Switching Junos Course

Massimiliano Sbaraglia

Junos Devices Architectures Control-Plane,Data-Plane and command cli base

Massimiliano Sbaraglia

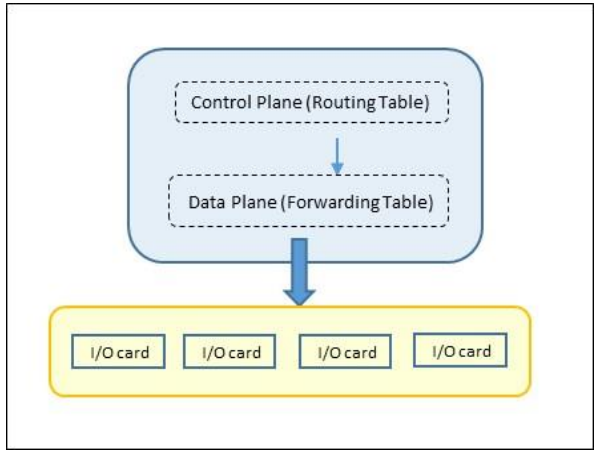
Junos Device Architecture

Come regola generale Juniper condivide la stessa architettura attraverso un sistema di Control-Plane e Forwarding-Plane a volte separato via hardware (ad esempio nella M-series multiservices edge router: from M5 to M320, M7i) ed a volte via software (ad esempio nella J-series i quali possono essere utilizzati in HA chassis cluster J2320, J2350, J4350 e J6350).

- Il Control Plane è riferito come Routing Engine (RE)
- Il Data Plane è riferito come Packet Forwarding Engine (PFE)

RE ha come funzione quello di gestione del PFE; questo significa il controllo delle funzionalità software devices, impostare via CLI le operazioni di configurazione, provvede a meccanismi di troubleshooting e mantiene le diverse tabelle di routing (L3) e forwarding (L2) dove quest'ultima poi è indirizzata verso il piano di PFE che provvede alla trasmissione dei pacchetti in esso transitante verso il corretto next-hop.

Junos è il sistema operativo del Juniper devices e lavora su base Free-BSD Kernel (sistema operativo di tipo Berkeley Software Distribution su base Unix,in grado di gestire dischi, memoria, sicurezza ed altro per architetture Intel, AMD64, IA-64, UltraSPARC, PowerPC, etc..)

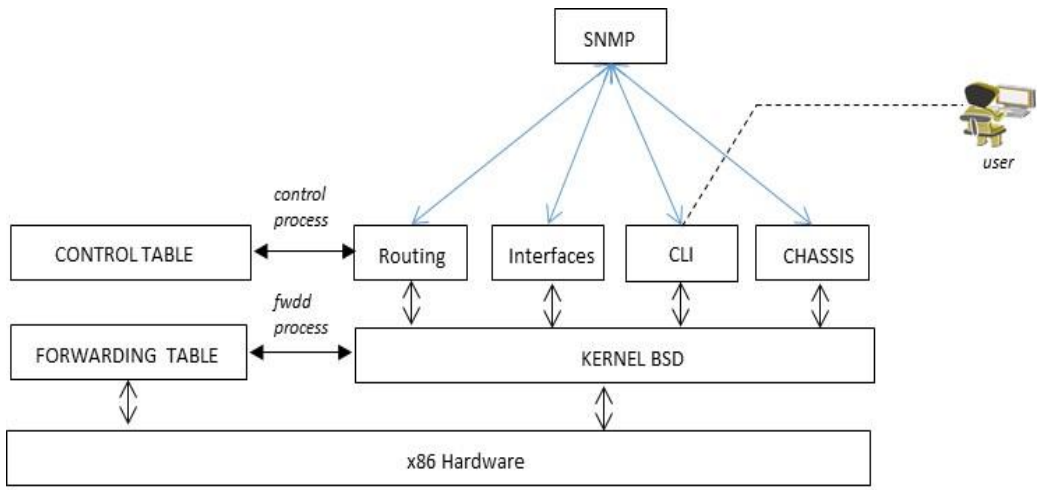


Junos Device Architecture

I processi software presenti sono tutti indipendenti tra loro in modo che qualsiasi problema possa esistere in uno di essi, questo non possa interagire con gli altri.

Attraverso il comando show system processes è possibile vedere una lista completa.

Di seguito un'esempio per il processo SNMP che prende informazioni dai vari processi per interface, chassis e routing table.



Junos Command Configuration

La modalità più comune di configurazione in un Juniper devices è la CLI (Command Line Interface); altre modalità possono essere la web-GUI chiamata jweb.

La CLI ha due opzioni:

- Operational: per la parte di troubleshooting e monitoraggio del software Junos
- Configuration: per la parte di configurazione di ogni componente quale interfacce, protocolli layer 2, protocolli layer 3, policies, etc

L'accesso al devices è possibile via telnet, ssh, console, https, ed il nodo si presente per la versione CLI con un prompt di login; una username ed una password consente il corretto accesso.

login: root

password: no password

!

root@% cli

root@>

La modalità di configurazione viene permessa attraverso il comando edit oppure configure

root@user > configure or edit

root@user #

Junos Command Configuration Base

Tutti i devices Junos hanno necessità di una configurazione iniziale (di default) per il root authentication ed anche per l'hostname, system time, access type (ssh, telnet)

root# edit

root# set system root-authentication plain-text-password

New password: <minimo 6 caratteri>

Retype new password: <minimo 6 caratteri>

root# commit and-quit

commit complete

!

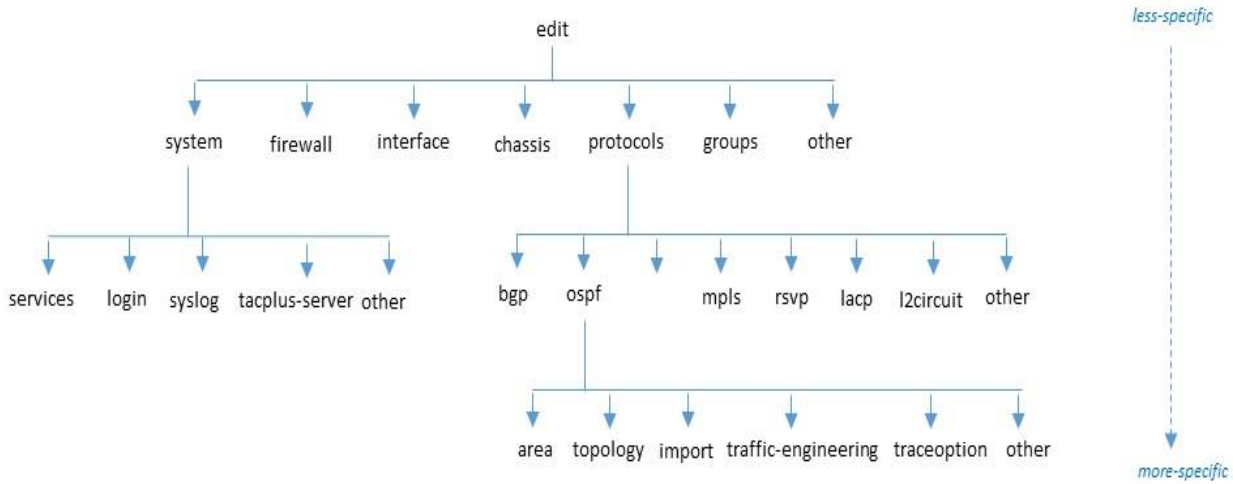
root# edit system

root# set host-name ROUTER1

root@ROUTER1# set time-zone Europe/Rome oppure set time-zone GMT+1

root@ROUTER1# set boot-server <ip_address_NTP boot_server>

root@ROUTER1# set server <ip_address_NTP_server>



Nota:

Il boot-server viene usato per settare il timer locale ad un boot time in modo da garantire che sia abbastanza vicino per sincronizzarsi al server NTP configurato (di default se la differenza tra l'orologio locale e l'orologio del server NTP è maggiore di 128 msec, i timer si sincronizzano lentamente; in caso di > 1000 sec gli orologi non si sincronizzano)

Junos Command Configuration Base

Tutti i devices Junos hanno necessità di una configurazione iniziale (di default) per il root authentication ed anche per l'hostname, system time, access type (ssh, telnet), etc

Servizi di Accesso:

root@ROUTER1# edit system

root@ROUTER1# set services telnet connection-limit 5

root@ROUTER1# set services ssh connection-limit 5

!

Creazione Account:

root@ROUTER1# edit system login

root@ROUTER1# set user massimiliano class ADMIN authentication plain-text-password

New password: <minimo 6 caratteri>

Retype new password: <minimo 6 caratteri>

!

root@ROUTER1# set class ADMIN permission all

Junos Command Configuration

In configuration mode è possibile inserire una determinata configurazione attraverso il comando set ed applicarla al device con il comando commit. Esempio:

root@user # set system hostname R1

Ci sono molte possibilità prima di salvare la configurazione attraverso il comando commit, come ad esempio:

root@R1# commit ?

Possible completions:

<[Enter]>	Execute this command
and-quit	Quit configuration mode if commit succeeds
at	Time at which to activate configuration changes
check	Check correctness of syntax; do not apply changes
comment	Message to write to commit log
confirmed	Automatically rollback if not confirmed
|	Pipe through a command

[edit]

Junos Command Configuration

Il pipe è una funzionalità abbastanza utile per filtrare la visione di una specifica configurazione attraverso il comando show.

root@R1> show configuration | ?

Possible completions:

compare	Compare configuration changes with prior version
count	Count occurrences
display	Show additional kinds of information
except	Show only text that does not match a pattern
find	Search for first occurrence of pattern
hold	Hold text without exiting the --More-- prompt
last	Display end of output only
match	Show only text that matches a pattern
no-more	Don't paginate output
request	Make system-level requests
resolve	Resolve IP addresses
save	Save output text to file
trim	Trim specified number of columns from start of line

Junos Interfaces

Le interfacce in Junos sono generalmente cosi rappresentate:

fxp0: è una interfaccia di management OOB di tipo ethernet; può essere utilizzata anche per trasmettere messaggi di syslog o snmp-traps.

Questa interfaccia è una *nontransit interface*, il che significa che attraverso questa porta non è consentito un passaggio di traffico né in ingresso né in uscita via una qualsiasi porta LAN/WAN.

fxp1: è una interfaccia internal di tipo fastethernet o gigabitethernet tra la RE e la PFE e può essere utile nei casi di troubleshooting per problemi legati al device.

lo0: questa è una interfaccia logica di loopback ed è possibile creare n interface di loopback per differenti motivazione e sotto differenti routing-instances.

sp: questa interfaccia è impiegata per funzionalità quali NAT, IPsec e stateful firewalls.

pimd: questa interfaccia ha un link-level type *PIM-Decapsulator* e permette un ad un multicast rendezvous point di processare PIM register messages.

pime: questa interfaccia ha un link-level type *PIM-Encapsulator* ed è impiegata in multicast per creare un unicast PIM register message da trasmettere al RP.

ipip: questa interfaccia ha un link-level type *IP-over-IP* encapsulation per la creazione di tunnelling IP-in-IP.

dsc: questa è una interfaccia discard ed è impiegata per scartare pacchetti; può essere usata per creare un choke-point per attacchi di tipo DDoS (Denial of Service).

tap: questa interfaccia ha un link-level type *Interface-Specific* ed è utilizzata per il monitoraggio del sistema FreeBSD.

Junos Interfaces

Tutte le versioni Junos applicano una logica per definire la tipologia e la posizione di una interfaccia; in generale questa logica fa riferimento alla sequenza MM-F/P/T

- MM = media type
- F = chassis slot number
- P = PIC slot number
- T = port number

Vediamo ora di chiarire meglio i suddetti punti.

Media Type:

ae: aggregate ethernet definito in IEEE802.3ad.

at: ATM interface ed è abilitata a trasmettere fixed 53-byte cells; di solito utilizzata per ATM over DSL connections.

br: interfaccia utilizzata per ISDN.

Junos Interfaces

e1: standard interface over copper rate 2.048 Mbps (Europe)

e3: standard interface over copper rate 34.368 Mbps (Europe)

t1: standard physical layer interface over digital signal level-1 rate 1.544 Mbps (North-America)

t3: standard physical layer interface over digital signal level-3 rate 44.736 Mbps (North-America)

fe: standard fast-ethernet interface 100 Mbps

ge: standard gigabit-ethernet interface 1 Gbps

xe: standard tengigabit-ethernet interface 10 Gbps

se: standard serial interface EIA530, V35, X21

ct1: standard channelized splitting interface into 24 DSO channels

Junos Chassis hardware

Chassis slot number and PIC slot number:

Il prossimo passo per la interfaccia è la lettera F (vedi sopra) che rappresenta lo chassis slot number rappresentato da un Flexible PIC concentrator (FPC) e la sua posizione, a seconda del modello device, può avere una collocazione fisica all'interno dello chassis orizzontale o verticale.

La parte di PIC slot number rappresentata dalla lettera P, ed è appunto il numero di slot presente all'interno di una FPC ed in generale inizia con zero e finisce con tre.

In caso di posizione verticale dell'FPC la numerazione parte dall'alto con il numero 0 verso il basso con il numero 3, in caso di posizione orizzontale la numerazione parte da destra con il numer 0 e prosegue verso sinistra sino al numero finale 3.

Port number:

L'ultima parte della convenzione è rappresentata dalla lettera T ed indica appunto il numero di porta stessa; il numero di porta dipende anche qui dalla posizione dei componenti FPC/PIC e dal modello di versione del device Juniper.

Esempio

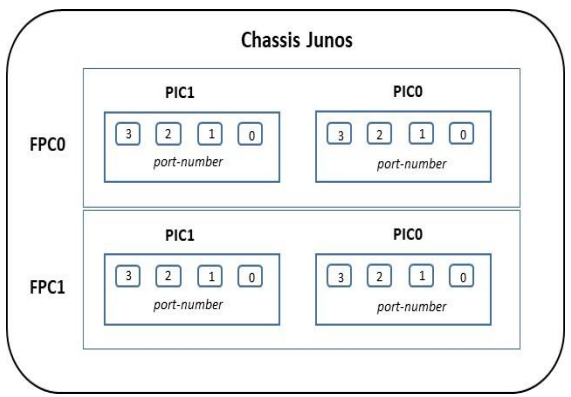
ge-0/0/0 dove:

ge = media-type;

primo 0/ = FPC slot

secondo 0/ = PIC slot

terzo 0 = numero di porta



Junos Chassis hardware

ge-0/0/0.0

infine il .0 alla fine della convenzione rappresenta una unit ed è possibile avere diverse unit per interface

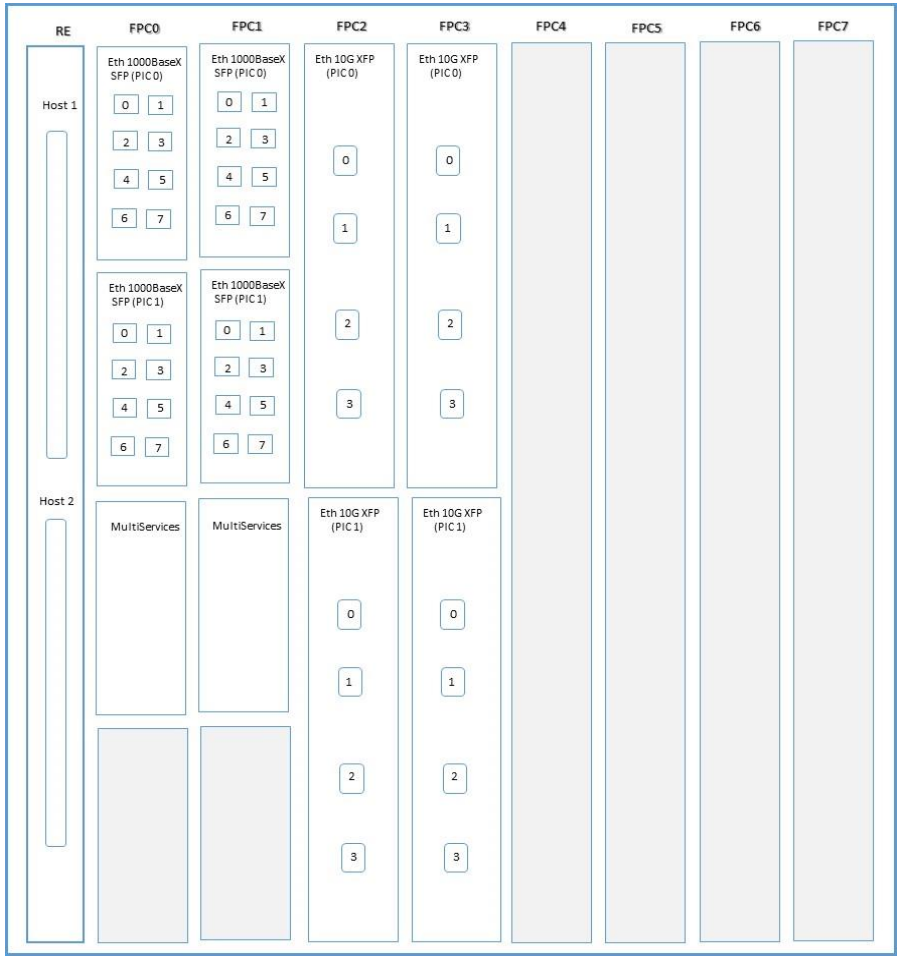
La modalità di *show* fpc-slot pic-status è rappresentato dal seguente output command cli:

root@R1> **show chassis fpc pic-status**

root@R1> **show chassis pic pic-slot 0 fpc-slot 1**

root@R1> **show chassis hardware**

Configurazione hardware T1600 Juniper:



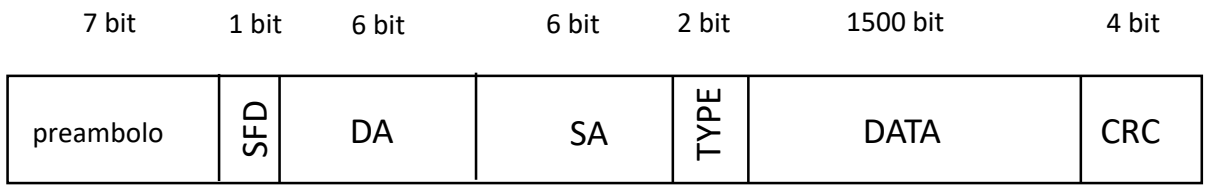
Ethernet Switching, RVI, Bridge-Domain, Virtual-Chassis, Routing-Instance with example configuration L2 and L3-IRB

Massimiliano Sbaraglia

Ethernet Protocol

Ethernet è una frame di livello 2 (data link riferimento modello ISO/OSI) per il trasporto di informazione dati, costituita da:

- Preambolo: ha il compito di sincronizzare mittente e destinatario a livello fisico (valore binario = 10101010)
- SFD: indica l'inizio di una frame ethernet con valore = 10101011
- DA: indica l'indirizzo MAC della parte host destinazione
- SA: indica l'indirizzo MAC della parte host sorgente
- Type: indica il tipo d protocollo utilizzato (802.3 ethernet)
- Data: contiene il carico (payload) dei dati (il contenuto dell'informazione stessa)
- CRC: rappresenta un controllo ciclico che permette la rivelazione di eventuali errori di trasmissione



Original Frame Ethernet

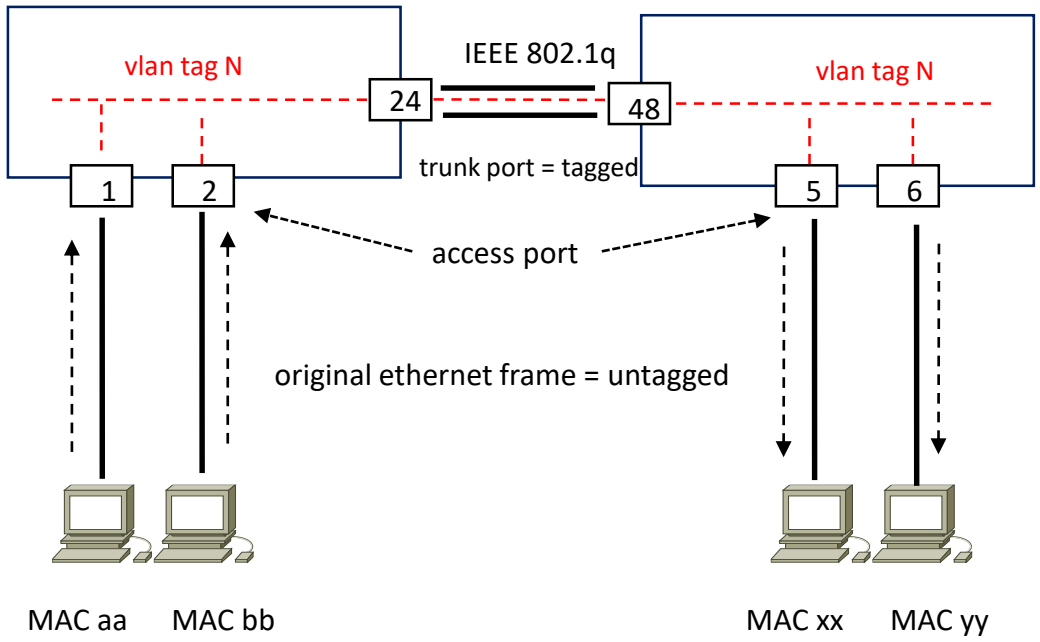
Ethernet Protocol untagged vs tagged

Porte di tipo ACCESS sono untagged, viceversa porte di tipo TRUNK sono tagged

switch A

MAC	PORTS
aa	1
bb	2
xx	24
yy	24

Bridge Table



switch B

MAC	PORTS
xx	5
yy	6
aa	48
bb	48

Bridge Table

Ethernet ARP

ARP è un protocollo per il mapping tra un indirizzo MAC (indirizzo fisico) ed il suo indirizzo IP (layer 3) associato all'interno di un dominio di broadcast (vlan).

Quando un pacchetto entrante è destinato ad una certa destinazione, questo arriva al suo default-gateway che genera una richiesta ARP per trovare il corrispondente indirizzo fisico del nodo destinazione, il quale a sua volta mappa l'indirizzo IP di destinazione indicato dal pacchetto stesso.

Un lookup ARP table è una funzionalità, quindi, utilizzata dal nodo gateway (layer 3) per trovare la corrispondenza IP/MAC (entry) e se questa esiste (match) viene inoltrato il pacchetto nella giusta direzione. Viceversa se non trova il match (no entry), il nodo gateway genera una richiesta ARP broadcast in modo tale che tutti i nodi presenti nella LAN possano verificare se l'indirizzo IP destinazione è presenti in uno degli host e creare cosi la giusta associazione tra sorgente e destinazione (l'host che riconosce come proprio l'indirizzo IP target genera una risposta di conferma).

Il nodo gateway aggiorna la sua cache ARP con la nuova associazione per future comunicazioni.

Un proxy ARP è una funzionalità che abilita un nodo layer 3 a rispondere ad ARP queries per indirizzi IP che sono all'esterno di un determinato segmento di rete vlan. Questo consente un trasporto di pacchetti tra differenti sottoreti.

NOTA:

Segmenti di rete vlan che utilizzano ARP sono soggetti a vulnerabilità (attacchi) conosciuti come ARP spoofing (ARP cache poisoning).

ARP spoofing è appunto una tecnica hacker dove messaggi fasulli in broadcast inviati in un segmento logico di rete (vlan) cercano di stabilire una connessione legittima tra il suo indirizzo IP/MAC con il resto della rete.

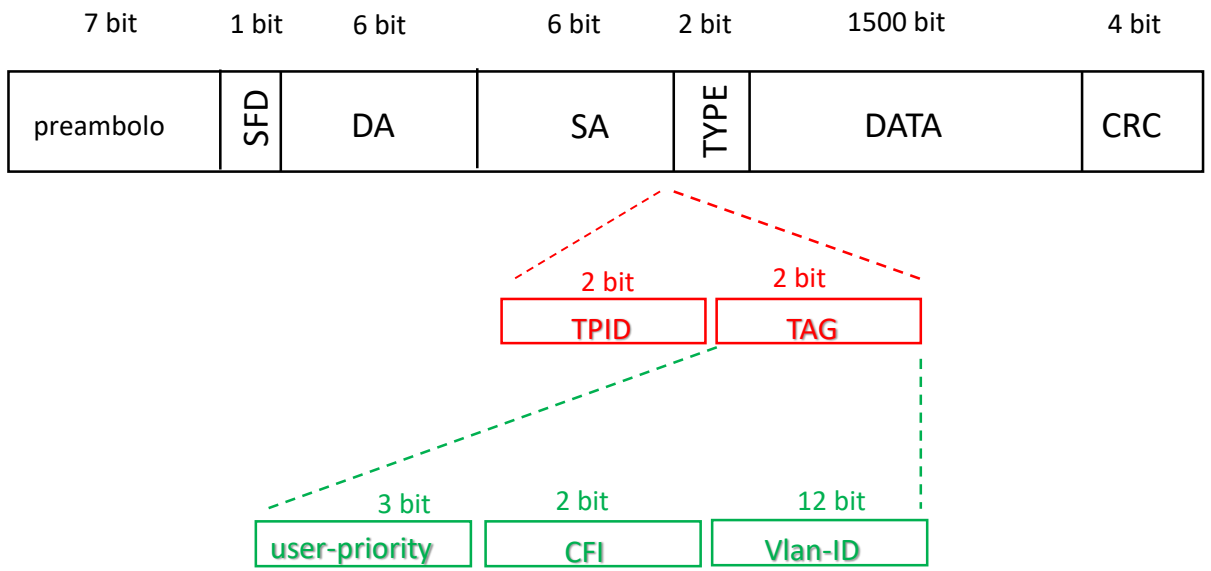
ARP spoofing può seriamente compromettere una intera rete attraverso questi specifici attacchi:

- man-in-the-middle
- denial-of-service
- session hijacking

Ethernet Protocol 802.1q tagging

Ethernet 802.1q è il protocollo che introduce il concetto di vlan (virtual lan) permettendo a questi segmenti logici di rete a condividere lo stesso media fisico.

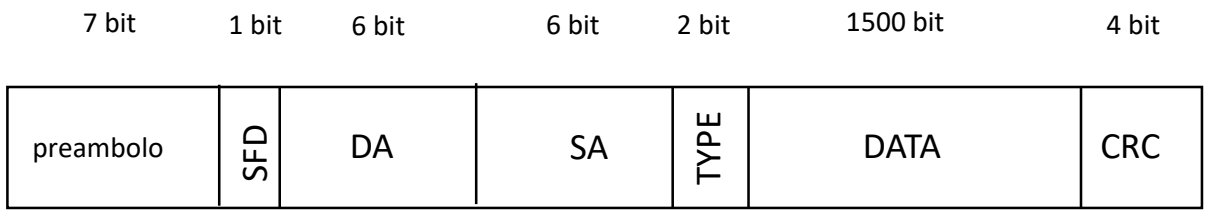
- TPID: indica il tipo di ethertype che assume il valore = 0x8100 per il protocollo 802.1q tagged
- TAG: contiene tre sotto informazioni:
  - User-Priority: indica un livello di priorità della frame; l'utilizzo di questo campo è definito in 802.1p per la classificazione di servizio cos.
  - CFI: indica se i MAC address della frame sono in forma canonica
  - VLAN-ID: assume un valore numerico in un range 1-4096 possibili segmenti logici di rete



Ethernet Protocol QinQ tunneling

E’ una tecnica utilizzata per encapsulare o meglio tunnellizzare un vlan-tag in un secondo vlan-tag all’interno di una frame ethernet; questo permette di separare ad esempio un traffico su base L2VPN utente all’interno di un backbone Services Provider.

E’ molto utilizzato anche in ambienti Data Center multi-tenants dove è prevista una quantità di segmenti vlan molto elevata (sostituita oggi in ambienti Fabric con vxlan)



Original Frame Ethernet

Tag Vlan Customers 802.1q

Tag Vlan Providers Q in Q tunneling

Ethernet Protocol QinQ tunneling

QinQ tunneling è una tecnica di tipo service provider che permette di creare un collegamento layer 2 tra due client sites.

Il Provider può segregare questi clienti in VLAN traffic over link (caso di overlapping vlan-id) oppure aggregate (bundle) differenti Vlan Client all'interno di un singolo Service VLAN.

- C-VLAN (UNI): è il tipo di pacchetto che traversa da un client verso il Provider's VLAN [al tag originale 802.1Q del cliente viene aggiunto il tag vlan 802.1Q (tunneling) del provider]
- S-VLAN (NNI): è il tipo di pacchetto che ha il compito di segregare il traffico del cliente con il proprio originale tag-vlan, grazie alla tecnica di QinQ 802.1Q tunneling che traversa la rete del Provider; in direzione downstream quando il pacchetto arriva al nodo di destinazione della rete Provider, S-VLAN viene rimossa e rilasciato il pacchetto nella sua forma originale.
- E' possibile mappare una C-VLAN verso una S-VLAN (rapporto di 1:1) oppure multiple C-VLAN verso una S-VLAN (rapporto N:1)
    - Access Interface sono le customer-facing ed accettano sia frame tagged che untagged
    - Quando si usa il rapporto N:1 è necessario utilizzare l'opzione native per specificare una S-VLAN per frame untagged e una priority per accettare pacchetti tagged; priority tagged packets hanno un Vlan-Id settato a 0 e il valore di priority può essere configurato attraverso un CoS value)
- Class of Service sono invariati in direzione downstream del pacchetto; in ingresso è possibile copiare priority e CoS settings to S-VLAN
- QinQ tunneling è configurabile solo in una porta in access mode (not trunk)
- MTU ha necessità di essere ridotto in un link access almeno di 4 byte in modo tale che la frame non ecceda il valore di MTU del trunk link quando la S-VLAN viene aggiunta; viceversa il trunk link ha necessità di essere aumentato per una migliore gestione di pacchetti con un frame size largo.
- La tecnica Vlan Translation sostituisce una C-VLAN tag con una S-VLAN tag invece di aggiungerla ed utilizza lo statement «mapping swap» a livello di «edit vlans interface» ed inoltre se la configurazione riguarda il rapporto 1:1 non vi è necessità di includere il comando «dot1q-tunneling» per la configurazione S-VLAN, viceversa con il rapporto N:1 è necessario utilizzare il comando «dot1q-tunneling»
- [EX] VLAN Translation (juniper.net)

Ethernet Protocol QinQ tunneling VLAN Tag Translation

A partire dalla release 14.1X53-D40, è possibile utilizzare la tecnica di Dual Vlan Tag Translation (anche conosciuta come Vlan Tag Rewrite) che permette l'ingresso di pacchetti di tipo single-tag, dual-tag ed untagged.

Operation	Function
swap-push	swap a VLAN tag and push a new VLAN tag
pop-swap	pop an outer Vlan tag and swap an inner Vlan tag
swap-swap	swap both outer and inner Vlan tags

[Configuring Q-in-Q Tunneling and VLAN Q-in-Q Tunneling and VLAN Translation | Junos OS | Juniper Networks]

Esempio di Config on PE Junos:

set interface ge-2/0/1 unit 1010 encapsulation vlan-ccc *# ccc = L2VPN circuit cross-connect specifica per un collegamento PE-CE*

set interface ge-2/0/1 unit 1010 vlan-id 1010

set interface ge-2/0/1 unit 1010 input-vlan-map swap

set interface ge-2/0/1 unit 1010 input-vlan-map vlan-id 2020

set interface ge-2/0/1 unit 1010 output-vlan-map swap

Verifica:

show interface ge-2/0/1.1010 | match vlan

VLAN-Tag [0x8100.1010]

In (swap-swap .2020) Out (swap-swap . 1010)

Encapsulation: VLAN-CCC

Bridging Mechanism

Ethernet Switching oppure Ethernet Lan, indica un meccanismo di Bridging (IEEE 802.1D-2004) attraverso il quale uno switch costruisce una tabella di forwarding (bridge table) basata su indirizzi MAC (Media Access Control), per mezzo di un processo di Learning and Forwarding state.

