



**Università degli Studi di Perugia – Facoltà di Scienze MM. NN. FF.
Dipartimento di Matematica ed Informatica – Corso di laurea triennale in Informatica**

Reti di Calcolatori: Protocolli
prof. Sergio Tasso

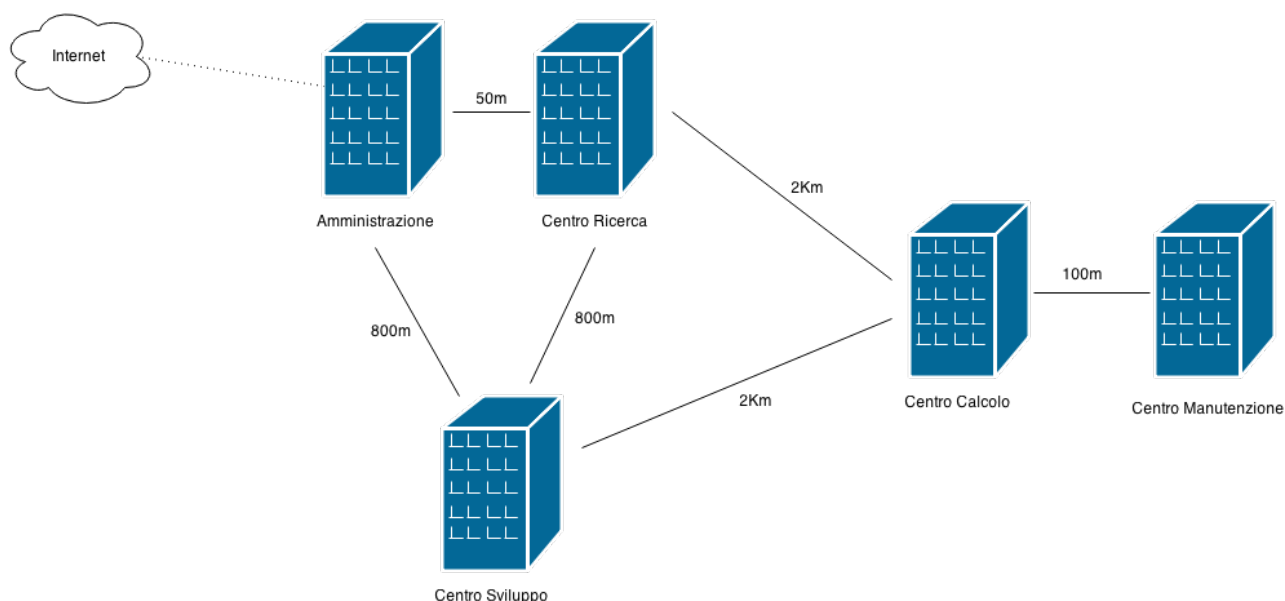
Progettazione della rete per un'azienda di ricerca e sviluppo informatico

**A cura di: - Ceccarelli Andrea
- Castellini Jacopo**

Anno Accademico 2013/14

Finalità del progetto

Scopo di questo progetto è quello di progettare, configurare e gestire la rete per una nota azienda di ricerca e sviluppo informatico. L'azienda è dislocata in cinque edifici, disposti e da collegare come in figura.



L'edificio Amministrazione contiene il quartier generale dell'azienda, dove vengono prese le decisioni in merito alle attività degli altri stabilimenti. Questo edificio, oltre ad essere collegato direttamente ad Internet, contiene la DMZ (DeMilitarized Zone), che consta di un Server Mail, un Server DNS, un Server Web ed un Server Proxy. Include inoltre, un Server DHCP per la gestione degli indirizzi da assegnare tramite la copertura Wi-Fi presente.

Il Centro di Ricerca non contiene alcun server, ed è il luogo dove vengono sviluppate le nuove tecnologie e migliorate quelle esistenti. L'edificio usato come Centro di Sviluppo invece è il luogo in cui le nuove tecnologie vengono impiegate per sviluppare prodotti all'avanguardia da rilasciare sul mercato. In esso è presente un ulteriore Server DNS. Un altro edificio, il Centro di Calcolo, fornisce ai due centri precedenti ulteriore potenza di calcolo fornendo macchine da sfruttare tramite tecniche di programmazione parallela e distribuita. Esso contiene quindi un Server Aziendale, che si fa carico di gestire le richieste da e per le macchine adibite al calcolo. In ultimo il Centro di Manutenzione, fornisce assistenza all'utenza che acquista i prodotti dell'azienda, ed esegue inoltre interventi di manutenzione straordinaria e ordinaria, sul Centro di Calcolo. Sono qui presenti un ulteriore Server DHCP per l'accesso alla rete Wi-Fi ed il Server di Backup, necessario all'azienda per non rischiare di perdere i risultati delle ricerche.

Nome edificio	N. Utenti	Servers	Wi-Fi
Amministrazione	100	DHCP, DNS, Mail, Web, Proxy	si
Centro Ricerca	100	/	no
Centro Sviluppo	100	DNS	no
Centro Calcolo	100	Aziendale	no
Centro Manutenzione	100	Backup, DHCP	si

Schema logico della rete

Ogni edificio è disposto su di un solo piano. Lo schema delle reti dei vari edifici è:

Nome edificio	Rete
Amministrazione	192.168.1.0 + 192.168.6.0 per la DMZ (Subnet Mask 255.255.255.0)
Centro Ricerca	192.168.2.0 (Subnet Mask 255.255.255.0)
Centro Sviluppo	192.168.3.0 (Subnet Mask 255.255.255.0)
Centro Calcolo	192.168.4.0 (Subnet Mask 255.255.255.0)
Centro Manutenzione	192.168.5.0 (Subnet Mask 255.255.255.0)

I router presenti in ogni edificio sono:

Nome edificio	Nome router	Indirizzo sulla sottorete locale
Amministrazione	Tanato Crono	192.168.1.1 eth0 192.168.6.6 eth0
Centro Ricerca	Atena	192.168.2.1 eth0
Centro Sviluppo	Apollo	192.168.3.1 eth0
Centro Calcolo	Ares	192.168.4.1 eth0
Centro Manutenzione	Dioniso	192.168.5.1 eth0

Sono tutti Interior Router usati per la connessione tra gli stabili, tranne Crono che è un Exterior Router che funge anche da NAT verso Internet per tutta la rete. Quest'ultimo avrà un indirizzo pubblico visibile a tutti su di un interfaccia. Inoltre il router Tanato è anche l'Interior Router di accesso alla DMZ, quindi avrà anche un indirizzo nella rete della DMZ.

I vari collegamenti tra i router sono definiti con questi IP:

Router A – Router B	Indirizzo A	Indirizzo B
Tanato - Crono	192.168.6.1 eth3	192.168.6.6 eth0
Tanato - Atena	192.168.11.1 eth1	192.168.21.1 eth1
Tanato - Apollo	192.168.12.1 eth2	192.168.31.1 eth1
Ares - Atena	192.168.41.1 eth1	192.168.23.1 eth3
Ares - Apollo	192.168.42.1 eth2	192.168.33.1 eth3
Ares - Dioniso	192.168.43.1 eth3	192.168.51.1 eth1
Atena - Apollo	192.168.22.1 eth2	192.168.32.1 eth2

Questa invece è l'assegnazione degli indirizzi IP statica degli host e dei server fatta nei vari edifici dell'azienda:

Amministrazione

Server DHCP Afrodite	192.168.1.2
Host 1	192.168.1.3
...	
Host 100	192.168.1.102

DMZ

Server Mail Hermes	192.168.6.2
Server DNS Zeus	192.168.6.3
Server Proxy Ade	192.168.6.4
Server Web Poseidone	192.168.6.5

