

# Stargate

**Manuale Utente**

# Stargate

**ADSL ROUTER**

***Manuale di riferimento tecnico***

***Rev.4***

***DATE: Maggio 2002***

## **INDICE**

<b><u>VFINDICE</u></b> .....	<b>3</b>
<b><u>AVVISI DI SICUREZZA</u></b> .....	<b>7</b>
<b><u>PRECAUZIONI</u></b> .....	<b>8</b>
<b><u>PULIZIA</u></b> .....	<b>8</b>
<b><u>CAPITOLO 1</u></b> .....	<b>9</b>
<b><u>1 INTRODUZIONE</u></b> .....	<b>9</b>
1.1 GENERALITÀ .....	9
1.2 UTENTI .....	9
1.3 CONTENUTI DEL MANUALE .....	9
1.4 CONVENZIONI .....	10
<b><u>CAPITOLO 2</u></b> .....	<b>11</b>
<b><u>2 GENERALITÀ STARGATE</u></b> .....	<b>11</b>
2.1 CARATTERISTICHE .....	11
2.2 PANNELLO FRONTALE .....	11
2.3 PANNELLO POSTERIORE .....	12
<b><u>CAPITOLO 3</u></b> .....	<b>14</b>
<b><u>3 INSTALLAZIONE STARGATE</u></b> .....	<b>14</b>
3.1 IMBALLO .....	14
3.2 POSIZIONAMENTO .....	14
3.3 CONNESSIONI .....	15

3.3.1	RETE LOCALE.....	15
3.3.2	LINEA ADSL.....	16
3.3.3	ALIMENTAZIONE.....	18
3.3.4	CONNESSIONE ALLA PORTA CONSOLE .....	18

## **CAPITOLO 4..... 19**

### **4 CONFIGURAZIONE STARGATE..... 19**

4.1	INFORMAZIONI GENERALI .....	19
4.2	CONFIGURARE LA CONNESSIONE AD INTERNET .....	19
4.3	CONFIGURAZIONE TRAMITE STARFIRE .....	20
4.4	CONFIGURAZIONE TRAMITE IL WEB SERVER INTERNO.....	21
4.5	CAMBIARE LA PASSWORD DI SISTEMA.....	24
4.6	MODIFICARE L'INDIRIZZO IP DELLO STARGATE .....	24
4.7	AVVIARE LA CONNESSIONE AD INTERNET.....	26

## **CAPITOLO 5..... 27**

### **5 PROGRAMMAZIONE DA CONSOLE CLI..... 27**

5.1	INTRODUZIONE.....	27
5.1.1	AVVIO DELLA SESSIONE CLI .....	27
5.1.2	UTILIZZO DELLA FUNZIONE DI AIUTO (HELP).....	28
5.1.3	DESCRIZIONE DELLA SINTASSI UTILIZZATA .....	29
5.1.4	SALVATAGGIO DELLA CONFIGURAZIONE .....	29
5.2	GENERALITÀ SUI COMANDI DI CONFIGURAZIONE .....	29
5.2.1	PROMPT.....	33
5.2.2	GERARCHIA DEI COMANDI.....	33
5.2.3	VISUALIZZAZIONE DELLA CONFIGURAZIONE .....	34
5.2.4	CONFIGURAZIONE PASSO-PASSO .....	35
5.2.5	SALVATAGGIO DELLA CONFIGURAZIONE .....	36
5.2.6	RIPRISTINO DELLA CONFIGURAZIONE DI FABBRICA .....	36
5.3	COMANDI DI CONFIGURAZIONE .....	36
5.3.1	CONFIGURAZIONE DI SISTEMA.....	36
5.3.2	CONFIGURAZIONE NAT.....	38
5.3.3	CONFIGURAZIONE PORTE WAN .....	41
5.3.4	CONFIGURAZIONE RIP.....	51
5.3.5	CONFIGURAZIONE RETE LOCALE (LAN) .....	53
5.3.6	CONFIGURAZIONE DHCP .....	54
5.3.7	CONFIGURAZIONE DNS.....	56
5.3.8	CONFIGURAZIONE SNMP .....	58
5.3.9	CONFIGURAZIONE PORTE DI SERVIZIO.....	59
5.3.10	VISUALIZZAZIONE DEGLI EVENTI (LOG).....	60
5.3.11	SALVATAGGIO E RIPRISTINO DI UN FILE DI CONFIGURAZIONE .....	62

