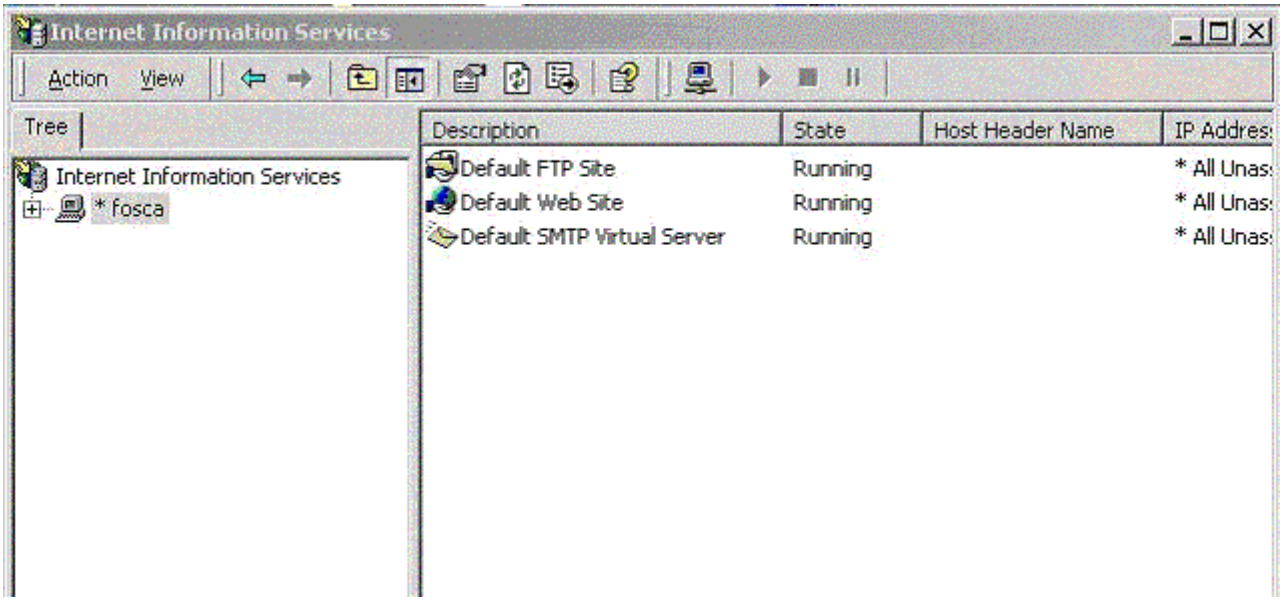
Aspetti avanzati di Microsoft IIS: Caratteristiche e Amministrazione
Amministrazione di IIS

Il ***server*** *Web* è un **processo** sempre attivo che ascolta richieste **HTTP** su una porta (80 per *default*). Su *Windows* NT un **processo** sempre attivo è chiamato servizio e viene gestito dall'amministratore di sistema dal pannello di controllo. Gestire un servizio vuol dire sostanzialmente attivarlo, fermarlo e configurarne i parametri di funzionamento. Per un *Web* ***server*** tali parametri sono:

- stabilire quali risorse devono essere viste dagli utenti;
- definire quali diritti hanno gli utenti sulle risorse del *Web* ***server***;
- definire il documento di *default* da visualizzare per ogni *directory*;
- stabilire i ***MIME*** *type* (quali applicazioni vanno associate alle estensioni dei *file*).

La finestra di amministrazione di **IIS** si apre dal pannello di controllo in NT e da Pannello di controllo > Strumenti di Amministrazione in *Windows* 2000. La *console* di amministrazione di **IIS** permette di gestire più ***server*** anche in remoto, per *default* comunque viene mostrato il ***server*** locale indicato dal nome del *computer*.



IIS mostra una *console* dalla quale si accede non solo al servizio **HTTP** ma anche **FTP** e SMTP. Cliccando su *Default Web site* troviamo tutte le cartelle che sono pubbliche nel nostro sito. Non tutto il disco della macchina su cui gira il ***server*** è visibile all'esterno, ma solo le parti che sono esplicitamente rese pubbliche da chi amministra il ***server*** *Web*. Per *default* tutte le cartelle e i *file* che stanno sotto la *directory Inetpub* sono pubbliche. L'amministratore può aggiungere altre cartelle alla lista delle *directory* visibili. Per fermare il servizio **HTTP** occorre selezionare il pulsante di *Stop*, per avviarlo sul pulsante di *Start*. Questa operazione però serve solo a fermare il funzionamento, ma il servizio rimane attivo e caricato in memoria.

Con il pulsate *Advanced*, si accede alla configurazione di siti multipla (non solo il predefinito!). Se non si specifica l'*IP address*, tutte le *directory* virtuali saranno visibili a tutti i ***server*** virtuali. In caso si installino più siti sullo stesso *Web* ***server***, è necessario utilizzare per i nomi una tra due alternative:

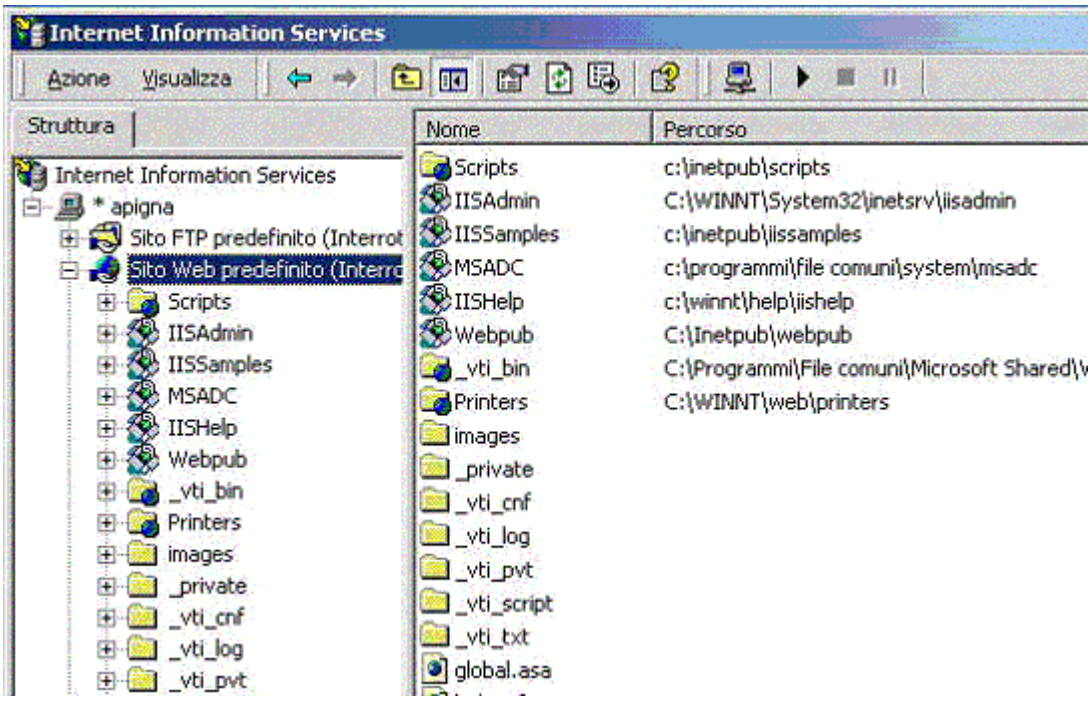
- un **indirizzo** *IP* sulla scheda di rete per ogni ***server*** virtuale.
- Una porta per ogni ***server*** su uno stesso **indirizzo** *IP*.

La prima tecnica è la più utilizzata e non richiede necessariamente *IP* pubblici.

Servizio WWW

Selezionato il sito *Web* sul quale siamo interessati a lavorare notiamo che al suo interno possono essere presenti tre tipi di oggetti:

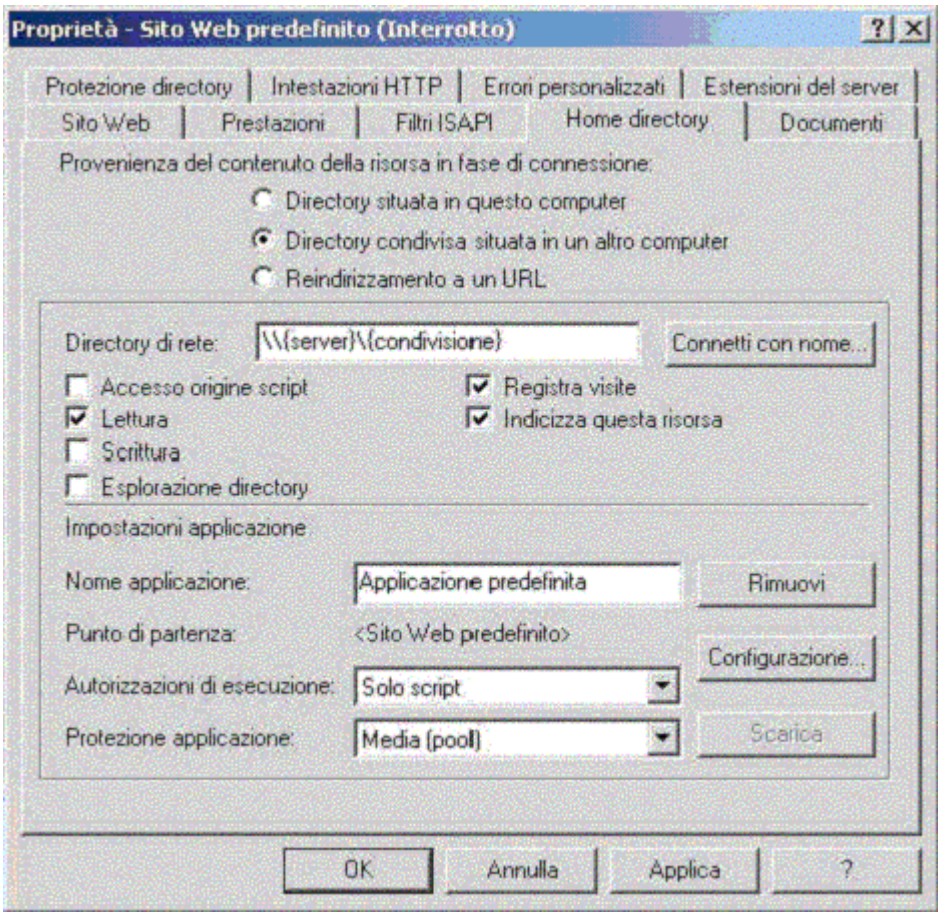
- **cartelle locali**: sono le sottocartelle normalmente presenti all'interno di *inetpub*.
- ***directory* virtuali**: definendo una *directory* virtuale *images* stabiliamo che alla **URL** http://Web.aipa.it/images corrisponda una determinata cartella nel disco del nostro ***server***, ad esempio `C:\mygifs\`. Essendo la cartella su C e non in *Inetpub* non sarebbe stata visibile dal ***server*** *Web*. Per tali cartelle è possibile definire un *alias*, ovvero un nome diverso col quale identificare la cartella su ***Internet***. Per modificare le proprietà di una *directory* virtuale già creata occorre selezionarla con il *mouse* dalla *console* di **IIS** e con il terzo bottone del *mouse* selezionare *Properties*... .
- ***Web***: sono sottocartelle speciali. Oltre a comportarsi come le cartelle virtuali, è possibile associarle ad un utente che, mediante *Front Page* può sincronizzare un proprio sito locale con un *Web*. Le estensioni del ***server*** (*Front Page Server Extension*) gestiscono il meccanismo di sincronizzazione.