Centro di Ricerca

Host 1	192.168.2.2
...	
Host 100	192.168.2.101

Centro di Sviluppo

Server DNS Eracle	192.168.3.2
Host 1	192.168.3.3
...	
Host 100	192.168.3.102

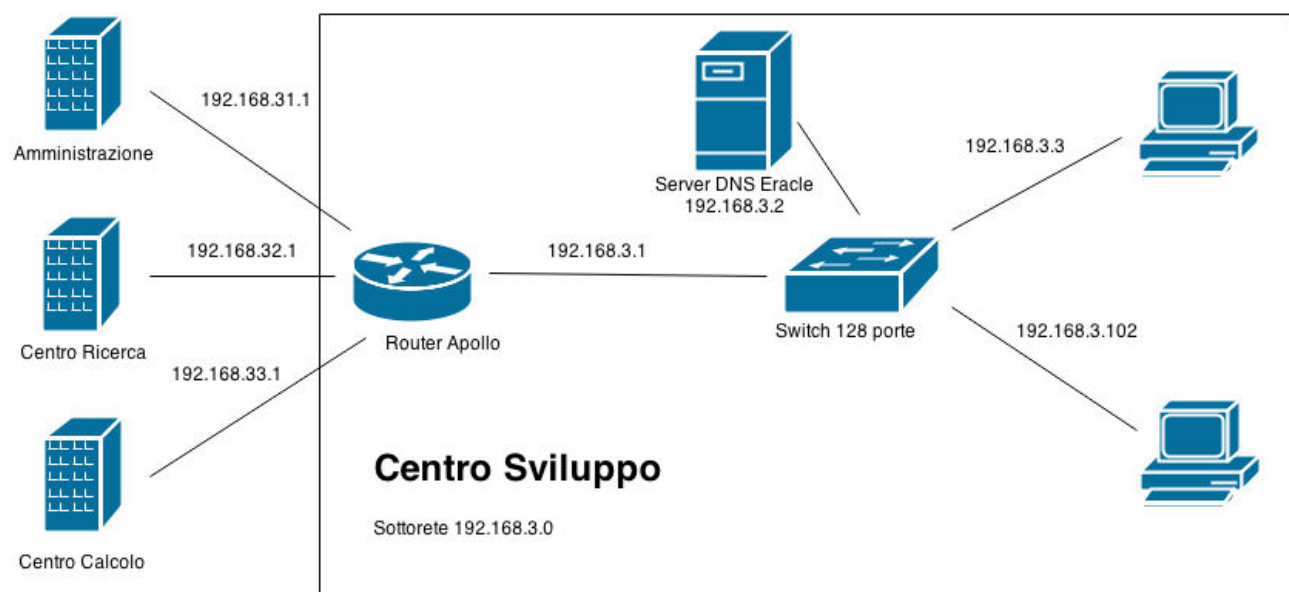
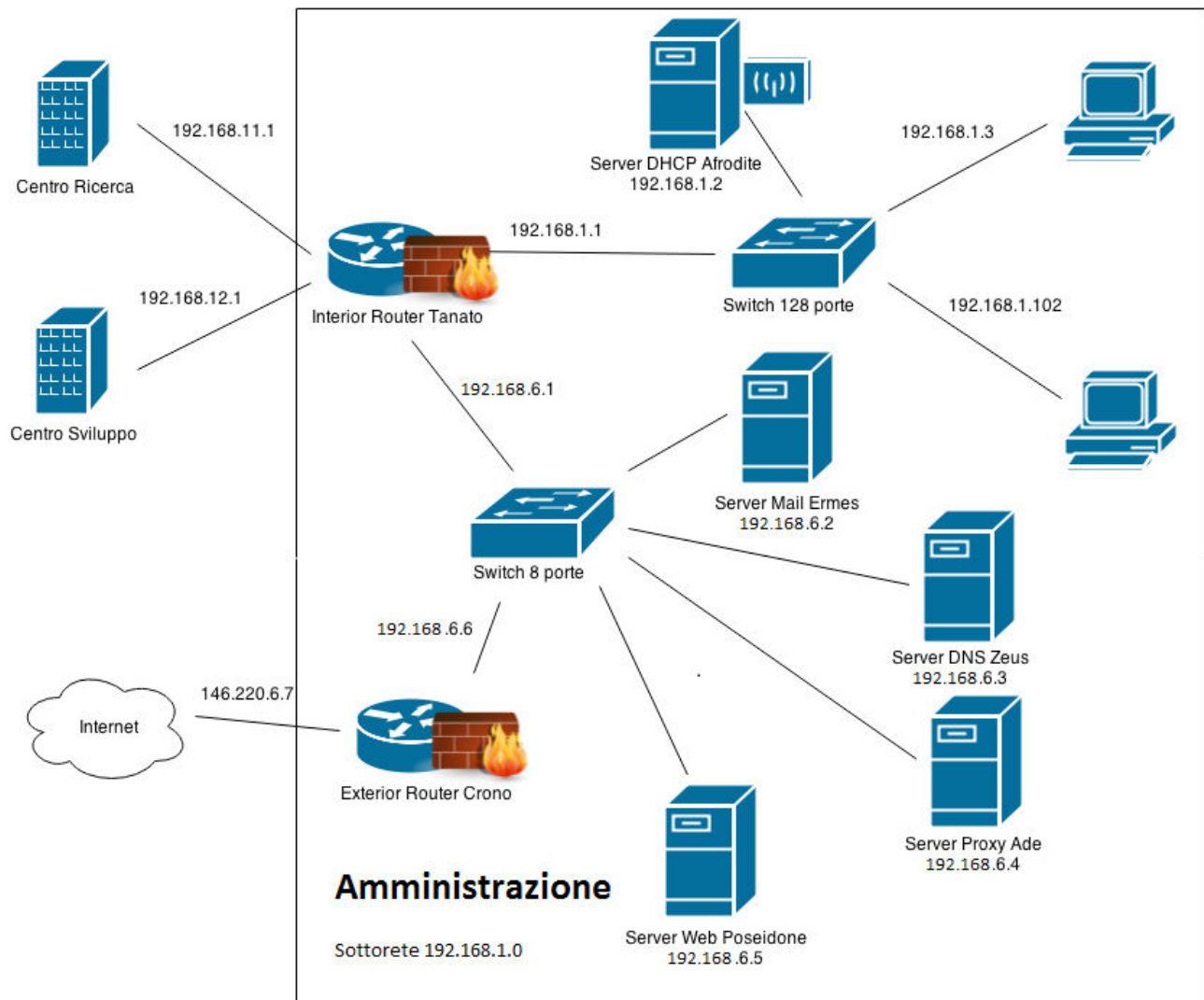
Centro di Calcolo

