Moderná sieťová infraštruktúra a jej dizajn

Aktuálne trendy v informatike

Peter Mesjar, Systems Engineer, CCIE 17428

pmesjar@cisco.com

Apríl 2017

The Challenge.

I want to design and deploy a network.

How can I anticipate what the network might need to do in the future so I don't have to revisit my design and deployment?

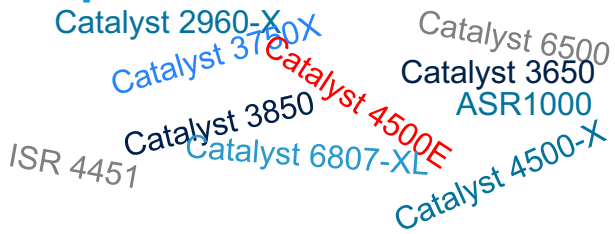
How can I do it quickly?

How do I manage it?

How do I put it all together?

Which platform should I choose?

Many to choose from at each place in the network



What are the best practices?

Next-Generation Campus Design

Unified Communications Evolution

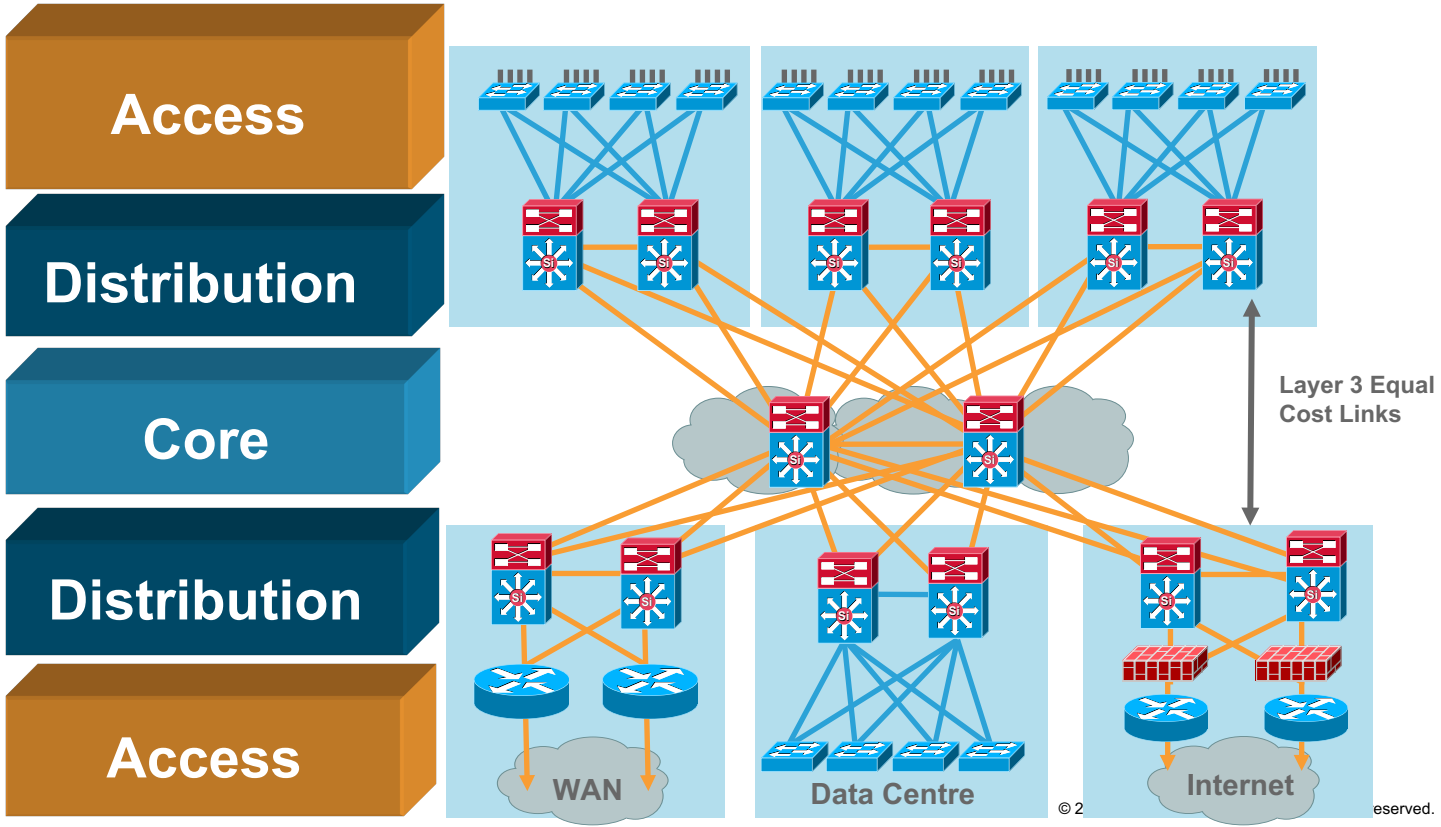
- VoIP and Video is now a mainstream technology
- Ongoing evolution to the full spectrum of Unified Communications
- High-definition executive communication application requires stringent Service-Level Agreement (SLA)
  - Reliable service—high availability infrastructure
  - Application service management—QoS

The New Normal

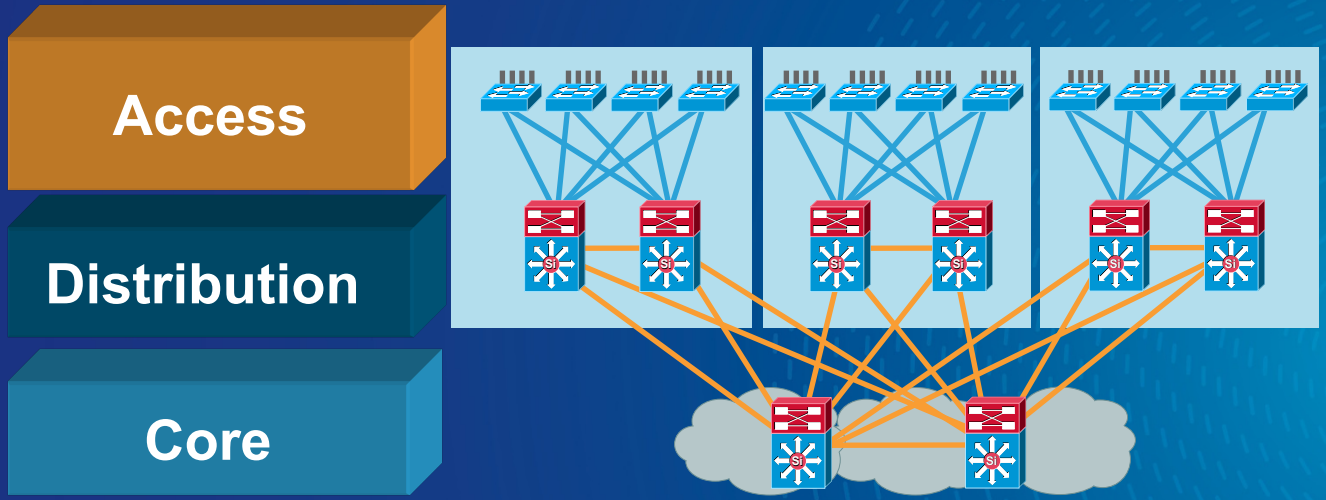
High-Availability Campus Design

Structure, Modularity, and Hierarchy

www.cisco.com/go/cvd/campus

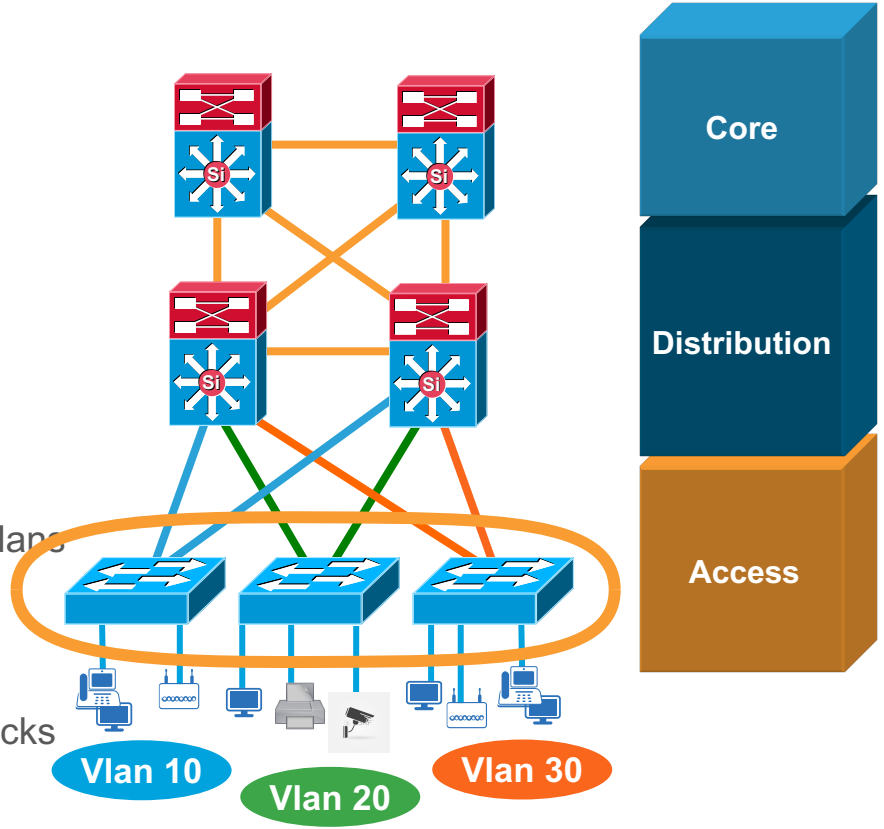


Agenda for today – starting with Access layer



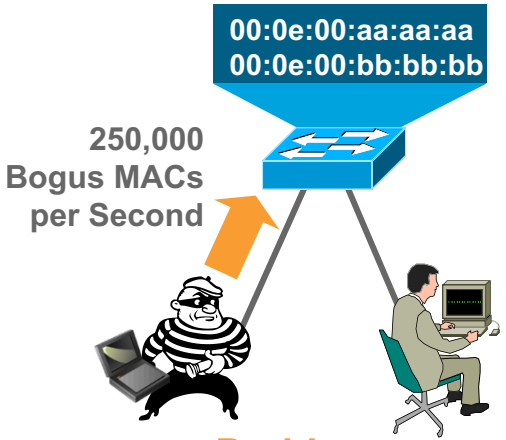
Access Layer Design

- Not only about connecting PCs
  - Application Visibility is also important
- Ethernet network access
  - Wired 10/100/1000/mGig(802.3bz)
  - Supports Wireless LAN 802.11a/b/g/n/ac access
- Simplified and flexible design
  - Layer 2 edge for applications that require spanned vlans
  - Avoid Spanning Tree loops for resiliency
- Policy enforcement point
  - Secure network and applications from malicious attacks
  - Identity based policies and packet marking
- Advanced Technologies support
  - Deliver PoE services: 802.3af(PoE), 802.3at(PoE+), Cisco Universal POE (UPOE) and 802.3bt
  - QoS enforcement to protect multimedia applications



Port Security

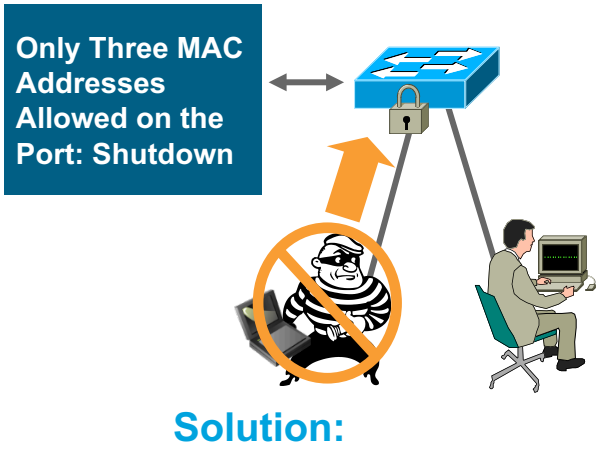
Cutting Off MAC-Based Attacks



Problem:

Script Kiddie Hacking Tools Enable Attackers Flood Switch CAM Tables with Bogus Macs; Turning the VLAN into a Hub and Eliminating Privacy

Switch CAM Table Limit Is Finite Number of Mac Addresses



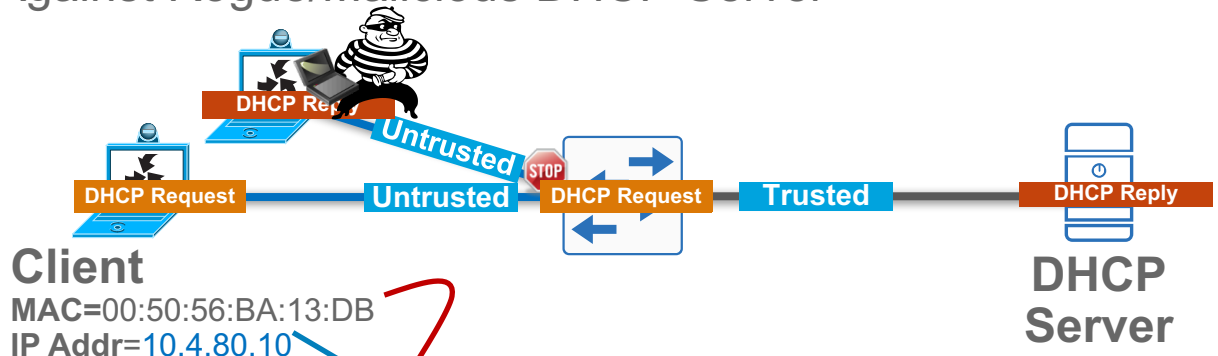
Solution:

Port Security Limits MAC Flooding Attack and Locks Down Port and Sends an SNMP Trap

```
switchport port-security
switchport port-security maximum 100
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

DHCP Snooping Binding Table

Protection Against Rogue/Malicious DHCP Server



Example DHCP Snooping Binding Table

MAC Address	IP Address	VLAN	Interface
00:50:56:BA:13:DB	10.4.80.10	10	GigabitEthernet2/0/1

Configure in the global configuration:

```
ip dhcp snooping vlan [data vlan], [voice vlan]
no ip dhcp snooping information option
ip dhcp snooping
```

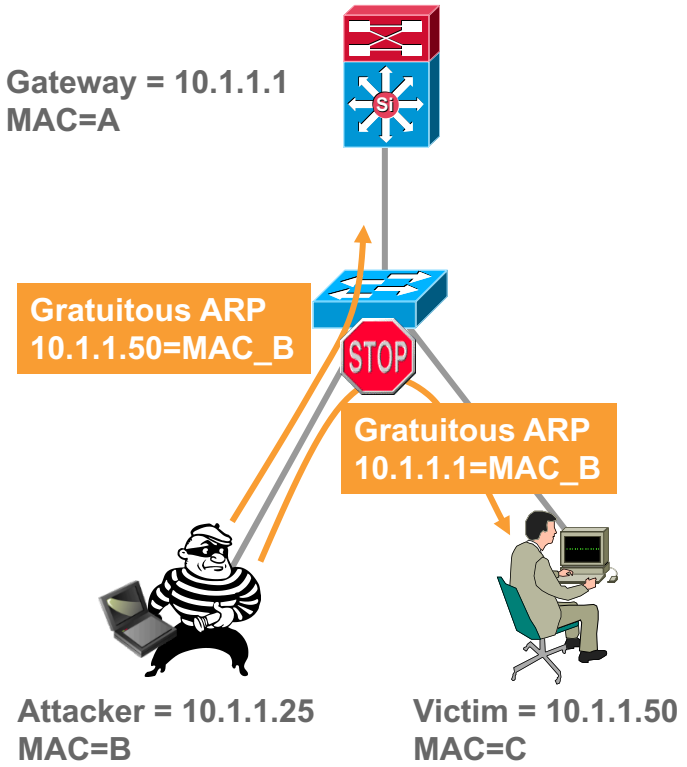
Configure on the client interface:

```
ip dhcp snooping limit rate 100
```

Dynamic ARP Inspection

Protection Against ARP Poisoning

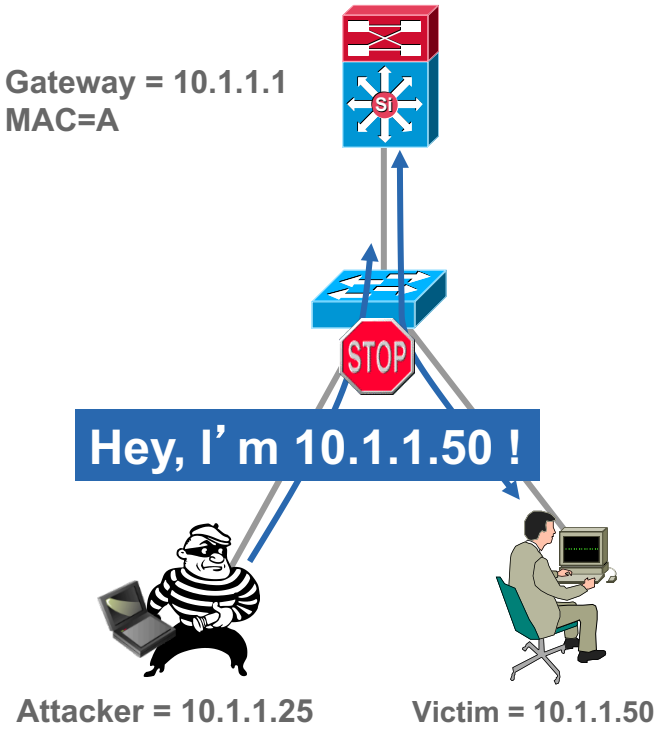
- Dynamic ARP inspection protects against ARP poisoning (ettercap, dsnif, arpspoof)
- Uses the DHCP snooping binding table
- Tracks MAC to IP from DHCP transactions
  - For non-DHCP MAC/IP Addresses you can write ARP ACL's to protect those devices
- Rate-limits ARP requests from client ports; stop port scanning
- Drop bogus gratuitous ARPs; stop ARP poisoning/MItM attacks



IP Source Guard

Protection Against Spoofed IP Addresses

- IP source guard protects against spoofed IP addresses
- Uses the DHCP snooping binding table
- Tracks IP address to port associations
- Dynamically programs port ACL to drop traffic not originating from IP address assigned via DHCP



IPv6 Router Advertisement Guard

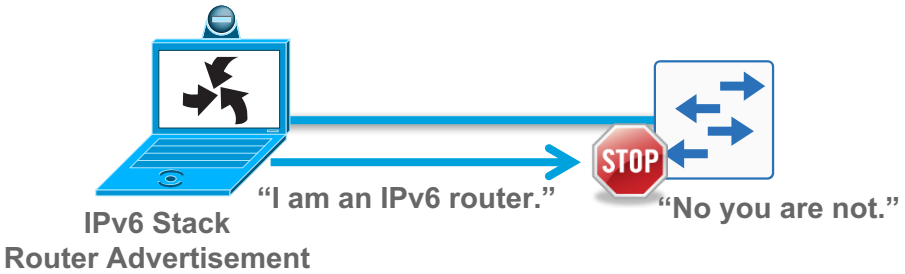
Client Facing Interface Configuration

Define policy in the global configuration:

```
ipv6 nd raguard policy HOST_POLICY
  device-role host
```

Attach policy configuration to the client interface:

```
ipv6 nd raguard attach-policy HOST_POLICY
```

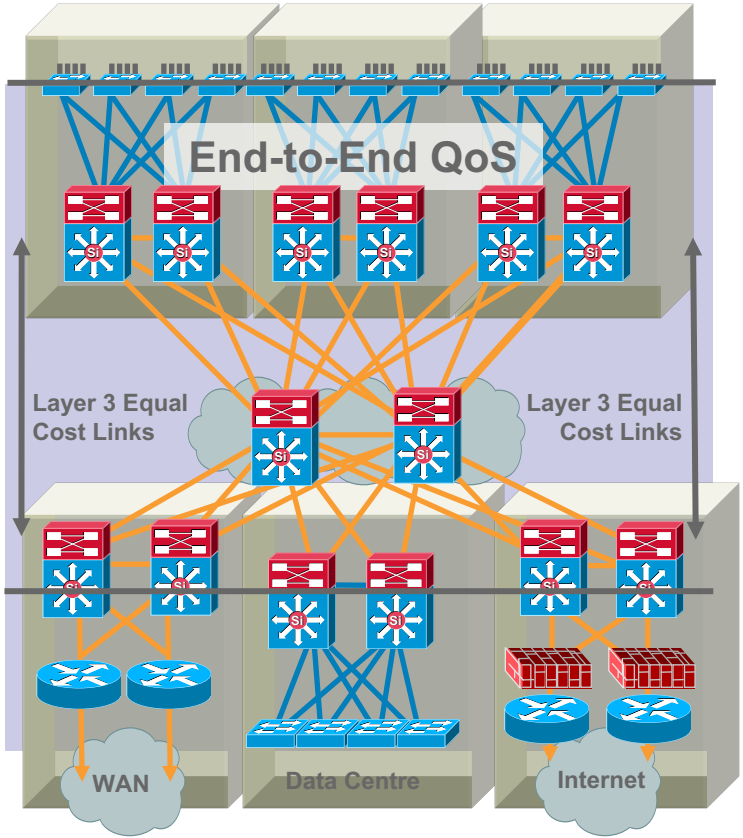


- If a port device role is configured as host, IPv6 First Hop Security (FHS) RA Guard drops all IPv6 Router Advertisement messages
- Useful even for IPv4-only networks
- Other port device role options include: monitor, router, and switch

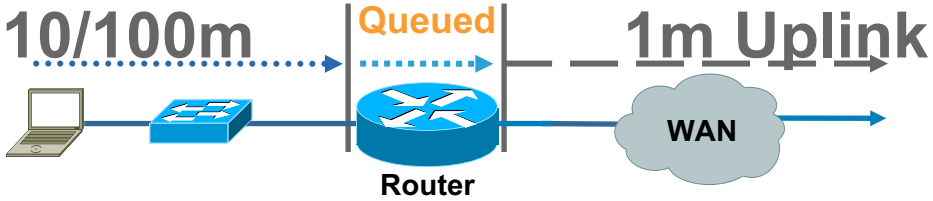
BRKSEC-2003: IPv6 Security Threats and Mitigations; BRKSEC-3003: Advanced IPv6 Security in the LAN

Best Practices - Quality of Service

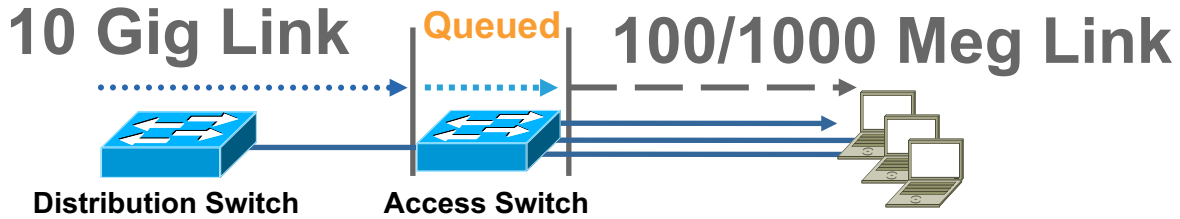
- Must be deployed end-to-end to be effective; all layers play different but equal roles
- Ensure that mission-critical applications are not impacted by link or transmit queue congestion
- Aggregation and rate transition points must enforce QoS policies
- Multiple queues with configurable admission criteria and scheduling are required



Transmit Queue Congestion



100 Meg in 1 Mb/s out—Packets Serialize in Faster than They Serialize Out
Packets Queued as They Wait to Serialize out Slower Link



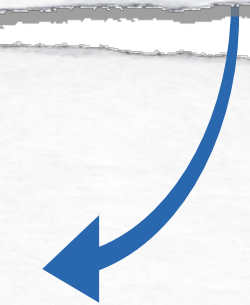
10 Gig In 100/1000 Meg out—Packets Serialize in Faster than They Serialize Out
Packets Queued as They Wait to Serialize out Slower Link

Auto QoS VoIP—Making It Easy …

Configures QoS for VoIP on Campus Switches

```
Access-Switch(config-if)#auto qos voip ?
cisco-phone      Trust the QoS marking of Cisco IP Phone
cisco-softphone  Trust the QoS marking of Cisco IP SoftPhone
trust            Trust the DSCP/CoS marking

Access-Switch(config-if)#auto qos voip cisco-phone
Access-Switch(config-if)#exit
```



