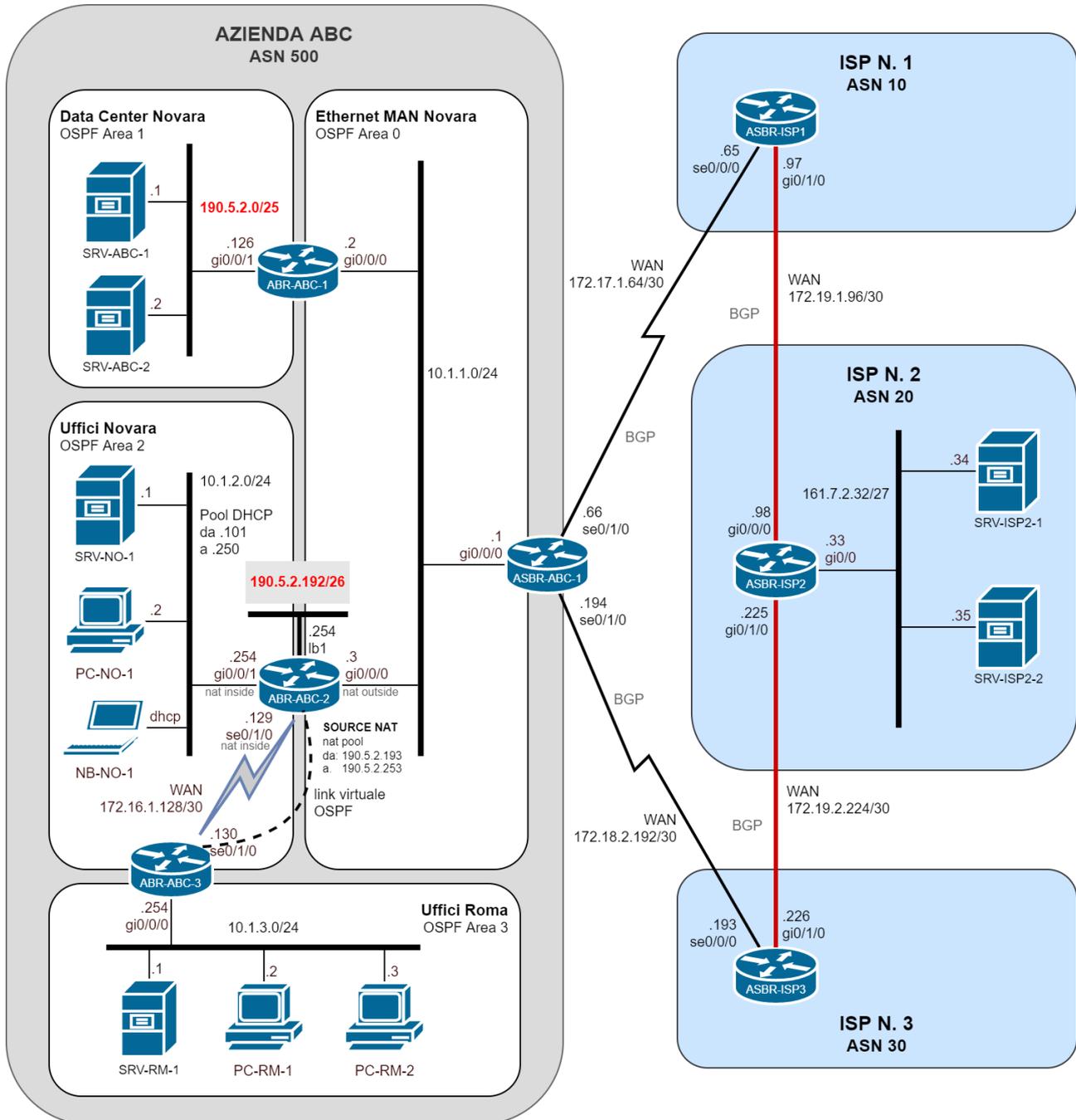


Interconnessione di reti aziendali e ISP mediante NAT, OSPF e BGP

Indice generale

Interconnessione di reti aziendali e ISP mediante NAT, OSPF e BGP.....	1
Schema del progetto.....	2
Configurazione della rete aziendale ABC.....	3
Configurazione delle interfacce dei router aziendali.....	3
Configurazione OSPF.....	4
Configurazione BGP (ISP e azienda).....	6
Configurazione NAT E DHCP.....	7
Esecuzione dei test.....	8
Esercizi.....	9

