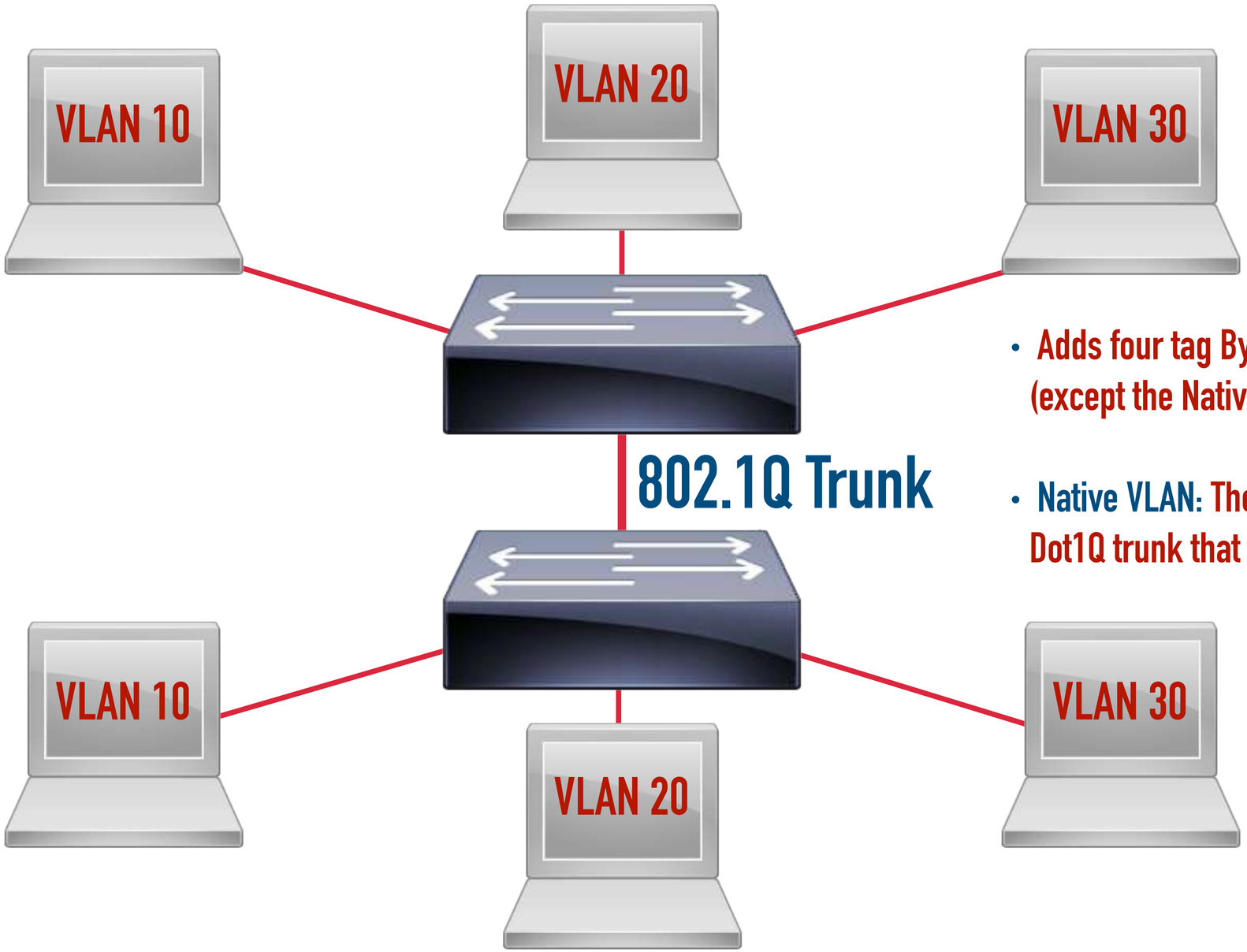
Module 3
Infrastructure Technologies

Layer 2 Infrastructure Technologies

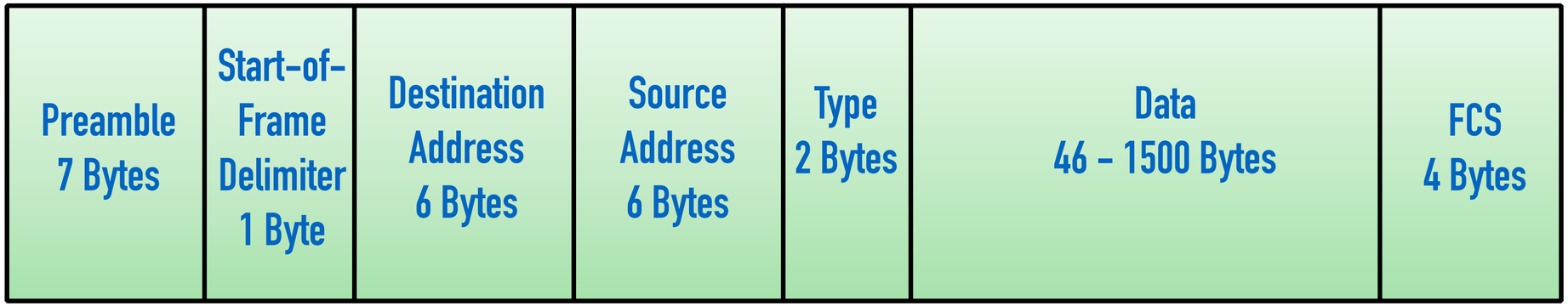
IEEE 802.1Q Trunk

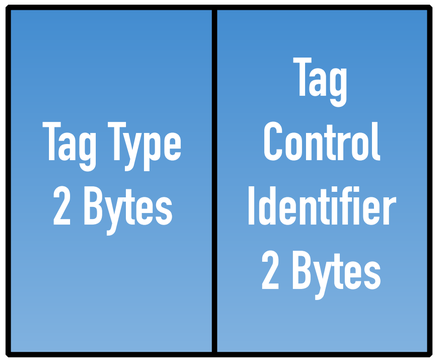


- Adds four tag Bytes to each frame (except the Native VLAN)
- Native VLAN: The one VLAN on a Dot1Q trunk that is untagged

IEEE 802.1Q Frame Format

Ethernet Frame





IEEE 802.1Q Frame

Troubleshooting 802.1Q Trunks

- Inter-Switch Link (ISL): A Cisco proprietary trunking protocol
- IEEE 802.1Q: An industry-standard trunking protocol

Troubleshooting 802.1Q Trunks

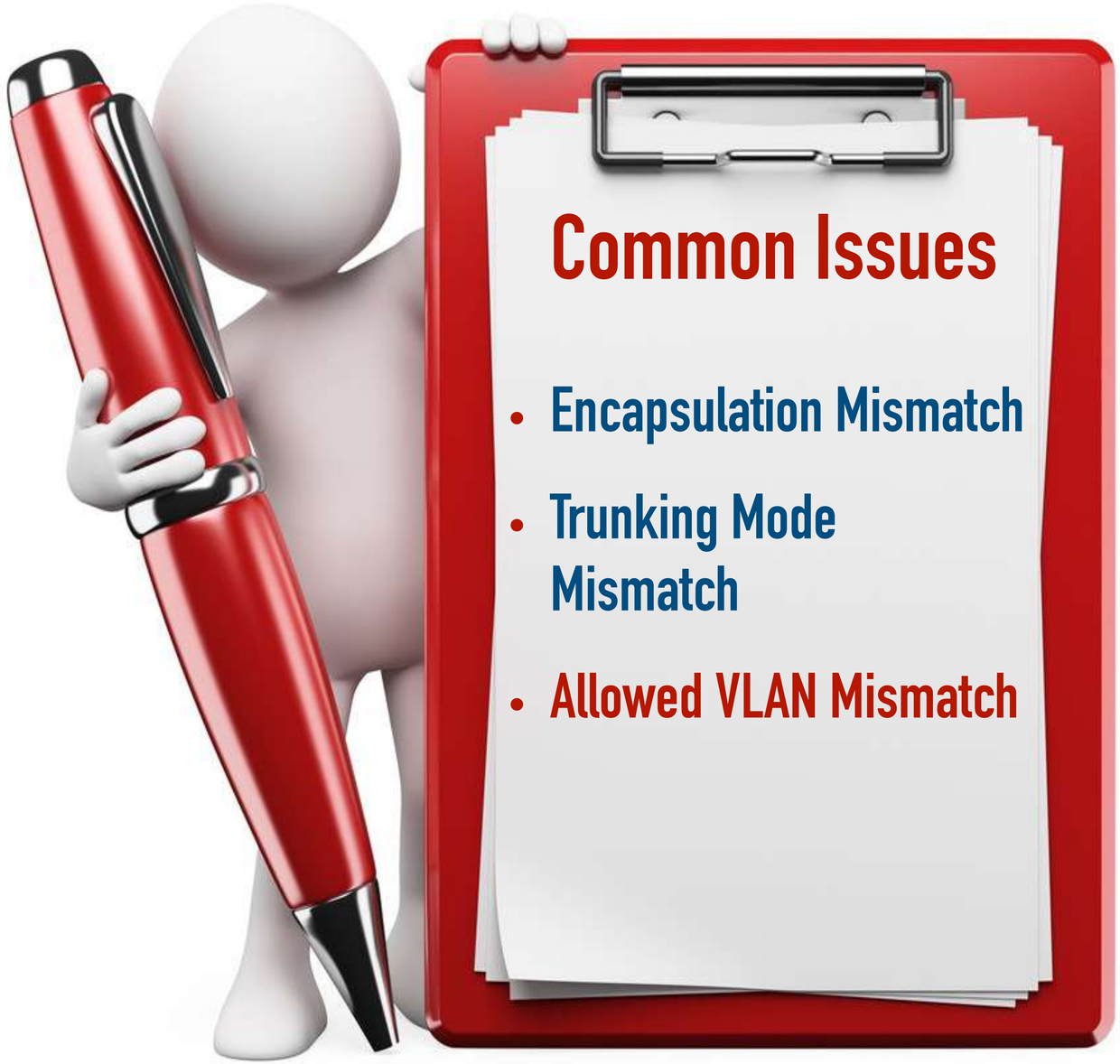
Common Issues

- Encapsulation Mismatch
- Trunking Mode Mismatch

Mode	Description
access	Forces a port to operate as an access port.
trunk	Forces a port to operate as a trunk port.
dynamic desirable	Initiates the negotiation of a trunk.
dynamic auto	Passively waits for the remote switch to initiate the negotiation of a trunk.

SW1 Mode	SW2 Mode	Trunk Formed
access	ANY	✗
trunk	dynamic desirable	✓
trunk	dynamic auto	✓
trunk	trunk	✓
dynamic desirable	dynamic desirable	✓
dynamic desirable	dynamic auto	✓
dynamic auto	dynamic auto	✗

Troubleshooting 802.1Q Trunks



Common Issues

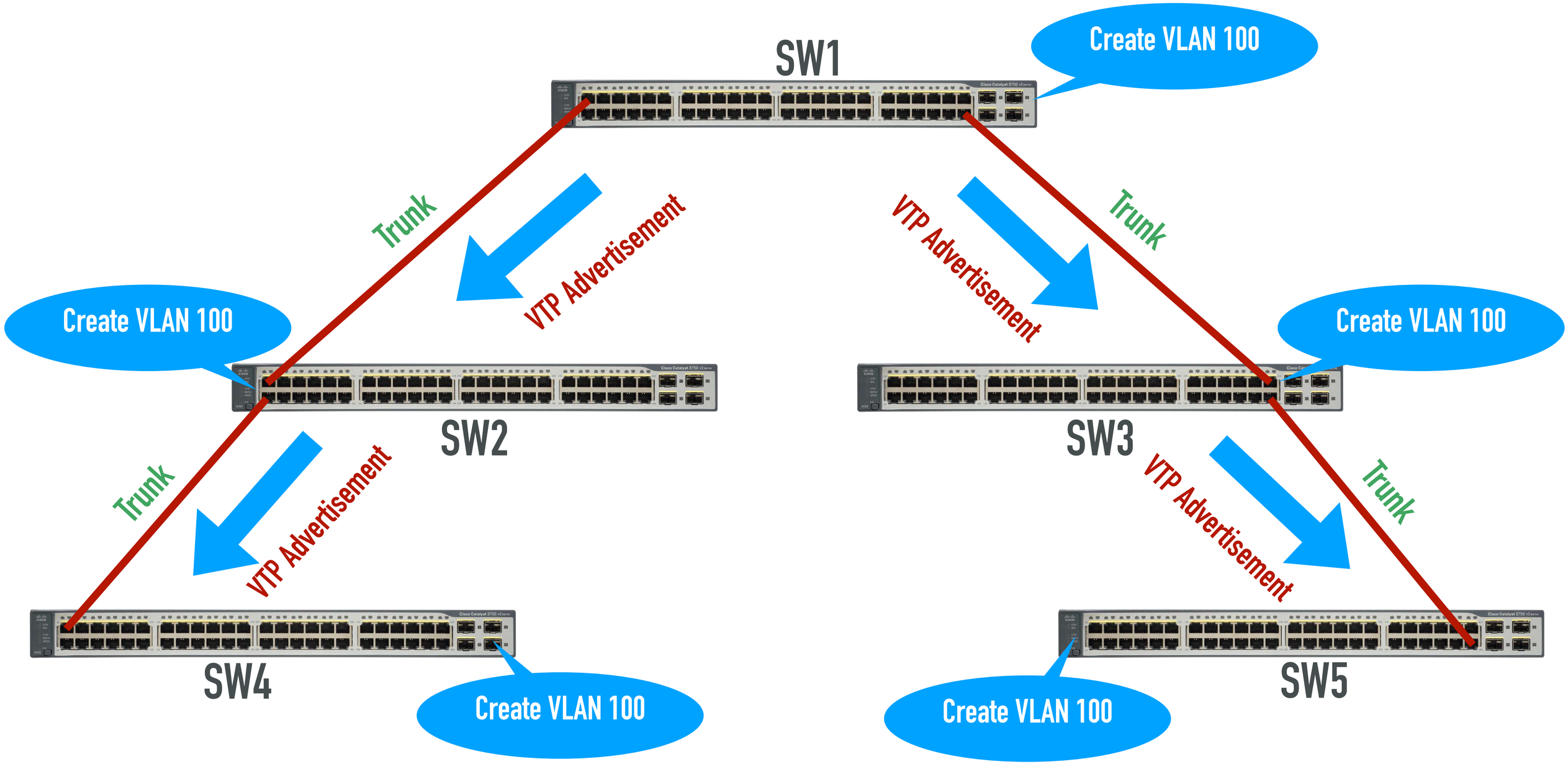
- Encapsulation Mismatch
- Trunking Mode Mismatch
- Allowed VLAN Mismatch

- Default: All VLANs allowed
- Pruning: Specifies VLANs to be allowed or denied (can improve security and performance)

Troubleshooting 802.1Q Trunks

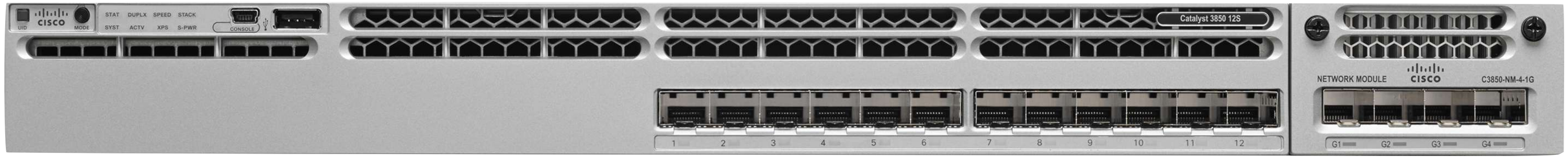
- Native VLAN: Does not add 4 Tag Bytes to a frame
- Default: VLAN 1

VLAN Trunking Protocol (VTP)

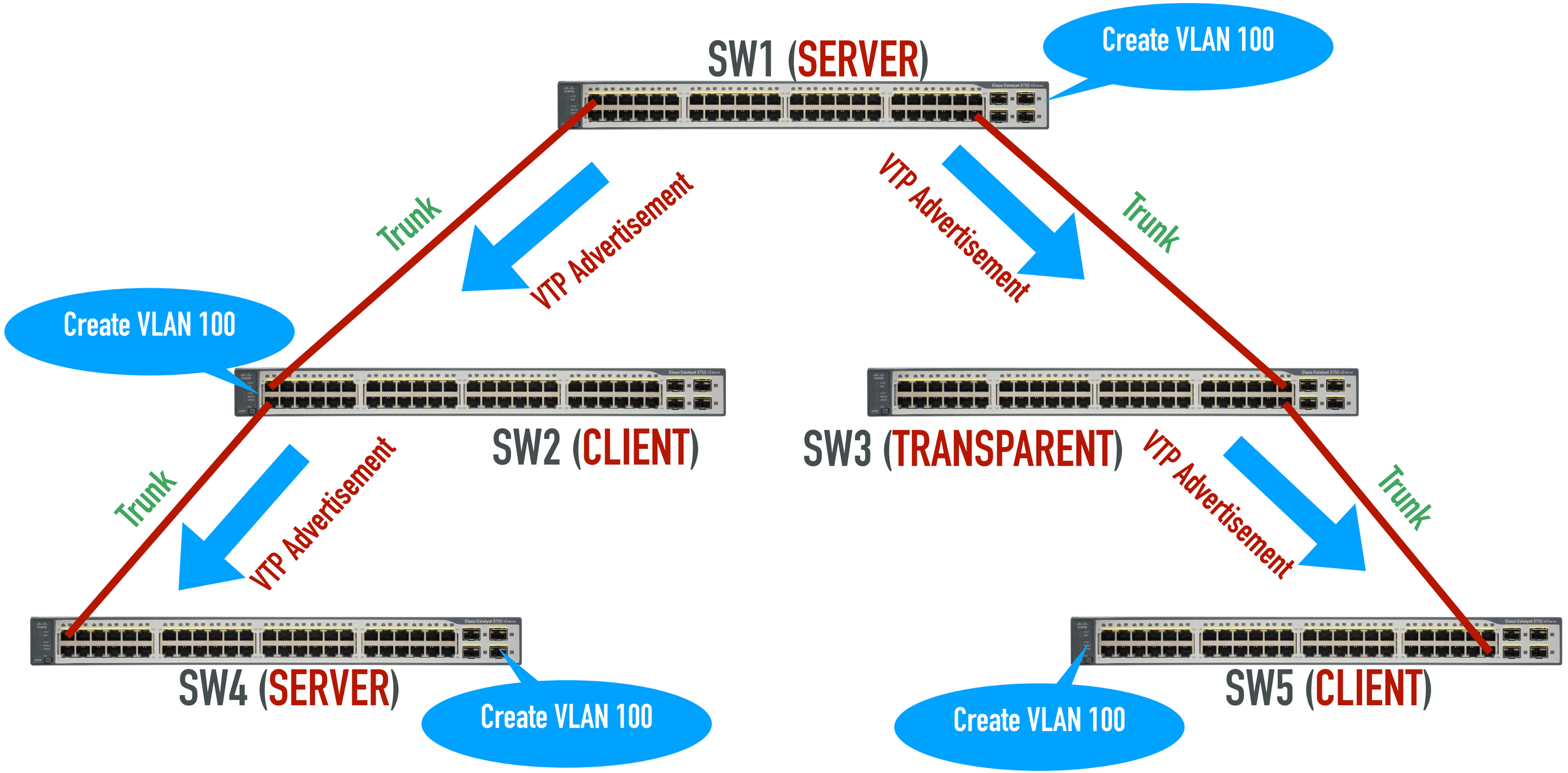


VTP Modes

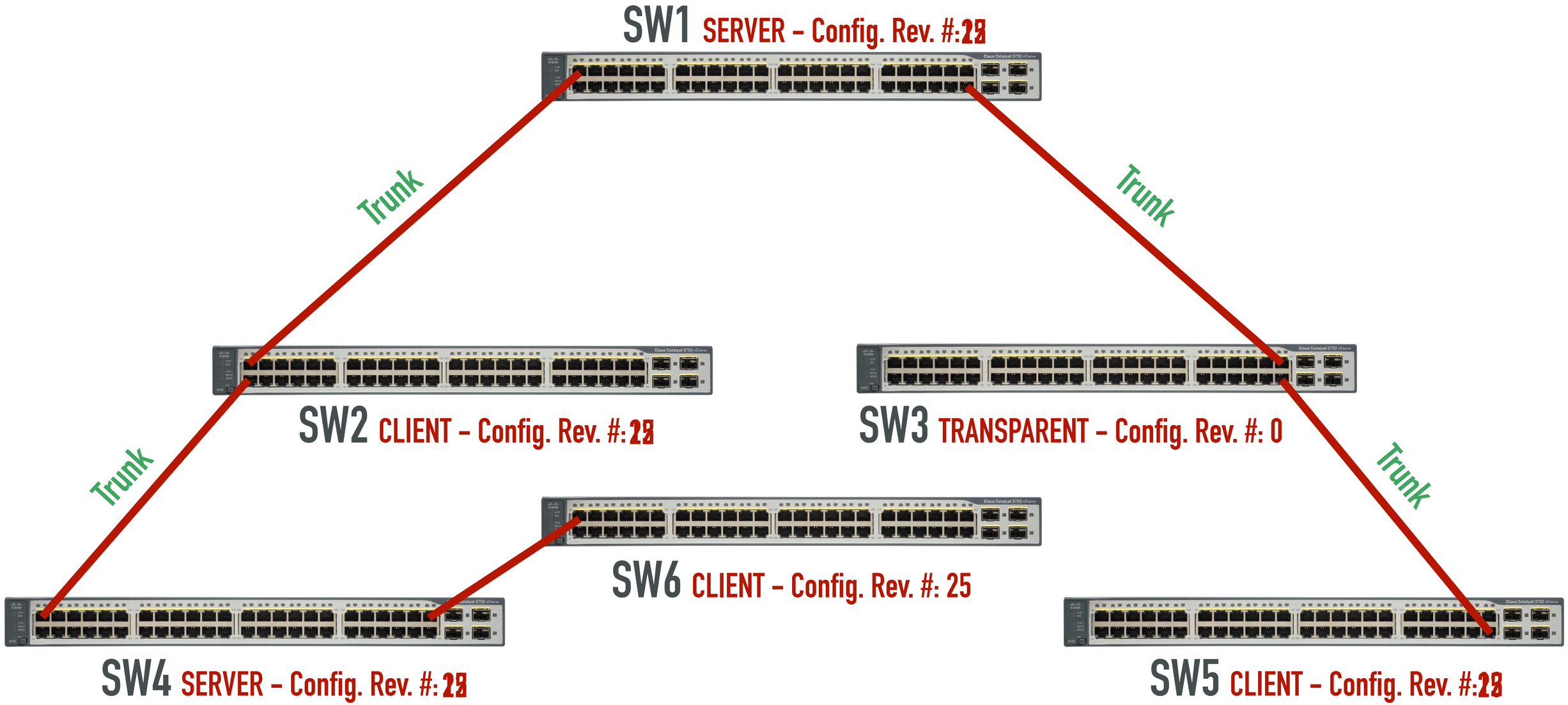
VTP Mode	Description
Server	• Can be used to create/delete/modify VLANs • Updates its VLAN database based on received advertisements • Forwards received VTP messages • Can originate VTP advertisements
Client	• Cannot be used to create/delete/modify VLANs • Updates its VLAN database based on received advertisements • Forwards received VTP messages • Can originate VTP advertisements
Transparent	• Can be used to create/delete/modify VLANs • Does not update its VLAN database based on received advertisements • Forwards received VTP messages • Does not originate VTP advertisements
Primary Server	• Available only in VTP version 3 • The only switch that can create/delete/modify VLANs • Prevents accidental overwriting of the VLAN database



VTP Modes Example

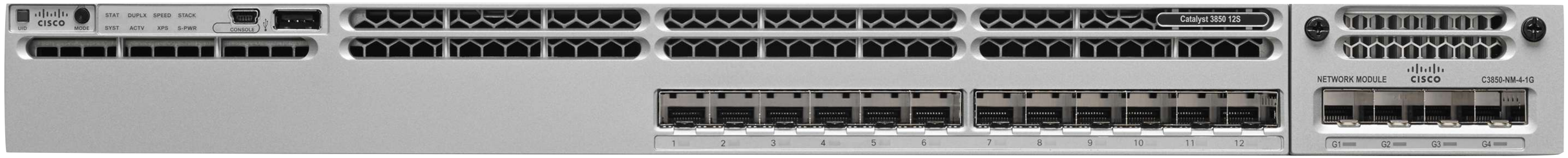


VTP Caution


SW1 SERVER – Config. Rev. #: 23
Trunk
Trunk
SW2 CLIENT – Config. Rev. #: 23
SW3 TRANSPARENT – Config. Rev. #: 0
Trunk
Trunk
SW6 CLIENT – Config. Rev. #: 25
SW4 SERVER – Config. Rev. #: 23
SW5 CLIENT – Config. Rev. #: 23

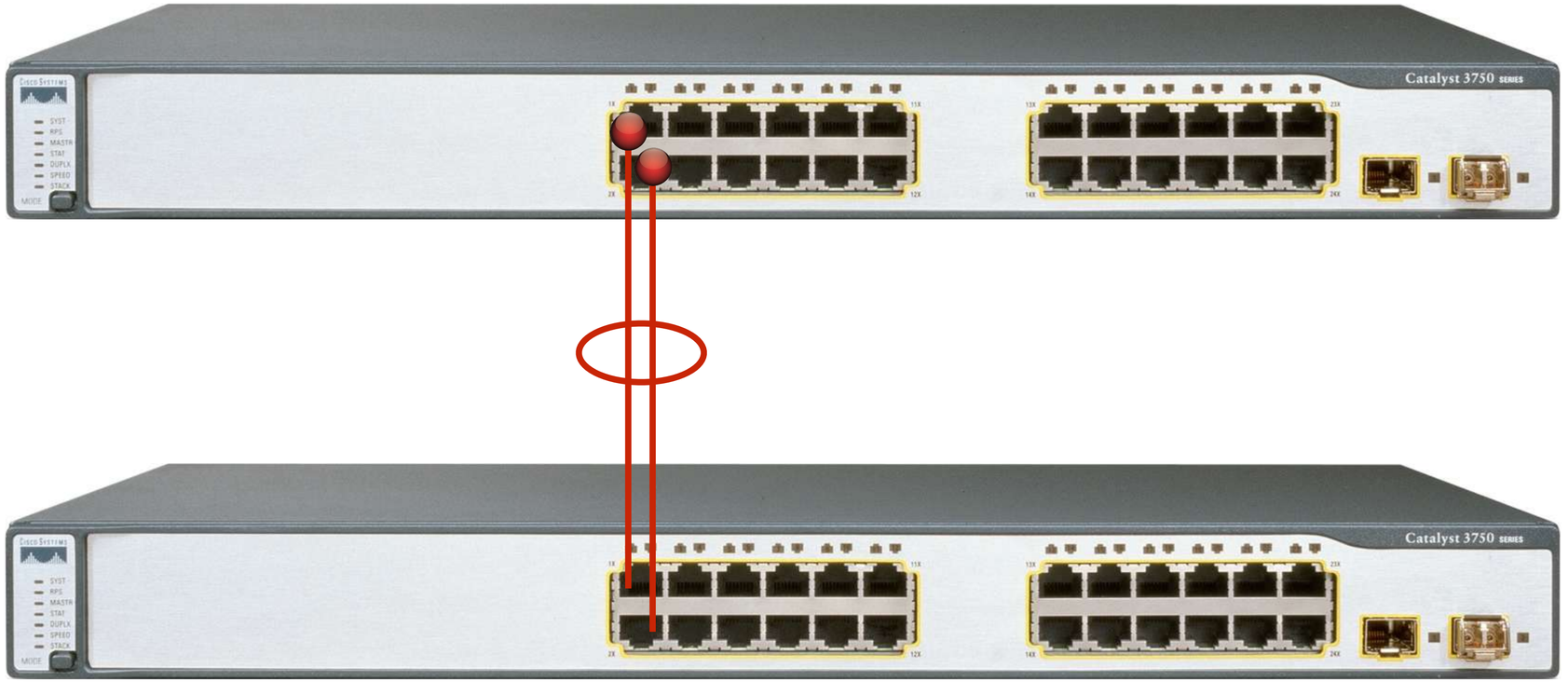
VTP Version Enhancements

VTP Version	Description
2	• Support for Token Ring VLANs • Transparent mode switch will forward a VTP frame without checking domain or version info
3	• Supports VTP Primary Server • Support for Extended VLANs (1006 – 4094) • Support for Private VLANs • MST support • Improved authentication • Support for an OFF mode • Compatible with versions 1 and 2



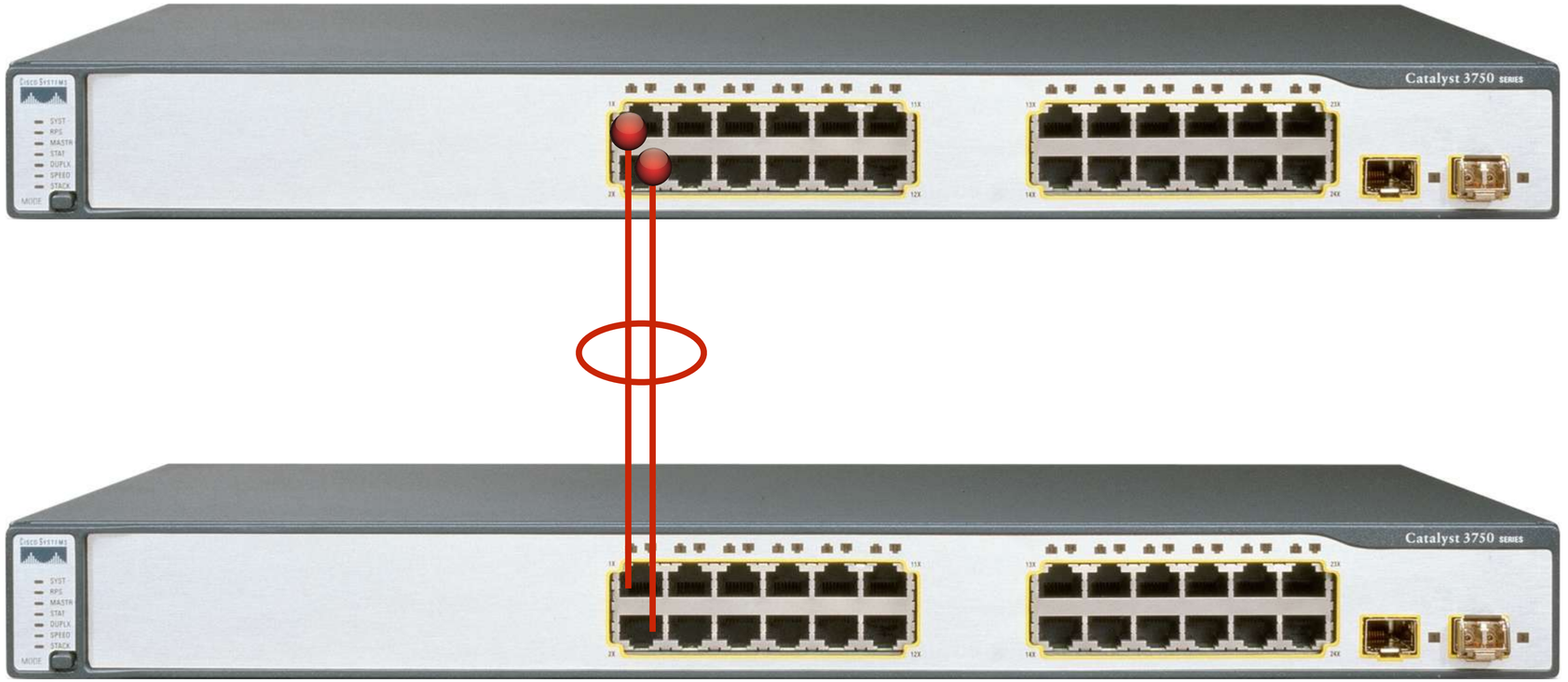
DEMO: VLAN Trunk Protocol (VTP)

Review of EtherChannel Operation



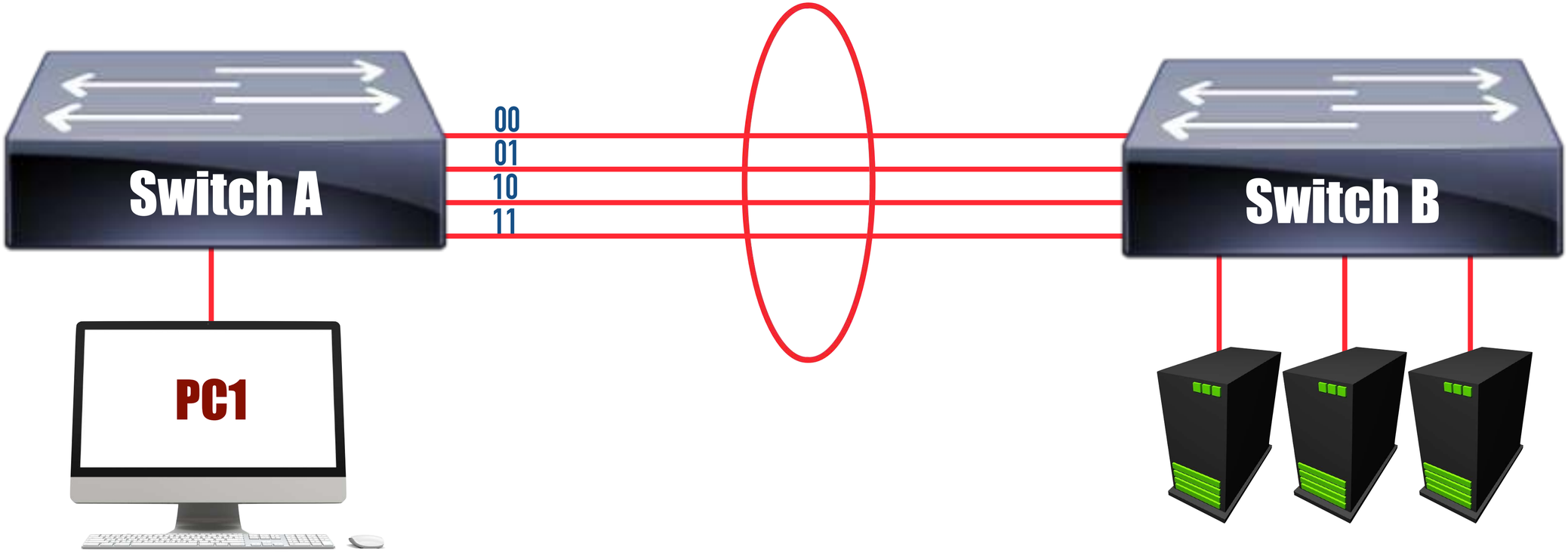
- Allows higher bandwidth between switches
- Provides load-balancing
- Creates redundant links

Review of EtherChannel Operation



- PAgP: Port Aggregation Protocol
- LACP: Link Aggregation Control Protocol

EtherChannel Load-Balancing



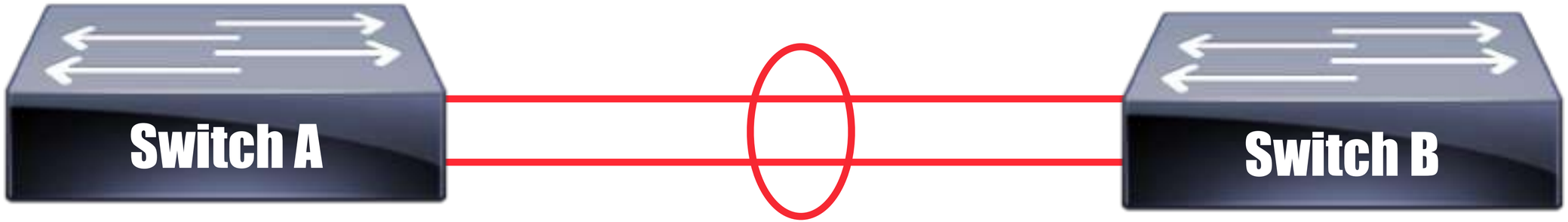
Load-Balancing Algorithms

- dst-ip
- dst-mac
- src-dst-ip
- src-dst-mac
- src-ip
- src-mac

Last Hex Digit in MAC Address: 1 5 D

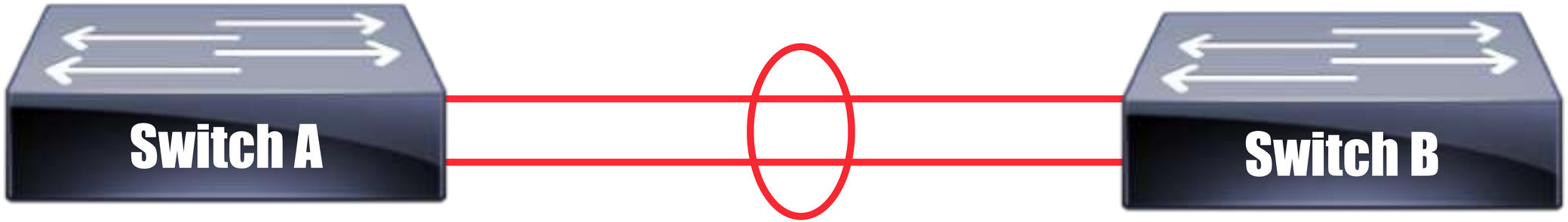
Hex	Binary
1	0001
5	0101
D	1101

PAgP Port Negotiation



PAgP Channel Mode	On	Auto	Desirable
On	✓	✗	✗
Auto	✗	✗	✓
Desirable	✗	✓	✓

LACP Port Negotiation



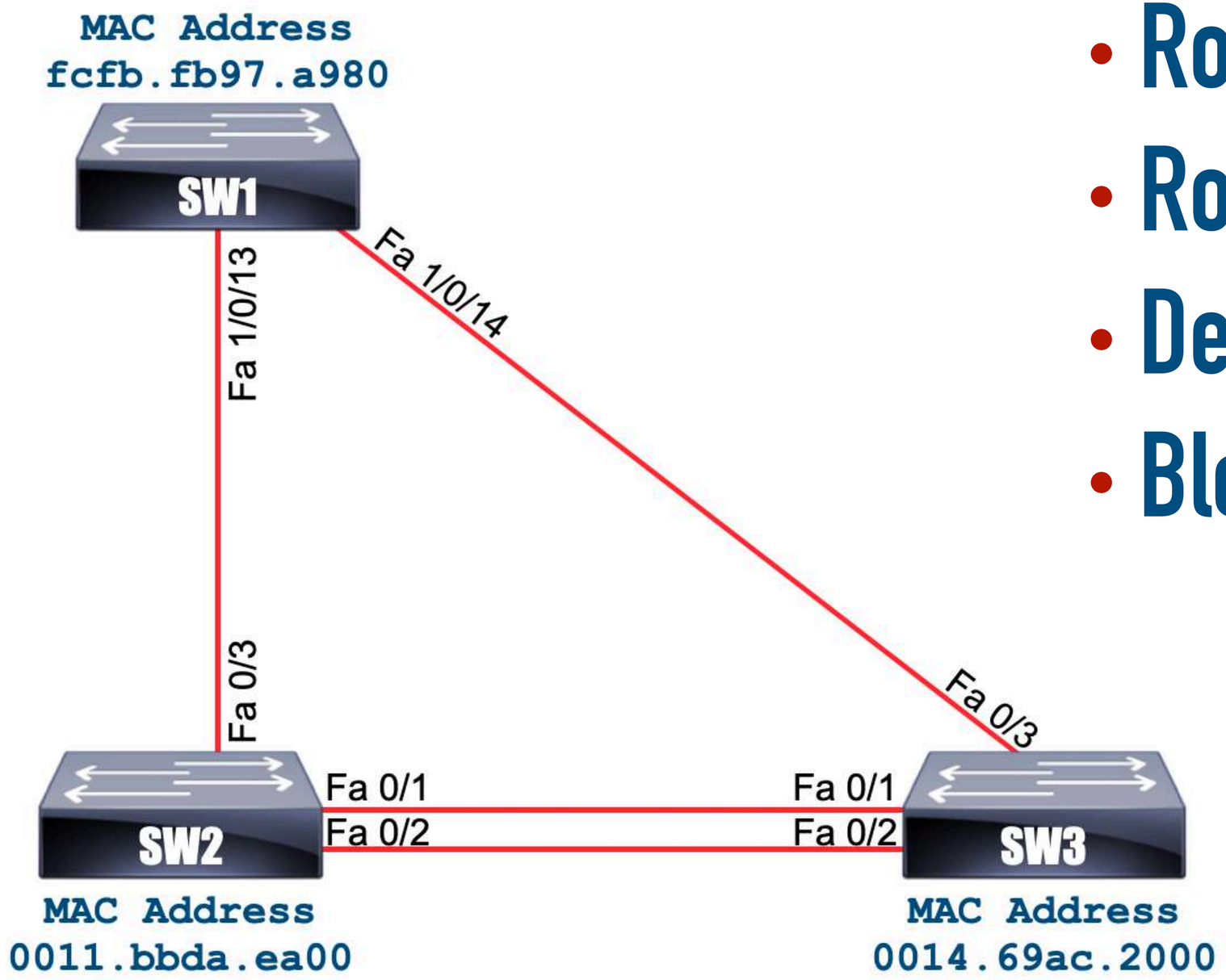
LACP Channel Mode	On	Passive	Active
On	✓	✗	✗
Passive	✗	✗	✓
Active	✗	✓	✓

