Budování SDN v datovém centru

Jiří Cihlář, CCIE #24609, Team Leader Data C

CO TO JE SDN?

Pojem SDN se vyvíjí…..

„SDN je fyzické oddělení „control plane“ od „data plane“ s tím, že „control plane“ řídí více zařízení.“

„SDN je přeposílání paketů v SW (na x86 procesorech).“

„SDN je „whitebox switching“ neboli běh síťového operačního systému na levném komoditním HW“.

„SDN je automatizace pomocí programovatelného přístupu do síťových zařízení.“

„SDN je nový přístup k síti, který abstrahuje síť jako takovou a dovoluje síťovým administrátorům ji spravovat pomocí menší úrovně detailů“.

ALEF

PŘECHOD OD TRADIČNÍHO DC K MODERNÍMU DC

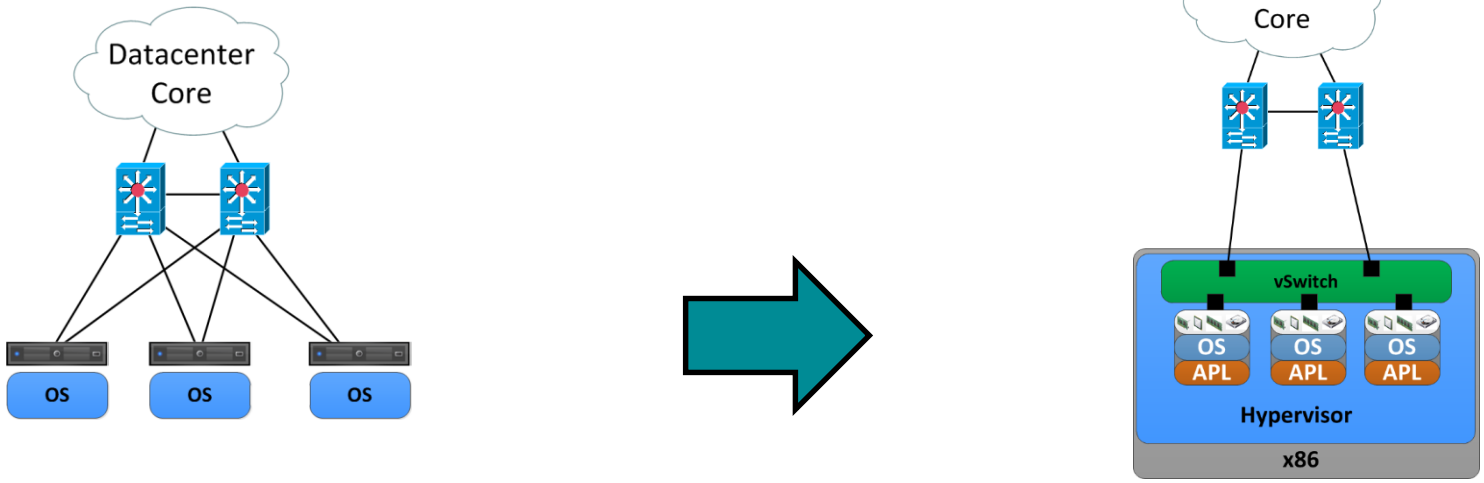
Co způsobilo evoluci (v poslední době navíc akcelerující) v datových centrech?

Moorův zákon	Virtualizace	Cloud
„Počet tranzistorů, které mohou být umístěny na integrovaný obvod, se při zachování stejné ceny zhruba každých 18 měsíců zdvojnásobí.“	*„Virtualizace serverů dovoluje běh více operačních systémů (virtuálních strojů) na jednom sdíleném hardware.“*	*„Způsob poskytování služeb či programů vzdáleně přes Internet.“*

