VRF LITE

Gianrico Fichera

19 aprile 2010

Indice

0.1 Introduzione

Le VPN rivestono un ruolo di fondamentale importanza nelle reti di comunicazione dati. Le aziende hanno necessità di collegare le loro sedi con dei circuiti sicuri, che impediscano intrusioni e violazioni della sicurezza. Per preservare i propri dati, le aziende hanno utilizzato negli anni '80 e negli anni '90 i servizi che mettevano a disposizione i carrier dell'epoca, quali circuiti X.25, Frame-relay e i più moderni circuiti ATM. Ma con l'avvento di Internet il protocollo TCP/IP si è diffuso più rapidamente delle altre tecnologie e si è sentita la necessità di rimpiazzare le tecnologie più datate, che iniziavano a diventare solo una voce di costo aggiuntiva.

Alla fine degli anni novanta fino ai giorni nostri, in un mondo oramai dominato dal protocollo TCP/IP e dall'Ethernet gli svantaggi derivanti dall'uso di tali infrastrutture appaiono evidenti. Mantenere una rete ATM è costoso, tanto più con l'aumentare della banda passante (difficilmente si arrivera' a interfacce con velocità superiori a 622mbps). Tecnologie come la Ethernet invece permettono di arrivare a bande passanti dell'ordine di 1/10 Gbit/s con costi minimi e possono essere utilizzate anche al di fuori dei limiti delle reti LAN aziendali per entrare in ambiente Metro/WAN. Il protocollo TCP/IP è ormai usato quasi ovunque. Ed è per questo che produttori come Cisco Systems hanno focalizzato l'attenzione su Ethernet e IP.

In Italia l'operatore monopolista possedeva una rete X.25 , successivamente affiancata da una rete Frame-Relay e quindi da una più recente rete ATM. Su quest'ultima degno di nota è il passaggio della maggior parte del traffico della rete italiana XDSL.

L'evoluzione ha fatto si che anche i collegamenti VPN si sono spostati su IP. Con l'abbassamento dei costi e l'aumento delle performance, e l'arrivo di più economici collegamenti di tipo XDSL, molte VPN si sono realizzate a livello 3, utilizzando protocolli quali IPSEC, senza alcun contributo dell'Internet Service Provider (ISP). In questo caso la VPN è ritagliata su un collegamento internet, sempre disponibile a buon mercato.

D'altro canto per gli ISP non vi era una soluzione differente dall'uso del protocollo Frame-relay o ATM per fornire VPN. Non esisteva un protocollo di trasporto differente in grado di utilizzare IP. Alla fine hanno comunque offerto VPN su rete XDSL, che comunque viaggia su ATM.

L'avvento del protocollo *Multiprotocol Label Switching* ($MPLS$) ha fornito ai provider una soluzione ai loro problemi consentendo loro di svincolarsi dalle vecchie pile protocollari e di concentrasi sull'uso di IP, Ethernet, SDH e XDSL. MPLS è una tecnica di trasmissione che utilizza delle *etichette* (*labels*) per differenziare i flussi di traffico. MPLS non è specifico per TCP/IP e può trasportare qualsiasi protocollo. Nel caso di IP utilizza tutte le specifiche di *Qualità di Servizio* (QoS) sviluppate nel corso degli anni per TCP/IP e fornisce gli strumenti per gestire Ingegneria del Traffico (IT) e VPN. E proprio la QoS e l'IT erano i vantaggi offerti dalla rete Frame-Relay e ATM, che permettevano di evitare congestioni, garantendo ai clienti la banda contrattualizzata. Venendo meno la principale limitazione del protocollo IP, ovvero la gestione dell'IT, i carrier avevano finalmente una valida alternativa a ATM e Frame-Relay.

Questo documento in realtà non parla di MPLS , ma di un suo prodotto derivato, ovvero il VRF-lite. MPLS viene infatti utilizzato nei backbone dei carrier e delle grosse reti. VRF-lite può essere utilizzato o in reti MPLS lato CE

o sempre in reti di tipo campus in alternativa o insieme alle VLAN Ethernet. VRF significa VPN Routing and Forwarding e consiste nella possibilità per un singolo router fisico di gestire diversi router virtuali, indipendenti tra di loro, ed e' quindi ideale per gestire diversi diverse VPN.

Questo documento parla del VRF-lite. Quindi non troverete configurazioni MPLS. Se siete interessati a gestire VPN in un ISP questo documento può essere da introduzione a MPLS.

0.2 Audience

Per la comprensione di questo documento è necessario avere conoscenza della configurazione dei router Cisco. Inoltre è necessario conoscere il protocollo IP, il routing statico e dinamico, e il relativo modo di configurarli in ambiente Cisco. Per poter applicare questi concetti è necessario anche conoscere un pò di teoria sulle VPN.

0.3 Versioni e aggiornamenti

- Versione 0.90 28 Agosto 2007: *Prima release*
- Versione 0.91 17 Settembre 2007: *Aggiunto paragrafo sul DHCP* –
- Versione 0.92 8 Marzo 2008: *Revisione complessiva, riscritte alcune parti, reimpaginato*
- Versione 0.93 18 Aprile 2010: *Aggiunta di materiale e revisione di alcune parti*
- – Sviluppato con TeXnicCenter —

0.4 Ringraziamenti

Si ringrazia per il supporto e la collaborazione l' Ing.Maurizio Intravaia. Alla memoria di Aldo Schinina', collega e amico. Tutti gli esempi riportati si riferiscono a implementazioni presso il laboratorio di ITESYS srl o presso clienti.

0.5 Feedback

Poiché il nostro obiettivo è quello di creare documentazione quanto più completa e corretta possibile saranno benvenuti commenti e suggerimenti. Potete inviare anche correzioni o materiale aggiuntivo purché originali e frutto del vostro personale lavoro. L'indirizzo email è `gianrico.fichera@itesys.it` o `info@itesys.it`.

0.6 Copyright

Capitolo 1

Configurazioni di base

1.1 Introduzione a MPLS

Multi Protocol Label Switching ($MPLS$) è un protocollo per il trasporto dati nelle reti a pacchetto. In riferimento al modello ISO/OSI si trova tra il livello 2 e il livello 3. Storicamente nasce per risolvere i limiti intrinsechi del protocollo IP nella gestione della QoS e dell'IT. Protocolli come Frame-Relay e ATM hanno dominato le reti geografiche in quanto in grado di gestire con molta efficienza la priorizzazione e l'isolamento del traffico. Ma la diffusione del protocollo IP seguita all'avvento di Internet hanno reso necessario affrontare il problema anche per questo protocollo non progettato per la QoS o l'IT.

MPLS opera utilizzando un MPLS-header, contenente uno stack di etichette in base alle quali viene effettuato l'IP forwarding. I pacchetti sono inviati attraverso un *label switch path* (LSP), un percorso che possiamo immaginare come un circuito ATM o Frame-Relay. I router della rete *label switch router* (LSR) effettuano le decisioni di instadamento in base al contenuto delle etichette.

MPLS può viaggiare su protocolli di Livello 2 come PPP, Ethernet, Frame-Relay o ATM e consente viceversa di far viaggiare altri protocolli al suo interno, e non solo l'IP, come ad esempio l'Ethernet, o il Frame-Relay.

La gestione delle VPN da parte di MPLS e' una conseguenza dell'isolamento del traffico che è in grado di garantire. Per consentire l'uso di classi di IP private da parte degli utenti le VPN in MPLS vengono realizzate con l'uso di BGP, e opzionalmente con *VPN Routing and Forwarding Tables* (VRF) ovvero VRF-lite (nel caso di CE multi-VPN). Per questo si parta di VPN BGP/MPLS. VRF-lite è basato sull'uso di tabelle di routing virtuali che sono associabili ognuna ad una diversa VPN. Il VRF è un'estensione dell'IP routing. Poiche' si usa BGP in ogni *provider edge router* (PE) che gestisce VPN deve supportare il protocollo BGP. Si ponga attenzione al fatto che MPLS non gestisce la criptazione dei dati, ad esempio con IPsec .

