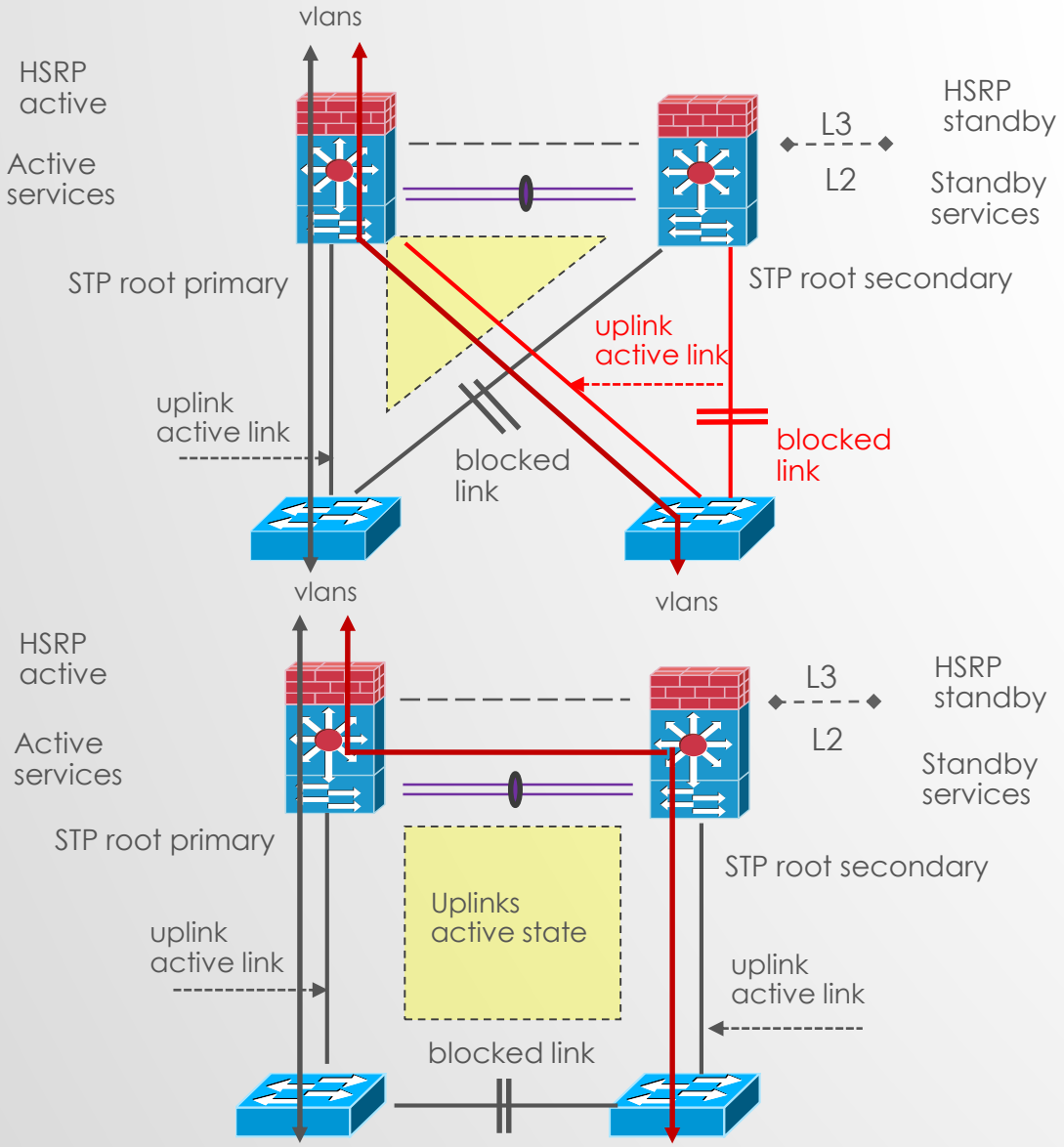
# SWITCHING ARCHITECTURES

Massimiliano Sbaraglia

# SWITCHING ARCHITECTURES DESIGN MODELS

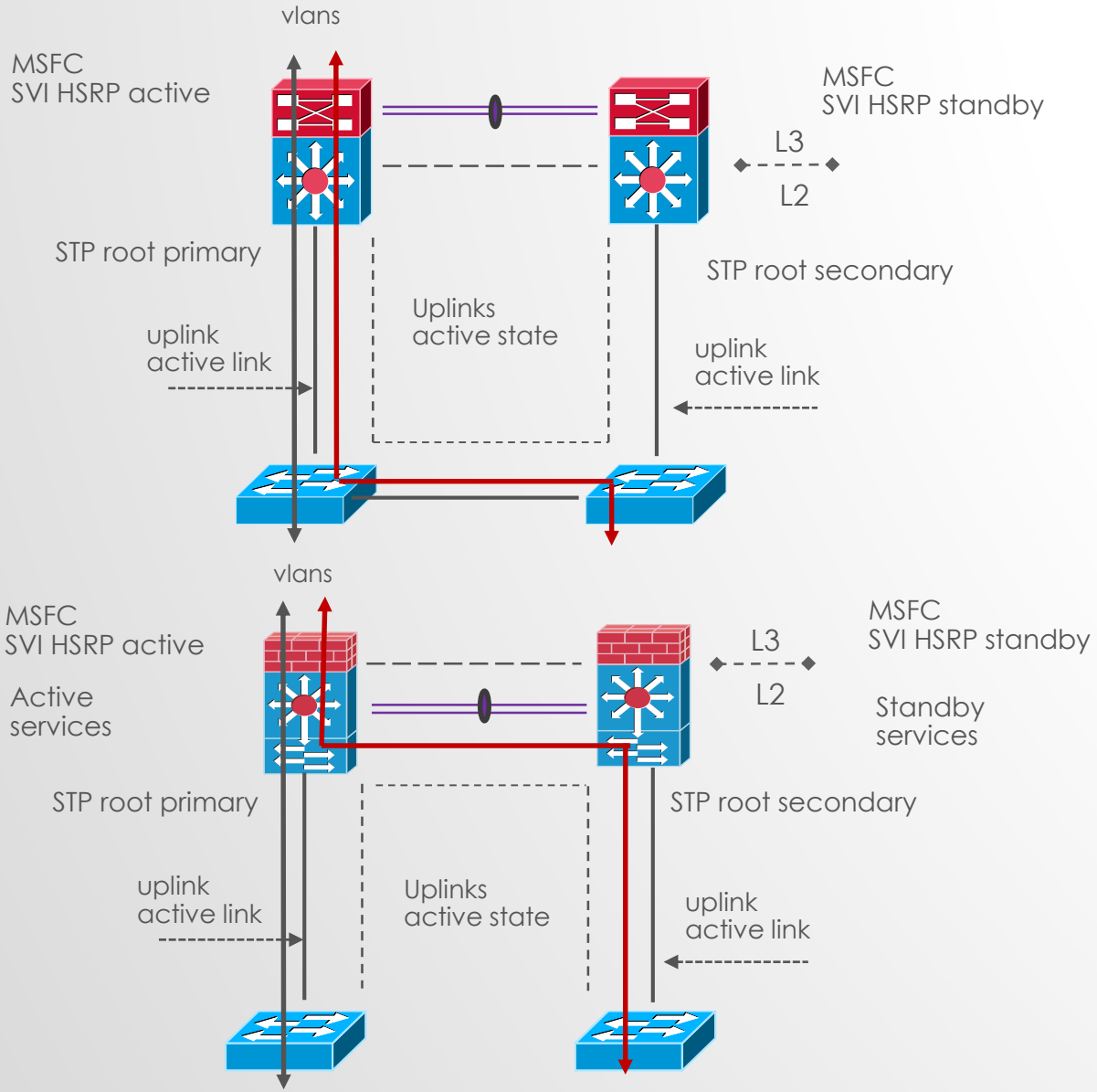



**Layer 2 Looped** : tutte le vlans **sono** estese a livello di aggregazione; offre particolari benefici per servizi di tipo statefull (significa la capacità di memorizzare dati per essere utilizzati a scopi specifici come quelli di FWSM o SLB)); il livello 3 (routing) è performato dal livello di aggregazione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

**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.

# SWITCHING ARCHITECTURES DESIGN MODELS

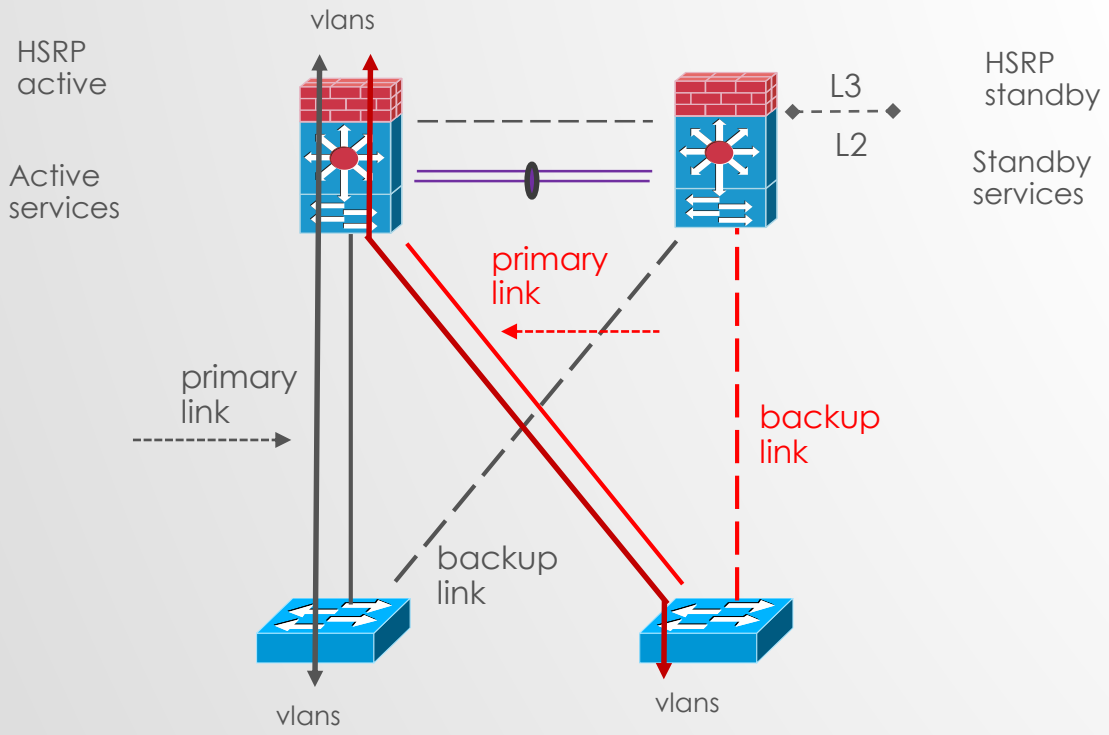



**Layer 2 Looped Free :** le vlans **non sono** estese a livello di aggregazione; il livello 3 (routing) è performato dal livello di aggregazione in su; lo spanning-tree protocol (STP) in questo scenario è in uno stato di background (non è assente) in caso di fault a livello fisico (cabling); Il throughput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

