Progetto di Reti di Calcolatori 2
-
Implementazione di una rete dorsale

Giorgio Ravera

A.A 2007/2008

Indice

Obiettivo

L'obiettivo del progetto è quello di realizzare una rete dorsale utilizzando apparati CISCO e NOKIA sulla base dei seguenti concetti visti a lezione:

- vlan
- frame relay
- ppp
- algoritmi di routing (IGP e BGP)
- MPLS
- VPN
- firewall

Il progetto è stato realizzato con la collaborazione del Prof. P.P. Baglietto e del Dott. Stefano Lassi.

Capitolo 1

Schema Globale

La rete che si è realizzata è riportata in figura 1.1.

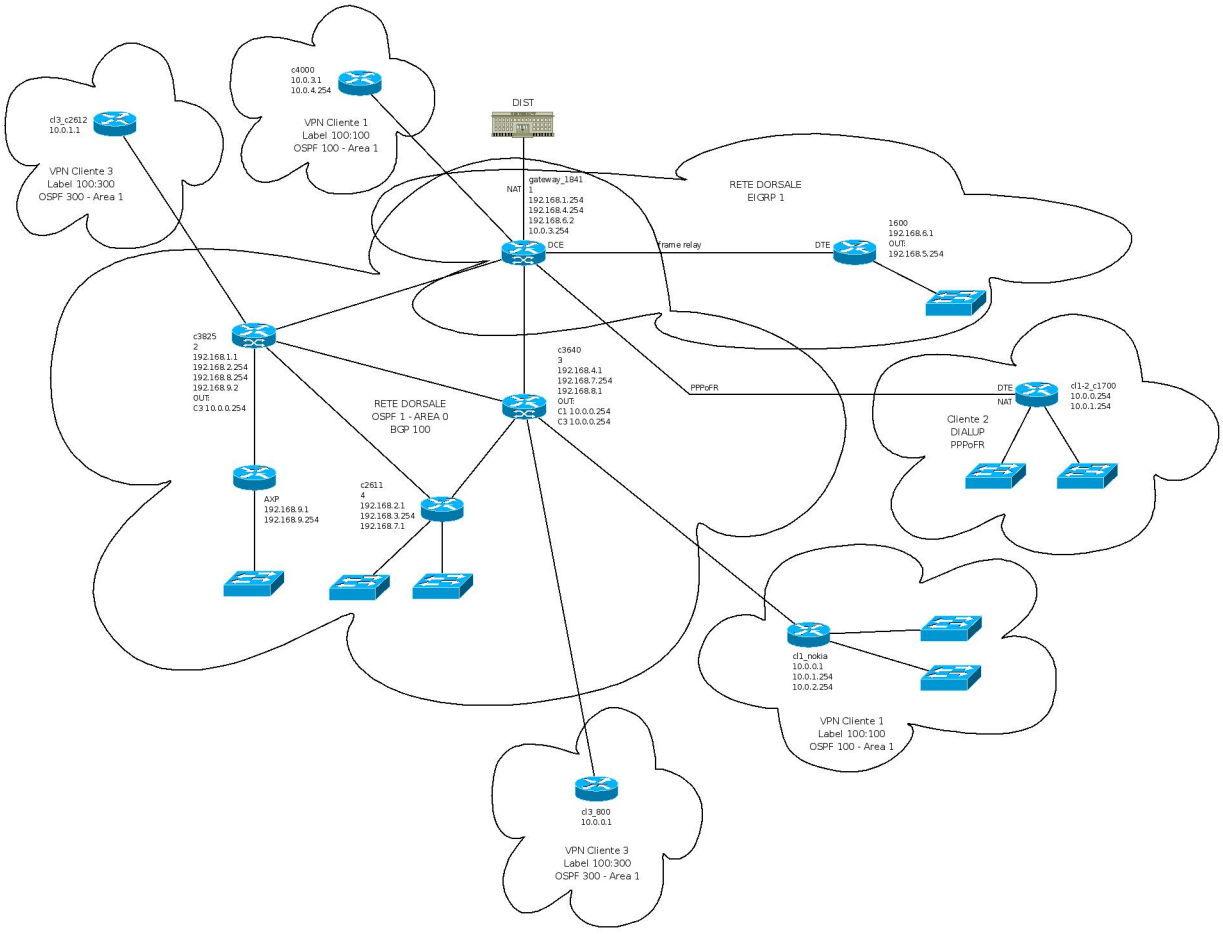

Figura 1.1: Schema della rete

Si possono identificare i seguenti elementi principali:

- Rete Dorsale Principale
- Rete Dorsale Secondaria
- VPN Cliente 1
- Rete Cliente 2
- VPN Cliente 3 (divisa in 2 regioni)
- Link verso Internet

1.1 Rete Dorsale Principale

La rete dorsale principale è composta da 4 router cisco:

- 1841
- 3825
- 3640
- 2611

Il livello fisico è realizzato attraverso **ethernet** sul quale vengono trasportati **pacchetti IP**. Per simulare una vera dorsale, tali router sono stati collegati tra loro attraverso più collegamenti in modo da garantire l'attività qualora uno o più link venissero scollegati. Si è utilizzato, come algoritmo di routing **OSPF** in cui tutte le reti sono dichiarate appartenenti all'area 0.

Sempre di questa rete fa parte il modulo Application eXtendible Platform, collegato come Network Module, al router 3800 che di fatto costituisce un router indipendente. La comunicazione con il reso della rete avviene attraverso un'interfaccia virtuale che collega il modulo con il router ospitante sulla qualle è stata creata una rete punto a punto su ethernet.

1.2 Rete Dorsale Secondaria

La rete è composta da 2 router cisco:

- 1841
- 1601

Il livello fisico è realizzato attraverso un **collegamento seriale** sul quale vengono vengono incapsulati **pacchetti IP** tramite **frame-relay**. Si è scelto di utilizzare l'algoritmo di routing **EIGRP** proprietario di Cisco. L'idea di realizzare questo ramo di rete è nata dal fatto di poter utilizzare link fisici differenti e algoritmi di routing diversi per poterli ridistribuire uno sull'altro.

1.3 VPN Cliente 1

La rete del cliente 2 è divisa in due blocchi collegati tra loro tramite la dorsale. I router utilizzati, Cisco 4000 per la prima parte e Nokia IP 120 per la seconda, comunicano tra loro attraverso la rete dorsale che incapsula i pacchetti ip in **pacchetti MPLS**. L'algoritmo di routing utilizzato è **OSPF** che viene opportunamente ridistribuito all'interno della dorsale stessa tramite il protocollo **BGP** tra i nodi di frontiera.

Logicamente le due reti sono interconnesse direttamente tra loro. La rete MPLS è totalmente trasparente all'utente che si dovrà limitare a configurare in maniera opportuna i due router di frontiera con le specifiche fonrite dal provider per il protocollo di routing interno (OSPF) e impostare gli ip dei rispettivi default gateway (router della dorsale che aggiungono o rimuovono dei label MPLS) dei due segmenti.

1.4 Rete Cliente 2

La rete di un ipotetico Cliente 2 è collegata alla dorsale utilizzando il **protocollo PPP** incapsulato su linea framerelay. Tutti i dati di connessione (default gateway, dns e ip) vengono negoziati tramite il protocollo stesso. Il router del cliente, in questo caso il cisco 1700 gestisce due reti separate che vengono mascherate in uscita verso la dorsale. All'interno della rete del cliente si è utilizzato il protocollo di routing **EIGRP**.

Questa situazione descrive un possibile scenario di utente casalingo che ha più di una rete e vuole connettere più macchine ad internet disponendo di un solo indirizzo ip pubblico. In questo caso, l'ip assegnato apparterrà alla dorsale stessa. L'idea era quella di utilizzare ATM e PPPoA ma non si disponevano di interfacce che lo supportassero.

1.5 VPN Cliente 3

Come la rete del cliente 1, anche quella del cliente 3 è divisa in due blocchi collegati tra loro tramite la dorsale. I router utilizzati, Cisco 2612 per la prima parte e Cisco 877 per la seconda, comunicano tra loro attraverso la rete dorsale che incapsula i pacchetti ip in **pacchetti MPLS**. L'algoritmo di routing utilizzato è **OSPF** che viene opportunamente ridistribuito all'interno della dorsale stessa tramite il protocollo **BGP** tra i nodi di frontiera.

Da notare che gli ip utilizzati all'interno della rete Cliente 1 e Cliente 3 sono gli stessi e quindi, senza MPLS andrebbero in collisione. Il fatto di utilizzare i label (100:100 per la

prima, 100:300 per la seconda). Anche gli algoritmi di routing vengono instradati tramite due istanze di routing virtuale differente (vrf Cliente1 e vrf Cliente3).

Capitolo 2

Vlan

2.1 Descrizione Generale

Per poter interconnettere tra loro i vari apparati si è scelto di utilizzare uno switch Cisco Catalyst 2950, dotato di 12 porte FastEthernet (10-100 Mbps). Per separare i domini di collisione di ogni rete si è scelto di usare il protocollo IEEE 802.1Q. In questo modo si è potuta realizzare una separazione logica delle reti.

In linea di principio, si è creata una vlan per ogni rete presente nello schema. In rari casi si è interconnesso i router direttamente tra loro per risparmiare porte dello switch. Per dare un idea più precisa viene riportato l'output parziale del comando **show vlans**:

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/17, Fa0/18, Fa0/19, Fa0/23
                                                 Gi0/1, Gi0/2
10   RETE_1                            active    Fa0/7, Fa0/8
20   RETE_2                            active    Fa0/9, Fa0/10
30   RETE_3                            active    Fa0/11, Fa0/12
40   RETE_4                            active    Fa0/13, Fa0/14
50   RETE_5                            active    Fa0/15, Fa0/16
70   RETE_7                            active
80   RETE_8                            active
100  Cliente1                          active    Fa0/1, Fa0/2
200  Cliente2                          active    Fa0/3, Fa0/4
300  Cliente3                          active    Fa0/5, Fa0/6
```

Come si può vedere dall'output del comando, le ultime 8 porte (17-24) non sono presenti in lista o appartengono alla vlan 1. Questo accade perché tali porte sono impostate in modalità **trunk**. Nel caso in cui lo stesso router sia connesso a più vlan si è scelto di connetterlo ad una sola porta ethernet dello switch impostandola in questa modalità. Nel router, è necessario dichiarare tante sotto interfacce quante sono le vlan al quale si desidera connetterlo e, per ognuna dichiarare un incapsulazione dot1q.

Da notare che sono state dichiarate due vlan (70 e 80) pur non avendo alcuna porta in access. Questa operazione è necessaria perché il traffico di tali porte passa ugualmente nelle interfacce dichiarate in trunk. Se non fossero state definite, i pacchetti ad esse associate non verrebbero instradati nelle porte in trunk.
Ecco, per completezza, un estratto del comando **show interfaces trunk**:

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/20      on           802.1q         trunking      1
Fa0/21      on           802.1q         trunking      1
Fa0/22      on           802.1q         trunking      1
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/20      1-4094
Fa0/21      1-4094
Fa0/22      1-4094
Fa0/24      1-4094

Port        Vlans allowed and active in management domain
Fa0/20      1,10,20,30,40,50,70,80,100,200,300
Fa0/21      1,10,20,30,40,50,70,80,100,200,300
Fa0/22      1,10,20,30,40,50,70,80,100,200,300
Fa0/24      1,10,20,30,40,50,70,80,100,200,300
```

