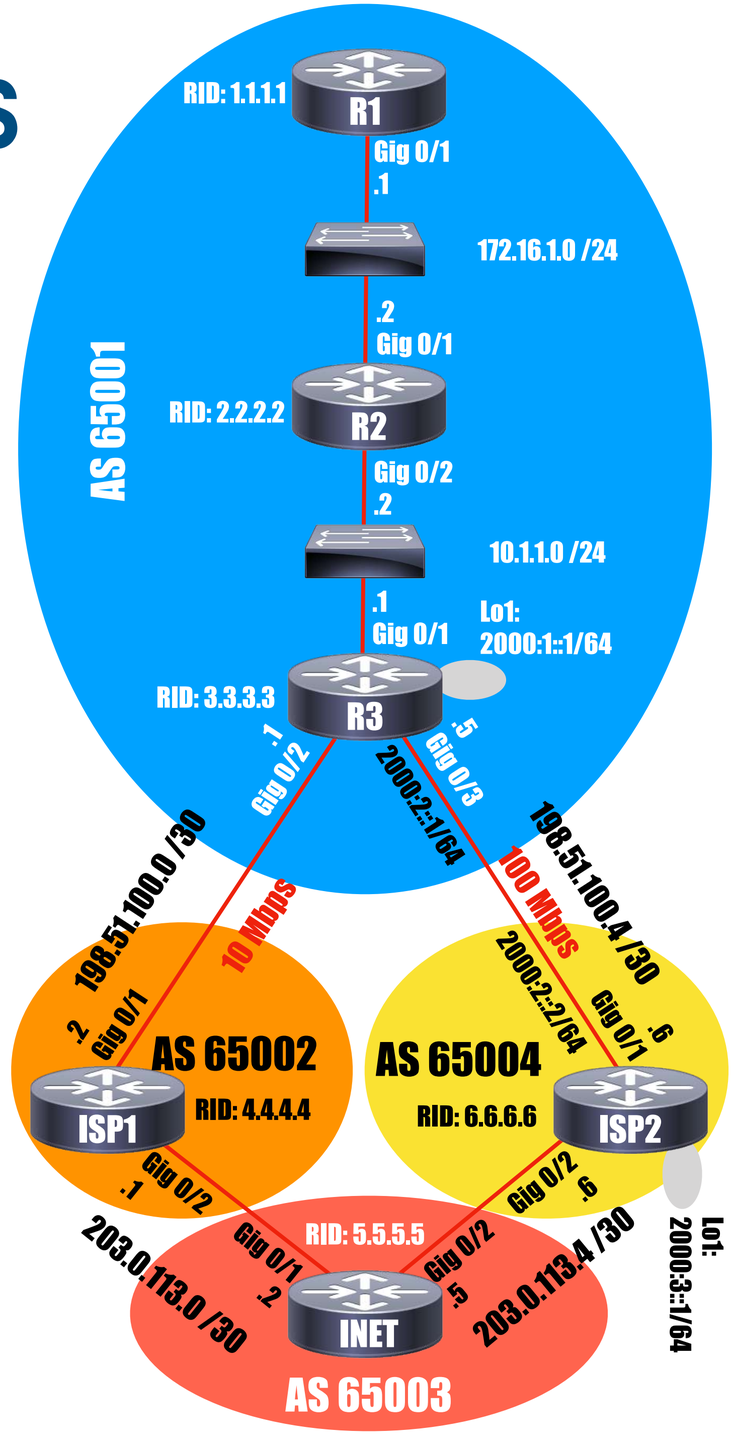
Module 1

Enterprise Architecture

ENCOR (350-401) Topics

- Enterprise Architecture
- Virtualization Technologies
- Infrastructure Technologies
- Network Management
- Network Security
- Network Automation
- Exam Preparation



Your Instructor

- Kevin Wallace
- CCIEx2 Emeritus #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
- 2x Cisco Live Distinguished Speaker

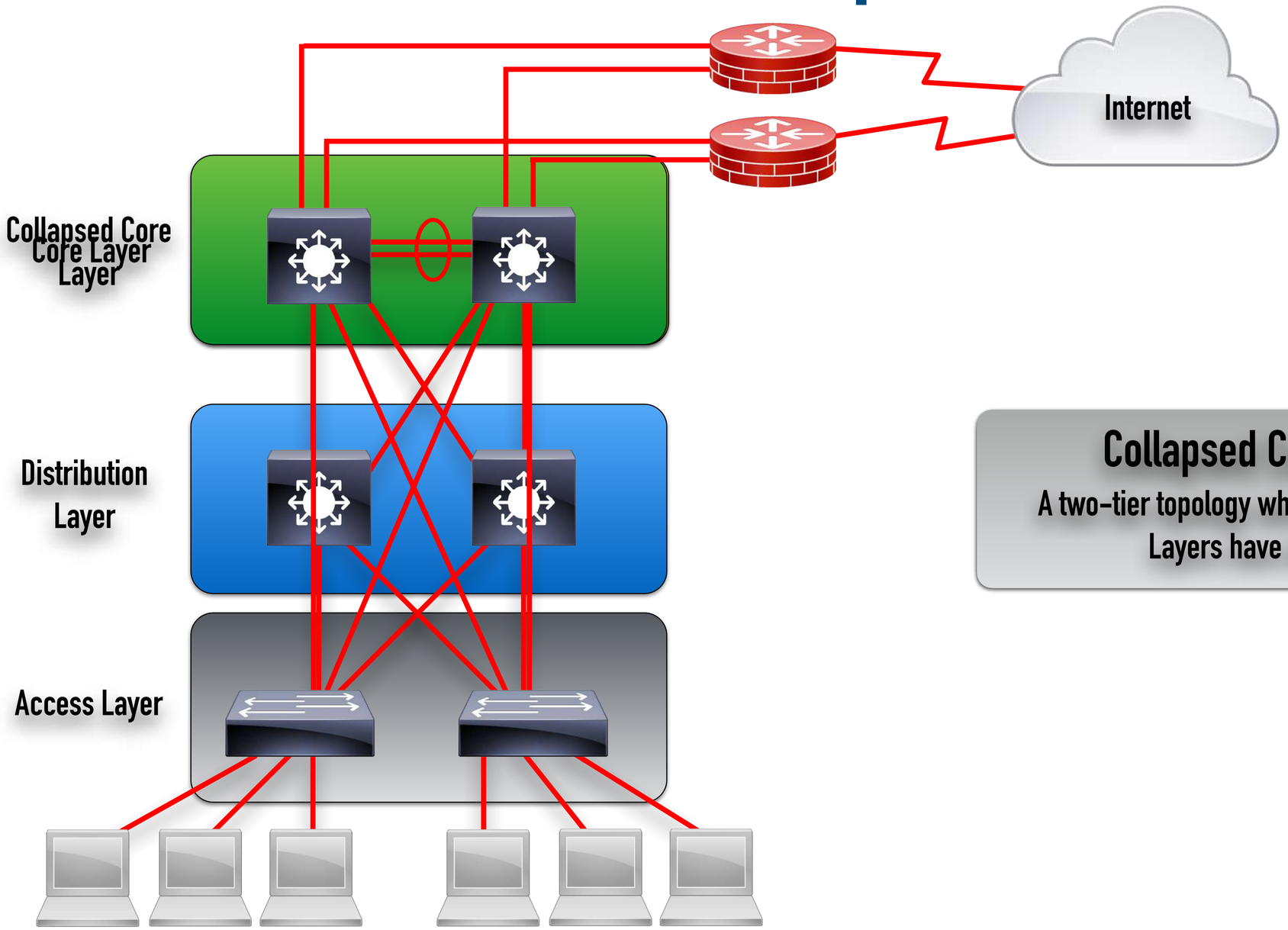
CISCO CERTIFIED CCIE ROUTING AND SWITCHING

CISCO CERTIFIED CCIE COLLABORATION

CISCO CERTIFIED CCIE 15 YEARS

Enterprise Network Design Considerations

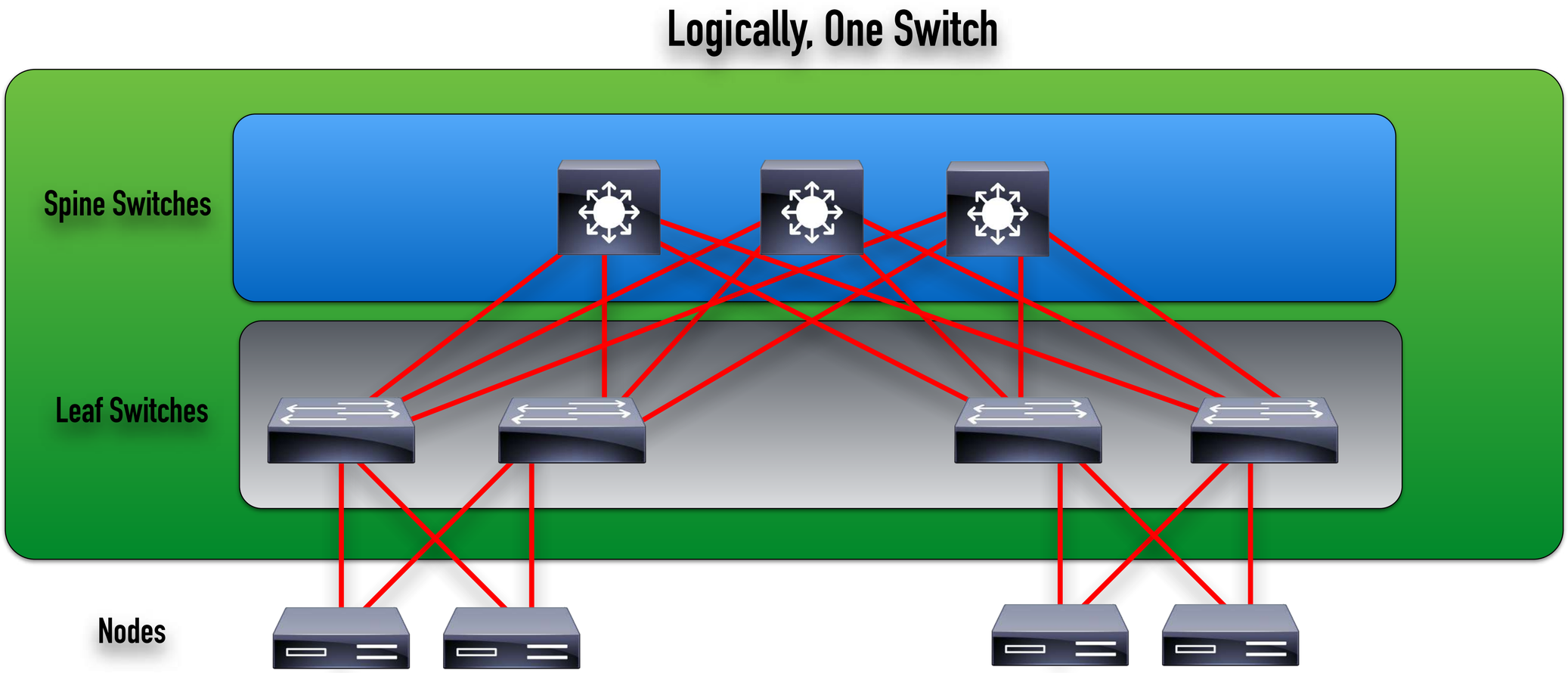
Three-Tier vs. Collapsed Core Architectures



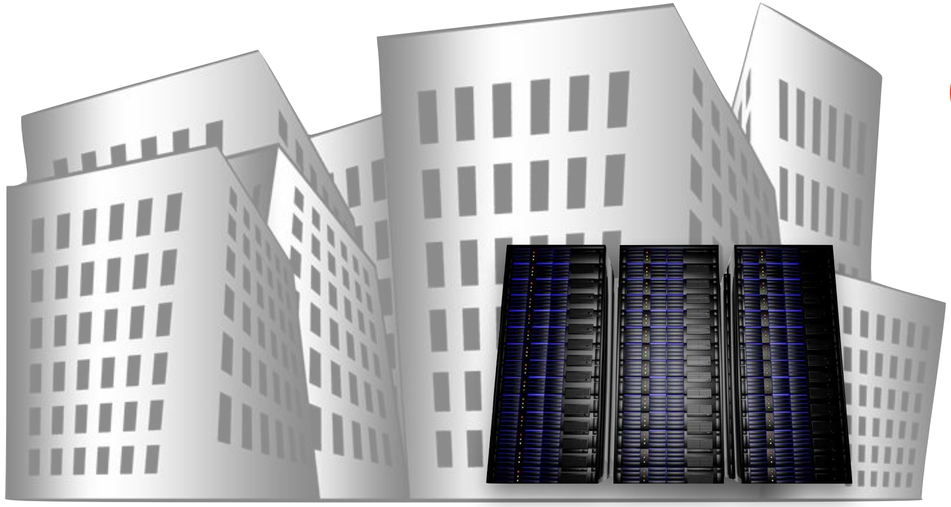
Collapsed Core Architecture

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

Spine-Leaf Design for Data Centers



On-Premise vs. Cloud Designs



Enterprise

Internet

VPN

Private WAN

MPLS

Metro Ethernet

Cloud Provider

On-Premise vs. Cloud Designs

Considerations

- With a Cloud deployment, there's no need to maintain local redundant power or hardware.
- With a Cloud deployment, you pay for resource usage instead of purchasing physical hardware.
- With an On-Premise deployment, it might be easier to meet compliance requirements.
- With an On-Premise deployment, it might be easier to maintain a good user experience.
- Many deployments, called Hybrid deployments, combine both On-Premise and Cloud deployments.

Fabric Capacity Planning

Nexus 7000 Series Switches

- How much data do we need to push through a data center switch?
- How much data can we push through a specific hardware configuration?
- What is the anticipated bandwidth demand increase over time?

Fabric Capacity Planning

Fabric Capacity Planning

Nexus 7000 Series Switches

Switch BW Capacity = (Inter-slot Switching Capacity * Number of I/O Slots) + [(Number of SE Modules * Inter-slot Switching Capacity) / 2]

Switch BW Capacity = (550 Gbps * 16) + [(2 * 550 Gbps) / 2]

Switch BW Capacity = (8800 Gbps) + 550 Gbps

Switch BW Capacity = 9350 Gbps

Full Duplex Switch BW Capacity = (9350 Gbps) * 2

Full Duplex Switch BW Capacity = 18.7 Tbps

Redundant Design

"The 5 Nines of Availability"