```
!
interface FastEthernet1/0/21
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape  10   0   0   0
mls qos trust device cisco-phone
mls qos trust cos
auto qos voip cisco-phone
end
```

Access Layer Platform Options

Catalyst 4500-E with Supervisor 8-E / 8L-E

- Modular switch with 1:1 redundancy for all critical systems (supervisors, power supplies, fans)
- Stateful switchover provides subsecond supervisor recovery
- Multiple Ethernet Connectivity options (fiber or copper with various densities)
- Quad Sup RPR (new)
- In-Service Software Upgrades
- PoE, PoE+, and UPOE
- Energy Efficient Ethernet
- Campus Fabric Edge (8-E)

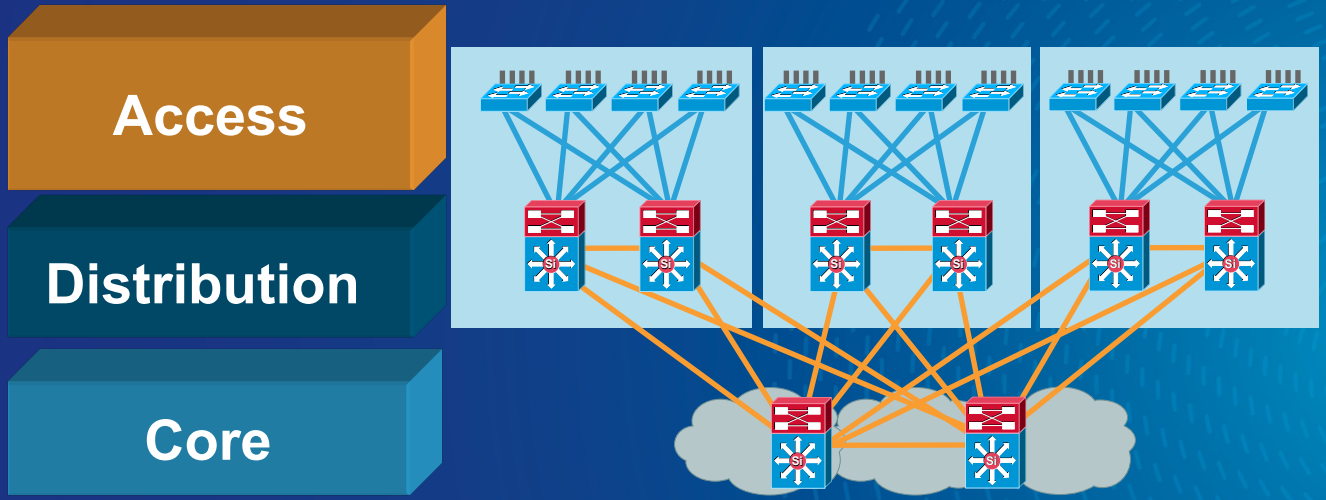
Catalyst 3850 and Catalyst 3650

- Fixed configuration stackable switch with central config and control
- Stateful switchover provides subsecond recovery
- Modular Uplinks (3850), power supplies, and fans
- StackWise480 and StackPower (3850), StackWise160 (3650)
- Up to 9 switches in a stack
- PoE, PoE+, UPOE
- Campus Fabric Border/Edge

Catalyst 2960-X and Catalyst 2960-XR

- Fixed configuration stackable switch with central config and control
- Up to 8 switches in a stack
- FlexStack+ 80G stacking (Stack Module Required)
- Stack or stack member failure recovery max 1 -2 seconds
- PoE and PoE+
- Redundant Power Supply and L3 Access option (XR)

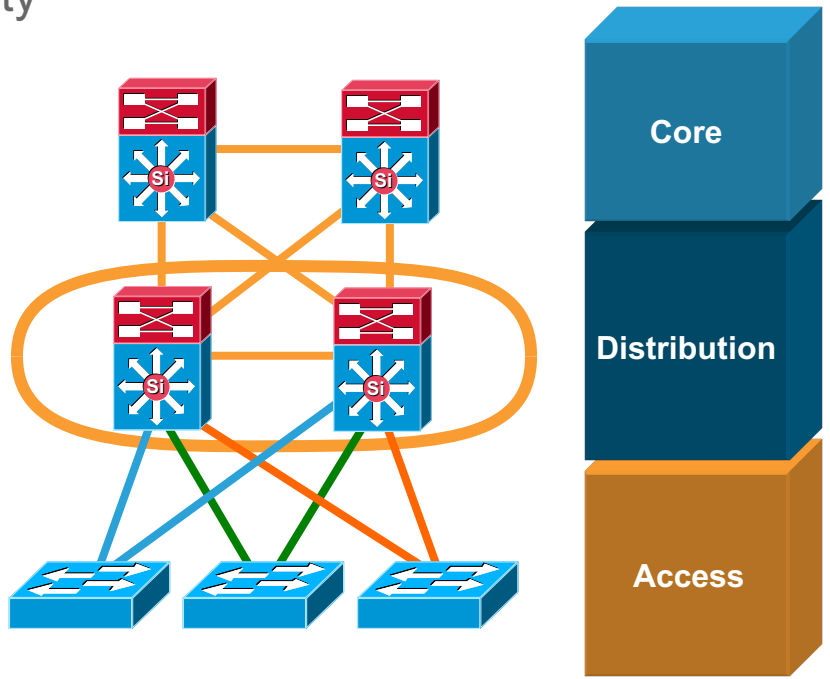
Agenda for today – Access connects do Distribution



Distribution Layer

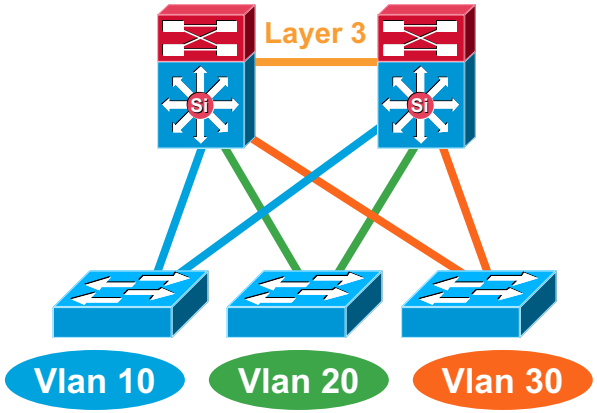
Policy, Convergence, QoS, and High Availability

- Availability, load balancing, QoS and provisioning are the important considerations at this layer
- Aggregates wiring closets (access layer) and uplinks to core
- Protects core from high density peering and problems in access layer
- Route summarization, fast convergence, redundant path load sharing
- HSRP or GLBP to provide first hop redundancy

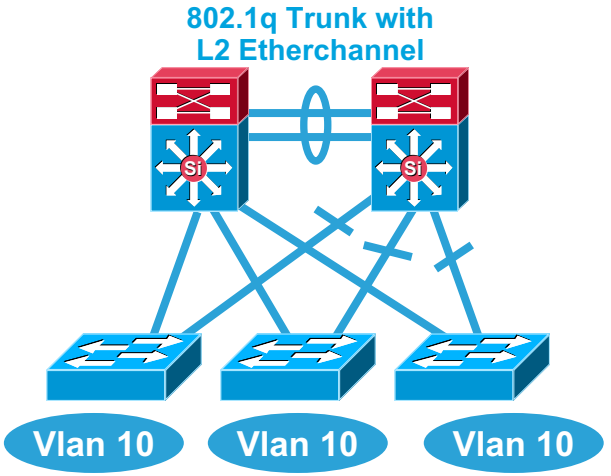


Multilayer Network Design

Layer 2 Access with Layer 3 Distribution



- Each access switch has unique VLANs
- No Layer 2 loops, no etherchannel
- Layer 3 link between distribution
- No blocked links

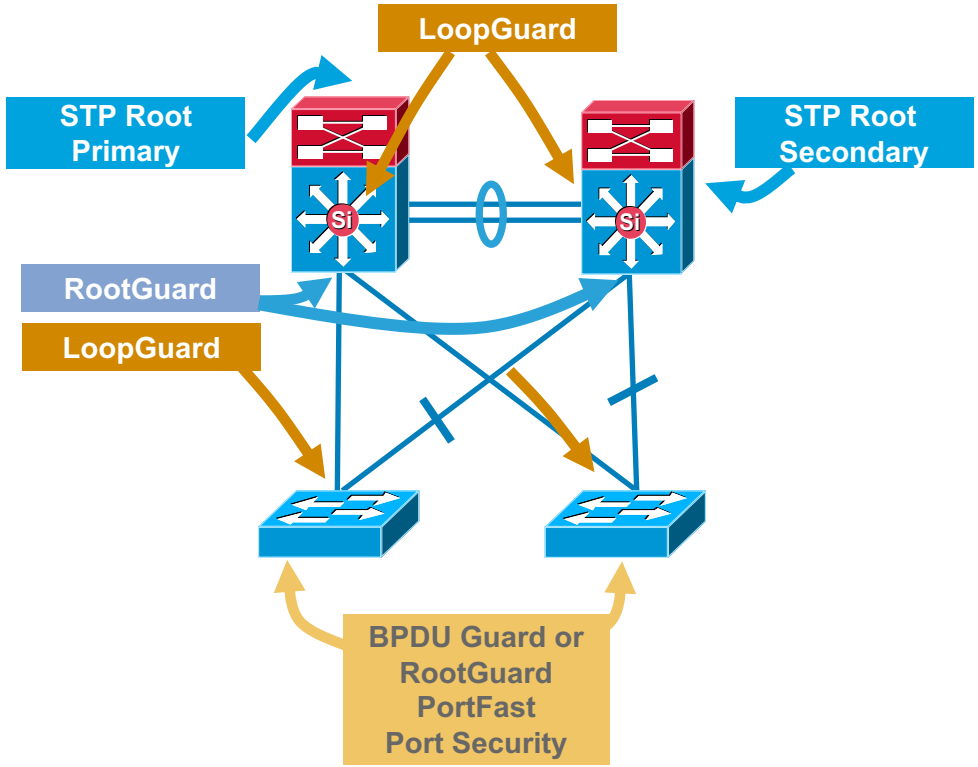


- At least some VLANs span multiple access switches
- Layer 2 loops
- Layer 2 and 3 running over link between distribution
- Blocked links even with etherchannels

STP Hardening

Spanning Tree Should Behave the Way You Expect

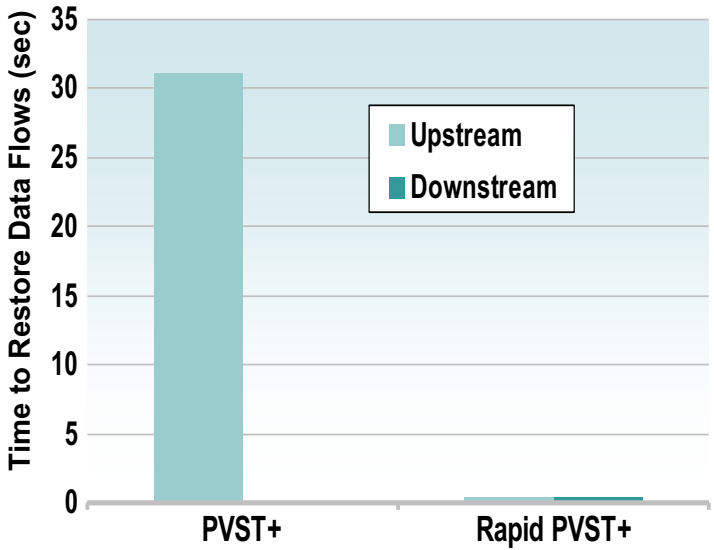
- Place the root where you want it
  - Root primary/secondary macro
- The root bridge should stay where you put it
  - RootGuard
  - LoopGuard
  - UplinkFast
  - UDLD
- Only end-station traffic should be seen on an edge port
  - BPDU Guard
  - RootGuard
  - PortFast
  - Port-security



Optimising L2 Convergence

PVST+, Rapid PVST+ or MST

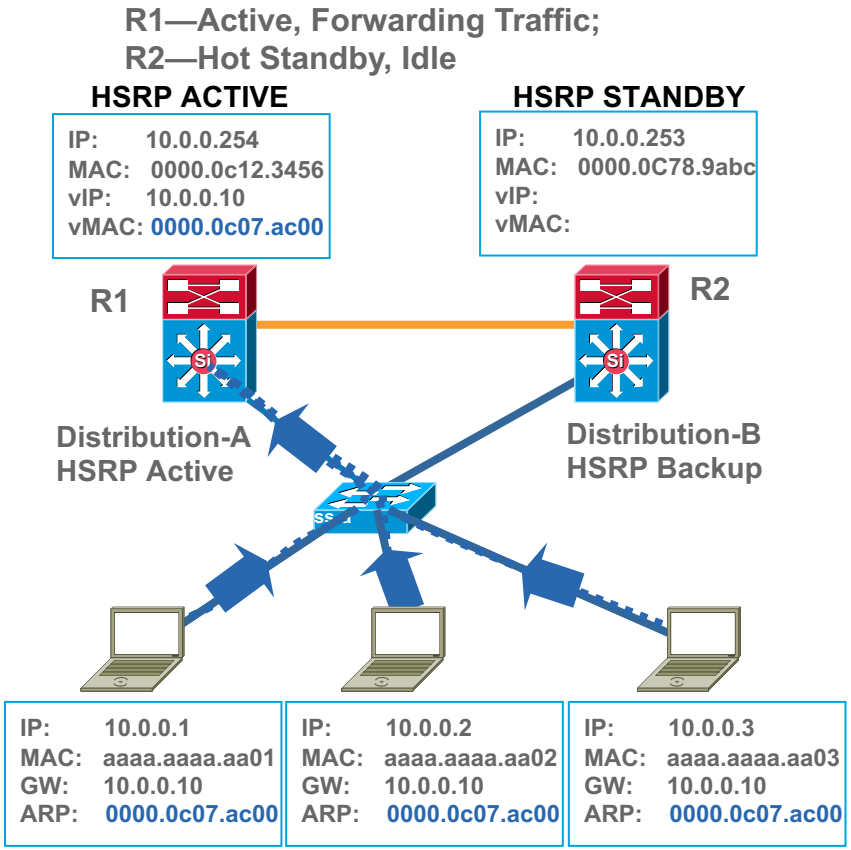
- Rapid-PVST+ greatly improves the restoration times for any VLAN that requires a topology convergence due to link UP
- Rapid-PVST+ also greatly improves convergence time over backbone fast for any indirect link failures
- PVST+ (802.1d)
  - Traditional spanning tree implementation
- Rapid PVST+ (802.1w)
  - Scales to large size (~10,000 logical ports)
  - Easy to implement, proven, scales
- MST (802.1s)
  - Permits very large scale STP implementations (~30,000 logical ports)
  - Not as flexible as rapid PVST+



First Hop Redundancy with HSRP

RFC 2281 (March 1998)

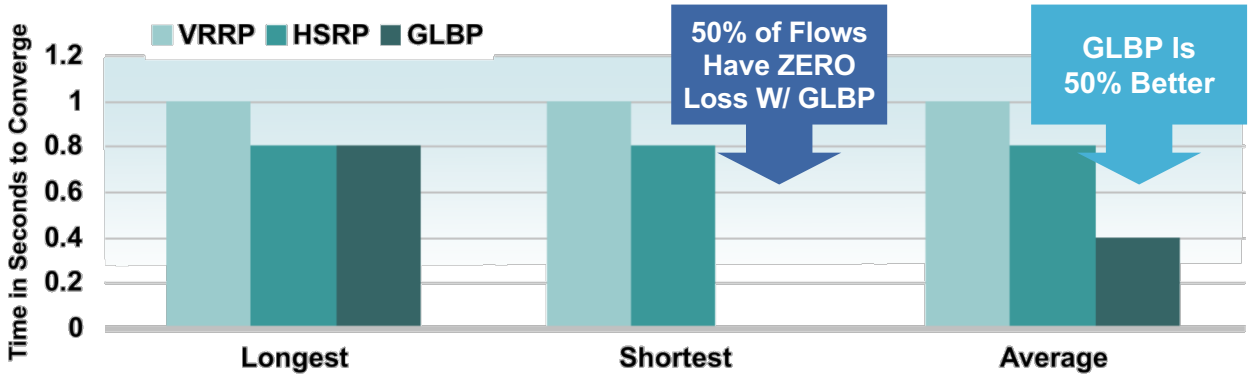
- A group of routers function as one virtual router by sharing one virtual IP address and one virtual MAC address
- One (active) router performs packet forwarding for local hosts
- The rest of the routers provide hot standby in case the active router fails
- Standby routers stay idle as far as packet forwarding from the client side is concerned
- Use preemption to avoid black-hole while network reconverges



Optimising Convergence: VRRP, HSRP, GLBP

Mean, Max, and Min—Are There Differences?

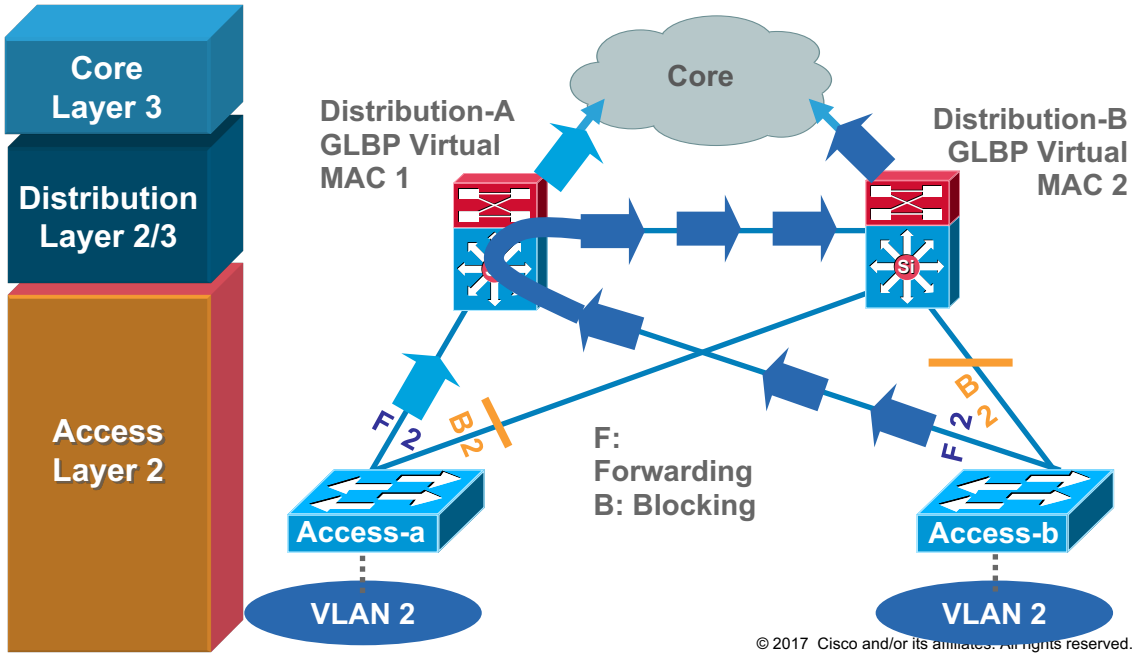
- VRRP not tested with sub-second timers and all flows go through a common VRRP peer; mean, max, and min are equal
- HSRP has sub-second timers; however all flows go through same HSRP peer so there is no difference between mean, max, and min
- GLBP has sub-second timers and distributes the load amongst the GLBP peers; so 50% of the clients are not affected by an uplink failure



If You Span VLANS, Tuning Required

By Default, Half the Traffic Will Take a Two-Hop L2 Path

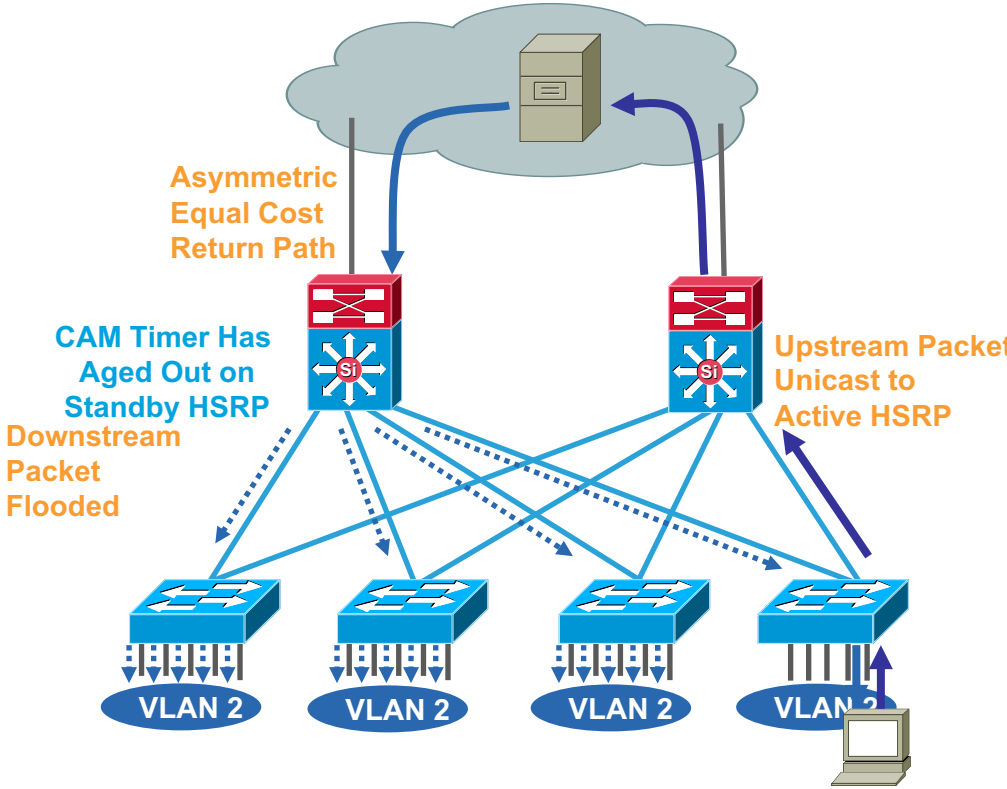
- Both distribution switches act as default gateway
- Blocked uplink caused traffic to take less than optimal path



Asymmetric Routing (Unicast Flooding)

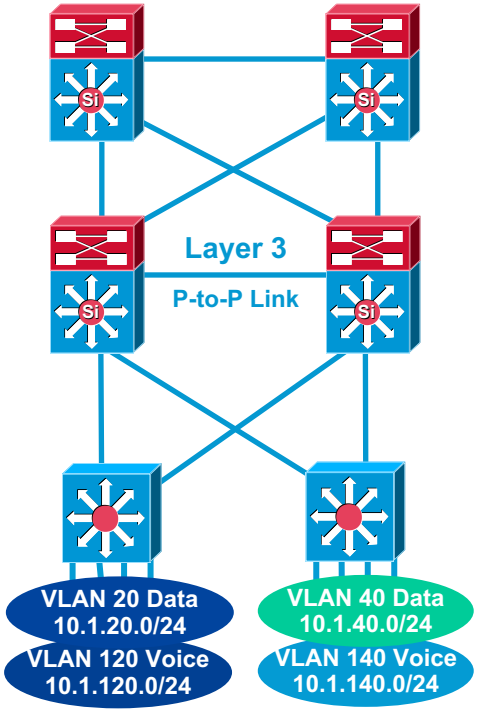
Affects redundant topologies with shared L2 access

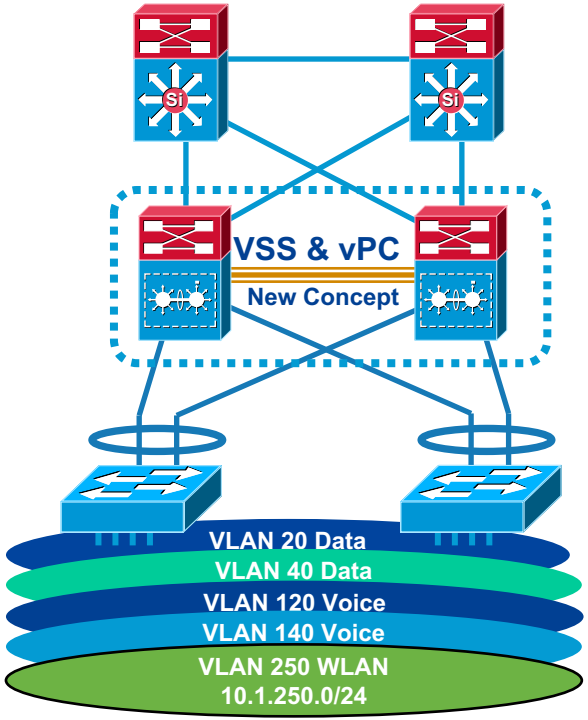
- One path upstream and two paths downstream
- CAM table entry ages out on standby HSRP
- Without a CAM entry packet is flooded to all ports in the VLAN
- To prevent this do not stretch VLANs – If you have to:
  - Tune ARP and CAM aging timers; CAM timer exceeds ARP timer
  - Bias routing metrics to remove equal cost routes



Routed Access and Virtual Switching System

Evolutions of and Improvements to Existing Designs

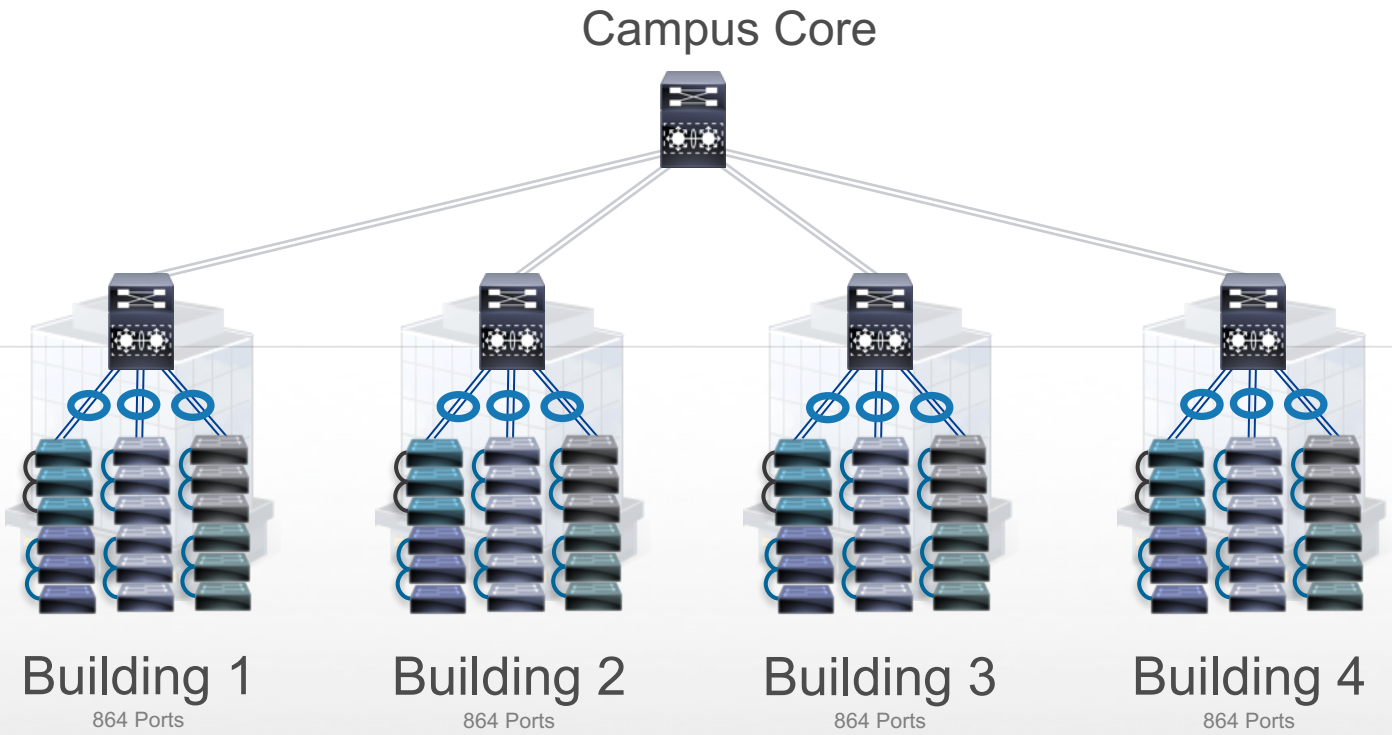




See BRKCRS-3035 - Advanced Enterprise Campus Design: Virtual Switching System (VSS)

See BRKCRS-3036 - Advanced Enterprise Campus Design: Routed Access

VSS Core with Access Stacking



VSS Switches

Stacked L2 Switches

Network Design

84 Physical Devices

5 VSS pairs and 24 stacks

29 Total Devices of Image & Configuration Management

24 Port-Channels

3456 User Ports

Design Considerations:

~~STP Loop Prevention~~

~~CAM & ARP Tuning~~

~~FHRP Tuning / Priority~~

~~Routing Protocol Tuning~~

~~PIM Tuning / DR priority~~

27

Distribution Layer Platform Options

Density, Resilience, Throughput, Scalability, Reduced failover times

Catalyst 6500/6807 Supervisor 6T/2T (VSS)

- Physically separate and resilient supervisors, line cards, and power supplies
- Clusters two physical chassis into a single logical entity
- Highest density Gigabit and 10 Gigabit Ethernet
- 40 Gigabit Ethernet
- Stateful Switchover (SSO) + Quad-Supervisor SSO (VS4O) available option
- VSS and Multi-Chassis EtherChannel for highly resilient connectivity

Catalyst 6880-X Catalyst 6840-X (VSS)

- Extensible fixed base chassis, with resilient line card expansion and power supplies
- Clusters two physical chassis into a single logical entity
- Used to aggregate a smaller number of Gigabit or 10 Gigabit access layer switches
- Stateful Switchover between chassis
- Enhanced Fast Software Upgrade (eFSU) capable

Catalyst 4500-E Supervisor 7, 8 (VSS) Catalyst 4500-X (VSS)

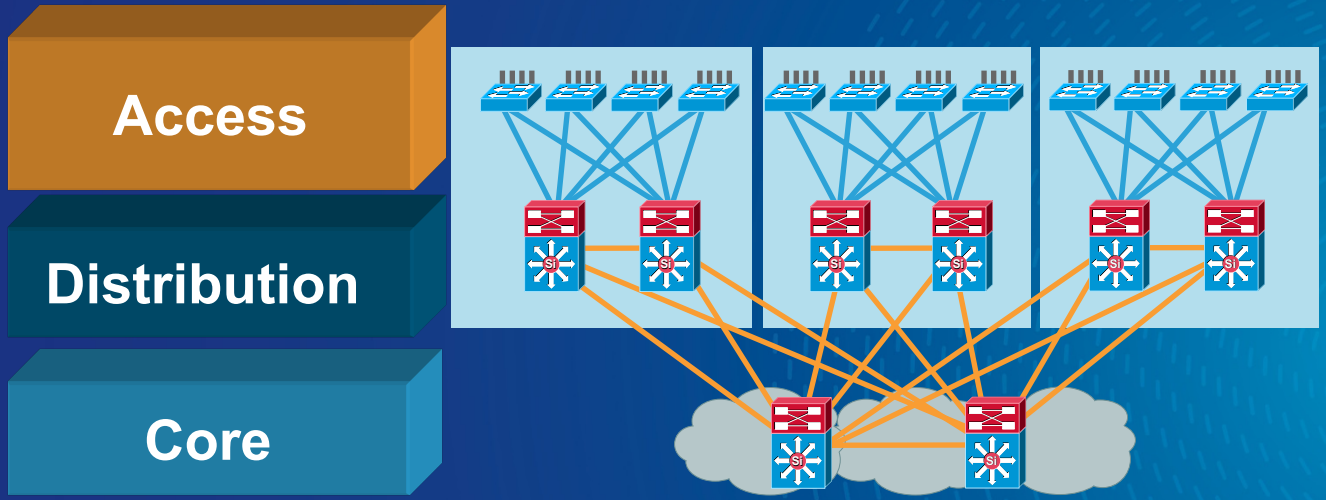
- Physically separate chassis, line cards, and power supplies, with fixed/modular options
- VSS-two physical chassis into a single logical entity
- SSO between chassis
- 4500-E Quad Sup RPR (new)
- Used to aggregate a smaller number of Gigabit or 10 Gigabit access layer switches
- In Service Software Upgrades (ISSU)

Catalyst 3850-12S Catalyst 3850-(12/24/48)XS (Stack)

- Centralized stack configuration, control, and management plane
- Used to aggregate a smaller number of Gigabit access layer switches
- Distributed, per switch, Layer 2/Layer 3 forwarding, CAM tables, and BPDU processing
- UADP – Wireless Capable

One common approach to configuring and operating the Distribution Layer

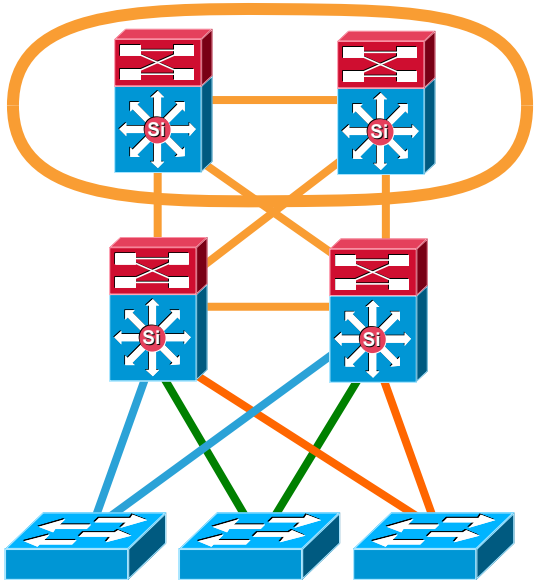
Agenda for today – do you always need Core?



Core Layer

Scalability, High Availability, and Fast Convergence

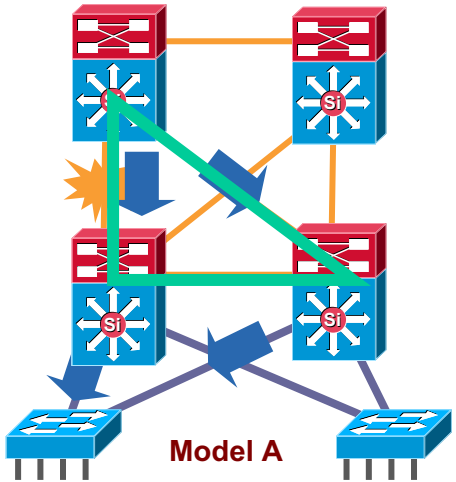
- Backbone for the network—connects network building blocks
- Performance and stability vs. complexity—less is more in the core
- Aggregation point for distribution layer
- Separate core layer helps in scalability during future growth
- Keep the design technology-independent



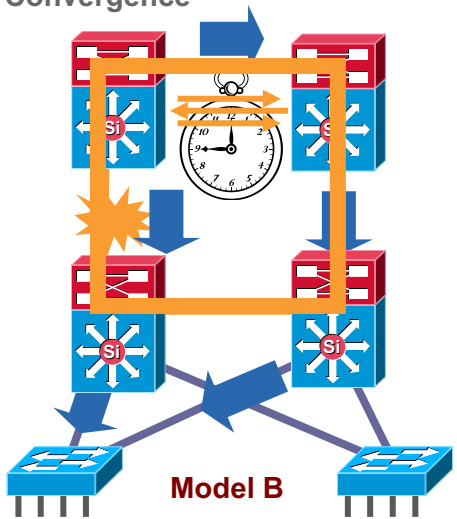
Best Practice - Build Triangles not Squares

Deterministic vs. Non-Deterministic

Triangles: Link/Box Failure Does not Require Routing Protocol Convergence



Squares: Link/Box Failure Requires Routing Protocol Convergence

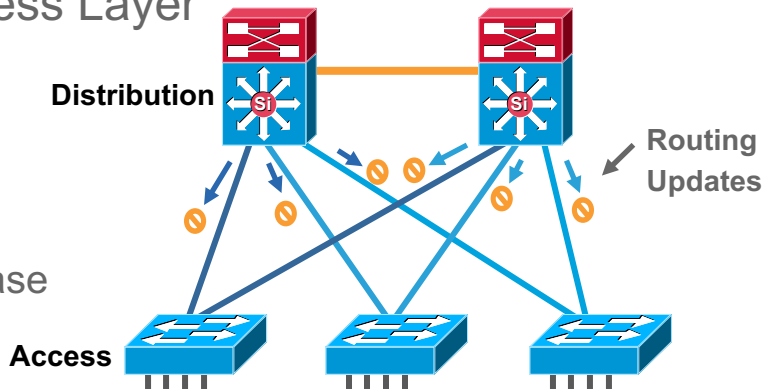


- Layer 3 redundant equal cost links support fast convergence
- Hardware based—fast recovery to remaining path
- Convergence is extremely fast (dual equal-cost paths: no need for OSPF or EIGRP to recalculate a new path)

Best Practice - Passive Interfaces for IGP

Limit IGP Peering Through the Access Layer

- Limit unnecessary peering using passive interface:
  - Four VLANs per wiring closet
  - 12 adjacencies total
  - Memory and CPU requirements increase with no real benefit
  - Creates overhead for IGP



OSPF Example:

```
Router(config)#routerospf 1
Router(config-router)#passive-
interfaceVlan 99
```

```
Router(config)#routerospf 1
Router(config-router)#passive-
interface default
Router(config-router)#no passive-
interface Vlan 99
```

EIGRP Example:

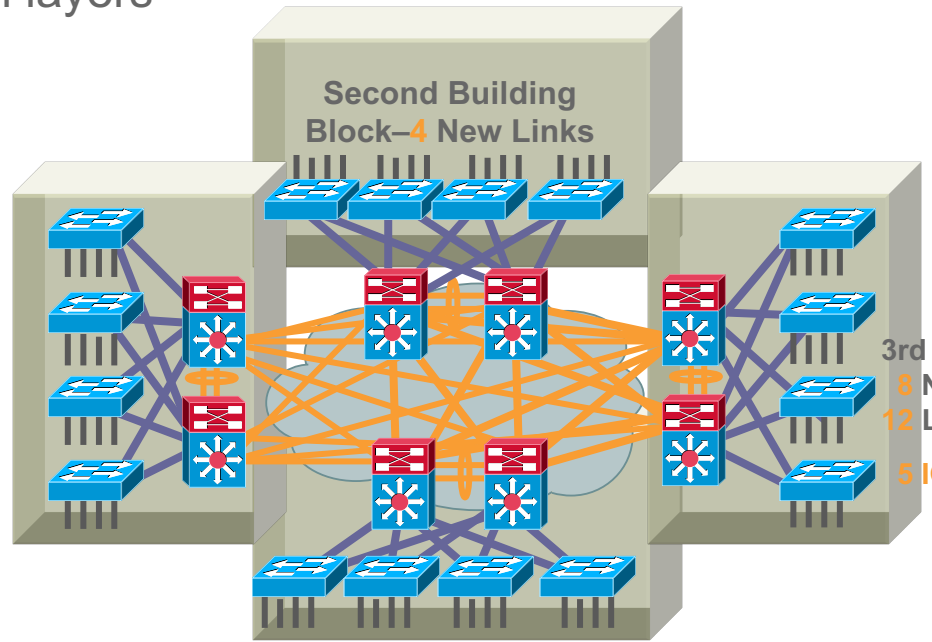
```
Router(config)#routereigrp 1
Router(config-router)#passive-
interfaceVlan 99
```