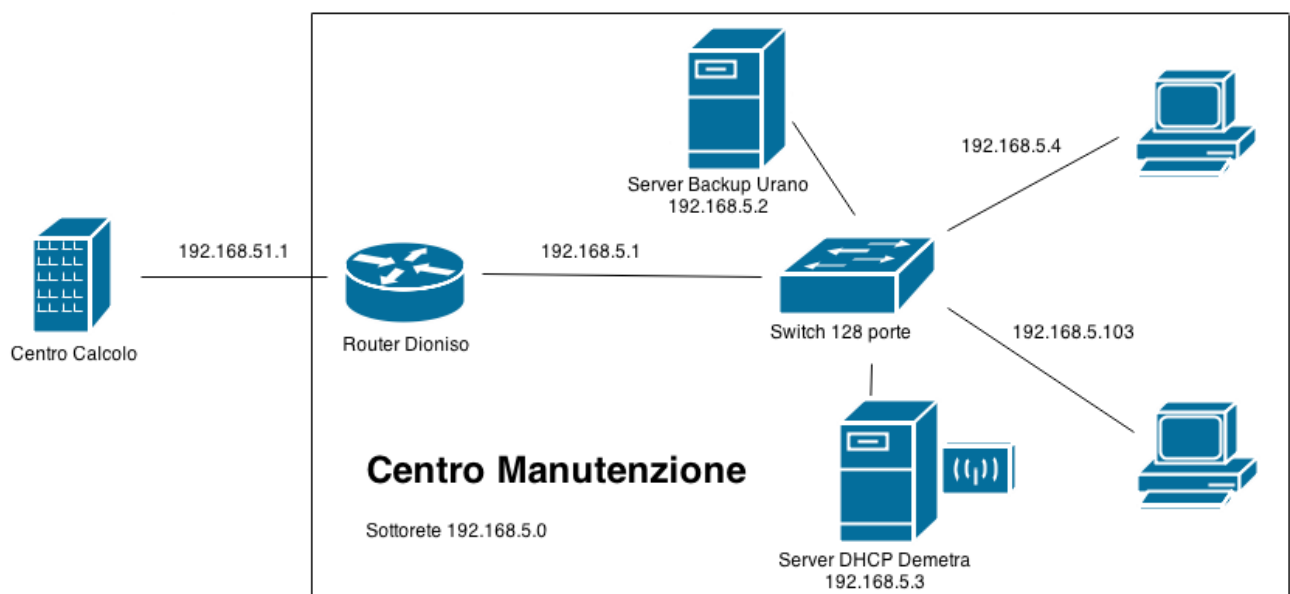
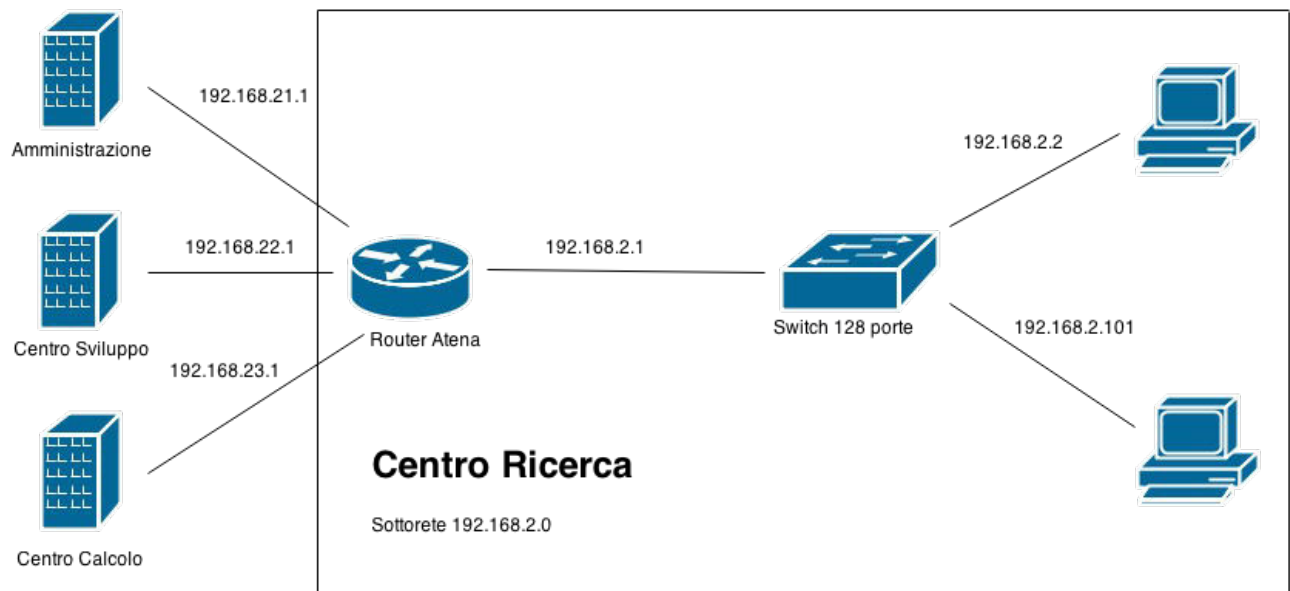
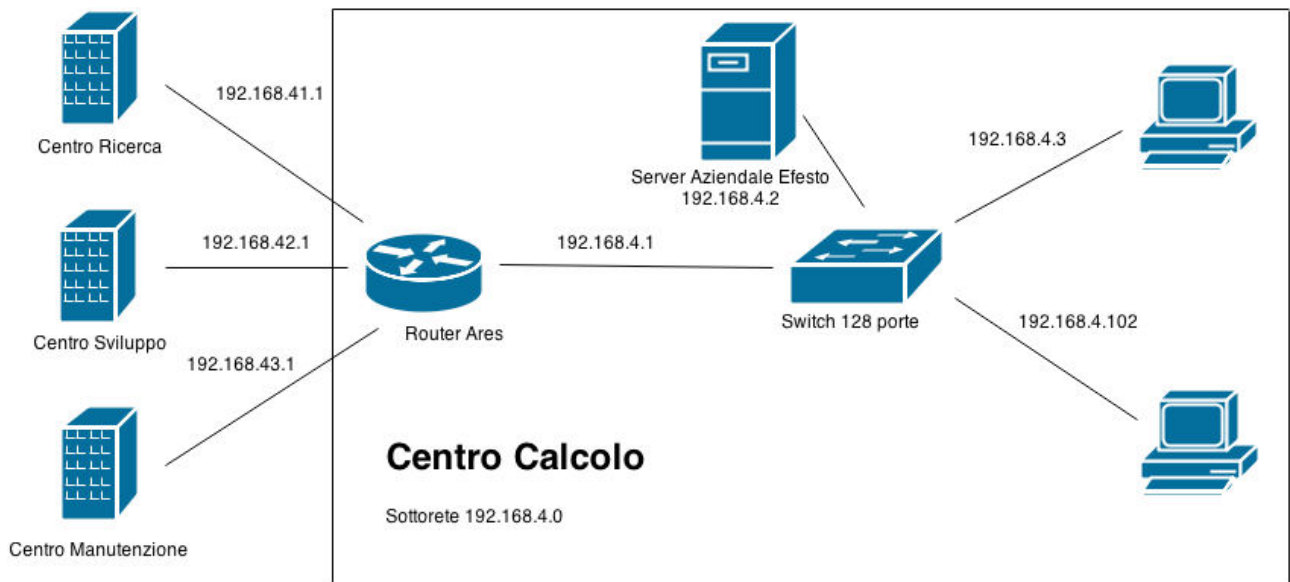
Server Aziendale Efesto	192.168.4.2
Host 1	192.168.4.3
...	
Host 100	192.168.4.102

Centro di Manutenzione

Server di Backup Urano	192.168.5.2
Server DHCP Demetra	192.168.5.3
Host 1	192.168.5.4
...	
Host 100	192.168.5.103

Diamo quindi uno schema logico delle varie configurazioni degli edifici dell'azienda.





Configurazione delle interfacce

Questi sono l'elenco dei comandi da usare in ogni edificio per configurare le interfacce sulle varie macchine, compresi i server ed i router.

```
#####  
# AMMINISTRAZIONE #  
#####
```

```
# INTERIOR ROUTER TANATO  
# Interfaccia sulla rete locale  
ifconfig eth0 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255  
# Interfaccia sulla rete del Centro Ricerca  
ifconfig eth1 192.168.11.1 netmask 255.255.255.0 broadcast 192.168.11.255  
# Interfaccia sulla rete del Centro Sviluppo  
ifconfig eth2 192.168.12.1 netmask 255.255.255.0 broadcast 192.168.12.255  
# Interfaccia con IP pubblico sulla DMZ  
ifconfig eth3 192.168.6.1 netmask 255.255.255.0 broadcast 192.168.6.255
```

```
# EXTERIOR ROUTER CRONO  
# Interfaccia con IP pubblico sulla DMZ  
ifconfig eth0 192.168.6.6 netmask 255.255.255.0 broadcast 192.168.6.255  
# Interfaccia con IP pubblico su Internet  
ifconfig eth1 146.220.6.7 netmask 255.255.255.255 broadcast 146.220.6.7
```

```
# SERVER DHCP AFRODITE  
ifconfig eth0 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
```

```
# HOSTS  
ifconfig eth0 192.168.1.3 netmask 255.255.255.0 broadcast 192.168.1.255  
...  
ifconfig eth0 192.168.1.102 netmask 255.255.255.0 broadcast 192.168.1.255
```

```
# SERVER MAIL DMZ ERMES  
ifconfig eth0 192.168.6.2 netmask 255.255.255.0 broadcast 192.168.6.255
```

```
# SERVER DNS DMZ ZEUS  
ifconfig eth0 192.168.6.3 netmask 255.255.255.0 broadcast 192.168.6.255
```

```
# SERVER PROXY DMZ ADE  
ifconfig eth0 192.168.6.4 netmask 255.255.255.0 broadcast 192.168.6.255
```

```
# SERVER WEB DMZ POSEIDONE  
ifconfig eth0 192.168.6.5 netmask 255.255.255.0 broadcast 192.168.6.255
```

```
#####  
# CENTRO CALCOLO #  
#####
```

```
# ROUTER ARES  
# Interfaccia sulla rete locale  
ifconfig eth0 192.168.4.1 netmask 255.255.255.0 broadcast 192.168.4.255  
# Interfaccia sulla rete del Centro Ricerca  
ifconfig eth1 192.168.41.1 netmask 255.255.255.0 broadcast 192.168.41.255  
# Interfaccia sulla rete del Centro Sviluppo  
ifconfig eth2 192.168.42.1 netmask 255.255.255.0 broadcast 192.168.42.255  
# Interfaccia sulla rete del Centro Manutenzione  
ifconfig eth3 192.168.43.1 netmask 255.255.255.0 broadcast 192.168.43.255
```

```
# SERVER AZIENDALE EFESTO
```

```
ifconfig eth0 192.168.4.2 netmask 255.255.255.0 broadcast 192.168.4.255

# HOSTS
ifconfig eth0 192.168.4.3 netmask 255.255.255.0 broadcast 192.168.4.255
...
ifconfig eth0 192.168.4.102 netmask 255.255.255.0 broadcast 192.168.4.255

#####
# CENTRO MANUTENZIONE #
#####

# ROUTER DIONISO
# Interfaccia sulla rete locale
ifconfig eth0 192.168.5.1 netmask 255.255.255.0 broadcast 192.168.5.255
# Interfaccia sulla rete del Centro Calcolo
ifconfig eth1 192.168.51.1 netmask 255.255.255.0 broadcast 192.168.51.255

# SERVER BACKUP URANO
ifconfig eth0 192.168.5.3 netmask 255.255.255.0 broadcast 192.168.5.255
# SERVER DHCP DEMETRA
ifconfig eth0 192.168.5.3 netmask 255.255.255.0 broadcast 192.168.5.255

# HOSTS
ifconfig eth0 192.168.5.4 netmask 255.255.255.0 broadcast 192.168.5.255
...
ifconfig eth0 192.168.5.103 netmask 255.255.255.0 broadcast 192.168.5.255

#####
# CENTRO RICERCA #
#####

# ROUTER ATENA
# Interfaccia sulla rete locale
ifconfig eth0 192.168.2.1 netmask 255.255.255.0 broadcast 192.168.2.255
# Interfaccia sulla rete dell'Amministrazione
ifconfig eth1 192.168.21.1 netmask 255.255.255.0 broadcast 192.168.21.255
# Interfaccia sulla rete del Centro Sviluppo
ifconfig eth2 192.168.22.1 netmask 255.255.255.0 broadcast 192.168.22.255
# Interfaccia sulla rete del Centro Calcolo
ifconfig eth3 192.168.23.1 netmask 255.255.255.0 broadcast 192.168.23.255

# HOSTS
ifconfig eth0 192.168.2.2 netmask 255.255.255.0 broadcast 192.168.2.255
...
ifconfig eth0 192.168.2.101 netmask 255.255.255.0 broadcast 192.168.2.255

#####
# CENTRO SVILUPPO #
#####

# ROUTER APOLLO
# Interfaccia sulla rete locale
ifconfig eth0 192.168.3.1 netmask 255.255.255.0 broadcast 192.168.3.255
# Interfaccia sulla rete dell'Amministrazione
ifconfig eth1 192.168.31.1 netmask 255.255.255.0 broadcast 192.168.31.255
# Interfaccia sulla rete del Centro Ricerca
ifconfig eth2 192.168.32.1 netmask 255.255.255.0 broadcast 192.168.32.255
# Interfaccia sulla rete del Centro Calcolo
ifconfig eth3 192.168.33.1 netmask 255.255.255.0 broadcast 192.168.33.255
```



```
# SERVER DNS ERACLE
ifconfig eth0 192.168.3.2 netmask 255.255.255.0 broadcast 192.168.3.255

# HOSTS
ifconfig eth0 192.168.3.3 netmask 255.255.255.0 broadcast 192.168.3.255
...
ifconfig eth0 192.168.3.102 netmask 255.255.255.0 broadcast 192.168.3.255
```

