# Guida Utente


## Centro Servizi per la Ricerca
**Università di Pisa**
**Dipartimento di Informatica**

**Guida Utente**

Centro Servizi per la Ricerca

# Sommario

# Lista delle Tabelle

# Introduzione

Questo documento descrive i servizi per l'utente messi a disposizione dal Centro Servizi per la Ricerca. Per i servizi piú importanti vengono riportati alcuni dettagli di configurazione e implementativi. Le versioni stampabili di questo documento sono disponibili in formato *rtf* (UserGuide.rtf) e *pdf* (UserGuide.pdf)

Questa documentazione ha anche lo scopo di fornire il punto di partenza per le discussioni sui futuri miglioramenti. Conoscere dettagliatamente la situazione attuale è essenziale per pianificare adeguatamente lo sviluppo del Centro e i servizi per gli utenti.

Suggerimenti o consigli riguardanti questa guida sono benvenuti e vanno indirizzati al servizio *help* (mailto:help@di.unipi.it).

# Capitolo 1. Servizi

## 1.1. Account

Il Centro mantiene un servizio centralizzato via web di gestione account. I sistemi Linux del dominio sono stati suddivisi in gruppi, denominati laboratori. Ogni laboratorio individua i sistemi che fanno parte di un determinato gruppo di ricerca. I laboratori attuali sono:

**Tabella 1-1. Laboratori**

| Nome | Home Server | Responsabile |
|---|---|---|
| dipartimento | osiris | Direttore Centro email (mailto:cdcdir@di.unipi.it) |
| agents | medialab | G. Attardi email (mailto:attardi@di.unipi.it) |
| medialab | medialab | G. Attardi email (mailto:attardi@di.unipi.it) |
| oikos | saladin | C. Montangero email (mailto:monta@di.unipi.it) |
| logic | strudel | F. Scozzari email (mailto:scozzari@di.unipi.it) |
| ldb | caronte | F. Turini email (mailto:turini@di.unipi.it) |
| fibonacci | datatop | G. Ghelli email (mailto:ghelli@di.unipi.it) |
| optimize | dantzig | A. Frangioni email (mailto:frangio@di.unipi.it) |
| p4 | paperino | M. Danelutto email (mailto:marcod@di.unipi.it) |
| neurolab | neuron | A. Micheli email (mailto:micheli@di.unipi.it) |
| inti | tosca | G. Ferrari email (mailto:giangi@di.unipi.it) |
| oipaz | tosca | G. Ferrari email (mailto:giangi@di.unipi.it) |

Ad ogni un nuovo account viene assegnata una classe, un laboratorio principale, zero, uno o piú laboratori aggiuntivi. La classe determina le modalità di accesso al File System Distribuito mentre i laboratori permettono l'uso dei sistemi dei laboratori.

Indipendentemente da queste caratteristiche il nuovo account ottiene i seguenti servizi:

- **Home** la home viene creata sull'home server del laboratorio principale (vedi tabella). Su tutti gli home server sono attivi i servizi per l'accesso alla home:
  - **ssh (scp)**
  - **Lan Manager (samba)**, utilizzabile per accedere alla home dai sistemi Windows e MacOs, mediante il path di rete *server**homes*

    **Nota:** Il sistema traduce automaticamente *homes* con nome di login utilizzato per il collegamento

> **Avvertimento**
>
> Il laboratorio *dipartimento* (server osiris) prevede una quota utente predefinita di **400 MB**. Per modificare tale valore rivolgersi al servizio di assistenza, specificando i motivi della richiesta.

- **Home Page** (vedi Home Pages)
- **E-mail** al nuovo account sono associati i seguenti indirizzi:
  - **user@di.unipi.it**
  - **Nome.Cognome@di.unipi.it** a meno di omonimie
  - **NCognome@di.unipi.it** a meno di omonimie

  In caso di omonimie verranno concordati con l'utente alias alternativi. Da notare che il sistema e-mail è "case unsensitive", quindi a sinistra del carattere '@' può essere utilizzata qualsiasi combinazione di lettere maiuscole o minuscole.

- **Iscrizione alla mailing list dipartimento** la consultazione dell'archivio e le opzioni associate alla propria iscrizione possono essere effettuate via Web alla URL Lista Dipartimento (https://mailserver.di.unipi.it/mailman/listinfo/dipartimento)
- **servizio di dump** vedi la sezione Servizio Dump

## 1.1.1. Classi di utenti

Sono attualmente definite le seguenti classi di utenti:

**Tabella 1-2. Classi di utenti**

| Classe | Descrizione | Gruppo Unix |
|---|---|---|

| Classe | Descrizione | Gruppo Unix |
|---|---|---|
| Personale | Personale docente e tecnico/amm.vo del Dipartimento | personal |
| Dottorandi | Iscritti alla scuola di dottorato | dottor |
| Ospiti | Visitatori temporanei | ospiti |
| Borsisti | Borsisti presso il Dipartimento | borsisti |
| Contrattisti | Consulenti con contratto con il Dipartimento | contract |
| Studenti | Tesisti | studenti |
| Collaboratori | Collaboratori del Dipartimento | collabor |
| Speciali | Account di gestione dei progetti | special |

La classe utente viene scelta in base alla qualifica del titolare del nuovo account e può essere cambiata secondo specifiche esigenze (vedi modifica account).

## 1.1.2. Profili utente

Le procedure di gestione account installano i profili utenti presenti sul server di laboratorio, ossia il contenuto della directory `/etc/skel` del sistema dove viene creata la home. Questo consente all'amministratore locale di personalizzare gli account del proprio laboratorio installando nella directory `/etc/skel` dell'home server profili personalizzati per i propri utenti. In particolare, il comando eseguito dalla procedura account è il seguente:

```
cp /etc/skel/.[a-z]* ~user
```

La shell di default associata agli account è **/bin/csh** e non è consentito cambiare questo valore nel database distribuito. Sui sistemi linux /bin/csh è solitamente un link a **/bin/tcsh**, quindi la shell di default risulta essere la tcsh (**`man tcsh`** per ulteriori informazioni). L'amministratore può modificare tale valore sul proprio sistema per dare ai propri utenti una shell di default alternativa. Ad esempio il comando:

```
root# ln -sf /bin/bash /bin/csh
```

Fa si che la shell di default per i propri utenti sia la bash (**`man bash`** per ulteriori informazioni)

### 1.1.2.1. Personalizzazione dei profili

Per personalizzare i profili è necessario stabilire quale sia la shell di default (che potrebbe variare a seconda del sistema) e creare o modificare il corrispondente file di startup. Per stabilire quale sia la shell è sufficiente utilizzare il comando:

```
ls -l /bin/csh
```

La seguente tabella riassume la situazione

**Tabella 1-3. Shells**

| Shell | Startup file |
|---|---|
| csh | `~users/.cshrc` |
| bash | `~user/.bashrc` |
| tcsh | `~user/.cshrc` |
| sh | `~user/.profile` |

Ad esempio, questo semplice `.cshrc` utilizza la bash per le sessioni interattive:

```
# .cshrc
# Non interactive
if !(${?prompt}) then
        alias rm rm -i
 alias cp cp -i
 alias mv mv -i
 exit
endif
# interactive: switch to bash if available
[ -x /bin/bash ] && exec bash
```

## 1.1.3. Cambio Password

È attivo un meccanismo di sincronizzazione che permette di avere la stessa password per i sistemi linux integrati e per i sistemi Windows del dominio.

> **Avvertimento**
>
> Questo è un servizio Web abilitato solo per la rete locale erogato attraverso il protocollo https. Se lo si vuole usare da una macchina fuori dalla rete del Dipartimento, è quindi necessario configurare l'utilizzo del proxy dipartimentale anche per il protocollo https.

Per cambiare la password:

- **Via web**: utilizzare la url  Cambio Password (http://webforms.di.unipi.it/account/pwd.html).
- In caso di problemai con la procedura Web rivolgersi ai sistemisti.

## 1.1.4. Richiedere nuovi account

La possibilità di richiedere nuovi account è limitata al personale docente e tecnico/amm.vo del Dipartimento (corrispondente alla classe *personale*). La richiesta deve essere inoltrata mediante la form disponibile all'indirizzo  http://webforms.di.unipi.it/account/aur.html (http://webforms.di.unipi.it/account/aur.shtml)

Chi richiede un nuovo account ne diviene il responsabile e può richiederne al Centro eventuali variazioni (nuova scadenza, cambio di classe, nuova quota).

> **Nota:** Il sistema non accetta richieste di accesso ad un laboratorio inoltrate da account non appartenenti al laboratorio stesso.