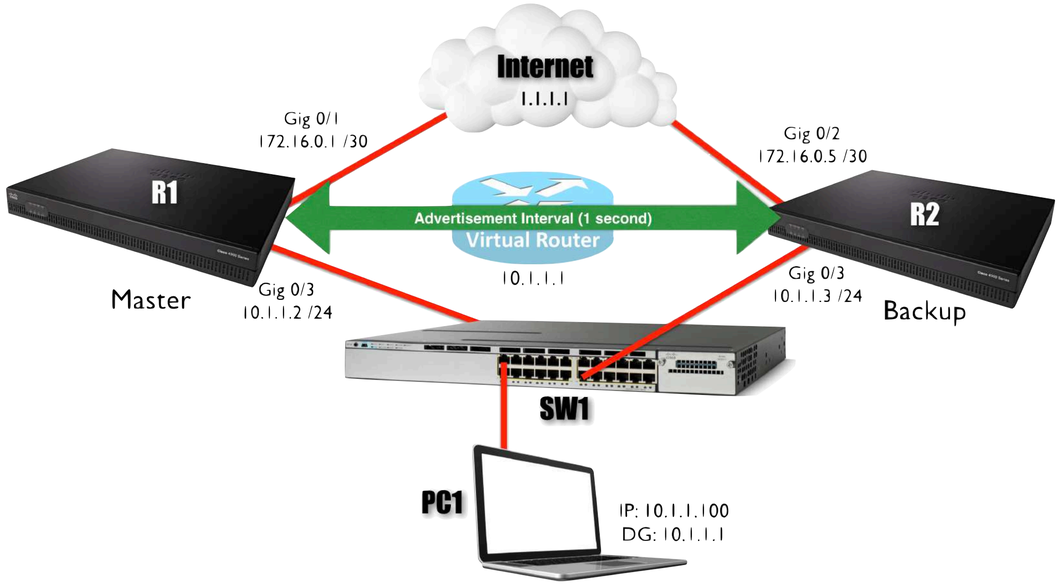
99.999 Percent Uptime

Approx. 5 Min. of Downtime/Year

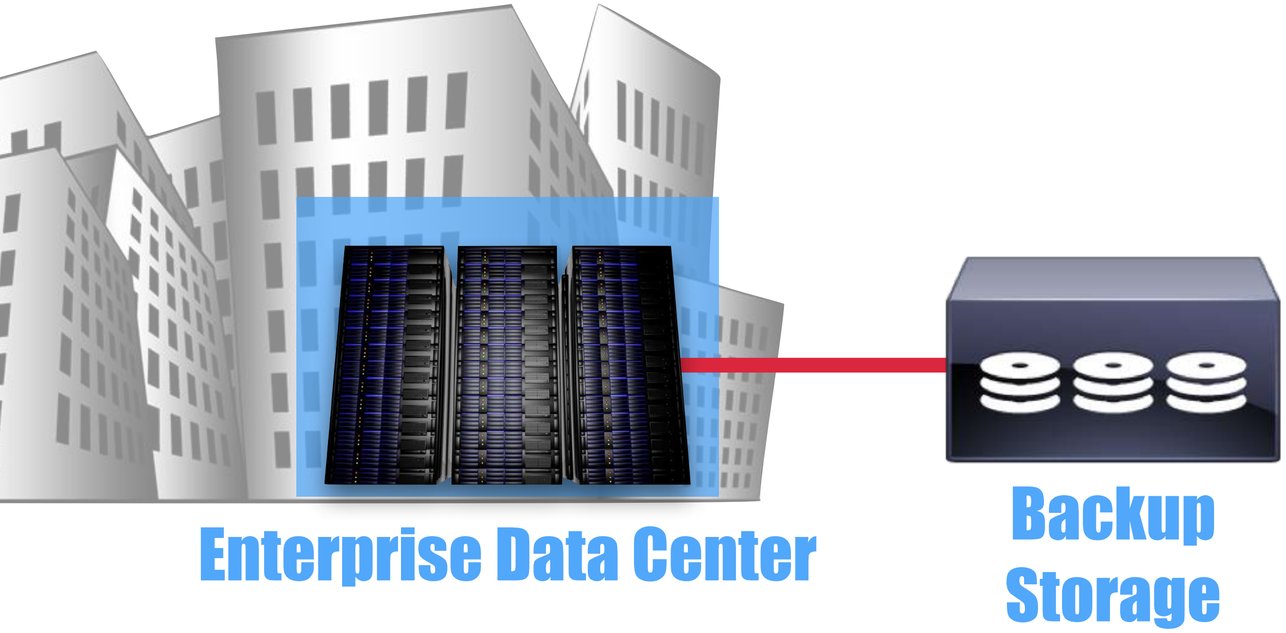
Redundant Design

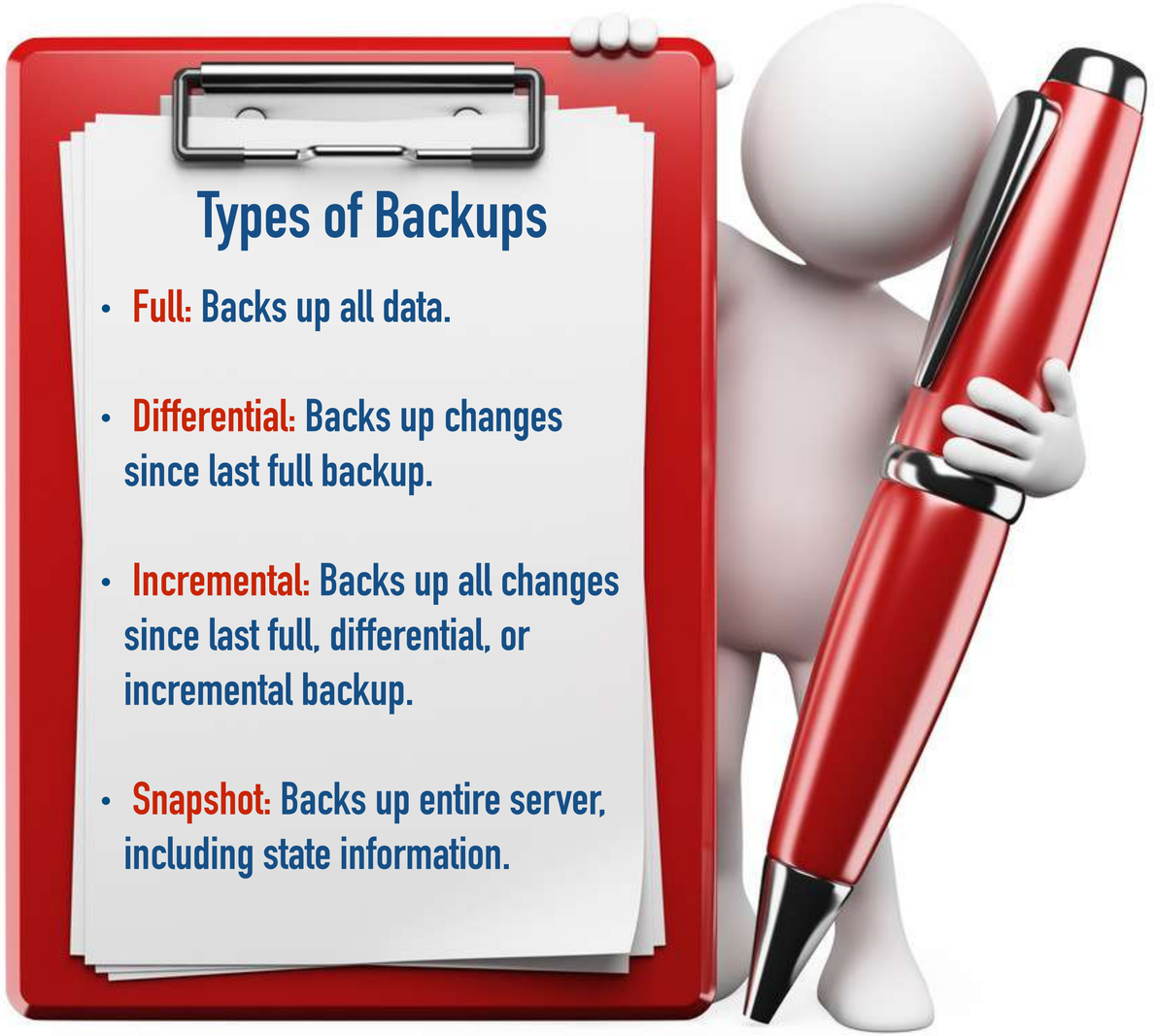
Higher Costs

- Redundant Components
- UPS/Generator
- FHRP



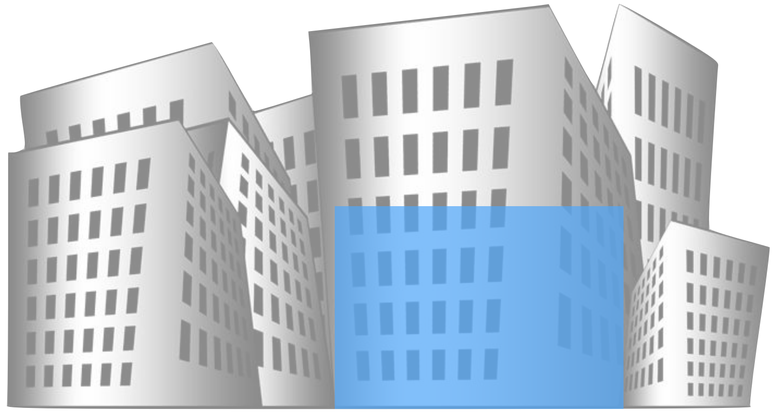
Redundant Design





Redundant Design

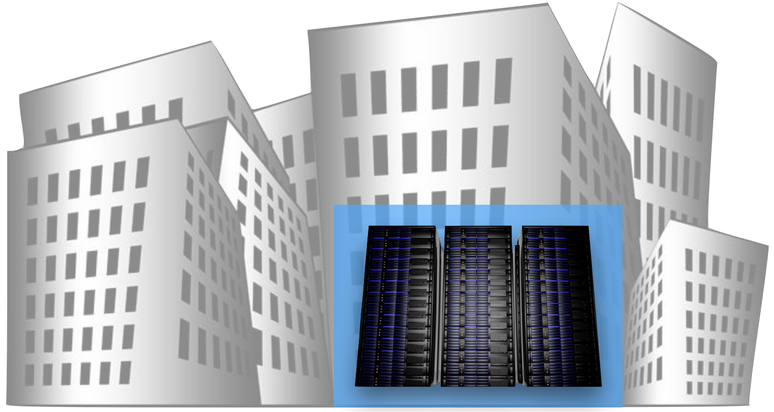
Enterprise Data Center



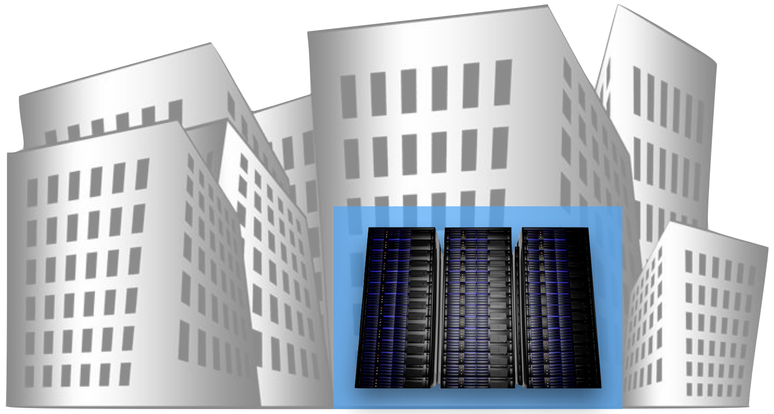
- Power
- HVAC
- Floor Space

Cold Site

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



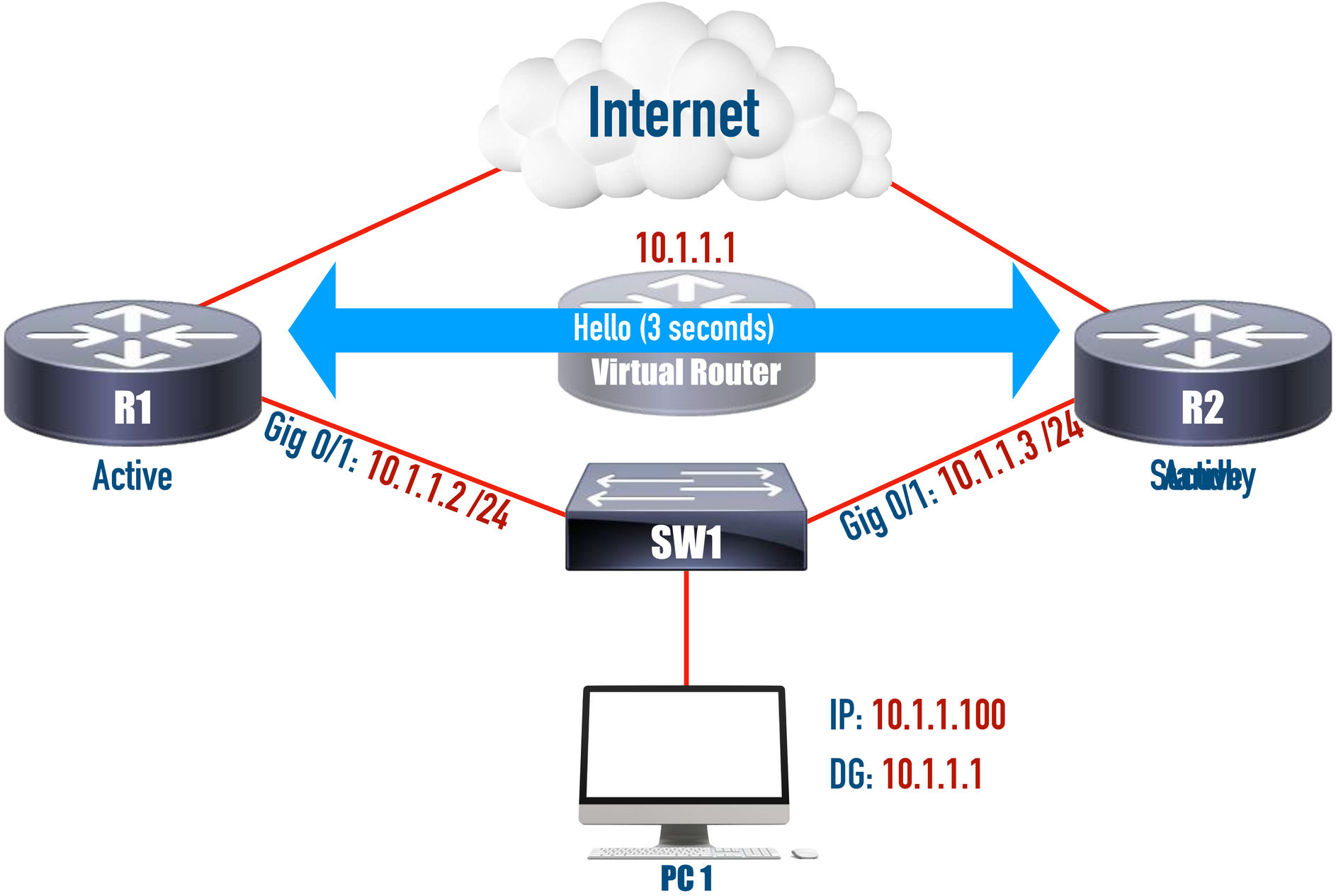
Hot Site



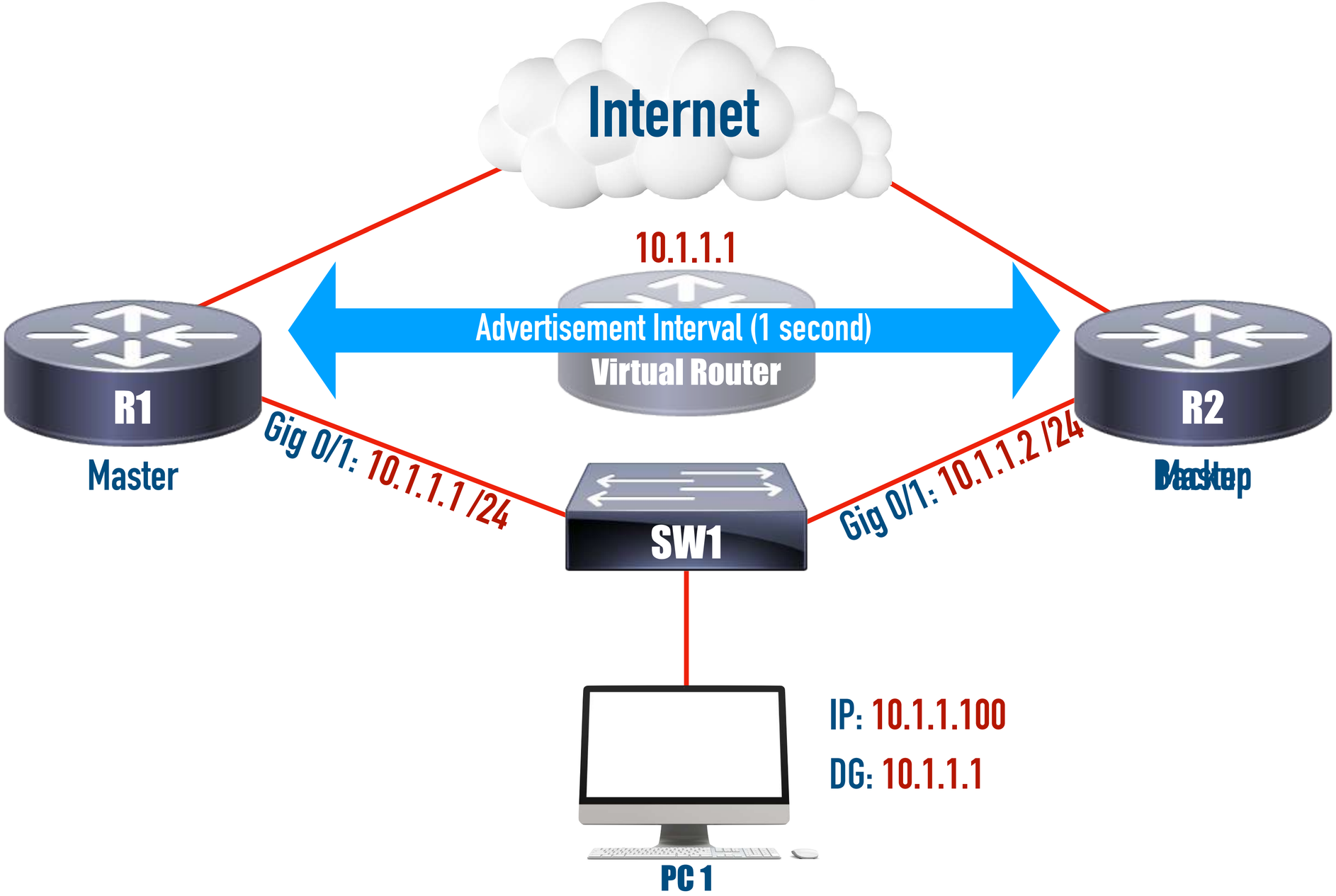
- Power
- HVAC
- Floor Space
- Server Hardware

Warm Site

Hot Standby Router Protocol (HSRP)

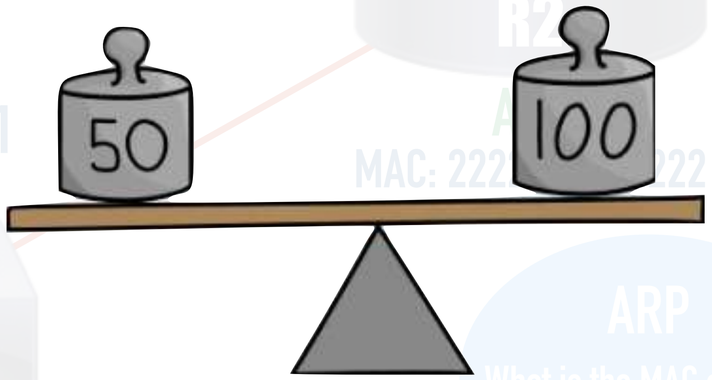


Virtual Router Redundancy Protocol (VRRP)

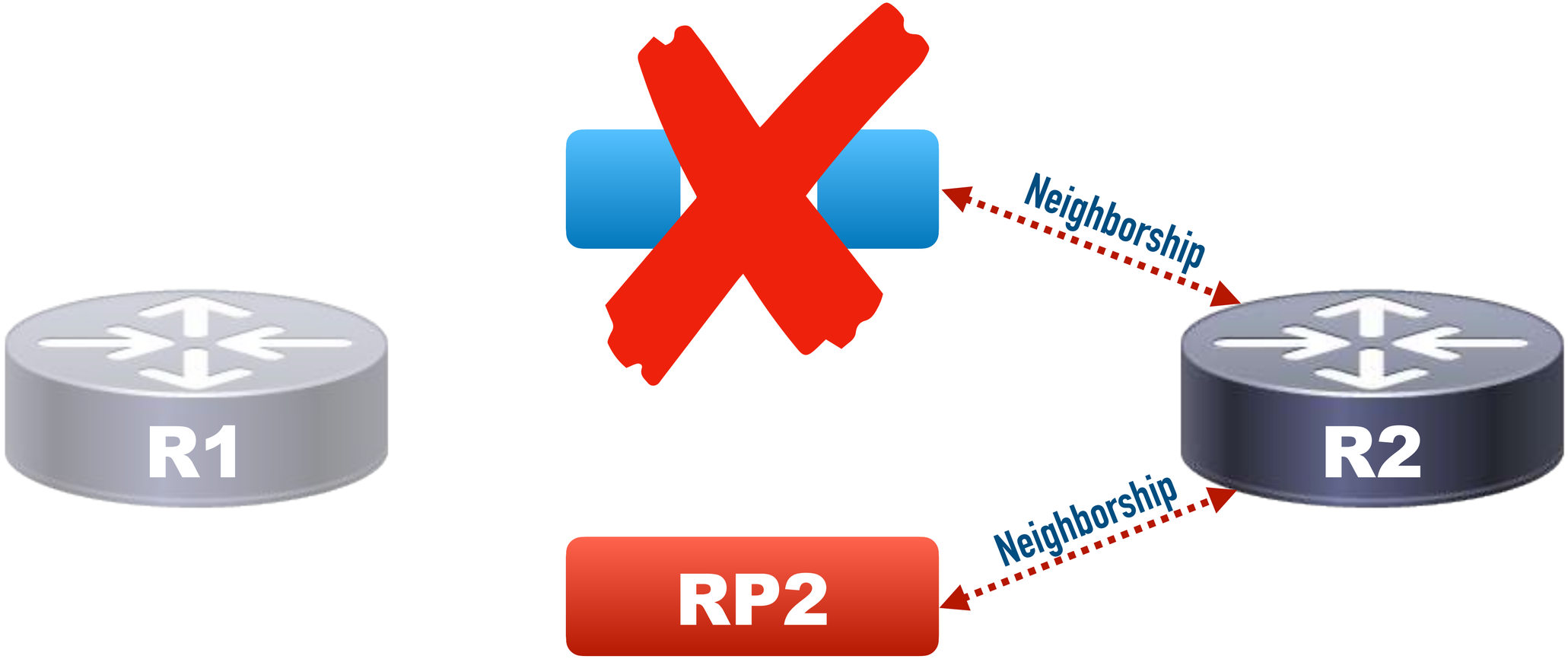


Gateway Load Balancing Protocol (GLBP)

- Round-Robin
- Host-Dependent
- Weighted

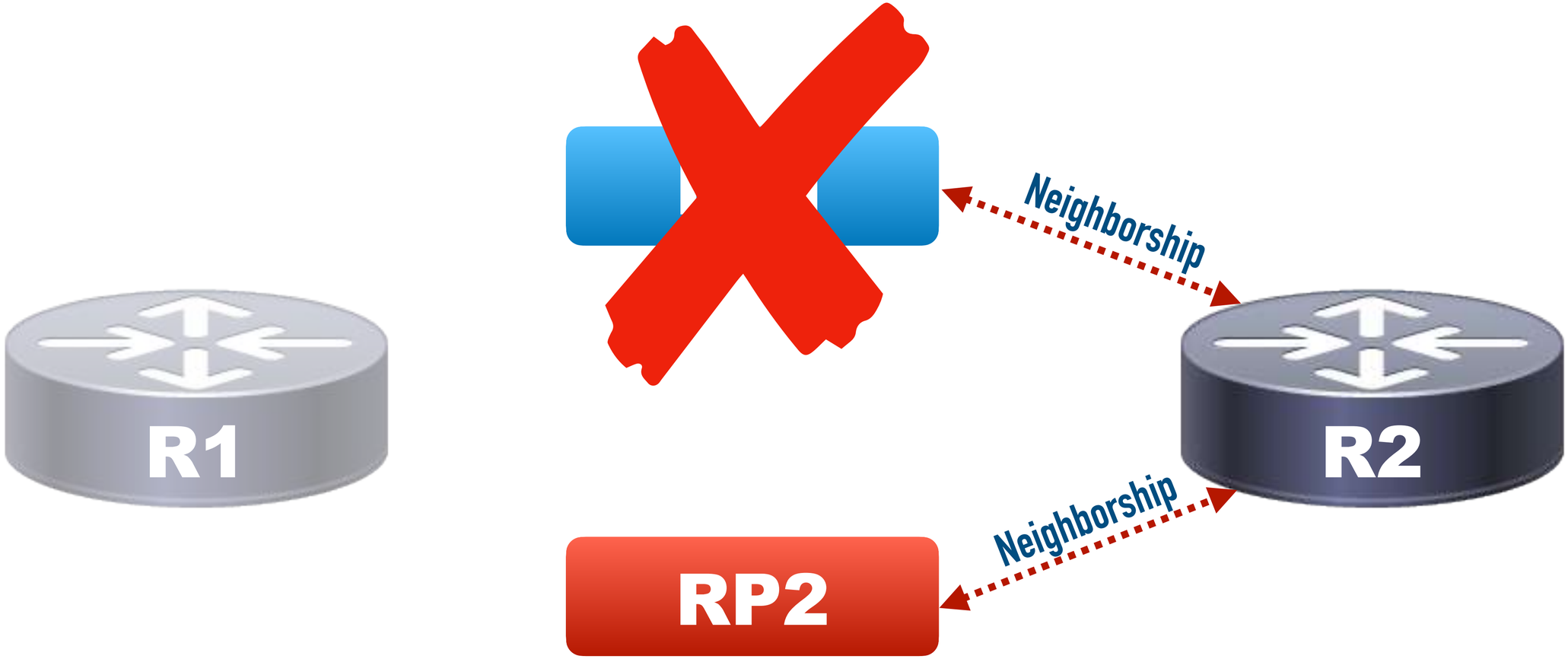


Stateful Switchover (SSO)



The Main Issue: Failing over to a backup route processor might cause routing protocol neighborships to reset.

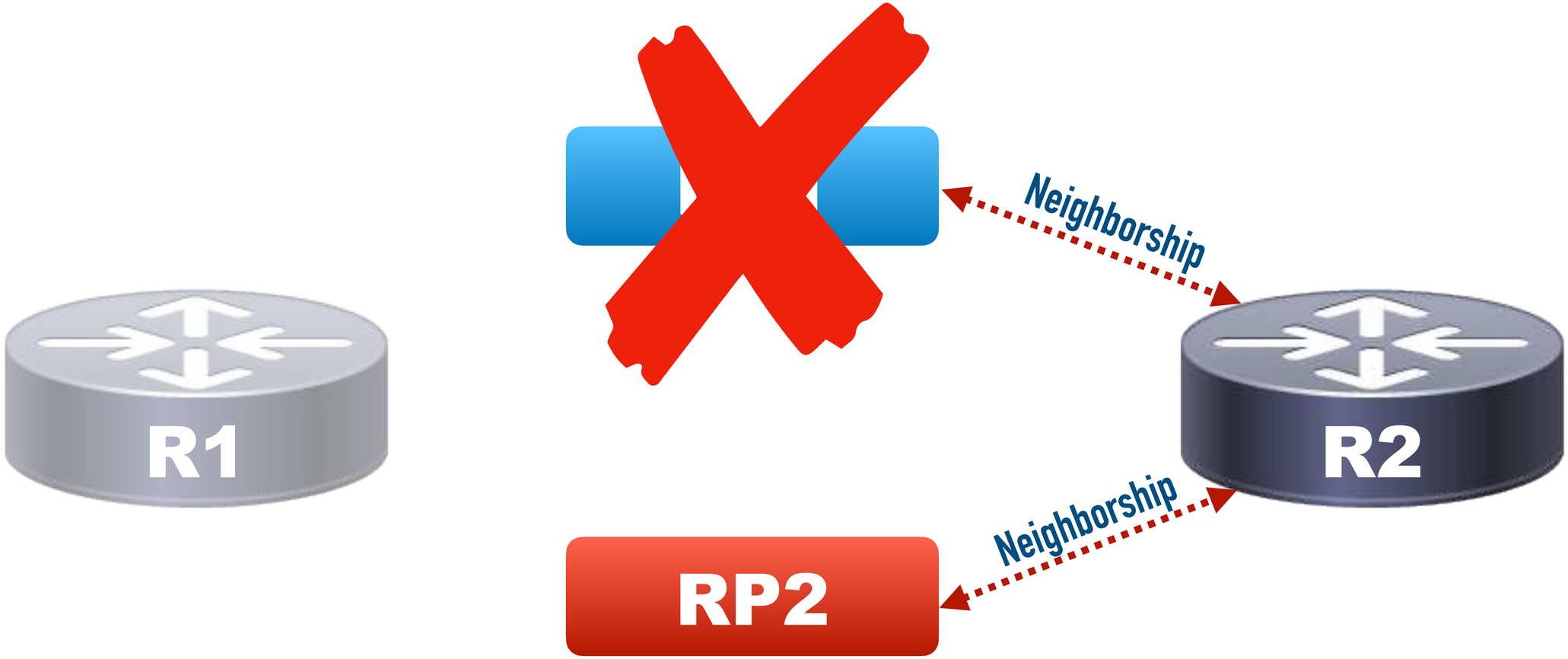
Stateful Switchover (SSO)



SSO: Sync (Config and State Information)

The Secondary Issue: Packets might be dropped until the forwarding table is rebuilt.

Stateful Switchover (SSO)



SSO: Sync (Config and State Information)

Nonstop Forwarding (NSF): Makes the routing information maintained by CEF available to the backup route processor

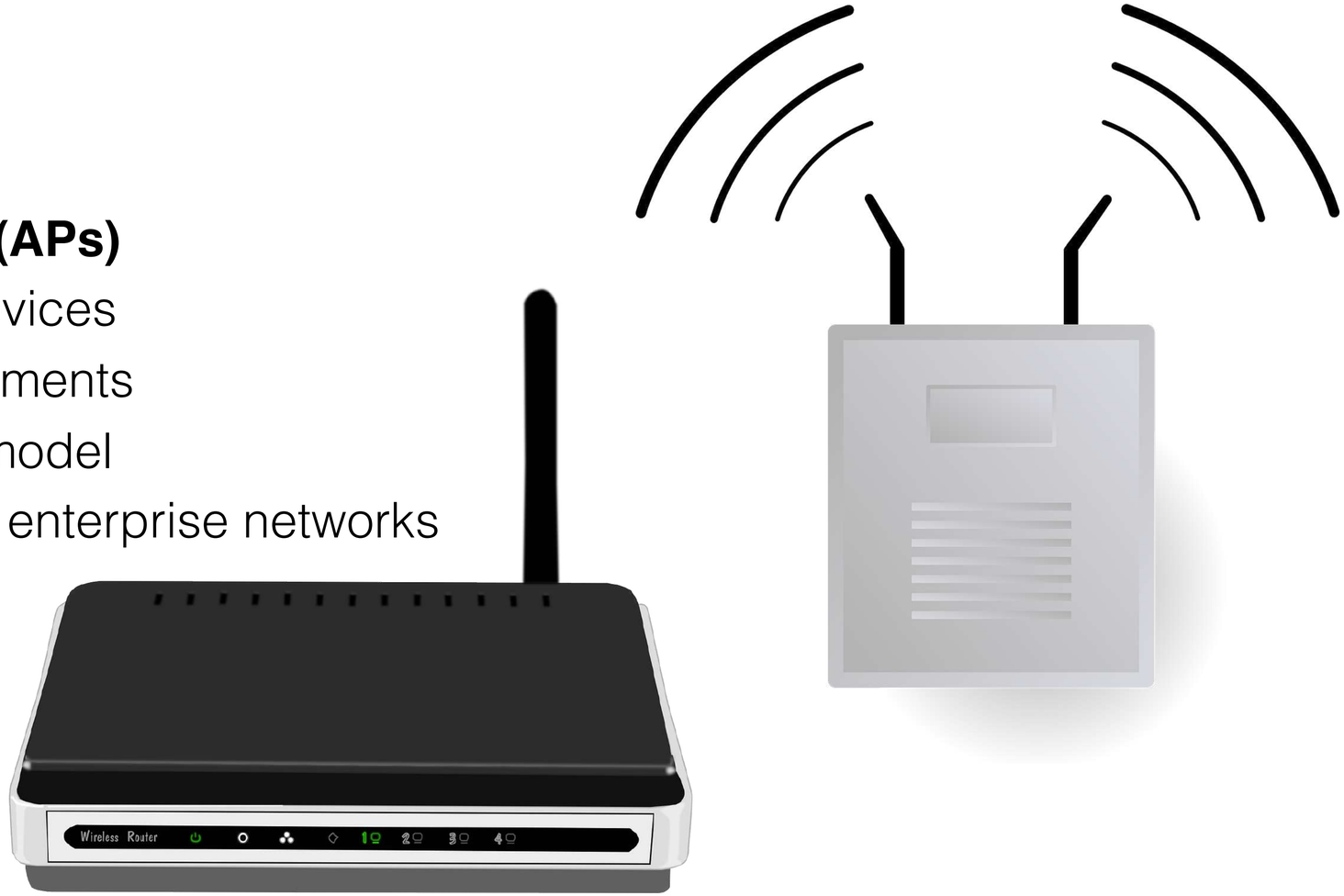
Wireless LAN (WLAN) Design Considerations

Wireless Deployment Options

Wireless Deployment Options

Autonomous Access Points (APs)

- Standalone, independent devices
- Home or small office environments
- Controller-less deployment model
- Not commonly used in large enterprise networks



Wireless Deployment Options

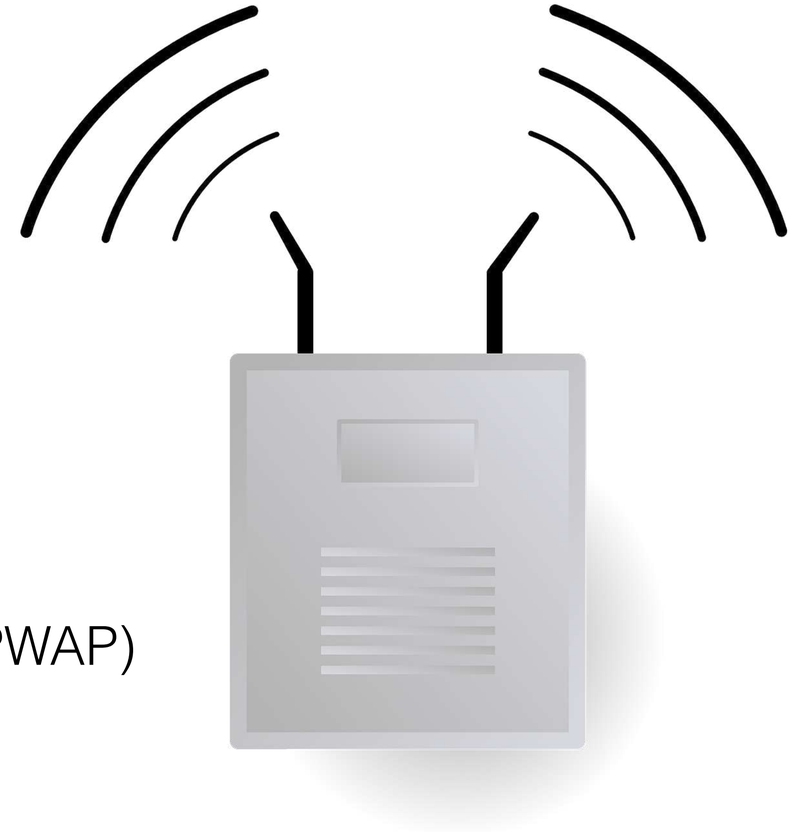
Management IP address:
10.1.1.1

Management IP address:
20.1.1.1

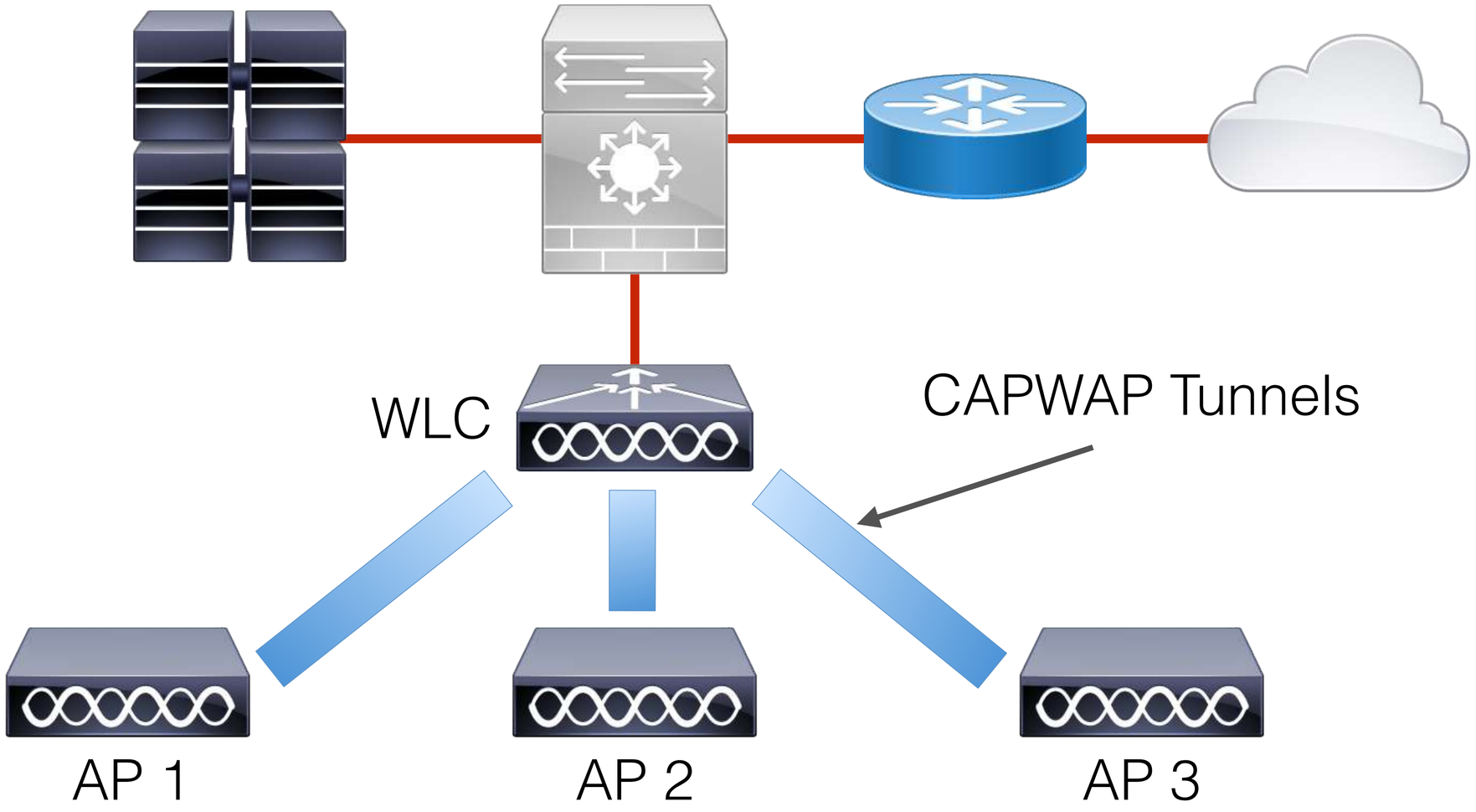
Wireless Deployment Options

Lightweight Access Points (APs)

