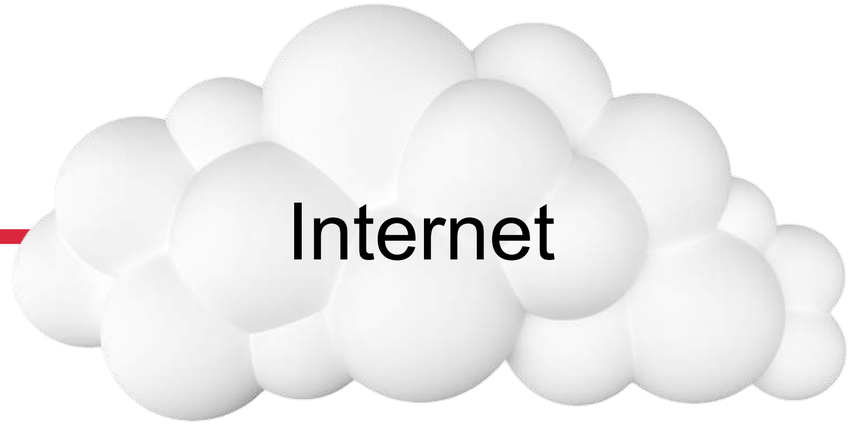


Demarcation Point (Demarc) and Smart Jack



Demarcation Point: Where network maintenance responsibility passes from the WAN provider to the customer.

Smart Jack: A network device (commonly located at a demarc) that can perform diagnostic tests on the connected circuit.



