Accesso remoto con Windows 2000
Default e Politiche Multiple

Default

Affinché sia possibile avere accesso remoto deve esistere sempre almeno una Politica di Accesso Remoto. Per garantire ciò in un *server* di accesso remoto è sempre presente Politica di Accesso Remoto di *Default* che è sufficiente per gestire la maggior parte dei casi.

Tale Politica di Accesso Remoto di *Default* viene applicata a tutti quei tentativi di connessione che non soddisfano le condizioni di nessun altra politica definita.

La Politica di Accesso Remoto di *Default* è denominata *Allow access if dial-in permission is enabled* e viene creata automaticamente quando viene installato *Routing and Remote Access*.

Di seguito sono specificate le impostazonii di tale politica:

- Condizione: Qualsiasi Giorno e Qualsiasi Ora.
- Permesso: *Deny access*.
- Profilo: Nessuno.

Modalità Nativa (nega tutti gli accessi a meno che l'*account* sia impostato ad *Allow*)

In un dominio in 'Modalità Nativa', settando i permessi di *dial-in* dell'*account* utente come '*Control access through Remote Access Policy*' la Politica di Accesso Remoto di *Default* ha come effetto quello di rifiutare qualsiasi connessione. Tuttavia se i permessi di *dial-in* dell'*account* utente sono settati come *Allow access* allora il tentativo di connessione di tale utente sarà accettato.

Modalità *Mixed* (la politica di *Default* viene sovrascritta)

Invece, in un dominio in 'Modalità Mista' la 'Politica di Accesso Remoto di *Default*' viene sempre sovrascritta dalle proprietà di *dial-in* specificate per l'*account* utente, poiché l'opzione '*Control access through Remote Access Policy*' non è disponibile sui controllori di dominio di un dominio che viene eseguito in 'Modalità Mista'.

Durante la conversione da 'Modalità Mista' a 'Modalità Nativa' il nelle proprietà di *dial-in* dell'*account* utente il '*Deny access*' diventa '*Control access through Remote Access Policy*' ed il '*Allow access*' resta '*Allow access*'.

Dunque, per quanto detto nel caso siano presenti più Politiche di Accesso Remoto ogni tentativo di connessione viene giudicato in base alla prima politica di cui sono soddisfatte le condizioni. Nel caso in cui la richiesta di connessione non soddisfi le condizioni di nessuna politica, resta la Politica di Accesso Remoto di *Default* le cui condizioni sono sempre soddisfatte e dunque la richiesta viene accettata solo se nelle proprietà di *dial-in* dell'utente che sta richiedendo la connessione sta specificato *Allow access*.

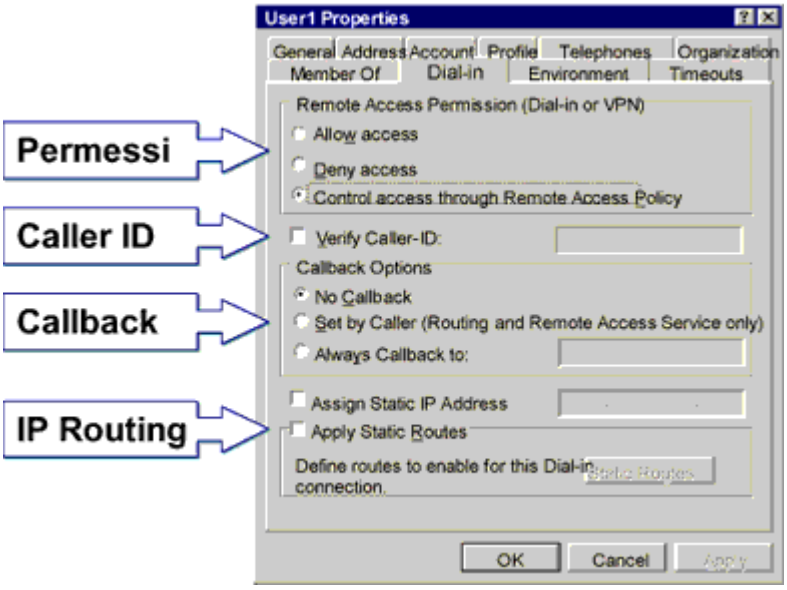
Creazione delle Politiche di Accesso Remoto

