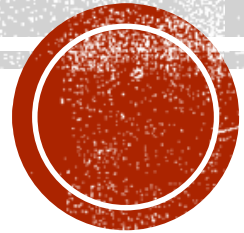
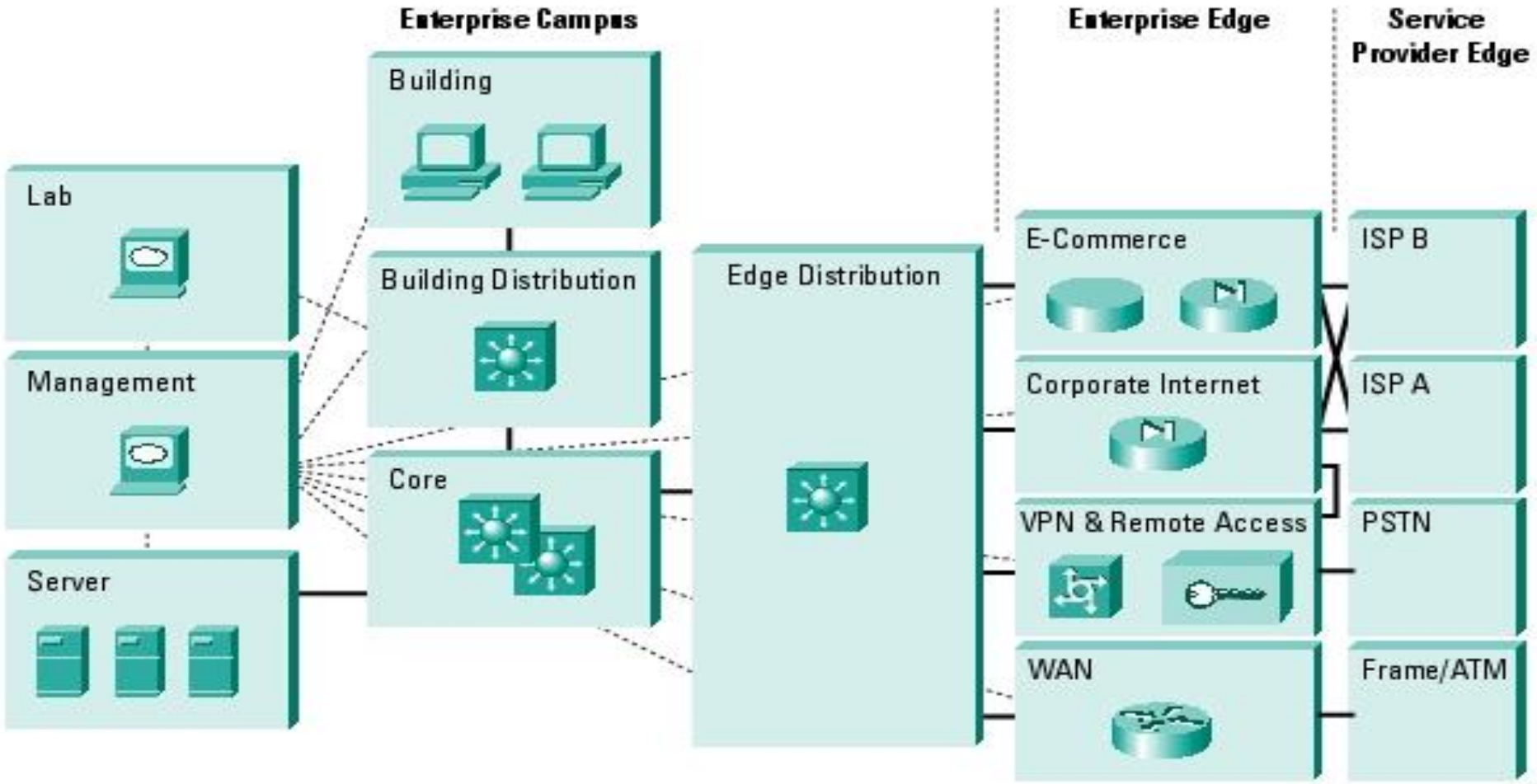
ENTERPRICES NETWORK CISCO DESIGN BEST PRACTICE

Massimiliano Sbaraglia

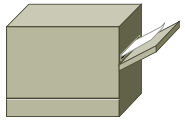


ENTERPRICES NETWORK MODULE



ENTERPRICES BUILDING ACCESS MODULE

Printer



PC

LapTop

VoIP Phone

LWAPP Access Point WIFI

ACCESS SWITCH

Layer 2 access connections to End-Point

Layer 2 connections trunk or layer 3 p2p to pair distribution switch

PVST+ or MST (Spanning Tree Protocol)

VLANs

Software Security End-Point: CSA (Cisco Security Agent) for safe host-based intrusion prevention system (HIPS)

Security Access Network: DHCP, ARP, IP Spoofing, NFP (Network Foundation Protection) and CISF (Catalyst Integrated Security Feature)

ENTERPRICES SECURITY ACCESS BEST PRACTICE (NFP)

- Security Infrastructure Level
  - Implement OOB (Out Of Band) interface to devices network management
  - Limit the accessible port devices and restrict the permitted communications
  - Legal Notification
  - Authenticate and Authorize access using AAA
  - Log and Account for all access
  - Protect sensitive data such as local-password
- Security Routing Level (for layer 3 access routing)
  - Authentication router neighbors
  - Use default passive interface
  - Log neighbor changes
  - Implement stub-routing when possible

ENTERPRICES SECURITY ACCESS BEST PRACTICE (NFP)

- Security Device Level
  - Disable unnecessary services
  - Filter and rate-limit control-plane traffic
  - Redundancy
- Security Network Telemetry
  - NTP (Network Time Protocol) to synchronize time to all network domain
  - Monitor interface statistics to all devices
  - Monitor system status information such as CPU, memory and process
  - Log all system status, traffic analysis, access device informations
- Security Policy Enforcement:
  - Implement management and infrastructure ACL (i-ACL)
  - Protect against IP spoofing with uRPF on routed edge interface and with IP source guard on access port

ENTERPRICES SECURITY ACCESS BEST PRACTICE (NFP)

