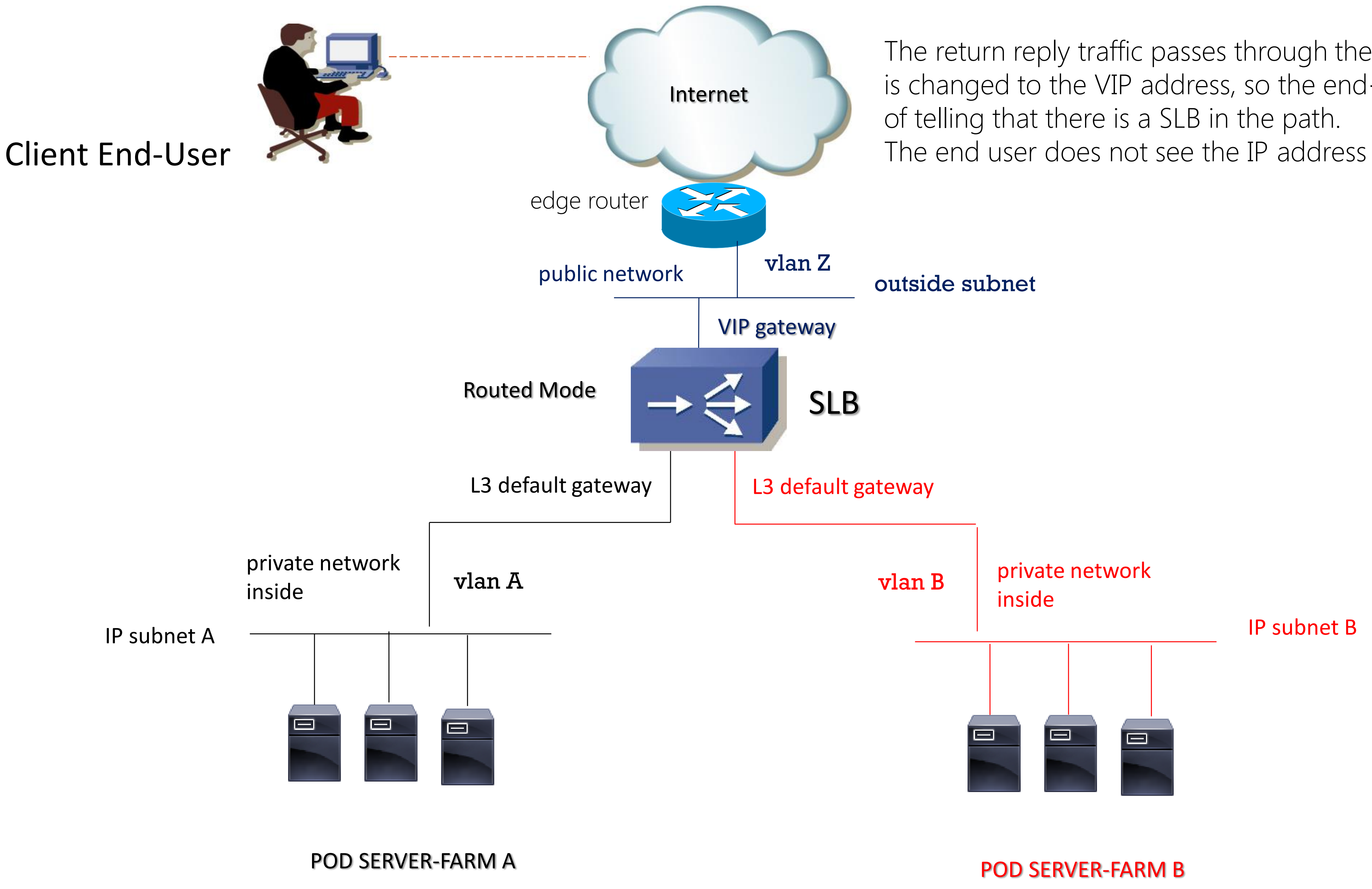
CISCO SLB AND FWSM NETWORK DESIGN

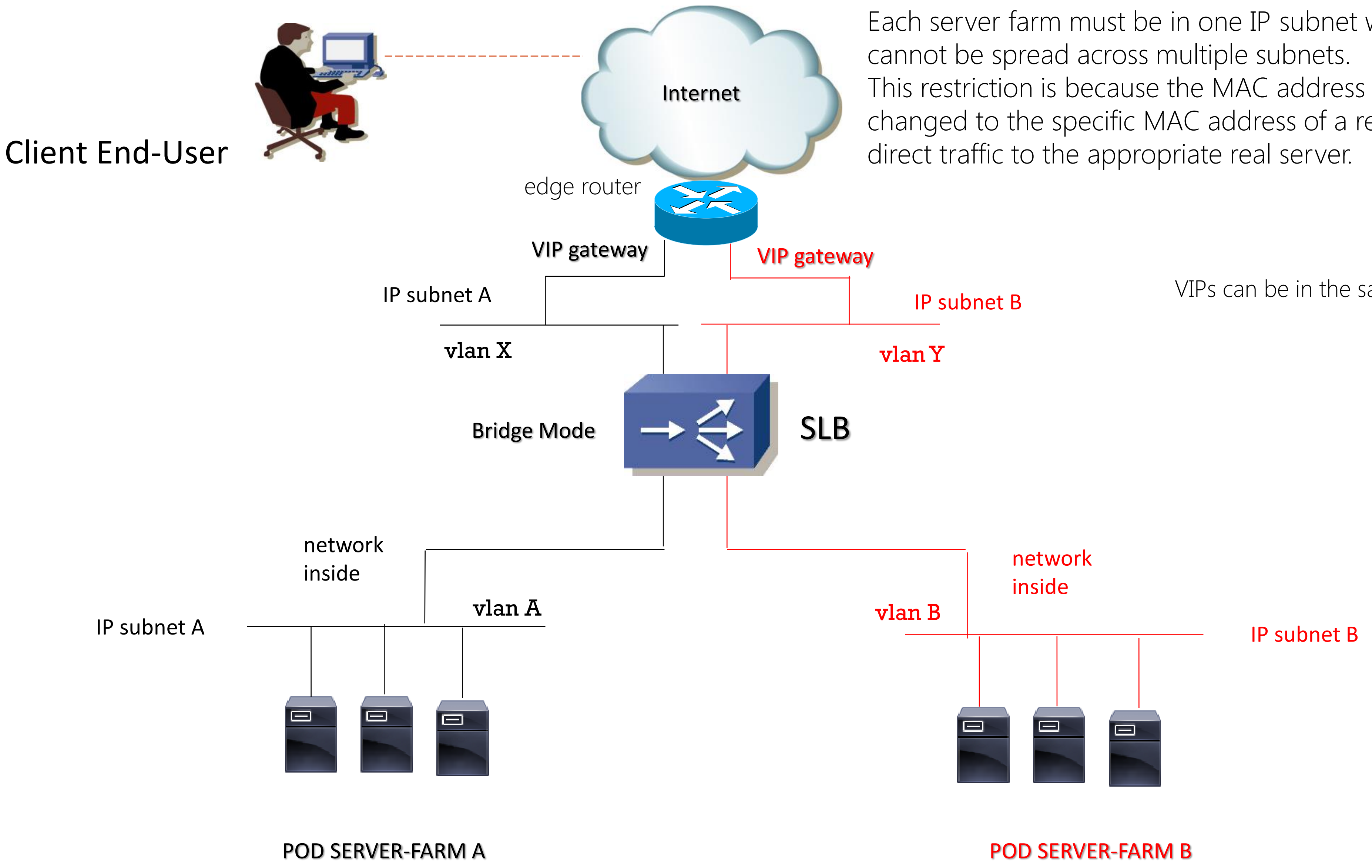
Massimiliano Sbaraglia

CISCO SLB ROUTED MODE



The return reply traffic passes through the SLB, the source real IP is changed to the VIP address, so the end-user has no direct way of telling that there is a SLB in the path.
The end user does not see the IP address of the real server.

