ACI CISCO

Application Centric Infrastructure

Massimiliano Sbaraglia

ACI Concepts

Cisco ACI (Application Centric Infrastructure) è basato sul concetto di group-based policy SDN;

End-User ACI può definire una serie di regole senza la conoscenza e/o informazioni che derivano dalla sruttura networking;

Cisco APIC (Application Policy Infrastructure Controller) è responsabile della gestione centralizzata delle policies configurate e distribuirle a tutti i nodi facenti parte della ACI Fabric;

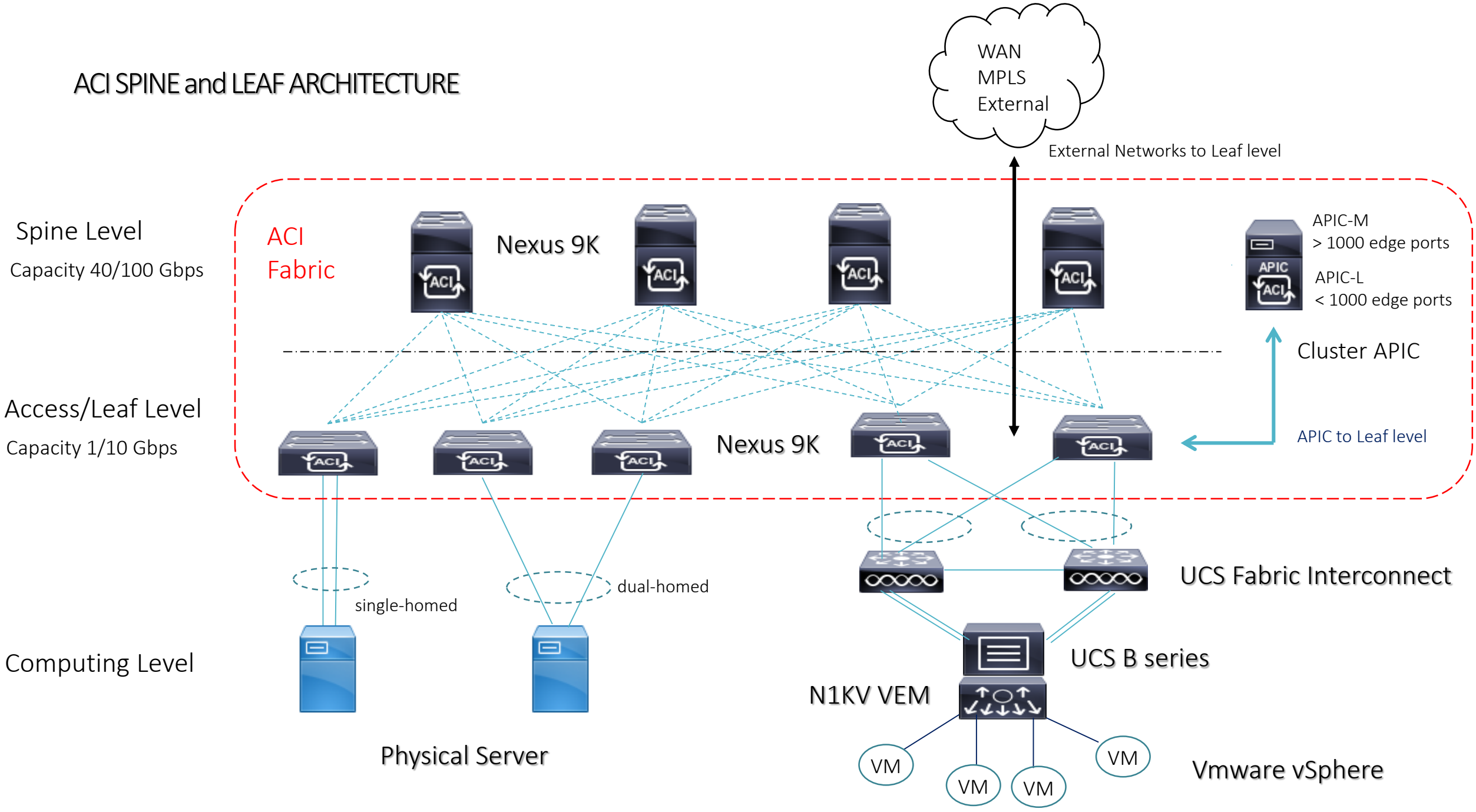
Cisco ACI è disegnato per scalare in modo trasparente nei confronti di cambiamenti di connettività, bandwidth, tenants e policies; la sua architettura è di tipo spine-leaf che si presta efficientemente a introdurre e/o cambiare requisiti di rete;