```
Router(config)#routereigrp 1
Router(config-router)#passive-
interface default
Router(config-router)#no passive-
interface Vlan 99
```

Do I Need a Core Layer?

It's Really a Question of Scale, Complexity, and Convergence

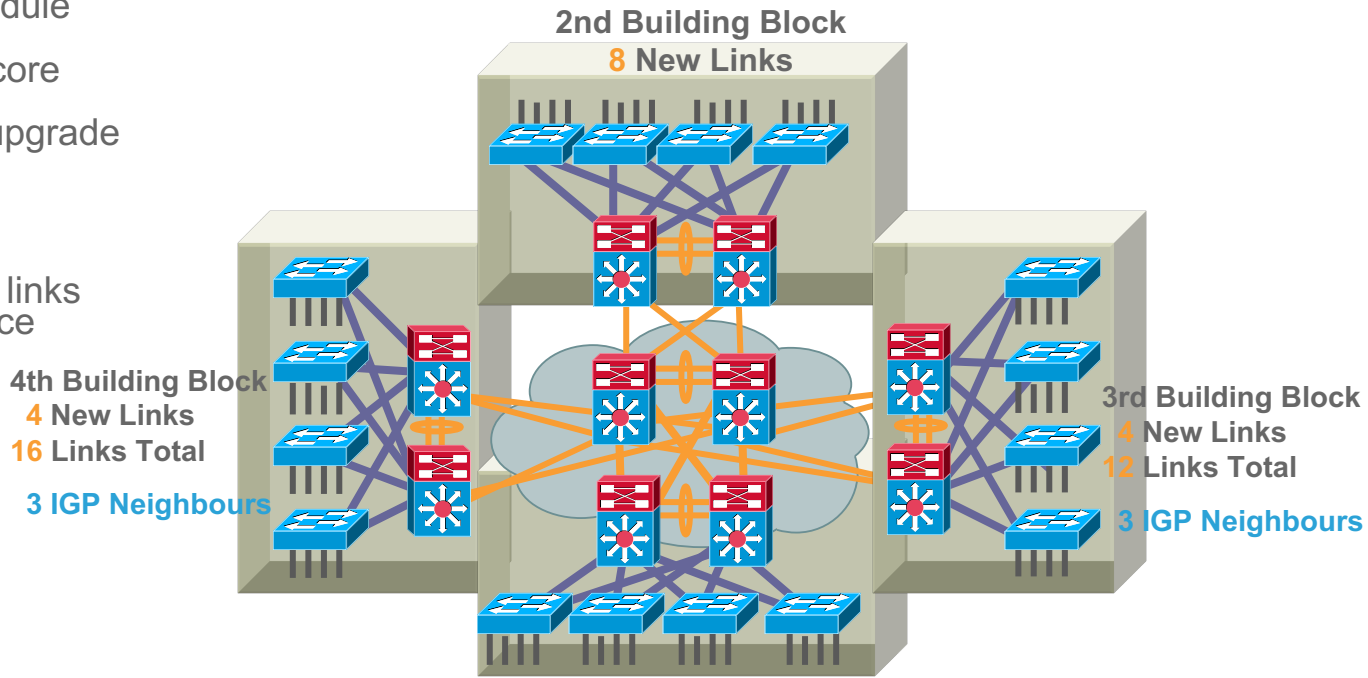
- No Core
- Fully-meshed distribution layers
- Physical cabling requirement
- Routing complexity



Do I Need a Core Layer?

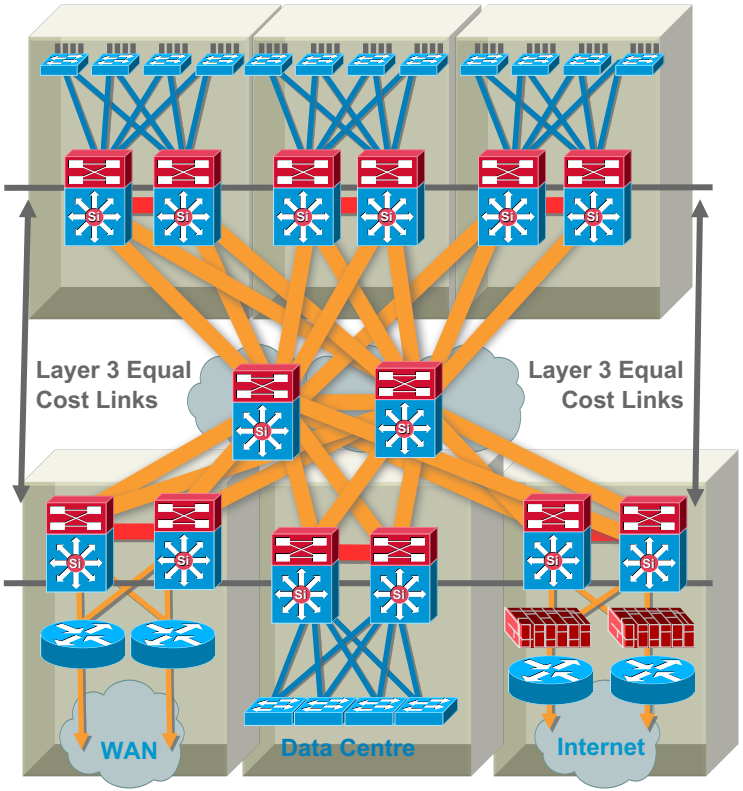
It's Really a Question of Scale, Complexity, and Convergence

- Dedicated Core Switches
- Easier to add a module
- Fewer links in the core
- Easier bandwidth upgrade
- Routing protocol peering reduced
- Equal cost Layer 3 links for best convergence



EtherChannels or Equal Cost Multipath

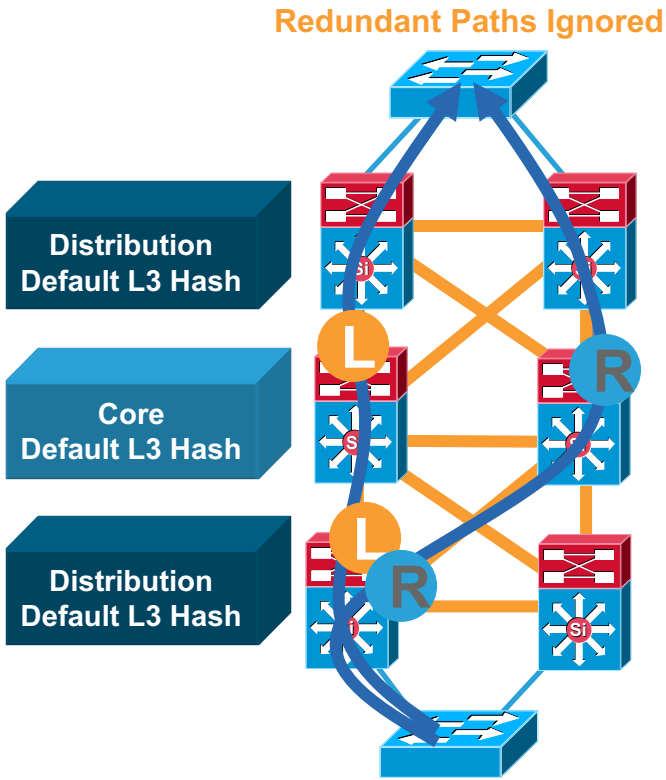
Why 10/40/100Gigabit Interconnects



- More links = more routing peer relationships and associated overhead
- EtherChannels allow you to reduce peers by creating single logical interface to peer over
- However, a single link failure might not be taken into consideration by routing protocols and overload is possible
- Single 10/40/100 gigabit links address both problems. Increased bandwidth without increasing complexity or compromising routing protocols ability to select best path

CEF Load Balancing

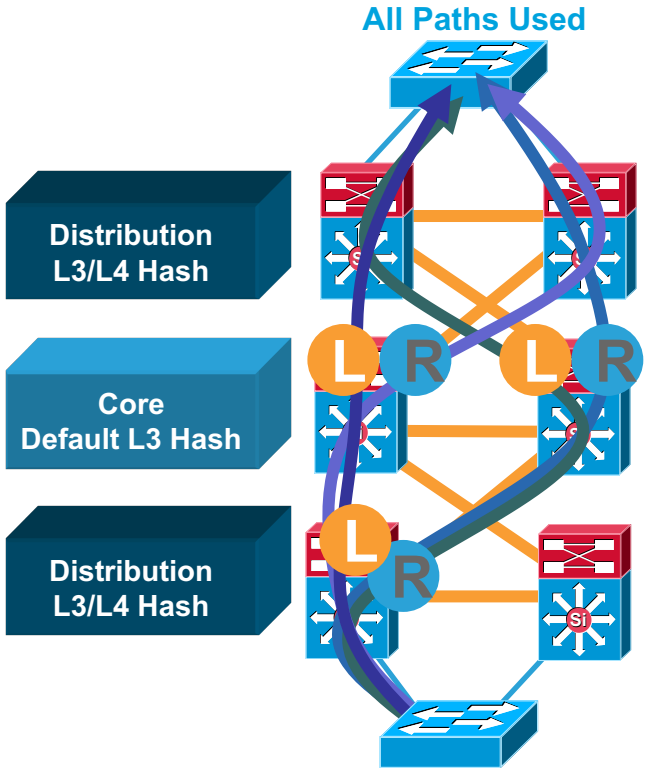
Avoid Under Utilizing Redundant Layer 3 Paths



- CEF polarization: without some tuning CEF will select the same path left/left or right/right
- Imbalance/overload could occur
- Redundant paths are ignored/underutilized
- The default CEF hash input is L3
- We can change the default to use L3 + L4 information as input to the hash derivation

CEF Load Balancing

Avoid Under Utilizing Redundant Layer 3 Paths

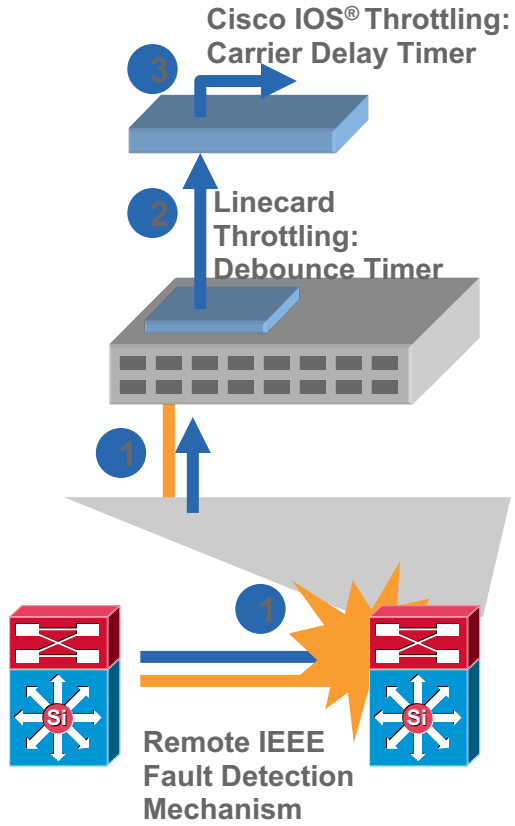


- The default will for Sup720/32 and latest hardware (unique ID added to default). However, depending on IP addressing, and flows imbalance could occur
- Alternating L3/L4 hash and L3 hash will give us the best load balancing results
- Use simple in the core and full simple in the distribution to add L4 information to the algorithm at the distribution and maintain differentiation tier-to-tier

Redundancy and Protocol Interaction

Link Redundancy and Failure Detection

- Direct point-to-point fibre provides for fast failure detection
- IEEE 802.3z and 802.3ae link negotiation define the use of remote fault indicator and link fault signalling mechanisms
- Bit D13 in the Fast Link Pulse (FLP) can be set to indicate a physical fault to the remote side
- Do not disable auto-negotiation on GigE and 10GigE interfaces
- The default debounce timer on GigE and 10GigE fibre linecards is 10 msec
- The minimum debounce for copper is 300 msec
- Carrier-delay
  - 3560, 3750, and 4500—0 msec
  - 6500—leave it set at default



Core Layer Platform Options

Catalyst 6807-XL, Supervisor 6T/2T (VSS Option)

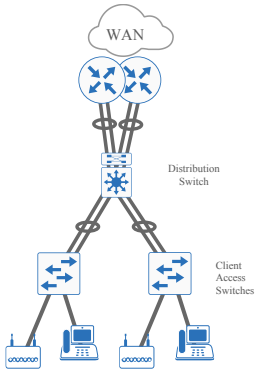
- LAN Core platform with consistent IOS interface and feature set as rest of LAN allowing single logical and resilient platform using Virtual Switching System (VSS)
- Redundant supervisor and SSO support, VSS, and Quad-Supervisor SSO available (VS4O), and load sharing power supplies
- Wide Range of connectivity from Gigabit Ethernet, GEC, 10 Gb Ethernet, 10-GEC, and 40 Gb Ethernet
- Up to 440G/slot (6807-XL / Sup 6T)
- VSS and Multi-Chassis EtherChannel for highly resilient connectivity and scalable distributed forwarding

Nexus 7700 with Supervisor 2E (2x Independent Chassis)

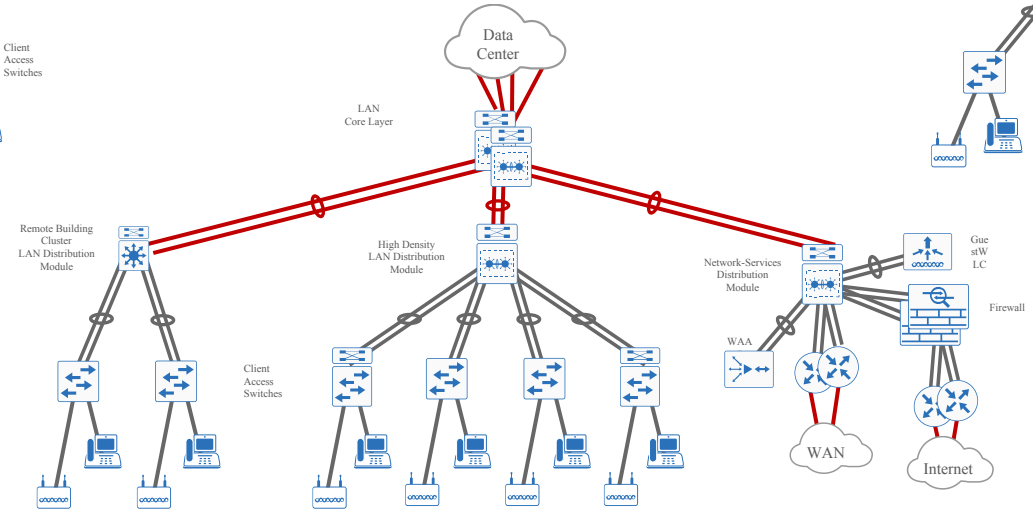
- LAN Core platform allowing independent control planes and a consolidated DC and LAN core possible through Virtual Device Contexts (VDC)
- Resilient supervisor and SSO support, and load sharing power supplies
- Wide Range of connectivity from Gigabit Ethernet, GEC, High Density 10 Gb Ethernet, 10-GEC, 40Gb and 100Gb Ethernet
- In Service Software Upgrades
- Data Center NX-OS heritage

You Now Have the Tools to Build This! (and more)

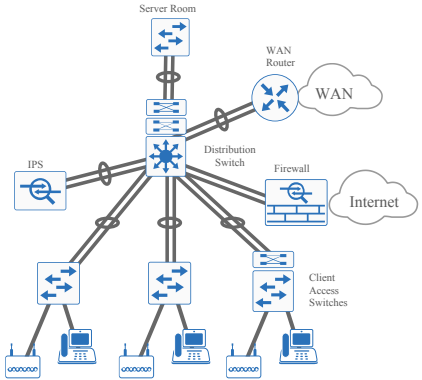
Two-Tier Remote-Site LAN



Three-Tier LAN Design



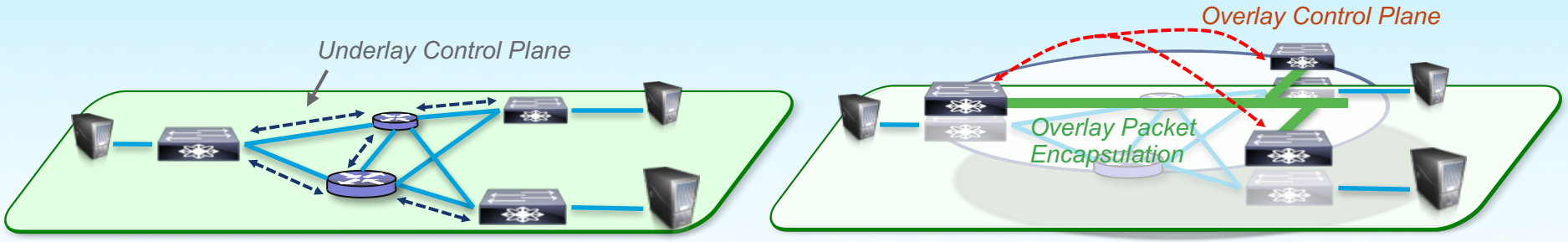
Two-Tier Collapsed LAN Core



Campus Fabric Introduction

What exactly is a Fabric?

Separate the Forwarding Plane from the Services Plane



Simple Transport Forwarding

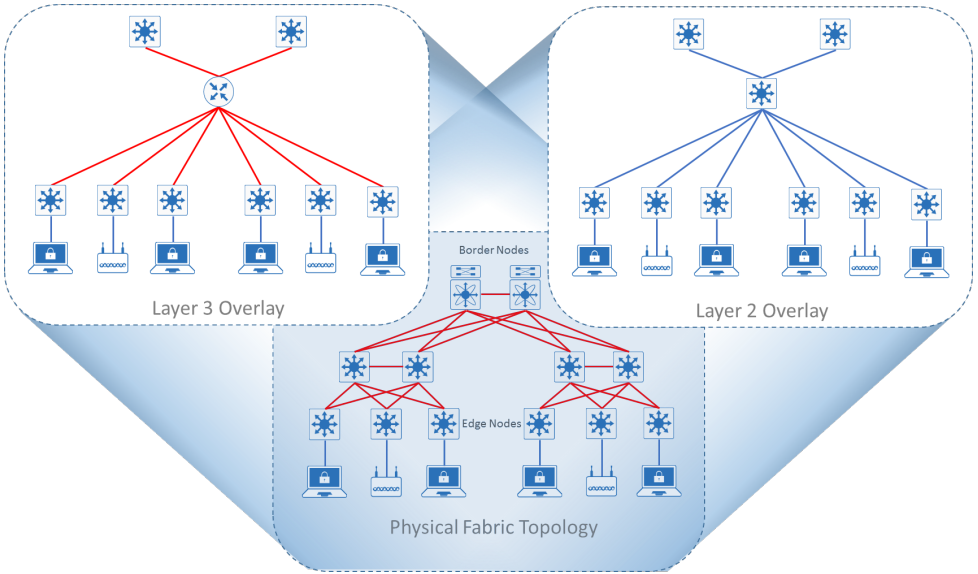
- Physical Devices and Paths
- Intelligent Packet Handling
- Maximize Network Availability
- Simple and Manageable
- Also called “Underlay”

Flexible Virtual Services

- Mobility – Track End-points at Edges
- Scalability – Reduce core state
  - Distribute state to network edge
- Flexibility and Programmability
  - Reduced number of touch points
- Also called “Overlays”

Campus Fabric Key Advantages

- Simplified Provisioning
  - Plug and play deployment of devices
  - Apply best practice configurations via smart CLI or programmability models
- Host Mobility
  - Stretched subnets using anycast default gateway
- Secure Segmentation
  - Build secure boundaries for users and things
- Policy enforcement
  - Based on your identity not IP address



Cisco Validated Design Guide for Campus Fabric:

http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2016/CVD-CampusFabricDesign-2016OCT.pdf

What is unique about Campus Fabric?

LISP based Control-Plane

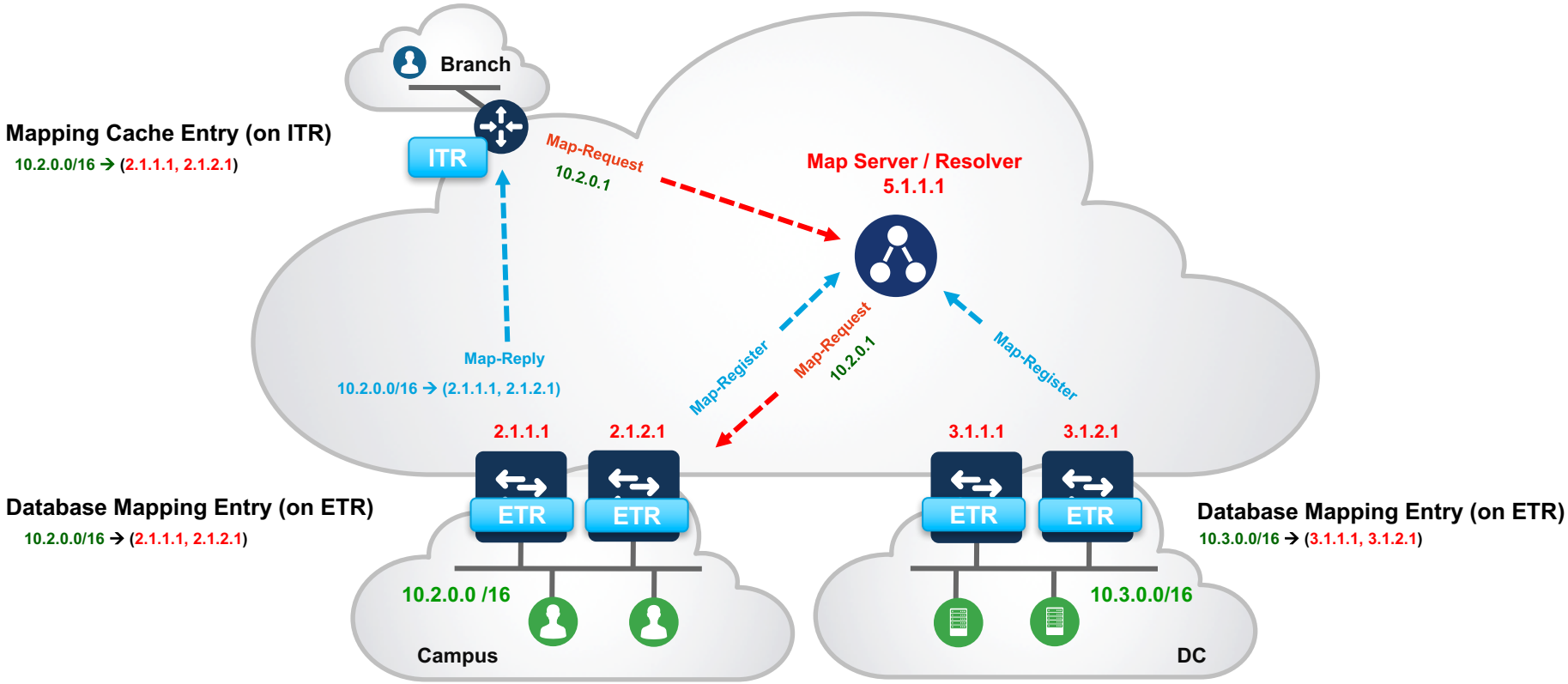
VXLAN based Data-Plane

Cisco TrustSec based Policy-Plane

Key Differences
• L2 + L3 Overlay -vs- L2 or L3 Only
• Host Mobility with Anycast Gateway
• Adds VRF + SGT into Data-Plane
• Virtual Tunnel Endpoints (No Static)
• No Topology Limitations (Basic IP)

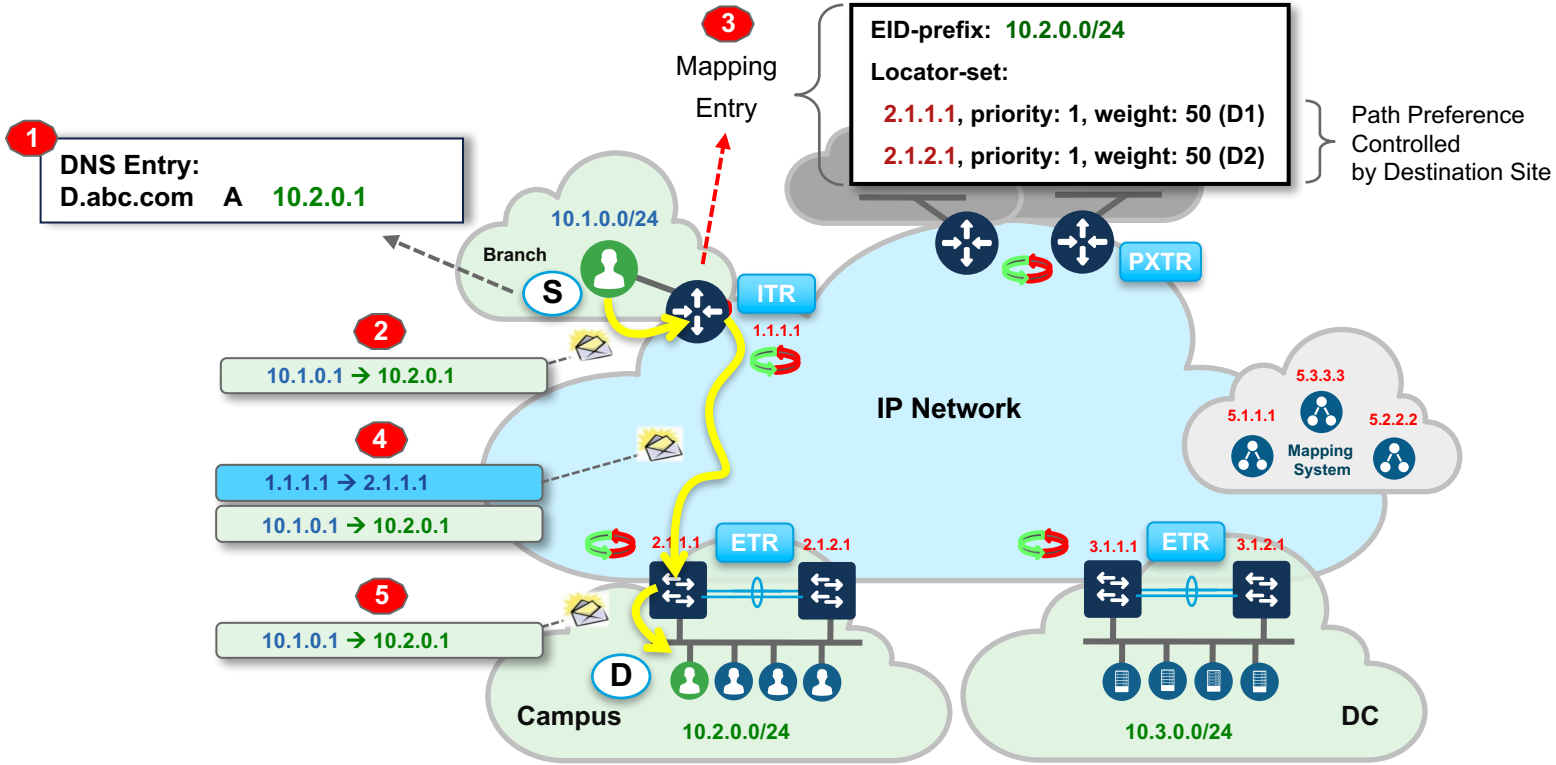
LISP Mapping process

Map Register & Resolution



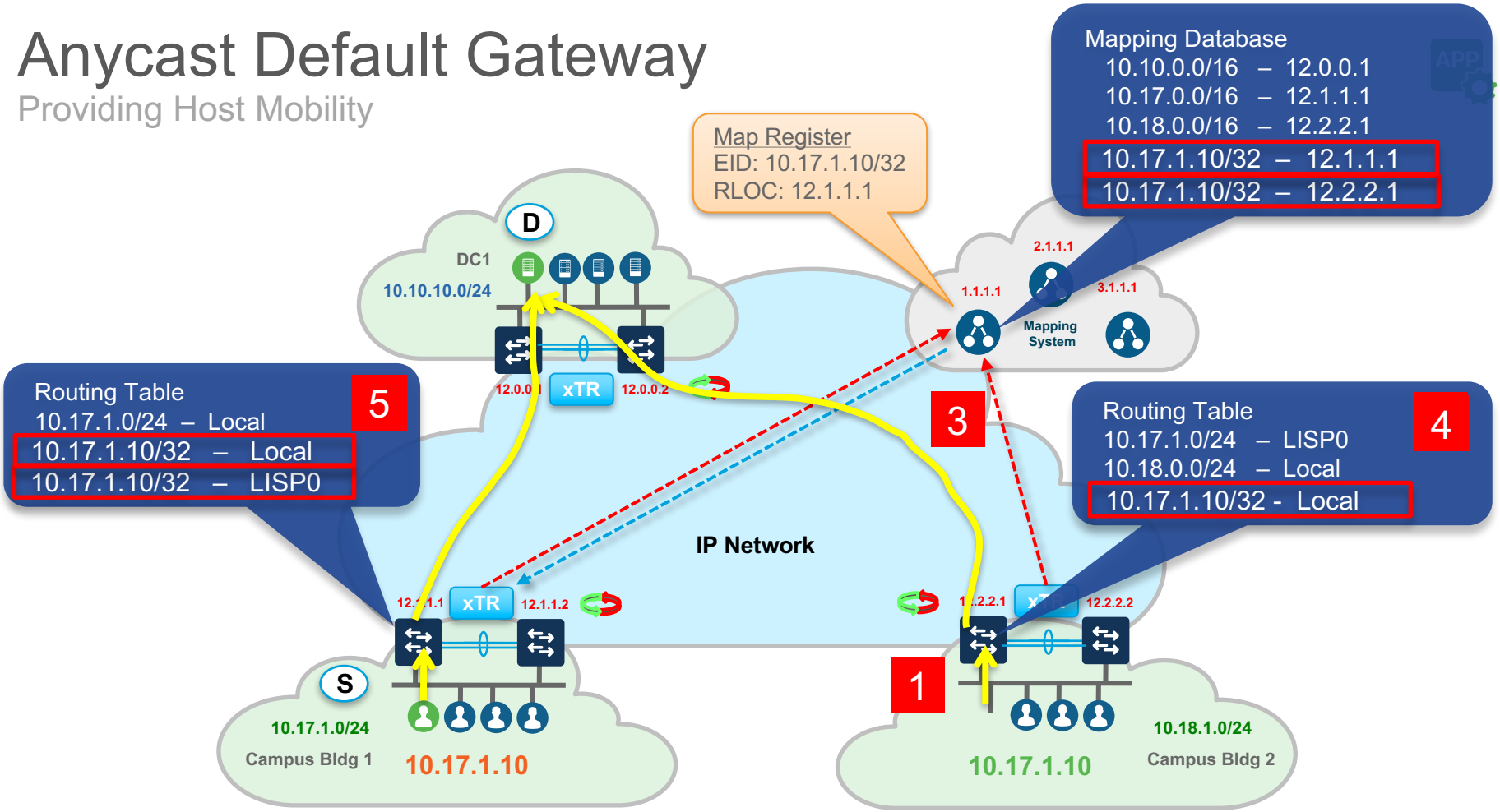
Traffic forwarding

Building VXLAN tunnels



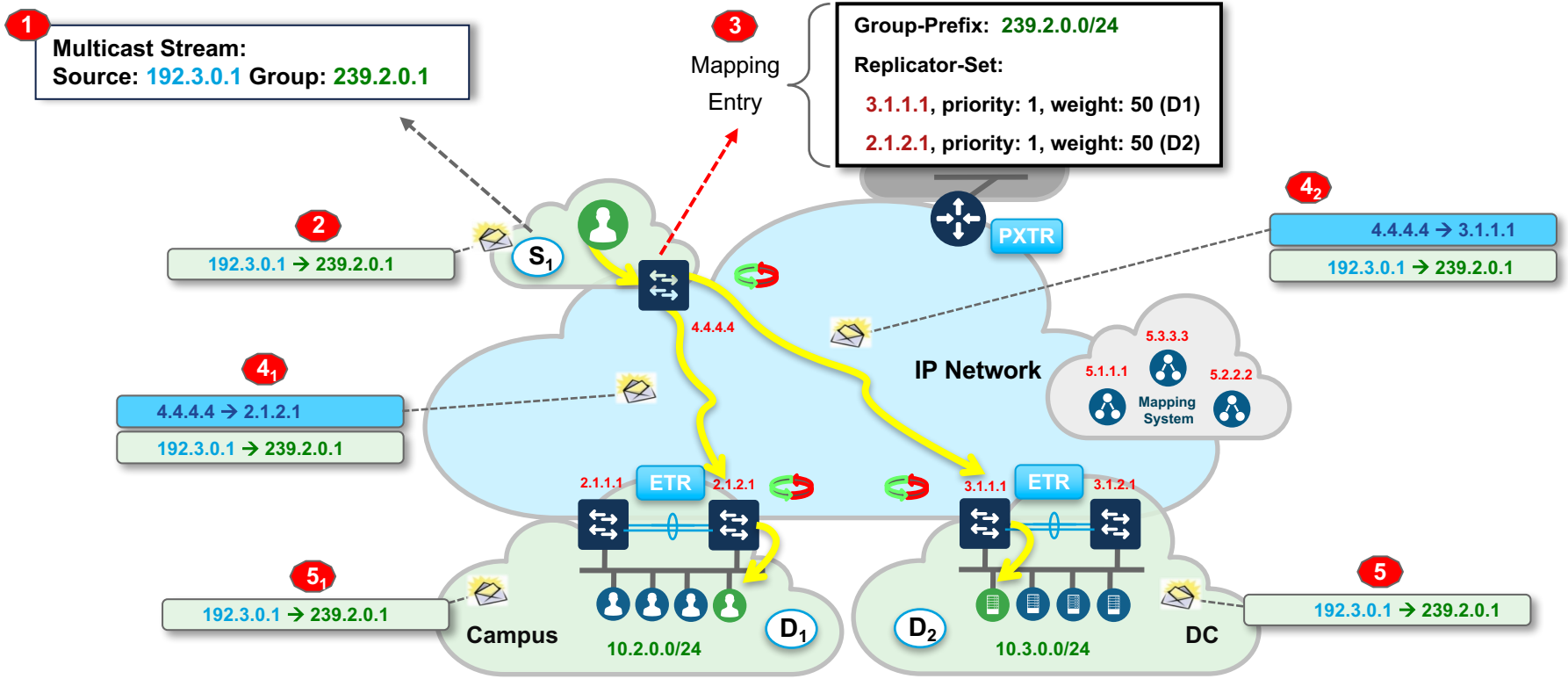
Anycast Default Gateway

Providing Host Mobility



LISP Multicast

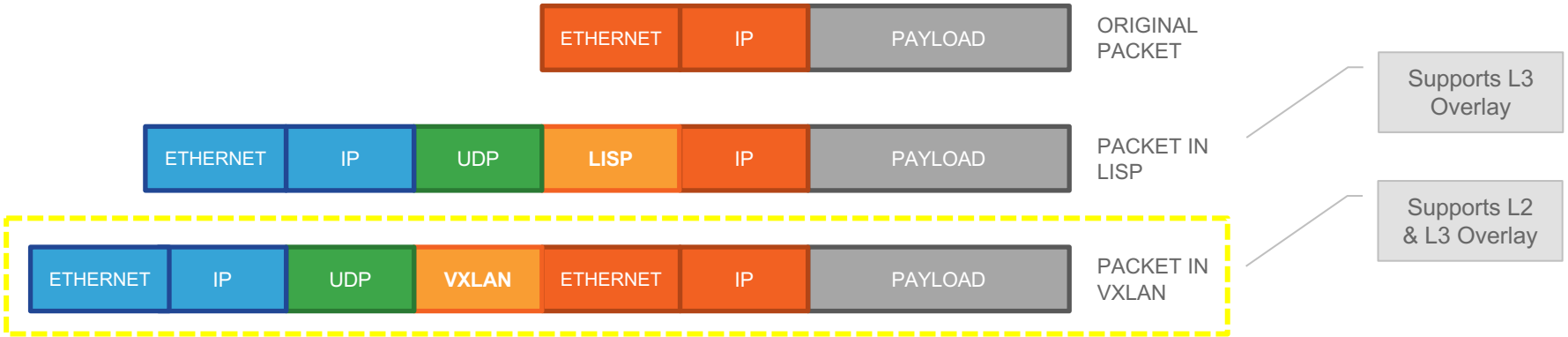
Head End Replication



How LISP and VXLAN interact?

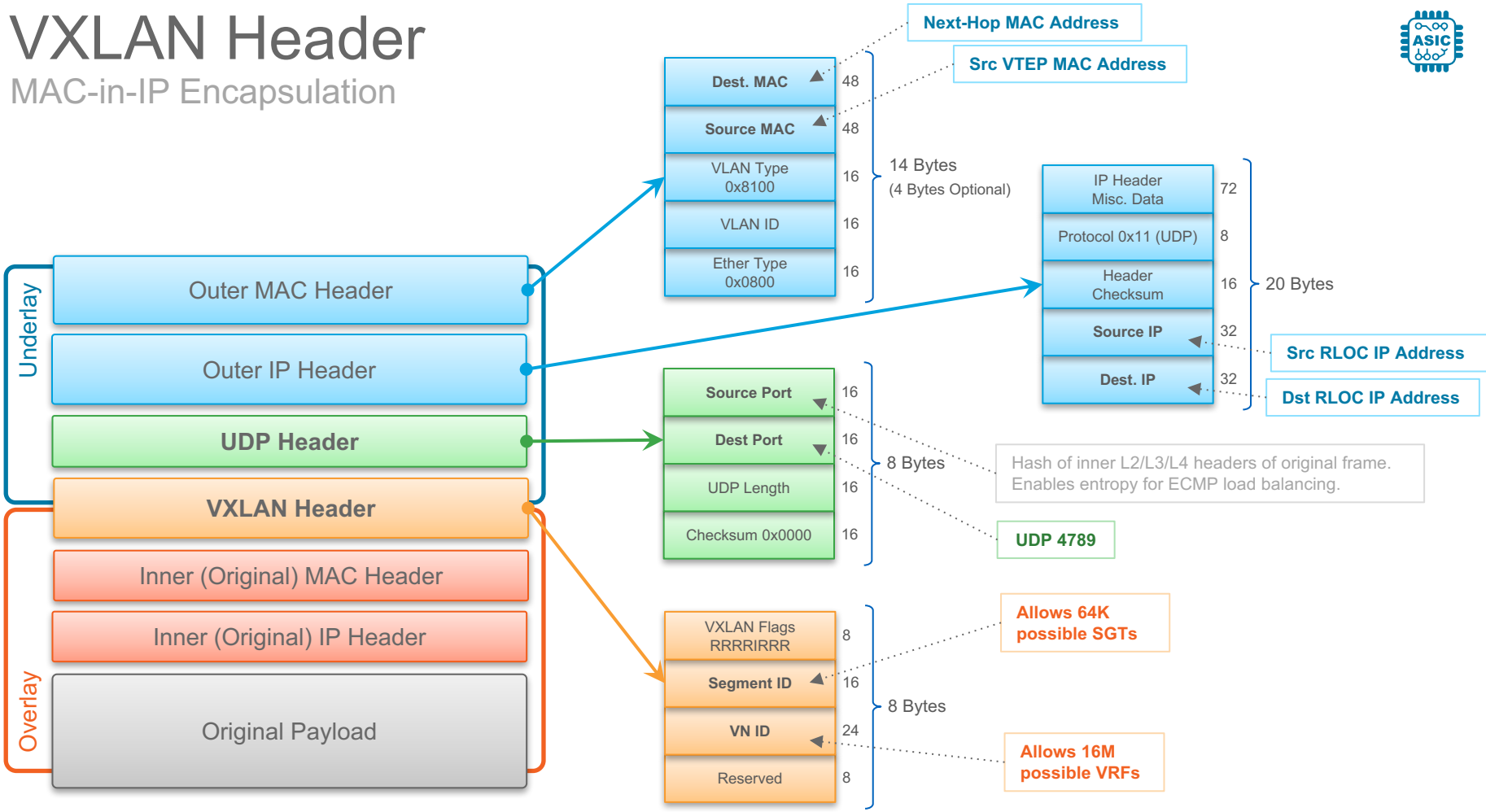
Forwarding traffic across fabric

1. **Control-Plane based on LISP**
2. **Data-Plane based on VXLAN**

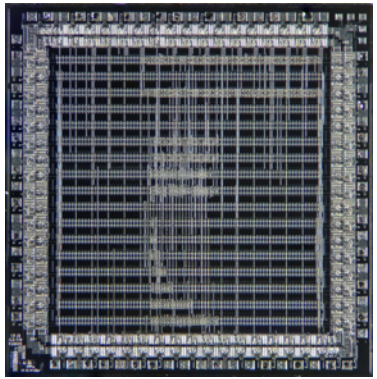


VXLAN Header

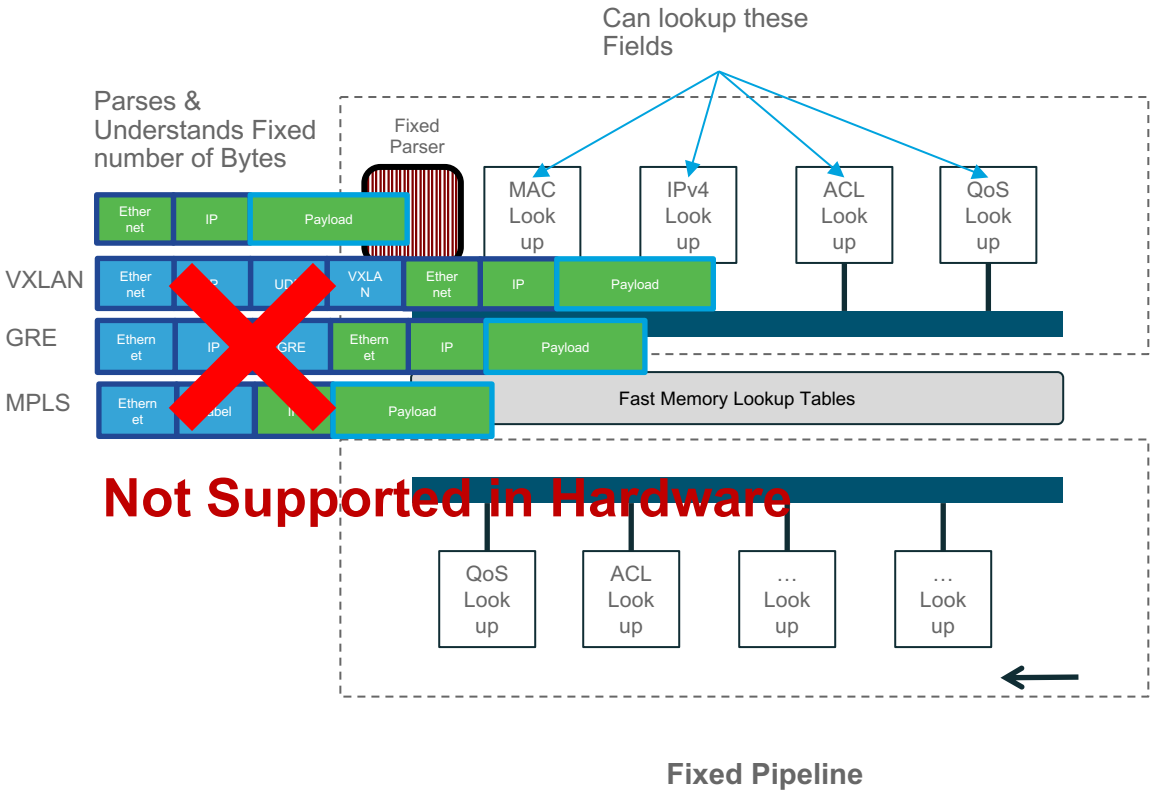
MAC-in-IP Encapsulation



Traditional ASIC Pipeline



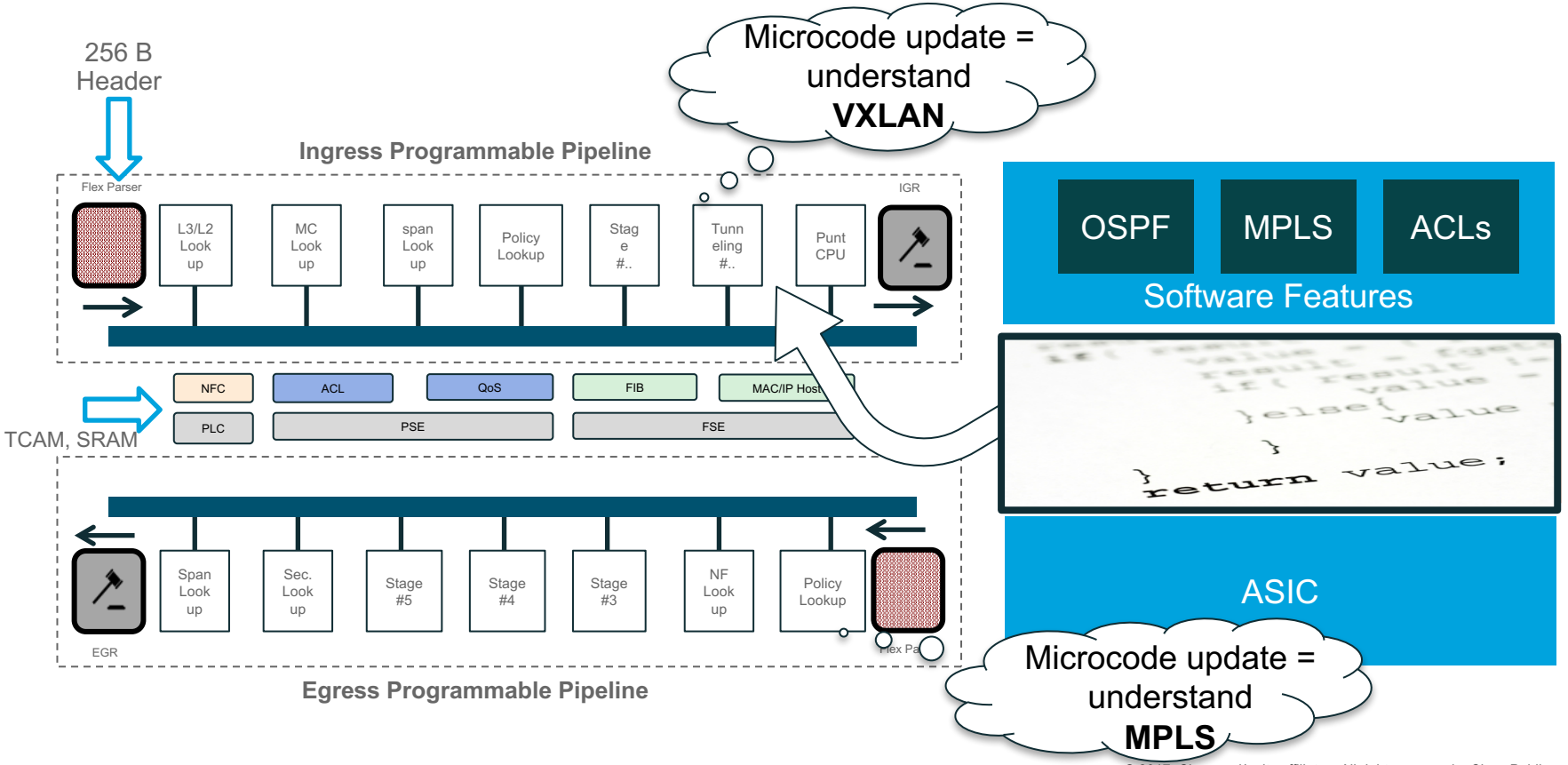
Traditional ASIC



Fixed Pipeline

Building a new ASIC takes a lot of time

UADP ASIC – Programmable Protocol Independent Packet Processor



UADP 1.0

External Name

First Generation of UADP ASIC

1G/10G
Ethernet

128 Bit
Encryption

24K
Netflow Records

240G
Stacking Capacity

6MB
Packet Buffer

56G
Bandwidth

Catalyst
3850 Copper

Catalyst
3650

Catalyst SFP
Fiber

First Programmable ASIC

UADP 1.1

External Name

Dual Core
Running @ 500MHz

1G/10G/40G
Ethernet

256 Bit
MACSEC
Encryption

24K x2
Netflow Records

1588
IEEE

240G
Stacking Capacity

6MB x2
Packet Buffer

148GE
Bandwidth

Catalyst 3850
Multigigabit

Catalyst 3850
SFP+

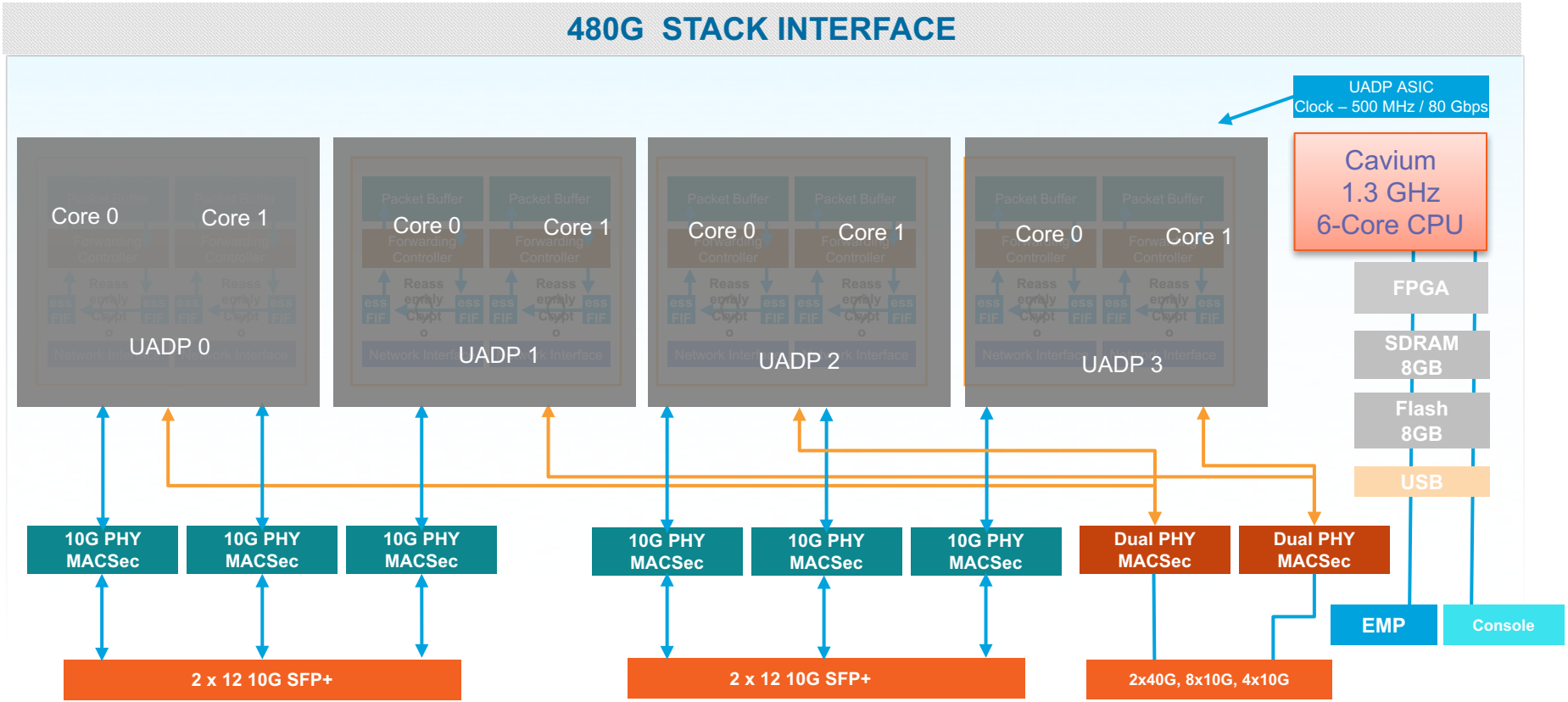
Catalyst 3650
Mini

Catalyst 3650
Multigigabit

Enhanced Version of UADP ASIC

Enhanced Power & Security Capability

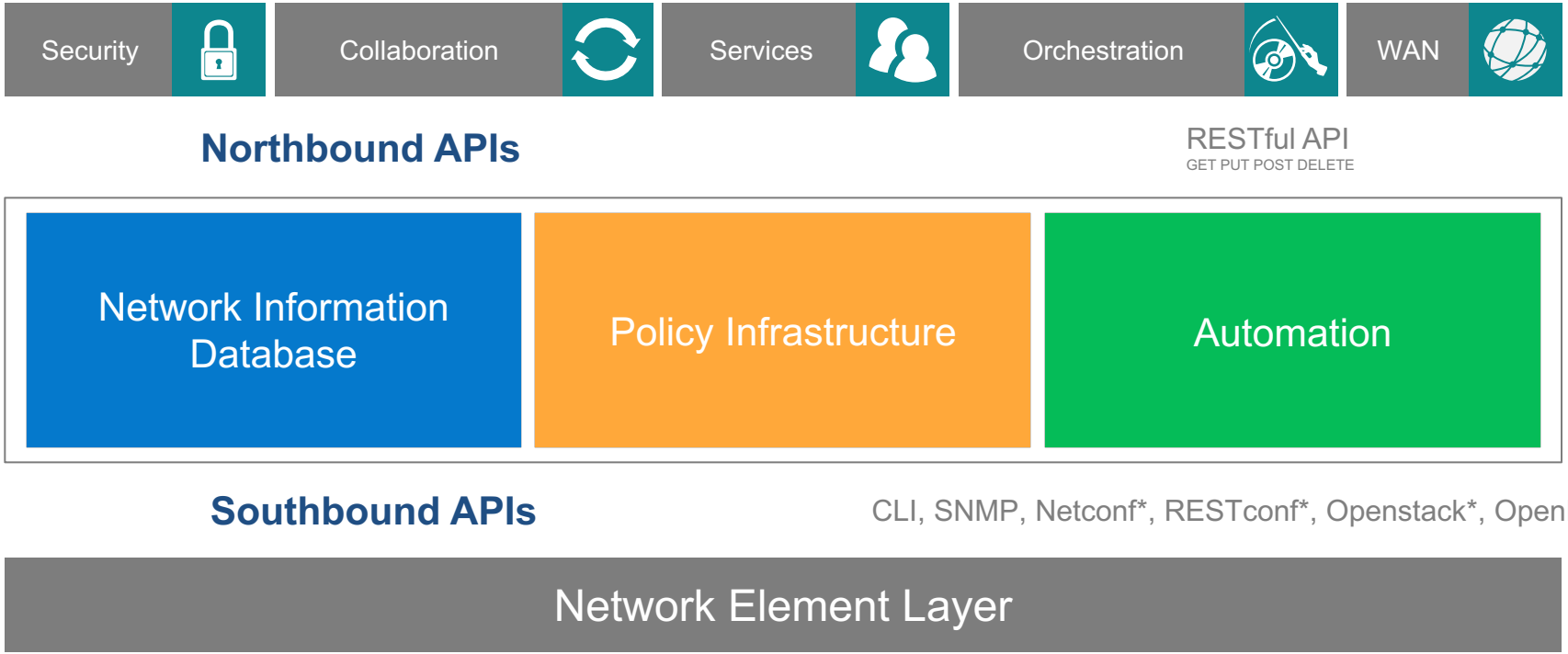
Catalyst 3850 SFP+ 48 Port – Block Diagram



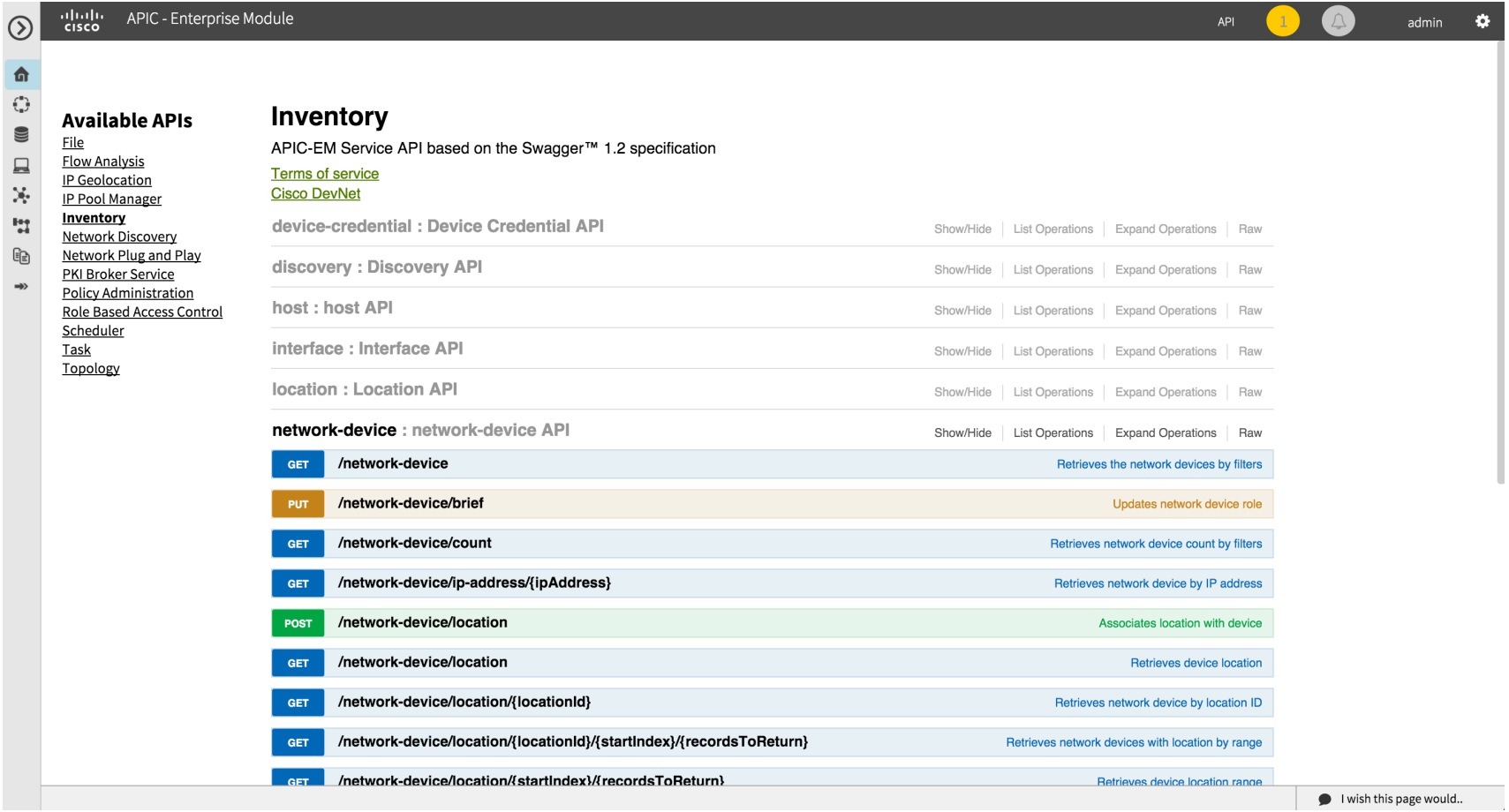
Automation in campus networks using APIC-EM

(Application Policy Infrastructure Controller Enterprise Module)

APIC-EM: High-Level Controller Architecture



Swagger



Try it out!!!

GET `/network-device/count` — Retrieves network device count by filters

Implementation Notes

Gets the count of network devices filtered by management IP address, mac address, hostname and location name

Response Class

Model | Model Schema