La configurazione del *Web* ***server*** avviene in modo modulare: *click* destro del *mouse* e menù proprietà. Il *click* sulle cartelle permette di configurarne le proprietà. *Click* su tutto il *Web* ***server*** ne consente la configurazione globale.

Impostare le proprietà del server

Nella sezione *Documents* è possibile definire quali sono i nomi del documenti di *default*, ossia da visualizzare quando la **URL** indica la *directory* ma non specifica il documento. Ad esempio se indichiamo la **URL** http://prove.aipa.it/subdir e il documento di *default* è *index.htm* allora il ***server*** restituirà al ***client*** il documento *index.html*. Nel *tab Home directory* invece è possibile impostare il percorso locale da associare al *Web* ***server***, e la modalità alla quale accedere alle cartelle (sola lettura, esplorazione *directory*, eccetera). Le possibilità sono le seguenti:



- Una *directory* sul *filesystem* locale.
- Una *share* (in formato UNC), richiede *User/Password*. Se su dominio diverso entrambi devono avere un utente con lo stesso nome. È sconsigliato.
- Un **URL**.

Nei primi due casi è possibile settare anche:

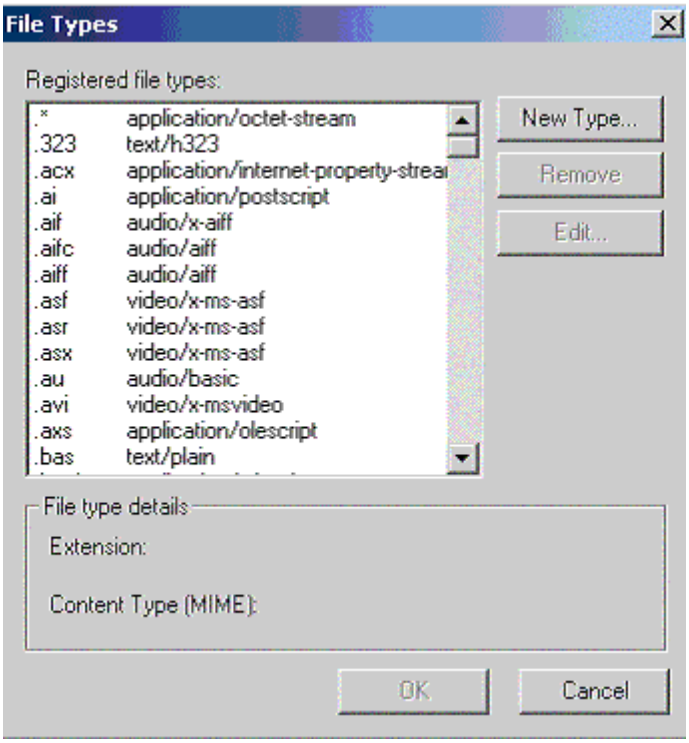
- *Permissions* da applicare. *Read* (*Default*), *Write* (necessita **HTTP** 1.1).
- *Browsing* permesso (in caso di non presenza *default page*) (a livello di sito, non di *directory*).
- *Log*, Sito indicizzato, Sito *FrontPage*.

In **IIS**, una cartella con relativi *file* e sotto-*directory*, viene definita Applicazione. È possibile collegare l'**applicazione** ad una *home page*. Si può far eseguire l'**applicazione** in uno spazio di memoria separato e dare *permission* di esecuzione:

- *None* (non esegue nulla).
- *Script* (esegue solo ***script***).
- *Execute* (esegue ***script*** ed eseguibili NT: dll, exe).