Cisco ACI include servizi layer 4 to layer 7, APIs (Application Programming Interface), virtual networking, computing, storage resources, wan routers, orchestration services.

Cisco ACI consiste in:

- Un insieme di software e hardware devices che costituiscono una Fabric
- APIC per la gestione delle policies centralizzata
- AVS (Application Virtual Switch) per virtual network edge level
- Integrazione di fisiche e virtuali infrastruttre
- Un aperto ecosistema di network, storage, management e orchestration vendor

ACI SPINE and LEAF ARCHITECTURE



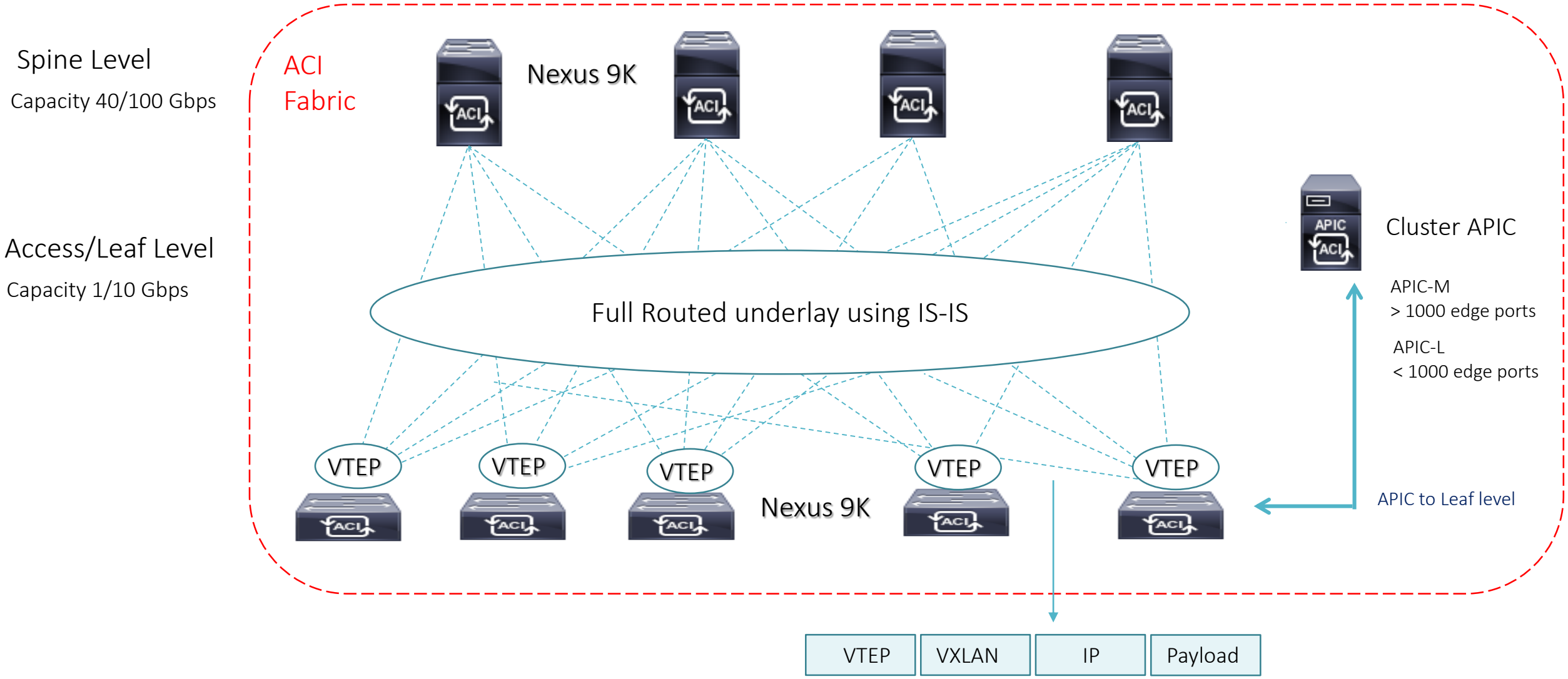
ACI FABRIC UNDERLAY and OVERLAY

ACI Fabric is IP-based with VXLAN overlay

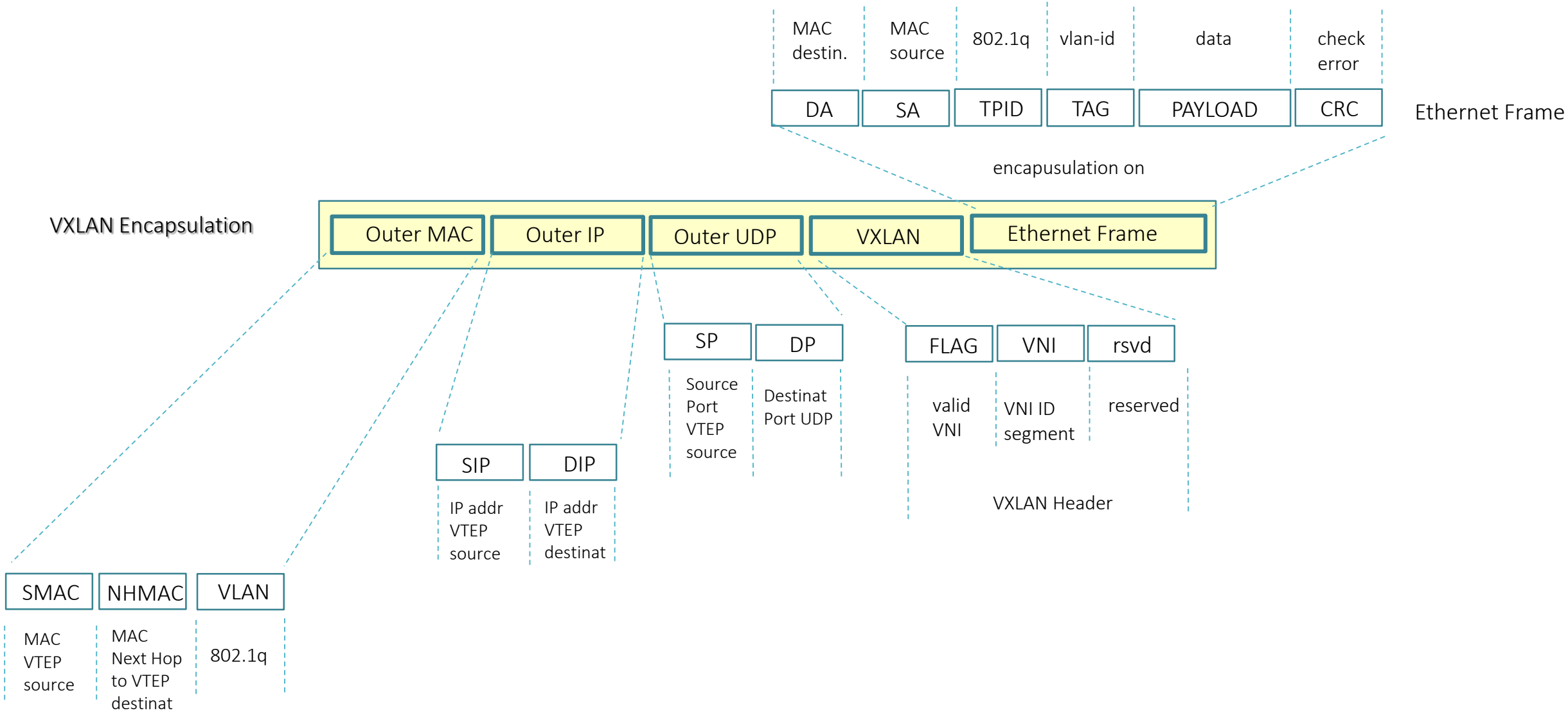
NO STP

VXLAN for encapsulation traffic inside the Fabric MAC-to-IP

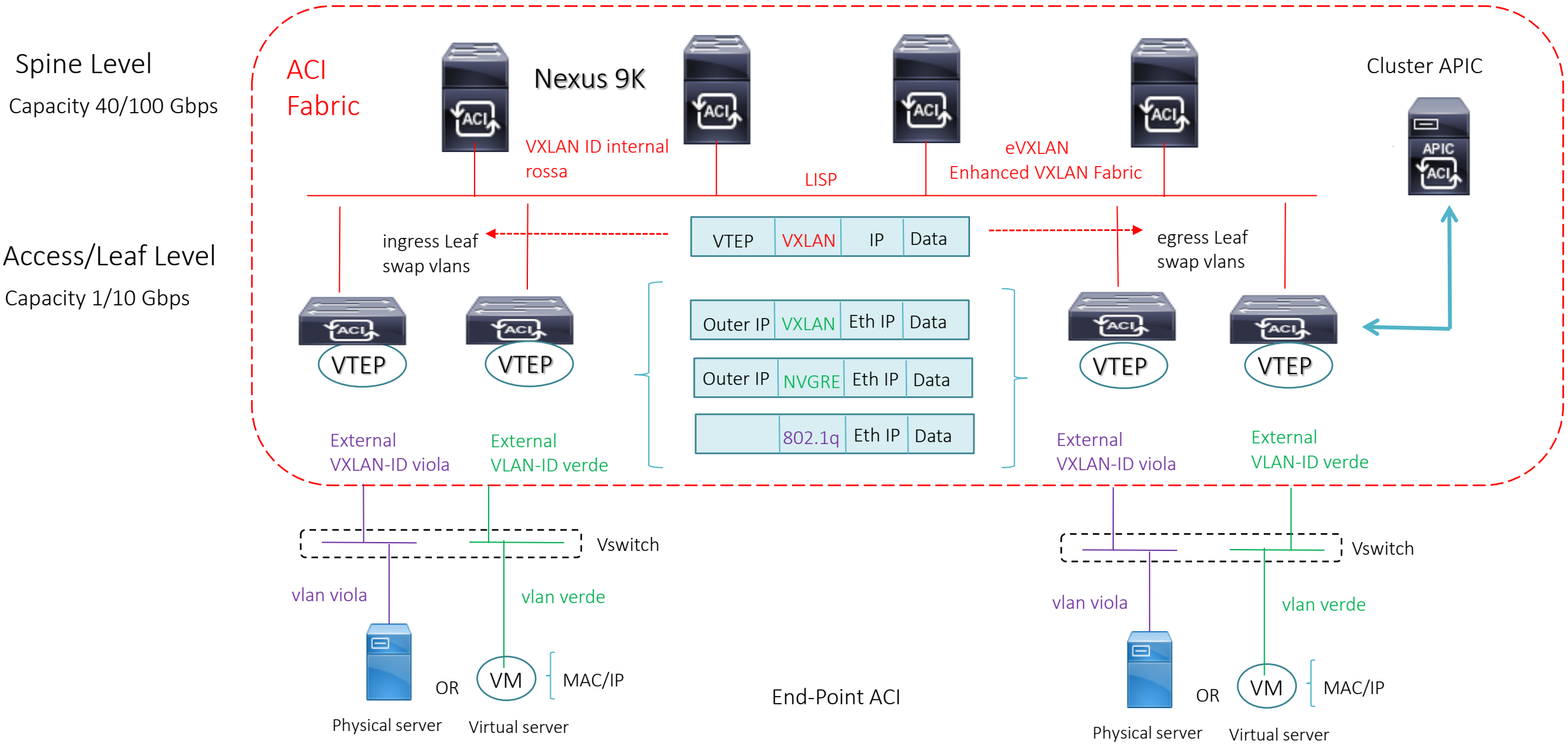
Leaf Switch acts as VTEP