- Il processo di Learning consiste nell'imparare da parte dello switch indirizzi MAC dei nodi ad esso collegati.
- Il processo di Forwarding è utilizzato dallo switch per trasmettere traffico da una interfaccia di incoming verso una interfaccia di outcoming guidandolo verso la destinazione.
- Il processo di Flooding è un meccanismo trasparente utilizzato per trasmettere pacchetti di tipo unknown MAC addresses.
- Il processo di Filtering è un meccanismo per limitare il traffico all'interno del proprio dominio di broadcast (VLAN).
- Il processo di Aging permette di avere nella propria tabella MAC solo indirizzi attivi.

BRIDGING MECHANISM				
Learning	**Forwarding**	**Flooding**	**Filtering**	**Aging**

Ethernet Switching Configuration Access and Trunk mode (EX-series)

Configurazione Switch:

```
root@vQFX-RE1> show configuration vlans VL100 | display set
set vlans VL100 vlan-id 100
!
root@vQFX-RE1> show configuration interfaces xe-0/0/3 | display set
set interfaces xe-0/0/3 unit 0 family ethernet-switching interface-mode access
set interfaces xe-0/0/3 unit 0 family ethernet-switching vlan members VL100
!
root@vQFX-RE1> show configuration interfaces xe-0/0/4 | display set
set interfaces xe-0/0/4 unit 0 family ethernet-switching interface-mode access
set interfaces xe-0/0/4 unit 0 family ethernet-switching vlan members VL100
!
root@vQFX-RE1> show configuration interfaces xe-0/0/0 | display set
set interfaces xe-0/0/0 unit 0 family ethernet-switching interface-mode trunk
set interfaces xe-0/0/0 unit 0 family ethernet-switching vlan members VL100
```

Ethernet Switching MAC Table with port access mode (only one switch EX or QFX series)

Verifica Output (tabella MAC Address Learning)

root@vQFX-RE1> show ethernet-switching table

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static, C - Control MAC

SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb MAC)

Ethernet switching table : 2 entries, 2 learned

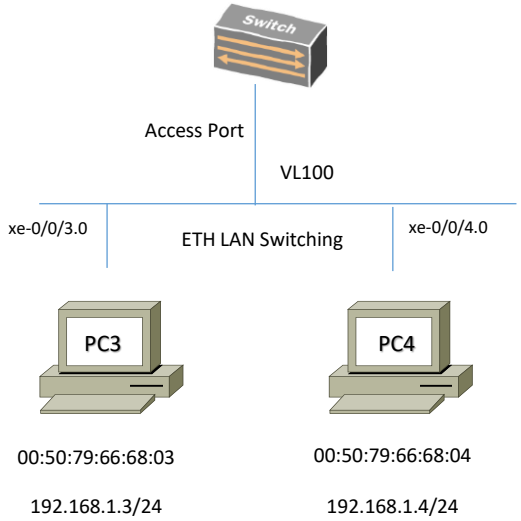
Routing instance : default-switch

Vlan name	MAC address	MAC flags	Age	Logical interface	NH Index	RTR ID
VL100	00:50:79:66:68:03	D	-	xe-0/0/3.0	0	0
VL100	00:50:79:66:68:04	D	-	xe-0/0/4.0	0	0

Nota:

Il processo di MAC Learning può essere disabilitato su ciascuna porta di uno switch EX.

Il comando è: set ethernet-switching-options interface xe-0/0/3.0 no-mac-learning



Ethernet Switching MAC Table with two switch in trunk (EX or QFX series)

Verifica Output (tabella MAC Address Forwarding and Flooding process)

root@vQFX-RE1> show ethernet-switching table

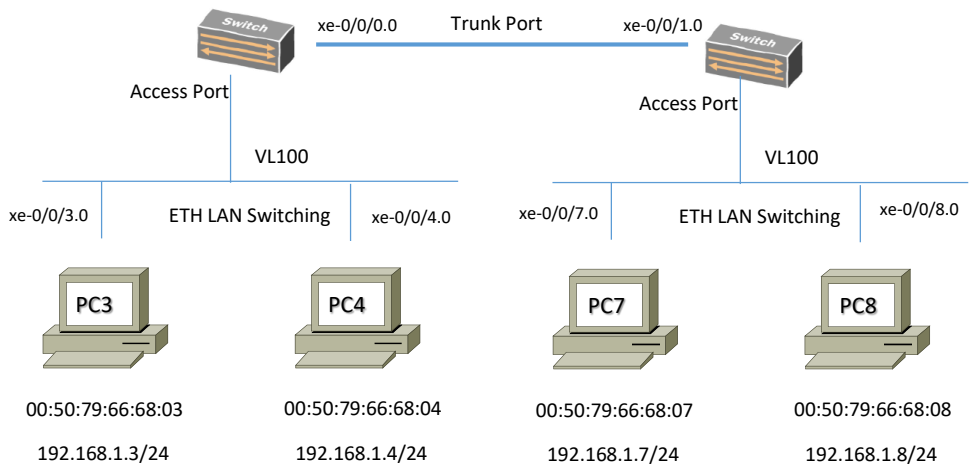
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static, C - Control MAC

SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb MAC)

Ethernet switching table : 4 entries, 4 learned

Routing instance : default-switch

Vlan name	MAC address	MAC flags	Age	Logical interface	NH Index	RTR ID
VL100	00:50:79:66:68:03	D	-	xe-0/0/3.0	0	0
VL100	00:50:79:66:68:04	D	-	xe-0/0/4.0	0	0
VL100	00:50:79:66:68:07	D	-	xe-0/0/0.0	0	0
VL100	00:50:79:66:68:08	D	-	xe-0/0/0.0	0	0



Nota:

Il processo di Forwarding è utilizzato per trasmettere traffico da una interfaccia di ingress ad una di egress verso la corretta destinazione consultando la sua bridge table.

Se la destinazione ha un indirizzo di tipo unknow, lo switch esegue il processo di flooding, trasmettendo la frame a tutte le porte di tipo outcoming [meno quella da cui ha ricevuto la frame (Ingress interface)]

Ethernet Switching MAC Table with two switch in trunk (EX or QFX series)

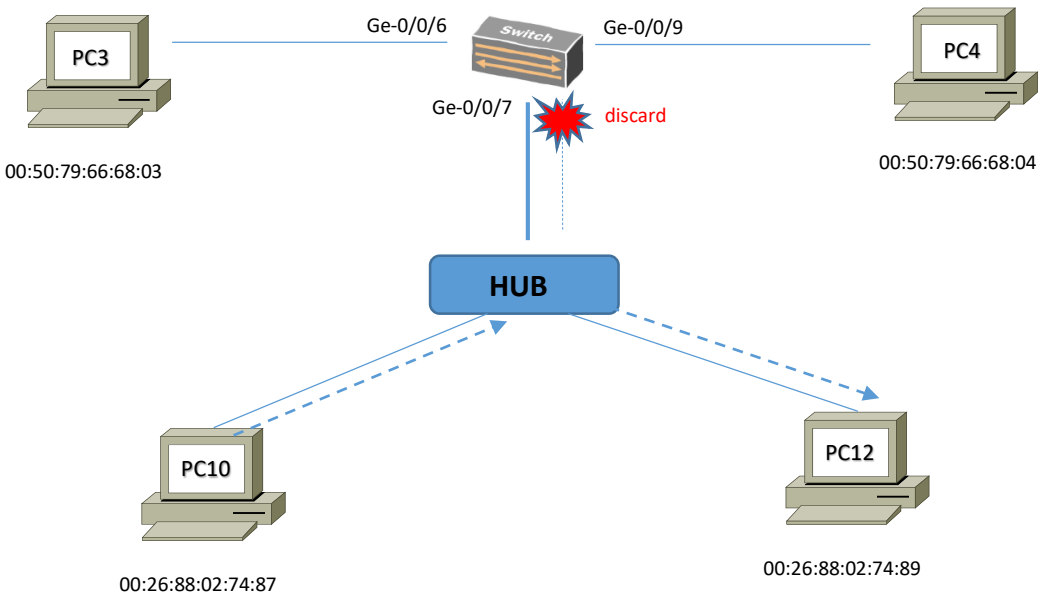
MAC Address Filtering Mechanism

Il processo di Filtering è impiegato per limitare traffico da associare ad una determinata porta.

In questo esempio lo switch evidenzia il processo di filtering associato al traffico con sorgente il PC10 e con destinazione il PC12.

Poiché la destinazione è associata alla stessa porta attraverso la quale ha ricevuto il pacchetto, lo switch consultando la sua bridge table decide di filtrare e/o scartare (drop) il pacchetto.

MAC ADDRESS	Interface
00:50:79:66:68:03	Ge-0/0/6
00:50:79:66:68:04	Ge-0/0/9
00:26:88:02:74:87	Ge-0/0/7
00:26:88:02:74:89	Ge-0/0/7



Ethernet Switching MAC Table with two switch in trunk (EX or QFX series)

MAC Address Aging Mechanism

Il processo di Aging è utilizzato da uno switch per assicurare che solo i MAC address attivi sono presenti nella sua bridge table.

Per ogni MAC address presente nella sua tabella, lo switch registra un timestamp da quando l'informazione è stata imparata; ogni volta che lo switch rileva traffico attivo da un MAC address, esso aggiorna il suo timestamp. Un timer periodicamente controlla il timestamp e se questo dovesse risultare vecchio rispetto ad un valore preimpostato da configurazione, lo switch rimuove l'indirizzo di MAC dalla sua bridge table.

Il valore di defaut per l'aging timer = 300 secondi e può essere configurato per tutte le vlans oppure per-vlan base

Comandi:

set ethernet-switching-options mac-table-aging-time < seconds >

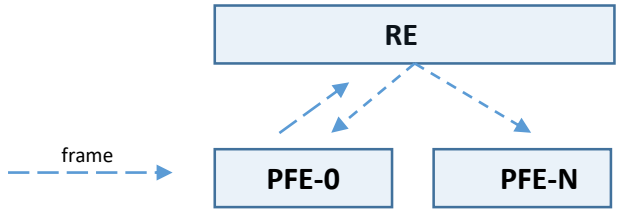
Ethernet Switching MAC Forwarding Table (EX or QFX series)

```
root@vQFX-RE1> show route forwarding-table family ethernet-switching
Routing table: __juniper_private1__.bridge
VPLS:
Destination        Type RtRef Next hop           Type Index    NhRef Netif
default            perm     0                    dscd   241    1

Routing table: default-switch.bridge
VPLS:
Destination        Type RtRef Next hop           Type Index    NhRef Netif
default            perm     0                    dscd  1686    1
xe-0/0/3.0         intf     0                    ucst  1729    4 xe-0/0/3.0
xe-0/0/4.0         intf     0                    ucst  1730    4 xe-0/0/4.0
xe-0/0/0.0         intf     0                    ucst  1734    5 xe-0/0/0.0

Routing table: default-switch.bridge
Bridging domain: VL100.bridge
VPLS:
Enabled protocols: Bridging, ACKed by all peers,
Destination                Type RtRef Next hop           Type Index    NhRef Netif
00:50:79:66:68:03/48       user     0                    ucst  1729    4 xe-0/0/3.0
00:50:79:66:68:04/48       user     0                    ucst  1730    4 xe-0/0/4.0
00:50:79:66:68:07/48       user     0                    ucst  1734    5 xe-0/0/0.0
00:50:79:66:68:08/48       user     0                    ucst  1734    5 xe-0/0/0.0
```

Frame Processing

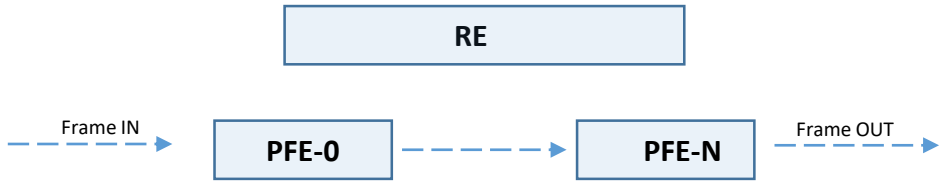
Processing steps for transit frames with an unknow source MAC address

1) Frame enters ingress port and attached ingress PFE
2) Ingress PFE performs a MAC address lookup and determines source MAC is unknow
3) Ingress PFE sends header information to RE, where MAC is added or discarded (MAC limiting)
4) If RE add new source MAC address to bridge table, newly added MAC entry is sent to and programmed into all PFEs



Processing steps for transit frames with an know destination MAC address

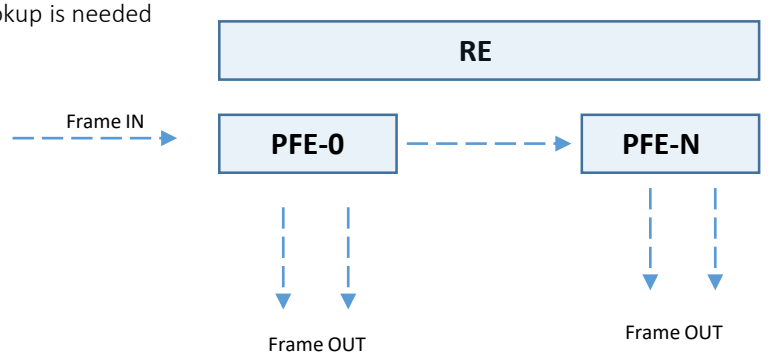
1) Frame enters ingress port and attached ingress PFE
2) Ingress PFE performs a MAC address lookup and determines the egress PFE port
3) Ingress PFE forward frame to egress PFE
4) Egress PFE forwards frame out egress port toward destination; no additional lookup is needed



Frame Processing

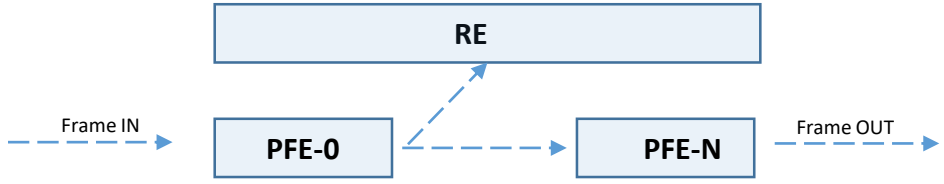
Processing steps for transit frames with an unknow destination MAC address

1) Frame enters ingress port and attached ingress PFE
2) Ingress PFE performs a MAC address lookup, determines no entry exists then replicates frame out to other PFE and all other ports in the same broadcast domain (vlan)
3) All other PFEs replicate frame and forward those frames out all egress ports in the same broadcast domain; no additional lookup is needed



Processing steps for frames destinated to the Switch's MAC address

1) Frame enters ingress port and attached ingress PFE
2) Ingress PFE performs a MAC address lookup. Because the destination MAC address belongs to the switch, PFE performs a Layer 3 lookup:
    a) If the destination IP address belongs to the switch, the decapsulated packet is sent to the RE for processing
    b) If the destination IP address does not belong to the switch, the packet is forwarded to the egress PFE
3) Egress PFE forwards packets out egress port toward destination. No additional lookup is needed



Verifica Interface

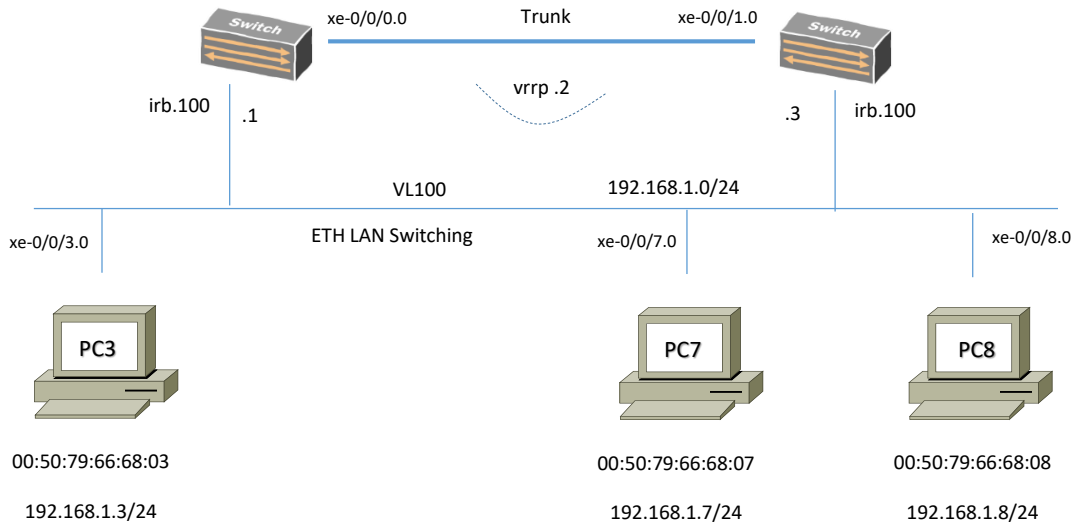
```
root@vQFX-RE1> show interfaces terse | match xe-0/0/3
xe-0/0/3              up    up
xe-0/0/3.0            up    up   eth-switch                    # layer 2 interface è configurata per Ethernet switching protocol

root@vQFX-RE1> show interfaces extensive xe-0/0/3
Physical interface: xe-0/0/3, Enabled, Physical link is Up
  Interface index: 653, SNMP ifIndex: 527, Generation: 144
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
  Duplex: Full-Duplex, BPDU Error: None, Loop Detect PDU Error: None,
  Ethernet-Switching Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Media type: Fiber
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 02:05:86:71:ba:0f, Hardware address: 02:05:86:71:ba:0f
  Last flapped   : 2023-10-02 10:00:30 UTC (2d 22:46 ago)
  Statistics last cleared: Never
```

RVI Routed Vlan Interface (EX series)

Una RVI è una interfaccia logica layer 3 utilizzata da uno switch Junos per ruotare traffico tra vlans; di fatto rappresenta una interface-vlan di Cisco anche conosciuta come SVI.

Questa RVI ha la funzione di IP default-gateway associata ad una determinata vlan e generalmente viene configurata a livello di aggregazione come pure di accesso a seconda delle necessità di progetto; tutti gli switch EX series supportano questa funzionalità .

```
set vlans VL100 vlan-id 100
set vlans VL100 l3-interface irb.100
!
set  interface xe-0/0/3 unit 0 family ethernet-switching vlan members  VL100
set interface xe-0/0/4 unit 0 family ethernet-switching vlan members VL100
!
set interface irb.100 unit 100 family inet address 192.168.1.1/24 vrrp-group 100 virtual-address 192.168.1.2
set interface irb.100 unit 100 family inet address 192.168.1.1/24 vrrp-group 100 priority 110
set interface irb.100 unit 100 family inet address 192.168.1.1/24 vrrp-group 100 accept-data
```

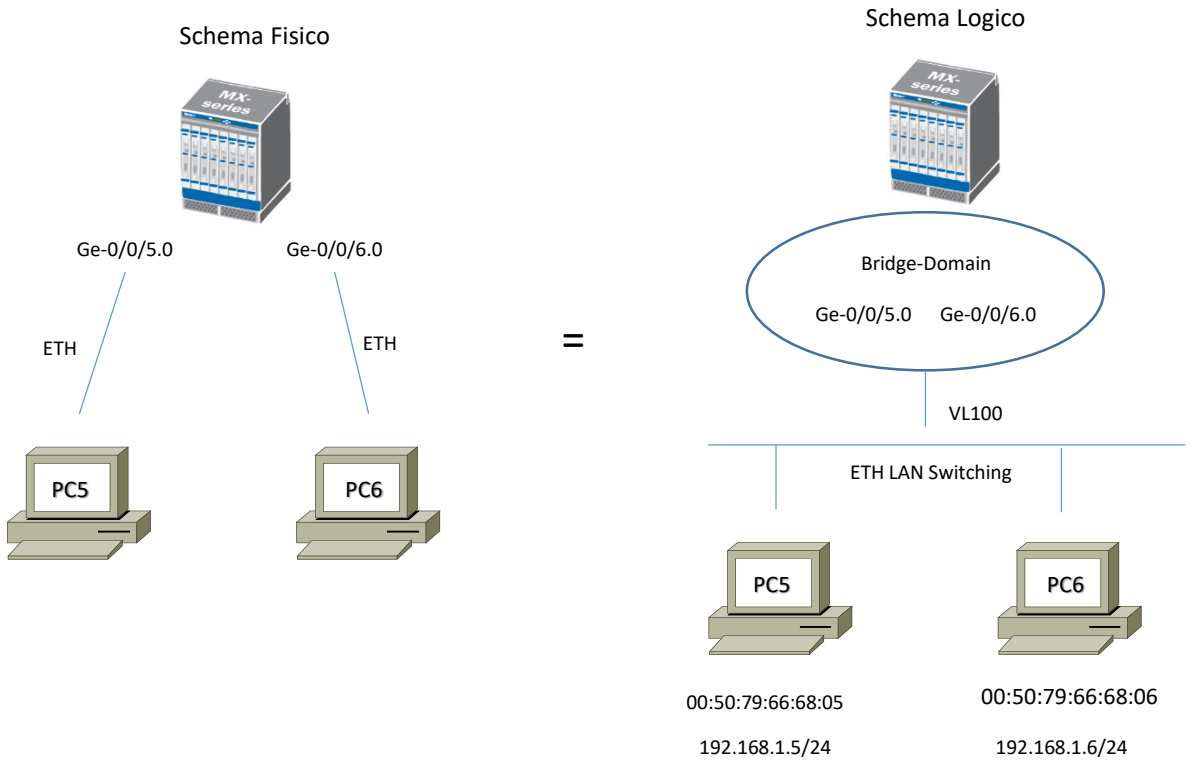


Verifica

```
show interface irb.100 terse
Interface        Admin  Link  Proto   Local    Remote
Vlan             up     up    inet
irb.100          up     up    inet    192.168.1.1
                                       192.168.1.2
```

Bridge-Domain Concept (MX series)

Un Bridge Domain è un set di porte che condividono lo stesso dominio di broadcast anche definito come Virtual-LAN (VLAN); tutte le porte del BD partecipano allo stesso processo di Learning, Forwarding and Flooding.



Bridge-Domain Configuration and MAC-Table (MX series)

```
root@vMX1> show configuration bridge-domains VLAN-100 | display set
set bridge-domains VLAN-100 vlan-id 100

root@vMX1> show configuration interfaces ge-0/0/5 | display set
set interfaces ge-0/0/5 unit 0 family bridge interface-mode access
set interfaces ge-0/0/5 unit 0 family bridge vlan-id 100

root@vMX1> show configuration interfaces ge-0/0/6 | display set
set interfaces ge-0/0/6 unit 0 family bridge interface-mode access
set interfaces ge-0/0/6 unit 0 family bridge vlan-id 100

root@vMX1> show bridge mac-table
MAC flags       (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
    O -OVSDB MAC, SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC, P -Pinned MAC)
Routing instance : default-switch
 Bridging domain : VLAN-100, VLAN : 100
   MAC                 MAC     Logical         NH     MAC         active
   address             flags   interface       Index  property    source
   00:50:79:66:68:05   D       ge-0/0/5.0
   00:50:79:66:68:06   D       ge-0/0/6.0
```

Bridge-Domain another kind of Configuration (MX series)

root@vMX1> show configuration bridge-domains | display set

set bridge-domains VLAN-100 domain-type bridge

set bridge-domains VLAN-100 interface ge-0/0/5.0

set bridge-domains VLAN-100 interface ge-0/0/6.0

root@vMX1> show configuration interfaces ge-0/0/5 | display set

set interfaces ge-0/0/5 encapsulation ethernet-bridge

set interfaces ge-0/0/5 unit 0

root@vMX1> show configuration interfaces ge-0/0/6 | display set

set interfaces ge-0/0/6 encapsulation ethernet-bridge

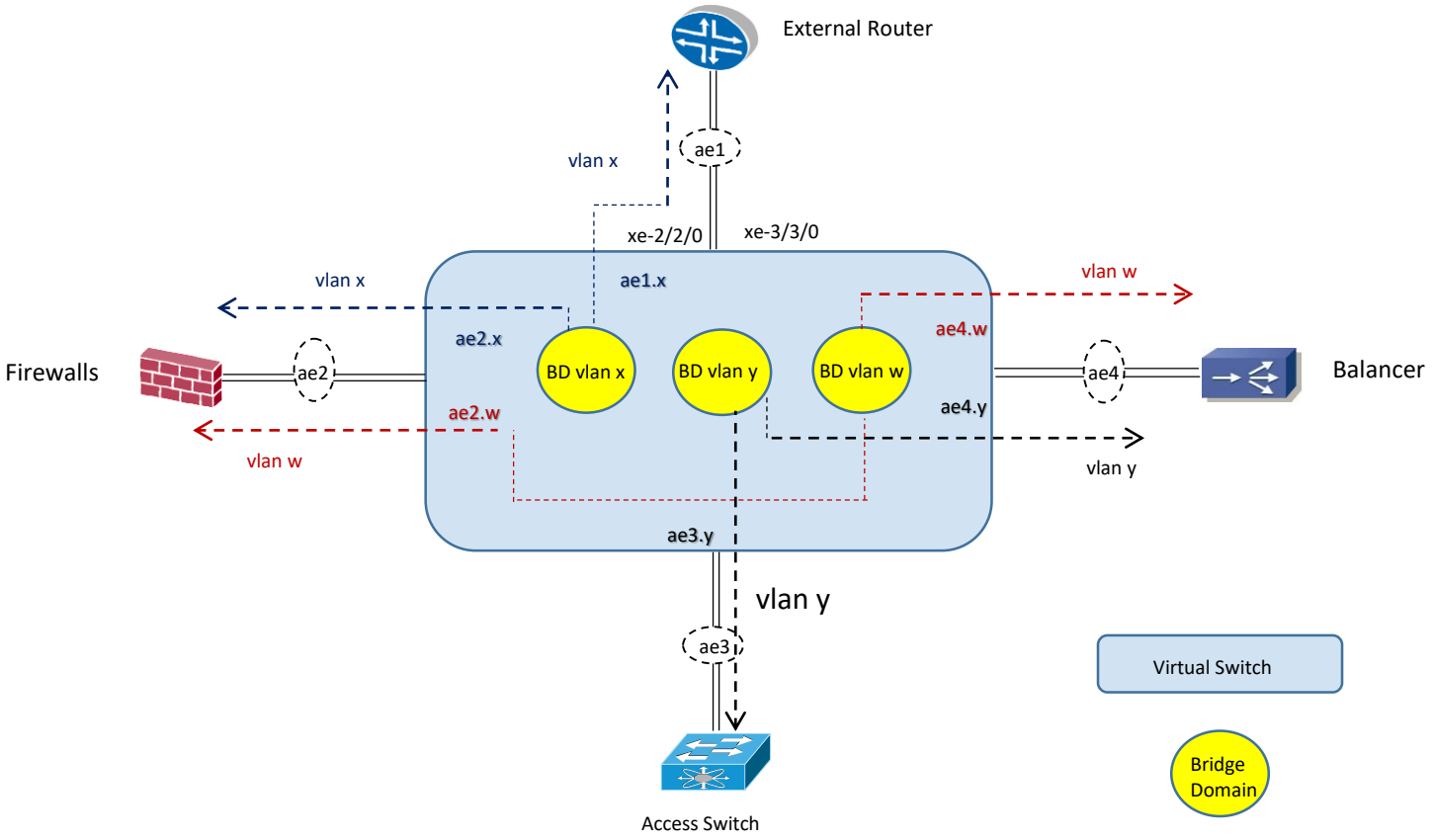
set interfaces ge-0/0/6 unit 0

Anche con questa configurazione abbiamo incluso due interfacce insieme al bridge domain; lo switch tratta queste interfacce sempre come access port e semplicemente trasmette frames tra loro.

Aggregate Ethernet Interface on L2VPN virtual bridge-domain

Un aggregate ethernet indica l'aggregazione di più link fisici ad un gruppo di ethernet interface ablitando così un solo link layer logico conosciuto con il nome di LAG oppure Bundle.

Questo consente connessioni di tipo p2p trunk; di seguito un esempio in termini di design e configuration guide eseguito per un bridge-domain Junos.



Aggregate Ethernet Interface on L2VPN virtual bridge-domain

Configuration Guide AGGREGATE ETHERNET

set chassis aggregate-devices ethernet device-count 10

!

set interface ae1 description «to MX960 External-Router»

set interface ae1 flexible-vlan-tagging

set interfaces ae1 encapsulation flexible-ethernet-services

set interface ae1 aggregate-ether-option link-speed 10g

set interface ae1 aggregated-ether-option lacp active

!

set interface xe-2/2/0 description «to MX960 External-Router interface-a»

set interface xe-2/2/0 gigather-option 802.3ad ae1

set interface xe-3/3/0 description «to MX960 External-Router interface-b»

set interface xe-3/3/0 gigather-option 802.3ad ae1

!

set interface ae1 unit x encapsulation vlan-bridge

set interface ae1 unit x vlan-id x

set interfaces ae1 unit x family bridge

Aggregate Ethernet Interface on L2VPN virtual bridge-domain

Configuration Guide BRIDGE DOMAIN

set routing-instances VSWITCH_CLIENTE instance-type virtual-switch

set routing-instances VSWITCH_CLIENTE bridge-domain VLAN-X interface ae1.x

set routing-instances VSWITCH_CLIENTE bridge-domain VLAN-X interface ae2.x

set routing-instances VSWITCH_CLIENTE bridge-domain VLAN-Y interface ae3.y

set routing-instances VSWITCH_CLIENTE bridge-domain VLAN-Y interface ae4.y

set routing-instances VSWITCH_CLIENTE bridge-domain VLAN-W interface ae4.w

set routing-instances VSWITCH_CLIENTE bridge-domain VLAN-W interface ae2.w

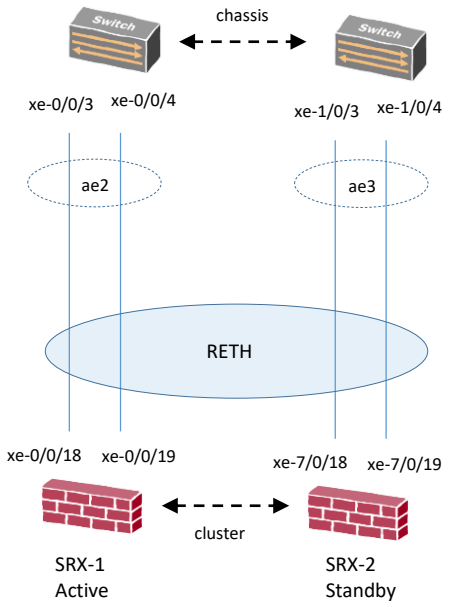
NOTA:

La configurazione per le interfacce fisiche di collegamento verso i firewalls, bilanciatori e switych di accesso hanno gli stessi passi di configurazione previsti nella slide precedente, applicate alle interfacce aggregate ethernet ae2, ae3, ae4

RETH Aggregate Interface

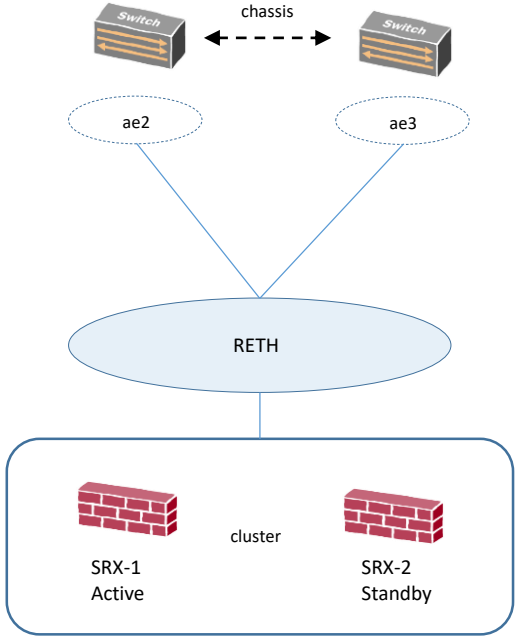
Una RETH (Redundant Ethernet) aggregate interface è una interfaccia che include almeno una porta fisica di due nodi in cluster tra loro.