Routing

Per il routing all'interno della rete privata abbiamo scelto di usare un routing dinamico configurando il protocollo RIP (Routing Information Protocol). RIP è un protocollo di routing interno basato su una metrica vettore-distanza, molto leggero da eseguire ed ormai standard in ambito Unix. Esso è gestito o dal demone routed o da quello gated (su cui è ricaduta la nostra scelta). Questi sono i file di configurazione gated.conf dei vari router:

```
#####
# Router Tanato #
#####

interfaces {
    interface 192.168.11.1 active; # Verso Atena
    interface 192.168.12.1 active; # Verso Apollo
    interface 192.168.1.1 passive; # Verso rete interna
};

rip yes {
    broadcast;
    interface 192.168.11.1 {
        version 2;
        multicast;
        authentication simple "RIPauth";
    };
    interface 192.168.12.1 {
        version 2;
        multicast;
        authentication simple "RIPauth";
    };
};

export proto rip metric 0 {;
    proto direct interface 192.168.1.1 {
        network 192.168.1.0;
    };
};

#####
# Router Ares #
#####

interfaces {
    interface 192.168.41.1 active; # Verso Atena
    interface 192.168.42.1 active; # Verso Apollo
    interface 192.168.43.1 active; # Verso Dioniso
    interface 192.168.4.1 passive; # Verso rete interna
};

rip yes {
```

```

        broadcast;
interface 192.168.41.1 {
    version 2;
    multicast;
    authentication simple "RIPauth";
};
interface 192.168.42.1 {
    version 2;
    multicast;
    authentication simple "RIPauth";
};
interface 192.168.43.1 {
    version 2;
    multicast;
    authentication simple "RIPauth";
};
};

export proto rip metric 0 {
    proto direct interface 192.168.4.1 {
        network 192.168.4.0;
    };
};

#####
# Router Dioniso #
#####

interfaces {
    interface 192.168.51.1 active; # Verso Ares
    interface 192.168.5.1 passive; # Verso rete interna
};

rip yes {
    broadcast;
    interface 192.168.51.1 {
        version 2;
        multicast;
        authentication simple "RIPauth";
    };
};

export proto rip metric 0 {
    proto direct interface 192.168.5.1 {
        network 192.168.5.0;
    };
};

#####
# Router Atena #
#####

interfaces {
    interface 192.168.21.1 active; # Verso Tanato
    interface 192.168.22.1 active; # Verso Apollo
    interface 192.168.23.1 active; # Verso Ares
    interface 192.168.2.1 passive; # Verso rete interna
};

rip yes {
    broadcast;

```

```

interface 192.168.21.1 {
    version 2;
    multicast;
    authentication simple "RIPauth";
};
interface 192.168.22.1 {
    version 2;
    multicast;
    authentication simple "RIPauth";
};
interface 192.168.23.1 {
    version 2;
    multicast;
    authentication simple "RIPauth";
};
};

export proto rip metric 0 {
    proto direct interface 192.168.2.1 {
        network 192.168.2.0;
    };
};

#####
# Router Apollo #
#####

interfaces {
    interface 192.168.31.1 active; # Verso Tanato
    interface 192.168.32.1 active; # Verso Atena
    interface 192.168.33.1 active; # Verso Ares
    interface 192.168.3.1 passive; # Verso rete interna
};

rip yes {
    broadcast;
    interface 192.168.31.1 {
        version 2;
        multicast;
        authentication simple "RIPauth";
    };
    interface 192.168.32.1 {
        version 2;
        multicast;
        authentication simple "RIPauth";
    };
    interface 192.168.33.1 {
        version 2;
        multicast;
        authentication simple "RIPauth";
    };
};

export proto rip metric 0 {
    proto direct interface 192.168.3.1 {
        network 192.168.3.0;
    };
};

```

Una scelta diversa invece è stata fatta per quanto riguarda il routing nella DMZ. Infatti, essendo poche le macchine collegate ed essendoci una sola strada percorribile per ogni gateway, abbiamo scelto di usare un routing statico. Ecco i comandi da eseguire sulle varie macchine:

```
#####  
# Routing DMZ #  
#####  
  
route -n add 192.168.6.2 192.168.6.1 # Server Mail Hermes  
route -n add 192.168.6.3 192.168.6.1 # Server DNS Zeus  
route -n add 192.168.6.4 192.168.6.1 # Server Proxy Ade  
route -n add 192.168.6.5 192.168.6.1 # Server Web Poseidone  
route -n add 192.168.6.6 192.168.6.1 # Exterior Router Crono
```

Server DHCP e Wi-Fi

In due degli stabilimenti, l'Amministrazione ed il Centro di Manutenzione, è stato richiesto di configurare un access point Wi-Fi. Abbiamo scelto di usare due server DHCP (Dynamic Host Configuration Protocol) per assegnare in modo dinamico gli indirizzi agli eventuali computer connessi ad essa ed due Access Point per erogare il segnale. Questi sono i file di configurazione del demone dhcpd usati (file dhcpd.conf):

```
#####  
# DHCP Afrodite #  
#####  
  
defaultleasetime 6000;  
maxleasetime 72000;  
option subnetmask 255.255.255.0;  
option routers 192.168.1.1;  
option domain-name-servers 192.168.3.2, 192.168.6.3, 8.8.8.8;;  
option domainname "AziendaInformatica.it";  
subnet 192.168.1.0 netmask 255.255.255.0 {  
    range 192.168.1.103 192.168.1.254;  
}
```

```
#####  
# DHCP Demetra #  
#####  
  
defaultleasetime 6000;  
maxleasetime 72000;  
option subnetmask 255.255.255.0;  
option routers 192.168.5.1;  
option domain-name-servers 192.168.3.2, 192.168.6.3, 8.8.8.8;  
option domainname "AziendaInformatica.it";  
subnet 192.168.5.0 netmask 255.255.255.0 {  
    range 192.168.5.104 192.168.5.254;  
}
```

Server Mail

Nella DMZ è presente un Server Mail per la gestione degli indirizzi di posta utilizzati nell'azienda. La nostra scelta è ricaduta sul programma sendmail, molto diffuso in ambito Unix ed altamente personalizzabile. Il programma usa due file (sendmail.cf e sendmail.mc) per la propria configurazione, più un file alias per la definizione degli indirizzi. Ecco i file:

sendmail.cf

```
#####  
# Mail Hermes #  
#####
```

/etc/sendmail.cf

```
-----# Macro utente (definizione obbligatoria) #-----  
Dwmail # Hostname  
DDAziendaInformatica.it # Impostazione dominio  
Dj$w.$D # Nome del dominio ufficiale del sito  
De$j Sendmail $v ready at $ # Messaggio iniziale SMTP  
DIFrom $g $d # Formato della UNIX  
DnMAILER-DAEMON # Messaggio d'errore  
Do.:%\\@!^=/ # Operatori validi indirizzi  
Dq$g$?x ($x)$ . # Indirizzo del mittente  
  
-----# Trusted users (utenti fidati che possono cambiare l'indirizzo del mittente usando il FLAG  
-f)#-----  
Troot  
Tdaemon  
Tuucp  
  
-----# Priorità messaggi nelle code #-----  
  
Pfirst-class=0  
Pspecial-delivery=100  
Pbulk=-60  
Pjunk=-100  
  
-----# Formato delle intestazioni #-----  
  
H?P?Return-Path: <$g> # Path del mailer  
HReceived: $?sfrom $s $.by $j ($v/$Z) # Ricevuta da  
H?D?Resent-Date: $a # Data di partenza  
H?D?Date: $ A  
H?F?Resent-From: $?x$x <$g>$|$g$. # Forward  
H?F?From : $?x$x $|$g$. # Nome mittente  
  
H?x?Full-Name: $x # Impostazione fullname  
HPosted-Date: $a # Data di partenza  
H!l?Received-Date: $b # Data  
HSubject:  
H?M?Resent-Message-Id: <$t.$i@$j> # Ora attuale  
H?M?Message-Id: <$t.$i@$j> # Ora in formato-id della  
  
-----# Definizione delle options #-----
```

```

OA/etc/alias # Definizione del file degli alias
OErrorHeader=/etc/sendmail.oE # Messaggi di errore di header/file
OF0600 # Permesso per i temporary file
OHman=/usr/lib/sendmail.hf # Help nel file di sendmail
OQueueDirectory=/var/spool/mqueue # Directory queue
OTimeout.queueereturn=5d # Tempo di coda
OTimeout.queuewarn=4h

OStatusFile=/var/tmp/sendmail.st # File di stato

OHostsFile=/etc/hosts # Hosts file

OPrivacyOptions=authwarnings,noexpn,novrfy # Impediamo agli spammer di usare i comandi di sendmail "EXPN" e
"VRFY" spesso sfruttati da questi