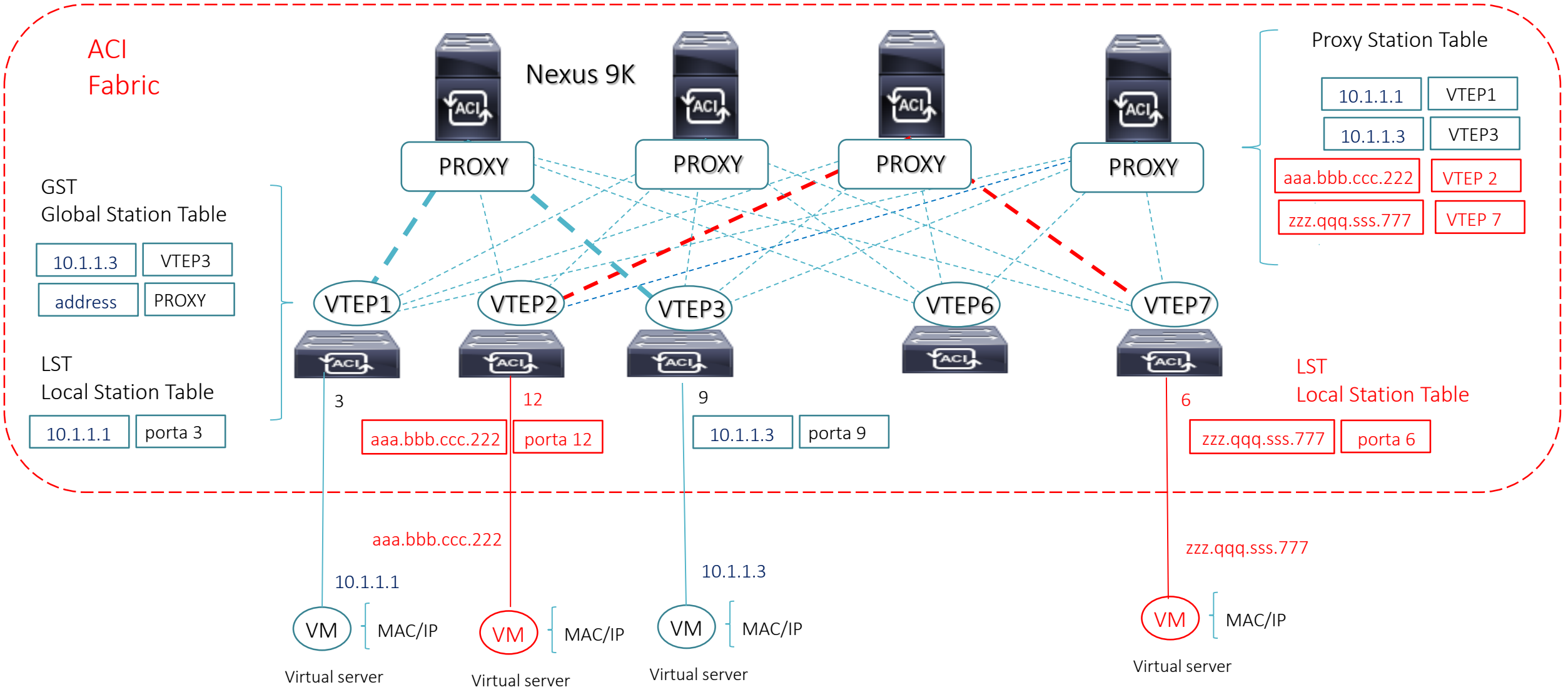
VXLAN HEADER FORMAT



ACI FABRIC FORWARDING PACKETS with VXLAN header



ACI FABRIC Control Plane with Mapping Database



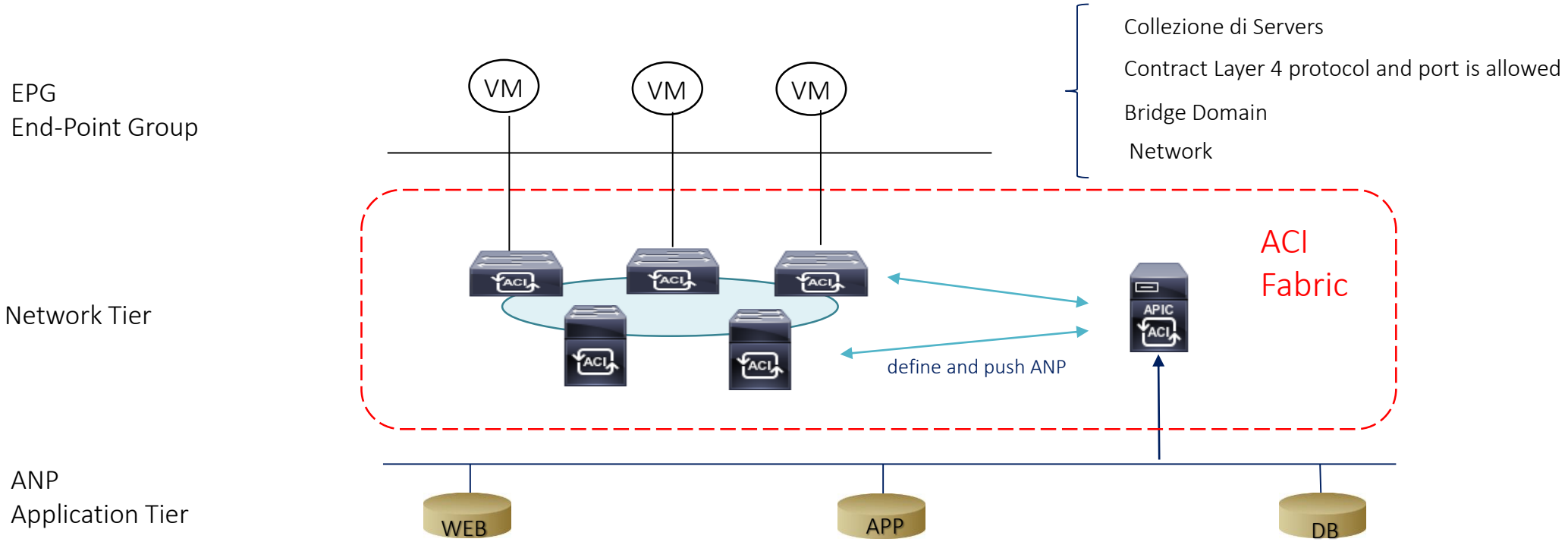
ACI Policy Based approach