## 1.1.5. Modifica account

La richiesta di modifica è limitata alla scadenza, al gruppo e all'accesso ai laboratori e deve essere inoltrata:

- mediante la form disponibile all'indirizzo  http://webforms.di.unipi.it/account/mur.html (http://webforms.di.unipi.it/account/mur.shtml) per scadenza e accesso ai laboratori
- mediante la form disponibile all'indirizzo  http://webforms.di.unipi.it/account/addgroup.html (http://webforms.di.unipi.it/account/addgroup.shtml) per inserimento utente in un gruppo

> **Nota:** Il sistema non accetta richieste di inserimento di utenti in un gruppo inoltrate da account non appartenenti al gruppo stesso .

Per qualsiasi altra modifica è necesario rivolgersi direttamente al servizio di assistenza.

## 1.1.6. Rimozione account

La rimozione di un account può essere richiesta solo da chi ne è responsabile ( in genere chi ne ha richiesto la creazione)

La richiesta di rimozione di un account deve essere inoltrata mediante la form disponibile all'indirizzo http://webforms.di.unipi.it/account/elim/index.php (http://webforms.di.unipi.it/account/elim/index.php).

Il titolare dell'account riceverà una mail di avviso .In assenza di altre indicazioni l'account verrà rimosso 10 giorni dopo la richiesta.

### 1.1.7. Creazione nuovo gruppo

È possibile richiedere la creazione di un nuovo gruppo mediante la form disponibile all'indirizzo http://webforms.di.unipi.it/account/gruppo.html (http://webforms.di.unipi.it/account/gruppo.shtml)

Chi ha richiesto la creazione di un gruppo viene automaticamente inserito fra gli utenti del gruppo

## 1.2. Mail e Mailing list (Nuovo Sistema)

La lettura della posta presente nella propria mailbox è possibile da un qualsiasi sistema collegato alla rete Internet (locale o remoto) mediante qualsiasi client pop o imap che supporti la connessione sicura, utilizzando la seguente configurazione:

**Tabella 1-4. Configurazione client e-mail**

| Campo | Valore | Opzioni |
|---|---|---|
| Incoming Server (imap o pop) | imaps.di.unipi.it/pops.di.unipi.it | Connessione sicura via SSL/TLS (obbligatoria): impostare la porta 993 (nel caso di imap) o 995 (nel caso di pop3) |
| Account | il vs. account | |
| Password | la vs. password | |
| Outgoing Server (*) | smtp.di.unipi.it | Autenticazione (LOGIN PLAIN), Connessione sicura via TLS |

**Nota: (*)** l'autenticazione è sempre necessaria. In caso di autenticazione attiva è consigliata la modalità sicura (vedi smtp.di.unipi.it con autenticazione )

L'accesso diretto alla propria mailbox, per motivi di sicurezza, al momento è consentito unicamente usando l'applicazione squirrelmail accessibile alla url https://www.di.unipi.it/webmail-1/src/login.php

### 1.2.1. Forward (Nuovo Sistema)

La gestione del Forward è possibile via web, mediante il servizio WebMail.

**Avvertimento**

Attenzione: gli utenti Microsoft Exchange/Outlook Web Access NON devono utilizzare il servizio WebMail sul mailserver principale per la gestione del vacation e forward. Le operazioni corrispondenti vanno eseguite unicamente mediante Outlook Web Access (https://exchange.di.unipi.it/owa)

Via webmail è sufficiente selezionare il menu *Filters* (o la pagina *Message Filters* all'interno del menu *Options*), inserire una nuova regola che specifichi come azione *Redirect* e riempire opportunamente i campi visualizzati.

> **Nota:** Per escludere dall'inoltro i messaggi sospetti di contenere spam e/o virus è sufficiente far precedere la regola che esegue l'azione *Redirect* da una che seleziona i messaggi marcati come sospetta spam o virus e ne previene il trattamento da parte di quelle successive: per ottenere questo risultato basta selezionare la checkbox *Stop* tra le *Additional Actions*

### 1.2.2. Vacation (Nuovo Sistema)

La gestione del Vacation è possibile via web, mediante il servizio WebMail.

**Avvertimento**

Attenzione: gli utenti Microsoft Exchange/Outlook NON devono utilizzare il servizio WebMail sul mailserver principale per la gestione del vacation e forward. Le analoghe operazioni vanno eseguite unicamente mediante Outlook Web Access (https://exchange.di.unipi.it/owa)

Via WebMail è sufficiente selezionare il menu *Filters* (o la pagina *Message Filters* all'interno del menu *Options*), inserire una nuova regola che specifichi come azione *Vacation/Autoresponder* e riempire opportunamente i campi visualizzati.

> **Nota:** Per evitare di inviare risposte automatiche ai messaggi sospetti di contenere spam e/o virus è sufficiente far precedere la regola che esegue l'azione *Vacation/Autoresponder* da una che seleziona i messaggi marcati come sospetta spam o virus e ne previene il trattamento da parte di quelle successive: per ottenere questo risultato basta selezionare la checkbox *Stop* tra le *Additional Actions*

## 1.2.3. Webmail (Nuovo Sistema)

L’accesso via web è disponibile alla url:

- Webmail (via Squirrermail ) (https://www.di.unipi.it/webmail-1/).

Per gli utenti Microsoft Exchange l’analogo servizio è disponibile alla url Outlook Web Access (https://exchange.di.unipi.it/owa).

> **Nota:** Il servizio è offerto mediante connessione sicura (protocollo https).

## 1.2.4. Servizio Antispam/Antivirus (Nuovo Sistema)

Il sistema di posta elettronica, implementa un servizio Antispam/Antivirus centralizzato. Il servizio tenta di riconoscere i messaggi spam e infetti e li marca, modificandone il campo "subject" in modo da permettere agli utenti che lo desiderino di creare dei filtri di gestione personalizzati.

Il subject dei messaggi riconosciuti come spam viene modificato aggiungendo il prefisso *{Spam?}* (o *{Spam?}{high-Spam?}* se la probabilità che il messaggio contenga spam è prossima alla certezza).

Il subject dei messaggi che contengono uno o piú allegati infetti viene modificato aggiungendo il prefisso *{Virus?}*. Il messaggio originale viene disinfettato (rimuovendo gli allegati identificati come malware) e inoltrato al destinatario sotto forma di allegato, preceduto da un messaggio di sistema, contenente una serie di informazioni che possono essere utili (nel caso di falsi positivi) ad accedere agli allegati rimossi.

Il subject dei messaggi che contengono uno o piú costrutti potenzialmente molto pericolosi ma non catalogabili con certezza come virus (ad esempio costrutti che scaricano automaticamente il contenuto di file remoti alla visualizzazione del messaggio, aggirando così il sistema antivirus) viene modificato aggiungendo il prefisso *{Disarmed}*. Il messaggio originale viene "disarmato" (ossia i costrutti interessati vengono sostituiti con altri meno pericolosi) e inoltrato al destinatario. Questa operazione può incidere sulla presentazione del messaggio.

In nessun caso, spam o virus, il sistema avvisa il mittente apparente (ormai quasi tutti gli spammer e i virus usano effettuare lo *spoofing* dell’indirizzo mittente) per non generare ulteriori messaggi indesiderati. In nessun caso il sistema scarta i messaggi riconosciuti spam, delegando al destinatario finale il compito di gestirli in modo opportuno.

## 1.2.5. Gestione automatizzata dei messaggi

I messaggi di posta elettronica in arrivo possono essere, fino ad un certo livello, gestiti in maniera automatica grazie alla possibilità di impostare *filtri* che selezionano i messaggi a cui associare semplici azioni (tipicamente il salvataggio in sottocartelle diverse) di trattamento degli stessi.

Nel seguito tratteremo questo argomento con riferimento specifico a come gestire i messaggi catalogati dal sistema centralizzato Antispam/Antivirus, ma le funzionalità illustrate in questo modo sono disponibili per trattare messaggi selezionati sulla base di una molteplicità di diversi attributi (ad es., sulla base del mittente).

### 1.2.5.1. Configurazione di filtri locali al client dell'utente

È possibile creare filtri sul proprio lettore di posta specificando di spostare in altri folder tutti i messaggi il cui subject *inizia* per {Spam?}, {Spam?}{high-Spam?}, [SPAM] o {Virus?}. Tutti i lettori di posta evoluti permettono di creare filtri in modo semplice. Per questa operazione si rimanda alla documentazione (è sufficiente l'help online) di ogni specifico client utilizzato.

**Nota:** Il prefisso [SPAM] è utilizzato dal Centro Serra, che funge da mailserver secondario.

**Nota:** Questi filtri sono applicati ai messaggi dallo specifico tool di lettura e al momento in cui i messaggi vengono letti, quindi se si accede alla propria posta elettronica attraverso piú client (es.: uno in ufficio ed uno a casa) e si usa questo tipo di filtri, ciascun client applicherà i filtri specifici che vi sono impostati.