ALEF

DŮSLEDKY VIRTUALIZACE

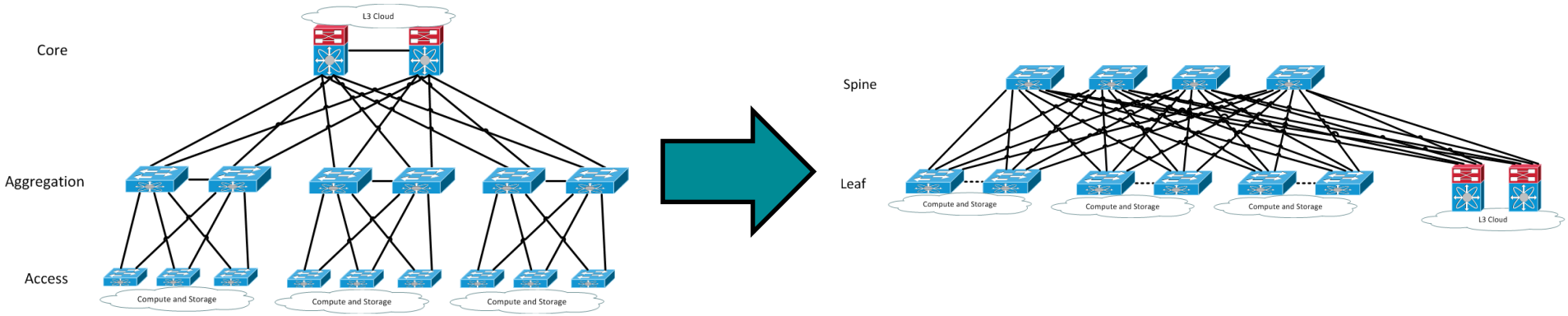
- Virtualizace vytváří novou vrstvu v síťové architektuře – virtuální přepínač
- Prolínání networking a compute oblasti z pohledu správy
- Přístupová vrstva se posouvá do oblasti virtuálního/SW přepínače



ALEF

DŮSLEDKY VIRTUALIZACE

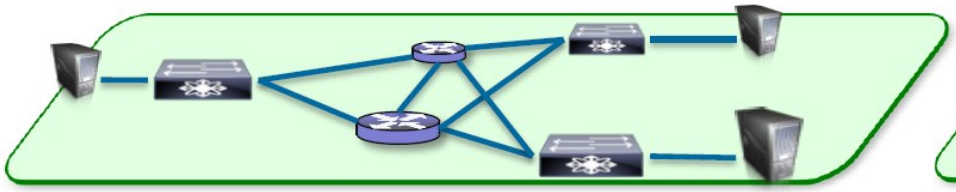
- Tradiční 3-úrovňová topologie se vyvinula pro client-server architekturu, kde většina komunikace (uvádí se více než 80%) probíhala North-South = od klientů k serverům
- Virtualizace a nové technologie (např. big data) kompletně mění rozložení provozu – postupná převaha East – West provozu (dnes se uvádí různá čísla, vždy vyšší než 80%).
- => Postupně byla reinkarnována CLOS topologie (používán název fabrika)



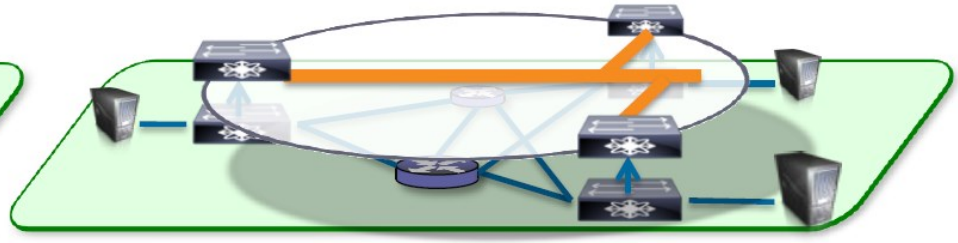
ALEF

DŮSLEDKY VIRTUALIZACE

- Virtualizace přinesla možnost živé migrace virtuálních strojů (vMotion)
- => požadavek na L2 konektivitu v celém datovém centru
- => velkým poskytovatelům služeb nedostačuje 4K VLAN
- => vznikají nové technologie, které mají splnit požadavek na L2 konektivitu ve velkém měřítku bez STP protokolu, více současně aktivních cest s rychlou dobou konvergence a extrémní škálovatelností



Underlay

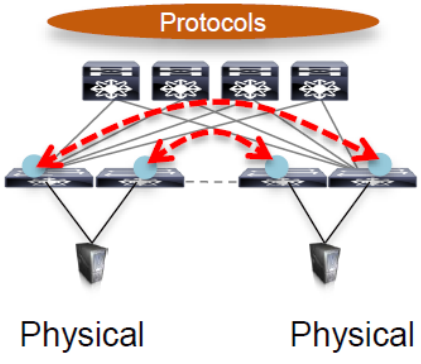


Overlay

Network Based overlays	Host Based overlays
IEEE 802.1q Tunneling	Stateless Transport Tunneling (STT)
Cisco FabricPath	**NVGRE**
TRILL	**VXLAN**
Overlay Transport Virtualization (OTV)	
LISP	
MPLS/VPLS VPN	

