Architetture Layer 2

Massimiliano Sbaraglia

Ethernet e 802.1Q

ETHERNET Protocol

Ethernet è una frame di livello 2 (data-link) del modello ISO/OSI per il trasporto di informazioni di dati; essa è composta da:

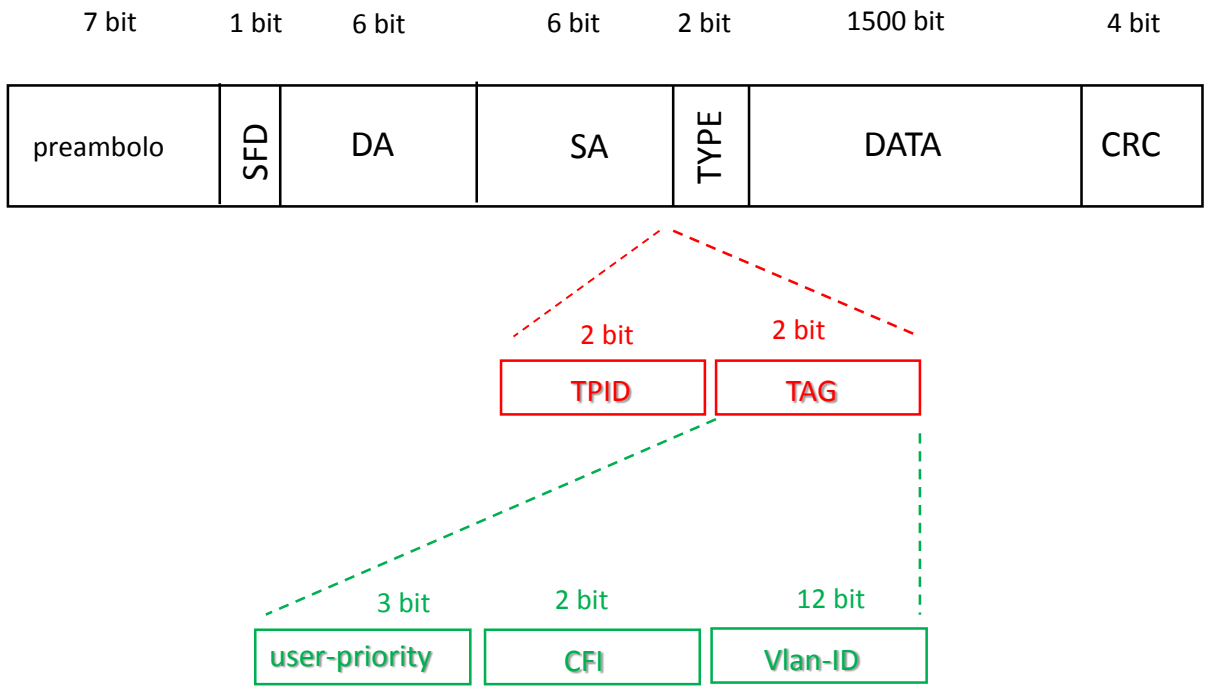
- Preambolo: ha il compito di sincronizzare il mittente con il destinatario a livello fisico con un valore binario = 10101010
- SFD: indica l'inizio di una frame con valore = 10101011
- DA: indica il MAC address dell'unità di destinazione
- SA: indica il MAC address dell'unità sorgente
- Type: indica il tipo di protocollo utilizzato (802.3 ethernet) oppure la lunghezza del campo data
- Data: contiene il payload (carico) dei dati e/o informazione
- CRC: è un controllo ciclico che permette la rivelazione di eventuali errori di trasmissione

Original Frame Ethernet

ETHERNET Protocol with 802.1q tagging

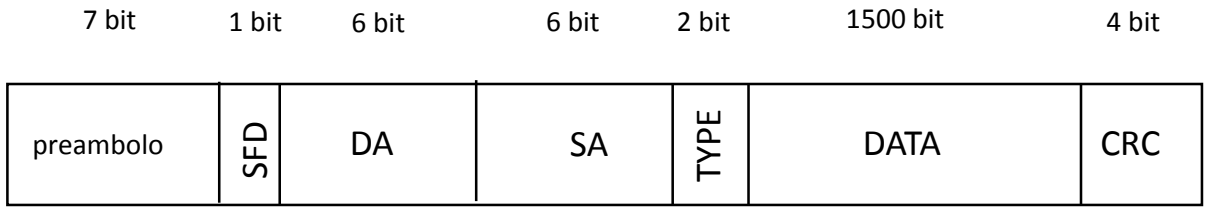
802.1q (protocollo standard): introduce il concetto di vlan (virtual LAN) permettendo a questi segmenti logici di rete di condividere lo stesso media fisico

- TPID: indica il tipo di ethertype che assume il valore 0x8100 indicando il nuovo frame 802.1q tagged
- TAG: contiene tre sotto-infomrazioni:
- user-priority: indica un livello di priorità della frame; l'utilizzo di questo campo è definito in 802.1p (definisce classi di servizio cos)
- CFI: indica se i MAC address della frame sono in forma canonica
- VLAN-ID: assume un valore numerico in un range sino a 4096 possibili segmenti logici di rete.



ETHERNET Protocol Q in Q tunneling

E’ una tecnica utilizzata per tunnellizzare un tag vlan in una secondo tag vlan all’interno di una frame Ethernet; questo permette di separare L2-VPN traffico utente all’interno di una rete services provider (ad esempio una Metro Ethernet).
E’ molto utilizzato anche in ambito datacenters multi-tenants,dove è prevista una quantità di vlans molto elevata.



Original Frame Ethernet

Tag Vlan Customers 802.1q

Tag Vlan Providers Q in Q tunneling

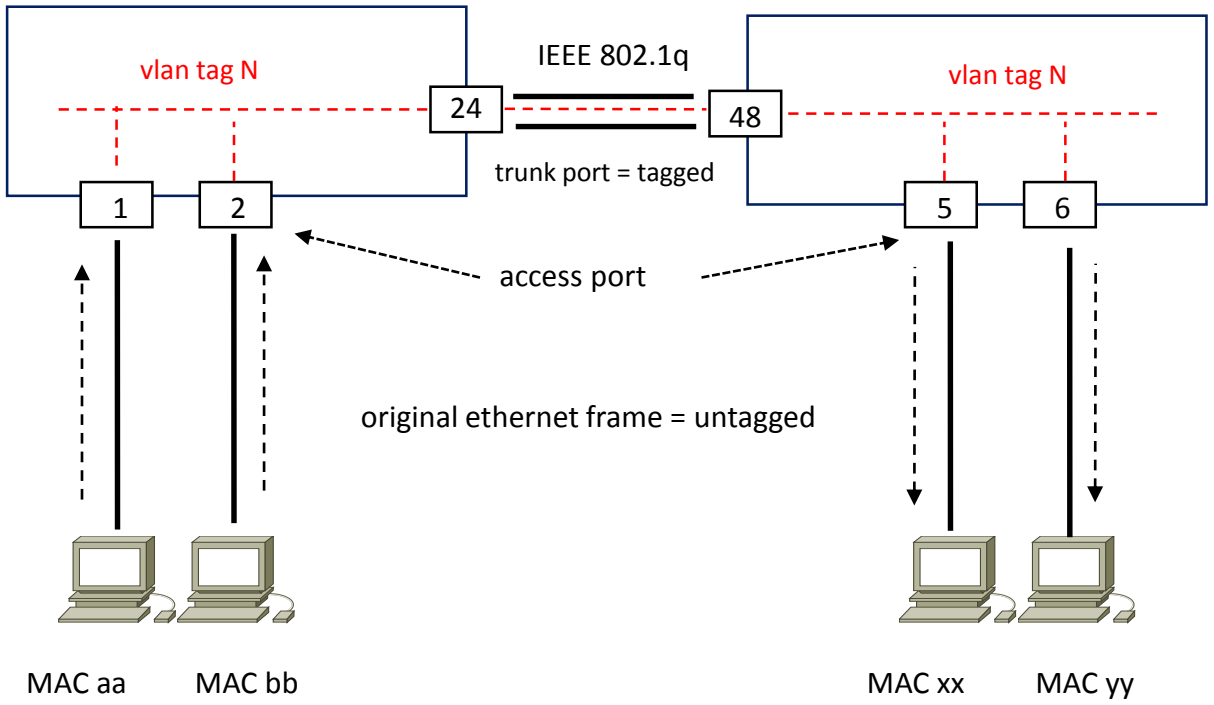
ETHERNET Protocol untagged vs tagged

Le porte in **access mode** sono di tipo **untagged;** Le porte in **trunk mode** sono di tipo **tagged**

Gli switch trasmettono e ricevono frame ethernt sulla base della loro MAC table address
Frame di tipo broadcast (FFFF.FFFF.FFFF) e unknown (sconosciuto il MAC di destinazione) vengono trasmesse su tutte le porte ad eccezione di quella dove hanno ricevuto la frame.
Cut-Through è una tecnica di forwardind della frame non appena lo switch riceve (e legge) il MAC di destinazione; bassa latenza, modalità sincrona (stesso bit rate tra porta sorgente e destinazione)
Store and Forward è una tecnica che permette la trasmissione di una frame interamente ricevuta e letta dallo switch; alta latenza ma con un maggior controllo via FCS.

switch A

MAC	PORTS
aa	1
bb	2
xx	24
yy	24



switch B

MAC	PORTS
xx	5
yy	6
aa	48
bb	48

VTP Vlan Trunking Protocol

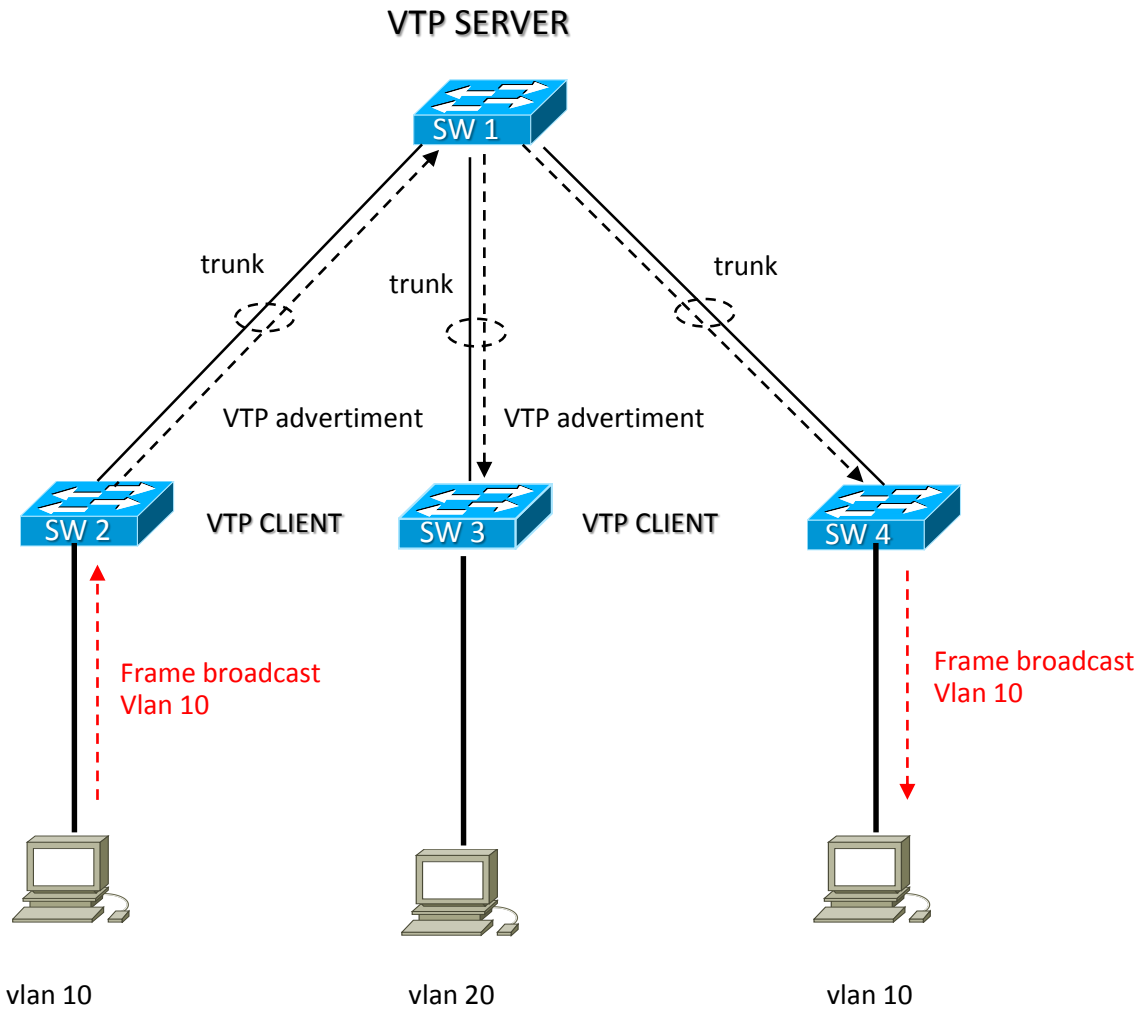
VTP è un protocollo che assicura uniformità e consistenza d vlans all'interno di un dominio LAN

Server Mode: può creare, modificare, eliminare vlans e decidere nuovi parametri di configurazione come ad esempio version e pruning per tutto il dominio VTP; VTP server annuncia e sincronizza tutto il vlans database a tutti gli switches client dello stesso dominio VTP attraverso gli advertisement ricevuti via trunk links (VTP server è configurato di default su switches cisco)

Client Mode: rappresentano altri switches settati in questo modo, appartenenti allo stesso dominio VTP del VTP server switch; questi switches non possono creare, modificare o eliminare nessun tipo di configurazione.

Trasparent Mode: rappresentano switches che non partecipano a nessun protocollo VTP (VTP off mode) e pertanto non annuncia e non sincronizza nessuna vlans del suo database; gli updates VTP sono ignorati e ritrasmessi in egress mode solo su trunks link

VTP Vlan Trunking Protocol



Spanning Tree Protocol

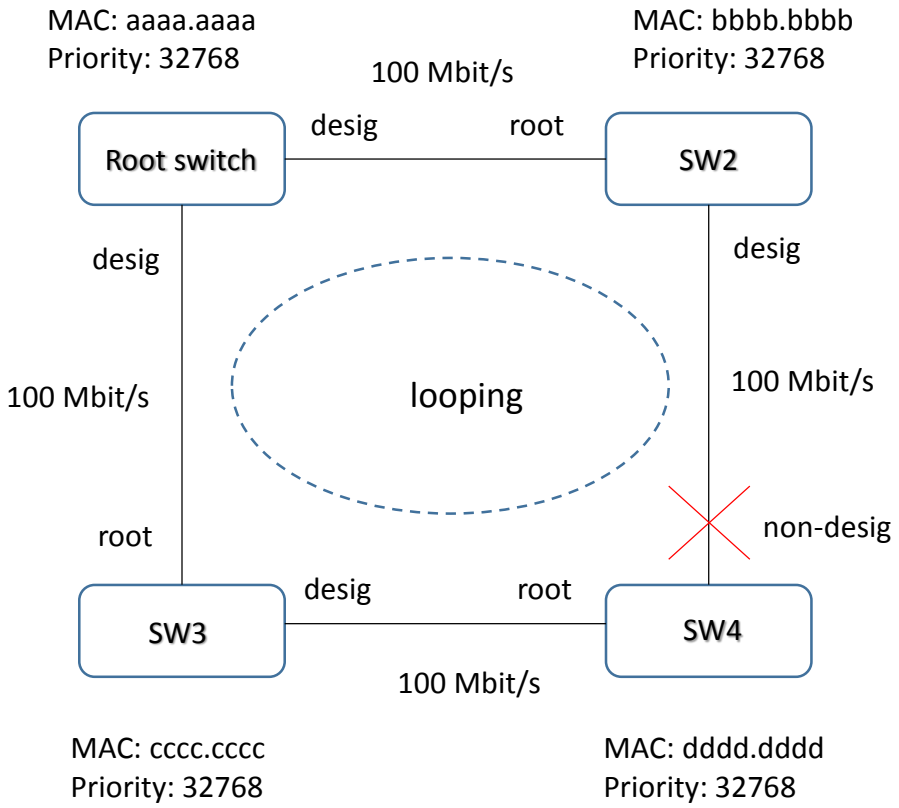
ARCHITETTURE CON STP

Port Role in STP 802.1d:

listening: la porta sta trasmettendo e ricevendo BPDU
learning: si occupa di costruire la sua tabella bridging STP free loop
blocking: non permette nessuna trasmissione di dati utente in egress alla porta
fowarding: permette la trasmissione e ricezione di dati utente
disable: non fa parte di nessuna azione STP; porta non attiva.

Port Status in STP 802.1d:

root: è la best port in forwarding status con direzione verso il root bridge
designated: in forwarding status port per ogni segmento di rete LAN
non-designated: in blocking status



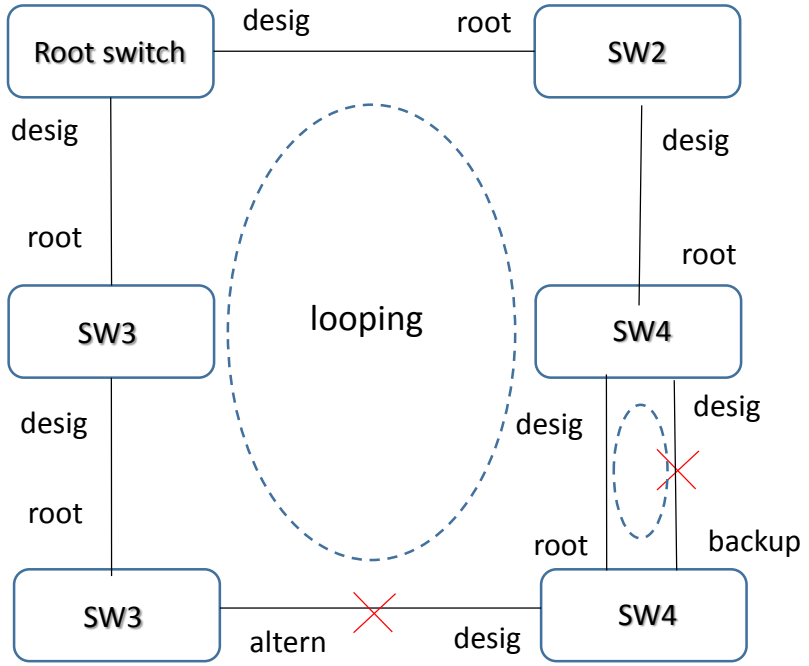
ARCHITETTURE CON STP

Port Role in RSTP 802.1w (usato per fast convergence: le porte dello switch scambiano un “handshake” quando transitano nello stato di forwarding)

root: è la best port in forwarding status con direzione verso il root bridge
designated: in forwarding status port per ogni segmento di rete LAN
alternate: in blocking status rappresenta il path alternativo verso il root bridge; questo path è differente da quello usato dalla best port
backup: in blocking status rappresenta il backup/ridondanza di un path verso un segmento LAN dove un altro switch è invece già connesso
disable: non necessariamente facente parte dello STP; è possibile manualmente disabilitare una porta.