- Security Switching Level
  - Restrict broadcast domain
  - Implement Spanning Tree Protocol against loops (RSTP, RPVST+) and BPDU guard, STP root guard
  - DHCP snooping enable on access vlans against dhcp starvation and rogue dhcp servers attacks
  - IP spoofing protecton with IP source guard enable on access port
  - ARP spoofing protection with dynamic ARP inspection (DAI) enable on access vlans
  - MAC flooding protection with port security enable on access port
  - Broadcast and Multicast protection with storm control enable on access port

- Security i-ACL level
  - A carefully planned addressing scheme
  - Ping and traceroute allowed
  - Block access to address assigned to the infrastructure devices
  - Block access to address assigned to the network management devices
  - Permit client transit traffic

ENTERPRICES SECURITY ACCESS BEST PRACTICE (NFP)

- Security Vlans Level
  - Restrict vlans on single switch
  - Configure separate vlans to voice and data
  - Disable vlans dynamic trunk negotiation trunking on access port (DTP off)
  - Configure explicity trunk mode on infrastructure ports rather autonegotiation
  - Use VTP mode transparent on switches
  - Disable unused ports (shutdown)
  - Do not use vlan 1 for anything
  - Use all tagged mode for native vlan on trunks port

ENTERPRICES NETWORK ACCESS CONTROL BEST PRACTICE

- IBNS (Identity-Based Networking Services)
  - 802.1x
  - MAB (MAC Authentication Bypass)

- NAC Appliance
  - Implemented on in-band or out-of-band
  - NAC servers and NAC manager placement
  - Access switch vlans requirements
  - Client redirection to NAC server
  - NAC agent
  - Client authentication

ENTERPRICES SECURITY ACCESS TYPE OF SERVICES

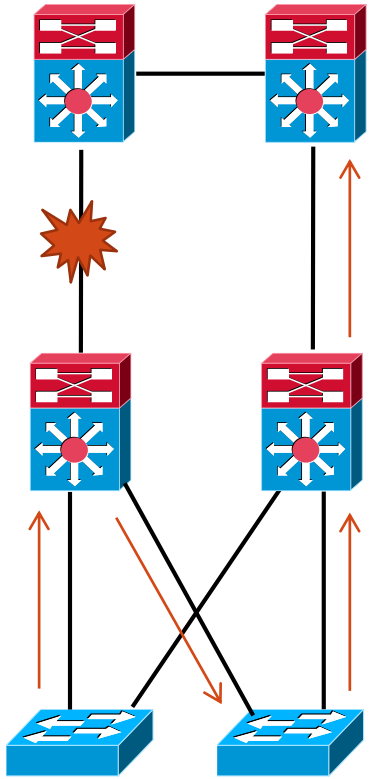
Service requirement	Type of Service
Discovery and Configuration	802.1AF (Authenticated Key Agreement MACsec) ; CDP ; LLDP ; LLDP-MED
Security Services	INBS (802.1x) ; CISF (Catalyst Integrated Security Feature) ; port security ; DHCP snooping ;DAI (Dynamic Arp Inspection) ; IPSG (IP source guard)
Network Identity and Access	802.1x ; MAB (Mac Authentication Bypass) ; Web-Auth
Application Recognition	QoS marking, policing, queueing ; NBAR (Network Based Application Recognition)
Intelligent Network Service Control	PVST+ ; Rapid PVST+ ; EIGRP ; OSPF ; DTP ; LACP or PAgP ; Flexlink ; port-fast ; uplink-fast ; backbone-fast ; loop-guard ; BPDU-guard ; port-security ; root-guard
Physical Infrastructure	PoE (Power of Ethernet)