Schema del progetto



Configurazione della rete aziendale ABC

La rete dell'azienda immaginaria ABC di Novara costituisce un *Autonomous System* (ASN 500) composto da un data center, uffici centrali e uffici periferici. Il data center e gli uffici centrali si trovano a Novara e sono collegati alla MAN cittadina. Gli uffici periferici si trovano a Roma e sono collegati alla sede centrale mediante una connessione WAN dedicata.

Le reti dell'azienda sono interconnesse tra loro e si scambiano le informazioni di routing mediante il protocollo OSPF. L'accesso a internet è garantito da un doppio collegamento a due ISP distinti ed il collegamento ai relativi AS è gestito tramite il protocollo BGP.

L'azienda dispone del blocco di indirizzi pubblici 190.5.2.0/24, suddiviso in tre sottoreti: la sottorete 190.5.2.0/25 è utilizzata per configurare i server del data center; la sottorete 190.5.2.128/26 non è attualmente impiegata, in quanto riservata per scopi futuri; la sottorete 190.5.2.192/26 è utilizzata per creare il pool di indirizzi necessario al *source* NAT dedicato ai client.

I router dell'azienda hanno le seguenti caratteristiche.

Router	Interfaccia	Indirizzo IP
Ethernet MAN di Novara ASBR-ABC-1 (Cisco ISR4331)	Gig0/0/0	10.1.1.1/24
	Se0/1/0	172.17.1.66/30
	Se0/1/1	172.18.2.194/30
Data Center di Novara ABR-ABC-1 (Cisco ISR4321)	Gig0/0/0	10.1.1.2/24
	Gig0/0/1	190.5.2.126/25
Uffici centrali di Novara ABR-ABC-2 (Cisco ISR4321)	Gig0/0/0	10.1.1.3/24
	Gig0/0/1	10.1.2.254/24
	Se0/1/0	172.16.1.129/30
	Loopback 1	190.5.2.254/25
Uffici periferici di Roma ABR-ABC-3 (Cisco ISR4321)	Gig0/0/0	10.1.3.254/24
	Se0/1/0	172.16.1.130/30

Configurazione delle interfacce dei router aziendali

! Router ASBR-ABC-1

```
interface GigabitEthernet0/0/0
 ip address 10.1.1.1 255.255.255.0
!
interface Serial0/1/0
 ip address 172.17.1.66 255.255.255.252
!
interface Serial0/1/1
 ip address 172.18.2.194 255.255.255.252
```

!

! Router ABR-ABC-1

```
interface GigabitEthernet0/0/0
 ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet0/0/1
 ip address 190.5.2.126 255.255.255.128
!
```

! Router ABR-ABC-2

```
interface Loopback1
 ip address 190.5.2.254 255.255.255.192
!
interface GigabitEthernet0/0/0
 ip address 10.1.1.3 255.255.255.0
!
interface GigabitEthernet0/0/1
 ip address 10.1.2.254 255.255.255.0
!
interface Serial0/1/0
 ip address 172.16.1.129 255.255.255.252
 clock rate 2000000
!
```

! Router ABR-ABC-3

```
interface GigabitEthernet0/0/0
 ip address 10.1.3.254 255.255.255.0
!
interface Serial0/1/0
 ip address 172.16.1.130 255.255.255.252
!
```

Configurazione OSPF

La rete privata della MAN è inserita nell'area 0 (backbone) di OSPF; la rete del data center nell'area 1; la rete LAN degli uffici centrali e il collegamento WAN Novara-Roma nell'area 2. La LAN degli uffici periferici è inserita nell'area 3 ed è collegata alla rete di backbone mediante un link virtuale realizzato tra i router ABR-ABC-2 e ABR-ABC-3.