```

-----# Configurazione del mailer #-----

```

Mlocal, P=/bin/mail, F=rlsDFMmn, S=10, R=20, A=mail -d $u
Mprog, P=/bin/sh, F=lsDFMe, S=10, R=20, A=sh -c $u
Mtcpld, P=[ICP], F=mDFMueXLC, S=17, R=27, A=IPC $h, E=\r\n
Mtcp, P=[ICP], F=mDFMueXLC, S=14, R=24, A=IPC $h, E=\r\n
Muucp, P=/usr/bin/uux, F=DFMhuU, S=13, R=23, M=100000,
A=uux - -r -z -a$f -gC $h!rmail ($u)

```

sendmail.mc

divert(-1)

This is the sendmail macro config file. If you make changes to this file,

you need the sendmail-cf rpm installed and then have to generate a new /etc/sendmail.cf by running the following command:

```
m4 /etc/mail/sendmail.mc > /etc/sendmail.cf
```

divert(0)

```
include(`/usr/share/sendmail-cf/m4/cf.m4')
```

```
VERSIONID(`linux')dnl
```

```
OSTYPE(`linux')
```

```
define(`confDEF_USER_ID',`8:12')dnl
```

```
undefine(`UUCP_RELAY')dnl
```

```
undefine(`BITNET_RELAY')dnl
```

```
define(`confAUTO_REBUILD')dnl
```

```
define(`confTO_CONNECT',`1m')dnl
```

```
define(`confTRY_NULL_MX_LIST',true)dnl
```

```
define(`confDONT_PROBE_INTERFACES',true)dnl
```

```
define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail')dnl
```

```
define(`ALIAS_FILE',`/etc/aliases')dnl
```

```
dnl define(`STATUS_FILE',`/etc/mail/statistics')dnl
```

```
define(`UUCP_MAILER_MAX',`2000000')dnl
```

```
dnl define(`confUSERDB_SPEC',`/etc/mail/userdb.db')dnl
```

```
define(`confPRIVACY_FLAGS',`authwarnings,novrfy,noexpn,restrictqrun')dnl
```

```
define(`confAUTH_OPTIONS',`A')dnl
```

```
TRUST_AUTH_MECH(`DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
```

```
define(`confAUTH_MECHANISMS',`DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
```

```
dnl define(`confTO_QUEUEWARN',`4h')dnl
```

```
dnl define(`confTO_QUEUERETURN',`5d')dnl
```

```
dnl define(`confQUEUE_LA',`12')dnl
```

```
dnl define(`confREFUSE_LA',`18')dnl
```

```
dnl FEATURE(delay_checks)dnl
```

```
MASQUERADE_AS(`AziendaInformatica.it')dnl
```

```
FEATURE(`masquerade_entire_domain')dnl
```

```
FEATURE(realy_based_on_MX)dnl
```

```

FEATURE('noverify')dnl
FEATURE('noexpn')dnl
FEATURE('no_default_msa','dnl')dnl
FEATURE('smrsh','/usr/sbin/smrsh')dnl
FEATURE('mailertable','hash -o /etc/mail/mailertable.db')dnl
FEATURE('virtusertable','hash -o /etc/mail/virtusertable.db')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
FEATURE(local_procmail,`, `procmail -t -Y -a $h -d $u')dnl
FEATURE('access_db','hash -o /etc/mail/access.db')dnl
FEATURE('dnsbl')dnl
EXPOSED_USER(`root')dnl
MAILER(SMTP)
dnl This changes sendmail to only listen on the loopback device 127.0.0.1
dnl and not on any other network devices. Comment this out if you want
dnl to accept email over the network.
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
dnl NOTE: binding both IPv4 and IPv6 daemon to the same port requires

```

alias

```

# Alias amministratori
amministratore_azienda: admin@AziendaInformatica.it
progettista_1: andrea.ceccarelli@AziendaInformatica.it
progettista_2: jacopo.castellini@AziendaInformatica.it

# Mailing list
admins: admin@AziendaInformatica.it, andrea.ceccarelli@AziendaInformatica.it,
jacopo.castellini@AziendaInformatica.it

```

Server DNS

Abbiamo configurato due Server DNS all'interno dell'azienda. Uno è situato nel Centro di Sviluppo e fa da DNS primario per la risoluzione dei nomi della rete locale. L'altro invece è situato nella DMZ e risolve i nomi dei vari servizi presenti in essa. Abbiamo usato la suite software BIND, che comprende il demone named per la risoluzione degli indirizzi da parte dei server e il software resolver che consente ai client di interrogare i server, oltre all'utilità nslookup.

Partiamo dal DNS interno alla rete locale. Il file di configurazione resolv.conf del resolver, su cui vengono elencati i name server da interrogare, da mettere su tutte le macchine è:

```

domain AziendaInformatica.it
nameserver 127.0.0.1
nameserver 192.168.3.2
nameserver 192.168.6.3
nameserver 8.8.8.8

```

Invece i file named.conf e gli zone files relativi alla rete privata usati dal demone named per rispondere alle query sono:

named.conf

```

#####
# DNS Eracle #
#####

```

```
options {
    directory "/etc/namedb";
    pid-file "named.pid";
    allow-query { any; };
    recursion no;
};

zone "."{
    type hint;
    file "named.ca";
};

zone "0.0.127.in-addr.arpa" {
    type master;
    file "named.local";
    notify no;
};

// Amministrazione
zone "amministrazione.AziendaInformatica.it" {
    type master;
    file "amministrazione.hosts";
    allow-transfer {};
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "amministrazione.rev";
    allow-transfer {};
};

// Centro Ricerca
zone "ricerca.AziendaInformatica.it" {
    type master;
    file "ricerca.hosts";
    allow-transfer {};
};

zone "2.168.192.in-addr.arpa" {
    type master;
    file "ricerca.rev";
    allow-transfer {};
};

// Centro Sviluppo
zone "sviluppo.AziendaInformatica.it" {
    type master;
    file "sviluppo.hosts";
    allow-transfer {};
};

zone "3.168.192.in-addr.arpa" {
    type master;
    file "sviluppo.rev";
    allow-transfer {};
};

// Centro Calcolo
zone "calcolo.AziendaInformatica.it" {
    type master;
    file "calcolo.hosts";
    allow-transfer {};
};
```



```

zone "4.168.192.in-addr.arpa" {
    type master;
    file "calcolo.rev";
    allow-transfer {};
};

// Centro Manutenzione
zone "manutenzione.AziendaInformatica.it" {
    type master;
    file "manutenzione.hosts";
    allow-transfer {};
};

zone "5.168.192.in-addr.arpa" {
    type master;
    file "manutenzione.rev";
    allow-transfer {};
};

```

named.ca

```

; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . <file>"
; configuration file of BIND domain name servers).
;
; This file is made available by InterNIC
; under anonymous FTP as
; file /domain/named.cache
; on server FTP.INTERNIC.NET
; -OR- RS.INTERNIC.NET
;
; last update: Jan 3, 2013
; related version of root zone: 2013010300
;
; formerly NS.INTERNIC.NET
;
. 3600000 IN NS A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000 A 198.41.0.4
A.ROOT-SERVERS.NET. 3600000 AAAA 2001:503:BA3E::2:30
;
; FORMERLY NS1.ISI.EDU
;
. 3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 A 192.228.79.201
;
; FORMERLY C.PSI.NET
;
. 3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000 A 192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
. 3600000 NS D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET. 3600000 A 199.7.91.13
D.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:2D::D
;
; FORMERLY NS.NASA.GOV
;
. 3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000 A 192.203.230.10