Cabling Tools

Crimper

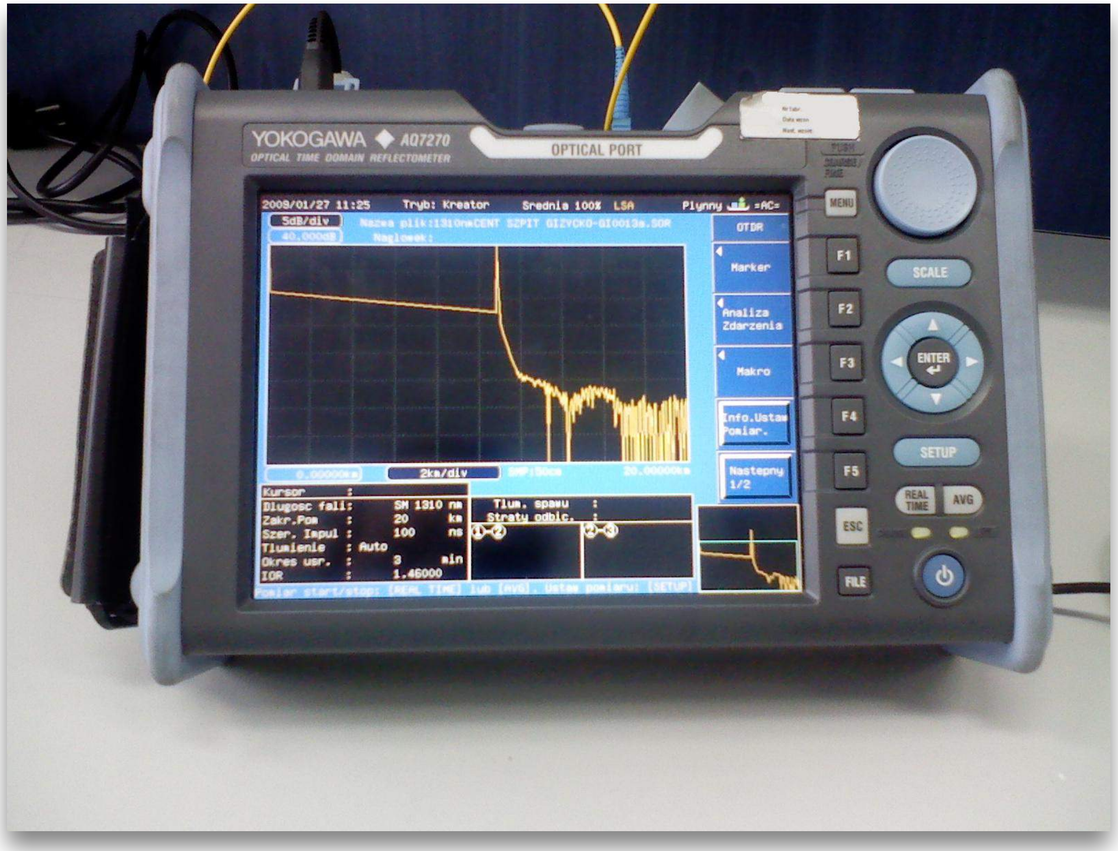
Cabling Tools

Cable Tester

Cabling Tools

Punch Down Tool

Cabling Tools

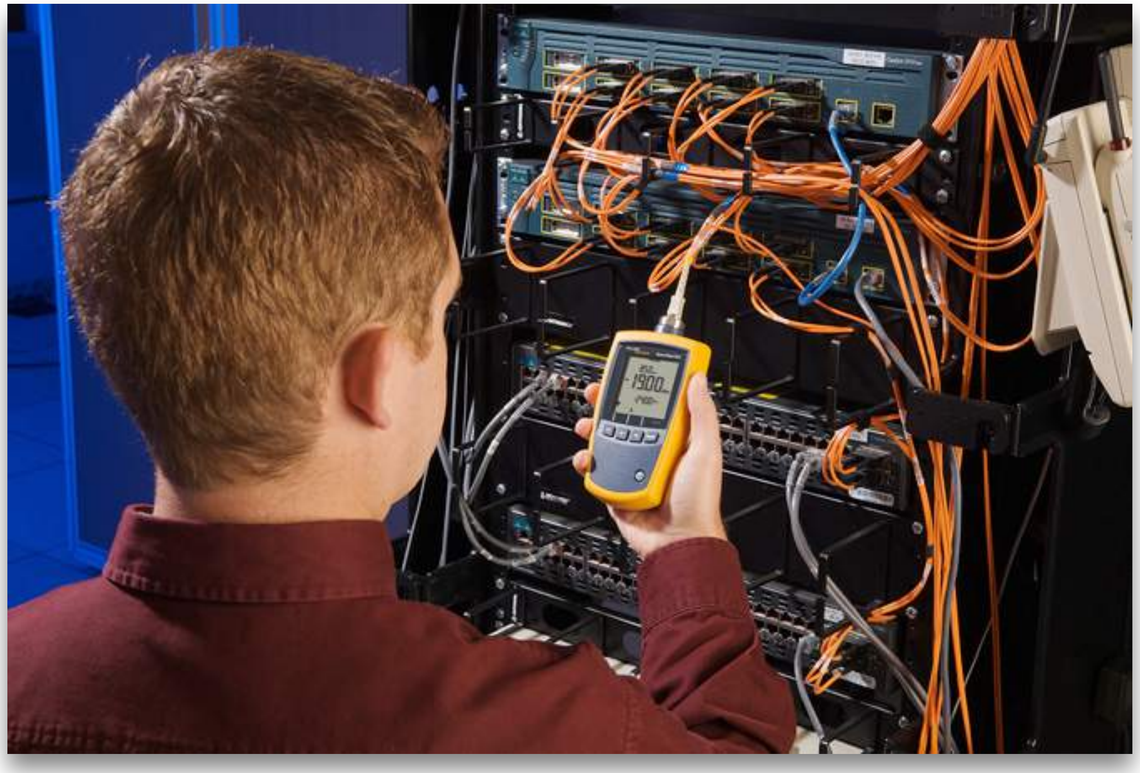


OTDR

Cabling Tools

BERT

Cabling Tools



Light Meter

Cabling Tools

Tone Generator

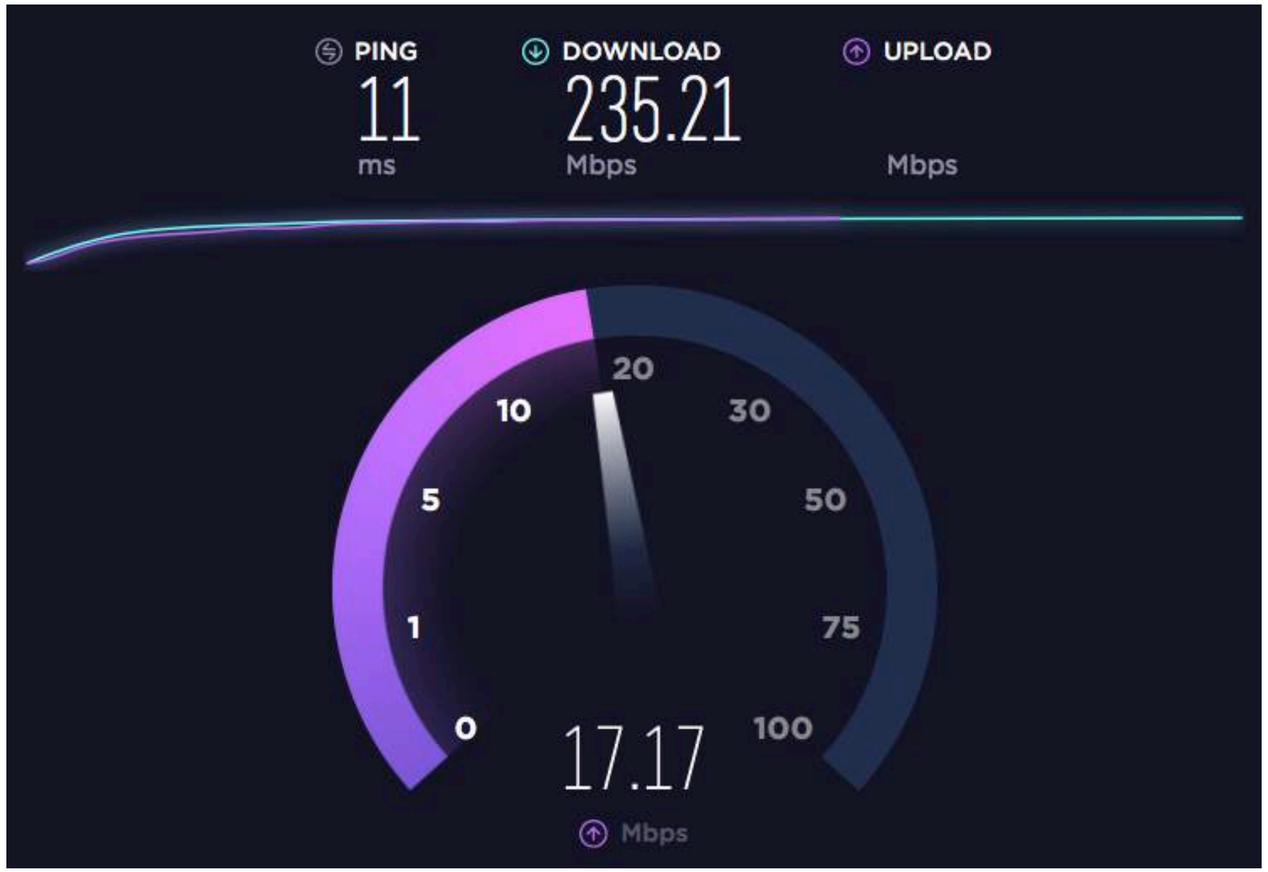
Cabling Tools

Loopback Adapter

Cabling Tools

Multimeter

Cabling Tools



Bandwidth Speed Tester

Cabling Tools

Spectrum Analyzer

Cabling Tools

- Crimper
- Cable Tester
- Punchdown Tool
- OTDR
- BERT
- Light Meter
- Tone Generator
- Loopback Adapter
- Multimeter
- Bandwidth Speed Tester
- Spectrum Analyzer

Module 6
Cables and Connectors

Q & A