# SWITCHING ARCHITECTURES DESIGN MODELS



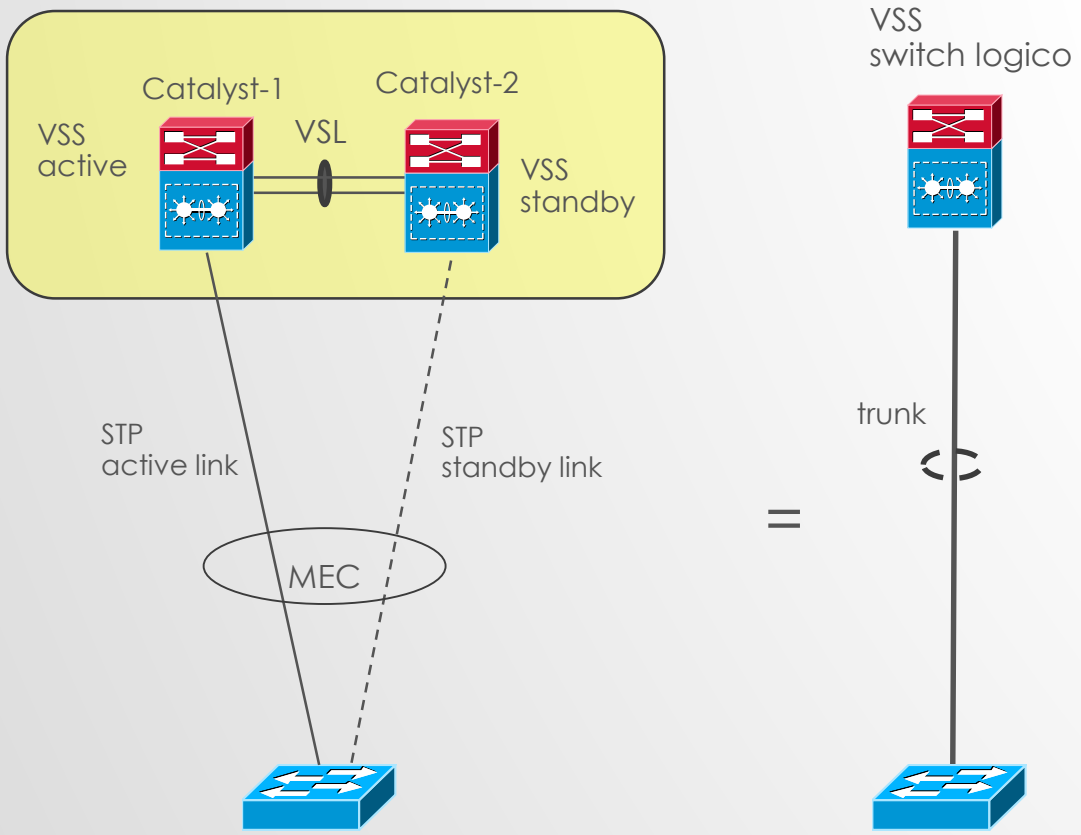

Flexlink : ogni switch di accesso ha due link verso gli switch di aggregazione con una configurazione di tipo Flex-Link

Flex-link disabilità il protocollo STP (No BPDU propagation) rendendo non conforme il modello 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 )*

# SWITCHING ARCHITECTURES DESIGN MODELS




physical view

=




logical view

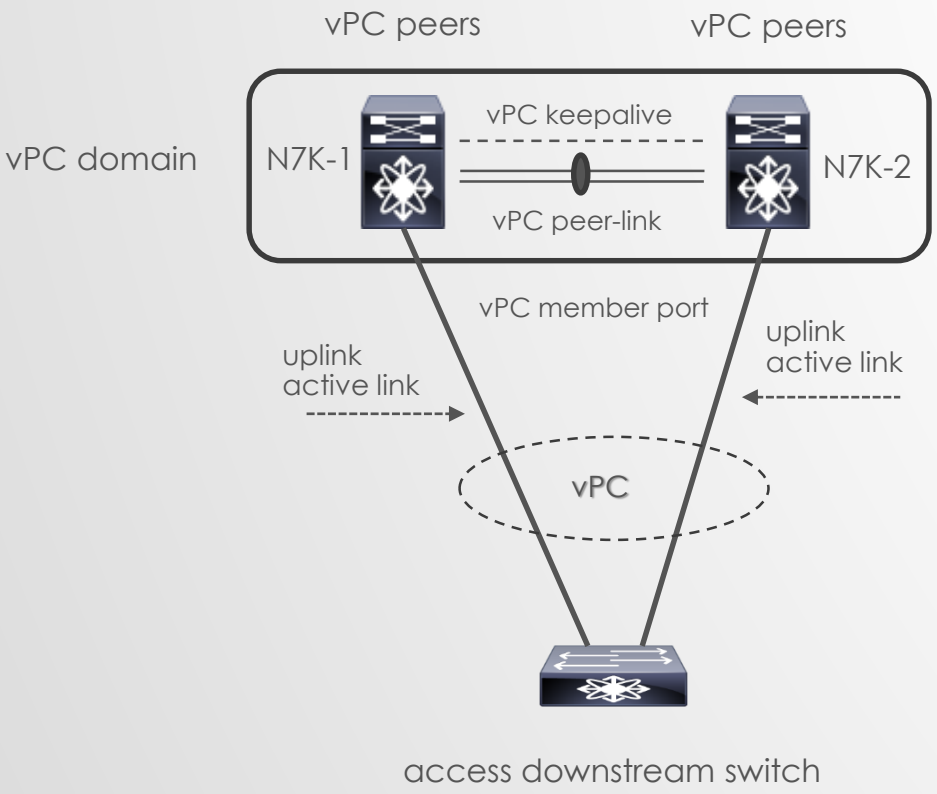
Star : Utlizzata quando un sistema VSS è impiegato insieme ad una configurazione MEC (MultiChassis Etherchannel)

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.

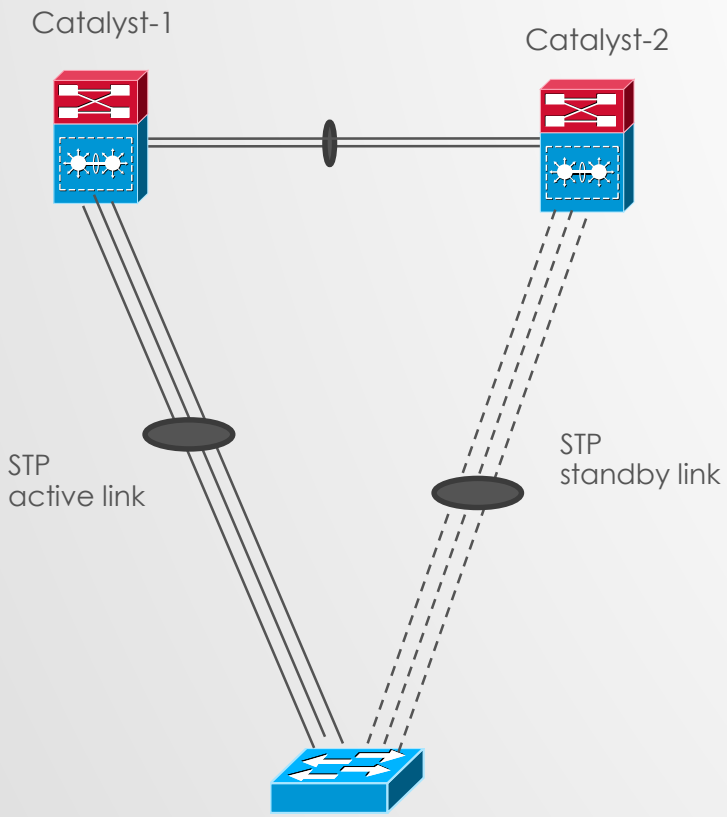
vPC per Nexus provvede ad una tecnica simile ma non viene visto come un singolo switch logico perchè tutti i link attivi sono visti come un unico uplink tra lo switch di accesso ed i due peers vPC (cioè se due switch di accesso hanno ciascuno un link in port-channel collegato ai due rispettivi switch Nexus questi link restano due uplinks distinti e non come un singolo logico trunk)

# VPC CONCEPT




- elimina SPT blocked port
- utilizza tutti I link disponibili e relativa bandwidth
- dual-homed servers in active-active mode
- fast-convergence in caso di fault link or switch
- split-horizon loop via port-channeling (traffico entrante in un po non può uscre dallo stesso port-channel)
- Un vPC domain è costituito da due peers, ognuno dei quali lavora con il proprio control-plane
- vPC significa un collegamento in port-channel tra due vPC peers ed un devices in downstream
- vPC domain è costruito attraverso la configurazione di un peer-keealive (per monitorare la condizione dei due peer) ed un peer-link (per la sincrozizzazione degli stati dei due peer)
- HA, link-level resiliency

# SWITCHING ARCHITECTURES DESIGN MODELS




**Etherchannel min-link :** questa feature permette di settare un minimo di link in bundle all'interno di entrambi i port-channel, rispettivamente collegati ai due peers di aggregazione.