Troubleshooting EtherChannels

Common Issues

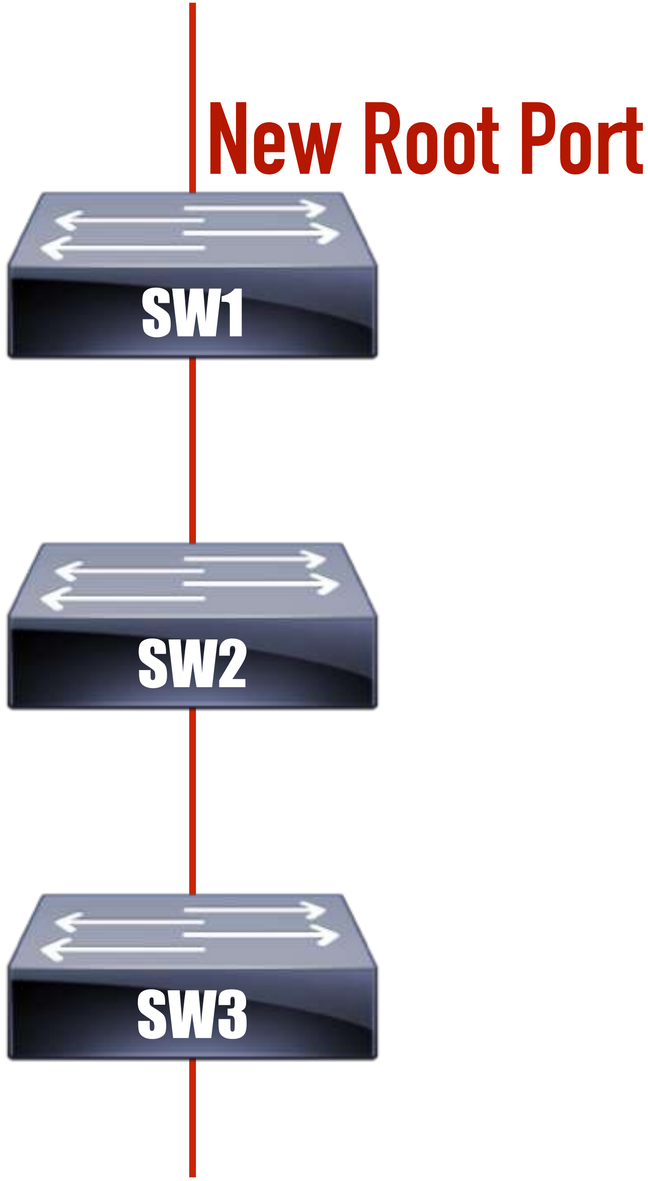
- Port Configuration Mismatch

- Speed
- Duplex
- Trunk Mode
- Native VLAN
- Allowed VLANs

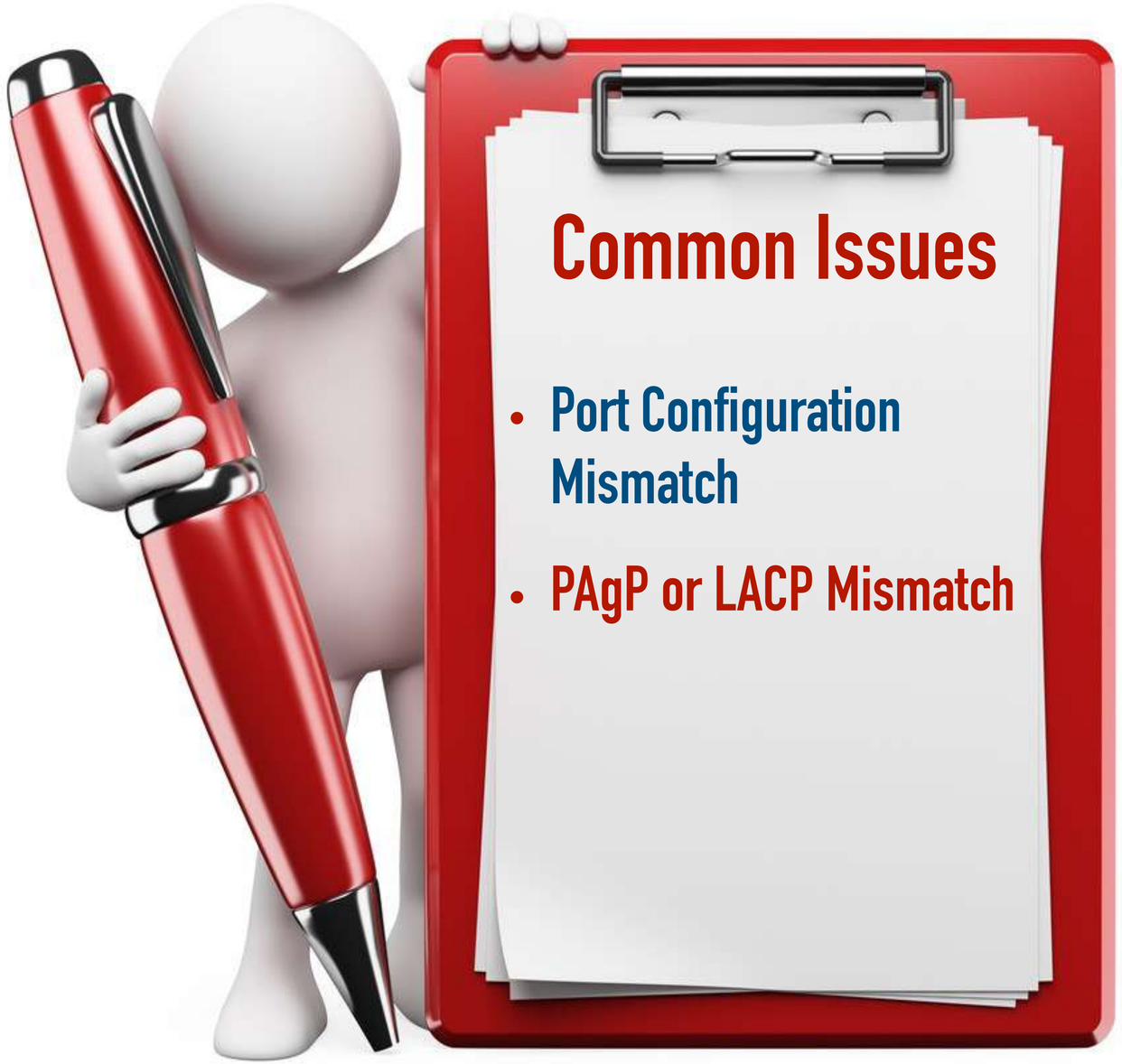


- Root Bridge?
- Root Ports?
- Designated Ports?
- Blocking Ports?

Rapid STP Synchronization



Troubleshooting EtherChannels



Common Issues

- Port Configuration Mismatch
- PAgP or LACP Mismatch

PAgP Channel Mode	On	Auto	Desirable
On	✓	✗	✗
Auto	✗	✗	✓
Desirable	✗	✓	✓

LACP Channel Mode	On	Passive	Active
On	✓	✗	✗
Passive	✗	✗	✓
Active	✗	✓	✓

Troubleshooting EtherChannels

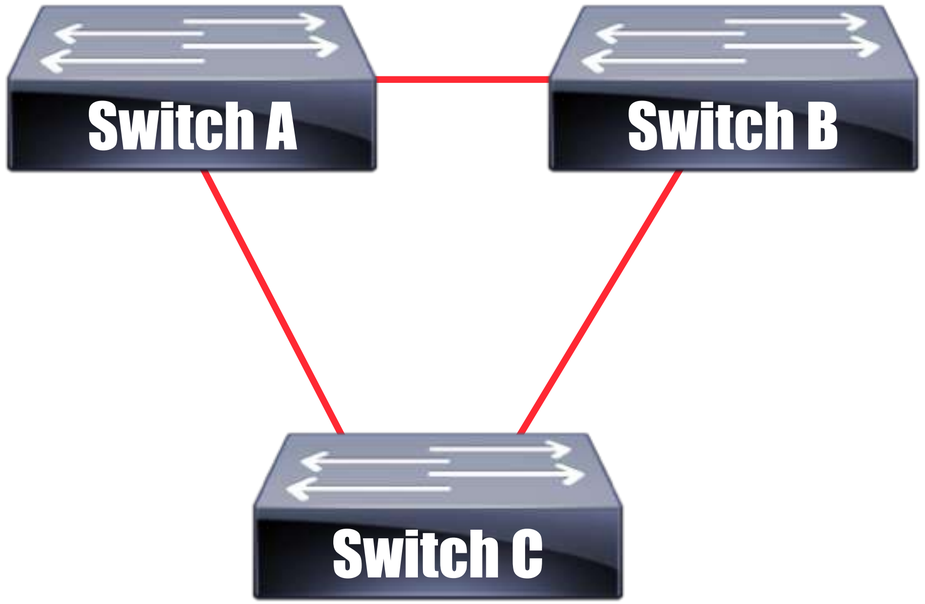
Common Issues

- Port Configuration Mismatch
- PAgP or LACP Mismatch
- Suboptimal Load-Balancing Algorithm

Load-Balancing Algorithms

- dst-ip
- dst-mac
- src-dst-ip
- src-dst-mac
- src-ip
- src-mac

MSTP

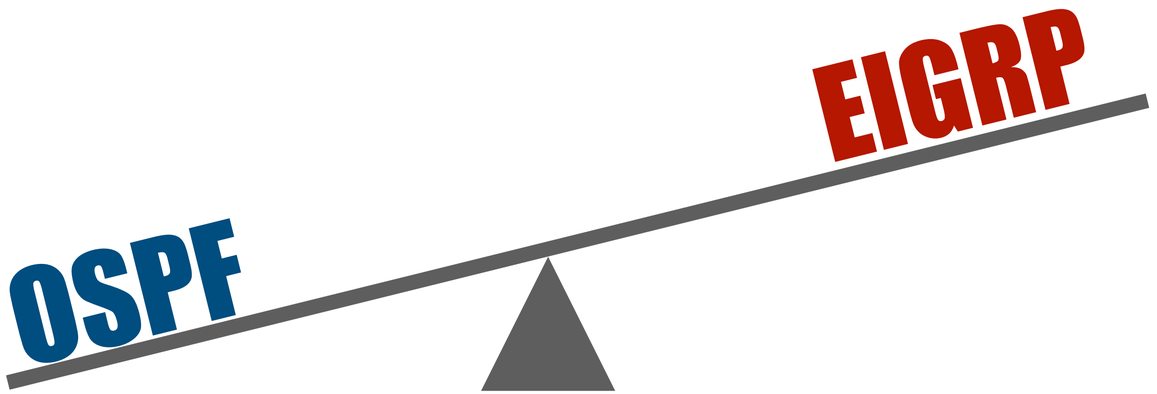


Instance	VLANs	Root
1	1, 2, 3, 4	Switch A
2	5, 6, 7, 8	Switch B

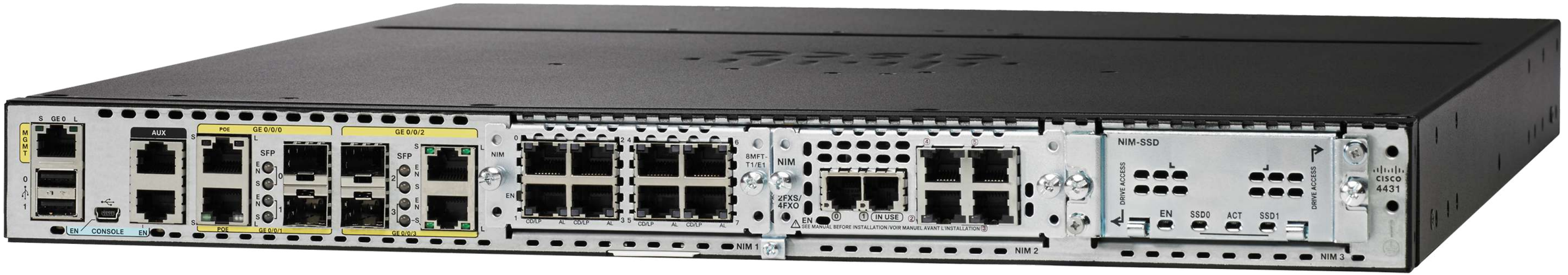
DEMO: STP

Comparing EIGRP with OSPF

Comparing OSPF and EIGRP



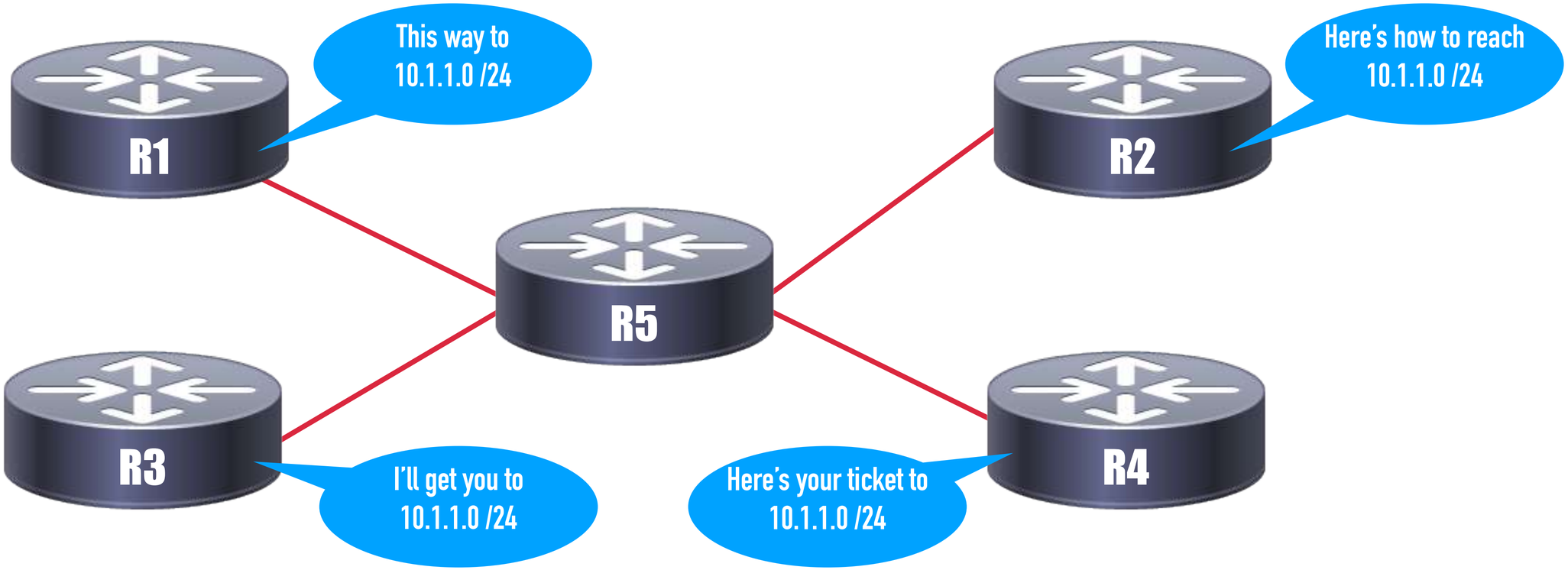
Routing Protocol Comparison



Routing Protocol	Distance-Vector	Link-State	Path-Vector
RIP	✓		
OSPF		✓	
IS-IS		✓	
EIGRP	✓		
BGP			✓

OSPF's Link State Database Compared to a Puzzle

Administrative Distance

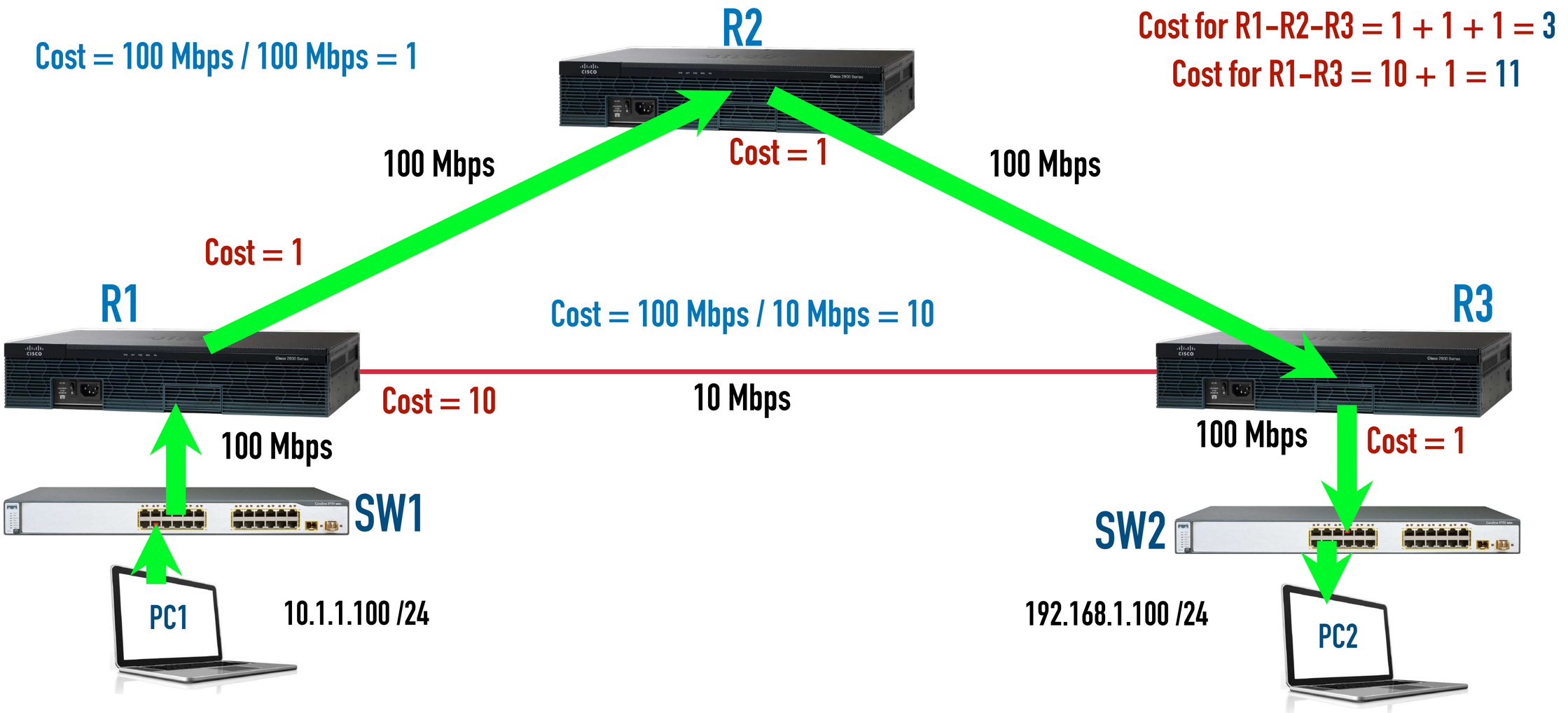


Routing Source	Administrative Distance
Connected	0
Static	1 (by default)
EIGRP	90
OSPF	110
RIP	120

OSPF Cost

Cost = Reference BW / Interface BW

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



EIGRP Metric Calculation

Bandwidth

Delay

Reliability

Load

MTU

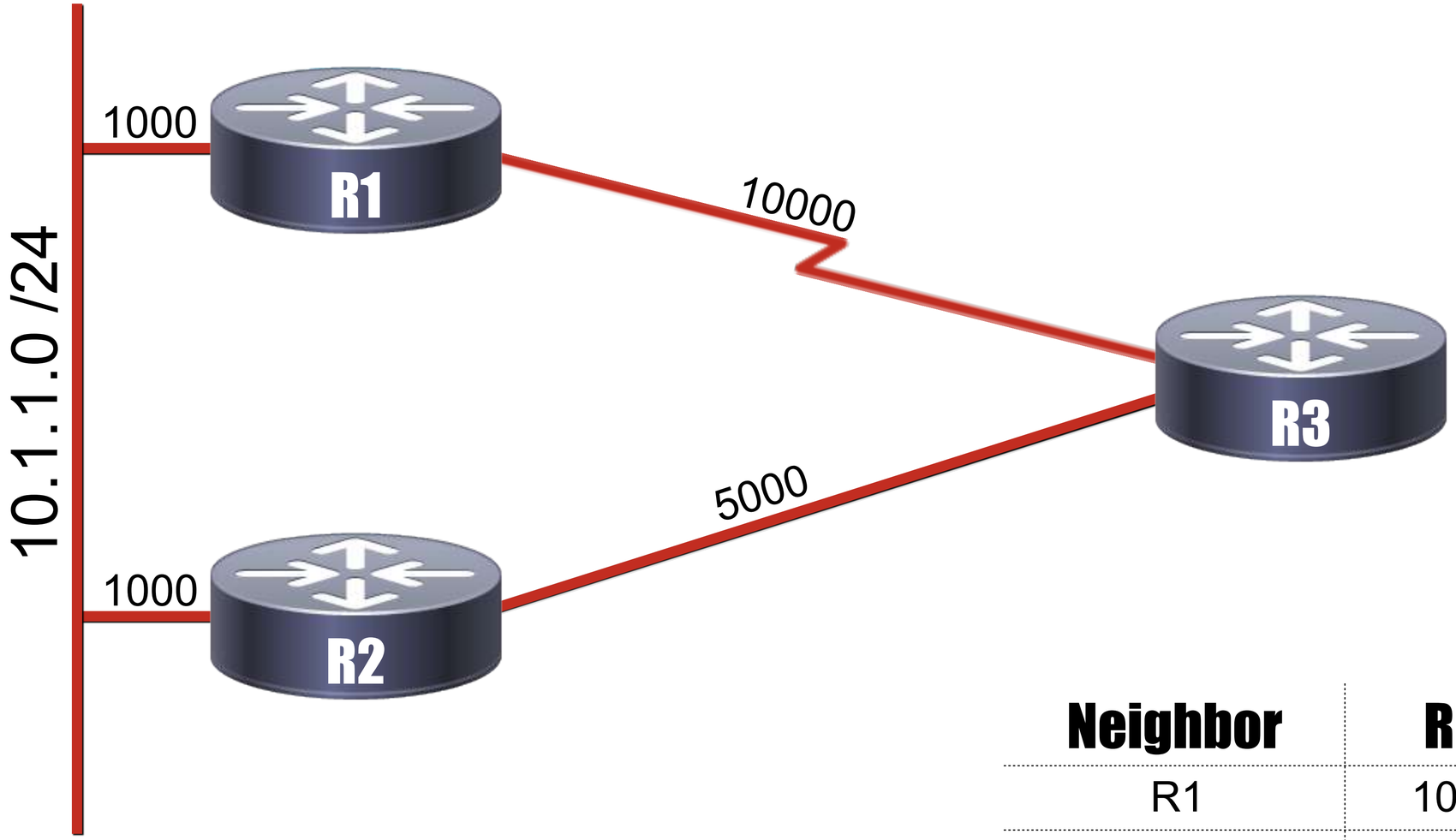
Default K Values:

K1 = 1
K2 = 0
K3 = 1
K4 = 0
K5 = 0

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

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

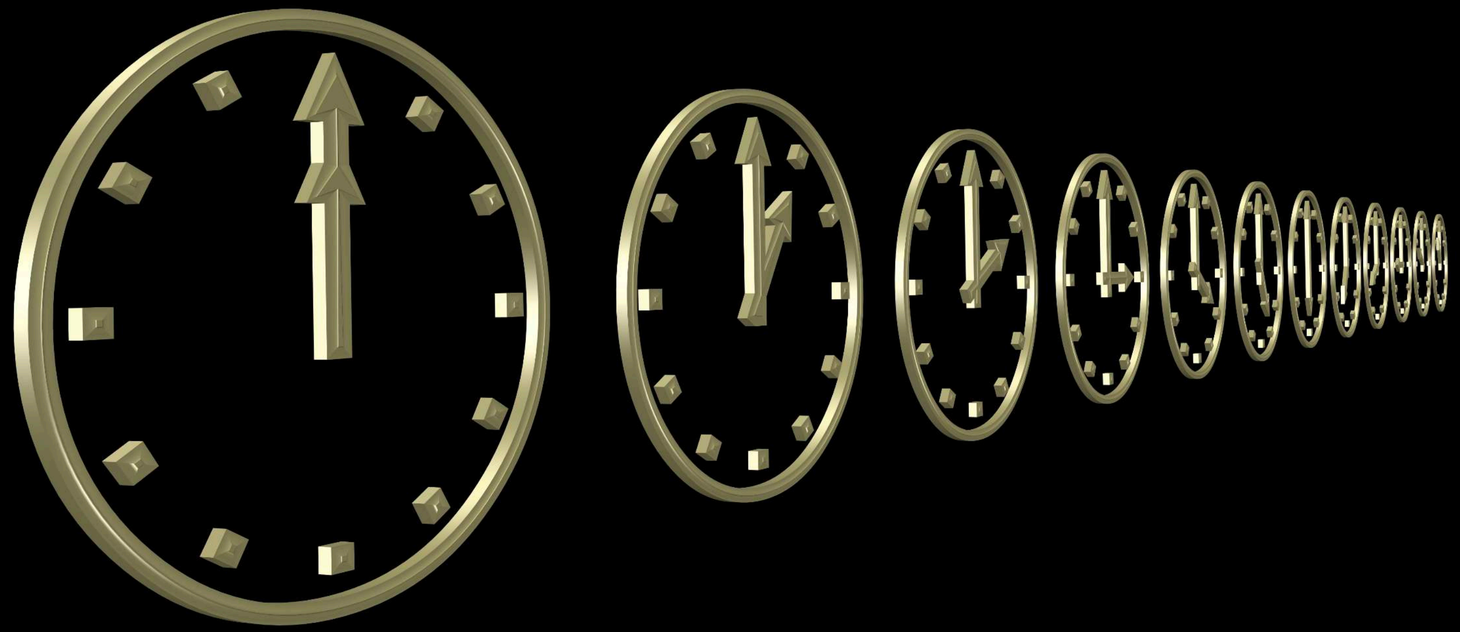
EIGRP Path Selection



Neighbor	RD	FD
R1	1000	11000
R2	1000	6000

Timer Comparison

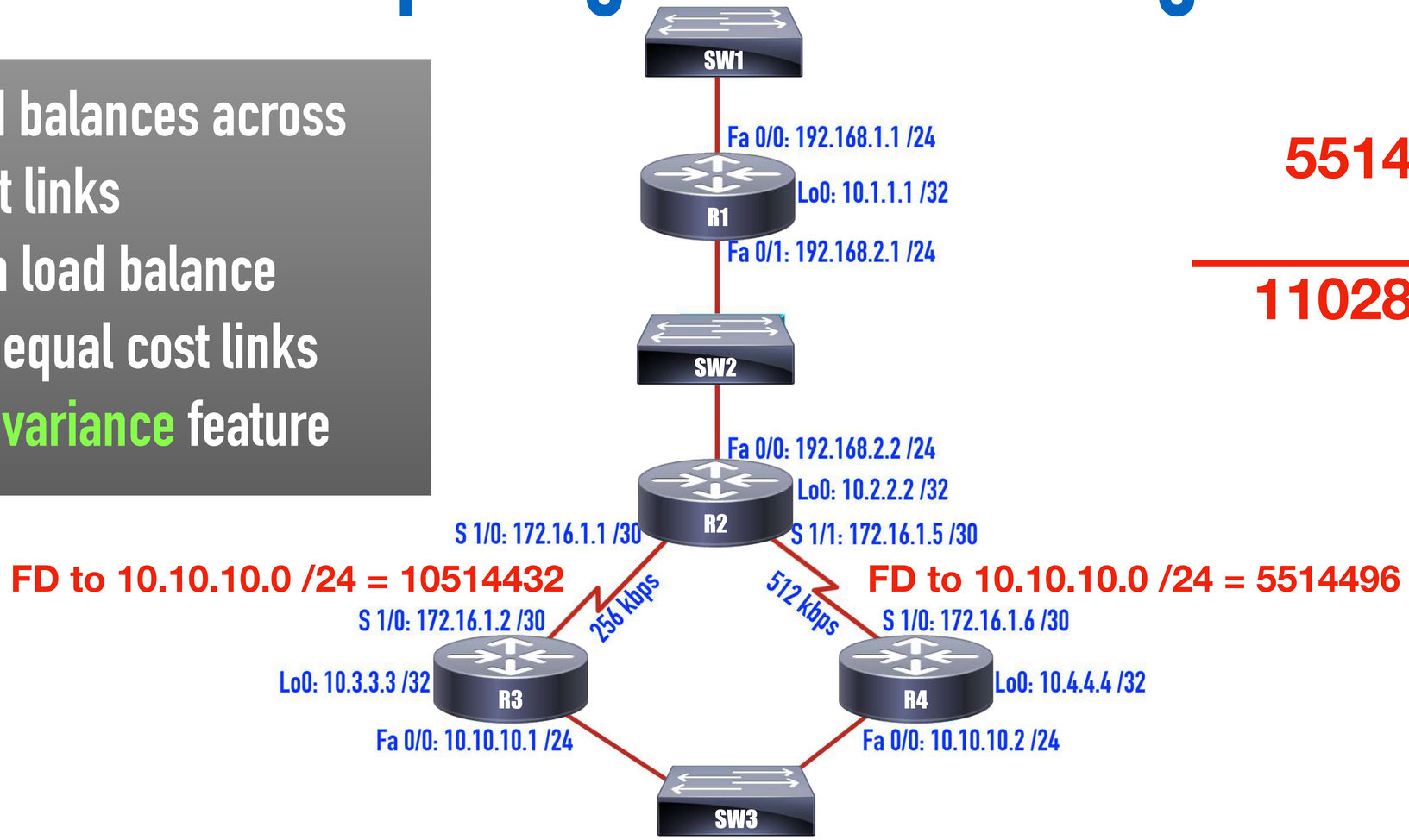
- **OSPF Hello Interval:** Specifies how long the local router waits between sending Hello messages
- **OSPF Dead Interval:** Specifies how long the local router waits for a Hello message from an OSPF neighbor before considering that neighbor to be unavailable



- **EIGRP Hello Interval:** Specifies how long the local router waits between sending Hello messages
- **EIGRP Hold Time:** Tells an EIGRP neighbor how long to wait before considering the local router unavailable

Comparing Load Balancing

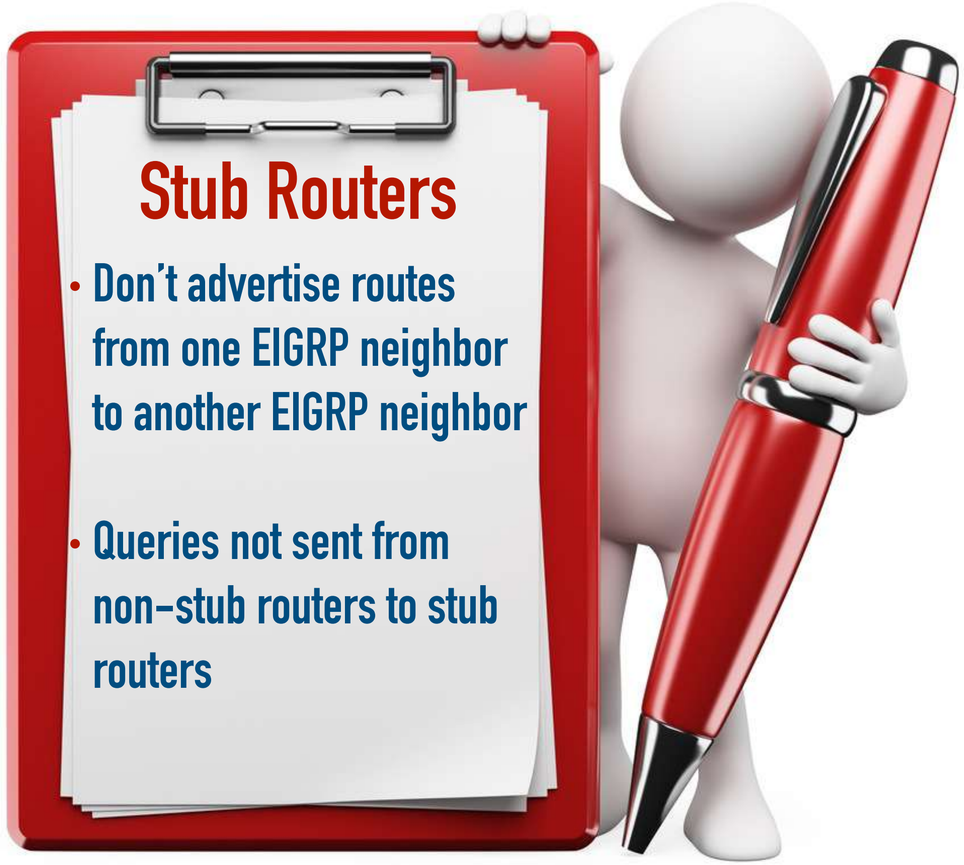
- OSPF load balances across equal cost links
- EIGRP can load balance across unequal cost links using the variance feature

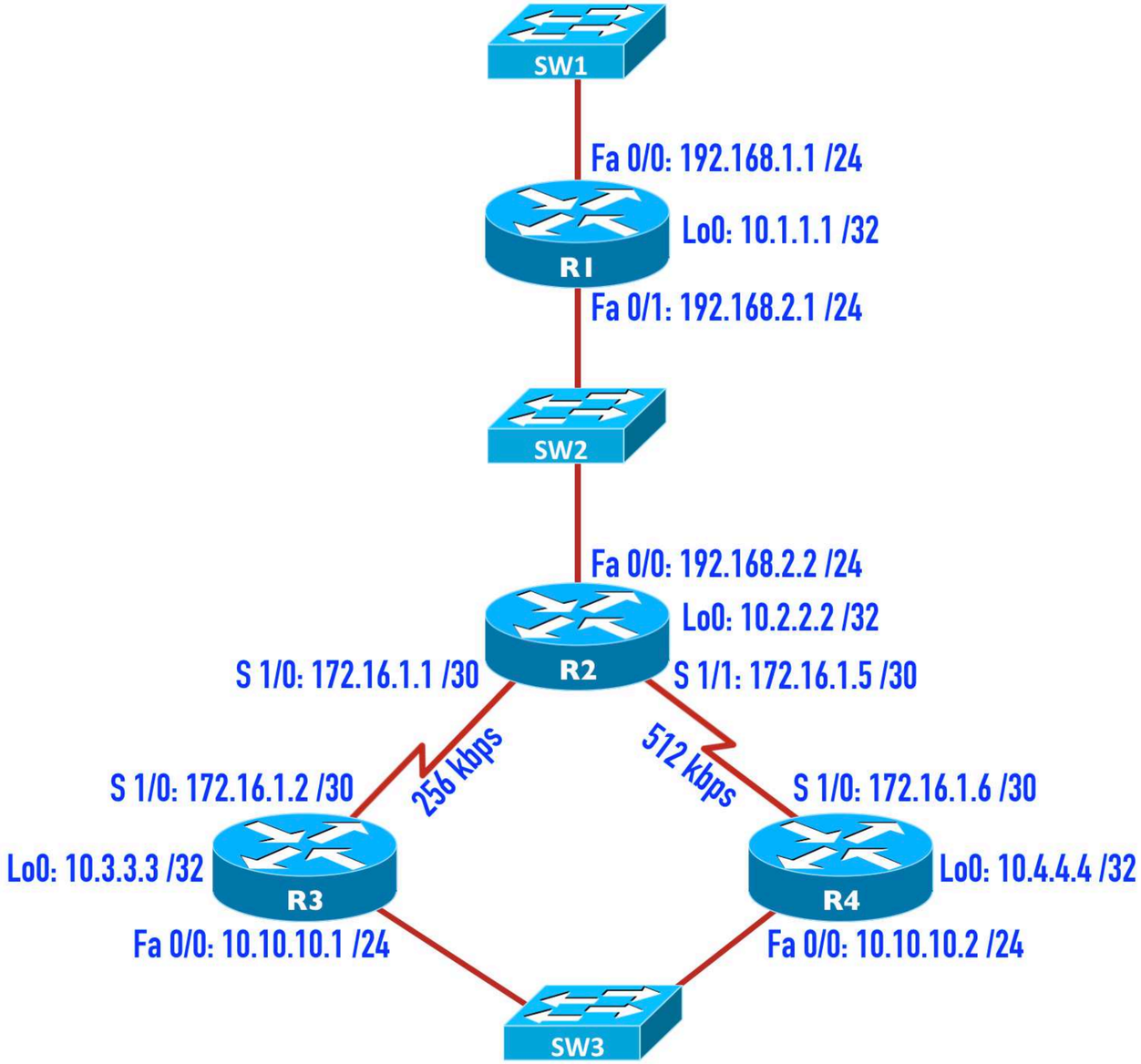


5514496
x2
11028992

R5(config-router)#**variance 2**

EIGRP Stub Routing





EIGRP Stub Routing


```
R1(config-router)#eigrp stub [option]
```

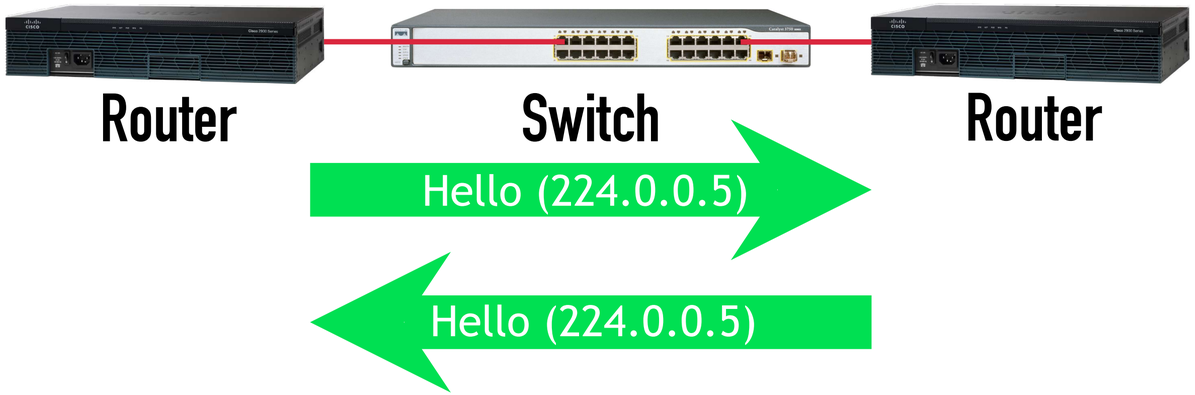
Stub Option	Description
connected	The stub router advertises connected routes matched with a **network** command.
summary	The stub router advertises summarized routes (either automatically or statically summarized).
static	The stub router advertises statically configured routes, if the **redistribute static** command has been configured.
leak-map *name*	The stub router's dynamic prefixes are based on a leak-map.
redistributed	The stub router advertises any redistributed routes.
receive-only	The stub router does not advertise any routes.