Port Status in RSTP 802.1w:

discarding: nessun pacchetto è trasmesso dalla porta
learning: popolazione della tabella Mac-Address free loop
forwarding: operativa



ARCHITETTURE CON STP

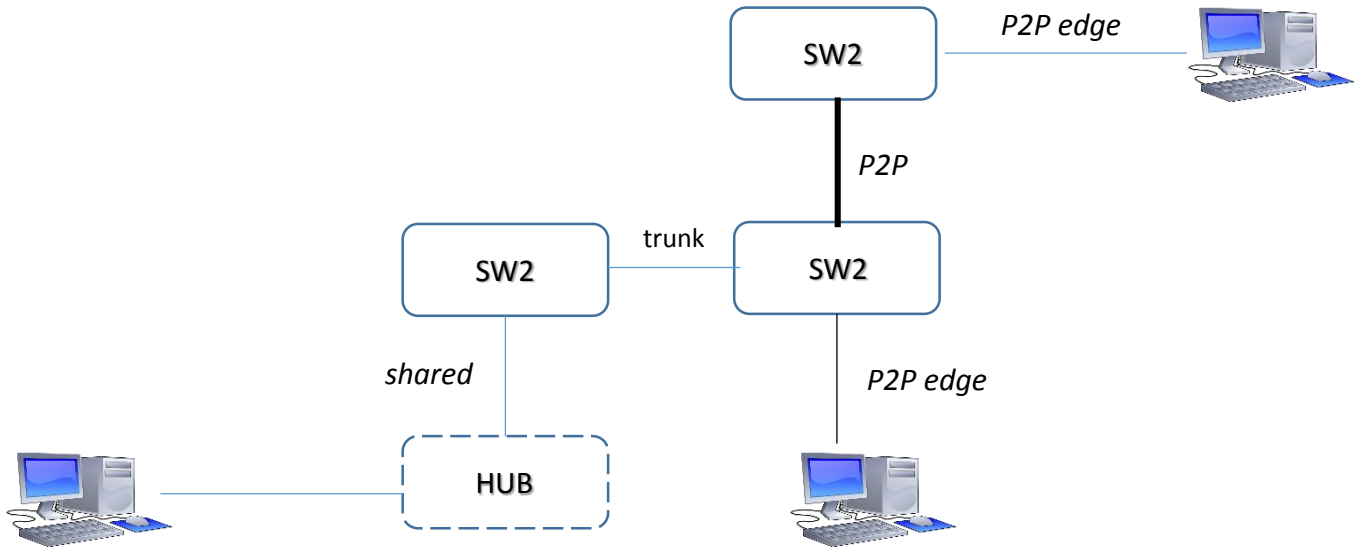
RSTP 802.1w Links Type to Forwarding

RSTP ha facoltà di categorizzare alcune porte in stato di forwarding senza attendere i timers del protocollo STP attraverso due variabili:

LINK TYPE: eseguito attraverso la configurazione della porta in half-duplex oppure full-duplex

full-duplex = link type point-to-point = connessione diretta tra due switches
half-duplex = link shared = connessione attraverso un terzo media dove multipli switches possono esistere

EDGE PORT: sono porte direttamente collegate tra uno switch ed un End-Point quali Host, Servers (ricordarsi che queste porte se ricevono BPDU perdono il loro ruolo/status di edge porte e diventano normali porte STP e, quindi, generano all'arrivo di BPDU un TCN



ARCHITETTURE CON STP

802.1s = MSTP = Multiple Spanning Tree = una istanza STP per un set o region di vlans.

Risulta molto utile nel caso di molte vlans in uso, dove invece di avere una istanza per singola vlans, è possibile ottenere differenti regioni associate a diversi gruppi di vlans (ad esempio una regione per un range di vlans 1-600 ed un'altra regione per un range di vlans 601 – 1000).

Supporta un numero ridotto di instanze di STP e risparmia CPU di uno switch rispetto a RSTP.

Proprietario Cisco = PVST+ = Per Vlan Spanning Tree plus = standard compliant 802.1d = una istanza STP per singola vlan

ARCHITETTURE CON STP

BPDU (Bridge Protocol Data Unit): uno switch trasmette un pacchetto BPDU usando un unico MAC-Address inerente la porta fisica come indirizzo sorgente e come indirizzo di destinazione un STP Multicast address 01:80:C2:00:00:00

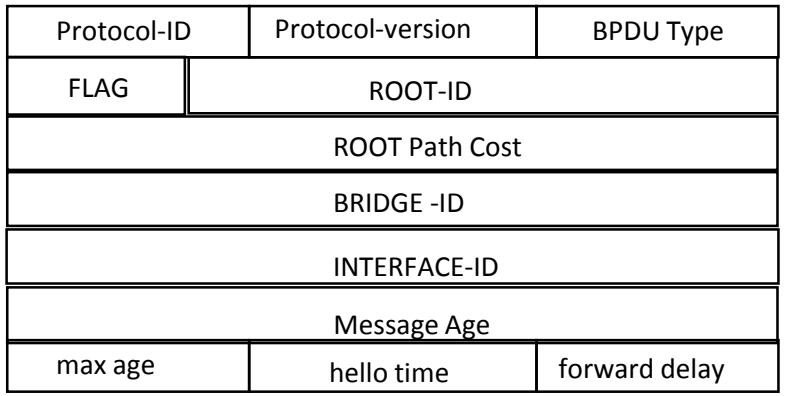
RSTP usa una estensione BPDU composta da:

CBPDU = Configuration BPDU
TCN = Topology Change Notification BPDU

Il processo di selezione basato su BPDU (Bridge Protocol Data Unit) è trasmesso tra switches per ogni porta fisica; gli switches usano quattro step di processo per stabilire e salvare una copia del best BPDU visto da ciascuna porta (quando una porta riceve un miglior BPDU, ferma la trasmissione delle proprie BPDU).

Dopo un intervallo di tempo (20 sec di default), se le BPDU smettono di arrivare, la porta fisica inizia a ritrasmettere le proprie BPDU. I quatto step di processo Best BPDU sono:

- Il più basso Bridge ID (BID)
- Il più basso Path Cost Root Bridge: dipende dalla throughput di bandwidth del link
- Il più basso Sender BID
- Il più basso port ID (esempio una porta fa0/1 è più bassa di una porta fa0/2)



BPDU Header

loop-guard e dove deve essere configurato

Loop Guard è una feature che protegge un link di collegamento tra switches a causare un loop; quindi previene una transazione da uno stato di blocking ad uno di forwarding, quando per cause di errore dovute a UDLD presente in uno specifico link.

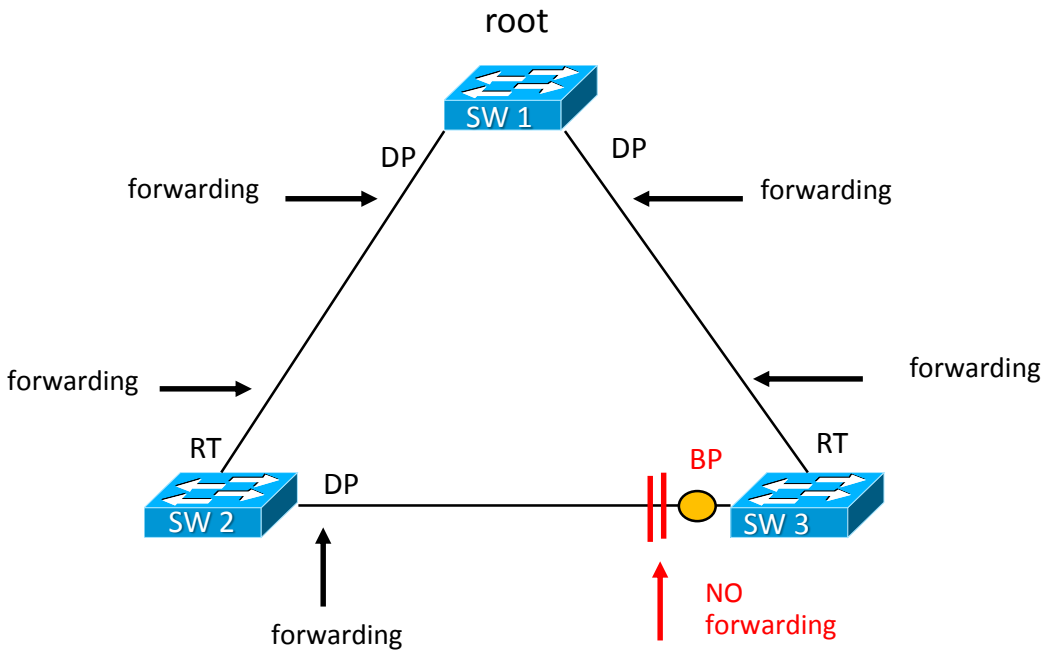
Lo swith 3 ha una porta in blocked state e, se ad esempio, non ricevesse più BPDU hello dallo switch 2 a causa di un ipotetico fault (ricordiamo che una porta bocking resta in ascolto delle BPDU), lo switch 3, pensando ad un nuovo processo STP transita in stato di forwarding la sua porta (per trasmettere le sue BPDU) ma essendo tutte le altre porte in stato di forwarding, si crea un loop

Se invece fosse presente loop-guard, la porta in stato blocking dello switch 3, in conseguenza di mancata ricezione di BPDU su quella porta, anziche transitare in uno stato di forwarding, transita in uno stato di loop-inconsistence che ha lo stesso valore e comportamento di una porta in blocking.

Di default loop-guard è disabilitato

interface gigabitethernet 1/10
spanning-tree loopguard

OR
spanning-tree loopguard default



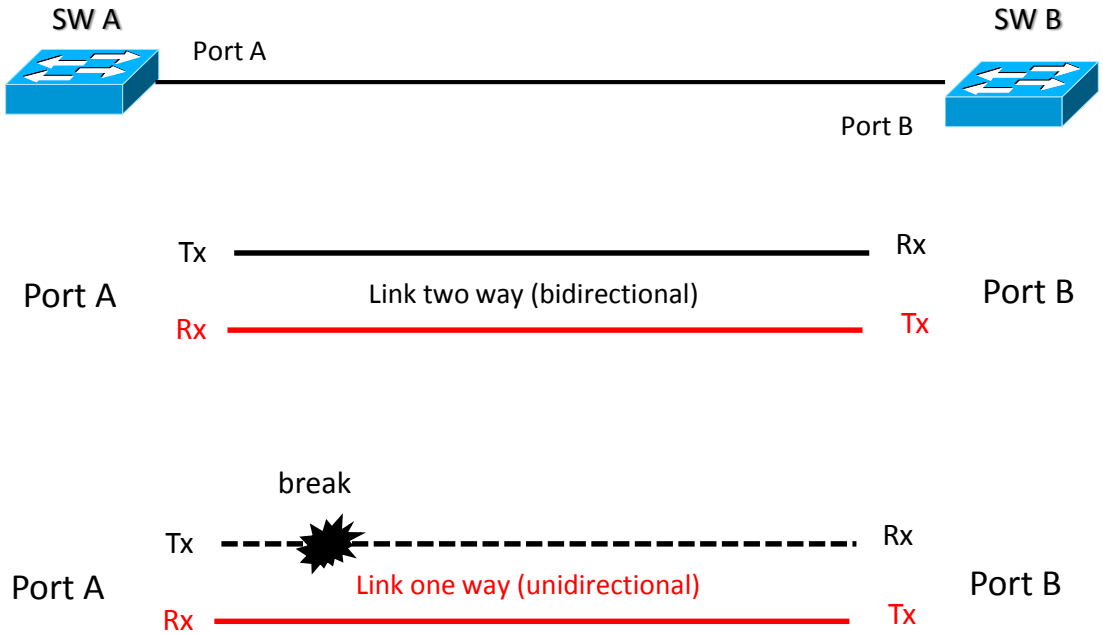
UDLD (Unidirectional Link Detection)

UDLD è un protocollo proprietario Cisco che pemette di prevenire problemi di loops tra una connessione in fibra ottica oppure in rame attraverso il riconoscimento di un link in one-way (unidirectional), disabilitando la porta in errore ed inviando un aler

UDLD Normal Mode: opera su una connessione di sola fibra ottica

UDLD Aggressive Mode: opera su connessioni sia in fibra ottica che rame

UDLD deve essere abilitato su base interfaccia o globalmente



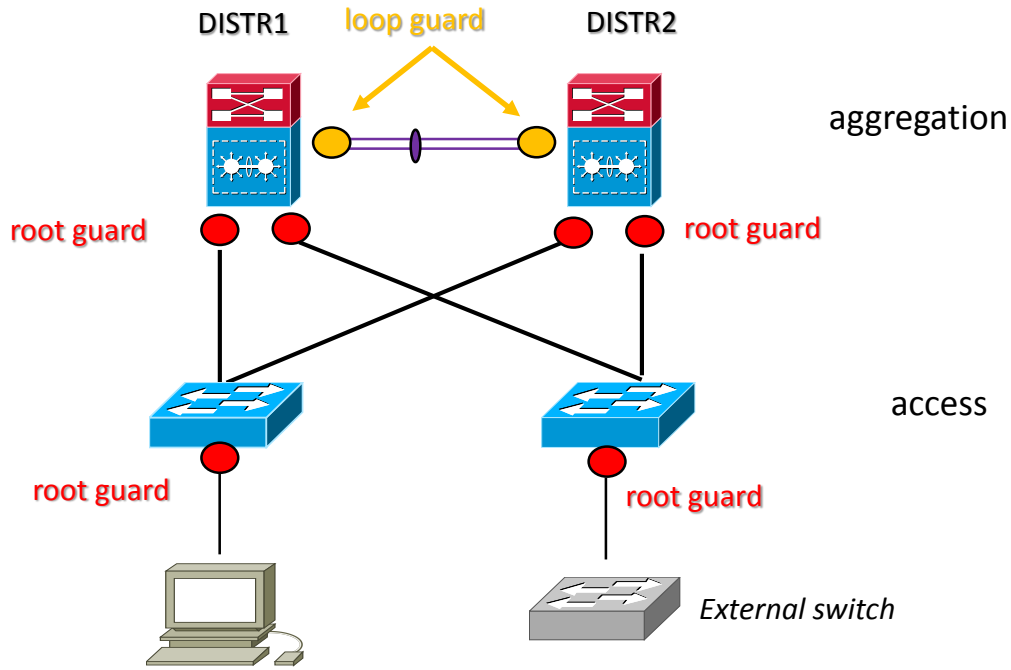
root-guard e dove deve essere configurato

Root Guard è una feature che previene una porta (differente dalla legittima root port) di uno switch (non il root-switch) a diventare root-port

Questa feature è raccomandabile a livello di aggregazione di un campus che vede la parte di accesso, evitando cosi che un eventuale errore di configurazione possa far ricalcolare un processo STP con una nuova elezione del root-bridge per una specifica vlan o istanza.

Anche a livello di accesso è buona norma configurare il root-guard per quelle porte di accesso alle quali sono collegati untrusted host che potrebbero introdurre malevoli traffici oppure, ad esempio, collegare external switch con un valore più basso di bridge ID rispetto a quello legittimo della rete, scatenando un ricalcolo dello STP con conseguenze distruttive per l'intera architettura.

interface gigabitethernet 1/10
spanning-tree guard root



bpdu-guard e dove deve essere configurato

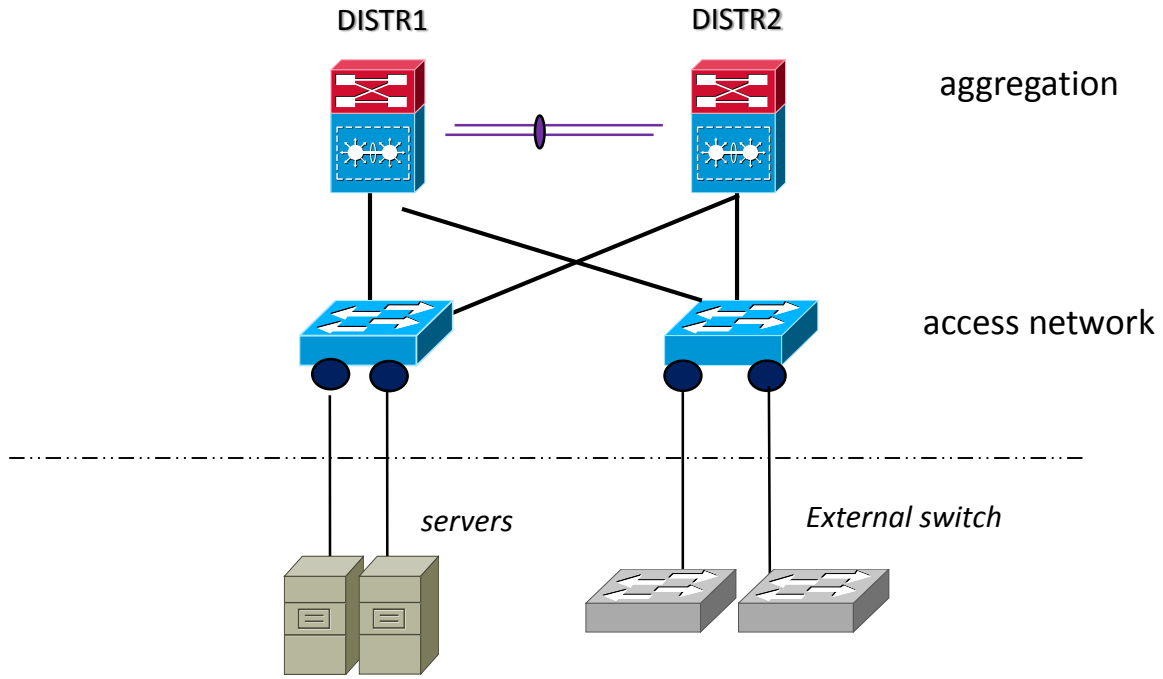
BPDU Guard è una feature che disabilita (shutdown) una porta di uno switch, non appena questa riceve una BPDU proveniente da un external switch o devices STP, ponendo la porta sulla quale era stato abilitato il bpdu-guard lo stato di err-disable.

In pratica si usa abbinare la configurazione bpdu guard con il **port-fast** per quelle connessioni verso servers per i quali è richiesta una rapida convergenza a trasmettere dati senza aspettare tempi (circa 50 sec) per cui una porta stablisce il suo stato di forwarding (bypassando di fatto gli stati intermedi di listening e learning);

In ogni caso considera che STP è sempre attivo e pertanto potrebbe portare in blocking queste porte; il BPDU guard previene da questa situazione.

BPDU guard + Port-fast garantiscono un dominio STP mantenendo la configurazione legittima e non permettendo a devices esterni al dominio di influenzarne il processo

interface gigabitethernet 1/10
spanning-tree bpdufilter enable



Architetture Layer 2

ARCHITETTURE ACCESS LEVEL

Access Level: è il livello edge di accesso per il collegamento di host quali PC, stampanti, IP-Phone, WIFI access-point, camera, etc.