ENTERPRICES BUILDING ACCESS MODULE TRAFFIC RECOVERY

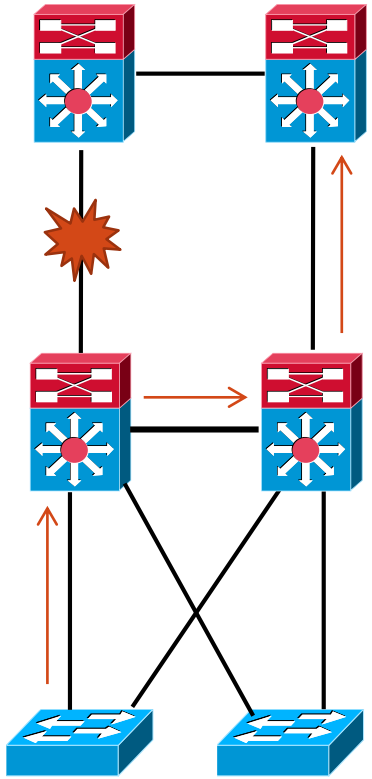
CORE SWITCH

DISTRIBUTION SWITCH

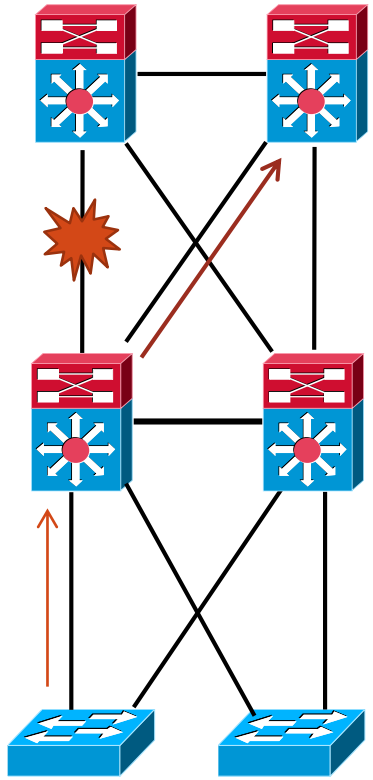
ACCESS SWITCH



NOT GOOD

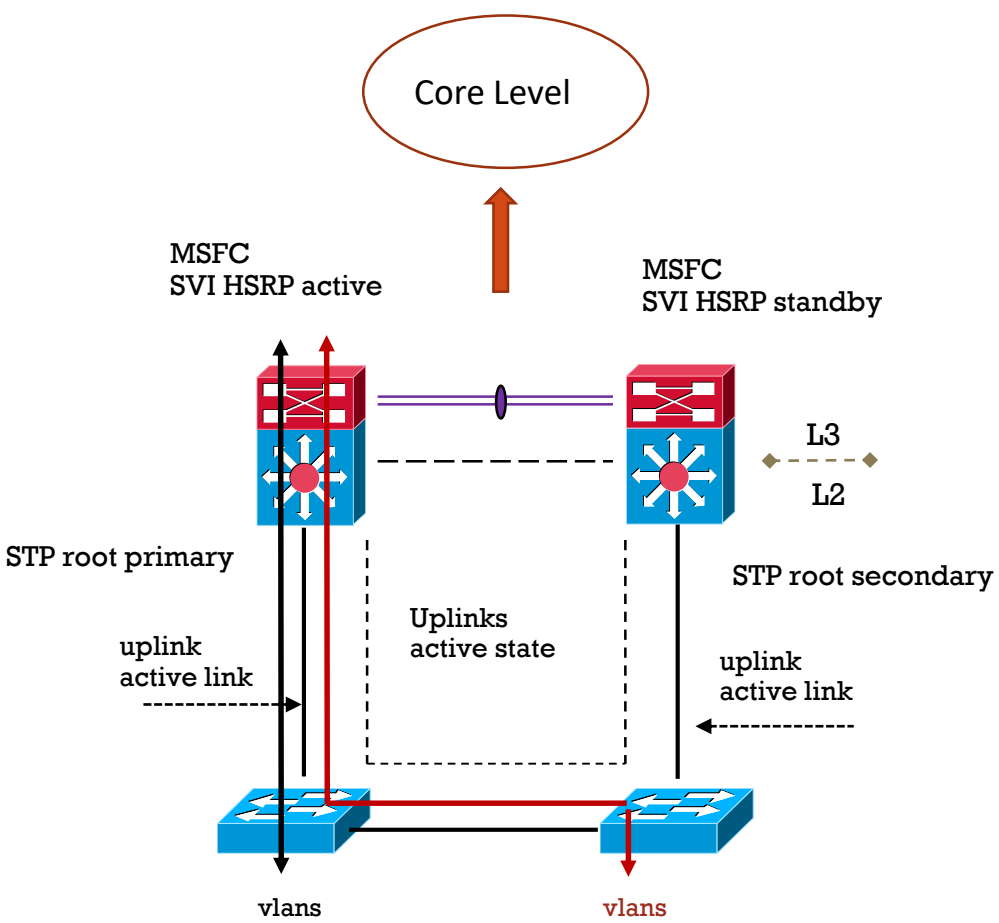


ACCEPTABLE



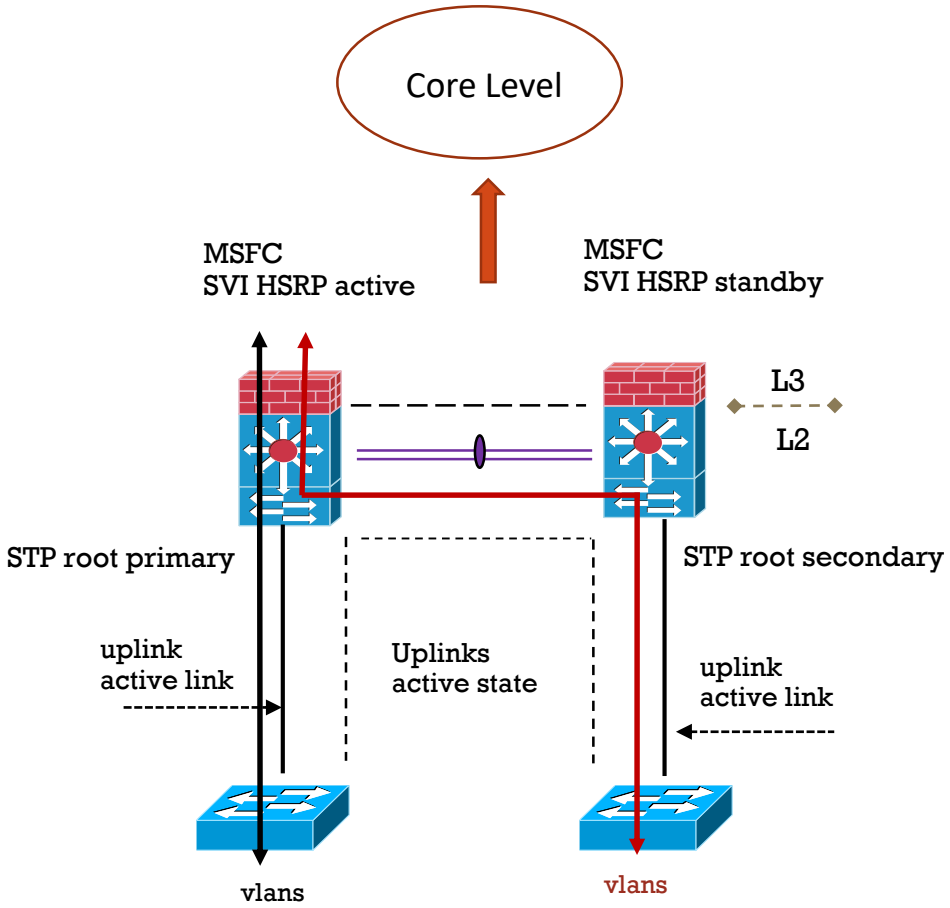
GOOD