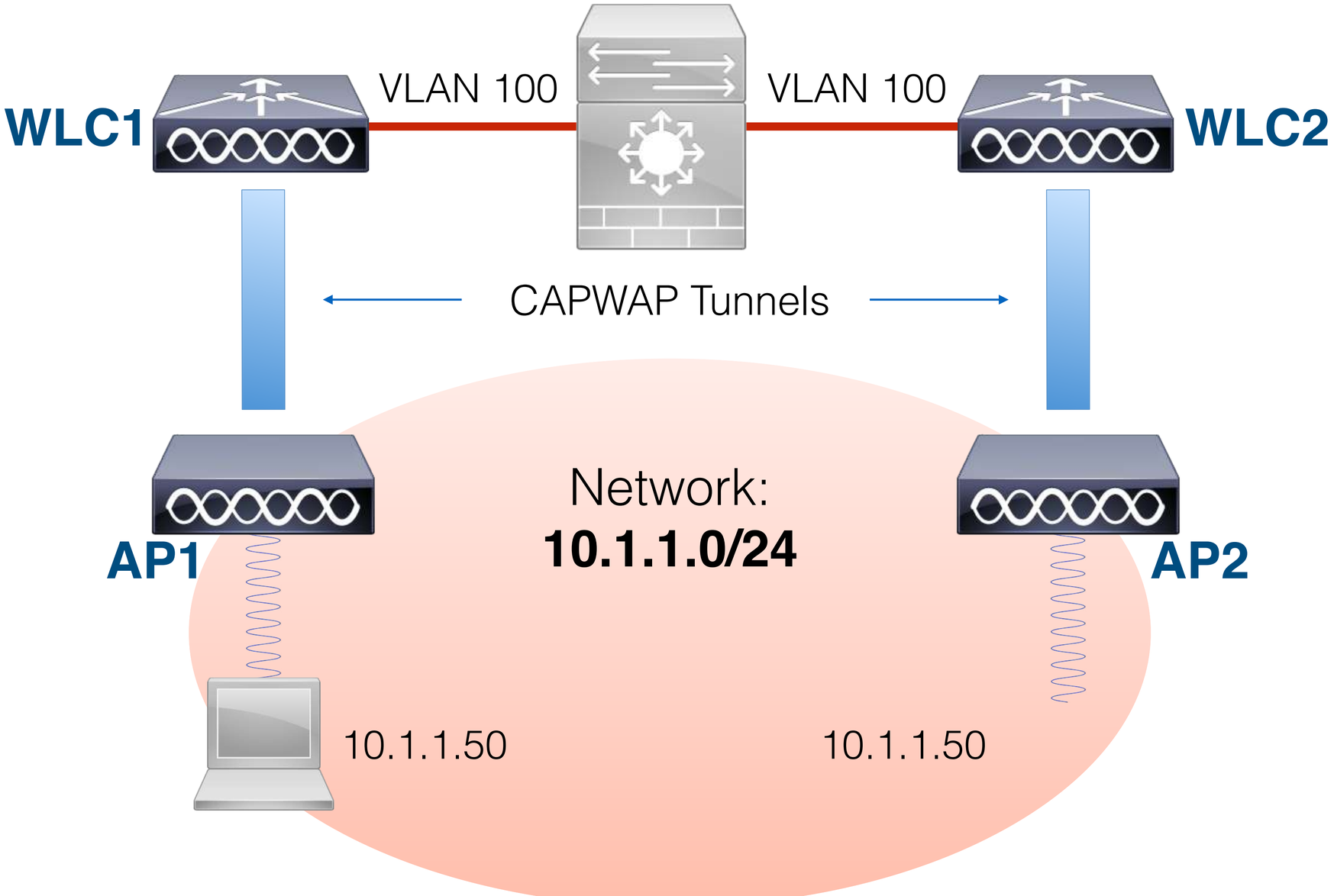
- Requires central wireless LAN controller (WLC)
- Controller-based deployment model
- WLCs can be physical or virtual
- Controller communicates changes to the APs
- Control and Provisioning of Wireless Access Points (CAPWAP)



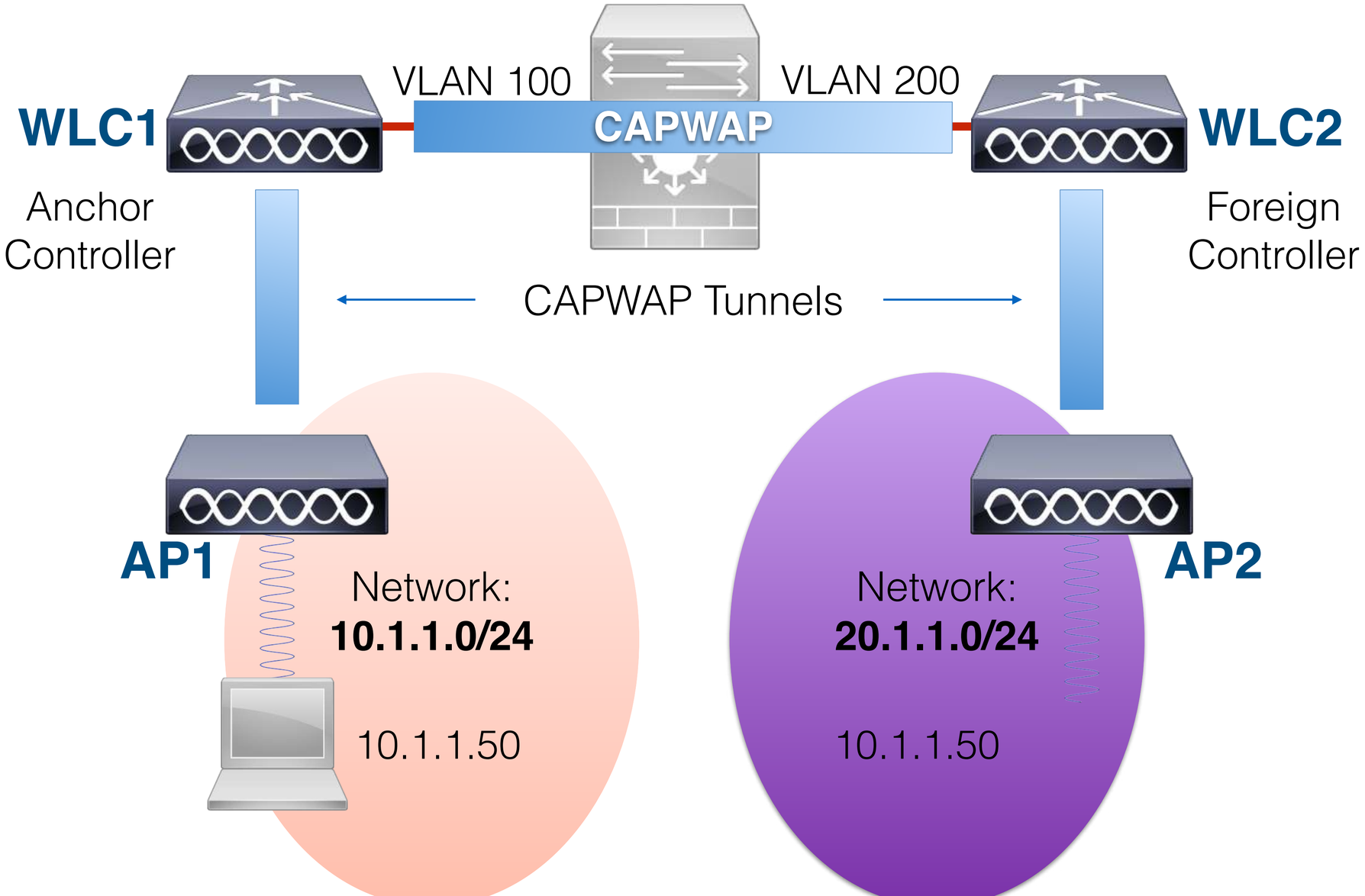
Wireless Deployment Options



Wireless Deployment Options



Wireless Deployment Options



Wireless Deployment Options

Cisco FlexConnect:

- Configure and control remote wireless network
- Similar to Layer 3 roaming with CAPWAP

Central Switched:

- Normal CAPWAP mode of operation
- Typically not the recommended mode

Local Switched:

- Map user traffic to VLAN on adjacent switch
- Control and management traffic still sent over CAPWAP to WLC

Location Services

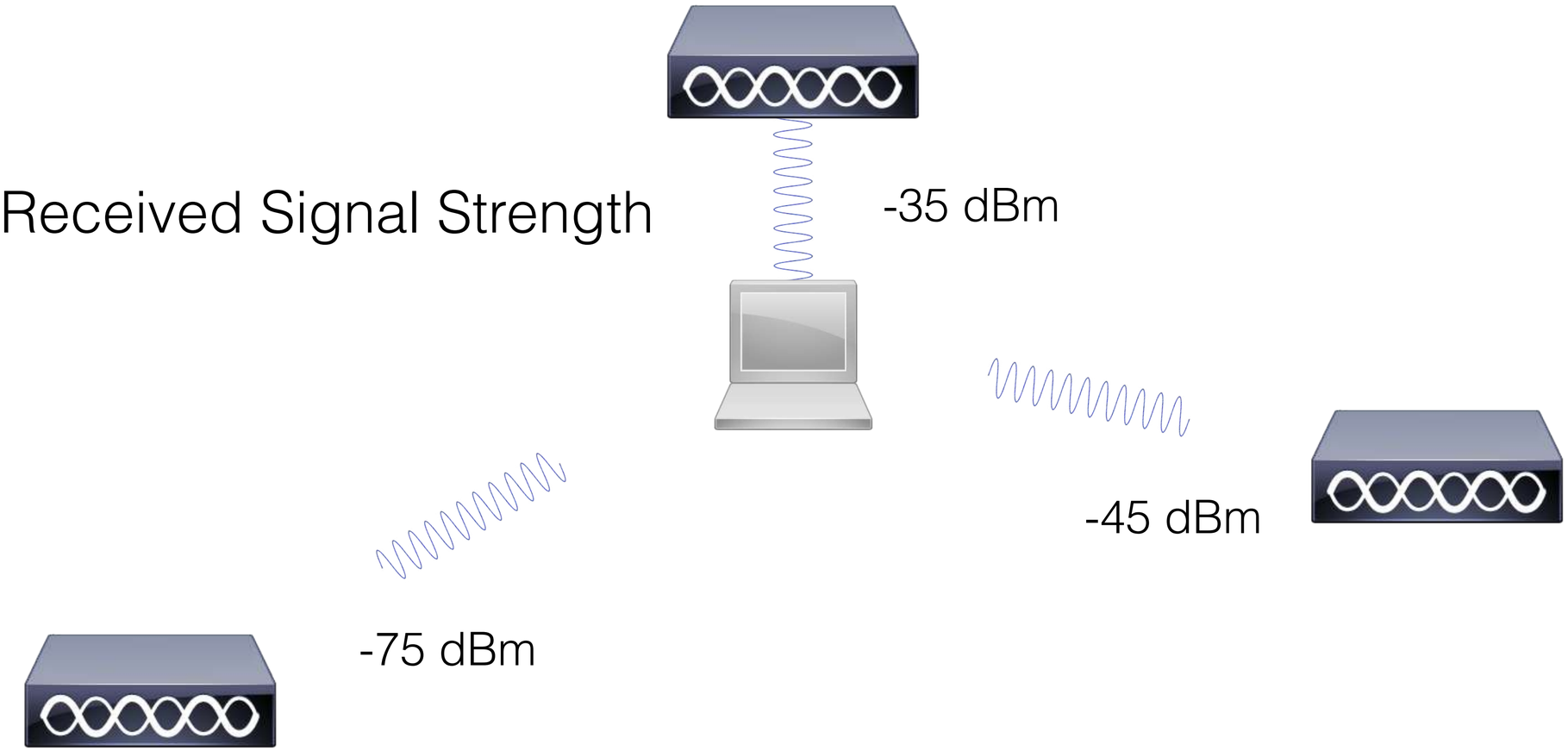
Location Services

Use Cases f rvices

- Enterpris
- Location g

Location Services

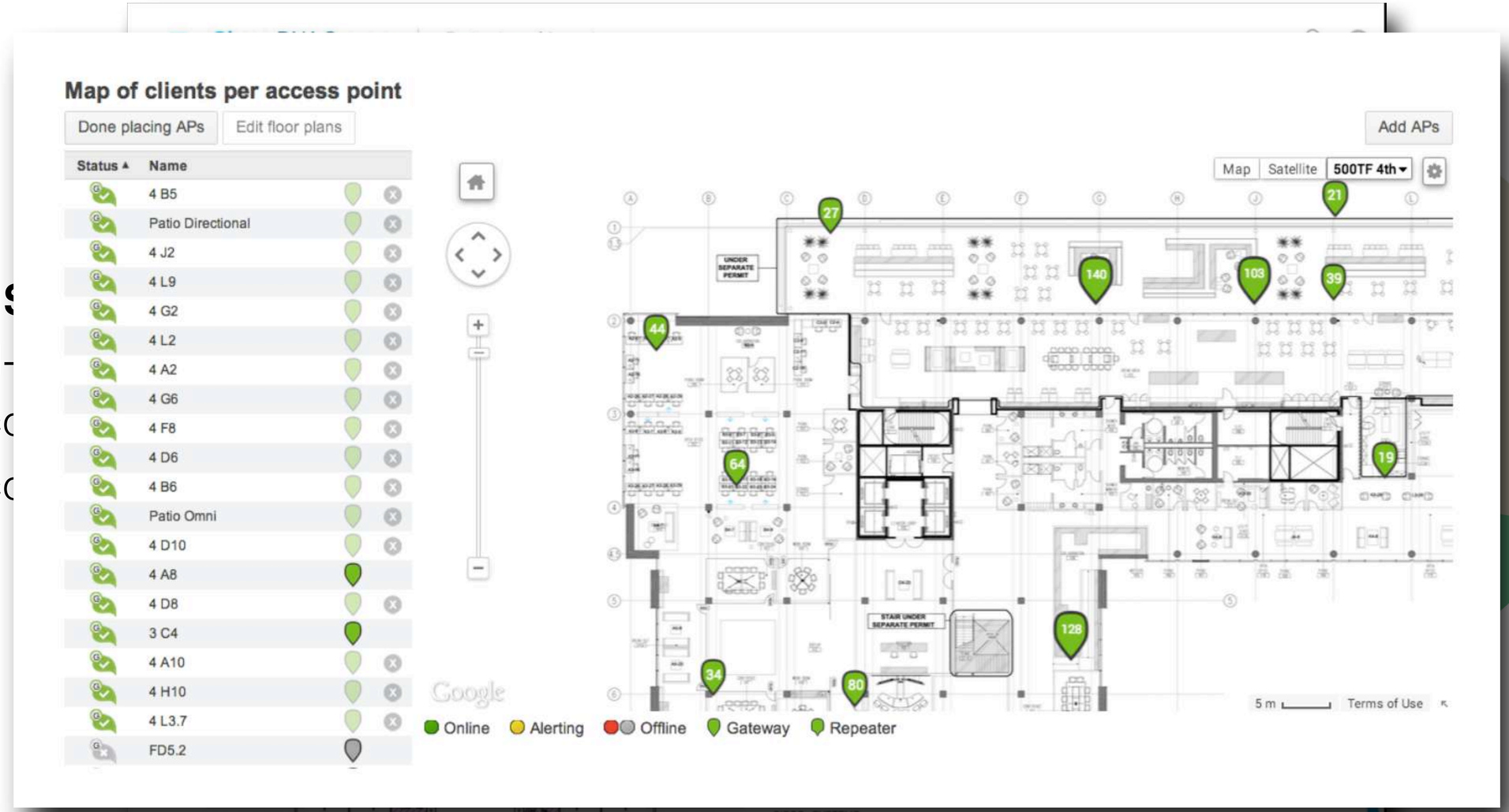
RSS = Received Signal Strength



Location Services

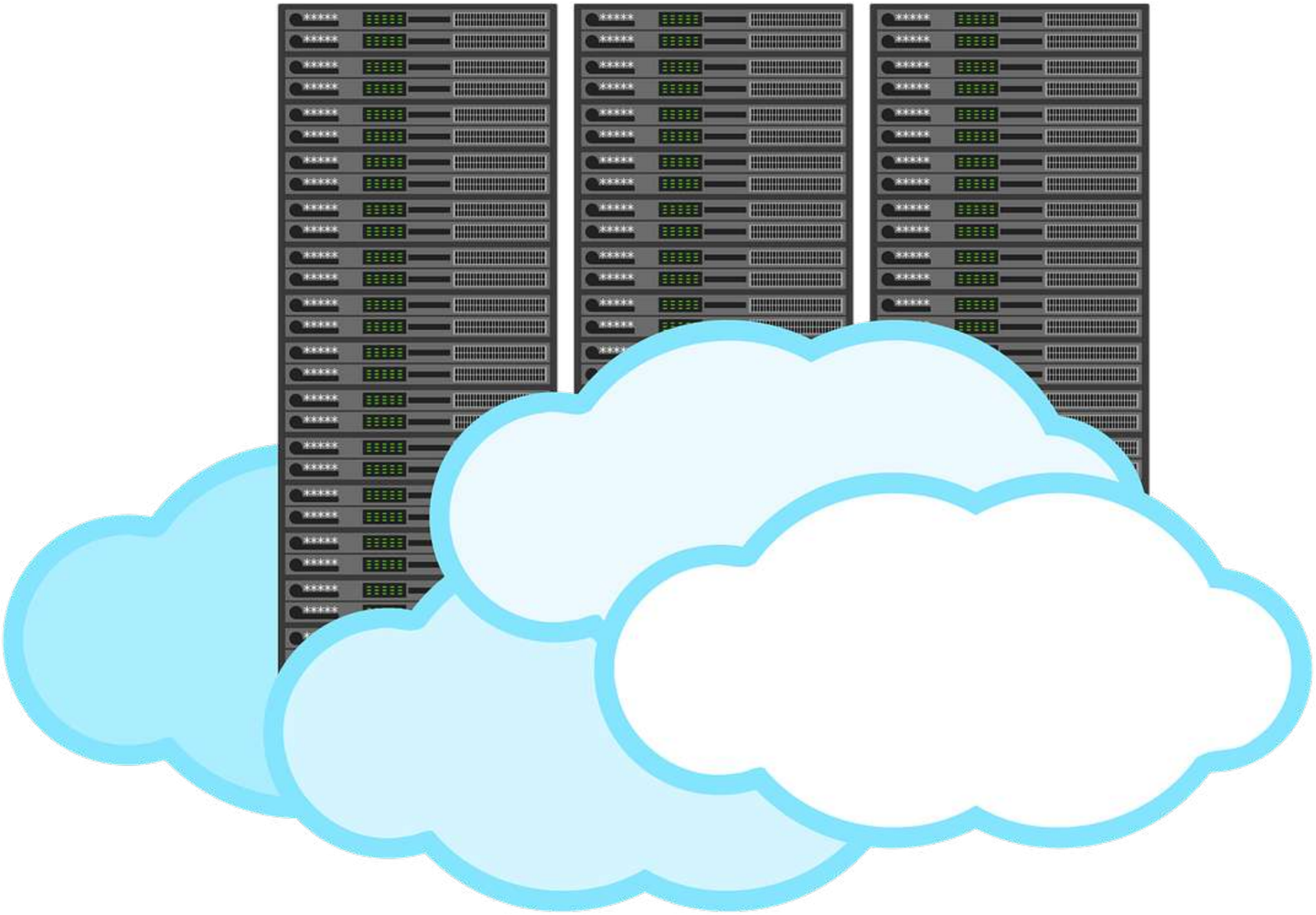
Cisco S

- Real-
- Cisco
- Cisco



Software-Defined WAN (SD-WAN)

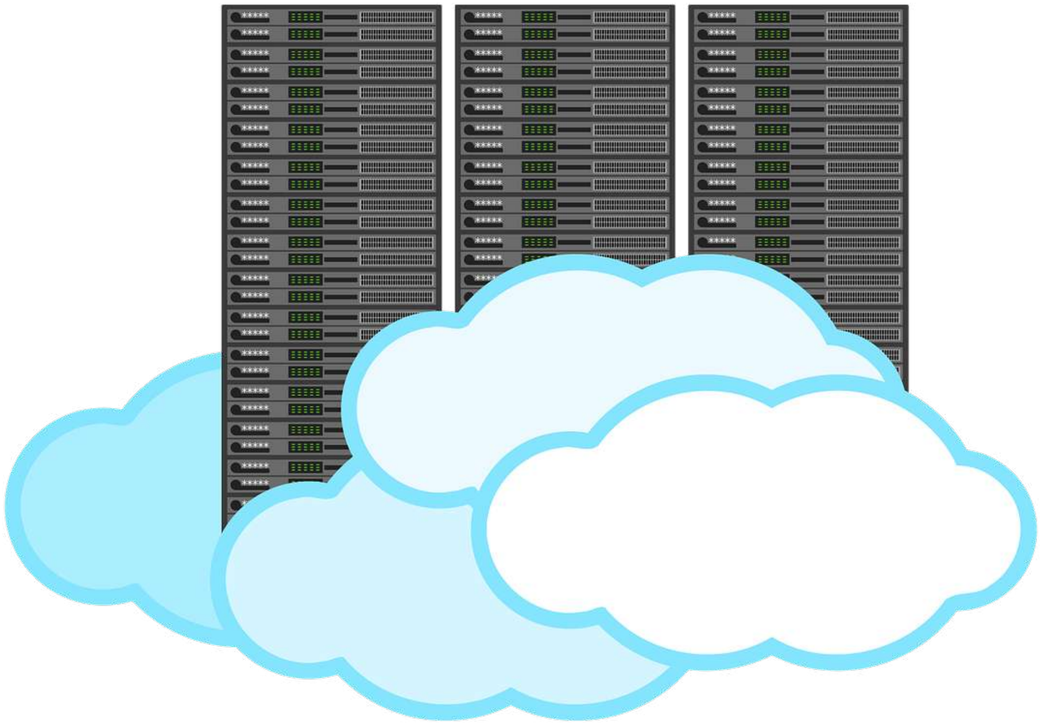
Overview of SD-WAN Technology



Overview of SD-WAN Technology

Enterprise WAN:

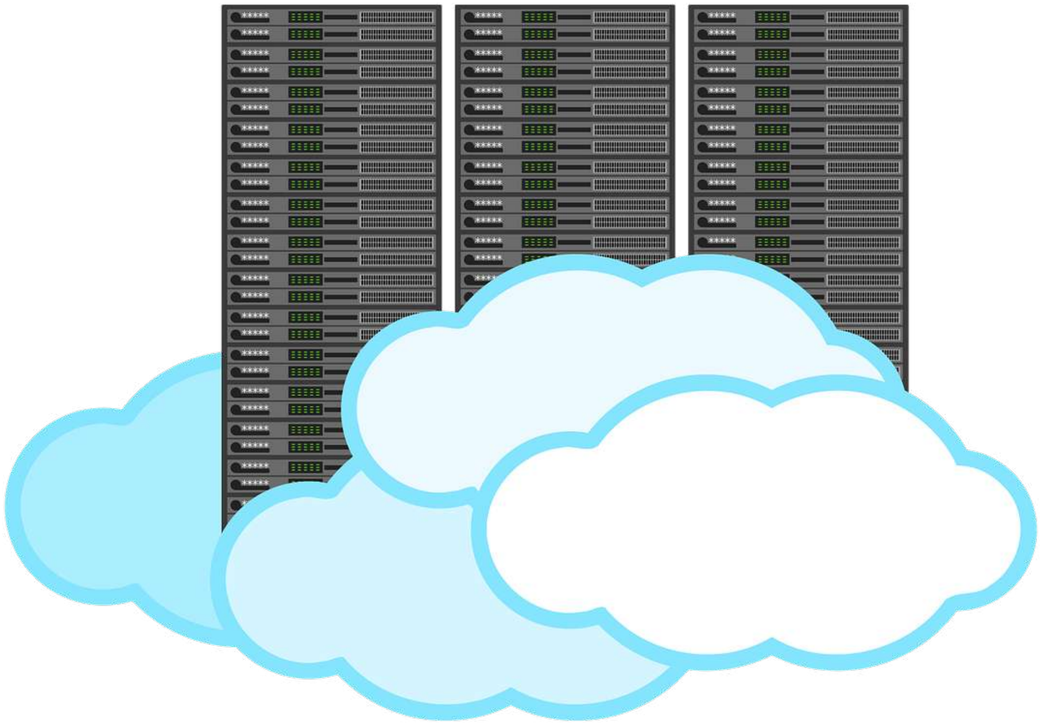
- Dedicated circuits traditionally used
- Provide reliability and security
- Rise in cloud usage requires simplicity



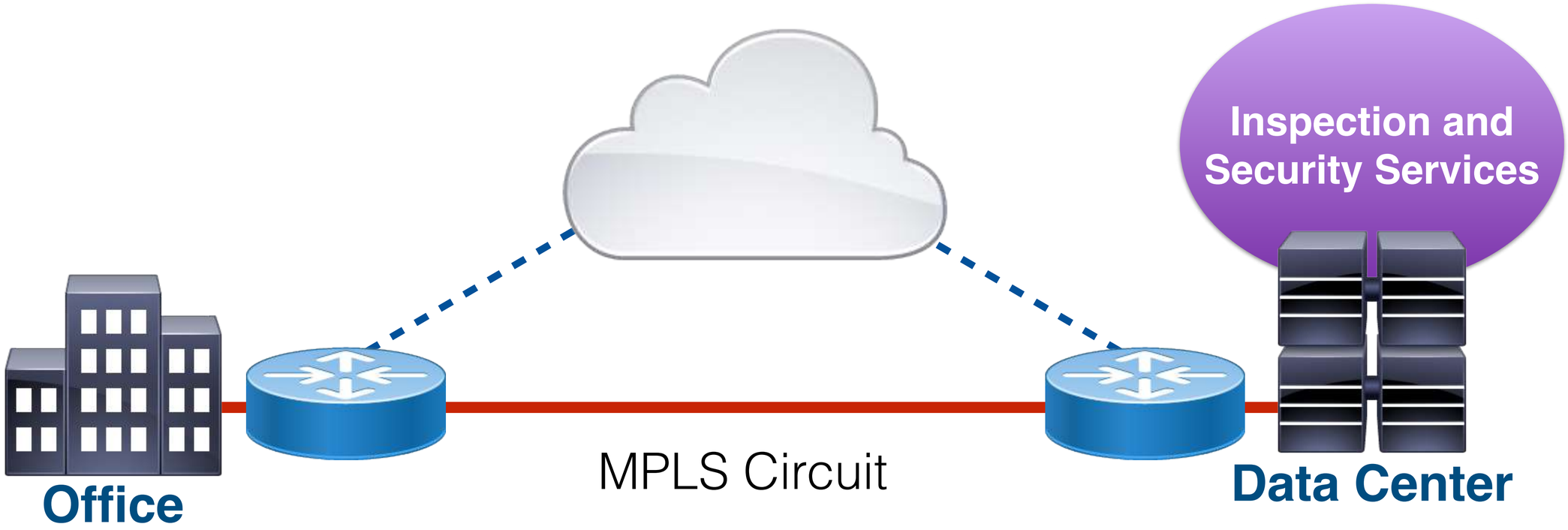
Overview of SD-WAN Technology

Software-Defined Wide Area Network (SD-WAN)