Il router ABR-ABC-2 configura l'interfaccia Loopback1 con un indirizzo della rete 190.5.2.192/26. La rete è definita di tipo multi-point per essere interamente propagata agli altri router con OSPF.

Di seguito sono riportate le configurazioni OSPF dei router ABR aziendali.

! Router ABR-ABC-1

```
!
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
```

```
network 10.1.1.0 0.0.0.255 area 0
network 190.5.2.0 0.0.0.127 area 1
!

! Router ABR-ABC-2
!
interface Loopback1
 ip address 190.5.2.254 255.255.255.192
 ip ospf network point-to-point
 ip ospf priority 1
!
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 area 2 virtual-link 4.4.4.4
 network 10.1.1.0 0.0.0.255 area 0
 network 10.1.2.0 0.0.0.255 area 2
 network 172.16.1.128 0.0.0.3 area 2
 network 190.5.2.192 0.0.0.63 area 2
!
```

```
! Router ABR-ABC-3
!
router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
 area 2 virtual-link 3.3.3.3
 network 172.16.1.128 0.0.0.3 area 2
 network 10.1.3.0 0.0.0.255 area 3
!
```

Il router ASBR ridistribuisce in OSPF le informazioni di routing acquisite con BGP e propaga nella rete la default route 0.0.0.0 (comando *default-information originate*), assumendo di fatto il ruolo di *default gateway* nell'accesso alle reti esterne all'azienda.

```
! Router ASBR-ABC-1
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 redistribute bgp 500 subnets
 network 10.1.1.0 0.0.0.255 area 0
 default-information originate
!
```

```
ASBR-ABC-1#show ip route ospf
 10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O IA 10.1.2.0 [110/2] via 10.1.1.3, 03:36:36, GigabitEthernet0/0/0
O IA 10.1.3.0 [110/66] via 10.1.1.3, 03:36:36, GigabitEthernet0/0/0
 172.16.0.0/30 is subnetted, 1 subnets
O IA 172.16.1.128 [110/65] via 10.1.1.3, 03:36:36, GigabitEthernet0/0/0
 190.5.0.0/16 is variably subnetted, 3 subnets, 2 masks
O IA 190.5.2.0 [110/2] via 10.1.1.2, 03:36:36, GigabitEthernet0/0/0
```

0 IA 190.5.2.128 [110/2] via 10.1.1.3, 03:36:36, GigabitEthernet0/0/0

Configurazione BGP (ISP e azienda)

Il router ASBR dell'azienda è collegato sia all'ISP n. 1 (ASN 10) sia all'ISP n. 3 (ASN 30).

Gli ISP annunciano, via BGP, la route 0.0.0.0/0 utile a impostare la default route su ASBR-ABC-1. In generale, per eseguire l'annuncio di una rete è necessario che la rete sia presente nella tabella del router. Poiché la rete 0.0.0.0 si sovrappone alle altre reti, i router degli ISP configurano per 0.0.0.0 una **discard route**: la regola è inserita in tabella per completare l'annuncio BGP ma, di fatto, viene ignorata. In una discard route, il next-hop è impostato a **Null0**.

Il router dell'ISP n. 2 annuncia anche la rete 161.7.2.32/27 composta da un certo numero di server pubblici.

Si riportano le configurazioni BGP dei router degli ISP.