ENTERPRICES BUILDING ACCESS MODULE LOOPED FREE TOPOLOGY



DISTRIBUTION SWITCH

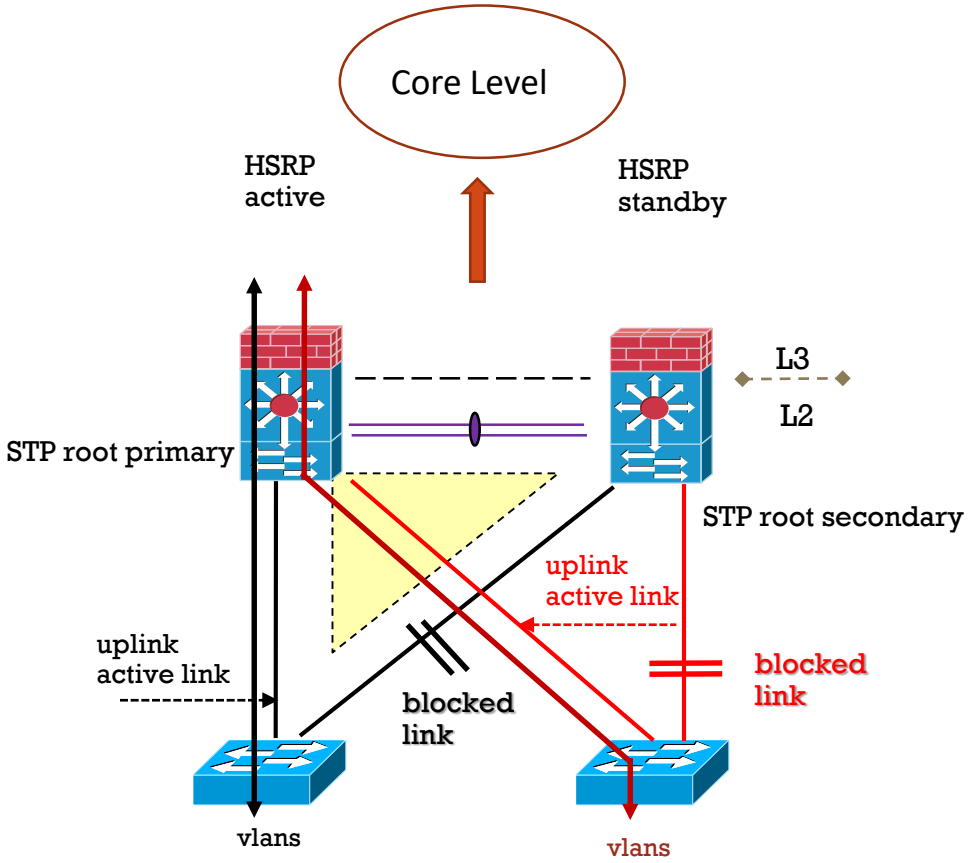
ACCESS SWITCH



Loop Free type U

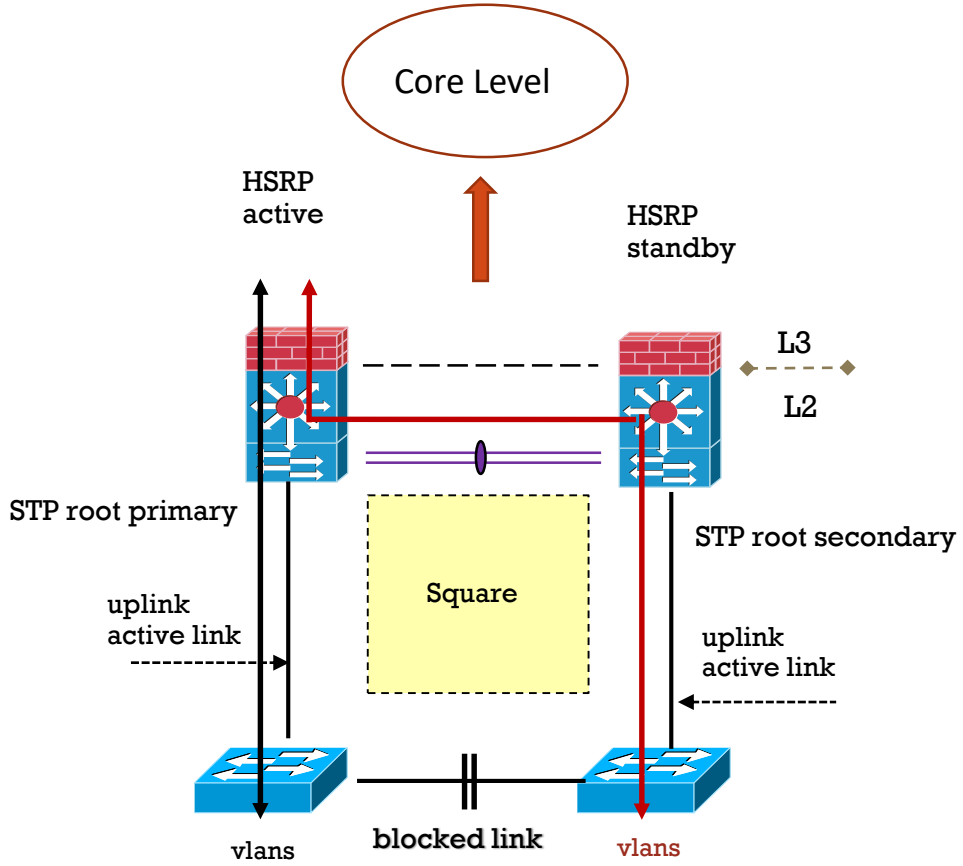
Loop Free type Inverted-U

ENTERPRICES BUILDING ACCESS MODULE LOOPED TOPOLOGY



DISTRIBUTION SWITCH

ACCESS SWITCH