- Traffic backhauling no longer required

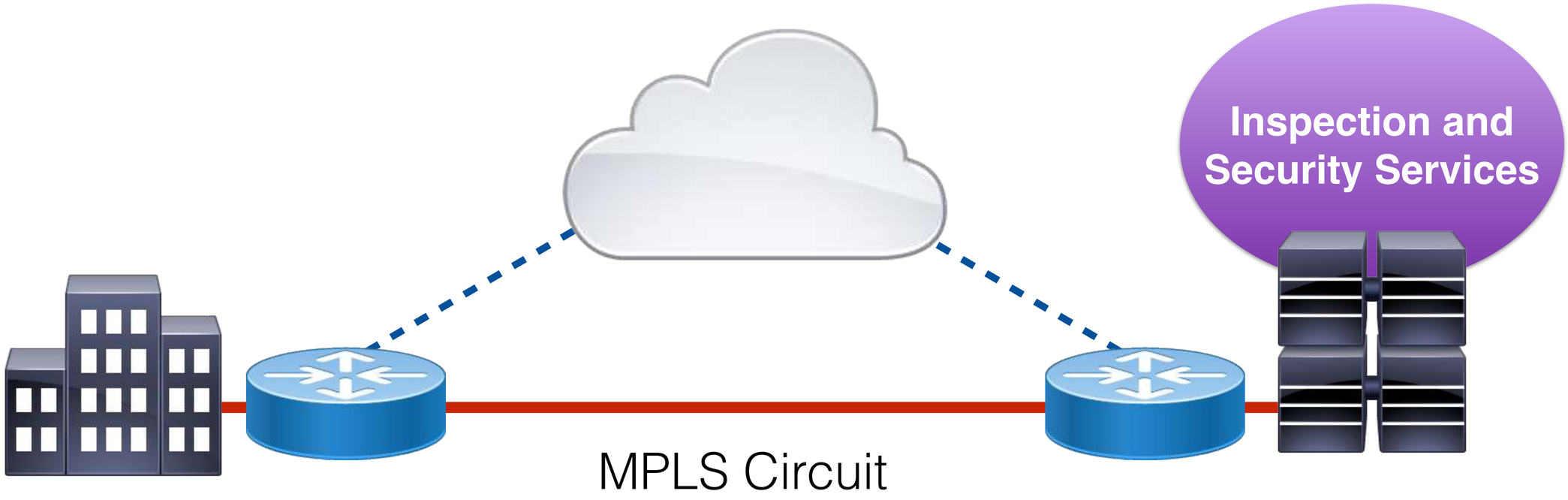


Overview of SD-WAN Technology



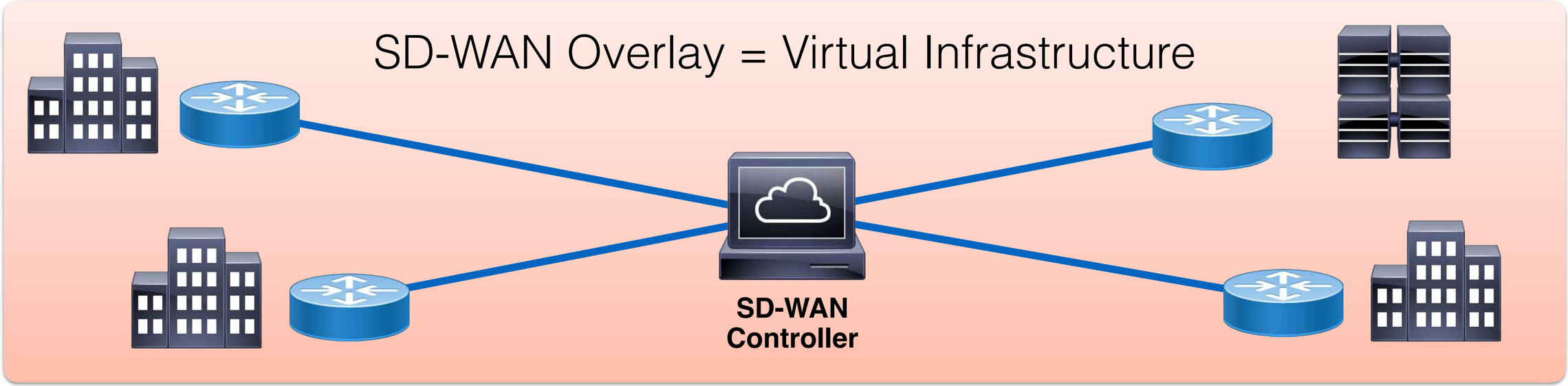
aws Azure Office

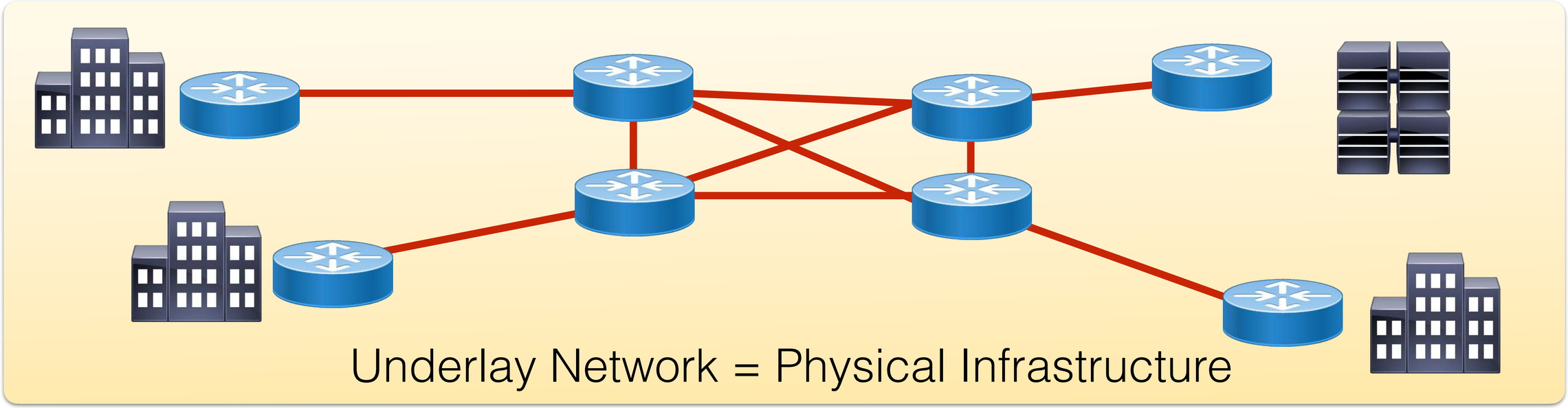
Overview of SD-WAN Technology



- End-to-end traffic encryption and inspection through SD-WAN
- Next generation security mechanisms added
- Anti-malware systems, botnet control intervention, etc.

Overview of SD-WAN Technology





SD-WAN Implementation

SD-WAN Implementation

Cisco SD-WAN:

- Data plane
- Control plane
- Management plane
- Orchestration plane

viptela

SD-WAN Implementation

vManage: User interface

vBond: Orchestration and provisioning

Management & Orchestration Plane

vSmart: SD-WAN - Policy Enforcement

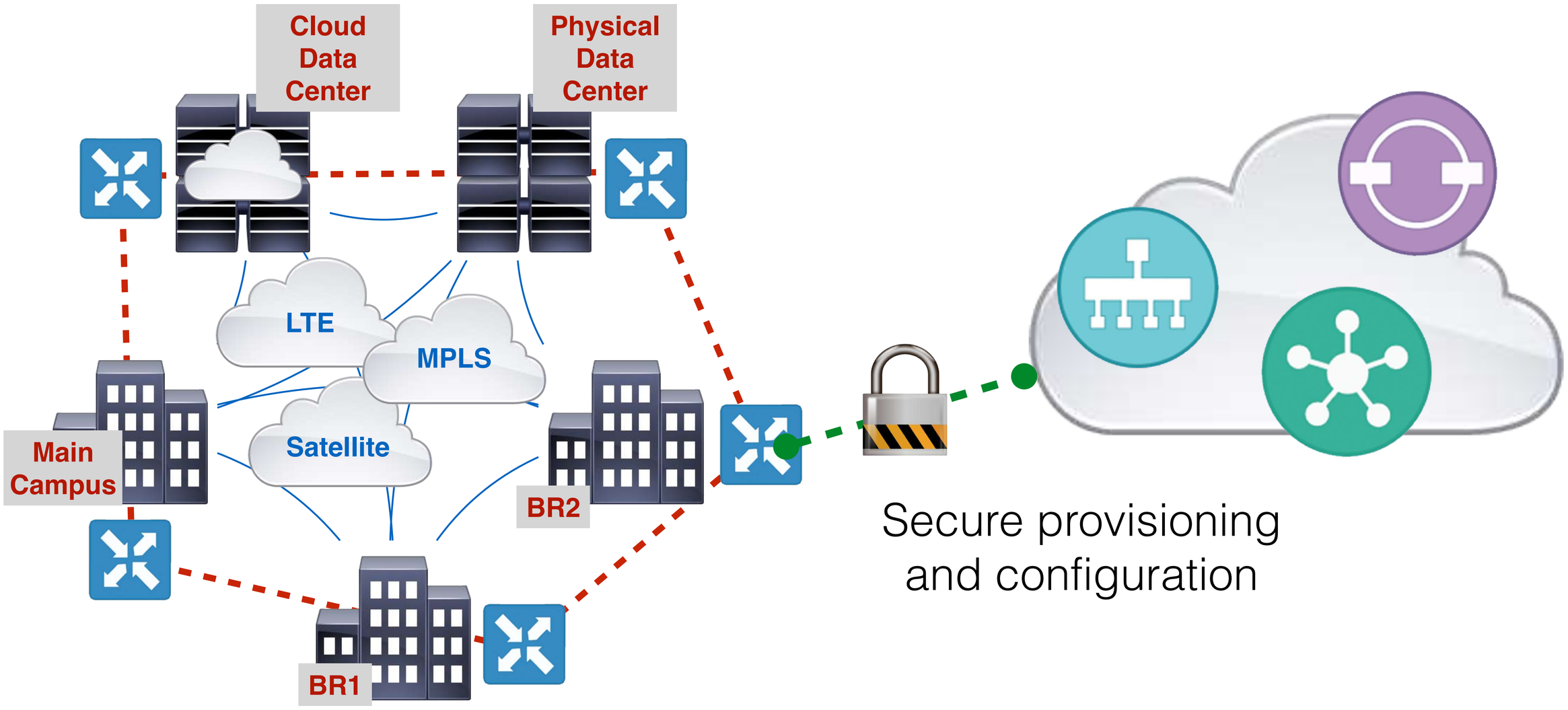
- Communicates via Overlay Management Protocol (OMP)

Control Plane

Cisco vEdge: Edge routers

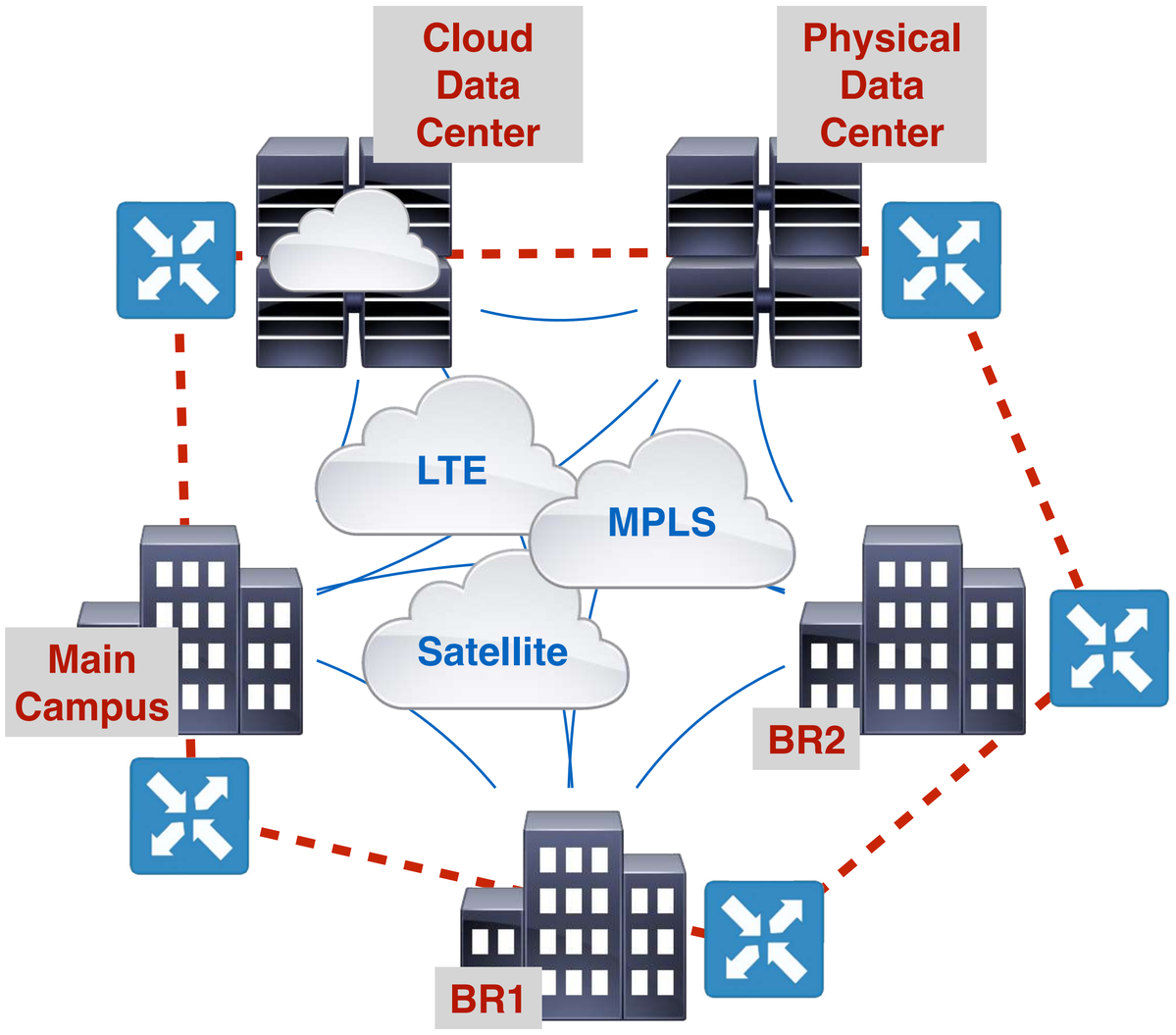
Data Plane

SD-WAN Implementation



Secure provisioning and configuration

SD-WAN Implementation



Edge Router Hardware Platforms:

- Cisco vEdge routers running Viptela OS
- ISR 1000 and 4000 Series routers
- ASR 1000 Series routers

Edge Router Software Platforms:

- CSR 1000v Router
- vEdge Cloud Router running Viptela OS

Cisco vManage

demo

DASHBOARD | MAIN DASHBOARD

2 ↑ vSmart - 2	8 ↑ WAN Edge - 8	2 ↑ vBond - 2	1 vManage - 1	Reboot Last 24 hrs 1	Warning 5 / Invalid 0

Control Status (Total 10)

Control Up	8
Partial	2
Control Down	0

Site Health (Total 5)

Full WAN Connectivity	0 sites
Partial WAN Connectivity	5 sites
No WAN Connectivity	0 sites

Transport Interface Distribution

< 10 Mbps	15
10 Mbps - 100 Mbps	6
100 Mbps - 500 Mbps	0
> 500 Mbps	0

View Percent Utilization

WAN Edge Inventory

Total	8
Authorized	8
Deployed	8
Staging	0

WAN Edge Health (Total 8)

Normal	Warning	Error
8	0	0

Transport Health

Type: By Loss

100 %
50 %
0

Top Applications

Usage: 931.32 GB, 9.31 GB, 95.37 MB, 976.56 KB, 9.77 KB, 100 B, 0

http, rtp, ex..., rtp..., smtp, ora..., ma..., citrix, un..., db...

Application

Application-Aware Routing

Type: By Loss

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
DC2-VEDGE2:biz-internet-BR1-CEDGE1:biz-in...	5.537	90.049	5.059
DC1-VEDGE2:biz-internet-BR1-CEDGE1:biz-in...	1.231	89.801	0.494
BR1-CEDGE1:biz-internet-DC2-VEDGE1:biz-in...	3.909	89.773	3.25
BR1-CEDGE1:biz-internet-DC2-VEDGE2:biz-in...	8.658	89.178	5.932

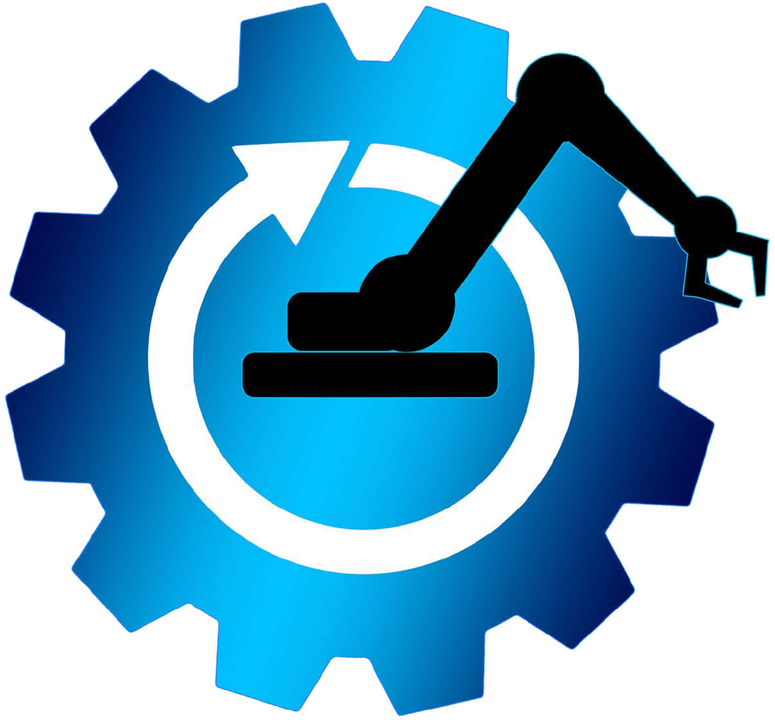
cisco.com/go/sdwandemos

Software-Defined Access (SD-Access)

Overview of SD-Access Technology

SD-Access Advantages:

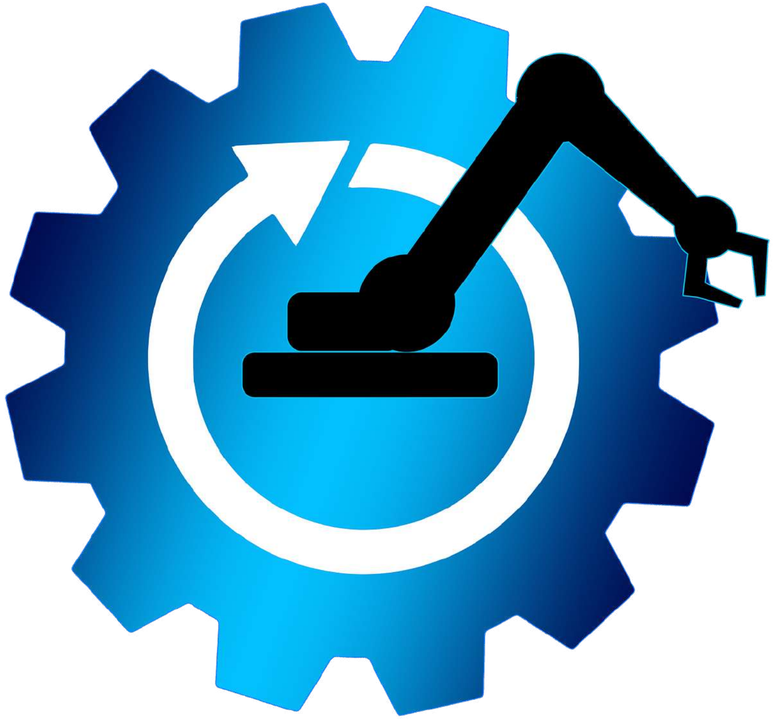
- Next-generation policy enforcement
- Security Group Access Control Lists (SGACLs)
- Policies are based on identity rather than addresses



Overview of SD-Access Technology

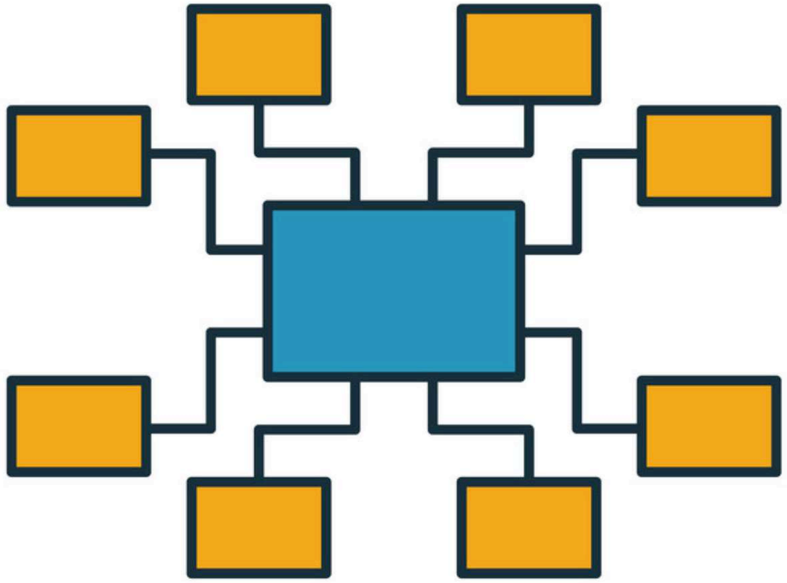
SD-Access Advantages:

- Secure network segmentation
- Virtualization of physical network
- Separate virtual networks can have separate policies



Overview of SD-Access Technology

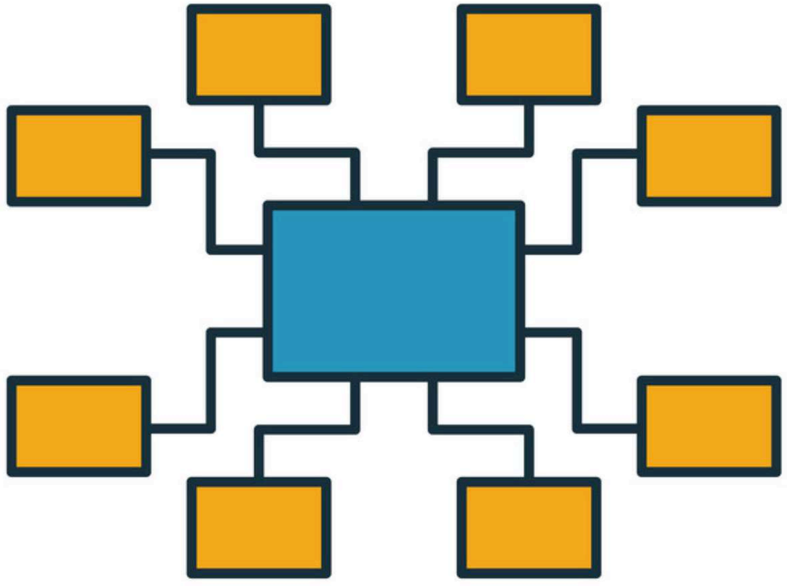
DNA Center



CAMPUS FABRIC

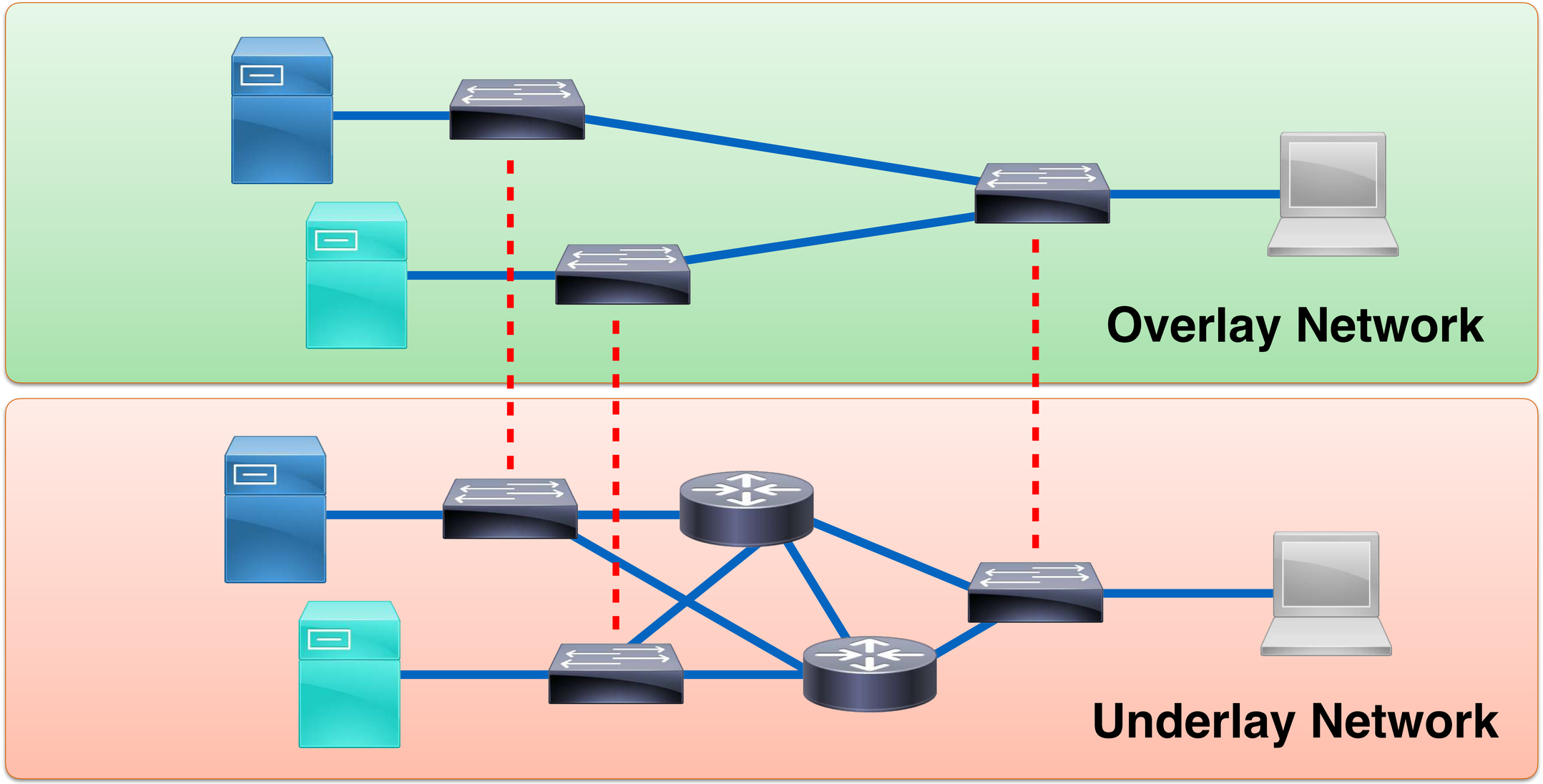
Overview of SD-Access Technology

- Virtual overlay network
- Ideally used with Cisco DNA Center
- NETCONF/YANG management
- Overcomes limitations found in traditional network architecture