MPLS progressivamente sostituirà i più costosi circuiti ATM a vantaggio di reti realizzate con infrastrutture di tipo SONET/SDH con *Packet over Sonet* (POS) e quindi MPLS (vedi Cisco tag-switching). Con tecnologie come MPLS over ATM è invece possibile intraprendere percorsi di migrazione di reti preesistenti.

1.2 Introduzione a VRF

Immaginiamo la rete di un grosso carrier o ISP. Distinguiamo i dispositivi *Customer Edge* (CE) , ovvero ad esempio router che si interfacciano verso l'ISP, e dispositivi *Provider Edge* (PE) , ovvero ad esempio router della rete dell'ISP collegato al CE. Con P indichiamo un router interno della rete dell'ISP , ovvero non Edge.

I motivi dell'introduzione di VRF-lite sono stati quelli di estendere delle funzionalità tipiche del PE sino al CE, consentendo di gestire i VRF anche nel CE, potendo garantire maggior sicurezza e una gestione multi-VPN per un cliente oppure più clienti con un solo CE (normalmente un CE gestisce solo per un cliente). I router CE che supportano il VRF-lite normalmente non supportano MPLS, ma sono pensati per interfacciarsi con una rete MPLS o più in generale con una rete IP con più livelli di servizio.

Nella nostra trattazione immaginiamo una rete geografica di un ISP, e i router di alcuni suoi clienti, che richiedono servizi Internet o di VPN. Nostro obiettivo è però di utilizzare i concetti introdotti per l'uso in reti molto più piccole, come campus o intranet, e quindi normalmente prive di MPLS.

In caso di VPN singole lato CE non è necessario un router con supporto VRF-lite o MPLS ma basta un apparato qualsiasi da configurare con statiche, RIP, EIGRP, OSPF che lato PE verranno iniettate nella rete BGP/MPLS. Anche nel caso VRF-lite lato CE si potrà adottare RIP, EIGRP, OSPF che sono in grado di supportare un ambiente multi-VRF.

Con il *VPN Routing and Forwarding* (VRF) si crea un router logico a tutti gli effetti. Quest'ultimo sarà identificabile come costituito da una tabella di routing IP, da alcune interfacce fisiche o logiche, e da alcuni servizi ad esso associati (DHCP, NAT etc.). Più VRF conviveranno nello stesso router fisico.

Con questo sistema è possibile gestire in uno stesso router più circuiti logici separati a livello 3. Possiamo gestire più VPN anche con overlapping degli indirizzi IP in quanto appartenenti a schemi logici isolati tra di loro. Possiamo fare quello a livello 3 quello che facciamo a livello 2 con le VLAN. Quindi possiamo separare diversi flussi di traffico IP con un'analogia con cui in ATM si separano diversi flussi di traffico e di conseguenza sempre diversi flussi di traffico IP.

VRF-lite si può usare in ambiente campus/azienda o nelle reti carrier tra CE e PE. Nel primo caso di usa per separare efficacemente flussi di traffico a livello 3 superando i limiti delle VLAN. Nel secondo caso si usa per 'entrarè in una rete MPLS. I protocolli di routing RIP, EIGRP, OSPF e BGP sono supportati. VRF-lite è a disposizione nell'immagine IOS di default di molti router CISCO, a partire dalla serie 8XX, purche' possediate un router abbastanza recente.

Nota sugli esempi: alcuni esempi potrebbero non funzionare se non avete un IOS abbastanza recente o con features adeguate. Conviene sicuramente utilizzare almeno IOS 12.3 o 12.4. Con alcuni IOS alcune funzionalità VRF-lite potrebbero funzionare solo parzialmente o potrebbero non essere supportati alcuni protocolli di routing.

1.3 Configurazione 1 - Startup -

1.3.1 Configurazione

```
interface FastEthernet0/0
description --- WAN ---
 ip address 192.168.30.124 255.255.255.0
!
interface FastEthernet0/1
 description --- LAN ---
 ip address 192.168.1.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.30.254
ip route 192.168.10.0 255.255.255.0 192.168.1.1
```

1.3.2 Descrizione

In questa configurazione non è presente VRF-lite: è una configurazione di partenza. Si tratta di una tipica configurazione di un router con due interfacce Ethernet. Una interfaccia è lato LAN e l'altra lato WAN. Una tipica configurazione per funzionalità di firewall o di filtering. Lato WAN è presente un gateway, all'indirizzo 192.168.30.254, che può essere ad esempio un secondo router interfacciato ad internet tramite collegamento XDSL. Lato LAN potrebbe essere presente un terzo router, ad esempio uno switch di layer 3.

Questa configurazione è abbastanza generica e flessibile per poter costruire gli esempi dei paragrafi successivi. Come avviene normalmente, il router ha una tabella di routing, costruita in base alle informazioni presenti nella configurazione inserita, ovvero dalle reti 192.168.10.0 e 192.168.30.0, oltre che dalle due statiche, verso 192.168.30.254 e verso 192.168.1.1. Ecco la tabella di routing, visibile con il comando **show ip route**:

```
ROUTER_A#show ip route
...snip...
Gateway of last resort is 192.168.30.254 to network 0.0.0.0

C 192.168.30.0/24 is directly connected, FastEthernet0/0
S 192.168.10.0/24 [1/0] via 192.168.1.1
C 192.168.1.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 192.168.30.254
```

1.4 Configurazione 2 - Prima configurazione VRF -

1.4.1 Configurazione

```
ip vrf blue                 (1)
rd 100:10                   (2) ←— Definiamo una nuova tabella di routing
!                                  La notazione standard è AS:valore o IP:valore
!
interface FastEthernet0/0
description --- WAN ---
ip address 192.168.30.124 255.255.255.0
!
interface FastEthernet0/1
description --- LAN ---
ip address 192.168.1.2 255.255.255.0
!
```

```
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.30.254
ip route 192.168.10.0 255.255.255.0 192.168.1.1
```

1.4.2 Descrizione

Osserviamo le righe (1) e (2). Queste definiscono una nuova tabella di routing di nome 'blue' e con identificativo 100:10. La nuova tabella di routing inizialmente è vuota, infatti le righe di routing statico fin qui configurate sono presenti nella tabella di routing 'globale' ovvero quella di default. Anche le righe di routing derivate dalle interfacce sono presenti nella tabella di routing globale.

L'identificativo, chiamato route-distinguisher (*RD*) diventa un prefisso per gli indirizzi IP, e questo consente di differenziare due indirizzi IP uguali ma appartenenti a differenti VRF. Indichiamo un indirizzo così ottenuto con la notazione RD:IP. Utilizzando questa notazione e un protocollo di routing in grado di supportarla è possibile far transitare del traffico tra differenti VRF. Il protocollo BGP, ma anche OSPF sono in grado di riconoscere i VRF, ovvero sono VRF-aware. Se più VRF devono restare isolati, ad esempio in un router di transito, è superfluo definire un RD (riga 2) ma è sufficiente solo la riga (1) che consente di creare una nuova tabella di routing, ovvero un nuovo VRF che chiamiamo 'blue'.

Dalla configurazione di sopra ci aspettiamo che la tabella di routing 'blue' sia vuota. Per vedere il contenuto della tabella di routing relativa ad un VRF si utilizza il comando **show ip route vrf blue**:

```
ROUTER_A#show ip route vrf blue
Routing Table: blue
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
```

La tabella di routing globale rimane invariata rispetto la configurazione di base:

```
ROUTER_A#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.30.254 to network 0.0.0.0

C 192.168.30.0/24 is directly connected, FastEthernet0/0
S 192.168.10.0/24 [1/0] via 192.168.1.1
C 192.168.1.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 192.168.30.254
```

1.5 Configurazione 3 - Popoliamo il VRF -

Con la configurazione del paragrafo precedente siamo riusciti a creare due tabelle di routing nel nostro router singorlo router fisico. Ma tutte le righe di routing figurano nella tabella di routing globale, ovvero quella di default, in quanto tutte le interfacce e le righe di routing statico non sono definite come appartenenti al vrf 'blue', ma, non essendo specificato nulla, alla tabella di routing di default (quella che vediamo con 'show ip route').