```

```

;
; FORMERLY NS.ISC.ORG
;
.      3600000    NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.  3600000    A    192.5.5.241
F.ROOT-SERVERS.NET.  3600000    AAAA  2001:500:2F::F
;
; FORMERLY NS.NIC.DDN.MIL
;
.      3600000    NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.  3600000    A    192.112.36.4
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.      3600000    NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.  3600000    A    128.63.2.53
H.ROOT-SERVERS.NET.  3600000    AAAA  2001:500:1::803F:235
;
; FORMERLY NIC.NORDU.NET
;
.      3600000    NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.  3600000    A    192.36.148.17
I.ROOT-SERVERS.NET.  3600000    AAAA  2001:7FE::53
;
; OPERATED BY VERISIGN, INC.
;
.      3600000    NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.  3600000    A    192.58.128.30
J.ROOT-SERVERS.NET.  3600000    AAAA  2001:503:C27::2:30
;
; OPERATED BY RIPE NCC
;
.      3600000    NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.  3600000    A    193.0.14.129
K.ROOT-SERVERS.NET.  3600000    AAAA  2001:7FD::1
;
; OPERATED BY ICANN
;
.      3600000    NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.  3600000    A    199.7.83.42
L.ROOT-SERVERS.NET.  3600000    AAAA  2001:500:3::42
;
; OPERATED BY WIDE
;
.      3600000    NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.  3600000    A    202.12.27.33
M.ROOT-SERVERS.NET.  3600000    AAAA  2001:DC3::35
; End of File

```

named.local

```

$TTL 86400
@      IN  SOA      localhost.      admin.AziendaInformatica.it {
        2014051601  ;Serial
        28800       ;Refresh
        14400       ;Retry
        3600000     ;Expire
        86400       ;Minimum
}
      IN  NS       localhost.
1      IN  PTR      localhost.

```

Amministrazione.hosts

```
$TTL 86400
@      IN      SOA    eracle.sviluppo.AziendaInformatica.it  admin.AziendaInformatica.it {
      2014051701      ;Serial
      86400           ;Refresh
      3600            ;Retry
      604800          ;Expire
      86400           ;Minimum
}
```

```
; Definizione server DNS e mail
IN NS eracle.servizi.AziendaInformatica.it
IN MX 10 ermes.AziendaInformatica.it
```

```
; Definizione host
tanato      IN      A      192.168.1.1      # Router
afrodite    IN      A      192.168.1.2      # Server DHCP
host_1      IN      A      192.168.1.3      # Host 1
...
host_100    IN      A      192.168.1.102    # Host 100
```

amministrazione.rev

```
$TTL 86400
@      IN      SOA    eracle.sviluppo.AziendaInformatica.it  admin.AziendaInformatica.it {
      2014051701      ;Serial
      86400           ;Refresh
      3600            ;Retry
      604800          ;Expire
      86400           ;Minimum
}
```

```
; Definizione server DNS di mail
IN NS eracle.servizi.AziendaInformatica.it
IN MX 10 ermes.AziendaInformatica.it
```

```
; Definizione host
1      IN      PTR     tanato.amministrazione.AziendaInformatica.it.  # Router
2      IN      PTR     afrodite.amministrazione.AziendaInformatica.it. # Server DHCP
3      IN      PTR     host_1.amministrazione.AziendaInformatica.it.   # Host 1
...
102    IN      PTR     host_100.amministrazione.AziendaInformatica.it. # Host 100
```

calcolo.hosts

```
$TTL 86400
@      IN      SOA    eracle.sviluppo.AziendaInformatica.it  admin.AziendaInformatica.it {
      2014051701      ;Serial
      86400           ;Refresh
      3600            ;Retry
      604800          ;Expire
      86400           ;Minimum
}
```

```
; Definizione server DNS e mail
IN NS eracle.servizi.AziendaInformatica.it
IN MX 10 ermes.AziendaInformatica.it
```

```
; Definizione host
ares          IN      A      192.168.4.1    # Router
efesto        IN      A      192.168.4.2    # Server Aziendale
host_1        IN      A      192.168.4.3    # Host 1
...
host_100      IN      A      192.168.4.102  # Host 100
```

calcolo.rev

```
$TTL 86400
@          IN      SOA     eracle.sviluppo.AziendaInformatica.it  admin.AziendaInformatica.it {
        2014051701      ;Serial
        86400           ;Refresh
        3600            ;Retry
        604800          ;Expire
        86400           ;Minimum
}
```

```
; Definizione server DNS di mail
IN NS eracle.servizi.AziendaInformatica.it
IN MX 10 ermes.AziendaInformatica.it
```

```
; Definizione host
1          IN      PTR     ares.calcolo.AziendaInformatica.it.    # Router
2          IN      PTR     efesto.calcolo.AziendaInformatica.it.  # Server Aziendale
3          IN      PTR     host_1.calcolo.AziendaInformatica.it.  # Host 1
...
102        IN      PTR     host_100.calcolo.AziendaInformatica.it. # Host 100
```

manutenzione.hosts

```
$TTL 86400
@          IN      SOA     eracle.sviluppo.AziendaInformatica.it  admin.AziendaInformatica.it {
        2014051701      ;Serial
        86400           ;Refresh
        3600            ;Retry
        604800          ;Expire
        86400           ;Minimum
}
```

```
; Definizione server DNS e mail
IN NS eracle.sviluppo.AziendaInformatica.it
IN MX 10 ermes.AziendaInformatica.it
```

```
; Definizione host
dioniso     IN      A      192.168.5.1    # Router
urano       IN      A      192.168.5.2    # Server Backup
demetra     IN      A      192.168.5.3    # Server DHCP
host_1      IN      A      192.168.5.4    # Host 1
...
host_100    IN      A      192.168.5.103  # Host 100
```

manutenzione.rev

```
$TTL 86400
@          IN      SOA     eracle.sviluppo.AziendaInformatica.it  admin.AziendaInformatica.it {
        2014051701      ;Serial
        86400           ;Refresh
```

```
        3600          ;Retry
        604800       ;Expire
        86400       ;Minimum
    }
```

```
;Definizione server DNS di mail
IN NS eracle.servizi.AziendaInformatica.it
IN MX 10 ermes.AziendaInformatica.it
```

```
;Definizione host
1      IN      PTR    dioniso.manutenzione.AziendaInformatica.it.    # Router
2      IN      PTR    urano.manutenzione.AziendaInformatica.it.    # Server Backup
3      IN      PTR    demetra.manutenzione.AziendaInformatica.it.  # Server DHCP
4      IN      PTR    host_1.manutenzione.AziendaInformatica.it.    # Host 1
...
103    IN      PTR    host_100.manutenzione.AziendaInformatica.it.  # Host 100
```

ricerca.hosts

```
$TTL 86400
@      IN      SOA    eracle.sviluppo.AziendaInformatica.it      admin.AziendaInformatica.it {
        2014051701    ;Serial
        86400         ;Refresh
        3600          ;Retry
        604800       ;Expire
        86400       ;Minimum
    }
```

```
; Definizione server DNS e mail
IN NS eracle.sviluppo.AziendaInformatica.it
IN MX 10 ermes.AziendaInformatica.it
```

```
; Definizione host
atena      IN      A      192.168.2.1      # Router
host_1     IN      A      192.168.2.2      # Host 1
...
host_100   IN      A      192.168.2.101    # Host 100
```

ricerca.rev

```
$TTL 86400
@      IN      SOA    eracle.sviluppo.AziendaInformatica.it      admin.AziendaInformatica.it {
        2014051701    ;Serial
        86400         ;Refresh
        3600          ;Retry
        604800       ;Expire
        86400       ;Minimum
    }
```

```
; Definizione server DNS di mail
IN NS eracle.servizi.AziendaInformatica.it
IN MX 10 ermes.AziendaInformatica.it
```

```
; Definizione host
1      IN      PTR    atena.ricerca.AziendaInformatica.it.        # Router
2      IN      PTR    host_1.ricerca.AziendaInformatica.it.        # Host 1
...
101    IN      PTR    host_100.ricerca.AziendaInformatica.it.      # Host 100
```

sviluppo.hosts

```
$TTL 86400
@      IN      SOA    eracle.sviluppo.AziendaInformatica.it  admin.AziendaInformatica.it {
        2014051701    ;Serial
        86400         ;Refresh
        3600          ;Retry
        604800        ;Expire
        86400         ;Minimum
}
```

; Definizione server DNS e mail

IN NS eracle.sviluppo.AziendaInformatica.it

IN MX 10 ermes.AziendaInformatica.it

; Definizione host

```
apollo      IN      A      192.168.3.1      # Router
host_1      IN      A      192.168.3.3      # Host 1
...
host_100    IN      A      192.168.3.102    # Host 100
```

sviluppo.rev

```
$TTL 86400
@      IN      SOA    eracle.sviluppo.AziendaInformatica.it  admin.AziendaInformatica.it {
        2014051701    ;Serial
        86400         ;Refresh
        3600          ;Retry
        604800        ;Expire
        86400         ;Minimum
}
```