<b>CAPITOLO 6</b> .....	<b>63</b>
<b>6 CONFIGURAZIONE VIA TELNET</b> .....	<b>63</b>
<b>CAPITOLO 7</b> .....	<b>64</b>
<b>7 CONFIGURAZIONE DA WEB</b> .....	<b>64</b>
<b>7.1 PAGINE DI CONFIGURAZIONE</b> .....	<b>64</b>
7.1.1 PAGINA INIZIALE.....	65
7.1.2 SISTEMA.....	65
7.1.3 L'INTERFACCIA WAN.....	66
7.1.4 L'INTERFACCIA LAN.....	68
7.1.5 PARAMETRI DHCP.....	69
7.1.6 PARAMETRI DNS.....	69
7.1.7 PARAMETRI NAPT (LAN E WAN).....	70
7.1.8 PARAMETRI IP (LAN E WAN).....	71
<b>CAPITOLO 8</b> .....	<b>72</b>
<b>8 CONFIGURAZIONE DELLE FUNZIONI DI FIREWALL</b> .....	<b>72</b>
<b>8.1 INTRODUZIONE</b> .....	<b>72</b>
<b>8.2 CREAZIONE E GESTIONE DELLE LISTE DI ACCESSO</b> .....	<b>73</b>
8.2.1 CREAZIONE DELLA LISTA ED EDITING DELLE REGOLE.....	73
8.2.2 CANCELLAZIONE DI UNA LISTA DI ACCESSO.....	76
8.2.3 ESEMPI D'USO: BLOCCO DELLA POSTA ELETTRONICA.....	76
8.2.4 VERIFICA DI UNA LISTA DI ACCESSO.....	77
8.2.5 BLOCCO DELL'ACCESSO AD INTERNET.....	78
8.2.6 BLOCCO DEL MANAGEMENT DI STARGATE.....	78
<b>8.3 ASSEGNAZIONE LISTA D'ACCESSO ALLA LAN E ALLE WANS</b> .....	<b>79</b>
<b>8.4 CONFIGURAZIONE ACCESS LISTS DA WEB</b> .....	<b>79</b>
8.4.2 ASSEGNAZIONE LISTE D'ACCESSO ALLA LAN E ALLE WANS.....	84
<b>CAPITOLO 9</b> .....	<b>86</b>
<b>9 BRIDGING</b> .....	<b>86</b>
<b>9.1 INTRODUZIONE</b> .....	<b>86</b>