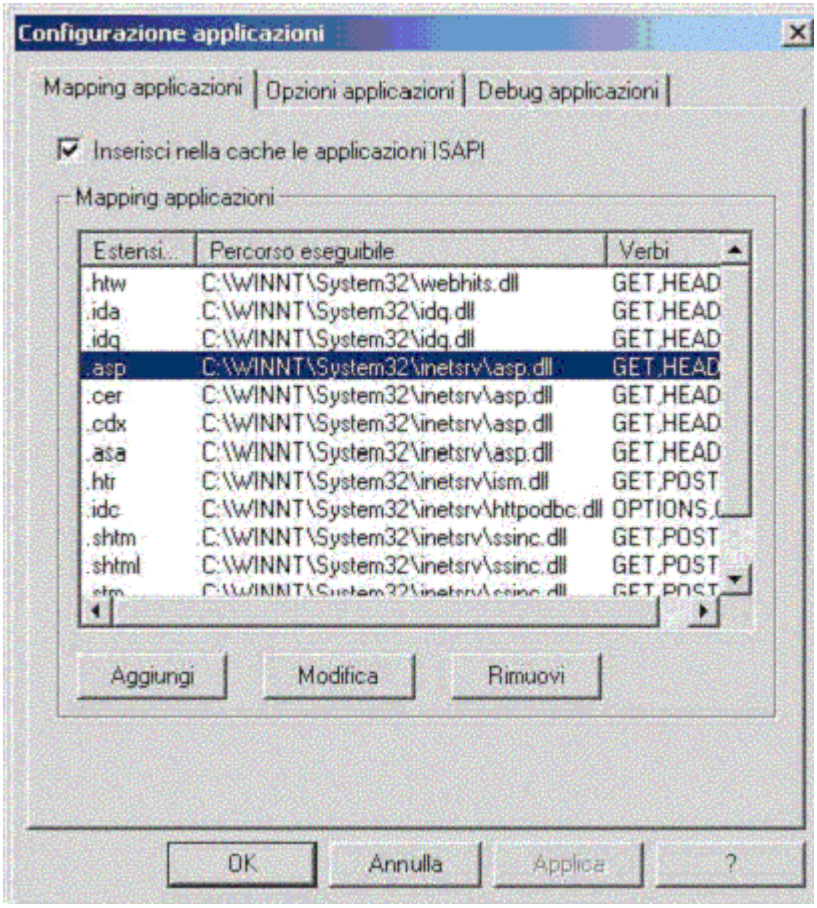
I ***MIME**-Type* invece servono al ***server** Web* per spedire al *browser* il tipo del documento. Infatti, secondo il protocollo **HTTP** assieme al documento deve essere spedito anche il tipo di questo documento (**HTML**, PDF, PS, eccetera...). Sapere il tipo del documento serve al *browser* per decidere quale azione intraprendere, cioé se parserizzare il codice e visualizzarlo (**HTML**) oppure aprire una **applicazione** esterna o un *plug-in* (PDF, PS ...). In caso il tipo del *file* ricevuto dal *browser* non sia un ***MIME**-Type* conosciuto il *browser* chiede all'utente cosa fare (salvarlo su disco...).

I ***MIME**-Type* del ***server*** *Web* si definiscono cliccando con il bottone destro del *mouse* sul nome del ***server***. Da qui si seleziona *Computer MIME Map* per definirne uno nuovo.



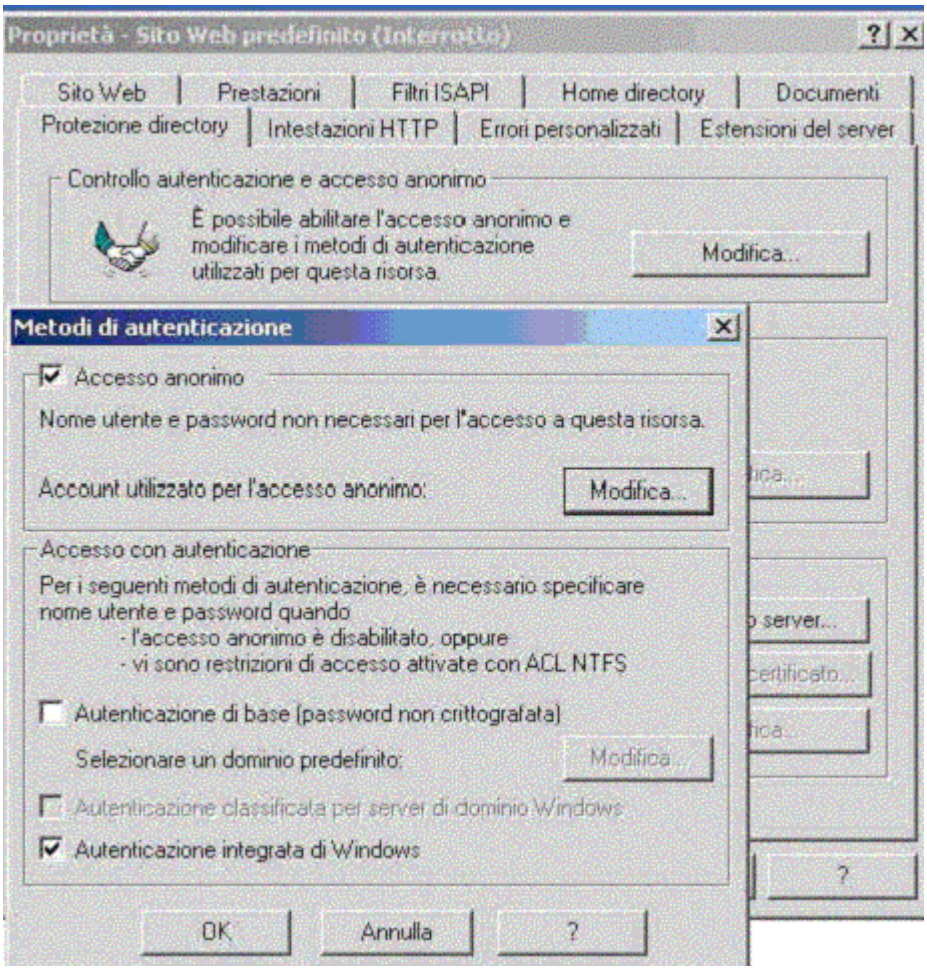
La finestra risultante visualizza tutte le estensioni ***MIME*** configurate per quel ***server*** *Web*. Con *New* possiamo definire una nuova estensione dove associamo ad una estensione del *file* un ***MIME**-Type*. Notiamo che i ***MIME*** *type* definiti qui sono validi per tutte le applicazioni del *Web* ***server***.