CISCO SLB INLINE BRIDGE MODE

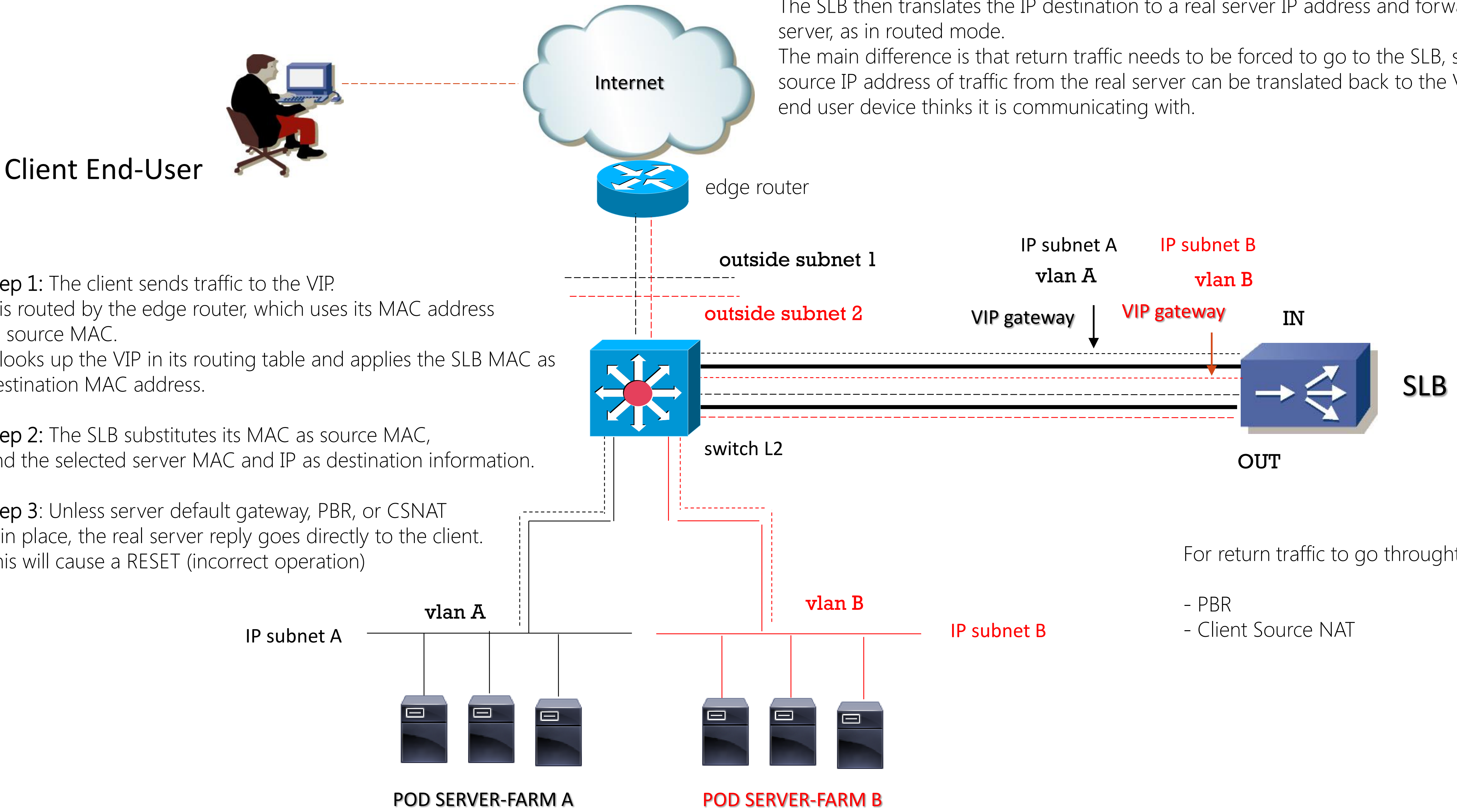


Each server farm must be in one IP subnet which means the servers cannot be spread across multiple subnets.
This restriction is because the MAC address of the common VIP is changed to the specific MAC address of a real server in order to direct traffic to the appropriate real server.

VIPs can be in the same or different subnet.

CISCO SLB ONE (TWO) -ARM MODE

Routing causes inbound end-user traffic to reach the VIP on the SLB.
The SLB then translates the IP destination to a real server IP address and forwards to the real server, as in routed mode.
The main difference is that return traffic needs to be forced to go to the SLB, so that the source IP address of traffic from the real server can be translated back to the VIP that the end user device thinks it is communicating with.



Step 1: The client sends traffic to the VIP.
It is routed by the edge router, which uses its MAC address as source MAC.
It looks up the VIP in its routing table and applies the SLB MAC as destination MAC address.

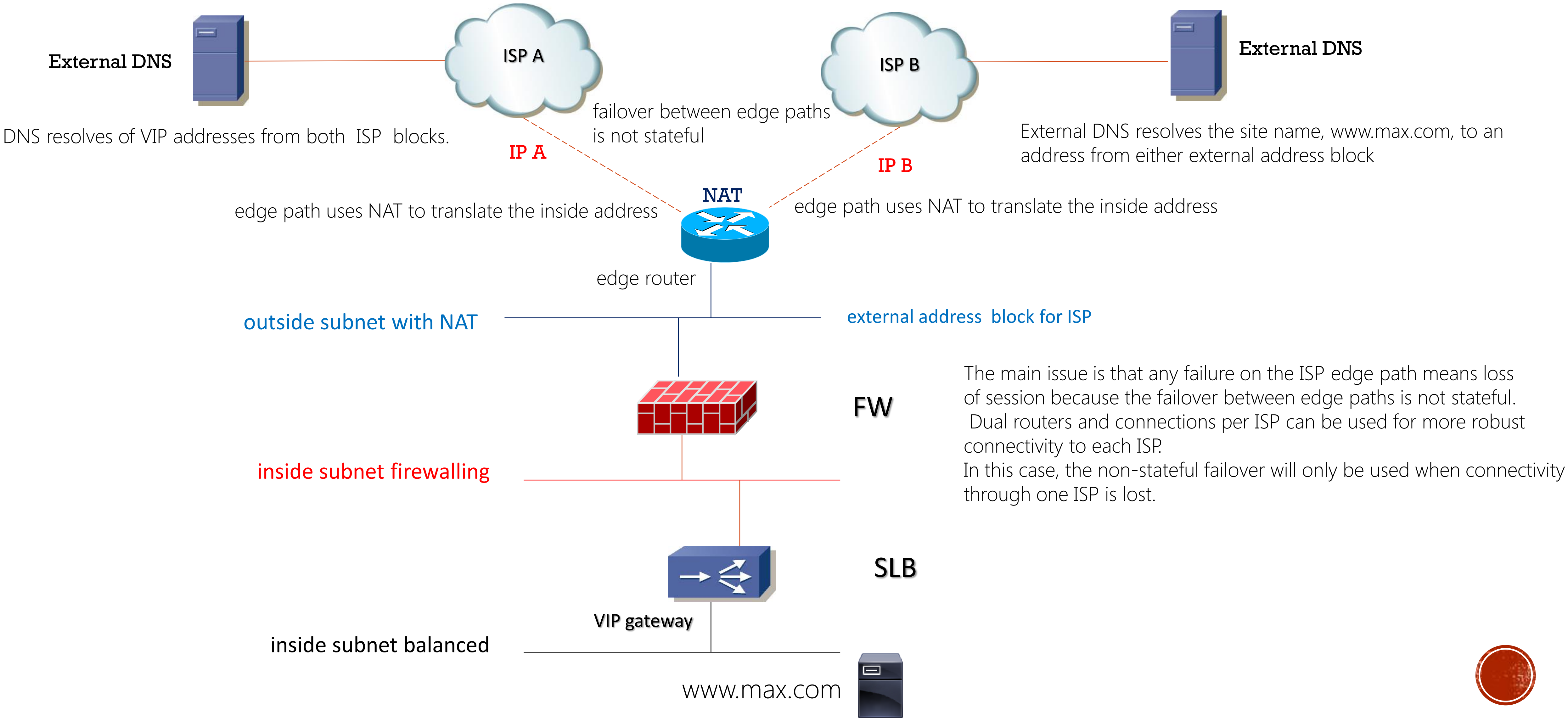
Step 2: The SLB substitutes its MAC as source MAC,
and the selected server MAC and IP as destination information.