1.5.1 Configurazione

```
ROUTER_A
!
ip vrf blue
rd 100:10
!
!
interface FastEthernet0/0
description --- RETE WAN ---
ip address 192.168.30.124 255.255.255.0
!
interface FastEthernet0/1
description --- RETE LAN ---
ip vrf forwarding blue                                    <-- (1)
ip address 192.168.1.2 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.30.254
ip route 192.168.10.0 255.255.255.0 192.168.1.1
ip route vrf blue 192.168.50.0 255.255.255.0 192.168.1.1      <-- (2)
!
```

1.5.2 Descrizione

Con la riga (1) inseriamo l'interfaccia Fastethernet0/1 nel vrf 'blue'. Questo vuol dire che l'interfaccia farà parte del VRF 'blue'. È come se facesse parte di un'altro router, o per analogia a livello 2 con uno switch, ad una VLAN differente. Non apparirà più in 'show ip route' in quanto facente parte del VRF 'blue'. Abbiamo cosi' creato un nuovo router virtuale con una interfaccia e una sua tabella di routing. Con la riga (2) aggiungiamo una route statica al VRF blue :

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
Gateway of last resort is 192.168.30.254 to network 0.0.0.0
C 192.168.30.0/24 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 [1/0] via 192.168.30.254
ROUTER_A# show ip route vrf blue
Routing Table: blue
Gateway of last resort is not set
S 192.168.50.0/24 [1/0] via 192.168.1.1
C 192.168.1.0/24 is directly connected, FastEthernet0/1
```

A questo punto siamo in grado di configurare più processi di routing e di associare ad ognuno di essi delle interfacce e delle righe di routing statico. Stiamo facendo, per il layer 3, qualcosa di simile a quanto si può fare con uno switch a livello 2, creando delle VLAN. Ma lavorare a livello 3 e' cosa assai diversa, potendo gestire i flussi di traffico IP.

1.6 Configurazione 4 - Comandi utili -

1.6.1 Configurazione

```
!
ip vrf bianco
rd 100:10
!
ip vrf blue
rd 102:10
!
ip vrf nero
rd 101:10
!
!
interface Loopback0
ip vrf forwarding bianco
ip address 192.168.88.1 255.255.255.0
!
interface Loopback1
ip vrf forwarding nero
ip address 192.168.89.1 255.255.255.0
!
interface Loopback2
ip vrf forwarding blue
ip address 192.168.90.1 255.255.255.0
!
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.252
!
ip classless
ip route 192.168.78.0 255.255.255.0 192.168.1.1
ip route 192.168.79.0 255.255.255.0 192.168.1.1
ip route 192.168.80.0 255.255.255.0 192.168.1.1
```

1.6.2 Descrizione

Nell'esempio abbiamo tre VRF di nome 'bianco', 'blue', 'nero' e tre interfacce associate ad essi. Ecco alcuni utili comandi in ambiente VRF.

Per avere un dettaglio dei VRF configurati:

```
ROUTER_A#sh ip vrf detail

VRF bianco; default RD 100:10; default VPNID <not set>
Interfaces:
Loopback0
Connected addresses are not in global routing table
No Export VPN route-target communities
No Import VPN route-target communities
No import route-map
No export route-map

VRF blue; default RD 102:10; default VPNID <not set>
Interfaces:
Loopback2
Connected addresses are not in global routing table
No Export VPN route-target communities
No Import VPN route-target communities
No import route-map
No export route-map

VRF nero; default RD 101:10; default VPNID <not set>
Interfaces:
Loopback1
Connected addresses are not in global routing table
No Export VPN route-target communities
No Import VPN route-target communities
```

```
No import route-map
No export route-map
```

Attenzione al fatto che il comando **ping**, se non indicato espressamente, fa riferimento alla tabella di routing globale (quella di default del router che non ha un VRF associato), quindi:

```
ROUTER_A#ping 192.168.89.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.89.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

fallisce pur essendo 192.168.89.1 un indirizzo IP di una interfaccia nello stesso router ma appartenente ad un VRF diverso. Invece:

```
ROUTER_A#ping vrf bianco 192.168.88.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.88.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Stessa cosa dicasi per gli altri comandi. Ad esempio:

```
ROUTER_A#show ip route 192.168.88.1
% Network not in table
```

fallisce anche se la riga di routing esiste ma non nella tabella di routing globale. Pertanto va utilizzata la seguente sintassi:

```
ROUTER_A#show ip route vrf bianco 192.168.88.1
Routing entry for 192.168.88.0/24
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via Loopback0
Route metric is 0, traffic share count is 1
```

1.7 Configurazione 5 - Accesso ad Internet -

Supponiamo di avere un router con più VRF configurati in un'azienda. Ogni VRF copre un ramo d'azienda che tra di loro, per motivi di sicurezza, devono restare isolati. Ma il router è anche connesso ad Internet e vorremmo darne l'accesso da tutti i VRF. Un'interfaccia non può appartenere a più VRF e quindi senza strumenti aggiuntivi non si può fare granchè. L'interfaccia verso Internet la lasciamo allora nella tabella di routing globale, quindi inizialmente isolata. Inserire una riga di routing di default in ogni VRF non servirebbe a nulla in quanto il next-hop non è nello stesso VRF e quindi risulta irraggiungibile.

```
ROUTER_A
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.252
...
```

```
ip route vrf bianco 0.0.0.0 0.0.0.0 192.168.1.1
...
ROUTER_A#show ip route vrf bianco
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
C 192.168.88.0/24 is directly connected, Loopback0 <--- notate l'assenza della
route statica
ROUTER_A#
ROUTER_A#
```

La soluzione consiste nell'utilizzare la parola chiave **global** nella route statica. Questa indica che il next-hop si trova nella tabella di routing globale:

```
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.252
...
ip route vrf bianco 0.0.0.0 0.0.0.0 192.168.1.1 global
ROUTER_A# sh ip route vrf bianco
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 192.168.1.1 to network 0.0.0.0
C 192.168.88.0/24 is directly connected, Loopback0
S* 0.0.0.0/0 [1/0] via 192.168.1.1  <--- notate come la riga di route sia stata recepita
                                        anche se eth0/0 non e' nel vrf bianco
```

I differenti VRF possono attingere il next-hop dalla tabella di routing globale ma non tra di loro (ad esempio con BGP). Ricordo che l'uso di IP privati nelle configurazioni è a titolo di esempio.

1.8 Configurazione 6 - Accesso ad Internet con NAT -

La configurazione mostrata nel paragrafo precedente ha senso solo nel caso in cui si utilizzino ip pubblici. Solo in quel caso la navigazione Internet funzionerebbe correttamente. In tutti gli altri casi, ovvero con il tradizionale uso di ip privati, sarà necessario utilizzare il NAT . Il NAT virtual interface (NVI), è l'adattamento del NAT per l'uso in ambiente VRF. Si potranno infatti configurare diversi profili di NAT per differenti VRF, indipendenti tra di loro. Possiamo allora dire che il NAT è 'VRF-aware' .

1.8.1 Configurazione

```
!
ip vrf bianco
rd 100:10
!
ip vrf nero
rd 101:10
!
interface ATM0
```

```
 no ip address
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.1 point-to-point
 ip address 12.123.141.12 255.255.255.0
 ip nat enable
 ip virtual-reassembly
 pvc 8/35
 encapsulation aal5snap
!
interface ethernet0
description --- LAN1 ---
ip vrf forwarding nero
ip address 192.168.30.2 255.255.255.0 (1)
ip nat enable
ip virtual-reassembly
!
!
interface ethernet1
description --- LAN2 ---
ip vrf forwarding bianco
ip address 192.168.30.2 255.255.255.0 (2)
ip route 0.0.0.0 0.0.0.0 ATM0.1 (5)
ip route vrf nero 0.0.0.0 0.0.0.0 12.123.141.12 global (4)
!
ip nat pool TEST 12.123.141.12 12.123.141.12 netmask 255.255.255.0
ip nat source list 20 pool TEST vrf nero overload (3)
!
access-list 20 permit 192.168.30.0 0.0.0.255
!