Filtri ISAPI: si possono aggiungere, e quindi gestire filtri. Si possono utilizzare per eseguire applicazioni remote attivate dal tipo di richiesta presente nell'**URL**. Sono DLL attivate dall'estensione dei *file*. Ad esempio richiedere al *Web* ***server*** un *file* **ASP** non solo implica lo scaricamento in locale, ma anche il filtraggio ovvero la computazione attraverso la DLL asp.dll



Directory Security

Permette di specificare l'*Access Control* alle risorse del *Web* ***server***:

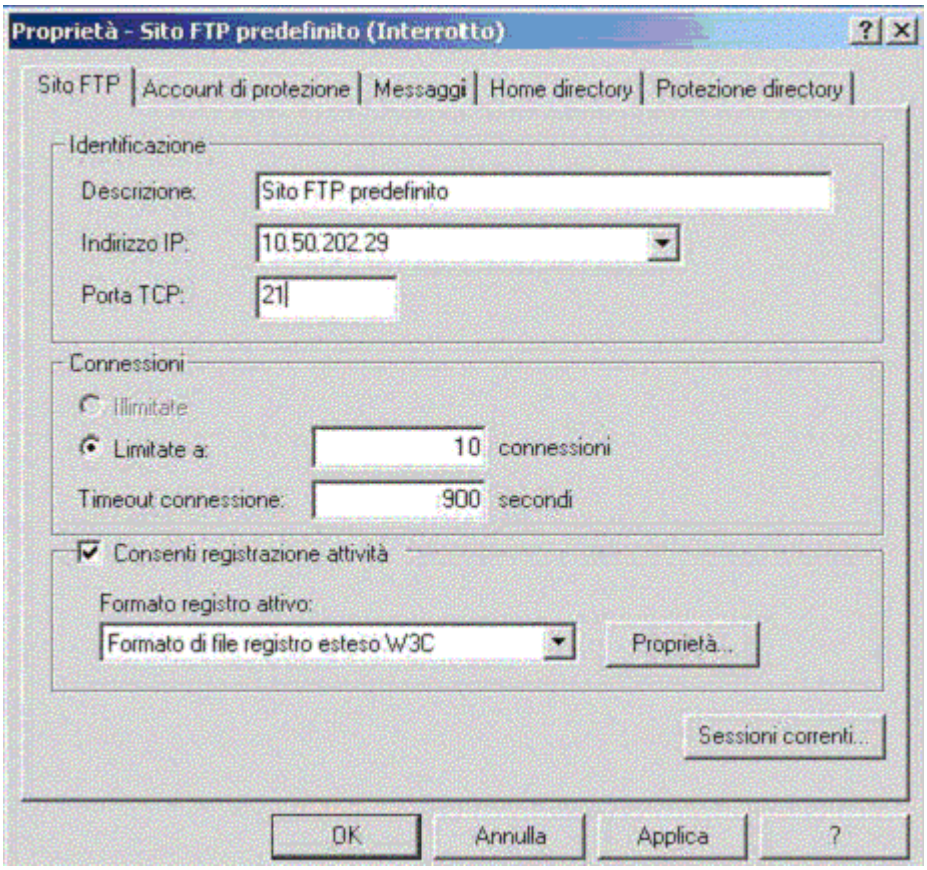


Allow ***Anonymous*** *Users* è l'opzione *default* per WWW. Viene comunque utilizzato un utente di NT, colui che fisicamente esegue i processi sulla macchina WWW. *Basic Authentication* richiede utente e *password* in chiaro utilizzando le *permission* NTFS. Richiede di disabilitare la prima opzione e richiede che l'utente esista per l'NTFS. WNT *Challeng/Response*, richiede utente e *password* criptate con l'algoritmo di NT, utilizza le *permission* NTFS e richiede di disabilitare la prima opzione.