Step 3: Unless server default gateway, PBR, or CSNAT
is in place, the real server reply goes directly to the client.
This will cause a RESET (incorrect operation)

For return traffic to go throught SLB:

- PBR
- Client Source NAT

CISCO ONE FIREWALL PER ISP



The external DNS needs to be aware of site connectivity so that it can cease resolving the domain name to addresses at the site that is down.

DNS resolves of VIP addresses from both ISP blocks.

failover between edge paths is not stateful

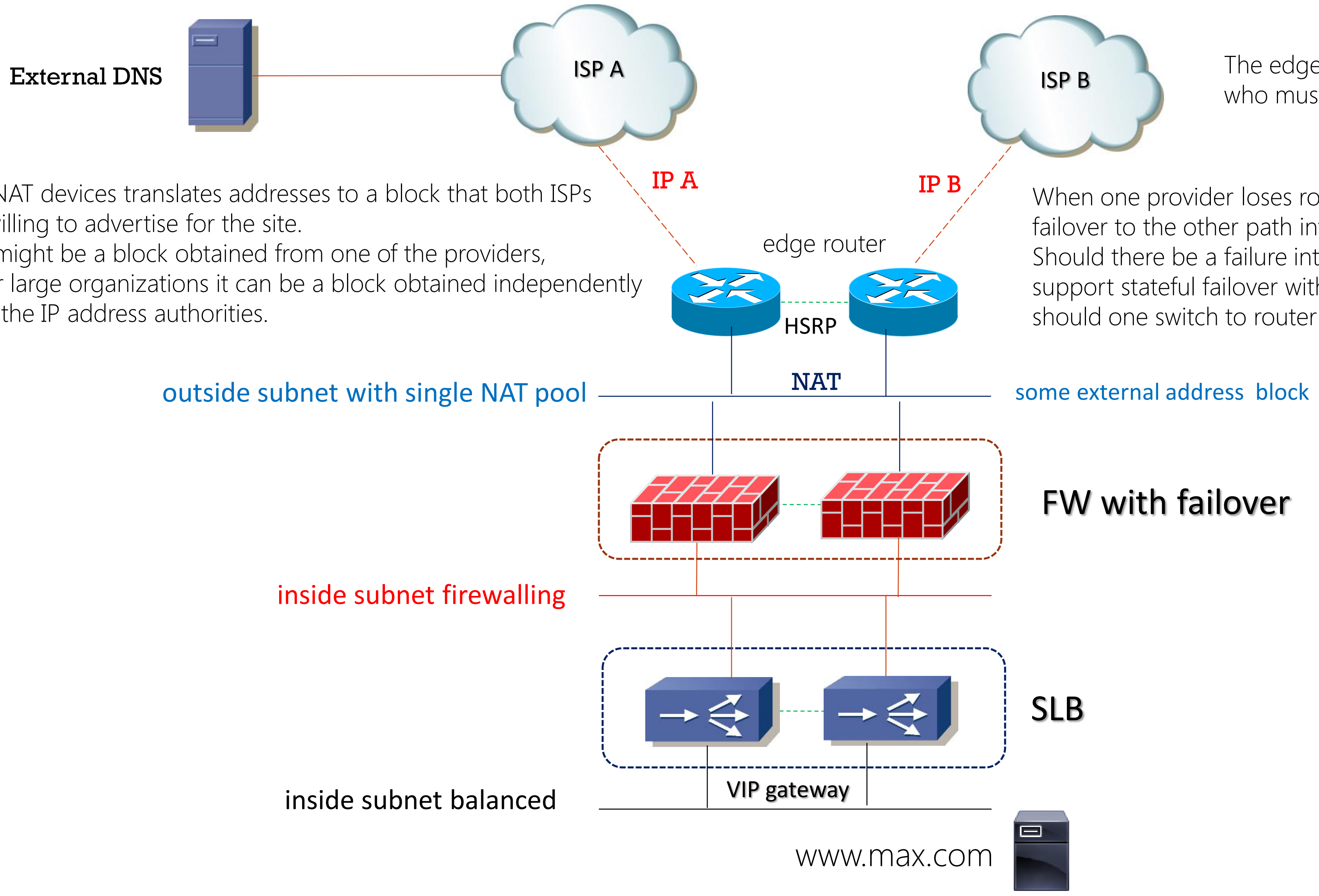
External DNS resolves the site name, www.max.com, to an address from either external address block

edge path uses NAT to translate the inside address

edge path uses NAT to translate the inside address

The main issue is that any failure on the ISP edge path means loss of session because the failover between edge paths is not stateful.
Dual routers and connections per ISP can be used for more robust connectivity to each ISP.
In this case, the non-stateful failover will only be used when connectivity through one ISP is lost.

CISCO STATEFUL FAILOVER FIREWALL WITH COMMON EXTERNAL PREFIX



The edge routers advertise this block via BGP to both ISPs, who must be willing to advertise it to their peers.