<b>9.2</b>	<b>IMPLEMENTAZIONE .....</b>	<b>86</b>
<b>9.3</b>	<b>CONFIGURAZIONE .....</b>	<b>87</b>
9.3.1	PARAMETRI DI CONFIGURAZIONE DEL NODO BRIDGES.....	87
9.3.2	PARAMETRI DI CONFIGURAZIONE DEL NODO SPANNINGTREEPROTOCOL.....	89
9.3.3	PARAMETRI DI CONFIGURAZIONE DEI NODI D'INTERFACCIA.....	89
9.3.4	PARAMETRI DI CONFIGURAZIONE DEL NODO BRIDGEPAR.....	90
 <b><u>CAPITOLO 10.....</u></b>		<b><u>91</u></b>
 <b><u>10 MULTICASTING .....</u></b>		<b><u>91</u></b>
10.1	INTRODUZIONE.....	91
10.2	CONFIGURAZIONE .....	91
 <b><u>CAPITOLO 11.....</u></b>		<b><u>92</u></b>
 <b><u>11 MONITOR.....</u></b>		<b><u>92</u></b>
11.1	VISUALIZZAZIONE STATO DELLO STARGATE .....	92
11.2	VISUALIZZAZIONE STATISTICHE.....	92
11.2.1	STATISTICHE ADSL.....	93
11.2.2	VISUALIZZAZIONE STATISTICHE ATM .....	94
11.2.3	VISUALIZZAZIONE STATISTICHE PPP .....	95
11.2.4	VISUALIZZAZIONE STATISTICHE PPPoE.....	96
11.2.5	VISUALIZZAZIONE STATISTICHE DHCP .....	97
11.2.6	VISUALIZZAZIONE STATISTICHE IP.....	98
 <b><u>CAPITOLO 12.....</u></b>		<b><u>100</u></b>
 <b><u>12 AGGIORNAMENTO SOFTWARE.....</u></b>		<b><u>100</u></b>
12.1	AGGIORNAMENTO TRAMITE INTERFACCIA SERIALE.....	100
12.1.1	SALVATAGGIO E RIPRISTINO FILE DI CONFIGURAZIONE CON STARFIRE .....	102
12.2	AGGIORNAMENTO TRAMITE LAN .....	103
 <b><u>APPENDICE A .....</u></b>		<b><u>104</u></b>
 <b><u>APPENDICE B .....</u></b>		<b><u>106</u></b>

## Avvisi di sicurezza



**APPARECCHIATURA DI CLASSE II CON TERRA FUNZIONALE**  
Connettere sempre ad una presa di corrente provvista di terra.



Al fine di garantire una protezione continua per la sicurezza dell'operatore, utilizzare esclusivamente l'adattatore di rete fornito in dotazione con l'apparato.



**ATTENZIONE:** connettere l'apparecchiatura ad una presa di corrente installata nelle immediate vicinanze e di facile accesso per l'operatore. In nessun caso è consentito tagliare la spina di rete per connettere l'apparecchiatura in modo fisso.



Al fine di evitare contatti accidentali con parti attive di circuiti TNV, connettere il cavo dell'interfaccia telefonica nella presa dell'apparato e successivamente alla linea esterna di telecomunicazione.



**ATTENZIONE:** Durante un temporale, non collegare mai l'apparato ad una linea esterna di telecomunicazione.



**ATTENZIONE:** In caso di emergenza l'apparecchiatura deve poter essere rimossa dal muro. Non effettuare un fissaggio permanente.



Il passaggio da ambienti freddi ad ambienti caldi può determinare formazioni di condensa all'interno dell'apparato. In questi casi, per evitare malfunzionamenti, si consiglia di attendere almeno 1ora prima di connettere l'apparato alla rete di alimentazione.



In caso di incendio, evitare in modo assoluto di usare acqua come mezzo estinguente.



**ATTENZIONE: RISCHIO DI SCOSSA ELETTRICA**  
L'alimentazione elettrica utilizzata per questo apparato comporta livelli di tensione letali.



Evitare di accedere alle parti interne dell'apparato (e/o dell'alimentatore).



In caso di penetrazione di oggetti o liquidi all'interno dell'apparato, scollegare immediatamente il cavo di alimentazione. Prima di riutilizzare l'apparato, farlo controllare da personale specializzato.



Per l'assistenza rivolgersi a personale qualificato.



In caso di intervento accertarsi sempre che l'apparato sia completamente ed efficacemente isolato dalla alimentazione.

## Precauzioni



### ATTENZIONE:

Molti dei componenti utilizzati in questo apparato sono sensibili alle scariche elettrostatiche.



Nel caso di eventuale manipolazione dei cavi di collegamento, disinserire l'alimentazione elettrica ed evitare contatti diretti con i terminali dei connettori.



Nella necessità di dover maneggiare qualsiasi componente elettronico, eliminare l'eventuale elettricità statica di cui si potrebbe essere portatori, toccando un piano di massa per scaricarla a terra. Se possibile, indossare un bracciale a massa.



L'inosservanza di queste precauzioni potrebbe causare danni permanenti all'apparato.