La reth interface del nodo active è responsabile per il trasporto del traffico (esempi di nodi Juniper in cluster abbiamo la famiglia di SRX). Di seguito vediamo un esempio reale di configurazione tra un cluster di SRX ed una coppia di switch EX in virtual-chassis.



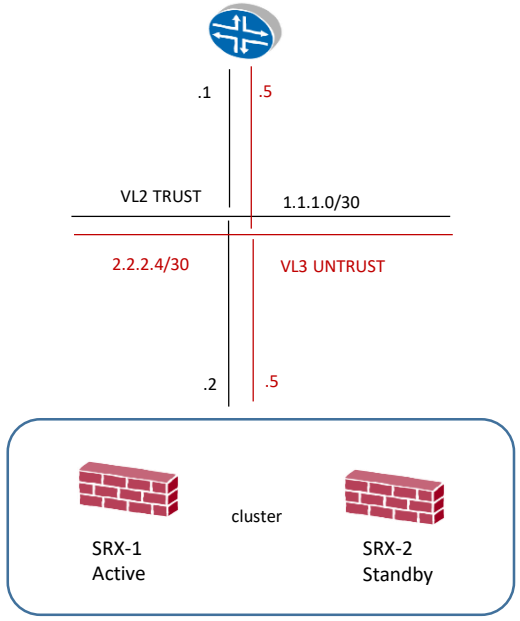
Schema Fisico

=



Schema Logico

=



Schema Logico with Layer 3

RETH Aggregate Interface

EX Switch (virtual-chassis):

```
set interface xe-0/0/3 ether-option 802.3ad ae2
set interface xe-0/0/4 ether-option 802.3ad ae2
set interface xe-1/0/3 ether-option 802.3ad ae3
set interface xe-1/0/4 ether-option 802.3ad ae3
!
set interface ae2 aggregate-eth-option lacp active
set interface ae2 description to-SRX-Node0
set interface ae2 unit 0 family ethernet-switching port-mode trunk
set interface ae2 unit 0 family ethernet-switching vlan members <2-3-4-5>
!
set interface ae3 aggregate-eth-option lacp active
set interface ae3 description to-SRX-Node1
Set interface ae3 unit 0 family ethernet-switching port-mode trunk
set interface ae3 unit 0 family ethernet-switching vlan members <2-3-4-5>
!
```

RETH Aggregate Interface

SRX Firewall (cluster):

```
set interface xe-0/0/18 gigether-option redundant-parent reth1
set interface xe-0/0/19 gigether-option redundant-parent reth1
set interface xe-7/0/18 gigether-option redundant-parent reth1
set interface xe-7/0/19 gigether-option redundant-parent reth1
!
set interface reth1 vlan-tagging
set interface reth1 redundant-ether-option redundancy-group 1
set interface reth1 redundand-ether-option lacp active
!
set interface reth1 unit 2 vlan-id 2
set interface reth1 unit 2 family inet address 1.1.1.2/30
set interface reth1 unit 3 vlan-id 3
set interface reth1 unit 3 family inet address 2.2.2.6/30
!
set security zones security-zone trust host-inbound-traffic system service all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interface reth1.2
!
set security zones security-zone untrust host-inbound-traffic system service all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interface reth1.3
```

Virtual-Chassis Concept (EX and QFX series)

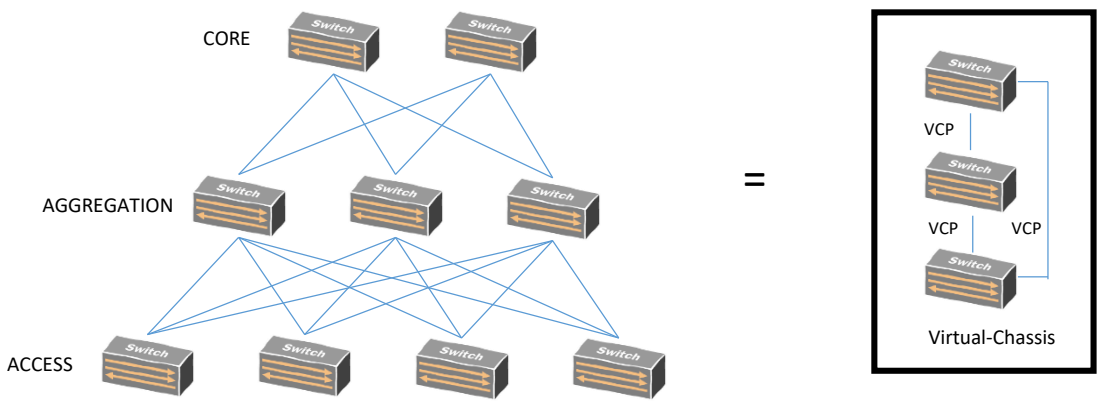
Virtual-Chassis è una tecnologia che dal punto di vista Juniper può essere implementata per combinare funzionalità di vari layers all'interno di un singolo network devices con unica gestione.

I vantaggi di questa tecnologia possono essere:

- Multiple devices sono gestiti come una singola entità logica.
- Aumenta la capacità di fault-tolerant e high availability: in caso di fault di uno dei nodi in VC, il traffico viene rediretto verso altri members switch.
- Semplifica una topologia STP layer 2 (Spanning-Tree) in quanto minimizza oppure elimina il bisogno di prevenzione dei loop, come pure VRRP.
- Provvede ad una maggiore scalabilità di espansione della rete in quanto l'inserimento di un nuovo members switch è semplice ed automatico.

Virtual-Chassis è configurato attraverso l'impiego di EX-series e QFX-series switches; i nodi interconnessi in VC sono chiamati members identificati attraverso un member ID all'interno del Virtual-Chassis

I members comunicano tra loro attraverso VCPs (Virtual Chassis Ports)



Virtual-Chassis Configuration per EX-series

Seguire i seguenti step di configurazione:

1) Enable VCP (VC Ports) per switch members

request virtual-chassis vc-port set fpc-slot 0 pic-slot 1 port 0

request virtual-chassis vc-port set fpc-slot 0 pic-slot 1 port 1

2) Verifica che le porte siano state abilitate correttamente

show virtual-chassis vc-port

3) Verifica che tutti i members switch sono presenti e funzionanti

show virtual-chassis

```
Virtual Chassis ID: c3d2.5525.cd30
Virtual Chassis Mode: Enabled
Mstr                 Mixed Route Neighbor List
Member ID  Status     Serial No       Model           prio  Role        Mode  Mode  ID   Interface
0 (FPC 0)  Prsnt      NW3619450867    ex3400-24p      128   Master*     N     VC    1    vcp-255/1/0
                                                                                   1    vcp-255/1/1
1 (FPC 1)  Prsnt      NW3619451026    ex3400-24p      128   Backup      N     VC    0    vcp-255/1/0
                                                                                   0    vcp-255/1/1
 Member ID for next new member: 2 (FPC 2)
```

Virtual-Chassis Configuration per QFX-series

Con gli switch QFX series possiamo costruire una struttura a Fabric di tipo Spine and Leaf (Clos Fabric)

Le principali funzionalità sono:

- Fabric Multi-Path: il piano di forwarding è regolato tra i nodi dal protocollo SPF (Shortest Path First)
- Intelligent Bandwidth Allocation: il nodo sorgente considera la quantità di banda disponibile per ogni multipath tra uno switch e l'altro, allocando la corretta risorsa end-to-end
- Bidirectional MDT (Multicast Distribution Tree): il VCF calcola multipli alberi multicast in modo bidirezionale ed ottimizza un load-balancing in questi percorsi
- L2 and L3 capability: in base alla licenza adottata, possiamo avere funzionalità layer2 e layer3 per IPv4 e IPv6 (MPLS, BGP, ISIS, etc..) ed inoltre supporta funzionalità quali FCoE, VXLAN, NVGRE, Vmware integration.
- Resiliency and High Availability: include redundant routing-engine in modalità active-backup, redundant data-plane active-active uplinks
- NSSU (No Stop Software Upgrade): disponibile per VCF con doppio RE e consente aggiornamenti software senza interruzioni e/o fault di servizio

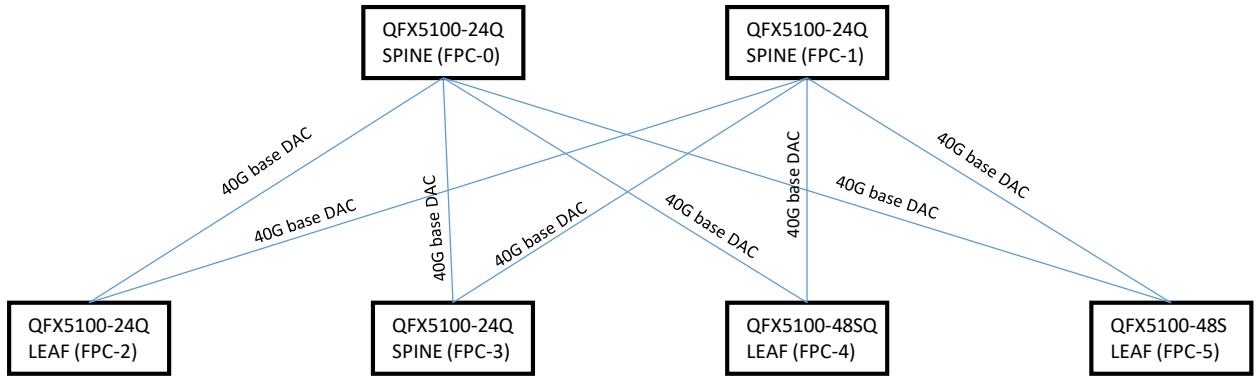
Le modalità di configurazioni prevedono:

- Preprovisioned: con il controllo di ciascun nodo assegnando un member-ID e ruolo.
- Non-provisioned: in questo caso è il nodo master che assegna un member-ID a ciascun switch; il ruolo è determinato dal valore di priority masterschip ed altri fattori che concorrono al ruolo del master.
- Master RE: è il nodo master RE che controlla tutta la Fabric VCF
- Backup RE: il nodo di backup RE resta in standby mode e mantiene lo stato dei protocolli in uso sincronizzato rispetto al nodo master
- Line-Card: a parte gli switch con ruolo master e backup, gli altri switch assumono il ruolo di line-card

Virtual-Chassis Configuration per QFX-series

Con gli switch QFX series possiamo costruire una struttura a Fabric di tipo Spine and Leaf.

```
set virtual-chassis preprovisioned
set virtual-chassis no-split-detection
set member 0 serial-number aaaa1111 role routing-engine
set member 1 serial-number bbbb2222 role routing-engine
set member 2 serial-number cccc3333 role line-card
set member 3 serial-number dddd4444 role line-card
set member 4 serial-number eeee5555 role line-card
set member 5 serial-number ffff6666 role line-card
```



In caso di situazione con un mixed Virtual-Chassis (una combinazione di differenti tipi di switches con eccezione con QFX3500, QFX3600, QFX5110, QFX5100) è richiesto il setting del seguente comando:

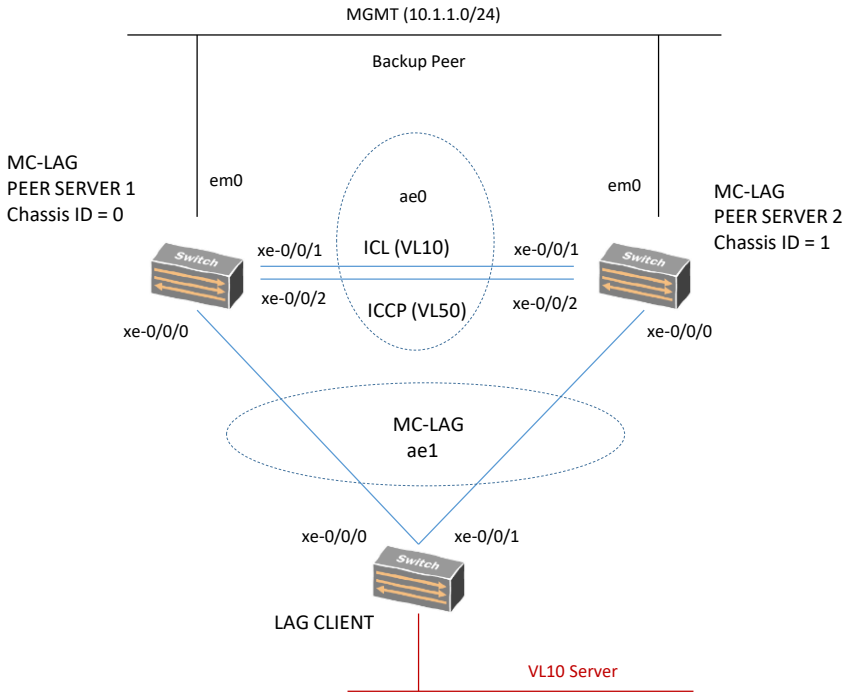
```
request virtual-chassis mode mixed reboot
```

MC-LAG Multichassis Link Aggregation

MC-LAGs groups è un protocollo proprietario Juniper che permette di creare una singola interfaccia logica tra due peer switch Server ed un peer switch Client, provvedendo ad un collegamento in ridondanza ed in load-balancing.

Supporta scenari multihoming e costituisce un loop-free layer 2 network (no Spanning Tree).

MC-LAG utilizza ICCP (Inter-Chassis Control Protocol) per scambiare informazioni e coordinarsi con il suo peer gemello per garantire una corretta trasmissione delle informazioni (forwarding traffic).



MC-LAG Multichassis Link Aggregation Configuration

PEER SERVER 1

set chassis aggregated-devices ethernet device-count 2

set interface xe-0/0/0 ether-option 802.3ad ae1

set interface xe-0/0/1 ether-option 802.3ad ae0

set interface xe-0/0/2 ether-option 802.3ad ae0

set interface ae0 aggregate-ether-option lacp active

set interface ae0 unit 0 family ethernet-switching interface-mode trunk

set interface ae0 unit 0 family ethernet-switching vlan members v10

set interface ae0 unit 0 family ethernet-switching vlan members v50

set interface ae1 aggregate-ether-option lacp active

set interface ae1 aggregate-ether-options lacp system-id aa:bb:cc:dd:ee:ff

set interface ae1 aggregate-ether-options lacp admin-key 3

set interface ae1 aggregate-ether-options mc-ae mc-ae-id 3

set interface ae1 aggregate-ether-options mc-ae redundancy-group 1

set interface ae1 aggregate-ether-options mc-ae chassis-id 0

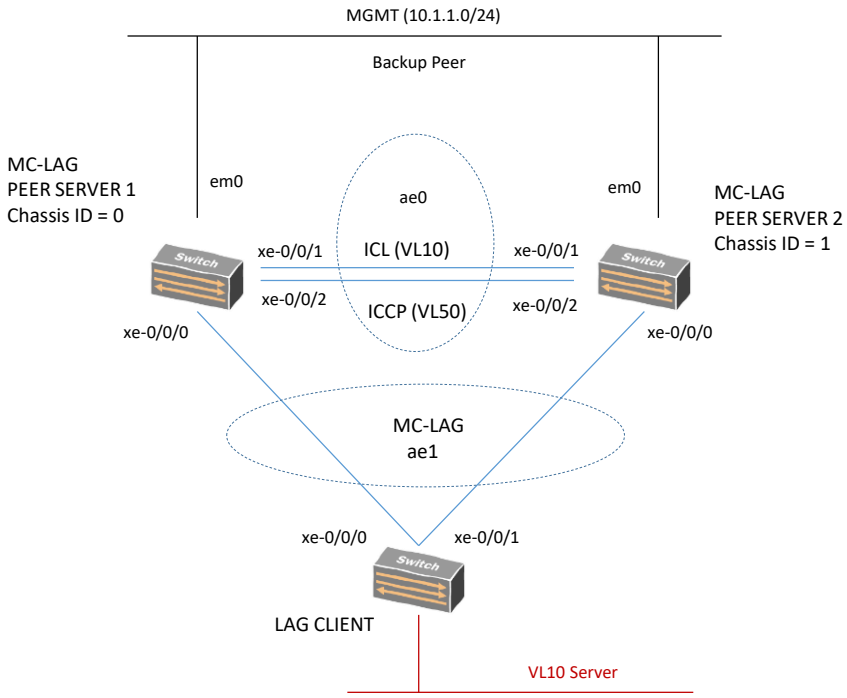
set interface ae1 aggregate-ether-options mc-ae mode active

set interface ae1 aggregate-ether-options mc-ae status-control active

set interface ae1 aggregate-ether-options mc-ae init-delay-time 240

set interface ae1 unit 0 family ethernet-switching interface-mode trunk

set interface ae1 unit 0 family ethernet-switching vlan members v10



MC-LAG Multichassis Link Aggregation Configuration

PEER SERVER 1

set interface em0 unit 0 family inet address 10.1.1.1/24

set interface irb unit 10 family inet address 10.10.10.1/24

set interface irb unit 50 family inet address 10.10.50.1/30

set multi-chassis multi-chassis protection 10.10.50.2 interface ae0

set protocols icpp local-ip-address 10.10.50.1

set protocols icpp peer 10.10.50.2 session-establishment-hold-time 340

set protocols icpp peer 10.10.50.2 redundancy-group-id-list 1

set protocols icpp peer 10.10.50.2 backup-liveness-detection backup-peer-ip 10.1.1.2

set protocols icpp peer 10.10.50.2 liveness-detection minimum-receive-interval 1000

set protocols icpp peer 10.10.50.2 liveness-detection transmit-interval minumum-interval 1000

set switch-option service-id 10

set vlan v10 vlan-id 10

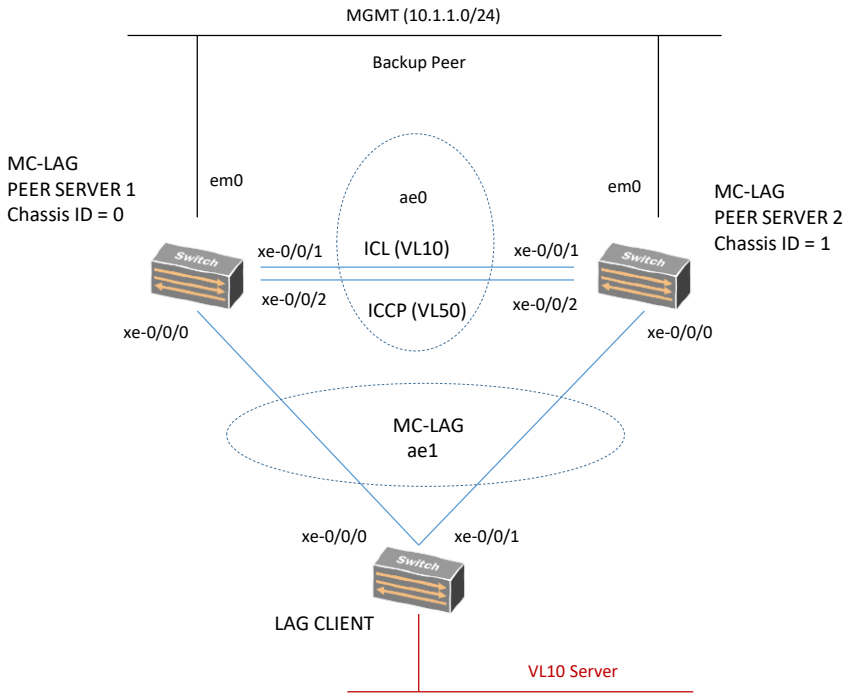
set vlans v10 l3-interface irb.10

set vlan v50 vlan-id 50

set vlans v50 l3-interface irb.50

Nota:

liveness-detection = BFD failure detection



MC-LAG Multichassis Link Aggregation Configuration

PEER SERVER 2

set chassis aggregated-devices ethernet device-count 2

set interface xe-0/0/0 ether-option 802.3ad ae1

set interface xe-0/0/1 ether-option 802.3ad ae0

set interface xe-0/0/2 ether-option 802.3ad ae0

set interface ae0 aggregate-ether-option lacp active

set interface ae0 unit 0 family ethernet-switching interface-mode trunk

set interface ae0 unit 0 family ethernet-switching vlan members v10

set interface ae0 unit 0 family ethernet-switching vlan members v50

set interface ae1 aggregate-ether-option lacp active

set interface ae1 aggregate-ether-options lacp system-id aa:bb:cc:dd:ee:ff

set interface ae1 aggregate-ether-options lacp admin-key 3

set interface ae1 aggregate-ether-options mc-ae mc-ae-id 3

set interface ae1 aggregate-ether-options mc-ae redundancy-group 1

set interface ae1 aggregate-ether-options mc-ae chassis-id 1

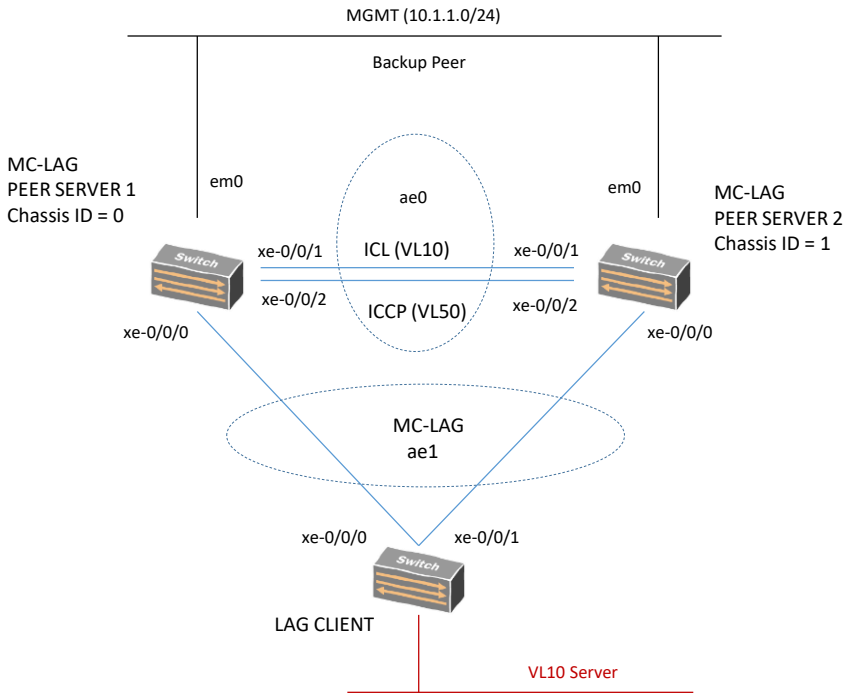
set interface ae1 aggregate-ether-options mc-ae mode active

set interface ae1 aggregate-ether-options mc-ae status-control active

set interface ae1 aggregate-ether-options mc-ae init-delay-time 240

set interface ae1 unit 0 family ethernet-switching interface-mode trunk

set interface ae1 unit 0 family ethernet-switching vlan members v10



MC-LAG Multichassis Link Aggregation Configuration

PEER SERVER 2

set interface em0 unit 0 family inet address 10.1.1.2/24

set interface irb unit 10 family inet address 10.10.10.2/24

set interface irb unit 50 family inet address 10.10.50.2/30

set multi-chassis multi-chassis protection 10.10.50.1 interface ae0

set protocols icpp local-ip-address 10.10.50.2

set protocols icpp peer 10.10.50.1 session-establishment-hold-time 340

set protocols icpp peer 10.10.50.1 redundancy-group-id-list 1

set protocols icpp peer 10.10.50.1 backup-liveness-detection backup-peer-ip 10.1.1.1

set protocols icpp peer 10.10.50.1 liveness-detection minimum-receive-interval 1000

set protocols icpp peer 10.10.50.1 liveness-detection transmit-interval minumum-interval 1000

set switch-option service-id 10

set vlan v10 vlan-id 10

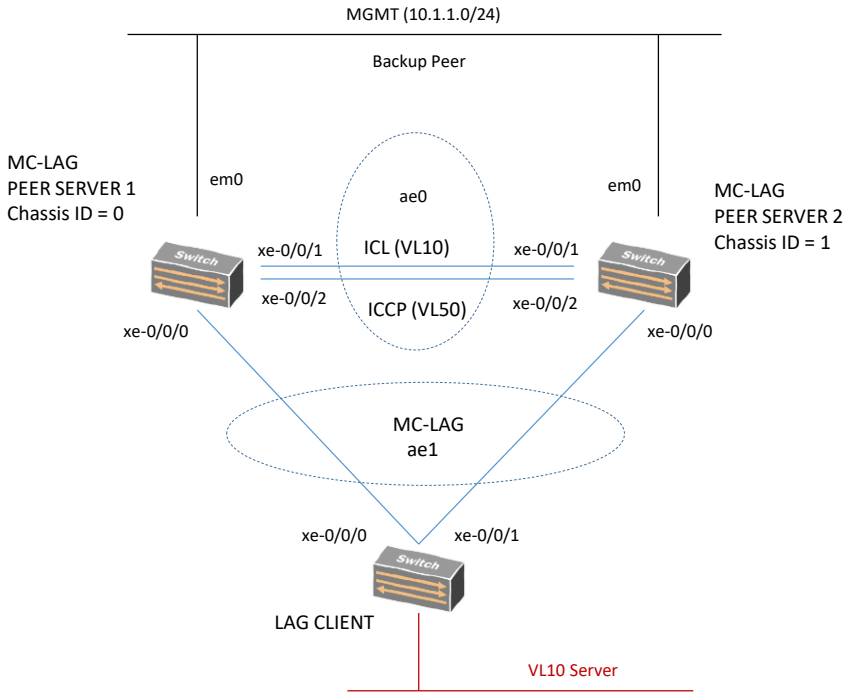
set vlans v10 l3-interface irb.10

set vlan v50 vlan-id 50

set vlans v50 l3-interface irb.50

Nota:

liveness-detection = BFD failure detection



MC-LAG Multichassis Link Aggregation Configuration

LAG CLIENT

set chassis aggregated-devices ethernet device-count 2

set interface xe-0/0/0 ether-options 802.3ad ae1

set interface xe-0/0/1 ether-options 802.3ad ae1

set interface xe-0/0/2 unit 0 family ethernet-switching interface-mode access

set interface xe-0/0/2 unit 0 family ethernet-switching vlan members v10

set interface ae1 aggregate-ethernet-option lacp active

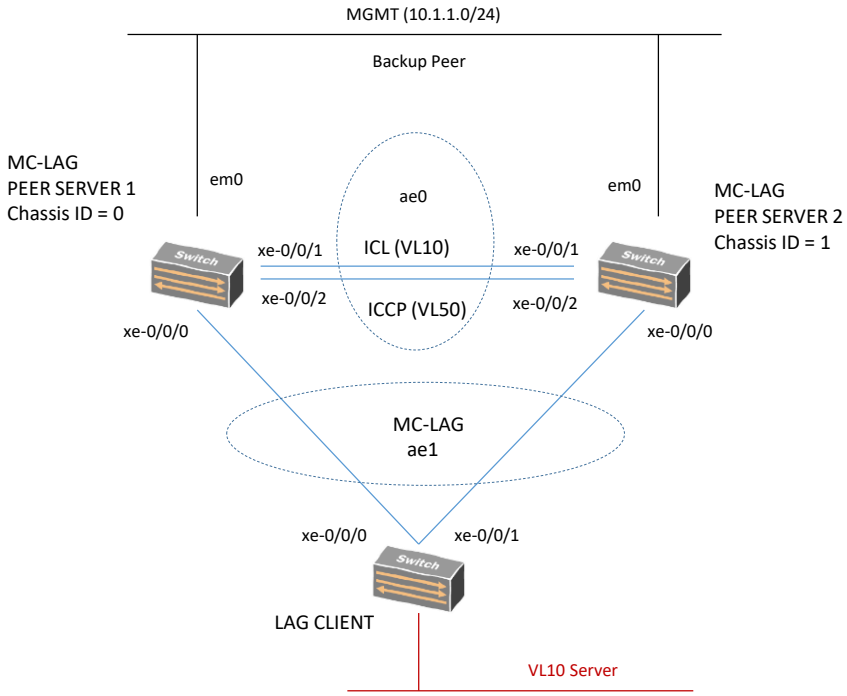
set interface ae1 unit 0 family ethernet-switching interface-mode trunk

set interface ae1 unit 0 family ethernet-switching vlan members v10

set interface irb unit 10 family inet address 10.10.10.3/24

et vlan v10 vlan-id 10

set vlans v10 l3-interface irb.10

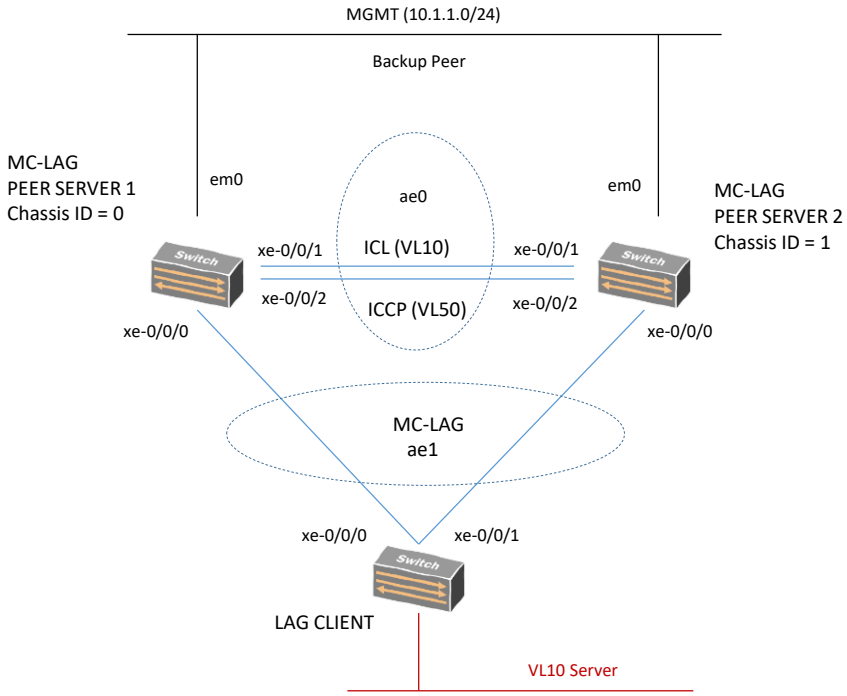


MC-LAG Multichassis Link Aggregation Verifica

Verifica

1) ICPP is running: show icpp
2) LACP is running: show lacp interface
3) MC-AE and ICL-PL interface is UP: show interface mc-ae
4) MAC learning is OK: show ethernet-switching table

[MC-LAG Examples | Junos OS | Juniper Networks]

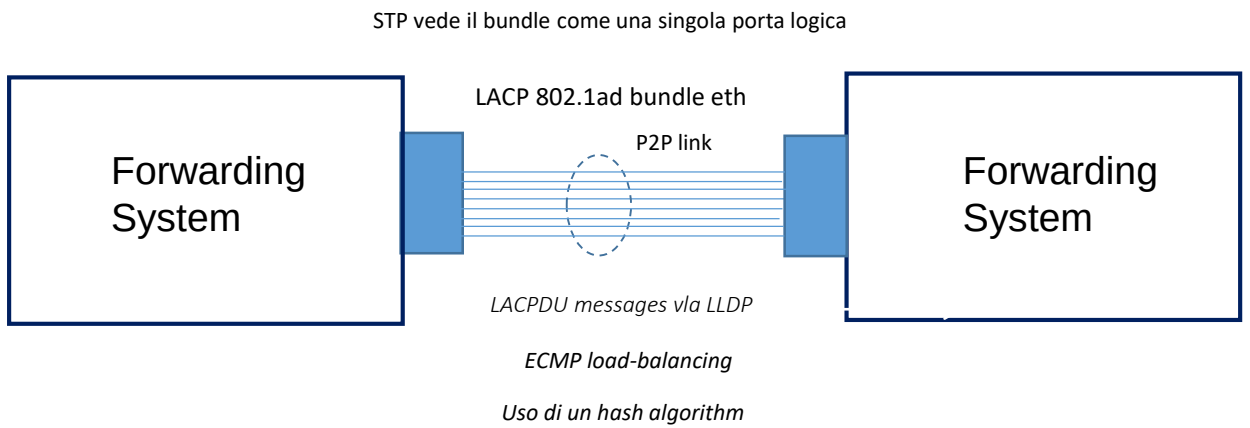


LACP (Link Aggregation Control Protocol) Teoria

LACP è un protocollo standard 802.1ad; i pacchetti LACP sono trasmessi ad un gruppo multicast MAC con indirizzo 01-80-c2-00-00-02; durante la negoziazione i pacchetti sono trasmessi ogni secondo.