```
CountResult {
  version (string, optional),
  response (integer, optional)
}
```

Response Content Type: application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
scope	All	**Authorization Scope for RBAC**	header	List

Error Status Codes

HTTP Status Code	Reason
200	This Request is OK
403	This user is Forbidden Access to this Resource
401	Not Authorized Yet, Credentials to be supplied
404	No Resource Found

Try it out! Hide Response

Request URL

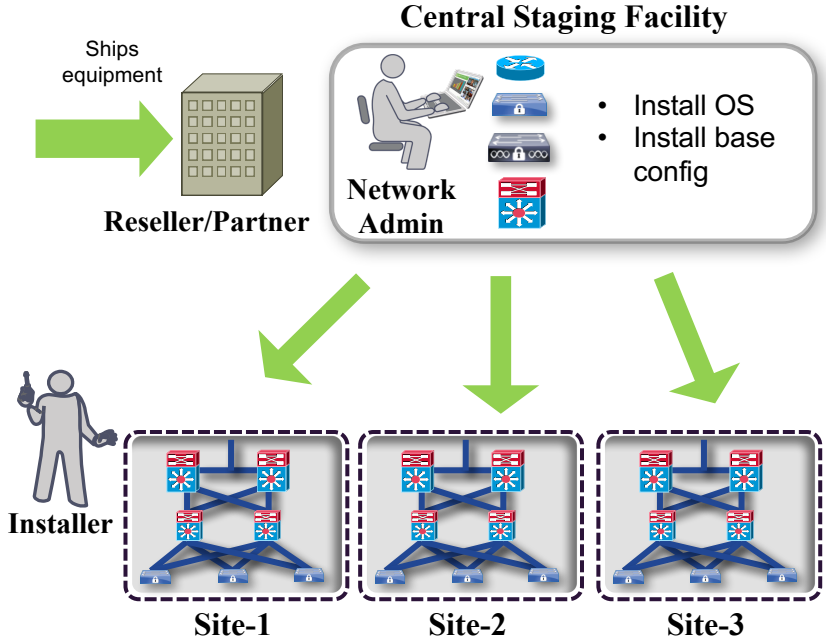
```
https://10.49.208.171/api/v1/network-device/count
```

Response Body

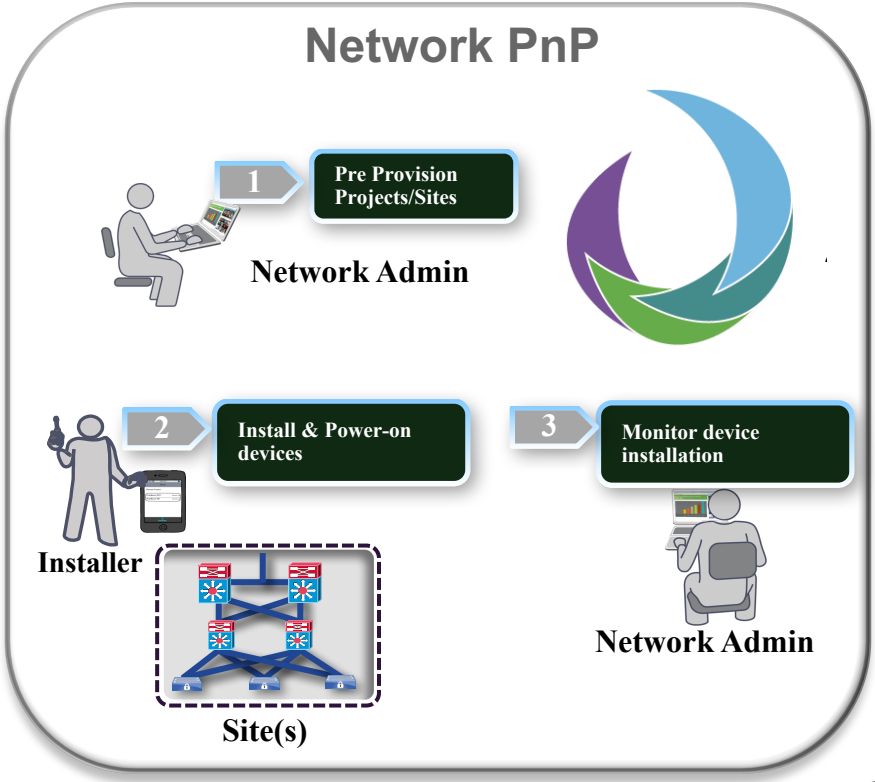