Quando un link fisico all'interno del port-channel fallisce ed il numero dei link attivi è inferiore al numero configurato con il comando *port-channel min-links* il trunk operante cadrà e verrà rediretto tutto il traffic via STP port-cost feature all'altro trunk port-channel

# SPANNING-TREE PROTOCOL OVERVIEW

La funzione dello STP è quello di creare una architettura di switching (layer 2) libera da loop (loop-free) attraverso un algoritmo matematico che consente di costruire tra diversi links ridondati una struttura ad albero (tree) con specifiche funzioni e ruoli

Questi ruoli sono assegnati rispettivamente agli switch facenti parte dell'architettura layer 2 e alle relative porte con le quali si interconnettono gli switch in una magliatura di links ridondati.

Per questo processo di selezione gli switch, una volta collegati tra loro, scambiano dei messaggi chiamati BPDU (Bridge Protocol Data Unit) all'interno dei quali troviamo tre valori che determinano la migliore BPDU vista da ciascuna porta connessa (quando una porta riceve una best-BPDU smette di trasmettere le proprie BPDU a vantaggio di questa; vi è un intervallo di tempo di circa 20sec di default per il quale se una porta non sente arrivare BPDU, inizia a ritrasmette le proprie). I tre valori sono:

- Il più basso bridge ID
- Il più basso path cost root-bridge
- Il più basso interface ID (ad esempio una porta fa0/1 ha valore più basso rispetto ad una fa0/2, fa0/3 etc… )

# STP BRIDGE-ID AND PATH COST ROOT CALCULATION

Il Bridge ID (System ID extension) è un parametro presente all'interno di una BPDU ed ha una lunghezza di 8 byte.

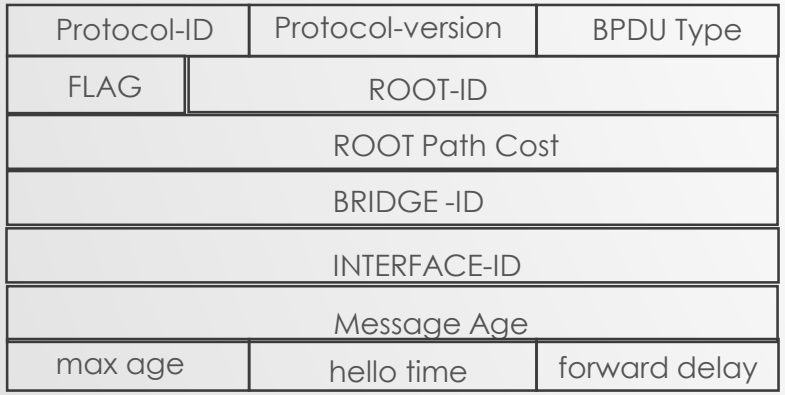
Si ottiene dalla relazione tra il valore di priority ed il valore di MAC address dello switch [ i primi due byte rappresentano la priority il quale è un valore compreso tra 0 e 65535 (di default = 32768) mentre i restanti 6 byte rappresentano il MAC address appartenete allo switch ]

In STP il valore piu basso di Bridge ID diventa root (è preferito); qualora due switch avessero identico valore di priority, viene messo a confronto anche il valore di MAC address dello switch e quello con valore più basso vince rispetto a quello con valore più alto.

BID = priority : MAC-address-switch

Il Path cost root bridge (best path) è calcolato sul valore della banda (bandwidth) che è associata all'interfaccia (porta)

# STP BPDU HEADER




**Protocol-ID:** indica il tipo di STP (standard = 0)

**Protocol Version:** indica la versione STP (802.1d = 0)

**BPDU type:** indica il tipo di messaggio BPDU (sempre = 0)

**FLAG:** indica il bit TC (Topology Change)

**Root-ID:** identifica il root-bridge (priority + MAC address switch riconoscito come root-bridge)

**Root Path Cost:** indica il costo totale per il path che raggiunge il root-bridge

**Bridge ID:** indentifica un valore che viene trasmesso da uno switch per essere eletto root-bridge (priority + MAC address dello switch che ha trasmesso la BPDU)

**Interface-ID:** identifica la porta con la quale è stata trasmessa la BPDU (priorità + id della porta stessa)

**Message Age:** indica un tempo da quando è stato eletto un root-bridge

**Max Age:** superata una soglia di tempo, viene riprocessata l'elezione del root-bridge

**Hello Time:** è il tempo che intercorre tra la generazione di due BPDU

**Fowarding Delay:** indica il tempo di permanenza tra gi stati di una porta tra listening → learning → forwarding

# STP PATH COST VALUE

| Banda | Cost STP |
|---|---|
| 4 Mbit /s | 250 |
| 10 Mbit /s | 100 |
| 16 Mbit /s | 62 |
| 100 Mbit /s | 19 |
| 1 Gbit /s | 4 |
| 2 Gbit /s | 3 |
| 10 Gbit /s | 2 |

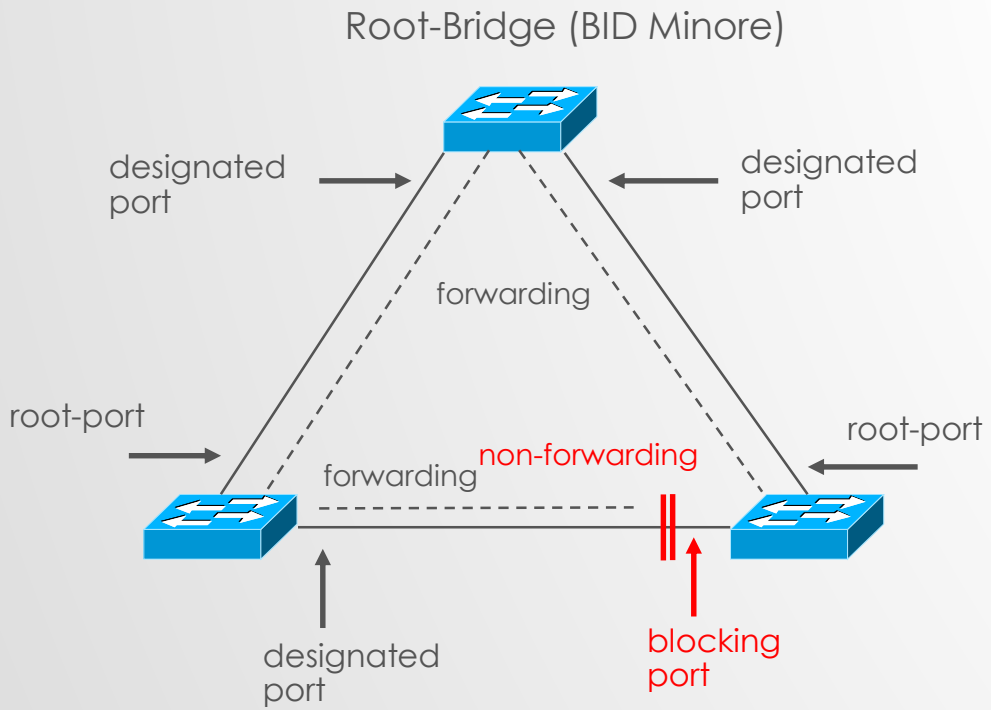
anno 1998

| Banda | Cost STP |
|---|---|
| 4 Mbit /s | 5,000,000 |
| 10 Mbit /s | 2,000,000 |
| 16 Mbit /s | 1,250,000 |
| 100 Mbit /s | 200,000 |
| 1 Gbit /s | 20,000 |
| 2 Gbit /s | 10,000 |
| 10 Gbit /s | 2,000 |

anno 2004

**Path Cost:** indica la velocità di un link associata alla porta di trasmissione

# STP INTERFACE ROLE




**disable:** indica una porta in stato shutdown

**listening and learning:** sono due stati intermedi prima di passare nello stato definitivo di blocking o forwarding che permette un tempo (circa 50 sec) ad una porta di poter trasmettere frame; il motivo è perchè se un collegamento si interrompe, uno switch potrebbe inoltrare traffico prima di avere una completa convergenza in tutta la rete provocando possibili percorsi doppi e loops fisici

**listening:** posiziona lo switch in ascolto di BPDU con i contenuti indicati nell'header BPDU e verificare quelli migliori

**learning:** offre la possibilità di imparare indirizzi MAC al fine di creare una tabella di MAC address (STP table)

**blocking:** indica una porta messa in uno stato di NON trasmissione e ricezione (anche conosciuta come non-designated)

**forwarding:** indica una porta in condizione di trasmettere e ricevere frame (un root-bridge ha tutte le sue porte in questo stato conosciuta anche come designated)

Per la definizione dei ruoli delle porte è previsto un processo di selezione che predeve i ruoli di root-port, designated-port e blocking-port

# STP TOPOLOGY CHANGE AND TIME

Con lo Spanning Tree a regime, le BPDU vengono emesse solo dai Root Bridge.

Se nel periodo di tempo indicato dal campo Max Age non si ricevono BPDU, viene rilanciata l'elezione tramite un processo di topology change.