In questo output non compaiono le porte 17 18 19 e 23 che nella schermata precedente erano state rilevate come appartententi alla vlan 1. Questo avviene perchè a tali porte non è connesso nulla.
Ecco un estratto del comando **show interfaces**:

```
Vlan10 is up, line protocol is up
  Hardware is EtherSVI, address is 001e.1330.2f41 (bia 001e.1330.2f41)
  Internet address is 192.168.1.253/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
.....
Vlan20 is up, line protocol is up
  Hardware is EtherSVI, address is 001e.1330.2f42 (bia 001e.1330.2f42)
  Internet address is 192.168.2.253/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
.....
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001e.1330.2f03 (bia 001e.1330.2f03)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
```

```
     reliability 255/255, txload 1/255, rxload 1/255
.....
FastEthernet0/2 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 001e.1330.2f04 (bia 001e.1330.2f04)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
.....
FastEthernet0/19 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 001e.1330.2f15 (bia 001e.1330.2f15)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
.....
FastEthernet0/20 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001e.1330.2f16 (bia 001e.1330.2f16)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

E' interessante notare che questo switch di livello 3 può possedere più di un indirizzo ip, uno per vlan. Lo si può vedere dall'interfaccia virtuale vlan10 e vlan20 corrispondenti alle vlan ominime.

2.2 Configurazione Access

Impostare una porta in modalità access su una vlan è molto semplice:

```
switch_mpls# configure terminal
switch_mpls(config)#interface FastEthernet 0/1
switch_mpls(config-if)#switchport mo
switch_mpls(config-if)#switchport mode acc
switch_mpls(config-if)#switchport mode access
switch_mpls(config-if)#switchport access vlan 100
switch_mpls(config-if)#end
switch_mpls#write mem
Building configuration...
[OK]
switch_mpls#
```

Una tale procedura genera, nel file di configurazione, le seguenti righe:

```
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode access
```

Come si può vedere l'output dei comandi riflette esattamente ciò che verrà inserito nel file di configurazione. Pertanto, nel proseguimento del testo, verranno solamente mostrati i file di configurazione.

2.3 Configurazione Trunk

Una porta, per essere configurata in modalità trunk, necessita la specifica del protocollo di incapsulamento da utilizzare. In questo caso si è scelto IEEE 802.1Q e quindi il protocollo, in ambiente cisco, prende il nome di **dot1q**.
Questo è un esempio di configurazione di un interfaccia in trunk:

```
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

2.4 Cisco Discovery Protocol

CDP è un protocollo che consente di identificare gli apparati cisco direttamente connessi. Per avere un idea della sua utilità viene presentato un output del comando **show cdp neighbors**

```
switch_mpls#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
cl1-2_c1700      Fas 0/3           164           R S      1721      Fas 0
gateway_1800     Fas 0/21          127          R S I     1841      Fas 0/1
cl3_c800         Fas 0/5           161          R S I     877       Fas 0
c3640            Fas 0/22          126          R S I     3640      Eth 0/0
c1600            Fas 0/15          162            R       1601      Eth 0
c2611            Fas 0/24          153            R       2611      Eth 0/0
c3825            Fas 0/20          179          R S I     3825      Gig 0/0
```

Appare chiaro come sono collegati i componenti tra loro e su quale porte vengono visti. Questo strumento può essere di grande aiuto. Per completezza si consiglia di visionare il file di configurazione dello switch nel paragrafo 6.1.1.

Capitolo 3

Frame Relay

3.1 Descrizione Generale

l Frame Relay o (Frame-mode Bearer Service) è una tecnica di trasmissione a commutazione di pacchetto su interfacce seriali, introdotta dalla ITU-T a partire dalla raccomandazione I.122 del 1988. Può essere pensato come una linea virtuale affittata tra 2 punti tra i quali si possono inviare frame di lunghezza variabile. Rispetto a X.25 fornisce un servizio minimale; infatti, non fornisce informazioni sull'avvenuta ricezione e non fornisce controllo di flusso.

Permette di inviare dati con banda a richiesta: lutente può richiedere banda più alta secondo il bisogno. Comunque si possono specificare banda minima garantita oltre che banda massima. Implementa solo lo strato fisico e quello di data-link (rispettivamente i livelli 1 e 2 del modello OSI), quindi può essere usato, per esempio, come trasporto per IP su internet. Viene usato per connettere diverse LAN su WAN, dal momento che permette di trasmettere frame di dimensione massima 8192 byte, e può mandare pacchetti senza problemi di frammentazione. Simula quindi una LAN estesa su WAN.

Nel progetto sono state realizzate due connessioni seriali:

- Rete Dorsale Secondaria
- Rete Cliente 2

In entrambe le reti si è scelto di incapsulare i pacchetti (IP nel primo caso e PPP nel secondo) in frame-relay. Per realizzare fisicamente un collegamento framerelay si possono scegliere due tecniche di realizzazione dei circuiti:

- Permanent Virtual Circuit: PVC
- Switched Virtual Circuit: SVC

Per semplicità si è scelto di creare il collegamento definendo a priori il circuito e basandoci su una mappaura IP-circuito dinamica e quindi automatica.

Frame relay usa due tipologie di interfacce: DTE (Data Terminal Equipment), utilizzata lato cliente, e DCE (Data Circuit-Terminating Equipment) usata lato provider. La

differenza deriva dal fatto che lato provider arrivano più circuiti virtuali (uno per utente) e serve uno switch che li commuti correttamente.

3.2 DTE

Lato utente la configurazione è molto semplice e viene riassunta dal seguente file di configurazione:

```
interface Serial0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type cisco
 ip address 192.168.6.1 255.255.255.252
 frame-relay interface-dlci 60
```

Come si può vedere il circuito virtuale permanente è il numero 60. Tale numero è identificato dal **DLCI** (Data Link Connection Identify). Sempre dal file di configurazione si può dedurre che esistono diverse implementazioni di **LMI** (Local Management Interface), uno standard di segnalamento tra router in ambiente frame-relay che fornisce informazioni su indirizzi globali, ip, circuiti e stati delle connessioni, i più comuni sono:

- cisco
- asci
- q933a

In caso di assenza di tale parametro, viene attivata una procedura di autosense. Da notare che non vengono indicate alcune mappature ip circuito virtuale. Questo indica che si utilizza un Dynamic Map. Per renderlo statico bastava aggiungere la seguente istruzione:

```
frame-relay map ip 192.168.6.2 60
```

che indicava che l'ip 192.168.6.2 si trovava all'altro capo del circuito virtuale 60.

In questa configurazione si può associare un solo circuito virtuale per linea seriale. E' possibile assegnare più di un circuito alla stessa linea tramite la definizionedi ulteriori interfacce virtuali. I parametri relativi alla linea resteranno nell'area relativa all'interfaccia, quelli specifici del canale (ip ad esempio) andranno in quella virtuale.

```
interface Serial0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type cisco
!
interface Serial0.60 point-to-point
```

```
 ip address 192.168.6.1 255.255.255.252
 frame-relay interface-dlci 60
!
```

Da notare che il nome dell'interfaccia virtuale è il numero del canale DLCI non devono essere necessariamente correlati. Lo si fa per semplicità e per mantenere una logica nella configurazione.

3.3 DCE

La configurazione dell'interfaccia DCE è un po' più complicata perché richiede parametri aggiuntivi. Segue un estratto del file di configurazione del router 1841:

```
frame-relay switching
!
...
interface Serial0/0/0
 bandwidth 2000
 no ip address
 encapsulation frame-relay
 clock rate 2000000
 frame-relay lmi-type cisco
 frame-relay intf-type dce
!
interface Serial0/0/0.60 point-to-point
 ip address 192.168.6.2 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 frame-relay interface-dlci 60
!
```

Come si può osservare è necessario, in questo caso, specificare sia la banda che il clockrate. Il DTE si calcola questi parametri dal DCE al quale è connesso e il DCE stesso li deve imporre. E' anche necessario indicare la tipologia di interfaccia (frame-relay intf-type dce) perché di default una seriale in frame-relay è imostata in modalità DTE.

Da notare frame-relay switching. Questa impostazione consente di fare switching tra due o più canali virtuali tramite interfacce dce. Quando si ha un interfaccia DCE è necessario impostare questa opzione.
Per comprendere meglio si osservino gli output sottostanti:

```
LATO DTE

c1600#show interfaces serial 0
Serial0 is up, line protocol is up
```

```
  Hardware is QUICC Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
.....

c1600#show interfaces serial 0.60
Serial0.60 is up, line protocol is up
  Hardware is QUICC Serial
  Internet address is 192.168.6.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY
  Last clearing of "show interface" counters never

c1600#show frame-relay pvc

PVC Statistics for interface Serial0 (Frame Relay DTE)

               Active     Inactive      Deleted       Static
  Local           1            0            0            0
  Switched        0            0            0            0
  Unused          0            0            0            0

DLCI = 60, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0.60

  input pkts 266           output pkts 254          in bytes 22029
  out bytes 23311          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 134       out bcast bytes 12880
  5 minute input rate 1000 bits/sec, 3 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
  pvc create time 00:12:33, last time pvc status changed 00:04:43

c1600#show frame-relay lmi interface serial 0

LMI Statistics for interface Serial0 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0 Invalid Prot Disc 0
  Invalid dummy Call Ref 0 Invalid Msg Type 0
  Invalid Status Message 0 Invalid Lock Shift 0
  Invalid Information ID 0 Invalid Report IE Len 0
```

```
  Invalid Report Request 0 Invalid Keep IE Len 0
  Num Status Enq. Sent 85 Num Status msgs Rcvd 66
  Num Update Status Rcvd 0 Num Status Timeouts 19
  Last Full Status Req 00:00:13 Last Full Status Rcvd 00:00:13

c1600#show frame-relay map
Serial0.60 (up): point-to-point dlci, dlci 60(0x3C,0xCC0), broadcast
          status defined, active

LATO DCE
gateway_1800#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 2000 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
.....

gateway_1800#show interfaces serial 0/0/0.60
Serial0/0/0.60 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.6.2/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY
  Last clearing of "show interface" counters never

gateway_1800#show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DCE)

              Active     Inactive      Deleted       Static
  Local          1            0            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0

DLCI = 60, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/0.60

  input pkts 21979         output pkts 21899        in bytes 1816000
  out bytes 1844280        dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
```

```
  out bcast pkts 20699     out bcast bytes 1778215
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 1d00h, last time pvc status changed 00:10:39
.....

gateway_1800# show frame-relay map
Serial0/0/0.60 (up): point-to-point dlci, dlci 60(0x3C,0xCC0), broadcast
          status defined, active
.....
```

3.4 SVC

Per impostare SVC si sarebbe dovuto inserire una serie di comandi simili alla seguente:

```
interface serial 0
 ip address 192.168.6.2 255.255.255.252
 encapsulation frame-relay
 map-group GR_NAME
 frame-relay lmi-type q933a
 frame-relay svc
!

map-list GR_NAME source-addr E164 123456 dest-addr E164 654321
 ip 192.168.1.254 class fast
 ip 192.168.2.1 class slow
!
map-class slow-class
  frame-relay cir in 128000
  frame-relay cir out 56000
!
map-class frame-relay fast
 frame-relay cir in 1000000
 frame-relay cir out 128000
!
```

Fondamentale è il comando map-list che da indicazione su sorgente e destinazione dei pacchetti per stabilire il circuito. Sempre attraverso le map-list si possono definire classi di servizio differenti.