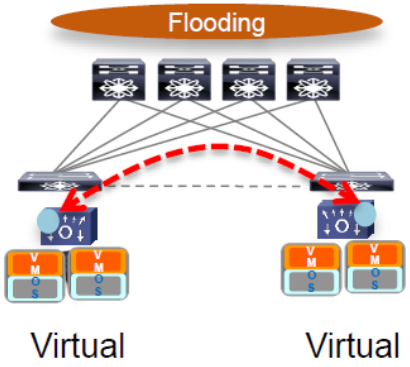
OVERLAY

Network overlay



Enkapsulace je prováděna na přepínačích v HW

Host based overlay

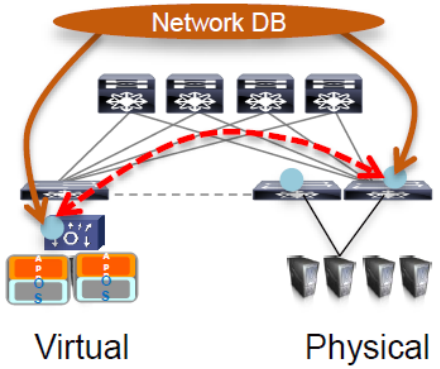


Enkapsulace je prováděna ve virtuálních přepínačích v SW

„There is limited visibility between the NSX virtual overlay and physical underlay networks,which can impact overall network visibility and increase time to troubleshoot and repair problems.“

(Source Gartner Magic Quadrant for Data Center Networking)

Hybrid overlay



Enkapsulace může být prováděna ve virtuálních přepínačích i v HW přepínačích.

Poskytuje i nadále síťařům informace o přenášeném provozu v underlay i overlay.

Umožňuje kombinovat virtualizované i nevirtualizované prostředí bez výkonnostních limitů.

Umožňuje kombinaci různých virtuálních platforem a normalizaci vstupní enkapsulace.

ALEF

JAK VZNIKL TLAK NA SDN V DATOVÉM CENTRU?

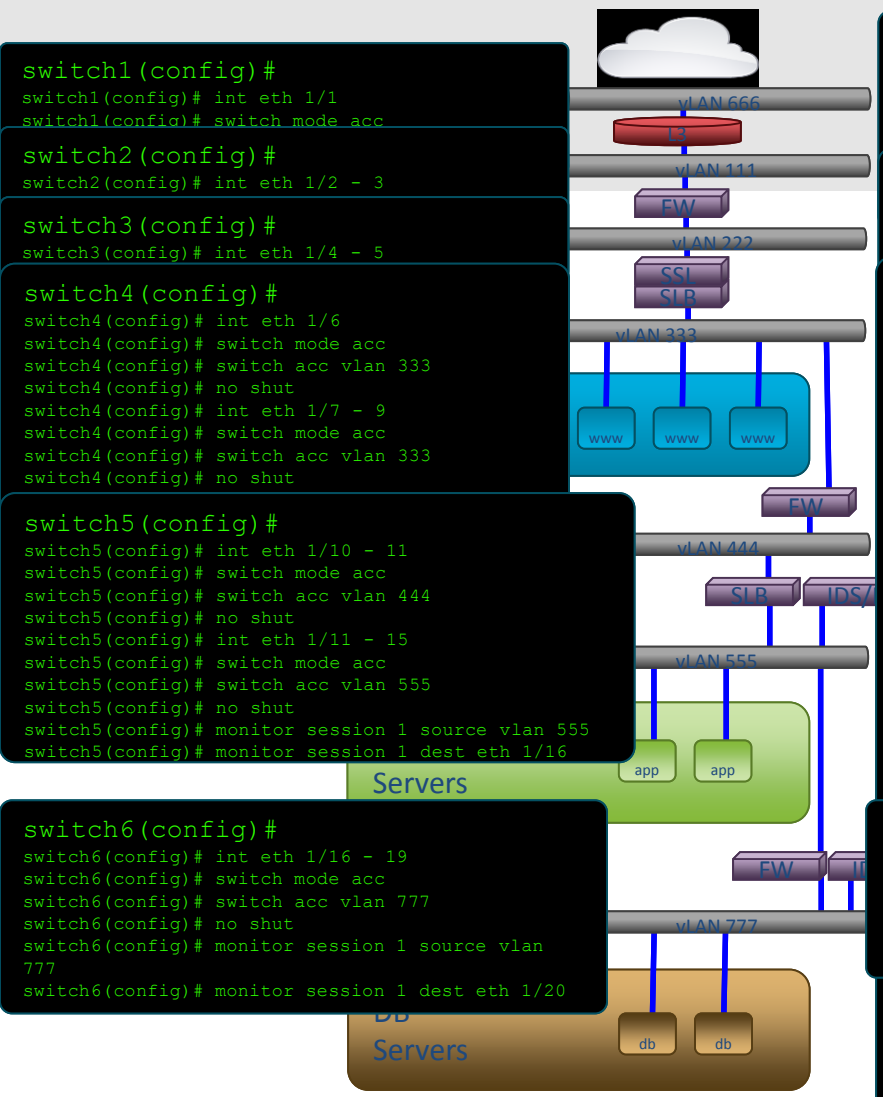
- Doposud síťaři řešili VLANy, IP subnety, VRF, STP, FHRP, směrovací protokoly,…
- Řešení byla postavena na box-by-box designu
- Bezpečnost a vysoká dostupnost řešena na fyzických zařízení k tomu určených a spravovaných samostatně
- V nových řešeních se navíc objevuje VXLAN, VXLAN L2/L3 GW, VXLAN bridging/routing, MBGP, distributed GW, overlay normalizace,….
- Sítě se stávají ještě složitější, což je v protikladu s požadavkem na rychlejší a flexibilnější nasazování aplikací