Si verifica un cambio nella topologia quando una porta di trunk nello stato di forwarding va in down, oppure quando uno switch ha una nuova porta che passa nello stato di forwarding. Lo switch che rileva l'evento invia verso il root bridge una trama di TCN, (Topology Change Notification); il root Bridge informa tutti gli switch della rete del cambiamento in corso, dando via ad una rinegoziazione dell'STP.

Gli switch con STP attivo inviano le BPDU nella rete ogni 2 secondi; questo tempo si chiama 'hello time' ed e' modificabile dall'operatore tra 1 e 10 secondi

Se non si ricevono BPDU per un tempo massimo pari per default a 20 secondi si considera perso lo switch mittente; questo tempo si chiama 'max age' ed e' modificabile dall'operatore tra 6 e 40 secondi

STP rimane in continuo ascolto per verificare tramite queste BPDU che non vi siano collegamenti interrotti o loop in rete.

Se si verifica l'interruzione di un collegamento, STP interviene per cambiare le porte dallo stato di blocked a quello di forwarding o viceversa.

Il cambiamento però non è istantaneo; il ricalcolo dei percorsi migliori nella rete varia dai 30 ai 50 secondi per ogni switch; in questo intervallo di tempo, nelle porte interessate da STP, i dati non possono transitare.

# ALCUNE DIFFERENZE TRA STP (802.1D), RSTP (802.1W), MSTP (802.1S)

802.1w = RSTP = Rapid Spanning Tree = usato per una veloce convergenza ; prevede collegamenti P2P full-duplex tra switch e si passa dai 50 sec di convergenza di STP a circa 10 sec con RSTP (si eliminano anche funzioni quali portfast ed uplinkfast inutili per questo modello)

- 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

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

# ALCUNE DIFFERENZE TRA STP (802.1D), RSTP (802.1W), MSTP (802.1S)

802.1s = MSTP = Multiple Spanning Tree = costruisce 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 = costruisce una istanza STP per singola vlan

# STORM CONTROL

Traffico di tipo Storm si verifica quando vi è un eccesso di pacchetti (flooding) per una data porta fisica LAN, degradando di conseguenza le prestazioni.

Il controllo per questo tipo di traffico, chiamato STORM CONTROL, previene le porte LAN di uno switch dall' essere disturbate da traffico storm sia broadcast, multicast, unicast; in altre parole, questo controllo monitorizza il livello di traffico in ingresso in un dato intervallo di tempo (1 sec) , comparando la quantità di traffico in uso su quella determinata interfaccia fisica e il livello di storm control che manualmente viene configurato.

Il livello di controllo di traffico storm è una percentuale del valore di bandwitdh della porta;

All'interno dell'intervallo di tempo (1 sec), quando il traffico in ingresso per il quale il controllo di storm traffic è abilitato, raggiunge il livello settato per quella determinata  porta fisica, il traffico viene scartato (drop).

*interface x/y*
*storm-control [ broadcast | multicast | unicast ] level [ percentage or pps ]*

# BROADCAST SUPPRESSION

Uno storm broadcast si verifica quando pacchetti di tipo broadcast o multicast inondano (flooding) un dominio di rete LAN creando malfunzionamenti e degrado delle prestazioni.

Broadcast suppression usa dei filtri di misurazione dell'attività broadcast all'interno della LAN per un periodo di circa 1 sec e varia a seconda del tipo di line-card e velocità settata sulla porta fisica dello switch, comparando questa misurazione con una soglia (threshold) predefinita.

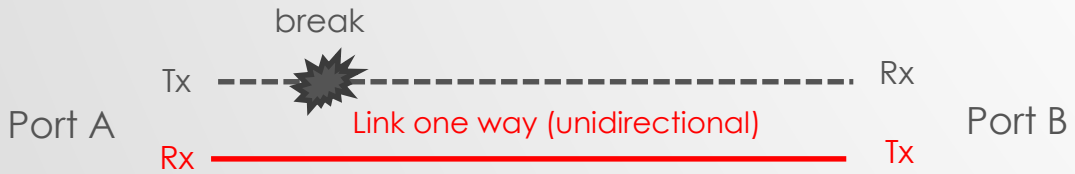
Se viene raggiunta questa soglia, il traffico broadcast viene soppresso per una durata di tempo specifico.

*interface x/y*
*broadcast suppression [ threshold ]*

threshold =
0,00 for suppress all broadcast traffic
0,01 for 0,01% (1/100 percent)
0,50 for 0,50% (one-half percent)
1 for 1% (one percent)

# UDLD UNIDIRECTIONAL LINK DETECTION





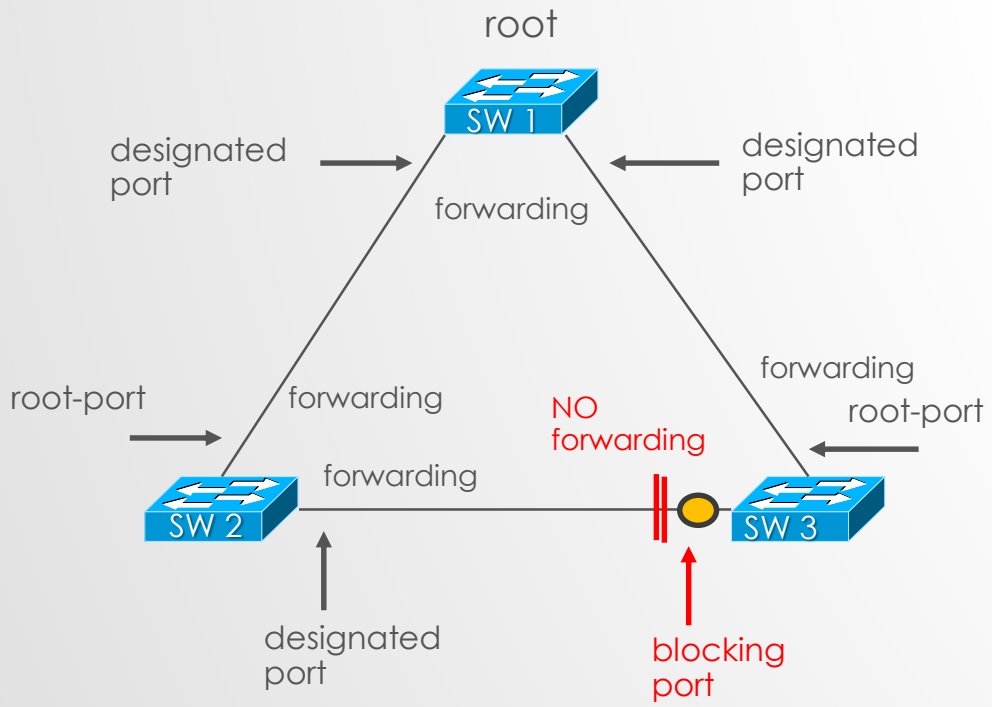

**UDLD** è un protocollo proprietario Cisco che pemette di prevenire problemi di loops tra una connessione in fibra ottica oppure in rame attraverso il riconoscimento di un link in one-way (unidirectional), disabilitando la porta in errore ed inviando un alert

**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

# COS'E' LOOP-GUARD E DOVE DEVE ESSERE CONFIGURATO




interface gigabitethernet 1/10
spanning-tree loopguard

OR
spanning-tree loopguard default

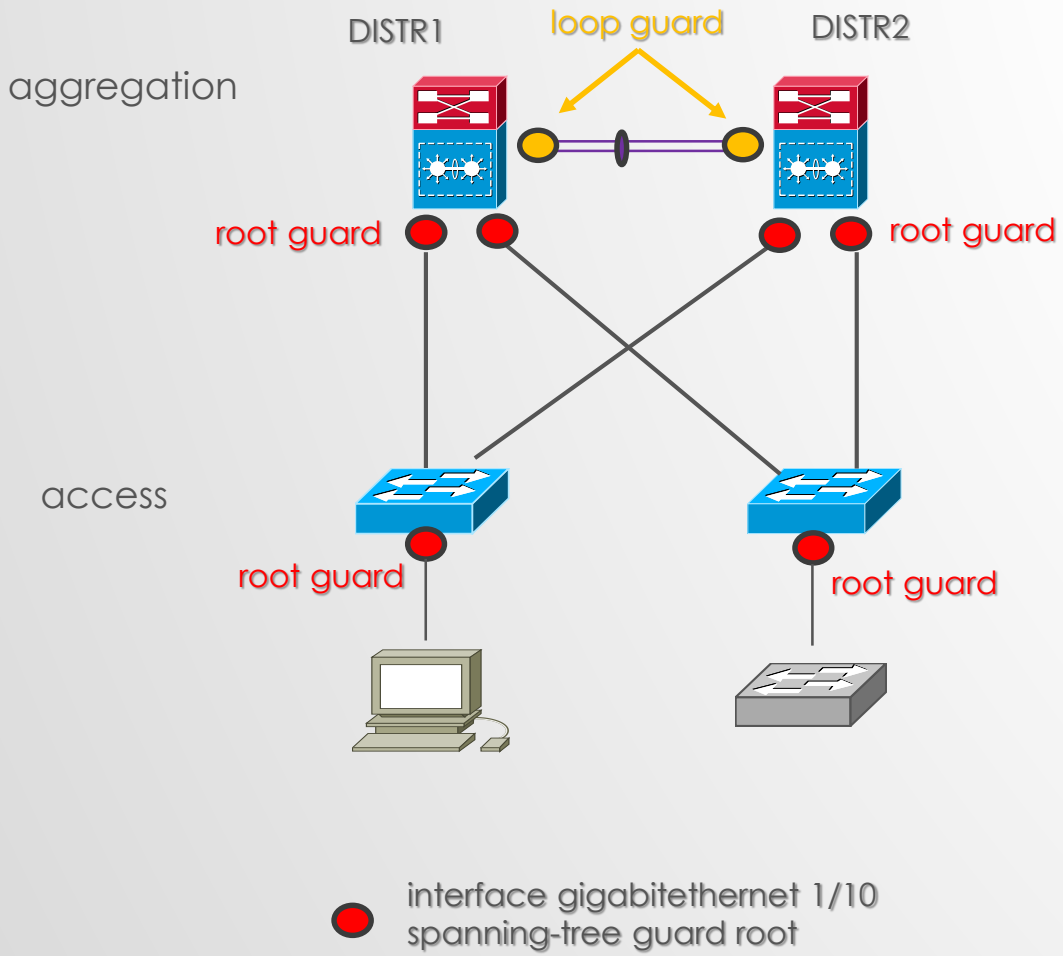
Loop Guard è una feature che protegge un link di collegamento tra switches a causare un loop; quindi previene una transazione da uno stato di blocking ad uno di forwarding, quando per cause di errore dovute a UDLD presente in uno specifico link.