3.5 PPP over Frame Relay

Il **PPP** (Pont-to-Point Protocol) è un protocollo

Le rete del Cliente 2 è stata creata per simulare una connessione dialin da parte di un generico cliente. L'idea originaria era quella di realizzare una connessione PPPoA o PPPoE su ATM nel primo caso, su ATM Lan Emulation nel secndo. Purtroppo, non dispondenti di interfacce seriali o SDH compatibili con tale tecnologia si è dovuto ripiegare su seriale con frame-relay.

L'idea è quella di utilizzare un collegamento seriale sul quale transitano pacchetti IP incapsulati prima in PPP e poi in frame-relay. Anche in questo caso sarà necessario definire l'interfaccia seriale come in precedenza (un capo DTE, l'altro DCE) e predisporre tante interfacce virtuali quanti sono i canali. Nel caso di PPP è necessario utilizzare un ulteriore interfaccia virtuale, chiamata **Virtual-Template** che serve per definire i parametri di atutenticazione e ciò che dovrà essere negoziato (ip, gateway, dns e altro ancora).
Vediamo, per prima cosa, i parametri di configurazione delle due interfacce seriali:

```
LATO DCE - Provider

interface Serial0/1/0
 bandwidth 2000
 no ip address
 encapsulation frame-relay
 no snmp trap link-status
 clock rate 2000000
 frame-relay lmi-type ansi
 frame-relay intf-type dce
!
interface Serial0/1/0.100 point-to-point
 frame-relay interface-dlci 100 ppp Virtual-Template1
!

LATO DTE - Client

interface Serial0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
!
interface Serial0.100 point-to-point
 frame-relay interface-dlci 100 ppp Virtual-Template1
!
```

Come si può notare, la configurazione delle due interfacce è analoga alla precedente. L'unica differenza risiede nell'interfaccia seriale virtuale. é necessario specificare che il canale DLCI (100 nel nostro caso) sia dedicato al traffico di pacchetti PPP e i parametri di tale protocollo sono definiti in un Virtual-Template (1 nel nostro caso). Vediamo ora la configurazione delle due interfacce Virtual-Template:

```
LATO DCE - Provider

username framerelay password 7 030752180500
!
...
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/1.10
 ip nat inside
 ip virtual-reassembly
 peer default ip address dhcp
 ppp authentication chap pap
 ppp chap hostname gateway
 ppp chap password 7 045802150C2E
 ppp pap sent-username gateway password 7 121A0C041104
!
LATO DTE - Client

interface Virtual-Template1
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
 ppp authentication chap dialin
 ppp chap hostname framerelay
 ppp chap password 7 0822455D0A16
 ppp pap sent-username framerelay password 7 02050D480809
 ppp ipcp dns request
 ppp ipcp route default
!
```

La keyword ip *unnumbered* indica che l'indirizzo IP dell'interfaccia sarà quello definito su quella in argomento al comando stesso (in questo caso FastEthernet0/1.10 ha come ip 192.168.1.254). In questo modo si realizza un bridge tra le due interfacce.

Per quanto riguarda l'autenticazione si è scelto di utilizzare, sia **PAP** (Password Authentication Protocol) che **CHAP** (Challenge-Handshake Authentication Protocol). Si imposta questa configurazione utilizzando la stringa *ppp authentication chap pap*. Siccome l'autenticazione deve essere fatta solo dal provider, lato client è necessario aggiungere la chiave callin che indica che non è necessario autenticare l'altro apparato.

Nel caso in cui non si usino sistemi di autenticazioni complessi come Radius, l'autenticazione viene fatta sulla base della coppia hostname - password (quest'ultima di default è *cisco*). Pertanto dovranno essere creati i rispettivi utenti su entrambe le macchine. Si possono bypassare tali imposizioni attraverso i comandi *ppp chap password* e *ppp pap*

sent-username. Come sempre, attivando il servizio **password-encryption**, nel file di configurazione non verrà mostrata la password in chiaro ma solamente il suo hashcode.

Infine si noti la gestione del peer: lato provider è necessario impostare la chiave *peer default ip address dhcp* che indica al router che dovrà assegnare l'indirizzo al peer tramite dhcp. Il server dhcp che verrà usato sarà quello assegnato alla rete su cui si trova l'interfaccia seriale. Nel nostro caso, siccome è dichiarata unnumbered su FastEthernet 0/1.10 si userà il dhcp della rete 192.168.1.0 che è il router Cisco 3847. Lato client sarà necessario impostare, il fatto che tramite PPP dovranno essere negoziati:

- indirizzo IP - *ip address negotiated*
- indirizzo del default gateway - *ppp ipcp route default*
- indirizzo dei server DNS - *ppp ipcp dns request*

Capitolo 4

Algoritmi di routing

Quando si realizza una rete di dimensioni molto grandi, composta da diverse sottoreti, è necessario, per ogni router, impostare le tabelle di routing e calcolare un percorso ottimo (o presento tale) verso il default gateway. Se i router sono tanti e di diverse tipologie, la loro configurazione può essere complicata e lunga. In più una minima variazione sulla topologia implicherebbe la riconfigurazione di molti apparati.

Una soluzione per ovviare a simili problemi è rappresentata dall'utilizzo di un appropriato algoritmo di routing. Esistono due tipologie di algoritmi differenti:

- **IGP**: Interior Gateway Protocoll: usato per distribuire le tabelle di routing tra più reti direttamente connesse
- **BGP**: Border Gateway Protocoll: usato nei router di frontiera per interconnettere più reti tra loro

4.1 IGP

I protocolli IGP hanno il compito di distribuire le tabelle di routing agli apparati direttamente connessi e si occupano di trovare il percorso ottimo per collegare tra loro le reti. Sono molto utili in caso di collegamenti multipi tra gli apparati per ricalcolare i percorsi quando un link dovesse interrompersi.
I protocolli IGP più diffusi sono classificati in due categorie differenti in base al loro funzionamento:

- **metrico** : calcola i pesi sulla base degli hop rilevati. I più diffusi sono:
  - **RIP** 1 e 2 (Routing Information Protocoll): il più famoso e facile da configurre ma presenta problemi di gestione e falle di sicurezza.
  - **IGRP** (Interior Gateway Routing Protoll): protocollo proprietario di Cisco sviluppato per migliorare RIP.
  - **EIGRP** (Enhanced Interior Gateway Routing Protoll): evoluzione di IGRP. Consente procedure di autenticazione.

- **link state**: calcola i pesi sulla base dello stato del link. I più diffusi sono:
  - **OSPF** (Open Short Path First): in assoluta è il protocollo più diffuso e performante. Consente procedure di autenticazione e può ragruppare più reti in una struttura gerarchica.
  - **IS-IS**: protocollo poco usato e difficile da configurare

Nel progetto sono stati implementati due algoritmi IGP: EIGRP ed OSPF. Il primo nella Dorsale Secondaria, il secondo nella Primaria con la redistribuzione di uno sull'altro e viceversa.

4.1.1 EIGRP

La configurazione di EIGRP è molto semplice se non si richiedono parametri particolari. E' necessario dichiarare un numero identificativo del processo di routing e inserire per esso le specifiche. E' possibile configurare diverse istanze di EIGRP, come di qualsiasi altro protocollo, impostando opportunamente i parametri.
Si consideri la seguente configurazione:

```
router eigrp 1
 network 192.168.5.0
 network 192.168.6.0 0.0.0.3
 no auto-summary
!
```

Da questa configurazione si può capire che l'istanza 1 di EIGRP è attiva sulle interfacce che appartengono alle reti 192.168.5.0/24 e 192.168.6.0/30. Questo vuol dire che su quelle interfacce verranno instradati i pacchetti EIGRP. Qualsiasi apparato che sia in una di quelle due reti sul quale sia attivo un processo EIGRP 1 saprà che il router in questione è connesso a 192.168.5.0/24 e 192.168.6.0/30 e gli comunicherà quali reti sono incluse nel proprio processo di routing.

Se il router in questione, però, fosse connesso anche ad altre reti, ad esempio 192.168.0.0/24, con questa configurazione, l'informazione non verrebbe inoltrata e su quella rete l'apparato non invierebbe ne ascolterebbe pacchetti EIGRP.

Il vantaggio di tale algoritmo è sicuramente la sua facilità di configurazione, un suo aspetto negativo, invece, è dovuto al fatto che è proprietario Cisco e quindi compatibile solo con apparati di tale fornitore.

Vediamo ora un estratto del comando **show ip route eigrp** che mostra la tabella di routing del router limitando la vista alle sole reti pervenute tramite eigrp:

```
gateway_1841#show ip route eigrp
D    192.168.5.0/24 [90/2195456] via 192.168.6.1, 2d01h, Serial0/0/0.60
```

Come si può vedere la rete 192.168.5.0/24 non è connessa direttamente al router ma la si raggiunge tramite 192.168.6.1 collegato all'interfaccia Serial0/0/0.60. La *D* prima dell'IP indica che tale rotta proviene da EIGRP.