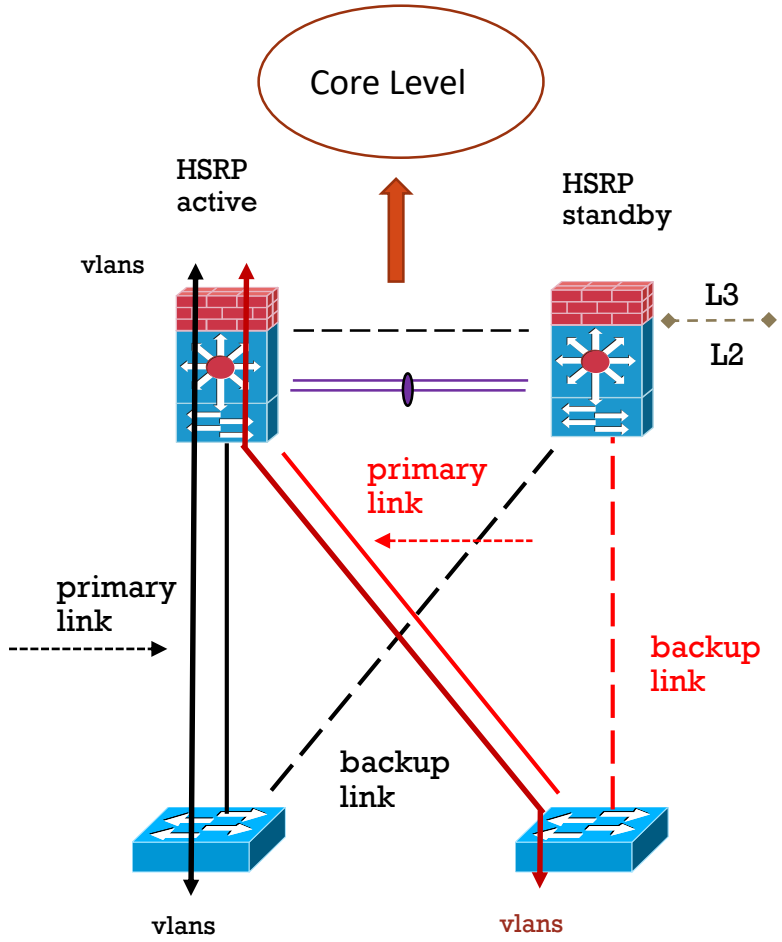
Loop type Triangle

Loop type Square

ENTERPRICES BUILDING ACCESS MODULE FLEX-LINK TOPOLOGY

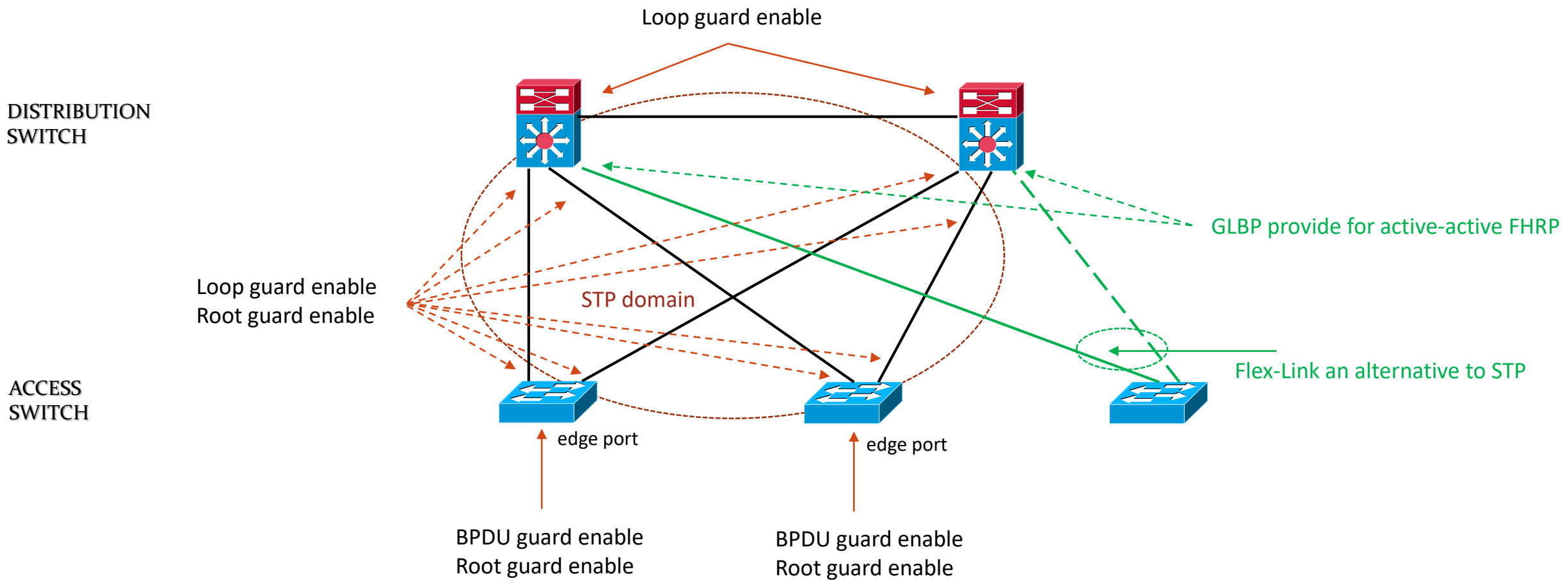
DISTRIBUTION SWITCH

ACCESS SWITCH



Flex-Link model

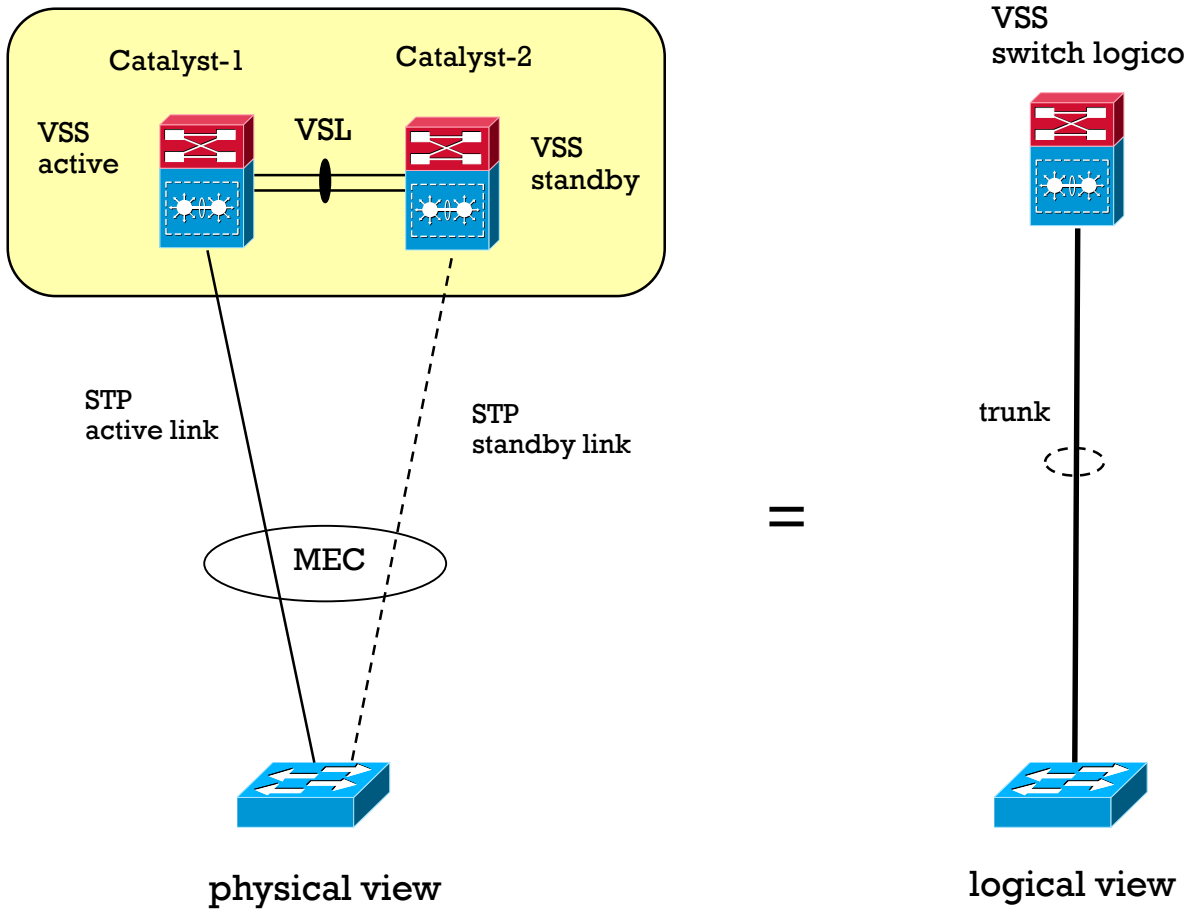
ENTERPRICES BUILDING ACCESS MODULE STP TOPOLOGY