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

# COS'E' ROOT-GUARD E DOVE DEVE ESSERE CONFIGURATO

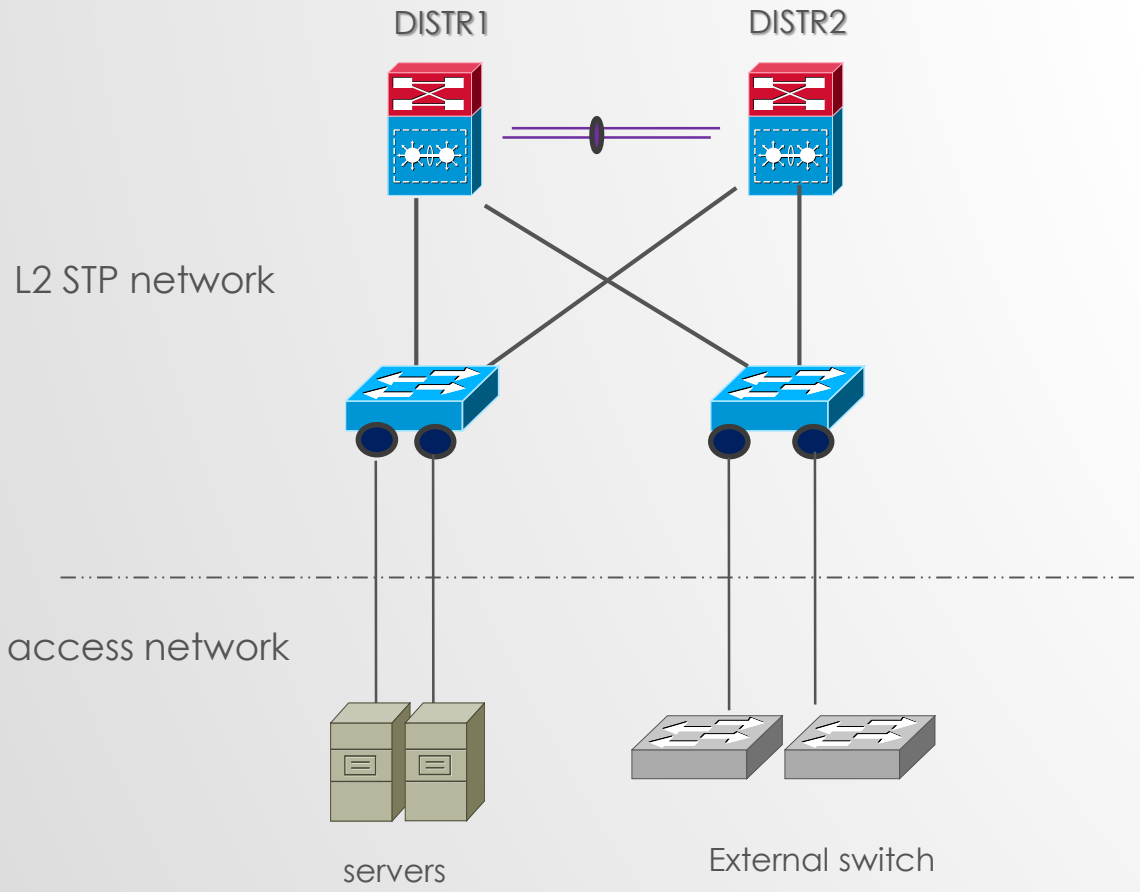



Root Guard è una feature che previene una porta (differente dalla legittima root port) di uno switch (non il root-switch) a diventare root-port

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.

# COS'E' BPDU-GUARD E DOVE DEVE ESSERE CONFIGURATO (E PORTFAST)




interface gigabitethernet 1/10
spanning-tree bpdufilter enable

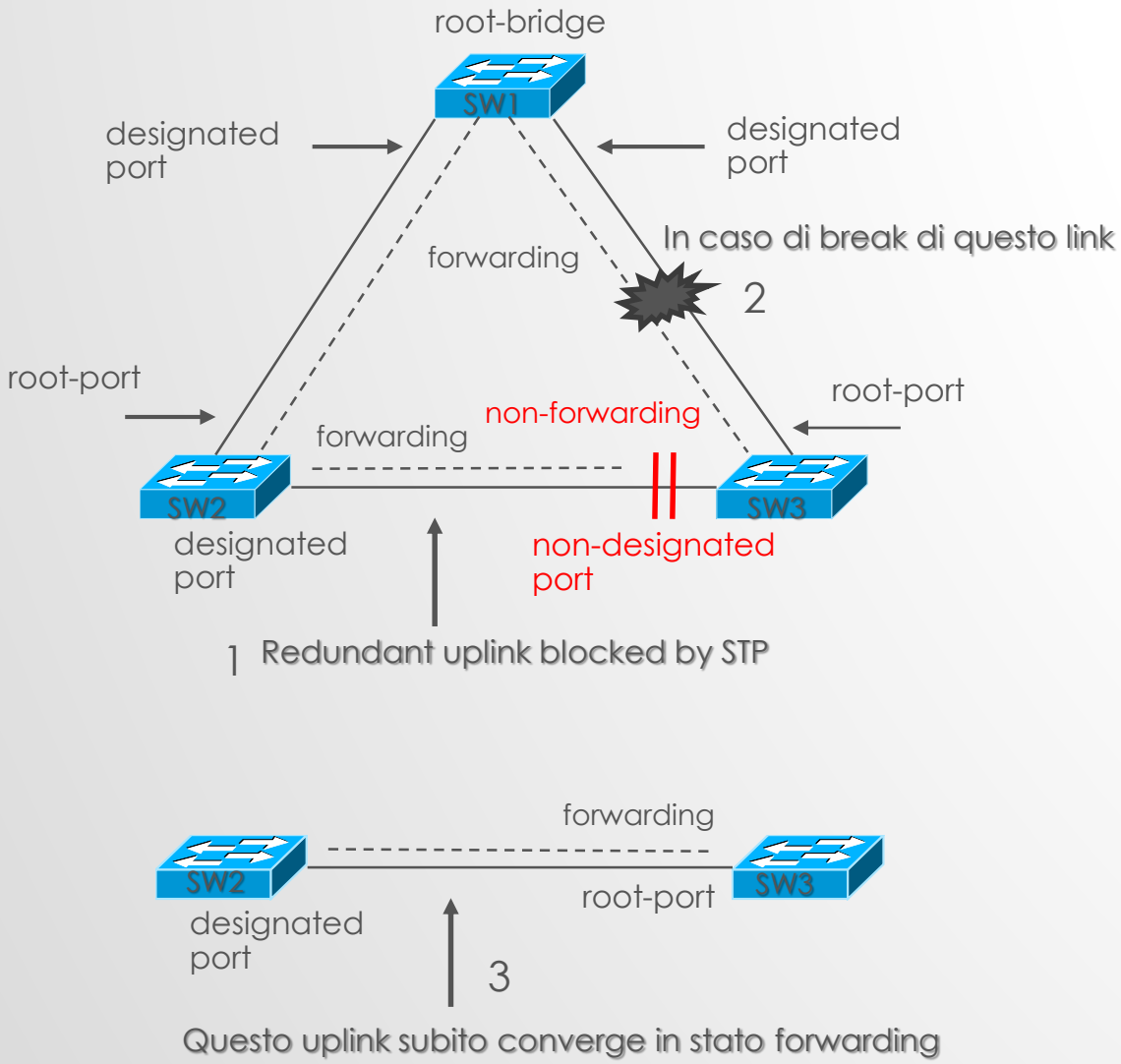
BPDU Guard è una feature che disabilita (shutdown) una porta di uno switch, non appena questa riceve una BPDU proveniente da un external switch o devices STP, ponendo la porta sulla quale era stato abilitato il bpdu-guard lo stato di err-disable.