Cisco APIC (Application Policy Infrastructure Controller): è responsabile della gestione centralizzata delle policies configurate e distribuirle a tutti i nodi facenti parte della ACI Fabric;

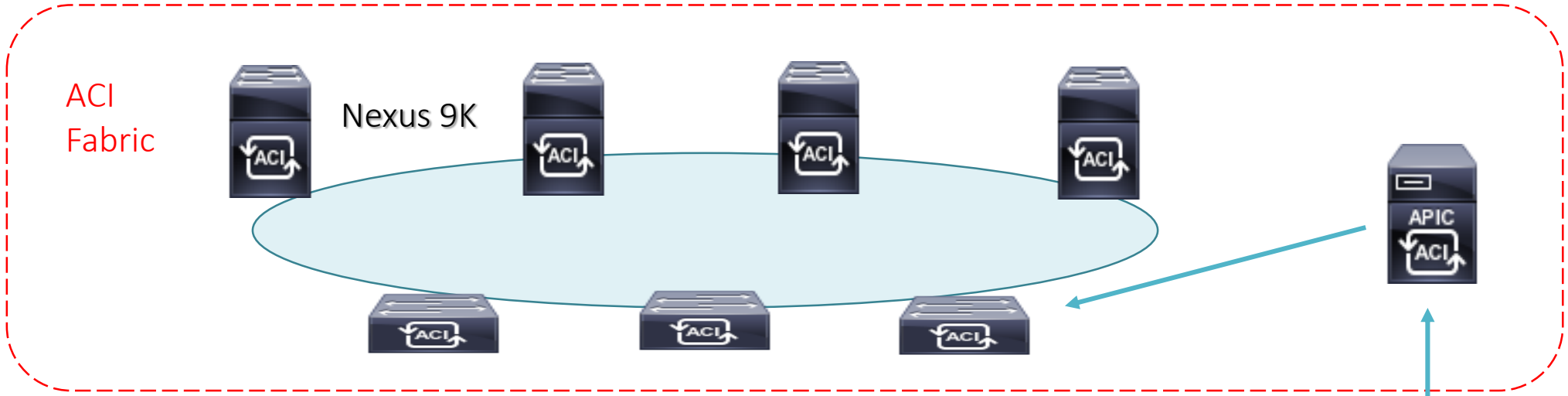
ANP (Application Network Profile): contiene le policies dei sistemi applicativi;