**Avvertimento**

Se il client usa il protocollo IMAP e mantiene i messaggi sul server, gli accessi successivi (dal medesimo o da altri client) vedranno l'effetto dell'applicazione dei filtri.

### 1.2.5.2. Configurazione di filtri sul server

Il server di gestione della posta in arrivo implementa un sistema di filtraggio della posta basato sul linguaggio standard Sieve (http://tools.ietf.org/html/rfc5228). L'implementazione supportata è quella fornita da pigeonhole (http://pigeonhole.dovecot.org/).

Questi filtri, a differenza dei precedenti, sono indipendenti dal lettore di posta utilizzato e vengono applicati direttamente dal server all'arrivo di ogni messaggio. Ciò si rivela decisamente efficace se si accede alla propria mailbox da postazioni e con modalità diverse. Il vantaggio diventa particolarmente evidente se non si dispone di un collegamento veloce (o a pagamento) perché i filtri evitano di dover scaricare tutti i messaggi riconosciuti spam o virus.

Inoltre, il fatto che questi filtri (e le azioni associate) siano applicati al momento del recapito del messaggio nella mailbox ed indipendentemente dall'accesso dell'utente li rende utilizzabili per operazioni piú sofisticate come, ad esempio, l'invio di risposte automatiche.

Per attivare questi filtri è possibile collegarsi al server di posta elettronica utilizzando il servizio WebMail selezionare il menu *Filters* (o la pagina *Message Filters* all'interno del menu *Options*), e inserire una o piú regole che specifichi l'azione a cui si desidera che il messaggio sia sottoposto e riempire opportunamente i campi di dettaglio visualizzati.

Ad esempio per impostare un filtro che specifica azioni che si applicano solo ai messaggi marcati come spam (dal servizio centralizzato del Dipartimento o da SerRA) è necessario impostare la seguente condizione:

- Condizione tra le regole che seguono: *OR*
- Prima regola: *Message::Header::Subject::matches regexp::^\{Spam\?\}.**
- Seconda regola: *Message::Header::Subject::matches regexp::^\[Spam\?\].**

Se, invece di "matches regexp", si usasse "contains" si tratterebbero anche i messaggi il cui subject contiene una delle stringhe di marcatura (non piú interpretata come espressione regolare) anche in posizione diversa da quella iniziale.

**Nota:** NOTA 1: Nel caso di filtri che si riferiscono a messaggi contenenti Spam/Virus suggeriamo di scegliere come azione *Move to Folder* o *Discard* (a seconda del risultato desiderato).

## Avvertimento

Nel caso sopra non scegliere MAI *Reject* per evitare di intasare i nostri server o di inviare spam ad indirizzi che siano stati soggetti a spoofing

**Nota:** NOTA 2: per evitare che un messaggio già trattato da una regola del filtro sia passato a quelle successive selezionare la checkbox *Stop* tra le *Additional Actions*

Tra le *Actions*, la *Keep Message* corrisponde a non far nulla (il messaggio viene recapitato in locale come avverrebbe se la regola non ci fosse) ma può essere utile nella definizione di strategie complesse di gestione dei messaggi: ad esempio se ci interessa applicare al messaggio una delle *Additional Actions*

Tra le *Additional Actions*, la *Notify* permette di inviare brevi avvisi rispetto alla ricezione di messaggi importanti ad eventuali altri indirizzi di servizio.

#### *1.2.5.2.1. Come leggere le mail spostate in cartelle diverse dalla INBOX dai filtri sul server*

Per chi usa il protocollo imap è sufficiente iscriversi (subscribe) ai folder utilizzati nei filtri sul server.

Chi non usa il protocollo imap (ma il protocollo pop3) può utilizzare il servizio Webmail e dal menu *Cartelle* selezionare le cartelle interessate e premere il pulsante *aggiungi una cartella*. Le nuove cartelle sono ora selezionabili dal menu a lista in alto a sinistra per visualizzarne il contenuto.

#### *1.2.5.2.2. Uso avanzato dei filtri*

Il sistema antispam assegna ad **ogni** messaggio un punteggio (spam score). Solo i messaggi con un punteggio superiore ad un certo limite di sistema (attualmente 3.5 per la marca *{Spam?}* e 7 per la marca *{Spam?}{high-Spam?}*) vengono classificati spam, con la modifica del subject.

Gli utenti hanno però la possibilità di utilizzare il punteggio spam per creare un filtro personale piú (o meno) aggressivo. In questo modo si aumenta (o riduce) la percentuale di spam catturato dal filtro ma si aumenta anche la propabiltà di un falso positivo (una mail non spam classificata spam), o di un falso negativo. Se si desidera un filtro personale piú sensibile si possono definire regole che tengano conto del punteggio attribuito, filtrando i messaggi sulla base del contenuto del campo dell'header *X-dipinformatica-mailscanner-spamscore*. Infatti, il punteggio di cui sopra è approssimato per difetto dal numero di caratteri *s* che costituiscono il valore di questo campo: ad esempio, il valore *ss* corrisponde ad un punteggio di spam compreso tra 2 e 2.999.

> **Nota:** Per avere lo stesso effetto intervenendo solo nel client di posta è necessario che quest'ultimo sia in grado di creare filtri classificando i messaggi con l'header specifico *X-dipinformatica-mailscanner-spamscore*

#### *1.2.5.2.3. Eliminazione automatica dei messaggi*

**Avvertimento**

QUESTA CONFIGURAZIONE È SCONSIGLIATA. Il Centro non può in nessun modo recuperare eventuali messaggi persi a causa di questa configurazione nè essere considerato responsabile di eventuali danni.

Se si stanno utilizzando i filtri sul server e si desidera eliminare in modo automatico i messaggi selezionati dal filtro (ad esempio, quelli marcati spam o virus) è sufficiente associare al filtro opportuno, l'azione *Discard*.

Se si stanno utilizzando i filtri del lettore di posta è sufficiente specificare la rimozione anziché la registrazione in folder dedicato.

Se si desidera comunque diminuire il numero di messaggi spam da controllare si consiglia di eliminare automaticamente solo quelli a punteggio spam elevato (marcati {Spam?}{high-Spam?}).

#### *1.2.5.2.4. Filtri antispam personali*

Il sistema antispam centralizzato è compatibile con qualasiasi filtro personale. Il sistema centralizzato fa un uso limitato del motore bayesiano (analisi del contentuto del messaggio), perché è risultato impossibile (per ora) trovare un modo realmente efficace per "addestrarlo" in maniera fine. Un filtro antispam personale, se adeguatamente addestrato, può rendere maggiormente efficace il riconoscimento di spam, concentrandosi sui messaggi non riconosciuti dal filtro centralizzato.

## 1.2.6. Invio della posta elettronica e relay dall'esterno (smtp autenticato)

Per poter inviare la posta elettronica da un client personale è necessario impostare come server della posta in uscita l'indirizzo *smtp.di.unipi.it* e attivare l'autenticazione smtp nel proprio sistema personale (client) di gestione della posta di posta (menu relativo alla configurazione del server smtp o outgoing server, tipo di autenticazione *LOGIN PLAIN*) e attivare il collegamento sicuro (**TLS** o meglio, se disponibile, **STARTTLS** specificando le porte TCP/443 o TCP/25). In questo caso l'uso di TLS è **obbligatorio** altrimenti la vostra password può essere intercettata.

Quando tenterete di inviare un messaggio, il sistema vi chiederà di fornire il vostro username e password registrati presso il Dipartimento. Senza autenticazione il sistema si rifiuta di spedire (funzione antirelay) e ritorna l'errore *Relay denied*.

La configurazione adottata permette di separare le valutazioni sulla legittimità dell'invio della posta dalla locazione (all'interno o all'esterno della rete dipartimentale) della macchina usata per l'invio e di associarla, invece, all'identificazione (autenticata) del mittente il messaggio. **In questo modo il server smtp del dipartimento** (nome dns *smtp.di.unipi.it*) **potrà essere utilizzato anche quando non si è collegati alla rete locale** (ad esempio in trasferta).

Inoltre, al momento, non sono noti virus/spambot che siano in grado di gestire/aggirare il protocollo di autenticazione utilizzato dal server smtp e diffondere spam attraverso di esso: se le password personali sono ben protette, l'adozione dell'autenticazione previene la possibilità che il server finisca nelle blacklist di Internet (con tutto ciò che ne consegue).

> **Nota:** Tutti i lettori hanno la possibilità di memorizzare la password (cosa che, comunque, sconsigliamo) evitando di doverla specificare ad ogni sessione.