Le reti direttamente connesse al router non appaiono nell'output di tale comando. Per completezza si considerino i seguenti output:

```
gateway_1841#show ip route static
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       10.186.47.1/32 [254/0] via 10.186.47.254, FastEthernet0/0
S*   0.0.0.0/0 [254/0] via 10.186.47.254

gateway_1841#show ip route connected
C    192.168.4.0/24 is directly connected, FastEthernet0/1.40
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.186.47.128/25 is directly connected, FastEthernet0/0
     192.168.6.0/30 is subnetted, 1 subnets
C       192.168.6.0 is directly connected, Serial0/0/0.60
     192.168.0.0/32 is subnetted, 3 subnets
C       192.168.0.1 is directly connected, Loopback0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/1.10
C       192.168.1.3/32 is directly connected, Virtual-Access1

gateway_1841#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.6.1             Se0/0/0.60        11 4d21h     228  1368  0  10
```

4.1.2 OSPF

La configurazione di OSPF è più complicata di EIGRP. Di fatto l'algoritmo prevede la definizione di più aree a partire dalla principale, area 0, che costituisce la dorsale. Si possono usare aree diverse per separare logicamente le reti. Per unire le varie aree si usano le modalità di redistribuzione che vedremo in seguito.
Analizziamo la configurazione:

```
router ospf 1
 log-adjacency-changes
 network 192.168.0.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
!
```

La definizione della rete è simile a quella per EIGRP a differenza del campo relativo all'area. Per una configurazione semplificata si sceglie, solitamente, di porre tutte le reti in area 0. Come prima non viene mostrata la maschera di rete ma il suo inverso. Da notare la prima rete: quel campo corrisponde all'ip assegnato sull'interfaccia di Loopback. Non facendo parte di una vera rete, è necessario inserire, in ciascun router, una entry nella forma IP/32. Il risultato è il seguente:

```
gateway_1841#show ip route ospf
O    192.168.8.0/24 [110/2] via 192.168.1.1, 00:04:13, FastEthernet0/1.10
     192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
O       192.168.9.0/30 [110/2] via 192.168.1.1, 00:04:13, FastEthernet0/1.10
O E2    192.168.9.128/25
           [110/20] via 192.168.1.1, 00:04:13, FastEthernet0/1.10
O    192.168.7.0/24 [110/11] via 192.168.4.1, 00:04:13, FastEthernet0/1.40
     192.168.0.0/32 is subnetted, 4 subnets
O       192.168.0.2 [110/2] via 192.168.1.1, 00:04:13, FastEthernet0/1.10
O       192.168.0.3 [110/2] via 192.168.4.1, 00:04:13, FastEthernet0/1.40
O       192.168.0.4 [110/3] via 192.168.1.1, 00:04:13, FastEthernet0/1.10
O    192.168.2.0/24 [110/2] via 192.168.1.1, 00:04:13, FastEthernet0/1.10
O    192.168.3.0/24 [110/12] via 192.168.1.1, 00:04:13, FastEthernet0/1.10
```

Come si può vedere tutte le reti sono indicate in modo analogo a quanto già visto per EIGRP. La lettera O, in questo caso, indica che tali rotte sono pervenute tramite algoritmo OSPF. Tuttti gli IP della rete 192.168.0.0 vengono inseriti sparatamente perché hanno la maschera 255.255.255.255.
Come per EIGRP, anche per OSPF è possibile identificare i vicini attraverso il seguente comando:

```
gateway_1841#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.8.1       1   FULL/BDR        00:00:35    192.168.4.1     FastEthernet0/1.40
192.168.9.2       1   FULL/BDR        00:00:37    192.168.1.1     FastEthernet0/1.10
```

E', infine, possibile introdurre una procedura di autenticazione per evitare che malintenzionati possano iniettare rotte errate per scopi poco leciti. In questo contesto, tali procedure non sono state trattate.

Per completezza si consideri ora la tabella di routing completa per il gateway della rete che, gestendo entrambi gli algoitmi di routing appena visti, avrà tutte le rotte al completo.

```
gateway_1800#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 10.186.47.254 to network 0.0.0.0

O    192.168.8.0/24 [110/2] via 192.168.1.1, 2d01h, FastEthernet0/1.10
     192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
O       192.168.9.0/30 [110/2] via 192.168.1.1, 2d01h, FastEthernet0/1.10
O E2    192.168.9.128/25 [110/20] via 192.168.1.1, 2d01h, FastEthernet0/1.10
C    192.168.4.0/24 is directly connected, FastEthernet0/1.40
D    192.168.5.0/24 [90/2195456] via 192.168.6.1, 2d01h, Serial0/0/0.60
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.186.47.128/25 is directly connected, FastEthernet0/0
S       10.186.47.1/32 [254/0] via 10.186.47.254, FastEthernet0/0
     192.168.6.0/30 is subnetted, 1 subnets
C       192.168.6.0 is directly connected, Serial0/0/0.60
O    192.168.7.0/24 [110/11] via 192.168.4.1, 2d01h, FastEthernet0/1.40
     192.168.0.0/32 is subnetted, 4 subnets
C       192.168.0.1 is directly connected, Loopback0
O       192.168.0.2 [110/2] via 192.168.1.1, 2d01h, FastEthernet0/1.10
O       192.168.0.3 [110/2] via 192.168.4.1, 2d01h, FastEthernet0/1.40
O       192.168.0.4 [110/3] via 192.168.1.1, 2d01h, FastEthernet0/1.10
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/1.10
C       192.168.1.3/32 is directly connected, Virtual-Access1
O    192.168.2.0/24 [110/2] via 192.168.1.1, 2d01h, FastEthernet0/1.10
O    192.168.3.0/24 [110/12] via 192.168.1.1, 2d01h, FastEthernet0/1.10
S*   0.0.0.0/0 [254/0] via 10.186.47.254
```

4.1.3 Adattamento automatico

Come si è detto in precedenza, avere un algoritmo di routing su una rete con percorsi multipli, e quindi con ridondanza, è utile quando uno o più linee dovessero saltare. L'algoritmo, in questo caso, va a ricalcolare i percorsi e agisce modificando le tabelle di routing.

Vediamo un esempio: consideriamo il link che unisce i router c3825 con il c3640 appartenente alla vlan 80 e spegnamo l'interfaccia corrispondete sul primo router. Si può osservare dall'output sottostante che il percorso per raggiungere il secondo (utilizzando come riferimento l'indirizzo di loopback) viene automaticamente cambiato dopo pochi istanti:

```
c3825#show ip route 192.168.0.3
Routing entry for 192.168.0.3/32
  Known via "ospf 1", distance 110, metric 2, type intra area
```

```
  Last update from 192.168.8.1 on GigabitEthernet0/0.80, 00:16:49 ago
  Routing Descriptor Blocks:
  * 192.168.8.1, from 192.168.8.1, 00:16:49 ago, via GigabitEthernet0/0.80
      Route metric is 2, traffic share count is 1
c3825#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
c3825(config)#interface GigabitEthernet 0/0.80
c3825(config-subif)#shutdown
c3825(config-subif)#exit
c3825(config)#end
c3825#show ip route 192.168.0.3
Routing entry for 192.168.0.3/32
  Known via "ospf 1", distance 110, metric 3, type intra area
  Last update from 192.168.1.254 on GigabitEthernet0/0.10, 00:00:01 ago
  Routing Descriptor Blocks:
  * 192.168.1.254, from 192.168.8.1, 00:00:01 ago, via GigabitEthernet0/0.10
      Route metric is 3, traffic share count is 1
c3825#ping 192.168.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

Si noti che l'id di ogni router nel processo di routing (OSPF in questo caso) viene calcolato dall'indirizzo IP più alto sulle proprie interfacce. Questo giustifica il fatto che il router c3640 continua ad essere visto con indirizzo IP 192.168.8.1. Nonostante l'altro capo sia in shutdown il link su quest'ultimo resta up perché è associato a un'interfaccia in trunk e rimane, quindi, sempre connessa allo switch.

Osserviamo, ora, la stessa cosa riattivando l'interfaccia spenta in precedenza disattivando, però, quella corrispondente al collegamento tra il c3825 e il c1841. Di seguito vengono mostrate le tabelle di routing prima e dopo:

```
gateway_1800#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 10.186.47.254 to network 0.0.0.0
```

```
O    192.168.8.0/24 [110/2] via 192.168.1.1, 2d01h, FastEthernet0/1.10
     192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
O       192.168.9.0/30 [110/2] via 192.168.1.1, 2d01h, FastEthernet0/1.10
O E2    192.168.9.128/25 [110/20] via 192.168.1.1, 2d01h, FastEthernet0/1.10
C    192.168.4.0/24 is directly connected, FastEthernet0/1.40
D    192.168.5.0/24 [90/2195456] via 192.168.6.1, 2d01h, Serial0/0/0.60
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.186.47.128/25 is directly connected, FastEthernet0/0
S       10.186.47.1/32 [254/0] via 10.186.47.254, FastEthernet0/0
     192.168.6.0/30 is subnetted, 1 subnets
C       192.168.6.0 is directly connected, Serial0/0/0.60
O    192.168.7.0/24 [110/11] via 192.168.4.1, 2d01h, FastEthernet0/1.40
     192.168.0.0/32 is subnetted, 4 subnets
C       192.168.0.1 is directly connected, Loopback0
O       192.168.0.2 [110/2] via 192.168.1.1, 2d01h, FastEthernet0/1.10
O       192.168.0.3 [110/2] via 192.168.4.1, 2d01h, FastEthernet0/1.40
O       192.168.0.4 [110/3] via 192.168.1.1, 2d01h, FastEthernet0/1.10
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/1.10
C       192.168.1.3/32 is directly connected, Virtual-Access1
O    192.168.2.0/24 [110/2] via 192.168.1.1, 2d01h, FastEthernet0/1.10
O    192.168.3.0/24 [110/12] via 192.168.1.1, 2d01h, FastEthernet0/1.10
S*   0.0.0.0/0 [254/0] via 10.186.47.254


gateway_1800#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 10.186.47.254 to network 0.0.0.0

O    192.168.8.0/24 [110/11] via 192.168.4.1, 00:00:18, FastEthernet0/1.40
     192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
O       192.168.9.0/30 [110/12] via 192.168.4.1, 00:00:18, FastEthernet0/1.40
O E2    192.168.9.128/25
           [110/20] via 192.168.4.1, 00:00:18, FastEthernet0/1.40
C    192.168.4.0/24 is directly connected, FastEthernet0/1.40
D    192.168.5.0/24 [90/2195456] via 192.168.6.1, 2d01h, Serial0/0/0.60
```

```
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.186.47.128/25 is directly connected, FastEthernet0/0
S       10.186.47.1/32 [254/0] via 10.186.47.254, FastEthernet0/0
     192.168.6.0/30 is subnetted, 1 subnets
C       192.168.6.0 is directly connected, Serial0/0/0.60
O    192.168.7.0/24 [110/11] via 192.168.4.1, 00:00:18, FastEthernet0/1.40
     192.168.0.0/32 is subnetted, 4 subnets
C       192.168.0.1 is directly connected, Loopback0
O       192.168.0.2 [110/12] via 192.168.4.1, 00:00:19, FastEthernet0/1.40
O       192.168.0.3 [110/2] via 192.168.4.1, 00:00:19, FastEthernet0/1.40
O       192.168.0.4 [110/12] via 192.168.4.1, 00:00:19, FastEthernet0/1.40
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/1.10
C       192.168.1.3/32 is directly connected, Virtual-Access1
O    192.168.2.0/24 [110/12] via 192.168.4.1, 00:00:19, FastEthernet0/1.40
O    192.168.3.0/24 [110/21] via 192.168.4.1, 00:00:19, FastEthernet0/1.40
S*   0.0.0.0/0 [254/0] via 10.186.47.254
```

Si può osservare la variazione che si ottiene nel raggiungere le reti 192.168.8.0/24, 192.168.9.0/30, 192.168.9.128/128, 192.168.2.0/24, 192.168.3.0/24 e l'IP 192.168.0.2 che passano dal gateway 192.168.1.1 (connesso a FastEthernet0/1.10) al 192.168.4.1 (connesso a FastEthernet0/1.40).

4.1.4 Redistribuzione

Nel caso si abbiano più algoritmi di routing all'interno della stessa rete e si vogliano scambiare le informazioni tra i due è necessario impostare un meccanismo di redistribuzione delle rotte. Per farlo è necessario configurare entrambi gli algoritmi utilizzando la chiave **redistribute** nel seguente modo:

```
router eigrp 1
 redistribute ospf 1 metric 1000 100 250 1 1500
 network 192.168.6.0 0.0.0.3
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 redistribute eigrp 1 subnets
 network 192.168.0.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
!
```

Nel primo caso è indicato al processo eigrp 1 di instradare le rotte di ospf utilizzando una metrica specifica:

- Bandwidth metric in Kbits per second: 1000
- EIGRP delay metric, in 10 microsecond units: 100
- EIGRP reliability metric: 250
- EIGRP Effective bandwidth metric: 1
- EIGRP MTU of the path: 1500

Nel secondo è stato semplicemente dichiarato che il protocollo ospf 1 deve redistribuire le rotte provenienti da eigrp 1. La chiave **subnets** indica al processo di ignorare le subnet di default associate agli indirizzi virtuali e inoltrarle. Senza questo si sarebbero generate incongruenze per reti non particolari (vedi 192.168.6.0/30 che sarebbe stata distribuita come 192.168.6.0/24).

Infine, se si volesse redistribuire rotte statiche è necessario includere nei parametri dell'algoritmo di routing il seguente comando: **redistribute static subnets**.

4.2 BGP

Il Border Gateway Protocol è un protocollo di routing che agisce nel 'cuore' di Internet. Il BGP funziona attraverso la gestione di una tabella di reti IP, o prefissi, che forniscono informazioni sulla raggiungibilità delle diverse reti tra più sistemi autonomi (Autonomous System, AS). Si tratta di un protocollo di routing a indicazione di percorso (path vector), che non usa metriche di carattere tecnico ma prende le decisioni di instradamento basandosi su politiche (regole) determinate da ciascuna rete.

Nel protocollo BGP le coppie di sistemi adiacenti, detti peer, vengono stabilite mediante configurazione manuale dei router stabilendo una sessione TCP sulla porta 179. L'iniziatore della sessione BGP (speaker) invia periodicamente (per default ogni 60 secondi) dei messaggi keepalive da 19 byte per mantenere attiva la connessione. Tra i protocolli di routing, il BGP è l'unico a utilizzare il TCP come protocollo di trasporto.

Passiamo alla configurazione degli apparati. BGP sfrutta gli algoritmi di routing già presenti nella rete e necessita di indicare manualmente quali sono gli altri peer. Analizziamo la configurazione sottostante:

```
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.0.1 remote-as 100
 neighbor 192.168.0.1 update-source Loopback0
 neighbor 192.168.0.2 remote-as 100
 neighbor 192.168.0.2 update-source Loopback0
 neighbor 192.168.0.4 remote-as 100
 neighbor 192.168.0.4 update-source Loopback0
```

```
 no auto-summary
 !
```

Si noti l'utilizzo delle interfacce di Loopback: tale scelta è dovuta al fatto che l'indirizzo di loopback rimate attivo anche se il canale fisico venisse a mancare. In una rete opportunamente ridondata, questa configurazione garantirebbe un funzionamento corretto anche in caso di guasti ad alcune linee (purchè resti possibile un collegamento fisico tra i router).

Tale configurazione indica solamente quali sono i peers. Per quanto riguarda le reti si discuterà nel capitolo successivo come utilizzare tale algoritmo, in collaborazione con MPLS, per realizzare VPN.
Come per gli altri algoritmi anche in questo caso è possibile esplorare i vicini:

```
c3640#show ip bgp summary
BGP router identifier 192.168.0.3, local AS number 100
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.0.1     4   100    3100    3105        1    0    0 2d03h           0
192.168.0.2     4   100    3108    3113        1    0    0 2d02h           0
192.168.0.4     4   100    3099    3112        1    0    0 2d02h           0


c3640#show ip bgp neighbors
BGP neighbor is 192.168.0.1,  remote AS 100, internal link
  BGP version 4, remote router ID 192.168.0.1
  BGP state = Established, up for 2d03h
  Last read 00:00:03, last write 00:00:44, hold time is 180, keepalive interval is 60
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                5          0
    Keepalives:          3094       3095
    Route Refresh:          0          0
    Total:               3100       3096
  Default minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
```

```
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              0          0
    Prefixes Total:                0          0
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0

                                 Outbound    Inbound
  Local Policy Denied Prefixes:  --------    -------
    Total:                              0          0
  Number of NLRIs in the update sent: max 0, min 0

 For address family: VPNv4 Unicast
  BGP table version 14, neighbor version 14/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
  Community attribute sent to this neighbor
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              2          0
    Prefixes Total:                5          0
    Implicit Withdraw:             3          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0

                                 Outbound    Inbound
  Local Policy Denied Prefixes:  --------    -------
    Bestpath from this peer:            1        n/a
    Bestpath from iBGP peer:            5        n/a
    Total:                              6          0
  Number of NLRIs in the update sent: max 1, min 1

  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

```
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 192.168.0.3, Local port: 179
Foreign host: 192.168.0.1, Foreign port: 23527

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xB12B4F0):
Timer          Starts    Wakeups            Next
Retrans          3102          6             0x0
TimeWait            0          0             0x0
AckHold          3094       2957             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:  193793205  snduna:  193852567  sndnxt:  193852567     sndwnd:  15966
irs: 1110478775  rcvnxt: 1110537634  rcvwnd:      15928  delrcvwnd:    456

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 536 bytes):
Rcvd: 6085 (out of order: 0), with data: 3095, total data bytes: 58858
Sent: 6160 (retransmit: 6, fastretransmit: 0, partialack: 0, Second Congestion: 0), w

BGP neighbor is 192.168.0.2,  remote AS 100, internal link
  BGP version 4, remote router ID 192.168.0.2
  BGP state = Established, up for 2d02h
  Last read 00:00:09, last write 00:00:11, hold time is 180, keepalive interval is 60
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          1
```

```
    Updates:                9          4
    Keepalives:          3097       3096
    Route Refresh:          0          0
    Total:               3109       3104
  Default minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             0          0
    Prefixes Total:               0          0
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          0
    Used as multipath:          n/a          0

                                 Outbound    Inbound
  Local Policy Denied Prefixes:  --------    -------
    Total:                              0          0
  Number of NLRIs in the update sent: max 0, min 0

 For address family: VPNv4 Unicast
  BGP table version 14, neighbor version 14/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
  Community attribute sent to this neighbor
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             2          1 (Consumes 68 bytes)
    Prefixes Total:               2          2
    Implicit Withdraw:            2          1
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          1
    Used as multipath:          n/a          0

                                 Outbound    Inbound
  Local Policy Denied Prefixes:  --------    -------
    Suppressed duplicate:               0          1
```

```
    Bestpath from iBGP peer:              2        n/a
    Total:                                2          1
  Number of NLRIs in the update sent: max 1, min 1

  Connections established 3; dropped 2
  Last reset 2d02h, due to Peer closed the session
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 192.168.0.3, Local port: 42179
Foreign host: 192.168.0.2, Foreign port: 179

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xB12BD14):
Timer          Starts    Wakeups            Next
Retrans          3010          0             0x0
TimeWait            0          0             0x0
AckHold          3010       2905             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3954273480  snduna: 3954330952  sndnxt: 3954330952     sndwnd:  16213
irs: 3665905680  rcvnxt: 3665963152  rcvwnd:      16213  delrcvwnd:    171

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: active open, nagle
IP Precedence value : 6

Datagrams (max data segment is 536 bytes):
Rcvd: 5744 (out of order: 0), with data: 3013, total data bytes: 57471
Sent: 6022 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), w

BGP neighbor is 192.168.0.4,  remote AS 100, internal link
  BGP version 4, remote router ID 192.168.0.4
  BGP state = Established, up for 2d02h
  Last read 00:00:05, last write 00:00:09, hold time is 180, keepalive interval is 60
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
```

```
   Address family VPNv4 Unicast: advertised and received
 Message statistics:
   InQ depth is 0
   OutQ depth is 0
                        Sent       Rcvd
   Opens:                  3          3
   Notifications:          1          0
   Updates:                9          0
   Keepalives:          3095       3092
   Route Refresh:          0          0
   Total:               3108       3095
 Default minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast
 BGP table version 1, neighbor version 1/0
Output queue size : 0
 Index 1, Offset 0, Mask 0x2
 1 update-group member
                               Sent       Rcvd
 Prefix activity:              ----       ----
   Prefixes Current:              0          0
   Prefixes Total:                0          0
   Implicit Withdraw:             0          0
   Explicit Withdraw:             0          0
   Used as bestpath:            n/a          0
   Used as multipath:           n/a          0

                                 Outbound    Inbound
 Local Policy Denied Prefixes:   --------    -------
   Total:                               0          0
 Number of NLRIs in the update sent: max 0, min 0

For address family: VPNv4 Unicast
 BGP table version 14, neighbor version 14/0
Output queue size : 0
 Index 1, Offset 0, Mask 0x2
 1 update-group member
 Community attribute sent to this neighbor
                               Sent       Rcvd
 Prefix activity:              ----       ----
   Prefixes Current:              2          0
   Prefixes Total:                2          0
   Implicit Withdraw:             2          0
```

```
    Explicit Withdraw:              0          0
    Used as bestpath:             n/a          0
    Used as multipath:            n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Bestpath from iBGP peer:             2        n/a
    Total:                               2          0
  Number of NLRIs in the update sent: max 1, min 1

  Connections established 3; dropped 2
  Last reset 2d02h, due to Peer closed the session
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 192.168.0.3, Local port: 179
Foreign host: 192.168.0.4, Foreign port: 51534

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xB12C200):
Timer          Starts    Wakeups            Next
Retrans          3010          0             0x0
TimeWait            0          0             0x0
AckHold          3010       2589             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 1720272292  snduna: 1720329764  sndnxt: 1720329764     sndwnd:  16213
irs: 2475484487  rcvnxt: 2475541731  rcvwnd:      15890  delrcvwnd:    494

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 4 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 536 bytes):
Rcvd: 5754 (out of order: 0), with data: 3010, total data bytes: 57243
Sent: 5703 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), w
```

Capitolo 5

MultiProtocol BGP con MPLS

Una metodologia per realizzare VPN di livello 3 è quella di utilizzare MPLS con BGP. Tale tecnica prende il nome di **MP-BGP** (Multi-Protocol BGP).

Il funzionamento è molto semplice: si collegano i **Client Edge** con i **Provider Edge** tramite un link su cui transita IP (IP over ATM, Ethernet, Frame Relay) per ogni PE si creano delle istanze di routing virtuale (vrf), una per VPN, e si incapsula il traffico proveniente dal CE in frame MPLS aggiungendo un label specifico. Infine, per permettere ai pacchetti di attraversare la dorsale MPLS fino a raggiungere l'altro segmento della rete è necessario utilizzare un protocollo di routing. L'ideale è BGP perché non impone link diretti tra i membri e ciò permette di separare il routing di dorsale da quello dei clienti.