Dunque le Politiche di Accesso Remoto permettono di gestire le richieste di accesso remoto tramite la definizione di regole che possono essere molto semplici o estremamente complesse, in base a quelle che sono le esigenze della nostra organizzazione.

Gli elementi di base nella definizione delle Politiche di Accesso Remoto sono dunque:

- I permessi di *dial-in* nelle proprietà dell'*account* utente in *Active Directory*.
- La creazione di una Politica di Accesso Remoto in *Routing e Remote Access* con le relative condizioni e permesso.
- Il Profilo associato ad ogni Politica di Accesso Remoto.

Proprietà di Accesso Remoto dell'Account



Per configurare le proprietà di *dial-in* di un utente su un *server stand-alone* utilizzare lo strumento '*Computer Management*' presente in *Start\Programs\Administrative Tools* e nel contenitore '*Local Users and Groups*' cercare l'utente desiderato e facendo clic con il tasto destro selezionare '*Properties*'.

Invece, per configurare le proprietà di *dial-in* di un utente in un dominio *Active Directory* utilizzare lo strumento '*Active Directory Users and Computers*' presente in *Start\Programs\Administrative Tools*, cercare l'utente desiderato e facendo clic con il tasto destro selezionare '*Properties*'e scegliere la scheda '*Dial-In*'.

Utilizzando la sezione '*Remote Access Permission (Dial-In or VPN)*' è possibile negare o permettere l'accesso remoto esplicitamente o, selezionando '*Control access through Remote Access Policy*', fare riferimento al permesso associato alla politica di accesso remoto di cui tale utente soddisfa le condizioni al momento dell'accesso. Quest'ultima opzione è disponibile solamente in un dominio in 'Modalità Nativa'.

Utilizzando il *check Verify Caller-ID* è possibile fare in modo che il *server* verifichi che il numero telefonico del chiamante coincida con quello ivi specificato.

La sezione *Callback Options* permette di definire se il *Callback* venga o meno abilitato (*No Callback*) e nel caso venga abilitato se il numero a cui il *server* effettua la richiamata è stabilito dall'utente (*Set By Caller*) o una volta per tutte dall'amministratore (*Always Callback To*).

Infine è possibile assegnare all'utente remoto un indirizzo IP statico (*Assign Static IP Address*) e/o configurargli delle *routes* statiche (*Apply Static Routes*).

Condizioni di una Politica di Accesso Remoto

Se la richiesta...

- Avviene tra le 8 a.m. - 5 p.m. di Lunedì-Venerdì.
- Proviene da un indirizzo IP che corrisponde a: 192.168.*.*.
- È di un utente del gruppo Vendite.

La Condizione di una Politica di accesso remoto è costituita da tutta una serie di attributi con relativi valori che verranno comparati con i corrispondenti attributi della richiesta di accesso remoto. Affinché una richiesta soddisfi una condizione, devono esserci corrispondenza con i valori di tutti gli attributi che costituiscono la condizione.

Di seguito elenchiamo quelle che sono le condizioni che è possibile specificare:

- *NAS IP Address*. Una stringa che identifica l'indirizzo IP del *network access server* (NAS).
- *Service Type*. Il tipo di servizio RADIUS richiesto.
- *Framed Protocol*. Il protocollo dei pacchetti in entrata (PPP, *AppleTalk*, SLIP, *Frame Relay*, e X.25).
- *Called Station ID*. Una stringa che identifica il numero telefonico del NAS.
- *Calling Station ID*. Una stringa che identifica il numero di telefono del chiamante.
- *NAS Identifier*. Una stringa che identifica il NAS da cui proviene la richiesta.
- *NAS Port Type*. Il tipo di media utilizzato dal chiamante (analogico, ISDN, e VPN).
- *Day and Time Restrictions*. Il giorno della settimana e l'ora del giorno in cui viene effettuata la connessione.
- *Client IP Address*. Una stringa di caratteri che identifica l'indirizzo del *client* RADIUS.
- *Client Vendor*. Il produttore del NAS che richiede l'autenticazione.
- *Client Friendly Name*. Una stringa di caratteri che identifica il nome del *client* RADIUS che richiede l'autenticazione.

Windows Groups. Il nome del gruppo di *Windows* 2000 cui l'utente che effettua la chiamata appartiene. Non esiste nessuna condizione per controllare il nome dell'utente.

- Per creare una Politica di Accesso Remoto con le relative condizioni ed il profilo associato utilizzare il *tool Routing and Remote Access* presente in *Start\Programs\Administrative Tools* e:
- Cliccare con il tasto destro su *Remote Access Policies* e selezionare *New Remote Access Policy*.
- Utilizzando il *wizard Add Remote Access Policy* inserire il nome in *Policy friendly name* selezionare *Next*.
- Per configurare le condizioni, per ognuna di esse, cliccare *Add*.
- In *Select Attribute* selezionare l'attributo da inserire e cliccare *OK*. Nella corrispondente finestra di dialogo inserire le informazioni richieste da quell'attributo e cliccare su *OK*.
- Una volta inserite tutte le condizioni cliccare *Next*.
- Per garantire l'accesso a chi soddisfa le condizioni selezionare *Grant remote access permission*, mentre per negarlo selezionare *Deny remote access permission*.
- A questo punto è possibile creare un Profilo o, cliccando *Finish* avere una Politica di Accesso Remoto senza specificare nessun Profilo.

Profilo di una Politica di Accesso Remoto

Il Profilo è...

- Tempo massimo di connessione 90 minuti.
- 4 linee multilink.
- Richiesta criptazione IP Sec.

Il Profilo relativo ad una Politica di Accesso Remoto permette di specificare quali sono le

caratteristiche che devono essere soddisfatte dalla connessione per tutta la sua durata, pena la disconnessione immediata.

Per configurare il Profilo per una Politica di Accesso Remoto utilizzare il *tool Routing and Remote Access* presente in *Start\Programs\Administrative Tools* e:

- Fare doppio click sul contenitore *Remote Access Policies*.
- Selezionare la Politica di Accesso Remoto desiderata.
- Cliccare con il tasto destro e scegliere *Properties*.
- Cliccare su *Edit Profile* ed utilizzare la finestra di dialogo *Edit Dial-in Profile* come di seguito descritto:
  - *Dial-in Constraints*. Permette di determinare la durata massima della connessione, la durata massima del periodo di inattività, il giorno, l'ora, il tipo di media (ISDN, VPN o altro) che sono permessi.
  - IP. Permette di filtrare pacchetti IP in ingresso ed in uscita in base alle loro caratteristiche.
  - Multilink. Permette di configurare le modalità del Multilink e di BAP (*Bandwith Allocation Protocol*).
  - *Authentication*. Permette di definire i protocolli di autenticazione autorizzati.
  - *Encryption*. Permette di definire il livello di cifratura richiesto e le modalità di utilizzo.
  - *Advanced*. Permette di configurare parametri addizionali tipo quelli inerenti RADIUS.

Server di Accesso Remoto

La modalità più semplice per permettere l'accesso alla rete ad utenti remoti è quella di definire su un *server* un *server Dial-Up* di accesso remoto.