; Definizione server DNS di mail

IN NS eracle.servizi.AziendaInformatica.it

IN MX 10 ermes.AziendaInformatica.it

; Definizione host

```
1      IN      PTR    apollo.sviluppo.AziendaInformatica.it.  # Router
3      IN      PTR    host_1.sviluppo.AziendaInformatica.it.  # Host 1
...
102    IN      PTR    host_100.sviluppo.AziendaInformatica.it. # Host 100
```

Veniamo ora alla DMZ. Questo è il file resolv.conf da mettere sui server che la compongono:

```
domain AziendaInformatica.it
nameserver 127.0.0.1
nameserver 192.168.6.3
nameserver 192.168.3.2
nameserver 8.8.8.8
```

Invece i file named.conf e gli zone files relativi sono:

named.conf

```
#####
# DNS Zeus #
#####

options {
    directory "/etc/namedb";
```

```

        pid-file "named.pid";
        allow-query { any; };
        recursion no;
};

zone "." IN {
    type hint;
    file "name.ca";
};

zone "localhost" IN {
    type master;
    file "localhost.zone";
    notify no;
};

zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "named.local";
    notify no;
};

# DMZ
zone "AziendaInformatica.it" {
    type master;
    file "DMZ.hosts";
    allow-transfer {};
};

zone "6.168.192.in-addr.arpa" {
    type master;
    file "DMZ.rev";
    allow-transfer {};
};

```

named.ca

```

; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . &lt;file&gt;"
; configuration file of BIND domain name servers).
;
; This file is made available by InterNIC
; under anonymous FTP as
;   file      /domain/named.cache
;   on server  FTP.INTERNIC.NET
; -OR-       RS.INTERNIC.NET
;
; last update: Jan 3, 2013
; related version of root zone: 2013010300
;
; formerly NS.INTERNIC.NET
;
.           3600000 IN NS   A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000 A   198.41.0.4
A.ROOT-SERVERS.NET. 3600000 AAAA 2001:503:BA3E::2:30
;
; FORMERLY NS1.ISI.EDU
;
.           3600000 NS   B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 A   192.228.79.201
;

```

```
; FORMERLY C.PSI.NET
;
.          3600000  NS  C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.  3600000  A  192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
.          3600000  NS  D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.  3600000  A  199.7.91.13
D.ROOT-SERVERS.NET.  3600000  AAAA 2001:500:2D::D
;
; FORMERLY NS.NASA.GOV
;
.          3600000  NS  E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.  3600000  A  192.203.230.10
;
; FORMERLY NS.ISC.ORG
;
.          3600000  NS  F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.  3600000  A  192.5.5.241
F.ROOT-SERVERS.NET.  3600000  AAAA 2001:500:2F::F
;
; FORMERLY NS.NIC.DDN.MIL
;
.          3600000  NS  G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.  3600000  A  192.112.36.4
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.          3600000  NS  H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.  3600000  A  128.63.2.53
H.ROOT-SERVERS.NET.  3600000  AAAA 2001:500:1::803F:235
;
; FORMERLY NIC.NORDU.NET
;
.          3600000  NS  I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.  3600000  A  192.36.148.17
I.ROOT-SERVERS.NET.  3600000  AAAA 2001:7FE::53
;
; OPERATED BY VERISIGN, INC.
;
.          3600000  NS  J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.  3600000  A  192.58.128.30
J.ROOT-SERVERS.NET.  3600000  AAAA 2001:503:C27::2:30
;
; OPERATED BY RIPE NCC
;
.          3600000  NS  K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.  3600000  A  193.0.14.129
K.ROOT-SERVERS.NET.  3600000  AAAA 2001:7FD::1
;
; OPERATED BY ICANN
;
.          3600000  NS  L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.  3600000  A  199.7.83.42
L.ROOT-SERVERS.NET.  3600000  AAAA 2001:500:3::42
;
; OPERATED BY WIDE
;
.          3600000  NS  M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.  3600000  A  202.12.27.33
M.ROOT-SERVERS.NET.  3600000  AAAA 2001:DC3::35
; End of File
```


named.local

```
$TTL 86400
@      IN      SOA    localhost.    admin.AziendaInformatica.it (
        2014051601    ;Serial
        28800         ;Refresh
        14400         ;Retry
        3600000       ;Expire
        86400         ;Minimum
)
      IN  NS      localhost.
1      IN  PTR     localhost.
```

localhost.zone

```
$TTL 86400
@      1D      IN      SOA    @      admin (
        2014052002    ;Serial
        36000         ;Refresh
        3600          ;Retry
        3600000       ;Expire
        36000         ;Minimum
)
      1D      IN      NS      @
      1D      IN      A       127.0.0.
```

dmz.hosts

```
$TTL 86400
@      IN      SOA      zeus.AziendaInformatica.it    admin.AziendaInformatica.it (
        2014052002    ;Serial
        36000         ;Refresh
        3600          ;Retry
        3600000       ;Expire
        36000         ;Minimum
)
```

```
; Definizione dei server DNS e mail
IN  NS  zeus.AziendaInformatica.it
IN  MX  10 ermes.AziendaInformatica.it
```

```
; Definizione host
tanato      IN      A       192.168.6.1    # Router
crono       IN      A       192.168.6.6    # Exterior Router
poseidone   IN      A       192.168.6.5    # Server Web
www         IN      CNAME    poseidone     # Alias del Server Web
ermes       IN      A       192.168.6.2    # Server Mail
mail        IN      CNAME    ermes         # Alias del Server Mail
ade         IN      A       192.168.6.4    # Server Proxy
dns         IN      CNAME    zeus          # Alias del Server DNS
```

dmz.rev

```
$TTL 86400
@      IN      SOA      zeus.AziendaInformatica.it    admin.AziendaInformatica.it (
        2014052002    ;Serial
        36000         ;Refresh
```

```

        3600          ;Retry
        3600000       ;Expire
        36000        ;Minimum
    )

; Definizione dei server DNS e mail
IN NS zeus.AziendaInformatica.it
IN MX 10 ermes.AziendaInformatica.it

; Definizione host
1      IN      PTR      tanato.AziendaInformatica.it.      # Interior Router
2      IN      PTR      ermes.AziendaInformatica.it.        # Server Mail
4      IN      PTR      ade.AziendaInformatica.it.          # Server Proxy
5      IN      PTR      poseidone.AziendaInformatica.it.     # Server Web
6      IN      PTR      crono.AziendaInformatica.it.         # Exterior Router

```

Firewall

Abbiamo configurato i firewall sui due router che sono collegati alla DMZ. Come firewall abbiamo scelto iptables, un software Unix che consente una grande configurabilità. Questa è la configurazione del firewall sull'Interior Router:

```

#####
# Firewall di Tanato #
#####

# Svuoto le catene
iptables -F FORWARD
iptables -F INPUT
iptables -F OUTPUT
iptables -F PREROUTING
iptables -F POSTROUTING

# Regola base scarta i pacchetti
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -t nat -P PREROUTING DROP

iptables -A FORWARD -i !eth3 -o eth3 -d 192.168.6.2 -p tcp --dport smtp -j ACCEPT # Connessioni al Server Mail in
SMTP
iptables -A FORWARD -i !eth3 -o eth3 -d 192.168.6.2 -p tcp --dport pop3 -j ACCEPT # Connessioni al Server Mail in
POP
iptables -A FORWARD -i !eth3 -o eth3 -d 192.168.6.2 -p tcp --dport imap -j ACCEPT # Connessioni al Server Mail in
IMAP
iptables -A FORWARD -i !eth3 -o eth3 -d 192.168.6.3 -p tcp --dport domain -j ACCEPT # Connessioni al
Server DNS con TCP
iptables -A FORWARD -i !eth3 -o eth3 -d 192.168.6.3 -p udp --dport domain -j ACCEPT # Connessioni al
Server DNS con UDP
iptables -A FORWARD -i !eth3 -o eth3 -d 192.168.6.4 -p tcp --dport webcache -j ACCEPT # Connessioni al Server
Proxy
iptables -A FORWARD -i !eth3 -o eth3 -d 192.168.6.5 -p tcp --dport www -j ACCEPT # Connessioni al Server Web

# Accetta pacchetti di connessioni stabilite o correlate
iptables -A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT

# Evita di rimanere bloccato su porte chiuse
iptables -A FORWARD -p tcp -j REJECT --reject-with tcp-reset

```

```
# Se mi vengono richiesti accessi ad Internet li faccio passare per il Proxy
iptables -t nat -A PREROUTING -i !eth3 -p tcp --dport www -j DNAT --to 192.168.6.4:8080
```