OSPF

Neighborship vs. Adjacencies

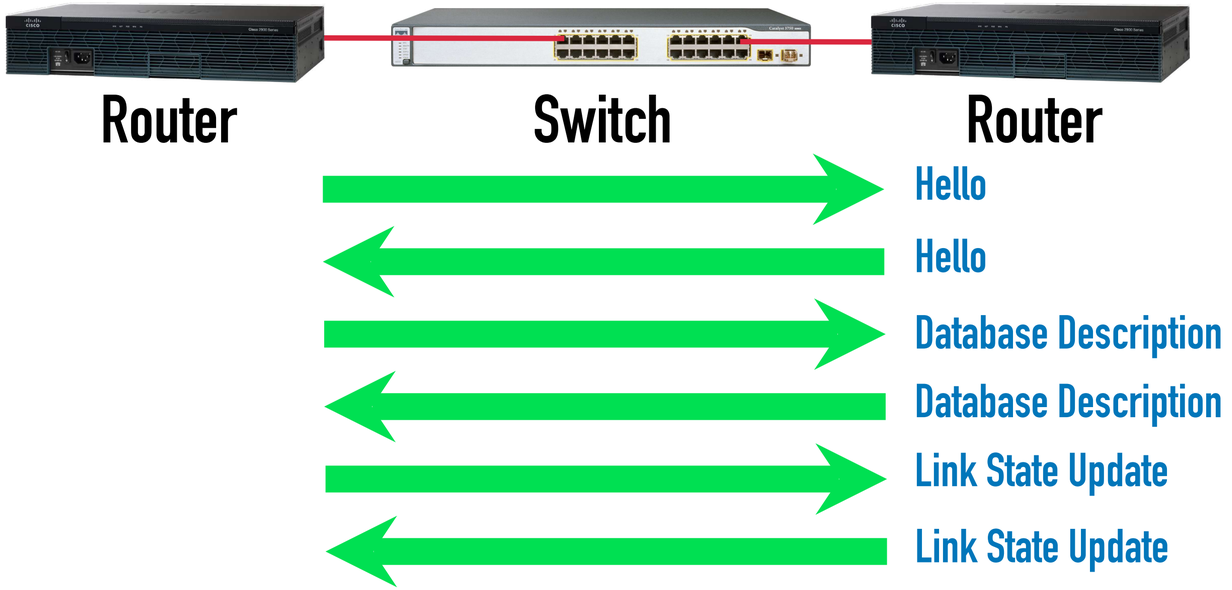
Neighbors are routers that:

- Reside on the same network link
- Exchange Hello messages



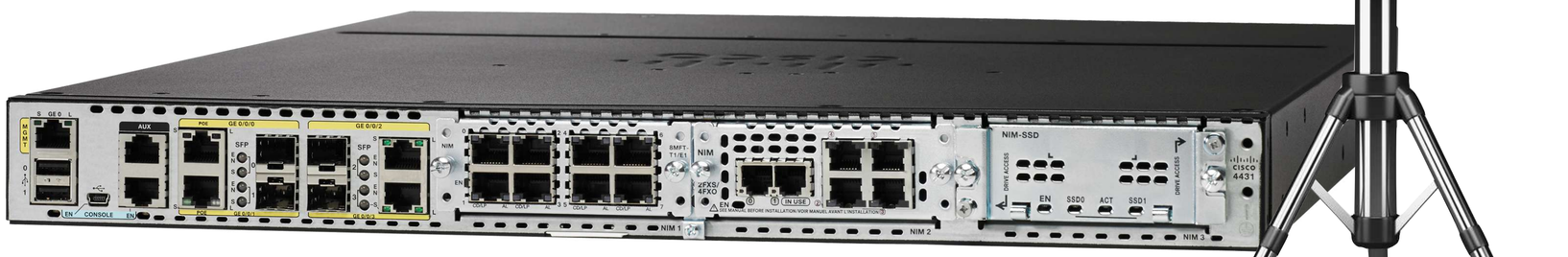
Adjacencies are routers that:

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

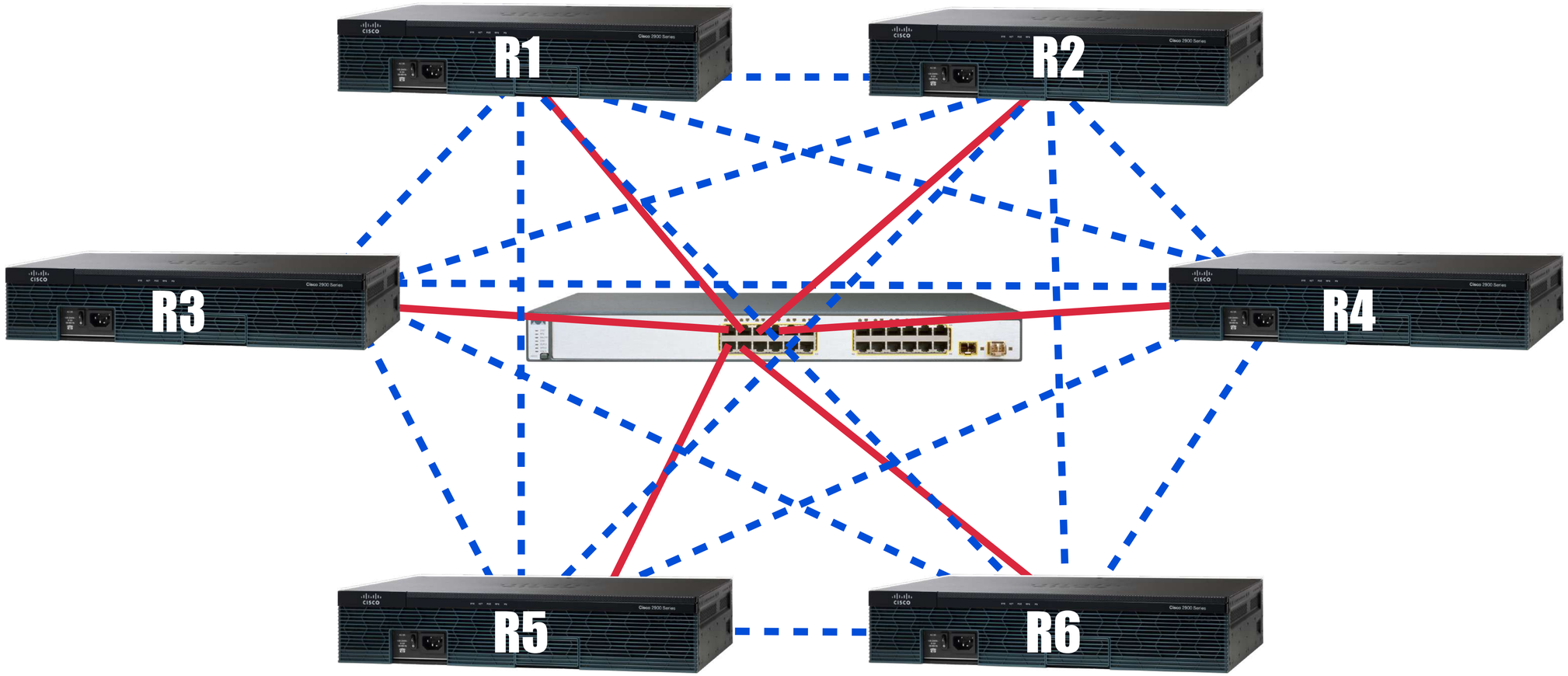


Neighborship Requirements

- Matching Area
- Matching Authentication
- Matching Subnet
- Matching Timers
- Matching Stub Flags
- Matching MTU (EXSTART/EXCHANGE State)



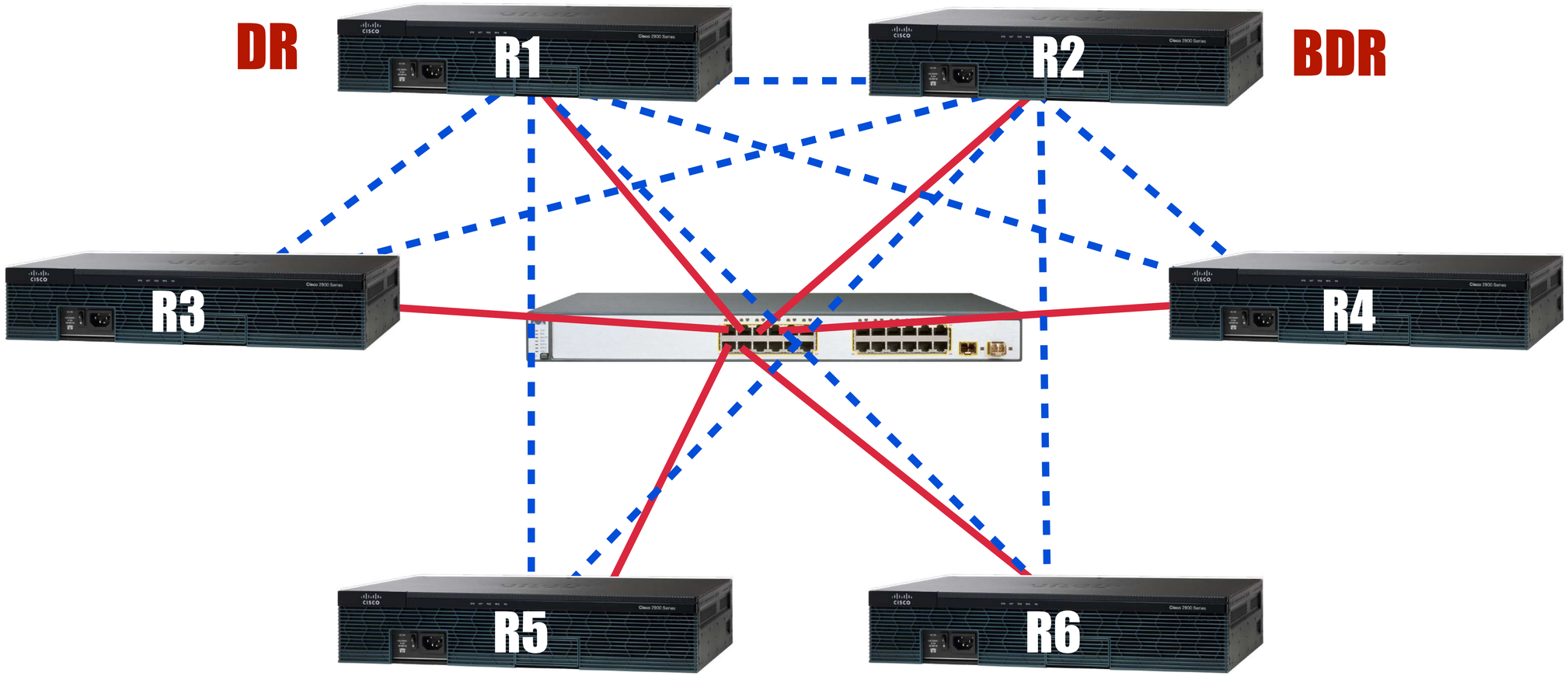
The Need for Designated Routers



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

The Need for Designated Routers

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



- 224.0.0.5 or FF02::5 – All OSPF routers
- 224.0.0.6 or FF02::6 – All designated routers

DR and BDR Election

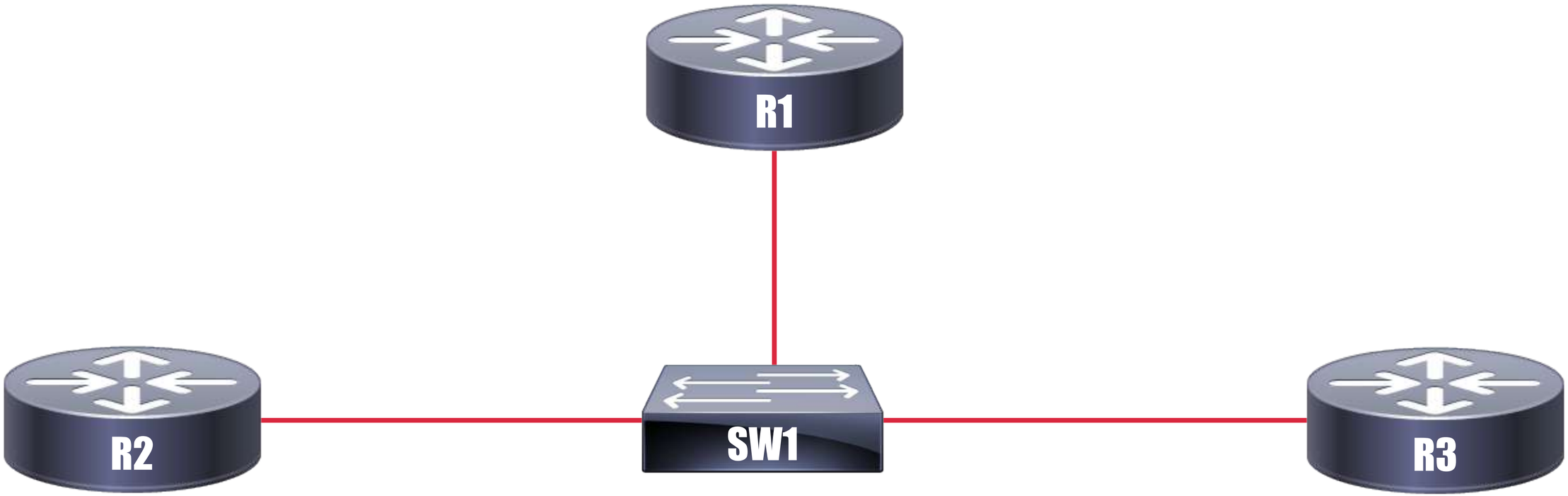
Highest Router Priority Wins

- Carried in Hello packet
- Configured in interface configuration mode:
  - `Router(config-if)# ip ospf priority number`
  - A priority of 0 prevents a router from participating in the election.

TIE BREAKER: Highest Router ID Wins

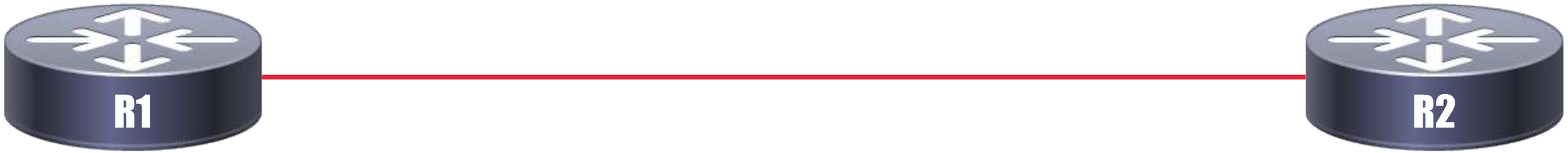
- Configured in router configuration mode:
  - `Router(config-router)# router-id id`
- If there's no configured Router ID, the highest IP address on a Loopback interface wins.
- If there's no Loopback interface, the highest IP address on an interface that's up wins.

Broadcast Network Type



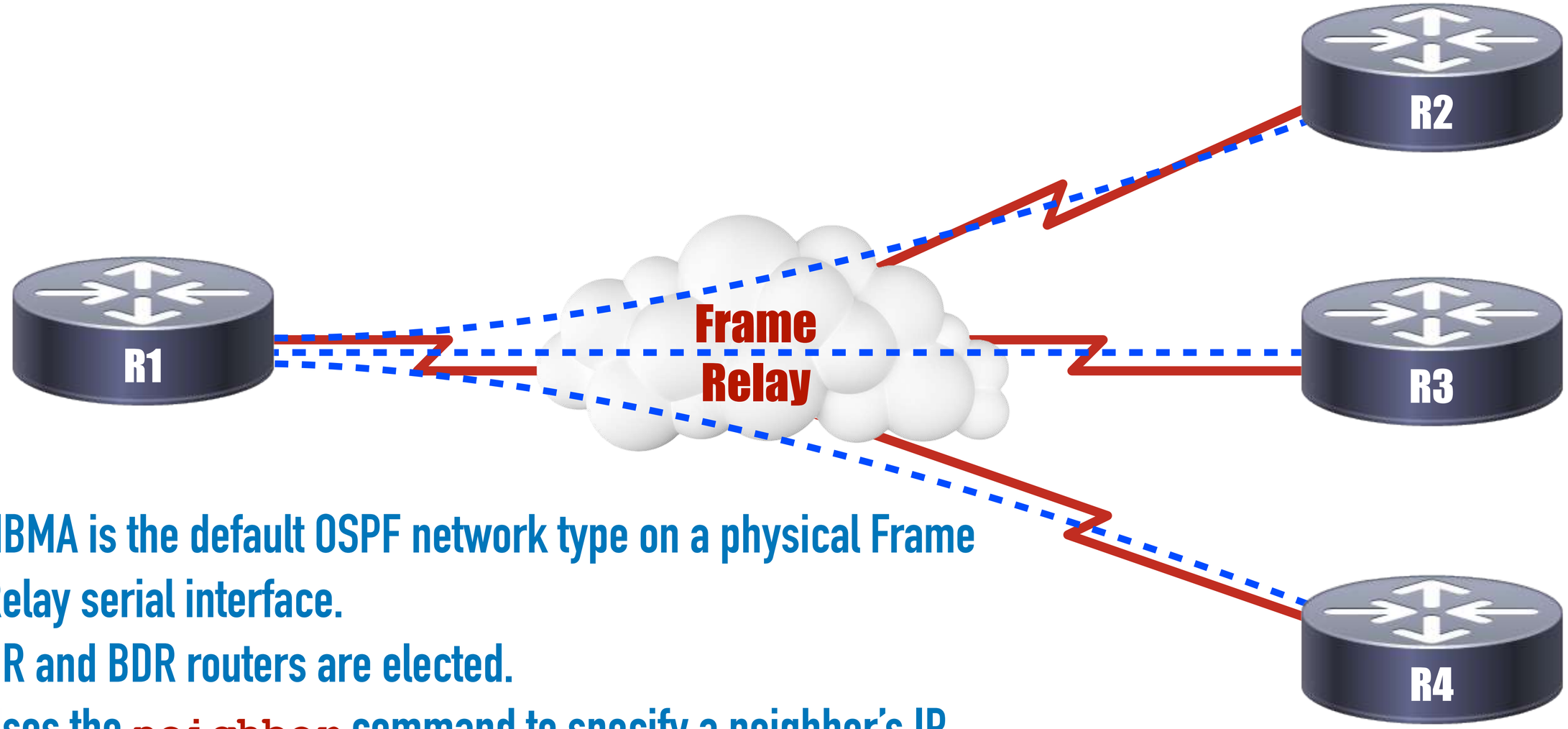
- Broadcast is the default OSPF network type for any Ethernet interface.
- DR and BDR routers are elected.
- Default HELLO interval: 10 seconds.

Point-to-Point Network Type



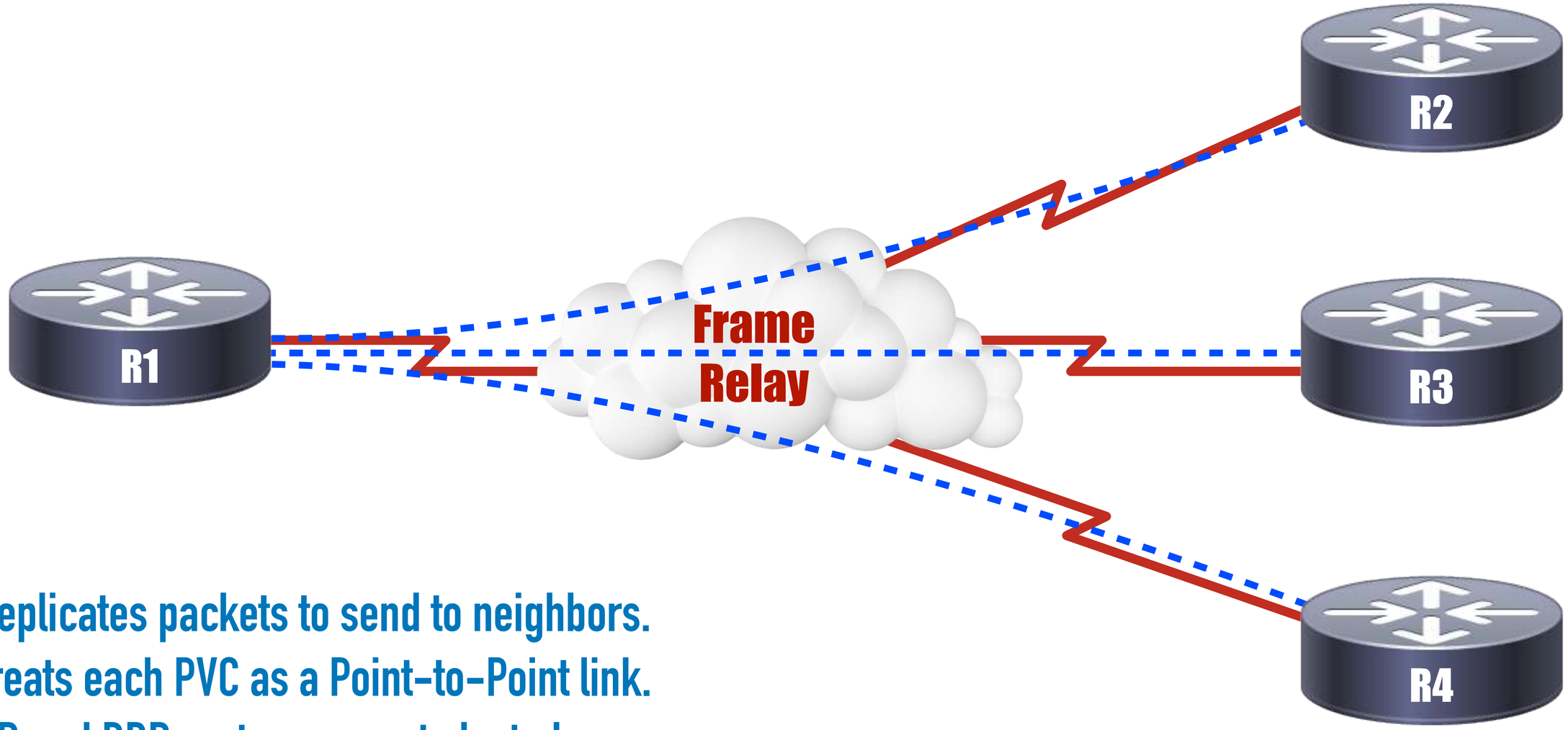
- Point-to-Point is the default OSPF network type on a non-Frame Relay serial interface.
- DR and BDR routers are not elected.
- Default HELLO interval: 10 seconds.

Non-Broadcast (NBMA) Network Type



- NBMA is the default OSPF network type on a physical Frame Relay serial interface.
- DR and BDR routers are elected.
- Uses the `neighbor` command to specify a neighbor's IP address.
- Default HELLO interval: 30 seconds.

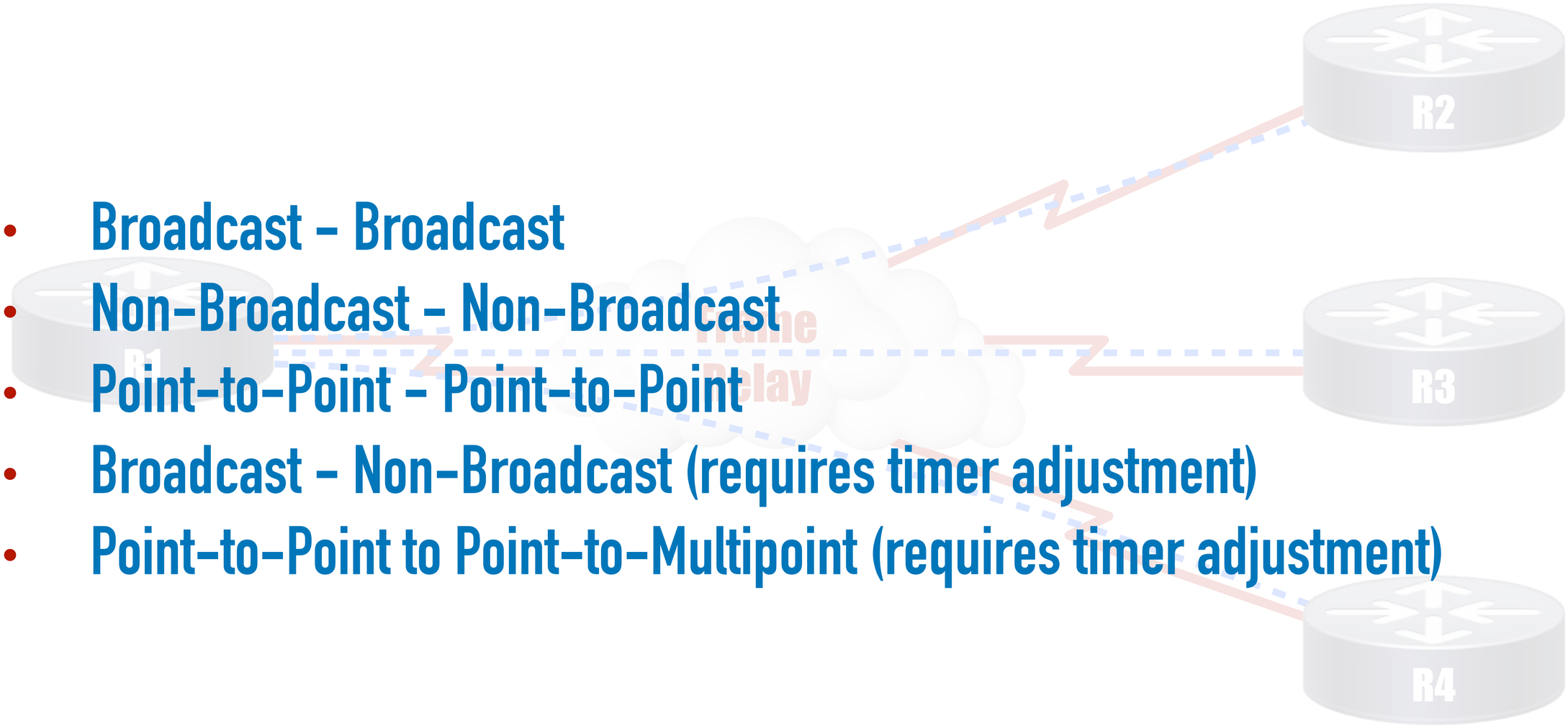
Point-to-Multipoint Network Type



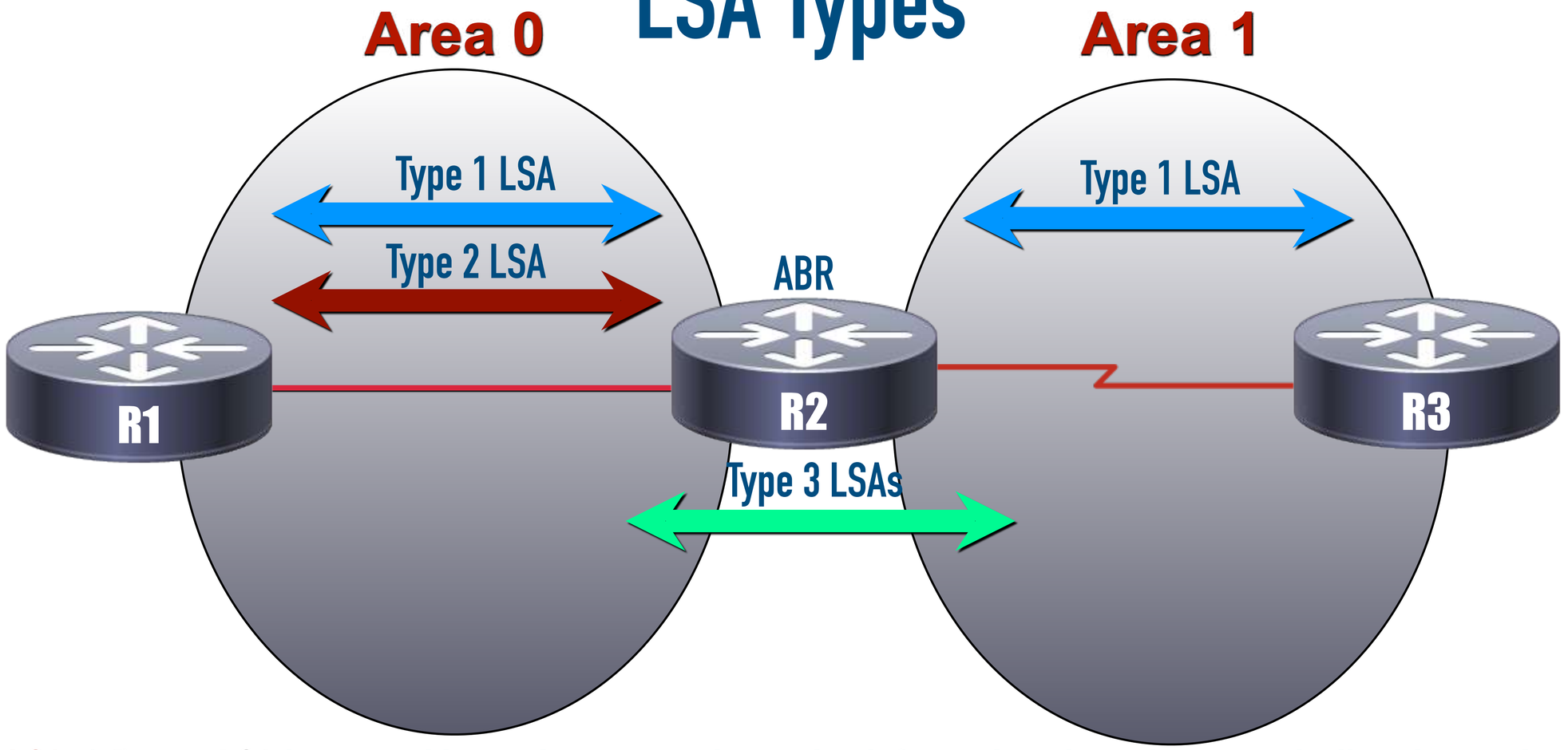
- Replicates packets to send to neighbors.
- Treats each PVC as a Point-to-Point link.
- DR and BDR routers are not elected.
- Default HELLO interval: 30 seconds.

Valid OSPF Network Types for Peers

- Broadcast – Broadcast
- Non-Broadcast – Non-Broadcast
- Point-to-Point – Point-to-Point
- Broadcast – Non-Broadcast (requires timer adjustment)
- Point-to-Point to Point-to-Multipoint (requires timer adjustment)

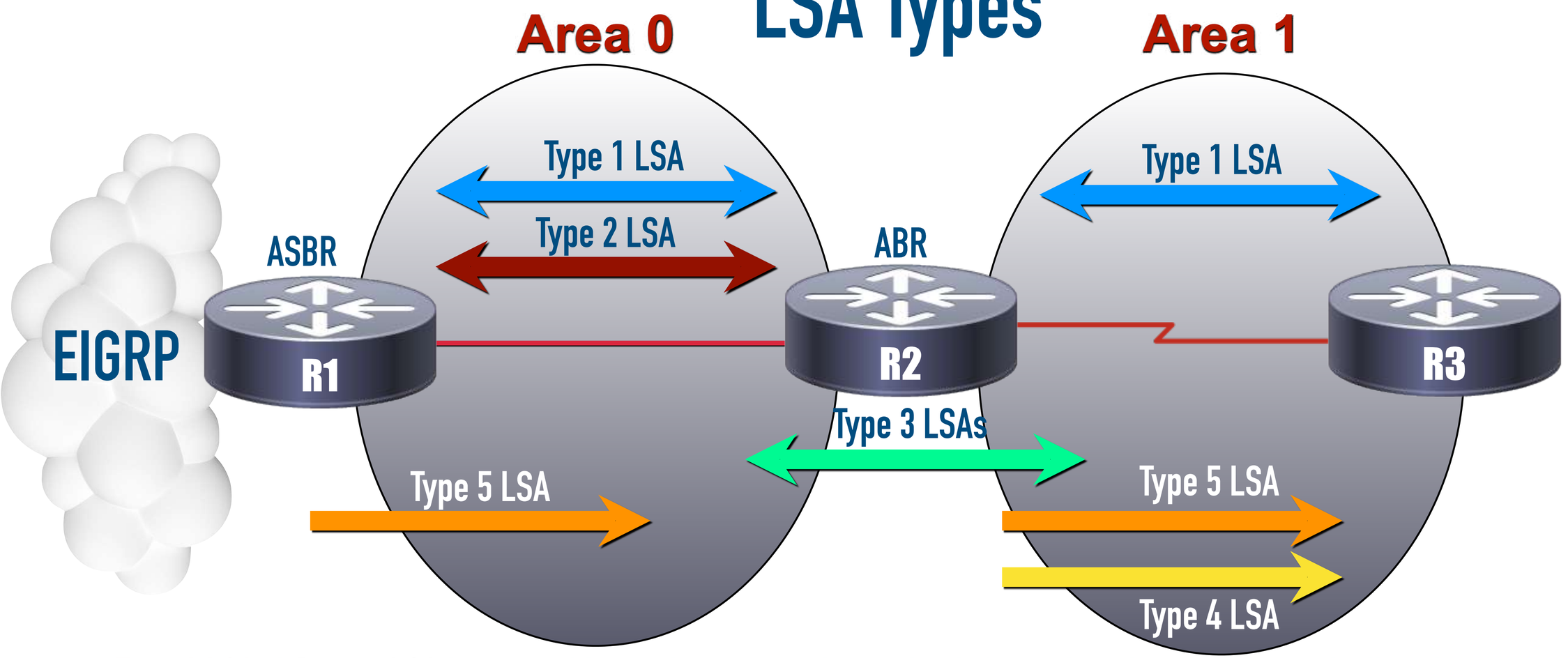


LSA Types



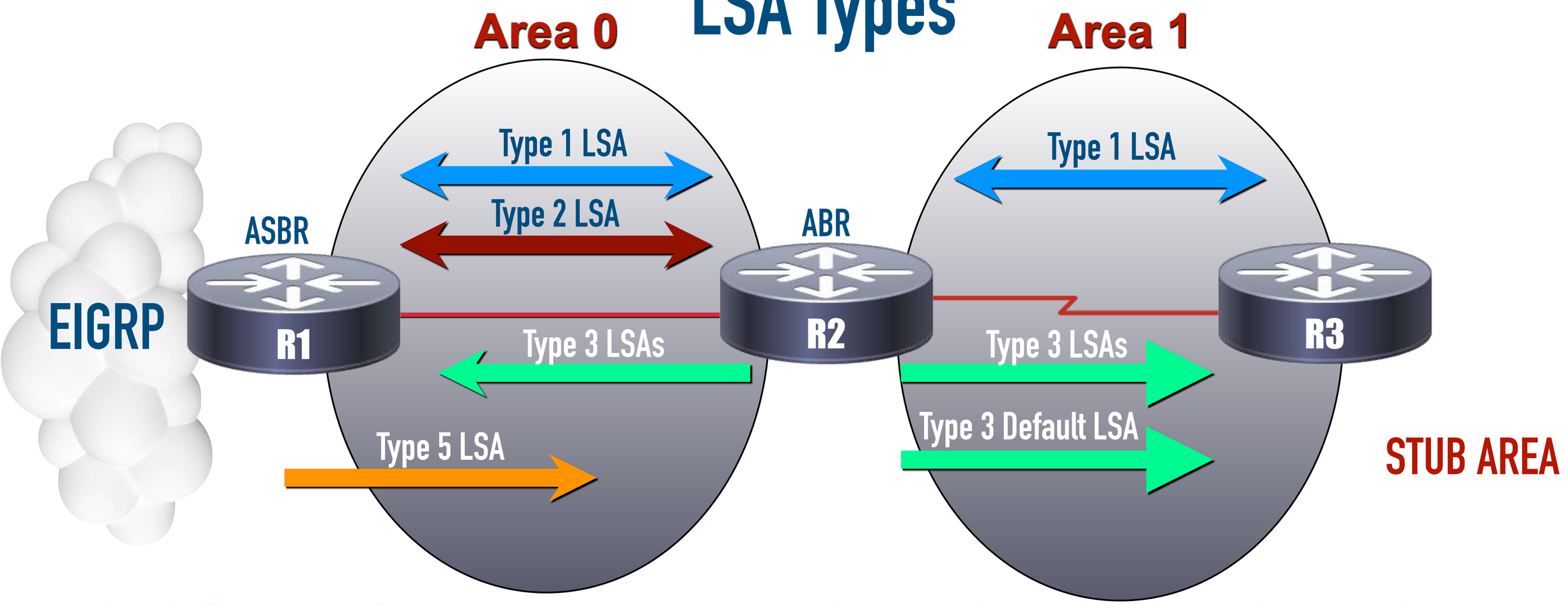
- **Type 1 LSA**: A Router LSA is created by each router and contains information about that router's directly attached networks.
- **Type 2 LSA**: A Network LSA is created for each transit network within an area on which a DR is elected.
- **Type 3 LSA**: A Summary LSA is sent from one area to another and is used to advertise a network in the source area.