> **Avvertimento**
>
> Alcuni gestori di rete, per limitare gli abusi originati da macchine collegate alla propria rete restringono l'uso di Internet a pochi servizi (impedendo, tra le altre, le connessioni in uscita destinate alla porta TCP/25, quella standard per il protocollo smtp, quello usato per la "posta in uscita"). Non possono però, per ovvie ragioni, limitare l'accesso ai servizi web. L'effetto pratico è che non si riesce a spedire posta dal proprio client, configurato in modo "standard". Webmail può essere sempre usato in tutte le sue funzionalità.
>
> In questi casi, se si vuole continuare ad usare il proprio client, è necessario modificare le impostazioni del proprio client **scegliendo come porta di destinazione del protocollo smtp la TCP/443 (e sicurezza "STARTTLS")** corrispondente, secondo gli standard, al protocollo https.

> **Avvertimento**
>
> **L'autenticazione è sempre necessaria**, anche quando si è collegati alla rete locale.

## 1.2.7. Mailing List

Il servizio è realizzato usando il tool Mailman (http://www.gnu.org/software/mailman/index.html). L'accesso a questo servizio è completamento guidato via web. La pagina di partenza è la url Mailing List (https://mailserver.di.unipi.it/mailman/listinfo) dalla quale è possibile effettuare tutte le usuali operazioni legate a questo servizio (consultazione archivi, iscrizione/deiscrizione, preferenze dell'utente) o accedere all'interfaccia di gestione (solo amministratori).

**Nota:** Il servizio è offerto mediante connessione sicura (protocollo https).

### 1.2.7.1. Amministrazione di una lista

L'attuale versione di mailman mette a disposizione dell'amministratore e del moderatore tutti gli strumenti necessari per gestire in modo efficace una lista. In particolare sono stati potenziati gli strumenti per la moderazione e il controllo dei messaggi indesiderati.

Tra le numerose opzioni a disposizione dell'amministratore vale la pena segnalare le seguenti, che possono rivelarsi estremamente utili in caso di numerosi post indesiderati (spam,virus)

- **Moderazione per singolo utente**: è possibile attivare (liste non moderate) o disattivare (liste moderate) la moderazione di un singolo utente, agendo sul flag *moderato* dell'utente nel menu *Gestione iscritti*.
- **Filtri sul mittente**: è possibile settare un'azione di default per gli utenti moderati (sospendi, rigetta o scarta) e per gli utenti non iscritti (accetta, sospendi, rigetta o scarta) utilizzando il menu *Opzioni per la Privacy -> Filtri sul mittente*.
- **Filtri antispam**: è possibile utilizzare il sistema antispam/antivirus centralizzato per scartare automaticamente i messaggi marcati spam o contenenti virus. Per attivare questi filtro utilizzare il menu *Opzioni per la Privacy -> Filtri antispam*, inserendo queste 2 regole:

```
Regola Anti-spam 1

 Espressione Regolare
         Anti-spam:  X-MailScanner-SpamScore: sssss
            Azione:  Scarta

Regola Anti-spam 2

 Espressione Regolare
         Anti-spam:  X-MailScanner: Found to be infected
            Azione:  Scarta
```

**Avvertimento**

Attenzione: il numero di caratteri **"s"** nella prima regola è 5, che corrisponde allo score spam di sistema. Abbassando il numero di **"s"** si ottiene un filtro piú aggressivo per l'eliminazione dello spam. Usare quest'ultima possibilità con estrema cautela perché i messaggi vengono automaticamente scartati.

- **Gestione delle richieste pendenti**: è possibile eliminare tutte le richieste pendenti settando il flag *Discard all messages marked Defer* del menu *Controlla richieste amministrative pendenti*

Per ulteriori informazioni si rimanda alla documentazione on line e alla Home Page di Mailman (http://www.gnu.org/software/mailman/index.html).

### 1.2.7.2. Nuove liste

**Avvertimento**

Questa operazione può essere effettuata solo accedendo da una macchina all'interno della LAN del Dipartimento di Informatica

La richiesta di una nuova lista deve essere inoltrata mediante la form disponibile all'indirizzo http://webforms.di.unipi.it/Lista/lista.html (http://webforms.di.unipi.it/Lista/lista.html)

Una volta creata la nuova lista, il sistema manda automaticamente un mail all'owner con tutte le informazioni necessarie per la personalizzazione e la gestione della lista. I gestori sono tenuti a considerare che le liste vengono create coi seguenti valori di default:

- *Archiviazione abilitata con accesso pubblico*
- *Iscrizione alla lista previa conferma e approvazione*
- *Invio dei messaggi ristretto agli iscritti* (i messaggi inviati da non iscritti vengono sospesi in attesa di azione dell'amministratore o del moderatore).
- *Moderazione non attiva*
- *Nessuna descrizione della lista*

In caso di difficoltà o per qualsiasi ulteriore informazione è possibile rivolgersi al servizio di assistenza.

## 1.3. Web

Il Centro gestisce il server Linux che ospita il web server dipartimentale *www.di.unipi.it*. Il Centro si occupa del corretto funzionamente e aggiornameto del server ma non è responsabile dei contenuti del sito, per i quali occorre fare riferimento alla Commissione Web (mailto:wwwadm@di.unipi.it). Per accedere al materiale pubblicato è possibile utilizzare uno dei seguenti metodi:

- La directory `/share/doc/Web`, disponibile **unicamente** sul server **osiris.di.unipi.it**
- Mediante il servizio Lan Manager (i dettagli sono illustrati nel prossimo paragrafo), utilizzando il path (\\server\risorsa) *\\www.di.unipi.it\www*

I diritti di accesso in scrittura dipendono dalle credenziali di accesso (username,password) utilizzate.

### 1.3.1. Home Pages

Il servizio di Home Page è garantito per tutti i possessori di account del dominio. La home page è pubblicata automaticamente all'indirizzo *www.di.unipi.it/~utente*. Il file iniziale deve avere una dei seguenti estensioni: **index.html index.htm index.php index.shtml Index.html Index.htm Index.php** (direttiva *DirectoryIndex*).

**Avvertimento**

Il sistema prevede una quota utente predefinita di **500 MB**. Per modificare tale valore rivolgersi al servizio di assistenza, specificando i motivi della richiesta.

#### 1.3.1.1. Gestione dalla Home Page

Per creare o modificare la propria Home Page è sufficiente salvare il proprio materiale nello spazio dedicato, accessibile nei seguenti modi:

- **Dalla Rete Locale o da Internet:** da qualsiasi indirizzo Internet è possibile utilizzare uno dei seguenti metodi:
  - collegarsi al webserver per le operazioni di upload e download mediante i seguenti progammi:
    - **Windows**: utilizzare il programma free **WinScp** (download WinScp (http://winscp.net/eng/download.php)) indicando:
      - Server: *www.di.unipi.it*
      - Directory: *public_html*
      - User e password: *i vostri username e password di dominio*
    - **Sistemi Linux e MacOs**: su questi sistemi è possibile utilizzare i comandi **scp, sftp o rsync**, ad esempio:

```
>scp file.html [user@]www.di.unipi.it:public_html    (copia file.html nella home page)
>rsync file.html [user@]www.di.unipi.it:public_html  (copia file.html nella home page)
>sftp [user@]www.di.unipi.it:public_html             (apre una sessione interattiva)
```

**Nota:** Il seguente comando sincronizza la dir public_html sul webserver con una directory public_html gestita localmente:

```
> rsync --delete -a public_html [user@]www.di.unipi.it:
```

**Nota:** Esistono tool grafici simili a WinScp per MacOs. Consigliamo il tool free **Fugu**, disponibile alla seguente url download Fugu (http://rsug.itd.umich.edu/software/fugu/download.html)

  - è anche possibile utilizzare la url Servizio WebFTP (https://www.di.unipi.it/webftp) fornendo le proprie credenziali di accesso (username/password registrate presso il dominio locale). Il servizio utilizza il protocollo sicuro *https* e consente le operazioni di upload/download del materiale della propria home page, registrato nella directory *public_html*.
- **Dalla rete locale:**
  - Via NFS (servizio NON autenticato) alla directory `/share/doc/WebHome/utente/public_html`, disponibile **unicamente** sul server **osiris.di.unipi.it**

**Nota:** Per semplicità d'uso il sistema provvede a creare automaticamente nelle home utente il link simbolico `public_html`

- Mediante il servizio **autenticato** Lan Manager (protocollo **smb**), utilizzando il path (\\server\risorsa) *www.di.unipi.it**homes**public_html* :
  - **Windows**: indicare *www.di.unipi.it**homes**public_html* in uno dei seguenti modi alternativi:
    - url di Internet Explorer
    - folder del menu *Map Network Driver*
    - argomento del menu *Start:Run*
  - **MacOs**: utilizzare il menu *Go:Connect to Server* indicando come Server Address *smb://www.di.unipi.it/homes/public_html*
  - **Linux**: in ambiente gnome è possibile utilizzare il menu *Places:Connect To Server* (corrispondente al comando *nautilus-connect-server*) indicando:
    - Service Type: *Windows share*
    - Server: *www.di.unipi.it*
    - Share: *homes*
    - Folder: *public_html*

    oppure montare il fs remoto mediante i comandi:

    ```
    >su
    Password: indicare la password di root
    #/usr/bin/smbmount //www.di.unipi.it/homes /mnt/www -ousername=user
    Password: indicare la password di user
    ```

    ed accedere come utente root alla dir /mnt/www. In questo caso il sistema assegna permessi sulla directory montata in accordo allo username utilizzato.