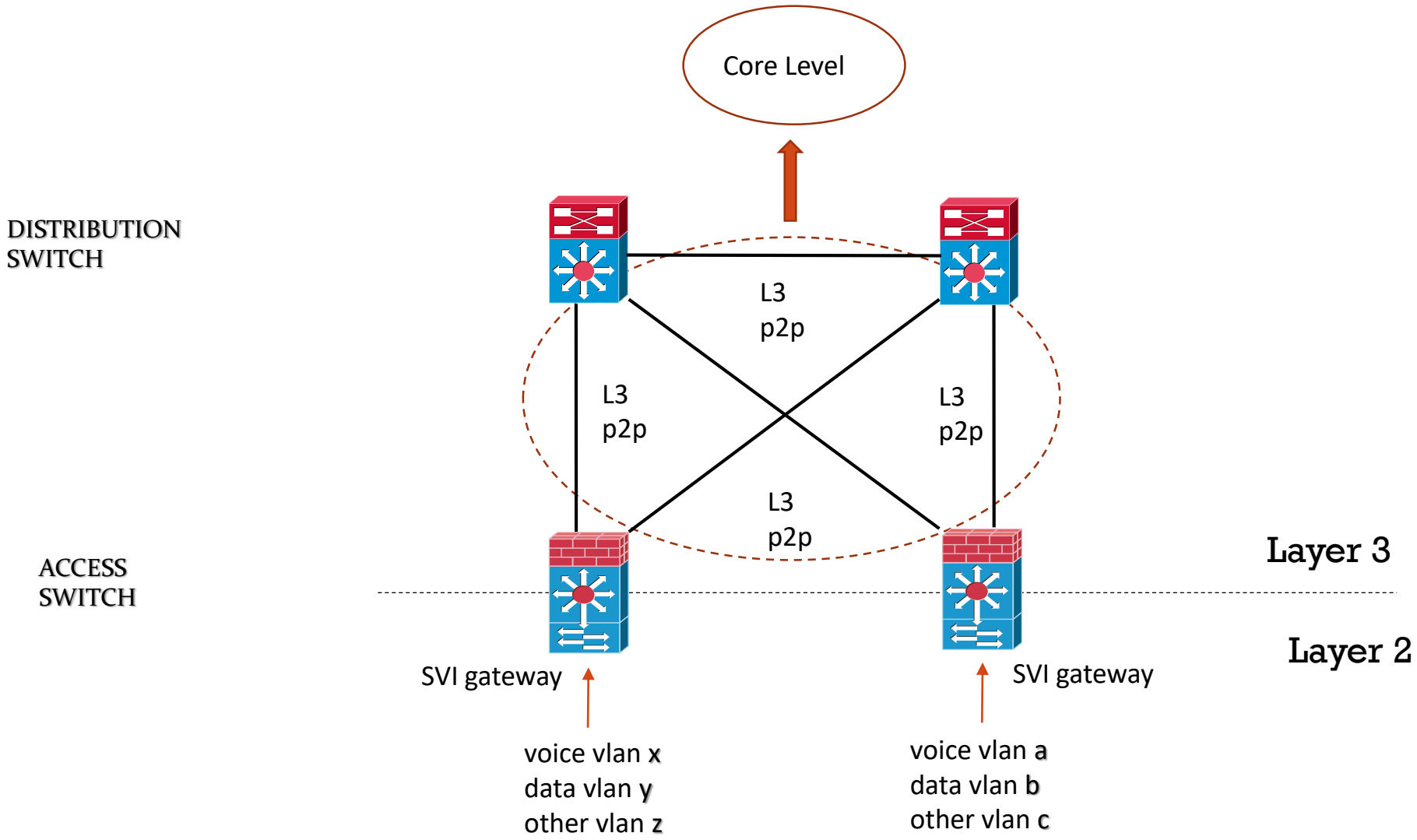
ENTERPRICES BUILDING ACCESS MODULE VIRTUAL-SWITCH TOPOLOGY

DISTRIBUTION SWITCH

ACCESS SWITCH



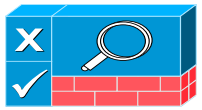
ENTERPRICES BUILDING ACCESS MODULE ROUTED TOPOLOGY



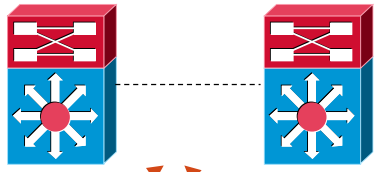
ENTERPRICES BUILDING DISTRIBUTION MODULE