Per configurare ed attivare tale *server* eseguire i seguenti passi:

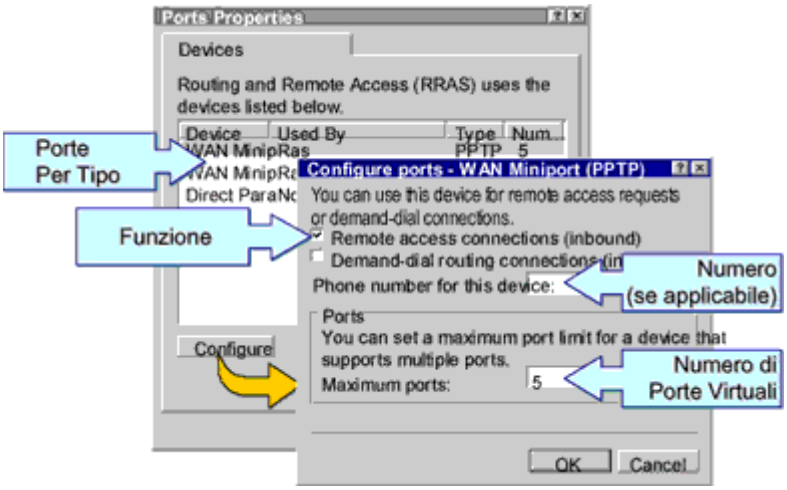
- Verificare la compatibilità dei dispositivi *hardware* (modem, adattatore ISDN o quant'altro) che si intendono utilizzare con *Windows* 2000, usando la *Hardware Compatibility List* (HCL) e, in caso di riscontro positivo, procedere alla loro installazione.
- Utilizzare lo strumento *Routing and Remote Access* contenuto in *Start\Programs\Administrative Tools* e cliccando con il tasto destro sul nome del *server* selezionare *Configure and Enable Routing and Remote Access*.
- Completare il *wizard* secondo quanto segue:
  - *Common Configurations*: *Remote access server*.
  - *Remote Client Protocols*: Se vi sono elencati tutti i protocolli che si intende utilizzare selezionare *Next*, altrimenti procedere alla loro installazione.
  - *IP Address Assignment*: Selezionare un metodo di installazione degli indirizzi IP ai *client*. Se si decide di definire sul *server* RRAS un *range* di indirizzi, piuttosto che appoggiarsi ad un *server* DHCP, occorre specificare tale *range* di indirizzi.
  - *Managing Multiple Remote Access Servers*: Selezionare se intende o meno utilizzare un *server* RADIUS. In caso di risposta positiva bisogna specificare il nome del *server* RADIUS, il nome di un eventuale *server* RADIUS di *backup* e la *password* da utilizzare per dialogare con tali *server*.
- Configurare eventualmente politiche di accesso remoto, e tutti i settaggi inerenti le modalità di autenticazione e cifratura.

Quando il *server* di accesso remoto *dial-up* parte la prima volta, *Windows* 2000 rileva automaticamente tutti i dispositivi *hardware* (modem, adattatori ISDN ...) installati e configura una porta modem per ognuno di essi.

Windows 2000 provvede anche a creare automaticamente una porta per ogni connessione ad una

porta seriale o parallela che dovesse rilevare.

È possibile, da questo momento in poi, modificare la configurazione di tali porte utlizzando il contenitore *Ports* presente nel lo strumento *Routing and Remote Access* contenuto in *Start\Programs\Administrative Tools*:



- Accedere alle proprietà del contenitore *Ports*.
- In *Ports Properties* selezionare una device e quindi *Configure*.
- In *Configure Device* selezionare *Remote access (inbound)* per abilitare le connessioni in ingresso.
- Nel caso in cui si stia configurando una porta modem inserire in numero di telefono in *Phone number of this device*.
- Selezionare *OK* in *Configure Device* e *Ports Properties*.