    **Nota:** Il sistema traduce automaticamente *homes* con nome utente utilizzato per il collegamento. Se il nome utilizzato sul sistema locale è diverso dal quello registrato sul server occorre specificarlo.

#### *1.3.1.1.1. Protezione degli accessi*

Le pagine possono essere protete creando nella directory che le contiene un file `.htaccess` e il relativo file di password. Ad esempio, per proteggere la url *http://www.di.unipi.it/~utente/protetta* con credenziali di acesso utente/password, creare il file `public_html/protetta/.htaccess`:

```
AuthType Basic
AuthUserFile /share/doc/WebHome/utente/public_html/protetta/passwords
```

```
AuthName "Area protetta"
Require valid-user
```

e il relativo file di password mediante i comandi:

```
cd ~utente/public_html/protetta
/usr/bin/htpasswd passwords utente (il sistema richiede la password)
chmod 444 passwords
```

e testare il risultato provando ad accedere alla url. Il sistema deve rispondere mediante un pop-up dove fornire username e password.

> **Nota:** Il comando **`htpasswd`** è disponibile sul server osiris.

#### *1.3.1.1.2. Redirezioni*

È possibile redirigere la propria home page o qualsiasi altra url. Per fare questo è sufficiente creare un file `index.html` nella directory contenente la url da redirigere di questo tipo:

```
<html>
  <head>
    <title>Redirecting</title>
    <META HTTP-EQUIV="Refresh"
      CONTENT="3; ❶  URL=http://..❷..">
  </head>
  <body>
    <br><br><br>
   <center>
     This page is being redirected.
     <br>
       (Click <a href="http://..❸..">here</a> if automatic redirection fails)
   </center>
  </body>
</html>
```

❶ 3: tempo (in secondi) di visualizzazione del messaggio

❷ url di redirezione

❸ url di redirezione

#### 1.3.1.2. Altre pubblicazioni

Oltre alla Home Page è possibile richiedere alla Commissione Web (mailto:wwwadm@di.unipi.it) la pubblicazione di altri spazi, indirizzabili come *www.di.unipi.it/nome*, ad esempio siti dedicati a gruppi di ricerca, eventi, collaborazioni, o qualsiasi altra attività legata al Dipartimento.

### 1.3.2. Http Proxy

È attivo un proxy http con cache all'indirizzo *proxy.di.unipi.it*, porta 8080. L'uso del proxy prevede autenticazione.

#### 1.3.2.1. Servizi Web ad accesso ristretto

Dalla rete locale è consentita la navigazione diretta quindi l'uso del proxy non è necessario. È però indispensabile se si vuole utilizzare dall'esterno un servizio Web abilitato solo per la rete locale. Ad esempio, per accedere ai servizi del Centro (gestione account, registrazione MAC Address) o per il servizio di *Library on Line*.

**Avvertimento**

Alcuni servizi ad accesso ristretto sono erogati attraverso il protocollo https, è quindi necessario configurare l'utilizzo del proxy anche per questo protocollo. La configurazione si ottiene abilitando ed utilizzando il campo "SSL Proxy" in Firefox 3.6.x, mentre viene effettuata di default in IE8.

#### 1.3.2.2. Navigazione sicura

Il servizio Poxy consente una navigazione sicura mediante l'utilizzo del sistema antivirus centralizzato. Il proxy impedisce il download e l'accesso a documenti contenenti virus mostrando una pagina di avviso. In caso di operazioni di download viene salvata in locale la pagina di avviso in sostituzione del documento richiesto.

## 1.4. Ftp

Il servizio ftp, sia anonimo che autenticato è ormai da considerarsi obsoleto e può essere sostituito totalmente dai servizi web (pubblicazione) e ssh/scp (download/upload).

# 1.5. Dns

Il Centro gestisce il servizio di naming per il dominio *di.unipi.it*. La sottorete assegnata al dominio è la *131.114.2.0/23*. Il server principale è *nameserver.di.unipi.it*, corrispondente all'indirizzo *131.114.3.6*. Gli altri server autoritativi sono *ns2.di.unipi.it*, indirizzo *131.114.3.12* e il name server fuori zona *nameserver.unipi.it*, indirizzo *131.114.21.15* (Centro Serra).

## 1.5.1. Richiesta di nuovi indirizzi (indirizzi fissi)

Per richiedere la registrazione di nuovo indirizzo è sufficiente mandare mail all'indirizzo help@di.unipi.it (mailto:help@di.unipi.it) specificando:

- **Nome:** il nome da assegnare al sistema; in caso di nome già registrato sarà concordato un nome alternativo.
- **Tipo:** indicare il tipo di macchina e il sistema (o i sistemi in caso di boot multiplo) operativo utilizzato; se si tratta di un sistema linux specificare anche la distribuzione.
- **Responsabile:** l'indirizzo e-mail del responsabile del sistema.

## 1.5.2. Dhcp (indirizzi dinamici)

È attivo un servizio DHCP dipartimentale con 64 indirizzi. Per utilizzare il servizio è necessario registrare il proprio MAC (hardware address della scheda Ethernet), utlizzando la url Registrazione MAC per DHCP (https://www.di.unipi.it/DHCP/dhcp.php). La pagina di registrazione richiede autenticazione e fornisce informazioni su come individuare il MAC Address nei vari sistemi operativi.

Il servizio consente di effettuare registrazioni con o senza scadenza. Le registrazioni con scadenza vengono automaticamente cancellate e sono pensate per autorizzazioni temporanee concesse ad ospiti o studenti del Dipartimento. Il servizio consente inoltre, mediante il pulsante *Visualizza*, di verificare e cancellare le registrazioni fatte con le proprie credenziali.

**Avvertimento**

Se non vengono fornite indicazioni (o se le indicazioni non sono esatte) circa l'identità dell'utilizzatore la resposabilità di tutte le attività riconducibili alla registrazione è a carico del richiedente.

**Nota:** Il servizio DHCP configura automaticamente i client con i parametri corretti della rete locale (name server, default gateway, netmask.)

# 1.6. Dialup (collegamenti via modem)

Il servizio dial-up è fornito dal Centro Serra ed è disponibile per tutti gli utenti di ateneo (vedi Servizio Dialup di Ateneo (http://www-serra.unipi.it/servizi/dial-up.html)). Il servizio di assistenza fornisce comunque un help desk di primo livello per questo servizio.

> **Nota:** Il Centro Serra fornisce anche il servizio di collegamento via ADSL (vedi Servizio ADLS di Ateneo (http://www-serra.unipi.it/servizi/adsl.html)).

Per usufruire del servizio è necessario:

1. scaricare, stampare, leggere e compilare il modulo di assunzione di responsabilità disponibile all'indirizzo Centro Serra Servizio Dial-up (http://www-serra.unipi.it/moduli/modulo_dial-up.html )
2. consegnare il modulo alla Segreteria Amministrativa del Dipartimento.
3. attendere comunicazione via e-mail per l'attivazione del servizio e i relativi codici di accesso.

**Tabella 1-5. Configurazione client e-mail via Serra**

| Campo | Valore | Opzioni |
|---|---|---|
| Incoming Server | **imap.di.unipi.it/pop.di.unipi.it** | Pop o Imap (consigliato SSL) |
| Account | il vs. account presso il dipartimento | |
| Password | la vs. password presso il dipartimento | |
| Outgoing Server | **mixer.unipi.it** oppure smtp.di.unipi.it con autenticazione | |

## 1.6.1. Collegamento da altri Provider

Se si utilizza un altro Provider occorre fare attenzione al servizio mail perché non è possibile utilizzare il server di ateneo (dial-up.unipi.it) per la spedizione dei messaggi a causa della protezione antirelay (vedi antirelay). Occorre quindi definire come server SMTP (Outgoing Server) quello indicato dal provider stesso o il server del Dipartimento smtp.di.unipi.it con autenticazione(vedi mailserver con autenticazione). È invece sempre possibile utilizzare il server del Dipartimento per leggere la propria mailbox. In questo caso si consiglia fortemente l'uso di connessioni sicure (imap o pop con SSL).