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

# COS'E' UPLINK-FAST AND BACKBONE-FAST




**Uplink Fast** è una feature che accelera la scelta di una nuova root-port quando un collegamento fallisce

**Backbone Fast** è una feature che fornisce una veloce convergenza in caso di un cambiameto topologico dello spanning-tree (STP); è una funzione usata ai livelli di aggregazione e core di un campus, dove ci sono più switch interconnessi tra loro

**Esempio di configurazione**

**Uplink-fast:**
spanning-tree uplinkfast [max-update-rate < value > ]

**Backbone-fast;**
spanning-tree backbonefast → *in modalità global*

# IL PROTOCOLLO ETHERNET


Original Frame Ethernet

**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

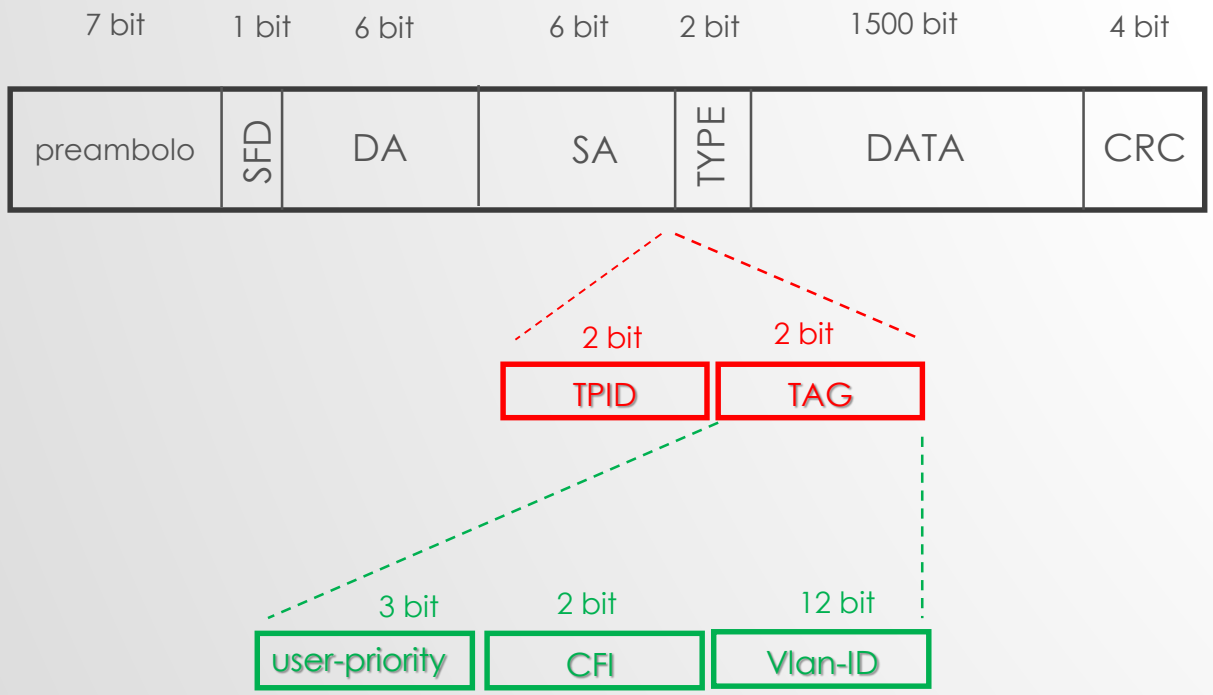
**SA:** indica il MAC address dell'unità sorgente

**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

# IL PROTOCOLLO ETHERNET 802.1Q TAGGING FRAME




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

Non encapsula il frame Ethernet originale

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)

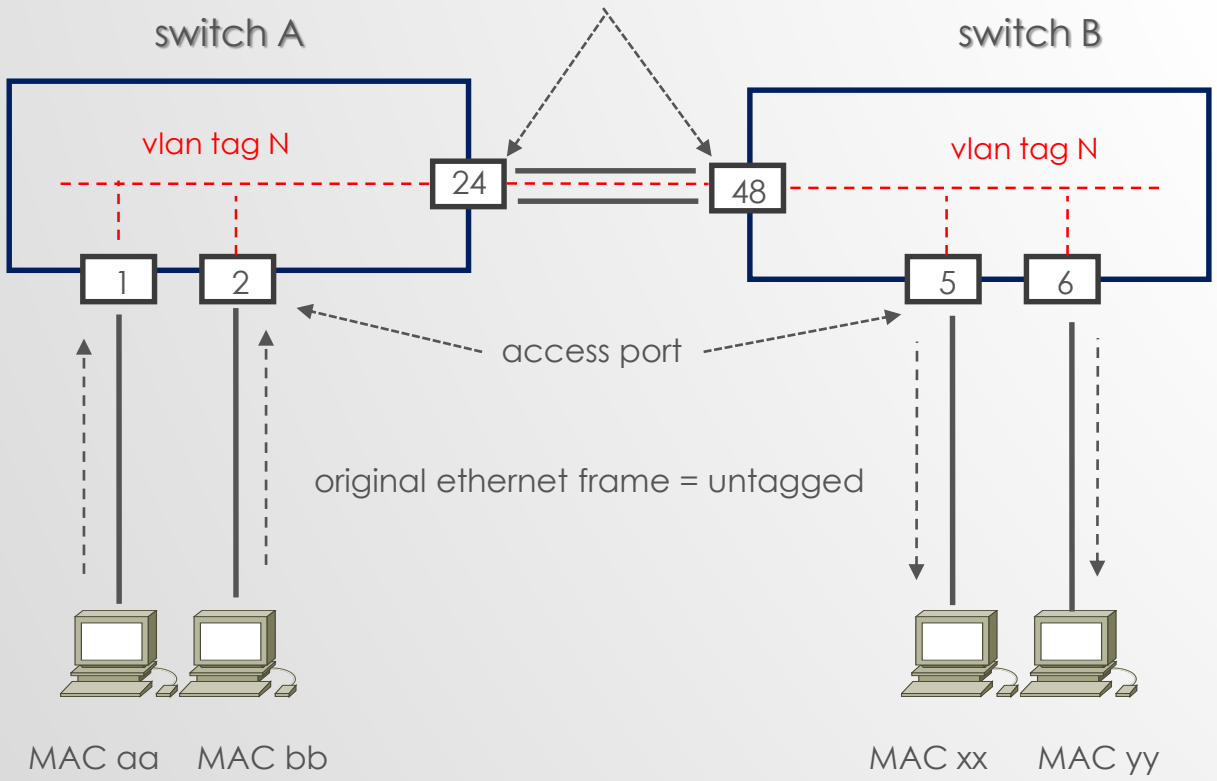
CFI: indica se i MAC address della frame sono in forma canonica

VLAN-ID: assume un valore numerico in un range sino a 4096 possibili segmenti logici di rete.

# UNTAGGED VS TAGGED PORTS

| MAC | PORTS |
|---|---|
| aa | 1 |
| bb | 2 |
| xx | 24 |
| yy | 24 |

| MAC | PORTS |
|---|---|
| xx | 5 |
| yy | 6 |
| aa | 48 |
| bb | 48 |




Le porte in **access mode** sono di tipo **untagged**

Le porte in **trunk mode** sono di tipo **tagged**

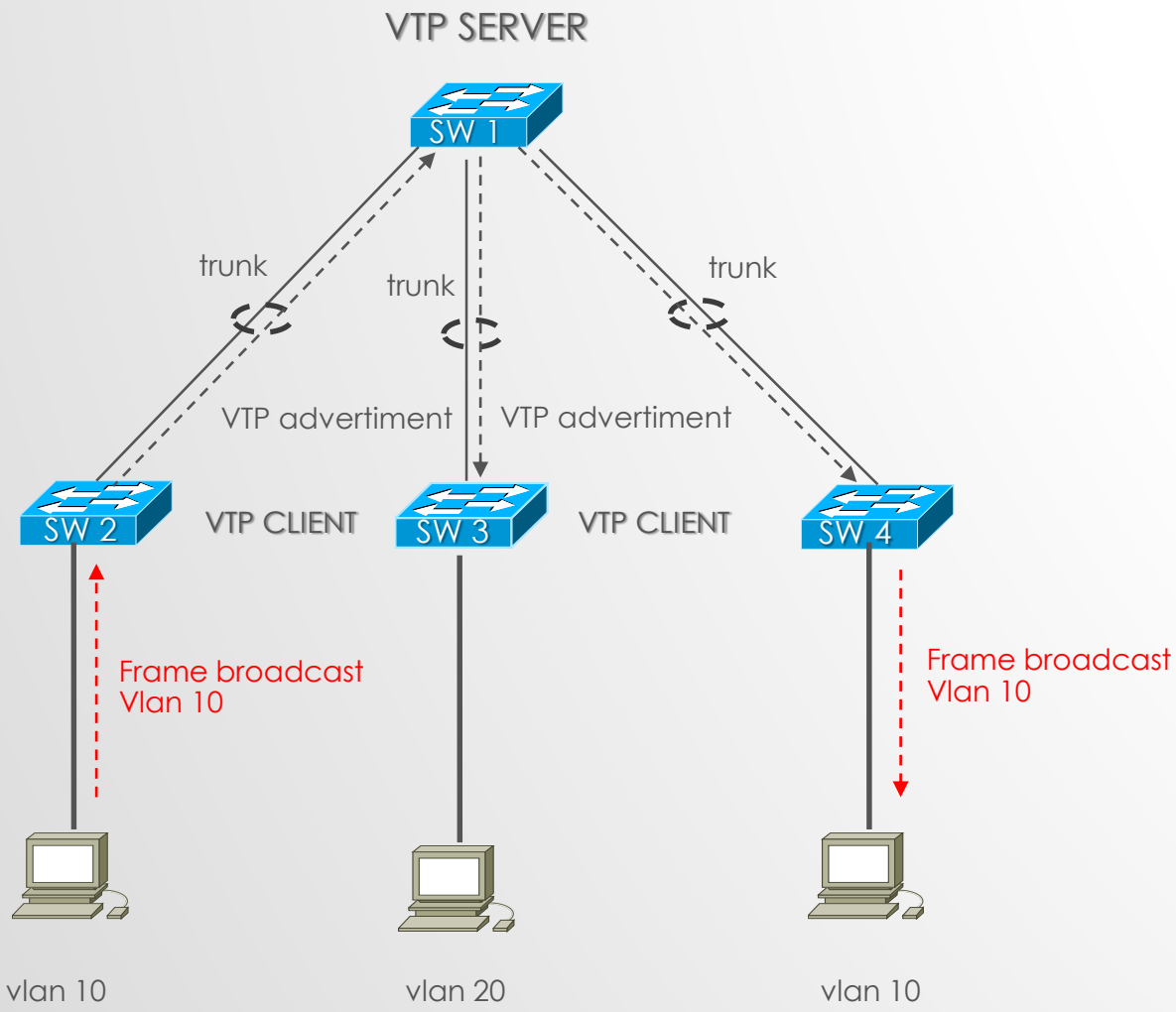
Gli switch trasmettono e ricevono frame ethernt sulla base della loro MAC table address

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.