\subsection{Descrizione}
\label{sec:Descrizione}
```

Si tratta di una semplice LAN con un router dotato di interfaccia ADSL e due ethernet. Le due ethernet le possiamo supporre collegate a due LAN di due aziende differenti, che condividono lo stesso router per l'accesso ad Internet ma devono restare isolate tra di loro. Con una configurazione tradizionale avremmo dovuto separare il traffico tra le due reti con delle access-list, e oltretutto avremmo dovuto fare attenzione all'indirizzamento adottato, in quanto (senza VRF) le due reti devono avere due classi di IP private differenti.

Utilizzando VRF-lite la configurazione si semplifica ed è molto più semplice da amministrare, inoltre le due reti sono completamente indipendenti, infatti notate l'uso della stessa classe di IP privati da parte delle due LAN. Nessun conflitto, in quanto vi sono due VFR differenti. La LAN2 non ha servizio di navigazione Internet. Con NVI si utilizza il comando **ip nat enable** invece dei più noti **ip nat inside**, **ip nat outside**. La riga chiave è la (3) dove si aggancia il pool degli indirizzi al VRF specifico.

Con questa configurazione solo la LAN1 navigherà su Internet. Notate come al punto (4) si sia utilizzato l'ip 12.123.141.12 invece dell'interfaccia atm0.1 come next-hop. Questo rende necessario la riga (5) per il raggiungimento dell'interfaccia fisica. Ricordiamoci che, operando con i VRF, ogni comando dev'essere riferito al VRF in oggetto, anche per il NAT:

- **show ip nat trans vrf bianco**
- **debug ip nat vrf**
- **clear ip nat trans vrf**

Negli esempi presentati abbiamo configurato VRF-LITE e spiegato come sia possibile creare diverse tabelle di routing isolate tra di loro ma all'interno dello stesso router fisico. Associando le interfacce ai VRF, sarà così possibile isolare gruppi di utenti. Possiamo anche inserire in un VRF un tunnel oppure una subinterface ethernet oppure una interfaccia logica. I diversi gruppi di utenti avranno policy differenti, ad esempio alcuni potrebbero avere accesso ad Internet mentre altri no.

1.9 Configurazione 7 - DHCP -

Anche il servizio DHCP è VRF-aware ed è quindi possibile attivare il DHCP esclusivamente nellambito di una singola interfaccia.

1.9.1 Descrizione

Supponiamo di scegliere la classe privata 192.168.152.0/24 da assegnare con DHCP. Innanzitutto è fondamentale il comando **ip dhcp use vrf connected** che abilita il dhcp per le interfacce vrf direttamente connesse (ad es. Ethernet). Poi escludiamo lip 192.168.152.254, che è il gateway, e altri 4 indirizzi IP che, in questo esempio, utilizziamo come ip statici nella network. Infine da notare il comando **vrf miovrf** con il quale agganciamo il pool DHCP ad un ben preciso VRF.

```
ip dhcp use vrf connected
ip dhcp excluded-address 192.168.152.254
ip dhcp excluded-address 192.168.152.10 192.168.152.13
ip dhcp pool DHCPSERVER
 vrf miovrf
 network 192.168.152.0 255.255.255.0
 dns-server 151.99.125.1 151.99.125.2
 default-router 192.168.152.254
ip vrf miovrf
 rd 1055:52
```

Con il comando **show ip dhcp pool DHCPSERVER** possiamo vedere le statistiche sul pool che abbiamo configurato:

```
router#show ip dhcp pool DHCPSERVER
Pool DHCPSERVER :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
VRF name : miovrf
Total addresses : 254
Leased addresses : 1
Pending event : none
1 subnet is currently in the pool :
Current index IP address range Leased addresses
192.168.152.1 192.168.152.1 - 192.168.152.254 1
```

Questa è una richiesta di indirizzo (potete attivare il debug con **debug ip dhcp server event**)

```
*Sep 17 14:19:52.088: DHCPD: Sending notification of DISCOVER:
*Sep 17 14:19:52.088: DHCPD: htype 1 chaddr 000e.3525.f394
*Sep 17 14:19:52.088: DHCPD: remote id 020a0000c0a898fe01000034
*Sep 17 14:19:52.088: DHCPD: circuit id 00000000
*Sep 17 14:19:52.088: DHCPD: table id 1 = vrf miovrf
*Sep 17 14:19:52.088: DHCPD: Seeing if there is an internally specified pool class:
```

```
*Sep 17 14:19:52.088: DHCPD: htype 1 chaddr 000e.3525.f394
*Sep 17 14:19:52.088: DHCPD: remote id 020a0000c0a898fe01000034
*Sep 17 14:19:52.088: DHCPD: circuit id 00000000
*Sep 17 14:19:52.088: DHCPD: table id 1 = vrf miovrf
*Sep 17 14:19:52.192: DHCPD: Sending notification of ASSIGNMENT:
*Sep 17 14:19:52.192: DHCPD: address 192.168.152.1 mask 255.255.255.0
*Sep 17 14:19:52.192: DHCPD: htype 1 chaddr 000e.3525.f394
*Sep 17 14:19:52.192: DHCPD: table id 1 = vrf miovrf
*Sep 17 14:19:52.192: DHCPD: lease time remaining (secs) = 86400
*Sep 17 14:19:55.504: DHCPD: Sending notification of ASSIGNMENT:
*Sep 17 14:19:55.504: DHCPD: address 192.168.152.1 mask 255.255.255.0
*Sep 17 14:19:55.504: DHCPD: htype 1 chaddr 000e.3525.f394
*Sep 17 14:19:55.504: DHCPD: table id 1 = vrf miovrf
*Sep 17 14:19:55.504: DHCPD: lease time remaining (secs) = 86400
```

Questa è una richiesta di rilascio dell'indirizzo:

```
*Sep 17 14:20:54.328: DHCPD: Sending notification of TERMINATION:
*Sep 17 14:20:54.328: DHCPD: address 192.168.152.1 mask 255.255.255.0
*Sep 17 14:20:54.328: DHCPD: reason flags: RELEASE
*Sep 17 14:20:54.328: DHCPD: htype 1 chaddr 000e.3525.f394
*Sep 17 14:20:54.328: DHCPD: table id 1 = vrf miovrf
*Sep 17 14:20:54.328: DHCPD: lease time remaining (secs) = 86341
*Sep 17 14:20:54.328: DHCPD: returned 192.168.152.1 to address pool DHCPSERVER.
*Sep 17 14:20:57.744: DHCPD: Sending notification of DISCOVER:
*Sep 17 14:20:57.744: DHCPD: htype 1 chaddr 000e.3525.f394
*Sep 17 14:20:57.744: DHCPD: remote id 020a0000c0a898fe01000034
*Sep 17 14:20:57.744: DHCPD: circuit id 00000000
*Sep 17 14:20:57.744: DHCPD: table id 1 = vrf miovrf
*Sep 17 14:20:57.744: DHCPD: Seeing if there is an internally specified pool class:
*Sep 17 14:20:57.744: DHCPD: htype 1 chaddr 000e.3525.f394
*Sep 17 14:20:57.744: DHCPD: remote id 020a0000c0a898fe01000034
*Sep 17 14:20:57.744: DHCPD: circuit id 00000000
*Sep 17 14:20:57.744: DHCPD: table id 1 = vrf miovrf
*Sep 17 14:20:59.744: DHCPD: client requests 192.168.152.1.
*Sep 17 14:20:59.744: DHCPD: Adding binding to radix tree (192.168.152.1)
*Sep 17 14:20:59.744: DHCPD: VPN 'miovrf'
*Sep 17 14:20:59.744: DHCPD: Adding binding to hash tree
*Sep 17 14:20:59.744: DHCPD: assigned IP address 192.168.152.1 to client 0100.0e35.25f3.94.
*Sep 17 14:20:59.784: DHCPD: Sending notification of ASSIGNMENT:
*Sep 17 14:20:59.784: DHCPD: address 192.168.152.1 mask 255.255.255.0
*Sep 17 14:20:59.784: DHCPD: htype 1 chaddr 000e.3525.f394
*Sep 17 14:20:59.784: DHCPD: table id 1 = vrf miovrf
*Sep 17 14:20:59.784: DHCPD: lease time remaining (secs) =
```

Capitolo 2

Routing Dinamico

2.1 Comunicazione tra VRF

Supponiamo di avere una configurazione con tre VRF. E' possibile far comunicare tra loro i diversi VRF in maniera simile a come comunicherebbero tra loro due router differenti ovvero scambiandosi informazioni di routing. I VRF possono scambiarsi informazioni di routing e quindi permetterci di aprire dei canali di passaggio tra i router virtuali.

Bisogna tenere in mente che VRF-Lite nasce per gestire il lato utente finale, delegando al provider con BGP/MPLS la gestione del routing extra-VRF. Tuttavia, senza utilizzare MPLS possiamo utilizzare il protocollo BGP per i nostri scopi, in questo caso anche su un singolo router, solo per gestire il traffico tra i diversi VRF. Ciò ha un senso. Infatti se in un singolo router fisico ci sono più router virtuali un protocollo di routing dinamico come BGP è perfettamente idoneo per far comunicare tra loro i diversi router (anche se logici). Segue una interessante configurazione fatta con un semplice Cisco 877 e IOS Service Provider 12.4 (che supporta il BGP). Le funzionalità VRF infatti sono disponibili anche sui router di fascia più bassa in quanto spesso utilizzati per far entrare gli utenti finali nelle reti MPLS (ovvero lato CE). Non è detto comunque che ci sia MPLS in quanto la rete VRF-Lite può esserne priva.

Facciamo adesso un altro passo avanti. Immaginiamo di avere più router in una WAN e di voler mantenere separato il traffico dei VRF attraverso la WAN. Una prima soluzione consiste nell'utilizzare tante interfacce fisiche quanti sono i VRF. Quindi un router della WAN saprà differenziale il traffico entrante in base all'interfaccia fisica di provenienza.

Tale approccio però ha dei limiti palesi. Utilizzare una differente interfaccia per ogni collegamento non e' scalabile ed e' costoso. Per seguire l'analogia con gli switch vorremmo avere l'equivalente di un trunk 802.1q ovvero tenere i VRF separati ma attraverso un unico collegamento fisico associandoli a delle subinterface. La risposta è che il protocollo MPLS si preoccupa di tenere separati i flussi di traffico in complesse reti WAN. VRF-Lite ha delle applicazioni più ristrette.

Per **route leak** si intende il passaggio da un primo VRF ad un secondo VRF di un pacchetto IP, causato da una configurazione di qualche tipo. Con

un protocollo VRF-aware come BGP o OSPF è possibile fare route leaking ed è il metodo consigliato. Tuttavia, in casi più semplici, è possibile far comunicare due VRF con semplici route statiche, ma con una sintassi ben precisa. Tecnicamente si parla di traffico **inter-VRF** che può essere inter-VRF to global o inter-VRF. Un esempio del primo caso è l'uso della parola chiave 'global' nelle route statiche. Abbiamo quindi già visto un esempio di inter-VRF to global. Nei paragrafi successivi vedremo anche un esempio di route inter-VRF. E' possibile disabilitare o abilitare l'utilizzo di route statiche per gestire il traffico inter-VRF. Nel caso di disabilitazione siamo costretti a configurare il traffico inter-VRF con un protocollo di routing dinamico.

2.2 Configurazione 8 - Routing BGP e VRF -

Non avrei mai immaginato di configurare il protocollo BGP su un unico router, senza neighboors, ottenendo una configurazione interessante ed utilizzabile, anzi chiave in un ambiente VRF-lite. Nell'esempio vediamo per la prima volta l'uso del comando **route-target**. I route-target (RT) sono degli identificativi associati ad un VRF che indicano la disponibilita di esportare o importare righe di routing verso un differente VRF. Affinché due VRF comunichino tra di loro sarà necessario che si scambino vicendevolmente le tabelle di routing.

I valori numerici indicati negli RT si chiamano 'extended communities'. Questi identificativi vengono usati dal protocollo BGP per il corretto import/export tra VRF. Il motivo dell'uso del protocollo BGP è che è l'unico in grado di agganciare alle route delle informazioni aggiuntive. Le 'communities' sono una funzionalità tipica del BGP e sono normalmente utilizzate per consentire delle policy sul traffico.

```
ip vrf bianco
!
ip vrf bianco
rd 1:1
route-target export 150:150     ⟵ il vrf bianco esporta le sue righe di
                                    routing con l'extended community 150:150
route-target import 101:10      ⟵ il vrf bianco importa le righe di routing
                                    con l'extended community 101:10, del vrf nero
!
ip vrf nero
rd 101:10
route-target export 101:10      ⟵ vrf nero esporta le sue righe di routing
route-target import 150:150     ⟵ il vrf nero importa l'extended community
                                    150:150 garantedosi l'accesso al VRF bianco
!
!
interface Loopback1
ip vrf forwarding bianco
ip address 192.168.30.2 255.255.255.0
!
interface Loopback2
ip vrf forwarding nero
ip address 192.168.31.2 255.255.255.0
!
...snip...
!
interface Vlan1
description --- WAN ---
```

```
ip vrf forwarding bianco
ip address 192.168.1.1 255.255.255.252
ip virtual-reassembly
!
router bgp 1000
no synchronization
bgp router-id 1.1.1.1
bgp log-neighbor-changes
no auto-summary
!
address-family ipv4 vrf nero
no synchronization
network 192.168.31.0
exit-address-family
!
address-family ipv4 vrf bianco
no synchronization
network 192.168.1.0
network 192.168.30.0
exit-address-family
!
```

Importante è osservare come nella tabella di routing del VRF nero vi sia anche la rete 30.0 appartenente al VRF-bianco

```
Router#show ip route vrf nero
C 192.168.31.0/24 is directly connected, Loopback2
B 192.168.30.0/24 is directly connected, 00:31:21, Loopback1
```

Nella tabella del VRF bianco vi è anche la rete 31.0, del VRF nero

```
Router#show ip route vrf bianco
B 192.168.31.0/24 is directly connected, 00:01:46, Loopback2
C 192.168.30.0/24 is directly connected, Loopback1
192.168.1.0/30 is subnetted, 1 subnets
C 192.168.1.0 is directly connected, Vlan1
```

Il risultato è che dal VRF bianco si raggiunge l'indirizzo 192.168.31.2, del VRF nero, e viceversa

```
Router#ping vrf bianco 192.168.31.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.31.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Router#ping vrf nero 192.168.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Vediamo quali route sono contenute nella tabella BGP:

```
Router#show ip bgp vpnv4 all
...
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf bianco)
*> 192.168.1.0/30 0.0.0.0 0 32768 ?
*> 192.168.30.0 0.0.0.0 0 32768 i
*> 192.168.31.0 0.0.0.0 0 32768 i
Route Distinguisher: 101:10 (default for vrf nero)
*> 192.168.1.0/30 0.0.0.0 0 32768 ?
*> 192.168.30.0 0.0.0.0 0 32768 i
*> 192.168.31.0 0.0.0.0 0 32768 i
Router#
```

Senza l'uso di MPLS abbiamo raggiunto il nostro obiettivo che ci consente di creare VPN complesse. Immaginiamo infatti il caso in cui un'azienda ha tre sedi A, B, C. Sia A che B devono raggiungere C ma non devono raggingersi a vicenda. Basterà allora utilizzare tre RD differenti per le tre sedi e con il BGP fare l'import/export tra A-C e B-C ma non A-B.

I protocolli di routing con VRF-lite sono pensati per un uso lato CE quando ci si aggancia da un PE per ottenere servizi MPLS. Lato provider ci sarà MPLS/BGP. Lato cliente si potrà utilizzare RIP, EIGRP, OSPF oppure BGP. In ogni caso lato provider le route verranno redistribuite nel BGP della rete MPLS dell'operatore. Ma noi vogliamo restare in ambito VRF-lite. Vediamo come utilizzare allora i protocolli di routing per agganciare tra loro tabelle VRF di router distinti mantenendo lisolamento delle VPN.