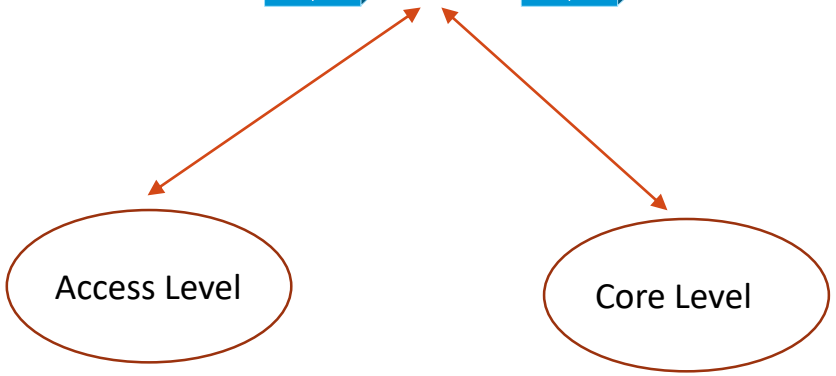
Intrusion Prevention

NAC Access control
Netflow
uRPF



DISTRIBUTION
SWITCH





Distribution module work between access and core levels

Distribution switch are implemented on pair for redundancy reasons

Protecting End-Point with network-based intrusion prevention system

Protecting Infrastructure with NFP best practice

ENTERPRICES SECURITY DISTRIBUTION BEST PRACTICE

- Security IPS Level
  - Provide filtering of know network worm and virus, DoS traffic attacks, hacking attacks
  - IPS is placed in traffic path (inline mode with bridged traffic) or in promiscuous mode via SPAN, RSPAN, VACL
  - Multiple IPS sensor may offer scalability and availability with load-balancing using ether-channel (ECLB)
  - IPS sensor may be used to see traffic on both directions (traffic symmetry)

- Security Infrastructure Level
  - Implement OOB (Out Of Band) interface to devices network management
  - Limit the accessible port devices and restrict the permitted communications
  - Legal Notification
  - Authenticate and Authorize access using AAA
  - Log and Account for all access
  - Protect sensitive data such as local-password

ENTERPRICES SECURITY DISTRIBUTION BEST PRACTICE

- Security Routing Level
  - Authentication router neighbor
  - Use default passive interface
  - Log neighbor changes
  - Implement stub-routing when possible

Note: Route filtering and stub routing in the distribution layer are only recommended for a multi-tier or VSS design where the routed edge interface is on the distribution switches. In a routed access design, these features are used in the access layer.

- Security Device Level
  - Disable unnecessary services
  - Filter and rate-limit control-plane traffic
  - Redundancy

ENTERPRICES SECURITY DISTRIBUTION BEST PRACTICE

- Security Network Telemetry
  - NTP (Network Time Protocol) to synchronize time to all network domain
  - Monitor interface statistics to all devices
  - Monitor system status information such as CPU, memory and process)
  - Log all system status, traffic analysis, access device information
  - Enable Netflow

- Security Policy Enforcement:
  - Implement management and infrastructure ACL (i-ACL)
  - Protect against IP spoofing with uRPF on routed edge interface

Note: uRPF is only applicable in the distribution layer of a multi-tier design where the routed edge interface is on the distribution switches. In a routed access design, this is enabled in the access layer.

ENTERPRICES SECURITY DISTRIBUTION BEST PRACTICE

- Security Switching Level

  - Restrict broadcast domain
  - Implement Spanning Tree Protocol against loops (RSTP, RPVST+) and BPDU guard, STP root guard
  - Implement vlans best practice

Note: VLAN and spanning tree best practices are only applicable in the distribution layer of a multi-tier design where Layer 2 extends to the distribution layer switches.

ENTERPRICES SECURITY DISTRIBUTION MODELS

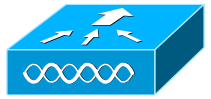
Protocol	Multi-Tier Access	Routed Access	Virtual Switch
Access distribution control-plane	PVST+ ; Rapid PVST+ ; MST	EIGRP ; OSPF	PaGP ; LACP
Spanning Tree	Required for redundancy and to prevent L2 loops	NO	NO
Network Recovery	STP and FHRP (HSRP ; GLPB ; VRRP)	EIGRP ; OSPF	MEC (multichassis eth)
VLAN spanning wiring closets	YES (required L2 STP loops)	NO	YES
Layer 2 / Layer 3 demarcation	Distribution level	Access level	Distribution level
First Hop Redundancy Protocol	HSRP ; GLPB ; VRRP	NO	NO
Access to Distribution per-flow load-balancing	NO	YES (ECMP)	YES (MEC)
Convergence	900 msec to 50 sec (depend on tuning STP and FHRP topology)	50 to 600 msec	50 to 600 msec
Change control	Dual distribution switch design requires manual configurationsynchronization but allows for independent code upgrades and changes	The same like multi-tier access	Single virtual switch auto-syncs the configuration between redundant hardware but does not currently allow independent code upgrades for individual member switches