```
{
  "response": 17,
  "version": "1.0"
}
```

Network Plug-n-Play – for Zero Touch Deployment

Today's Process



Network PnP



Unskilled Installer

GUI Based

Consistent for devices & PIN(Campus/Branch)

Secure

Greenfield & Brownfield

Day 0

Network Plug and Play (PnP) – Components

PnP Helper App

[Optional]

Delivers bootstrap, status and troubleshooting checks

Redpark RJ45
Apple 8pin

Redpark RJ45
Apple 30pin

GetConsole
Airconsole2.0
Bluetooth Adapter

Cloud Redirect Service

[Optional]

Roadmap Phase 2

PnP Server

Central Server on APIC-EM

Manages sites, devices, images, licenses, workflow

Provides Northbound REST APIs

PnP Protocol

Runs between Agent and Server

Open Schema

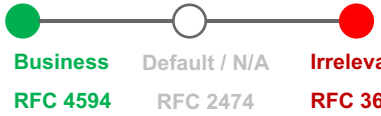
PnP Agent

Runs on Cisco® switches, routers, and wireless access points

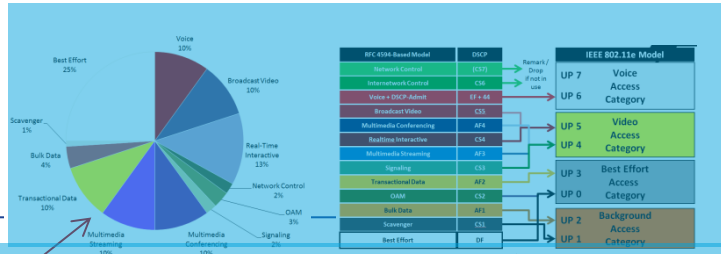
Discovers PnP server using DHCP, DNS, USB stick, PnP Helper App

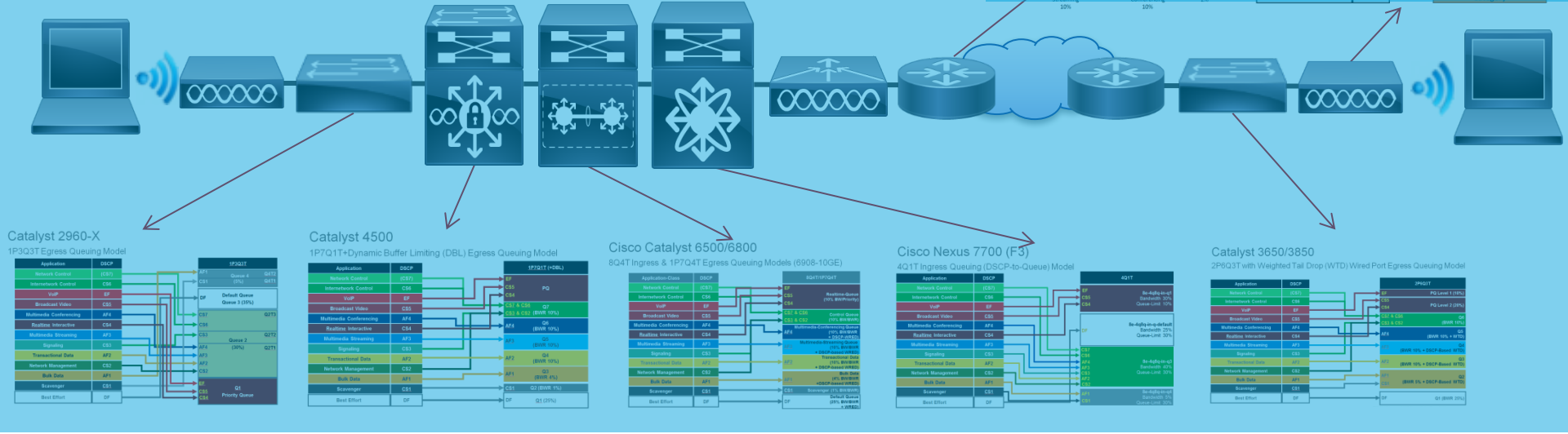
Automates the deployment process

Provision End-to-End DSCP-based Queuing



+ Cisco Validated Design {CVD} +





Catalyst 2960-X
1P3Q3T Egress Queuing Model

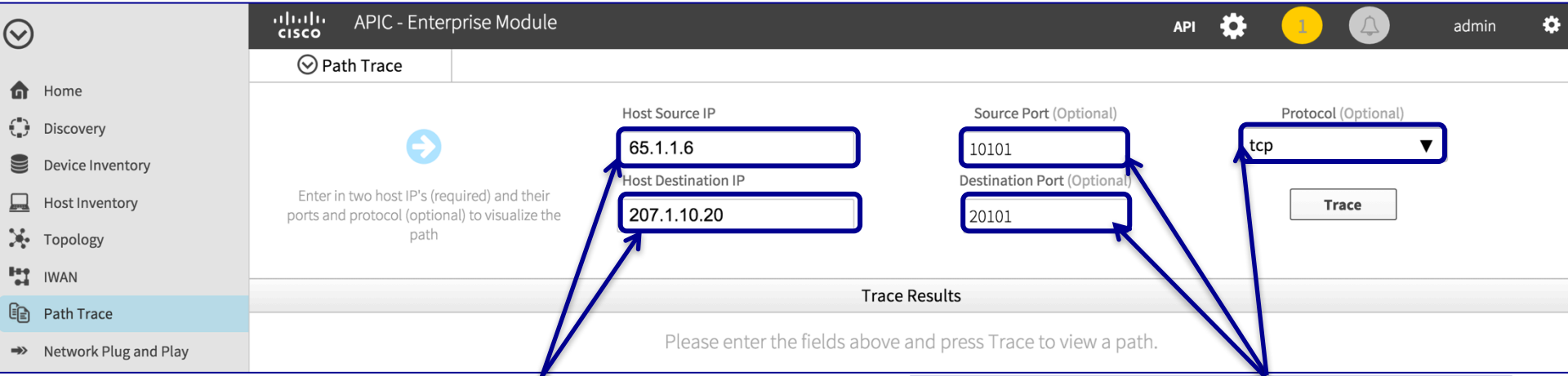
Catalyst 4500
1P7Q1T+Dynamic Buffer Limiting (DBL) Egress Queuing Model

Cisco Catalyst 6500/6800
8Q4T Ingress & 1P7Q4T Egress Queuing Models (6908-10GE)

Cisco Nexus 7700 (F3)
4Q1T Ingress Queuing (DSCP-to-Queue) Model

Catalyst 3650/3850
2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model

Path Visualization: 5-tuple Input via User Interface



Required Information

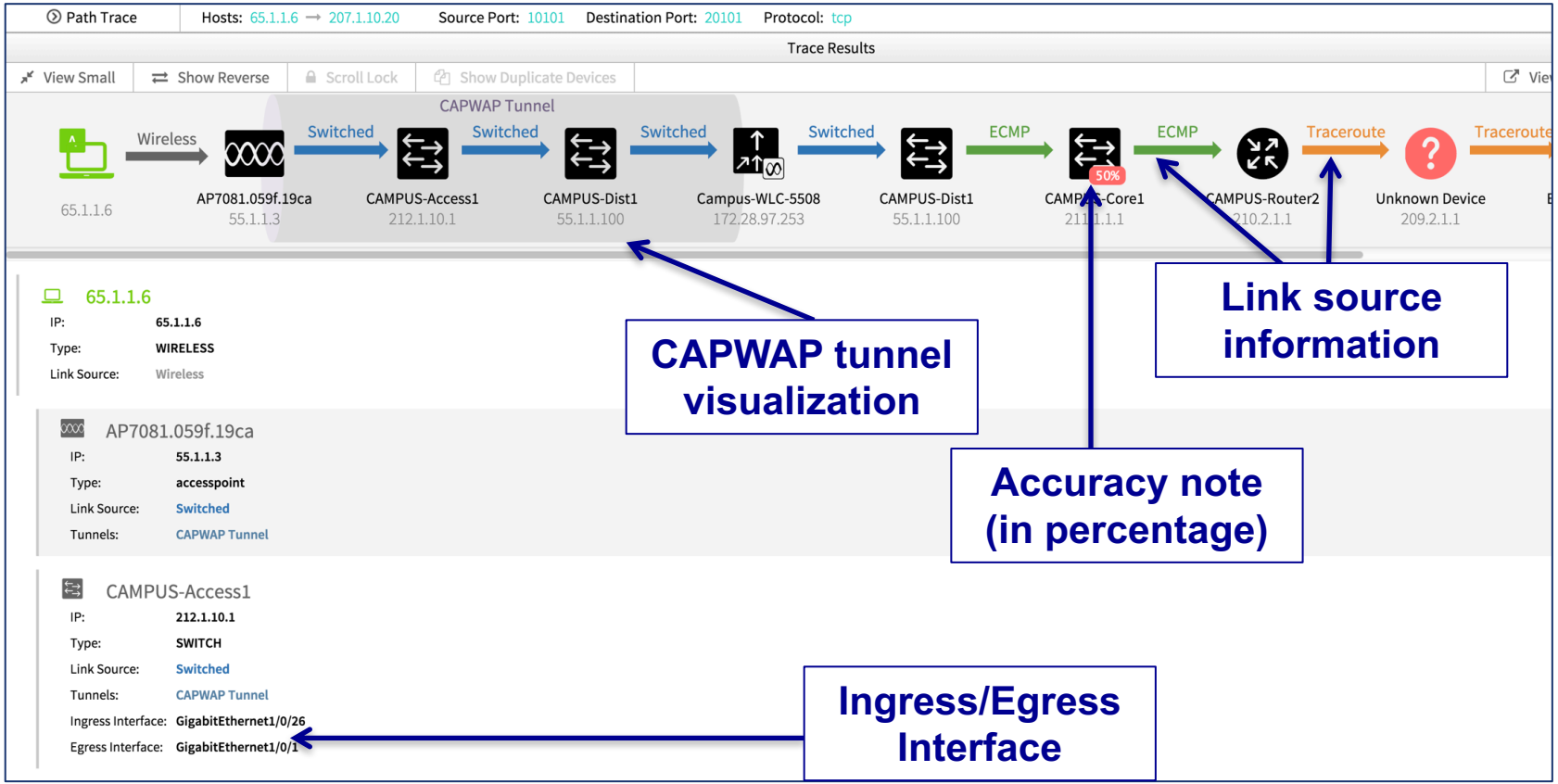
SRC and DEST IP Address [End-Host or L3 Interface]

Optional Information

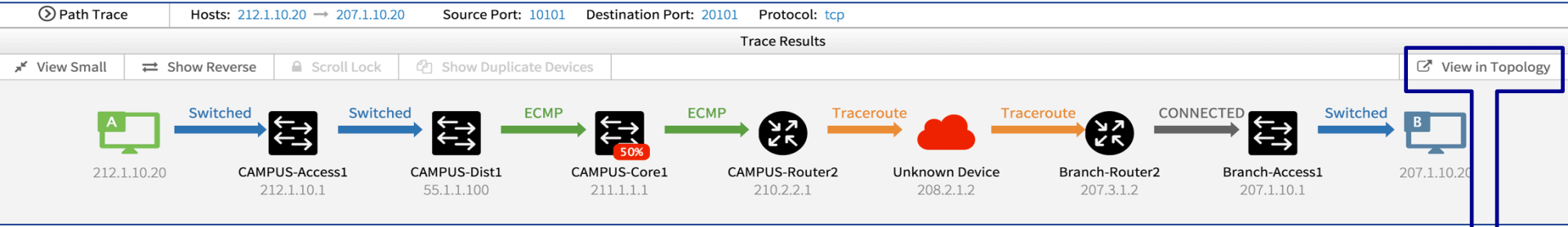
SRC and DST L4 Port Numbers; L4 Protocol (TCP or UDP)

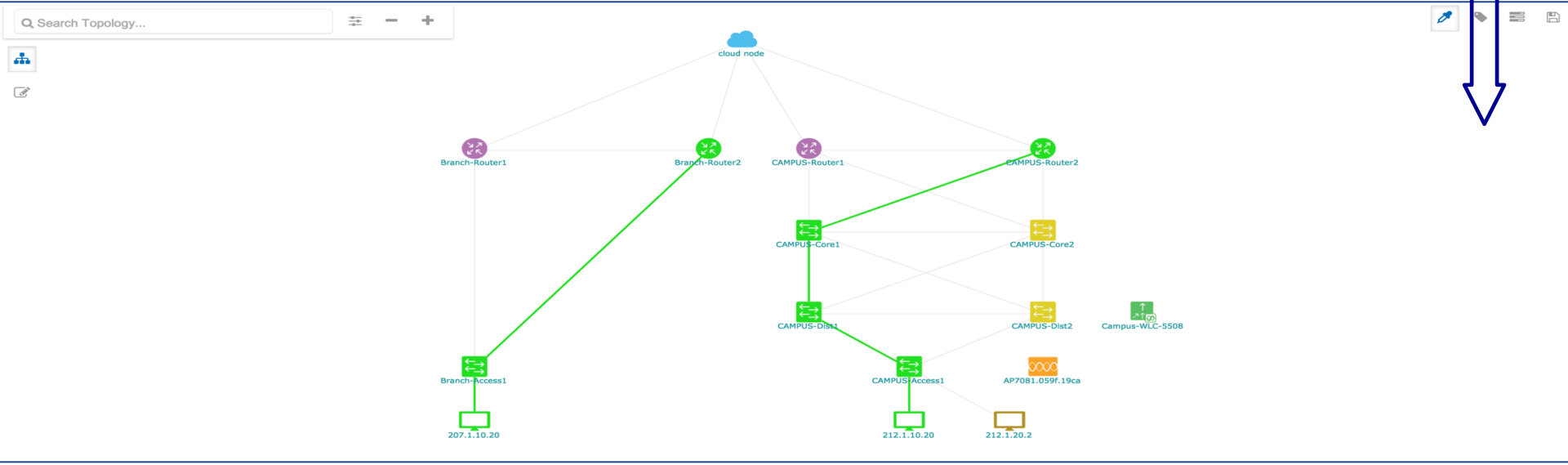
Note: L4 Port and Protocol information is optional but highly recommended for accurate path calculation

Path Visualization: Enhanced Application Flow Visibility

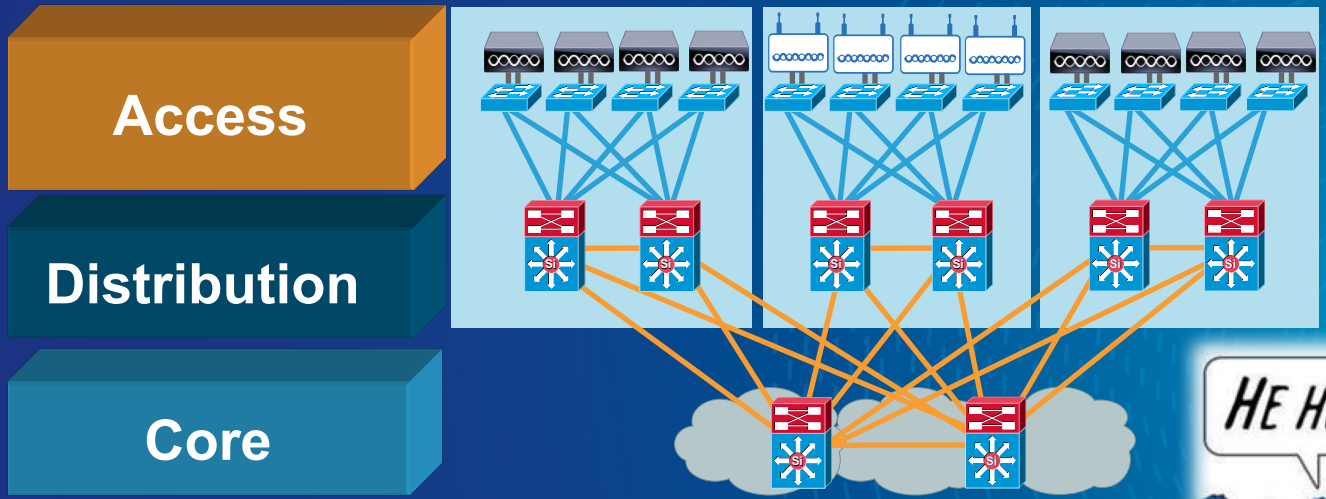


Path Visualization: Topology View





Agenda for today – Wireless access



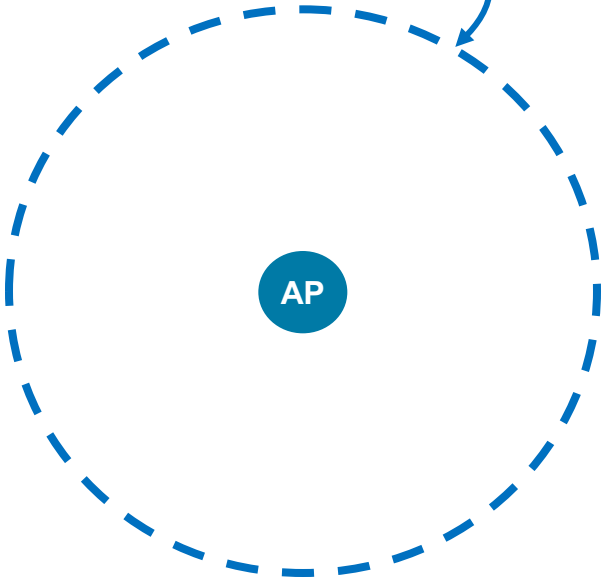
Real Life Example

Medical Center

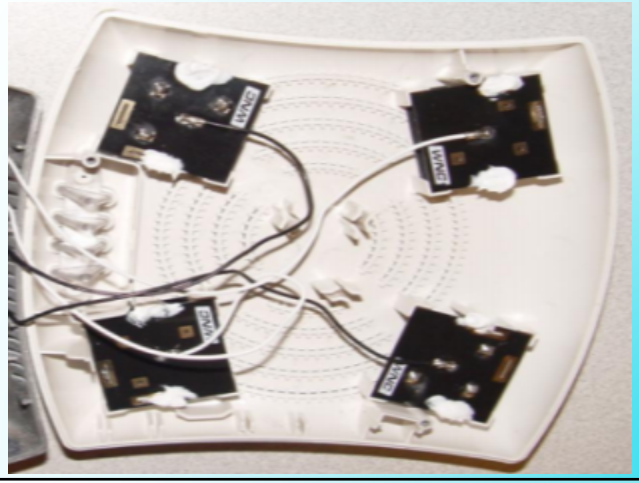
- Density studies show active 12 users / cell on average
  - Expected 2 HD video calls (Skype type)
  - 5 audio calls
  - Other users may browse
- Let's do the math:
  - 2 HD video calls = 1.2 Mbps x 2 x 2 ways = 4.8 Mbps
  - 5 audio calls… mmm what application?
    - Maybe SfB 30 kbps x 5 x 2 ways = 860 kbps
  - Others are browsing (5 people)… 250 kbps / user?
  - Total = ~**6.7 Mbps needed**

APs are capable for much more so design for best MOS/QoE (Quality of Experience)

I need 6.7 Mbps throughput everywhere in the cell
. . . therefore I need it here
(-67dBm voice/video,
-72dBm data only)



Everything starts from good AP quality…

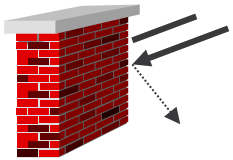
Competitor	Cisco AP
	
Off-the-Shelf plastic designs. Open air vent cooling. Poor Performance AP made with Consumer-grade Materials.	Sealed metal shell for heat-dissipation and durability. No air flow. High Performance Enterprise-Class AP with Reliable Coverage.

…and proper AP placement ☺

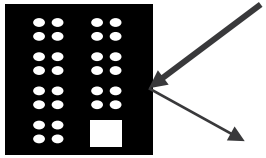
Source: www.bad-fi.com

Proper AP placement comes out of Site Survey

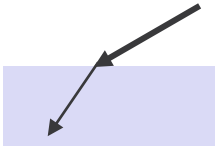
Because a lot happens in the air:



shadowing



reflection



refraction

scattering

diffraction

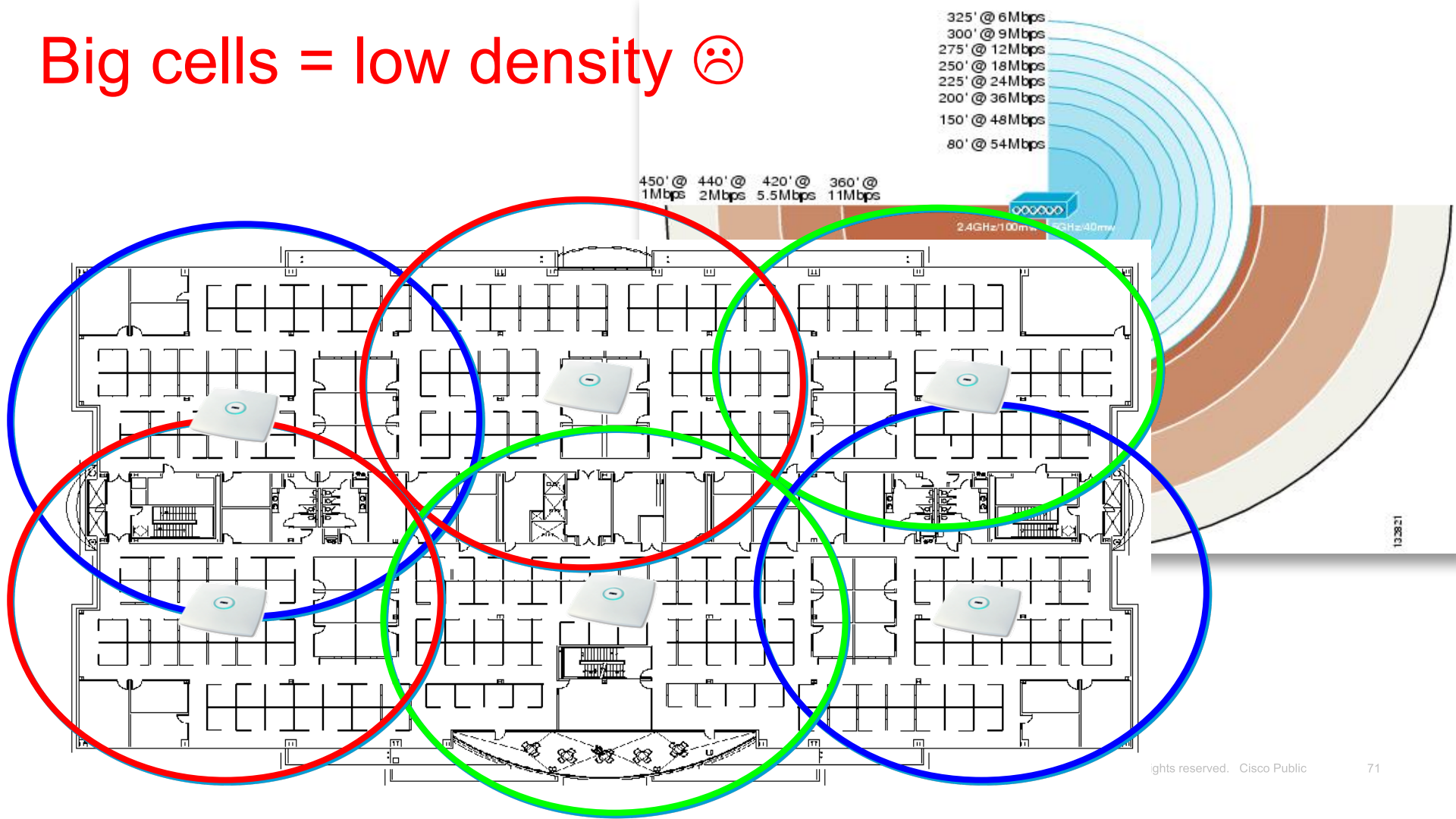
Predictive site surveys
(network plan, simulation) – How many APs, Where, What power, channels, antennas

Pre-Deployment site surveys
(AP on a stick) – Where to physically mount APs, How does real RF look like, is there any wifi/non-wifi interference

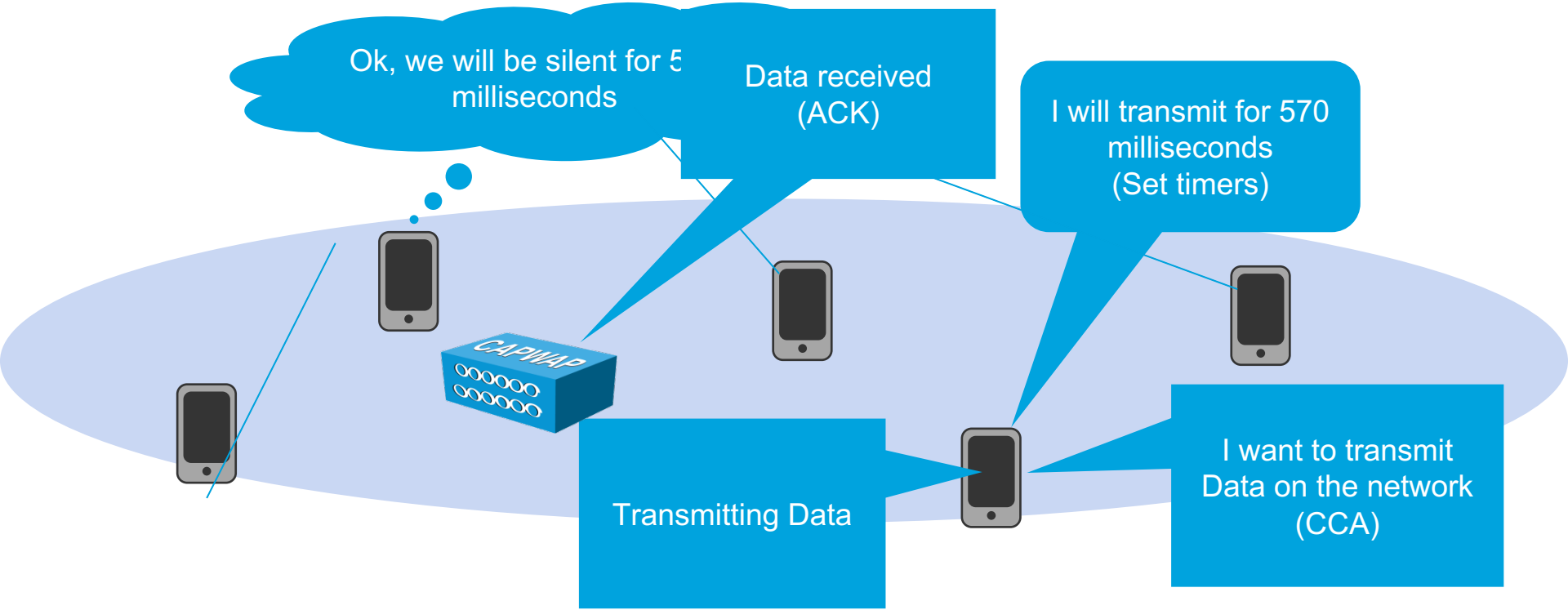
Post-Deployment site surveys
(validation) – Does the network actually work?

Periodic site surveys
(health check) – If the network does not work, what has changed?

Big cells = low density ☹

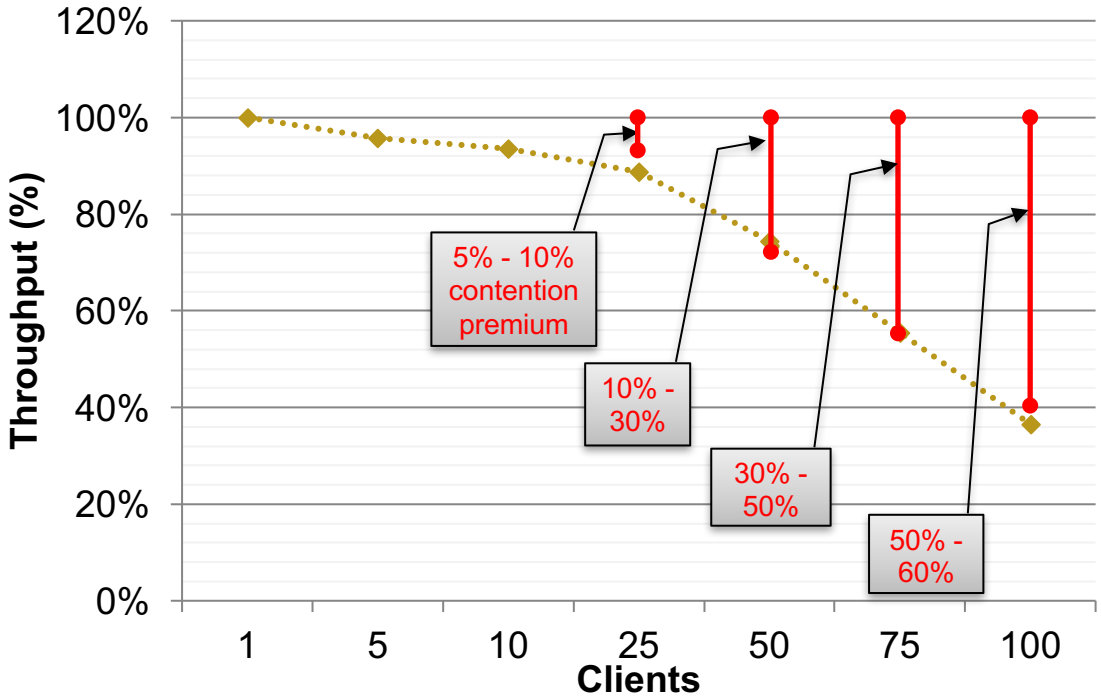


Accessing the Medium: EDCA & CSMA/CA



How Much Does Contention Affect Performance

The Breaking Point Depends on How Many Clients You Have



As more clients associate and transmit, WLAN contention increases for all clients. Retry attempts increase and each station spends more and more time in the "waiting and listening" state, driving down performance

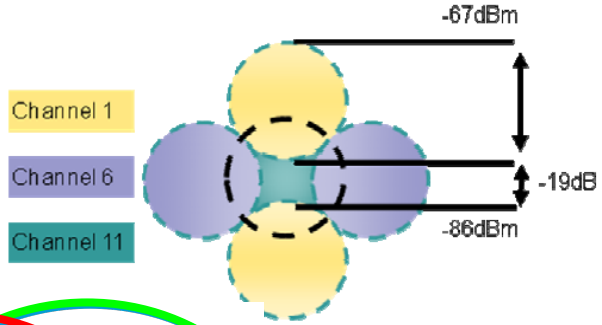
(source: IEEE 802.11-15/0351r2)

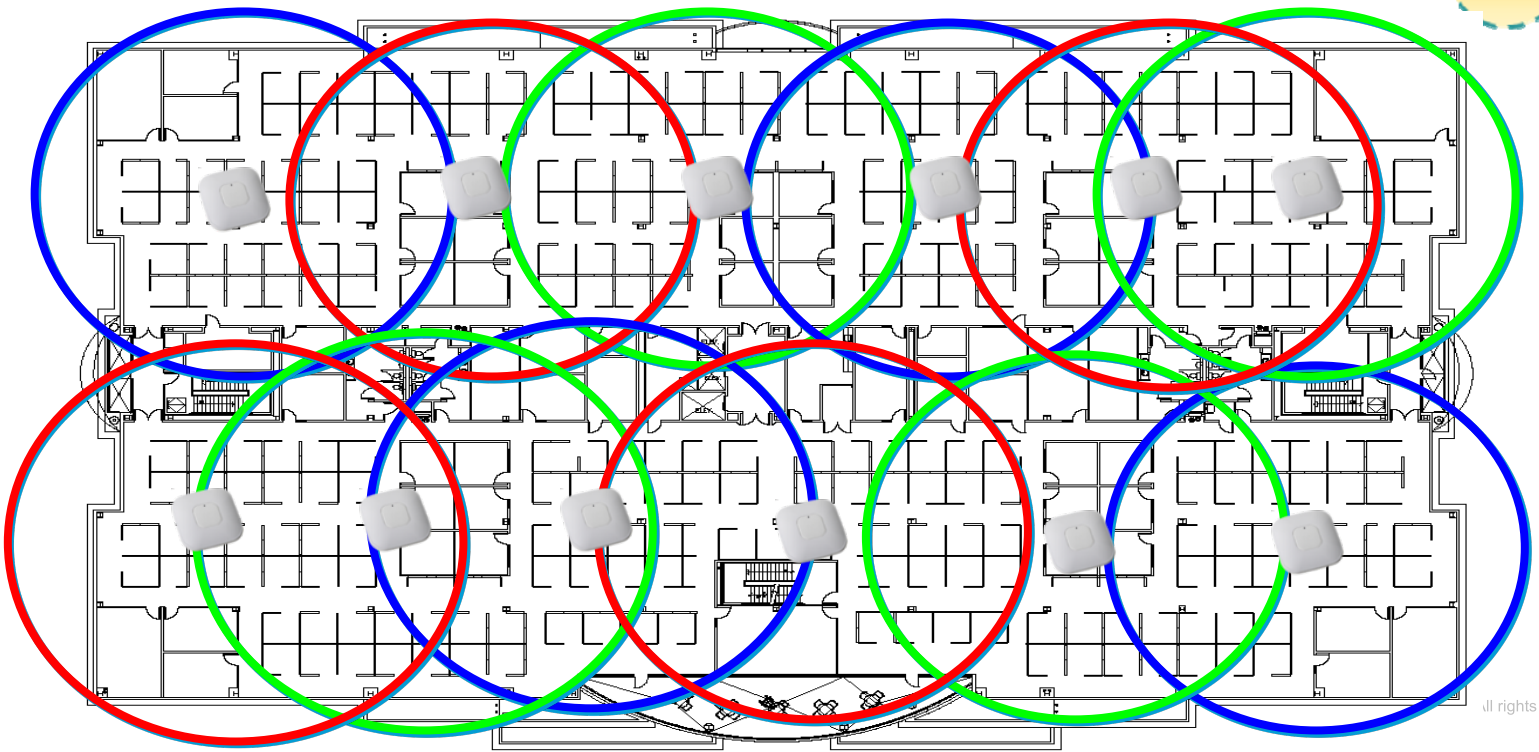
73

Very High Channel Utilization – Cisco CleanAir

Unhealthy Network

Smaller cells = more density ☺





Beefing Up Wireless…

BEST OF INTEROP

http://nsashow.com/FRA/
http://nsashow.com/Hyperlocation/

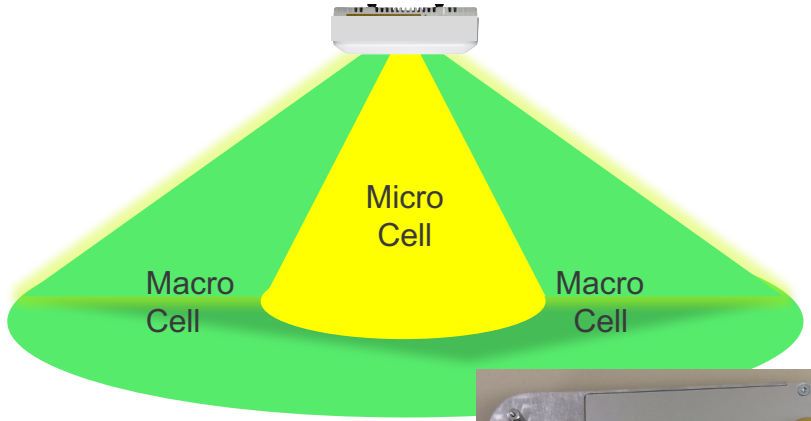
2010	2015	2016
Cisco AP3500 with **CleanAir Technology**	Cisco **Hyperlocation** Module	Cisco **Flexible Radio Assignment**

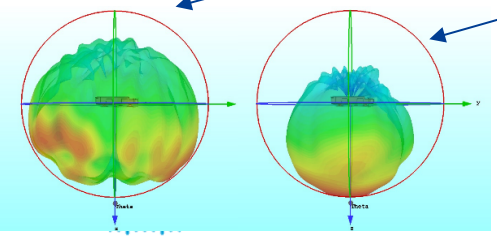
… Dual 5GHz is King!!!

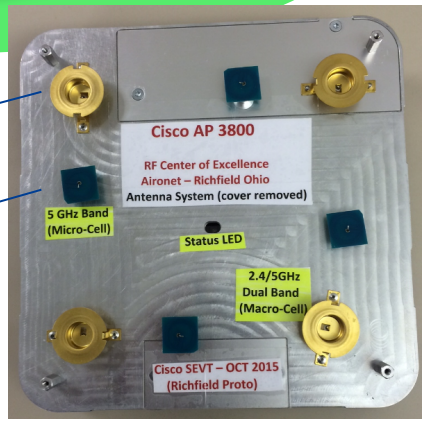
http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/802-11ac-solution/miercom-report-cisco-aruba-wave.pdf

Dual 5GHz – Macro/Micro Cell

Improves Client Performanceand Capacity







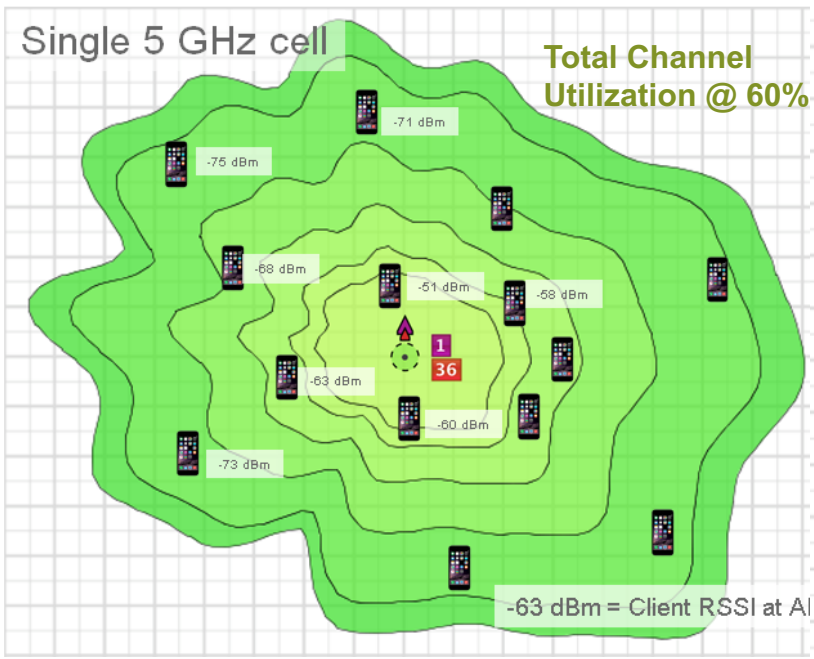
- Improves the Effective Spectrum Usage
- Micro-Radio
  - High Performance 802.11ac Clients near the AP at 802.11ac data rates
  - Excellent speed and performance
- Macro-Radio
  - All legacy Clients join macro-cell

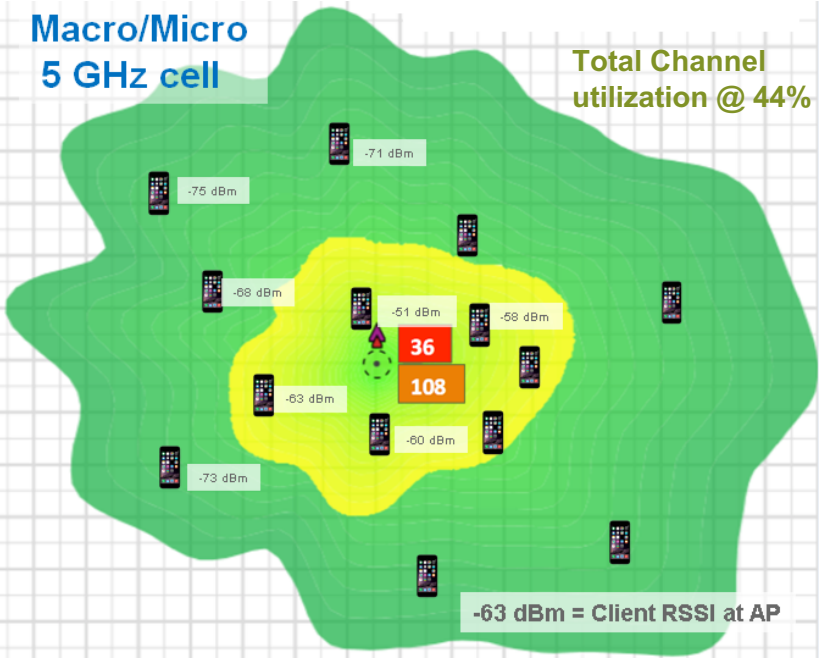
but …

- Cells must be isolated
  – overlap in RF Frequency = shared airtime = lost efficiency
- Begins in the Silicon design, extends to the AP/Antenna selections

Users have a better overall experience on a Dual 5GHz Access Point

Single Cell versus Macro/Micro Cell





Single channel 36 utilization at 60% (clients far away take longer airtime)

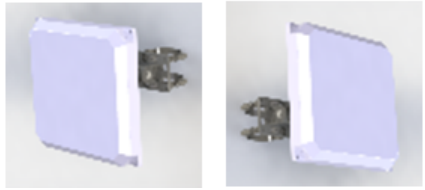
Using Micro/Macro (Dual 5 GHz) Channel 36 @ 20% & Channel 108 @ 24%

Take-away -- LESS retries, faster data-rates & less channel utilization

Now let's look at External Antenna Models

Dual 5 GHz “E” model Macro-Macro cells or Micro-Micro cells or any combination

Cable allows for secondary 5 GHz radio antenna to be physically spaced away from the primary radio allowing for Macro-Macro operation



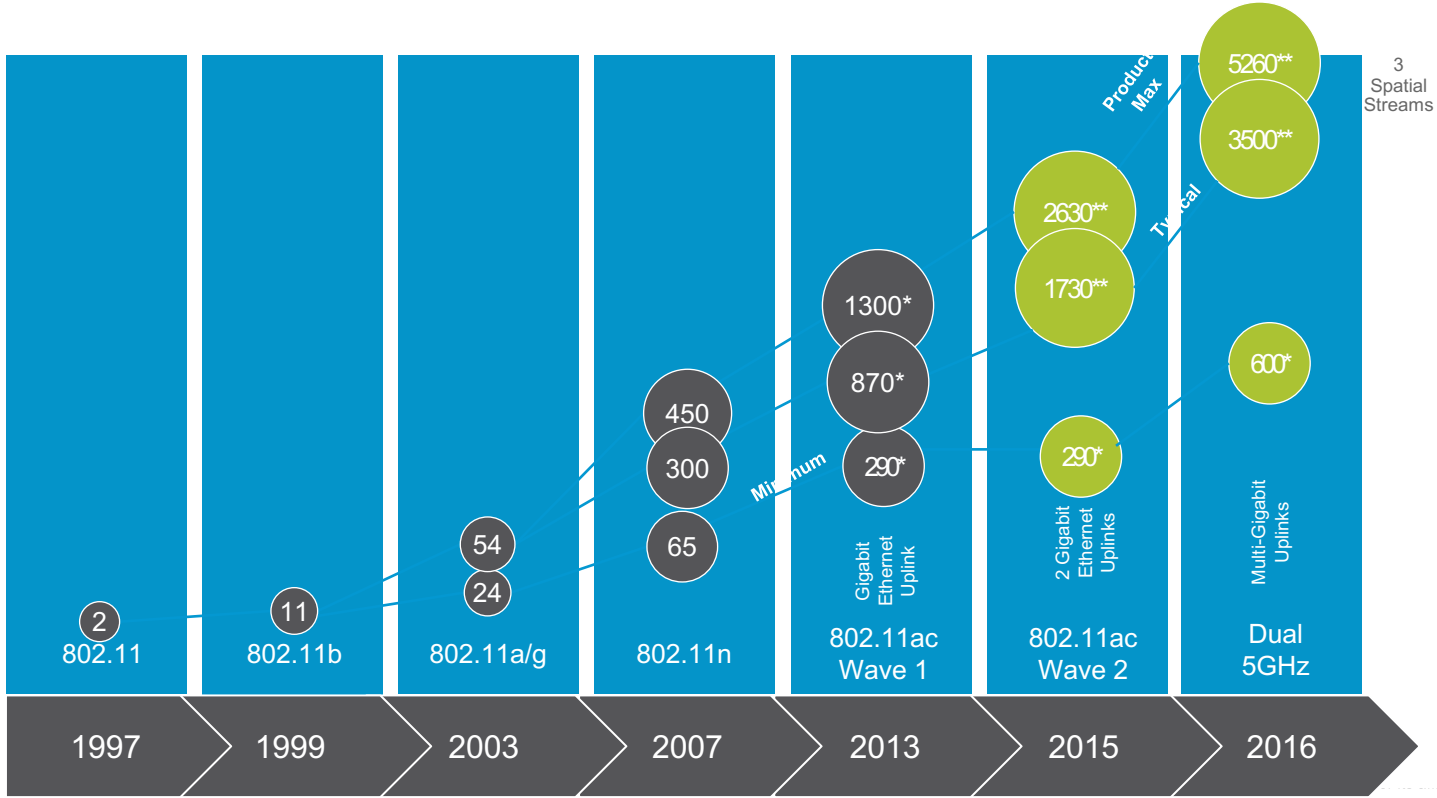
Stadium antenna deployments for different coverage areas or higher density areas

ANT-2566 in different directions or even back-to-back tilted downward for Factory and warehouse deployments

Omni + directional deployments

Wi-Fi Connectivity Speed Timeline

Gigabit Wi-Fi As Primary Access



3SS	Desktops / Laptops
2SS	Laptops / Tablets
1SS	Tablets / Smartphones

● = Connect Rates (Mbps)

SS = Spatial Streams

*Assuming 80 MHz channel is available and suitable

**Assuming 160 MHz channel is available and suitable

802.11ac Data Rates @ 1,2 & 3 Spatial Streams (Wave1)

802.11n was 450 Mbps at 40 MHz bonded @ 3-SS.

.11ac can achieve nearly the same speed @ 1-Spatial Stream

MCS	Modulation	Ratio	20 MHz channel	40 MHz channel	80 MHz channel WAVE-1
			400 ns GI	400 ns GI	400 ns GI
0	BPSK	1/2	7.2	15	32.5
1	QPSK	1/2	14.4	30	65
2	QPSK	3/4	21.7	45	97.5
3	16-QAM	1/2	28.9	60	130
4	16-QAM	3/4	43.3	90	195
5	64-QAM	2/3	57.8	120	260
6	64-QAM	3/4	65	135	292.5
7	64-QAM	5/6	72.2	150	325
8	256-QAM	3/4	86.7	180	390
9	256-QAM	5/6	N/A	200	433.3

802.11ac rates @ 1 Spatial Stream

802.11ac Data Rates — XX RATE NOT SUPPORTED

				Mb/s					
				20 MHz		40 MHz		80 MHz	
				Guard	Interval	Guard	Interval	Guard	Interval
Spatial Streams	MCS Index	Modulation	Coding	800ns	400ns	800ns	400ns	800ns	400ns
2	0	BPSK	1/2	13	14.4	27	30	58.5	65
	1	QPSK	1/2	26	28.9	54	60	117	130
	2	QPSK	3/4	39	43.3	81	90	175.5	195
	3	16-QAM	1/2	52	57.8	108	120	234	260
	4	16-QAM	3/4	78	86.7	162	180	351	390
	5	64-QAM	2/3	104	115.6	216	240	468	520
	6	64-QAM	3/4	117	130	243	270	526.5	585
	7	64-QAM	5/6	130	144.4	270	300	585	650
	8	256-QAM	3/4	156	173.3	324	360	702	780
	9	256-QAM	5/6	XX	XX	360	400	780	866.7
3	0	BPSK	1/2	19.5	21.7	40.5	45	87.8	97.5
	1	QPSK	1/2	39	43.3	81	90	175.5	195
	2	QPSK	3/4	58.5	65	121.5	135	263.3	292.5
	3	16-QAM	1/2	78	86.7	162	180	351	390
	4	16-QAM	3/4	117	130	243	270	526.5	585
	5	64-QAM	2/3	156	173.3	324	360	702	780
	6	64-QAM	3/4	175.5	195	364.5	405	XX	XX
	7	64-QAM	5/6	195	216.7	405	450	877.5	975
	8	256-QAM	3/4	234	260	486	540	1053	1170
	9	256-QAM	5/6	260	288.9	540	600	1170	1300

Using Wave-2 & 4SS

.11ac MCS rates (unlike 802.11n) don't exceed 0-9 -- but rather it is 0-9 and then you call out how many Spatial Streams

1 stream (80MHz) is 433 Mbps
2 stream (80MHz) is 866 Mbps
3 stream (80MHz) is 1300 Mbps
4 stream (80 MHz) is 1733 Mbps (Wave 2)
3 stream (160 MHz) is 2340 Mbps (Wave 2)

Note: While 4-SS appears attractive, it is very difficult to maintain a 4-SS link given you cannot beam-form a 4-SS signal given you only have 4 antennas

Beamforming requires N+1 antennas

802.11ac Data Rates — * RATE NOT SUPPORTED — Mb/s

Spatial Streams	MCS Index	Modulation	Coding	20 MHz Guard 800ns	20 MHz Guard 400ns	40 MHz Guard 800ns	40 MHz Guard 400ns	80 MHz Guard 800ns	80 MHz Guard 400ns	160 MHz Guard 800ns	160 MHz Guard 400ns
2	0	BPSK	1/2	13	14.4	27	30	58.5	65	117	130
	1	QPSK	1/2	26	28.9	54	60	117	130	234	260
	2	QPSK	3/4	39	43.3	81	90	175.5	195	351	390
	3	16-QAM	1/2	52	57.8	108	120	234	260	468	520
	4	16-QAM	3/4	78	86.7	162	180	351	390	702	780
	5	64-QAM	2/3	104	115.6	216	240	468	520	936	1040
	6	64-QAM	3/4	117	130	243	270	526.5	585	1053	1170
	7	64-QAM	5/6	130	144.4	270	300	585	650	1170	1300
	8	256-QAM	3/4	156	173.3	324	360	702	780	1404	1560
	9	256-QAM	5/6	*	*	360	400	780	866.7	1560	1733.3
3	0	BPSK	1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195
	1	QPSK	1/2	39	43.3	81	90	175.5	195	351	390
	2	QPSK	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
	3	16-QAM	1/2	78	86.7	162	180	351	390	702	780
	4	16-QAM	3/4	117	130	243	270	526.5	585	1053	1170
	5	64-QAM	2/3	156	173.3	324	360	702	780	1404	1560
	6	64-QAM	3/4	175.5	195	364.5	405	*	*	1579.5	1755
	7	64-QAM	5/6	195	216.7	405	450	877.5	975	1755	1950
	8	256-QAM	3/4	234	260	486	540	1053	1170	2106	2340
	9	256-QAM	5/6	260	288.9	540	600	1170	1300	*	*
4	0	BPSK	1/2	26	28.9	54	60	117	130		
	1	QPSK	1/2	52	57.8	108	120	234	260		
	2	QPSK	3/4	78	86.7	162	180	351	390		
	3	16-QAM	1/2	104	115.6	216	240	468	520		
	4	16-QAM	3/4	156	173.3	324	360	702	780		
	5	64-QAM	2/3	208	231.1	432	480	936	1040		
	6	64-QAM	3/4	234	260	486	540	1053	1170		
	7	64-QAM	5/6	260	288.9	540	600	1170	1300		
	8	256-QAM	3/4	312	346.7	648	720	1404	1560		
	9	256-QAM	5/6	*	*	720	800	1560	1733.3		

Not all Wave-2 products support 160 MHz

MCS values achieved by clients at various SNR levels

Protocol	Channel	1	2	3	4	5	6	7	8	9	10
802.11b	20MHz	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1
802.11a/g	20MHz	None	MCS 0	MCS 0	MCS 1	MCS 2	MCS 2	MCS 2	MCS 2	MCS 3	MCS 3
802.11n	20MHz	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2
802.11n	40MHz	None	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1
802.11ac	20MHz	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2
802.11ac	40MHz	None	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1
802.11ac	80MHz	None	None	None	None	None	None	None	MCS 0	MCS 0	MCS 0
802.11ac	160MHz	None	None	None	None	None	None	None	None	None	None

Modulation Key
None = Grey
BPSK = Red
QPSK = Orange
16-QAM = Yellow
64-QAM = Blue
256-QAM = Green

SNR in dB		11	12	13	14	15	16	17	18	19	20
802.11b	20MHz	MCS 2	MCS 2	MCS 2	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 4	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 5	MCS 6	MCS 6	MCS 7
802.11n	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6
802.11n	40MHz	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4
802.11ac	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6
802.11ac	40MHz	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4
802.11ac	80MHz	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3
802.11ac	160MHz	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2	MCS 3

802.11 Type Key
802.11b
802.11ag
802.11n
802.11ac

SNR in dB		21	22	23	24	25	26	27	28	29	30
802.11b	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	20MHz	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	40MHz	MCS 5	MCS 5	MCS 6	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7
802.11ac	20MHz	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7	MCS 7	MCS 8	MCS 8
802.11ac	40MHz	MCS 5	MCS 5	MCS 6	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7
802.11ac	80MHz	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6	MCS 6	MCS 6	MCS 6	MCS 6
802.11ac	160MHz	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6	MCS 6

SNR in dB		31	32	33	34	35	36	37	38	39	40
802.11b	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	40MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11ac	20MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	40MHz	MCS 7	MCS 8	MCS 8	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	80MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 8	MCS 8	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	160MHz	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7	MCS 7	MCS 8	MCS 8	MCS 9