2.3 Configurazione 9 - Routing RIP -

RIP determina il VRF di un annuncio in base al VRF dell'interfaccia di provenienza. RIP propaga le route sulle interfacce in cui è attivo se hanno VRF corrispondente all'address-family in cui la route è definita. Vediamo una possibile configurazione:

```
ip vrf bianco
!
rd 100:10
!
ip vrf nero
rd 101:10
!
!
interface Loopback1
ip vrf forwarding nero
ip address 192.168.89.1 255.255.255.0
!
interface Loopback3
ip vrf forwarding bianco
ip address 192.168.88.1 255.255.255.0
!
interface Tunnel1
ip vrf forwarding nero
ip address 192.168.40.2 255.255.255.252
tunnel source 192.168.1.2      ⟵ Il tunnel attraversa un collegamento senza VRF.
                                  Altrimenti avremmo usato 'tunnel vrf NAME'
tunnel destination 192.168.1.1
!
interface Tunnel10
ip vrf forwarding bianco
ip address 192.168.50.2 255.255.255.252
tunnel source 192.168.1.2
tunnel destination 192.168.1.1
!
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.0
half-duplex
!
router rip
version 2
!
address-family ipv4 vrf nero
```

```
network 192.168.40.0
network 192.168.89.0
no auto-summary
version 2
exit-address-family
!
address-family ipv4 vrf bianco
network 192.168.50.0
network 192.168.88.0
no auto-summary
version 2
exit-address-family
!
```

Questo esempio è stato reso volutamente più complicato con l'uso dei tunnel. Il motivo è che per tenere i VRF separati tra router e router abbiamo bisogno di una interfaccia per ogni VRF. Se non vi sono interfacce fisiche a sufficienza dobbiamo crearne di logiche. Quindi possiamo usare tunnel o, se preferite, subinterfaces ethernet laddove possibile. In questo esempio gli aggiornamenti RIP passano attraverso i tunnel. I tunnel GRE non sono certo una novità in ambiente Cisco. Ma una loro applicazione relativamente recente li vede accoppiati alla feature VRF-lite.

Il comando **address-family ipv4 vrf NOME** permette di gestire i diversi VRF in modo disgiunto. Attenzione al fatto che RIP perde le informazioni relative all'RD oppure ad eventuali RT. Infatti non è in grado di trasportarle. La loro configurazione in questi esempi è utile solo laddove c'è il BGP, in grado di trasportarli e gestirli. Supponiamo di avere una LAN di tipo Campus dove bisogna distribuire vari livelli di accesso. Fino ad ora questo era fatto con le VLAN. Una VLAN guest darebbe un accesso ad Internet libero senza autenticazione mentre il traffico protetto andrebbe su VLAN differenti.

Utilizzando VRF si hanno nuove opportunità. Un modo più semplice è quello di raggruppare tutto il traffico della rete guest in un unico VRF in ciscuno switch di distribuzione. Quindi il traffico e trasportato attraverso la rete LAN mediante un GRE tunnel verso un dispositivo centrale che conduce verso Internet.

2.4 Configurazione 10 - Uso di EIGRP -

Con il protocollo EIGRP è possibile specificare l'AS e questo permette di mettere in corrispondenza AS differenti e quindi di tenere separate le differenti VRF tra router distinti. Tuttavia non sarà possibile propagare l'RD per il mancato supporto multiprotocollo da parte di EIGRP. A fini didattici è interessante osservare che i parametri relativi ai VRF 'possono essere diversi nei due router' in quanto non si propagano ma la corrispondenza è forzata tramite il numero di AS. E' una configurazione utilizzabile solo in assenza di BGP in 'casi di emergenza', come migrazioni transitorie.

```
hostname yourname
ip vrf blue                         ⟵ Con EIGRP non si può propagare
rd 100:10                           ⟵ Con EIGRP non si può propagare
!
!
interface FastEthernet0/0
description -- back to back ---
ip vrf forwarding blue              ⟵ Può essere diverso nei due router
ip address 192.168.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
description --- Internet ---
ip vrf forwarding blue              ⟵ Può essere diverso nei due router
ip address 192.168.30.152 255.255.255.0
duplex auto
speed auto
!
!
router eigrp 100                    ⟵ Può essere diverso nei due router
auto-summary
!
address-family ipv4 vrf blue        ⟵ Può essere diverso nei due router
network 192.168.1.0
auto-summary
autonomous-system 101               ⟵ Dev'essere uguale al router neighbor per metter su la
                                       sessione.  Questo comando esiste solo se si specifica la
                                       keywork vrf nel comando 'address-family ipv4'
exit-address-family
!
ip route vrf blue 0.0.0.0 0.0.0.0 192.168.30.254
!
prompt# show ip eigrp vrf blue interfaces
IP-EIGRP interfaces for process 101
Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers Un/Reliable SRTT Un/Reliable Flow Timer Routes
Fa0/0 1 0/0 9 0/1 50 0
yourname#
```

2.4.1 Descrizione

Con EIGRP possiamo creare una sessione tra due router distinti e trasferire le informazioni di routing dei corrispondenti VRF. Nelle configurazioni non è necessario che i due (o più) router condividano gli stessi RD. Le corrispondenze tra i processi EIGRP dei due router distinti si hanno con gli *l'Autonomous System Number* (AS) .

Ovviamente le network per essere propagate devono appartenere ad interfacce con VRF corrispondenti a quelli definiti con il comando addressfamily. L'autonomous system è configurabile solo se si usa il comando **address-family**.

Sfruttando diversi AS mettiamo in corrispondenza i processi EIGRP di router differenti. EIGRP non propaga l'RD tuttavia associando in fase di progetto gli RD agli AS possiamo mantenere separati i VRF tra router distinti. Ricordo ancora una volta che è necessario il BGP quando si vogliono propagare RD e RT.

2.5 Configurazione 11 - Inter-VRF con statiche -

Osserviamo le due righe di routing:

```
ip route vrf interno 0.0.0.0 0.0.0.0 10.0.1.1 global                (1)
ip route vrf interno 0.0.0.0 0.0.0.0 FastEthernet0 10.0.0.1         (2)
```

Nella riga (2) incontriamo una nuova sintassi. Supponiamo che la FastEthernet0 sia nella rete 10.0.0.0/24 e che non sia in un VRF. Allora le due righe fanno esattamente la stessa cosa e possono essere usate indifferentemente. La seconda contiene una informazione aggiuntiva rispetto la prima in quanto indica l'interfaccia la cui rete contiene l'indirizzo ip 10.0.0.1. La prima indica semplicemente che l'indirizzo ip si trova nella tabella di routing globale dove poi si determinerà l'interfaccia per ricorsione. Tecnicamente il route mappa staticamente l'ARP dell'indirizzo IP 10.0.0.1 sulla FastEthernet0. Supponiamo ora che la FastEthernet0 NON si trovi nella tabella di routing globale ma in un secondo VRF. Allora la (1) NON funziona ma la (2) si. Con la notazione (2) si può fare infatti route leak tra VRF. L'indicazione dell'interfaccia e dell'IP permette di bypassare il muro tra VRF e creare un canale diretto con la destinazione.

Con questo nuovo strumento possiamo fare NAT anche tra due VRF. Supponiamo un router con un VRF verso Internet ed uno differente verso la LAN. Ecco la configurazione funzionante per garantire la navigazione Internet al VRF lato LAN:

```
!  Cisco 1841 con IOS 15.1T
!
interface FastEthernet0/0
description --- rete interna ---
ip vrf forwarding reteinterna
ip address 192.168.30.254 255.255.255.0
ip nat enable
!
interface FastEthernet0/1
description --- Accesso ad Internet ---
ip vrf forwarding reteesterna
ip address 82.85.14.104 255.255.255.240
ip nat enable
!
ip nat pool INTERNET 82.85.14.104 82.85.14.104 netmask 255.255.255.224
ip nat source list 112 pool INTERNET vrf reteinterna overload
ip route vrf reteesterna 0.0.0.0 0.0.0.0 82.85.14.97
ip route vrf reteinterna 0.0.0.0 0.0.0.0 FastEthernet0/1 82.85.14.97
!
access-list 112 permit ip 192.168.30.0 0.0.0.255 any
!
```

La possibilità di utilizzare routing inter-VRF può essere inibita utilizzando il comando *no ip route static inter-vrf*. Se si inserisce questo comando nella configurazione il router non accetterà route statiche rimuovendo quelle già presenti con un messaggio del tipo:

```
*Mar 20 22:49:00.123: %IPRT-6-STATICROUTESACROSSVRF: Un-installing static route
0.0.0.0/0 from reteinterna routing table with outgoing interface FastEthernet0/1
```

2.6 Configurazione finale

La configurazione presentata deriva da un'applicazione reale. E' applicabile in qualsiasi circostanza in cui sono presenti diverse VLAN. Ma stavolta le reti restono separate anche a livello 3 nel router, grazie ai VRF, garantendo una reale autonomia delle varie aree, e una interazione tra esse solo quando espressamente voluto. Possiamo immaginare scuole, alberghi, uffici, con collegamenti VPN o meno. Le reti sono rigorosamente separate a tutti i livelli. I vantaggi sono:

- Un maggior grado di sicurezza. Il passaggio da una VLAN all'altra è bloccato dai VRF a livello3;
- Meno possibilità di errori e maggiore semplicità nella manutenzione;
- Possibilità di usare la stessa rete IP in VLAN differenti;
- Maggiore semplicita' nella gestione di flussi di traffico differenti;
- La separazione delle reti non termina nel router ma può proseguire verso VPN esterne (tunnel GRE ad esempio);
- Maggiore scalabilità della infrastruttura di rete
- Predisposizione all'accesso ad una rete MPLS, ad esempio nel caso di grosse reti
- Spesso consente di evitare l'aggiunta di un firewall, e quindi semplifica la rete

Nella configurazione di questo esempio convivono reti con livelli di sicurezza e servizi differenti.