Discovery: CDP and LLDP

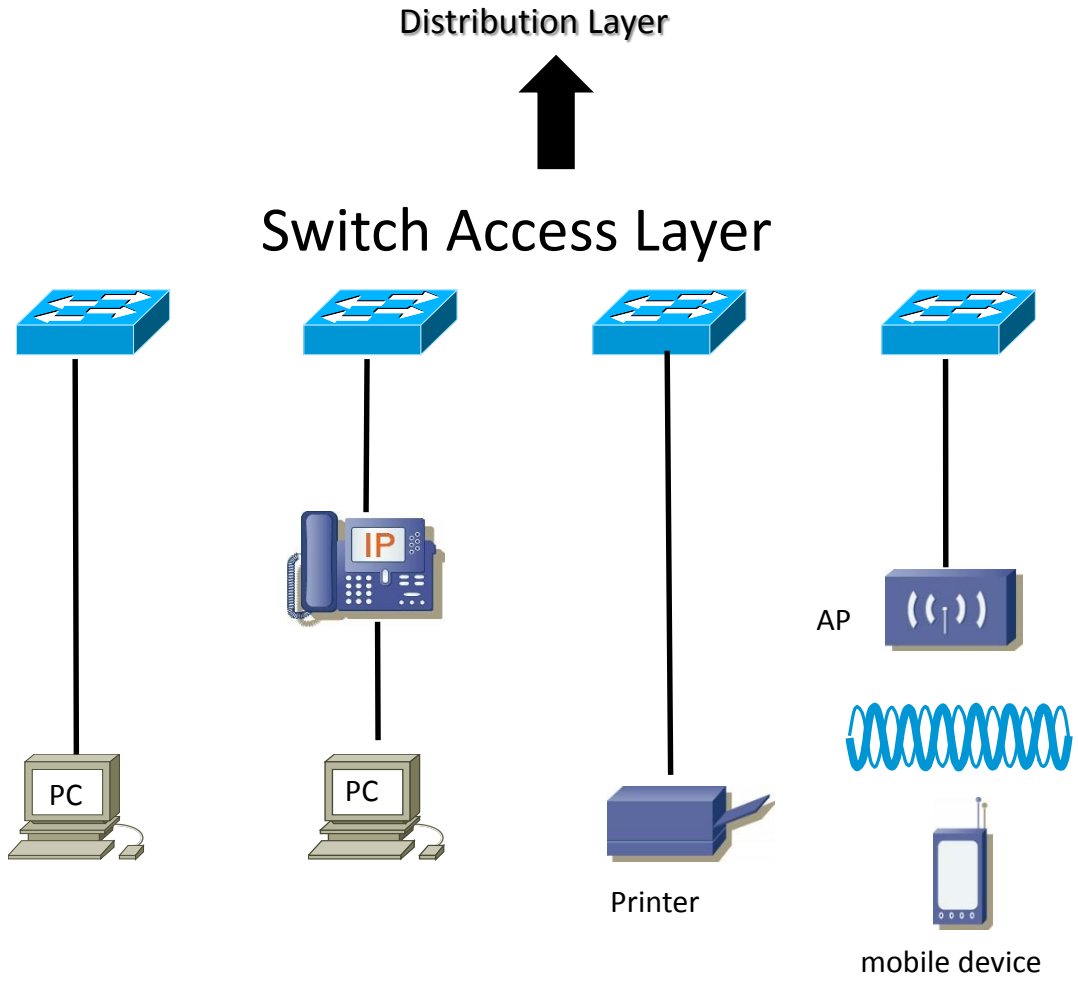
Security and Network Identity: 802.1x, port-security, DHCP snooping, IBNS (Identity Base Network Services) , IPSG (IP source-guard), Web-Auth, DAI (Dynamic ARP Inspection)

Application Recognition Services: QoS marking, policing, queueing, deep packet inspection NBAR

Network Control Service: STP, RPST, PVST+, VTP, LACP, PAgP, UDLD, port-fast, uplink-fast, backbone-fast, loop-guard, BPDU-guard, rot-guard, port-security, EIGRP, OSPF (access routing layer)

Physical Infrastructure Services: PoE (Power of Ethernet)

ARCHITETTURE ACCESS LEVEL



ARCHITETTURE DISTRIBUTION LEVEL

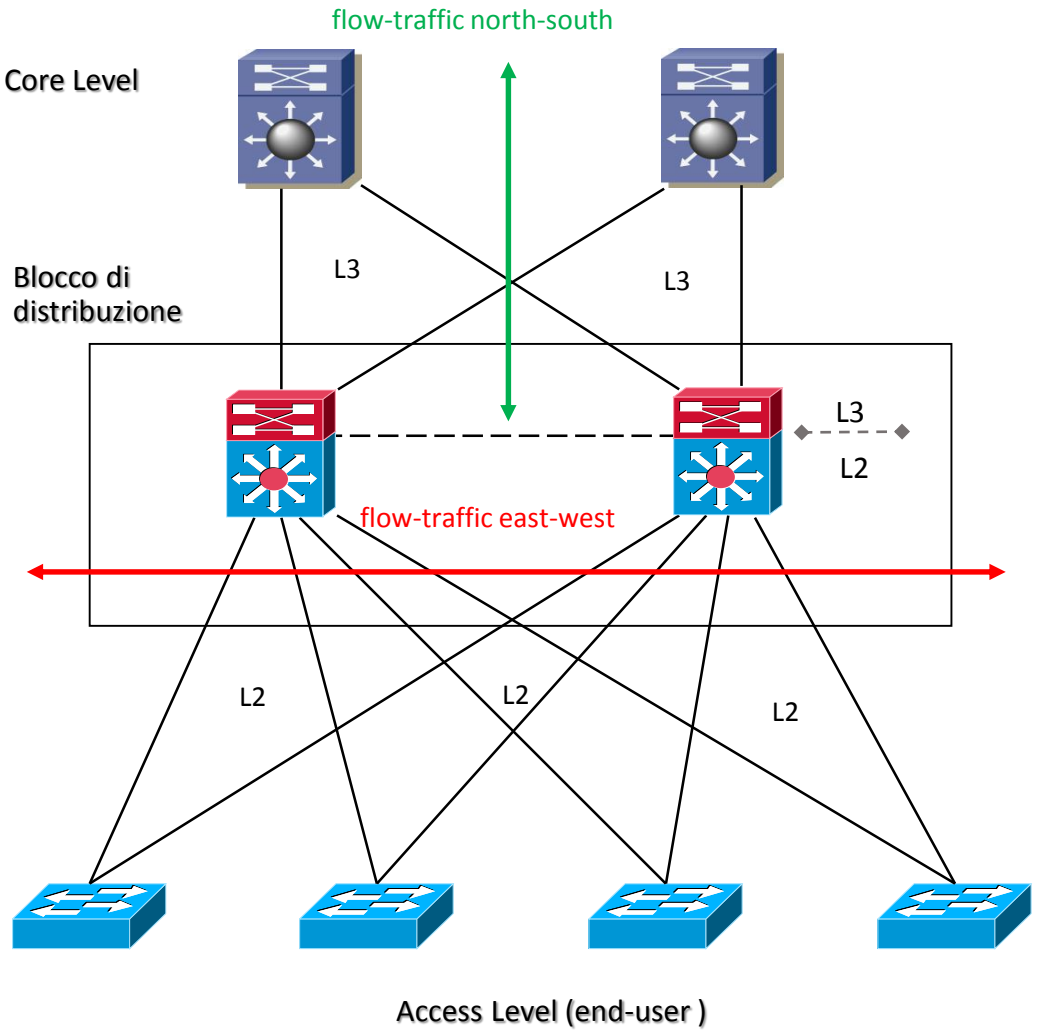
Distribution Level: è il livello che consente un punto di aggregazione tra il livello di accesso (end-user) ed il livello di core (external domain)

Provvede alla connettività e policy di servizio, all'interno di un singolo blocco di distribuzione, per flussi di traffico transitanti tra end-user node (east-west flow traffic)

Provvede alla connettività, policy di controllo ed un punto di demarcazione tra il blocco di distribuzione (campus di rete) ed il resto della rete per flussi di traffico diretti verso external network domain.

Partecipa a configurazioni di routing per scalabilità e performance di convergenza tra il livello di distribuzione ed il livello di core

ARCHITETTURE DISTRIBUTION LEVEL



ARCHITETTURE CORE LEVEL

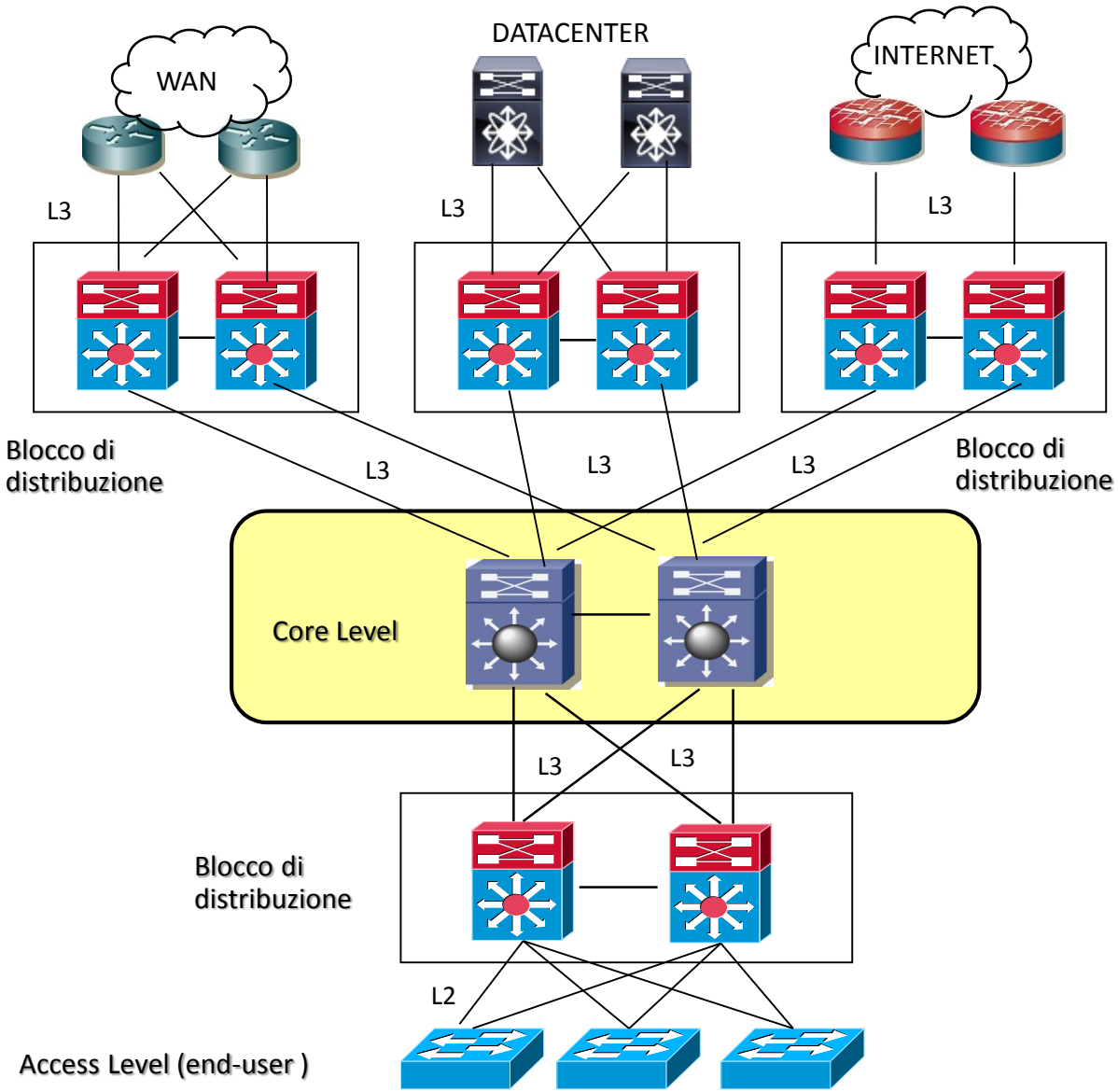
Core Level: è il livello che deve garantire alta affidabilità, ridondanza, resilienza, security, non-stop service capability

Consente un livello di aggregazione tra differenti blocchi di distribuzione

Consente l'interoperabilità tra differenti ed external network domain (Internet, WAN, DataCenters) con il livello di accesso (End-User)

Consente immediato data-flow recovery in caso di fault di qualsiasi componente della rete

ARCHITETTURE CORE LEVEL



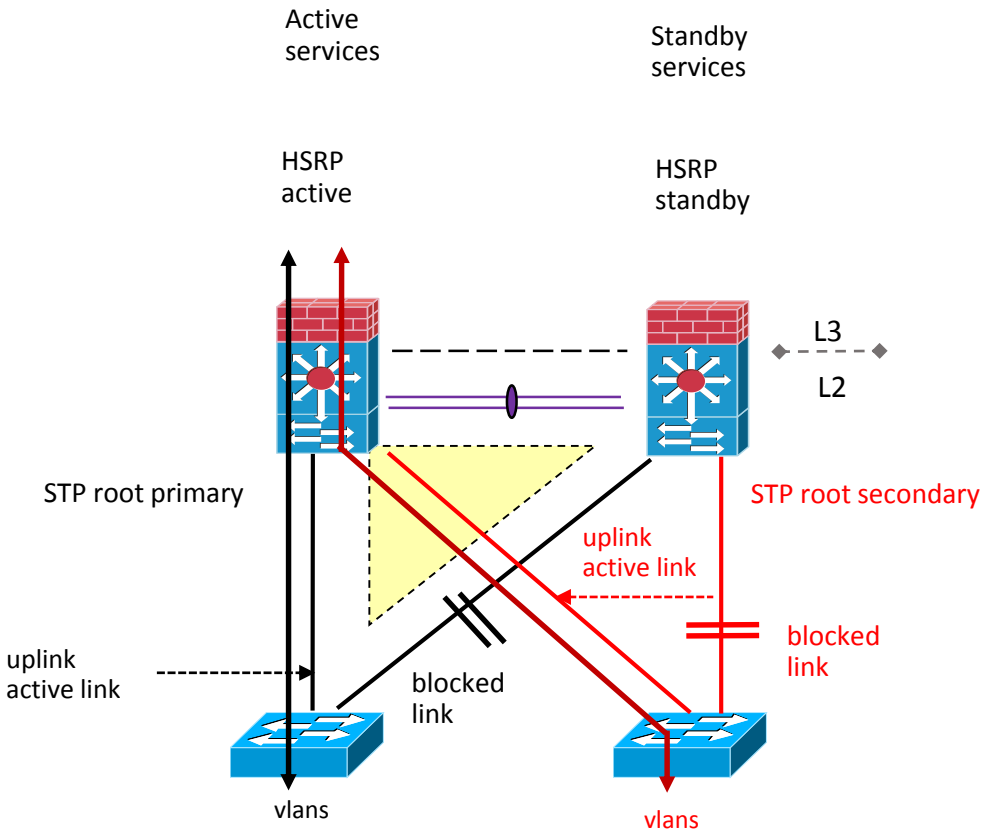
Looped Switching Architectures Design Cisco Models

Layer 2 Looped : tutte le vlans **sono** estese a livello di aggregazion edoffre particolari benefici per servizi di tipo statefull (significa la capacità di memorizzare dati per essere utilizzati a scopi specifici come quelli di FWSM o SLB); il livello 3 (routing) è performato dal livello di aggregazione in alto

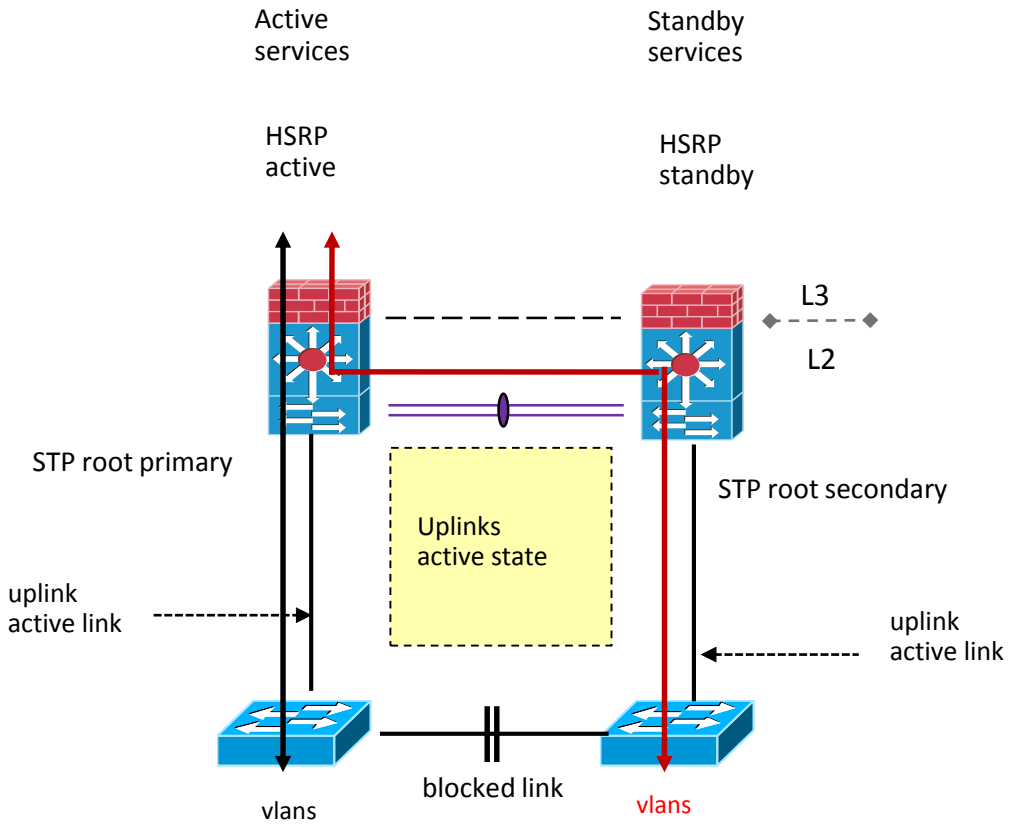
Looped Triangle : provvede ad una ridondanza di tipo active standby tra due peers di aggregazione (Distribution Switch), garantendo HA tramite protocolli HSRP o VRRP e, per effetto dello spanning tree, abbiamo un link in stato active e l'altro in stato blocked (o standby) tra il livello di accesso ed il livello di aggregazione allineando di fatto tutti i componenti e protocolli di rete performati a livello aggregation in stato active solo su uno dei due peers di aggregazione. Il throughput di banda a disposizione è pari al 50% del valore effettivo utilizzabile; non è presente nessun collegamento tra gli switch di accesso (access inter-switch link)

Looped Square : rispetto al modello di cui sopra, la differenza consiste nel permettere collegamento tra gli switch di accesso (access inter-switch link) in stato blocked; permette un solo collegamento tra lo switch di accesso e lo switch di aggregazione.