The NAT devices translates addresses to a block that both ISPs are willing to advertise for the site.
This might be a block obtained from one of the providers, or for large organizations it can be a block obtained independently from the IP address authorities.

When one provider loses routing or its link, BGP provides users with automatic failover to the other path into the site.
Should there be a failure internal to the site (switches or links), the firewalls can support stateful failover with an active/active design. HSRP is used for failover should one switch to router link fail.

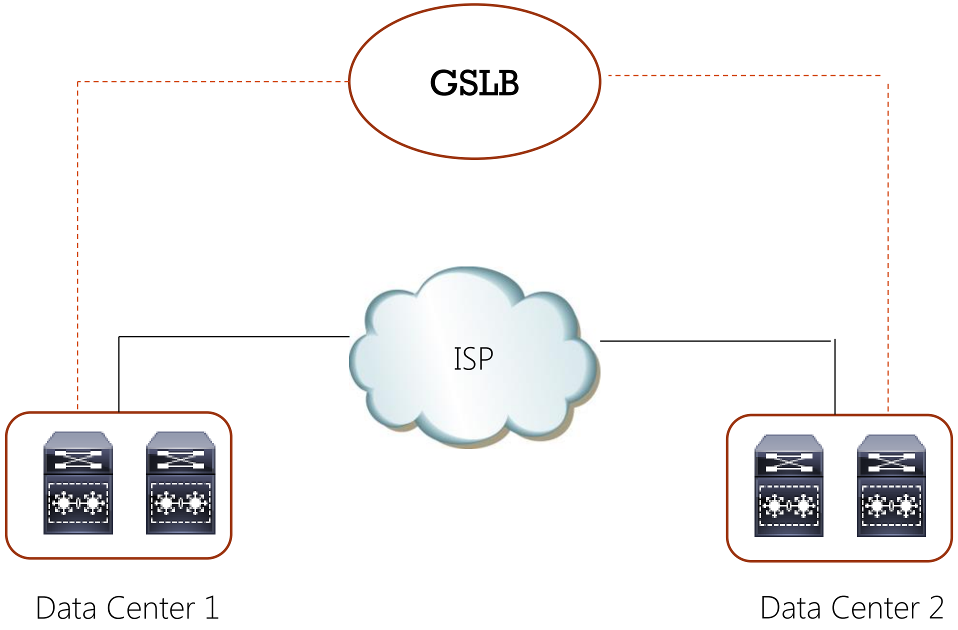
OFF-THE-AIR FAILOVER CISCO GSS GLOBAL SITE SELECTOR

To support the distributed data center design, applications need to be migrated to technology allowing active/active hot databases as opposed to active database and mirrored hot spare database.

Another key element when using distributed sites is technology to detect when a site is "off the air" and should be failed over. The devices that detect the need for failover andrespond must be external to the two sites. This technology can be an external service, or can be provided by equipment at one or more Service Provider co-location facilities.

The "off the air" detection might be provided by an external service such Akamai or Ultra DNS ; it might also be provided using the Cisco Global Site Selector (GSS) technology, typically within a provider colocation facility.

The function provided is called Global Server Load Balancing (GSLB).



CISCO E-COMMERCE BASE DESIGN ONE FWSM-LAYER

Layer 3 firewall used Firewall perimeter at the core layer aggregation and access are considered trusted zones