EPG (End Point Group): consiste di un numero di end-point groups rappresentati da uno o più servers all'interno di uno stesso segmento di rete (vlans)

Contract: consiste di policies che definiscono il modo con cui comunicano tra loro gli EPG.



ACI FABRIC Access Policies



5	Switch Profile
4	Interface Policy and Profile
3	Attachable Access Entity Profile (AAEP)
2	Physical Domain
1	Vlan Pool

VM — MAC/IP — Virtual server

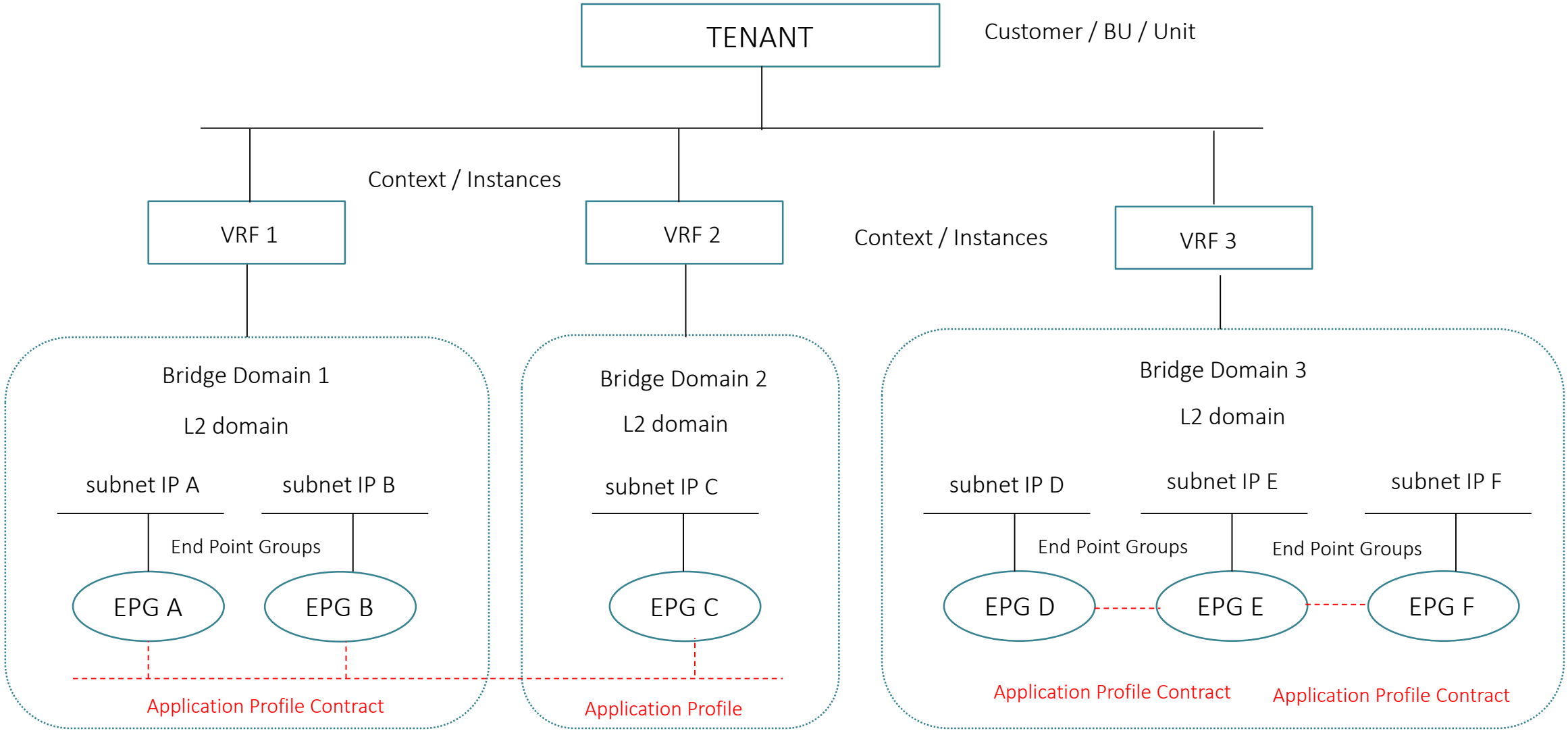
VM — MAC/IP — Virtual server

MAC/IP — MAC/IP — Physical server

ACI FABRIC Access Policies

- **vlan pool:** definisce un singolo segmento di rete (vlan) oppure un pool di vlans;
- **Physical Domain:** definisce un dominio (scopo) dove è creato il vlans pool;
- **AAEP (Attachabe Access Entity Profile):** definisce un modo di raggruppare multipli domini applicabili ad un profilo su base interfaccia;
- **Interface Policy and Profile:** questa policy definisce i parametri richiesti come può essere un LLDP, LACP, ete; contiene la interface policy e specifica a quale port number deve essere applicata usando la port-selector;
- **Switch Profile**: applica il profilo su base interfaccia con la policy associata ad uno o più multiple access Leaf Nodes

ACI FABRIC Building Blocks Tenants



ACI FABRIC steps layer 2 network

1. VRF instances;

2. BD (Bridge Domain) associato alla VRF instance (senza abilitare nessun layer 3 IP SVIs subnet);

3. Configurazione del Bridge Domain per ottimizzare la funzionalità di switching (hardware-proxy-mode) usando il mapping database oppure il tradizionale flood-and-learn;

4. EPG (End Point Group) relazionandoli ai bridge domain di riferimento; possiamo avere multipli EPG associati allo stesso bridge domain;

5. Creare policy Contracts tra EPG come necessario; possiamo anche considerare una comunicazione tra diversi EPG senza ausilio di filtri, settando la VRF instance in modalità < unenforced >