- Il vrf 'access-point' è una rete wireless con accesso ad Internet. Vogliamo che su questa rete sia attivo un servizio DHCP per facilitare l'accesso ai clients. Vogliamo che questa rete non abbia accesso a null'altro che Internet, per preservare le altre reti Internet, considerando che la rete wireless e' normalmente la meno sicura o quella ad accesso piu' ampio;
- Il vrf 'rete-interna' è la parte privata della rete, ad esempio relativa ad uffici;
- Il vrf 'servizi' è una terza rete che fornisce servizi quali ad es. stampanti, server di posta etc.
- Il vrf 'voce' rappresenta una rete voip. Ottenere l'accesso vuol dire poter utilizzare telefoni software in quanto il PBX ip è in questa rete. Per quanto riguarda i telefoni hardware, in questo esempio usano un VLAN ID, e questo gli consente di essere collocati in qualsiasi rete bypassando i VRF, in quanto è responsabilità dello switch la connettività layer2.

Il codice non è ottimizzato e non vuole esserlo. Notate anche la configurazione di una VPDN PPTP e il fatto che anch'esse sono VRF-aware. Infatti da remoto si puo' accedere solo al VRF voce.

```
ip cef
!
!
ip dhcp use vrf connected
ip dhcp excluded-address 192.168.152.254
ip dhcp excluded-address 192.168.152.10 192.168.152.13
!
ip dhcp pool WIRELESSDHCP
 vrf accesspoint                                    ←— Questo pool DHCP è attivo
 network 192.168.152.0 255.255.255.0                    solo nel VRF ‘accesspoint’
 dns-server 10.99.125.1 10.99.125.2                     l’unico con servizio DHCP
 default-router 192.168.152.254
!
!
ip vrf accesspoint
 rd 1055:52                                         ←— Non esporta o importa nulla.  E’ una rete isolata
 !                                                      L’unico servizio e’ la navigazione Internet.
 !
ip vrf reteinterna                                  ←— La rete interna esporta e importa verso il vrf voc
 rd 1055:99                                         e quello servizi.  Qui si possono usare telefoni softw
 route-target export 1111:99
 route-target import 1111:444
 route-target import 1111:200
 !
ip vrf conferenceroom1                              ←— Ha accesso al VRF servizi
 rd 1055:50
 route-target export 1111:50
 route-target import 1111:200
 !
ip vrf conferenceroom2
 rd 1055:51
 route-target export 1111:51
 route-target import 1111:200
 !
ip vrf stanza101
 rd 1055:101
 route-target export 1111:101                           Anche le stanze hanno accesso ai servizi
 route-target import 1111:200
 !
ip vrf stanza102
 rd 1055:102
 route-target export 1111:102
 route-target import 1111:200
 !
ip vrf stanza103
 rd 1055:103
 route-target export 1111:103
 route-target import 1111:200
!
ip vrf voce
 rd 1055:10
 route-target export 1111:444
 route-target import 1111:99
 route-target import 1111:200
!
ip vrf servizi
 rd 1055:200
 route-target export 1111:200
 route-target import 1111:99
```

```
 route-target import 1111:101
 route-target import 1111:102
 route-target import 1111:103
 route-target import 1111:51
 route-target import 1111:50
!
vpdn enable
 !
vpdn-group 1                                        ←— Un accesso PPTP dall'esterno per manutenzione
 !  Default PPTP VPDN group                             Vedete più in basso la virtual-template che
 accept-dialin                                          limita l'accesso ai client vpn al VRF voce
 protocol pptp
 virtual-template 1
!
!
interface FastEthernet0/0
 ip address 10.5.157.178 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description --- VLAN trunk ---
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 description --------- vlan/vrf stanza101 -------------
 encapsulation dot1Q 101
 ip vrf forwarding stanza101
 ip address 192.168.101.254 255.255.255.0
 ip nat enable                                      ←— Tutti i VRF con lo stesso canale Internet
!
interface FastEthernet0/1.2
 description --------- vlan/vrf stanza102 -------------
 encapsulation dot1Q 102
 ip vrf forwarding stanza102
 ip address 192.168.102.254 255.255.255.0
 ip nat enable
!
interface FastEthernet0/1.3
 description --------- vlan/vrf stanza103 -------------
 encapsulation dot1Q 103
 ip vrf forwarding stanza103
 ip address 192.168.103.254 255.255.255.0
 ip nat enable
!
...snip...
!
interface FastEthernet0/1.24
 description ----- VOCE ------
 encapsulation dot1Q 10
 ip vrf forwarding voce
 ip address 192.168.100.254 255.255.255.0
 ip nat enable
!
interface FastEthernet0/1.25
 description --- NATIVA VLAN 1 VERSO SWITCH ---
 encapsulation dot1Q 1 native
 ip vrf forwarding reteinterna
 ip address 192.168.1.253 255.255.255.0
 ip nat enable
```

```
!
interface FastEthernet0/1.26
 description --- CONFERENCE ROOM 2---
 encapsulation dot1Q 51
 ip vrf forwarding conferenceroom2
 ip address 192.168.151.254 255.255.255.0
 ip nat enable
!
interface FastEthernet0/1.27
 description --- CONFERENCE ROOM 1 ---
 encapsulation dot1Q 50
 ip vrf forwarding conferenceroom1
 ip address 192.168.150.254 255.255.255.0
 ip nat enable
!
interface FastEthernet0/1.28
 description --- ACCESS-POINT ---
 encapsulation dot1Q 52
 ip vrf forwarding accesspoint
 ip address 192.168.152.254 255.255.255.0
 ip nat enable
!
interface FastEthernet0/1.29
 description ---------- servizi ----------
 encapsulation dot1Q 200
 ip vrf forwarding servizi
 ip address 192.168.200.254 255.255.255.0
 ip nat enable
!
interface ATM0/0/0                                  ←— Questi sono accessi Internet
 ...snip...
!
!
interface ATM0/1/0
 ...snip...
!
!
interface Virtual-Template1
 ip vrf forwarding voce
 ip unnumbered FastEthernet0/1.24
 peer default ip address pool VPNPOOL
 ppp authentication pap ms-chap
!
interface Dialer0
 ip address negotiated
 ip nat enable
 encapsulation ppp
 no ip route-cache cef
 no ip route-cache
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp chap hostname WSyA11@adsl
 ppp chap password 0 bEwm
 ppp pap sent-username WSA411@adsl password 0 bEwm
!
interface Dialer1
 ip address negotiated
 ip nat enable
 encapsulation ppp
 dialer pool 2
 dialer-group 2
```

```
 ppp chap hostname y0001@itesys.it
 ppp chap password 0 sy18
 ppp pap sent-username y001@itesys.it password 0 sy18
!
router bgp 222
 no synchronization
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 no auto-summary
!
 address-family ipv4 vrf voce
 no synchronization
 network 192.168.100.0
 exit-address-family
!
!
 address-family ipv4 vrf stanza103
 no synchronization
 network 192.168.103.0
 exit-address-family
!
 address-family ipv4 vrf stanza102
 no synchronization
 network 192.168.102.0
 exit-address-family
!
 address-family ipv4 vrf stanza101
 no synchronization
 network 192.168.101.0
 exit-address-family
!
 address-family ipv4 vrf servizi
 no synchronization
 network 192.168.200.0
 exit-address-family
!
 address-family ipv4 vrf conferenceroom2
 no synchronization
 network 192.168.151.0
 exit-address-family
!
 address-family ipv4 vrf conferenceroom1
 no synchronization
 network 192.168.150.0
 exit-address-family
!
 address-family ipv4 vrf reteinterna
 no synchronization
 network 192.168.1.0
 exit-address-family
!
ip local pool VPNPOOL 192.168.100.225 192.168.100.226
ip route 0.0.0.0 0.0.0.0 Dialer0                    <-- Tabella global
ip route vrf accesspoint 0.0.0.0 0.0.0.0 Dialer0        VRF diversi, stesso canale Internet
ip route vrf reteinterna 0.0.0.0 0.0.0.0 Dialer0        E' una conf.  NAT ripetuta per ogni VRF
ip route vrf conferenceroom1 0.0.0.0 0.0.0.0 Dialer0
ip route vrf conferenceroom2 0.0.0.0 0.0.0.0 Dialer0
ip route vrf servizi 0.0.0.0 0.0.0.0 Dialer0
ip route vrf stanza101 0.0.0.0 0.0.0.0 Dialer0
ip route vrf stanza102 0.0.0.0 0.0.0.0 Dialer0
ip route vrf stanza103 0.0.0.0 0.0.0.0 Dialer0
ip route vrf voce 0.0.0.0 0.0.0.0 Dialer0
```

```
!
!
no ip http server
no ip http secure-server
ip nat pool Internet 10.5.157.181 10.5.157.181 netmask 255.255.255.248
ip nat source list 127 pool Internet vrf accesspoint overload
ip nat source list 199 pool Internet vrf reteinterna overload
ip nat source list 126 pool Internet vrf conferenceroom1 overload
ip nat source list 125 pool Internet vrf conferenceroom2 overload
ip nat source list 198 pool Internet vrf servizi overload
ip nat source list 101 pool Internet vrf stanza101 overload
ip nat source list 102 pool Internet vrf stanza102 overload
ip nat source list 103 pool Internet vrf stanza103 overload
ip nat source list 124 pool Internet vrf voce overload
ip nat source static tcp 192.168.100.182 22 10.5.157.182 22 vrf voce extendable
ip nat source static tcp 192.168.100.183 80 10.5.157.182 80 vrf voce extendable
!
access-list 101 permit ip 192.168.101.0 0.0.0.255 any
access-list 102 permit ip 192.168.102.0 0.0.0.255 any
access-list 103 permit ip 192.168.103.0 0.0.0.255 any
access-list 124 permit ip 192.168.100.0 0.0.0.255 any
access-list 125 permit ip 192.168.151.0 0.0.0.255 any
access-list 126 permit ip 192.168.150.0 0.0.0.255 any
access-list 127 permit ip 192.168.152.0 0.0.0.255 any
access-list 198 permit ip 192.168.200.0 0.0.0.255 any
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
dialer-list 1 protocol ip permit
dialer-list 2 protocol ip permit
```

```
prompt#show ip bgp vpnv4 vrf voce
BGP table version is 110, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1055:10 (default for vrf voce)
*> 192.168.1.0      0.0.0.0                  0         32768 i
*> 192.168.100.0    0.0.0.0                  0         32768 i
```