CAMPUS FABRIC

Overview of SD-Access Technology



Overview of SD-Access Technology

SD-Access Fabric

Control Plane

- LISP encapsulation
- Simplified routing

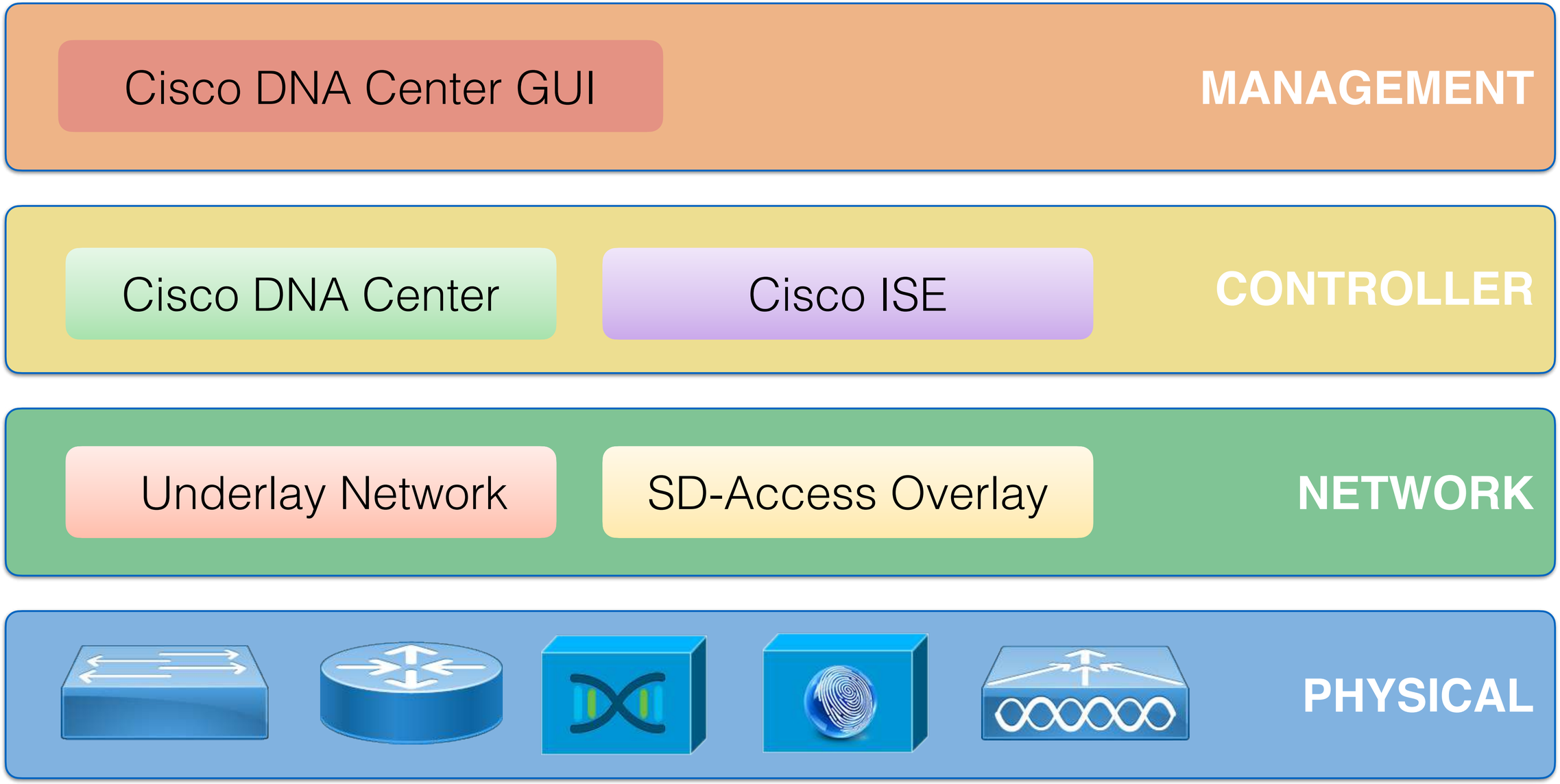
Data Plane

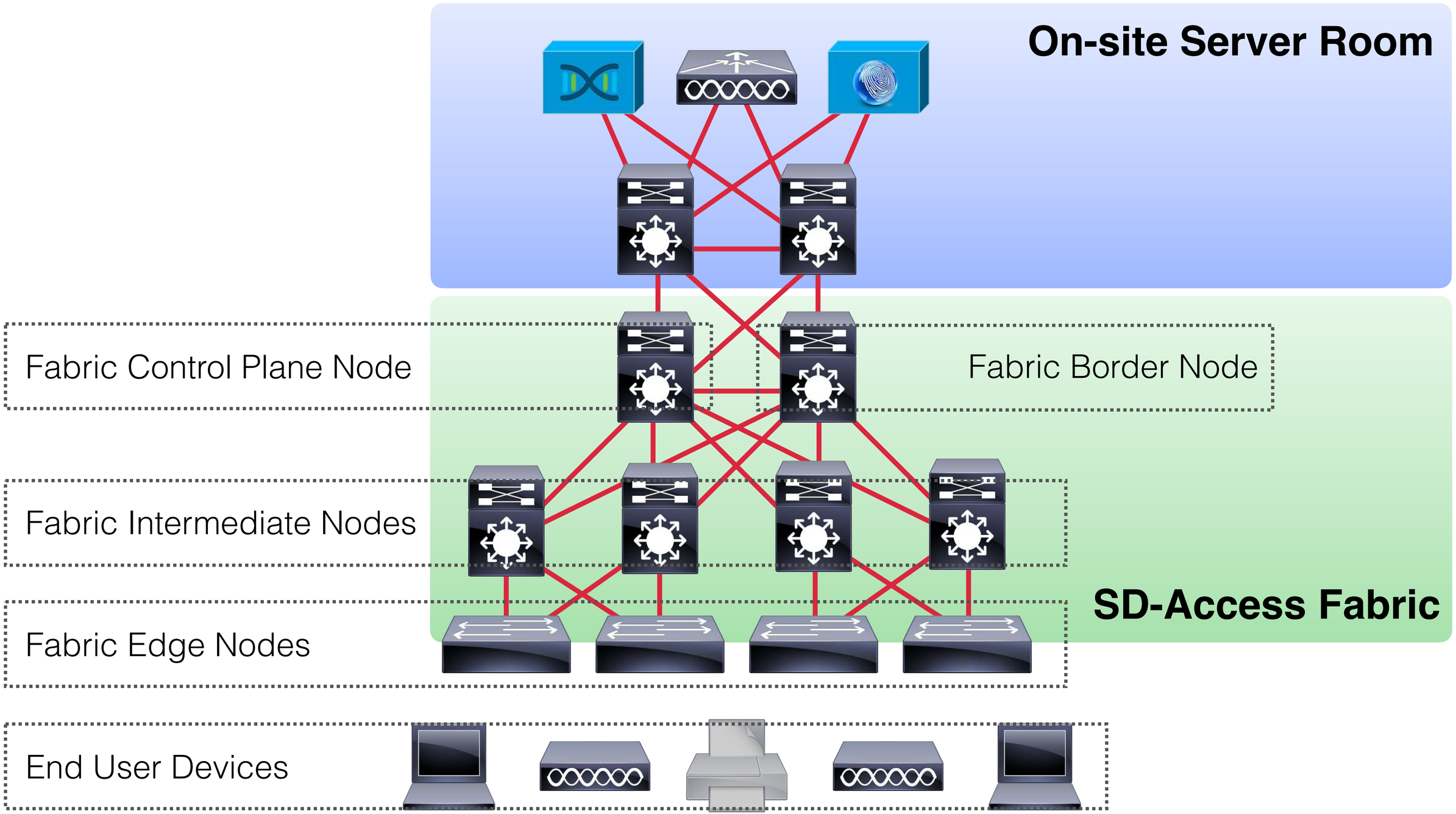
- VXLAN Tunneling
- Virtual networks

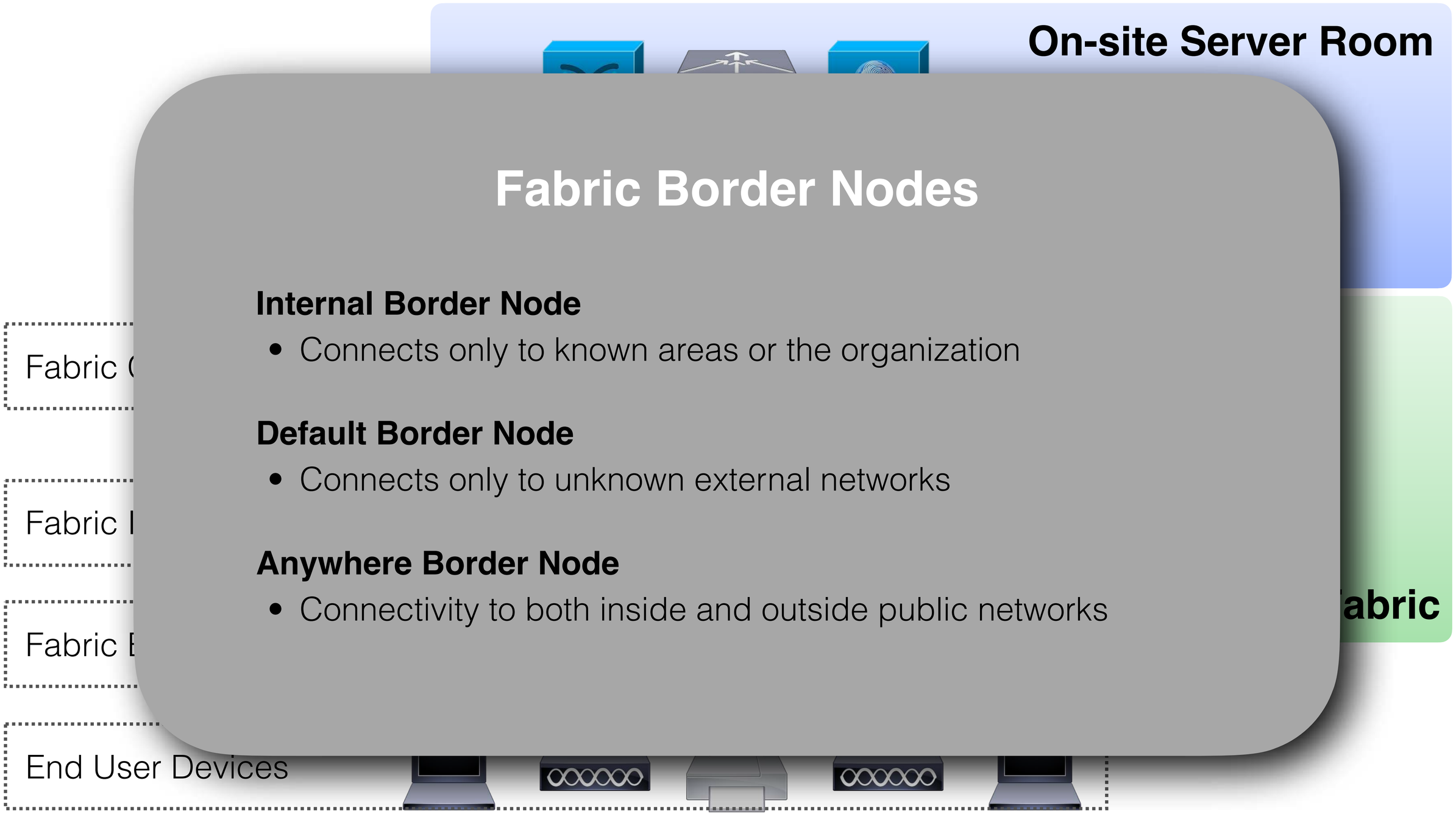
Policy Plane

- Cisco TrustSec
- Security groupings

Overview of SD-Access Technology




On-site Server Room
Fabric Control Plane Node
Fabric Border Node
Fabric Intermediate Nodes
Fabric Edge Nodes
SD-Access Fabric
End User Devices



Fabric Border Nodes

Internal Border Node

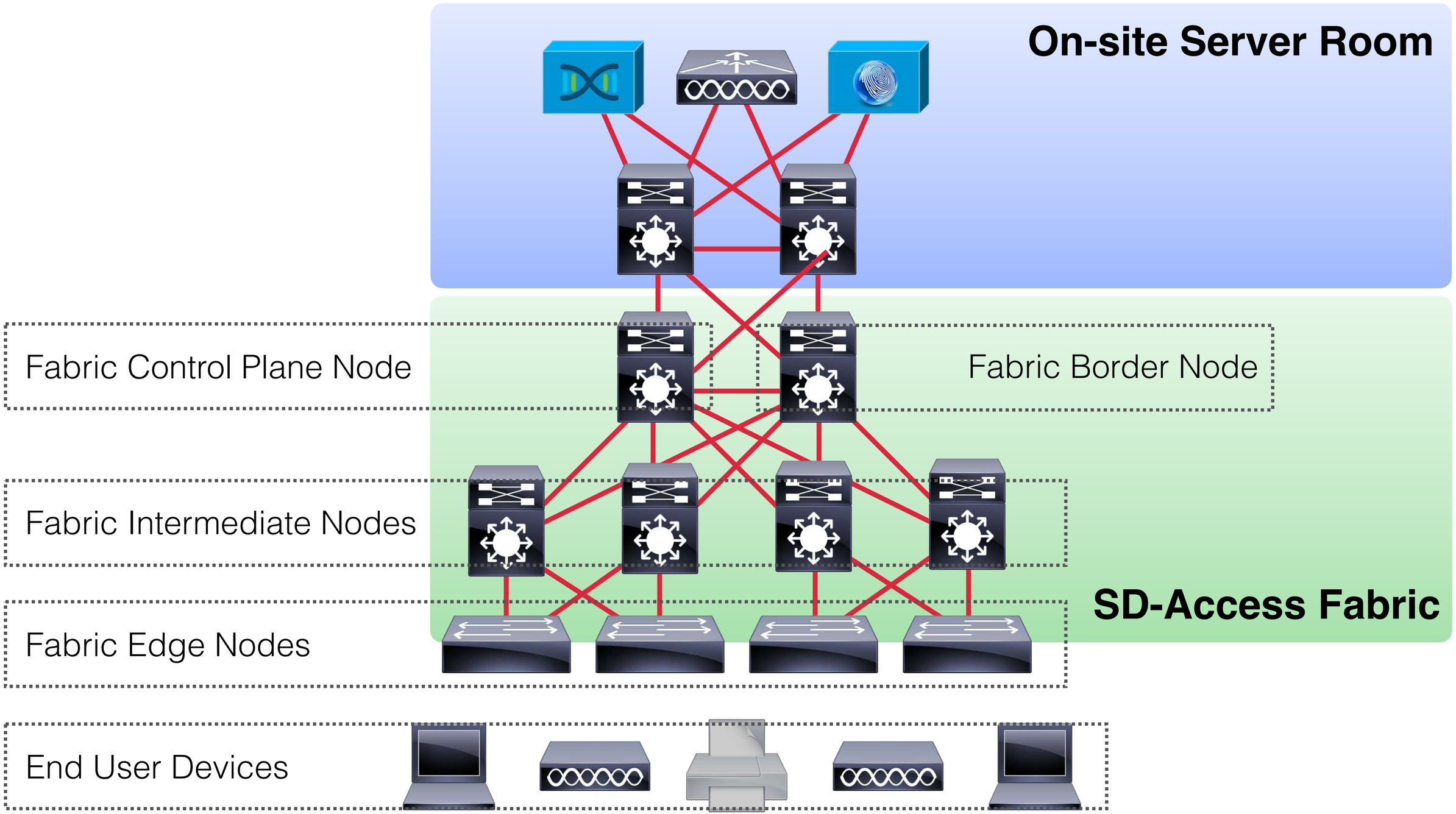
- Connects only to known areas or the organization

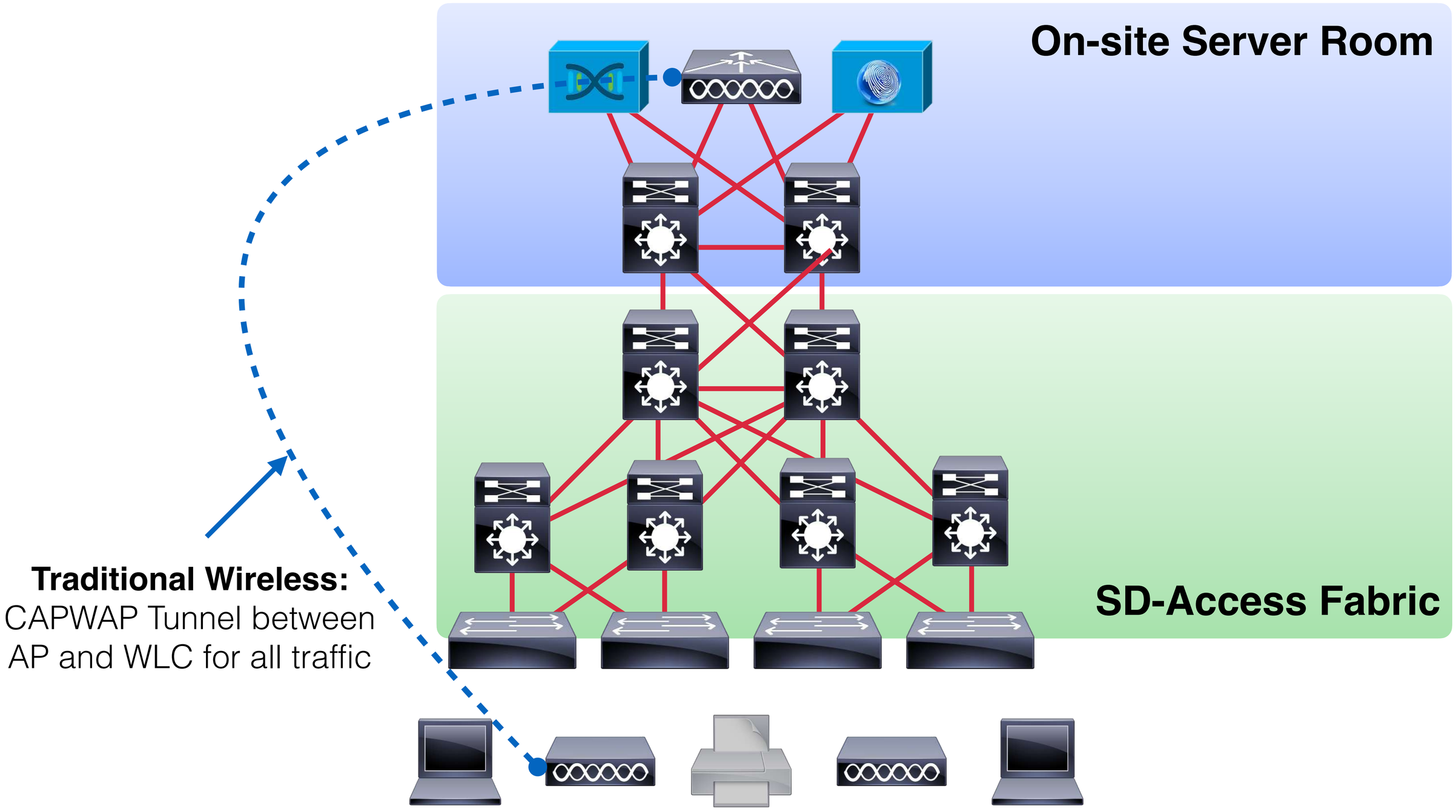
Default Border Node

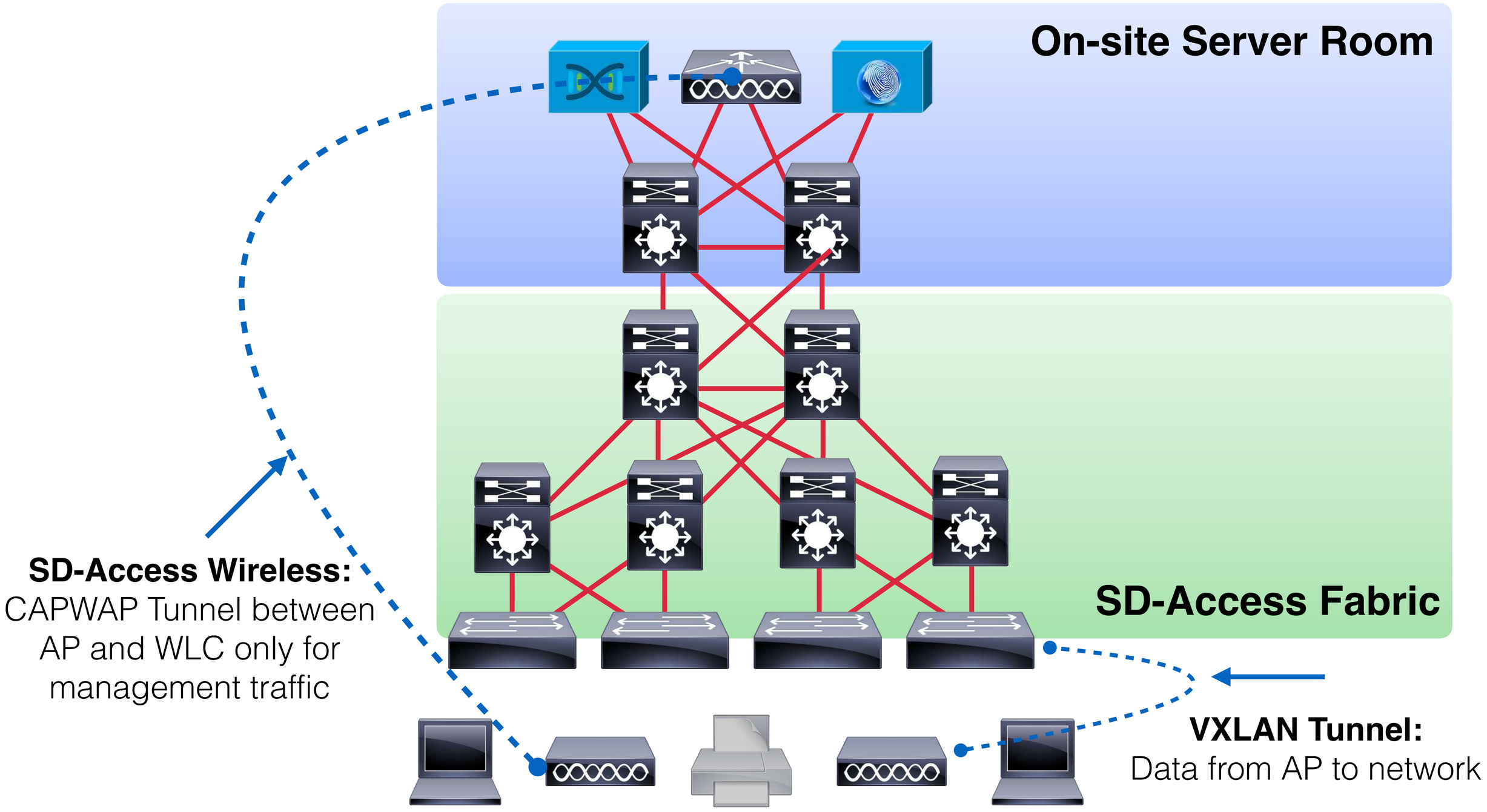
- Connects only to unknown external networks

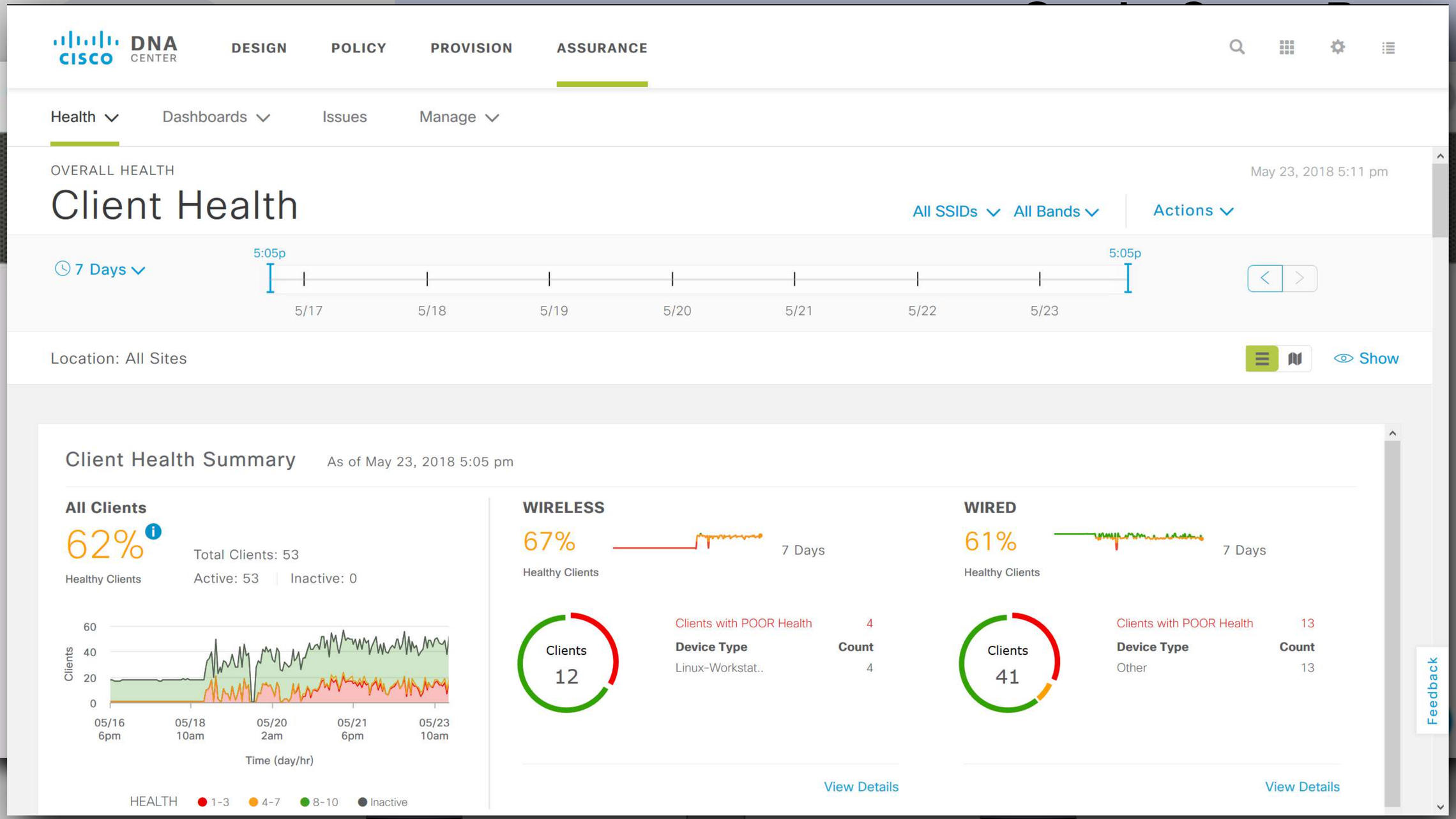
Anywhere Border Node

- Connectivity to both inside and outside public networks


On-site Server Room
Fabric Control Plane Node
Fabric Border Node
Fabric Intermediate Nodes
Fabric Edge Nodes
SD-Access Fabric
End User Devices