Security perimeter not possible between web/app/DB servers

CSM is used in routed mode

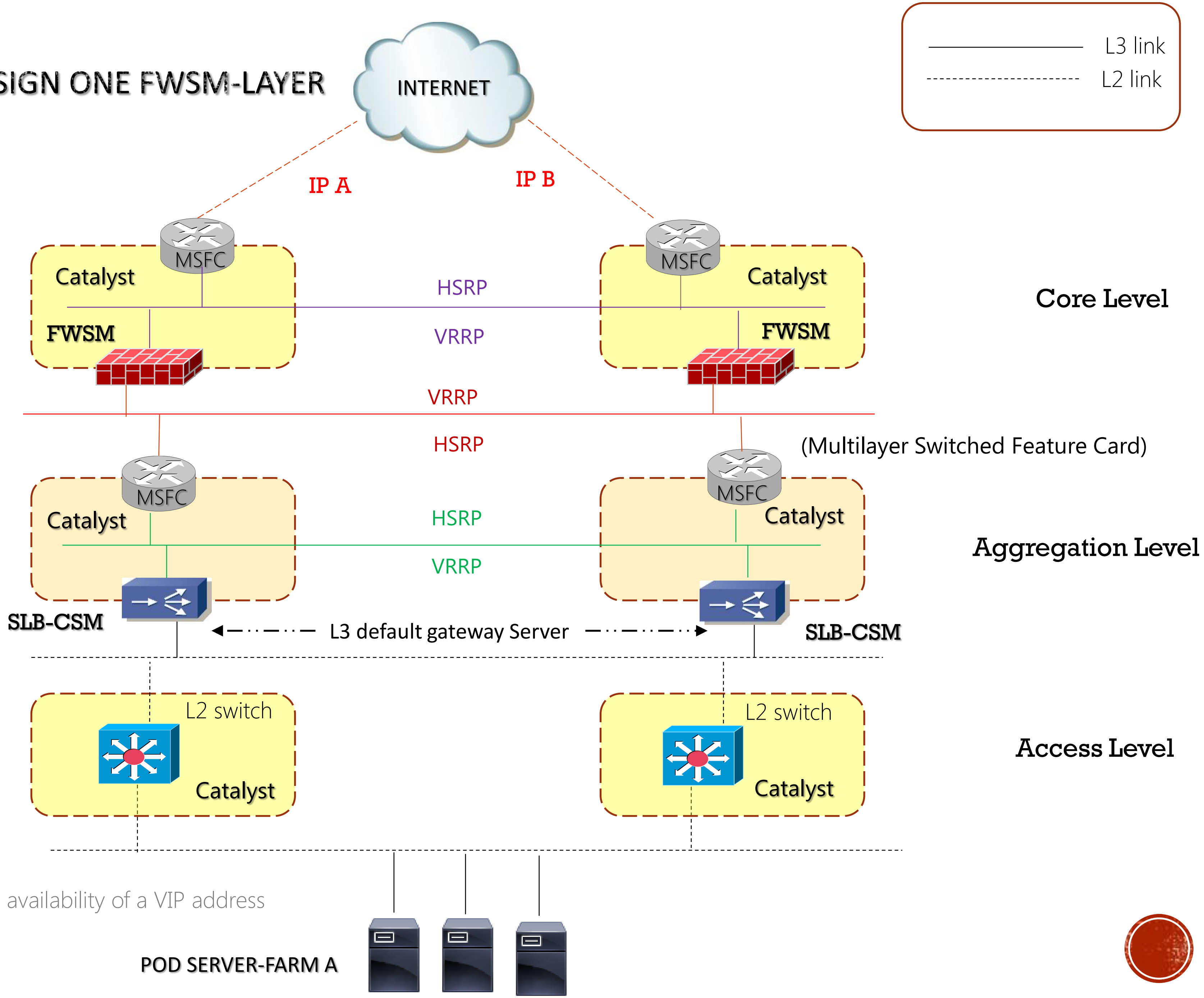
Servers default gateway is the CSM VIP

CSM default gateway is the HSRP group on the MSFC with RHI (Route Health Injection) is possible.

All server traffic goes through the CSM

Additional configurations needed for direct access to servers and non-loadbalanced server initiated sessions