LSA Types



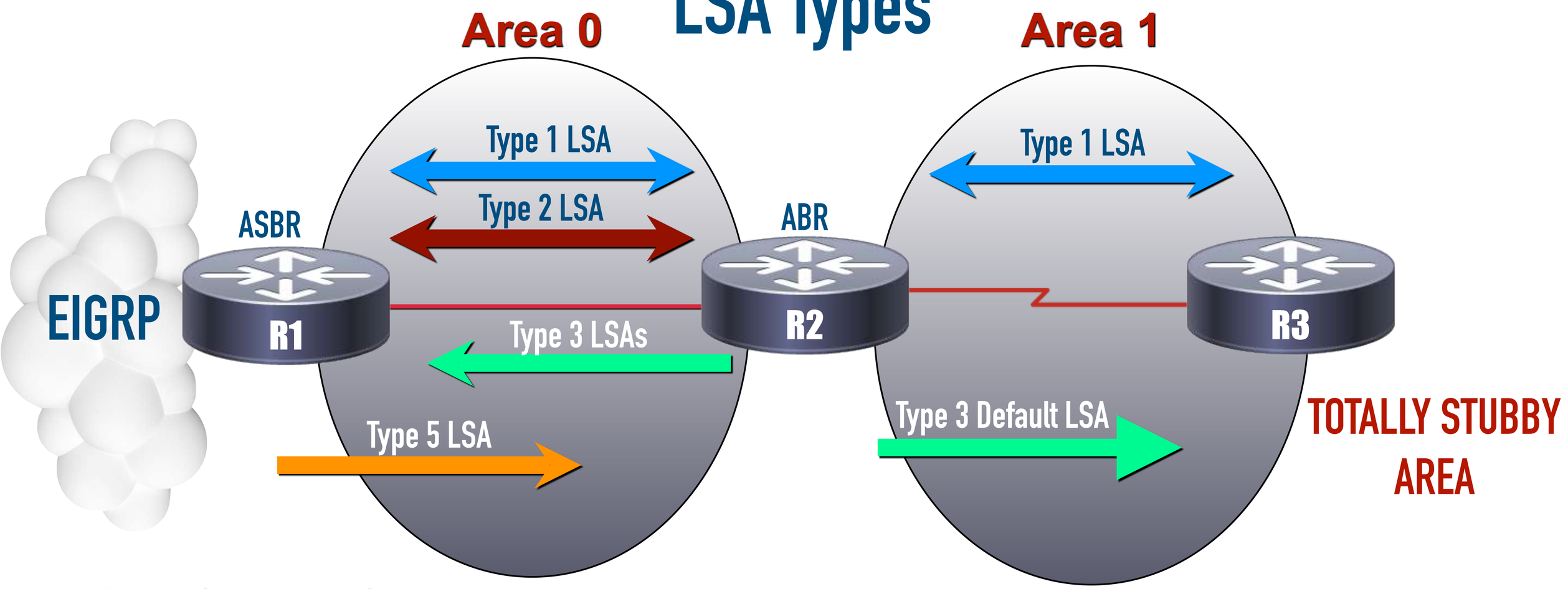
- **Type 1 LSA**: A Router LSA is created by each router and contains information about that router's directly attached networks.
- **Type 2 LSA**: A Network LSA is created for each transit network within an area on which a DR is elected.
- **Type 3 LSA**: A Summary LSA is sent from one area to another and is used to advertise a network in the source area.
- **Type 4 LSA**: A Summary ASBR LSA is created by an ABR to tell members of an area how to reach an ASBR.
- **Type 5 LSA**: An AS External LSA is created by and ASBR to advertise networks in a different AS.

LSA Types



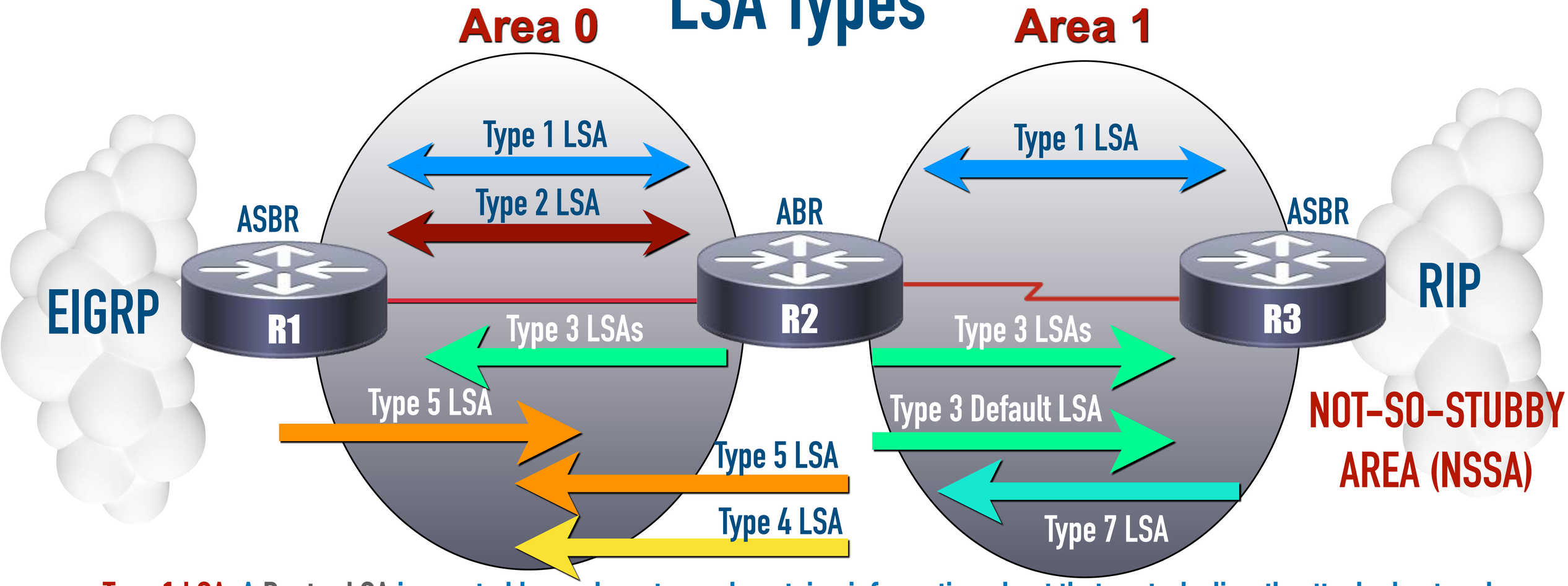
- **Type 1 LSA**: A Router LSA is created by each router and contains information about that router's directly attached networks.
- **Type 2 LSA**: A Network LSA is created for each transit network within an area on which a DR is elected.
- **Type 3 LSA**: A Summary LSA is sent from one area to another and is used to advertise a network in the source area.
- **Type 4 LSA**: A Summary ASBR LSA is created by an ABR to tell members of an area how to reach an ASBR.
- **Type 5 LSA**: An AS External LSA is created by and ASBR to advertise networks in a different AS.

LSA Types



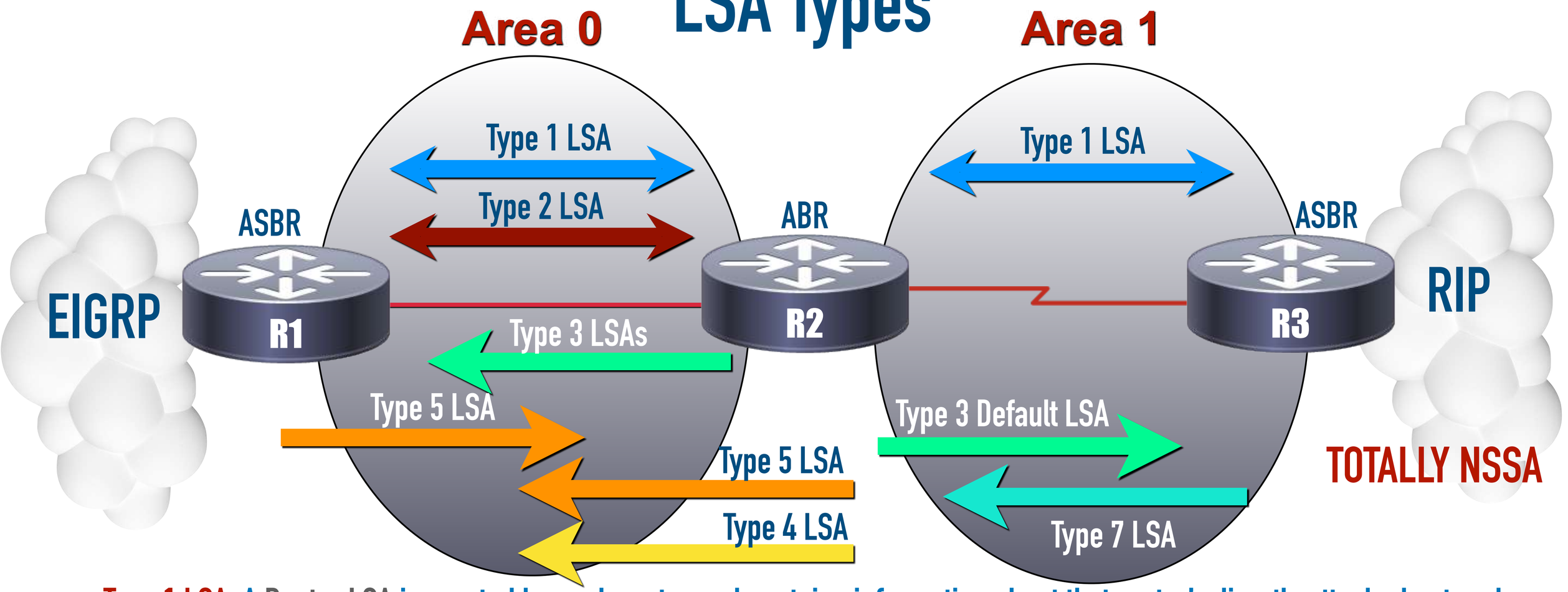
- **Type 1 LSA**: A Router LSA is created by each router and contains information about that router's directly attached networks.
- **Type 2 LSA**: A Network LSA is created for each transit network within an area on which a DR is elected.
- **Type 3 LSA**: A Summary LSA is sent from one area to another and is used to advertise a network in the source area.
- **Type 4 LSA**: A Summary ASBR LSA is created by an ABR to tell members of an area how to reach an ASBR.
- **Type 5 LSA**: An AS External LSA is created by and ASBR to advertise networks in a different AS.

LSA Types



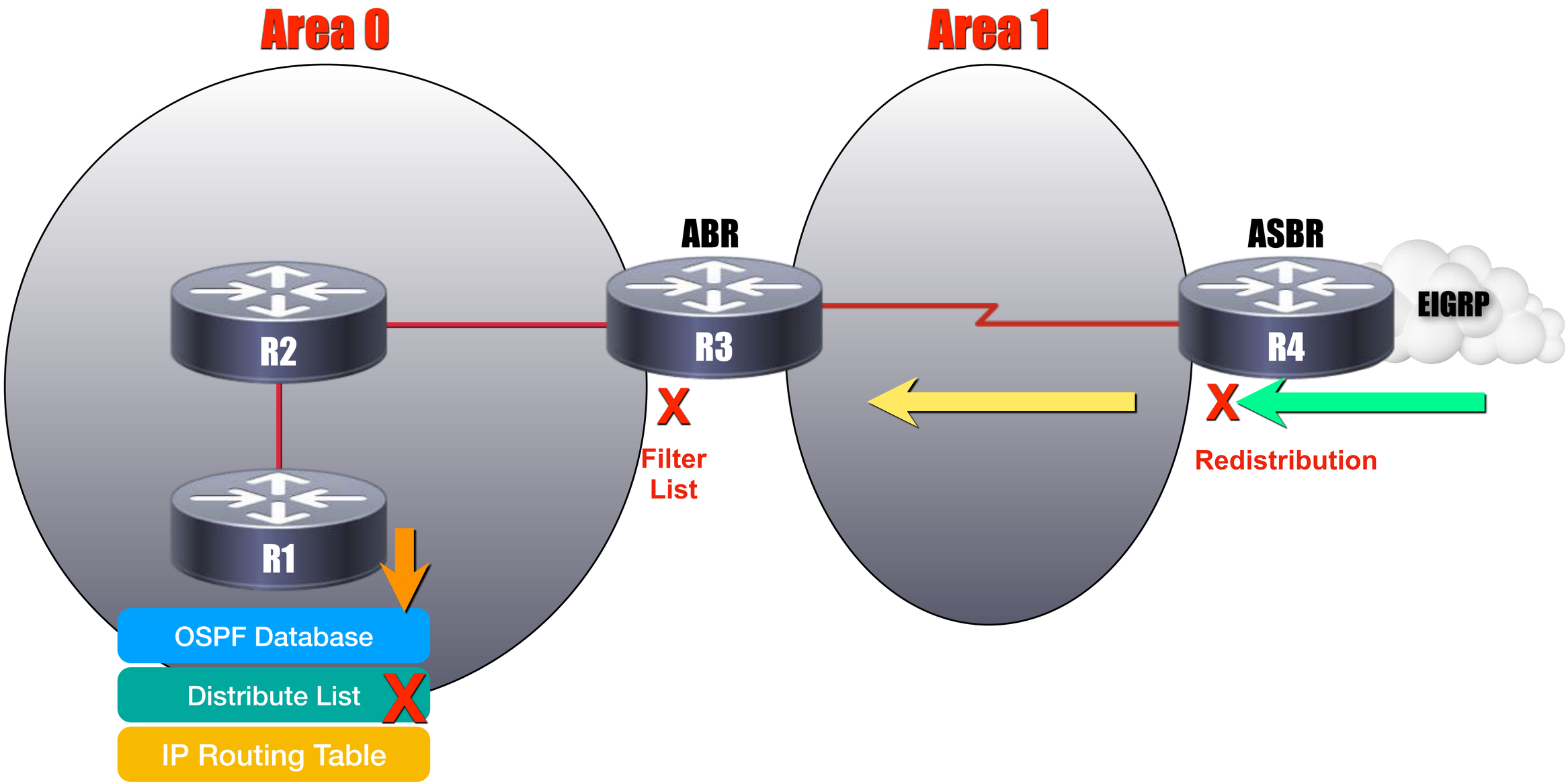
- **Type 1 LSA**: A Router LSA is created by each router and contains information about that router's directly attached networks.
- **Type 2 LSA**: A Network LSA is created for each transit network within an area on which a DR is elected.
- **Type 3 LSA**: A Summary LSA is sent from one area to another and is used to advertise a network in the source area.
- **Type 4 LSA**: A Summary ASBR LSA is created by an ABR to tell members of an area how to reach an ASBR.
- **Type 5 LSA**: An AS External LSA is created by and ASBR to advertise networks in a different AS.
- **Type 7 LSA**: An NSSA LSA is sent from an ASBR into an NSSA to advertise networks from a different AS.

LSA Types



- **Type 1 LSA**: A Router LSA is created by each router and contains information about that router's directly attached networks.
- **Type 2 LSA**: A Network LSA is created for each transit network within an area on which a DR is elected.
- **Type 3 LSA**: A Summary LSA is sent from one area to another and is used to advertise a network in the source area.
- **Type 4 LSA**: A Summary ASBR LSA is created by an ABR to tell members of an area how to reach an ABR.
- **Type 5 LSA**: An AS External LSA is created by and ASBR to advertise networks in a different AS.
- **Type 7 LSA**: An NSSA LSA is sent from an ASBR into an NSSA to advertise networks from a different AS.

Filtering OSPF Routes



Route Summarization

192.168.0.0 /24

192.168.1.0 /24

192.168.2.0 /24

192.168.3.0 /24

Route Summarization

Network Address	Octet 1	Octet 2	Octet 3	Octet 4
192.168.0.0 /24				
192.168.1.0 /24	11000000	10101000	00000001	00000000
192.168.2.0 /24	11000000	10101000	00000010	00000000
192.168.3.0 /24	11000000	10101000	0000	

192.168.0.0 /22

All Networks Have Their First 22 Bits In Common

Subnet Mask (Binary)	11111111	11111111	11111100	00000000
Subnet Mask (Decimal)	255	255	252	0
Network Address (Binary)	11000000	10101000	00000000	00000000
Network Address (Decimal)	192	168	0	0

Route Summarization

192.168.0.0 /24

192.168.1.0 /24

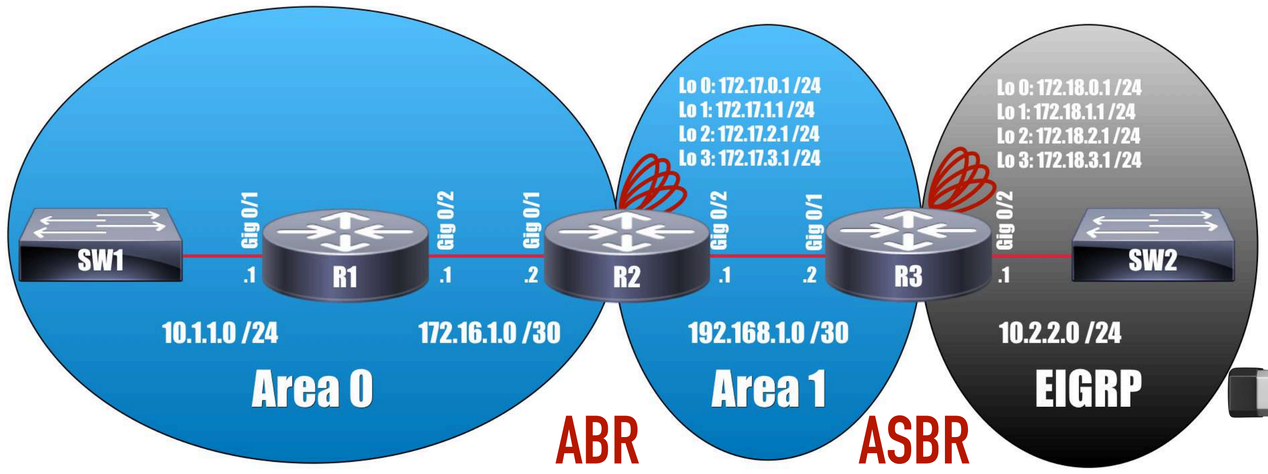
192.168.2.0 /24

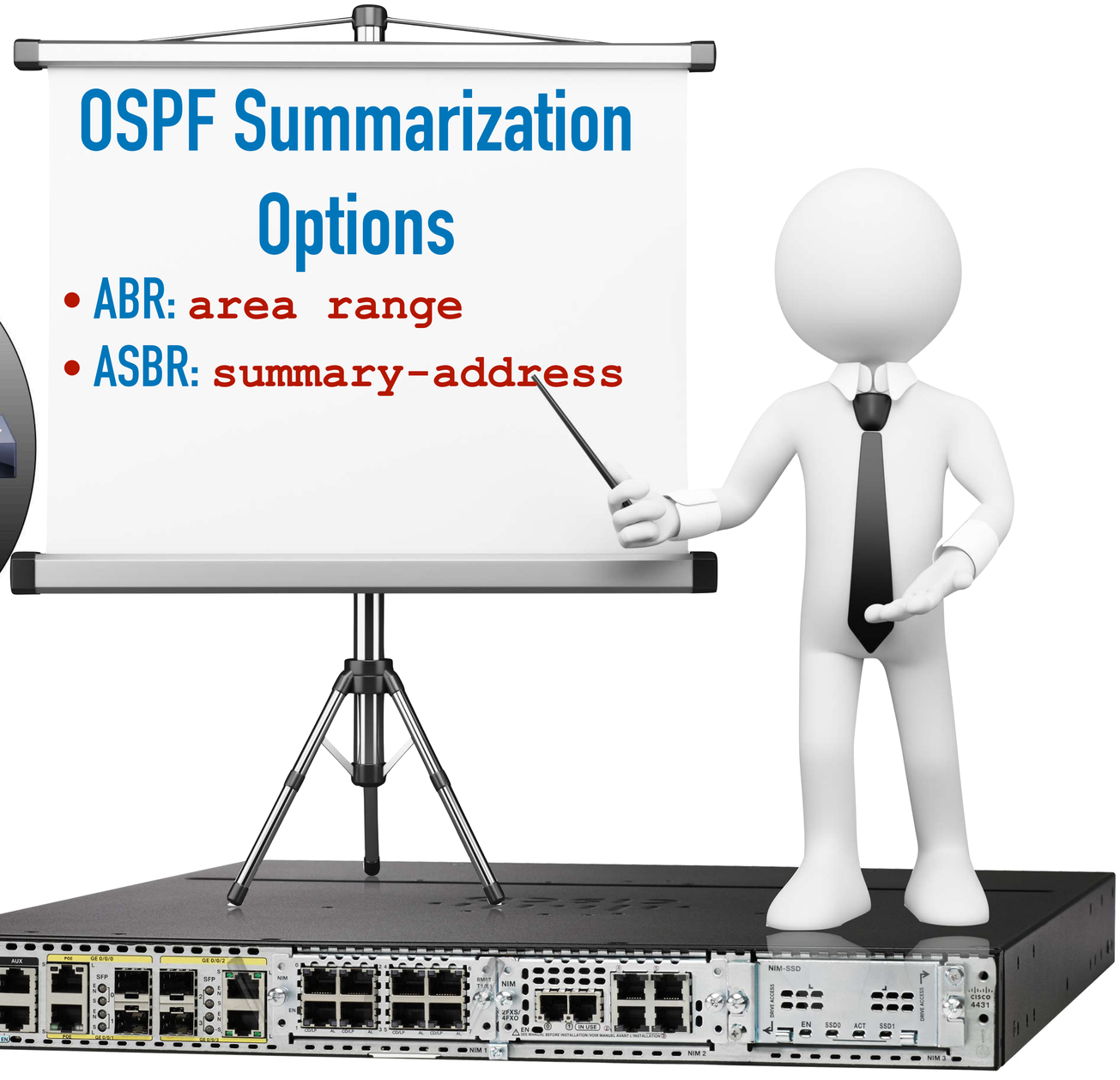
192.168.3.0 /24

192.168.0.0 /22

192.168.0.0 /22

Route Summarization Options



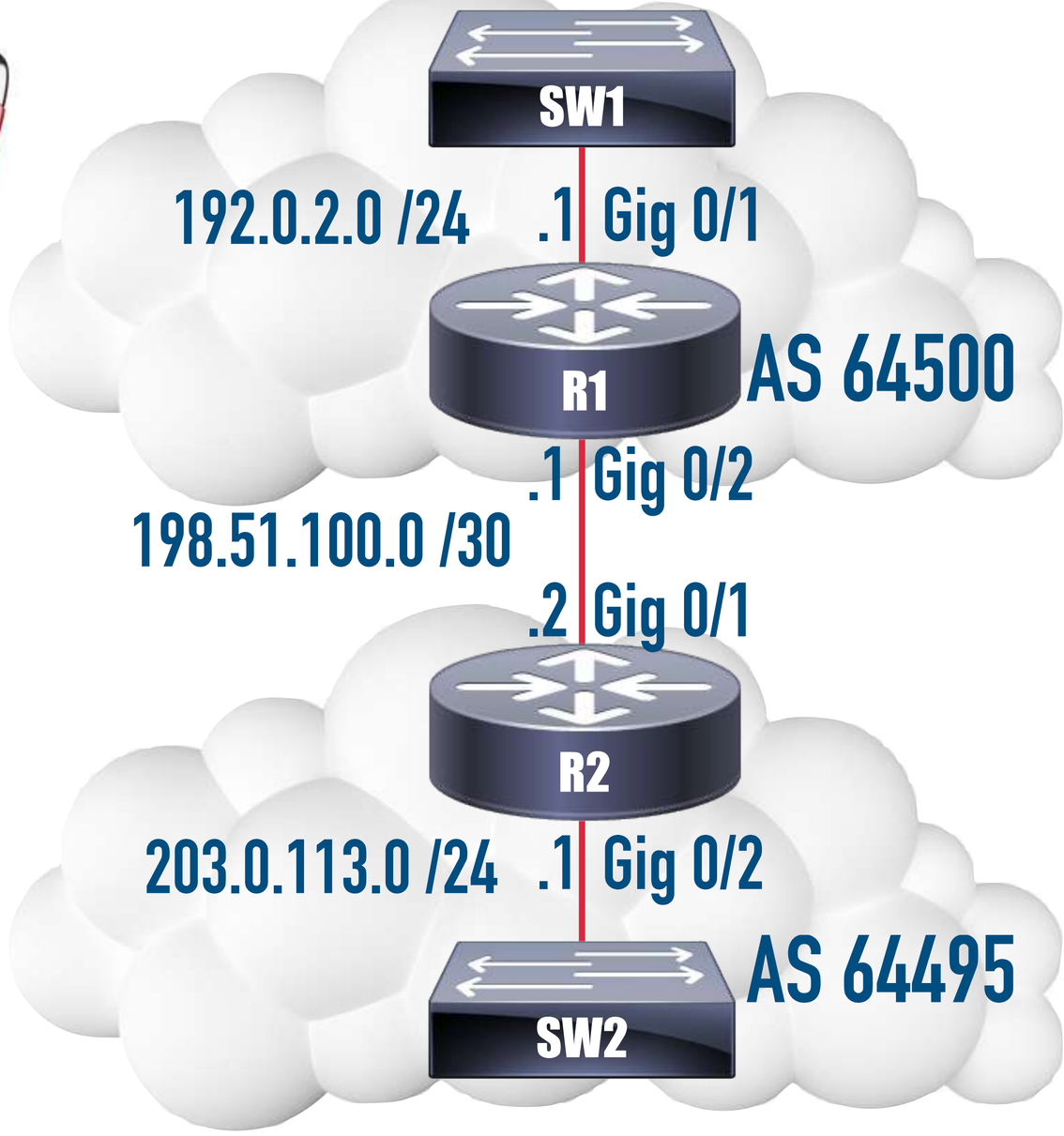


DEMO: OSPF Configuration

BGP

Border Gateway Protocol (BGP)

- Exterior Gateway Protocol (EGP)
- Forms Neighborships
- Neighbor's IP Address is Explicitly Configured
- A TCP Session is Established Between Neighbors
- Advertises Address Prefix and Length (Called Network Layer Reachability Information (NLRI))
- Advertises a Collection of Path Attributes Used for Path Selection
- Path Vector Routing Protocol

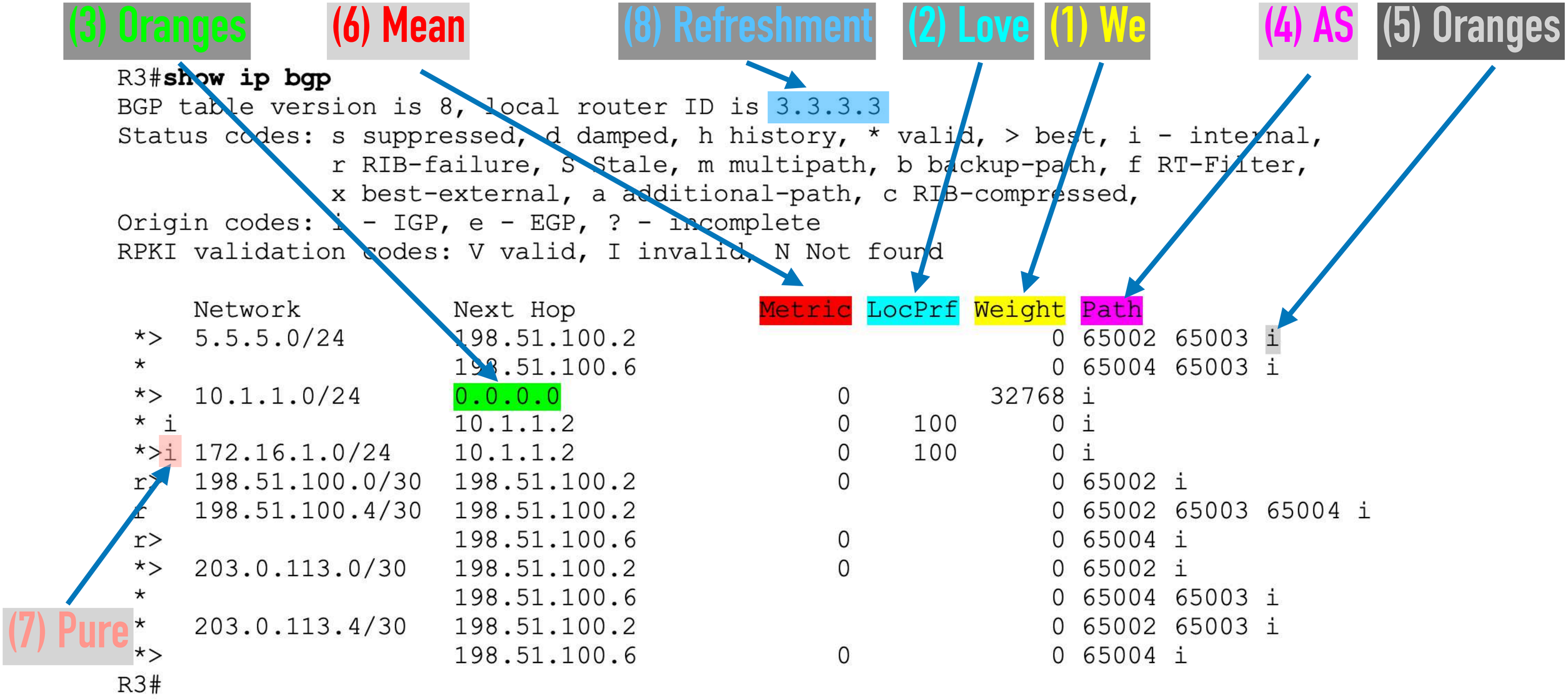


Weight
Local Preference
Originate
AS Path Length
Origin Type
Multi-Exit Discriminator (MED)
Paths
Router ID

We Love Oranges AS Oranges Mean Pure Refreshment

Path Selection Parameter	Description
Weight	A locally significant, Cisco-specific parameter that a router can set when receiving updates. A higher Weight is preferred. Commonly used to influence outbound routing decisions.
Local Preference	A parameter communicated throughout a single AS. A higher Local Preference is preferred. Commonly used to influence outbound routing decisions.
Originate	Paths sourced locally are preferred.
AS Path Length	The number of autonomous systems in the AS_PATH path attribute. Lower AS path lengths are preferred.
Origin Type	Indicates how the route was injected into BGP: i (`network` command), e (EGP), or ? (redistributed). i is preferred to e, and e is preferred to ?.
Multi-Exit Discriminator (MED)	A parameter set and advertised by routers in one AS to influence the BGP path selection decisions of routers in another AS. A lower MED is preferred.
Paths	Prefer eBGP path over iBGP path.
Router ID	A tie breaker, where the route received from the router with the lowest router ID is preferred.

BGP Path Selection



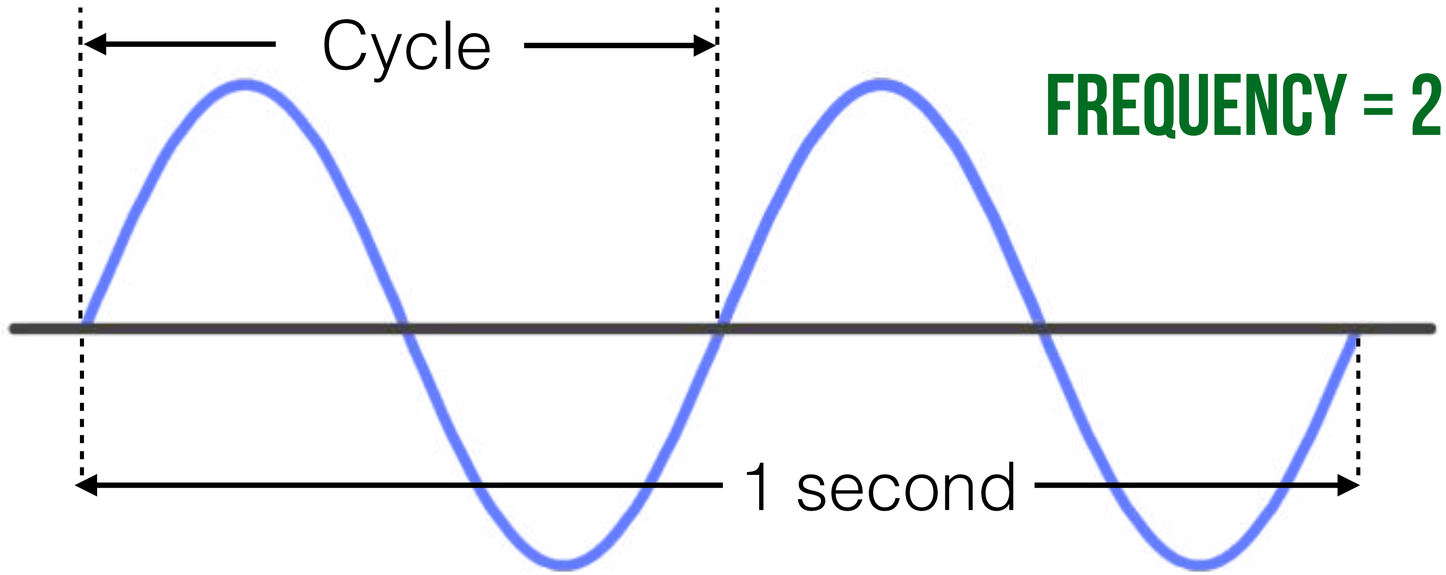

```
R3#show ip bgp
BGP table version is 8, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  5.5.5.0/24       198.51.100.2                          0 65002 65003 i
 *                    198.51.100.6                          0 65004 65003 i
 *>  10.1.1.0/24      0.0.0.0                  0         32768 i
 * i                  10.1.1.2                 0    100      0 i
 *>i 172.16.1.0/24    10.1.1.2                 0    100      0 i
 r>  198.51.100.0/30  198.51.100.2            0             0 65002 i
 r   198.51.100.4/30  198.51.100.2                          0 65002 65003 65004 i
 r>                   198.51.100.6             0             0 65004 i
 *>  203.0.113.0/30   198.51.100.2             0             0 65002 i
 *                    198.51.100.6                          0 65004 65003 i
 *   203.0.113.4/30   198.51.100.2                          0 65002 65003 i
 *>                   198.51.100.6             0             0 65004 i
R3#
```

BGP Configuration Demo

Wireless Technologies

Wireless Communication Theory

Wireless Communication Theory



FREQUENCY = 2 HERTZ (HZ)

Frequency = Number of complete cycles per second

Cycle = One complete up and down motion

Hertz = Measurement of cycles per second

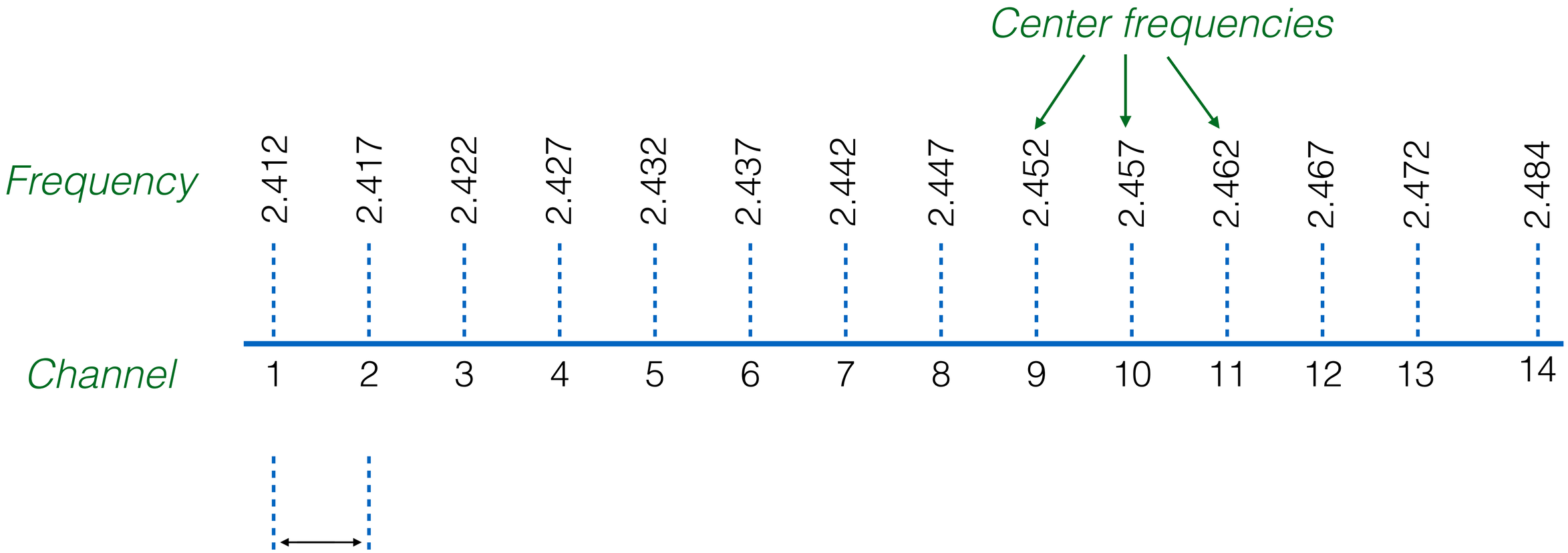
Wireless Communication Theory

Radio Frequency (RF) Range:

- Between 3 kilohertz (kHz) and 300 Gigahertz (GHz)
- Wireless communication found within this range
- 2.4 GHz band = 2.4 to 2.4835 GHz
- 5 GHz band = 5.15 to 5.85 GHz
- Wireless bands subdivided into channels

Wireless Communication Theory

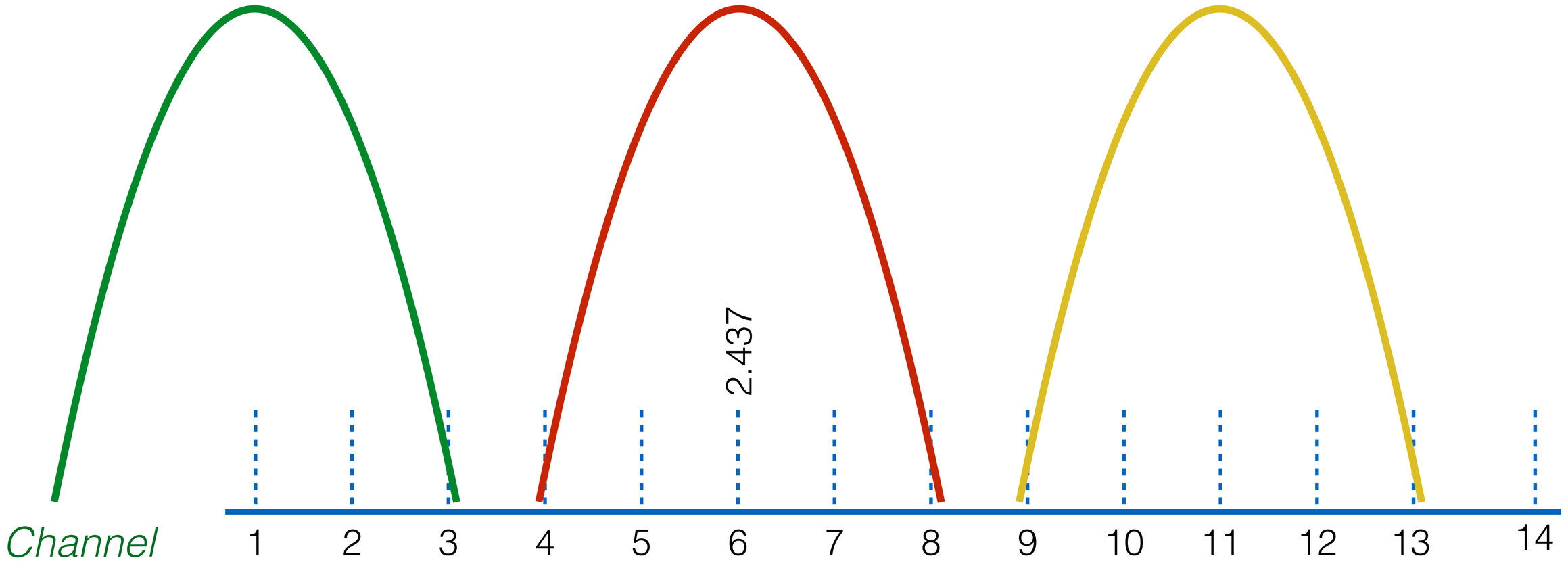
2.4 GHz Wireless Band



5 MHz (0.005 GHz) between bands

Wireless Communication Theory

2.4 GHz Wireless Band



Wireless Communication Theory

RF Signal Strength:

- Measured in decibel milliwatts (dBm)
- Transmitters range between 1 and 100 milliwatts (mW)
- Milliwatt (mW) = 1/1000 of a watt

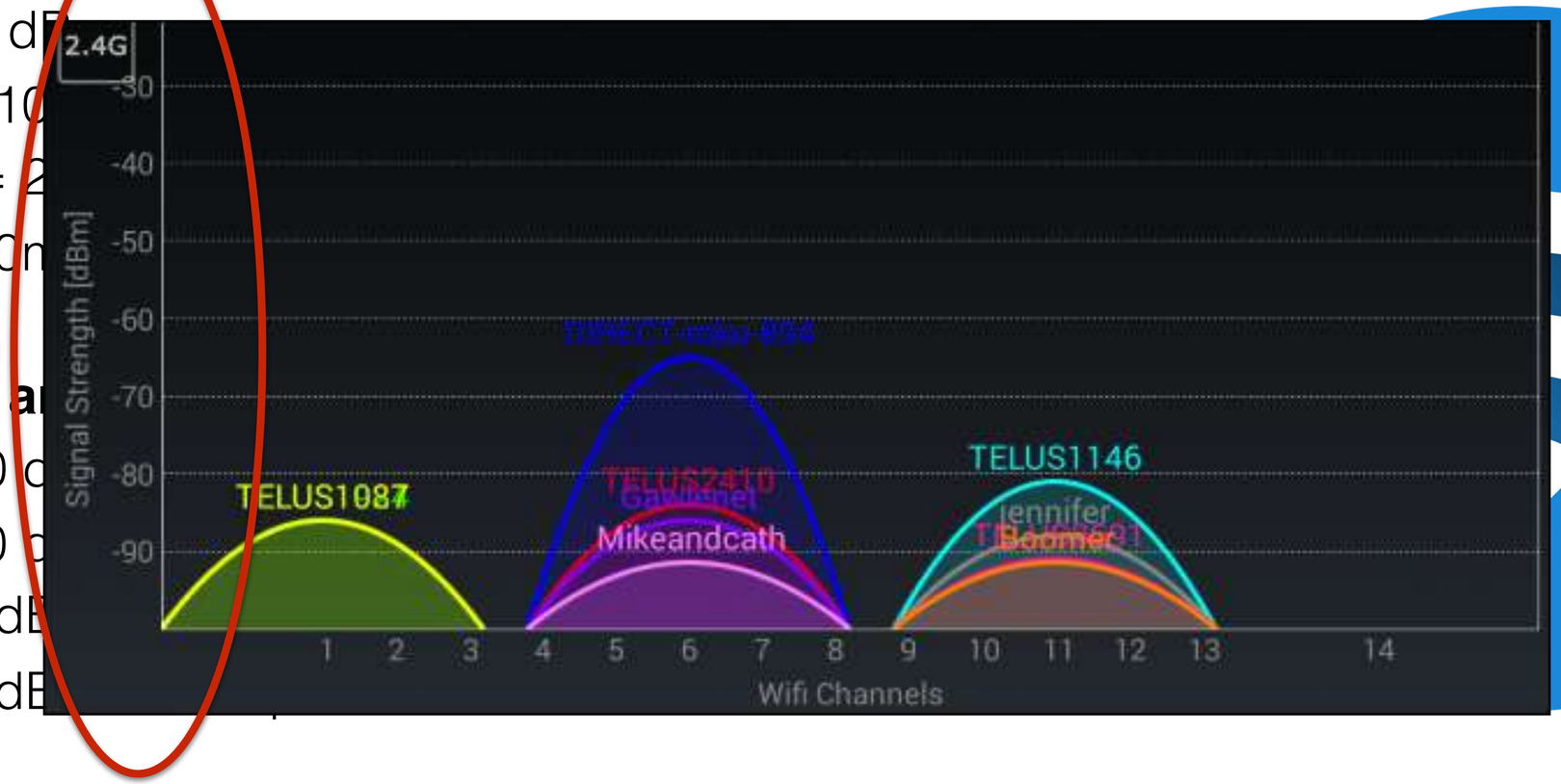
Wireless Communication Theory

mW to dBm Relationship:

- 1 mW = 0 dB
- 10 mW = 10
- 100 mW = 2
- 1W = 1000m

Rule of 10s a

- Gain of 10 d
- Loss of 10 d
- Gain of 3 dB
- Loss of 3 dB



Received Signal Strength Indicator (RSSI):

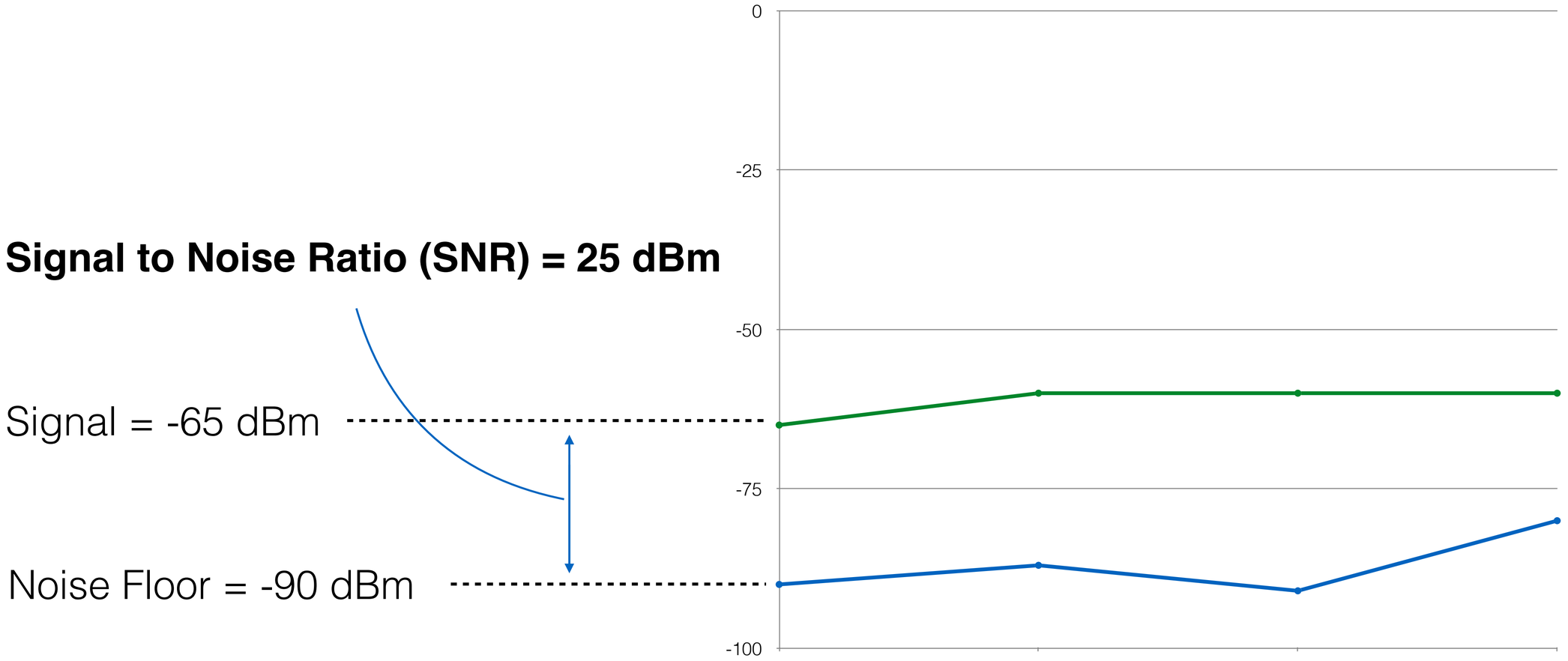
- Closer to zero value means a stronger signal

Wireless Communication Theory

Signal to Noise Ratio (SNR):

- Difference in decibels between signal and background noise

Signal to Noise Ratio (SNR) = 25 dBm



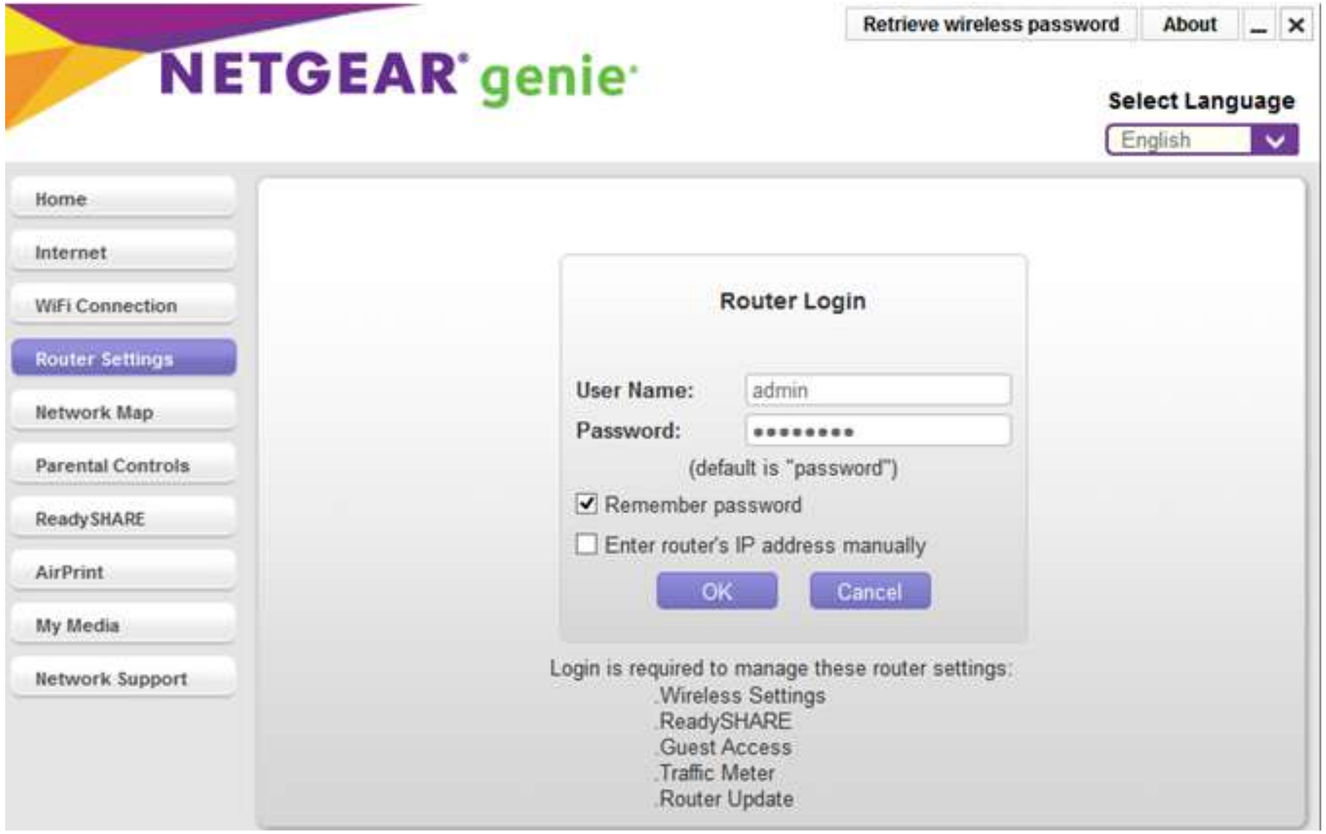
Access Point Modes

Access Point Modes

Autonomous Access Points:

- Each access point works as a st
- No knowledge of other acc
- Configured individually wit
- Not ideal when needing mor

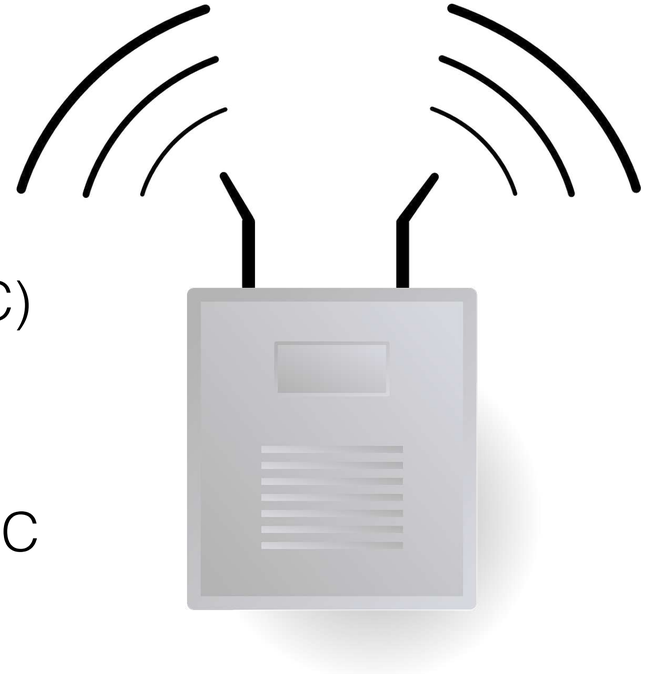
Access Point Modes



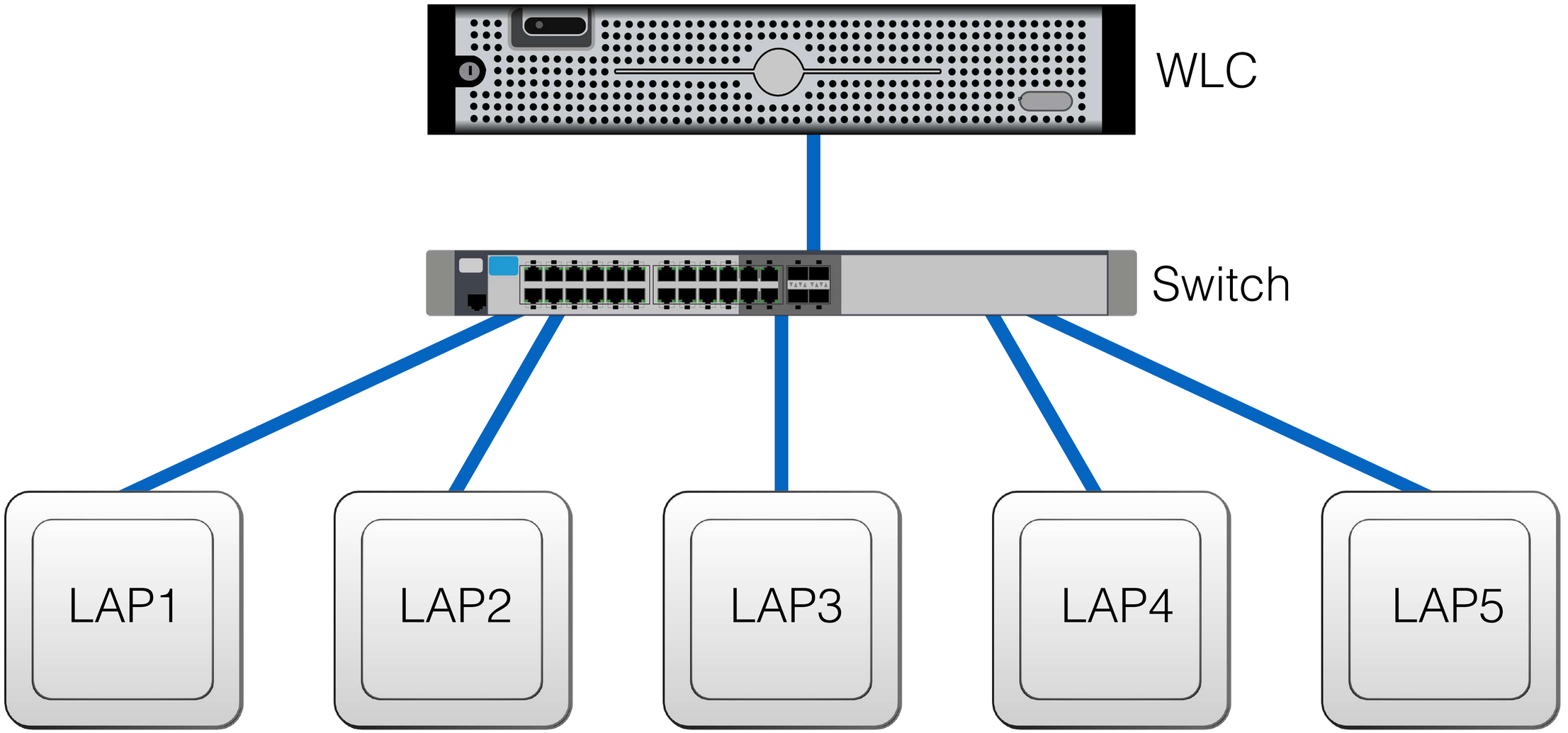
Access Point Modes

Lightweight Access Points:

- Under the management of a wireless LAN controller (WLC)
- Propagate an SSID throughout a large area
- Cisco solutions are moving to software-based WLCs
- All configuration and management takes place on the WLC

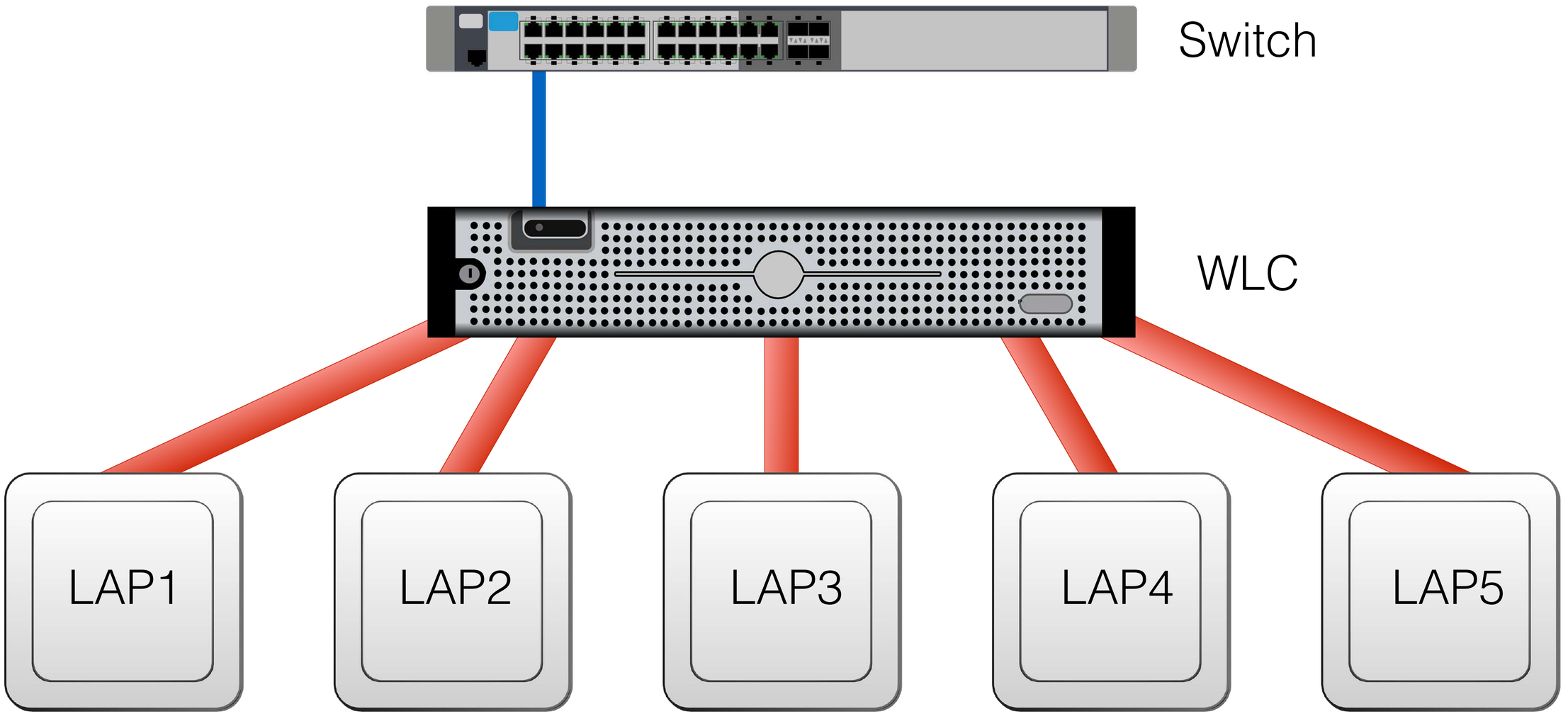


Access Point Modes



Power over Ethernet (PoE): Allows network cables to carry data and power to LAPs

Access Point Modes



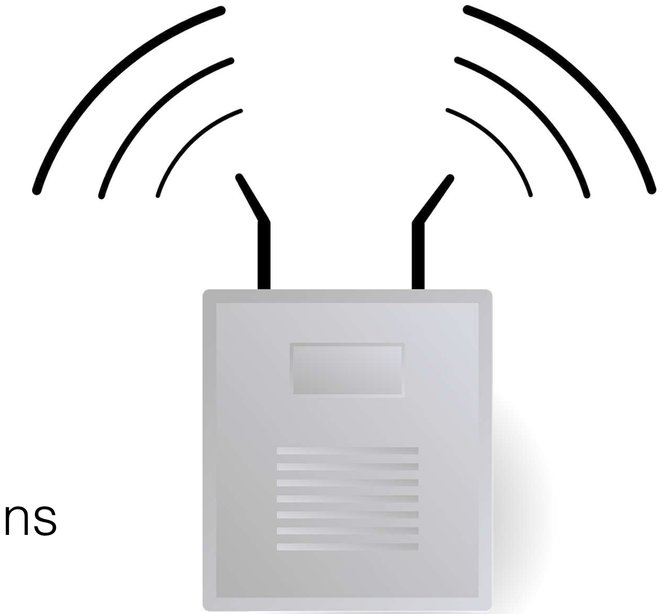
Control and Provisioning of Wireless Access Points (CAPWAP): Encrypted tunnel communication

Access Point Modes

LAP Special Purpose Modes

Local Mode:

- Default operating mode for LAPs
- Provides SSID and wireless network access
- When not actively in use, LAP will perform background operations

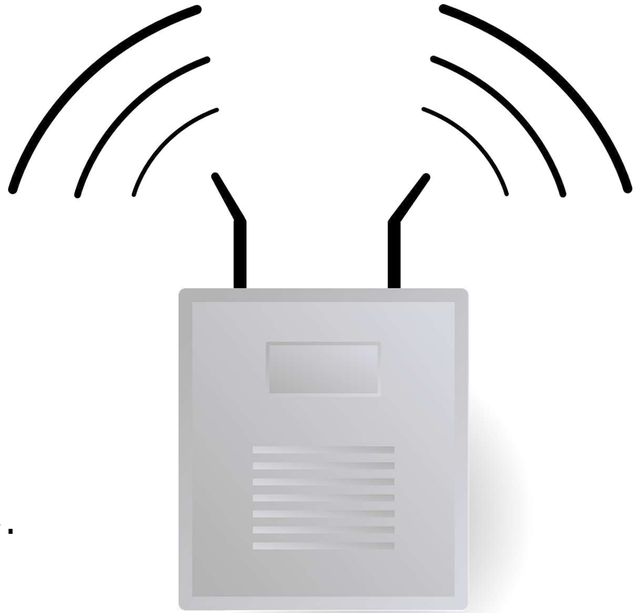


Access Point Modes

LAP Special Purpose Modes

Monitor Mode:

- LAP only performs background operations
- No network access provided to users
- Monitoring of IDS event, rogue APs, location-based services, etc.



Access Point Modes

LAP Special Purpose Modes

FlexConnect Mode:

- Allows for management of LAPs at a remote location
- Controlled over a WAN connection

Access Point Modes

LAP Special Purpose Modes

Sniffer Mode:

- LAP acts as a packet capture device
- Dedicated to receiving wireless traffic
- Traffic forwarded to a traffic analyzer system for analysis

Access Point Modes

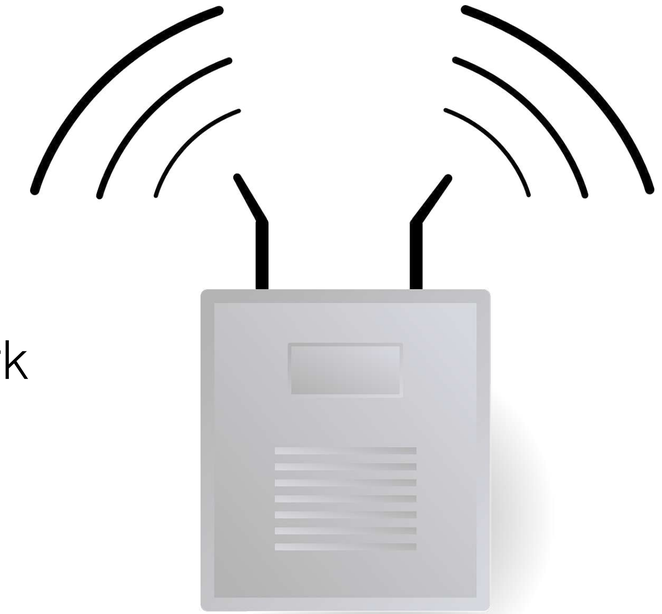
LAP Special Purpose Modes

Rogue Detector Mode:

- LAP is dedicated to the discovery of rogue devices
- Checks the MAC addresses of clients against known addresses
- Helps to prevent MAC spoofing and similar attacks

Access Point Modes

LAP Special Purpose Modes



Bridge Mode:

- LAP is used to bridge together separate sites as a mesh network
- Point-to-point
- Point-to-multipoint

Access Point Modes

LAP Special Purpose Modes

Flex+Bridge Mode:

- Combines FlexConnect and Bridge mode function
- Mesh network that can be controlled remotely

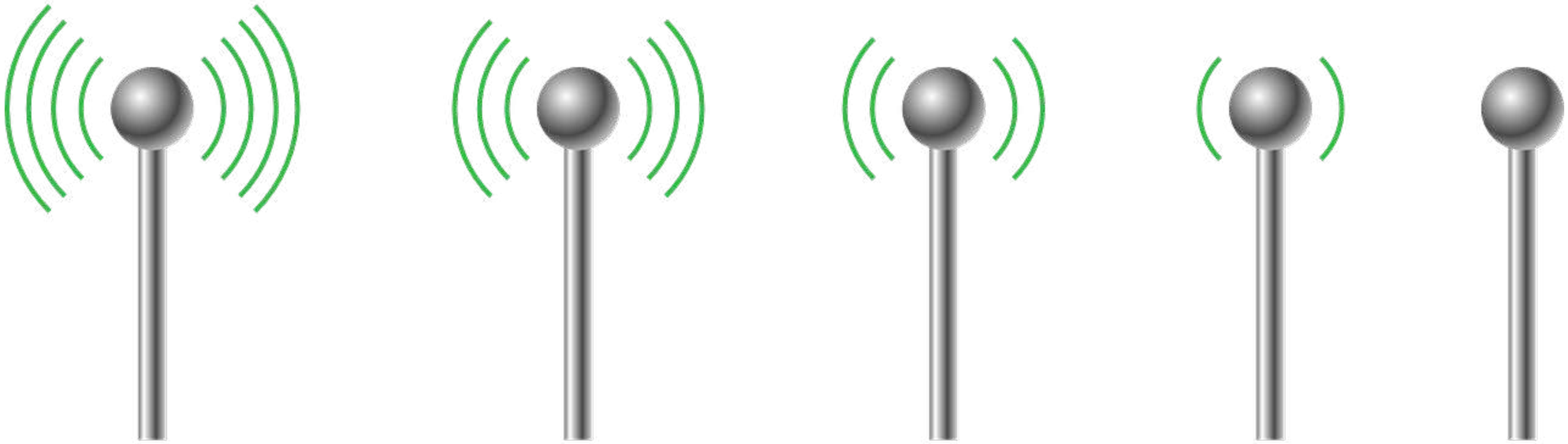
Access Point Modes

LAP Special Purpose Modes

SE-Connect Mode

- LAP operates as a spectrum analyzer device
- Gathers information about all channels
- Forwards information to a spectrum analysis tool
- Cisco Spectrum Expert

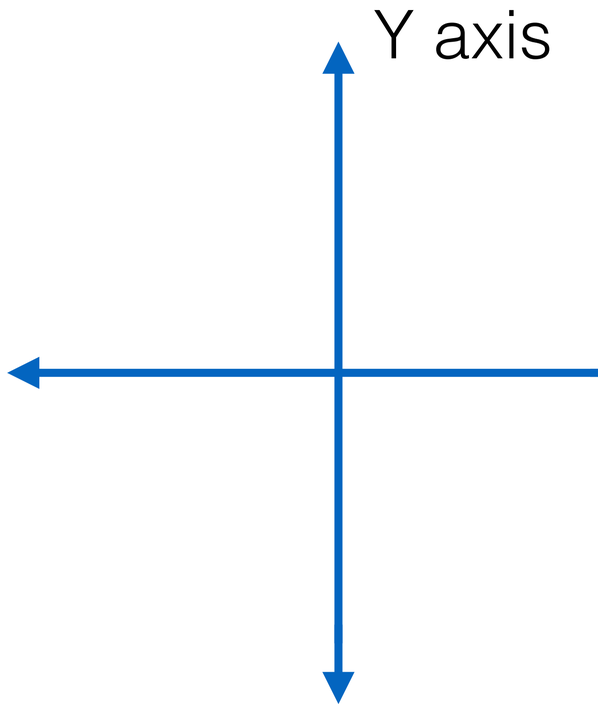
Antenna Types



Antenna Types

Radiation Pattern:

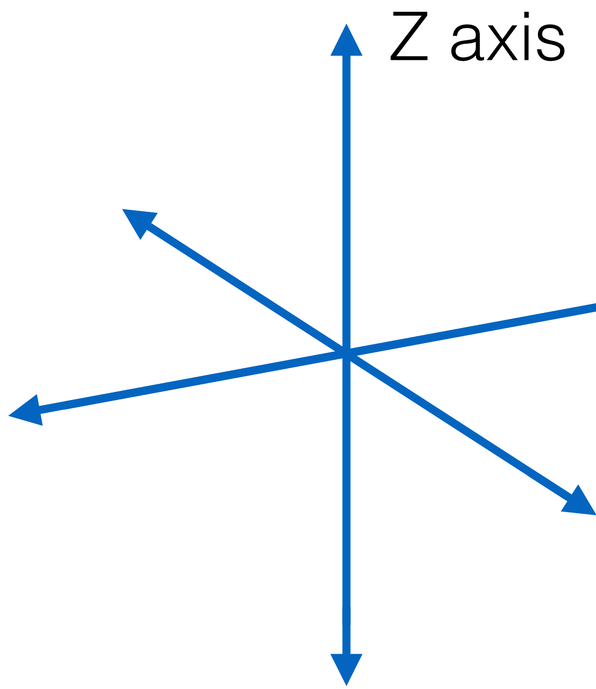
- The measure of signal strength around an antenna



Antenna Types

Radiation Pattern:

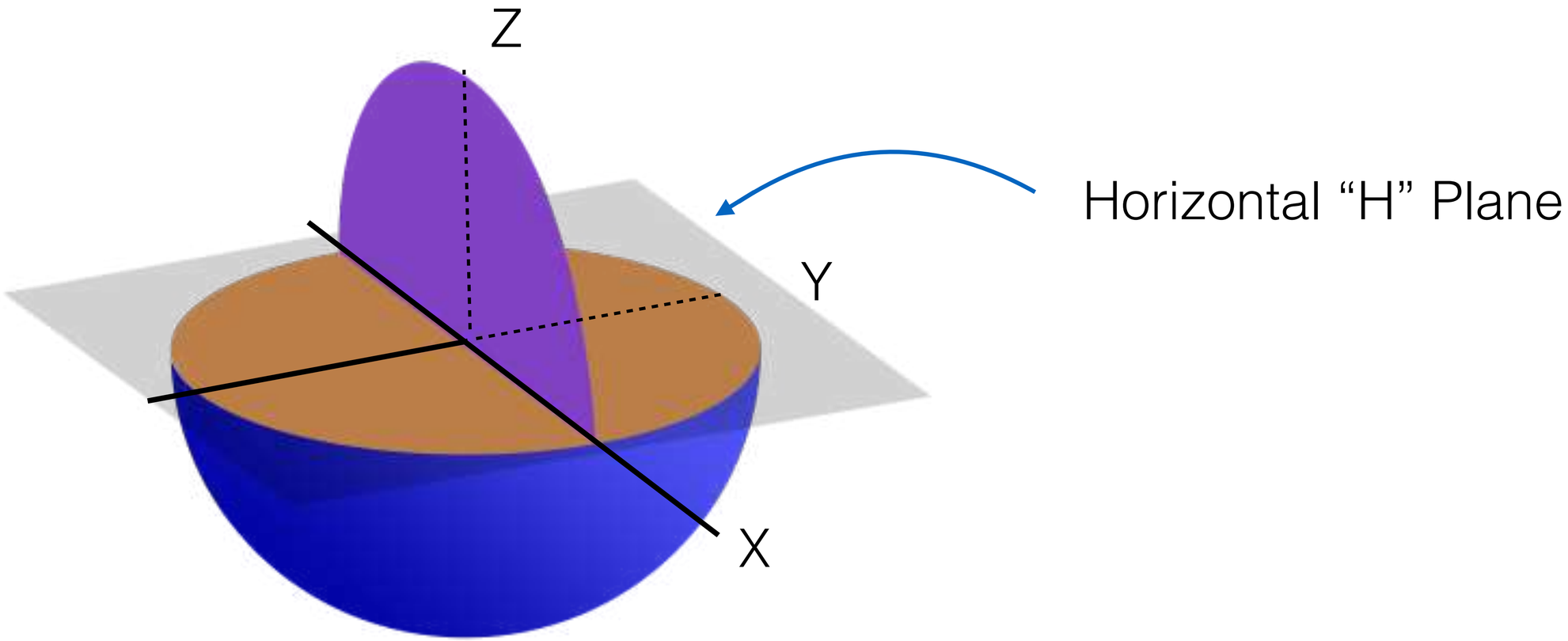
- The measure of signal strength around an antenna



Antenna Types

Radiation Pattern:

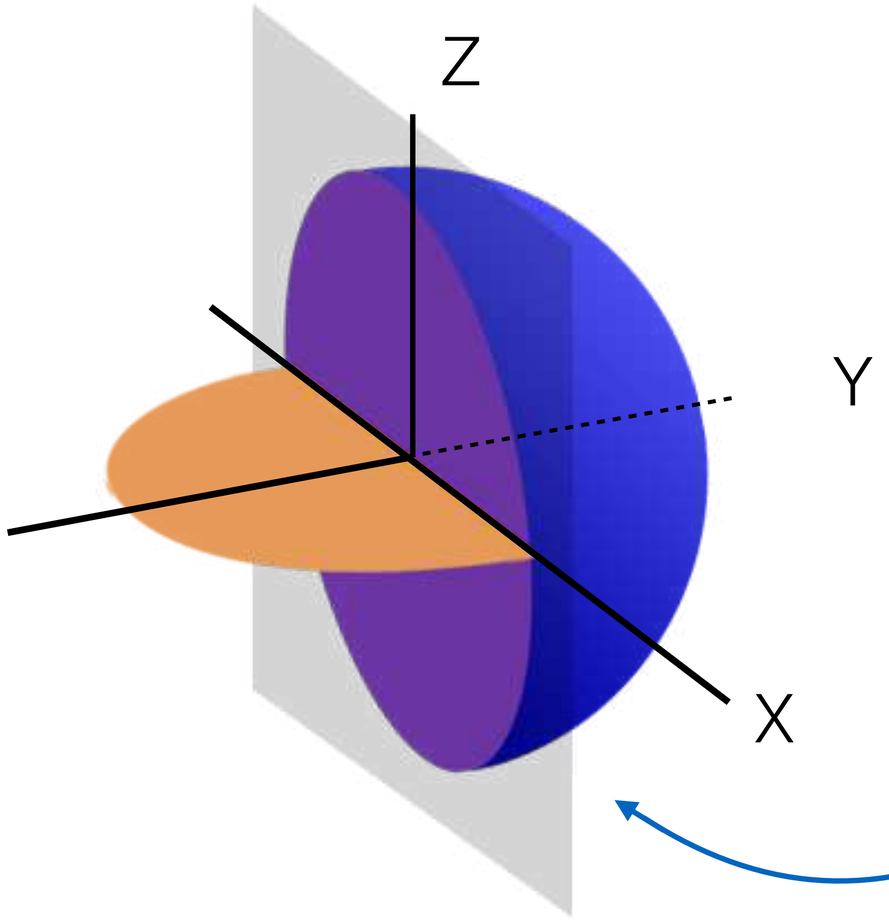
- The measure of signal strength around an antenna

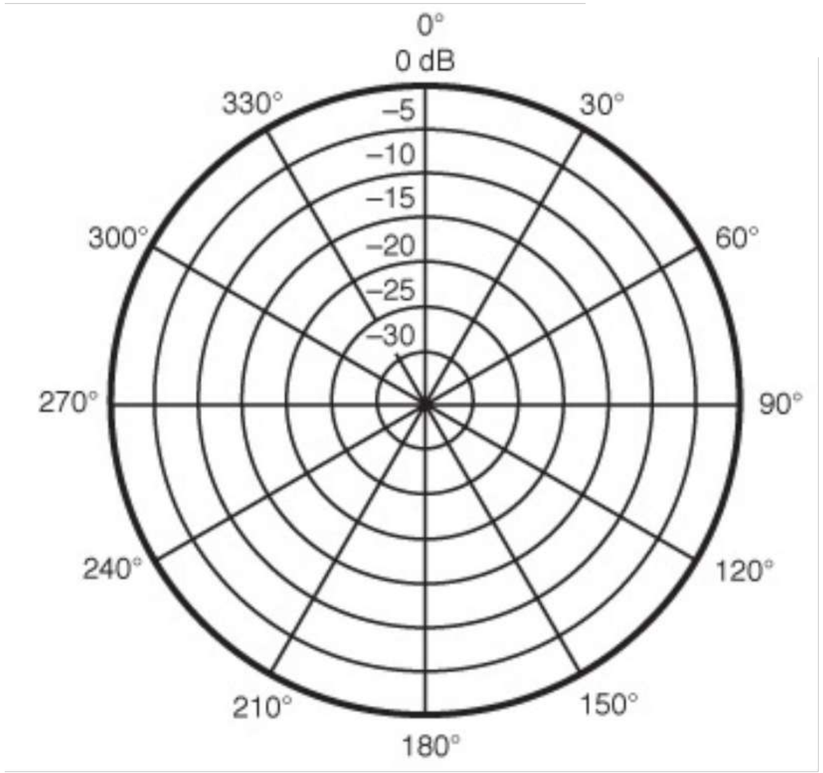


Antenna Types

Radiation Pattern:

- The measure of signal strength around an antenna



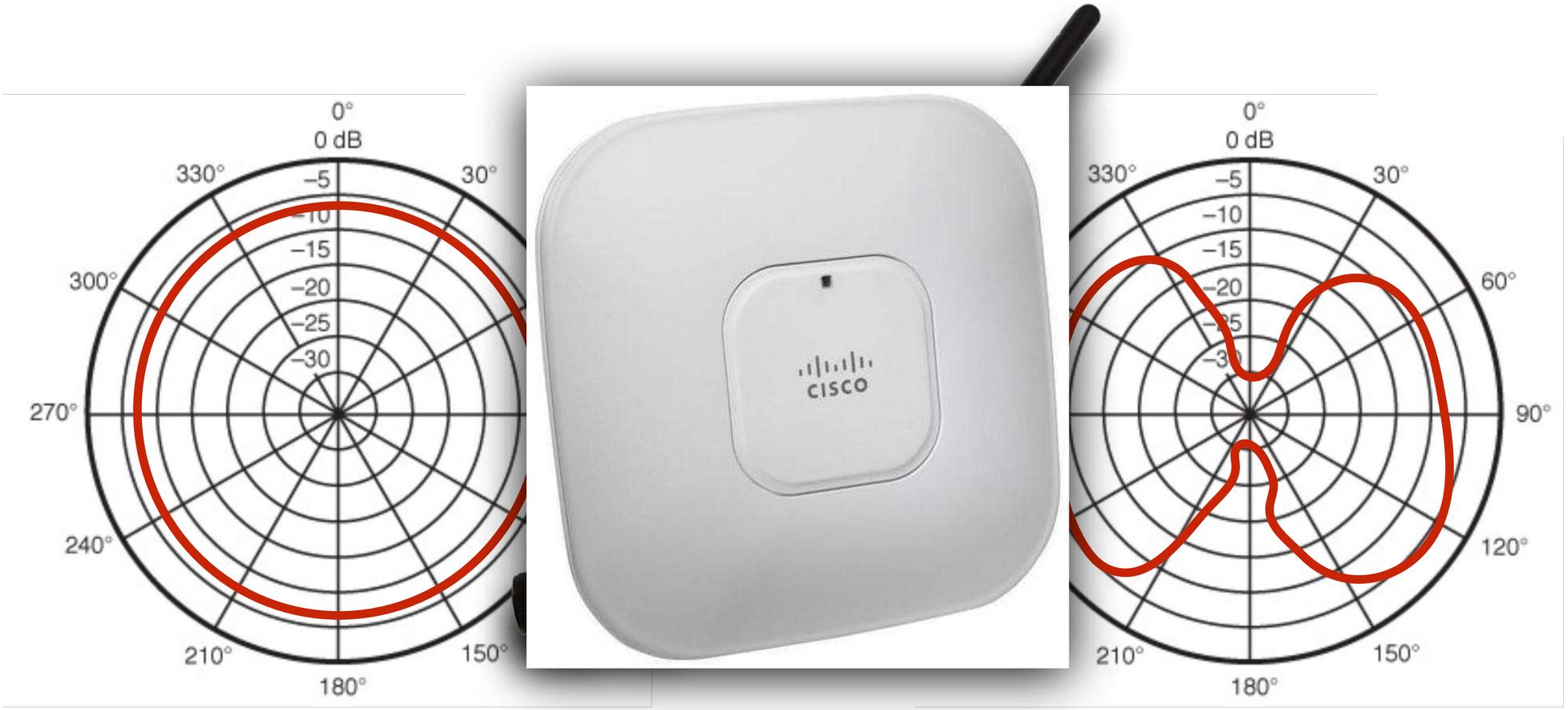


Elevation “E” Plane

Antenna Types

Omnidirectional Antennas:

- Designed to propagate signal in all directions



H Plane

E Plane

Antenna Types

Directional Antennas:

- Designed to propagate in a specific direction

Patch Antenna

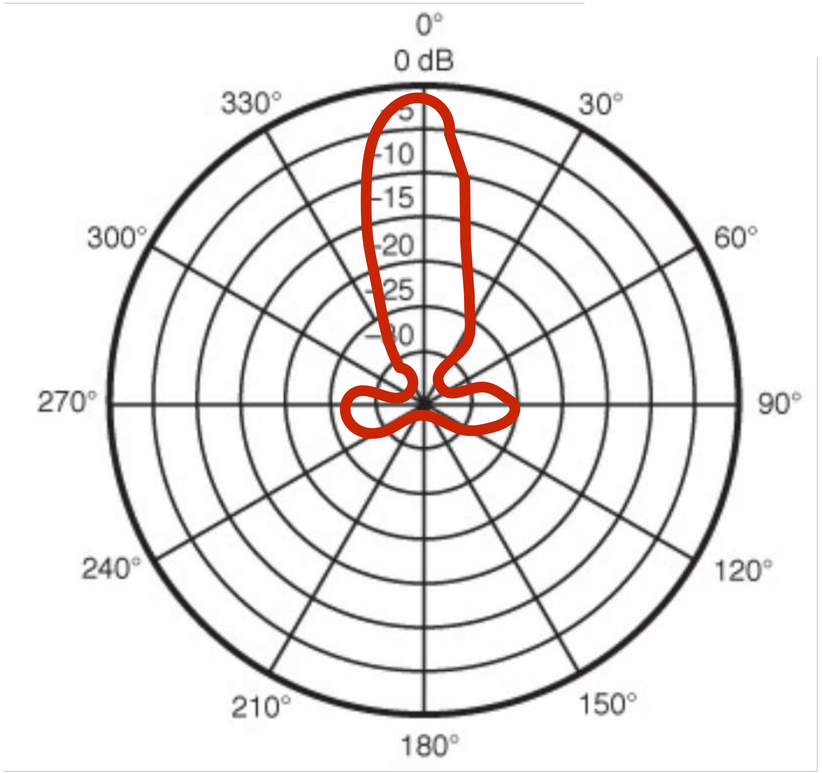
Yagi Antenna

Dish Antenna

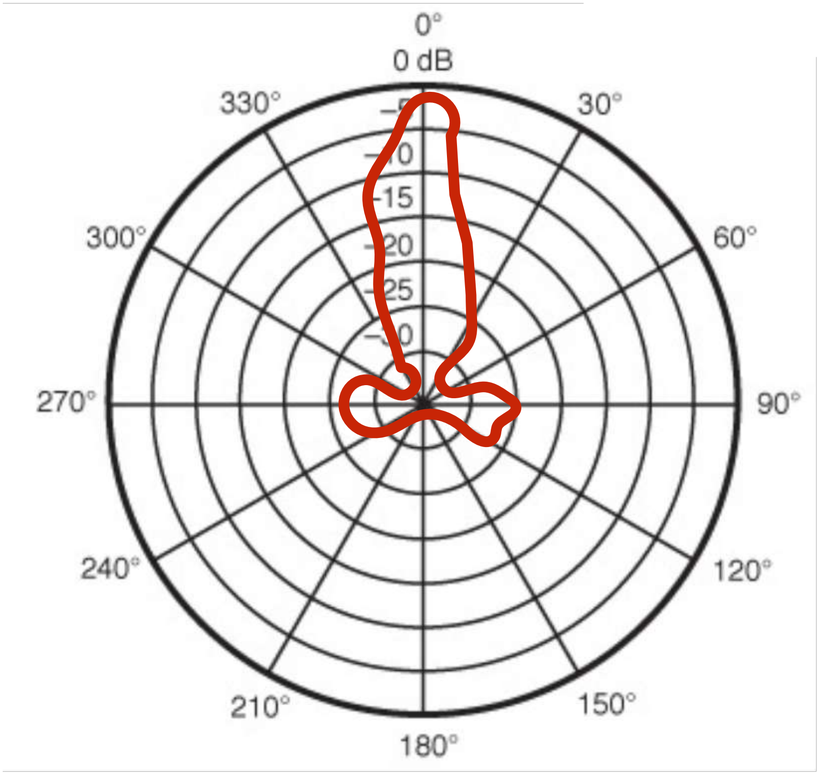
Antenna Types – Yagi Example

Directional Antennas:

- Designed to propagate in a specific direction



H Plane

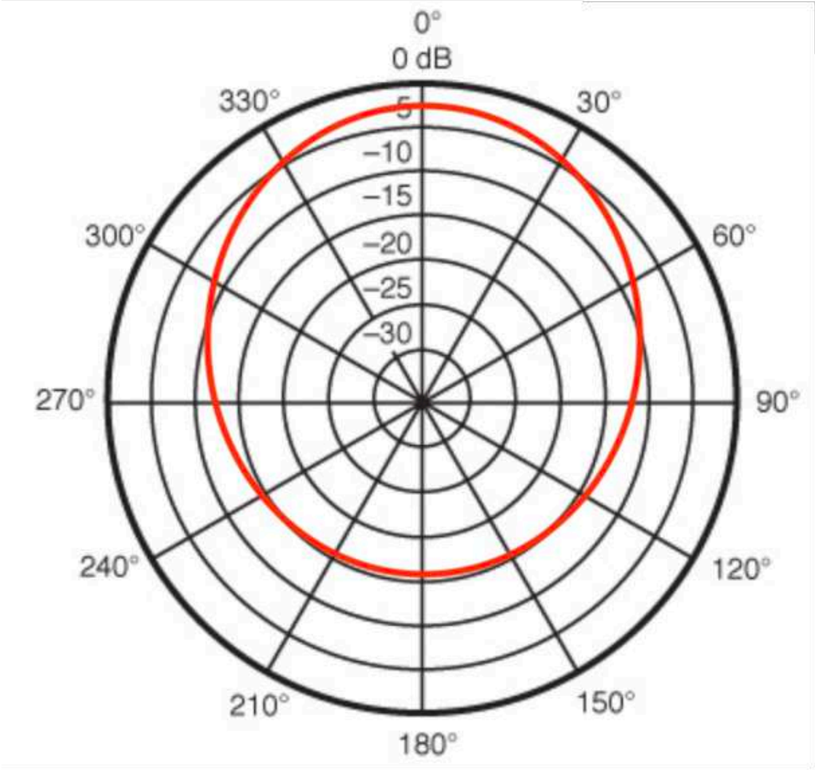


E Plane

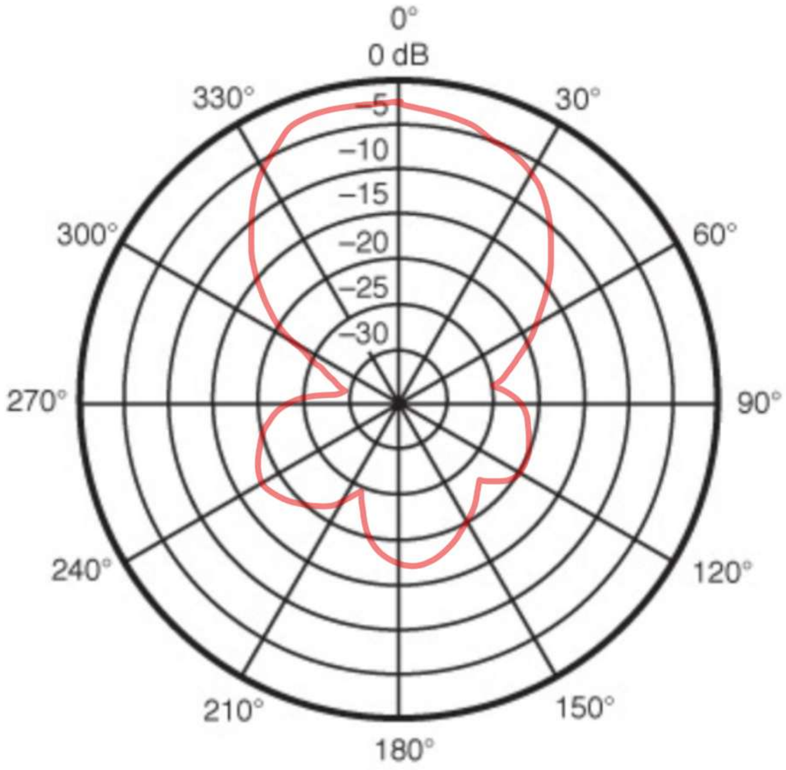
Antenna Types – Patch Example

Directional Antennas:

- Designed to propagate in a specific direction



H Plane



E Plane

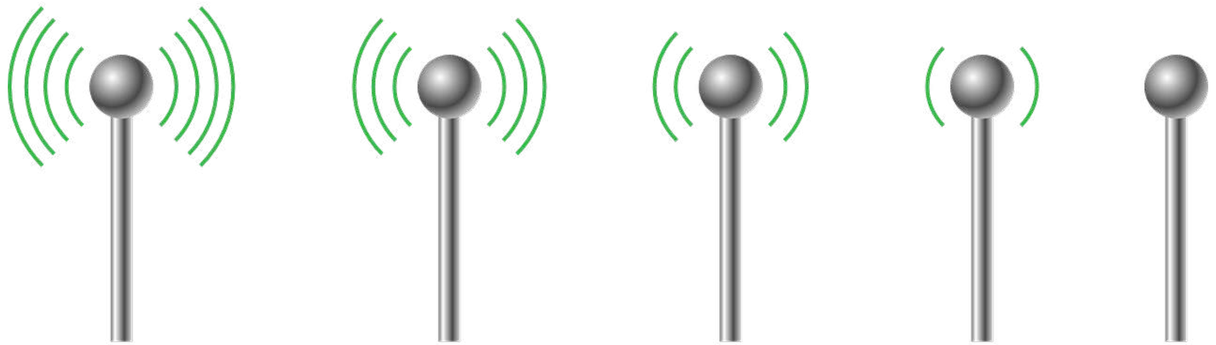
Antenna Types

Omnidirectional Antennas:

- Lower gain, with a less focused path
- Better for broad coverage

Directional Antennas:

- Higher gain, with a very focused path
- Better for specifically directing coverage

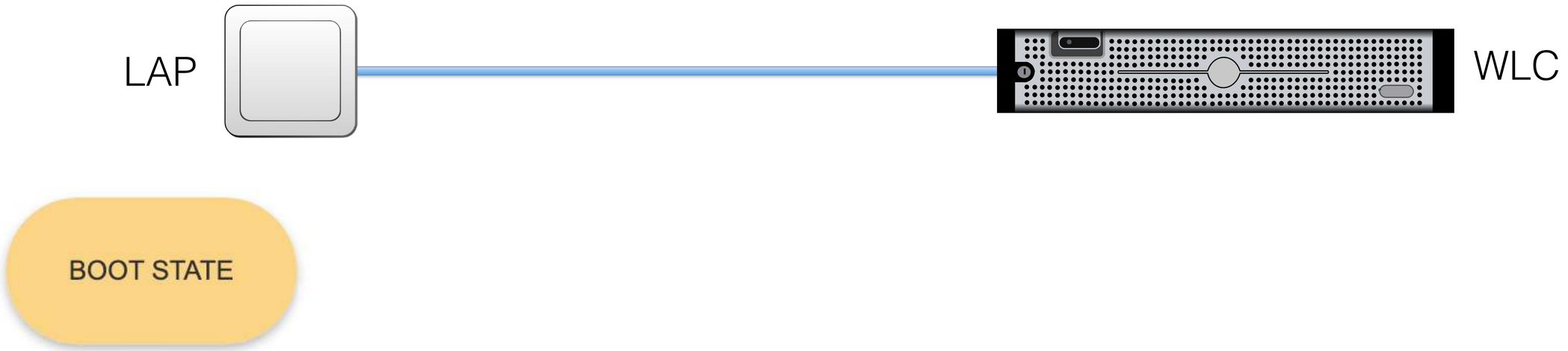


Access Point Operation

Lightweight Access Points:

- Cisco LAPs are designed as “touch free”
- All configuration is on the WLC side of things
- Eight common states that the LAP progresses through

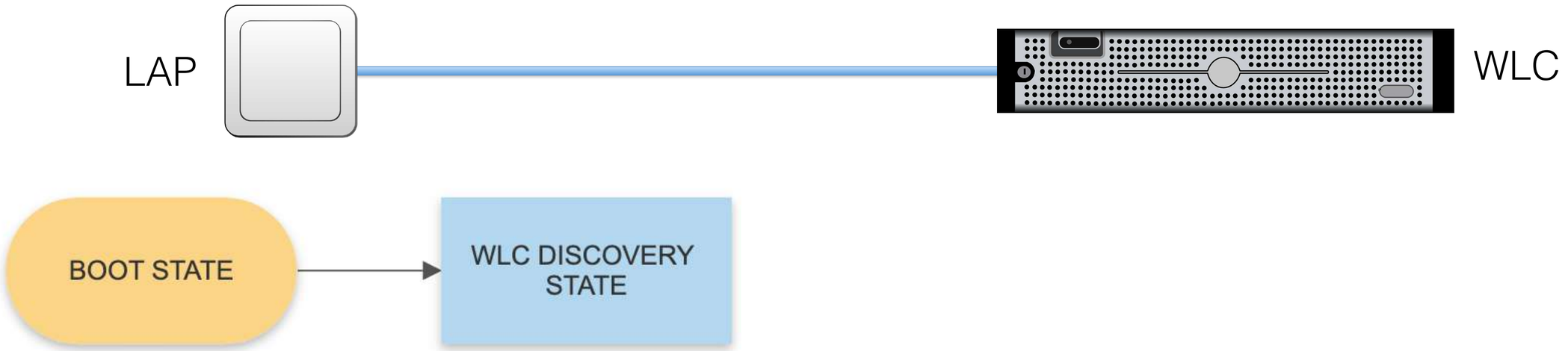
Access Point Operation



Boot State:

- LAP boots from local IOS image and receives addressing

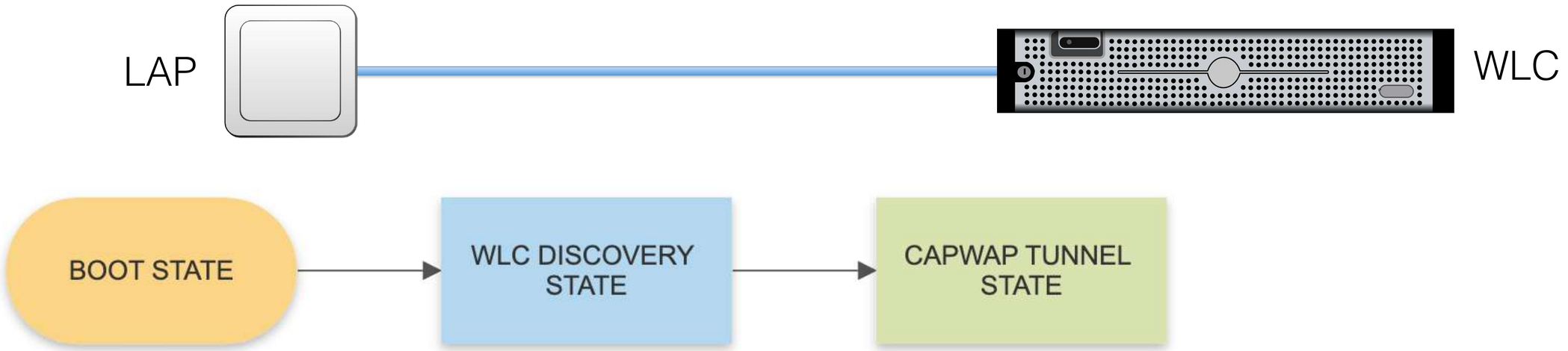
Access Point Operation



WLC Discovery State:

- LAP actively searches for a controller with CAPWAP Discovery Request messages
- Broadcast over UDP 5246 and directly to known WLC IP addresses

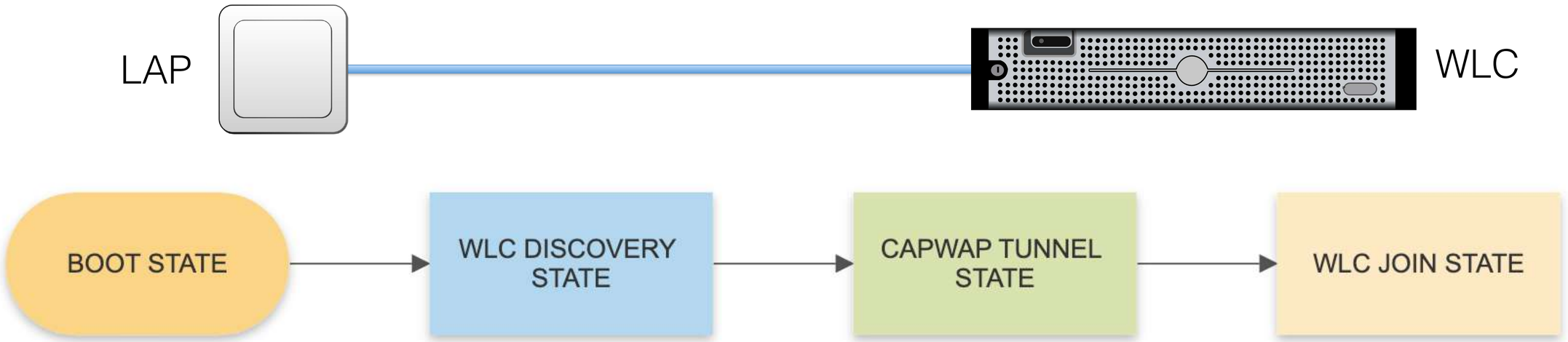
Access Point Operation



CAPWAP Tunnel State:

- CAPWAP tunnels are established between LAP and WLC

Access Point Operation



WLC Join State:

- CAPWAP message exchange authenticates and associates LAP with WLC

Access Point Operation

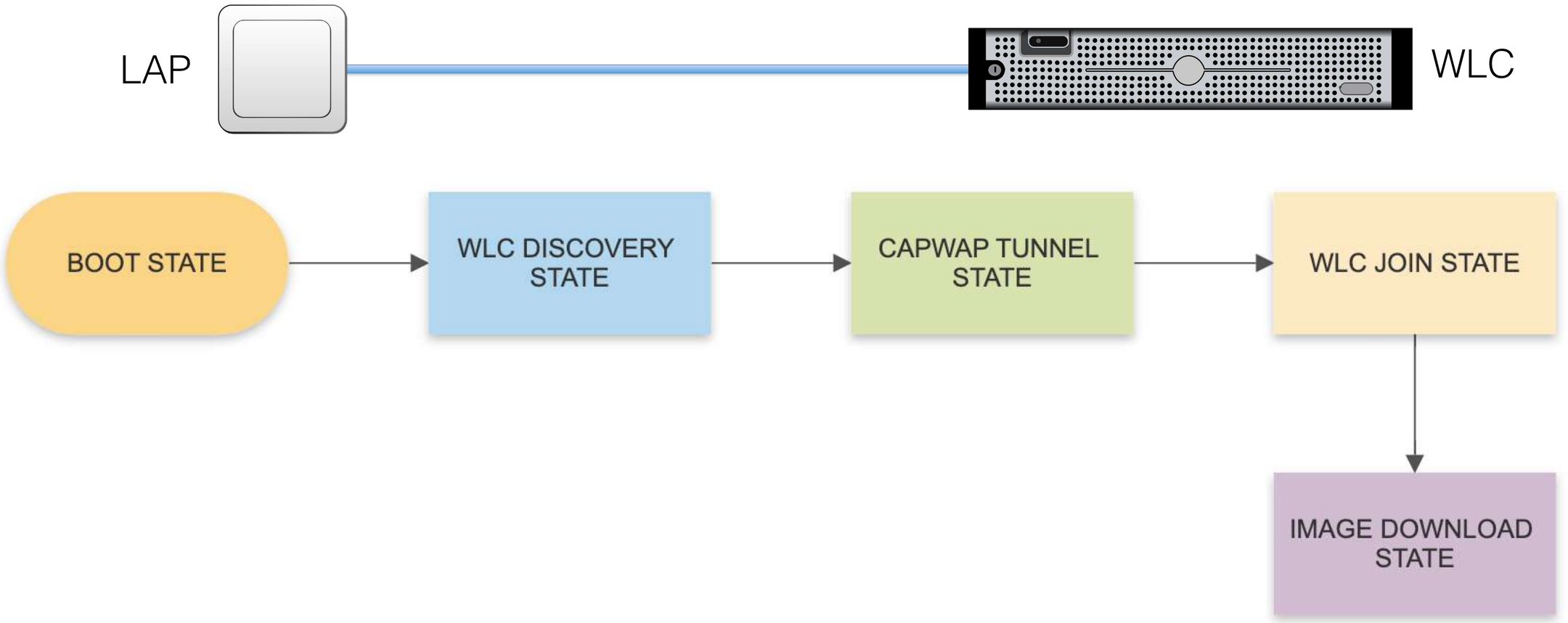
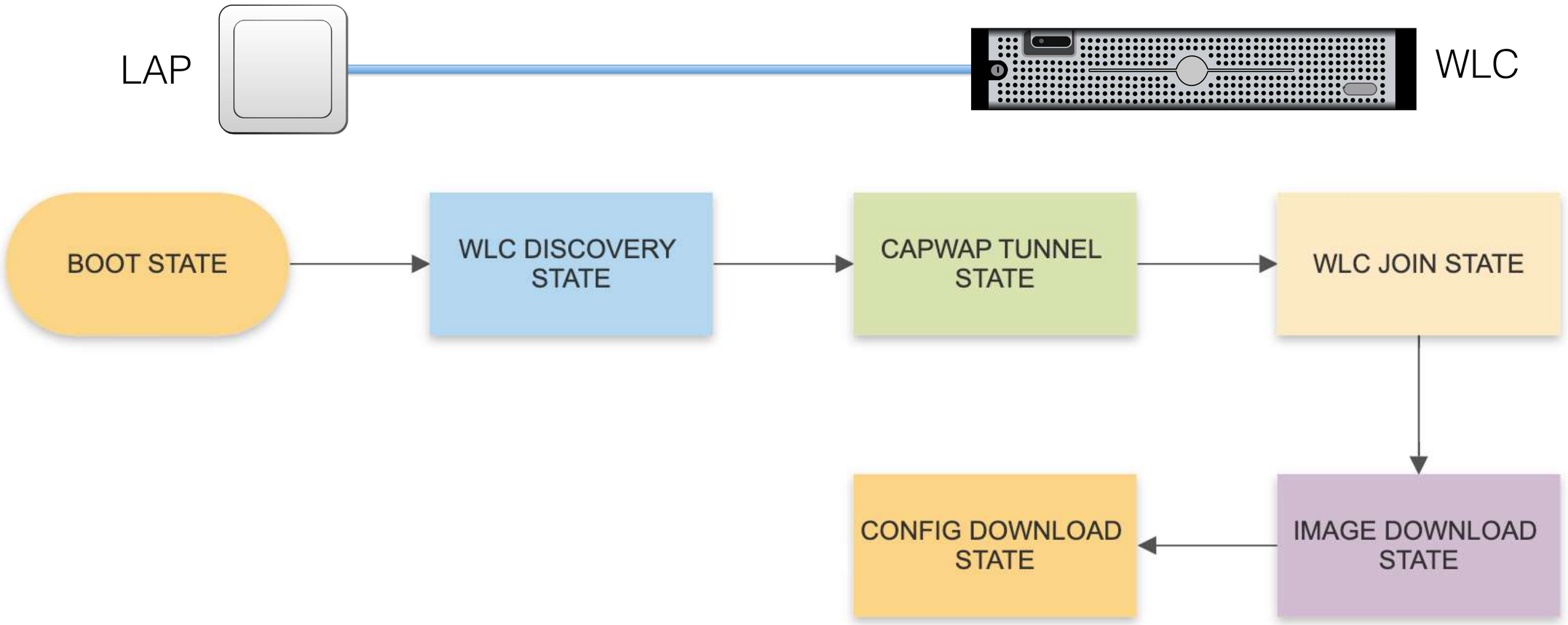


Image Download State:

- LAP compares local software image version to that of the WLC and updates if necessary

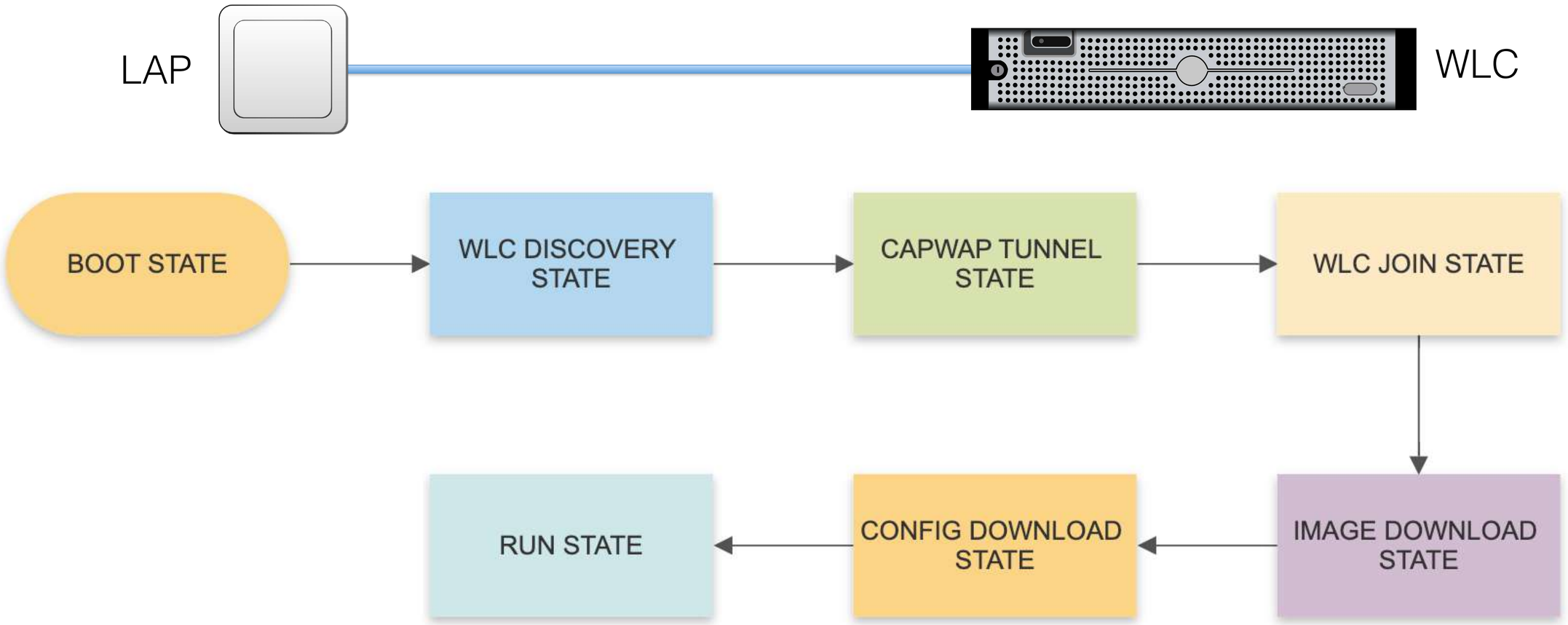
Access Point Operation



Config Download State:

- LAP polls the WLC for configuration information (security, QoS, SSID, etc.)