JAK STAVÍME SÍTĚ DNES?

- Architektura aplikace
- Komponenty a služby
- Uživatelé
  - Kolik, odkud
- Očekávané vytížení
- Odkud budou uživatelé přistupovat
- Bezpečnostní požadavky
- Závislosti
- SLA
- …

- Alokace VLAN, IP adres
- Konfigurace Trunk
- Konfigurace VLAN na switchi a hypervizoru
- Konfigurace pravidel, NAT/PAT
- Konfigurace VIP a protokolů
- Propagace do [illegible] protokolů

ALEF




```
switch1(config)#
switch1(config)# int eth 1/1
switch1(config)# switch mode acc
```

```
switch2(config)#
switch2(config)# int eth 1/2 - 3
```

```
switch3(config)#
switch3(config)# int eth 1/4 - 5
```

```
switch4(config)#
switch4(config)# int eth 1/6
switch4(config)# switch mode acc
switch4(config)# switch acc vlan 333
switch4(config)# no shut
switch4(config)# int eth 1/7 - 9
switch4(config)# switch mode acc
switch4(config)# switch acc vlan 333
switch4(config)# no shut
```

```
switch5(config)#
switch5(config)# int eth 1/10 - 11
switch5(config)# switch mode acc
switch5(config)# switch acc vlan 444
switch5(config)# no shut
switch5(config)# int eth 1/11 - 15
switch5(config)# switch mode acc
switch5(config)# switch acc vlan 555
switch5(config)# no shut
switch5(config)# monitor session 1 source vlan 555
switch5(config)# monitor session 1 dest eth 1/16
```

```
switch6(config)#
switch6(config)# int eth 1/16 - 19
switch6(config)# switch mode acc
switch6(config)# switch acc vlan 777
switch6(config)# no shut
switch6(config)# monitor session 1 source vlan
777
switch6(config)# monitor session 1 dest eth 1/20
```

```
router(config)#
router(config)# int eth 1
router(config)# ip add 6.6.6.1 255.255.255.0
router(config)# not shut
router(config)# int eth 2
```

```
fw1(config)#
fw1(config)# int eth 0/1
fw1(config)# nameif outside 0
fw1(config)# int eth 0/2
```

```
slb1 (CONFIG)
probe http http-probe
 interval 30
 expect status 200 200
rserver host websrvr1
  description foo web server
  ip address 3.3.3.1
  inservice
```

```
fw2(config)#
fw2(config)# int eth 0/1
fw2(config)# nameif webfront 20
```

```
slb2 (CONFIG)
rserver host appsrvr1
  description foo app server
  ip address 5.5.5.1
  inservice
rserver host appsrvr2
  description foo app server
  ip address 5.5.5.2
  inservice
rserver host appsrvr3
  description foo app server
  ip address 5.5.5.3
```

```
fw3(config)#
fw3(config)# int eth 0/1
fw3(config)# nameif appfront 70
fw3(config)# int eth 0/2
fw3(config)# nameif dbfront 90
fw3(config)# object network db_cluster
fw3(config)# host 7.7.7.7
fw3(config)# nat (dbfront,appfront) static 5.5.5.50
fw3(config)# access-list web_to_app permit tcp any host 5.5.5.50 eq 1433
```

```
  policy-map type loadbalance first-match FOO_APP-MATCH
        class FOO_APP
          sticky-serverfarm sn_cookie
  policy-map multi-match FOO_APP-VIP
        class FOO_APP_VIP_CLASS
          loadbalance vip inservice
          loadbalance policy FOO_APP-MATCH
          loadbalance vip icmp-reply
          loadbalance vip advertise active
          loadbalance vip inservice
          loadbalance policy FOOWEB-MATCH
          loadbalance vip icmp-reply
          loadbalance vip advertise active
        class FOOSSL_VIP_CLASS
          loadbalance vip inservice
          loadbalance policy FOOSSL-MATCH
          loadbalance vip icmp-reply
          loadbalance vip advertise active
          ssl-proxy server FOOWEB_SSL
interface vlan 222
  service-policy input FOOWEB_SSL
```