Looped Switching Architectures Design Cisco Models



Looped Triangle



Looped Square

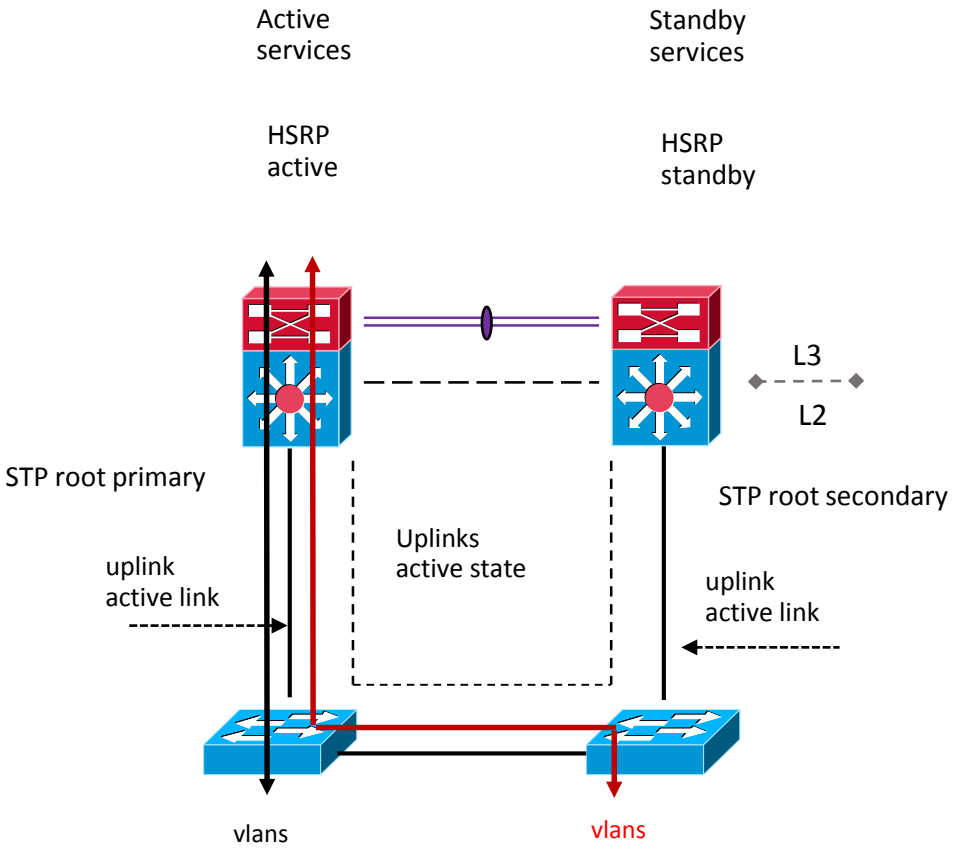
Looped-FREE Switching Architectures Design Cisco Models

Layer 2 Looped Free : le vlans **non sono** estese a livello di aggregazione; il livello 3 (routing) è performato dal livello di aggregazione in su; lo spanning-tree protocol (STP) in questo scenario è in uno stato di background (non è assente) in caso di fault a livello fisico (cabling); Il throughput di banda utilizzato è del 100%.

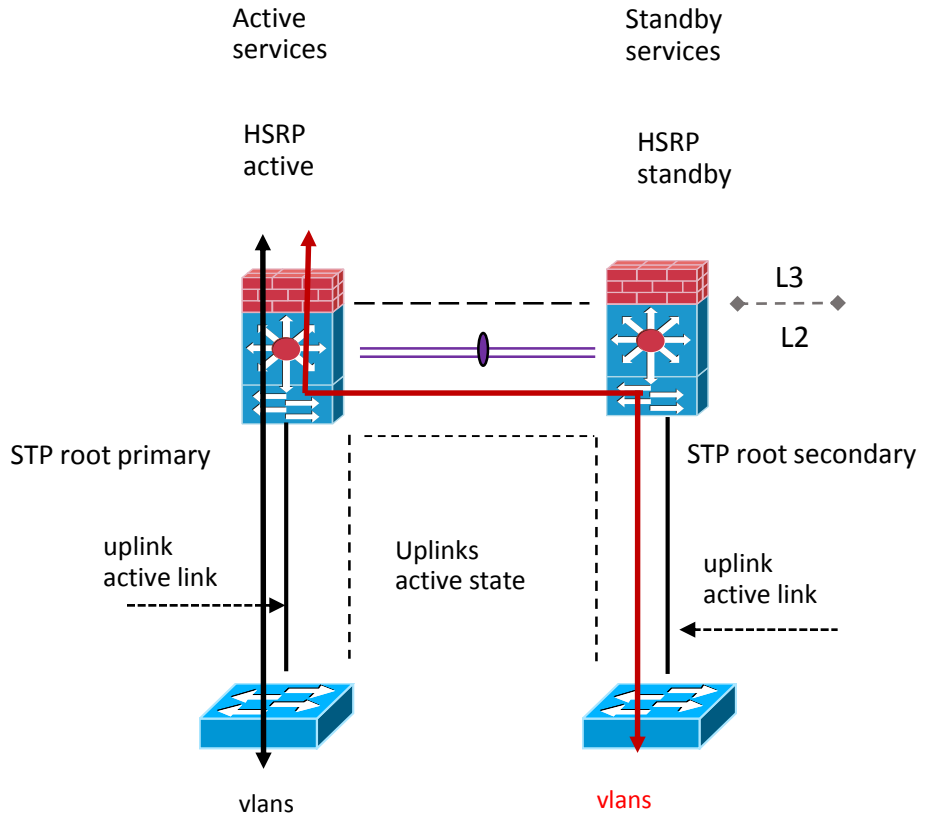
Loop-Free type U : in questo modello le vlans transitano tra gli switch di accesso avendo un collegamento tra loro (inter-switch link) e terminano per L3 SVI gateway tra i due peers di distribuzione (non tutti i modular services sono supportati da questo modello): lo svantaggio prevede un black-holing traffic a causa di un eventuale fault di un singolo link perchè le vlans non sono estese a livello di switch di aggregazione.

Loop-Free Inverted U : rispetto al modello di cui sopra, la differenza consiste nel permettere la distribuzione delle vlans a livello di aggregazione e non attraverso gli switch di accesso; tutti i modular services supportano questo modello

Looped-FREE Switching Architectures Design Cisco Models



Loop-Free type U



Loop-Free Inverted U

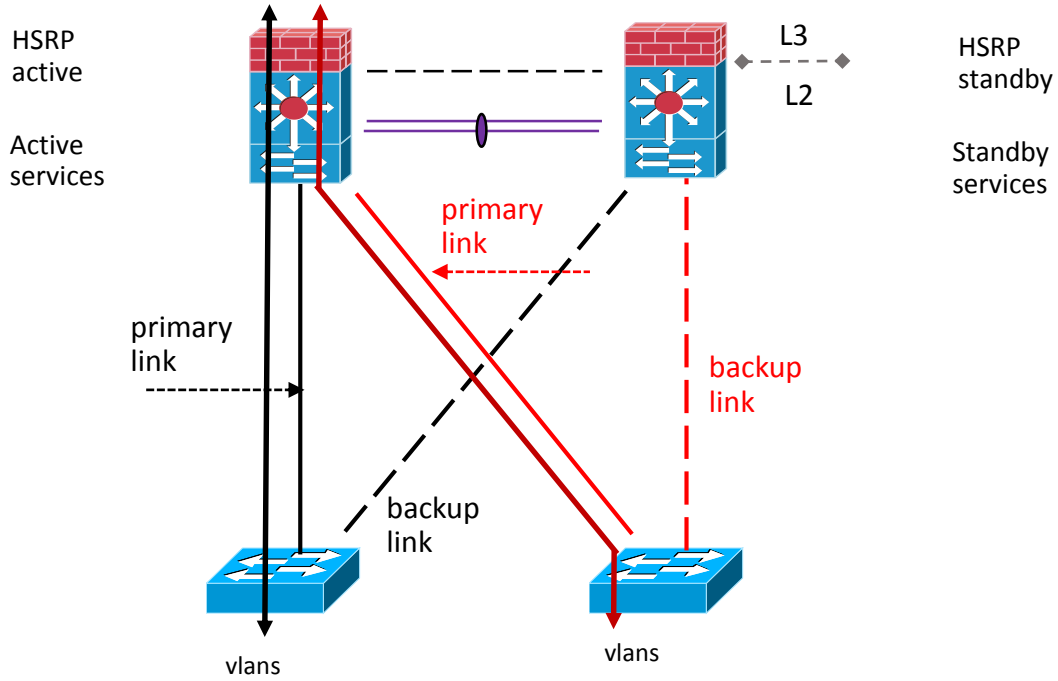
Flex-Link Switching Architectures Design Cisco Models

Flexlink : ogni switch di accesso ha due link verso gli switch di aggregazione con una configurazione di tipo Flex-Link

Flex-link disabilità il protocollo STP (No BPDU propagation) rendendo non conforme il modello di ricalcolo new-path in caso di fault di un link a livello fisico; in ogni caso il failover tra i due links è all'interno di 1 o 2 secondi

Gli switch di distribuzione non sono consapevoli della configurazione Flex-Link

La configurazione prevede che a livello di link primario venga inserito questo comando: switchport backup *interface interface-id)*



Ottimizzazioni Layer 2

STAR Switching Architectures Design Cisco Models

Star : Utlizzata quando un sistema VSS è impiegato insieme ad una configurazione MEC (MultiChassis Etherchannel)

Questa configurazione logicamente significa un solo switch logico di aggregazione avente un solo link MEC in trunk verso lo switch di accesso

Tre switch di accesso sono quindi rappresentati come tre raggi ciascuno collegati in modo indipendente al proprio hub di centro-stella rappresentato dalla coppia di switch VSS.

VSS Virtual Switching System Architectures Design Cisco Models

Un sistema VSS opera via SSO (Stateful Switch Over) tra peers attraverso le Supervisor Engine active e standby ospitate nei rispettivi chassis

VSS Supervisor Engine active controlla le funzionalità layer 2 (switching) and layer 3 (routing) per entrambi gli chassis (single control-plane, single management point, dual active forwarding planes)

Il piano di forwarding del traffico è performato da entrambi i peers VSS

In caso di fault della Supervisor Engine active, quella in stato standby assume il suo ruolo(switchover)

VSL (Virtual Switch Link) è un collegamento tra i peers VSS per lo scambio di messaggi di controllo processati dalla Supervisor Engine active ma trasmessi e ricevuti su interface presenti nel peer VSS standby

VSS opera in un contesto di Spanning Tree Protocol; il VSS standby redirige le BPDU STP via VSL verso il peer active

Il STP bridge ID è un valore comune ed è calcolato sul MAC address chassis; non cambia a seguito di uno switchover peers.

MEC Multi-Chassis Etherchannel Architectures Design Cisco Models

Un MEC è un collegamento Multihassis Etherchannel tra un nodo di accesso verso entrambi i peers VSS active e standby

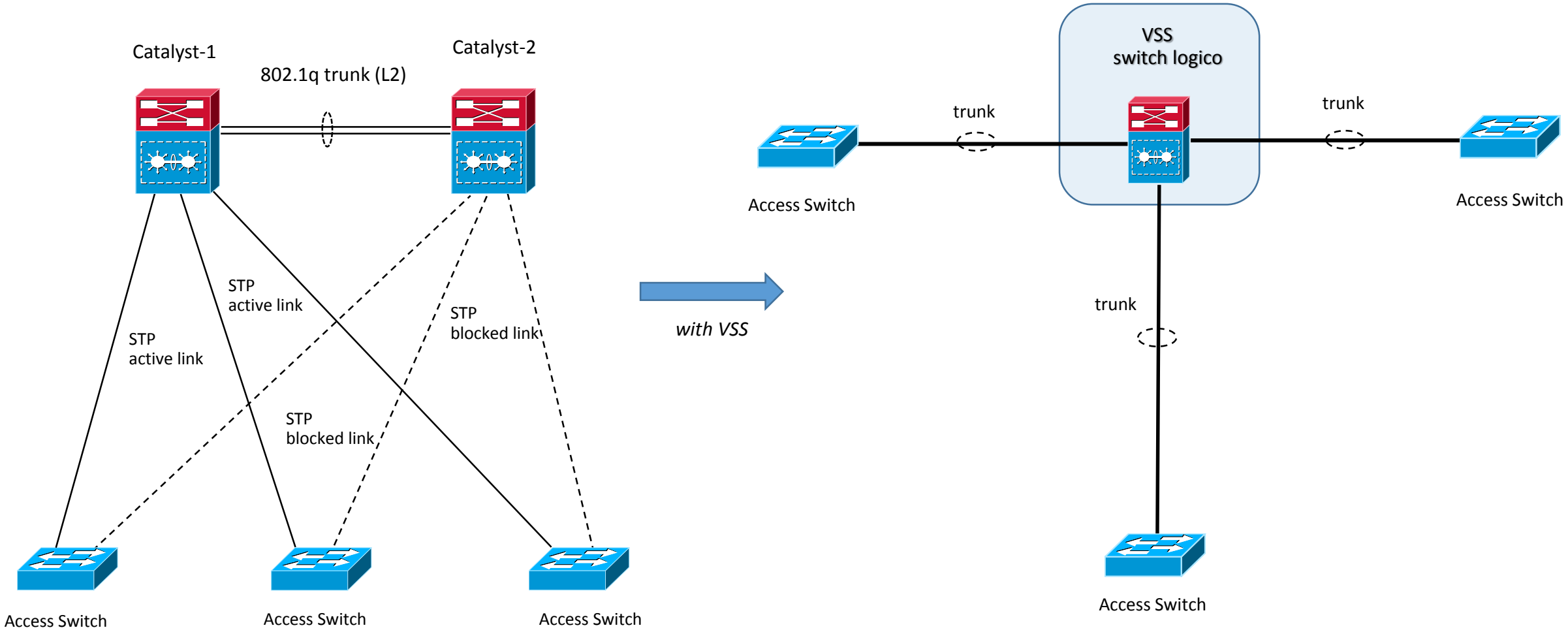
Un VSS MEC può collegare qualsiasi elemento di rete che supporti etherchannel (quale host, server, switch, router)

Un VSS MEC supporta protocolli quali LACP (Link Aggregation Protocol) oppure PAgP (Port Aggregation Protocol)

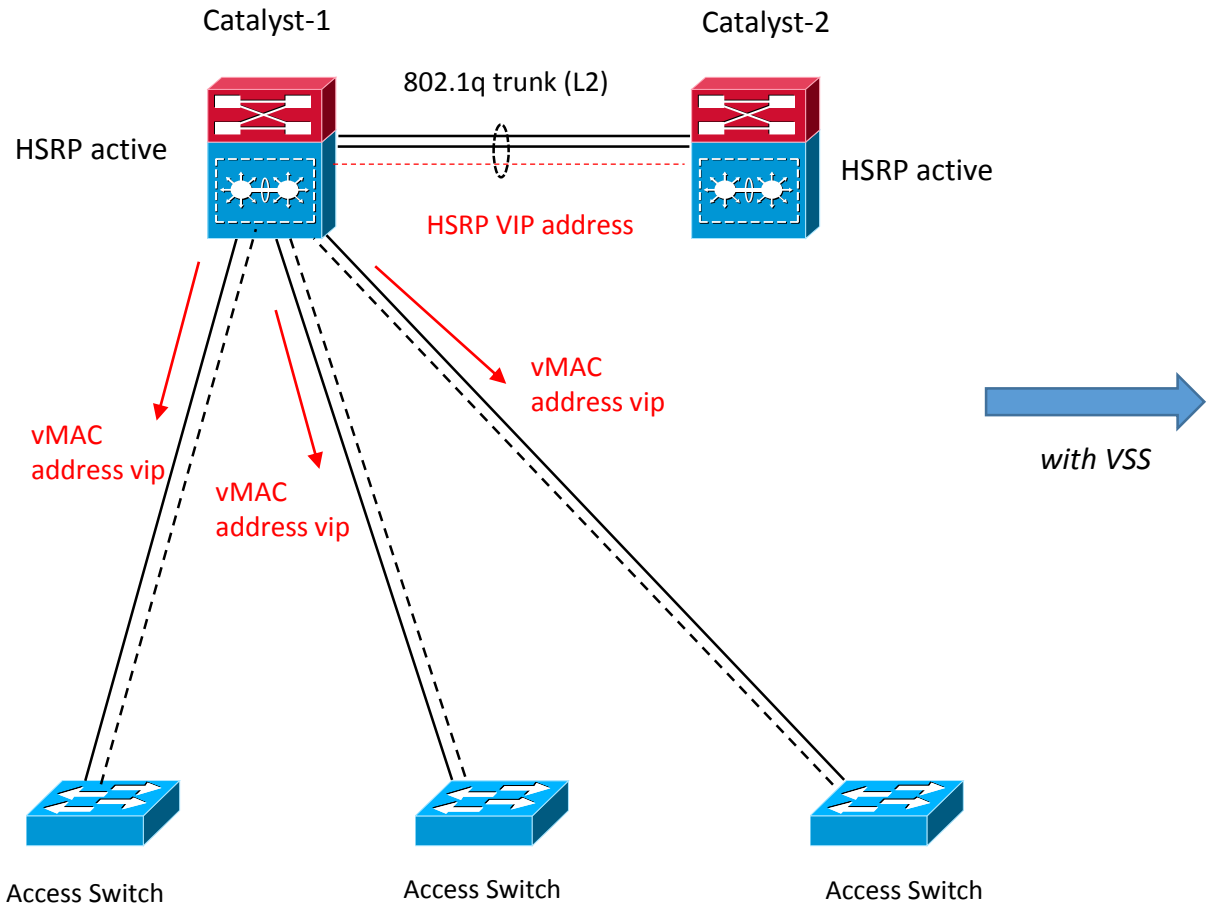
Il MSFC (Multilayer Switch Feature Card) presente nella Supervisor Engine active lavora a livello 3 (routing) ed entrambi i peers VSS performano il forwarding del traffico sulle rispettive interface sia in ingresso che in uscita

In genere un traffico in ingresso è trasmesso (forwarding) da una interfaccia di uscita appartenente allo stesso chassis per ridurre cosi la quantità di dati transitante via VSL.