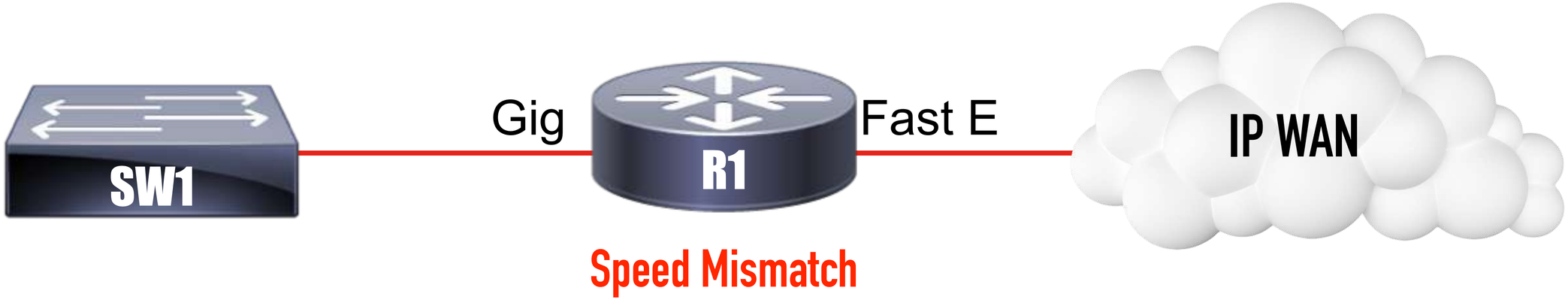

On-site Server Room
SD-Access Fabric
Traditional Wireless:
CAPWAP Tunnel between
AP and WLC for all traffic

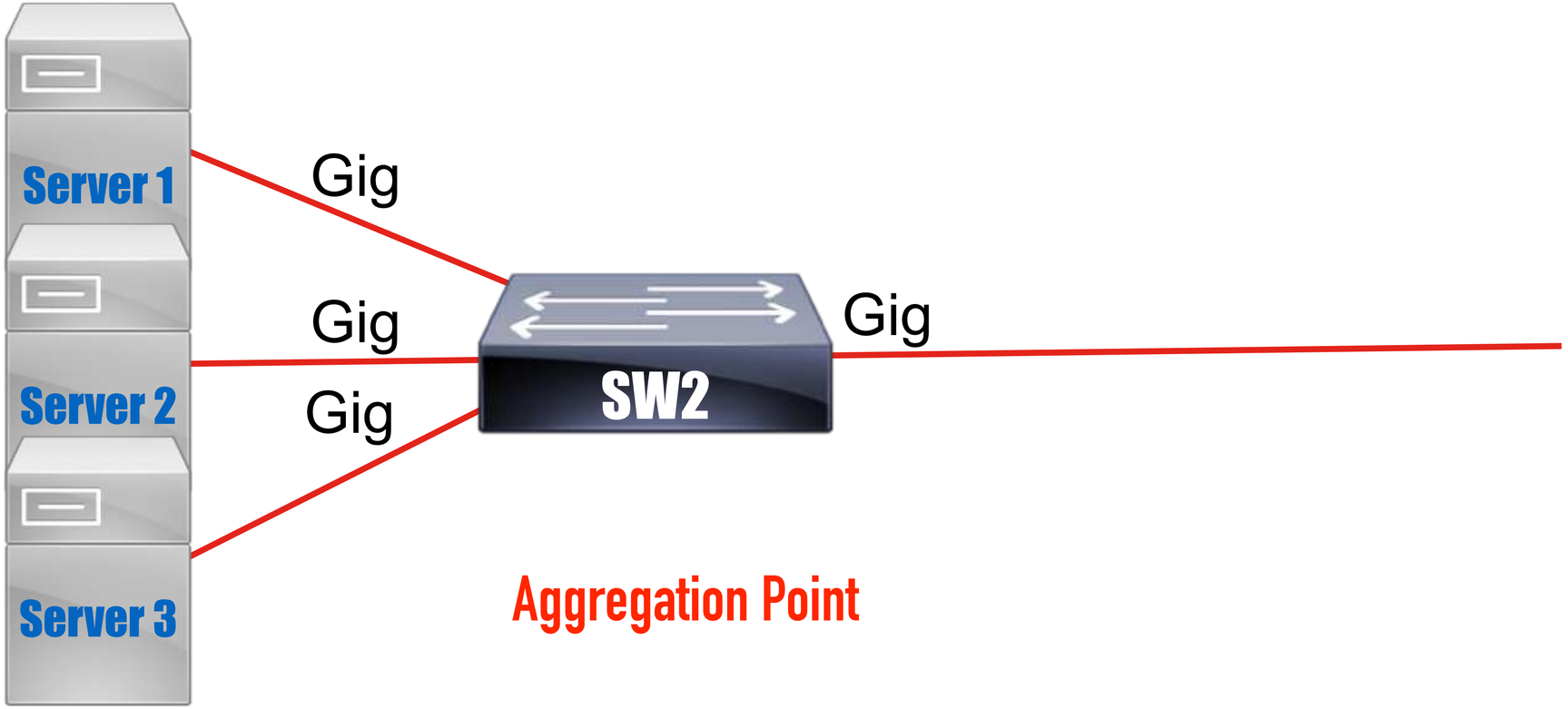

On-site Server Room
SD-Access Fabric
SD-Access Wireless:
CAPWAP Tunnel between AP and WLC only for management traffic
VXLAN Tunnel:
Data from AP to network


DNA CENTER
DESIGN
POLICY
PROVISION
ASSURANCE
Health
Dashboards
Issues
Manage
OVERALL HEALTH
May 23, 2018 5:11 pm
Client Health
All SSIDs
All Bands
Actions
7 Days
5:05p
5:05p
5/17
5/18
5/19
5/20
5/21
5/22
5/23
Location: All Sites
Show
Client Health Summary
As of May 23, 2018 5:05 pm
All Clients
62%
Healthy Clients
Total Clients: 53
Active: 53
Inactive: 0
Clients
60
40
20
0
05/16 6pm
05/18 10am
05/20 2am
05/21 6pm
05/23 10am
Time (day/hr)
HEALTH
1-3
4-7
8-10
Inactive
WIRELESS
67%
Healthy Clients
7 Days
Clients
12
Clients with POOR Health
4
Device Type
Count
Linux-Workstat..
4
View Details
WIRED
61%
Healthy Clients
7 Days
Clients
41
Clients with POOR Health
13
Device Type
Count
Other
13
View Details
Feedback

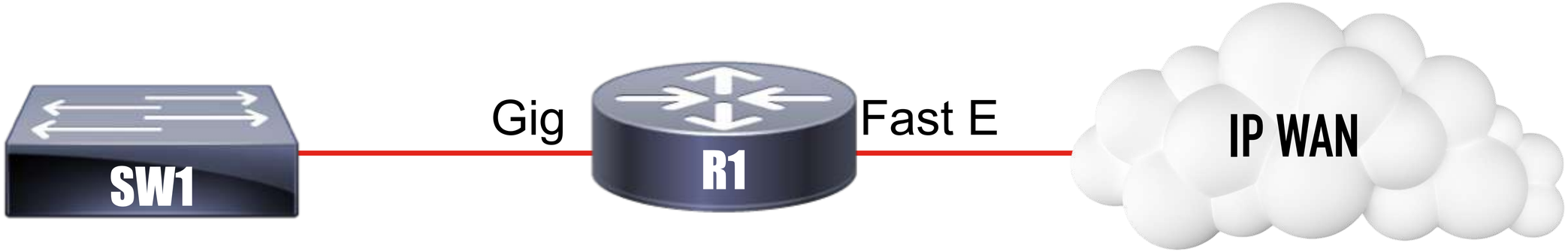
Quality of Service (QoS)

Do You Need QoS?

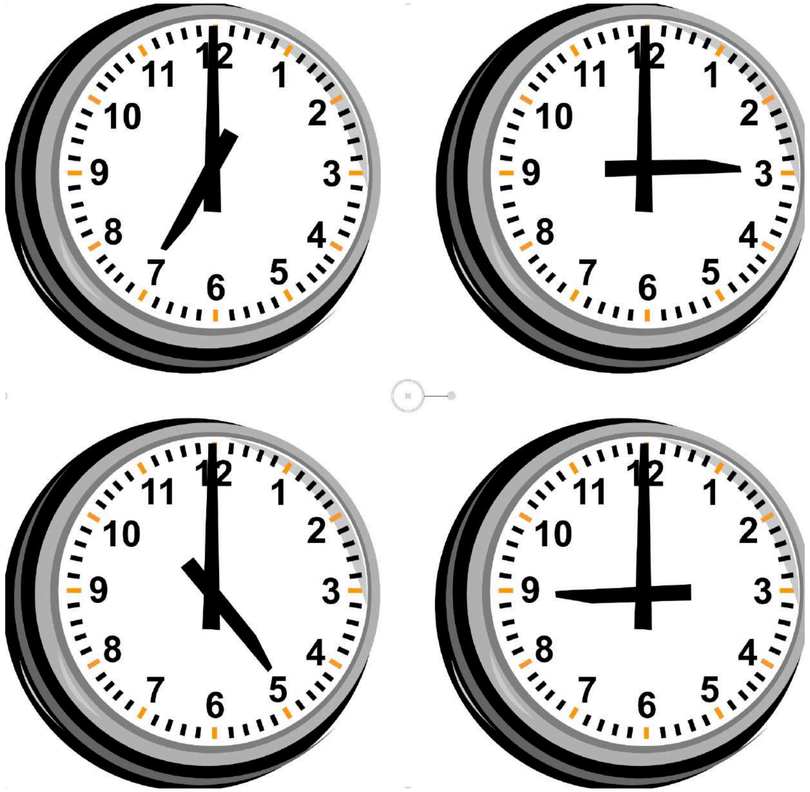




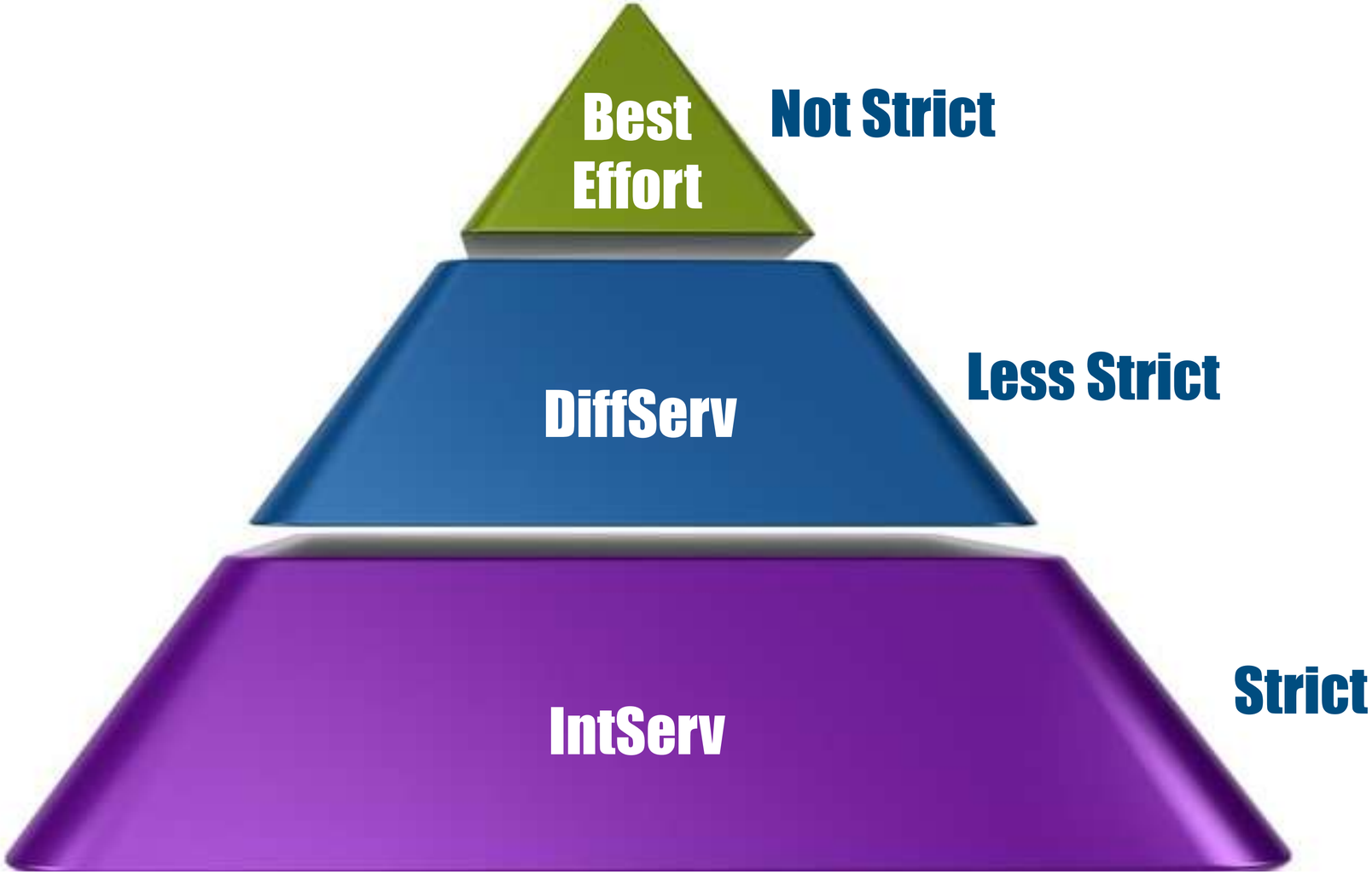
Do You Need QoS?



Periodic Congestion



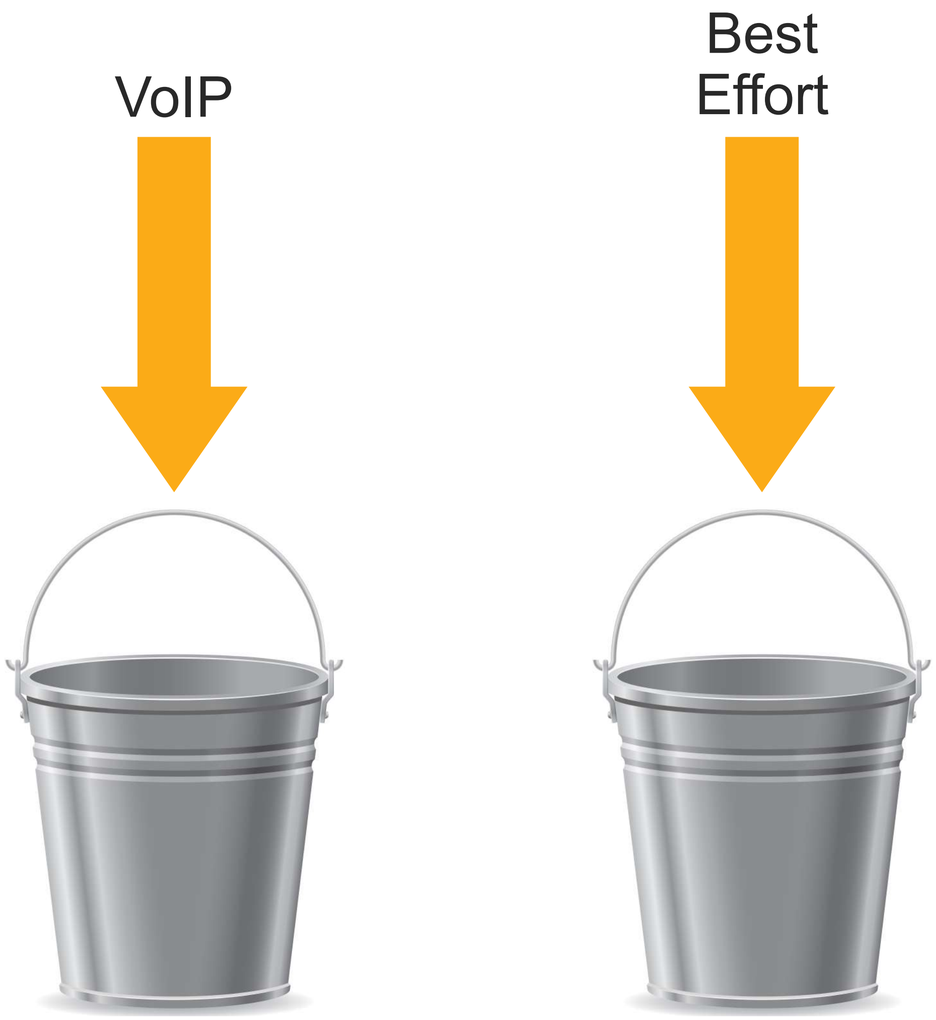
3 Categories of QoS



Common QoS Mechanisms

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

Common QoS Mechanisms



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

Common QoS Mechanisms

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

Common QoS Mechanisms

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

Common QoS Mechanisms

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

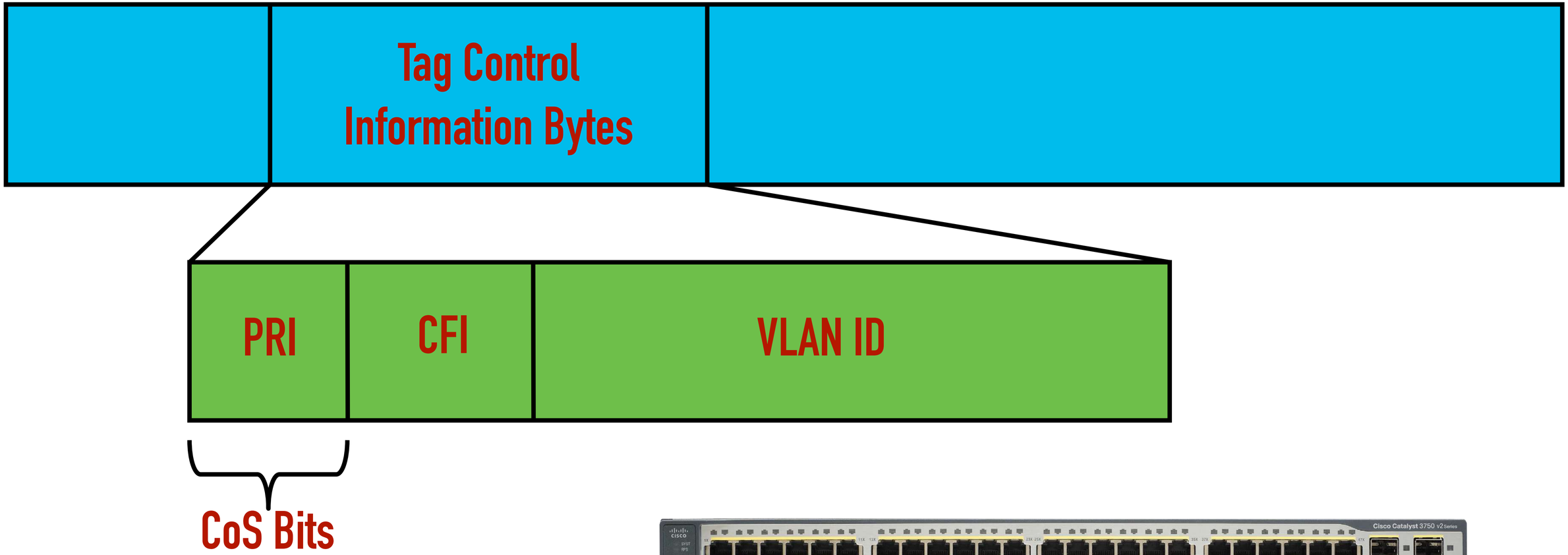
Wi-Fi Multimedia (WMM)

- IEEE 802.1P markings map to WMM access categories
- Access category determines Interframe Space (IFS) and Random Backoff Timer

4 Access Categories	802.1P
AC_VO (Voice)	6 & 7
AC_VI (Video)	4 & 5
AC_BE (Best Effort)	0 & 3
AC_BK (Background)	1 & 2

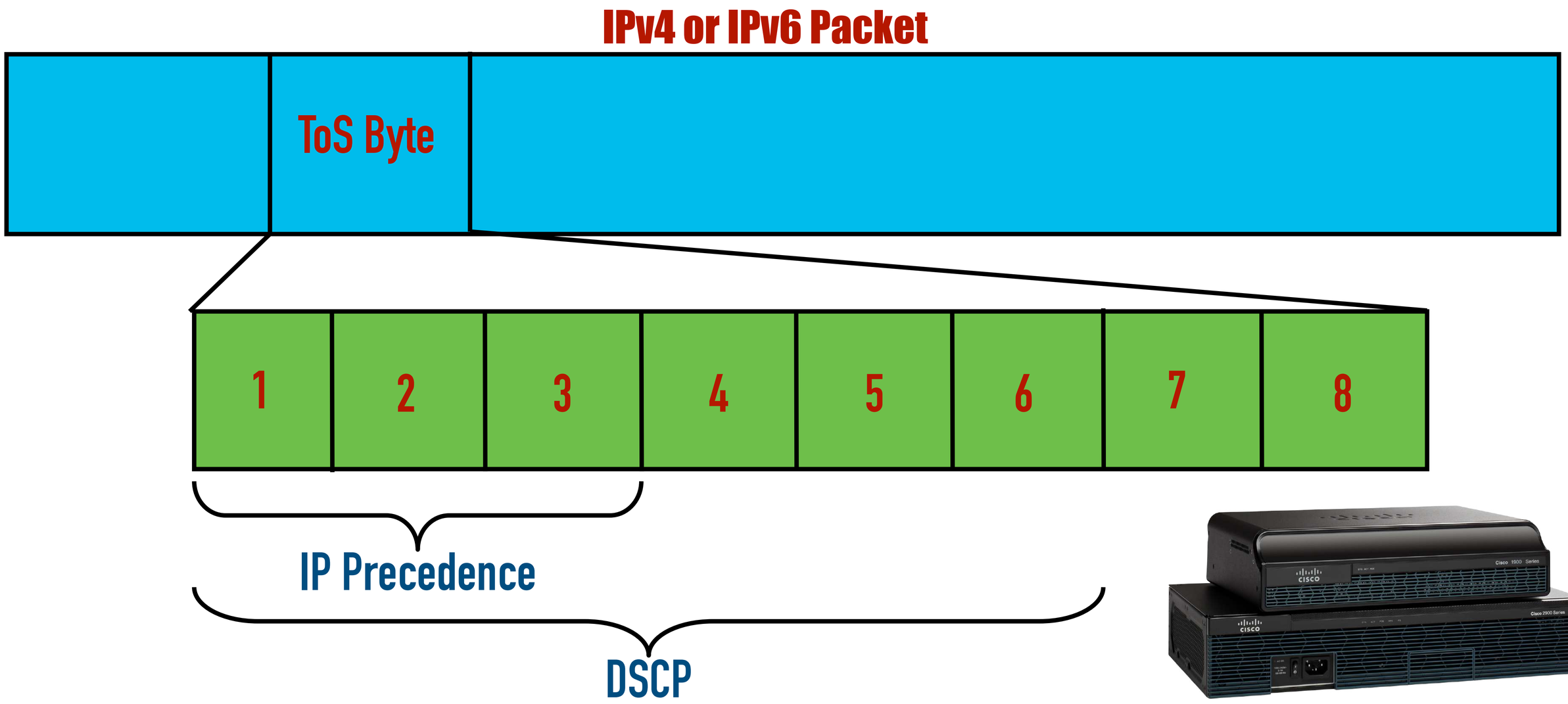
Class of Service (CoS)