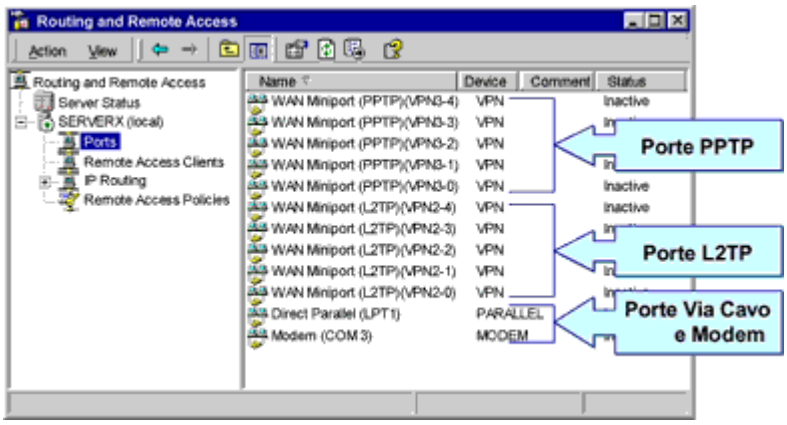
Server VPN

Tra gli svantaggi di un *server* di accesso remoto di tipo *dial-up* ricordiamo essenzialmente il problema dei costi dovuto alla necessità di effettuare chiamate spesso extraurbane ed alla necessità di disporre di tante connessioni fisiche quanti sono i *client* che si vuole accedano contemporaneamente al *server* da remoto.

Utilizzare lo strumento *Routing and Remote Access* contenuto in *Start\Programs\Administrative Tools* e cliccando con il tasto destro sul nome del *server* selezionare *Configure and Enable Routing and Remote Access*.

Completare il *wizard* secondo quanto segue:

- Verificare la compatibilità dei dispositivi *hardware* (modem, adattatore ISDN o quant'altro) che si intendono utilizzare con *Windows* 2000, usando la *Hardware Compatibility List* (HCL) e, in caso di riscontro positivo, procedere alla loro installazione.
- Utilizzare lo strumento *Routing and Remote Access* contenuto in *Start\Programs\Administrative Tools* e cliccando con il tasto destro sul nome del *server* selezionare *Configure and Enable Routing and Remote Access*.



- Completare il *wizard* secondo quanto segue:
  - *Common Configurations*: *Virtual private network (VPN) server*.
  - *Remote Client Protocols*: Se vi sono elencati tutti i protocolli che si intende utilizzare selezionare *Next*, altrimenti procedere alla loro installazione.
  - *IP Address Assignment*: Selezionare un metodo di installazione degli indirizzi IP ai *client*. Se si decide di definire sul *server* RRAS (Routing and Remote Access Services) un *range* di indirizzi, piuttosto che appoggiarsi ad un *server* DHCP (Dynamic Host Configuration Protocol), occorre specificare tale *range* di indirizzi.
  - *Managing Multiple Remote Access Servers*: Selezionare se intende o meno utilizzare un *server* RADIUS. In caso di risposta positiva bisogna specificare il nome del *server* RADIUS, il nome di un eventuale *server* RADIUS di *backup* e la *password* da utilizzare per dialogare con tali *server*.
- Configurare eventualmente politiche di accesso remoto, e tutti i settaggi inerenti le modalità di autenticazione e cifratura.

Quando il *server* di accesso remoto VPN parte per la prima volta, *Windows* 2000 crea e configura automaticamente 128 porte PPTP (*Point to Point Tunneling Protocol*) *ports* e 128 porte L2TP (*Layer Two Tunneling Protocol*) *ports*. Il numero di porte virtuali disponibili non è limitato da considerazioni legate al numero di dispositivi *hardware* bensì semplicemente da considerazioni relative alle *performance*.

È possibile, da questo momento in poi, modificare la configurazione di tali porte utlizzando il contenitore *Ports* presente nel lo strumento *Routing and Remote Access* contenuto in *Start\Programs\Administrative Tools*:

- Accedere alle proprietà del contenitore *Ports*.
- In *Ports Properties* selezionare una device VPN, *WAN Miniport* (PPTP) o *WAN Miniport* (L2TP), quindi *Configure*.
- In *Configure Device* selezionare *Remote access (inbound)* per abilitare le connessioni in ingresso.
- Opzionalmente, è possibile aumentare o diminuire il numero di porte virtuali disponibili.
- Selezionare *OK* in *Configure Device* e *Ports Properties*.