Grazie alla definizione di un vrf per VPN è possibile la sovrapposizione degli indirizzi IP. Ciascun pacchetto viene, infatti, etichettato con un label identificato da due campi detti **Route-Distinguisher** (RD).

5.1 Configurazione CE

La configurazione lato cliente non richiede particolari accorgimenti. La Dorsale è del tutto trasparente all'utente. Il PE è visto come il gateway verso le altre reti e si può quindi utilizzare un protocollo di routing per indirizzare le reti appartenenti alla VPN. I pacchetti di tale protocollo verranno instradate al PE (che dovrà essere configurato per utilizzare il medesimo protocollo di routing sulla vrf corrispondente alla VPN in questione) che si occuperà di instradare tale algoritmo nel BGP.
Per completezza viene riportata la configurazione del router Cisco 877:

```
interface FastEthernet0
 switchport access vlan 300
!
interface FastEthernet1
 switchport access vlan 300
!
interface FastEthernet2
```

```
 switchport access vlan 300
!
interface FastEthernet3
 switchport access vlan 300
!
interface Vlan300
 ip address 10.0.0.1 255.255.255.0
!
router ospf 300
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 1
!
ip default-gateway 10.0.0.254
ip route 0.0.0.0 0.0.0.0 10.0.0.254
```

Come si può notare, la configurazione è semplice e non richiede particolari conoscenza. Serve solo concordare con il provider il protocollo di routing e il suo id e gli indirizzi dei PE.

5.2 Configurazione PE

Lato PE la configurazione è alquando complessa. I passi da eseguire sono i seguenti:

- configurare il vrf per ogni VPN ad esso collegata
- configurare l'interfaccia di rete a cui è connesso ciascun CE indicando a quale vrf è associato e l'indirizzo ip di tale interfaccia.
- configurare opportunamente il routing per ogni VPN.

5.2.1 Virtual Routing and Forwarding

Definire un VRF è semplice:

```
ip vrf Cliente3
 rd 100:300
 vpn id 100:300
 route-target export 100:3000
 route-target import 100:3000
!
```

I comandi sono molto semplici e intuitivi: rd 100:300 è il label che il router dovrà porre ai pacchetti provenienti dal CE e che gli consentirà anche di identificare a quale interfaccia instradarli. *route-target* import ed *export* consentono di definire le policies per l'utilizzo

di vrf. Le policies vengono usate per popolare le tabelle di routing all'interno del vrf escludendo dalla lista le reti all'esterno del vrf, e quindi della VPN.

Tale configurazione dovrà essere identica su tutti i router di frontiera a cui sono connessi direttamente i segmenti della stessa VPN. Un router di frontiera, come nel caso del c3845, possono avere più istanze di routing virtuale associate a più VPN. Eccone un esempio:

```
c3640#show ip vrf brief
  Name                             Default RD          Interfaces
  Cliente1                         100:100             Et0/0.100
  Cliente3                         100:300             Et0/0.300


c3640#show ip vrf id
VPN Id          Name                             RD
100:100         Cliente1                         100:100
100:300         Cliente3                         100:300
```

5.2.2 Configurazione Interfacce di rete

Fatto questo è necessario configurare le interfacce di rete che sono collegate al CE in modo da assegnarle ad una specifica istanza di routing virtuale. L'esempio sottostante deve servire da riferimento:

```
interface GigabitEthernet0/1
 ip vrf forwarding Cliente3
 ip address 10.0.1.254 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
```

Come si può osservare la configurazione è analoga a quelle viste in precedenza ad eccezione fatta per *ip vrf forwarding Cliente3*. L'inserimento di questo campo provoca la cancellazione dell'indirizzo IP e ciò obbliga l'amministratore a doverne reinserire l'indirizzo.

A questo punto è necessario configurare i router della dorsale perché instradino correttamente i pacchetti MPLS, e quindi effettuino un tag-switching su IP. Per fare ciò è necessario inserire l'istruzione **tag-switching ip** e il risultato che si ottiene è il seguente:

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.0
 mpls ip
!
```

Se alcuni router della dorsale non disponessero di un firmware con questa funzionalità (per i cisco è necessario un firmware enterprise o advanced enterprise) bisognerà configurare la rete in maniera opportuna per avere almeno un percorso MPLS che colleghi i router di frontiera tra loro.
Ecco alcuni comandi utile per capire su quali interfacce è attivo il tag-switching e quali interfacce sono collegate ai vari VRF:

```
c3640#show tag-switching interfaces
Interface              IP            Tunnel   Operational
Ethernet0/0.40         Yes (ldp)     No       Yes
Ethernet0/0.70         Yes (ldp)     No       Yes
Ethernet0/0.80         Yes (ldp)     No       Yes

c3640#show ip vrf interfaces
Interface              IP-Address      VRF                               Protocol
Et0/0.100              10.0.0.254      Cliente1                          up
Et0/0.300              10.0.0.254      Cliente3                          up
```

5.2.3 Routing per VPN - BGP

A questo punto è necessario configurare il routing. Occorre configurare BGP per far comunicare tra loro i PE e poi un algoritmo di routing a scelta all'interno della VPN.

```
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.0.1 remote-as 100
 neighbor 192.168.0.1 update-source Loopback0
 neighbor 192.168.0.3 remote-as 100
 neighbor 192.168.0.3 update-source Loopback0
 neighbor 192.168.0.4 remote-as 100
 neighbor 192.168.0.4 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 192.168.0.1 activate
  neighbor 192.168.0.1 send-community both
  neighbor 192.168.0.3 activate
  neighbor 192.168.0.3 send-community both
  neighbor 192.168.0.4 activate
  neighbor 192.168.0.4 send-community both
 exit-address-family
 !
 address-family ipv4 vrf Cliente1
```

```
  redistribute connected
  no synchronization
 exit-address-family
!
 address-family ipv4 vrf Cliente3
  redistribute connected
  no synchronization
 exit-address-family
!
```

La prima parte delle istruzioni si occupa di definire il funzionamento di BGP e in particolare i vicini. La seconda parte (*address-family vpnv4*) si occupa di definire gli aspetti legati alle vpn ed in particolare quali router impegnati nel istanza 100 del protocollo BGP gestiscono l'accesso a segmenti di VPN. gli ultimi due campi (*address-family ipv4 vrf Cliente1* e *address-family ipv4 vrf Cliente3*) si occupano di gestire direttamente parametri del protocollo legati alle singole VPN.

Con questa configurazione ora gli end-point della rete sono in grado di comunicare e quindi inviarsi pacchetti. La VPN così ottenuta non utilizza ancora algoritmi di routing. Vediamo alcuni comandi di esempio:

```
c3825#show ip cef vrf Cliente3 10.0.1.1
10.0.1.1/32, version 13, epoch 0, connected, cached adjacency 10.0.1.1
0 packets, 0 bytes
  via 10.0.1.1, GigabitEthernet0/1, 0 dependencies
    next hop 10.0.1.1, GigabitEthernet0/1
    valid cached adjacency


c3825#show ip cef vrf Cliente3 10.0.0.1
10.0.0.0/24, version 14, epoch 0, cached adjacency 192.168.8.1
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Gi0/0.80, 192.168.8.1, tags imposed: {27}
  via 192.168.0.3, 0 dependencies, recursive
    next hop 192.168.8.1, GigabitEthernet0/0.80 via 192.168.0.3/32
    valid cached adjacency
    tag rewrite with Gi0/0.80, 192.168.8.1, tags imposed: {27}


c3640#show ip cef vrf Cliente3 10.0.0.1
10.0.0.1/32, version 12, epoch 0, connected, cached adjacency 10.0.0.1
0 packets, 0 bytes
  via 10.0.0.1, Ethernet0/0.300, 0 dependencies
```

```
    next hop 10.0.0.1, Ethernet0/0.300
    valid cached adjacency


c3640#show ip cef vrf Cliente3 10.0.1.1
10.0.1.0/24, version 15, epoch 0, cached adjacency 192.168.8.254
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Et0/0.80, 192.168.8.254, tags imposed: {25}
  via 192.168.0.2, 0 dependencies, recursive
    next hop 192.168.8.254, Ethernet0/0.80 via 192.168.0.2/32
    valid cached adjacency
    tag rewrite with Et0/0.80, 192.168.8.254, tags imposed: {25}


c3640#traceroute vrf Cliente3 10.0.1.1

Type escape sequence to abort.
Tracing the route to 10.0.1.1

  1 10.0.1.254 4 msec 0 msec 4 msec
  2 10.0.1.1 4 msec *  4 msec

c3825#traceroute vrf Cliente3 10.0.0.1

Type escape sequence to abort.
Tracing the route to 10.0.0.1

  1 10.0.0.254 [MPLS: Label 27 Exp 0] 4 msec 0 msec 4 msec
  2 10.0.0.1 4 msec *  0 msec

c3825#ping vrf Cliente3 10.0.0.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

c3825#ping vrf Cliente3 10.0.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.254, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

c3825#ping vrf Cliente3 10.0.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

c3825#ping vrf Cliente3 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Vediamo alcuni comandi utili a studiare il funzionamento della VPN:

```
c3640#show ip bgp vpnv4 all
BGP table version is 14, local router ID is 192.168.0.3
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: 100:100 (default for vrf Cliente1)
*> 10.0.0.0/24      0.0.0.0                  0         32768 ?
Route Distinguisher: 100:300 (default for vrf Cliente3)
*> 10.0.0.0/24      0.0.0.0                  0         32768 ?
*>i10.0.1.0/24      192.168.0.2              0    100      0 ?


c3640#show tag-switching tdp neighbor
    Peer LDP Ident: 192.168.0.1:0; Local LDP Ident 192.168.0.3:0
TCP connection: 192.168.0.1.646 - 192.168.0.3.22592
State: Oper; Msgs sent/rcvd: 3523/3541; Downstream
Up time: 2d03h
LDP discovery sources:
  Ethernet0/0.40, Src IP addr: 192.168.4.254
        Addresses bound to peer LDP Ident:
          10.186.47.134   192.168.0.1     192.168.4.254   192.168.1.254
          192.168.6.2
    Peer LDP Ident: 192.168.0.2:0; Local LDP Ident 192.168.0.3:0
```

```
TCP connection: 192.168.0.2.646 - 192.168.0.3.29433
State: Oper; Msgs sent/rcvd: 3454/3447; Downstream
Up time: 2d02h
LDP discovery sources:
  Ethernet0/0.80, Src IP addr: 192.168.8.254
        Addresses bound to peer LDP Ident:
          192.168.0.2     192.168.9.2     192.168.2.254   192.168.8.254
          192.168.1.1


c3640#show tag-switching tdp discovery
 Local TDP Identifier:
    192.168.0.3:0
    Discovery Sources:
    Interfaces:
Ethernet0/0.40 (ldp): xmit/recv
    LDP Id: 192.168.0.1:0
Ethernet0/0.70 (ldp): xmit
Ethernet0/0.80 (ldp): xmit/recv
    LDP Id: 192.168.0.2:0


c3640#show tag-switching tdp parameters
Protocol version: 1
Downstream tag generic region: min tag: 16; max tag: 100000
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery directed hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 255
Downstream on Demand Path Vector Limit: 255
LDP for directed sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: off
```

TDP è il Tag Distribution Protocol, mentre **LDP** è il Label Distribution Protocol che si occupano di gestire la distribuzione dei label nella rete MPLS.