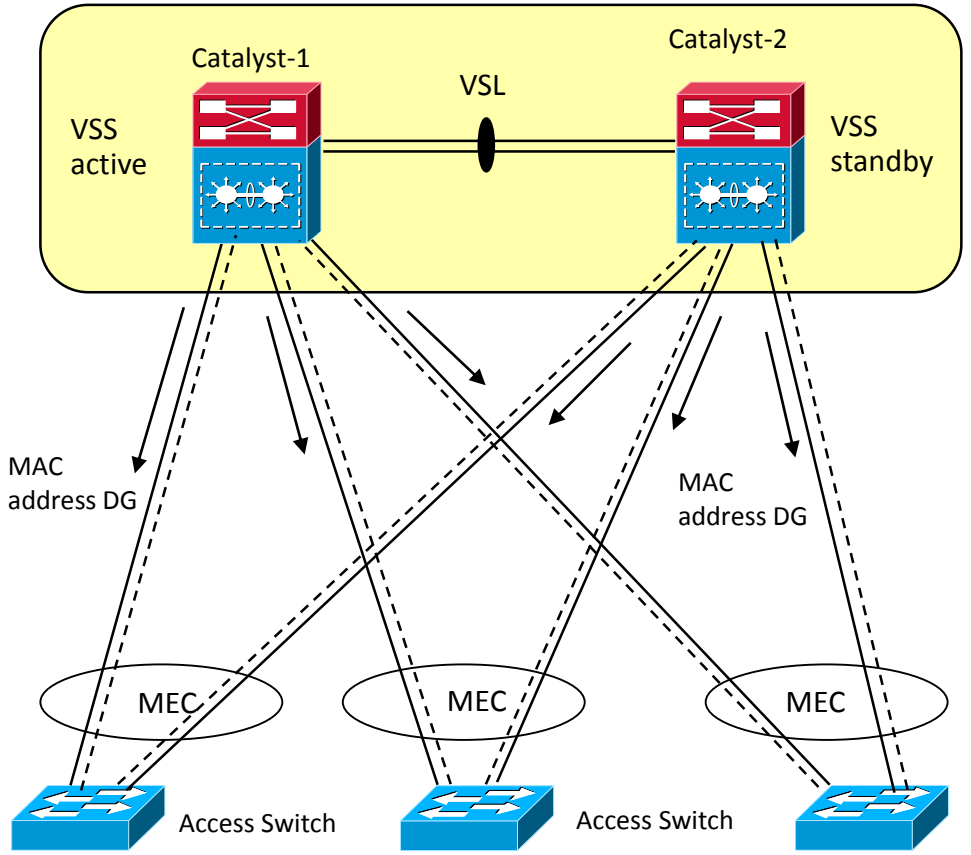
STAR Switching Architectures Design Cisco Models



STAR Switching Architectures Design Cisco Models



with VSS

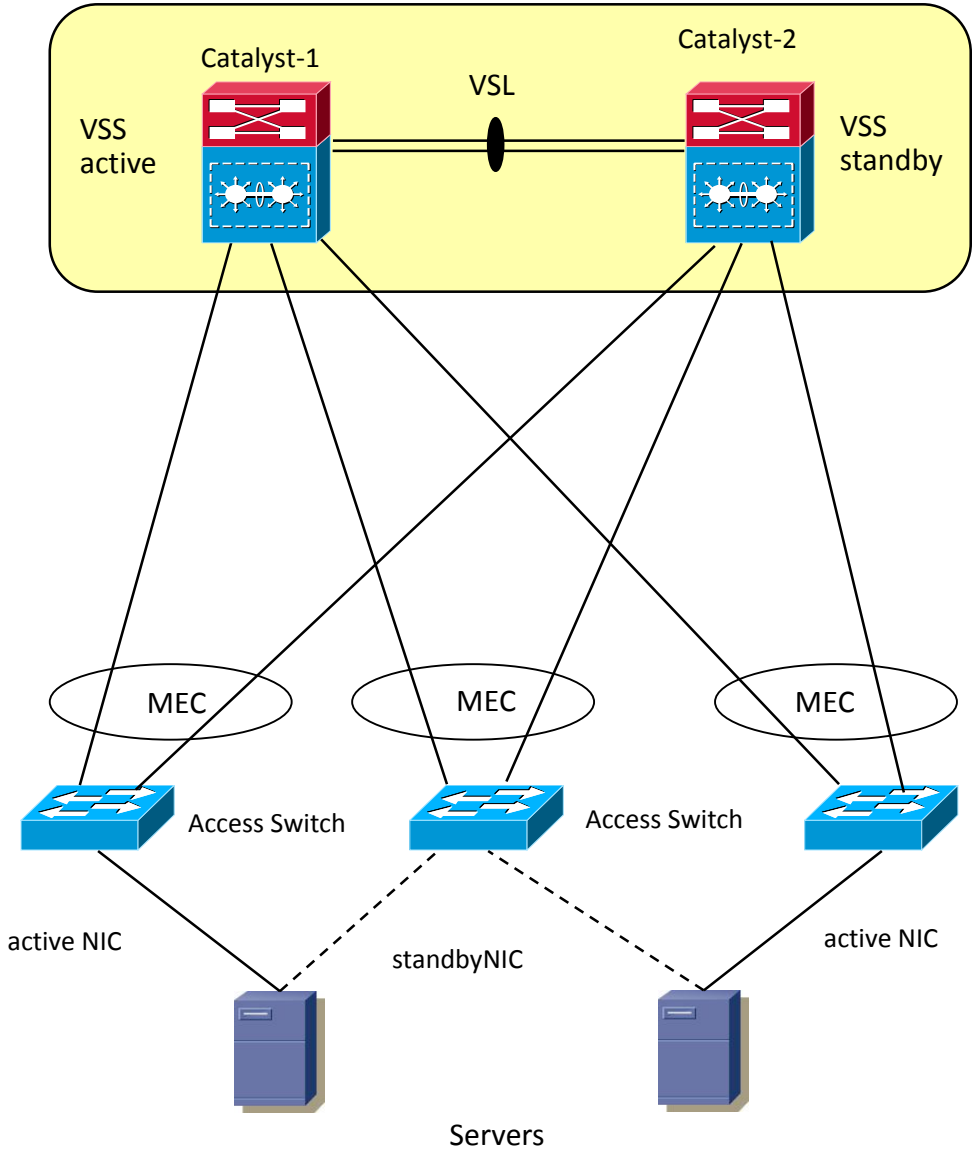


50% di utilizzo della rete layer 2

100% di utilizzo della rete layer 2

MEC Multi-Chassis Etherchannel Architectures Design Cisco Models

Multichassis Ethernet Channel



Stackwise Virtual System Architectures Design Cisco Models

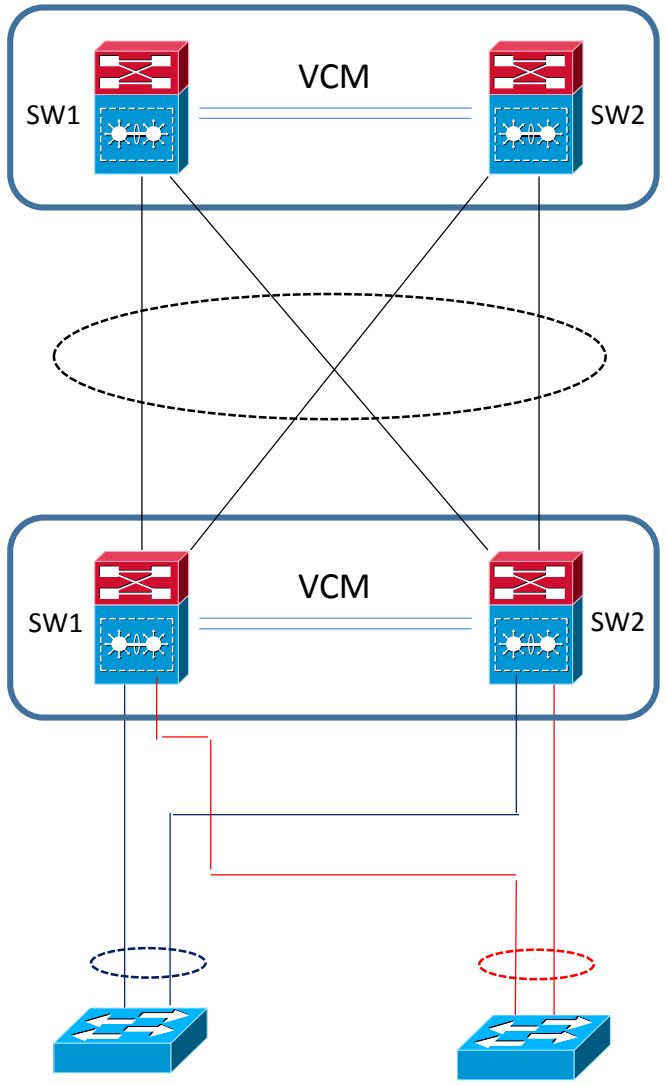
Un sistema “stackwise virtual” cisco opera in modo che due (o più) switch catalyst sono unificati all’interno di un’unico sistema di switching con un solo piano di controllo (control-plane) ed un piano di management (gestione), un piano di forwarding distribuito (significa che ogni switch facente parte dello stackwise è capace di trasmettere traffico attraverso le sue porte locali senza coinvolgere quelle di altri switch membri; un pacchetto entrante in una determinate porta locale, comunque, è soggetto ad una trasmissione su differente porta distribuità su tutti gli switch membri sino a considerare lo switch egress per quella specifica destinazione)

Attraverso un meccanismo di elezione un membro dello stack viene eletto master e gli altri standby (lo switch master è responsabile del piano di controllo, di forwarding e di management.

Gli switch membri dello stack comunicano tra loro attraverso un virtual software module chiamato VCM (Virtual Communication Manager) via links.

Stackwise Virtual System Architectures Design Cisco Models

Domain 10

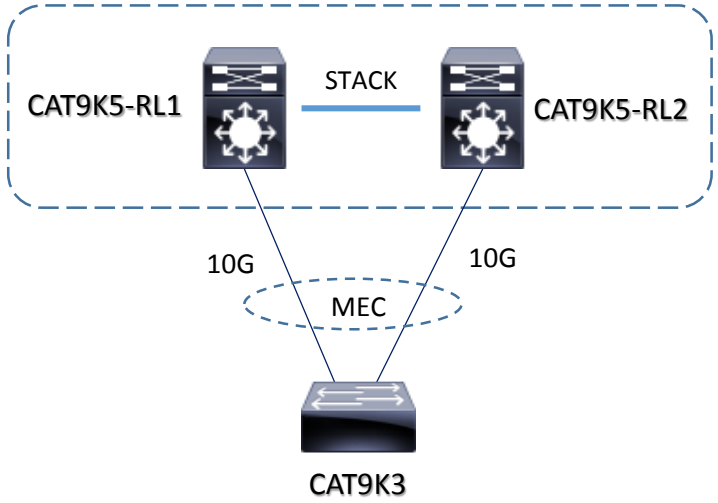


CORE stackwise level

Domain 20

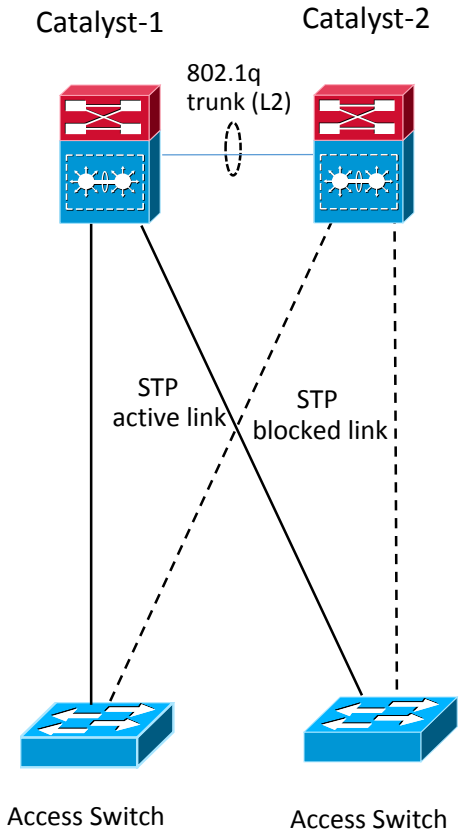
DISTRIBUTION stackwise level

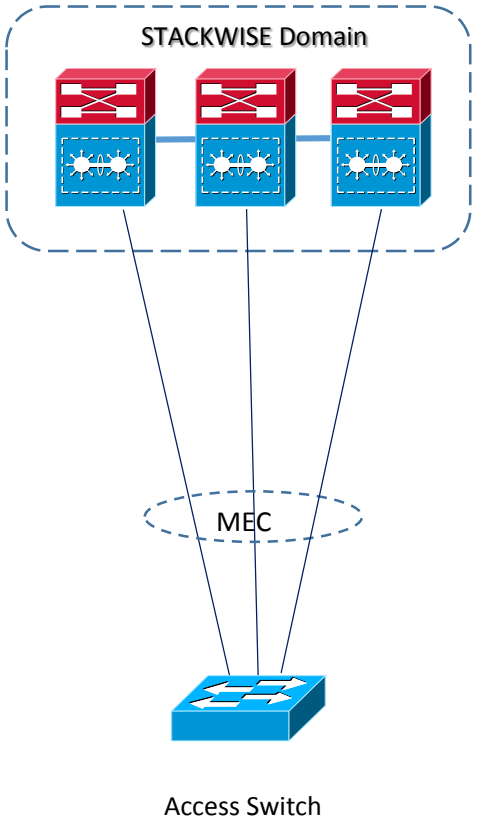
ACCESS level

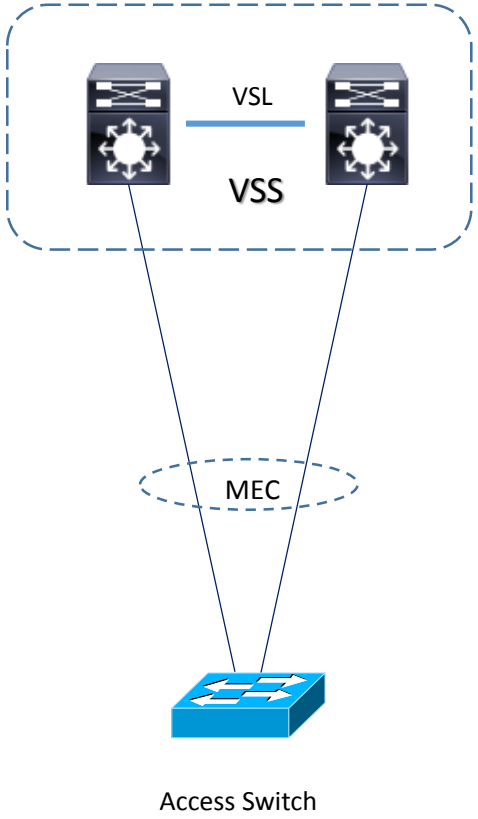


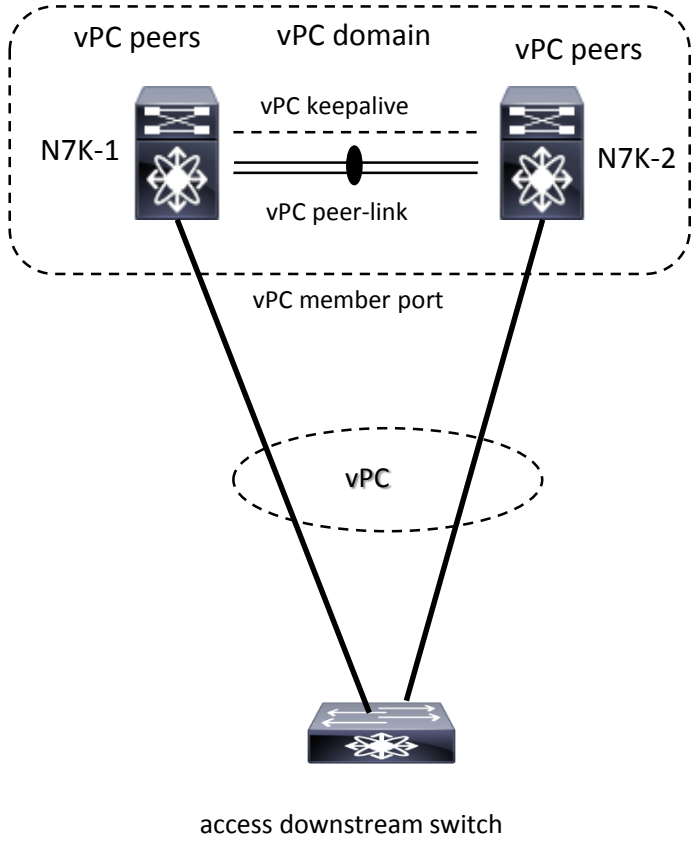
configurazione stackwise catalyst 9K cisco

Comparazione STP, StackWise / VSS / VPC









STP domain

STACKWISE domain

VSS domain

vPC domain

vPC Architectures Design Cisco Models

Con vPC, ogni Nexus mantiene il proprio control-plane ed il proprio management:

- vPC IEEE 802.3ad: è un port-channel tra un devices in downstream e due Nexus Devices con stessa release software
- vPC peer: è uno dei due devices (or VDC) che formano la coppia di Nexus in aggregazione
- vPC member port: è una interfaccia che appartiene ad uno specific vPC port-channel di uno dei due vPC peers
- vPC domain: un unico identificativo per coppia di Nexus (ogni Nexus switch or VDC supporta un solo dominio)
- vPC peer-link: usato per la sincronizzazione dei rispettivi status switches e per il forward del traffic o tra i due peers
- vPC peer-keepalive: usato per la verifica heartbeat tra I due switches vPC peers (in modo esplicito per verificare failure dei peer-link e peer-keepalive)
- CSF (Cisco Fabric Services): è automaticamente abilitato in un vPC e rappresenta la capacità di sincrinizzare lo stato e la configurazione tra i due vPC peers

NOTA CISCO: quando si configura un vPC domain tra i due vPC peers, questi generano un condiviso MAC address che viene usato come un logico switch bridge ID in SpanningTree Protocol.

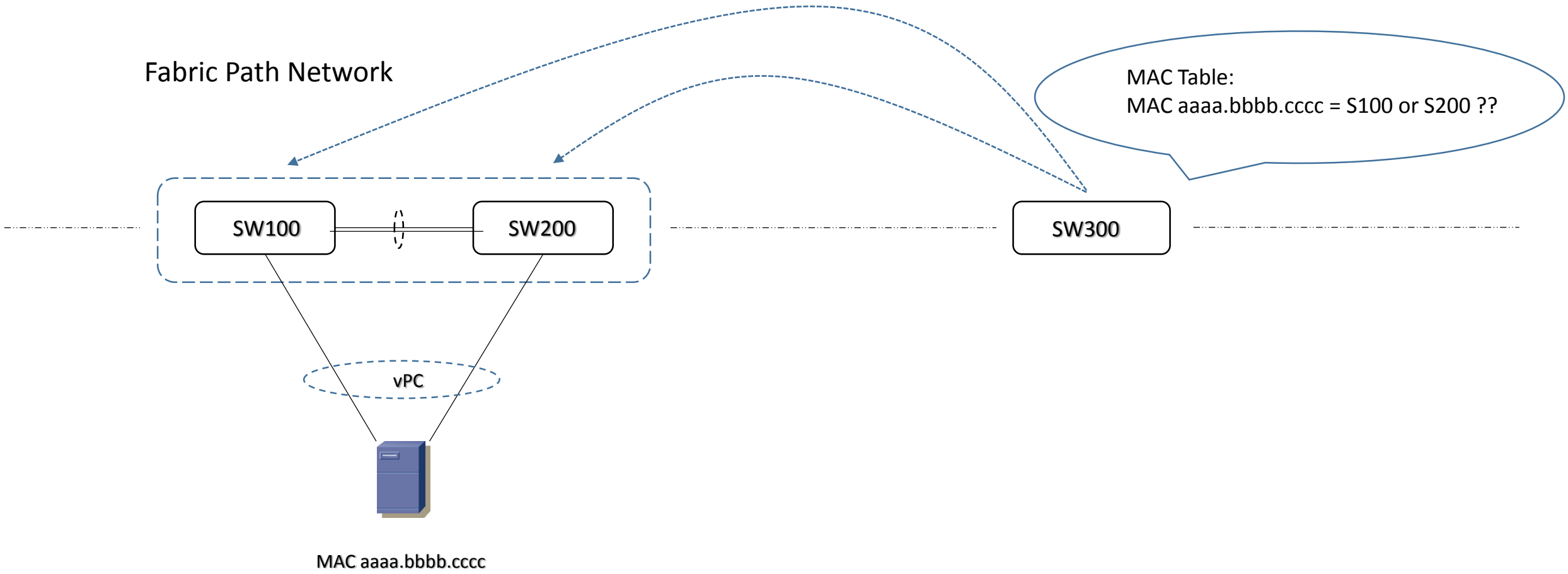
All'interno di un vPC domain ad ogni peer è assegnato un ruolo: primario e secondario (di default lo switch con il più basso MAC address diventa il primario; è un valore comunque che l'operatore può cambiare)

La comunicazione per il control-plane avviene attraverso il peer-link tra i due peers.