Le combinazione agli estremi del channel possono essere:

- on - on
- auto – desiderable
- desiderable – desiderable (only for PAgP; proprietario Cisco)
- active – active (only for LACP)
- passive – active (only for LACP)



Il significato di queste opzioni sono:

- auto = negoziazione passiva del link aggregation
- on = nessun protocollo è usato; si assume che su entrambi i capi del channel è abilitato il link aggregation
- desiderable = negoziazione attiva del link aggregation solo per PAgP
- active = negoziazione attiva del link aggregation solo per LACP

LACP (Link Aggregation Control Protocol) Teoria

LACP è abilitato su una interface aggregate ethernet (ae) semplicemente settando la modalità active or passive; ad ogni modo per l'inizio di una trasmissione di messaggi PDU in forma bidirezionale è necessario abilitare il protocollo LACP in entrambi i peer (local and remote ends of the link) e settare la modalità active almeno su un peer.

Active Mode: con la combinazione Actor e Partner in mode active, essi possono scambiare link aggregation control PDU; il nodo actor trasmette quindi control PDU al suo partner convenendo sullo stato del protocollo suo e del suo partner.

Passive Mode: con la combinazione Actor e Partner in mode passive questi non possono scambiare nessun link aggregation control PDU e come risultato il protocollo LACP resta in Down status.

Di default Actor e Partner scambiano messaggi LACP-PDU ogni secondo; è possibile settare differenti periodic rates con il periodic statement sulla interfaccia local side. E' la configurazione su local side che specifica il comportamento del remote side.

Interval Fast = ogni secondo

Interval Slow = ogni 30 secondi

Esempio di configurazione:

```
set interface ge-0/0/5 ether-option 802.3ad ae0

set interface ge-0/0/6 ether-option 802.3ad ae0

!

set interface ae0 vlan-tagging

set interface ae0 aggregate-ether-option lacp active periodic fast
```

LACP (Link Aggregation Control Protocol) Configuration per MX series

root@vMX1> show configuration chassis | display set

set chassis aggregated-devices ethernet device-count 8

root@vMX1> show configuration interfaces ae1 | display set

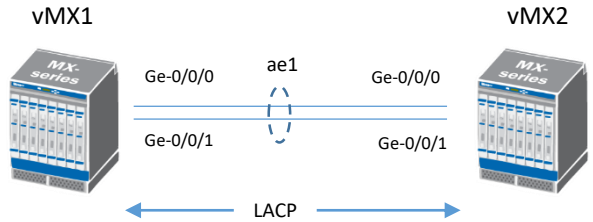
set interfaces ae1 flexible-vlan-tagging *# supporta 802.1Q vlan single-tag and dual-tag frames on logical interface*

set interfaces ae1 encapsulation flexible-ethernet-services *# enable a physical interface to support different type of Ethernet encapsulation at logical interface level; Junos provide two different style of configuration about support to service-provider style and enterprise style. This command support both styles.*

set interfaces ae1 aggregated-ether-options minimum-links 2

set interfaces ae1 aggregated-ether-options lacp active

set interfaces ae1 aggregated-ether-options lacp force-up



root@vMX1> show configuration interfaces ge-0/0/0 | display set

set interfaces ge-0/0/0 gigether-options 802.3ad ae1

root@vMX1> show configuration interfaces ge-0/0/1 | display set

set interfaces ge-0/0/1 gigether-options 802.3ad ae1

Nota: stessa configurazione su vMX2

Ethernet Type Encapsulation

set interfaces ae1 encapsulation flexible-ethernet-services *# enable a physical interface to support different type of Ethernet encapsulation at logical interface level; Junos provide two different style of configuration about support to service-provider style and enterprise style. This command support both styles.*

root@vMX1# set interfaces ae1 unit 0 encapsulation ?

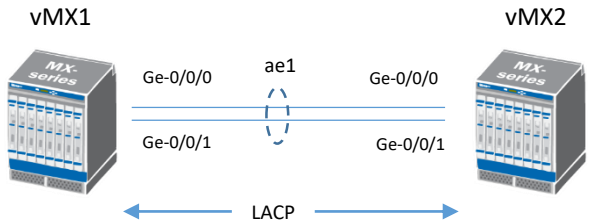
Possible completions:

dix	Ethernet DIXv2 (RFC 894)
ppp-over-ether	PPPoE encapsulation
vlan-bridge	VLAN layer-2 bridging
vlan-ccc	802.1q tagging for a cross-connect
vlan-vpls	VLAN virtual private LAN service

{master}[edit]

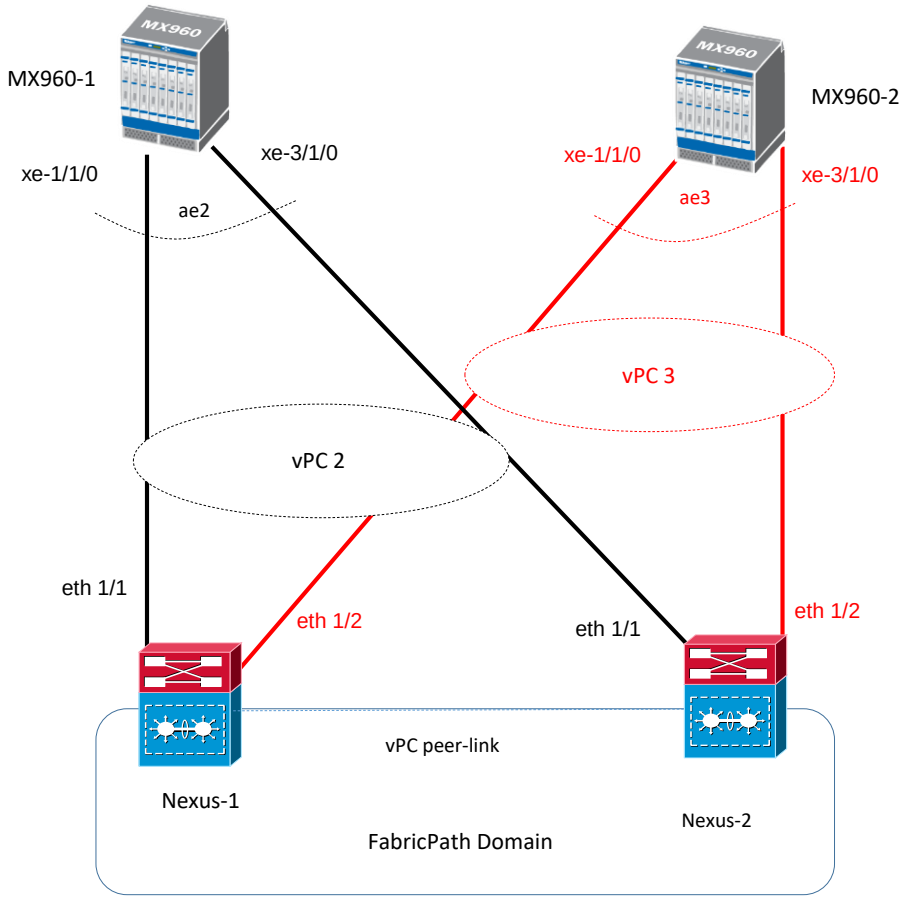
LACP (Link Aggregation Control Protocol) Configuration Verifica per MX series

```
root@vMX1> show interfaces terse | match ae1
ge-0/0/0.32767        up    up   aenet    --> ae1.32767
ge-0/0/1.32767        up    up   aenet    --> ae1.32767
ae1                   up    up
ae1.32767             up    up   multiservice
root@vMX1> show lacp interfaces
Aggregated interface: ae1
    LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
      ge-0/0/0     Actor    No    No   Yes  Yes  Yes   Yes    Fast    Active
      ge-0/0/0   Partner    No    No   Yes  Yes  Yes   Yes    Fast    Active
      ge-0/0/1     Actor    No    No   Yes  Yes  Yes   Yes    Fast    Active
      ge-0/0/1   Partner    No    No   Yes  Yes  Yes   Yes    Fast    Active
    LACP protocol:        Receive State  Transmit State          Mux State
      ge-0/0/0              Current   Fast periodic Collecting distributing
      ge-0/0/1              Current   Fast periodic Collecting distributing
root@vMX1> show lacp statistics interfaces ae1
Aggregated interface: ae1
    LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
      ge-0/0/0             2661        2719          0            0
      ge-0/0/1             2660        2720          0            0
```



LACP (Link Aggregation Control Protocol) Configuration Esempio di Configurazione reale

Architettura Reale:



LACP (Link Aggregation Control Protocol) Configuration Esempio di Configurazione reale

MX960-1:

set interface ae2 description «vPC multichassis to Nexus»

set interface ae2 flexible-vlan-tagging

set interface ae2 encapsulation flexible-ethernet-services

set interface ae2 aggregate-ether-option link-speed 10g

set interface ae2 aggregate-ether-option lacp active

!

set interface xe-1/1/0 gigaether-option 802.3ad ae2

set interface xe-3/1/0 gigaether-option 802.3ad ae2

MX960-2:

set interface ae3 description «vPC multichassis to Nexus»

set interface ae3 flexible-vlan-tagging

set interface ae3 encapsulation flexible-ethernet-services

set interface ae3 aggregate-ether-option link-speed 10g

set interface ae3 aggregate-ether-option lacp active

!

set interface xe-1/1/0 gigaether-option 802.3ad ae3

set interface xe-3/1/0 gigaether-option 802.3ad ae3

Routing Instance Concept

Juniper consente di creare multiple instanze per separare logicamente tabelle di bridging/stp, routing, policies ed interface (a seconda del modello di devices utilizzato); di default Junos ha la instance inet.0

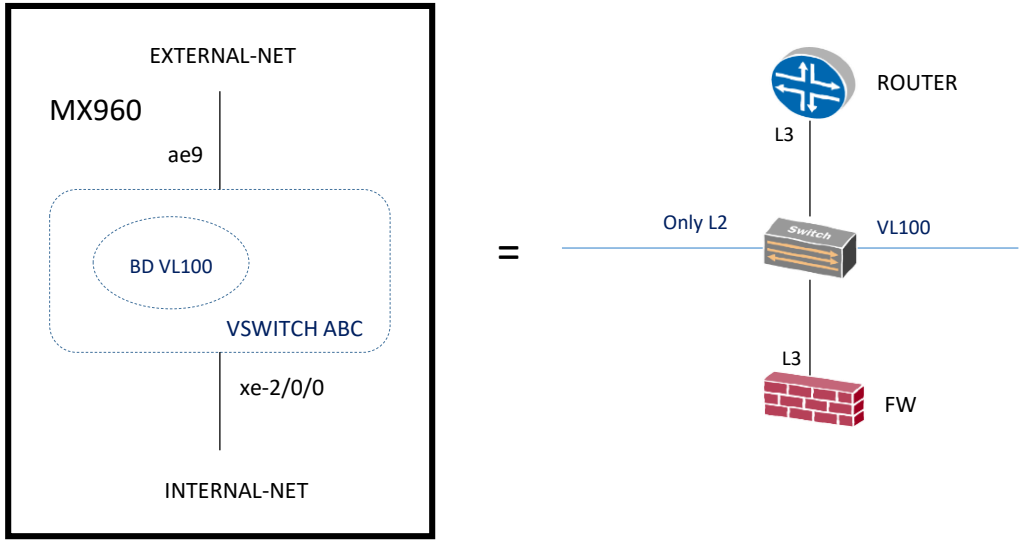
Junos OS utilizza di default queste tabelle:

- inet.0 = per IPv4 unicast routes.
- inet.1 = per IPv4 multicast forwarding cache con IPv4 (S,G) groups entries dinamicamente create.
- inet.2 = utilizzata per subsequence address family indicator 2 (SAFI) quando è abilitato il protocollo MP-BGP; è possibile importare routes da inet.0 a inet.2 utilizzando RIB Groups (Routing Information Base) oppure installando routes all'interno di inet.2 da un protocollo di routing multicast.
- inet.3 = per IPv4 MPLS label-switched path (LSP); questa tabella è utilizzata solo quando il devices si comporta da Ingress-Node verso un LSP.
- inet.6 = per IPv6 unicast routes.
- inet.6.1 = per IPv6 multicast forwarding cache con IPv6 (S,G) gropus entries dinamicamente create.
- instance-name.inet.0 = in caso di configurazione di una nuova routing instances, Junos OS crea di default una tabella per essa (appunto instance.name.inet.0)
- Instance-name.inet.2 = in caso di configurazione di una nuova routing-instances con instance-name protocol bgp family inet multicast in una routing-instance di tipo VRF, Junos crea di default una tabella instance-name.inet.2
- Instance-name.inetflow.0 = in caso di configurazione di una flow route Junos OS crea una tabella associata
- bgp.l2.vpn.0 = per Layer-2 VPN routes imparate da BGP; questa tabella memorizza routes apprese da PE (Provider Edge) e le informazioni sono copiate all'interno di una L2-VPN VRF basata su valori di target community.
- bgp.le.vpn.0 = per Layer-3 VPN routes imparate da BGP; le routes in questa tabella sono copiate all'interno di una L3-VPN VRF quando esiste un matching nella routing table.
- L2circuit.0 = per L2 circuit routes imparate via LDP; queste routes sono trasmesse e ricevute per L2circuit signaling messages
- mpls.0 = per MPLS label switching operations; questa tabella è utilizzata quando il devices si comporta come Transit Router
- iso.0 = per ISIS routes;
- juniper_private = per comunicazione interna tra RE (Routing Engine) e le PIC hardware del sistema Junos OS

Routing Instance Configuration (example only L2) per MX series

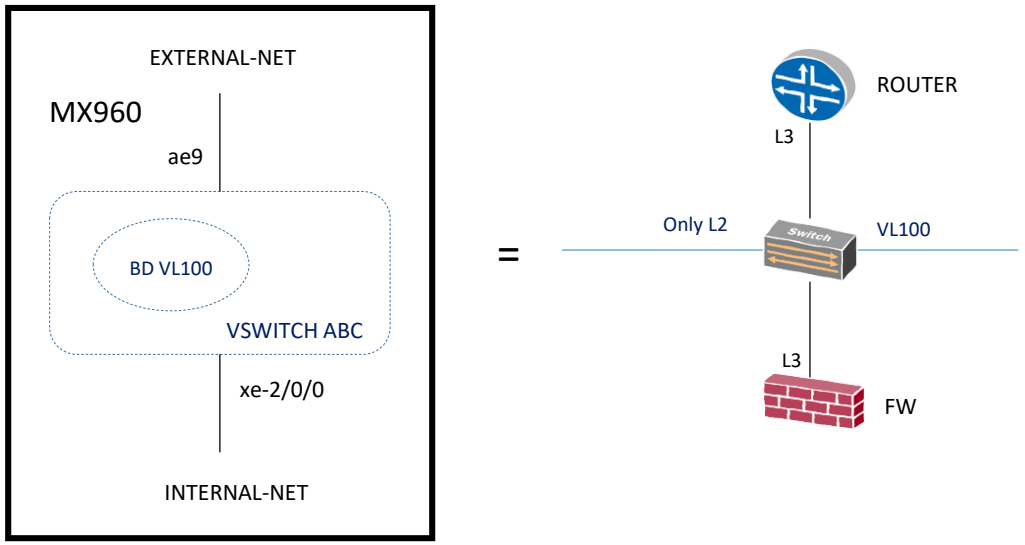
Configurazione Instances type virtual-switch (parte 1)

```
routing-instances {
  VSWITCH-ABC {
       instance-type virtual-switch;
       bridge-domains {
          VL-100 {
             vlan-id 100;
             interface xe-2/0/0.100;
             interface ae9.100;
      }
}
```



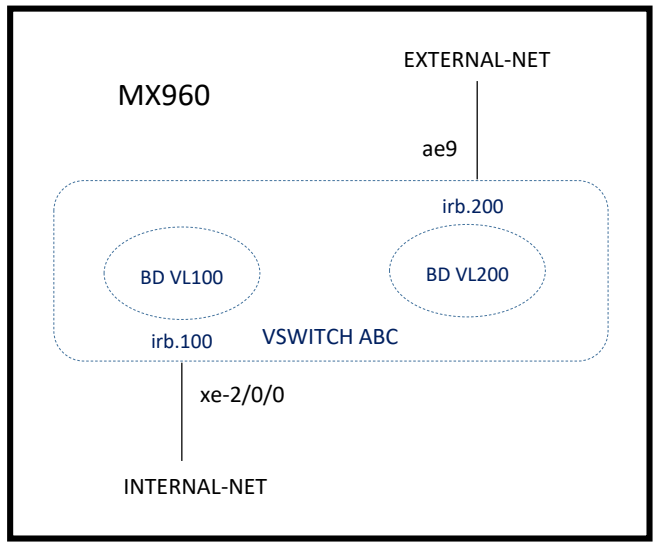
Routing Instance Configuration (example only L2) per MX series

```
ae9 {
      description «External Network";
       flexible-vlan-tagging;
      encapsulation flexible-ethernet-services;
      aggregated-ether-options {
         link-speed 10g;
         lacp {
            active;
         }
      unit 100 {
         description to_ROUTER;
         encapsulation vlan-bridge;
         vlan-id 100;
         family bridge;
      }
xe-2/0/0 {
      description "to FW";
      flexible-vlan-tagging;
      encapsulation flexible-ethernet-services;
 }
      unit 100 {
         description to_INTERNAL-FW;
         encapsulation vlan-bridge;
         vlan-id 100;
         family bridge;
      }
```

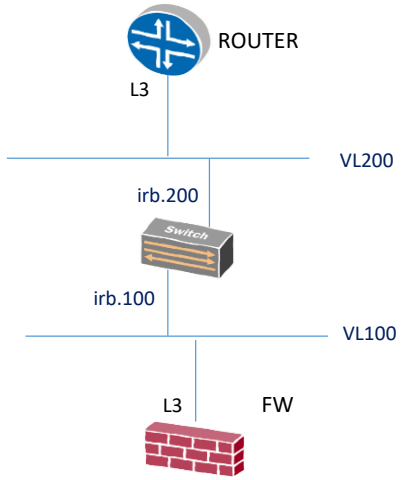


Routing Instance Configuration with L3 interface IRB (Integrated Routing and Bridging) per MX series

```
routing-instances {
  VSWITCH-ABC {
      instance-type virtual-switch;
      bridge-domains {
         VL-100 {
            vlan-id 100;
            interface xe-2/0/0.100;
            routing-interface irb.100
     }
 }
     VL-200 {
            vlan-id 200;
            interface ae9.100;
            routing-interface irb.200
     }
irb {
     unit 100 {
     family inet {
     address 192.168.1.1/24 {

unit 200 {
     family inet {
    address 192.168.2.1/24 {
```



=



Monitoring and Security Switches campus

Massimiliano Sbaraglia

Monitoring and Security Network

Il monitoraggio della rete consiste principalmente in queste fasi:

- port mirroring
- syslog
- SNMP
- RPM

La sicurezza della rete consiste in queste altre fasi:

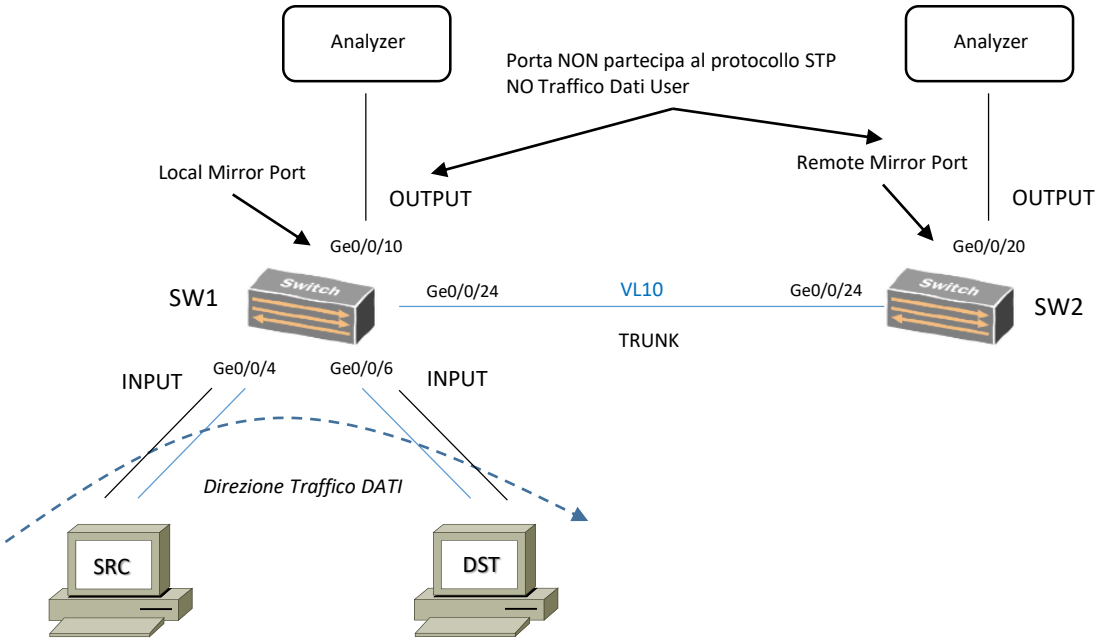
- port security
- port-based authentication
- spoofing protection
- private vlan
- vlan acl

Port Mirroring

Il port mirroring è utile per esaminare:

- pacchetti in entrata o in uscita da una porta
- pacchetti in entrata su base vlan
- pacchetti in uscita su base vlan (valido solo per EX8200)
- Pacchetti in entrata su una porta oppure su una vlan che sono selezionati da un «firewall filter», ossia pacchetti che attraversano un filtro in ingresso e vengono inviati ad un analyzer; questo ultimo può essere locale ad uno switch (local analyzer port) oppure d uno switch remoto (analyzer vlan)

Nota: è possibile campionare i pacchetti da replicare, ad esempio con un ratio = 200 (significa 1 pacchetto su 200)



Port Mirroring Configuration

LOCAL ANALYZER PORT:

root@SW1# edit ethernet-switching options analyzer TEST

[edit ethernet-switching options analyzer TEST]

root@SW1# set input ingress interface ge-0/0/4.0

root@SW1# set input egress interface ge-0/0/6.0

root@SW1# set output interface ge-0/0/10.0

REMOTE ANALYZER PORT:

root@SW1# edit ethernet-switching options analyzer TEST

[edit ethernet-switching options analyzer TEST]

root@SW1# set input ingress interface ge-0/0/4.0

root@SW1# set input egress interface ge-0/0/4.0

root@SW1# set loss-priority high *# di default la loss-priority è con valore low; in caso di output vlan bisogna mettere secondo best-practice high*

root@SW1# set output vlan remote-analyzer

root@SW1# set vlans remote-analyzer vlan-id 10

root@SW1# set interface ge-0/0/24.0 family ethernet-switching port-mode trunk

root@SW1# set interface ge-0/0/24.0 family ethernet-switching vlan members 10

!

root@SW2# edit ethernet-switching options analyzer TEST

root@SW2# set input ingress vlan remote-analyzer

root@SW2# set output interface ge-0/0/20.0

root@SW2# set vlans remote-analyzer vlan-id 10

root@SW2# set interface ge-0/0/24.0 family ethernet-switching port-mode trunk

root@SW2# set interface ge-0/0/24.0 family ethernet-switching vlan members 10

!

Port Security MAC Limiting

Per port security si intende caratteristiche quali il MAC limiting, DHCP snooping, Dynamic ARP inspection (DAI) ed infine il IP Source Guard.

Di default le porte non hanno nessun limite di MAC addresses che esse possono imparare.

- MAC Limiting:
  - Limita il numero di MAC addresses imparati da ogni singola porta in access
  - Previene azioni di MAC address spoofing, esplicitando il numero di MAC address per porta oppure monitorando cambiamenti da un MAC address ad un altro tra porte all'interno di un segmento Vlan (MAC move limiting).

Quando un MAC address oppure MAC move limit supera un valore di «exceeded» lo switch performa le seguenti azioni:

- ✓ None: specificando l'azione come «none» nessuna azione viene intrapresa in caso di mac-limiting or ma-move-limiting exceeded.
- ✓ Syslog Only: genera un errore log
- ✓ Drop and Syslog: scarta le frame in eccesso (considerate di hacking) e genera un error log (nota: comportamento di default in caso di nessuna azione specificata)
- ✓ Shutdown: spegne la porta e genera un errore log

Aspetti di Configurazione:

```
set ethernet-switching-option secure-access-port interface ge-0/0/6.0 allowed-mac [ mac-address-1 mac-address-2 ]

set ethernet-switching-option secure-access-port interface ge-0/0/7.0 mac-limit 2 action log

set ethernet-switching-option secure-access-port interface ge-0/0/8.0 mac-limit 2 action drop

set ethernet-switching-option secure-access-port interface ge-0/0/9.0 mac-limit 2 action shutdown

set ethernet-switching-option secure-access-port vlan default mac-move-limit 1 action shutdown
```

Verifica:

```
show log messages | match limit | match 0/0/6
```

Port Security MAC Limiting

Autorecovery è una tecnica che permette allo switch di essere configurato con il comando «port-error-disable» e consente di disabilitare le interfacce per un recovery automatico definito da un periodo temporale.

Esempio di configurazione:

set ethernet-switching-options port-error-disable disable-timeout 3600

Di default autorecovery è disabilitato ed il range timeout ha un valore compreso tra 10 – 3600 secondi; in caso non si specifichi un tempo è possibile utilizzare il «clear» per la disabled port da volere disabilitare.

clear ethernet-switching port-error interface

Persistent MAC Learning anche conosciuto come MAC sticky è una tecnica di sicurezza utilizzata per trattenere MAC addresses appresi in modo dinamico in caso di restart di uno switch oppure in caso di una interfaccia che subisce un up/down/up

Questa tecnica è disabilita di default ed abilitando persistent MAC learning insieme al MAC limit è possibile avere una configurazione trust di indirizzi provenienti da ambienti sicuri.

Le linee guida per il Persistent MAC Learning sono:

- Le interfacce debbono essere in mode access;
- Non si può configurare persistent mac learning su interfacce di tipo redundant trunk group;
- Non si può configurare persistent mac learning su interfacce con 802.1X configurato
- Non si può configurare persistent mac learning su interfacce dove il «no-mac-learning» è configurato

Esempio di configurazione:

set ethernet-switching-option secure-port-access interface ge-0/0/6.0 persistent-learning

Verifica:

show ethernet-switching table → verifica la colonna Type Flood with Persistent

Port Security DHCP snooping

DHCP snooping è una tecnica di sicurezza che previene eventuali attacchi/vulnerabilità da Rogue DHCP server via DoS attack.

Questa tecnica costruisce e mantiene un database di indirizzi IP validi assegnati per mezzo di un server DHCP trust. DHCP snooping permette di leggere queste informazioni di leasing e costruire questa mappatura tra IP address, MAC address e Vlan associata.

DHCP snooping, quindi, protegge lo switch andando ad ispezionare i DHCP packets sulle porte di tipo untrusted ed inoltre traccia un lease time (assegnato dal DHCP server trust) e smaltisce tutte le entries che sono eccedute da tale valore temporale.

DHCP snooping include il DHCP option 82 (DHCP relay agent), il quale aiuta nella protezione di uno switch contro attacchi di tipo spoofing di IP addresses e MAC addresses.

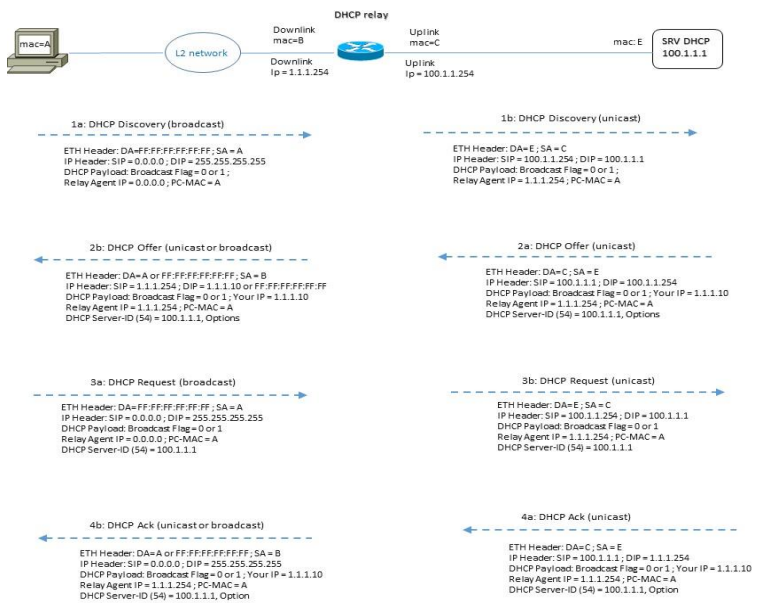
E' possibile abilitare DHCP option 82 per una singola vlan oppure per tutte le vlans in uno switch; inoltre è possibile configurare un layer 3 interface (IRB/RVI) quando lo switch ha ruolo di Relay Agent.

La serie EX switches implementa DHCP option 82 con tre sotto-option:

- ✓ Circuit-ID: questa opzione identifica il circuito (interface, vlan, entrambe = ge-0/0/6:vlan1 ad esempio) dove la richiesta è stata ricevuta; in caso la richiesta arriva al livello 3 (ip address) il circuit-id si presenta solo con il nome della interfaccia (ge-0/0/6)
- ✓ Remote-ID: questa opzione identifica un host; di default il remote-id è l'indirizzo MAC dello switch ma è possibile definirlo come hostname dello switch oppure la description interface oppure con un testo scelto.
- ✓ Vendor-ID: questa opzione identifica il vendor di un host; il valore di default = Juniper.

DHCP snooping process:

- Client sends DHCPDISCOVER or DHCPREQUEST
- Switch snoops packet and updates snooping database
- Switch forwards DHCPDISCOVER or DHCPREQUEST
- Server sends DHCPOFFER, DHCPPACK or DHCPNAK
- Switch snoops packet and updateds snooping database
- Switch forward DHCPOFFER, DHCPPACK or DHCPNAK



Port Security DHCP snooping

DHCP snooping Esempio di Configurazione:

set ethernet-switching-options secure-access-port interface ge-0/0/6.0 no-dhcp-trusted → *proibisce la porta dal ricevere DHCP Server traffic (default settings per access port*

set ethernet-switching-options secure-access-port interface ge-0/0/7.0 dhcp-trusted → *permette di ricevere DHCP Server traffic*

set ethernet-switching-options secure-access-port vlan default examine-dhcp → *abilita DHCP snooping per vlan-specified*

!

set ethernet-switching-option secure-access-port dhcp-snooping-file location /var/tmp/snoop-dawg-n-co;

set ethernet-switching-option secure-access-port dhcp-snooping-file write-interval 60;

JunOS richiede di settare un path di location dove le entries vengono loggate con un intervallo definito dal write-interval.