5.2.4 Redistribuzione Routing VPN

Resta da configurare la redistribuzione degli algoritmi di routing delle singole VPN attraverso la rete dorsale senza generare interferenze. Per prima cosa bisogna definire sul PE l'algoritmo di routing utilizzato per la VPN vincolandolo al VRF ad essa associata:

```
router ospf 300 vrf Cliente3
```

```
 log-adjacency-changes
 redistribute bgp 100 metric 20 subnets
 network 10.0.1.0 0.0.0.255 area 1
!
```

Con questa sintassi si avvia un istanza di OSPF sulla VRF di Cliente3 da distribuire sulla rete 10.0.1.0/24 appartenente all'area 1. Su tale algoritmo si andranno a distribuire anche i dati che proverranno da bgp 100.

Fatto ciò bisogna configurare in BGP la ridistribuzione dell'algoritmo di routing scelto per la VPN:

```
 address-family ipv4 vrf Cliente3
  redistribute connected
  redistribute ospf 300 vrf Cliente3
  no synchronization
 exit-address-family
!
```

L'istruzione *redistribuite connected* impone al router di instradare le informazioni sulle reti ad esso direttamente connesse. In questo contesto le reti sono vincolate al VRF considerato (Cliente3). Queste operazioni vanno fatte per ogni coppia PE-CE di ciascuna VPN. Osseriviamo ora le tabelle di routing di entrambi i PE:

```
c3640#show ip route vrf Cliente3

Routing Table: Cliente3
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

     10.0.0.0/24 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, Ethernet0/0.300
B       10.0.1.0 [200/0] via 192.168.0.2, 2d02h



c3825#show ip route vrf Cliente3
```

```
Routing Table: Cliente3
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

     10.0.0.0/24 is subnetted, 2 subnets
B       10.0.0.0 [200/0] via 192.168.0.3, 2d02h
C       10.0.1.0 is directly connected, GigabitEthernet0/1
```

Come si può notare sono state popolate correttamente.

Riponiamoci nella situazione già vista in precedenza in caso di caduta di un link. Se gli algoritmi IGP interni alla dorsale fanno il loro lavoro, BGP continua a funzionare correttamente e, di conseguenza, la VPN continuerà a funzionare. La conferma ne deriva dall'esempio sottostante:

```
c3825#show ip route 192.168.0.3
Routing entry for 192.168.0.3/32
  Known via "ospf 1", distance 110, metric 2, type intra area
  Last update from 192.168.8.1 on GigabitEthernet0/0.80, 00:16:49 ago
  Routing Descriptor Blocks:
  * 192.168.8.1, from 192.168.8.1, 00:16:49 ago, via GigabitEthernet0/0.80
      Route metric is 2, traffic share count is 1
c3825#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
c3825(config)#interface GigabitEthernet 0/0.80
c3825(config-subif)#shutdown
c3825(config-subif)#exit
c3825(config)#end
c3825#show ip route 192.168.0.3
Routing entry for 192.168.0.3/32
  Known via "ospf 1", distance 110, metric 3, type intra area
  Last update from 192.168.1.254 on GigabitEthernet0/0.10, 00:00:01 ago
  Routing Descriptor Blocks:
  * 192.168.1.254, from 192.168.8.1, 00:00:01 ago, via GigabitEthernet0/0.10
      Route metric is 3, traffic share count is 1

c3825#ping vrf Cliente3 10.0.0.254
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
c3825#ping vrf Cliente3 10.0.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Osservando, invece, le rotte si ottiene:

```
PRIMA

c3640#show ip cef vrf Cliente3 10.0.1.1
10.0.1.0/24, version 15, epoch 0, cached adjacency 192.168.8.254
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Et0/0.80, 192.168.8.254, tags imposed: {25}
  via 192.168.0.2, 0 dependencies, recursive
    next hop 192.168.8.254, Ethernet0/0.80 via 192.168.0.2/32
    valid cached adjacency
    tag rewrite with Et0/0.80, 192.168.8.254, tags imposed: {25}

DOPO

c3640#show ip cef vrf Cliente3 10.0.1.1
10.0.1.0/24, version 15, epoch 0, cached adjacency 192.168.4.254
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Et0/0.40, 192.168.4.254, tags imposed: {22 25}
  via 192.168.0.2, 0 dependencies, recursive
    next hop 192.168.4.254, Ethernet0/0.40 via 192.168.0.2/32
    valid cached adjacency
    tag rewrite with Et0/0.40, 192.168.4.254, tags imposed: {22 25}
```

Capitolo 6

File di Configurazione

Per rendere più completa la trattazione del lavoro svolto, vengono allegati i file di configurazione dei vari router utilizzati.

6.1 Switch

6.1.1 Cisco 2950

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname switch_mpls
!
enable secret 5 $1$i8L2$Fq9Z3LCnYp./xbiIF.dzN1
!
username admin password 7 14141B180F0B
no aaa new-model
system mtu routing 1500
ip subnet-zero
ip routing
ip name-server 130.251.1.4
!
!
!
!
no file verify auto
```

```
!
spanning-tree mode pvst
spanning-tree extend system-id
no spanning-tree vlan 547
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/4
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/5
 switchport access vlan 300
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 300
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/8
```

```
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/10
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/11
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/12
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/13
 switchport access vlan 40
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport access vlan 40
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport access vlan 50
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 50
 switchport mode access
 spanning-tree portfast
```

```
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
!
interface Vlan10
```

```
 ip address 192.168.1.253 255.255.255.0
!
interface Vlan20
 ip address 192.168.2.253 255.255.255.0
!
interface Vlan30
 ip address 192.168.3.253 255.255.255.0
!
interface Vlan40
 ip address 192.168.4.253 255.255.255.0
!
interface Vlan70
 no ip address
!
interface Vlan80
 no ip address
!
ip default-gateway 192.168.1.254
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip http server
!
!
control-plane
!
!
line con 0
line vty 0 4
 password 7 094F471A1A0A
 login local
line vty 5 15
 login
!
end
```

6.2 Dorsale Principale

6.2.1 Cisco 1841

```
!
version 12.3
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
service password-encryption
!
hostname gateway_1841
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$lLSw$dl1fvu7mr4WOv0sb7XPEd/
!
no aaa new-model
!
resource policy
!
clock timezone Rome 2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
ip vrf Cliente1
 rd 100:100
 vpn id 100:100
 route-target export 100:1000
 route-target import 100:1000
!
!
no ip ips deny-action ips-interface
!
!
frame-relay switching
!
!
!
!
!
username admin password 7 094F471A1A0A
username framerelay password 7 030752180500
```

```
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.1.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 no snmp trap link-status
 mpls ip
!
interface FastEthernet0/1.40
 encapsulation dot1Q 40
 ip address 192.168.4.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 no snmp trap link-status
 mpls ip
!
interface FastEthernet0/1.100
 encapsulation dot1Q 100
 ip vrf forwarding Cliente1
 ip address 10.0.3.254 255.255.255.0
```

```
 ip virtual-reassembly
 no snmp trap link-status
 mpls ip
!
interface Serial0/0/0
 bandwidth 2000
 no ip address
 encapsulation frame-relay
 clock rate 2000000
 frame-relay lmi-type cisco
 frame-relay intf-type dce
!
interface Serial0/0/0.60 point-to-point
 ip address 192.168.6.2 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 frame-relay interface-dlci 60
!
interface Serial0/1/0
 bandwidth 2000
 no ip address
 encapsulation frame-relay
 no snmp trap link-status
 clock rate 2000000
 frame-relay lmi-type ansi
 frame-relay intf-type dce
!
interface Serial0/1/0.100 point-to-point
 frame-relay interface-dlci 100 ppp Virtual-Template1
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/1.10
 ip nat inside
 ip virtual-reassembly
 peer default ip address dhcp
 ppp authentication chap pap
 ppp chap hostname gateway
 ppp chap password 7 045802150C2E
 ppp pap sent-username gateway password 7 121A0C041104
!
router eigrp 1
 redistribute ospf 1 metric 1000 100 250 1 1500
 network 192.168.6.0 0.0.0.3
```

```
 no auto-summary
!
router ospf 100 vrf Cliente1
 router-id 10.0.3.254
 log-adjacency-changes
 redistribute bgp 100 metric 20 subnets
 network 10.0.3.0 0.0.0.255 area 1
!
router ospf 1
 log-adjacency-changes
 redistribute eigrp 1 subnets
 network 192.168.0.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.0.2 remote-as 100
 neighbor 192.168.0.2 update-source Loopback0
 neighbor 192.168.0.3 remote-as 100
 neighbor 192.168.0.3 update-source Loopback0
 neighbor 192.168.0.4 remote-as 100
 neighbor 192.168.0.4 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 192.168.0.2 activate
 neighbor 192.168.0.2 send-community both
 neighbor 192.168.0.3 activate
 neighbor 192.168.0.3 send-community both
 neighbor 192.168.0.4 activate
 neighbor 192.168.0.4 send-community both
 exit-address-family
!
 address-family ipv4 vrf Cliente1
  redistribute connected
  redistribute ospf 100 vrf Cliente1
  no synchronization
 exit-address-family
!
!
ip classless
```

```
!
!
ip http server
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/0 overload
!
access-list 1 permit 192.168.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.0.255.255
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
banner login ^]Cisco 1841^]
banner prompt-timeout ^]login timeout^]
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
!
scheduler allocate 20000 1000
ntp clock-period 17179261
ntp server 193.204.114.232
end
```