IEEE 802.1Q Frame

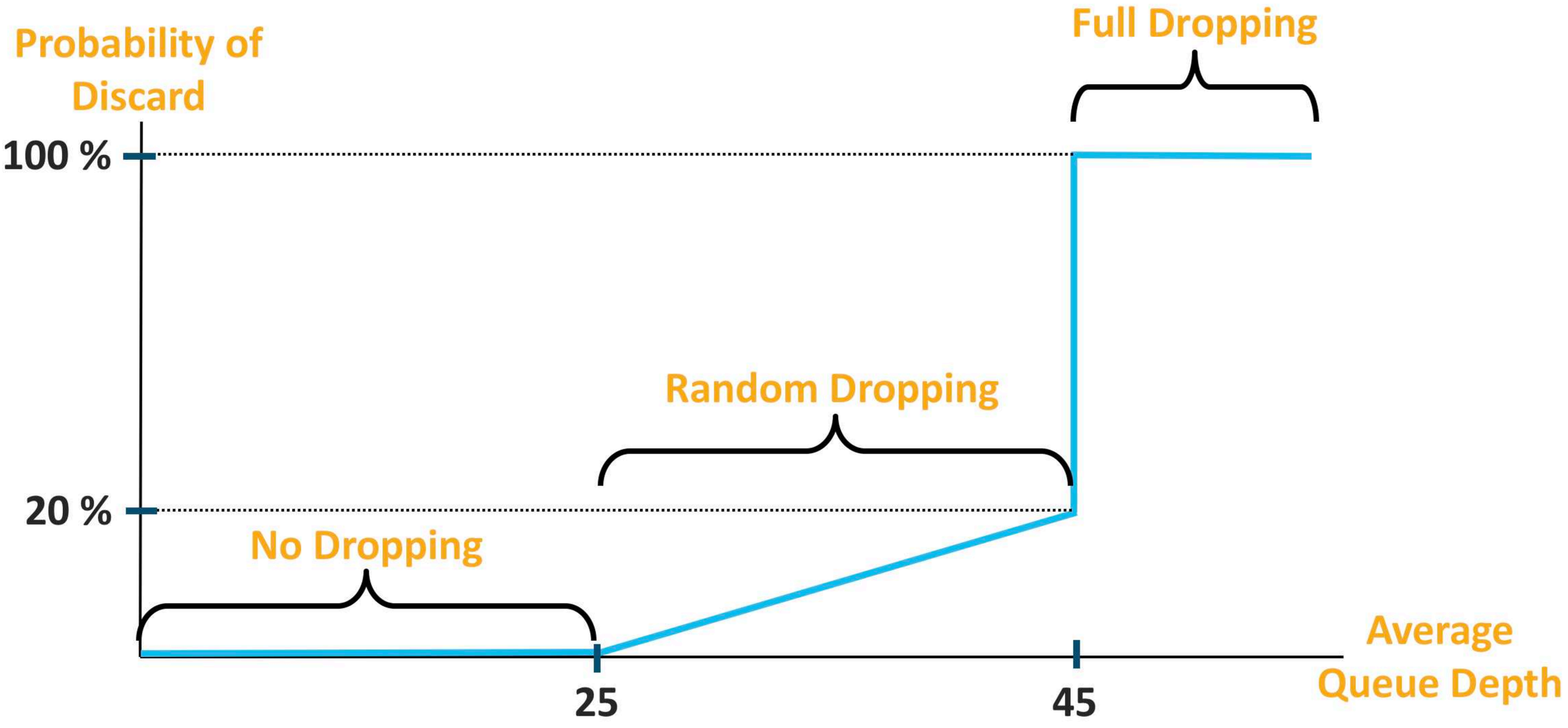


Type of Service (ToS) Byte

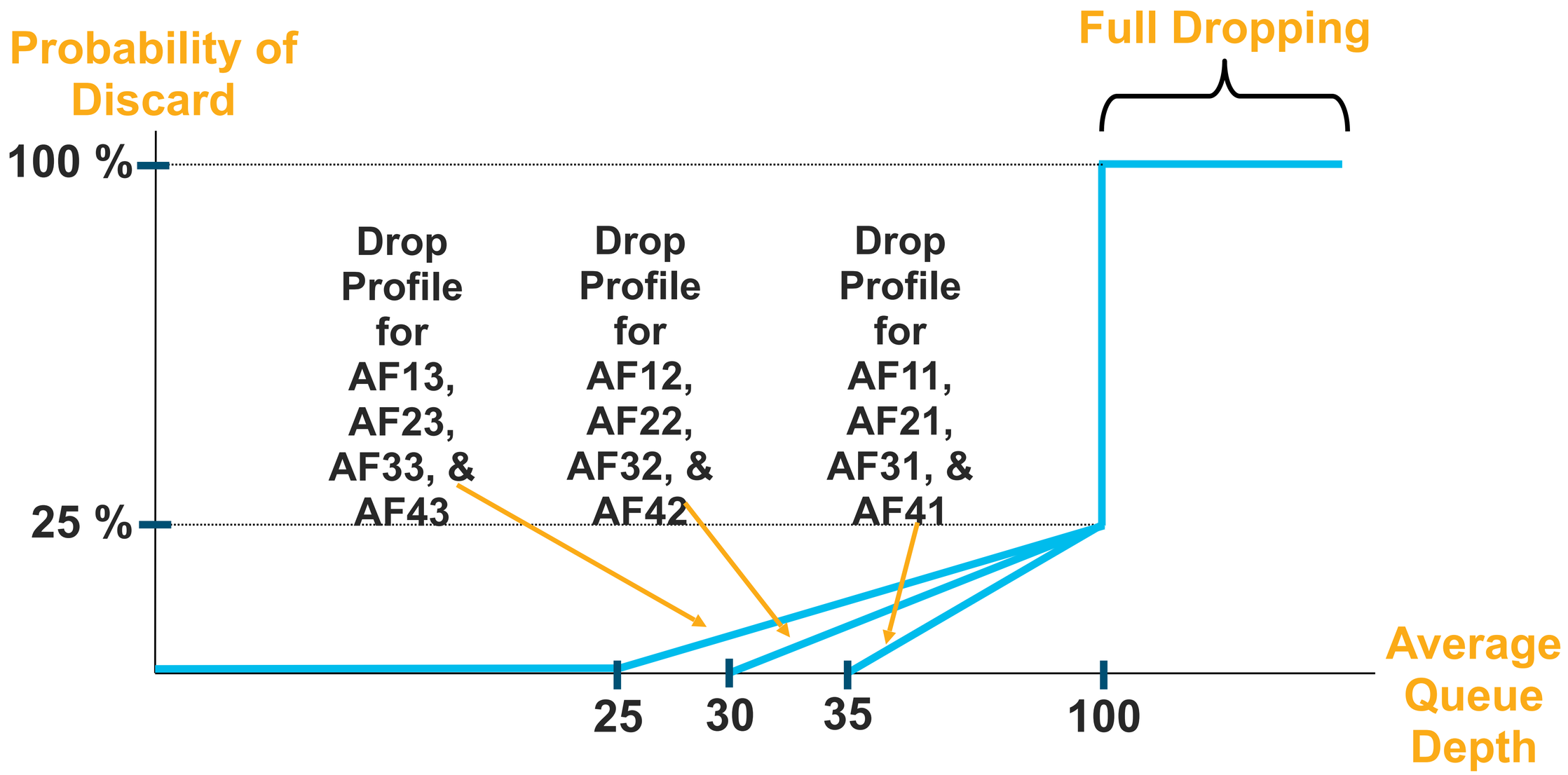
Traffic Class Byte in IPv6



RED Drop Ranges



RED Profiles

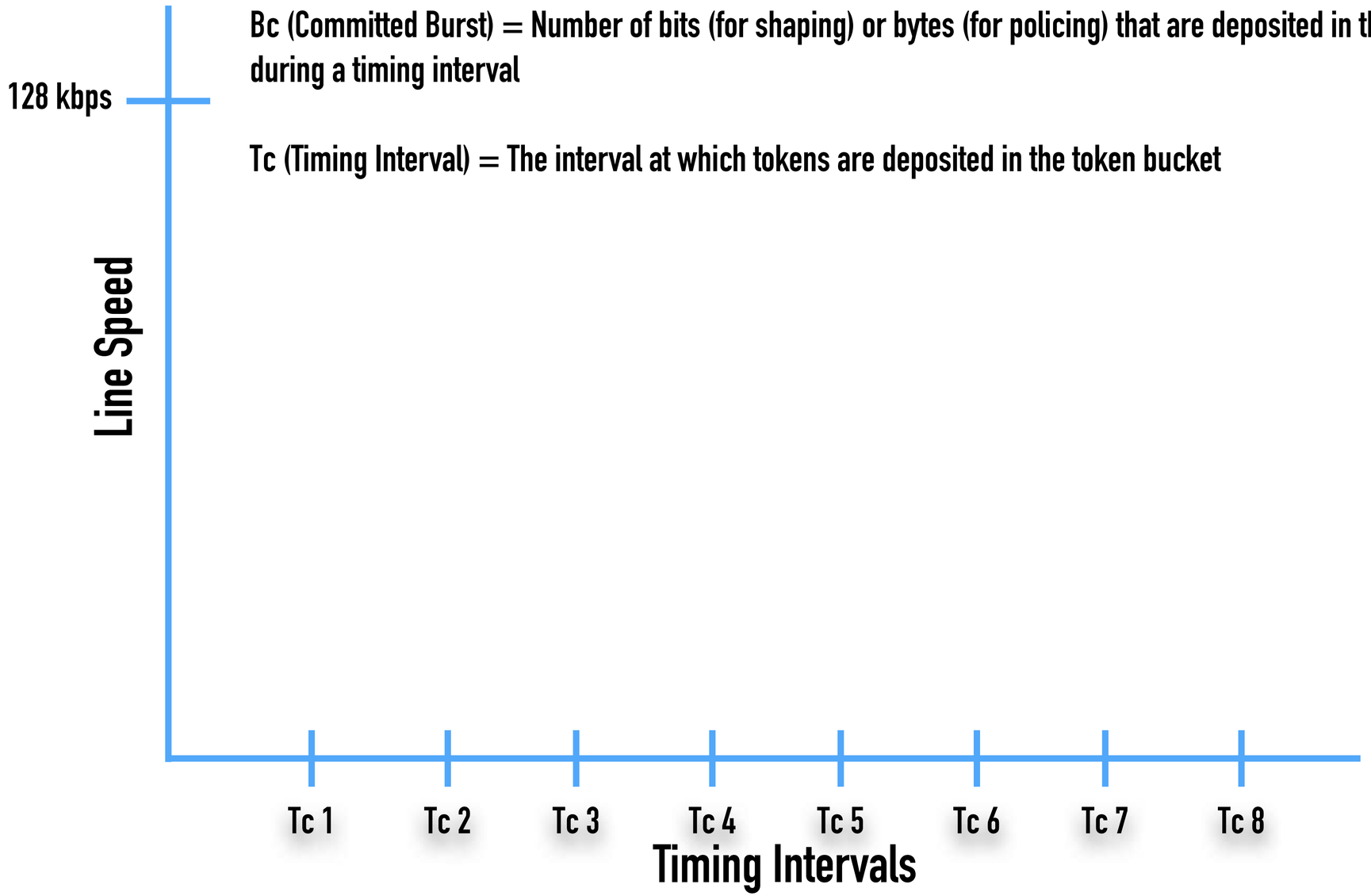


CIR = Bc / Tc

CIR (Committed Information Rate) = AVERAGE speed over the period of a second

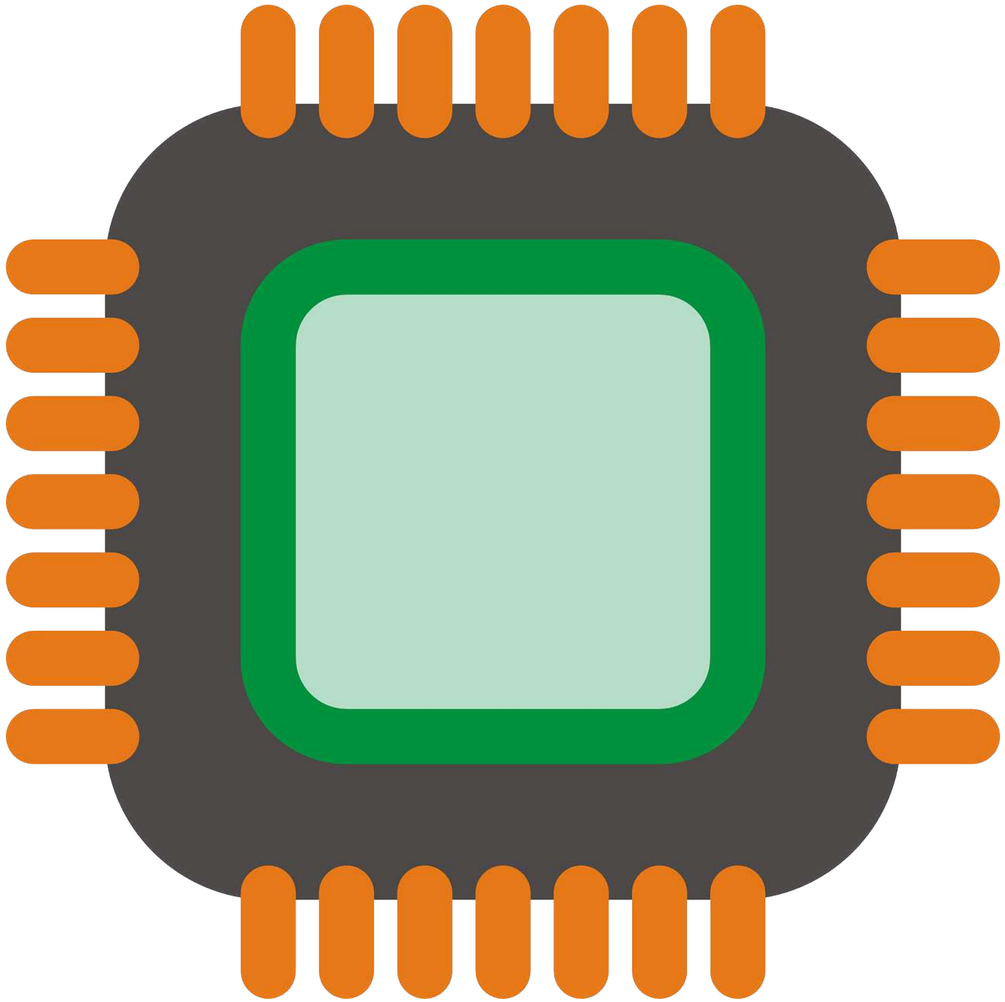
Bc (Committed Burst) = Number of bits (for shaping) or bytes (for policing) that are deposited in the token bucket during a timing interval

Tc (Timing Interval) = The interval at which tokens are deposited in the token bucket



Switching Mechanisms

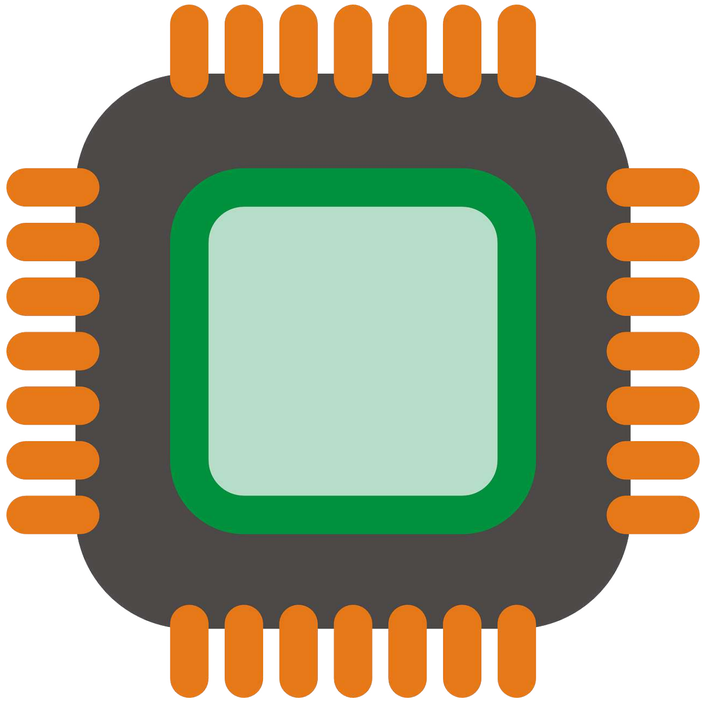
Process Switching



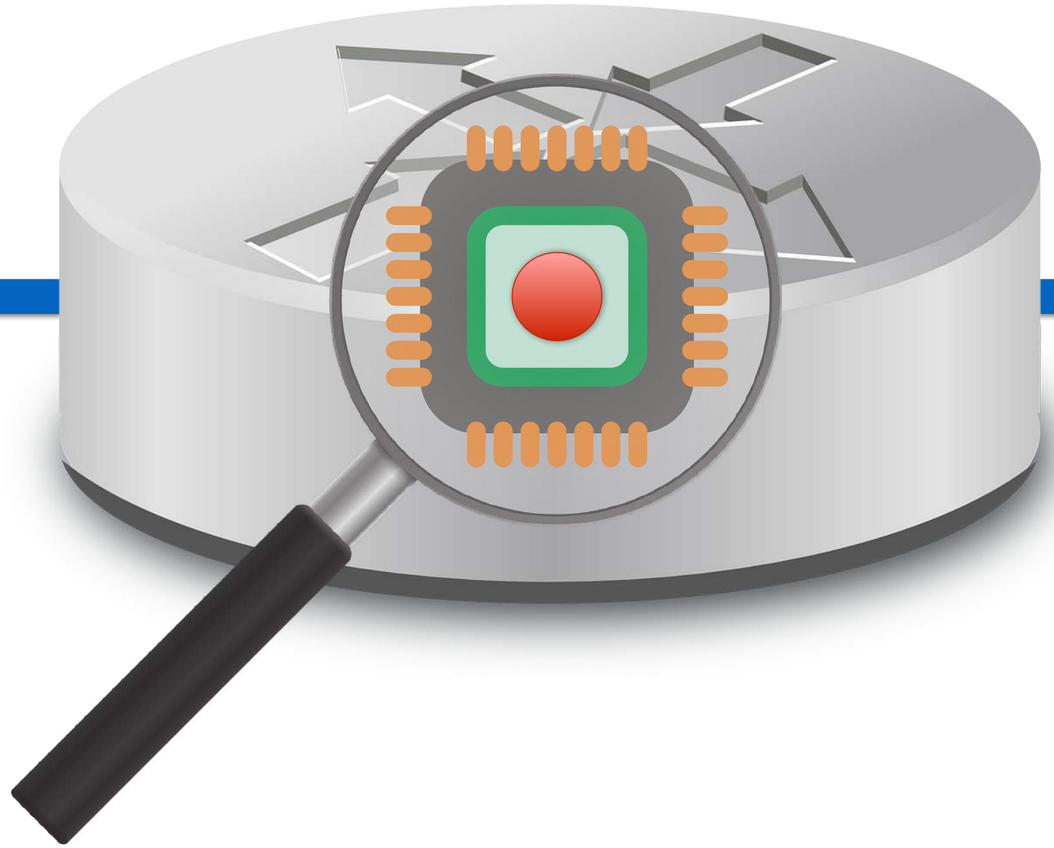
Process Switching

Process Switching:

- Oldest method for Cisco IOS switching
- Every packet is inspected by CPU



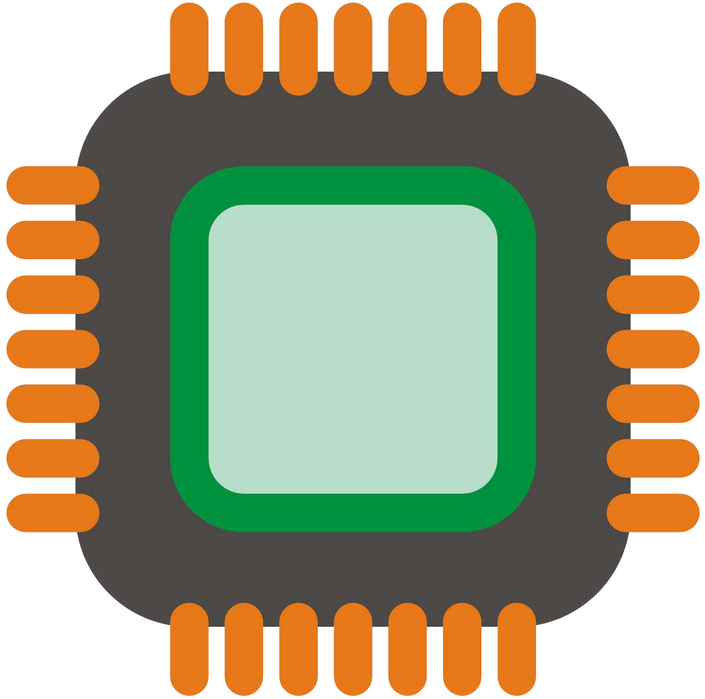
Process Switching



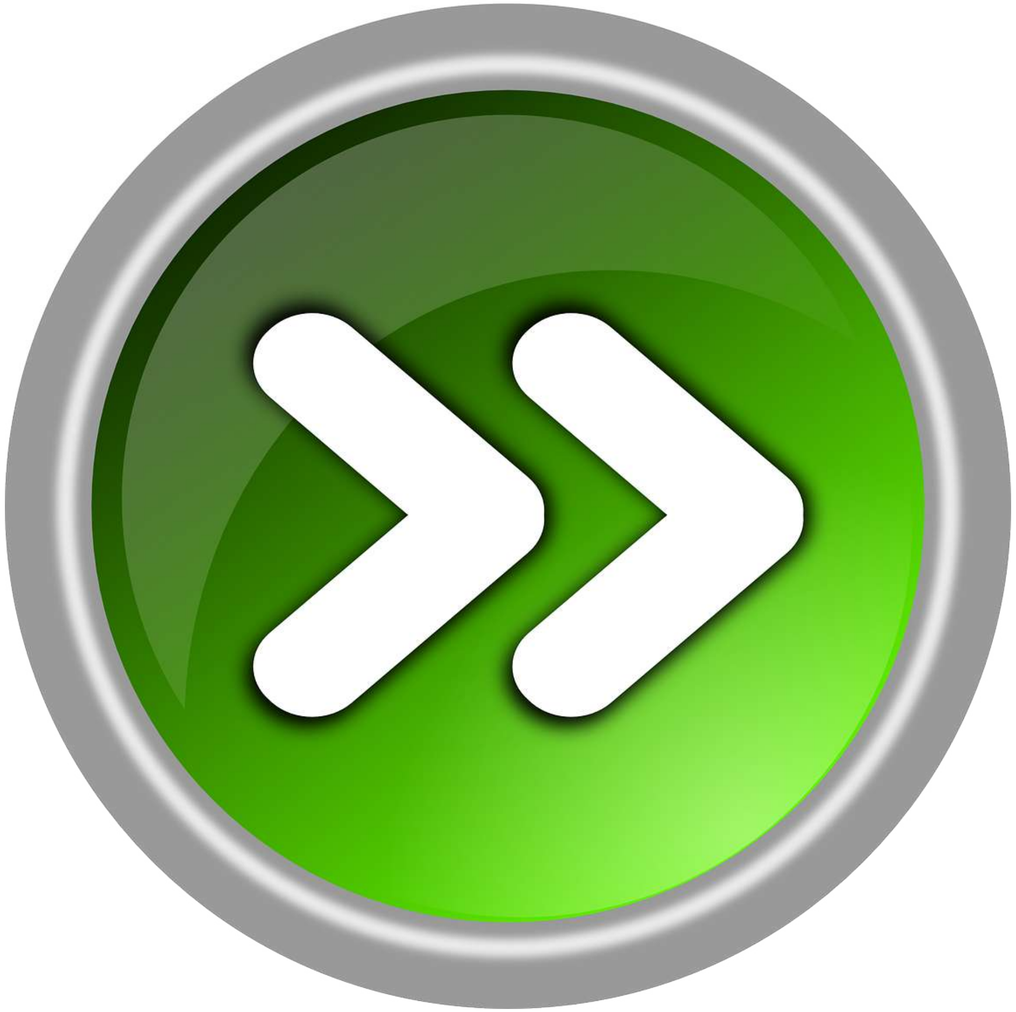
Process Switching

Process Switching:

- Processor is directly involved with every packet
- Not ideal in modern networks
- Available on every Cisco router platform
- Debugging uses process switching



Cisco Express Forwarding (CEF)



Cisco Express Forwarding (CEF)

Cisco Express Forwarding (CEF):

- Most preferred Cisco IOS switching process
- Default in most modern Cisco IOS devices
- Optimized lookup and efficient packet handling

Cisco Express Forwarding (CEF)

CEF Benefits:

- Less CPU-intensive than older switching methods
- Distributed CEF (dCEF) allows line card forwarding
- CEF Forwarding Information Base (FIB)
- CEF Adjacency Table

Cisco Express Forwarding (CEF)

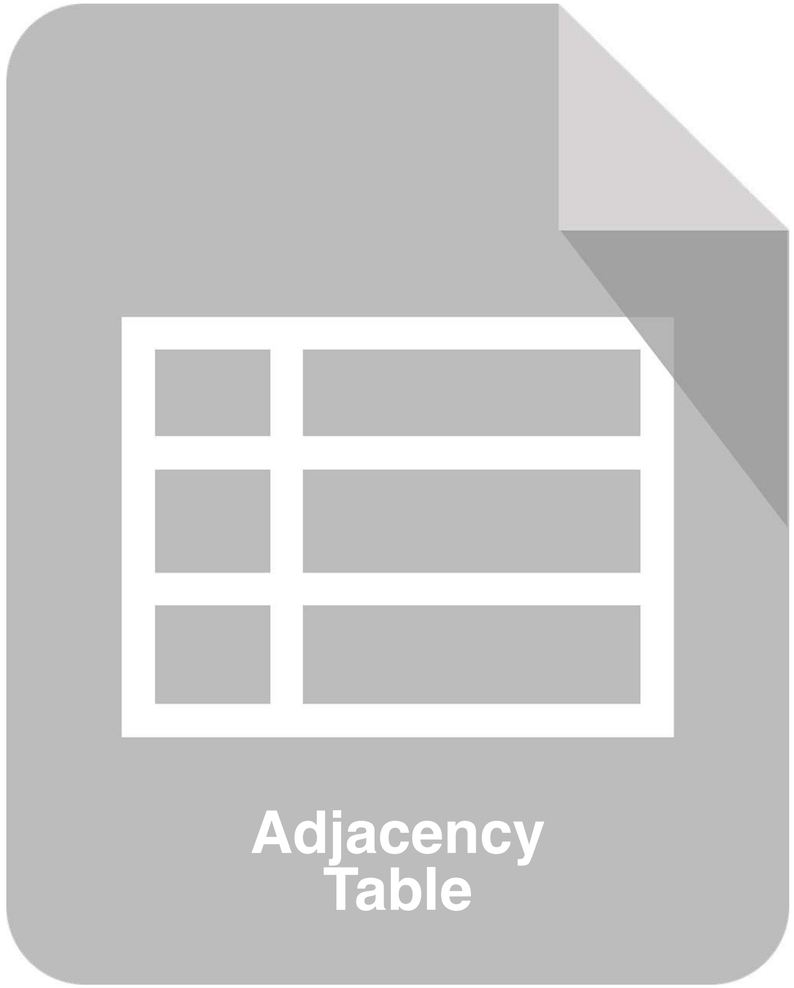
CEF Forwarding Information Base (FIB):

- Similar to a routing table
- FIB is updated with each routing table update
- Processor is not involved with route lookup
- FIB is a more efficient lookup structure

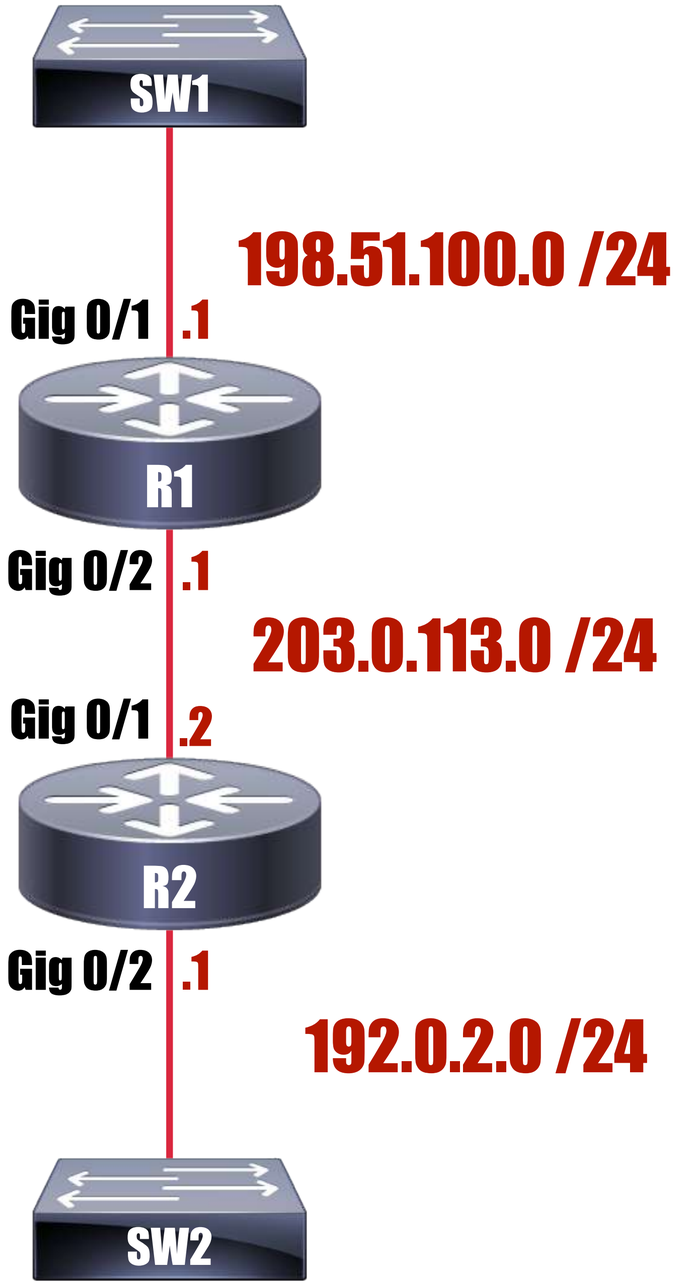
Cisco Express Forwarding (CEF)