Per verificarne il contenuto DHCP snooping file, si usa il «file show» command, seguito dalla stringa del path

Esempio:

edit ethernet-switching-option

run file show /var/tmp/snoop-dawg-n-co

Per le statistiche:

run show dhcp snooping statistics

Per monitorare:

show dhcp snooping binding

Port Security DHCP snooping

Per pulire il DHCP snooping database, si possono eseguire i seguenti comandi:

clear dhcp snooping binding → *clear di tutte le entries*

clear dhcp snooping binding vlan <vlanid> → *clear entries for specified vlan*

clear dhcp snooping binding vlan <vlanid> mac <mac_address> → *clear rntry for specified mac-address*

Per aggiungere una specifica entry:

set ethernet-switching-options secure-access-port interface ge-0/0/6.0 static-ip 192.168.1.4 vlan default mac 00:26:88:02:74:89;

set ethernet-switching-options secure-access-port vlan default examine-dhcp;

Port Security ARP spoofing

ARP è una tecnologia per mappare MAC addresses di uno switch all'interno di un segmento di rete LAN con IP addresses (MAC-to-IP).

Quando un ARP entry per uno specifico MAC address non esiste nell'ARP table, un pacchetto broadcast viene generato e trasmesso fuori lo switch per imparare/conoscere il MAC address corrispondente con il livello 3 address.

ARP spoofing (conosciuto anche come ARP poisong) è un attacco di tipo «man-in-the-middle» che simula (di fatto spoofs via un ARP packet) un MAC address di un nodo vittima e di fatto il traffico devia da sorgente a destinazione leggittima a sorgente a destinazione illeggittima.

Il processo DAI (Dynamic ARP Inspection) previene da questo tipo di attacchi, andando ad intercettare l'ARP packets sulle porte di tipo untrusted e validarlo secondo il DHCP snooping database.

Controlla se il MAC address sorgente dell'ARP packet match con le entries valide del DB DHCP snooping e:

- ✓ Se non c'è corrispondenza (IP-MAC entry) nel database, il DAI scarta l'ARP packet
- ✓ Se l'indirizzo IP all'interno del pacchetto è invalido, il DAI scarta l'ARP packet

Di default l'ARP spoofing è disabilitato ed è possibile abilitarlo per singola VLAN (no per ogni porta).

Se una porta in access-mode è collegata ad un host con un indirizzo IP statico di un segmento di rete LAN che ha il DHCP snooping ed il DAI abilitato, è necessario configurare la porta come trusted port e permettere all'ARP packet di passare.

Il comando per settare le porte come trusted è «dhcp-trusted»

Esempio di configurazione DAI:

set ethernet-switching-option secure-access-port interface ge-0/0/6.0 dhcp-trusted → *marca interfaccia come sicura e bypass ARP inspection*

set ethernet-switching-option secure-access-port vlan default arp-inspection → *abilita il DAI per specified vlan*

set ethernet-switching-option secure-access-port vlan default examine-dhcp → *abilita DHCP snooping per specified vlan (required for DAI)*

Verifica:

show dhcp snooping binding

show arp inspection statistics interface ge-0/0/6.0

Port Security IP Source Guard

IP Source Guard è una tecnica per controllare il source IP e MAC addresses in un pacchetto che entra attraverso una porta di tipo untrusted access e le informazioni del DHCP snopping database.

Se IP Source Guarda determina che il pacchetto contiene un indirizzo invalido (sia esso IP oppure MAC), lo switch non trasmette il pacchetto ma lo scarta.

E' possibile abilitare il IP Source Guard per una o più vlans.

Di default le porte in access sono definite untrusted, mentre le porte in trunk sono considerate trusted (EX series switch).

Esempio di configurazione:

set ethernet-switching-options secure-access-port interface ge-0/0/6.0 dhcp-trusted

set ethernet-switching-options secure-access-port vlan default examine-dhcp

set ethernet-switching-options secure-access-port vlan default ip-source-guard → *in questo caso l'ip-source-guard è abilitato per la vlan di default*

In caso uno switch non dovesse supportare DHCP, è necessario definire una static entry per il DHCP snooping database:

set ethernet-switching-options secure-access-port interface ge-0/0/6.0 static-ip 192.168.1.4 vlan default mac 00:26:88:02:74:89;

set ethernet-switching-options secure-access-port vlan default examine-dhcp;

set ethernet-switching-options secure-access-port vlan default ip-source-guard

Verifica:

show dhcp snooping binding

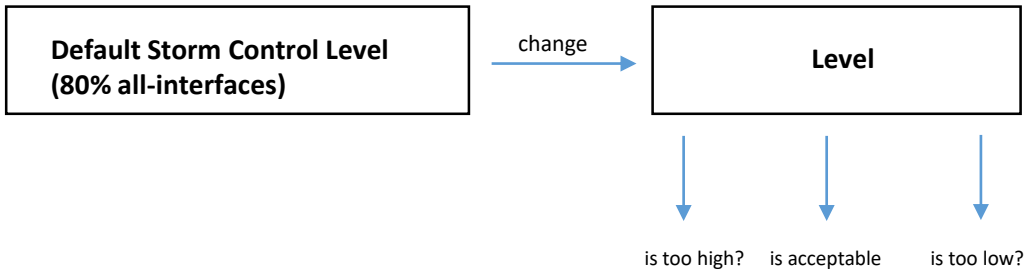
show ip-source-guard

Storm Control

Si definisce traffic storm un tipo di traffico conosciuto come BUM (broadcast, unknow-unicast e multicast) che è trasmesso in modo flooding attraverso la rete tale da pregiudicare le prestazioni e le risorce della rete stessa.

BUM è normale operazione di una rete LAN e pertanto per riconoscere il traffico Storm bisogna superare una soglia di allarme che prevede un tipo di traffico anomalo.

Storm Control abilita uno switch a monitorare il livello di traffico e scartare il traffico BUM quando uno specifico livello, chiamato storm control level, è ecceduto.



Per regolare un livello adeguato è possibile variare il valore di default in modo che le interfacce attraverso le quali si presenta uno storm control violation, sono messe in shutdown.

Esempio di Configurazione:

set ethernet-switching-option storm-control interface all → *azione di default ed il traffico viene scartato in caso di violazione*

set ethernet-switching-option storm-control action-shutdown → *questo ci permette di variare il valore/comportamento di default andando a disabiliare la porta*

set ethernet-switching-option storm-control interface-all

In caso di automatico recovery da una condizione di errore:

set ethernet-switching-option port-error-disable disable-timeout 300

set ethernet-switching-option storm-control action-shutdown

set ethernet-switching-option storm-control interface all

Syslog

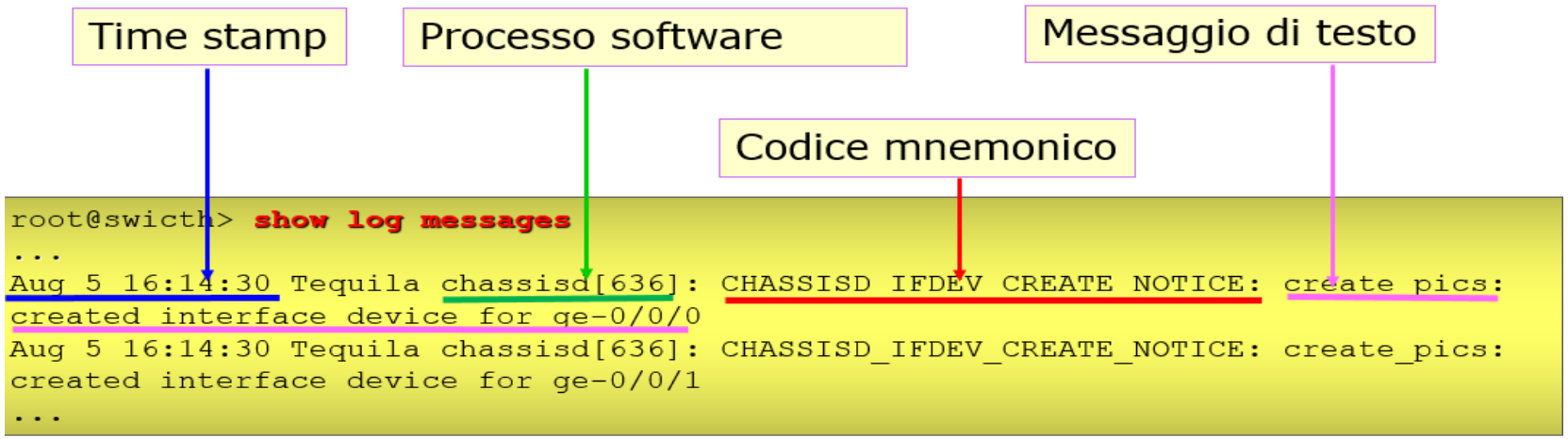
Il Syslog esamina attraverso dei log eventuali errori e vengono gestiti via

- Localmente su console
- Su memoria RAM (buffer)
- Su linea VTY
- Su un server esterno

Porta UDP 514

I messaggi vengono salvati in un file locale (path default /var/log/messages) ed inviati ad un Server Syslog, console eppure ad un utente quando accede allo switch.

In Junos di default i messaggi syslog non riportano priorità (facility + severity) e per riportare la priority bisogna specificare la keyword explicit-priority



Syslog Severity

Livelli di Severity:

- Emergency: 0
- Alert: 1
- Critical: 2
- Error: 3
- Warning: 4
- Notice: 5
- Informational: 6
- Debug: 7

Syslog Facilities

Facilities:

- Any
- Authorization
- Change-Log
- Conflict-Log
- Daemon
- DFC (Dynamic Flow Capture)
- Firewall
- FTP
- Interactive commands
- Kernel
- PFE (Packet Forwardig Engine)
- User

Syslog Config

Esempio di Configurazione:

```
root@vMX1> configure
Entering configuration mode
{master}[edit]
root@vMX1# edit system syslog
{master}[edit system syslog]
root@vMX1# set ?
Possible completions:
  allow-duplicates                Do not suppress the repeated message for all targets
+ apply-groups                    Groups from which to inherit configuration data
+ apply-groups-except             Don't inherit configuration data from these groups
> archive                         Archive file information
> console                         Console logging
> file                            File in which to log data
> host                            Host to be notified
  log-rotate-frequency            Rotate log frequency (1..59 minutes)
  routing-instance                 Routing instance
> server                           Enable syslog server
  source-address                   Use specified address as source address
> time-format                     Additional information to include in system log timestamp
> user                            Notify a user of the event
{master}[edit system syslog]
```

Syslog Config

Esempio di Configurazione:

```
root@vMX1# show
user * {
    any emergency;
}
host 10.4.5.18
    any any;
    explicit-priority;
}
file messages {
    any notice;
    authorization info;
}
file interactive-commands {
    interactive-commands any;
}

{master}[edit system syslog]
root@vMX1#
```

SNMP Protocol

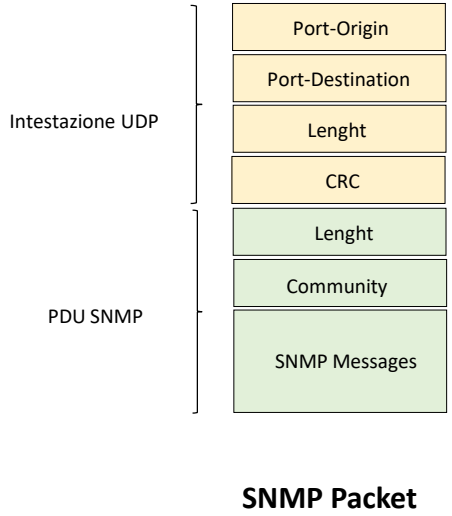
SNMP fornisce un sistema primitivo di sicurezza basato su una comunicazione manager (NMS) – agent (Nodo o Network Element)

- In ogni agente sono definite comunità di manager a cui sono associati diritti nell'accesso alle variabili:
  - Read Only
  - Read Write
- I manager inseriscono il community-name in ogni messaggio inviato all'agente (get, get-next, set)
- La conoscenza della community-name da parte del manager è considerata come autenticazione del manager da parte dell'agente
- La set è permessa solo per variabili di lettura-scrittura e community con il diritto di scrittura

Limitazione: community-name in chiaro

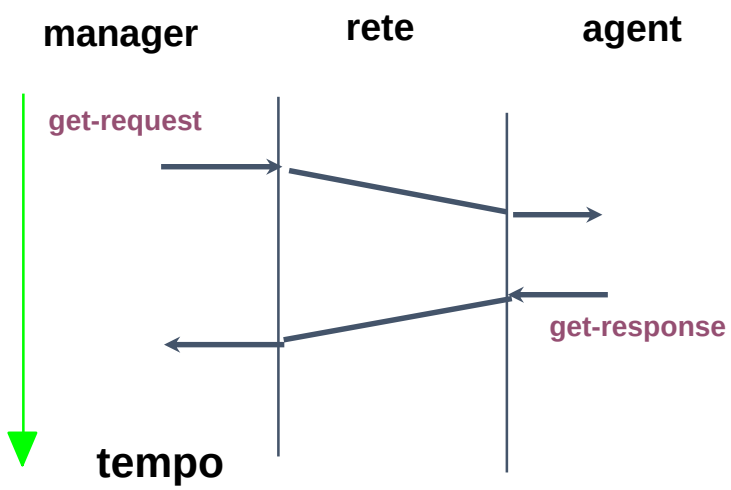
Due modalità di trasferimento informazioni:

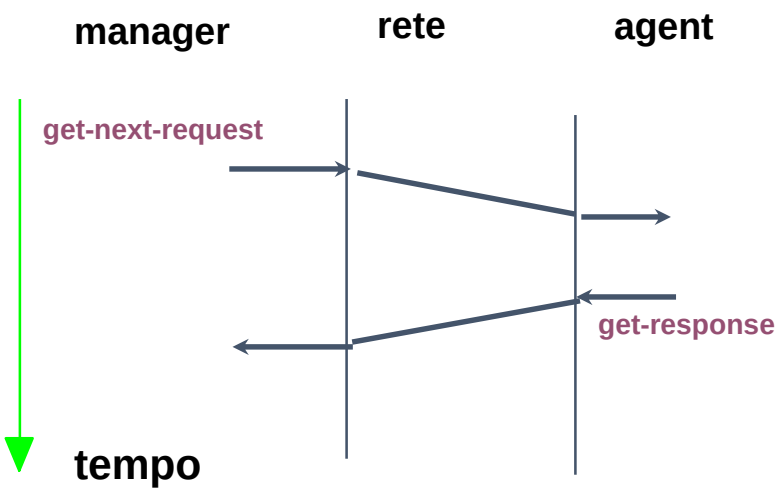
- Polling
- Messaggi asincroni:

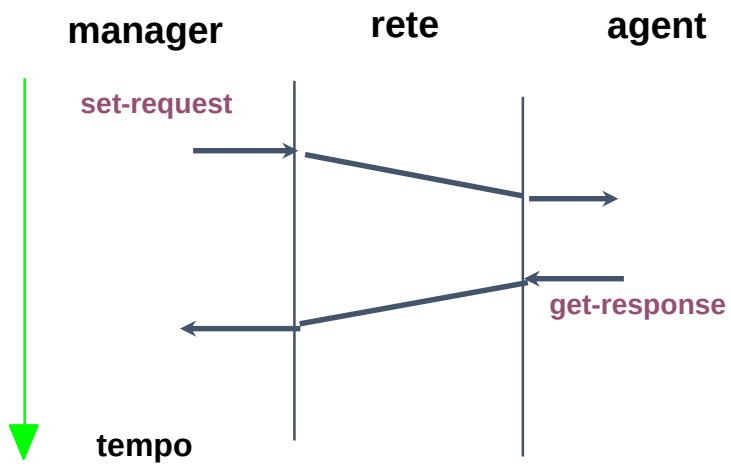


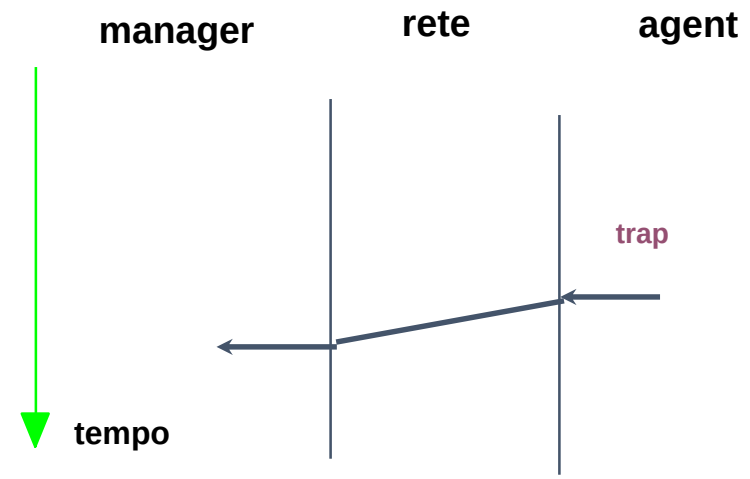
SNMP Packet

SNMP primitive di comunicazione









SNMP Version

- SNMP Version 1
  - Modello di protocollo request/responce
  - Primitive: Get, GetNext, Set e Trap
  - Autenticazione con community string in «clear text»

- SNMP Version 2
  - Formato delle Trap semplificato
  - Nuovi Messaggi: GetBulk & Inform
    - GetBulk: retrival di più righe di una tabella contemporaneamente (velocizza molto il trasferimento di dati)
    - Set-Request: modellata come una transizione (protocollo «two phase commitment», estensione delle possibili cause di fallimento, garantisce atomicità della set)
    - Trap: ridefinita la sintassi del messaggio come una Get-Responce asincrona
    - Inform: come una Trap, ma richiede un ACK (acknowledge)
  - Diverse varianti con diversi modelli di security

- SNMP Version 3
  - RFC 3411 e RFC 3418
  - Recepisce i miglioramenti del protocollo SNMPv2
  - Definisce un modello di sicurezza più flessibile

SNMP esempio di configurazione

```
[edit snmp]
root@switch# show

interface me0.0;
community ADMIN {
        authorization read-write;
        view admin-mib;
        clients {
                10.10.12.4/32;
                0.0.0.0/0 restrict;
                }
        }
trap-group CONTROL {
        categories {
                chassis;
                link;
                }
         targets {
              10.10.12.4;
                }
         }
view admin-view{
         oid  all include;
         }
```

L'accesso (ex. GETs) da parte dei manager viene ristretto ad una particolare interfaccia e per un particolare insieme di clients. Senza l'opzione *clients,* chiunque conosce il nome della community (cioè ADMIN) può accedere al MIB, in base ai diritti di accesso o autorizzazioni della community.

di default è read-only, se c'è read-write è necessaria definire ed associare una MIB view

Configurazione della modalità TRAP

destinatari delle traps

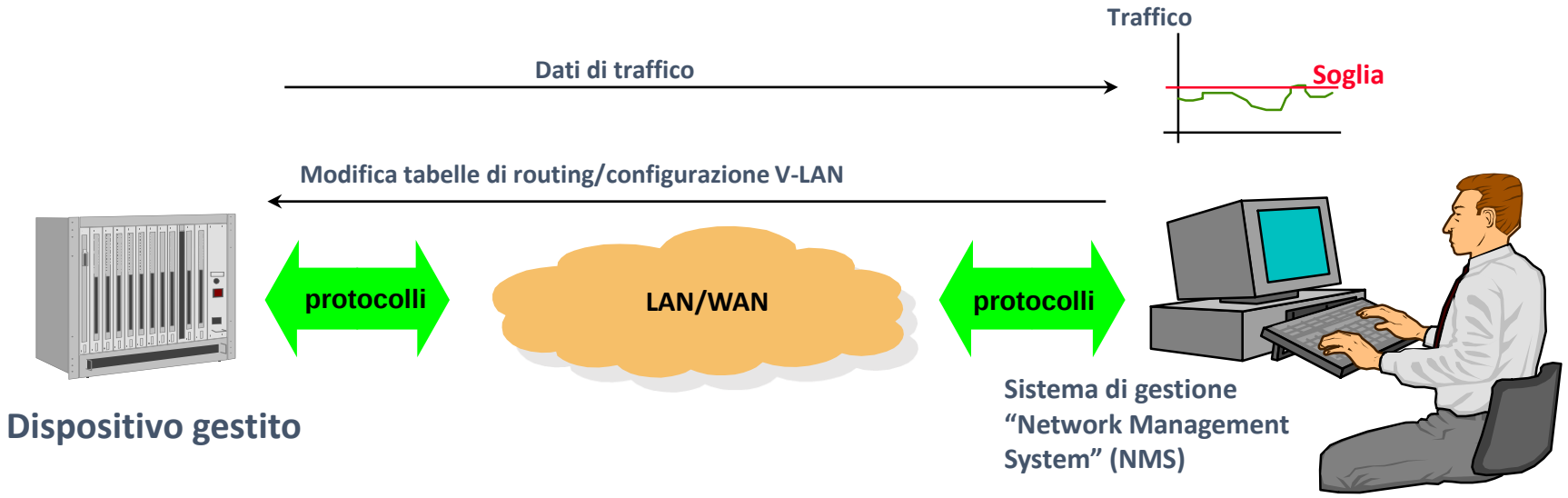
SNMP: raccolta ed analisi dati

Con SNMP si intende un centro di gestione che coinvolge:

- Supervisione delle risorse di rete
- Le risorse sono rappresentate da qualunque entità, fisica o logica presente in rete
- La gestione di rete si traduce in:
  - Assicurare il corretto comportamento della rete
  - Monitoraggio impiego delle risorse di rete
  - Registrare le riconfigurazioni ed i cambiamenti della rete
  - Produrre e raccogliere informazioni sulle operazioni effettuate in rete

I nodi di rete (anche conosciuti come Network Element) sono strumentati per raccolta di dati sul comportamento del nodo e la esecuzione di operazioni di controllo sul nodo stesso.

L'architettura di gestione NMS (Network Management System) raccoglie i dati ed invia controlli, come il personale addetto gestisce i guasti, prestazioni, configurazioni, etc…

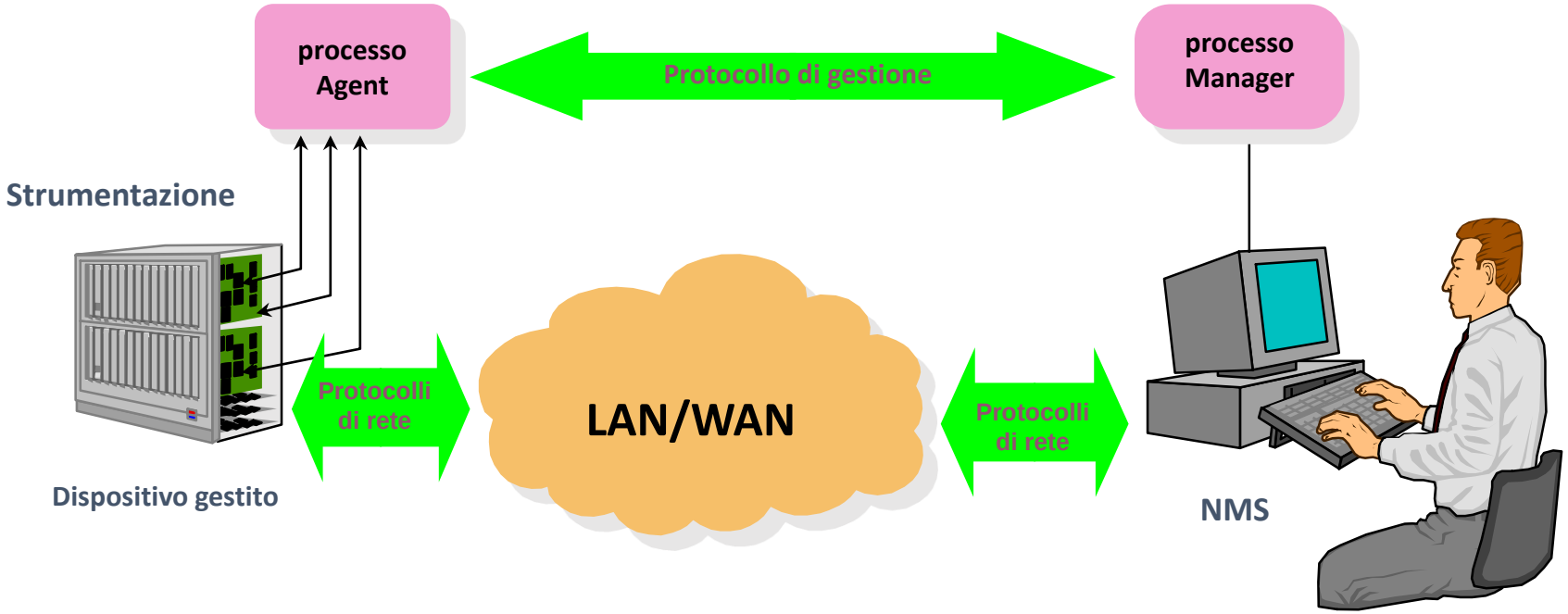


SNMP: gestione manager ed agent

Il colloquio tra NMS e Network Element si svolge tra:

- Processo «Agent» sul nodo
- Processo «Manager» su NMS

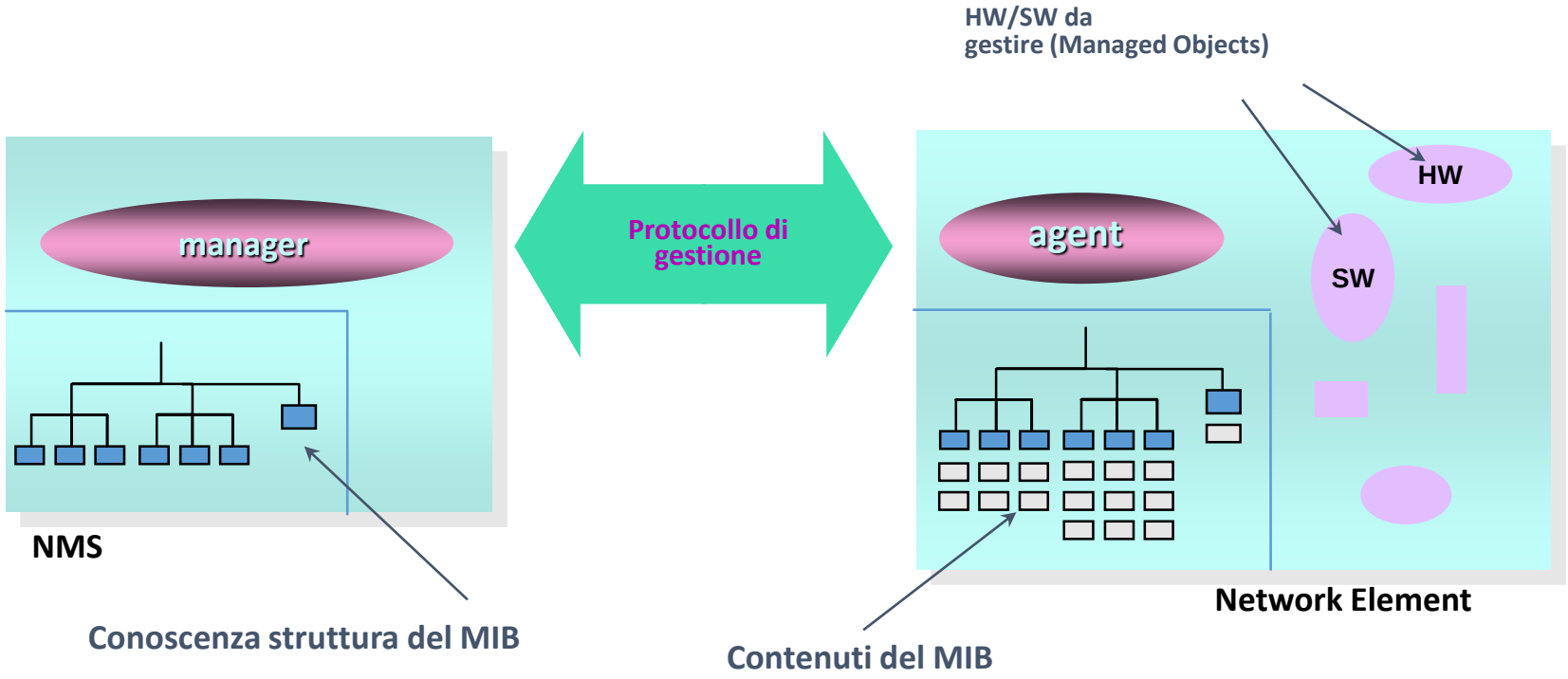
Il protocollo utilizzato per questa comunicazione si basa su un protocollo di gestione SNMP/CMIP



SNMP: MIB

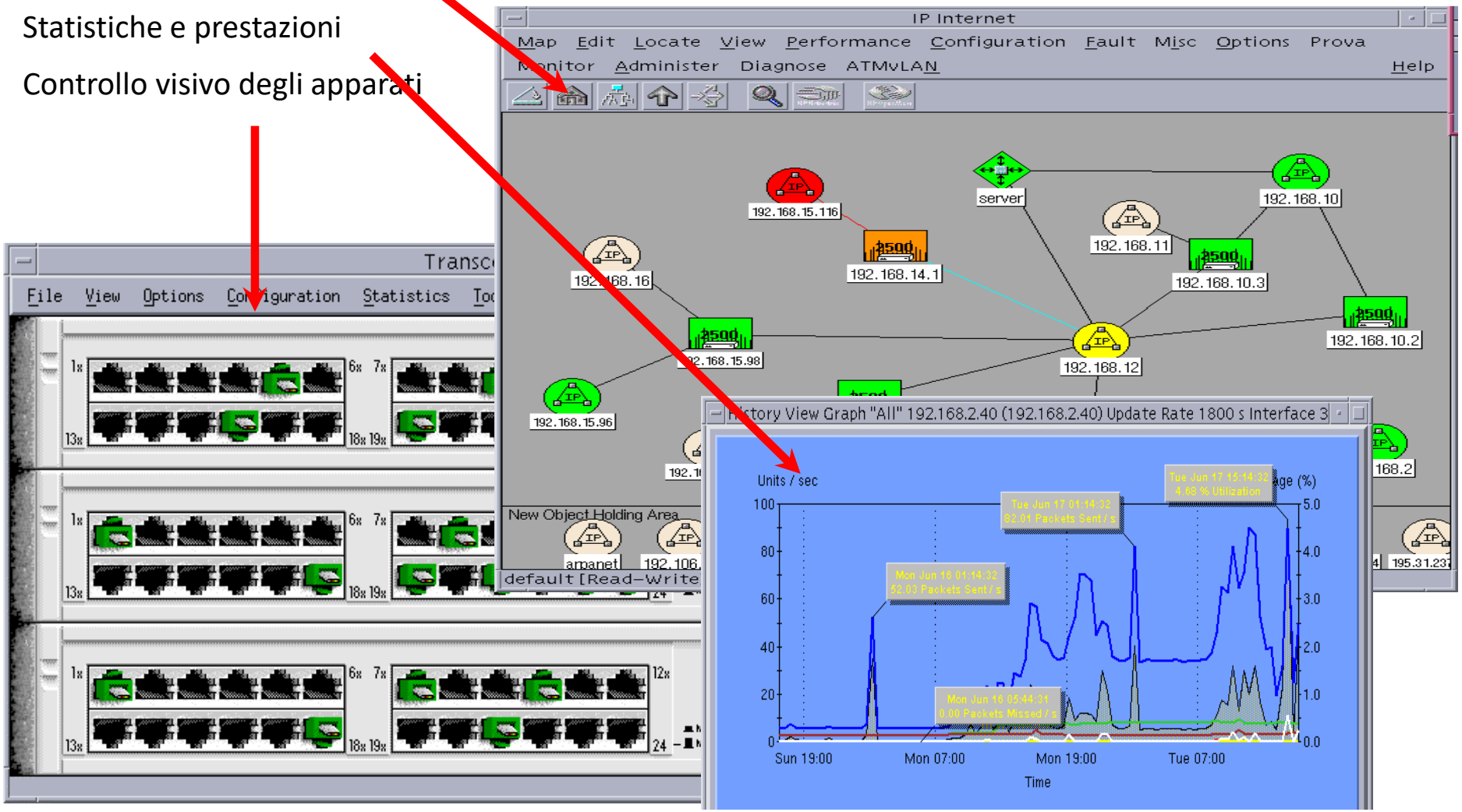
Il MIB (Management Information Base) è la rappresentazione logica degli oggetti gestiti:

- Organizzata come una directory con struttura ad albero
- Le variabili del MIB rappresentano lo stato degli oggetti
- Il protocollo di gestione è uno strumento per effettuare interrogazioni (query) sul MIB



SNMP: Servizi di Presentazione

- Rappresentazione grafica della rete
- Statistiche e prestazioni
- Controllo visivo degli apparati



SNMP: stumenti per la gestione

- Strumenti generici
  - MIB browser, ping, mapping, discovery, trouble ticketing

- Strumenti specifici
  - Dipendono dal tipi di nodo (hub, switch, port switching, vlan, router, etc…

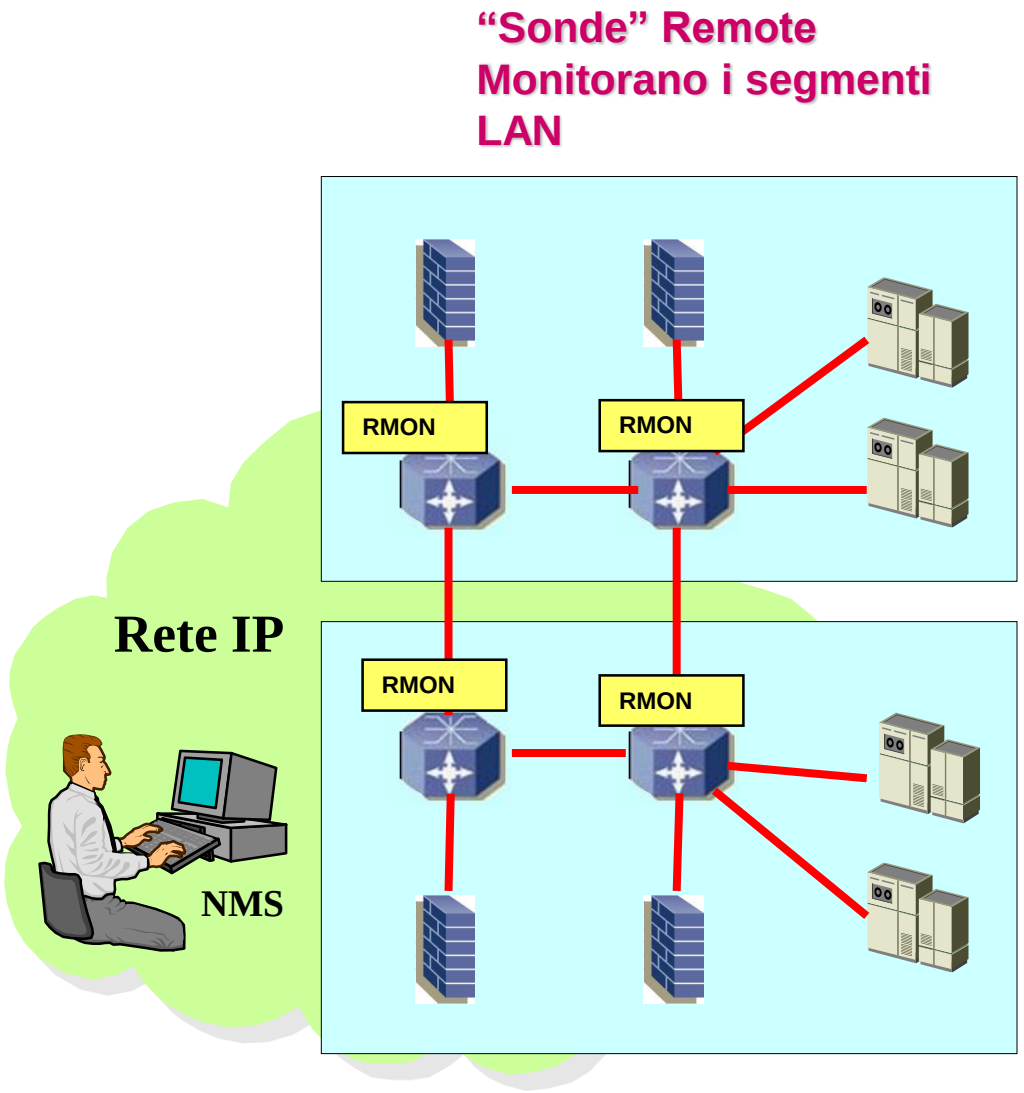
- La piattaforma di gestione
  - Fornisce strumenti generici
  - Permette di lanciare in modo semplice l’esecuzione di strumenti specifici
  - Fa da supporto (archivi, visualizzazione, API di gestione) per l’esecuzione di strumenti specifici

SNMP: RMON (Remote Monitoring)

- Analisi di traffico continua
- Dati inviati al Manager solo su richiesta
  - Riduzione del traffico di gestione
  - Gestione semplificata
  - Maggiore controllo su apparati di rete
  - Riduzione dei costi

- RMON può essere installato su:
  - Sonde dedicate
  - CPU principale dei nodi
  - Blade dedicate su switch modulati

- Configurazione
  - Switch# edit snmp rmon



Firewall Filters

Massimiliano Sbaraglia

Firewall Filter

Firewall Filter sono equivalente a dire Access Control List (ACL) per Cisco.

Stateless firewall filter esamina ogni pacchetto singolarmente (viceversa uno stateful firewall filter, traccia connessioni e ci permette di specificare un azione da prendere per tutti i pacchetti compresi in un flusso di comunicazione).

La natura stateless del firewall filter, quindi, ci porta a considerare la scrittura di un filtro esplicitando il permit del traffico in entrambe le direzioni per ciascuna connessione da permettere.

Viceversa uno stateful firewall filter (non supportato su EX switches) richiede solo di permettere una comunicazione all'inizio eppoi in modo automatico consente il suo passaggio in modo bidirezionale.

E' possibile usare firewall filter per monitoring task.

In EX series switches le firewall filter hanno il controllo in hardware (non in software process).

I tipi di filtri che possiamo applicare sono:

- Port-based: applied to layer 2 switch port in ingress and egress directions
- Vlan-based: applied to layer 2 switch Vlans in the ingress and egress directions
- Router-based : applied to layer 3 routed interfaces in ingress and egress directions

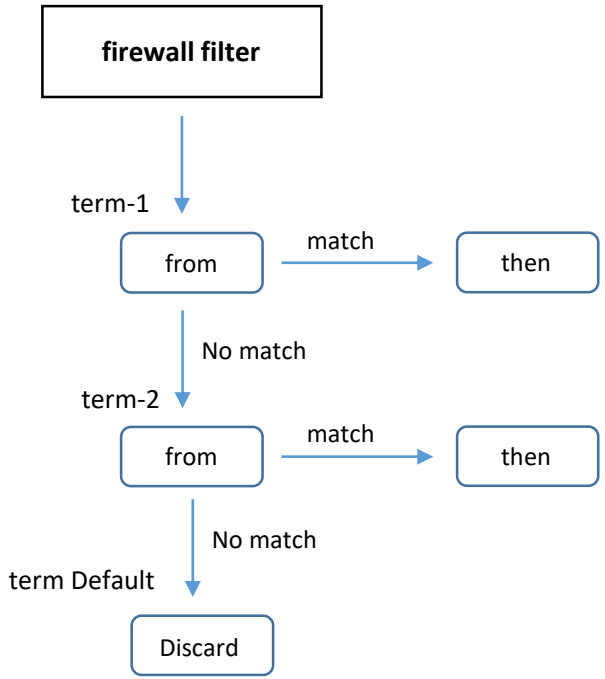
Esempio di Configurazione:

[edit firewall]

edit family any	→ *protocol-independent filter*
edit family ethernet-switching	→ *protocol family ethernet switching for firewall filter*
edit family inet	→ *protocol family IPv4 for firewall filter*
edit family inet6	→ protocol family IPv6 for firewall filter

Firewall Filter Building Block

«Term» è il fondamentale building block per un firewall filter; un «term» contiene zero o più match conditions and una o più actions.



Firewall Filter Matching

Lo switch processa ogni pacchetto attraverso le sue firewall filter configurate.

- Match based on header fields
- Match condition categories
  - Numeric range
  - Address
  - Bit field

```
{master:0}[edit firewall]
user@Switch-1# set family ethernet-switching filter test term test from ?
Possible completions:
+ apply-groups          Groups from which to inherit configuration data
+ apply-groups-except   Don't inherit configuration data from these groups
> destination-address   Match IP destination address
> destination-mac-address  Match MAC destination address
+ destination-port      Match TCP/UDP destination port
> destination-prefix-list  Match IP destination prefixes in named list
+ dot1q-tag             Match Dot1Q Tag Value
+ dot1q-user-priority   Match Dot1Q user priority
+ dscp                  Match Differentiated Services (DiffServ) code point
+ ether-type            Match Ethernet Type
  fragment-flags        Match fragment flags (in symbolic or hex formats) - (Ingress
only)
+ icmp-code             Match ICMP message code
+ icmp-type             Match ICMP message type
> interface             Match interface name
  is-fragment           Match if packet is a fragment
+ precedence            Match IP precedence value
+ protocol              Match IP protocol type
> source-address        Match IP source address
> source-mac-address    Match MAC source address
+ source-port           Match TCP/UDP source port
> source-prefix-list    Match IP source prefixes in named list
  tcp-established       Match packet of an established TCP connection
  tcp-flags             Match TCP flags (in symbolic or hex formats) - (Ingress only)
  tcp-initial           Match initial packet of a TCP connection - (Ingress only)
+ vlan                  Match Vlan Id or Name
```

Firewall Filter Action

Lo switch processa ogni pacchetto attraverso le sue firewall filter configurate.

- Actions
  - accept
  - discard
  - reject

- Action modifiers
  - analyzer.count.log and syslog
  - forwarding-class and loss-priority
  - policer

- Action default
  - discard (in caso di nessuna firewall filter configurata, l'azione di default è accept)

Spanning-Tree Protocol

Massimiliano Sbaraglia

Spanning Tree Protocol Teoria

STP IEEE 802.1d è un protocollo che assicura assenza di loop all'interno di un dominio di switching layer 2; utilizza un valore dello switch chiamato BRIDGE-ID per eleggere il root-switch trasportato all'interno di BPDU di 8 bytes di cui:

- i primi due bytes rappresentano il Bridge Priority assumendo un range di valori decimali da 0 a 65.353 (valore di default = 32.768)
- Gli ultimi sei bytes rappresentano l'indirizzo MAC proprio dello switch

In STP il valore più basso di Bridge-ID è preferito; in caso di parità della priority (valore per il quale uno switch assume il ruolo di root), il secondo passo è quello di confrontare il valore più basso di MAC address tra i due switch in contesa.

Il ruolo delle porte è il seguente:

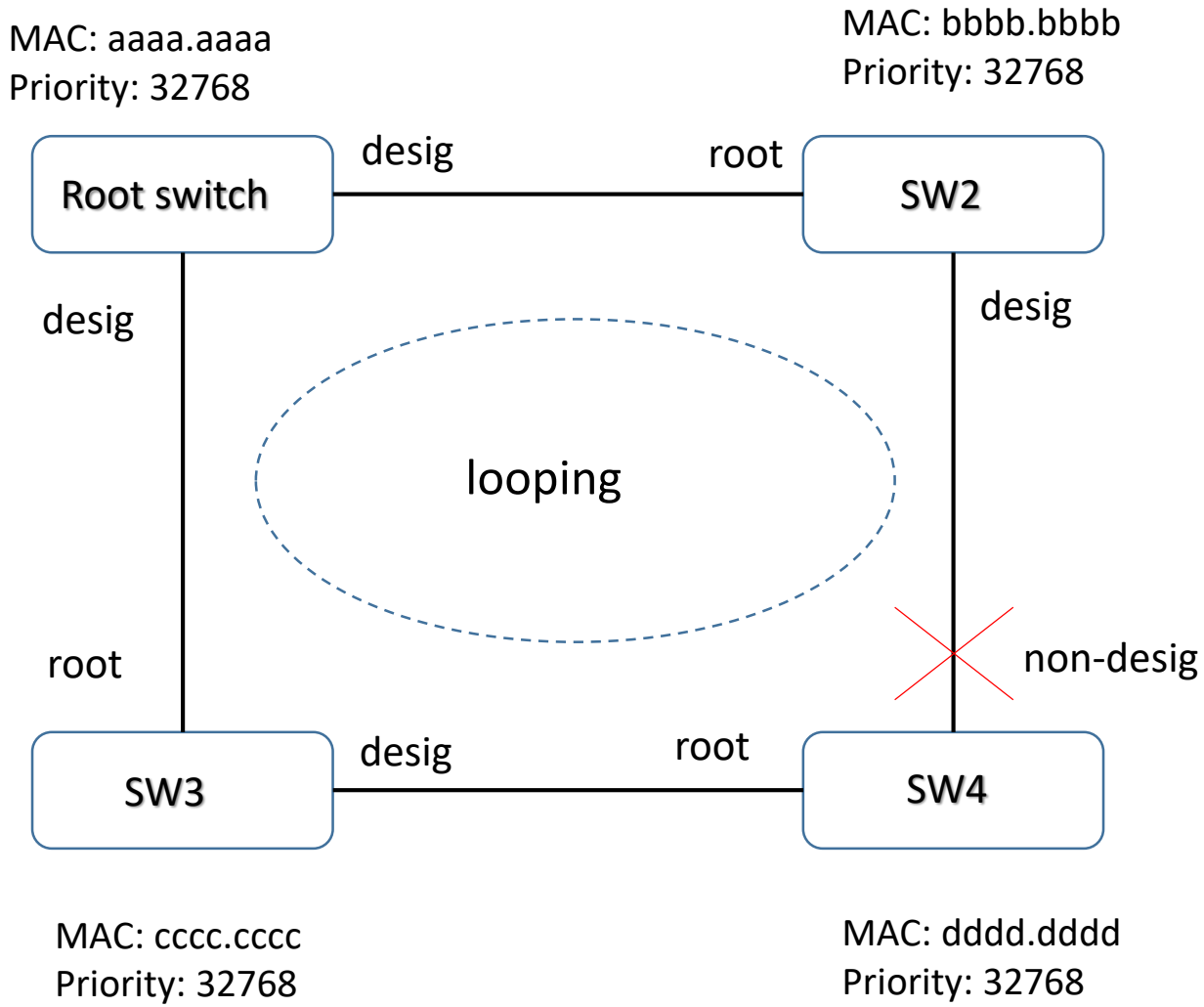
- Listening = la porta sta trasmettendo e ricevendo BPDU (Bridge Protocol Data Unit)
- Learning = acquisisce le informazioni di MAC address del nodo collegato alla porta e permette così la costruzione di una tabella di bridging MAC addresses
- Blocking = non permette nessuna trasmissione di dati user in uscita alla porta (ma resta in ascolto delle BPDU)
- Forwarding = permette la trasmissione e ricezione di dati user e BPDU
- Disable = porta non attiva

Lo status delle porte è il seguente:

- ✓ Root = significa la Best Port in forwarding status con direzione verso il root bridge
- ✓ Designated = in forwarding state per ogni segmento di rete LAN
- ✓ Non-designated = risulta in blocking

Spanning Tree Protocol Teoria

Esempio di design STP IEEE 802.1d:



Spanning Tree Protocol Teoria

RSTP IEEE 802.1w è un protocollo sempre per evitare loop all'interno di un dominio di switching ma a differenza del 802.1d garantisce migliori tempi di convergenza

Il ruolo delle porte è il seguente:

- Forwarding = permette la trasmissione e ricezione di dati user
- Learning = acquisisce le informazioni di MAC address del nodo collegato alla porta e permette così la costruzione di una tabella di bridging MAC addresses
- Discarding = nessun pacchetto è trasmesso dalla porta

Lo status delle porte è il seguente:

- ✓ Root = significa la Best Port in forwarding status con direzione verso il root bridge
- ✓ Designated = in forwarding state per ogni segmento di rete LAN
- ✓ Alternate = in blocking state ma rappresenta il path alternativo verso il root bridge; questo path è differente da quello utilizzato dalla best port.
- ✓ Backup = in blocking state rappresenta il backup (ridondanza) di un path verso un segmento LAN dove un altro switch è invece già connesso.
- ✓ Disable = è possibile in modo amministrativo disabilitare una porta

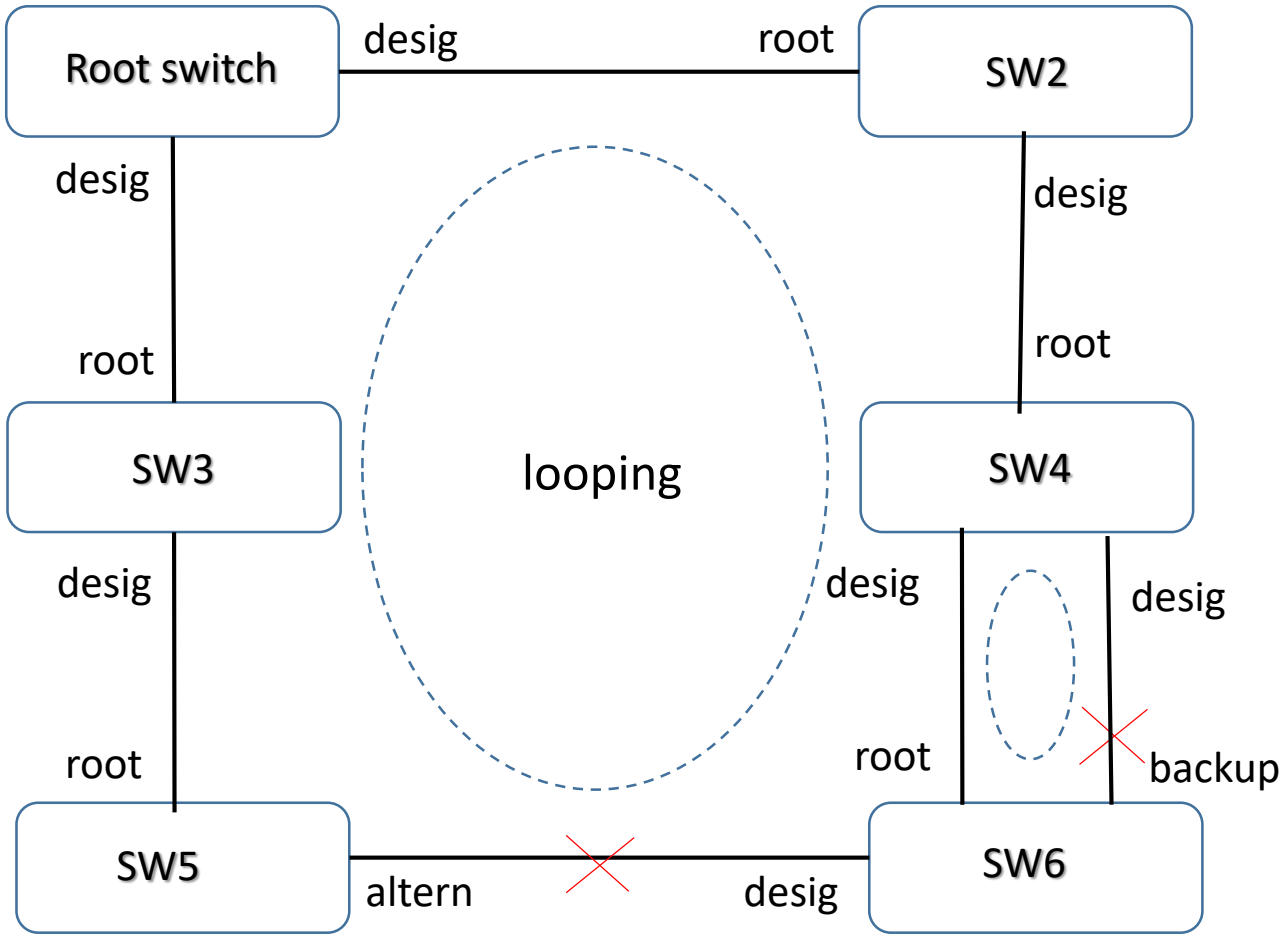
Differenza Tempi di Convergenza:

RSTP: circa 10 sec (spesso anche 2 sec)

STP: 50 secondi

Spanning Tree Protocol Teoria

Esempio di design STP IEEE 802.1w:



Spanning Tree Protocol Teoria

RSTP IEEE 802.1w 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 tra due switch
  - 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 quale può essere un host, server, etc; [attenzione al fatto che queste porte se ricevono BPDU (quindi collegate ad altri switch) perdono il loro ruolo di Edge Port e diventano normali porte STP, andando cosi a generare all'arrivo di BPDU un TCN (Topology Change Notification)

Il best-path è calcolato su base valore del bandwidth interface del link associato ad un valore di costo della porta

DATA RATE	STP COST (802.1D)	RSTP COST (802.1W)
10 Mbit/s	100	2,000,000
16 Mbit/s	62	1,250,000
100 Mbit/s	19	200,000
1 Gbps	4	20,000
2 Gbps	3	10,000
10 Gbps	2	2,000
100 Gbps	NA	200
1 Tbps	NA	20

Spanning Tree Protocol Teoria

MSTP IEEE 802.1s significa avere una istanza STP per un set o region di vlans (Multiple Spanning Tree)

Risulta molto utile nel caso di molte vlan in uso, invece di avere una singola instanza per vlan, ottenere (configurare) differenti regioni associate a gruppi di vlan (ad esempio una regione alla quale appartengono un range di vlan da 2-800 ed un'altra regione con un range da 801-1000)

Questo comporta appunto un numero di istanze minori di STP ed un risparmio in termini di CPU di uno switch rispetto ad esempio RSTP.

BPDU Ethernet Frame

STP utilizza questi pacchetti come segnalazione per costruire il suo albero loop-free; una volta che STP è stabile, lo switch eletto root trasmette BDPU ogni 2 seconds di default

I campi che costituiscono le BPDU sono:

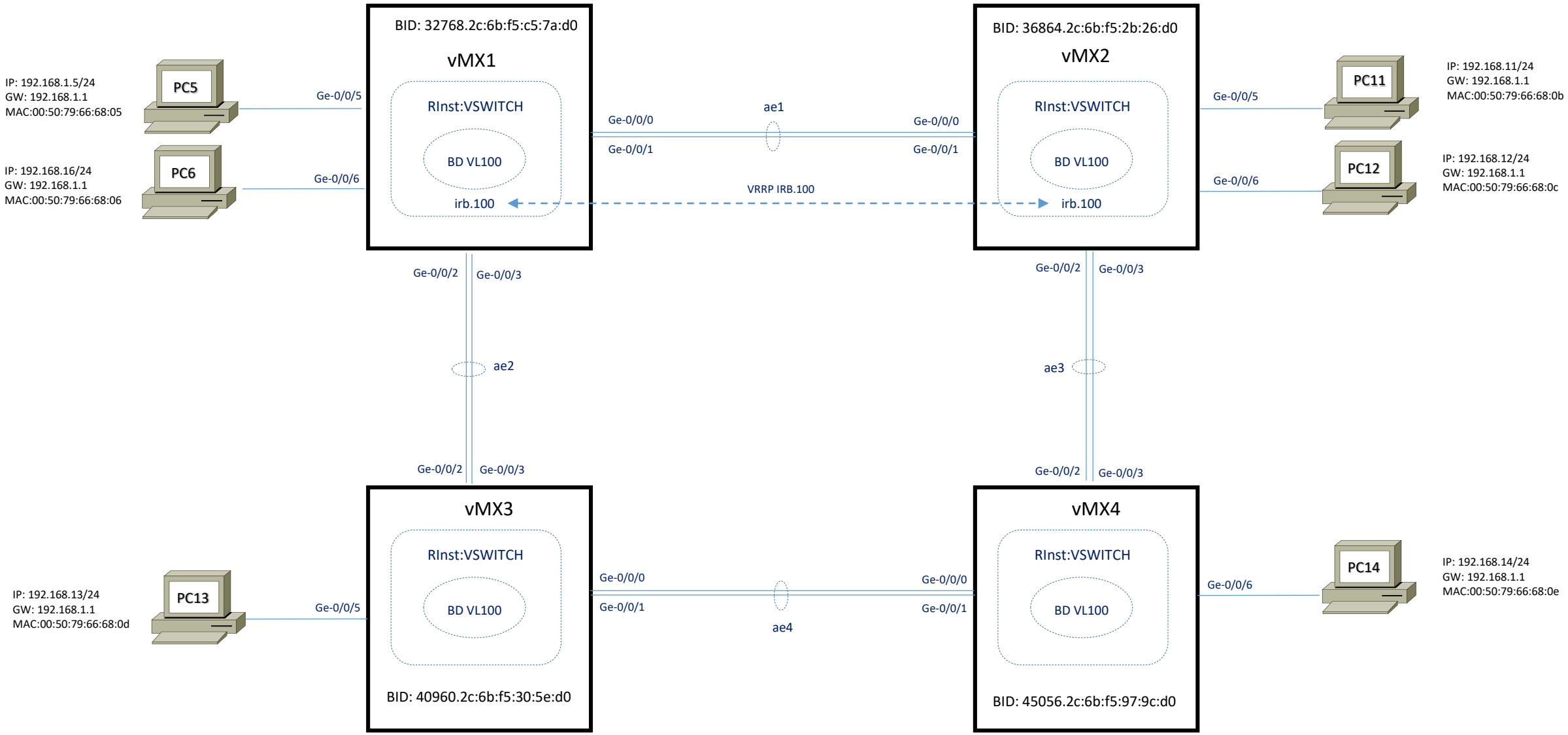
- Protocol ID (2 bytes) = questo valore è sempre 0
- Protocol version (1 bytes) = questo valore è sempre 0
- BPDU Type (1 bytes) = questo campo serve per determinare se la frame BPDU è di tipo Configuration (0x00) oppure TCN (Change Topology = 0x80)
- Flags (1 bytes) = questo campo è utilizzato per gestire changes in una topologia attiva
- Root ID (8 bytes) = contiene il valore di Bridge ID del Root Bridge; dopo la convergenza tutti gli switch debbono avere lo stesso valore per vlan instance
- Root path cost (4 bytes) = è un valore cumulativo in termini di cost di tutti i links a partire dal root bridge
- Bridge ID (8 bytes) = è il valore identificativo del bridge che genera la BPDU; questo valore deve sempre essere lo stesso per tutte le BPDU trasmesse da ogni singolo switch per vlan instance, ma deve essere differenti da tutti gli altri switch presenti nel dominio STP. Il BID è una combinazione del valore di priority (default = 32.768) dello switch sender ed il valore di MAC Address.
- Port ID (2 bytes) = contiene un valore unico per ciascuna porta; questo valore è una combinazione del priority della porta outbound ed un unico ID che rappresenta la porta stessa (di default la priority port = 128). Un esempio può essere indicato dalla porta ge-1/0/0 con valore pari a 128:513 e la porta ge-1/0/1 con valore pari a 128:514; ad ogni porta è associato un costo inversamente proporzionale alla velocità
- Message Age (2 bytes)= questo valore memorizza un tempo da quando il root bridge ha generato le informazioni dalle quali il corrente BPDU è derivato
- Max Age (2 bytes) = questo valore indica un tempo massimo per cui una determinata BPDU è stata salvata (range = 6 – 40 sec; default = 20 sec)
- Hello Time (2 bytes) = questo valore misura il tempo di trasmissione tra periodici BPDU configuration (default = 2 sec)
- Forward Delay (2 bytes) = questo valore misura il tempo che uno switch utilizza nello status di listening e learning ed influenza anche i timers durante un processo di TCN (range = 4 – 30 sec; defaut = 15 sec)

RSTP Configuration Parameters

Configurazione con parametri di default:

```
set protocols rstp bridge priority 32k
set protocol rstp max-age 20
set protocol rstp hello-time 2
set protocol rstp forward-delay 15
set protocol rstp interface ge-0/0/8.0 disable                    # esclude la porta dal partecipare al protocollo RSTP
}
 set interface ge-0/0/1.0 cost 20000                              # valore del costo per interfaccia a 1 GBps
set interface ge-0/0/1.0 mode point-to-point                      # default mode per interfaccia operativa in full-duplex
}
set interface ge-0/0/2.0 priority 128                             # default valore usato per influenzare i downstream switches ad utilizzare il percorso a minor costo verso il root-switch
set interface ge-0/0/2.0 mode shared                              # default mode per interfaccia operativa in half-duplex
}
set interface ge-0/0/3.0 mode edge                                # default mode per interfaccia NON connessa ad altro switch operante con RSTP (ma solo a devices NO-STP enabled)
```

RSTP LAB Junos Switches



RSTP Verifica MAC table from vMX1

```
root@vMX1> show bridge mac-table

MAC flags       (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
    O -OVSDB MAC, SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC,
P -Pinned MAC)

Routing instance : VSWITCH
 Bridging domain : VL-100, VLAN : 100
   MAC               MAC      Logical         NH     MAC        active
   address           flags    interface       Index  property   source
   00:50:79:66:68:05 D        ge-0/0/5.0
   00:50:79:66:68:06 D        ge-0/0/6.0
   00:50:79:66:68:0d D        ae2.0
   00:50:79:66:68:0e D        ae1.0

{master}
root@vMX1>
```

RSTP Verifica MAC table from vMX2

```
root@vMX2> show bridge mac-table

MAC flags       (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
    O -OVSDB MAC, SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC,
P -Pinned MAC)

Routing instance : VSWITCH
 Bridging domain : VL-100, VLAN : 100
   MAC               MAC      Logical         NH     MAC        active
   address           flags    interface       Index  property   source
   00:00:5e:00:01:64 D        ae1.0                             # VRRP Mac address
   00:50:79:66:68:06 D        ae1.0
   00:50:79:66:68:0e D        ae3.0
   2c:6b:f5:c5:7a:f0 D        ae1.0

root@vMX2>
```

RSTP Verifica MAC table from vMX3

```
root@vMX3> show bridge mac-table

MAC flags       (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
    O -OVSDB MAC, SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC,
P -Pinned MAC)

Routing instance : VSWITCH
 Bridging domain : VL-100, VLAN : 100
   MAC               MAC      Logical         NH     MAC        active
   address           flags    interface       Index  property   source
   00:00:5e:00:01:64 D        ae2.0
   00:50:79:66:68:0d D        ge-0/0/5.0
   00:50:79:66:68:0e D        ae2.0
   2c:6b:f5:c5:7a:f0 D        ae2.0

root@vMX3>
```

RSTP Verifica MAC table from vMX4

```
root@vMX4> show bridge mac-table

MAC flags       (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
    O -OVSDB MAC, SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC,
P -Pinned MAC)

Routing instance : VSWITCH
 Bridging domain : VL-100, VLAN : 100
   MAC               MAC      Logical          NH     MAC        active
   address           flags    interface        Index  property   source
   00:00:5e:00:01:64 D        ae3.0
   00:50:79:66:68:0d D        ae3.0
   00:50:79:66:68:0e D        ge-0/0/6.0
   2c:6b:f5:c5:7a:f0 D        ae3.0

root@vMX4>
```