Il servizio FTP

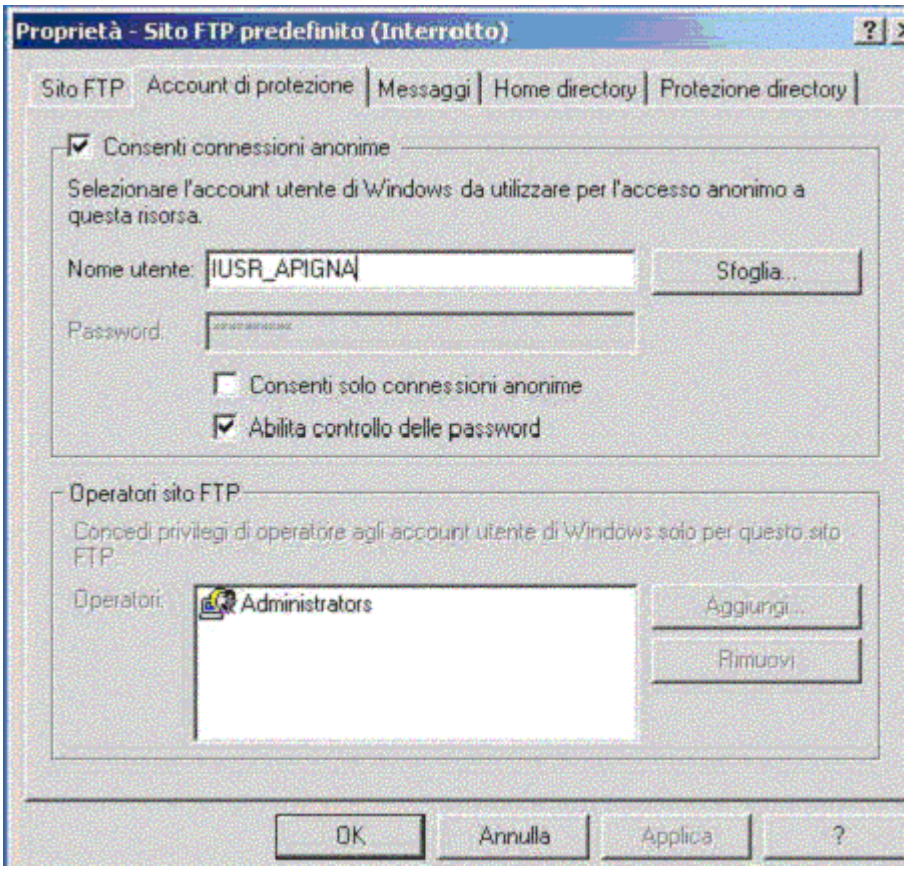
È il metodo più usato per trasferire *file* in ***Internet***. È ottimizzato perché utilizza 2 porte, una per mandare e una per ricevere. La connessione tra loro stabilita rimane attiva per tutta la sessione. Utilizza 5 *tab* di proprietà e supporta la stessa gerarchia descritta per il *Web:* `Master/Default/File`.

FTP Site: permette di specificare Nome, *IP*, Porta (21), Numero di connessioni massime e *Timeout* di sessione. Con *Current session* è possibile vedere in tempo reale l'elenco degli utenti attualmente collegati al ***server*** **FTP**.



Security Accounts: definisce la sicurezza per il sito **FTP**: con *Allow anonymous account* si dà la possibilità di connessioni anonime, ed occorre specificare l'utente/*password* di NT che verrà utilizzato per validare l'accesso.

Si può specificare di avere SOLO connessioni anonime e di sincronizzare in automatico la *password* di ***Anonymous*** con l'*account* di NT. In *Operators* si può specificare quali *account* di NT possono gestire il sito.



Messages: si possono impostare dei messaggi da inviare al ***client***. Di *default* sono vuoti: *Welcome*, *Exit* e *Maximum Connections*.

Home directory: può essere locale o remota su un'altro PC. Si può specificare se permettere Lettura, Scrittura o Entrambe e se si vuole tenere il *log* degli accessi a questa *directory*. È possibile inoltre visualizzare la *directory* in stile MS-Dos o *Unix*.

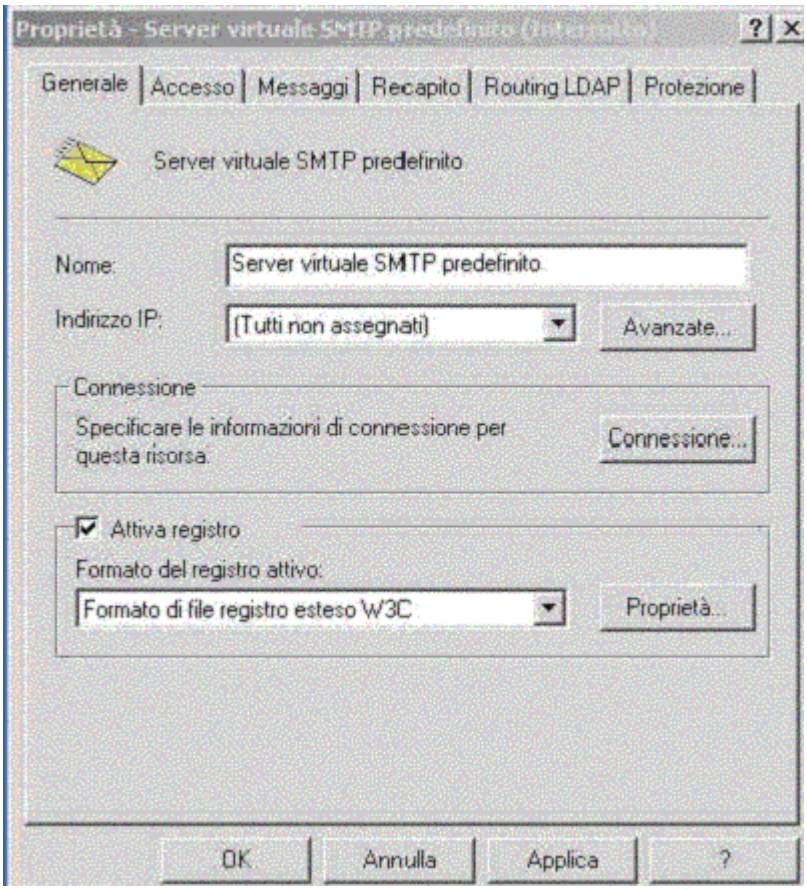
Directory Security: utilizza proprietà ed impostazioni analoghe a quelle descritte per il sito *Web*.