6.2.2 Cisco 3825

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

```
hostname c3825
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$S5TF$q7LBh/yhZMwHsxhuBAmTF.
!
no aaa new-model
clock timezone Rome 2
network-clock-participate wic 0
dot11 syslog
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.253
ip dhcp excluded-address 192.168.1.254
ip dhcp excluded-address 192.168.2.254
ip dhcp excluded-address 192.168.2.1
ip dhcp excluded-address 192.168.2.253
ip dhcp excluded-address 192.168.1.2
!
ip dhcp pool vlan10
   import all
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.254
   dns-server 130.251.1.4
   domain-name vlan10.org
!
ip dhcp pool vlan20
   import all
   network 192.168.2.0 255.255.255.0
   default-router 192.168.2.254
   dns-server 130.251.1.4
   domain-name vlan20.org
!
!
ip vrf Cliente1
 rd 100:100
 vpn id 100:100
 route-target export 100:1000
 route-target import 100:1000
```

```
!
ip vrf Cliente3
 rd 100:300
 vpn id 100:300
 route-target export 100:3000
 route-target import 100:3000
!
ip name-server 130.251.1.4
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
isdn switch-type basic-net3
voice-card 0
 no dspfarm
!
!
!
!
voice service voip
 redirect ip2ip
 sip
  registrar server
!
!
!
!
!
username admin secret 5 $1$L5SR$FCn09C/8IX2Og5qdirT6C/
username sysadmin password 7 070C285F4D06
archive
 log config
  hidekeys
!
!
!
!
interface Loopback0
 ip address 192.168.0.2 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
```

```
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.0
 mpls ip
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.2.254 255.255.255.0
 mpls ip
!
interface GigabitEthernet0/0.80
 encapsulation dot1Q 80
 ip address 192.168.8.254 255.255.255.0
 mpls ip
!
interface GigabitEthernet0/1
 ip vrf forwarding Cliente3
 ip address 10.0.1.254 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
interface BRI0/0/0
 no ip address
 isdn switch-type basic-net3
 isdn overlap-receiving
 isdn tei-negotiation first-call
 isdn point-to-point-setup
 isdn incoming-voice voice
 isdn send-alerting
 isdn sending-complete
 isdn static-tei 0
 isdn skipsend-idverify
!
interface BRI0/0/1
 no ip address
 isdn switch-type basic-net3
 isdn overlap-receiving T302 5000
 isdn not-end-to-end 64
```

```
 isdn protocol-emulate network
 isdn layer1-emulate network
 isdn incoming-voice voice
 isdn send-alerting
 isdn sending-complete
 isdn static-tei 0
 isdn skipsend-idverify
 line-power
!
interface Integrated-Service-Engine1/0
 ip address 192.168.9.2 255.255.255.252
 service-module ip address 192.168.9.1 255.255.255.252
 service-module ip default-gateway 192.168.9.2
 no keepalive
!
router ospf 300 vrf Cliente3
 log-adjacency-changes
 redistribute bgp 100 metric 20 subnets
 network 10.0.1.0 0.0.0.255 area 1
!
router ospf 1
 log-adjacency-changes
 redistribute static subnets
 network 192.168.0.2 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.8.0 0.0.0.255 area 0
 network 192.168.9.0 0.0.0.3 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.0.1 remote-as 100
 neighbor 192.168.0.1 update-source Loopback0
 neighbor 192.168.0.3 remote-as 100
 neighbor 192.168.0.3 update-source Loopback0
 neighbor 192.168.0.4 remote-as 100
 neighbor 192.168.0.4 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 192.168.0.1 activate
  neighbor 192.168.0.1 send-community both
```

```
  neighbor 192.168.0.3 activate
  neighbor 192.168.0.3 send-community both
  neighbor 192.168.0.4 activate
  neighbor 192.168.0.4 send-community both
 exit-address-family
 !
 address-family ipv4 vrf Cliente3
  redistribute connected
  redistribute ospf 300 vrf Cliente3
  no synchronization
 exit-address-family
!
ip default-gateway 192.168.1.254
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.9.128 255.255.255.128 192.168.9.1
!
!
ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
voice-port 0/0/0
!
voice-port 0/0/1
!
voice-port 0/1/0
!
voice-port 0/1/1
!
!
!
!
!
dial-peer voice 10 voip
 destination-pattern 6000
```

```
 session protocol sipv2
 session target ipv4:10.255.2.13
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco
!
dial-peer voice 20 voip
 destination-pattern .T
 session target ipv4:10.255.1.1
!
!
sip-ua
!
!
!
gatekeeper
 shutdown
!
banner login ^]Cisco 3847 - Border^]
!
line con 0
 password 7 14141B180F0B
 login local
line aux 0
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 5
 password 7 13061E010803
 login local
!
scheduler allocate 20000 1000
ntp clock-period 17180103
ntp server 193.204.114.232
!
end
```

6.2.3 Cisco 3640

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname c3640
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$mhBI$UC2OwWgvexhr1EJ6lrGW21
!
no aaa new-model
memory-size iomem 25
!
!
ip cef
ip name-server 130.251.1.4
!
!
ip vrf Cliente1
 rd 100:100
 vpn id 100:100
 route-target export 100:1000
 route-target import 100:1000
!
ip vrf Cliente3
 rd 100:300
 vpn id 100:300
 route-target export 100:3000
 route-target import 100:3000
!
!
!
!
!
!
username admin password 7 02050D480809
!
!
!
!
!
interface Loopback0
 ip address 192.168.0.3 255.255.255.255
!
```

```
interface Ethernet0/0
 no ip address
 half-duplex
!
interface Ethernet0/0.40
 encapsulation dot1Q 40
 ip address 192.168.4.1 255.255.255.0
 mpls ip
!
interface Ethernet0/0.70
 encapsulation dot1Q 70
 ip address 192.168.7.254 255.255.255.0
 mpls ip
!
interface Ethernet0/0.80
 encapsulation dot1Q 80
 ip address 192.168.8.1 255.255.255.0
 mpls ip
!
interface Ethernet0/0.100
 encapsulation dot1Q 100
 ip vrf forwarding Cliente1
 ip address 10.0.0.254 255.255.255.0
!
interface Ethernet0/0.300
 encapsulation dot1Q 300
 ip vrf forwarding Cliente3
 ip address 10.0.0.254 255.255.255.0
!
interface TokenRing0/0
 no ip address
 shutdown
 ring-speed 16
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/1
 no ip address
 shutdown
```

```
 duplex auto
 speed auto
!
router ospf 300 vrf Cliente3
 router-id 192.168.0.3
 log-adjacency-changes
 redistribute bgp 100 metric 20 subnets
 network 10.0.0.0 0.0.0.255 area 1
!
router ospf 100 vrf Cliente1
 router-id 10.0.0.254
 log-adjacency-changes
 redistribute bgp 100 metric 20 subnets
 network 10.0.0.0 0.0.0.255 area 1
!
router ospf 1
 router-id 192.168.8.1
 log-adjacency-changes
 network 192.168.0.3 0.0.0.0 area 0
 network 192.168.4.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
 network 192.168.8.0 0.0.0.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.0.1 remote-as 100
 neighbor 192.168.0.1 update-source Loopback0
 neighbor 192.168.0.2 remote-as 100
 neighbor 192.168.0.2 update-source Loopback0
 neighbor 192.168.0.4 remote-as 100
 neighbor 192.168.0.4 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 192.168.0.1 activate
  neighbor 192.168.0.1 send-community both
  neighbor 192.168.0.2 activate
  neighbor 192.168.0.2 send-community both
  neighbor 192.168.0.4 activate
  neighbor 192.168.0.4 send-community both
 exit-address-family
 !
```

```
 address-family ipv4 vrf Cliente3
  redistribute connected
  redistribute ospf 300 vrf Cliente3
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf Cliente1
  redistribute connected
  redistribute ospf 100 vrf Cliente1
  no synchronization
 exit-address-family
!
ip default-gateway 192.168.4.254
ip http server
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.4.254
!
!
!
!
!
!
control-plane
!
!
!
voice-port 2/0/0
!
voice-port 2/0/1
!
!
!
!
!
!
banner login ^]Cisco 3640 - Border^]
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
!
```

```
!
end
```

6.2.4 Cisco 2611

6.2.5 Cisco AXP

6.3 Dorsale Secondaria

6.3.1 Cisco 1601

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname c1600
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$G2Ok$F.s13nMN8k3wdv/Lg46Th.
!
clock timezone Rome 2
no aaa new-model
ip subnet-zero
ip name-server 130.251.1.4
!
username admin password 7 02050D480809
!
!
!
!
interface Ethernet0
 ip address 192.168.5.254 255.255.255.0
!
interface Serial0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type cisco
!
interface Serial0.60 point-to-point
```

```
 ip address 192.168.6.1 255.255.255.252
 frame-relay interface-dlci 60
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
!
router eigrp 1
 network 192.168.5.0
 network 192.168.6.0 0.0.0.3
 no auto-summary
!
ip default-gateway 192.168.6.2
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.6.2
ip http server
!
!
line con 0
 login local
line vty 0 4
 login local
!
end
```

6.4 VPN Cliente 1

6.4.1 Cisco 4000

6.4.2 Nokia IP 120

6.5 Rete Cliente 2

6.5.1 Cisco 1711

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname cl1-2_c1700
```

```
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$wZJD$g3hZAKan7pgJm0bTsmb/T.
!
no aaa new-model
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.0.0.254
ip dhcp excluded-address 10.0.1.254
!
ip dhcp pool vlan80
   import all
   network 10.0.0.0 255.255.255.0
   default-router 10.0.0.254
   dns-server 130.251.1.4
!
ip dhcp pool vlan90
   import all
   network 10.0.1.0 255.255.255.0
   default-router 10.0.1.254
   dns-server 130.251.1.4
!
!
!
frame-relay switching
!
!
!
username admin password 7 121A0C041104
username gateway password 7 0822455D0A16
!
!
!
!
!
!
interface Ethernet0
 ip address 10.0.1.254 255.255.255.0
 ip nat inside
```

```
 ip virtual-reassembly
 half-duplex
!
interface FastEthernet0
 ip address 10.0.0.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 speed auto
!
interface Serial0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type ansi
!
interface Serial0.100 point-to-point
 frame-relay interface-dlci 100 ppp Virtual-Template1
!
interface Virtual-Template1
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
 ppp authentication chap dialin
 ppp chap hostname framerelay
 ppp chap password 7 0822455D0A16
 ppp pap sent-username framerelay password 7 02050D480809
 ppp ipcp dns request
 ppp ipcp route default
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 10.0.1.0 0.0.0.255
 auto-summary
!
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Virtual-Template1 overload
!
access-list 1 permit 10.0.0.0 0.0.0.255
access-list 1 permit 10.0.1.0 0.0.0.255
!
control-plane
!
```

```
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
!
end
```

6.6 VPN Cliente 3

6.6.1 Cisco 800

```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname cl3_c800
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
enable secret 5 $1$nDBg$S34xTL.T8.5/DHXx/lVNh0
!
no aaa new-model
!
resource policy
!
ip cef
!
!
no ip domain lookup
ip name-server 130.251.1.4
!
!
!
username admin password 7 1511021F0725
!
!
```

```
!
!
!
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface FastEthernet0
 switchport access vlan 300
!
interface FastEthernet1
 switchport access vlan 300
!
interface FastEthernet2
 switchport access vlan 300
!
interface FastEthernet3
 switchport access vlan 300
!
interface Vlan300
 ip address 10.0.0.1 255.255.255.0
!
router ospf 300
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 1
!
ip default-gateway 10.0.0.254
ip route 0.0.0.0 0.0.0.0 10.0.0.254
!
ip http server
ip http access-class 23
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
!
!
control-plane
!
```

```
!
line con 0
 login local
 no modem enable
line aux 0
line vty 0 4
 login local
 transport input telnet ssh
!
scheduler max-task-time 5000
end
```

6.6.2 Cisco 2612