ENTERPRICES BUILDING SERVICE BLOCK MODULE

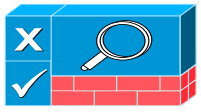
DHCP Server
DNS Server
FTP Server

Cisco Call Manager

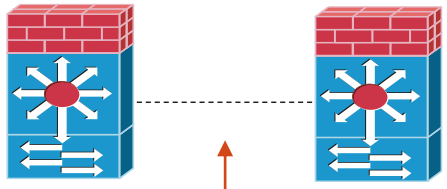
WLAN Controller



NAC Access Control



Service Block
SWITCH



Core Level

Centralized LWAPP wireless Controller

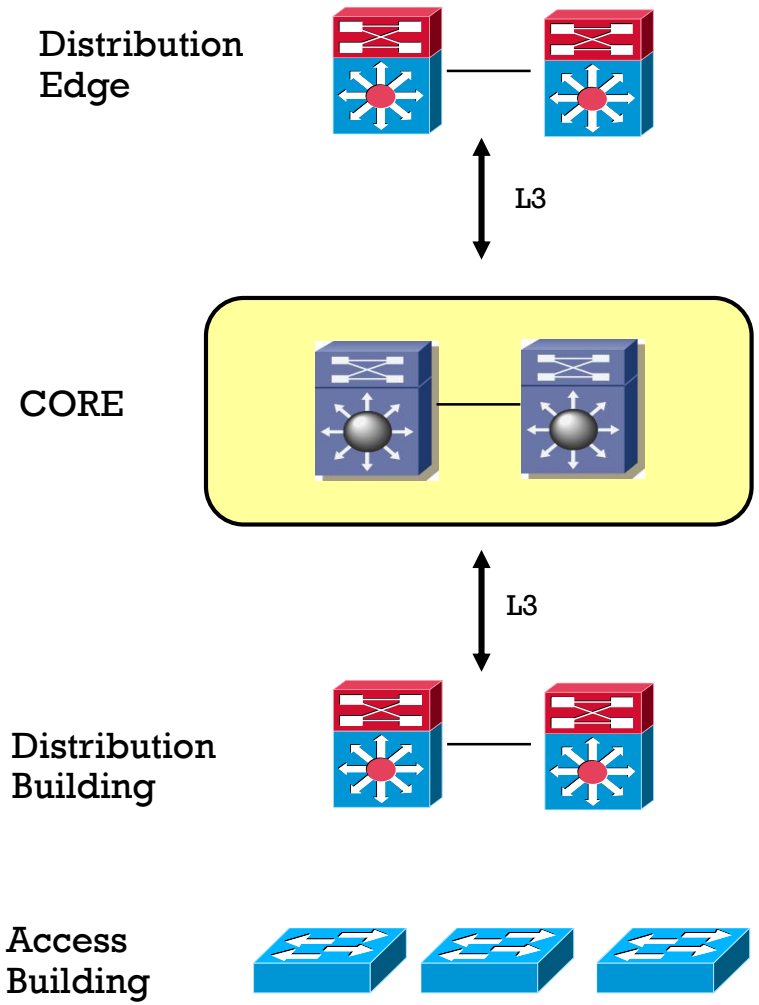
IPv6 ISATAP tunnel termination

Local Internet Edge

Cisco Unified Communication services

Policy Gateways

ENTERPRICES BUILDING CORE MODULE

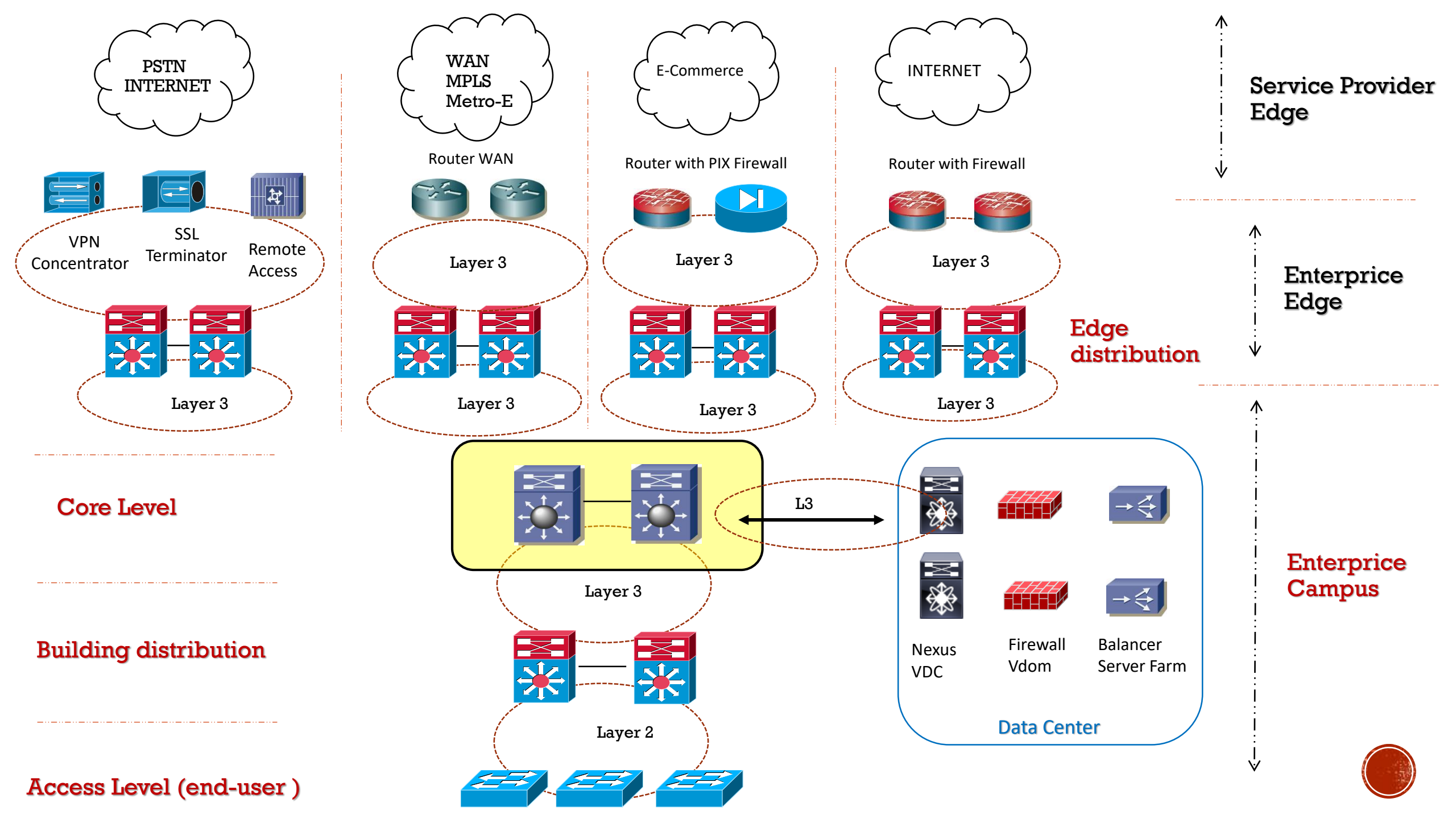


High Availability and always-on operate

It is the backbone and connect all distribution block on Enterprices campus

Appropriate redundancy level to ensure any kind of failure (switch, supervisor, line-card, cabling)

Upgrade hardware and software without any disruption of network application


PSTN
INTERNET
WAN
MPLS
Metro-E
E-Commerce
INTERNET
Service Provider Edge
Router WAN
Router with PIX Firewall
Router with Firewall
VPN Concentrator
SSL Terminator
Remote Access
Layer 3
Layer 3
Layer 3
Layer 3
Layer 3
Edge distribution
Enterprice Edge
Core Level
L3
Layer 3
Building distribution
Layer 2
Nexus VDC
Firewall Vdom
Balancer Server Farm
Data Center
Enterprice Campus
Access Level (end-user)

ENTERPRICES QOS BEST PRACTICE