SMTP

Permette di gestire la posta di ***Internet*** ed è amministrabile con MMC o HTMLA. Permette di ricevere tutta la posta in arrivo e metterla in una cartella *Drop*, per ogni Dominio specifico. Per spedire i messaggi utilizza *TCP*. Si possono mettere i messaggi in una cartella *Pickup* in modo da poter essere trasferiti automaticamente.

Per ogni SMTP *Service* è possibile configurare i Domini, e visualizzare le sessioni correnti. Non viene installato di *Default*, ma dall'opzione *custom* su *Windows* NT. È installato per *default* invece su *Windows* 2000 *Server*. All'installazione crea `\Inetpub\Mailroot` e sotto di essa crea 5 altre cartelle:

- ***BadMail*** Messaggi non recapitabili.
- ***Drop*** Messaggi in arrivo. Si può spostare. Se ne può avere una per dominio.
- ***Pickup*** Messaggi in uscita. Recapitati in automatico.
- ***Queue*** Messaggi in attesa. Vengono depositati quelli che non era possibile inviare.



Funzionamento. Quando un messaggio arriva alla porta *TCP* designata o viene inserito nella *PickUp*, il messaggio viene innanzitutto inserito nella cartella *Queue*. Poi il ***server*** determina se il destinatario è locale o remoto. Se locale sposta il messaggio nella cartella *Drop* del dominio/i configurato, altrimenti viene rispedito.

Modalità di inoltro. I messaggi contenuti nella cartella *Queue* vengono ordinati per dominio e spediti in gruppo. Il ***server*** tenta di contattare il ***server*** remoto per assicurarsi che è disponibile a trasmettere, altrimenti riaccoda il messaggio. Poi vengono verificati i destinatari (se un destinatario non è raggiungibile viene generato un NDR) quindi messaggio viene spedito. Il compito di SMTP *Service* termina nel momento che il ***server*** remoto conferma la ricezione del messaggio. Se è stata abilitata la cifratura **SSL**, il ***server*** cripta i messaggi in uscita.

Attenzione! Mettere in Pausa il servizio SMTP siginifica non accettare connessioni ***client*** ma continuare l'inoltro di posta ai ***server*** remoti.

SMTP *Site*: Permette di specificare nome sito, e *IP address*. Per le connessioni in entrata e in uscita si può configurare separatamente:

- Porta *TCP*. *Default* 25.
- Numero massimo connessioni contemporanee. *Default* 1000.
- *Timeout*. *Default* 600 sec.
- Numero massimo connessioni (in uscita) per dominio. *Default* 100.

Operators: specifica quali utenti di NT hanno diritto ad amministrare il ***server***. Non utilizzabile con HTMLA.

Messages. Si possono impostare le limitazioni sui messaggi da inoltrare. Se un messaggio supera i limiti consentiti viene dichiarato NDR e viene rispedito al mittente. Se neanche il mittente è

raggiungibile, viene spostato nella *directory* di *BadMail*. È possibile impostare l'ampiezza del singolo messaggio lato ***server*** e della singola sessione. Se un messaggio in arrivo supera il primo valore viene accettato fino al massimo invalicabile del secondo, dopodiché la sessione viene chiusa. Inoltre si può settare:

- Numero massimo di messaggi da inviare per connessione (20).
- Numero massimo di destinatari per messaggio (100).
- Amministratore che riceverà copia di tutti i messaggi non spedibili, *Directory* di *Badmail*.

Delivery: può essere diviso in 3 categorie di opzioni:

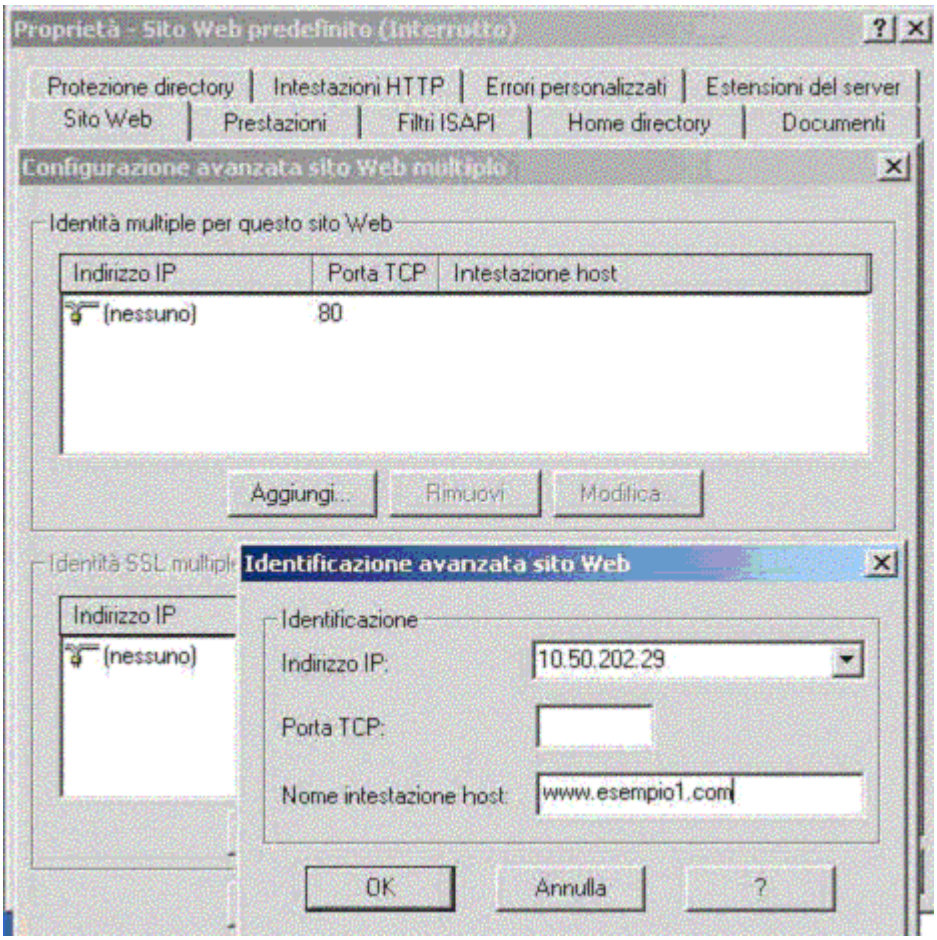
- Trasmissione Numero massimo di tentativi (48) prima di dichiarare un messaggio NDR. Intervallo in minuti tra due tentativi (60) Sono specificati sia per code Locali che Remote. Instradamento Numero massimo di Salti (15) prima di considerare un messaggio NDR.
- Nome del ***server*** di instradamento (MX), Nome del ***server*** *Smart*. Sicurezza *Masquerade Domain*, per nascondere il dominio di provenienza.
- *Reverse* **DNS** dell'*IP* del *sender* per controllare che la *mail* del *From* arrivi effettivamente dal dominio specificato. *Outbound Security* per specificare il tipo di autenticazione supportata per i messaggi in uscita : Nessuna, *Basic*, NT, TLS.