## Pulizia



Per la pulizia usare un panno soffice ed asciutto o appena imbevuto di una leggera soluzione detergente. Non usare alcun tipo di solvente, come alcool o benzina, al fine di evitare danneggiamenti alle finiture.



Questo prodotto è conforme ai requisiti della Direttiva EMC 89/336/CE, della Direttiva Bassa Tensione 73/23/CE, come emendate dalle Direttive 92/31/CE e 93/68/CE.

## CAPITOLO 1

### 1 Introduzione

#### 1.1 Generalità

Benvenuti nel mondo dell'alta velocità ADSL. Con l'ausilio di Stargate potrete navigare in Internet con rapidità o connettere la vostra rete locale (LAN) ad altre reti locali (WAN) con prestazioni sensazionali.

Questo manuale vi descriverà le operazioni da compiere per connettere lo Stargate alla vostra rete locale (LAN), alla linea ADSL (WAN) e come configurare l'apparato per le funzionalità di HUB/Router. Per evitare errori nelle varie fasi dell'installazione, leggete attentamente questo manuale prima dell'utilizzo.

#### 1.2 Utenti

Il manuale è rivolto ad utenti ed amministratori di rete, responsabili dell'Hardware e del Software di reti locali Ethernet o di singole postazioni PC.

#### 1.3 Contenuti del manuale

- ⇒ **Capitolo 1** - Introduzione: questo capitolo.
- ⇒ **Capitolo 2 - Generalità Stargate**: contiene la descrizione delle caratteristiche tecniche, del pannello frontale e di quello posteriore.
- ⇒ **Capitolo 3 - Installazione Stargate**: descrive il contenuto dell'imballo dello Stargate e fornisce le indicazioni su come collegare le varie interfacce.
- ⇒ **Capitolo 4 – Configurazione Stargate**: illustra come fare una configurazione minima dell'apparato per un rapido accesso alla rete.
- ⇒ **Capitolo 5 - Console CLI**: descrive come usare l'interfaccia seriale RS232 di un PC per configurare l'apparato tramite l'apposito cavo in dotazione.
- ⇒ **Capitolo 6 – Configurazione via Telnet**: descrive come avviare una sessione Telnet per accedere alla configurazione dello Stargate da un PC collegato in LAN.
- ⇒ **Capitolo 7 – Configurazione da WEB Browser**: descrive come configurare lo Stargate usando un qualsiasi Web Browser da un PC collegato ad una delle quattro interfacce Ethernet.
- ⇒ **Capitolo 8 – Firewall** : descrive come creare dei filtri per la personalizzazione della gestione del traffico uscente ed entrate dello Stargate.
- ⇒ **Capitolo 9 – Bridging**: descrive la funzionalità di bridge ed il modo in cui tale funzionalità può essere configurata su Stargate.
- ⇒ **Capitolo 10 – Multicasting**: vengono illustrate le modalità di configurazione del sistema per abilitare Stargate alla ricezione di traffico multicast (lato LAN e WAN).
- ⇒ **Capitolo 11 - Monitor**: descrive come monitorare le performance dello Stargate.

- ⇒ **Capitolo 12 – Aggiornamento Software:** illustra come aggiornare il firmware dell'apparato, via rete o tramite l'interfaccia seriale con l'applicativo incluso nel software a corredo "StarFire".
- ⇒ **Appendice A – Specifiche tecniche:** fornisce dettagli tecnici sulle caratteristiche dello Stargate.
- ⇒ **Appendice B – Approfondimenti:** Fornisce delle informazioni su tematiche quali ADSL, ATM, DHCP, DNS, TCP/IP e routing con riferimenti al comportamento di Stargate.