ALEF

JAK VZNIKL TLAK NA SDN V DATOVÉM CENTRU?

- Doposud síťaři řešili VLANy, IP subnety, VRF, STP, FHRP, směrovací protokoly,…
- Řešení byla postavena na box-by-box designu
- Bezpečnost a vysoká dostupnost řešena na fyzických zařízení k tomu určených a spravovaných samostatně
- V nových řešeních se navíc objevuje VXLAN, VXLAN L2/L3 GW, VXLAN bridging/routing, MBGP, distributed GW, overlay normalizace,….
- Sítě se stávají ještě složitější, což je v protikladu s požadavkem na rychlejší a flexibilnější nasazování aplikací
- Pravděpodobnost selhání lidského faktoru se zvyšuje, profylaxe konfigurace se stává ještě složitejší
- Tlak na automatizaci a tím i na SDN
- Řešením je abstrakce sítě a její konfigurace pomocí centrálního řadiče – **přesně tímto řešením je Cisco ACI (Application Centric Infrastructure)**

CO ŘEŠÍME, KDYŽ STAVÍME SDN?

- Fyzická topologie v podobě CLOS fabric s dostatečnou propustností a škálovatelností
- Hybrid based overlay v HW přepínačích a SW virtuálních přepínačích pod jednotnou správou (overlay, underlay, fyzické i virtuální přepínače)
- Možnost monitorování a troubleshootingu síťového provozu kdekoliv v síti – v underlay i overlay
- Řízení sítě pomocí centrálního řadiče
- Funkčnost sítě i při výpadku centrálního řadiče a i v takový moment reakce na výpadky a poruchy
- Podpora připojení virtualizovaných serverů i bare metal serverů
- Podpora více platforem virtuálních řešení
- Možnost integrace do vyšších softwarových orchestračních vrstev
- Možnost integrace se zařízeními vyšších síťových vrstev L4 – L7 typu firewall, load balancer
- Propojení do stávající infrastruktury po L2 nebo L3

ALEF

CO ŘEŠÍME, KDYŽ STAVÍME SDN?

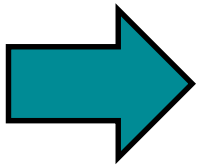
Ale především…

- SDN a obecně SDDC znamená kompletně nový přístup mimo zajeté firemní procesy, organizační strukturu, nasazované technologie apod.
- Opomenutí jakékoliv oblasti a soustředění se například pouze na technologickou oblast může znamenat neúspěch takovéhoto projektu.

ALEF

POSTUP K ÚSPĚŠNÉMU NASAZENÍ SDN?

- Tradičně postavená datová centra jsou často technologicky jen obtížně posunutelná do oblasti softwarově řízených datových center.
- Možnost kompletní náhrady je často odmítnuta z důvodů finančních (ochrana investic) a technických (nutnost zajistit provoz stávajících služeb kritických pro chod společnosti).



- Vybudování samostatného řešení datového centra stojícího mimo stávající produkční řešení.
- Obě řešení jsou od sebe fyzicky i logicky odděleny a pouze dle požadavků společnosti mezi sebou propojeny.