! Router ASBR-ISP1

```
!  
ip route 0.0.0.0 0.0.0.0 Null0  
!  
router bgp 10  
  neighbor 172.17.1.66 remote-as 500  
  neighbor 172.19.1.98 remote-as 20  
  network 0.0.0.0  
!
```

! Router ASBR-ISP2

```
!  
router bgp 20  
  neighbor 172.19.1.97 remote-as 10  
  neighbor 172.19.2.226 remote-as 30  
  network 161.7.2.32 mask 255.255.255.224  
!
```

! Router ASBR-ISP3

```
!  
ip route 0.0.0.0 0.0.0.0 Null0  
!  
router bgp 30  
  neighbor 172.18.2.194 remote-as 500  
  neighbor 172.19.2.225 remote-as 20  
  network 0.0.0.0  
!
```

Nel router aziendale ASBR-ABC-1, gli annunci BGP sono limitati ai soli indirizzi pubblici in possesso dell'azienda. Allo scopo di ridurre il numero di annunci, anziché redistribuire gli annunci OSPF relativi alle due sottoreti 190.5.2.0/25 e 190.5.2.192/26, il router ASBR-ABC-1 annuncia agli altri AS la sola rete 190.5.2.0/24: anche in questo caso, per evitare problemi di sovrapposizione il router imposta una *discard route* per la rete 190.5.2.0/24.

La configurazione del router ASBR-ABC-1 è la seguente:

! Router ASBR-ABC-1

```
!
ip route 190.5.2.0 255.255.255.0 Null0
!
router bgp 500
 neighbor 172.17.1.65 remote-as 10
 neighbor 172.18.2.193 remote-as 30
 network 190.5.2.0 mask 255.255.255.0
!
```

ASBR-ABC-1#show ip route

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C    10.1.1.0/24 is directly connected, GigabitEthernet0/0/0
L    10.1.1.1/32 is directly connected, GigabitEthernet0/0/0
O IA  10.1.2.0/24 [110/2] via 10.1.1.3, 04:24:59, GigabitEthernet0/0/0
O IA  10.1.3.0/24 [110/66] via 10.1.1.3, 04:24:59, GigabitEthernet0/0/0
161.7.0.0/27 is subnetted, 1 subnets
B    161.7.2.32/27 [20/0] via 172.17.1.65, 00:00:00
172.16.0.0/30 is subnetted, 1 subnets
O IA  172.16.1.128/30 [110/65] via 10.1.1.3, 04:24:59, GigabitEthernet0/0/0
172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.17.1.64/30 is directly connected, Serial0/1/0
L    172.17.1.66/32 is directly connected, Serial0/1/0
172.18.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.18.2.192/30 is directly connected, Serial0/1/1
L    172.18.2.194/32 is directly connected, Serial0/1/1
190.5.0.0/16 is variably subnetted, 3 subnets, 2 masks
S    190.5.2.0/24 is directly connected, Null0
O IA  190.5.2.0/25 [110/2] via 10.1.1.2, 04:24:59, GigabitEthernet0/0/0
O IA  190.5.2.192/26 [110/2] via 10.1.1.3, 04:24:59, GigabitEthernet0/0/0
B*   0.0.0.0/0 [20/0] via 172.17.1.65, 00:00:00
```

Configurazione NAT E DHCP

Il router ABR-ABC-2 offre il servizio DHCP per la sola LAN dell'ufficio di Novara. Il configurazione DHCP utilizza il pool di indirizzi da 10.1.2.101 a 10.1.2.250, imposta il default gateway a 10.1.2.254 e il DNS server a 8.8.8.8 (in questa attività il servizio DNS non è configurato).

Il router attiva anche il processo di *source NAT* dinamico per i computer degli uffici. Le interfacce collegate alla LAN dell'ufficio di Novara e al router ASBR-ABC-3 sono di tipo “*inside*”, quella collegata alla MAN di tipo “*outside*”. Gli indirizzi privati sono tradotti in indirizzi pubblici tramite il pool NAT da 190.5.2.193 a 192.15.2.253.

Di seguito sono riportate le configurazioni NAT e DHCP del router ABR-ABC-2.

! Router ABR-ABC-2