CEF Adjacency Table:

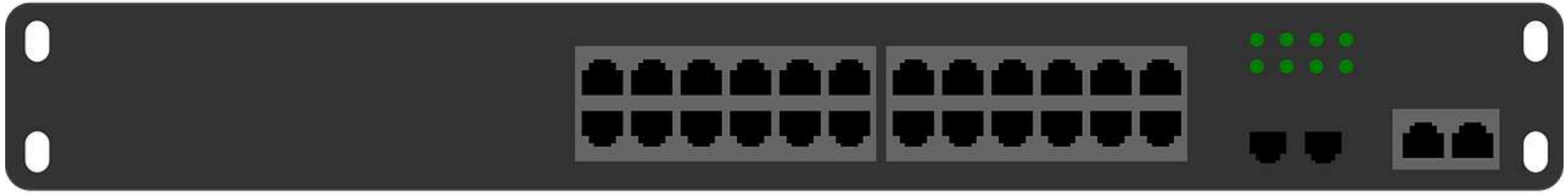
- Information about directly connected devices
- Adjacency = reachable via single link-layer hop
- Layer 2 next-hop address maintained in table



CEF Demo


SW1
198.51.100.0 /24
Gig 0/1
.1
R1
Gig 0/2
.1
203.0.113.0 /24
Gig 0/1
.2
R2
Gig 0/2
.1
192.0.2.0 /24
SW2

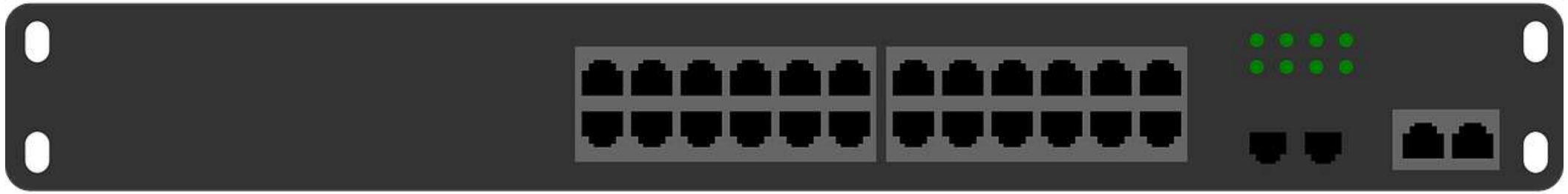
CAM vs. TCAM



CAM vs. TCAM

Content Addressable Memory (CAM)

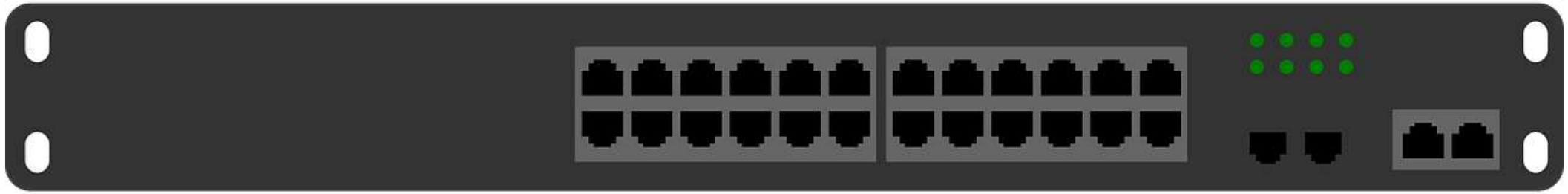
- Layer 2 switching
- Source MAC addresses recorded in CAM table
- Used to determine ports for frame delivery



CAM vs. TCAM

Content Addressable Memory (CAM)

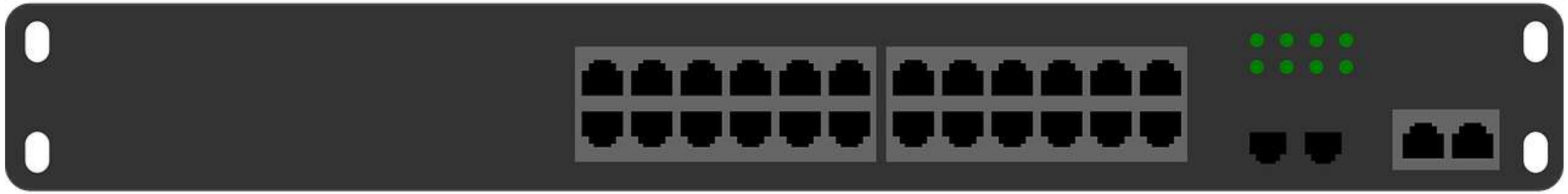
- Arrival port number, source MAC address, and arrival timestamp
- Stale entries removed after aging timer expires
- Default aging timer is 300 seconds
- **Switch(config)#***mac address-table aging-time <seconds>*



CAM vs. TCAM

Content Addressable Memory (CAM)

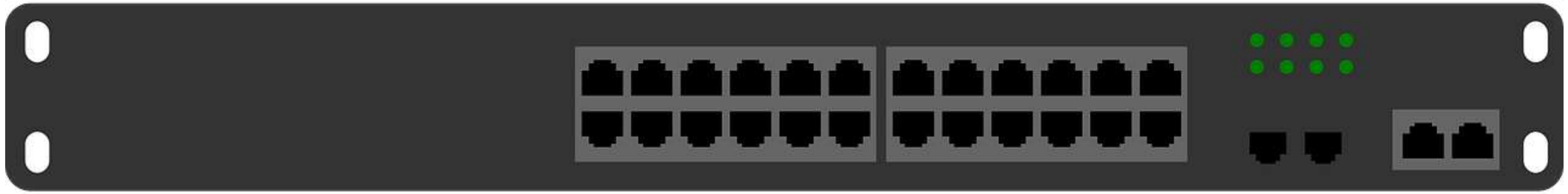
- True (1) or False (0) value returned upon lookup
- Searches for exact binary match



CAM vs. TCAM

Ternary Content Addressable Memory (TCAM):

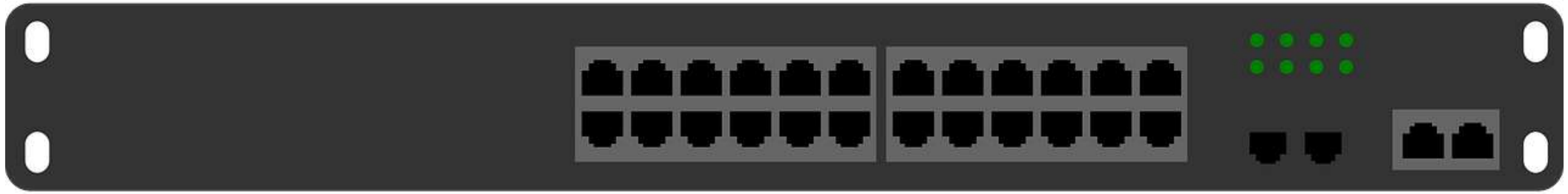
- Some L2 switches use TCAM for QoS
- Primarily a multilayer switch component
- Access Control Lists (ACLs) commonly use TCAM



CAM vs. TCAM

Ternary Content Addressable Memory (TCAM):

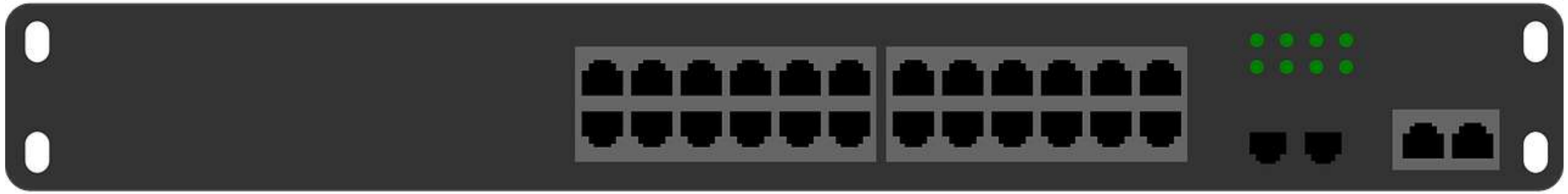
- Extension of the Content Addressable Memory (CAM)
- Returns True (1), False (0), or Do Not Care (X)
- Ternary = mathematical value based in three



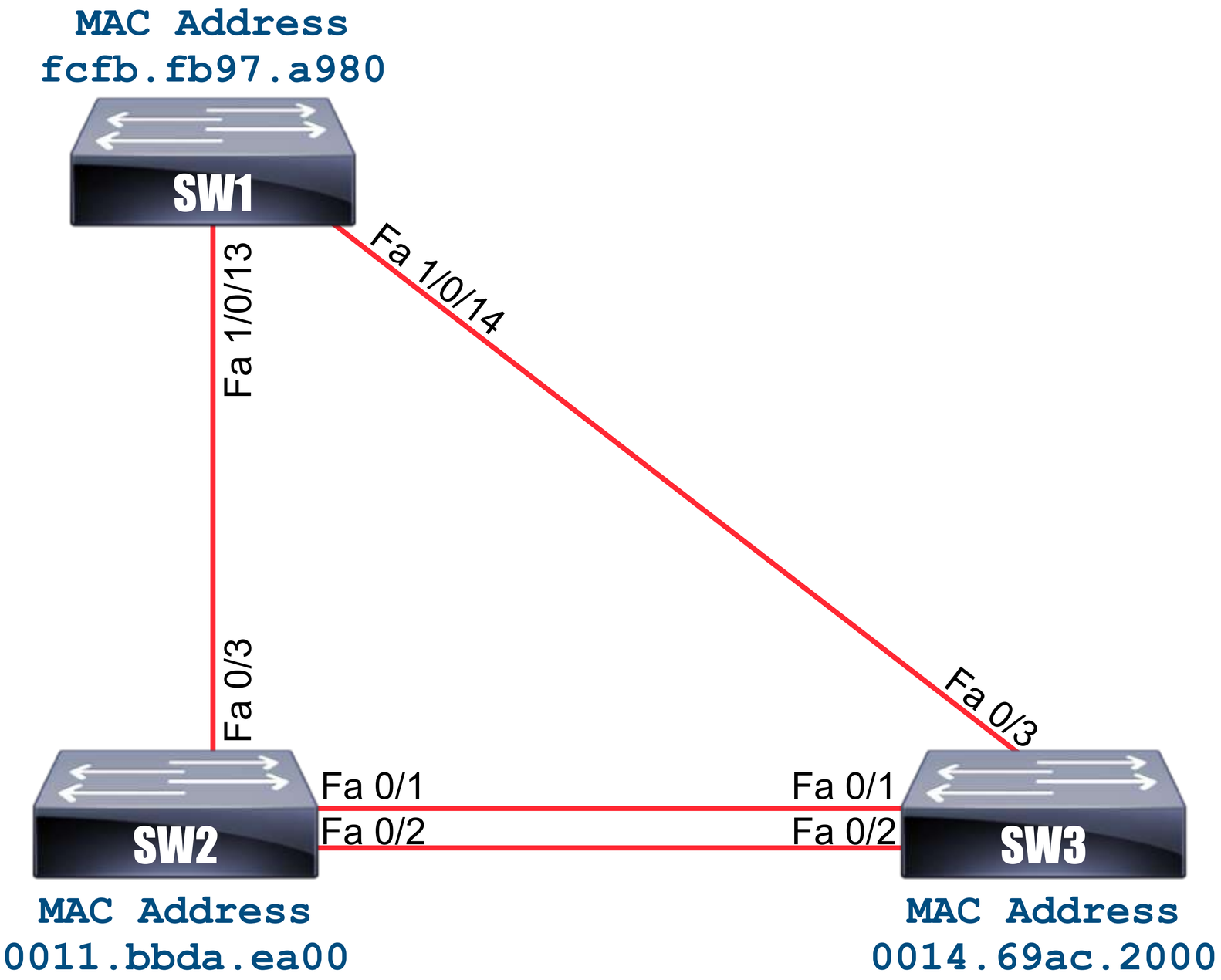
CAM vs. TCAM

Ternary Content Addressable Memory (TCAM):

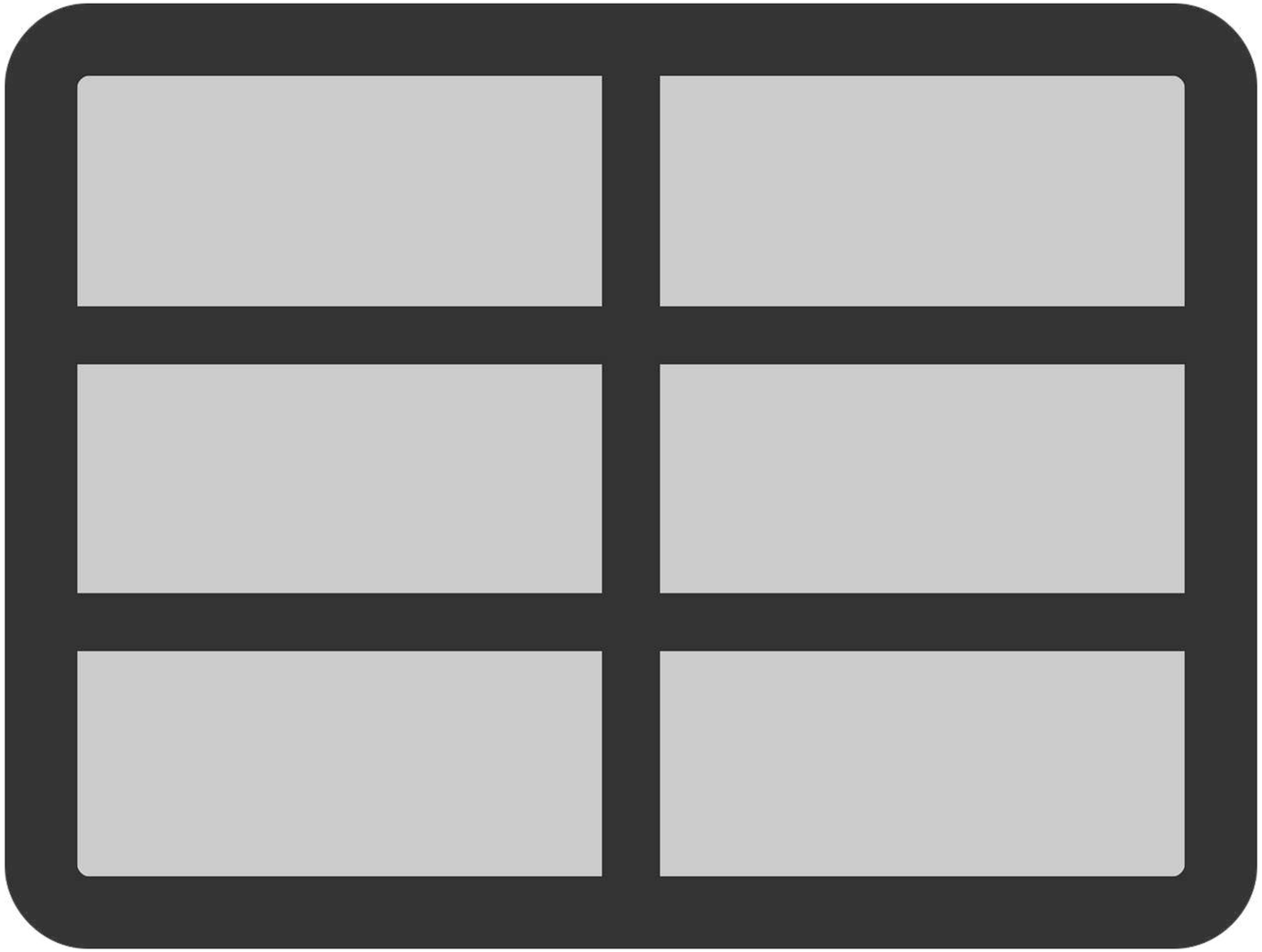
- TCAM uses VMR format (value, mask, and result)
- Value = IP addresses, protocol ports, etc.
- Mask = mask bits associated with matching values
- Result = permit, deny, QoS policing, etc.



CAM and TCAM Demo



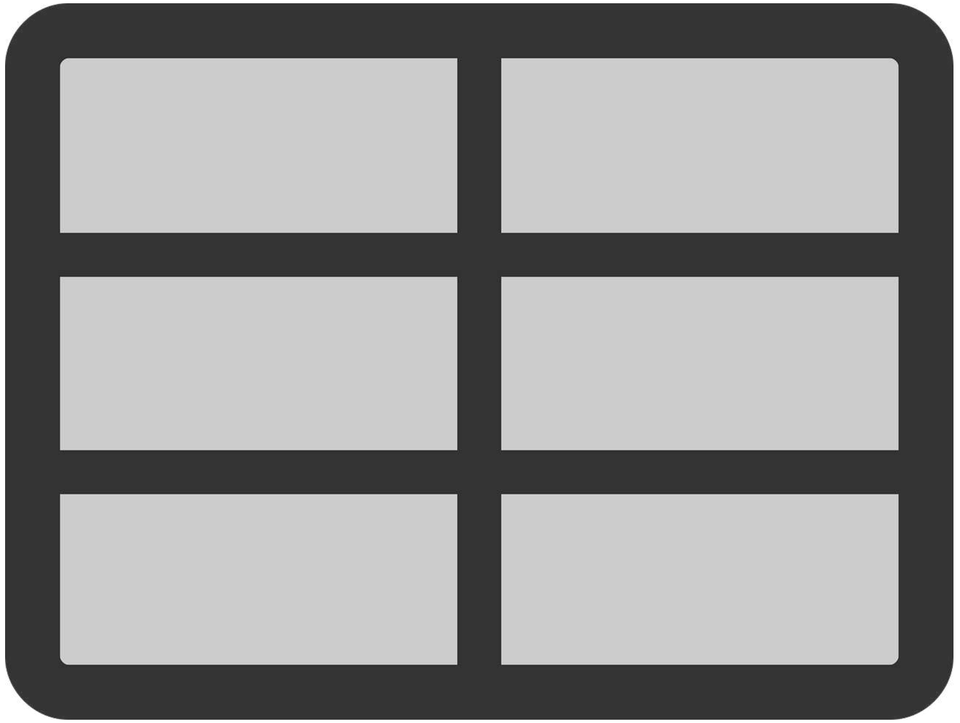
FIB vs. RIB



FIB vs. RIB

Forwarding Information Base (FIB)

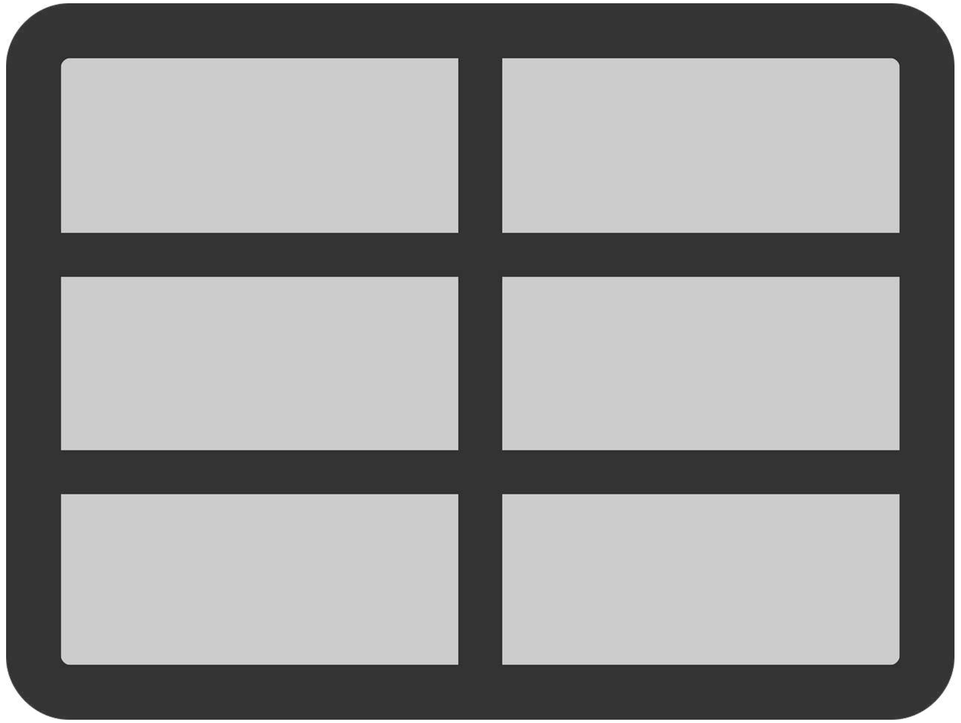
- IP forwarding table or CEF table
- IP destination prefix-based switching decisions



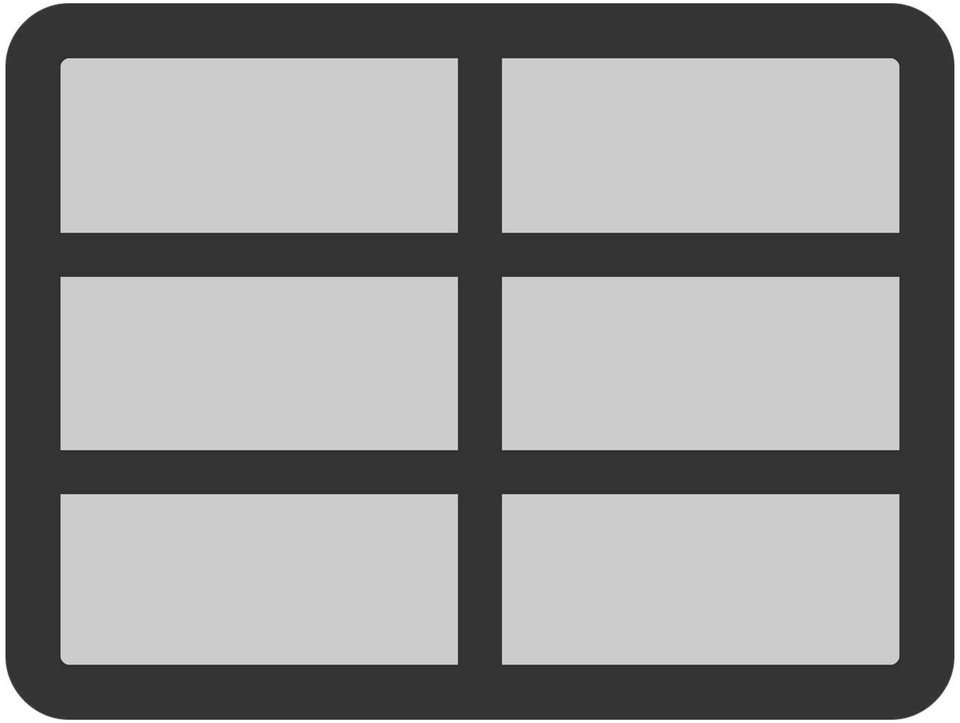
FIB vs. RIB

Forwarding Information Base (FIB)

- FIB capacity can dictate forwarding efficiency
- Modern ASICs provide line-speeds
- dCEF offloads the FIB to line card modules



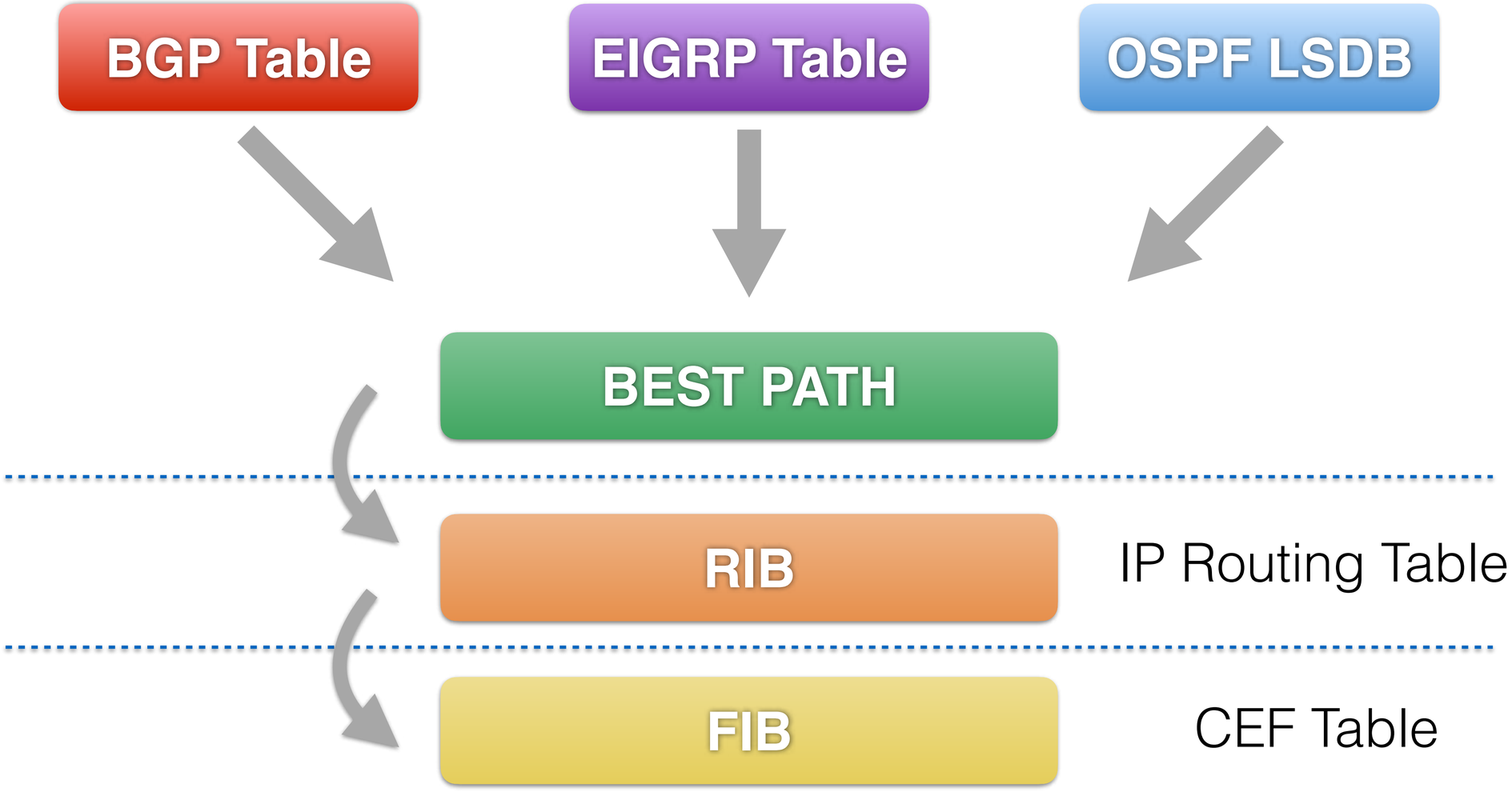
FIB vs. RIB



Routing Information Base (RIB)

- IP routing related information stored
- Used by all routing protocols (OSPF, BGP, etc.)
- Learned routes inserted into RIB
- Unreachable routes removed and RIB updated
- Dynamic, static, and directly connected routes

FIB vs. RIB


BGP Table
EIGRP Table
OSPF LSDB
BEST PATH
RIB
IP Routing Table
FIB
CEF Table