## 1.4 Convenzioni

In questo manuale vengono usate le seguenti convenzioni per visualizzare le informazioni:

- ⇒ i comandi vengono visualizzati con caratteri in **grassetto e corsivi**;
- ⇒ le scritte che appaiono sul terminale vengono visualizzate in questo manuale con il carattere `courier`;
- ⇒ il testo inserito dall'utente appare con il carattere **`courier grassetto`**;
- ⇒ i caratteri ottenuti premendo contemporaneamente il test CTRL e un tasto alfanumerico (nell'esempio il carattere M) sono rappresentati come `CTRL-M` o `^M`.
- ⇒ il simbolo ↵ indica il carattere di Carriage Return ottenuto premendo il tasto RETURN o INVIO.

Le convenzioni sintattiche sono le seguenti:

- ⇒ i comandi opzionali sono racchiusi da parentesi quadre ([ ]);
- ⇒ le opzioni alternative sono racchiuse da parentesi graffe ( { } );
- ⇒ le variabili a cui assegnare un valore sono scritte con il carattere `courier italic`.

## CAPITOLO 2

### 2 Generalità Stargate

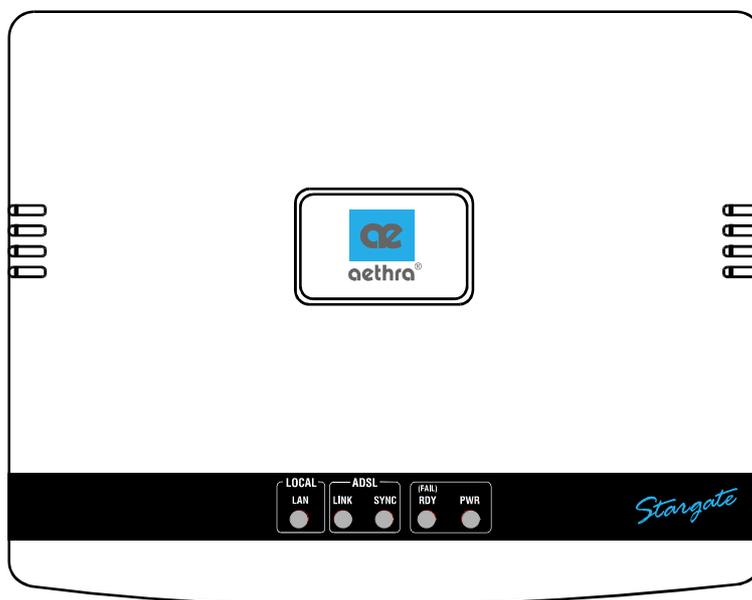
Lo Stargate è un router ADSL (Asymmetric Digital Subscriber Line) con aggiunta la funzionalità di HUB Ethernet 10BaseT. Può connettere PC, stampanti o qualsiasi altro dispositivo dotato di scheda di rete Ethernet ad Internet o ad altre reti remote (WAN).

#### 2.1 Caratteristiche

- ⇒ Tecnologia ADSL che fornisce fino a 8Mbps di banda dati in ricezione (downstream);
- ⇒ trasporto ATM (Asynchronous Transfer Mode): supporta fino a 8 circuiti virtuali (VC) per la trasmissione dati;
- ⇒ integra un HUB Ethernet 10BaseT con accesso diretto dal pannello posteriore per la rapida connessione dei dispositivi di rete;
- ⇒ semplice procedure di configurazione per un'immediata connessione degli apparati alla rete;
- ⇒ configurazione guidata tramite Web Browser da un qualsiasi PC collegato alla rete locale;
- ⇒ funzionalità di Network Address Translation (NAT) che consente di condividere un solo indirizzo IP tra più stazioni della rete locale e fornisce un adeguato sistema di sicurezza delle connessioni;
- ⇒ funzionalità di server Dinamic Host Configuration Protocol (DHCP), che consente la configurazione automatica dei PC collegati allo Stargate sulla rete locale;
- ⇒ funzionalità di Server e forwarder DNS (Domain Name System) per la risoluzione dei nomi di host e di dominio nei relativi indirizzi IP;
- ⇒ funzione di Firewall per proteggere la rete interna dagli attacchi esterni indesiderati e per la gestione personalizzata dei diritti ai vari servizi di rete dei singoli host.
- ⇒ controllo e monitoraggio del traffico WAN in uscita dallo Stargate in termini di Banda;

#### 2.2 Pannello Frontale

Sul pannello frontale sono facilmente individuabili 5 led che, a seconda delle situazioni, forniscono indicazioni sul funzionamento dello Stargate:



Led LOCAL LAN:

- ⇒ spento se non c'è nessun flusso di dati sulla rete locale (LAN);
- ⇒ lampeggio nel normale funzionamento quando transitano dati sulla rete locale (LAN).