```
!
! Configurazione DHCP
ip dhcp excluded-address 10.1.2.1 10.1.2.100
ip dhcp excluded-address 10.1.2.251 10.1.2.254
!
ip dhcp pool dhcp-novara
 network 10.1.2.0 255.255.255.0
```

```
default-router 10.1.2.254
dns-server 8.8.8.8
!
! Configurazione NAT
interface GigabitEthernet0/0/0
ip address 10.1.1.3 255.255.255.0
ip nat outside
duplex auto
speed auto
!
interface GigabitEthernet0/0/1
ip address 10.1.2.254 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface Serial0/1/0
ip address 172.16.1.129 255.255.255.252
ip nat inside
clock rate 2000000
!
ip nat pool pool-uffici 190.5.2.193 190.5.2.253 netmask 255.255.255.192
ip nat inside source list 1 pool pool-uffici overload
!
access-list 1 permit 10.1.3.0 0.0.0.255
access-list 1 permit 10.1.2.0 0.0.0.255
```

Esecuzione dei test

Terminata la configurazione dei vari dispositivi, verificarne il corretto funzionamento eseguendo i seguenti test:

- Raggiungibilità, mediante comando *ping*, del server di data center 190.5.2.1 da un PC dell'ufficio centrale di Novara.
- Raggiungibilità del server di data center 190.5.2.2 da un PC dell'ufficio periferico di Roma.
- Raggiungibilità del server pubblico 161.7.2.34 dell'ISP n. 2 da un PC dell'ufficio centrale di Novara
- Raggiungibilità del server pubblico 161.7.2.35 dell'ISP n. 2 da un PC dell'ufficio periferico di Roma
- Raggiungibilità del server di data center 190.5.2.1 da uno dei server dell'ISP n. 2
- Raggiungibilità del server di data center 190.5.2.2 dal router dell'ISP n. 1
- **Irraggiungibilità** del server interno alla LAN dell'ufficio centrale da un server di data center (il server dell'ufficio ha un indirizzo privato e quindi non può essere raggiunto da un indirizzo pubblico)

Esercizi

1. Realizzare, interconnettere e configurare le reti dell'azienda e degli ISP descritte nello schema del progetto.
2. Verificare che la sottorete di comunicazione con cui l'azienda ABC accede a internet è tollerante al guasto di un collegamento nel seguente modo:
 - a) In modalità simulazione, determinare il percorso dei pacchetti inviati dal client di ABC per raggiungere un server dell'ISP n. 2 (Client / ABR-ABC-2 / ASBR-ABC-1 / ABR-ISP? / ABR-ISP2 / Server): il penultimo router attraversato può essere quello dell'ISP n.1 oppure quello dell'ISP n. 3.
 - b) In modalità real-time, rimuovere il collegamento tra ASBR-ABC-1 e ABR-ISP? e far trascorrere il tempo premendo il bottone *Fast Forward Time*.
 - c) In modalità simulazione, determinare il nuovo percorso dei pacchetti inviati dal client di ABC per raggiungere lo stesso server dell'ISP n. 2
 - d) Ripristinare il collegamento, premere il bottone *Fast Forward Time* e controllare nuovamente il percorso dei pacchetti.
3. Integrare il progetto aggiungendo e configurando un secondo data center composto da server pubblici. Dopo aver aggiunto un nuovo router ABR-ABC-4 e aver collegato una sua interfaccia alla MAN cittadina, collegare il nuovo data center a una seconda interfaccia del router, assegnando agli host gli indirizzi della rete residua 192.15.2.128/26. Verificare che i nuovi server siano raggiungibili sia dall'interno dell'azienda sia dall'esterno.
4. Integrare il progetto aggiungendo e configurando alcuni server pubblici per l'ISP n. 3. I server devono appartenere alla rete IP 200.3.1.96/28. Verificare che sia possibile accedere ai server dell'ISP dai client aziendali.