Esiste un meccanismo di loop-avoidance split-horizon loop via port-channeling dove il traffico entrante in un port-channel non può uscire dallo stesso port-channel)

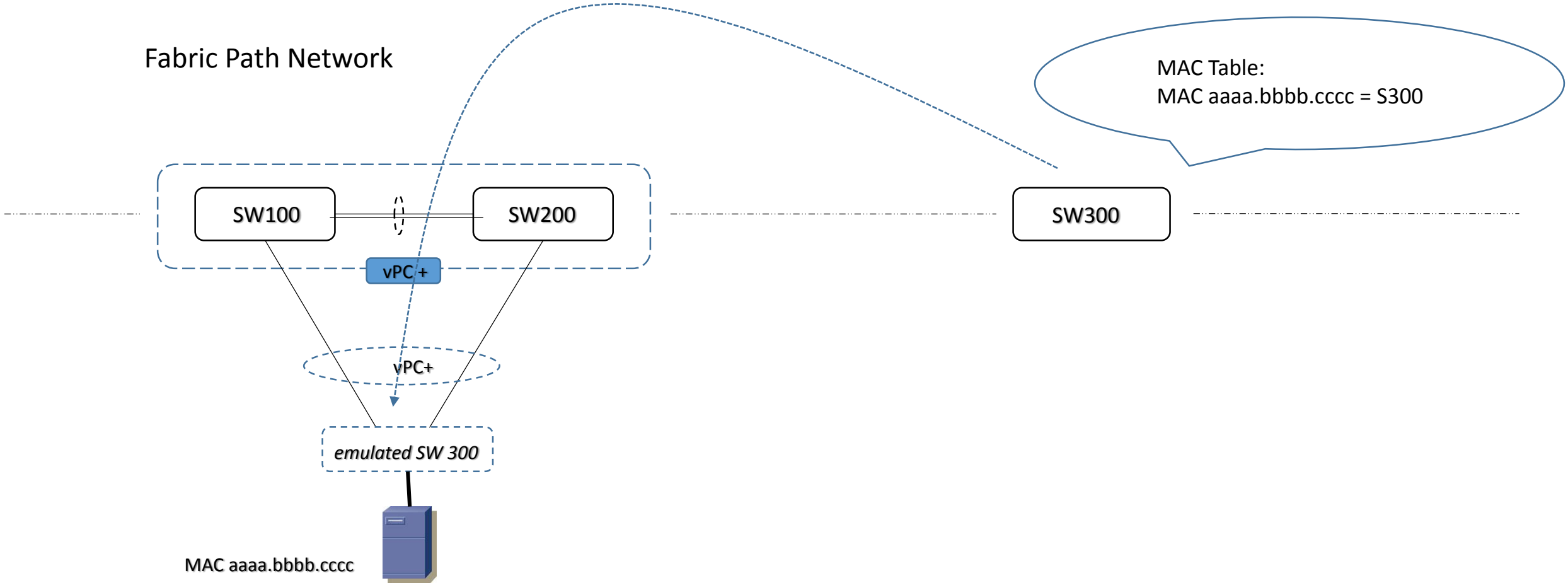
vPC Plus (vPC+) Architectures Design Cisco Models

vPC+ è una tecnologia di virtualizzazione Cisco che provvede ad un Layer 2 multipathing quale FP verso connessioni a switch non-FabricPath; in altre parole la differenza tra vPC+ ed vPC è che vPC+ performa la formazione di un " emulated FabricPath switch " la quale garantisce il load balancing di frames dirette verso un virtual port-channel attraverso una rete FabricPath

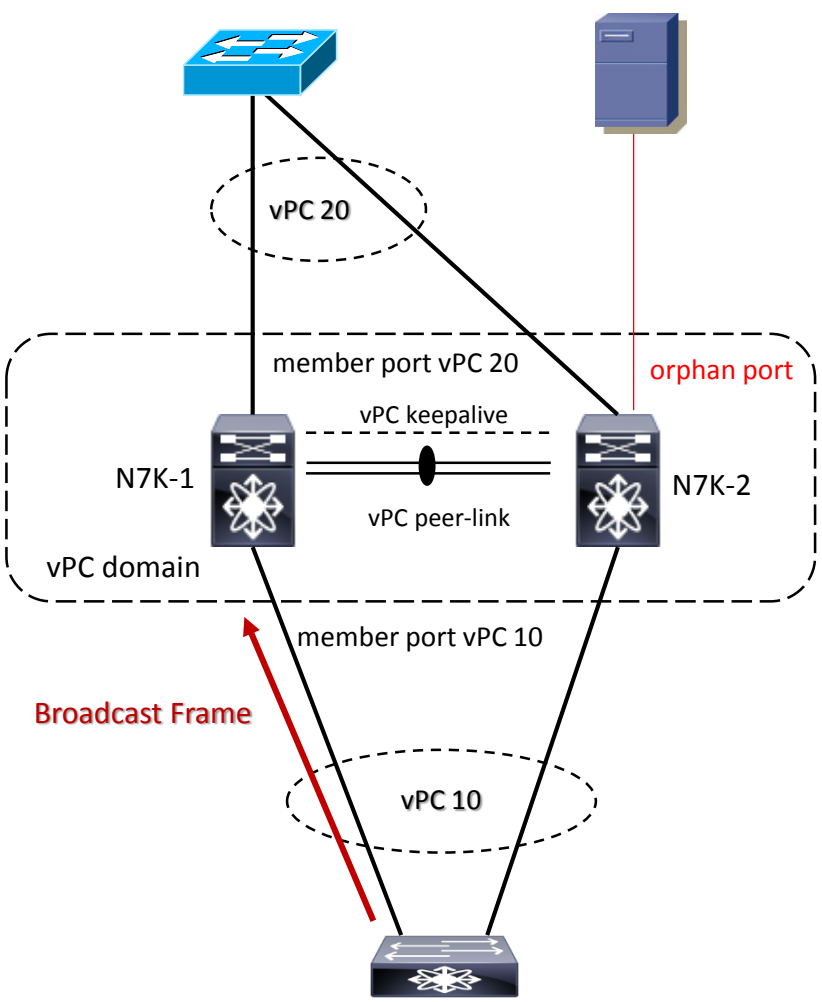


vPC Plus (vPC+) Architectures Design Cisco Models

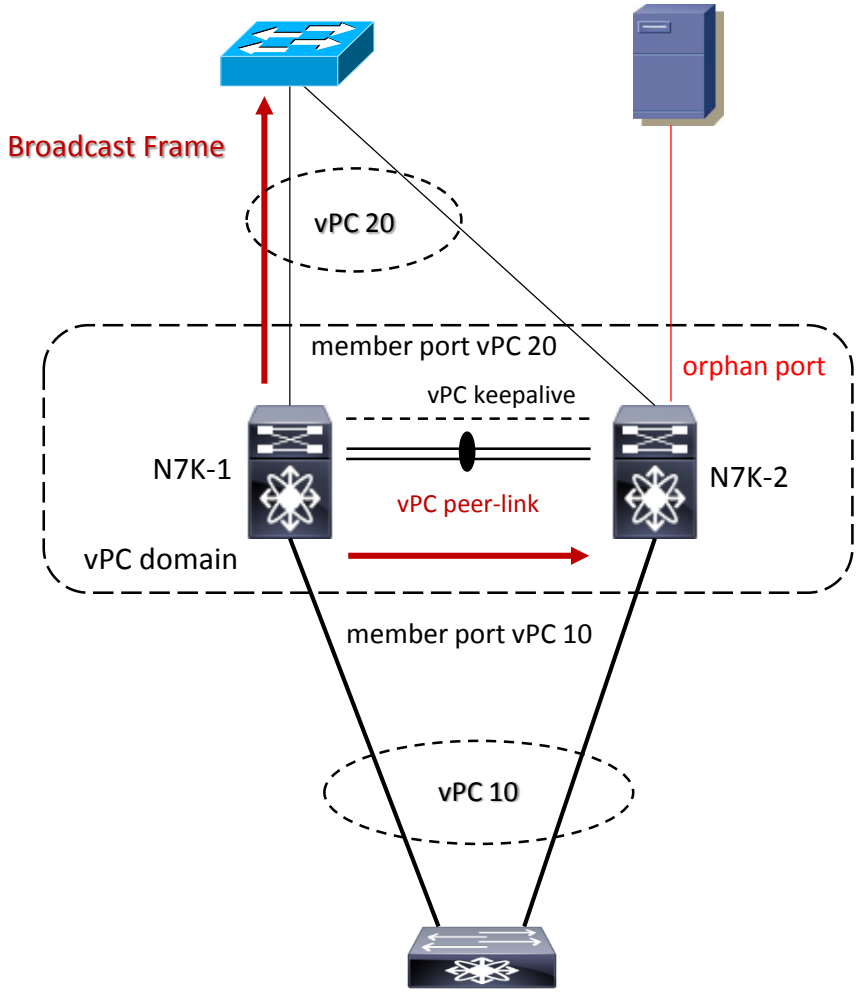
vPC+ è una tecnologia di virtualizzazione Cisco che provvede ad un Layer 2 multipathing quale FP verso connessioni a switch non-FabricPath; in altre parole la differenza tra vPC+ ed vPC è che vPC+ performa la formazione di un " emulated FabricPath switch " la quale garantisce il load balancing di frames dirette verso un virtual port-channel attraverso una rete FabricPath



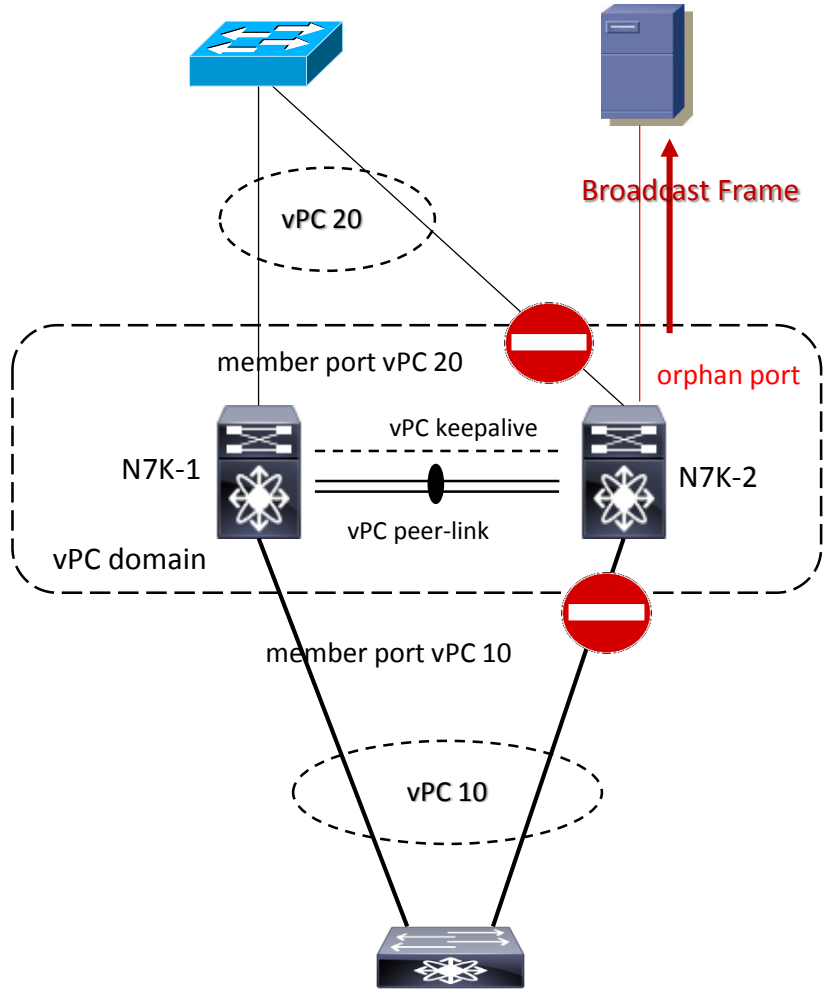
vPC broadcast frame forwarding and loop-avoidance



1

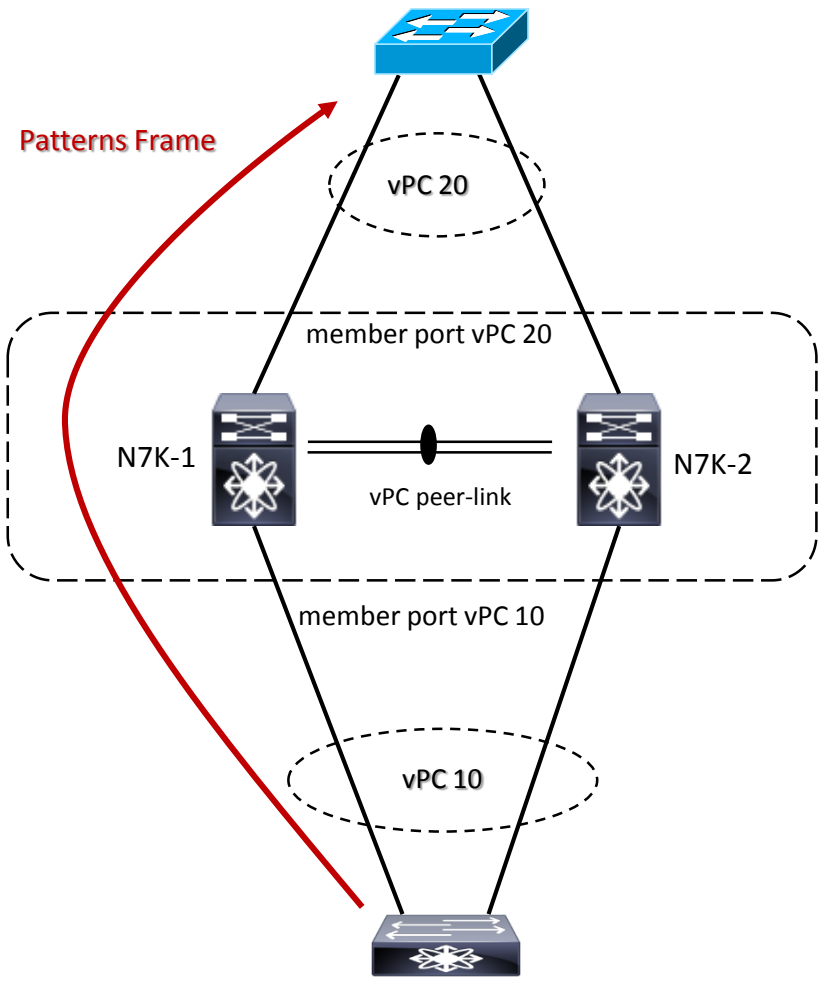


2

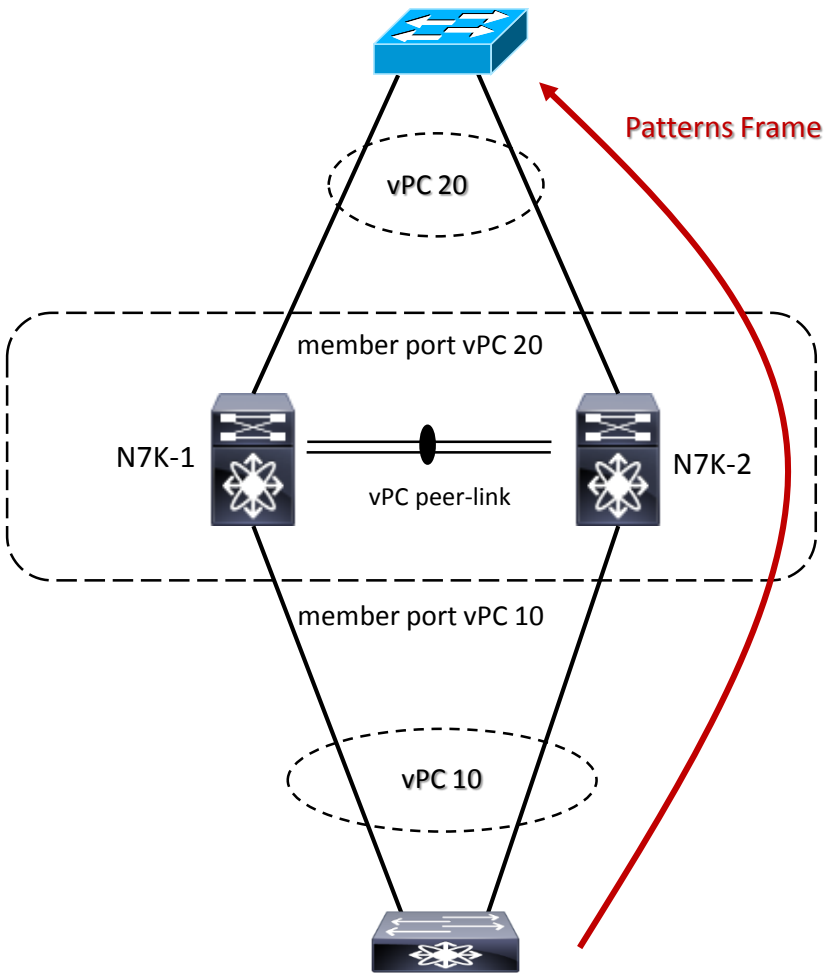


3

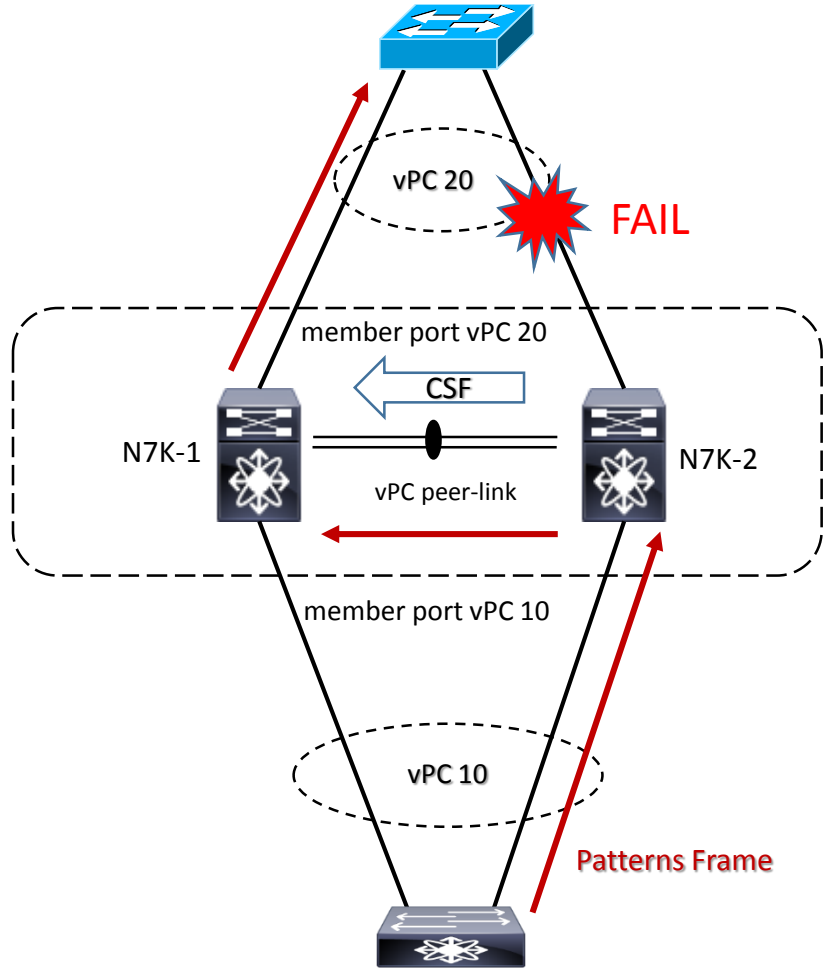
vPC Traffic Patterns possible and Failure link