SNR in dB		41	42	43	44	45	46	47	48	49	50
802.11b	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	40MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11ac	20MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	40MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	80MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	160MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9

http://www.wlanpros.com/mcs-index-802-11n-802-11ac-chart-3/

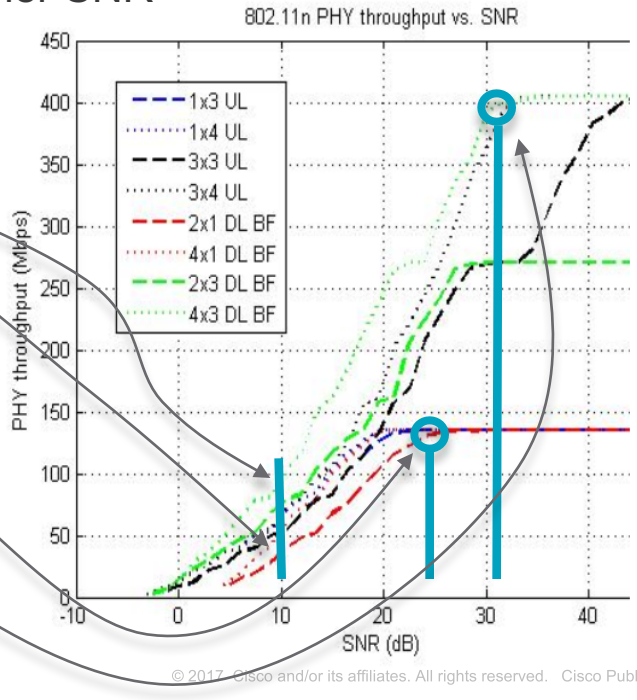
Multiple Streams Make SNR Requirement Higher

- Do not think that multiple stream devices are always better
- They may have higher power, but also require higher SNR

e.g.: 4 streams gives you a higher throughput at same SNR level, than 2 streams

BUT the 2 stream device reaches its max speed at 24 dB SNR,
while the 4 stream device needs 30+ dB

Conclusion: at same distance from the AP, multiple stream devices will operate faster than single stream device, but each individual stream is slower



So how do these data rates apply in the real world?

Smartphones 210 Mbps*

1 stream (80MHz) is 433 Mbps

Tablets 460 Mbps*

2 stream (80MHz) is 866 Mbps

High End Laptops +680 Mbps*

3 stream (80MHz) is 1300 Mbps

4SS	Desktops
3SS	Desktops / Laptops
2SS	Laptops / Tablets
1SS	Tablets / Smartphones

Wave-2 with 4 stream (80 MHz) is 1733 Mbps
No 4-ss mobility clients exist in the market today only PCIe (desktop clients))

Real throughput changes dynamically based on number of spatial streams, channel bonding MCS (radio data-rate) negotiated

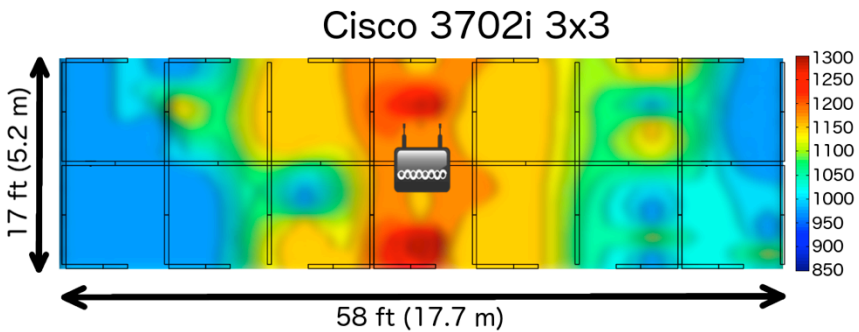
The actual throughput is less than the MCS data-rate due to overhead

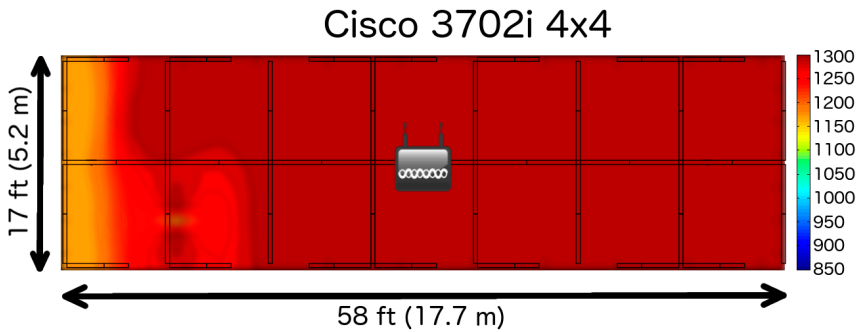
Note: The goal is to save physical size and battery life yet increase throughput

*Assumes 70% MAC efficiency and half duplex

Cisco ClientLink

- Cisco ClientLink is Beamforming at the chip level:
  - Implemented in hardware, no software component, no performance degradation
- ClientLink creates a better quality RF for all clients (a/g/n/ac)
- Do I need a 4x4 AP? Yes, and even more critical with 802.11ac





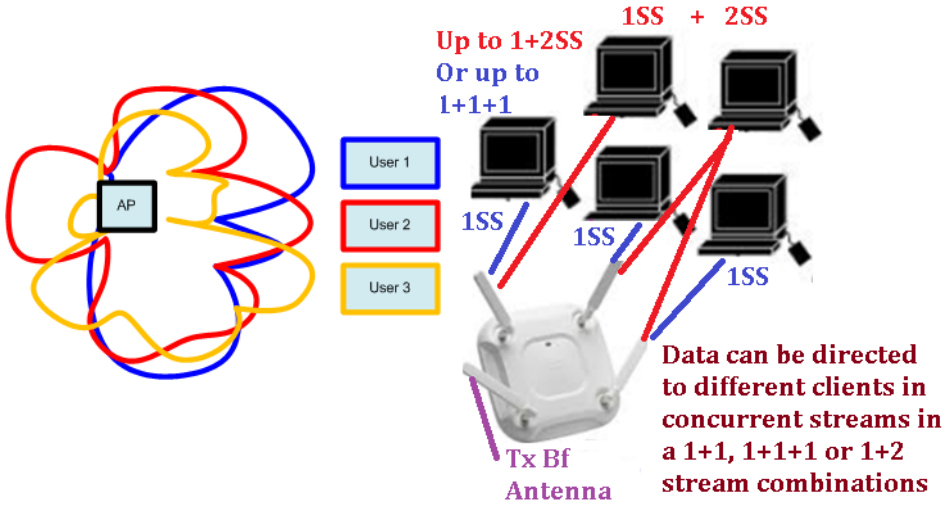
- Best practice: on by default

http://www.youtube.com/watch?v=0q_shbSpOIA

Downlink Data Rate Comparison				
Modulation	MCS	Data Rate (Mbps)	Cisco 3700 3x3	Cisco 3700 4x4
64QAM	m7	975	46%	0%
256QAM	m8	1170	49%	15%
256QAM	m9	1300	5%	85%

MU-MIMO Overview

Performs TxBF, while nulling and also sending similar size data packets using 4th antenna TxBF



AP is using the 4th antenna to beam-form and null. In reality the clients are ideally spaced apart around the AP and not clustered together like the diagram depicts.

Each Wave-2 client sends CSI (Channel State Information) about how to best beam-form to it.

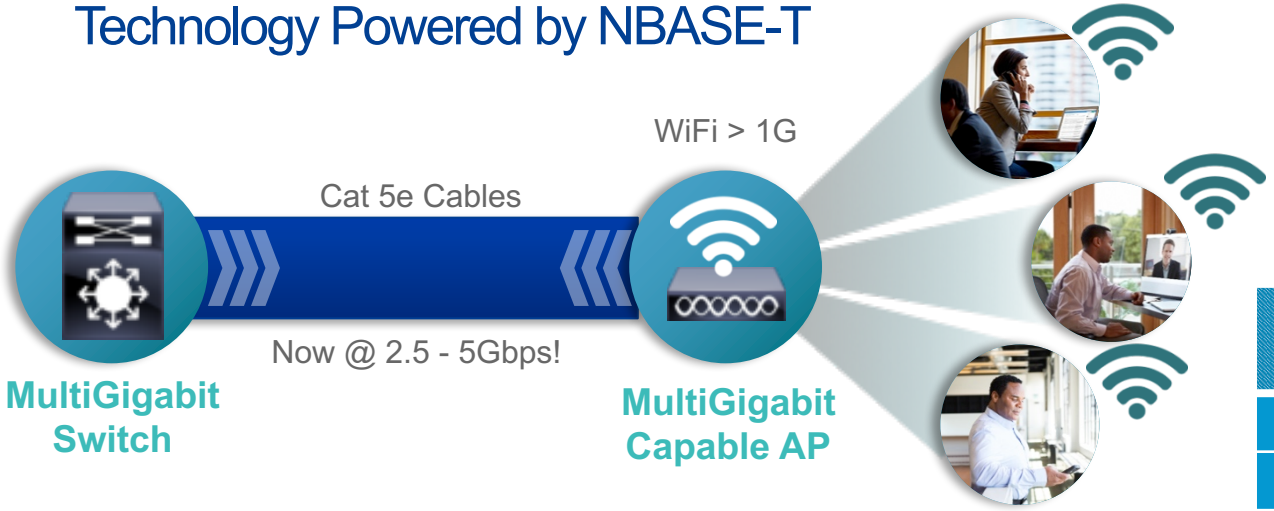
The AP then determines how it will beam-form and null to each of the 2-3 clients and then clusters these "ideal" clients into groups.

On a per-packet-basis each member of a group receives a similar size packet at the same time (downstream).

Take away – MU-MIMO is complex and challenging and requires client support

Cisco MultiGigabit

Technology Powered by NBASE-T



Cisco MultiGigabit with NBASE-T™ -> IEEE 802.3bz

Cable Type	1G	2.5G	5G	*10G*
Cat5e	✓	✓	55m	*NA*
Cat6	✓	✓	✓	*55m*
Cat6A	✓	✓	✓	✓

Is a game-changing innovation allowing enterprise networks to evolve beyond 1G

Enables 2.5 and 5 Gbps up to 100m on legacy cables

Supports all PoE standards up to 60W

Delivers up to 5X Speeds in Enterprise without replacing Cabling Infrastructure

Cisco and Apple Best Practices

RF

- Preferred 5 GHz network design
- Apple client device should observe a minimum of 2 APs with an RSSI measurement of -67 dBm
- Average Channel Utilization < 40%.
- Client SNR >= 25 dB.
- 802.11 retransmissions < 15%, Packet Loss < 1% and Jitter < 100 ms.
- Cisco highly recommends leaving all MCS rates enabled
- Channel width 40 Mhz or Best for Typical deployments, 20 MHz for High Density

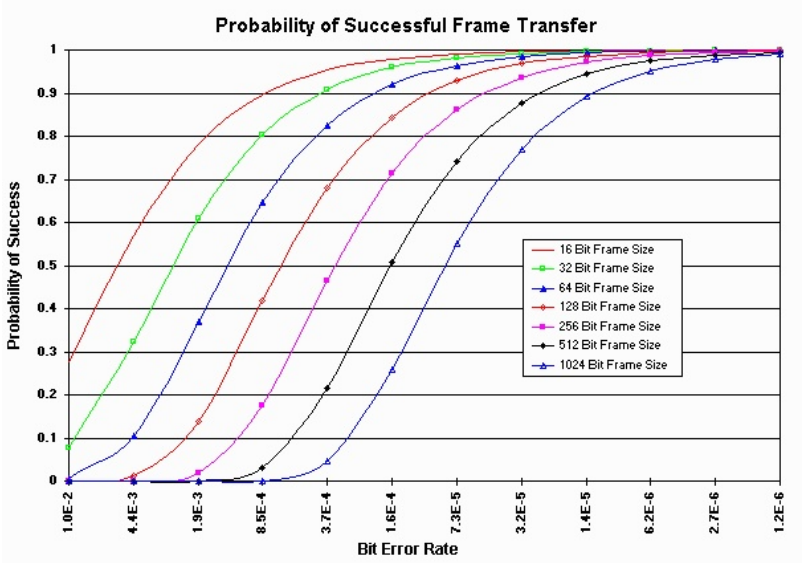
QoS

- Enable FastLane : Trust DSCP, Platinum for Unicast, EDCA as FastLane and over 70 lines of Best Practice Configuration
- WMM Set to Required
- AVC profile is AUTOQOS-AVCPROFILE
- 11k and 11v BSS Transition Enabled
- mDNS Snooping Enabled
- FT should be enabled or Adaptive, AKM Set to FT PSK or FT 802.1x

http://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-3/Optimizing_WiFi_Connectivity_and_Prioritizing_Business_Apps.pdf
http://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-3/Enterprise_Best_Practices_for_Apple_Devices_on_Cisco_Wireless_LAN.pdf

- 67 dBm? How Much is That in Data Rate?

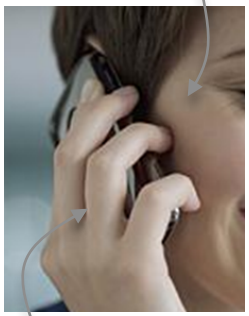
- And BER is important, because more retries means more chances that the frame will be dropped
- Your job is to limit frame drops to 1% or less to maintain 4.1 MOS
- **At -67 dBm RSSI, SNR is typically around 25 dB or more***
- You can run any rate of 24 Mbps and up, and still have good frame success rate



* well, at least in ideal conditions… see next slides

BTW, where is an antenna on a device?

Head – not good

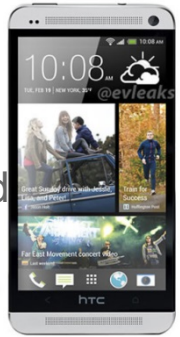


Hand – not good

Iphone 5,
Antenna is at
bottom

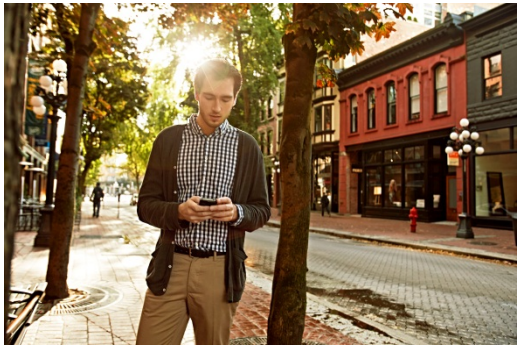
Samsung S5, antenna
is at bottom, behind button

HTC One, whole
back cover is metal and
antenna



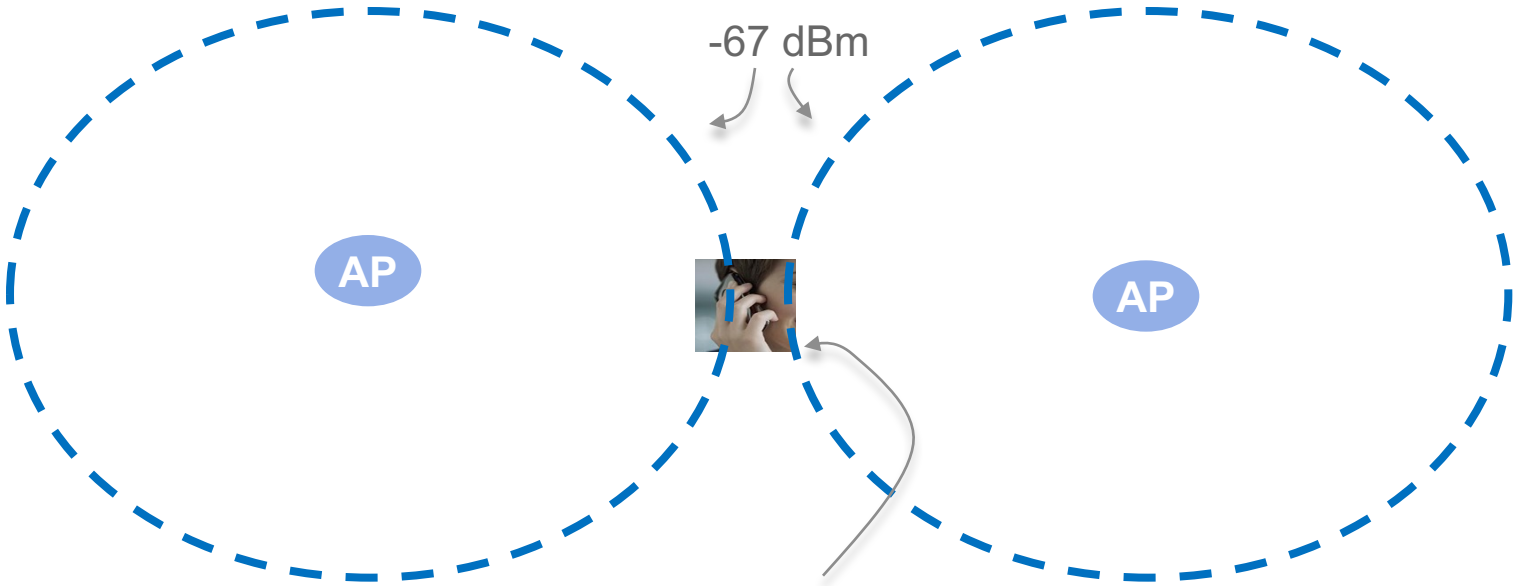
Hand and Phone Position Affect Signal

Object in Signal Path	Signal Attenuation Through Object
Plasterboard wall	3 dB
Glass wall with metal frame	6 dB
Cinderblock wall	4 dB
Office window	3 dB
Metal door	6 dB
Metal door in brick wall	12 dB
Phone and body position	3 - 6 dB
Phone near field absorption	Up to 15 dB



There can be a 20 dB difference between these photos

Big Hands are Okay if Your Design is Clever



-67 – 20 = -87 dBm
Signal is too weak…
But you can roam to the other AP @ -67 dBm!

Cisco Aironet 802.11ac Wave 2 Access Point Portfolio

Industry's most comprehensive and innovative

Beginning CY17

Enterprise Class

Mission Critical

Best in Class

DNA Ready | RF Excellence | CMX | Centralized, FlexConnect or Mobility Express

Dual 5 GHz | Flexible Radio | HDX

Future Proof

1815

Indoor / High-powered Indoor Wall Plate / Teleworker

- 2x2:2SS 80 MHz
- 867 Mbps Performance
- Tx Beam Forming
- Integrated BLE Gateway[1]
- Max Transmit Power (dBm) per local regulations[2]
- 3 GE Local Ports, including 1 PoE out[3]
- Local ports 802.1x ready[3]
- USB 2.0[4]

1830

- 3x3:2SS 80MHz
- 867 Mbps Performance
- Tx Beam Forming
- 1 GE Port Uplink
- USB 2.0

1850

- 4x4:3SS 80Mhz
- 1.7 Gbps Performance
- Internal or External Antenna
- Tx Beam Forming
- 2 GE Ports Uplink
- USB 2.0

2800

- 4x4:3SS 160 MHz
- 5 Gbps Performance
- 2.4 and 5GHz or Dual 5GHz
- 2 GE Ports Uplink
- CleanAir and ClientLink
- Internal or External Antenna
- Smart Antenna Connector
- USB 2.0

3800

- 4x4:3SS 160 MHz
- 5 Gbps Performance
- 2.4 and 5GHz or Dual 5GHz
- 2 GE Ports Uplink or 1 GE + 1 mGig (5G)
- CleanAir and ClientLink
- StadiumVision
- Internal or External Antenna
- Smart Antenna Connector
- USB 2.0
- Investment Proof Modularity

[1]Future availability [2] Available for High-powered only [3] Available for wall-plate and teleworker only [4] Available for teleworker only

Cisco Aironet Portfolio – Outdoor AP

Enterprise Class

1530

- 802.11n
- 2 models, low profile
- 2G: 3x3:3; 5G: 2x3:2
- Internal or External antenna
- Flexible Antenna Ports
- Centralized, FlexConnect, & Mesh

1560

- 802.11ac W2
- 4 models (I/E/D/PS)
- 3x3:3, 80MHz, 1.3G (I)
- 2x2:2, 80MHz, 867M (D/E/PS)
- MU-MIMO
- SFP
- Internal Directional Ant. (D)
- 4.9 GHz (PS: Public Safety)
- Flexible Antenna Ports
- CleanAir 80 MHz
- ClientLink 4.0
- Centralized, FlexConnect, Mesh & Mobility Express

Best in Class

1572EAC

- 802.11ac W1
- 4x4:3 80 MHz; 1.3 G
- External antenna
- SFP
- GPS
- PoE-Out (803.2at)
- Flexible Antenna Ports
- CleanAir 80 MHz
- ClientLink 3.0
- Modularity
- Centralized, FlexConnect & Mesh

Cable Operators

1572IC/EC

- 802.11ac W1
- 4x4:3 80 MHz; 1.3 G
- Internal or External antenna
- DOCSIS 3.0, 24x8
- SFP
- GPS
- PoE-Out (803.2at) (EC)
- Flexible Antenna Ports
- CleanAir 80 MHz
- ClientLink 3.0
- Modularity
- Centralized, FlexConnect & Mesh

Functions of the WLAN Controller

- **Centralized configuration and policy enforcement** of the Wireless LAN
- Controller **acts as security gateway** for clients
  - Authentication profiles, ACL enforcement, Bandwidth controls, RADIUS, DHCP, DNS, VLANs, ARP broadcasts, etc…
  - All access to network resources goes through the controller (APs in Local Mode)
- **Manages all access points** on the network
  - Nonoverlapping channel and power assignments, automatic channel width in 5GHz, coverage hole detection, RF analysis
  - Firmware upgrade, statistics gathering, WIPS, rogue AP detection & containment
- **Highly Available** and simple plug and play deployment model
  - Facilitate seamless Layer2 and Layer3 roaming
  - No need to re-subnet the network for deployment, AP's can be dropped into any local or remote network segment

Cisco Wireless Controller Portfolio

Large Campus and Service Provider

5520

- Up to 1500 APs
- 20,000 clients
- 20 Gbps

8540

- Up to 6000 APs
- 64,000 clients
- 40 Gbps

Small Campus / Branch (Controller on Premise)

Mobility Express

- Up to 25 Aps
- **500** clients
- Scale increase in AireOS 8.4

2504

- 5 to 75 APs
- 1k clients
- 1 Gbps

Catalyst 3650

- 1-**50** APs per switch/stack
  Directly connected APs
- 1000 clients per stack
- 40 Gbps per switch

Catalyst 3850

- 1-**100** APs per stack
  Directly connected APs
- 2K clients per stack
- 40 Gbps per switch

Catalyst 4500-E SUP

- 1-**100** APs per SUP
  Indirectly connected APs
- 2K clients per stack
- 40 Gbps per switch

Branch (Controller in DC)

Virtual WLC

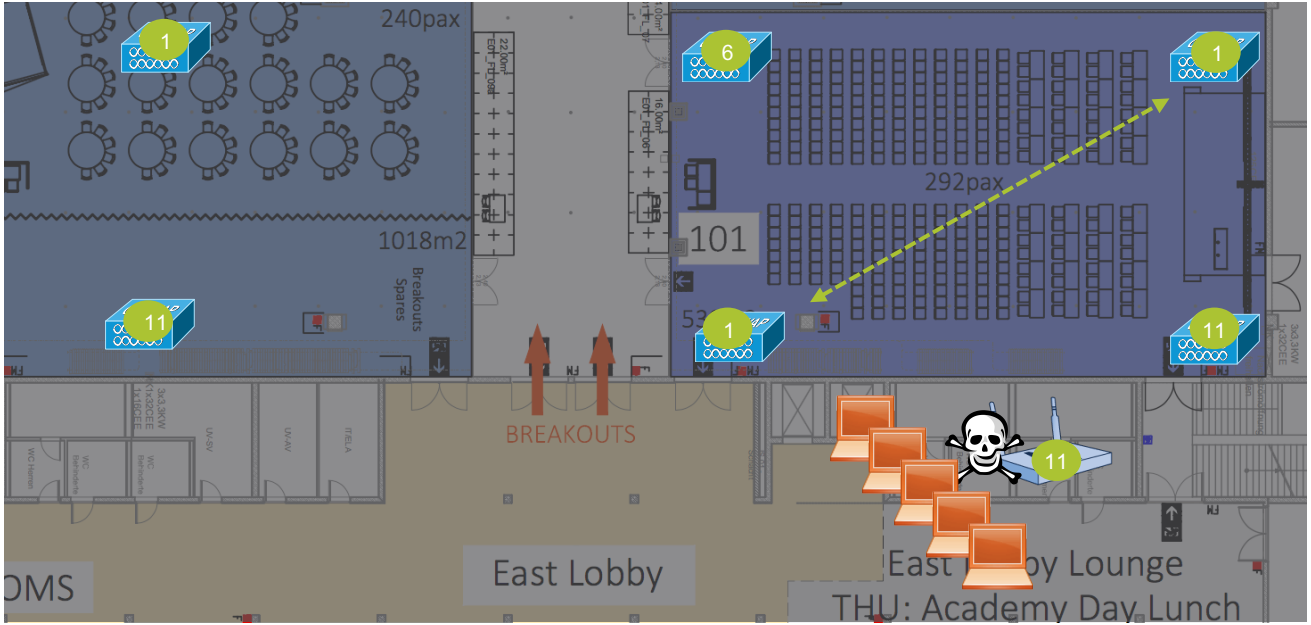
- Up to 3k APs
- **20k** clients
- 500 Mbps

5520 (or 8540)

- Up to 1500 APs
- 20,000 clients
- 20 Gbps

RF High Availability: Cisco RRM

RRM DCA in action



- RRM will determine the optimal channel plan based on AP layout (NDP)
- A rogue AP is detected on channel 11
- RRM will assess the RF and take a decision in less than couple 10s of seconds (ED-RRM with rogue contribution)
- Channel change is triggered to improve the RF
- Note how the 3 non overlapping channels are still maintained!
- RRM has a RF system view. AP view would be limited and could result in sub-optimal RF plan

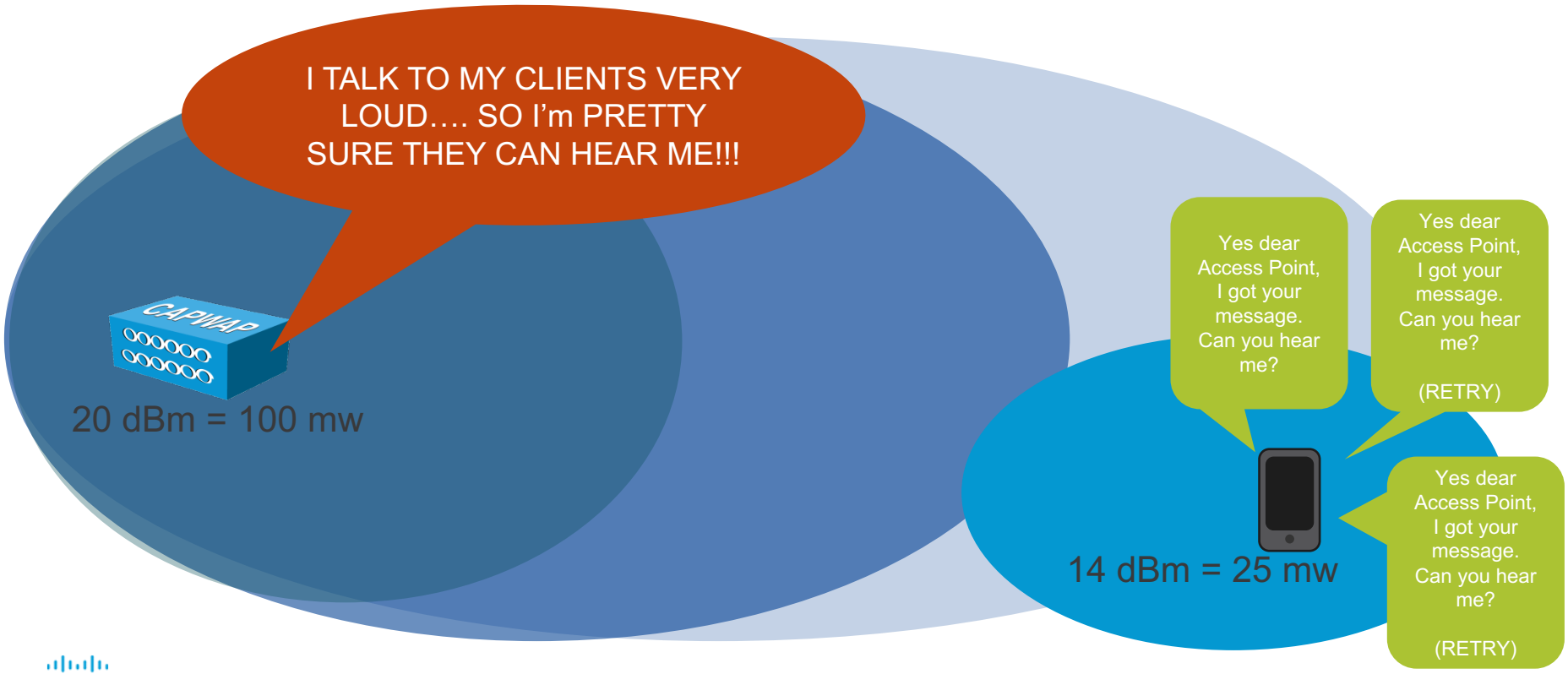
Don't Use Maximum Power!!! Why?

Jussi Kiviniemi heeft geretweet

Jason Hintersteiner
@EmperorWiFi

Setting Tx power is like drinking scotch: The right amount is great, but "more" does not mean "better", & too much will make you sick...

Clients are not Maximum Power



Can Power Really Damage Cell Conditions?

- Bad design example: HTC One @14 dBm, AP @20 dBm

17	0.039879000	172.31.255.101	172.31.255.103	UDP	1420	34	-35 55 dB	54.0	Source port: 50857 Destination port: search-agent
18	0.040266000	172.31.255.101	172.31.255.103	UDP	1420	34	-35 55 dB	54.0	Source port: 50857 Destination port: search-agent
19	0.040648000	172.31.255.101	172.31.255.103	UDP	1420	34	-34 56 dB	54.0	Source port: 50857 Destination port: search-agent
20	0.041938000	172.31.255.101	172.31.255.103	UDP	1420	34	-34 56 dB	54.0	Source port: 50857 Destination port: search-agent
21	0.042217000	172.31.255.101	172.31.255.103	UDP	1420	34	-29 61 dB	36.0	Source port: 50857 Destination port: search-agent
22	0.043444000	172.31.255.101	172.31.255.103	UDP	1420	34	-29 61 dB	12.0	Source port: 50857 Destination port: search-agent
23	0.043445000		Cisco_0a:04:2e (RA)	802.11	40		-45 45 dB	12.0	Acknowledgement, Flags=........C
24	0.043850000	172.31.255.101	172.31.255.103	UDP	1420	34	-34 56 dB	54.0	Source port: 50857 Destination port: search-agent
25	0.044245000	172.31.255.101	172.31.255.103	UDP	1420	34	-34 56 dB	54.0	Source port: 50857 Destination port: search-agent
26	0.044641000	172.31.255.101	172.31.255.103	UDP	1420	34	-34 56 dB	54.0	Source port: 50857 Destination port: search-agent
27	0.045023000	172.31.255.101	172.31.255.103	UDP	1420	34	-35 55 dB	54.0	Source port: 50857 Destination port: search-agent
28	0.045750000	172.31.255.101	172.31.255.103	UDP	1420	34	-29 61 dB	36.0	Source port: 50857 Destination port: search-agent
29	0.046223000	172.31.255.101	172.31.255.103	UDP	1420	34	-29 61 dB	36.0	Source port: 50857 Destination port: search-agent
30	0.047450000	172.31.255.101	172.31.255.103	UDP	1420	34	-29 61 dB	12.0	Source port: 50857 Destination port: search-agent
31	0.047450000		Cisco_0a:04:2e (RA)	802.11	40		-47 43 dB	12.0	Acknowledgement, Flags=........C