# VTP VLAN TRUNKING PROTOCOL




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

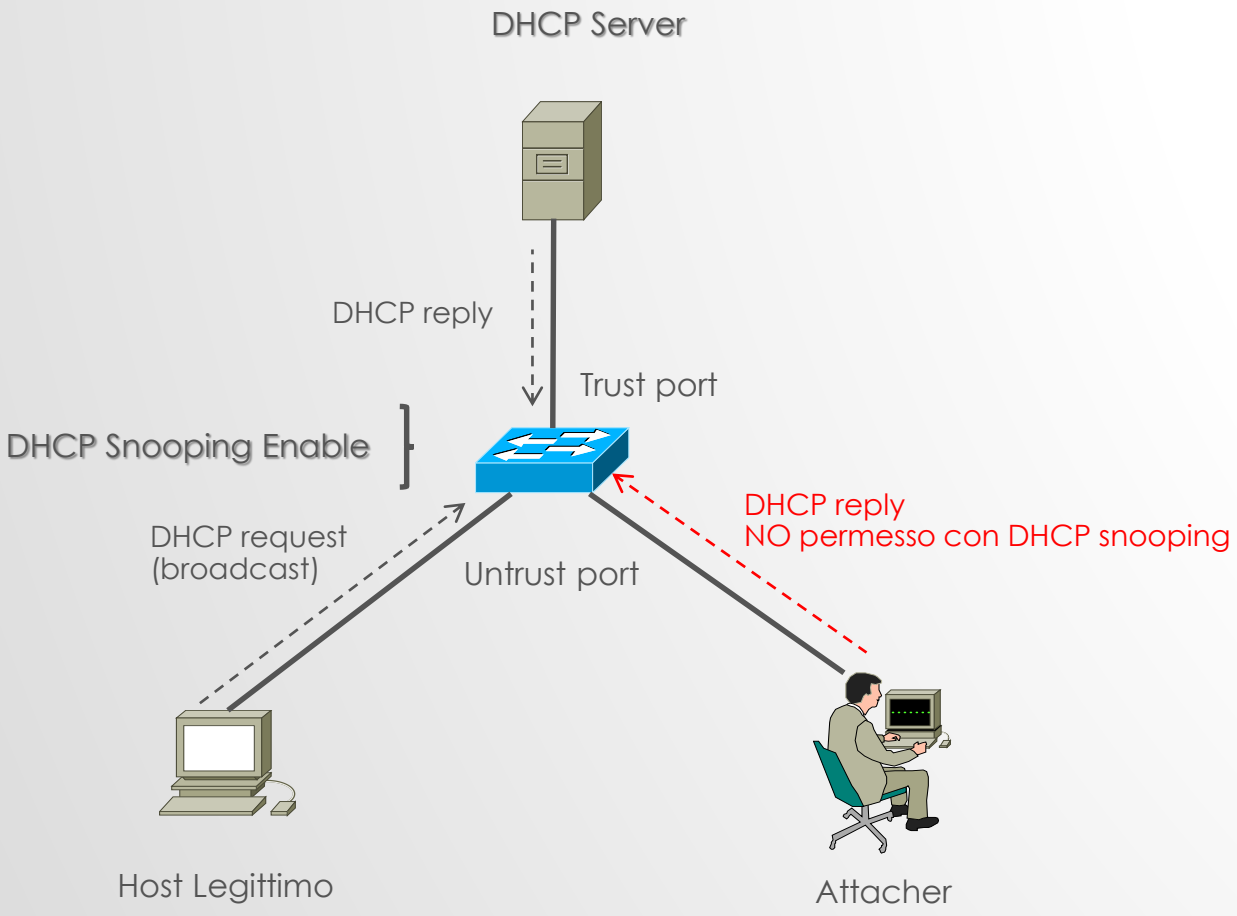
Server Mode: può creare, modificare, eliminare vlans e decidere nuovi parametri di configurazione come ad esempio version e pruning per tutto il dominio VTP; VTP server annuncia e sincronizza tutto il vlans database a tutti gli switches client dello stesso dominio VTP attraverso gli advertisement ricevuti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

.

# DHCP SNOOPING



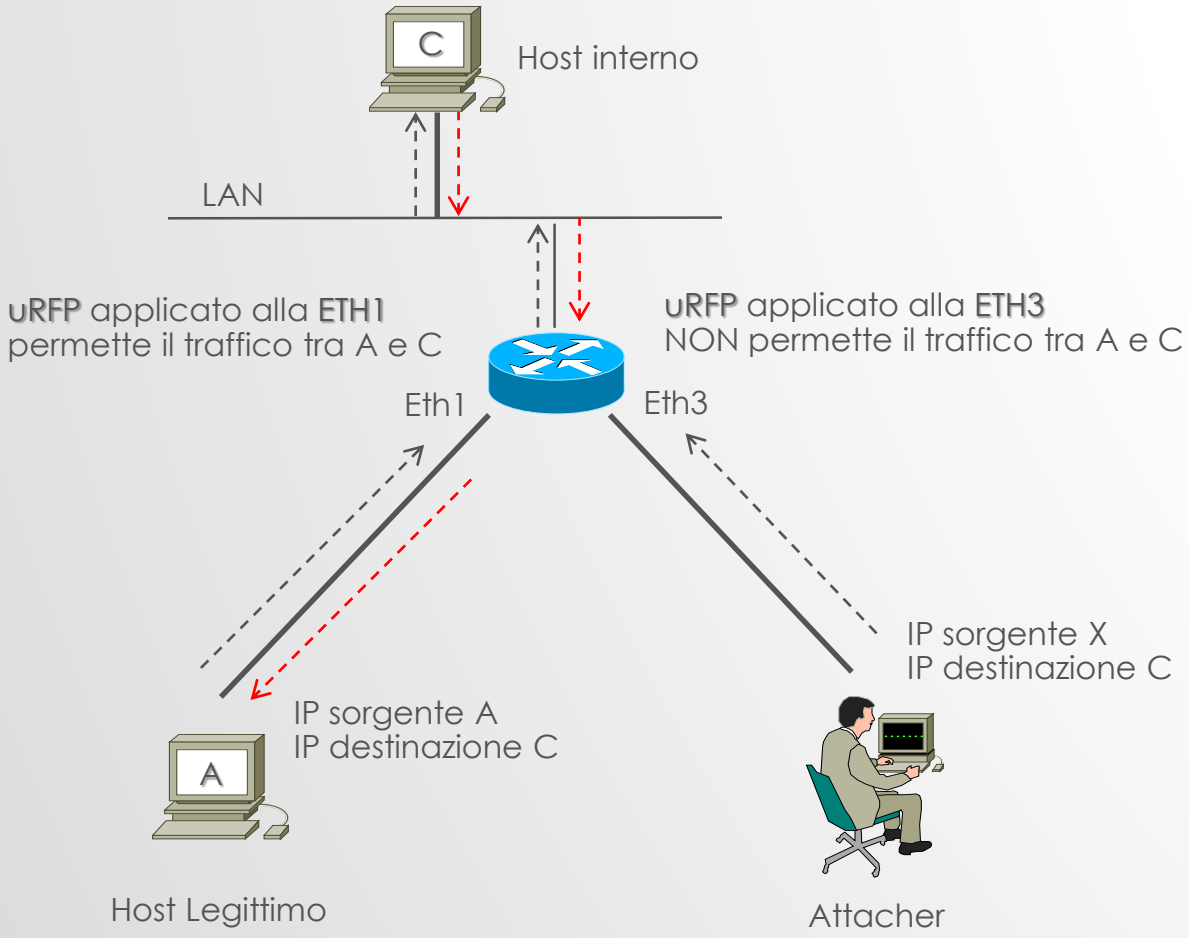

DHCP Snooping è una tecnica di sicurezza attraverso il filtering di DHCP messages ed attraverso un database che permette il controllo di questi messaggi ed accessi

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)