Led ADSL SYNC:

- ⇒ acceso quando Stargate cerca di stabilire la connessione con il modem in centrale.

Led ADSL LINK:

- ⇒ acceso quando la connessione con il modem ADSL in centrale è avvenuta correttamente.

Led RDY (fail):

- ⇒ lampeggio lento (1 Hz) nella prima fase di inizializzazione (accensione) dell'apparato;
- ⇒ ampeggio asimmetrico (breve accensione con periodo di circa 1 Hz) nella seconda fase di inizializzazione;
- ⇒ acceso fisso quando la fase di inizializzazione è andata a buon fine;
- ⇒ lampeggio veloce (3 Hz) indica un malfunzionamento dello Stargate.

Led PWR:

- ⇒ spento quando l'apparato non è alimentato;
- ⇒ acceso quando lo Stargate è alimentato correttamente.

## 2.3 Pannello Posteriore

Sul pannello posteriore sono alloggiare:



### **Stargate**

- ⇒ 1 porta LINE per il collegamento della linea ADSL (WAN) su connettore RJ-11 (6p/2c);
- ⇒ 4 porte Ethernet 10BaseT per il collegamento LAN su connettori RJ-45;
- ⇒ 1 porta Console per la programmazione dello Stargate attraverso la porta seriale di un terminale o di un PC;
- ⇒ 1 porta PWR per collegare l'adattatore di alimentazione in dotazione;
- ⇒ 1 Interruttore ON/OFF per l'accensione e lo spegnimento dell'apparato.

All'estremità superiori di ogni connettore Ethernet RJ-45 sono inseriti due led (giallo a sinistra, verde a destra) che forniscono le seguenti indicazioni:

- ⇒ entrambi spenti quando non è collegato nessun apparato all'interfaccia Ethernet;
- ⇒ entrambi accesi quando è collegata una interfaccia Ethernet di un qualsiasi dispositivo ma non vengono scambiati flussi di dati;
- ⇒ led giallo lampeggiante quando Stargate riceve dati dal dispositivo collegato;
- ⇒ led verde lampeggiante quando Stargate trasmette dati all'apparato collegato.

## CAPITOLO 3

### 3 Installazione Stargate

L'installazione di Stargate è semplice e immediata. Per aiutarvi nell'installazione vi consigliamo di attenervi all'ordine con cui vi presentiamo le varie fasi.

#### 3.1 Imballo

Togliere dall'imballo lo Stargate, gli accessori a corredo e verificare che il contenuto corrisponda a quanto descritto in questo manuale. Nella figura sottostante sono facilmente individuabili tutti gli elementi che troverete nell'imballo: lo Stargate, un kit di accessori per le varie connessioni, un alimentatore, un CD contenente software e istruzioni dello Stargate.

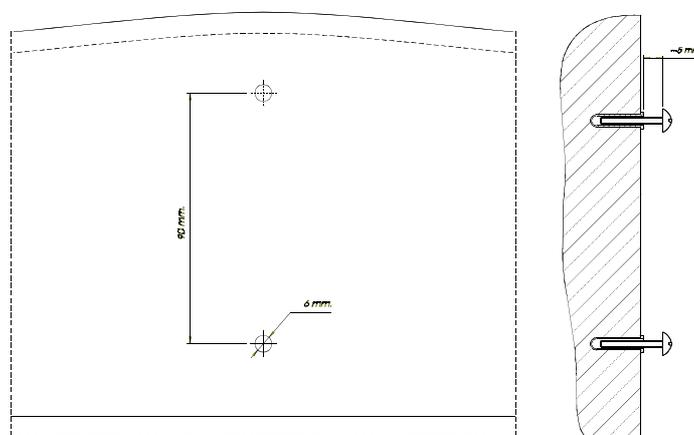


#### 3.2 Posizionamento

Lo Stargate permette l'installazione sia a parete che da tavolo.