# 1.7. Dump

Il servizio dump è in fase di ristrutturazione. Attualmente è realizzato mediante i tool Amanda (http://www.amanda.org/), per sistemi Linux, e Veritas Backup (http://www.veritas.com/) per i sistemi Windows. I dettagli tecnici e le informazioni utili per l'utente del nuovo servizio verranno pubblicati appena sarà reso operativo.

## 1.7.1. Richieste di Restore

Attualmente la richiesta di restore deve essere inviata via mail all'indirizzo help@di.unipi.it (mailto:help@di.unipi.it) specificando nome del sistema e path completo del materiale da recuperare. È necessario anche specificare se il ripristino deve essere fatto utilizzando l'ultima copia disponibile o versioni precedenti.

## 1.7.2. Il nuovo servizio

Gli obbiettivi della riorganizzazione di questo servizio sono:

- **MacOsX**: estendere il servizio ai sistemi MacOsX.
- **Backup on Demand**: possibilità di eseguire un backup del proprio sistema su richiesta. Questo servizio permetterà di supportare adeguatamente i sistemi portatili.
- **Restore utente**: possibilità dell'utente di eseguire i restore dei propri dati senza interagire con servizio di assistenza. Questo permetterà di velocizzare le operazioni e di eseguire i restore anche fuori dall'orario di assistenza o durante i periodi di chisura del Centro.
- **Potenziamento risorse hardware**: rendere disponibili risorse hardware sufficienti per estendere il servizio a tutti i sistemi locali.

# 1.8. Stampe

Il Centro mantiene un servizio di stampa centralizzato, che utilizza le seguenti risorse:

**Tabella 1-6. Risorse di stampa**

| Nome Stampante | Modello | Locazione |
|---|---|---|
| lj2 | HP LaserJet 9000 PS (Postscript) | Room 296b DE |

| Nome Stampante | Modello | Locazione |
|---|---|---|
| lj3 | HP LaserJet 9000 PS (Postscript) | Room 317 D0 |
| lj5 | Rico Aficio 2051 PCL | Room 284 DE |
| lj6 | HP LaserJet 4515n | Room 284 DE |
| lj7 | HP LaserJet 4515n | Room 329b DO |

**Nota:** Le due multifunzione Xerox sono state dotate di firmware postscript e sono utilizzabili anche in ambiente mac e linux.

È stata introdotta la possibilità di eseguire scansione su email. Il massimo formato previsto è A3, in modalità monocromatica con scala di grigi a 16bit.

## 1.8.1. Configurazione dei client

- **Sistemi Unix/Linux**: nei sistemi integrati le stampanti sono automaticamente configurate. Per i sistemi non integrati utilizzare il comando:

  ```
  system-config-printer
  ```

  indicando:

  - Queue name: il nome della stampante (es lj1)
  - Short description (opzionale): modello e locazione
  - Queue type: Networked JetDirect, port 9100 (default)
  - Printer model: il modello corrispondente

- **Sistemi Windows**: il nodo di accesso è *\\printers.di.unipi.it* ed è accessibile previa autenticazione .

  **Nota:** Sono diponibili i driver sia Postscript che PCL per ogni stampante a eccezione della lj5 (Aficio).

  Una volta reinstallato il driver è necessario controllare che l'opzione fronteretro sia abilitata.

- **Sistemi Mac**: utilizzare il comando:

  ```
  Application:Utility:PrintCenter
  ```

  indicando:

  - IP PRINTING
  - il nome della stampante completo di dominio (es: lj1.di.unipi.it)
  - il modello corretto e il driver corrispondente.

Per le stampanti Lj6 e Lj7 selezionare il Driver di stampa ESP Modello ( HP LaserJet Series Cups v1.1 )

**Importante:** Assicurarsi sempre di aver impostato A4 come formato di stampa.

# 1.9. Sicurezza

Il Dipartimento ha approvato da tempo una Politica di Sicurezza per i sistemi delle Segreteria Ammi.va. Questi sistemi sono protetti mediante firewall. Non esiste invece una Politica di Sicurezza per il resto della rete dipartimentale. In mancanza di questa sono state adottate una serie di protezioni basate sul "buon senso", nel tentativo di ridurre il rischio di intrusione sui sistemi.

Le successive sezioni descrivono le caratteristiche essenziali della "Politica di Sicurezza" per il Dipartimento

## 1.9.1. Protezione degli accessi

- **Connessioni uscenti** (Da Rete Locale a Internet): **nessuna limitazione**
- **Connessioni entranti** (Da Internet a Rete Locale): vengono trattate in modo differente in base al servizio (porta). In particolare per tutti gli host sono abilitati i seguenti servizi (porte):

**Tabella 1-7. Connessioni entranti**

| Servizio | Porta | Protocollo |
|---|---|---|
| ssh | 22 | tcp |
| http | 80 | tcp |
| https | 443 | tcp |
| telnet | 23 | tcp |
| Windows Remote Desktop | 3389 | tcp |

**altri servizi :** È possibile, per specifiche esigenze, richiedere l'abilitazione di alcuni servizi (porte). La richiesta va inviata all'indirizzo help@di.unipi.it (mailto:help@di.unipi.it) indicando: Nome della macchina, servizio, porta/protocollo, sorgente. Ad esempio:

```
Nome del sistema: nomesistema
Servizio: Mysql
Porta: 3306/tcp, 3306/udp
Sorgente: 131.114.x.x
```

```
Nome del sistema: nomesistema
Servizio: Real Time Stream Control Protocol (rtsp)
Porta: 554/tcp
Sorgente: any
```

> **Avvertimento**
>
> Se possibile è consigliato specificare una sorgente per diminuire i potenziali rischi di intrusione.

- **Connessioni entranti** (livello di Ateneo- Rete Universitaria): questa parte viene gestita dal Centro Serra. Attualmente sono bloccati i seguenti servizi (porte):

**Tabella 1-8. Servizi bloccati**

| Servizio | Porta | Protocollo |
|---|---|---|
| netstat | 15 | tcp |
| finger | 79 | tcp |
| link | 87 | tcp |
| supdup | 95 | tcp |
| pop2 | 109 | tcp |
| news | 144 | tcp |
| exec | 512 | tcp |
| openwin | 2000 | tcp |
| bootp | 67/68 | udp |
| tftp | 69 | udp |
| snmptrap | 162 | udp |
| biff | 512 | udp |
| printer | 515 | udp |
| route | 520 | udp |
| radius-old | 1645/1646 | udp |
| echo | 7 | tcp/udp |
| systat | 11 | tcp/udp |
| daytime | 13 | tcp/udp |
| quotd | 17 | tcp/udp |
| chargen | 19 | tcp/udp |
| time | 37 | tcp/udp |
| tacacs | 49 | tcp/udp |
| nbios-ns | 137 | tcp/udp |
| nbios-dgm | 138 | tcp/udp |

| Servizio | Porta | Protocollo |
|---|---|---|
| nbios-ssn | 139 | tcp/udp |
| netware-ip | 396 | tcp/udp |
| timed | 525 | tcp/udp |
| mountd | 635 | tcp/udp |
| wins | 1512 | tcp/udp |
| nfs | 2049 | tcp/udp |

Questi servizi possono quindi transitare all'interno della Rete di Ateneo ma vengono bloccati se provenienti dall'esterno.

Tutte le informazioni riguardanti le porte ufficiali assegnate ai servizi Internet sono disponibili presso la Internet Assigned Numbers Authority (http://www.iana.org)

## 1.9.2. Antispoofing

La funzionalità antispoofing impedisce che il traffico in ingresso/uscita sia volontariamente "camuffato" per aggirare le regole di filtraggio. Opera in due sensi:

- **Dall'interno verso l'esterno** impedisce l'uscita dei pacchetti con source address non appartenente alla sottorete ufficialmente assegnata al Dipartimento (131.114.2.0/23)
- **Dall'esterno verso l'interno** impedisce l'ingresso dei pacchetti con source address appartenente alla rete del Dipartimento

Si tratta dunque di una misura che non ha alcun effetto sul normale utilizzo dei servizi.

## 1.9.3. Antirelay

La funzionalità antirelay riguarda il servizio di posta elettronica ed è utile ricordare che è una forma di controllo ormai **obbligatoria**. Non adottarla significa infatti avere la certezza di essere individuati e classificati come potenziali fonte internazionale di spam. In questo caso la conseguenza è l'impossibilità di comunicare via posta elettronica con tutti i domini Internet che adottano l'antirelay (e sono ormai la maggiornaza).