Route Health Injection (RHI) allows the ACE to advertise the availability of a VIP address throughout the intranet as a host route.



CISCO E-COMMERCE BASE DESIGN TWO FWSM-LAYER

Layer 3 firewall used as firewall perimeter at the core

Layer 3 firewall with single context at the aggregation layer

Firewall services are deployed in the aggregation between Web/App/DB tiers

CSM is used in bridged design with multiple bridged VLAN pairs

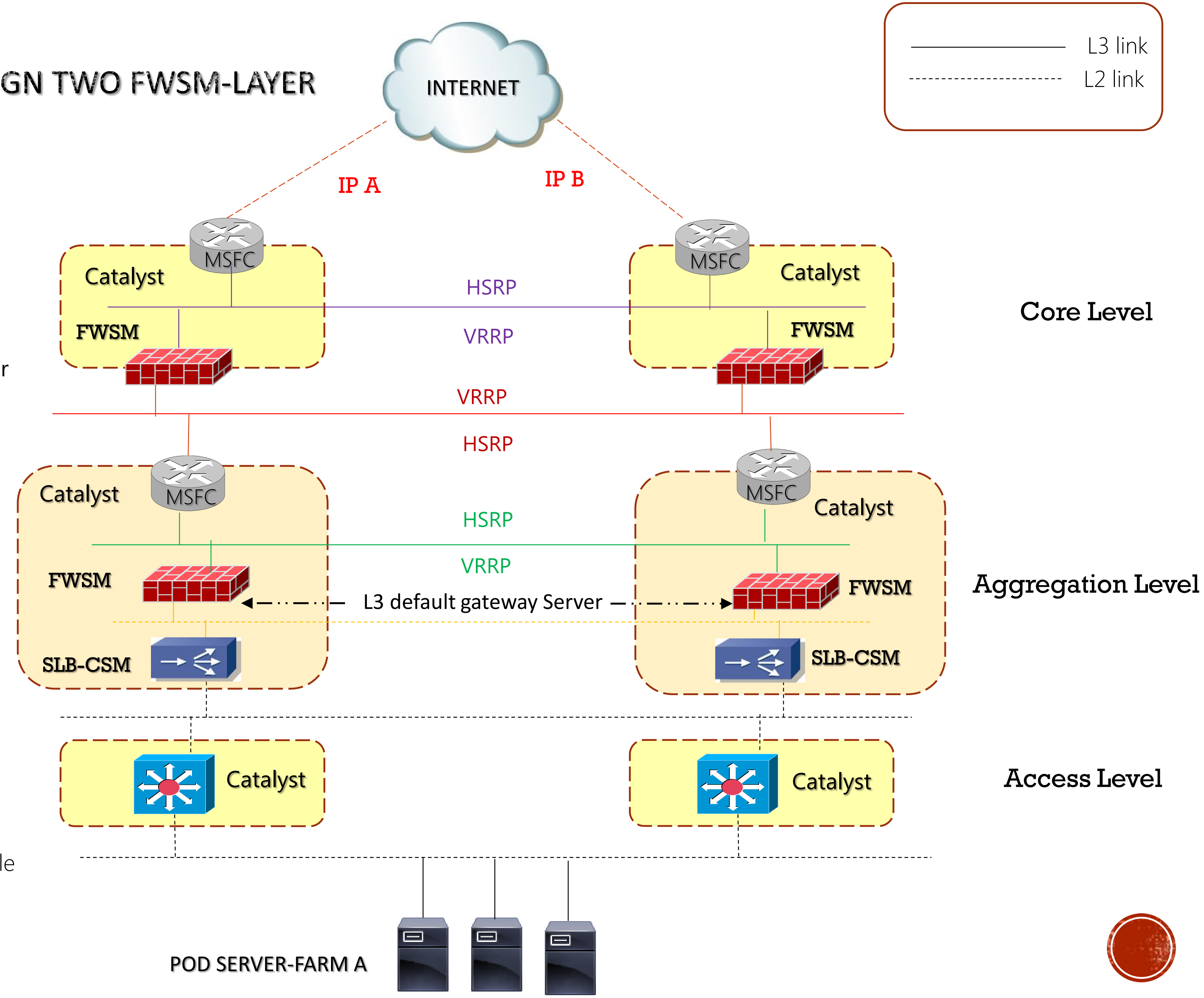
Server default gateway is the aggregation firewall primary IP address