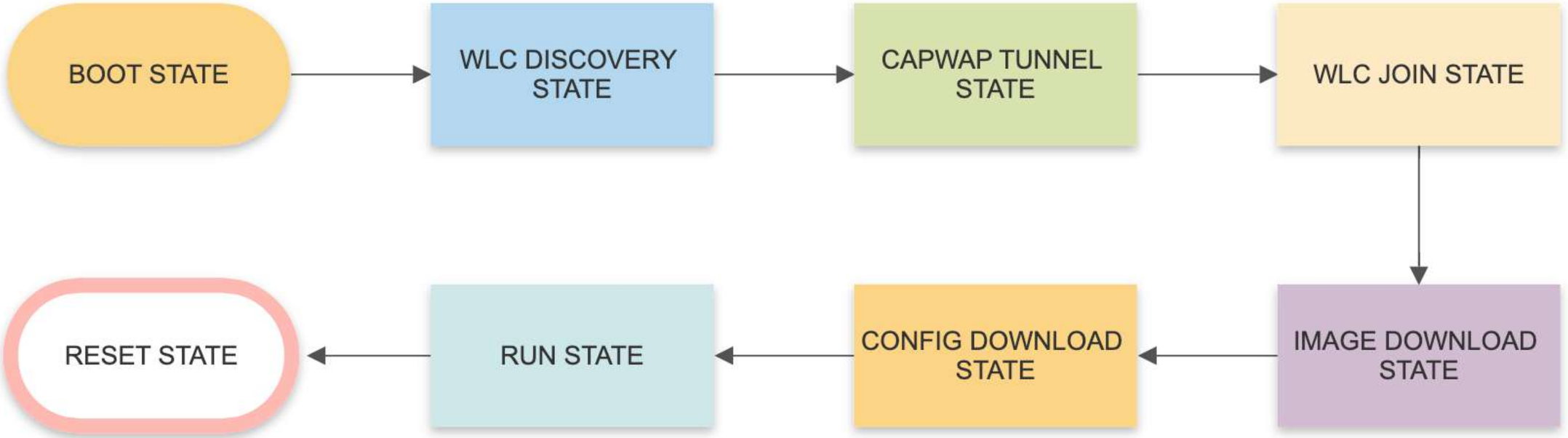
Access Point Operation



Run State

- LAP is fully operational and providing network access via a basic service set (BSS)

Access Point Operation



Reset State:

- LAP tears down CAPWAP tunnels and erases client associations, then restarts process

Access Point Operation

WLC Discovery Process:

- Goal is to find as many controllers as possible

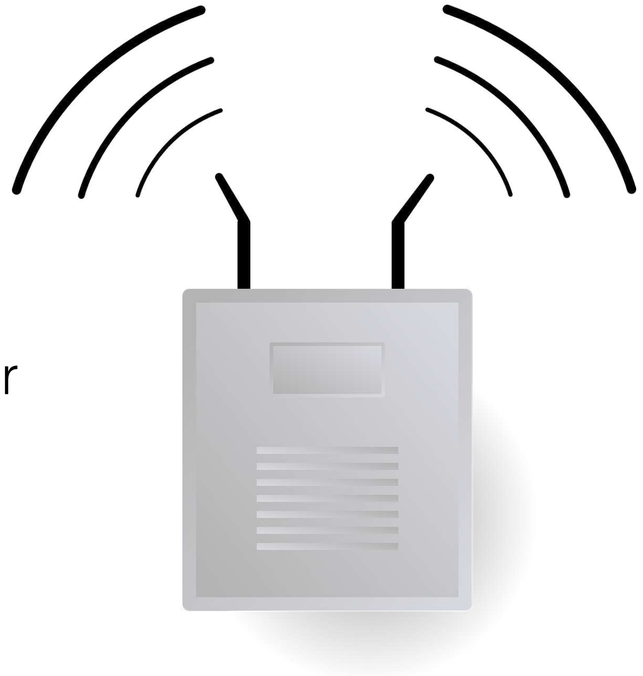
1. *CAPWAP Discovery Request* messages sent out from LAP as a broadcast on the local subnet

2. Locally stored WLC management IP addresses used

3. DHCP Option 43 information used, if configured on DHCP server

4. LAP attempts to resolve a DNS request to *CISCO-CAPWAP-CONTROLLER.localdomain*

5. If no controller is found, the LAP will reboot and go through the discovery process again



- **At the end of the discovery, the LAP will have a list of available WLCs on the network**

Access Point Operation

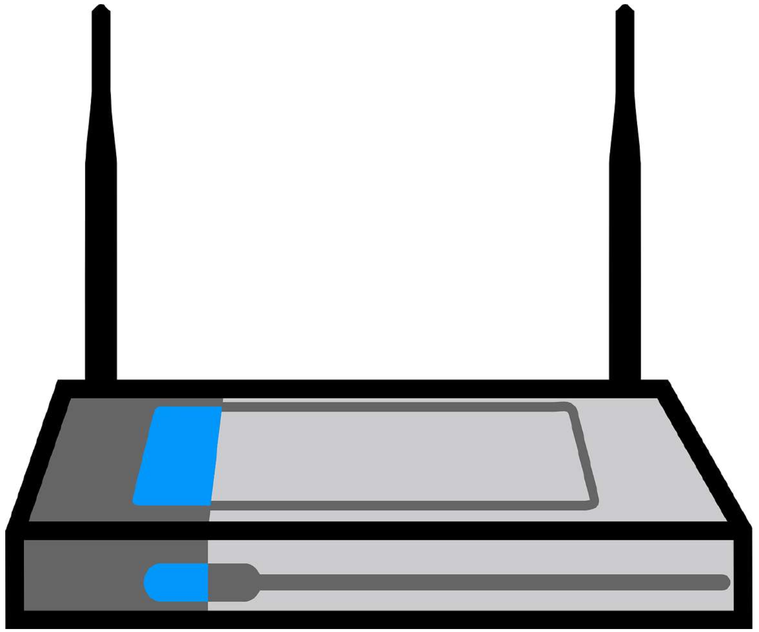
WLC Selection Process:

1. Join a previously known controller
2. Join a master controller
3. Join the least-loaded controller

Layer 2 and Layer 3 Roaming

Roaming:

- When a wireless client changes its access point association



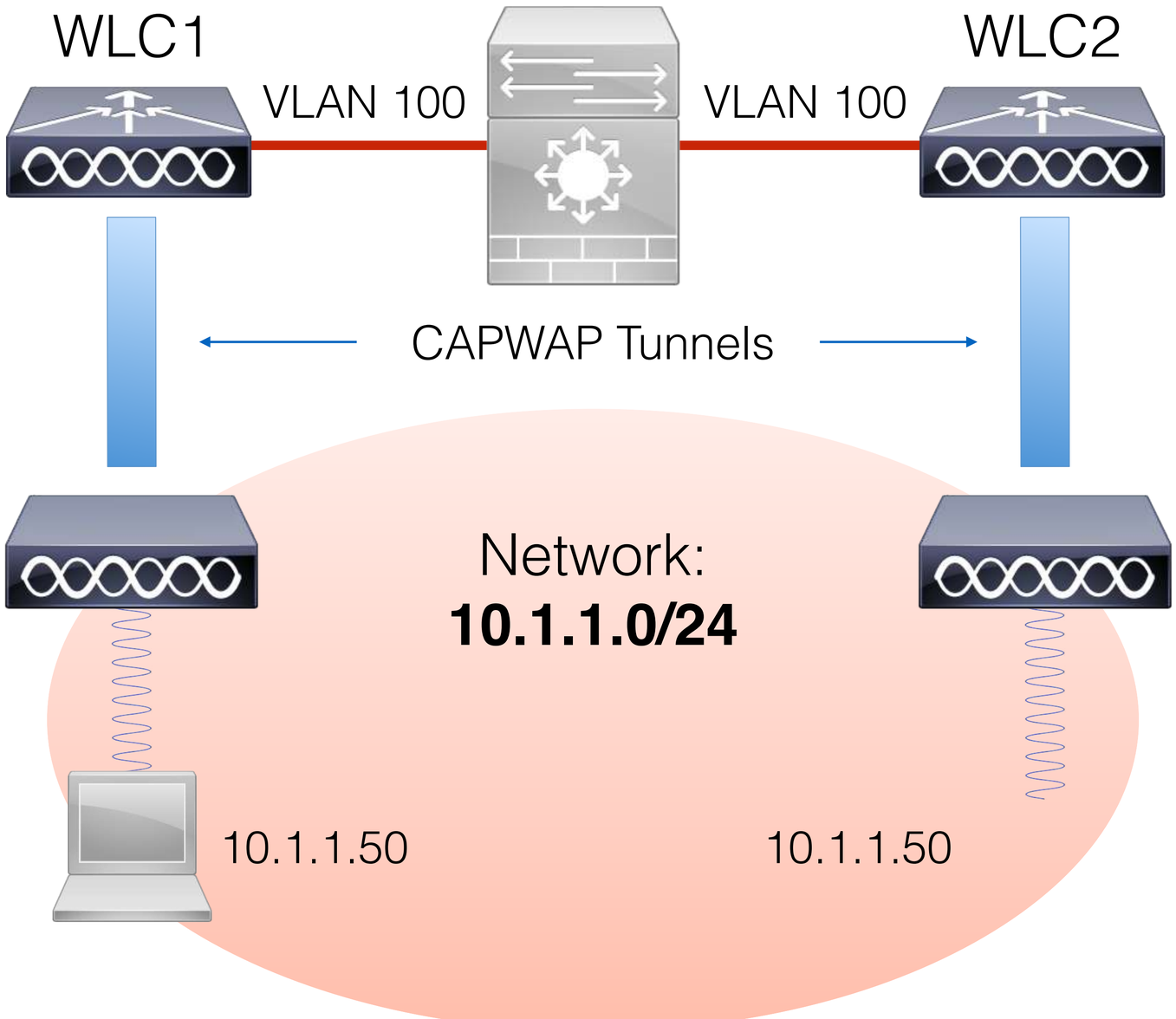
Intracontroller Roaming:

- Roaming between access points which are connected to the same wireless LAN controller

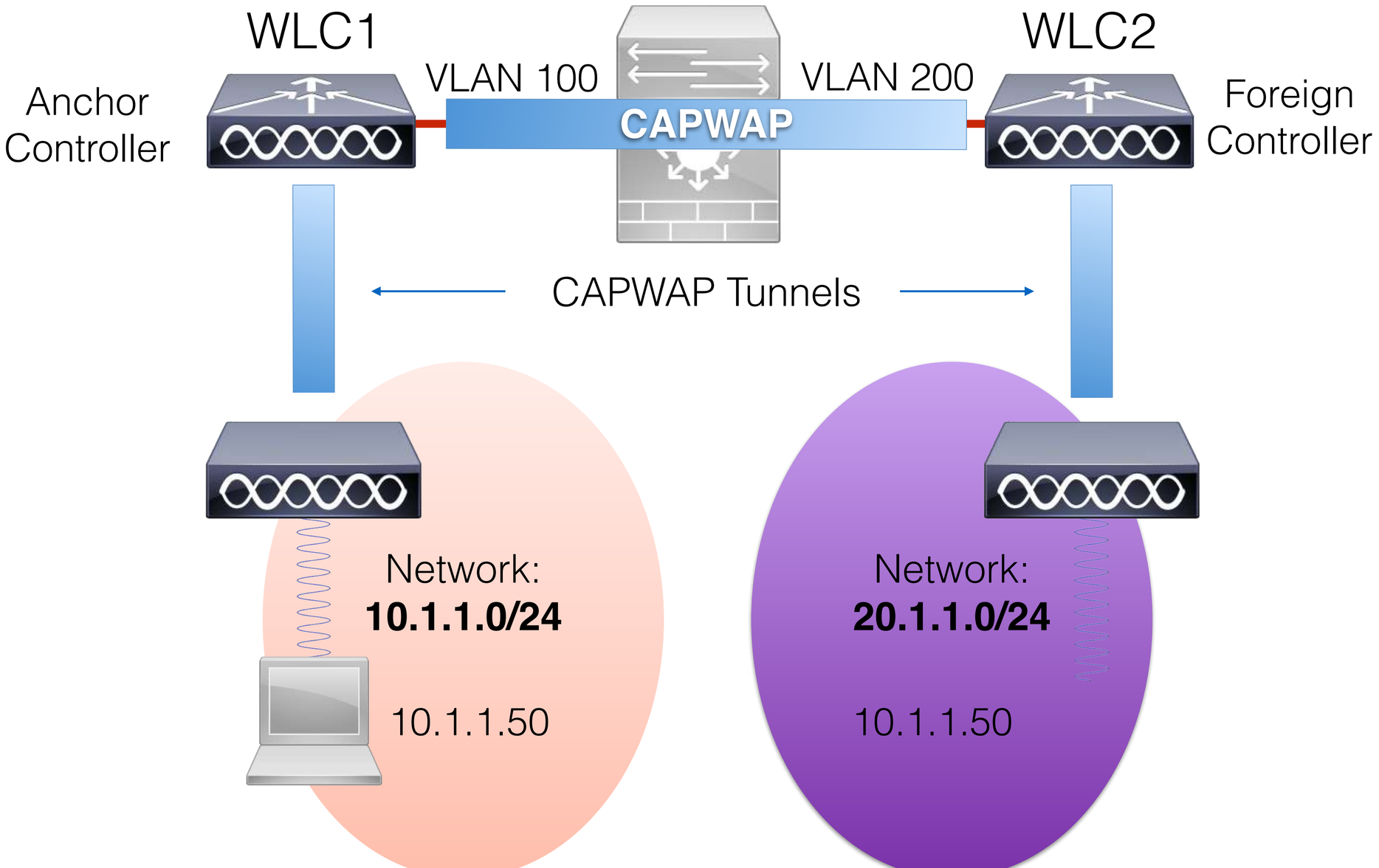
Intercontroller Roaming:

- Roaming between access points which are connected to the different wireless LAN controllers

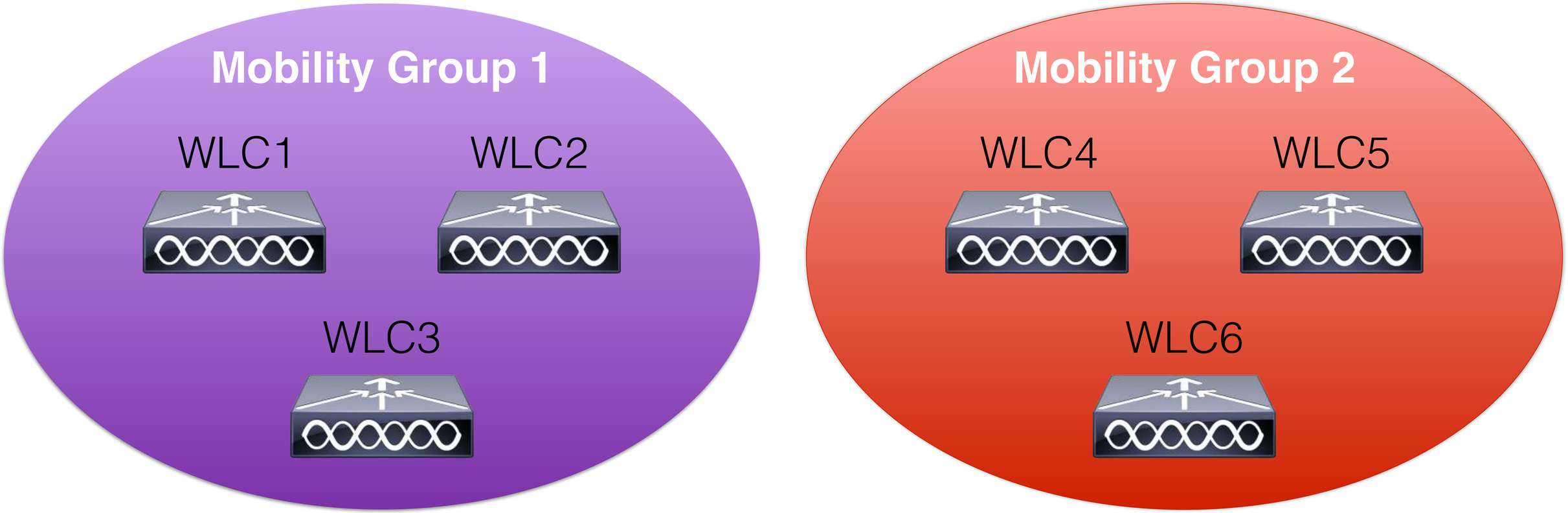
Layer 2 and Layer 3 Roaming



Layer 2 and Layer 3 Roaming



Layer 2 and Layer 3 Roaming



WLAN Troubleshooting

WLAN Troubleshooting

Successful Client WLAN Association:

- Client must be within the access point RF range
- Client must properly authenticate to the WLAN
- Client should receive a valid IP address on the subnet

WLAN Troubleshooting

START	Wireless association is just beginning
AUTHCHECK	Client must pass Layer 2 authentication
8021X_REQD	Client must pass 802.1x authentication
L2AUTHCOMPLETE	Layer 2 authentication is successful, Layer 3 policies can begin
WEP_REQD	Client must pass WEP authentication
DHCP_REQD	Client obtains an IP address and the controller records the address
WEBAUTH_REQD	Client must pass web authentication
RUN	Layer 2 and Layer 3 policies successful, client is operational

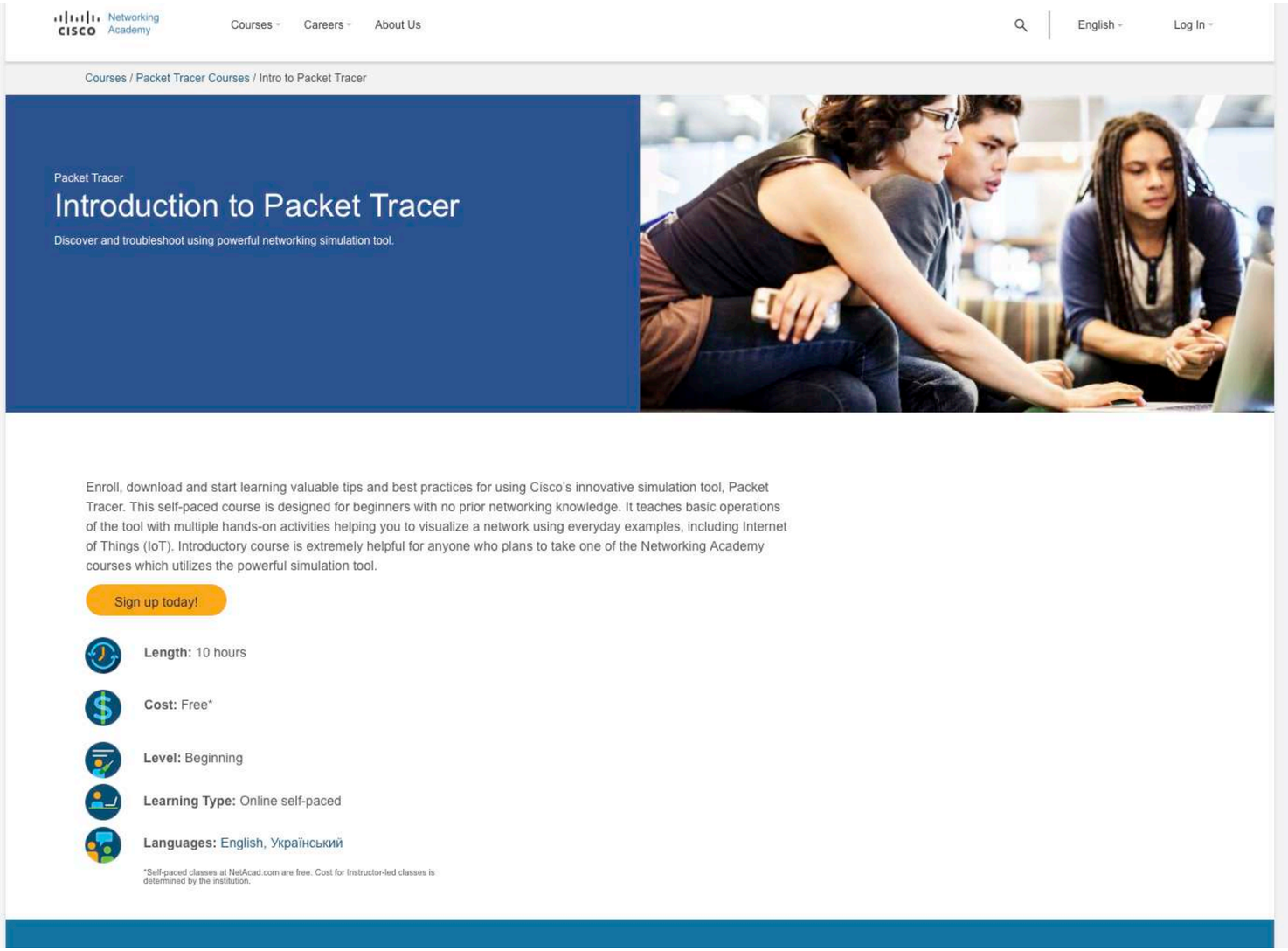
Getting Your Hands Dirty with a Cisco WLC – Option 1

Get Cisco Packet Tracer for Free

https://kwtrain.com/pt

Download Kevin's WLC Topology

https://bit.ly/ptconfig



Getting Your Hands Dirty with a Cisco WLC – Option 2

Purchase Used

Cisco Airspace AIR-WLC4136-K9 Wirelesss LAN Controller
Pre-Owned

$99.99
or Best Offer
+$15.29 shipping
♡ Watch
See more like this

Cisco 4400 Series Wireless Lan Controller AIR-WLC4402-25-K9 4402
Pre-Owned

$49.00
Buy It Now
+$24.00 shipping
♡ Watch

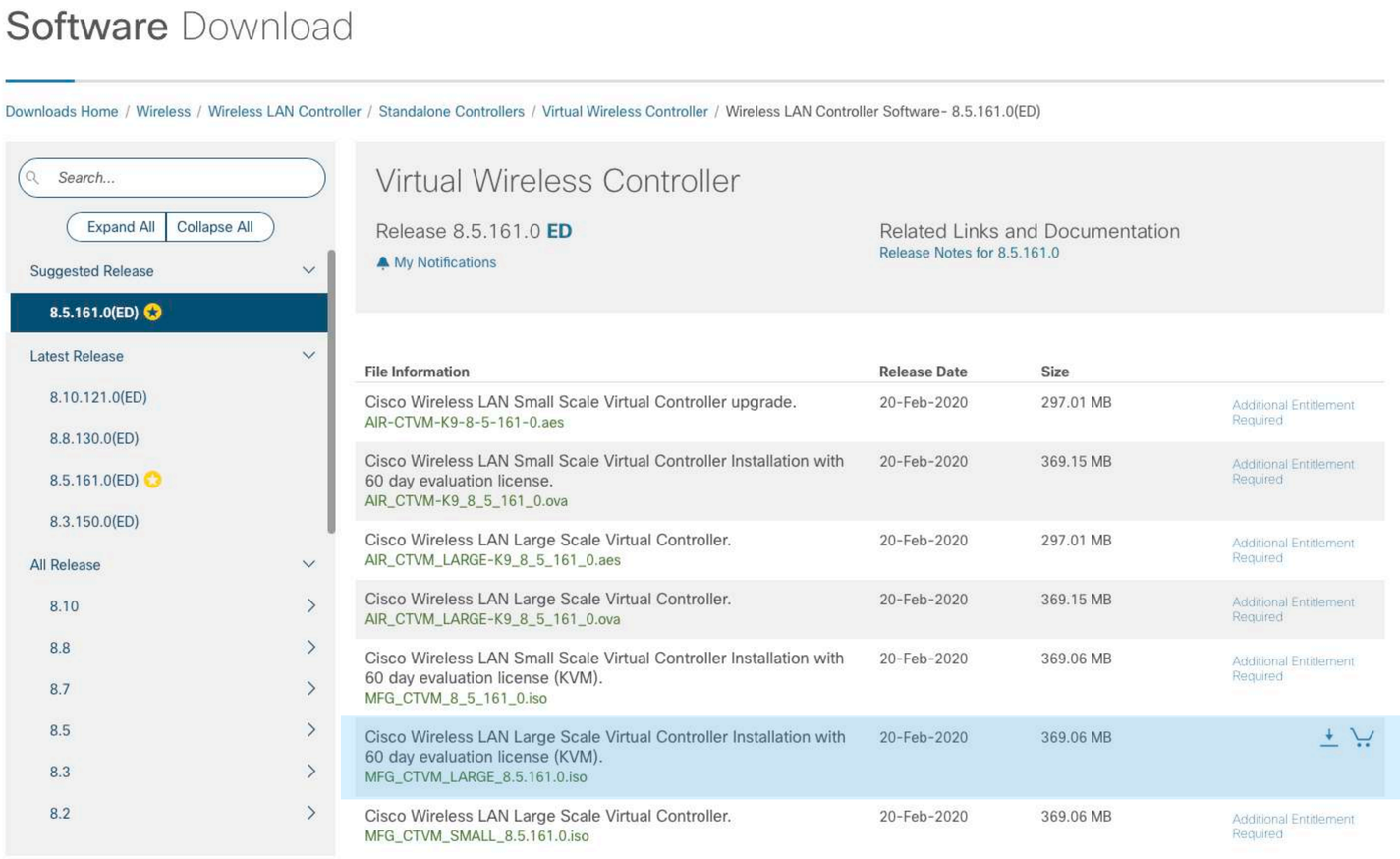
Pre-owned Cisco 520 Series Wireless LAN Controller AIR-WLC526-K9
Pre-Owned

$50.00
or Best Offer
+$30.00 shipping
4 watchers
♡ Watch
See more like this

SPONSORED
Cisco 4400 Series AIR-WLC4402-50-K9 V03 Wireless LAN Controller w/ Rack Ears
Pre-Owned

$26.79
Top Rated Plus
or Best Offer
+$49.99 shipping
Free Returns
♡ Watch

Getting Your Hands Dirty with a Cisco WLC – Option 3



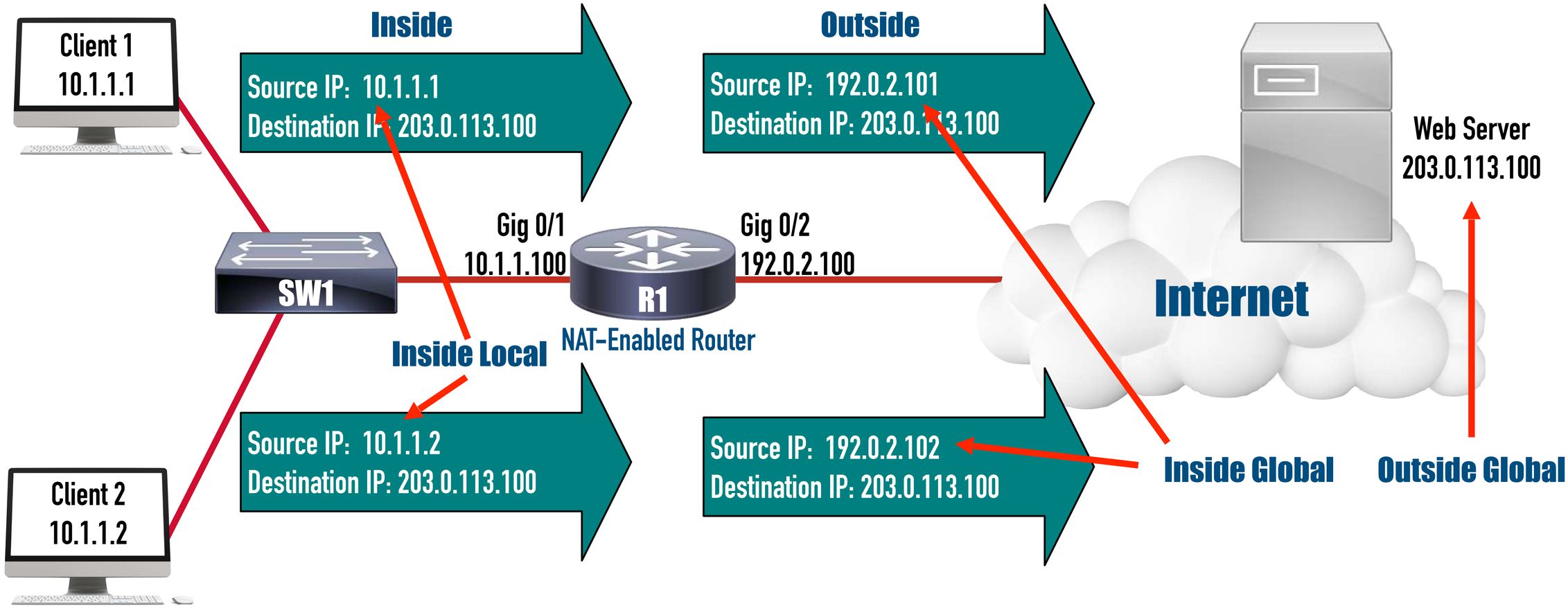
Install Trial Version of Cisco WLC Virtual on VMware ESXi

https://bit.ly/wlcdownload

- Linux Cent 4/5 or Layer (64-bit)
- 2 CPUs
- 8 GB Mem
- 8 GB HD

Network Services

Network Address Translation (NAT) Theory

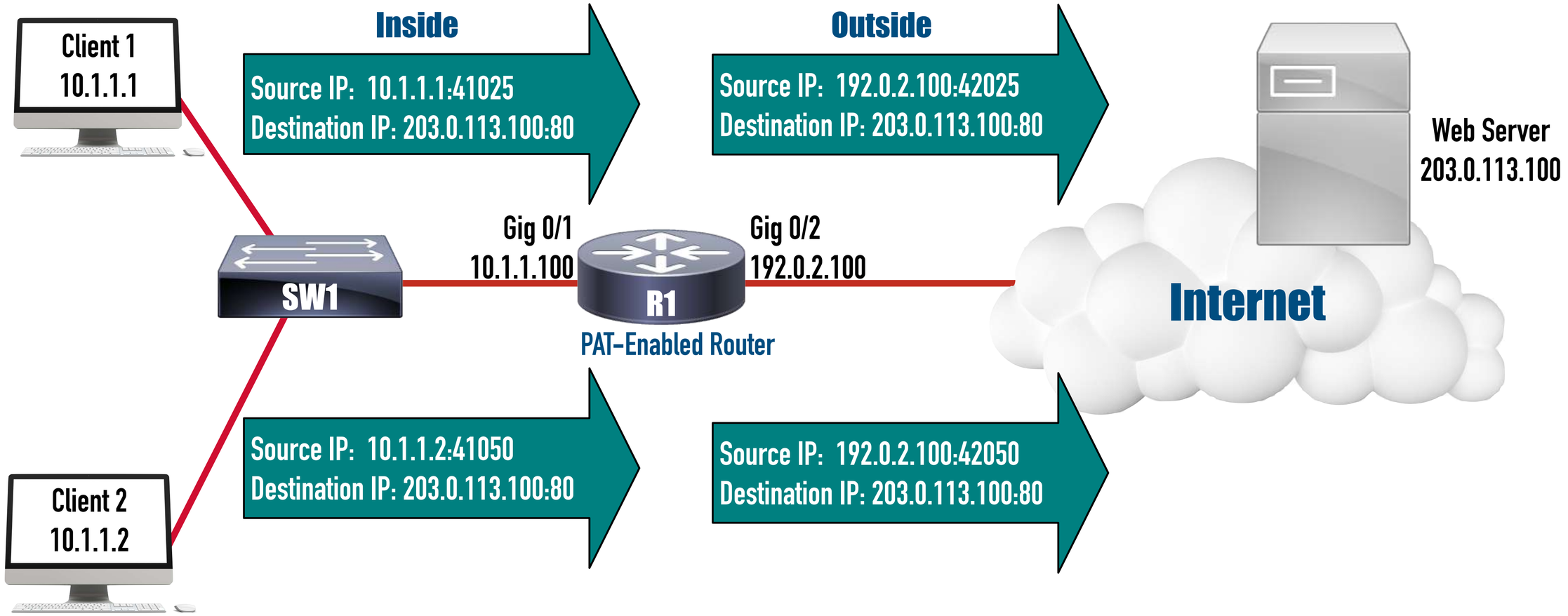


Pool of Addresses:
192.0.2.101 – 192.0.2.199

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

Port Address Translation (PAT) Theory

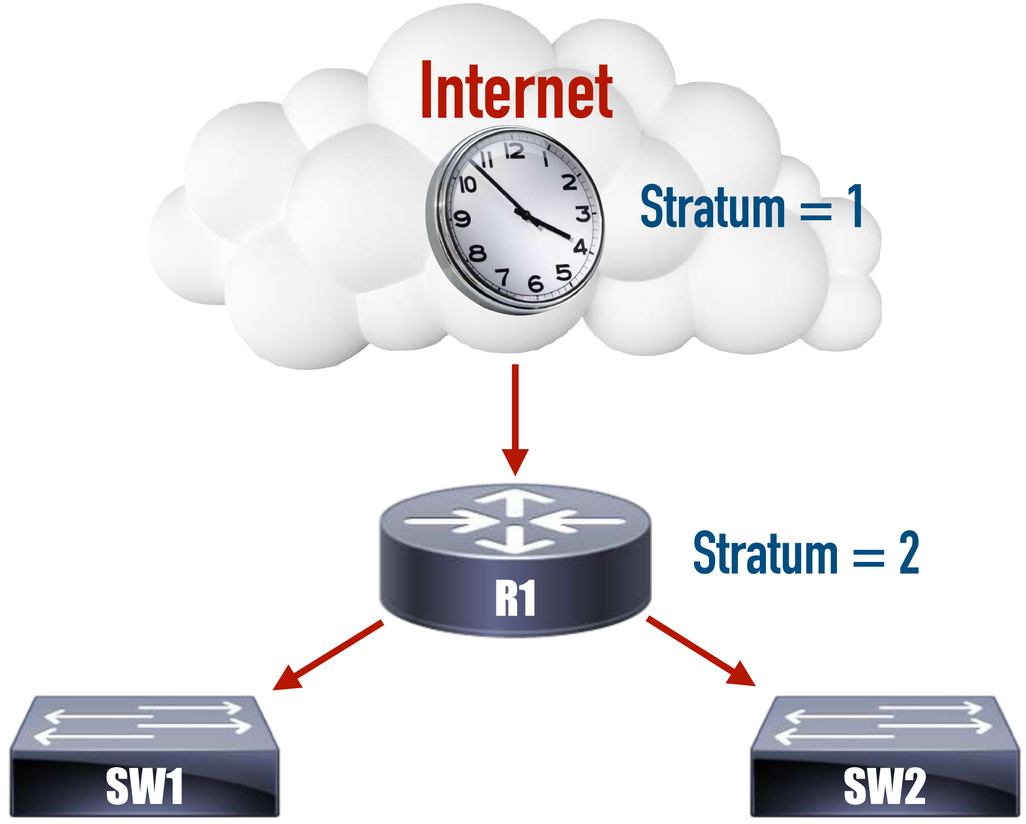


Router R1's NAT Translation Table

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

NAT and PAT Demo

Network Time Protocol (NTP) Theory

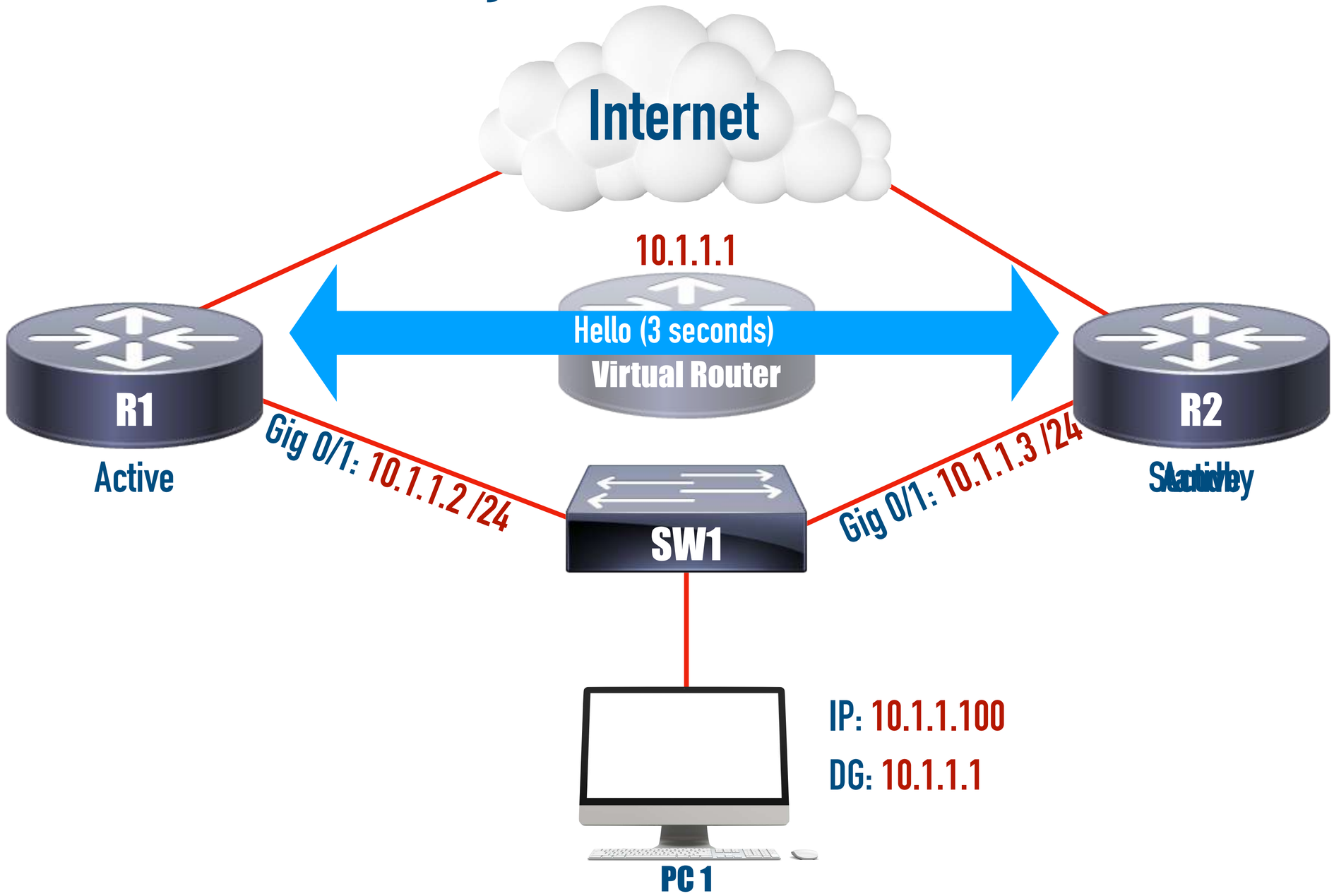


- Uses UDP Port 123
- Uses a stratum number to measure the believability of a time source

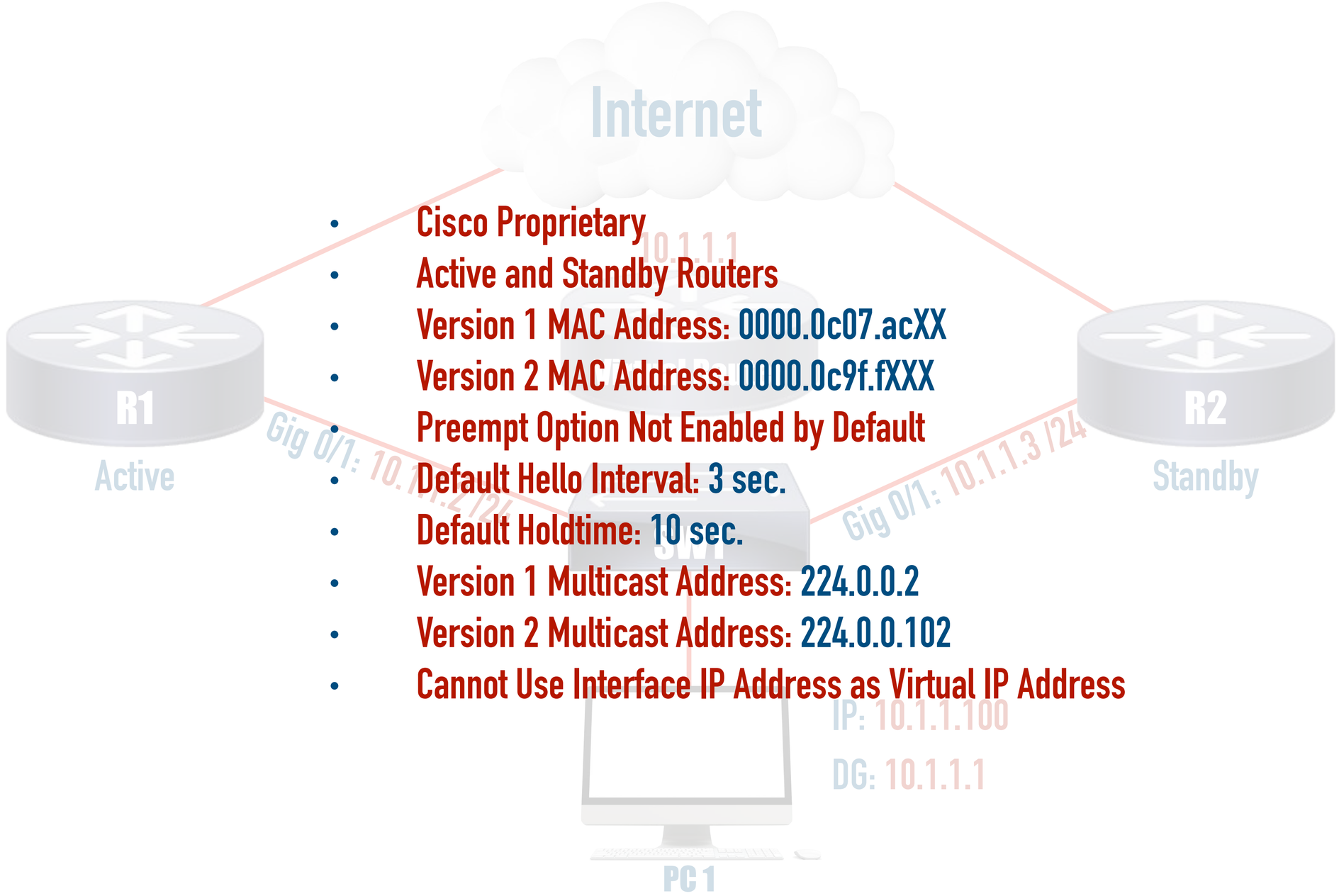
NTP Demo

HSRP and VRRP

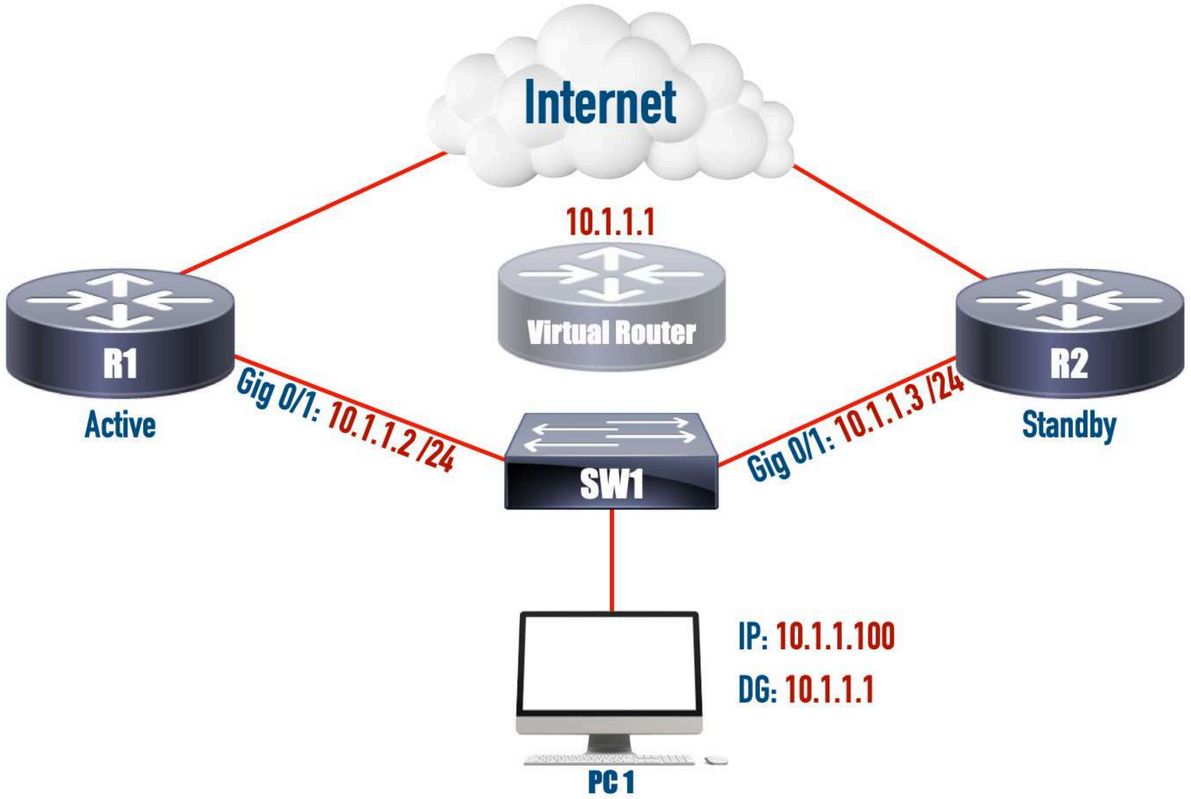
Hot Standby Router Protocol (HSRP)