La funzione antirelay impedisce a tutti gli indirizzi internet **non esplicitamente autorizzati** l'uso dei server SMTP (sendmail) per **spedire a destinatari non appartenenti al/ai dominio/i e-mail di propria competenza**. Non interessa invece la lettura della mailbox mediante i protocolli pop, imap (o i corrispondenti spop, simap) che è disponibile (previa autenticazione) per tutti i sistemi interni ed esterni.

Nella configugurazione del server smtp del Dipartimento la funzionalità di relay è garantita agli indirizzi della rete locale e al resto degli indirizzi internet mediante l'uso dell'autenticazione (vedi

smtp.di.unipi.it con autenticazione )

## 1.9.4. Connessioni sicure (comandi s*)

### 1.9.4.1. Sistemi Linux

Su tutte le distribuzioni Linux sono presenti i comandi s* (ssh, slogin, scp) che consentono di effettuare collegamenti e copie di file in modo sicuro (criptato). I comandi sostituiscono i vecchi r* (rsh, rlogin, rcp) e telnet.

### 1.9.4.2. Sistemi Windows

È disponibile il tool **Putty**, un client ssh/telnet/rlogin. Per installarlo sul vostro PC è sufficiente scaricarlo da PuTTY Download Page (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html)

### 1.9.4.3. Sistemi MacOsX

È disponibile di default il tool **ssh** .Per connettersi via ssh al Mac è necessario attivare il servizio:

- Aprire System Preferences
- Selezionare Sharing e attivare Remote Login

## 1.9.5. Personal Firewall

La complessità delle esigenze legate alle attività del Dipartimento rende difficile perfezionare una politica di sicurezza realmente efficace. In mancanza di una deguata protezione centralizzata è consigliabile l'uso di firewall personali, come ad esempio accade automaticamente sui sistemi Windows XP aggiornati al Service Pack 2. Per i sistemi Linux Fedora è ora possibile attivare protezioni basate su Firewall (**`iptables`**) e SELinux. Per ulteriori dettagli si rimanda alla sezione *Livello di sicurezza* della Guida di installazione (http://www.di.unipi.it/internaldoc/InstallFedora7/InstallFedora7.html) e alla documentazione Microsoft Understanding Windows Firewall (http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.msp)

**Avvertimento**

L'uso di firewall personali non crea normalmente alcun problema sui sistemi client ma può complicare notevolmente la corretta configurazione dei sistemi server.

# 1.10. Collegamento alla rete locale

I sistemi possono essere collegati alla rete locale con due modalità: rete fissa (wired) e rete mobile (wireless). Il metodo di indirizzamento può essere con ip statico o dinamico per la rete wired e dinamico per la rete wireless.

## 1.10.1. Rete wired

Le prese utente sono collegate a switch con porte 100 Mb full duplex. Se la presa non è attiva (segnalata dalla mancanza del link sulla scheda di rete) è sufficiente richiederne l'attivazione al servizio di assistenza, specificando l'identificativo che compare sulla presa (un'etichetta del tipo: BE18-1).

Se si desidera usare l'indirizzamento dinamico è sufficiente registrate il MAC Address (vedi Registrazione MAC) e non è necessario specificare nessun altro parametro di rete. Se si usa un indirizzo statico occorre invece occorre impostare la seguente configurazione:

- **Primary Name server IP**: 131.114.3.6
- **Secondary Name server IP**: 131.114.3.12
- **Gateway IP**: 131.114.3.2
- **NetMask**: 255.255.254.0 (corrispondente a /23)

## 1.10.2. Rete wireless

Esistono 2 reti distinte, con diverse modalità di accesso e servizi. Le reti si annunciano all'interno del Dipartimento coi seguenti identificativi (SSID):

- **Computer.Science**: per gli utenti registrati presso il dominio o per singoli ospiti e collaboratori del Dipartimento.
- **Guest.Di.Unipi.it**: per gli ospiti del Dipartimento e per tutti gli utenti in possesso delle Credenziali di Ateneo. Questa rete è pensata per gestire in modo efficace eventi quali seminari e conferenze, ossia situazioni che prevedono un alto numero di utenti con accesso limitato alla durata dell'evento.

### 1.10.2.1. Servizi e modalità di accesso

- Rete **Computer.Science**: questa rete non prevede alcuna limitazione per l'uso dei servizi Intranet/Internet. In altre parole i servizi sono gli stessi previsti per la rete wired.

  I parametri di configurazione per accedere alla rete sono:

  - **Network Name (SSID)**: Computer.Science
  - **Data Encryption**: WPA PSK

- **Passphrase**: qazxswedc
- **Authentication IEEE 802.1x**: disabled
- **TCP/IP**: IP e DNS automatico

  **Importante:** Per collegarsi deve essere registrato il MAC Address (vedi Registrazione MAC). Per gli osptiti temporanei è sufficiente creare una registrazione MAC con scadenza.

- Rete **Guest.Di.Unipi.it**: La connessione a questo SSID non necessita di alcuna registrazione DHCP e l'autenticazione è affidata al servizio di captive portal. **Gli utenti dotati di credenziali di Ateneo possono usarle per autenticarsi al captive portal e accedere a Internet senza alcuna ulteriore formalità** . Per effettuare registrazioni, si prega di inviare una mail al support help, specificando la data e durata dell'evento, responsabile ed in allegato in formato testo (Nome, Cognome) l'elenco dei partecipanti.

  I parametri di configurazione per ottenere l'associazione agli AP della rete sono:

  - **Network Name (SSID)**: Guest.Di.Unipi.It
  - **Data Encryption**: WPA PSK
  - **Passphrase**: cdewsxzaq
  - **Authentication IEEE 802.1x**: disabled
  - **TCP/IP**: IP e DNS automatico

    **Importante:** Se si usano le credenziali di Ateneo per autenticarsi al captive portal è necessario specificare nello username il dominio **unipi.it**. Ad esempio, il titolare dell'account di Ateneo a001234 dovrà usare:

    - **Username**: a001234@unipi.it
    - **Password**: <password della credenziale di ateneo>

## 1.11. Servizi di Multi-video Conferenza

Il Dipartimento dispone di un servizio di multivideoconferenza usato (in modo sperimentale) da marzo 2011.

Il servizio (qui (http://master1.di.unipi.it/) potete vedere la pagina di accesso personalizzata per la Scuola di Dottorato Galileo Galilei), basato sul software opensource BigBlueButton (http://www.bigbluebutton.org), consente di condurre piú videoconferenze indipendenti in parallelo, ciascuna con un numero arbitrario (entro i limiti dell'hardware) di partecipanti. Non richiede l'installazione di hardware software specifico sulle macchine usate dagli utenti: è sufficiente un browser web dotato di player flash, microfono ed eventuale webcam per chi interviene attivamente.

L'accesso al sistema (e a ciascuna videoconferenza) avviene attraverso l'uso di **username** e **password** personali. Nella fase sperimentale del servizio, tenuto conto dei limiti delle risorse disponibili è necessario prenotare lo svolgimento dell'attività (e richiedere le credenziali per gli eventuali ospiti) scrivendo a help@di.unipi.it (mailto:help@di.unipi.it).

## 1.12. Installazioni del sistema operativo

Il Centro offre un servizio di installazione dei sistemi operativi Linux/Fedora e Windows XP Professional. Copia dei cdrom di installazione (Fedora boot, XP versione inglese e italiana) e istruzioni (Fedora) sono depositati presso la Segreteria Ammnistrativa.

> **Importante:** Tutto il personale del Dipartimento può liberamente installare Windows XP (e tutti gli altri sistemi operativi Microsoft) sui propri sistemi (vedi MSDNAA). Occorre tener presente questa possibilità quando si acquistano nuovi PC, evitando, se possibile, la spesa relativa alla licenza del sistama operativo.

> **Importante:** Le funzionalità descritte di seguito sono realizzabili solo con la versione **Professional** di XP.

### 1.12.1. Linux Fedora

È attivo un servizio di installazione di rete, utilizzando un mirror locale, aggiornato con frequenza giornaliera, della distribuzione Fedora. Su richiesta inoltre il sistema può essere configurato in modo automatico per il corretto accesso alle risorse e servizi di dominio (sistemi integrati). Le informazioni sono reperibili alla url Guida di installazione (http://www.di.unipi.it/internaldoc/InstallFedora7/InstallFedora7.html).

#### 1.12.1.1. Altre distribuzioni linux

Il Centro garantisce il corretto utilizzo dei servizi locali solo per installazioni Fedora integrate. Prima di installare altre distribuzioni, nel caso ci sia l'esigenza di utilizare servizi di rete locali, suggeriamo di contattare il servizio di assistenza per una corretta valutazione.