6. Creare access policies switch e port profiles assegnando i parametri richiesti, associate al nodo Leaf di pertinenza

ACI FABRIC layer 2 extending to layer 2 external domain parameter

1. Enable fllooding of layer 2 unknown unicast;

2. Enable ARP flooding;

3. Disable unicast routing (può essere abilitato successivamente ad una fase di migrazione ad esempio ed gli end-point usano come IP gateway il sistema ACI Fabric);

L2Out option provvede ad una L2 extension da ACI Fabric ad un External domain bridged network

ACI FABRIC Leaf Node to External Networks parameters

- **Layer 3 interface routerd:** usata quando si connette un determinato external devices per tenant /VRF;
- **Subinterface with 802.1q tagging:** usata quando vi è una connessione condivisa ad un determinato external devices attraverso tenants/ VRF-lite;
- **Switched Virtual Interface (SVI):** usata quando entrambi i layer L2 ed L3 di connessione sono richiesti sulla stessa interfaccia

La propagazione di external network all'interno di un dominio ACI Fabric utilizza il MP-BGP (Multi Protocol BGP) tra Spine e Leaf (si può avere anche la funzionalità di Route Reflector abilitato a livello Spine) all'interno di un unico AS;

L3Out option prevede i seguenti steps:

1. Create un external routed network
2. Set a layer 3 border leaf node for the L3 outside connection
3. Set a layer 3 interface profile for the L3 outside connection
4. Repeat step 2 and 3 if you need to add additional leaf nodes/interface
5. Configure an external EPG (ACI Fabric maps theexternal L3 router to the external EPG by using the IP prefix and mask
6. Configure a contract policies between the external and internal EPG (without this all connectivity to the outside will be blocked)