RSTP Configuration vMX1: chassis and interfaces

```
chassis {
  aggregated-devices {
     ethernet {
        device-count 8;
}
interfaces {
   ge-0/0/0 {
      gigether-options {
         802.3ad ae1;
 }
   ge-0/0/1 {
      gigether-options {
         802.3ad ae1;
 }
    ge-0/0/2 {
      gigether-options {
         802.3ad ae2;
}
 ge-0/0/3 {
     gigether-options {
        802.3ad ae2;
     }
  }
  ge-0/0/5 {
     encapsulation ethernet-bridge;
     unit 0 {
        family bridge;
     }
  }
  ge-0/0/6 {
     encapsulation ethernet-bridge;
     unit 0 {
        family bridge;
     }
  }
ae1 {
     description lacp_to_mx2;
     vlan-tagging;
     encapsulation flexible-ethernet-services;
     aggregated-ether-options {
        lacp {
           active;
        }
     }
       unit 0 {
         encapsulation vlan-bridge;
          vlan-id 100;
          family bridge;
     }
  }
ae2 {
     description lacp_to_mx3;
     vlan-tagging;
     encapsulation flexible-ethernet-services;
     aggregated-ether-options {
        lacp {
           active;
        }
     }
     unit 0 {
        encapsulation vlan-bridge;
        vlan-id 100;
        family bridge;
     }
   }
irb {
     unit 100 {
        family inet {
           address 192.168.1.2/24 {
              vrrp-group 100 {
                 virtual-address 192.168.1.1;
                 priority 110;
                 preempt;
                 accept-data;
              }
           }
        }
     }
   }
}
```

RSTP Configuration vMX1: Routing-Instances virtual-switch VSWITCH

```
VSWITCH {
    instance-type virtual-switch;
    protocols {
        rstp {
            bridge-priority 32k;
            max-age 20;
            hello-time 2;
            forward-delay 15;
            interface ae1;
            interface ae2;
        }
    }
    bridge-domains {
        VL-100 {
            vlan-id 100;
            interface ae1.0;
            interface ae2.0;
            interface ge-0/0/5.0;
            interface ge-0/0/6.0;
            routing-interface irb.100;
        }
```

RSTP Configuration vMX2: chassis and interfaces

```
chassis {
  aggregated-devices {
     ethernet {
        device-count 8;
}
interfaces {
   ge-0/0/0 {
      gigether-options {
         802.3ad ae1;
 }
   ge-0/0/1 {
      gigether-options {
         802.3ad ae1;
 }
    ge-0/0/2 {
      gigether-options {
         802.3ad ae3;
}
 ge-0/0/3 {
     gigether-options {
        802.3ad ae3;
     }
  }
  ge-0/0/5 {
     encapsulation ethernet-bridge;
     unit 0 {
        family bridge;
     }
  }
  ge-0/0/6 {
     encapsulation ethernet-bridge;
     unit 0 {
        family bridge;
     }
  }
ae1 {
     description lacp_to_mx1;
     vlan-tagging;
     encapsulation flexible-ethernet-services;
     aggregated-ether-options {
        lacp {
           active;
        }
     }
       unit 0 {
         encapsulation vlan-bridge;
          vlan-id 100;
          family bridge;
     }
  }
ae3 {
     description lacp_to_mx4;
     vlan-tagging;
     encapsulation flexible-ethernet-services;
     aggregated-ether-options {
        lacp {
           active;
        }
     }
     unit 0 {
        encapsulation vlan-bridge;
        vlan-id 100;
        family bridge;
     }
   }
irb {
     unit 100 {
        family inet {
           address 192.168.1.2/24 {
              vrrp-group 100 {
                 virtual-address 192.168.1.1;
                 preempt;
                 accept-data;
              }
           }
        }
     }
   }
}
```

RSTP Configuration vMX2: Routing-Instances virtual-switch VSWITCH

```
VSWITCH {
    instance-type virtual-switch;
    protocols {
        rstp {
            bridge-priority 36k;
            max-age 20;
            hello-time 2;
            forward-delay 15;
            interface ae1;
            interface ae3;
        }
    }
    bridge-domains {
        VL-100 {
            vlan-id 100;
            interface ae1.0;
            interface ae3.0;
            interface ge-0/0/5.0;
            interface ge-0/0/6.0;
            routing-interface irb.100;
        }
```

RSTP Configuration vMX3: chassis and interfaces

```
chassis {
  aggregated-devices {
      ethernet {
          device-count 8;
}
interfaces {
   ge-0/0/0 {
      gigether-options {
          802.3ad ae4;
 }
   ge-0/0/1 {
      gigether-options {
          802.3ad ae4;
 }
    ge-0/0/2 {
      gigether-options {
          802.3ad ae2;
}
```

```
ge-0/0/3 {
    gigether-options {
       802.3ad ae2;
    }
 }
 ge-0/0/5 {
    encapsulation ethernet-bridge;
    unit 0 {
       family bridge;
    }
 }
 ge-0/0/6 {
    encapsulation ethernet-bridge;
    unit 0 {
       family bridge;
    }
 }
```

```
ae2 {
    description lacp_to_mx1;
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
       lacp {
          active;
       }
    }
      unit 0 {
        encapsulation vlan-bridge;
         vlan-id 100;
         family bridge;
    }
  }
ae4 {
    description lacp_to_mx4;
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
       lacp {
          active;
       }
    }
    unit 0 {
       encapsulation vlan-bridge;
       vlan-id 100;
       family bridge;
    }
  }
```

RSTP Configuration vMX3: Routing-Instances virtual-switch VSWITCH

```
VSWITCH {
    instance-type virtual-switch;
    protocols {
        rstp {
            bridge-priority 40k;
            max-age 20;
            hello-time 2;
            forward-delay 15;
            interface ae2;
            interface ae4;
        }
    }
    bridge-domains {
        VL-100 {
            vlan-id 100;
            interface ae2.0;
            interface ae4.0;
            interface ge-0/0/5.0;
```

RSTP Configuration vMX4: chassis and interfaces

```
chassis {
  aggregated-devices {
      ethernet {
          device-count 8;
}
interfaces {
   ge-0/0/0 {
      gigether-options {
          802.3ad ae4;
 }
   ge-0/0/1 {
      gigether-options {
          802.3ad ae4;
 }
    ge-0/0/2 {
      gigether-options {
          802.3ad ae3;
}
```

```
ge-0/0/3 {
    gigether-options {
       802.3ad ae3;
    }
 }
 ge-0/0/5 {
    encapsulation ethernet-bridge;
    unit 0 {
       family bridge;
    }
 }
 ge-0/0/6 {
    encapsulation ethernet-bridge;
    unit 0 {
       family bridge;
    }
 }
```

```
ae2 {
    description lacp_to_mx1;
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
       lacp {
          active;
       }
    }
      unit 0 {
        encapsulation vlan-bridge;
         vlan-id 100;
         family bridge;
    }
  }
ae4 {
    description lacp_to_mx4;
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    aggregated-ether-options {
       lacp {
          active;
       }
    }
    unit 0 {
       encapsulation vlan-bridge;
       vlan-id 100;
       family bridge;
    }
  }
```

RSTP Configuration vMX4: Routing-Instances virtual-switch VSWITCH

```
VSWITCH {
    instance-type virtual-switch;
    protocols {
        rstp {
            bridge-priority 44k;
            max-age 20;
            hello-time 2;
            forward-delay 15;
            interface ae3;
            interface ae4;
        }
    }
    bridge-domains {
        VL-100 {
            vlan-id 100;
            interface ae2.0;
            interface ae4.0;
            interface ge-0/0/6.0;
```

RSTP Verifica Elezione Root Bridge from vMX1

root@vMX1> show spanning-tree bridge routing-instance VSWITCH detail

STP bridge parameters

Routing instance name : VSWITCH

Context ID : 1

Enabled protocol : RSTP

Root ID : 32768.2c:6b:f5:c5:7a:d0

Hello time : 2 seconds

Maximum age : 20 seconds

Forward delay : 15 seconds

Message age : 0

Number of topology changes : 4

Time since last topology change : 254 seconds

Local parameters

Bridge ID : 32768.2c:6b:f5:c5:7a:d0

Extended system ID : 0

Hello time : 2 seconds

Maximum age : 20 seconds

Forward delay : 15 seconds

Path cost method : 32 bit

RSTP Verifica Elezione Root Bridge from vMX2

root@vMX1> show spanning-tree bridge routing-instance VSWITCH detail

STP bridge parameters

Routing instance name : VSWITCH

Context ID : 1

Enabled protocol : RSTP

Root ID : 32768.2c:6b:f5:c5:7a:d0

Root cost : 10000

Root Port : ae1

Hello time : 2 seconds

Maximum age : 20 seconds

Forward delay : 15 seconds

Message age : 1

Number of topology changes : 2

Time since last topology change : 393 seconds

Local parameters

Bridge ID : 36864.2c:6b:f5:2b:26:d0

output omitted (ext-system-id, hello-time, max-age, forward-delay, path cost method)

RSTP Verifica Elezione Root Bridge from vMX3

root@vMX1> show spanning-tree bridge routing-instance VSWITCH detail

STP bridge parameters

Routing instance name : VSWITCH

Context ID : 1

Enabled protocol : RSTP

Root ID : 32768.2c:6b:f5:c5:7a:d0

Root cost : 10000

Root Port : ae2

Hello time : 2 seconds

Maximum age : 20 seconds

Forward delay : 15 seconds

Message age : 1

Number of topology changes : 2

Time since last topology change : 999 seconds

Local parameters

Bridge ID :40960.2c:6b:f5:30:5e:d0

output omitted (ext-system-id, hello-time, max-age, forward-delay, path cost method)

RSTP Verifica Elezione Root Bridge from vMX4

root@vMX1> show spanning-tree bridge routing-instance VSWITCH detail

STP bridge parameters

Routing instance name : VSWITCH

Context ID : 1

Enabled protocol : RSTP

Root ID : 32768.2c:6b:f5:c5:7a:d0

Root cost : 20000

Root Port : ae3

Hello time : 2 seconds

Maximum age : 20 seconds

Forward delay : 15 seconds

Message age : 1

Number of topology changes : 2

Time since last topology change : 1075 seconds

Local parameters

Bridge ID : 45056.2c:6b:f5:97:9c:d0

output omitted (ext-system-id, hello-time, max-age, forward-delay, path cost method)

RSTP Verifica Interface Detail from vMX1

root@vMX1> show spanning-tree interface routing-instance VSWITCH detail

Spanning tree interface parameters for instance 0

Interface name : ae1

Port identifier : 128.4

Designated port ID : 128.4

Port cost : 10000

Port state : Forwarding

Designated bridge ID : 32768.2c:6b:f5:c5:7a:d0

Port role : Designated

Link type : Pt-Pt/NONEDGE

Interface name : ae2

Port identifier : 128.5

Designated port ID : 128.5

Port cost : 10000

Port state : Forwarding

Designated bridge ID : 32768.2c:6b:f5:c5:7a:d0

Port role : Designated

Link type : Pt-Pt/NONEDGE

RSTP Verifica Interface Detail from vMX2

root@vMX1> show spanning-tree interface routing-instance VSWITCH detail

Spanning tree interface parameters for instance 0

Interface name : ae1

Port identifier : 128.4

Designated port ID : 128.4

Port cost : 10000

Port state : Forwarding

Designated bridge ID : 32768.2c:6b:f5:c5:7a:d0

Port role : Root

Link type : Pt-Pt/NONEDGE

Interface name : ae3

Port identifier : 128.6

Designated port ID : 128.6

Port cost : 10000

Port state : Forwarding

Designated bridge ID : 36864.2c:6b:f5:2b:26:d0

Port role : Designated

Link type : Pt-Pt/NONEDGE

RSTP Verifica Interface Detail from vMX3

root@vMX1> show spanning-tree interface routing-instance VSWITCH detail

Spanning tree interface parameters for instance 0

Interface name : ae2

Port identifier : 128.5

Designated port ID : 128.5

Port cost : 10000

Port state : Forwarding

Designated bridge ID : 32768.2c:6b:f5:c5:7a:d0

Port role : Root

Link type : Pt-Pt/NONEDGE

Interface name : ae4

Port identifier : 128.7

Designated port ID : 128.7

Port cost : 10000

Port state : Forwarding

Designated bridge ID : 40960.2c:6b:f5:30:5e:d0

Port role : Designated

Link type : Pt-Pt/NONEDGE

RSTP Verifica Interface Detail from vMX4

root@vMX1> show spanning-tree interface routing-instance VSWITCH detail

Spanning tree interface parameters for instance 0

Interface name : ae3

Port identifier : 128.6

Designated port ID : 128.6

Port cost : 10000

Port state : Forwarding

Designated bridge ID : 36864.2c:6b:f5:2b:26:d0 *# questo è lo switch vMX2 direttamente connesso to root bridge preferito*

Port role : Root

Link type : Pt-Pt/NONEDGE

Interface name : ae4

Port identifier : 128.7

Designated port ID : 128.7

Port cost : 10000

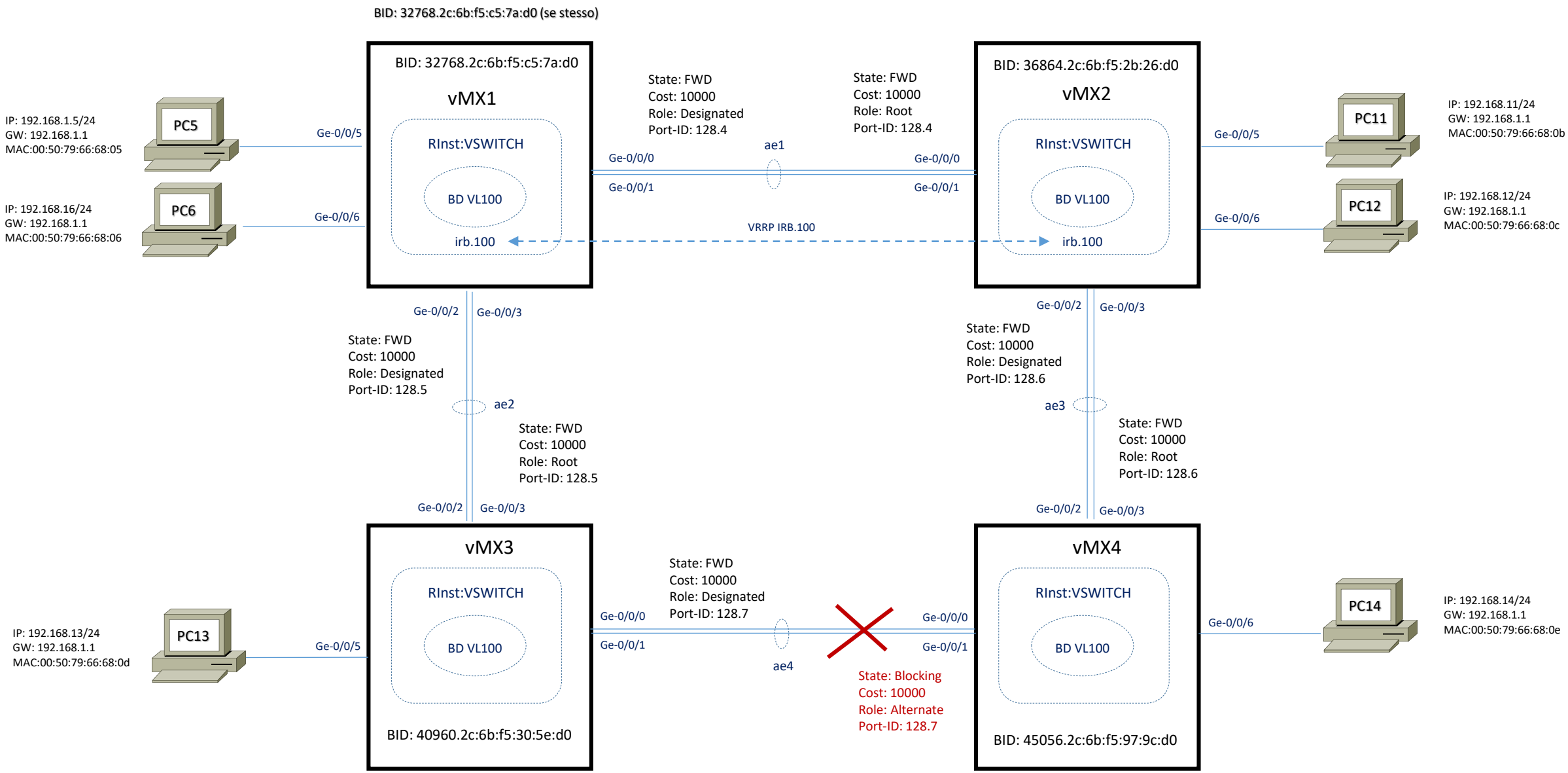
Port state : Blocking

Designated bridge ID : 40960.2c:6b:f5:30:5e:d0

Port role : Alternate

Link type : Pt-Pt/NONEDGE

RSTP LAB Junos Switches dopo convergenza protocollo (root-bridge election and status port)



Spanning-Tree Protocol Prevention Features

Massimiliano Sbaraglia

BPDU Protection

Scenario con Rogue Switch:

Poiché uno switch esterno comunque partecipa al processo STP questo trasmette e riceve BPDU frames, di fatto provocando un ricalcolo del protocollo stesso e quando questo è terminato il rogue switch è parte integrante del sistema STP (questo ha un impatto negativo in termini di performance e gestione della rete stessa ad esempio un potenziale loop layer 2 con conseguenza disastrose).

Abilitando meccanismi di protezione BPDU su porte per le quali se ricevono queste frames, l'interfaccia è disabilitata e transita in una status di blocking; è possibile usare drop option per scartare BPDU entranti, permettendo al tempo stesso di trasmettere traffico legittimo

Configurazione con STP abilitato:

set protocol rstp interface ge-0/0/6 edge

set protocol rstp bpdu-block-on-edge

Verifica BPDU prima della protezione:

show spanning-tree interface ge-0/0/6 → state = FWD and Role = DESG

Verifica BPDU dopo enable della protezione:

show spanning-tree interfaces ge-0/0/6 → state = BLK

Per sbloccare la porta:

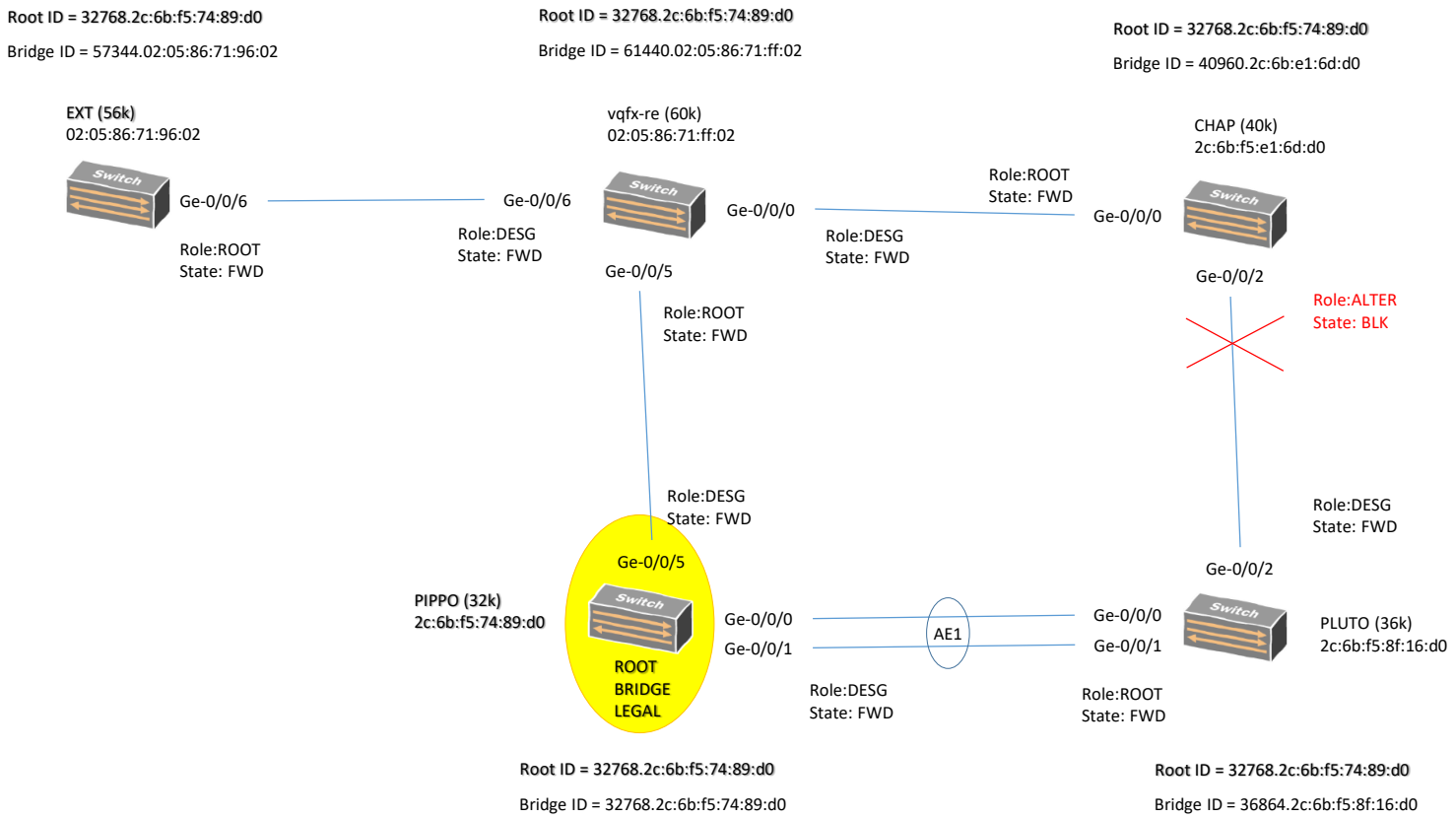
clear ethernet-switching bpdu-error oppure

set ethernet-switching-option bpdu-block disable-timeout <10..3600 sec)

BPDU Protection

Scenario con Rogue Switch (EXT):

- EXT ha un BRIDGE-ID alto e pertanto non influenza un cambio di Root Bridge



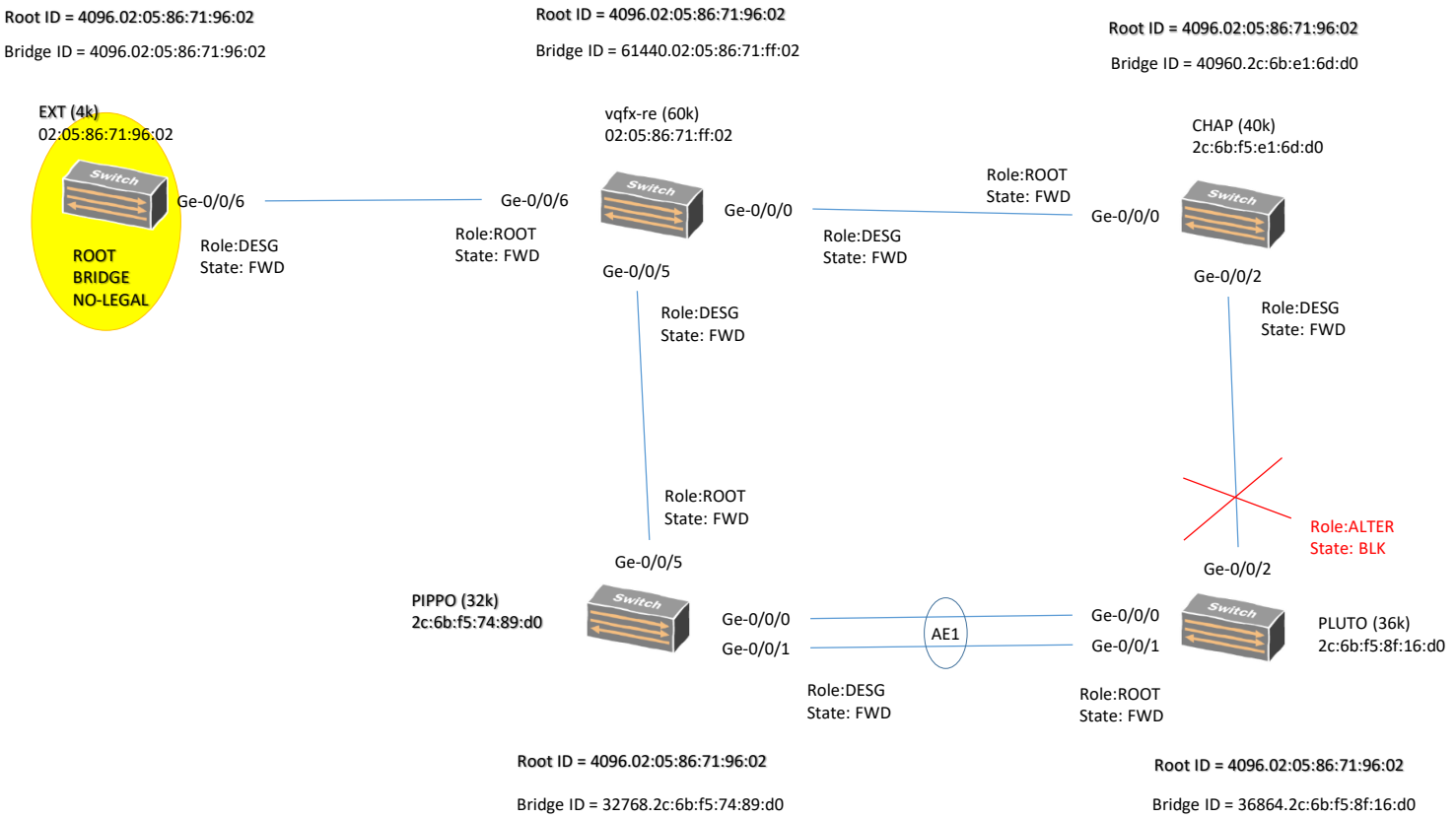
BPDU Protection

Scenario con Rogue Switch (EXT):

- EXT ha un BRIDGE-ID basso e pertanto influenza un cambio di Root Bridge (Change Topology)

root@vqfx-re> show spanning-tree statistics interface

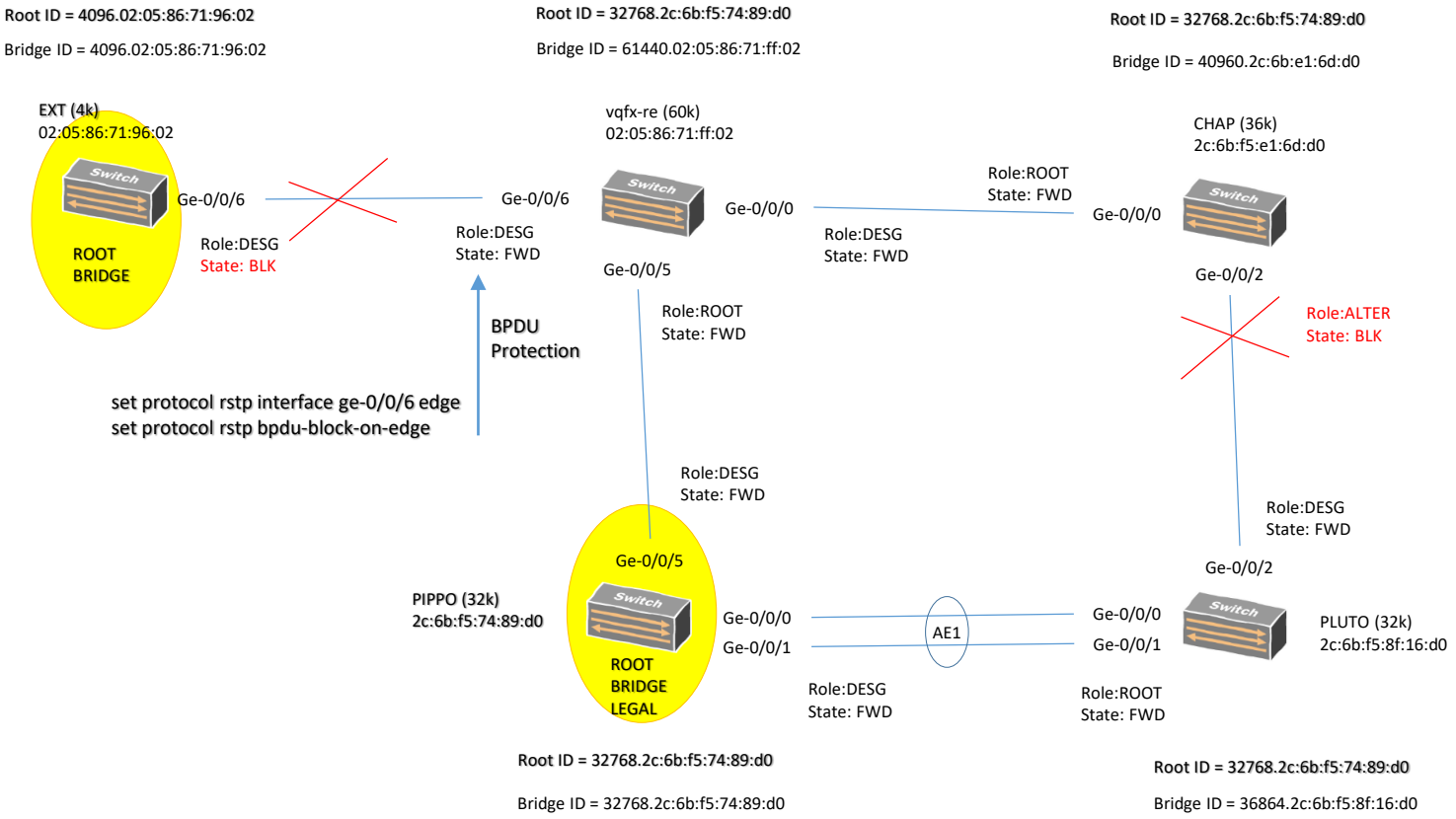
Interface	BPDUs Sent	BPDUs Received	Next BPDU Transmission	TCs Tx/Rx	Proposal Tx/Rx	Agreement Tx/Rx
xe-0/0/0	30060	62	1	0/37	0/4	30060/46
xe-0/0/5	23193	7794	1	0/28	0/12	23193/17
xe-0/0/6	2554	25109	0	0/19	0/2053	2554/22747



BPDU Protection

Scenario con Rogue Switch (EXT):

- EXT ha un BRIDGE-ID basso e pertanto influenza un cambio di Root Bridge (Change Topology)



Loop Protection

È necessario abilitare un sistema di loop protection in tutte le porte in non-designated role.

Quando il loop protection è abilitato, il protocollo STP rileva root ports e blocked ports ed assicura che entrambe stanno ricevendo BPDU. Se una porta con loop protection abilitato interrompe la ricezione di BPDU da una designated port ad essa collegata, questa reagisce mettendo la porta in uno role di loop-inconsistence eppoi transita in uno status di blocking quando riceve una nuova BPDU.

E' raccomandabile inserire il loop-protection su tutte quelle porte che hanno possibilità di diventare root port oppure designated port

Configurazione SW3 (example)

set protocol rstp interface ge-0/0/10.0 bpdu-timeout-action block *# al posto di block si può usare alarm*

set protocol rstp interface ge-0/0/12.0 bpdu-timeout-action block *# al posto di block si può usare alarm*

NOTA:

Con il temine block, se una violazione esiste, la porta entra immediatamente in uno ruolo di DIS (Loop-Incons) e stata di blocking.

Con il termine alarm, questa non forza a cambiare il ruolo della porta ma semplicemente rescrive in log messages nel log file.