Siti virtuali con intestazioni host

In questo paragrafo viene illustrata la procedura dettagliata per l'*hosting* di più siti *Web* utilizzando un unico **indirizzo** *IP*. *Microsoft Internet Information Services* (**IIS**) consente di eseguire il *mapping* di più siti *Web* aventi lo stesso numero di porta a un unico **indirizzo** *IP* utilizzando una funzionalità denominata Nome intestazione ***host***. Attraverso l'assegnazione di un nome intestazione ***host*** univoco a ciascun sito *Web*, questa funzionalità consente di eseguire il *mapping* di più siti *Web* a un solo **indirizzo** *IP*.

Per configurare siti *Web* utilizzando la funzionalità Nome intestazione ***host***, eseguire le seguenti operazioni:

- Fare *click* con il pulsante destro del *mouse* sul sito *Web* desiderato, quindi scegliere Proprietà dal menù di scelta rapida.
- Nel gruppo **Identificazione** sito *Web* selezionare l'**indirizzo** *IP* che si desidera assegnare al sito *Web* nell'elenco Indirizzo *IP*.
- Fare *click* sul pulsante Avanzate.
- Nel gruppo Identità multiple per questo sito *Web* fare *click* sull'**indirizzo** *IP*, quindi scegliere modifica. Verrà visualizzata la finestra di dialogo Identificazione avanzata sito *Web*.
- Nella casella Nome intestazione ***host*** digitare l'intestazione ***host*** desiderata. Ad esempio, digitare www.esempio1.com. Aggiungere il numero di porta, selezionare l'**indirizzo** *IP* dall'elenco, quindi scegliere OK.



Se si desidera configurare il sito *Web* con identità aggiuntive, scegliere Aggiungi. Utilizzare lo stesso **indirizzo** *IP* e porta *TCP*, ma immettere un Nome intestazione ***host*** univoco. Se si desidera ad esempio accedere allo stesso sito *Web* sia da ***Internet*** che da una rete *Intranet* locale, è possibile configurare l'identità del sito *Web* come indicato di seguito:

```
192.168.0.100 80 www.esempio1.com
192.168.0.100 80 esempio1.com
```

- Fare *click* con il pulsante destro del *mouse* sul sito *Web* successivo, quindi scegliere Proprietà dal menù di scelta rapida.
- Nell'elenco Indirizzo *IP* selezionare lo stesso **indirizzo** *IP* selezionato al passaggio 4, quindi scegliere Avanzate.
- Nel gruppo Identità multiple per questo sito *Web* fare *click* sull'**indirizzo** *IP*, quindi scegliere Modifica. Verrà visualizzata la finestra di dialogo Identificazione avanzata sito *Web*.
- Nella casella Nome intestazione ***host*** digitare un'intestazione ***host*** univoca per il sito *Web*. Ad esempio, digitare www.esempio2.com. Aggiungere il numero di porta, selezionare l'**indirizzo** *IP* dall'elenco, quindi scegliere OK.
- Ripetere i passaggi illustrati per tutti i siti *Web* che si desidera ospitare nello stesso **indirizzo** *IP*.
- Registrare le intestazioni ***host*** con il sistema di risoluzione dei nomi appropriato, ad esempio un ***server*** **DNS** (*Domain Name System*) oppure, per una rete di piccole dimensioni, un *file Host*.

I siti *Web* sono ora configurati in modo tale da accettare richieste *Web* in ingresso sulla base delle rispettive intestazioni ***host***.

Attenzione, non assegnare un'intestazione ***host*** al sito *Web* predefinito. Molti programmi prevedono

che il sito *Web* predefinito utilizzi un **indirizzo** *IP* configurato su (Nessuno), una porta *TCP* configurata su 80 e non utilizzino alcun nome intestazione ***host***.