No extra configurations needed for direct access to servers or non-load balanced server initiated sessions

CSM default gateway is the firewall primary IP address

MSFC is not directly connected to the CSM, RHI is not possible

All server traffic goes through the CSM



CISCO ONE-ARMED WITH TWO FWSM DESIGN

Layer 3 firewall is used as firewall perimeter at the core.

Layer 3 firewall with single context is used at the aggregation layer.

Firewall services are deployed in the aggregation between Web/App/DB tiers.

CSM is used in a one-armed fashion:

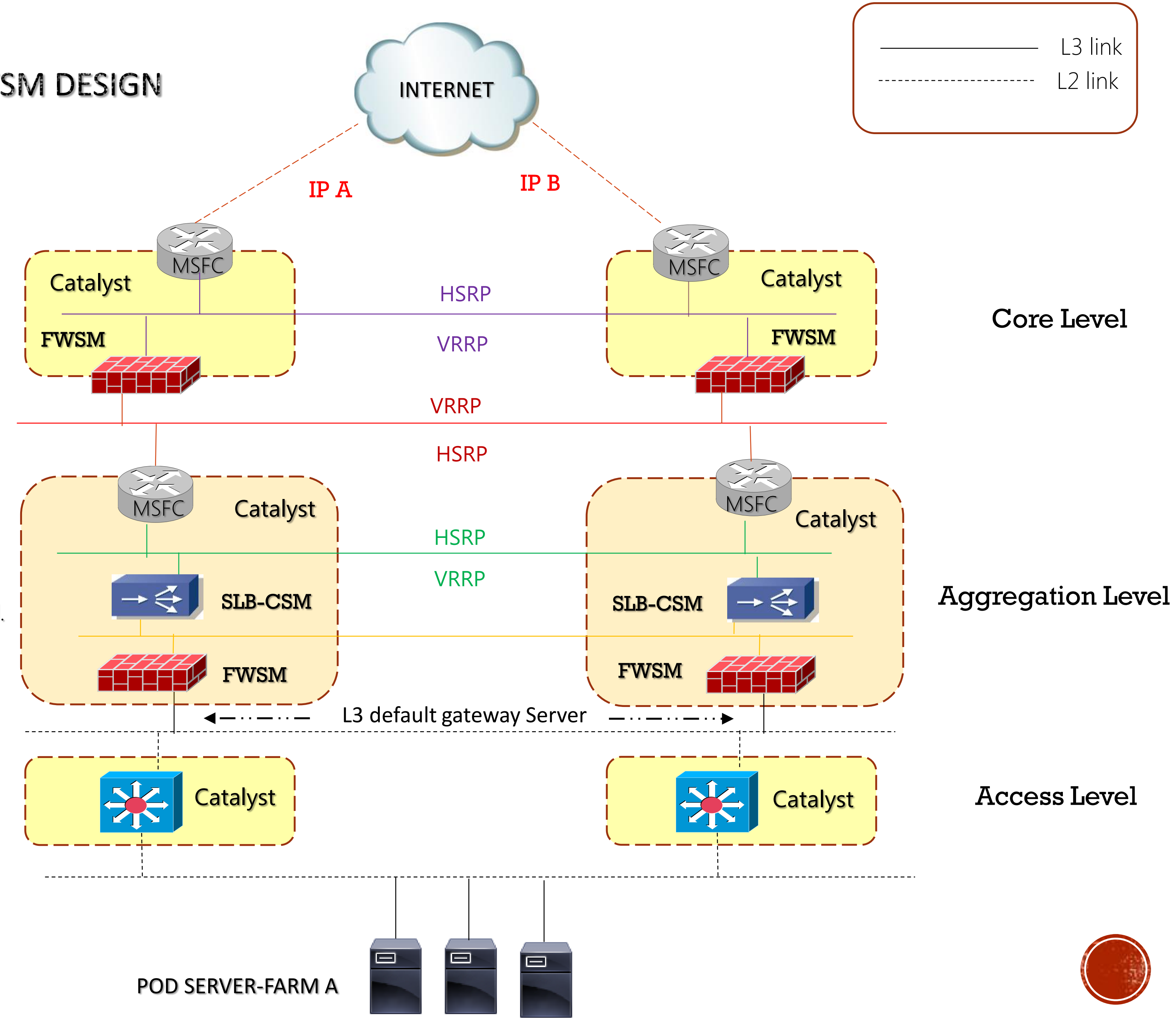
Servers default gateway is the aggregation firewall primary IP add.