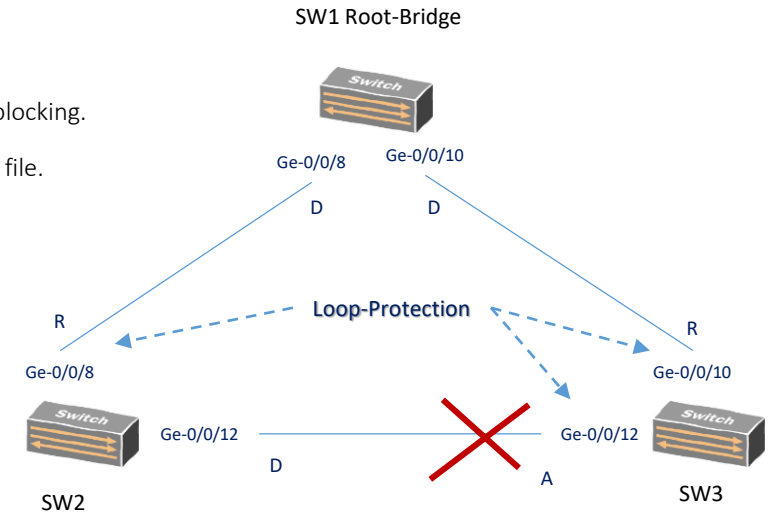
Se questa ultima opzione è utilizzata la porta assume il role di DESG e state di FWD una volta che il suo max-age termina.

Una porta può essere configurata sia per loop-protection oppure root protection, ma non entrambe

Verifica

show spanning-tree interface <interface>

show log message | match «loop|protect»



Root Protection

È necessario abilitare un sistema di root protection in tutte le porte che dovrebbero non ricevere superior BPDU e non dovrebbero mai essere elette a root port.

Se uno switch riceve BPDU di valore superiore in una porta con root-protection abilitato, questa porta transita in uno ruolo di Inconsistency con status di blocking; questo previene uno switch (che non deve mai essere un root bridge) a diventare appunto root bridge.

Configurazione SW1 (Root Bridge):

set protocol rstp bridge-priority 4k

set protocol rstp interface all no-root-port

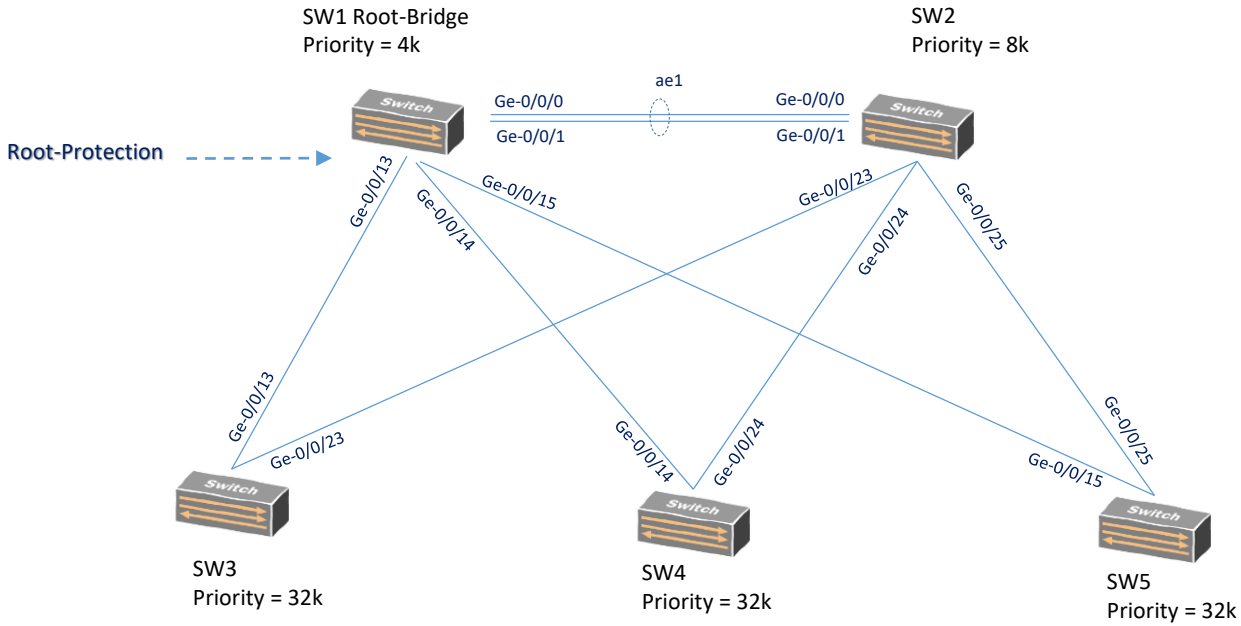
Configurazione SW2:

set protocol rstp bridge-priority 8k

set protocol rstp interface ge-0/0/23.0 no-root-port

set protocol rstp interface ge-0/0/24.0 no-root-port

set protocol rstp interface ge-0/0/25.0 no-root-port



Verifica from SW1 prima che una superior BPDU arriva su una porta protetta

show spanning-tree interface

Ge-0/0/13.0 with state = FWD and Role = DESG

Verifica from SW1 dopo che una superior BPDU arriva su una porta protetta

show spanning-tree interface

Ge-0/0/13.0 with state = BLK and Role = ALT (Root-Incon)

Ethernet OAM

Massimiliano Sbaraglia

Ethernet OAM features

Ethernet OAM (Operation, Administration and Maintanance) è un meccanismo di controllo della operatività per un link IEEE 802.3ah LFM di tipo P2P ethernet e lavora attaverso:

- Discovery and link monitoring:
    - Active Mode: le interfacce dei peer scoprono e monitorano i link di collegamento dei peer se essi supportano entrambi la funzionalità OAM 802.3ah
    - Passive Mode: un peer inizia il processo di discovery ed appena in funzione entrambi i peer partecipano al processo stesso; lo switch performa il link monitoring inviando specifiche OAMPDU.
- remote failure detection
- remote loopback control

ed utilizza frame conosciute come OAMPDU standardizzate in IEEE 802.3ah clause 57)

Per link monitoring si intende la trasmissione di OAMPDU in modo periodico e trasportano informazioni relative a capability ed event notification. Dying gasp si riferisce al remote failure indication e le OAMPDU sono trasmesse in caso di down di un nodo; dedicate codifiche sono create in relazioni al tipo di evento (admin shutdown, power loss, reboot).

Il peer neighbor che riceve queste OAMPDU reagisce secondo l'azione configurata.

- SNMP trap
- Syslog message
- Interface disable
- Active interworking mechanism

Remote loopback è utile per differenti use-case in particolare per operazioni di troubleshooting; quando una interfaccia riceve una frame non OAM-PDU (pause frame), il peer la trasmette indietro (back) sulla stessa interfaccia da cui l'ha ricevuta e questo significa uno stato active del link. E' possibile utilizzarla per testare delay, jitter ed anche il throughput di un link.

Ethernet OAM features

- IEEE 802.3ah: provvede ad un link-local keepalive scambiato tra due peer con adianceza L2-capable (ethernet)
- IEEE802.3ag: provvede sempre ad un gerarchico end-to-end keepalive ma tra peer remote che non necessariamente sono direttamente collegati tra loro.

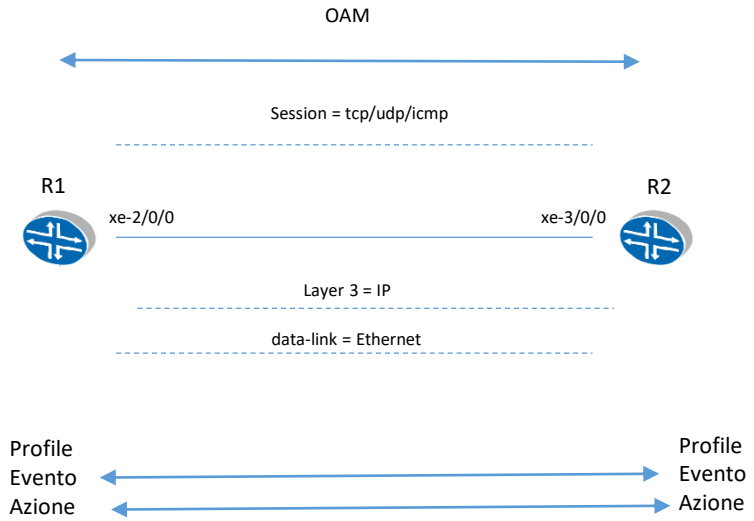
E’ possibile creare dei profili specifici assegnando ad esse eventi e relative azioni:

ESEMPIO:

Profile	Evento	Azione
OAM BASIC	LINK-ADJACENCY-LOSS	SYSLOG
OAM EVENTS	LINK-EVENT-RATE: FRAME ERROR 4 LINK-EVENT-RATE: SYMBOL PERIOD 4	SYSLOG
OAM BACK-ADJ	LINK-ADJACENCY-LOSS	SYSLOG
OAM BACK FRAMEPERIOD	LINK-EVENT-RATE: FRAME ERROR 1	SYSLOG
OAM BACK SYMBOL	LINK-EVENT-RATE: SYMBOL PERIOD 1	SYSLOG

Ethernet OAM Configurations (esempio)

```
set protocols oam ethernet link-fault-management traceoptions file traceoam
set protocols oam ethernet link-fault-management traceoptions file size 4m
set protocols oam ethernet link-fault-management traceoptions flag protocol
!
set protocols oam ethernet link-fault-management action-profile oam_basic event link-adjacency-loss
set protocols oam ethernet link-fault-management action-profile oam_basic action syslog
!
set protocols oam ethernet link-fault-management action-profile oam_events event link-event-rate symbol-period 4
set protocols oam ethernet link-fault-management action-profile oam_events event link-event-rate frame-error 4
set protocols oam ethernet link-fault-management action-profile oam_events action syslog
!
set protocols oam ethernet link-fault-management action-profile oam_back-adj event link-adjacency-loss
set protocols oam ethernet link-fault-management action-profile oam_back-adj action syslog
!
set protocols oam ethernet link-fault-management action-profile oam_back-frame period event link-event-rate frame-period 1
set protocols oam ethernet link-fault-management action-profile oam_back-frame period action syslog
!
set protocols oam ethernet link-fault-management action-profile oam_back-symbol event link-event-rate symbol-period 1
set protocols oam ethernet link-fault-management action-profile oam_back-symbol action syslog
!
```



Ethernet OAM Configurations (esempio)

I suddetti profili poi debbono essere applicate alle interfacce (La logica applicate è quella di assegnare alle interface 10G gli ultimi tre profili indicati nella tabella e settare un link-discovery active, mentre per le interface 1G sono stati assegnati I primi due profili e settare un link-discovery passive.

ESEMPIO:

set protocols oam ethernet link-fault-management interface xe-2/0/2 apply-action-profile oam_back-symbol

set protocols oam ethernet link-fault-management interface xe-2/0/2 apply-action-profile oam_back-frame period

set protocols oam ethernet link-fault-management interface xe-2/0/2 apply-action-profile oam_back-adj

set protocols oam ethernet link-fault-management interface xe-2/0/2 pdu-interval 500

set protocols oam ethernet link-fault-management interface xe-2/0/2 link-discovery active

set protocols oam ethernet link-fault-management interface xe-2/0/2 pdu-threshold 3

set protocols oam ethernet link-fault-management interface xe-2/0/2 event-thresholds symbol-period 1

set protocols oam ethernet link-fault-management interface xe-2/0/2 event-thresholds frame-error 1

!

set protocols oam ethernet link-fault-management interface ge-0/0/0 apply-action-profile oam_events

set protocols oam ethernet link-fault-management interface ge-0/0/0 apply-action-profile oam_basic

set protocols oam ethernet link-fault-management interface ge-0/0/0 pdu-interval 1000

set protocols oam ethernet link-fault-management interface ge-0/0/0 link-discovery passive

set protocols oam ethernet link-fault-management interface ge-0/0/0 pdu-threshold 5

set protocols oam ethernet link-fault-management interface ge-0/0/0 event-thresholds symbol-period 4

set protocols oam ethernet link-fault-management interface ge-0/0/0 event-thresholds frame-error 4

Ethernet IP-SLA RPM (Real-Time Performance Monitoring)

Massimiliano Sbaraglia

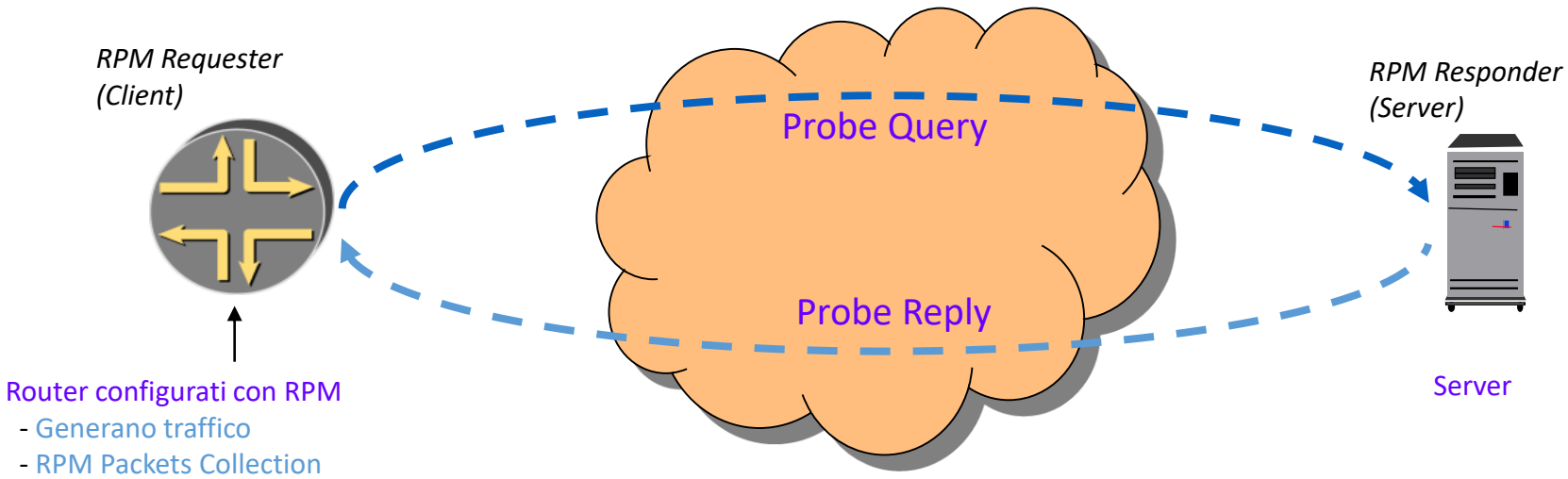
RPM (Real-Time Performance Monitoring)

Un sistema di Real-Time Performance Monitoring (RPM) permette di misurare le performance tra due peer endpoints.

Quando un RPM è configurato il nodo calcola le performance di rete basandosi sul tempo di risposta del peer endpoint, come pure per jitter e packet-loss attraverso ICMP request probe.

Per considerare la latenza oppure il jitter nella comunicazione dei messaggi di probe, si deve configurare il timestamping dei pacchetti di probe.

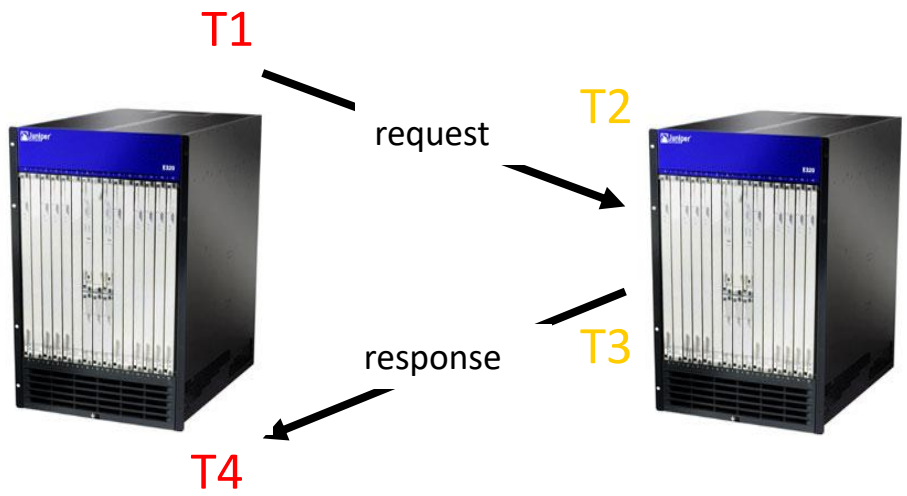
- RPM utilizza il concetto di test
- Durante il test un nodo invia dei probe packets verso una macchina (router, server, nodo) che risponde
- Diversi tipi di probe packets: icmp-ping, icmp-ping-timestamp, http-get, http-metadata-get, tcp-ping, udp-ping, udp-ping timestamp



RPM (Real-Time Performance Monitoring)

I probe di tipo timestamp (icmp-ping-timestamp, udp-ping-timestamp) permettono di effettuare misure temporali di tipo «one-way» e di eseguire misure di latenze o jitter.

- Misurazione più accurate
- Sul responder necessario per misure one-way (attenzione alla sincronizzazione NTP)

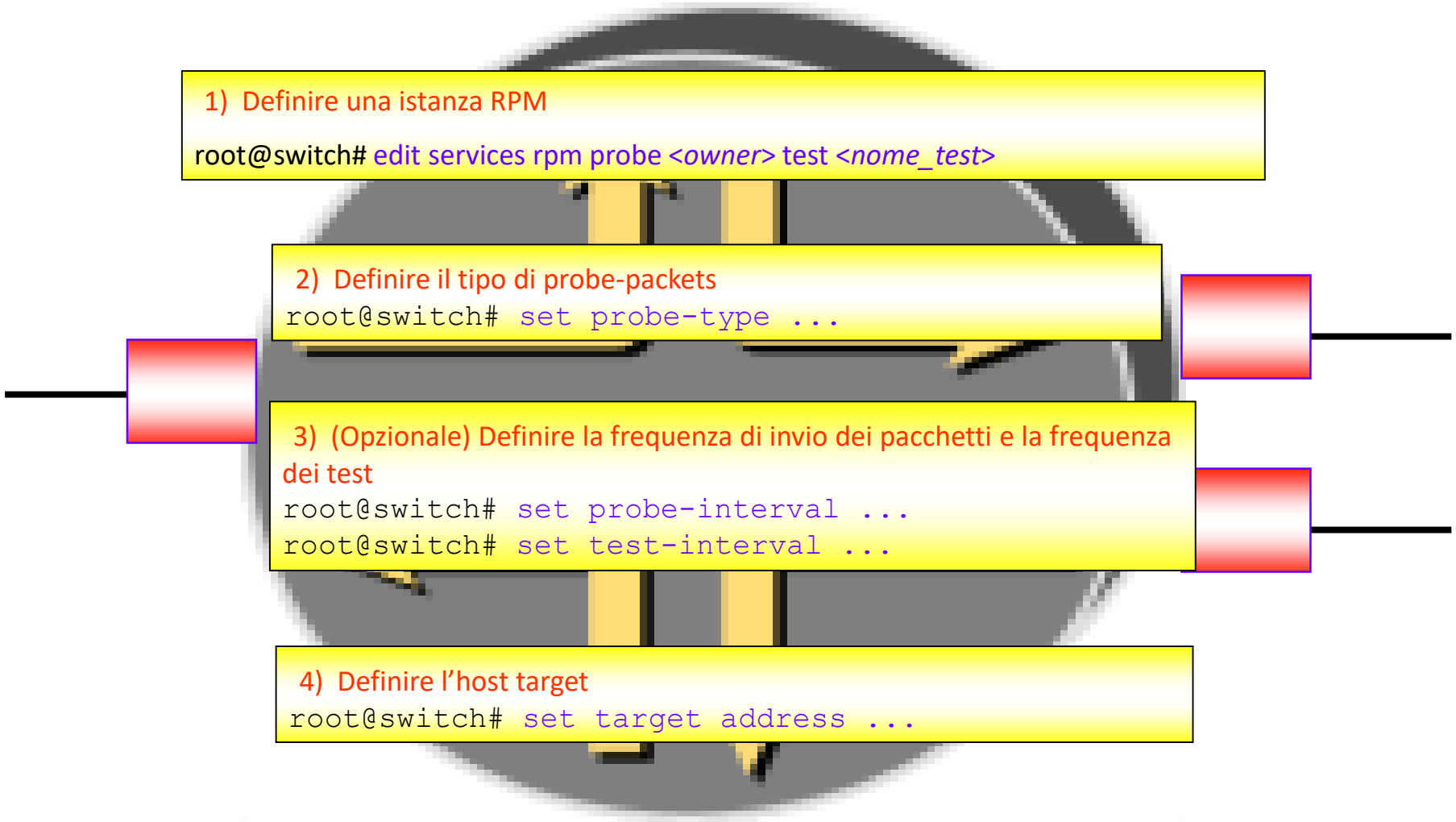


RESPONDER

- **CON *hardware timestamp***
  Round-TripTime = (T2-T1)+(T4-T3)

- **SENZA *hardware timestamp***
  Round-TripTime=(T4-T1)/2

RPM Esempio di Configurazione in grafica



RPM definizione istanza

- La combinazione ADMIN, PING_TEST rappresenta una singola instanza RPM
- Il test PING_TEST è costituito da un determinato numero di probes di uno specificato tipo

```
root@switch# edit services rpm
[edit services rpm]
root@switch# set probe ADMIN test PING_TEST
```

```
[edit services rpm probe ADMIN test PING_TEST]
root@switch# set ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
  data-fill            Define contents of the data portion of the probes
  data-size            Size of the data portion of the probes (0..65507)
  destination-interface  Name of output interface for probes
  destination-port     TCP/UDP port number 7, 49160 through 65535 (7..65535)
  dscp-code-points     Differentiated Services code point bits or alias
  history-size         Number of stored history entries (0..255)
  moving-average-size  Number of samples used for moving average (0..255)
  one-way-hardware-timestamp  Enable hardware timestamps for one-way measurements
  probe-count          Total number of probes per test (1..15)
  probe-interval       Delay between probes (1..255 seconds)
  probe-type           Probe request type
  routing-instance     Routing instance used by probes
  source-address       Source address for probe
> target               Target destination for probe
  test-interval        Delay between tests (0..86400 seconds)
> thresholds           Probe and test threshold values
+ traps                Trap to send if threshold is met or exceeded
```

RPM definizione istanza

- Esempio di probe: ICMP-echo

```
[edit services rpm probe ADMIN test PING_TEST]
root# set probe-type ?
Possible completions:
  http-get              Perform HTTP Get request at target URL
  http-metadata-get     Perform HTTP Get request of metadata at target URL
  icmp-ping             Send ICMP echo request to target address
  icmp-ping-timestamp   Send ICMP timestamp request to target address
  tcp-ping              Send TCP packets to target
  udp-ping              Send UDP packets to target
  udp-ping-timestamp    Send UDP packets with timestamp to target

root@switch# set probe-type icmp-ping
root@switch# set probe-count 15           ← 1÷15 secs
root@switch# set probe-interval 1         ← 1÷255 secs
root@switch# set target address 192.168.100.1
root@switch# set test-interval 3600       ← 0÷86400 secs
```

RPM definizione istanza

- Visualizzazione delle caratteristiche configurate

```
root@switch> show configuration services rpm
```

- Visualizzazione delle statistiche configurate

```
root@switch> show services rpm ?
Possible completions:
  active-servers       Show configured servers
  history-results      Show history results
  probe-results        Show probe results
```

RPM definizione istanza esempio

- Visualizzazione delle caratteristiche configurate

```
root@switch> show configuration services rpm
```

- Visualizzazione delle statistiche configurate

```
root@switch> show services rpm ?
Possible completions:
  active-servers       Show configured servers
  history-results      Show history results
  probe-results        Show probe results
```

RPM Esempio di Configurazione di un router serie T

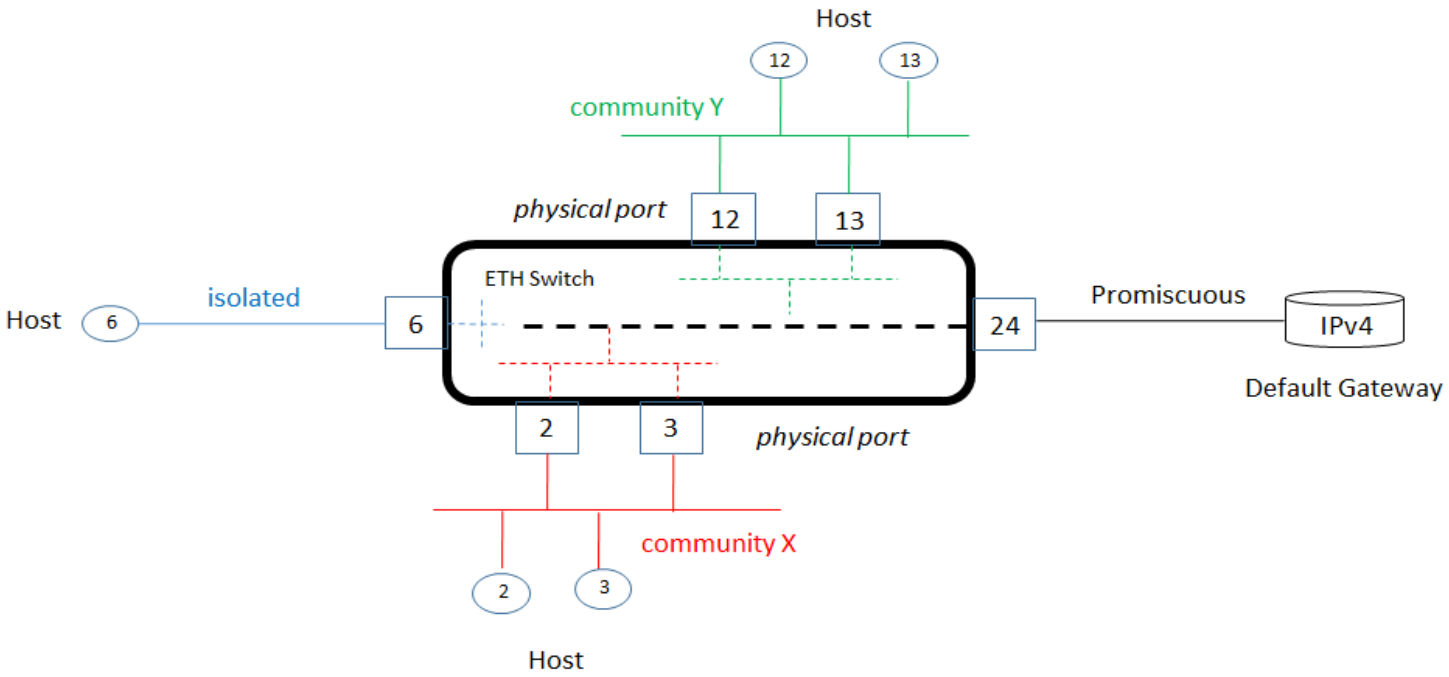
```
set services rpm probe IPSLA test link_to_RMN-2 probe-type icmp-ping
set services rpm probe IPSLA test link_to_RMN-2 target address 10.10.10.237
set services rpm probe IPSLA test link_to_RMN-2 probe-count 1
set services rpm probe IPSLA test link_to_RMN-2 probe-interval 1
set services rpm probe IPSLA test link_to_RMN-2 test-interval 1
set services rpm probe IPSLA test link_to_RMN-2 source-address 10.10.10.238
set services rpm probe IPSLA test link_to_RMN-2 thresholds rtt 35000
!
set services rpm probe IPSLA test link_to_RMN-1 probe-type icmp-ping
set services rpm probe IPSLA test link_to_RMN-1 target address 10.10.10.233
set services rpm probe IPSLA test link_to_RMN-1 probe-count 1
set services rpm probe IPSLA test link_to_RMN-1 probe-interval 1
set services rpm probe IPSLA test link_to_RMN-1 test-interval 1
set services rpm probe IPSLA test link_to_RMN-1 source-address 10.10.10.234
set services rpm probe IPSLA test link_to_RMN-1 thresholds rtt 35000
```

PVLAN (Private Vlan)

Massimiliano Sbaraglia

Private VLANs PVLAN

Private VLAN è una tecnologia che permette la segregazione in sottodomini di vlans definite attraverso vlan configurate come Community, Isolated e Promiscuos.



Private VLANs PVLAN

- Primary VLAN: definita con un 802.1Q tag (vlan-id) che comprende l'intero dominio Private-VLAN e può contenere multiple secondary vlan di cui una isolated vlan e multiple community vlans

- Secondary VLANS
- Isolated VLAN: una interfaccia in Isolated Vlan può trasmettere packets solo verso porte configurate come promiscuos oppure attraverso un ISL (Inter Switch Link); una Isolated port NON può trasmettere e/o ricevere traffico da altre Isolated interfaces.
- Community VLAN: possiamo avere multiple community Vlan all'interno di un singolo dominio Private-VLAN; una porta all'interno di una determinata community può stabilire una comunicazione layer 2 con tutte le altre porte appartenenti alla stessa community vlan. Inoltre una interfaccia in community può comunicare con una interfaccia di tipo promiscuos oppure ISL.
- Promiscuos Port: questo tipo di porte ha comunicazione layer 2 con tutte le interfacce appartenenti al dominio PVLAN (senza riguardo a come queste porte sono configurate/appartenenti); la promiscuos port appartiene alla Primary Vlan e non è inclusa in nessun sottodominio. Layer 3 gateway, DHCP server ed altri nodi di questo tipo che necessitano di comunicare con host/server della PVLAN sono collegati a questo tipo di porta.
- ISL Inter Switch Link: è un collegamento trunk che connette multipli switches in un dominio PVLAN e può contenere due o più vlans (utilizzato quando il dominio PVLAN è esteso su più switches)

Private VLANs PVLAN configuration example

- Configuration Primary VLAN:

set vlan PVLAN vlan-id 100 no-local-switching

- Configuration Promiscuos Trunk Port:

set interface ge-0/0/0 unit 0 family ethernet-switching port-mode trunk

set interface ge-0/0/0 unit 0 family ethernet-switching vlan members PVLAN

- Assign promiscuos trunk port in primary vlan:

set vlans PVLAN interface ge-0/0/0

- Configure Access Ports (All Community and Isolated ports must be in access port mode):

set interface ge-0/0/3 unit 0 family ethernet-switching port-mode access

set interface ge-0/0/4 unit 0 family ethernet-switching port-mode access

set interface ge-0/0/5 unit 0 family ethernet-switching port-mode access

Private VLANs PVLAN verifica configuration example on EX

- Configure Community VLANs and assign ports to the Community:

[edit vlans]

set Marketing-10 vlan-id 10

set Marketing-10 primary-vlan PVLAN

set Marketing-10 interface ge-0/0/3

set Engineering-20 vlan-id 20

set Engineering-20 primary-vlan PVLAN

set Engineering-20 interface ge-0/0/4

set Production-30 vlan-id 30

set Production-30 primary-vlan PVLAN

set Production-30 interface ge-0/0/4

- Assign port to Isolated PVLAN:

set vlans PVLAN interface ge-0/0/5.0

- show vlans
- show vlans pvlan extensive
- show vlans extensive
- run show vlans
- run show vlans PVLAN extensive

ERP Ethernet Ring Protection

Massimiliano Sbaraglia

ERPS Ethernet Ring Protection Switching

ERPS è un sistema che provvede alla stabilità di una rete layer 2 switch; i links di fatto non formano mai un loop in quanto utilizzano uno specifico link a protezione dell'intero anello.

Questo speciale link è conosciuto come RPL (Ring Protection Link) controllato da uno nodo della rete chiamato RPL owner (esiste un solo RPL owner in un anello) ed è responsabile di bloccare e sbloccare il traffico a seconda di avvenimento di un failure.

Il protocollo conosciuto come APS (Automatic Protection Switching) è impiegato per coordinare l'azione di protezione attraverso l'anello di rete; questo protocollo è in grado, quindi, di bloccare il traffico nel link failed e sbloccare il traffico via RPL link

ERPS è definito come ITU-T G.8032

- Designed toloop-free protection sub-50 msec over Ethernet
- Ethernet must be in a ring topology with at least three switches
- ERP replace spanning-tree protocols on the ring