1

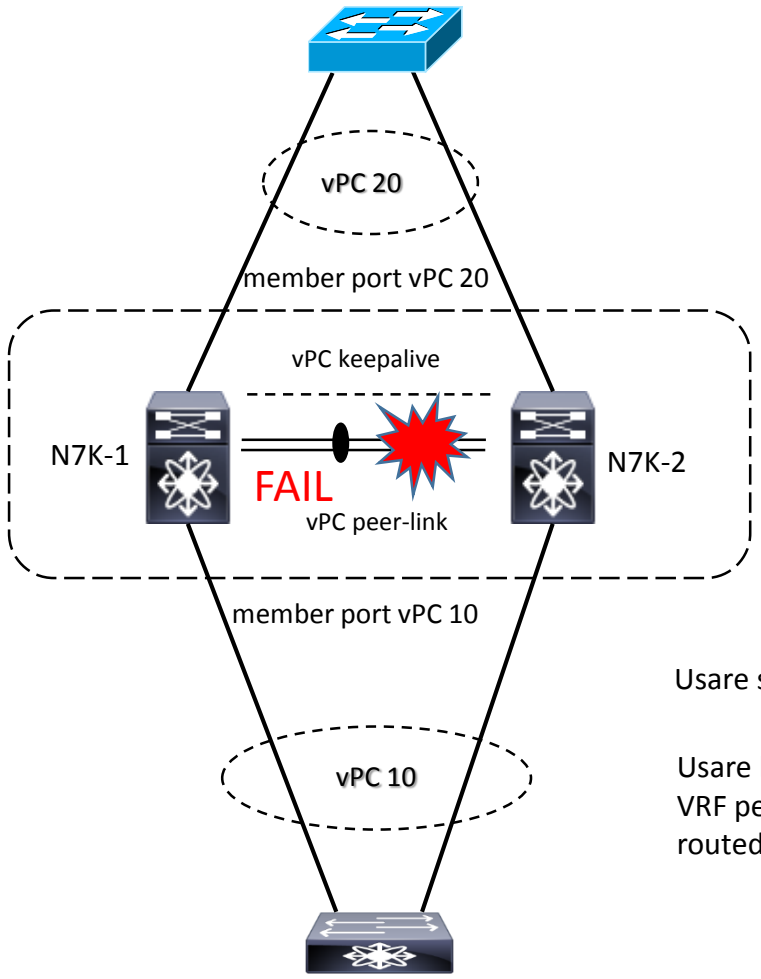


2

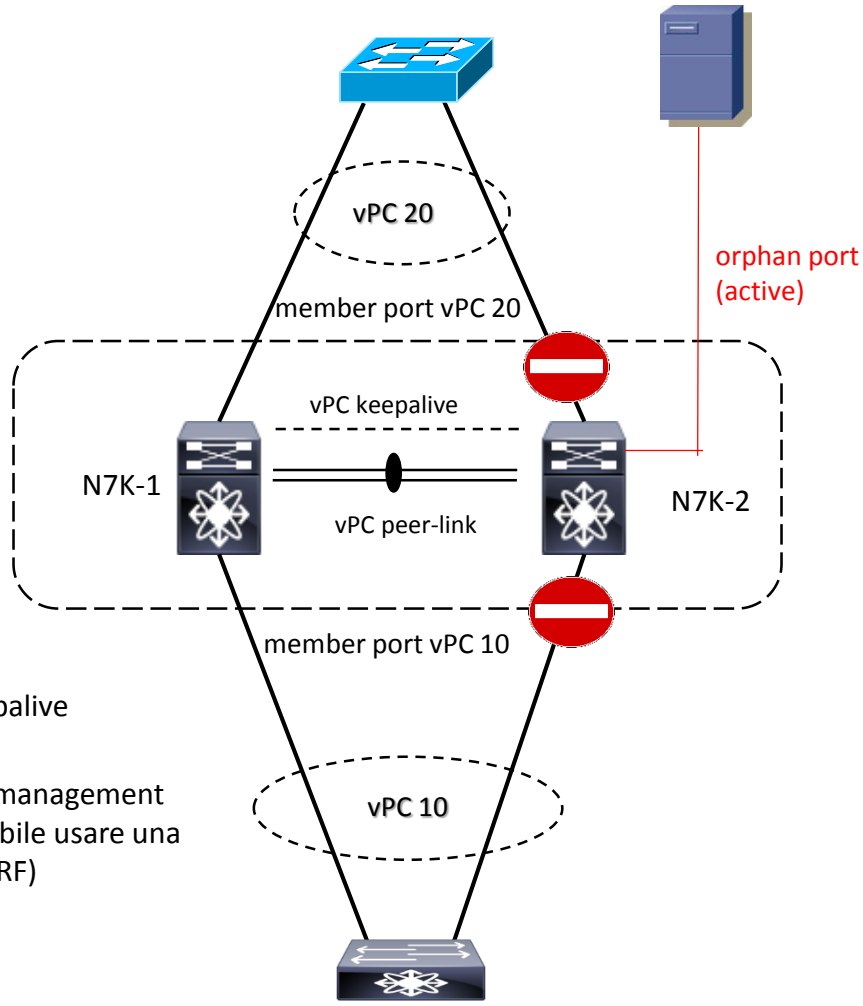


3

vPC peer-link Failure scenario



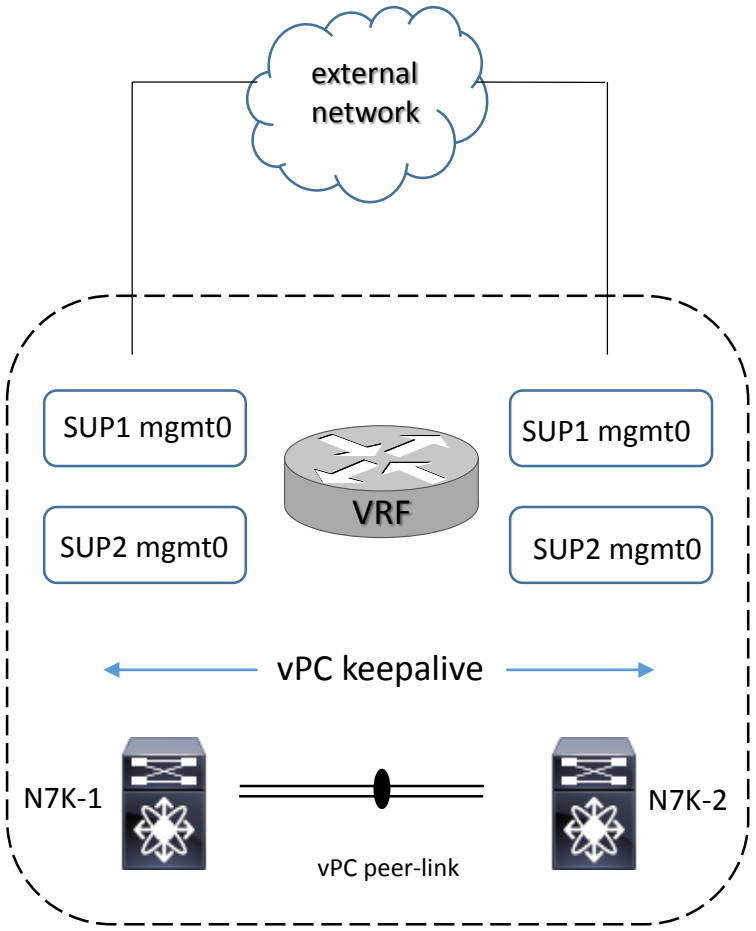
Keepalive Messages

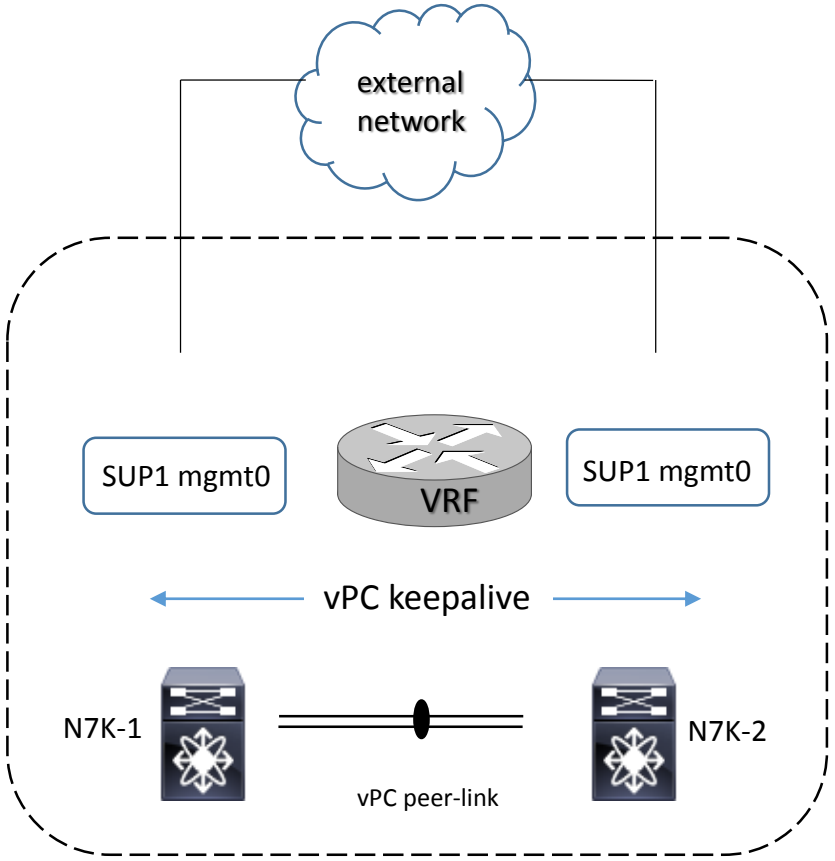


Usare sempre link differenti tra vpc peer-link e keepalive

Usare la mgmt0 interface è la routing-instances di management VRF per la configurazione keepalive (se non è possibile usare una routed interface che appartiene ad una esclusiva VRF)

vPC peer-keepalive link option





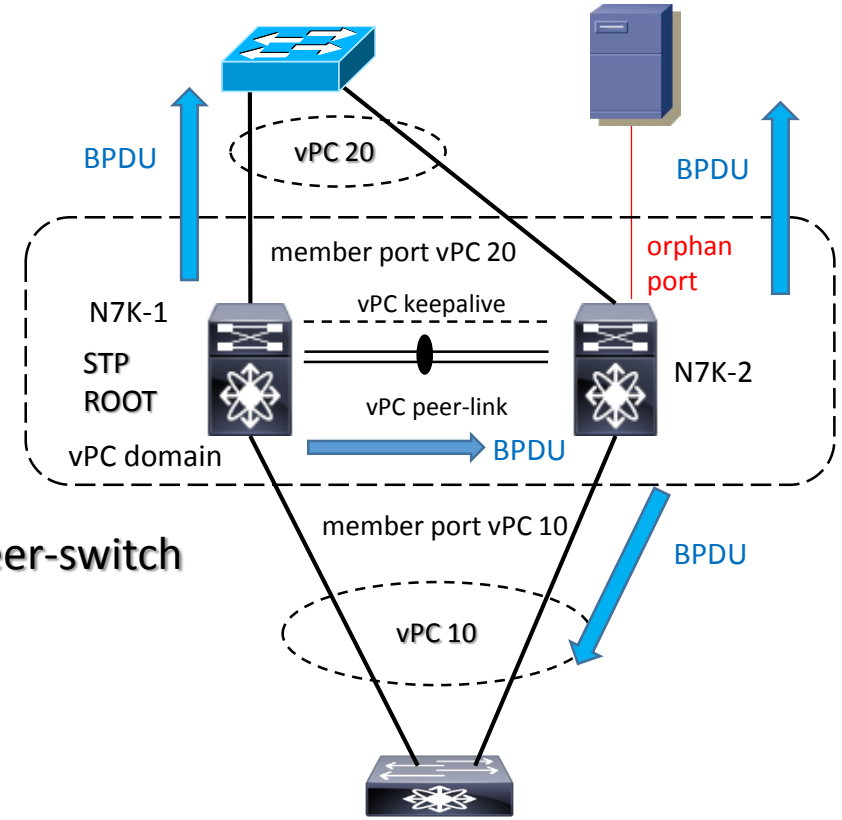
Non usare un cavo diretto tra mgmt0 per evitare perdità di connettività tra i due Nexus SUP; poiché solo la active SUP è l'unica a trasmettere heartbeat, una diretta connessione tra un active ed un standby SUP può risultare come un falso chassis state detection

vPC Architectures and STP Spanning Tree Protocol

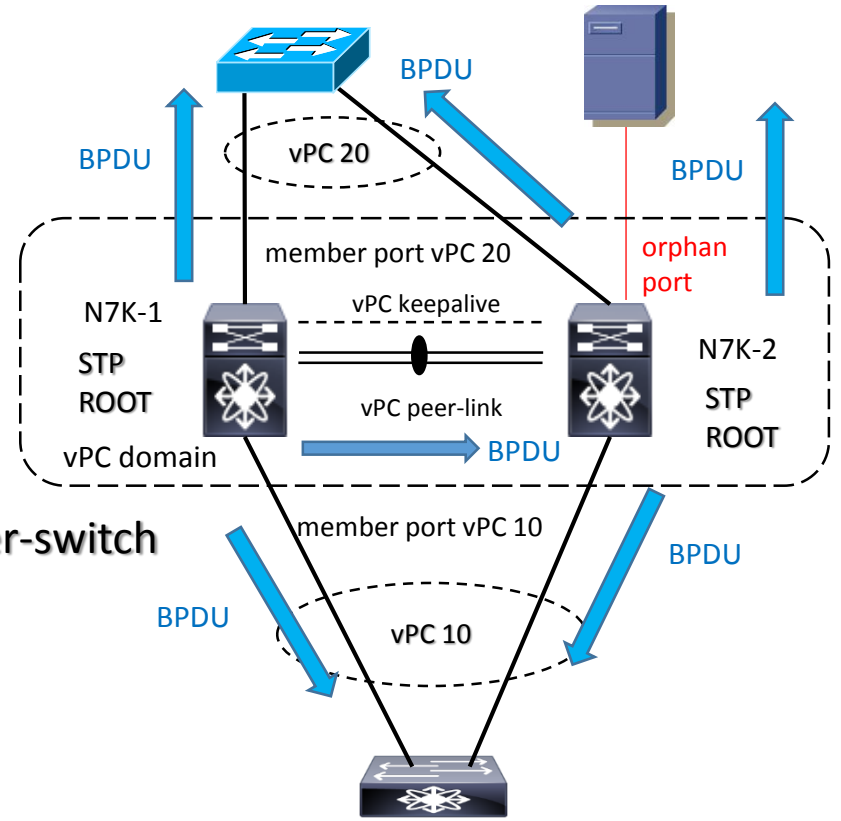
Con vPC NON elimina lo Spanning Tree Protocol

Il peer primario è responsabile per tutte le comunicazioni STP attraverso i vPC configurati; il peer secondario genera quindi BPDU solo per le interfaccie non membri vPC ma solo attraverso le sue non-vPC interface (esempio le orphan port)