## 1.12.2. Integrazione sistemi Windows XP (join di dominio)

Dopo l'installazione via CD è possibile integrare il sistema con i servizi dipartimentali mediante la join al dominio *INFORMATICA*. Questo permette un uso piú semplice delle risorse e servizi locali e la configurazione automatica delle stampanti e di alcune impostazioni di sistema per l'interazione coi sistemi Linux locali.

> **Avvertimento**
>
> La join di dominio è **sconsigliata** per sistemi con indirizzamento **dinamico (dhcp)**, ad esempio i portatili (vedi prossimo paragrafo).

Per eseguire la join procedere nel seguente modo:

1. accedere al sistema con diritti di amministratore locale
2. selezionare *Control Panel:System*
3. selezionare il tab *Computer Name (Nome Computer)*
4. utilizzare pulsante *Network ID (ID di Rete)* per attivare il wizard di configurazione. Di seguito saranno descritte le scelte da eseguire:
   - **This computer is a part of a business network, and I use it to connect to other computer at work**
   - **My company uses a network with a domain**
   - immettere i seguenti dati:

     ```
     User name: proprio account dipartimentale
     Password:  password account dipartimentale
     Domain:    INFORMATICA
     ```

   - immettere i seguenti dati:

     ```
     Computer name:   il nome del sistema assegnato dal Centro
     Computer Domain: INFORMATICA
     ```

   - immettere (nuovamente!) i seguenti dati:

     ```
     User name: proprio account dipartimentale
     Password:  password account dipartimentale
     Domain:    INFORMATICA
     ```

     Se i dati forniti sono corretti la procedura esegue la join e chiede quali diritti assegnare all'utente sul sistema locale (*Administrator, Restricted user o Standard user*) . In questo modo si può ottenere il controllo completo del sistema locale col proprio account dipartimentale.

Per ulteriori informazioni si rimanda alla documentazione Microsoft disponibile alla url Aggiunta e protezione del computer client in un dominio (http://www.microsoft.com/italy/pmi/sicurezza/sgc/articles/xpwinnet.mspx#EHDAC).

**Nota:** La join di dominio permette di accedere senza ulteriore richiesta di autenticazione alle risorse del dominio *INFORMATICA*. Per accedere alle risorse disco sui sistemi Linux senza dover fornire le credenziali di accesso ad ogni sessione si può utilizzare la procedura descritta in
Gestione della password

## 1.12.3. Sistemi Windows XP non integrati (notebook, sistemi con indirizzamento dinamico)

Per i sistemi non integrati (es portatili) si possono ottenere analoghi benefici della join per l'uso delle risorse dipartimentali, utilizzando le seguenti configurazioni:

- **Gestione passwords**
  - selezionare *Control Panel:User Accounts*
  - selezionare il vostro account in uso sul sistema (può differire dall'account dipartimentale)
  - selezionare ora il menu *Menage my network passwords*
  - Tramite il pulsante *Add* aggiungere una entry con i seguenti dati:

    ```
    Server: *.di.unipi.it
    User name: informatica\account (il vs account dipartimentale)
    Password: la password dell'account dipartimentale
    ```

- **Stampanti**: vedi Stampe da sistemi Windows
- **Accesso alle risorse disco su sistemi Linux**: se si desidera accedere a risorse disco gestite da server linux (ad esempio la home directory) è necessario abilitare le *Plain Text Password*.. Una utile url per eseguire la modifica al Registry in modo automatico è la seguente:  Enable Plain Text Passwords (http://www.willamette.edu/wits/resources/docs/network/home/plaintextpassword.htm)

## 1.12.4. Installazione assistita

In caso di difficoltà è possibile contattare il servizio di assistenza per prenotare un'installazione a cura del personale del Centro. Il sistema dovrà essere consegnato presso l'ufficio degli amministratori fornito di tutte le periferiche (ad esclusione del monitor) e della documentazione di corredo.

# 1.13. Servizi specifici

Oltre ai servizi presentati nelle precedenti sezioni esistono servizi specifici, legati al particolare sistema operativo in uso. Di seguito vengono presentati i principali.

## 1.13.1. Sistemi Linux

Per i servizi specifici per sistemi Linux si rimanda alla Guida di installazione (http://www.di.unipi.it/internaldoc/InstallFedora7/InstallFedora7.html), con particolare riferimento alla sezioni *Mirror locale, Livello di sicurezza, Integrazione, Aggiornamenti*.

## 1.13.2. Sistemi Windows

- **Exchange** è possibile spostare la propria casella di posta sul server Microsoft Exchange. Per farlo è necessario inviare una mail di richiesta all'indirizzo help@di.unipi.it (mailto:help@di.unipi.it).
- **Antivirus** il Centro mantiene un servizio antivirus centralizzato basato su software Trend Micro (http://www.tremdmicro.com). Per attivare il servizio è sufficiente utilizzare la url (accessibile solo dalla rete locale e con autenticazione) Installazione OfficeScan (http://antivirus.di.unipi.it) (vedi *Install Office Scan Client*). Una volta completata l'installazione, occorre segnalare l'operazione al servizio di assistenza, indicando i fondi sui quali addebitare la licenza (circa 9 Euro/anno) per conferma o la richiesta di deinstallazione, regionevolmente entro una settimana.

  **Nota:** Una volta installato l'antivirus NON può essere deinstallato/disattivato dall'utente.

- **Microsoft Academic Alliance** il Dipartimento ha attivato il programma MSDNAA. Si tratta di un catalogo software comprendente i sistemi operativi e tutti i piú comuni strumenti di sviluppo. Tutti i prodotti compresi nel catalogo possono essere liberamente installati dal personale del Dipartimento per attività accademiche. I CD di installazione vanno richiesti al servizio di assistenza. Per ulteriori informazioni si rimanda alla url *Microsoft MSDNAA Home (http://www.msdnaa.net)*.

  **Importante:** La Suite OFFICE NON fa parte del programma MSDNAA. Copia dei cd di installazuione in versione inglese e italiana sono depositati presso la Segreteria Amministrativa. Per l'utilizzo di questi CD occorre indicare alla Segreteria i fondi per l'acquisto della licenza.

- **Repository locale per l' Update** servizio in fase di attivazione. L'obbiettivo è avere un sistema centralizzato per l'aggiornamento e il controllo dei sistemi integrati (dominio INFORMATICA).

### 1.13.3. Sistemi MacOsX

È attualmente in corso la riorganizzazione del supporto al sistema operativo MacOsX. L'obbiettivo è arrivare ad un'integrazione di questo sistema, in modo analogo a quanto disponibile per i sistemi Linunx/Fedora integrati. In particolare sono oggetto di questa riorganizzazione i servizi di autenticazione, stampa, dump e accesso al Network File System.

# Capitolo 2. Assistenza

## 2.1. Orari e modalità di utilizzo

Il servizio è attivo dal lunedi al venerdi dalle ore 09:00 alle ore 18:00. Le richieste di assistenza devono essere **inoltrate via e-mail** all'indirizzo help@di.unipi.it (mailto:help@di.unipi.it), specificando dettagliatamente il problema, il sistema utilizzato (nome e sistema operativo in caso di sistemi dual boot) e tutte le indicazioni utili per riprodurre il malfunzionamento.

In caso di impossibilità di utilizzo della posta elettronica contattare telefonicamente il personale (vedi Numeri Assistenza (http://www.di.unipi.it/amministrazione/cdcammin.html)).

Durante i periodi di chiusura del Dipartimento il personale del Centro assicura il monitoraggio giornaliero dei principali servizi e il servizio di assistenza utente via posta elettronica.

**Avvertimento**

Eventuali richieste inviate a indirizzi diversi (tipicamente indirizzi personali degli amministratori) saranno ignorate.

## 2.2. Gestione delle chiamate

Il servizio di assistenza si occupa e garantisce i servizi presentati in questa guida. Sono previsti 3 livelli di priorità:

- **Alta:** segnalazioni di malfunzionamenti che pregiudicano (o possono pregiudicare) il normale funzionamento dei servizi in assistenza, richieste di restore, segnalazioni di abusi o accessi illegali ai sistemi. Tempi di risposta: entro 24 ore.
- **Media:** qualsiasi richiesta o segnalazione che NON pregiudica il normale funzionamento dei servizi in assistenza. Tempi di risposta: entro 48 ore. Entro tale periodo il Centro si impegna a risolvere la chiamata oppure a fissare un intervento.
- **Bassa:** segnalazioni di malfunzionamenti per pacchetti installati direttamente dagli utenti comunque legati alle funzionalità dei servizi in assistenza. Tempi di risposta: entro una settimana lavorativa.

Qualsiasi altra segnalazione o richiesta non riguarda il servizio di assistenza, pertanto non viene garantita la risoluzione della chiamata.