```
Frame 29: 1420 bytes on wire (11360 bits), 1420 bytes captured (11360 bits) on interface 0
Radiotap Header v0, Length 26
IEEE 802.11 QoS Data, Flags: ....R.F.C
  Type/Subtype: QoS Data (0x28)
⊟ Frame Control: 0x0A88 (Normal)
    Version: 0
    Type: Data frame (2)
    Subtype: 8
  ⊟ Flags: 0xA
      .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x02)
      .... .0.. = More Fragments: This is the last fragment
      .... 1... = Retry: Frame is being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = Protected flag: Data is not protected
      0... .... = Order flag: Not strictly ordered
```

Based on Rx AP signal, BYOD thinks 54 Mbps rate is okay…
But client message is too weak, and AP does not ACK until rate falls to 12 Mbps

Each message **takes 8 times** more to be transmitted (including EIFS and retries)

Some Client Max EIRPs

Model	EIRP 2.4 GHz	Worst* EIRP 5 GHz
Iphone 6S	14.8 dBm	10.3 dBm
Ipad 4	15.2 dBm	22.67 dBm
Samsung S7	14.8 dBm	10.14 dBm
Samsung S4 tab	12.05 dBm	11.24 dBm
Samsung S6	13.5 dBm	10.66 dBm
HTC One	14.4 dBm	13.8 dBm
Nokia Lumia 1520	13.1 dBm	11.6 dBm
ASUS PCE-AC66	22 dBm	22.83 dBm

* EIRP varies with sub-band, displaying worst of all sub-bands

- In short: **half your worst client max power**

  e.g. if you design for 5 GHz and worst client max is at 11 dBm, set your AP power to 8 dBm

BEST PRACTICES (AirOS)

INFRASTRUCTURE

- Enable High Availability (AP and Client SSO)
- Enable AP Failover Priority
- Enable AP Multicast Mode
- Enable Multicast VLAN
- Enable Pre-image download
- Enable AVC
- Enable NetFlow
- Enable Local Profiling (DHCP and HTTP)
- Enable NTP
- Modify the AP Re-transmit Parameters
- Enable FastSSID change
- Enable Per-user BW contracts
- Enable Multicast Mobility
- Enable Client Load balancing
- Disable Aironet IE
- FlexConnect Groups and Smart AP Upgrade

MESH

- Set Bridge Group Name
- Set Preferred Parent
- Multiple Root APs in each BGN
- Set Backhaul rate to "Auto"
- Set Backhaul Channel Width to 40/80 MHz
- Backhaul Link SNR > 25 dBm
- Avoid DFS channels for Backhaul
- External RADIUS server for Mesh MAC Authentication
- Enable IDS
- Enable EAP Mesh Security Mode

SECURITY

- Enable 802.1x and WPA/WPA2 on WLAN
- Enable 802.1x authentication for AP
- Change advance EAP timers
- Enable SSH and disable telnet
- Disable Management Over Wireless
- Disable WiFi Direct
- Secure Web Access (HTTPS)
- Enable User Policies
- Enable Client exclusion policies
- Enable rogue policies and Rogue Detection RSSI
- Strong password Policies
- Enable IDS
- BYOD Timers

WIRELESS / RF

- Disable 802.11b data rates
- Restrict number of WLAN below 4
- Enable channel bonding – 40 or 80 MHz
- Enable BandSelect
- Use RF Profiles and AP Groups
- Enable RRM (DCA & TPC) to be auto
- Enable Auto-RF group leader selection
- Enable Cisco CleanAir and EDRRM
- Enable Noise &Rogue Monitoring on all channels
- Enable DFS channels
- Avoid Cisco AP Load

http://www.cisco.com/c/en/us/td/docs/wireless/technology/wlc/82463-wlc-config-best-practice.html

Thank You

Additional resources from CiscoLive 2017

BRKCRS-2031 - Enterprise Campus Design: Multilayer Architectures and Design Principles

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=93710&backBtn=true

BRKARC-3438 - Cisco Catalyst 3850 and 3650 Series Switching Architecture

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=93707&backBtn=true

BRKARC-3465 - Cisco Catalyst 6800 Switch Architectures

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=94000&backBtn=true

BRKCRS-2900 - Driving Enterprise Network Innovation - From the Gates to the GUI

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=94402&backBtn=true

Additional resources from CiscoLive 2017

BRKEWN-2010 - Design and Deployment of Enterprise WLANs

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=93721&backBtn=true

BRKEWN-2670 - Designing Next-Gen Wireless Open Office

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=94063&tclass=popup

BRKEWN-3011 - Advanced Troubleshooting of Wireless LANs

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=94130&tclass=popup

BRKEWN-2017 - Understanding RF Fundamentals and the Radio Design for 11ac Wireless Networks

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=94061&tclass=popup

BRKEWN-2027 - Design and Deployment of Outdoor Wireless Networks

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=94064&backBtn=true

Additional resources from CiscoLive 2017

BRKEWN-3010 - Improve enterprise WLAN spectrum quality with Cisco's advanced RF capacities (RRM, CleanAir, ClientLink, etc)

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=94062&tclass=popup

BRKEWN-2000 - Design and Deployment of Wireless LANs for real time Applications

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=93867&tclass=popup

BRKEWN-3000 - Analyzing and fixing WiFi issues - Cisco WLC tools and packet capture analysis techniques

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=93868&tclass=popup

BRKEWN-2012 - Designing a precise location based service on WiFi to support Connected Mobile Experiences (CMX)

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=93829&backBtn=true

Cisco TrustSec

Would you like to know more?

Suggested Reading:

BRKCRS-2891 - Enterprise Network Segmentation with Cisco TrustSec

BRKSEC-2203 - Enabling TrustSec Software-Defined Segmentation

BRKSEC-2695 - Building an Enterprise Access Control Architecture using ISE and TrustSec

Other References:

Cisco TrustSec Marketing Site	http://www.cisco.com/go/trustsec/
Cisco TrustSec Config Guide	cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec.html
Cisco TrustSec Matrix	http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/solution-overview-listing.html
Cisco TrustSec Design Guides	http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/design-guide-listing.html
Fundamentals of TrustSec	https://www.youtube.com/watch?v=78-GV7Pz18I

Locator / ID Separation Protocol (LISP)

Would you like to know more?

Suggested Reading:

BRKRST-3045 - LISP - A Next Generation Networking Architecture

BRKRST-3047 - Troubleshooting LISP

BRKCRS-3800 - DNA Campus Fabric – A Look Under the Hood

BRKCRS-2802 - DNA Campus Fabric - Monitoring and Troubleshooting

Other References:

Cisco LISP Site	http://lisp.cisco.com
Cisco LISP Marketing Site	http://www.cisco.com/go/lisp/
LISP Beta Network Site	http://www.lisp4.net or http://www.lisp6.net
IETF LISP Working Group	http://tools.ietf.org/wg/lisp/
Fundamentals of LISP	https://www.youtube.com/watch?v=lKrV1qB8uqA


CISCO