Questa invece è quella sull'Exterior Router:

```
#####
# Firewall di Crono #
#####
```

```
# Svuoto le catene
iptables -F FORWARD
iptables -F INPUT
iptables -F OUTPUT
iptables -F PREROUTING
iptables -F POSTROUTING
```

```
# Regola base scarta i pacchetti
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -t nat -P PREROUTING DROP
iptables -t nat -P POSTROUTING DROP
```

```
# Accetto le connessioni provenienti dalla DMZ
iptables -A FORWARD -i eth0 -o eth1 -p tcp -s 146.220.6.2 --dport smtp -j ACCEPT # Connessione a Server Mail
iptables -A FORWARD -i eth0 -o eth1 -p tcp -s 146.220.6.3 --dport domain -j ACCEPT # Connessione al DNS con TCP
iptables -A FORWARD -i eth0 -o eth1 -p udp -s 146.220.6.3 --dport domain -j ACCEPT # Connessione al DNS con UDP
iptables -A FORWARD -i eth0 -o eth1 -p tcp -s 146.220.6.4 --dport www -j ACCEPT # Connessioni a Server Proxy
iptables -A FORWARD -i eth0 -o eth1 -p tcp -s 146.220.6.5 --dport www -j ACCEPT # Connessioni a Server Web
```

```
# Accetta pacchetti di connessioni stabilite o correlate
iptables -A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED, RELATED -j ACCEPT
```

```
# Evita di rimanere bloccato su porte chiuse
iptables -A FORWARD -i eth0 -o eth1 -p tcp -j REJECT --reject-with tcp-reset
```

```
# Redirige le connessioni provenienti da Internet al giusto server
iptables -t nat -A PREROUTING -i eth1 -o eth0 -p tcp -d 146.220.6.7 -dport smtp -j dnat --to-destination 192.168.6.2 # Connessione a Server Mail
iptables -t nat -A PREROUTING -i eth1 -o eth0 -p tcp -d 146.220.6.7 -dport domain -j dnat --to-destination 192.168.6.3 # Connessione al DNS con TCP
iptables -t nat -A PREROUTING -i eth1 -o eth0 -p udp -d 146.220.6.7 -dport domain -j dnat --to-destination 192.168.6.3 # Connessione al DNS con UDP
iptables -t nat -A PREROUTING -i eth1 -o eth0 -p tcp -d 146.220.6.7 -dport www -j dnat --to-destination 192.168.6.5 # Connessioni a Server Web
```

```
# Fa da NAT, cioè fa uscire ogni messaggio dalla DMZ col proprio indirizzo
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Hardening

Nella nostra configurazione abbiamo dovuto dare particolare attenzione alla protezione del Server di Backup presente nel Centro di Manutenzione. Abbiamo usato tecniche di hardening configurando il demone xinetd, che contiene di monitorare e controllare l'accesso a determinati servizi, ed abbiamo configurato i file necessari per il TCP Wrapper. Questi sono i file di configurazione di xinetd:

xinetd.conf

```
defaults {
    instances=60 # n. massimo istanze del servizio
    log_type=SYSLOG authpriv # tipo di log
    log_on_success=HOST PID # info. su log in caso di successo
    log_on_failure=HOST # info. su log in caso di fallimento
    cps=25 30 # n. massimo di connessioni al secondo
}
includedir /etc/xinetd.d
```

xinetd.d/ftpd.conf

```
service ftp {
    disable=yes
    flags=REUSE
    socket_type=stream
    wait=no
    user=root
    server=/usr/sbin/proftpd
    server_args=-c /etc/proftpd.conf
    log_on_failure+=DURATION USERID
    log_on_success+=PID HOST EXIT
}
```

xinetd.d/sshd.conf

```
service ssh {
    socket_type=stream
    wait=no
    user=root
    log_on_success+=USERID
    log_on_failure+=USERID
    server=/usr/sbin/in.sshd
    log_on_failure+=DURATION USERID
    log_on_success+=PID HOST EXIT
}
```

xinetd.d/telnetd.conf

```
service telnet {
    flags=REUSE
    socket_type=stream
    wait=no
    user=root
    server=/usr/sbin/in.telnetd
}
```

```
    log_on_failure+=USERID
    disable=yes
}
```

I due file del wrapper invece sono:

hosts.allow

```
# Definisco le reti che possono accedere al Server di Backup
sshd: 192.168.2.0/24, 192.168.3.0/24, 192.168.5.0/24
nfsd: 192.168.2.0/24, 192.168.3.0/24, 192.168.5.0/24
statd: 192.168.2.0/24, 192.168.3.0/24, 192.168.5.0/24
mountd: 192.168.2.0/24, 192.168.3.0/24, 192.168.5.0/24
lockd: 192.168.2.0/24, 192.168.3.0/24, 192.168.5.0/24
```

hosts.deny

```
# Gli accessi non consentiti vengono bloccati ed i dati relativi vengono salvati su log
ALL:ALL: spawn /bin/date %c >> /var/log/denied.log
```

Strumenti di diagnostica

Una volta configurata, è importante verificare che la rete continui a funzionare come ci si aspetta e senza problemi. Oltre a monitorare l'integrità delle risorse hardware ed il loro funzionamento, elenchiamo ora alcuni strumenti software per assicurarci che anche la configurazione usata continui a lavorare come deve.

- ifconfig: comando Unix usato per configurare indirizzo IP e Subnet Mask di un'interfaccia di rete TCP/IP su di un host. Consente inoltre di attivare e disattivare un'interfaccia.
- arp: sfruttando l'omonimo protocollo, fornisce informazioni sul nome dell'interfaccia associata ad un dato indirizzo IP.
- netstat: consente di monitorare le connessioni attive su un host.
- ping: tramite pacchetti ICMP, permette di verificare la raggiungibilità di un host da un altro, e di misurare il tempo impiegato in caso di successo.
- nslookup: presente nella suite software BIND, permette di interrogare, anche in modo interattivo, un Server DNS ed ottenere così informazioni sui nomi associati agli indirizzi o viceversa.
- dig: comando simile a nslookup
- traceroute: strumento che permette di monitorare il percorso seguito da un pacchetto sulla rete per giungere a destinazione. Vengono pertanto riferiti gli indirizzi IP di tutti i router che il pacchetto attraversa.
- ripquery: consente di effettuare query RIP ad un host remoto.
- etherfind: permette di controllare tutte le informazioni, compreso l'header, dei pacchetti TCP/IP in transito sulla rete.

Componentistica e costo dell'installazione

Oltre a 500 computer dedicati all'utilizzo da parte degli utenti ed alle nove macchine server, vengono usati anche sei router, due access point Wi-Fi e cinque switch da 128 ingressi, più uno switch da 8 ingressi. Inoltre abbiamo utilizzato cavi di tipo UTP per collegare i computer agli switch, due cavi STP per connettere il Centro di Ricerca e l'Amministrazione e il Centro di Calcolo con quello di Manutenzione, due cavi in fibra ottica per connettere il Centro di Sviluppo con quello di Ricerca e con l'Amministrazione. Infine abbiamo connesso il Centro di Calcolo con quelli di

Ricerca e di Sviluppo usando una rete VPN.

Un router è una macchina dotata di più interfacce di rete, configurata ognuna su di una rete diversa, che gli consente di comunicare tra loro. Uno switch invece è un dispositivo di rete dotato di più porte che, ricevuto un pacchetto da una macchina collegata ad una di esse, lo inoltrano sulla porta a cui è collegato il suo destinatario.

Un cavo UTP (Unshielded Twisted Pair) è un cavo in rame facile da torcere ed adatto alle brevi distanze. Un cavo STP (Shielded Twisted Pair) invece è sempre un cavo di rame, ma schermato maggiormente. Questo lo rende più difficile da stendere, ma più resistente alle interferenze e quindi più adatto alle distanze maggiori. Un cavo in fibra ottica invece sfrutta particolari proprietà riflessive di alcuni materiali per portare un segnale ottico a grande distanza e con molta precisione.

Infine una VPN (Virtual Private Network) è una tecnologia che, sfruttando una rete pubblica come Internet, fornisce a chi la usa una connessione privata crittografata del tutto analoga ad una rete privata reale. Il suo utilizzo delle reti pubbliche la rende priva di limiti di distanza.

Questa tabella riporta tutto il materiali che abbiamo comprato per l'installazione della rete e la relativa spesa:

Componente	Modello	Numero	Prezzo cad.	Totale
Router	CISCO 2901K9	2	616€	4.684€
	CISCO 2901K9 + modulo EHVIL 4 porte	1	836€	
	CISCO 2901K9 + modulo EHVIL 4 porte + modulo fibra ottica	3	872€	
Switch 128 porte	2 x CISCO 2968S-F48FPS-L (switch 48 porte) + CISCO WSC290S-F24PS (switch 24 porte) + 3 x FLEX STACK-S (connettore)	5	6205€	31.025€
Switch 8 porte	CISCO SG200	1	270€	270€
Cavo UTP	cat.6	516 (8m l'uno ca.)	1.17€ al m	4.829,76€
Cavo STP	cat.7	50 m + 100 m	1.44€ al m	216€
Fibra ottica		800 m + 800 m	6€ + 20 per scavo al m	41.600€
Access Point WiFi	CISCO WAP321	2	169,52€	339.04€

La spesa totale delle componenti è di 82.963,80€, più il costo del servizio che è 40.000€, per un totale di 122.963.80€.

N.B. La configurazione riportata non è mai stata provata su una rete concreta.