No extra configurations needed for direct access to servers
or non-load balanced server initiated sessions.

All non-load balanced traffic to/from servers will bypass the CSM.

CSM default gateway is the HSRP group address on the MSFC.

Since MSFC is directly connected to the CSM, RHI is possible.



CISCO ONE-ARMED WITH VIRTUAL FWSM CONTEXT

Layer 2 firewall used with multiple contexts (transparent mode)

Firewall perimeter at outside, internal and each DMZ.

Aggregation MSFC is a secure internal segment with protection from each connected network.

CSM is used in a one-armed fashion:

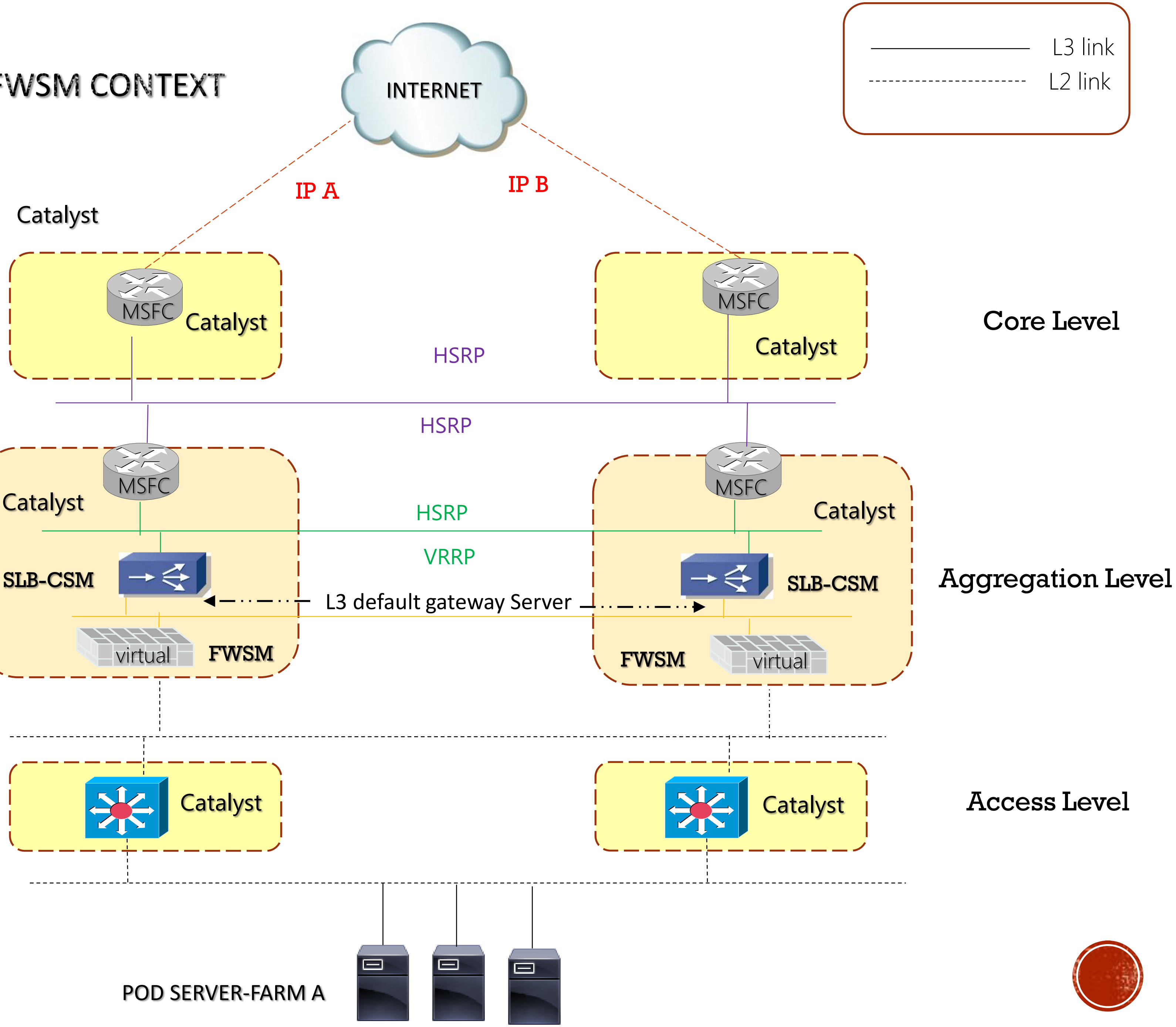
Servers default gateway is the HSRP primary IP address.

No extra configurations needed for direct access to servers or non-load balanced server initiated sessions.

All non-load balanced traffic to/from servers will bypass the CSM.

CSM default gateway is the HSRP group address on the MSFC.
CSM is in routed mode

Since MSFC is directly connected to the CSM, RHI is possible.



L3 link
L2 link
INTERNET
IP A
IP B
Catalyst
MSFC
Catalyst
MSFC
Catalyst
Core Level
HSRP
HSRP
MSFC
Catalyst
MSFC
Catalyst
HSRP
VRRP
SLB-CSM
SLB-CSM
L3 default gateway Server
virtual
FWSM
FWSM
virtual
Aggregation Level
Catalyst
Catalyst
Access Level
POD SERVER-FARM A