Hot Standby Router Protocol (HSRP)



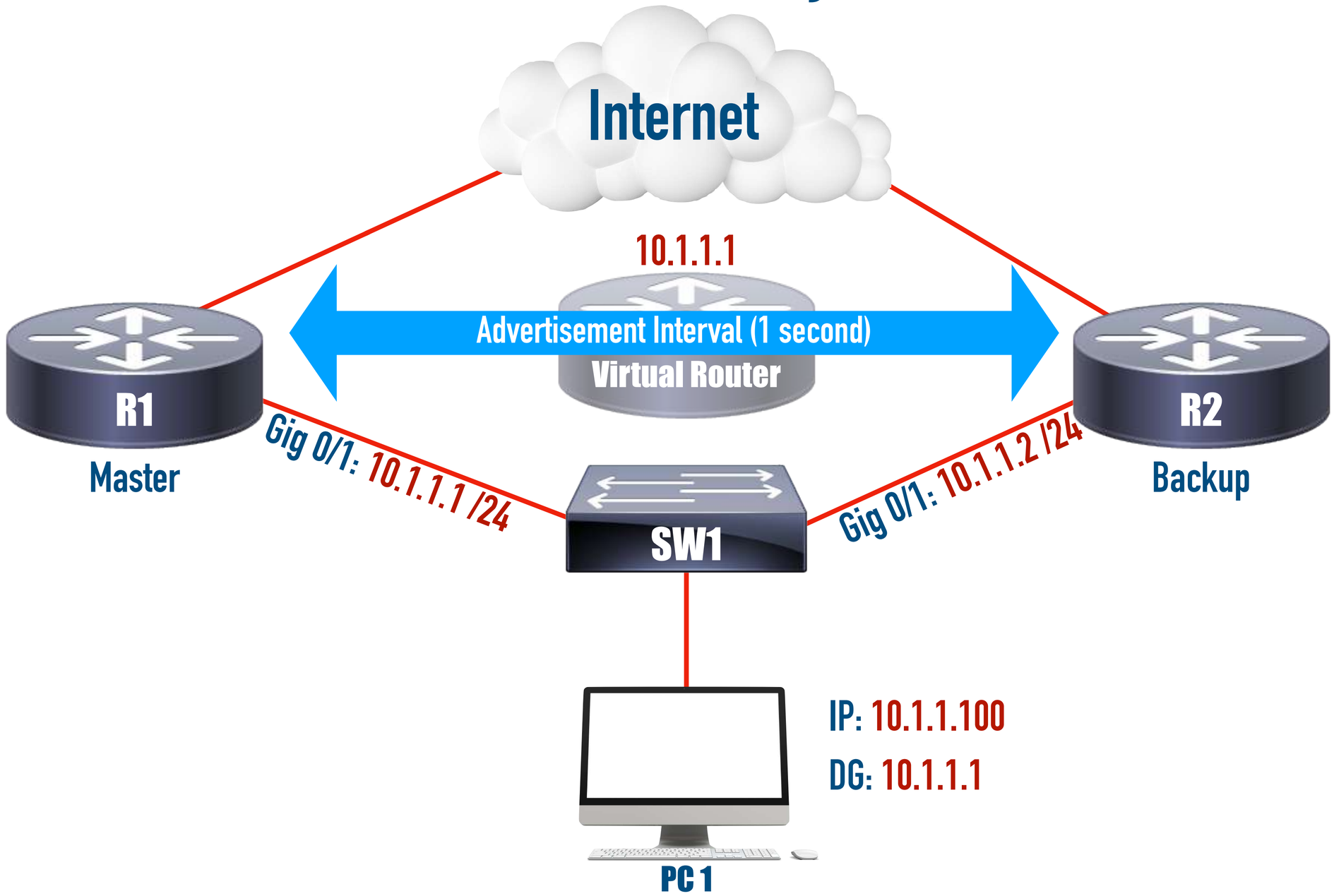
- Cisco Proprietary
- Active and Standby Routers
- Version 1 MAC Address: 0000.0c07.acXX
- Version 2 MAC Address: 0000.0c9f.fXXX
- Preempt Option Not Enabled by Default
- Default Hello Interval: 3 sec.
- Default Holdtime: 10 sec.
- Version 1 Multicast Address: 224.0.0.2
- Version 2 Multicast Address: 224.0.0.102
- Cannot Use Interface IP Address as Virtual IP Address



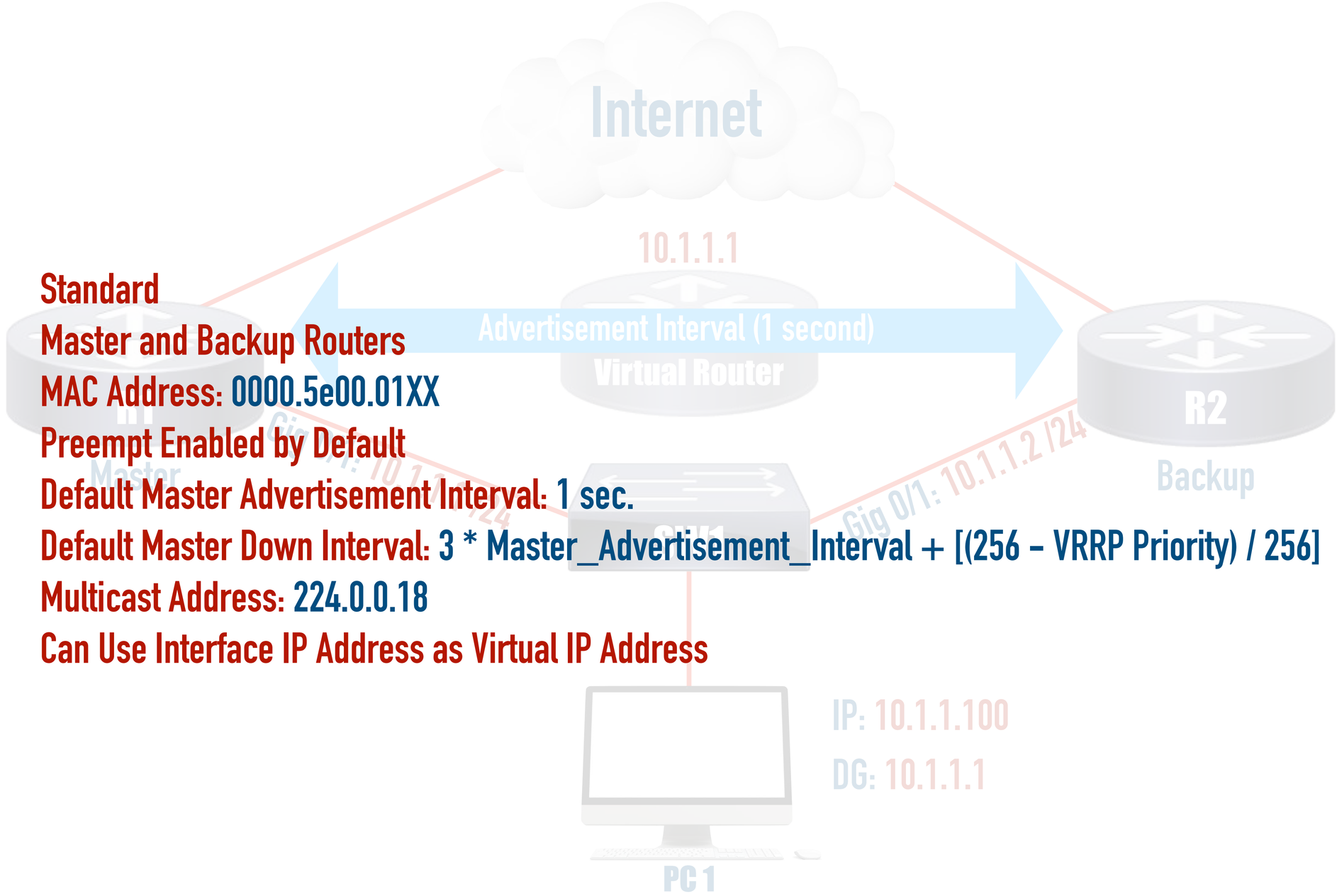
HSRP States

Active	Device is actively servicing the virtual IP address and is forwarding packets.
Standby	Device is ready to forward traffic if the Active router fails.
Speak	Device is sending and receiving Hello messages.
Listen	Device is receiving Hello messages.
Learn	Device has not received a Hello message and does not yet know the virtual IP address.
Init or Disabled	Device is not yet participating in HSRP.

Virtual Router Redundancy Protocol (VRRP)



Virtual Router Redundancy Protocol (VRRP)



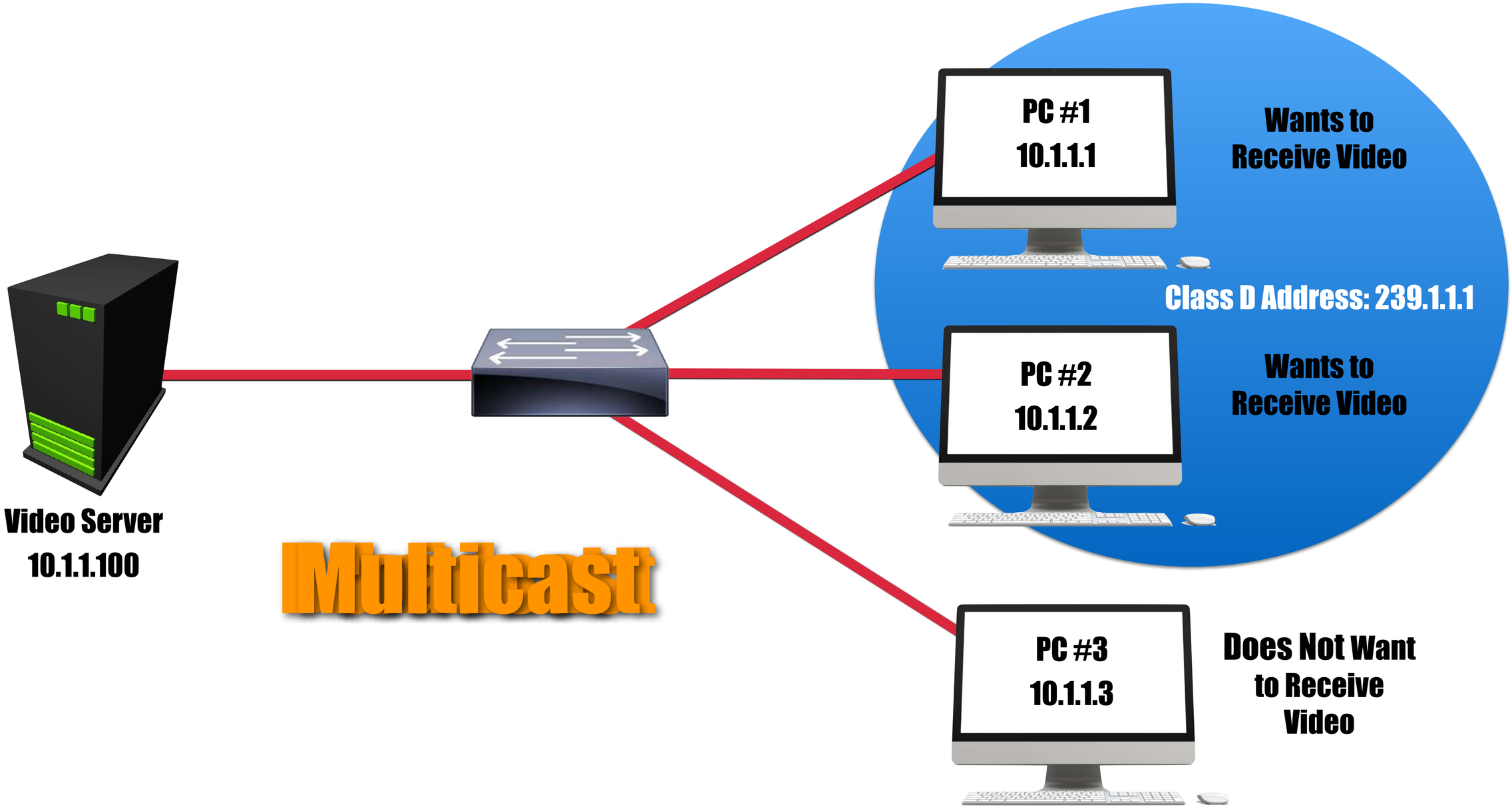
- Standard
- Master and Backup Routers
- MAC Address: 0000.5e00.01XX
- Preempt Enabled by Default
- Default Master Advertisement Interval: 1 sec.
- Default Master Down Interval: 3 * Master_Advertisement_Interval + [(256 – VRRP Priority) / 256]
- Multicast Address: 224.0.0.18
- Can Use Interface IP Address as Virtual IP Address

HSRP and VRRP Demo

NTP Security Demo

Multicast

The Benefit of Multicast



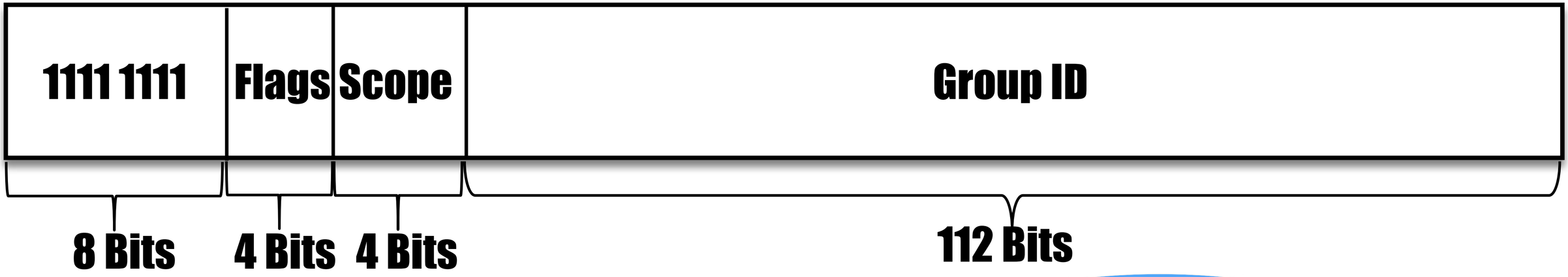
IPv4 Multicast Addressing

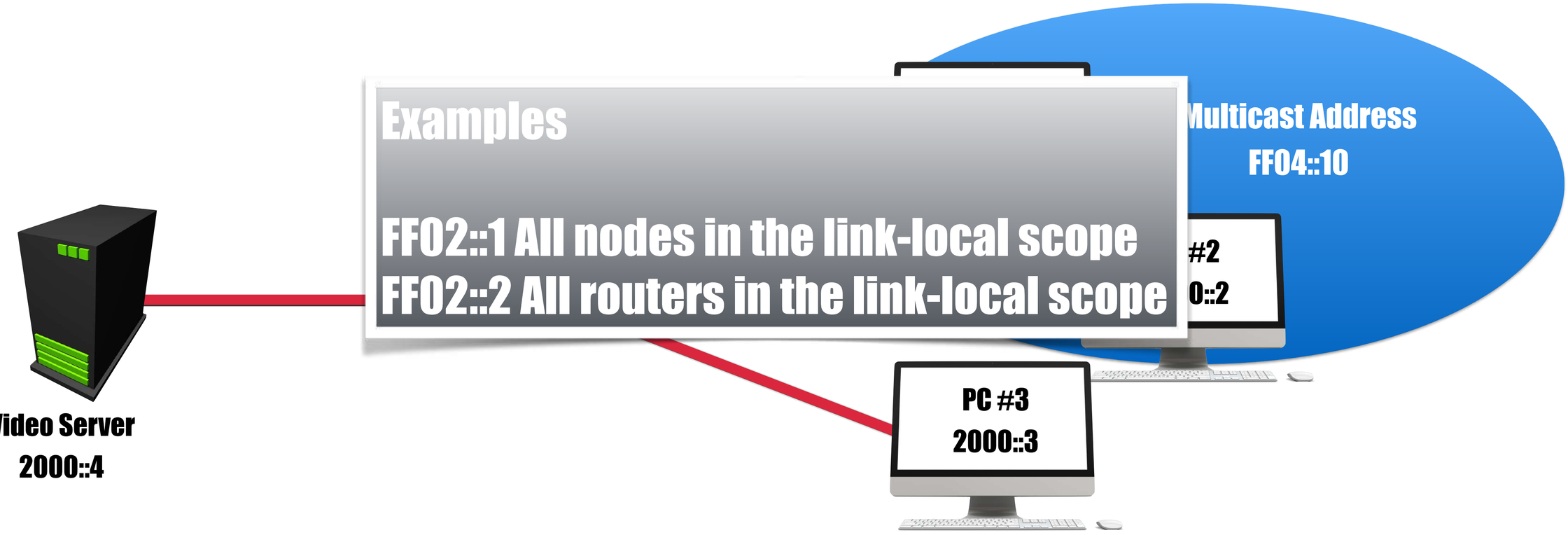
Class D Address Range
224.0.0.0 - 239.255.255.255

Reserved Address Range	Purpose of Reserved Range
224.0.0.0 - 224.0.0.255	Reserved Link Local Addresses
224.0.1.0 - 238.255.255.255	Globally Scoped Addresses
232.0.0.0 - 232.255.255.255	Source Specific Multicast Addresses
233.0.0.0 - 233.255.255.255	GLOP Addresses
239.0.0.0 - 239.255.255.255	Limited Scope Addresses

IPv6 Multicast Addressing

- Addressing has an FF as the first two hexadecimal digits





Constructing a Multicast MAC Address

Given an IPv4 multicast address of 224.1.10.10, calculate the corresponding MAC address.

Step #1: Convert the last three octets to binary.

0000.0001.0000.1010.0000.1010

Step #2: Change the leftmost bit to **0**, if it's not already 0.

0000.0001.0000.1010.0000.1010

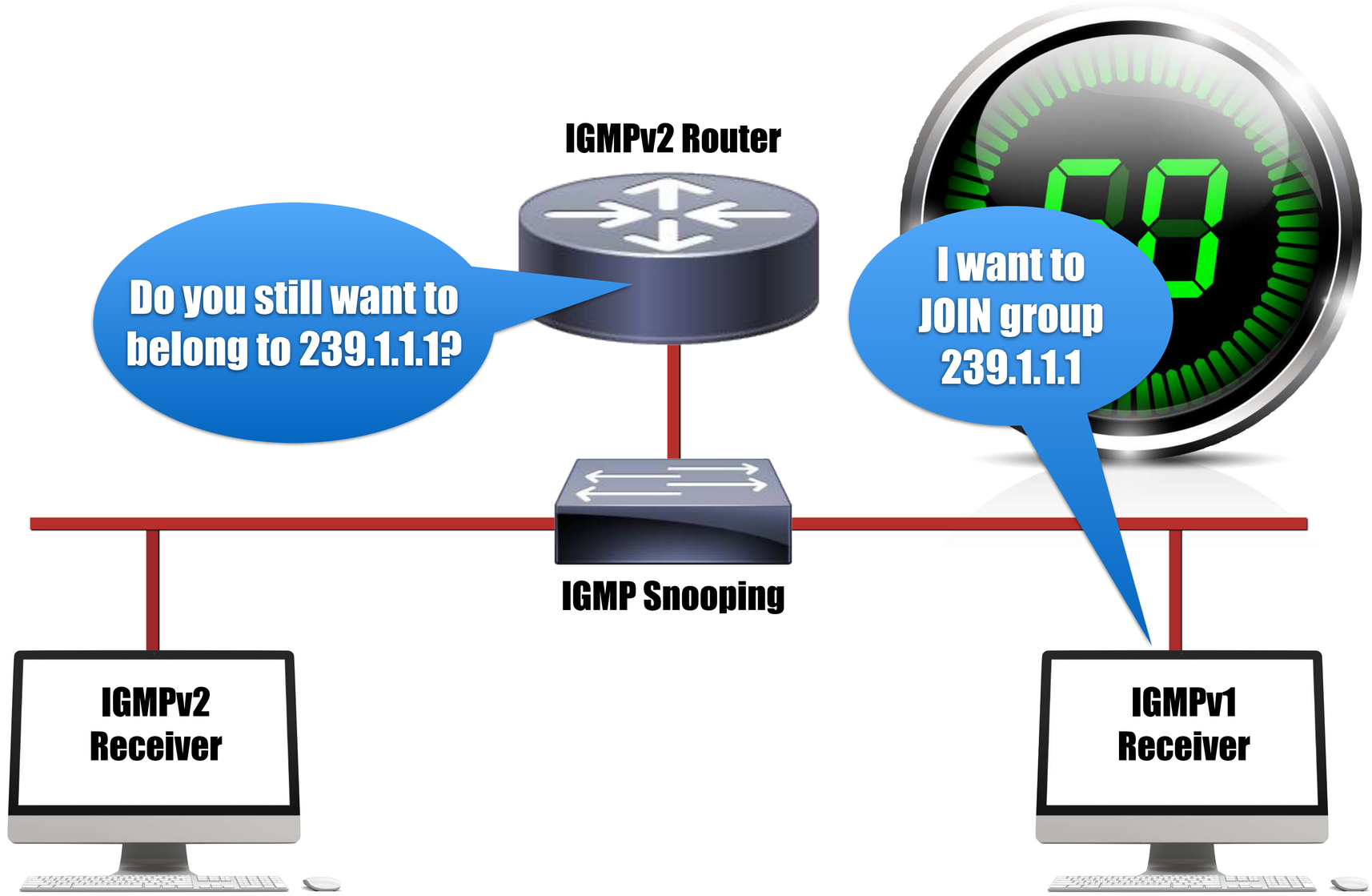
Step #3: Convert each nibble into hex.

01-0a-0a

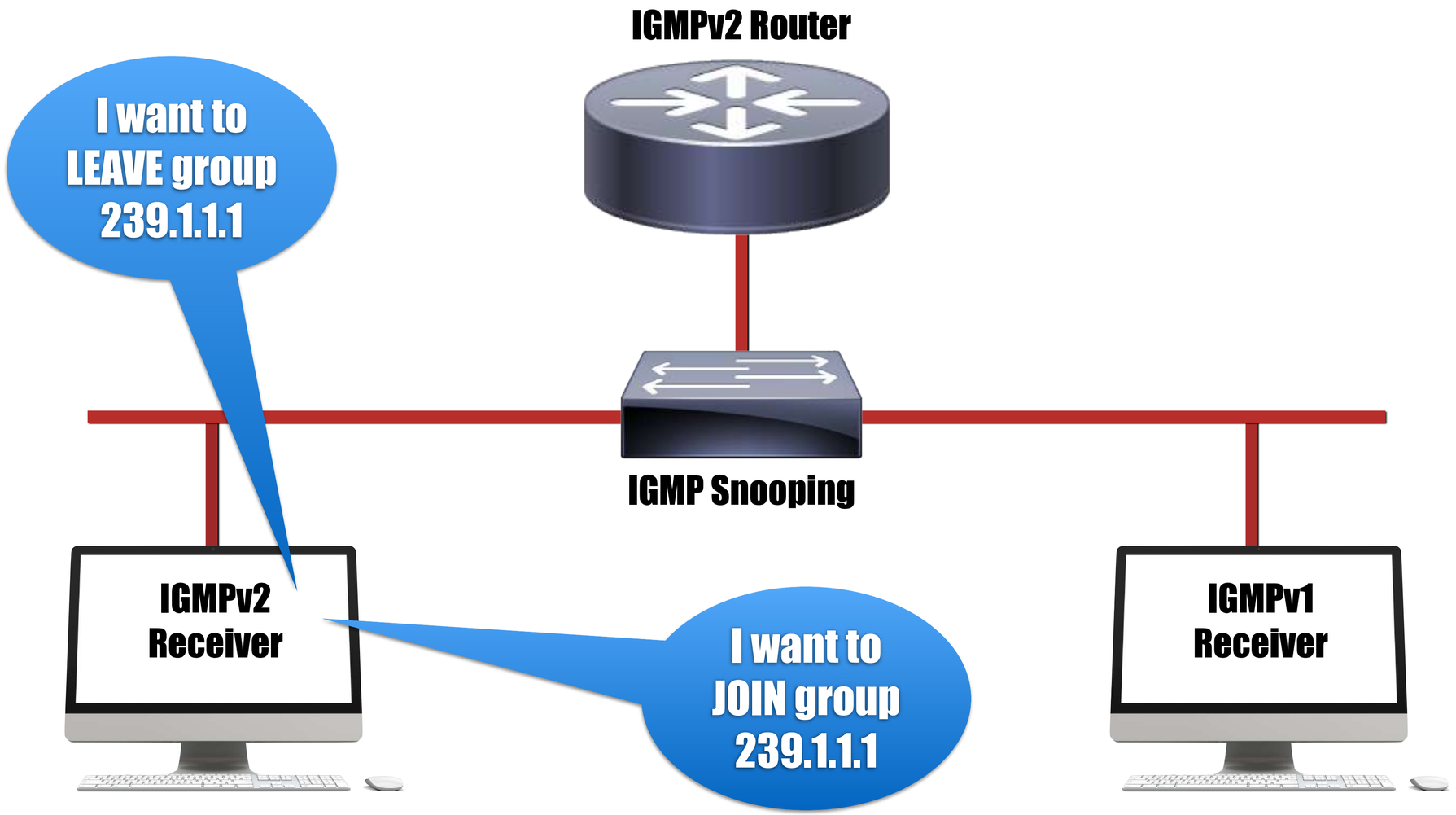
Step #4: Prepend **01-00-5e**.

01-00-5e-01-0a-0a

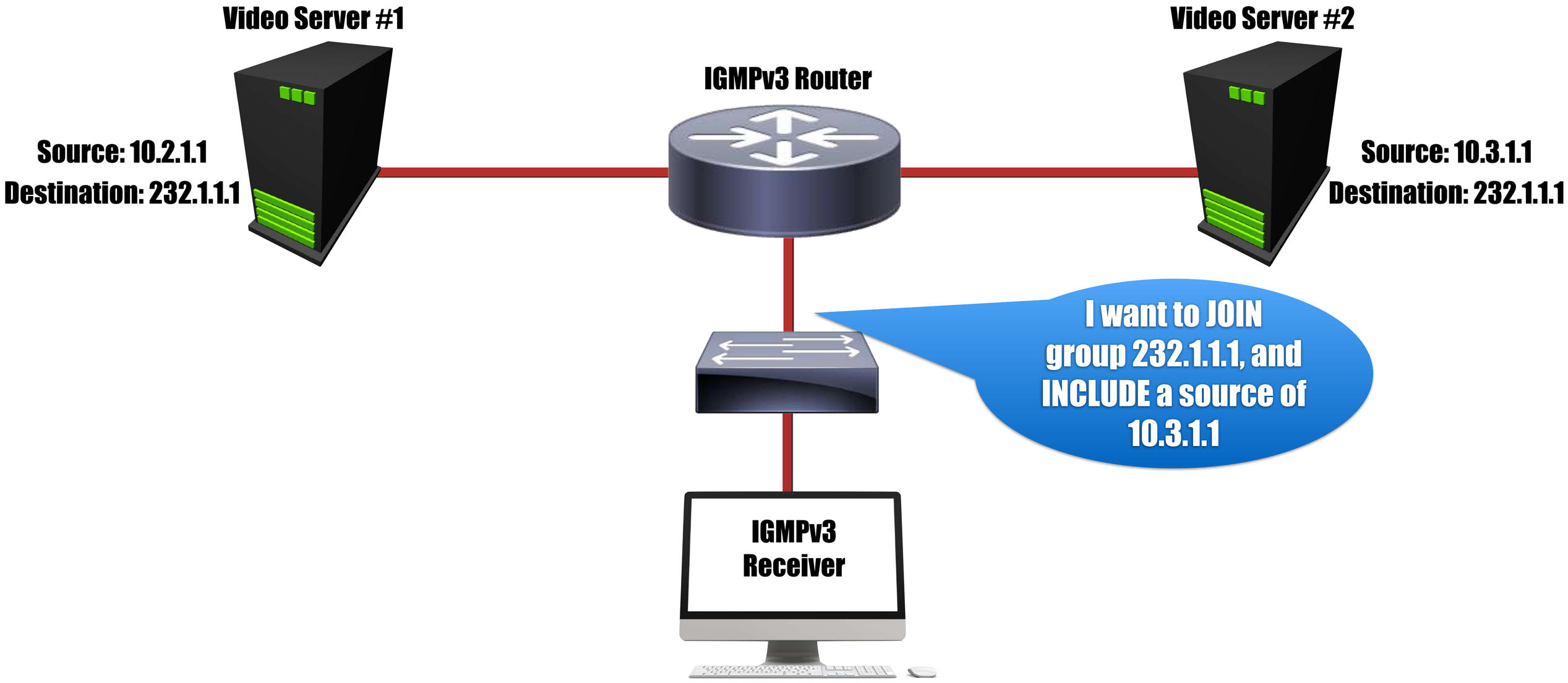
Internet Group Management Protocol (IGMP)



Internet Group Management Protocol (IGMP)



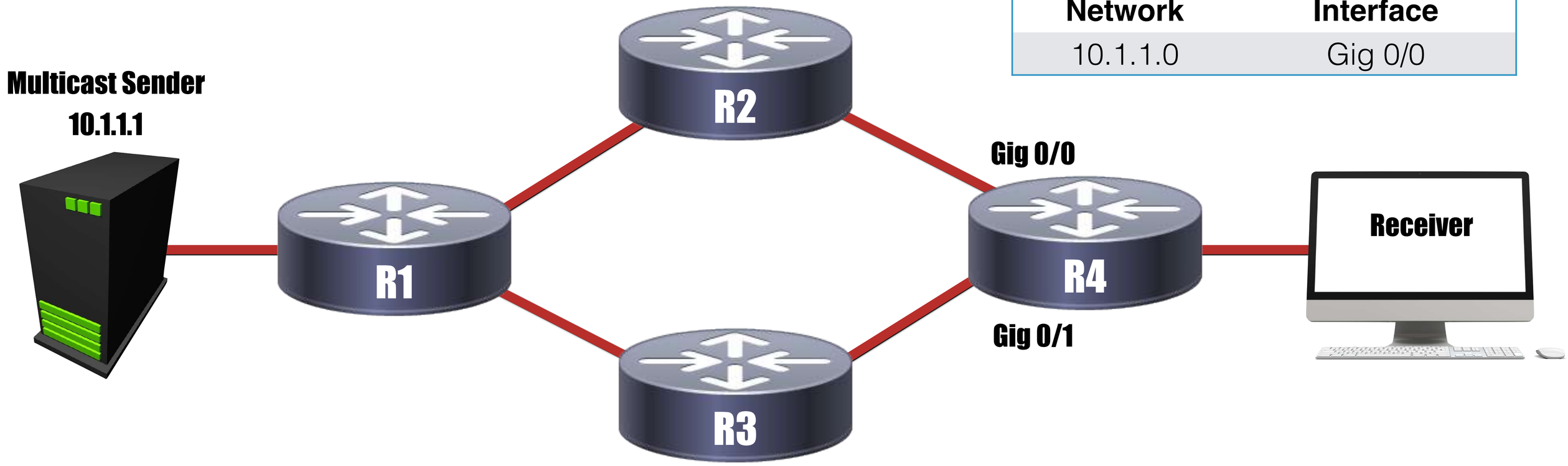
Internet Group Management Protocol (IGMP) version 3



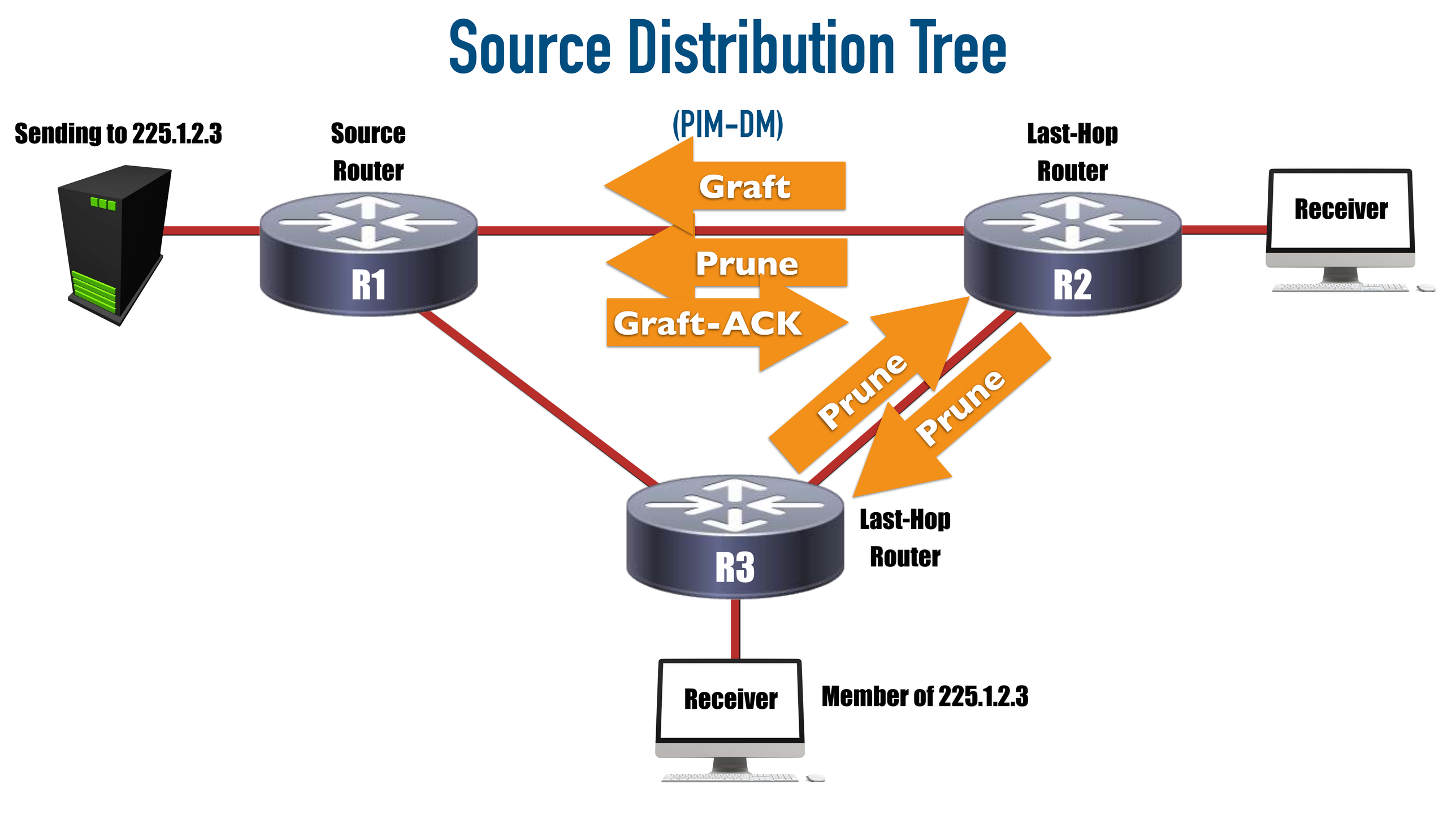
Reverse Path Forwarding (RPF) Check

Entry from Router R4's Routing Table

Network	Interface
10.1.1.0	Gig 0/0



Source Distribution Tree



Shared Distribution Tree

(PIM-SM)