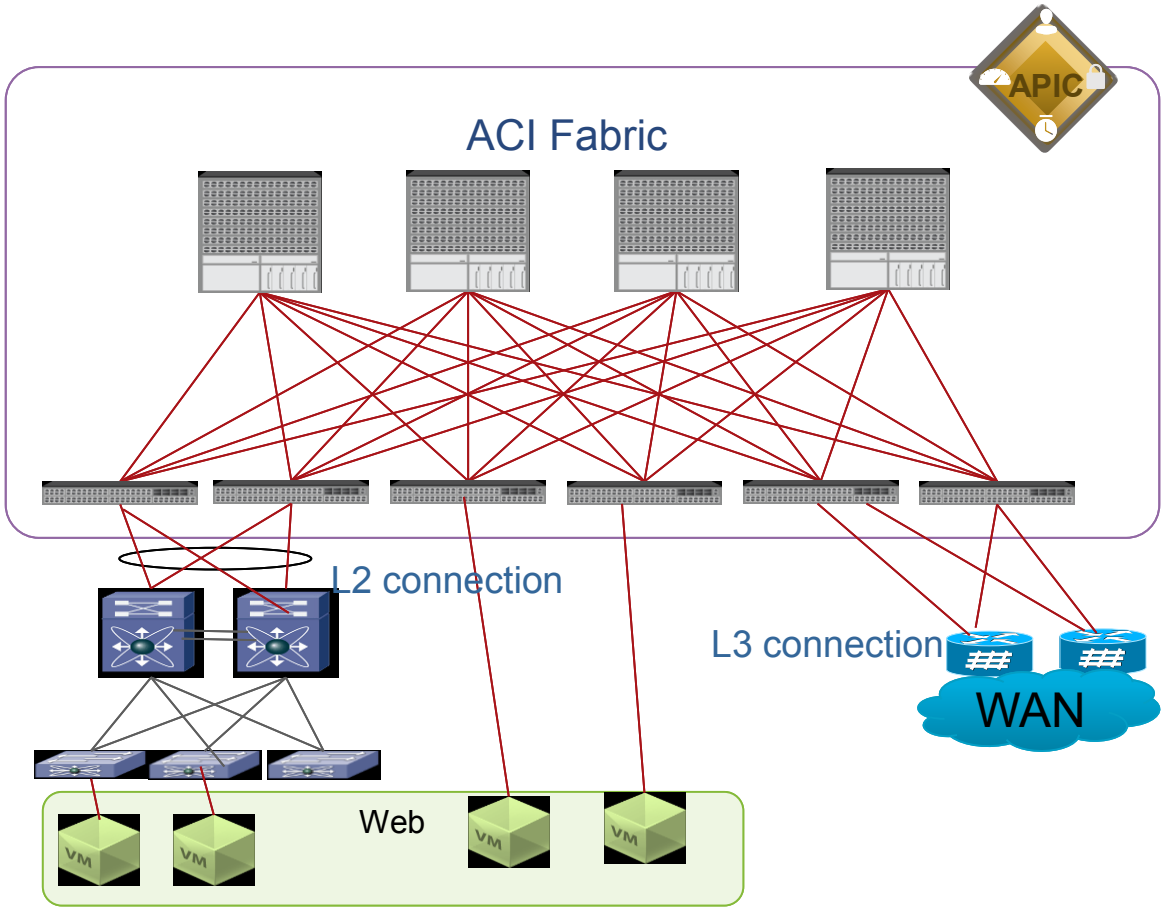
ALEF

CO MI TO PŘINESE?

- Možnost otestovat technické řešení nutné pro běh SDN / SDDC
- Možnost otestovat škálovatelnost a výkonnost řešení v dlouhodobějším provozu
- Možnost ověřit koncept bezpečnosti a vysoké dostupnosti v novém řešení
- Možnost vést diskuzi a následně vydefinovat služby, které je možné poskytovat automatizovaně (odpovídá servisnímu katalogu služeb)
- Možnost vyzkoušet si procesní a organizační fungování v novém prostředí a následně zahájit diskuzi o nutných změnách v procesech uvnitř organizace
- **Možnost v případě, kdy budou zvládnuty procesy a technické rozdíly, začít přesouvat aplikace a služby do nového prostředí**

ALEF

SDN = CISCO ACI



ALEF