192.168.100.0, 192.168.1.0 sono il VRF 'voce' e quello 'interno'. Il vrf voce esporta solo verso la rete interna, per questo abbiamo solo queste due righe di routing in tabella bgp. Vediamo cosa succede se togliamo l'export dalla rete interna. Ci aspettiamo che nel VRF voce non arrivi più l'annuncio. Pertanto i due VRF non potranno più comunicare.

```
router(config)#ip vrf reteinterna
router(config-vrf)#no  route-target export 1111:99
router(config-vrf)#exit
router(config)#exit
router#show ip bgp vpnv4 vrf voce   (oppure: show ip bgp vpnv4 rd 1055:10)
BGP table version is 113, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1055:10 (default for vrf voce)
*> 192.168.100.0    0.0.0.0                  0         32768 i
```

Affinchè due VRF comunichino nelle tabelle BGP di entrambi devono apparire le route che ne consentano la comunicazione.

Si noti infine che in questa configurazione vi è un salto dalle tabelle di routing VRF alla tabella di routing. Lo si effettua per navigare verso Internet. La dialer0, con cui si va verso Internet, NON ha VRF, ma giace nella tabella di routing globale. La riga di route 'ip route vrf servizi 0.0.0.0 0.0.0.0 Dialer0' è molto interessante. Proprio per il salto da una tabella di routing all'altra senza annunci o uso di BGP. Ma ricordiamoci che c'e' il NAT e l'ip pubblico tramite NAT è configurato su ogni VRF.

```
router#show ip route vrf voce

Routing Table: voce
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

B    192.168.1.0/24 is directly connected, 00:12:25, FastEthernet0/1.25
C    192.168.100.0/24 is directly connected, FastEthernet0/1.24
S*   0.0.0.0/0 is directly connected, Dialer0
```

Note:

1. Se togliete la configurazione di un pool NAT ma non il comando 'ip nat enable' noterete che non riuscirete a fare routing tra interfacce appartenenti allo stesso VRF. Probabilmente questo è dovuto alla logica di funzionamento del NAT all'interno del router;

2. Se provate a cancellare un NAT pool vi potrebbe apparire il messaggio di errore 'Dynamic map in use'. Normalmente basta un comando 'clear ip nat trans ...' per risolvere il problema. In alcuni IOS ciò potrebbe non bastare e potremmo essere costretti a cancellare e poi ricreare un intero vrf. Ecco l'esempio:

   ```
   router#clear ip nat tran vrf voce *
   router#conf t
   Enter configuration commands, one per line.  End with CNTL/Z.
   router(config)#no ip nat source list 124 pool MIOPOOL vrf voce overload
   Dynamic mapping in use, do you want to delete all entries? [no]: yes
   %Error: Dynamic mapping still in use, cannot remove
   ```

3. Attenzione alle righe di nat statico come questa: 'ip nat source static 192.168.120.152 IPPUBBLICO vrf miovrf' Se IPPUBBLICO non è presente in nessuna interfaccia fisica o logica, e questo è possibile quando ad esempio il pool è composto di una classe di indirizzi ip, potrebbe essere necessario creare una interfaccia di loopback con nat abilitato e come unico indirizzo IP il valore IPPUBBLICO. L'interfaccia di loopback andrebbe associata a 'miovrf', con 'ip vrf forwarding miovrf'. Solo a questo punto l'indirizzo IPPUBBLICO viene associato al vrf corretto. La sintomatologia legata a un problema del genere è un malfunzionamento del NAT, che potrebbe funzionare solo per alcuni secondi per poi improvvisamente bloccare le traduzioni.

2.7 Conclusioni

L'RD è un identificativo di 8 byte che viene unito ad un indirizzo IP creando un indirizzo VPN-IPv4 univoco, con la forma RD:IP.

A meno che non usiate il BGP, l'uso dell'RD in una configurazione VRF-lite non è fondamentale, si può usare il comando **ip vrf NOME** senza rd specificato e IOS creerà una nuova tabella di routing.

Nel caso di reti MPLS/VPN viene utilizzato BGP con il supporto alle estensioni multiprotocollo, RFC2858 . È il protocollo BGP che può trasportare indirizzi RD:IP che non sono indirizzi IP, edè per questo che si usa nelle reti MPLS. BGP infatti è multiprotocollo. Inoltre può trasportare altri dati come le communities, nel nostro caso eventuali valori route-target dove si indica, con i comandi 'import/export' quali circuiti di una VPN possono vederne altri e così via.

La configurazione di una rete VRF-lite con l'uso dei protocolli di routing in realtà è cosa complessa. E' necessario conoscere a priori i vari algoritmi di routing dinamico e poi passare al loro utilizzo in ambito VRF-lite.

Infine bisogna scegliere con attenzione l'immagine IOS dei router Cisco in uso, in quanto si corre il serio pericolo di non avere attive tutte le features necessarie (in particolare i protocolli di routing).

Indice analitico