- peer-switch: permette ad entrambi i peer vPC switches di emulare un singolo STP bridge; cosi entrambi gli switch trasmettono BPDU down su tutte le loro interface usando lo stesso STP bridge ID (il vPC system MAC address è usato via le BPDU



senza peer-switch

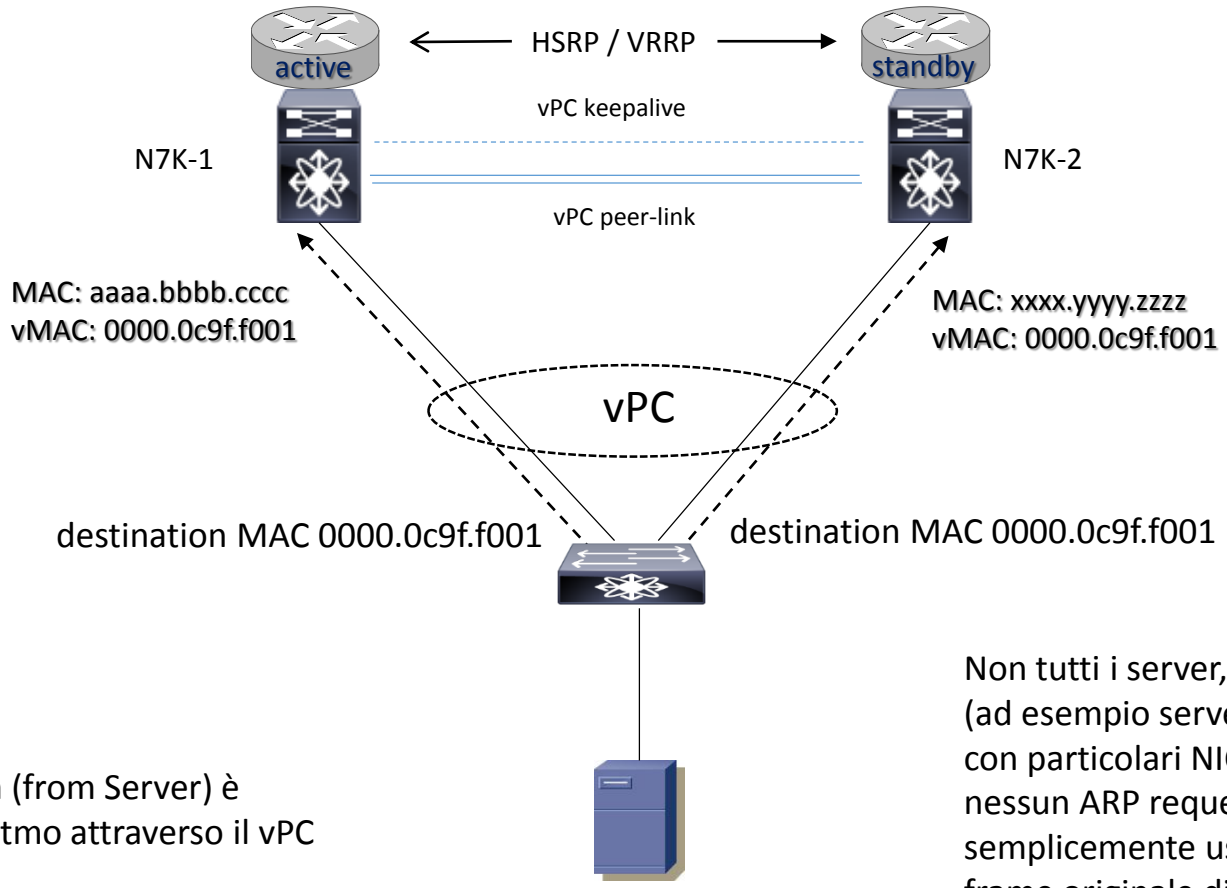


con peer-switch

vPC Architectures and First Hop Routing Protocols (1/1)

vPC peers può essere configurator come default gateway, affinchè entrambi gli switches hanno layer 3 capability.

```
interface vlan 10
no shutdown
no ip redirects
ip address 10.10.10.1/24
hsrp version 2
hsrp 10
 preempt
 priority 150
 ip 10.10.10.254
```



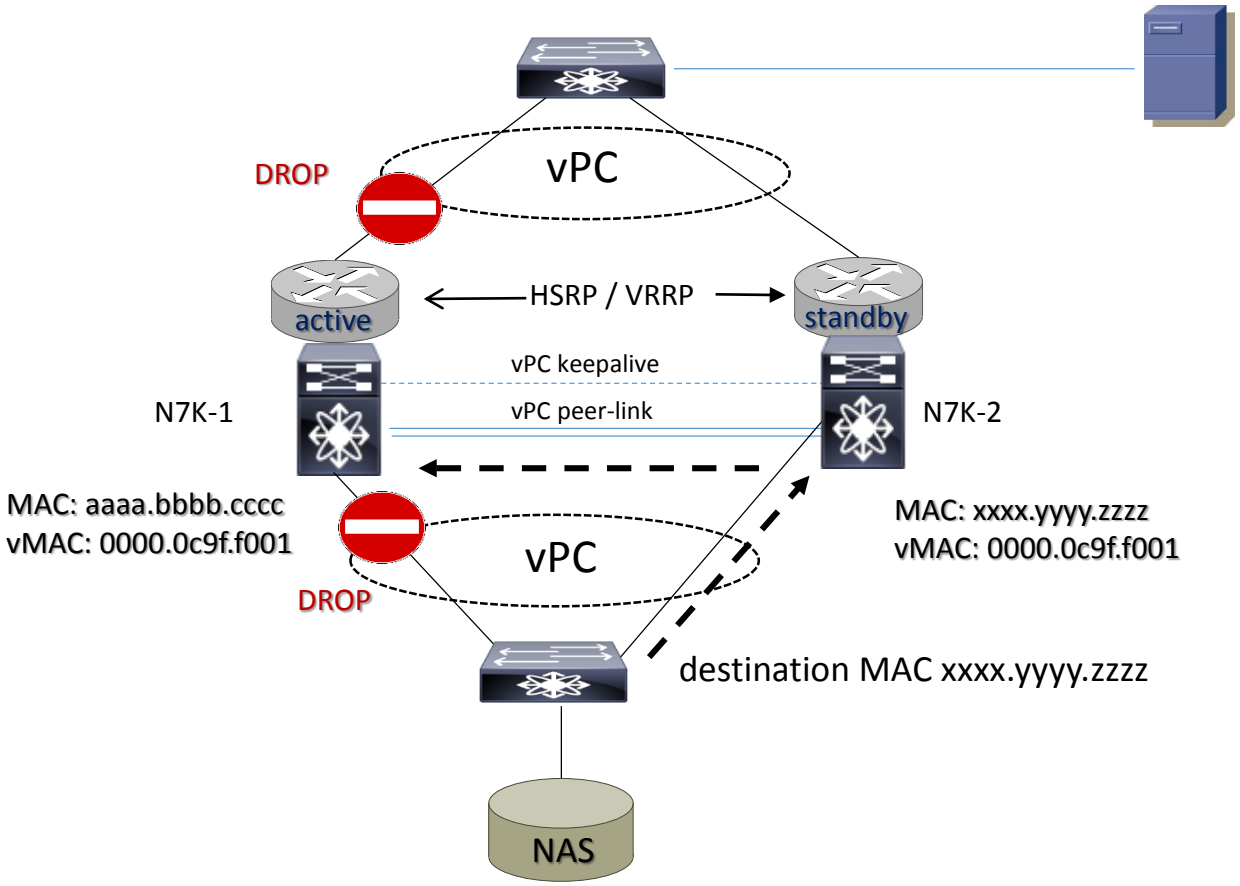

```
interface vlan 10
no shutdown
no ip redirects
ip address 10.10.10.2/24
hsrp version 2
hsrp 10
 ip 10.10.10.254
```

La trasmissione in upstream (from Server) è bilanciata via un hash algoritmo attraverso il vPC

Non tutti i server, però, necessitano di bilanciamento (ad esempio server NAS Network Storage) o server con particolari NIC teaming) perché non trasmettono nessun ARP request per scoprire indirizzi MAC, ma semplicemente usano il MAC address ricevuto nella frame originale di risposta.

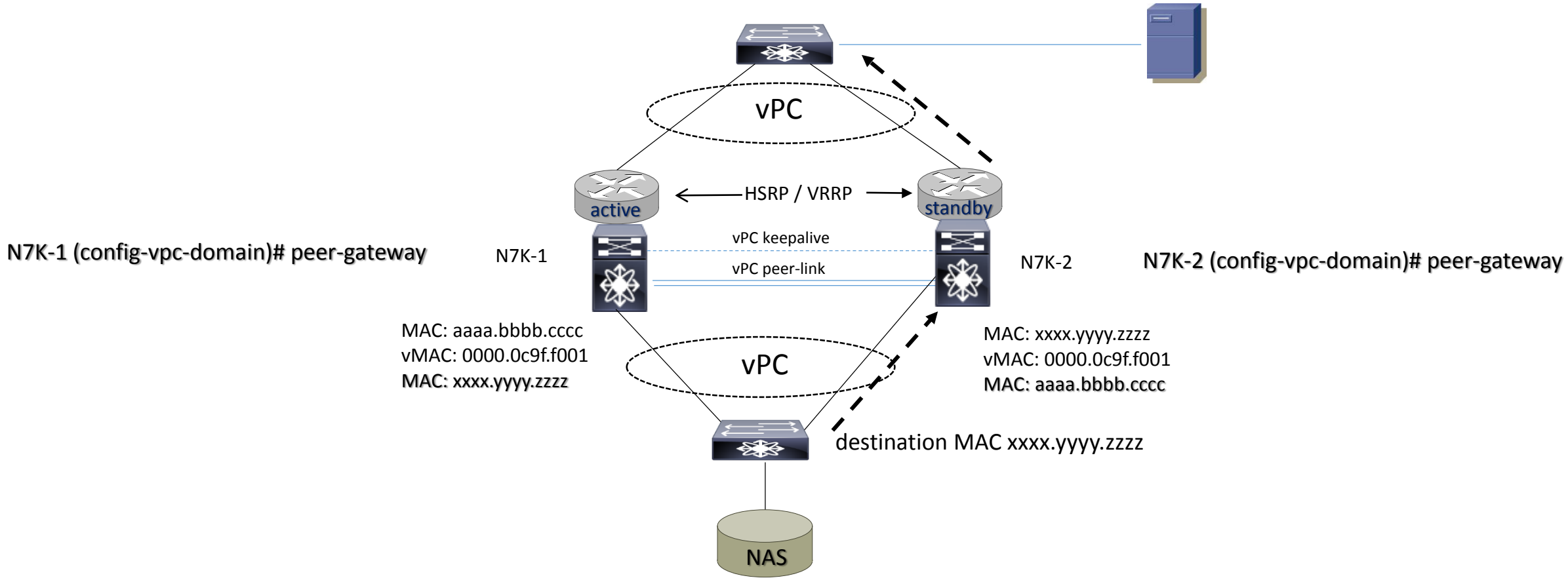
vPC Architectures and First Hop Routing Protocols (1/2)

- Il NAS trasmette un pacchetto IP diretto al MAC aaaa.bbbb.cccc (int vlan 10 N7K-1), usando però una interfaccia collegata al N7K-2 perchè cosi ha deciso l'hash algoritmo vPC port-channel
- N7K-2 switches questa frame verso il N7K-1 usando il proprio MAC address
- N7K-1 può bloccare questo pacchetto perchè supposto essere trasmesso fuori da o verso un vPC (split-horizon loop via port-channeling dove il traffico entrante in un port-channel non può uscire dallo stesso port-channel)



vPC Architectures and First Hop Routing Protocols (1/3)

- peer gateway è una caratteristica che risolve il problema indicato nella slide 1/2; in questo caso entrambi gli switches sono configurati come peer gateway e sono abilitati a ruotare pacchetti che sono diretti ai propri peer MAC address



L2 Security

DHCP SNOOPING

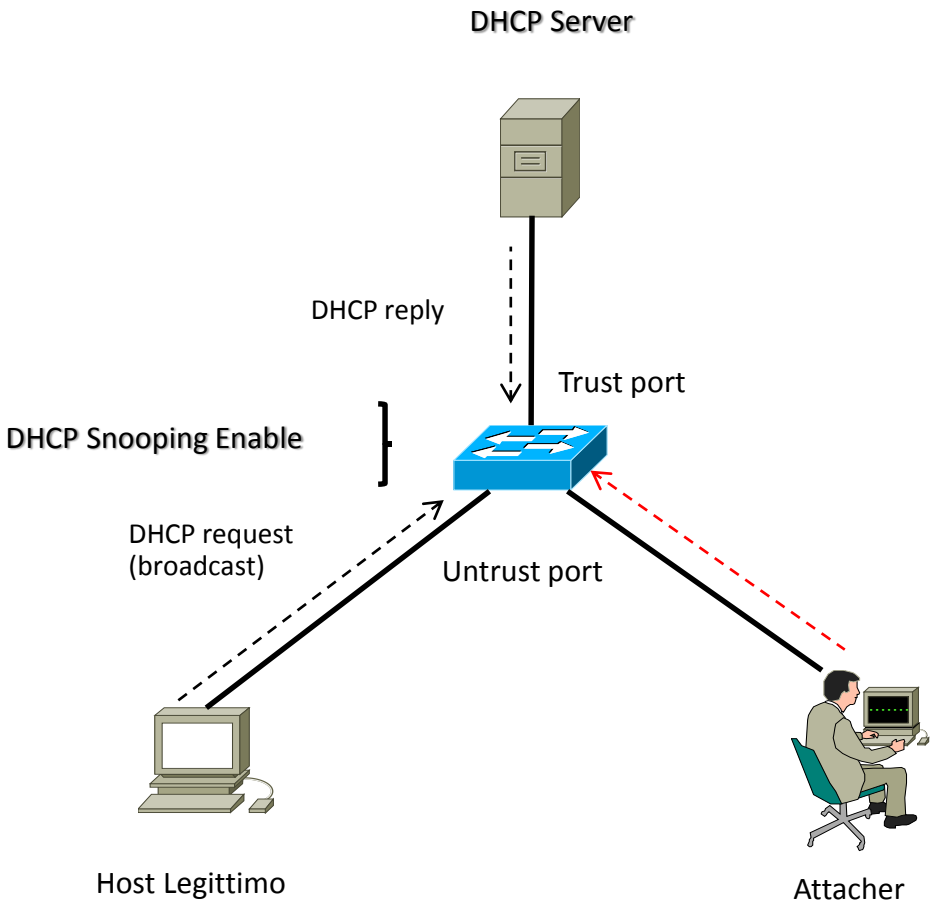
DHCP Snooping è una tecnica di sicurezza attraverso il filtering di DHCP messages ed attraverso un database che permette il controllo di questi messaggi ed accessi.

DHCP Snooping agisce come un firewall tra untrusted host ed il DHCP Server, permettendo solo messaggi di tipo trusted.

Quando DHCP Snooping è abilitato a livello switch, le porte sono classificate come trustred oppure untrusted ; le porte trusted hanno il permesso di trasmettere tutti i tipi di messaggi DHCP, viceversa le porte untrusted hanno autorizzazione a richiedere solo richieste DHCP (se lo switch vede un DHCP reply attraverso una porta untrusted questa viene disabilitata (shutdown)

E' solito utilizzare DHCP Snooping con IP source guard dove quest'ultimo controlla sia il MAC sorgente associato all'indirizzo IP verificando il match con il DHCP database (se il match è negativo la frame è filtrata)

DHCP SNOOPING



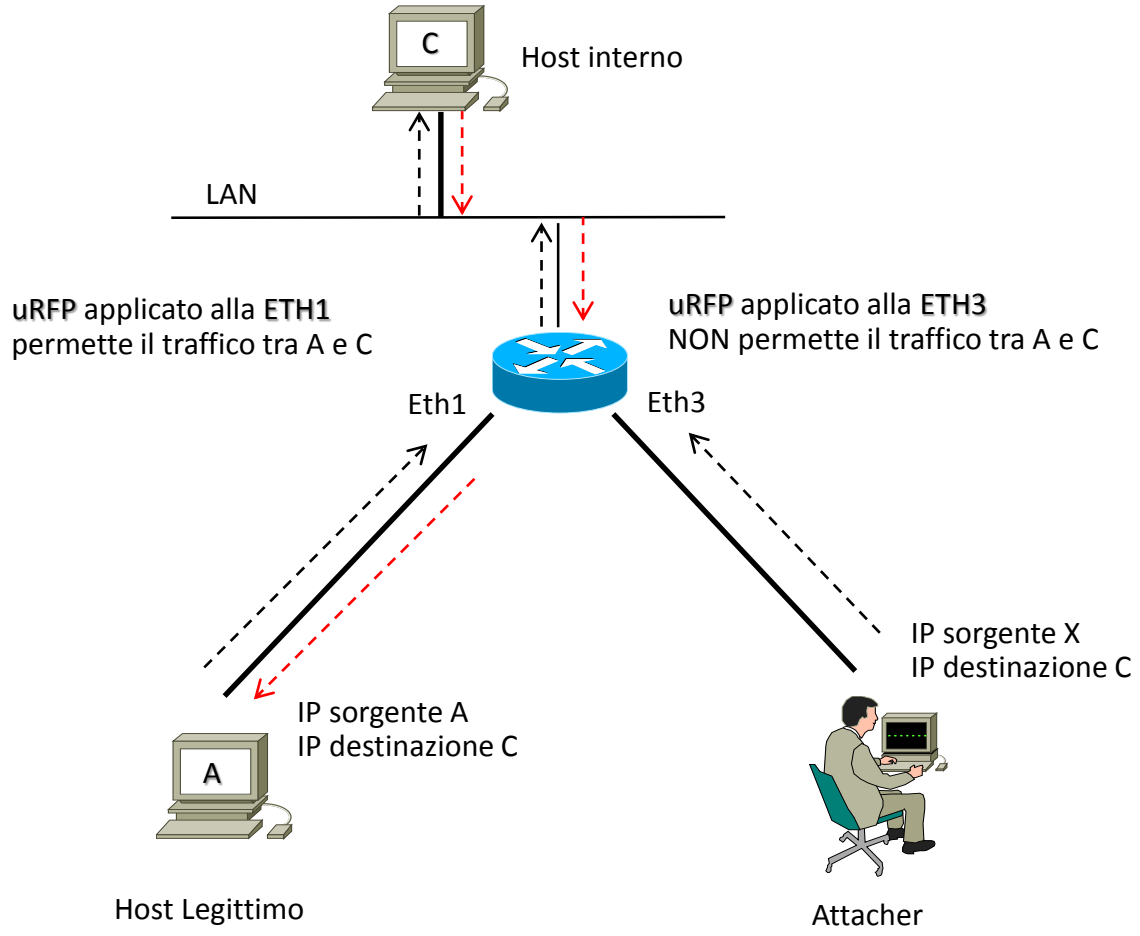
IP Source Guard e Unicast Reverse Path Forwarding

IP Source Guard è una tecnica di sicurezza contro IP spoofing dove un attacher utilizza un indirizzo IP legittimo della rete per cercare di guadagnare un accesso ad essa.

IP Source Guard, quindi, controlla e verifica l'indirizzo IP di un host associato ad una determinata porta di uno switch e previene traffic o dati se sorgente da un differente indirizzo IP da quello legittimo.

IP Source Guard può verificare anche il binomio IP address e MAC address di un host collegato allo switch
Unicast Reverse Path Forwarding (uRPF) garantisce sicurezza attraverso la verifica dell'indirizzo IP sorgente per traffico transitante attraverso un router, con il drop dei pacchetti se l'indirizzo IP sorgente non è compatibile e verificato con quello legittimo

IP Source Guard e Unicast Reverse Path Forwarding



MAC Address Limiting (port security)

E’ una funzionalità di protezione layer 2 switching, applicata a livello di porta di accesso, contro attacchi che usano MAC addresses quali MAC flooding e MAC spoofing (DoS attack).

MAC limit: permette di specificare il numero massimo di MAC addresses che possono essere appresi attraverso una singola porta di accesso; una volta che lo switch raggiunge il numero limite di MAC, tutto il traffico sorgente da nuovi MAC address sono droppati, sulla base della azioni previste in configurazione

MAC allowed: permette di definire MAC addresses per una specifica porta di accesso; qualsiasi MAC addresses che non è specificato nella lista per quella determinata porta non sarà preso in considerazione e pertanto negato.

```
interface gigabitethernet 1/10
switchport mode access
switchport port-security mac-address sticky
---
switchport port-security maximum  <value>
---
switchport port-security violation  [ restriction | shutdown ]
```