Politiche di Accesso Remoto

Le **Politiche di Accesso Remoto** ci permettono di controllare in maniera molto dettagliata chi si connette, come si connette, quando si connette e, una volta connesso, quali sono le caratteristiche della connessione.

Conoscere come sono fatte e quali sono i criteri che regolamentano la loro applicazione, ci permette di utilizzare tale strumento in maniera molto proficua.

La prima osservazione da fare riguarda il fatto che le informazioni relative alla configurazione delle Politiche di Accesso Remoto non sono memorizzate in *Active Directory*, come ci si potrebbe aspettare, bensì localmente al *server* per il quale vengono definite.

Una politica di accesso remoto consiste di tre componenti:

- **Condizioni**. Le condizioni sono un insieme di parametri, come ad esempio la data e l'ora, l'appartenenza a gruppi, il numero di telefono o l'indirizzo IP del chiamante, che devono coincidere con i parametri del *client* che sta effettuando la chiamata. La prima politica di accesso remoto le cui condizioni coincidono con quelle del *client* è quella che viene applicata. Dunque deve esistere almeno una politica di accesso remoto, vale la prima di cui il *client* soddisfa le condizioni (per cui il loro ordine è significativo) e se non sono soddisfatte le condizioni di nessuna politica la connessione viene rifiutata.
- **Permesso**. Nel caso in cui vengano soddisfatte le condizioni relative ad una politica allora la connessione viene permessa o negata in base ad una combinazione del permesso specificato nelle proprietà dell'*account* utente e del permesso specificato nella politica.Questo permette di avere una certa flessibilità specificando una politiche che permette o nega l'accesso ad un certo gruppo di utenti con certe caratteristiche e specificando poi l'eccezione per particolari utenti che pure appartengono a quel gruppo.
- **Profilo**. Quando le condizioni di una politica sono soddisfatte ed il permesso concede la connessione, viene applicato a tale connessione un profilo. Nel profilo sono contenute quelle che devono essere le caratteristiche della connessione (per esempio la durata) e la loro violazione provoca la terminazione della connessione.

Logica di Valutazione

Vediamo innanzitutto qual'è la logica seguita nella valutazione delle Politiche di Accesso Remoto. Tale logica giudica le richieste di connessione mixando le condizioni, i permessi della politica e dell'utente che richiede la connessione e le impostazionii specificate nel profilo.

La logica di valutazione delle Politiche di Accesso Remoto è la seguente:

- I parametri del *client* che sta effettuando la chiamata vengono confrontati con le condizioni specificate nelle Politiche di Accesso Remoto
    - Se essi non coincidono con le condizioni di nessuna Politiche di Accesso Remoto allora la chiamata viene rifiutata.
    - Se essi coincidono con le coindizioni di una Politica di Accesso Remoto, allora tale politica viene usata per determinare l'accesso.
- Innanzitutto vengono controllate la proprietà di *dial-in* relative all'*account* utente che sta richiedendo la connessione:
    - Se essa è settata a *Deny access*, la connessione viene negata.
    - Se essa è settata a *Allow access*, la connessione viene accettata e viene applicato il permesso della politica.
    - Se essa è settata a *Control access through Remote Access Policy* (opzione disponibile solo nei domini in Modalità Nativa), viene applicato il permesso relativo alla politica. Se esso permette l'accesso la connessione viene accettata e viene applicato il permesso della politica, altrimenti viene rifiutata.
- Nel caso in cui la connessione sia stata accettata i parametri del richiedente vengono continuamente confrontati con quelli del profilo e non appena non dovesse essere più riscontrata corrispondenza, la connessione viene terminata.