# IP SOURCE GUARD AND UNICAST RPF (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

# MAC ADDRESS LIMITING (PORT SECURITY)

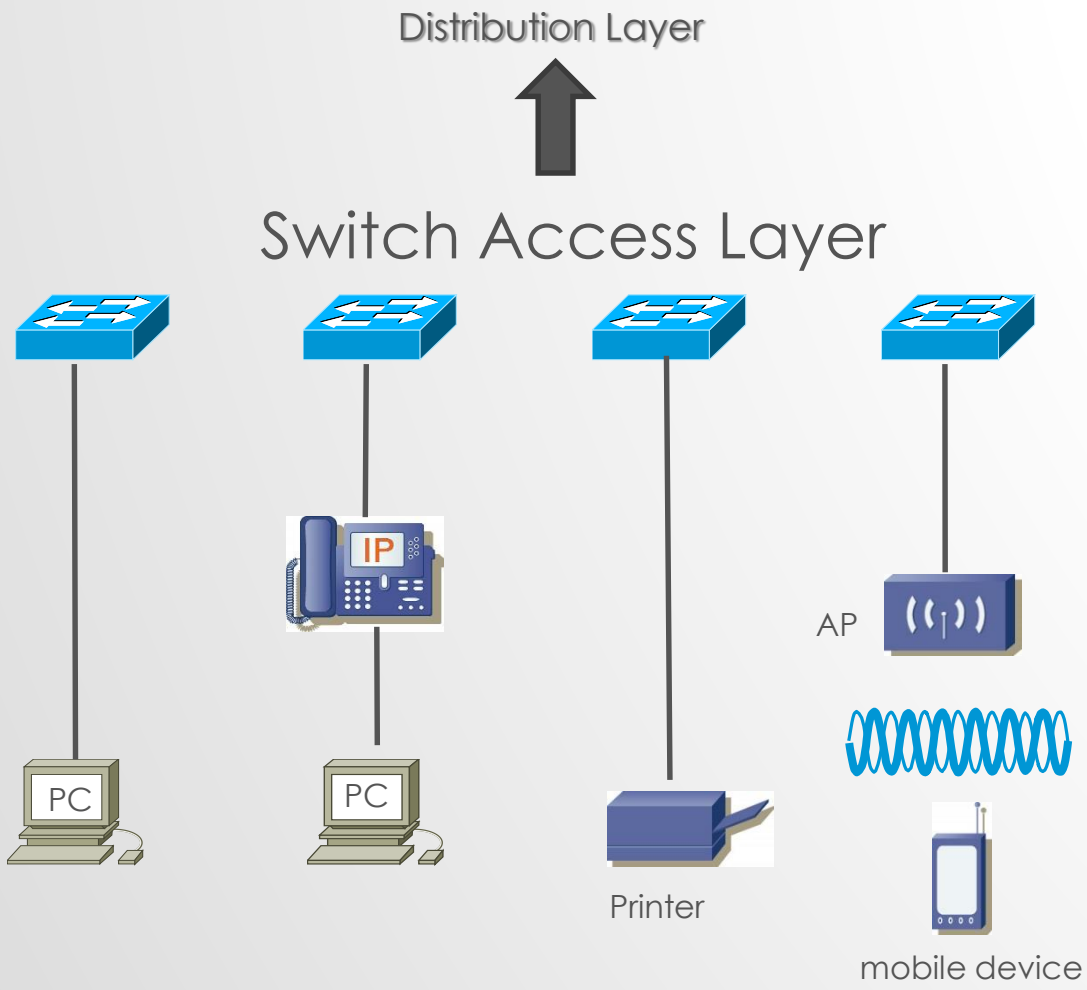

```
interface gigabitethernet 1/10
switchport mode access
switchport port-security mac-address sticky
---
switchport port-security maximum  <value>
---
switchport port-security violation  [ restriction  |  shutdown ]
```

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.

# 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

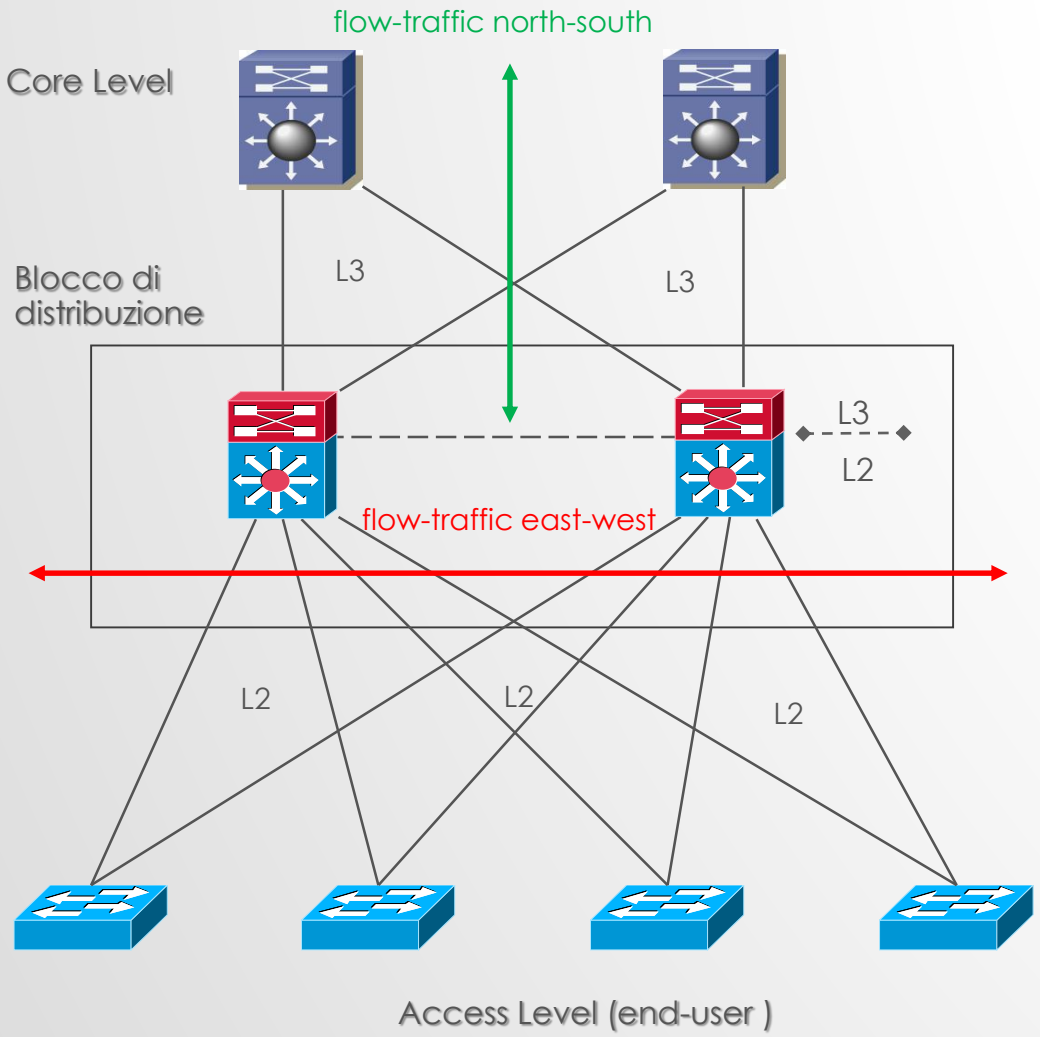
**Security and Network Identity:** 802.1x, port-security, DHCP snooping, IBNS (Identity Base Network Services) , IPSG (IP source-guard), Web-Auth, DAI (Dynamic ARP Inspection)

**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)

# DISTRIBUTION LEVEL



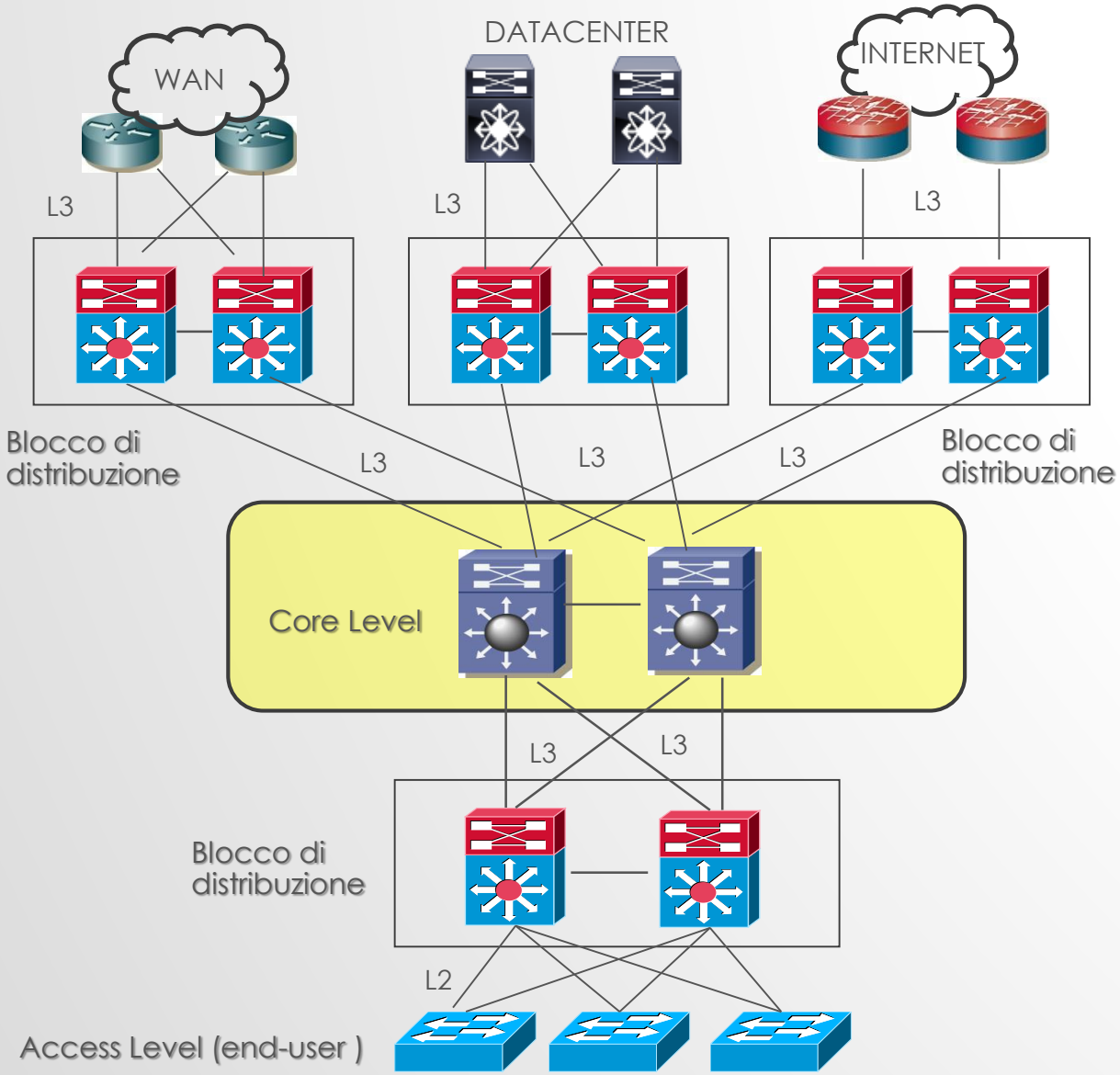

**Distribution Level:** è il livello che consente un punto di aggregazione tra il livello di accesso (end-user) ed il livello di core (external domain)

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

# 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,