*Individuare una posizione facilmente raggiungibile con le connessioni da effettuare e in prossimità di una presa di corrente con caratteristiche rispondenti alle norme attualmente vigenti. In nessun caso è consentito tagliare la spina di rete e collegare l'adattatore fornito con Stargate direttamente alla rete elettrica.*

*L'apparato deve essere posizionato in luoghi asciutti e con possibilità di ventilazione. Non chiudere mai il dispositivo in luoghi dove non è consentita alcuna ventilazione. Per l'installazione a parete (altezza minima da terra 20 cm), eseguire nella parete due fori da 6 mm di diametro in modo che coincidano con i fori indicati in questa figura esempio:*



*Inserire i tasselli nei fori praticati, avvitare le viti con il distanziatore in dotazione e agganciare lo Stargate sulle asole presenti sul fondo.*

### **3.3 Connessioni**

Le connessioni da effettuare sono di tre tipi:

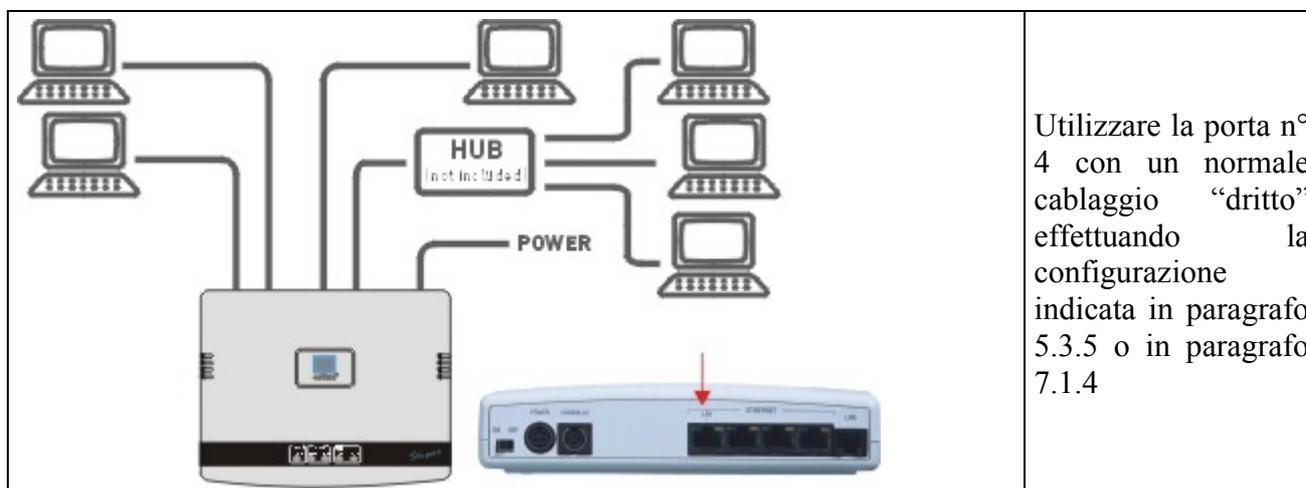
- ⇒ rete locale (LAN);
- ⇒ linea ADSL (WAN);
- ⇒ alimentazione elettrica.

#### **3.3.1 Rete locale**

Potete connettere direttamente fino a 4 Personal computer o altri dispositivi dotati di interfaccia Ethernet 10BaseT alle porte RJ-45 contrassegnate con la descrizione "Ethernet" mediante cavetti a "treccia", di qualità adeguata e terminati con gli opportuni spinotti RJ-45.

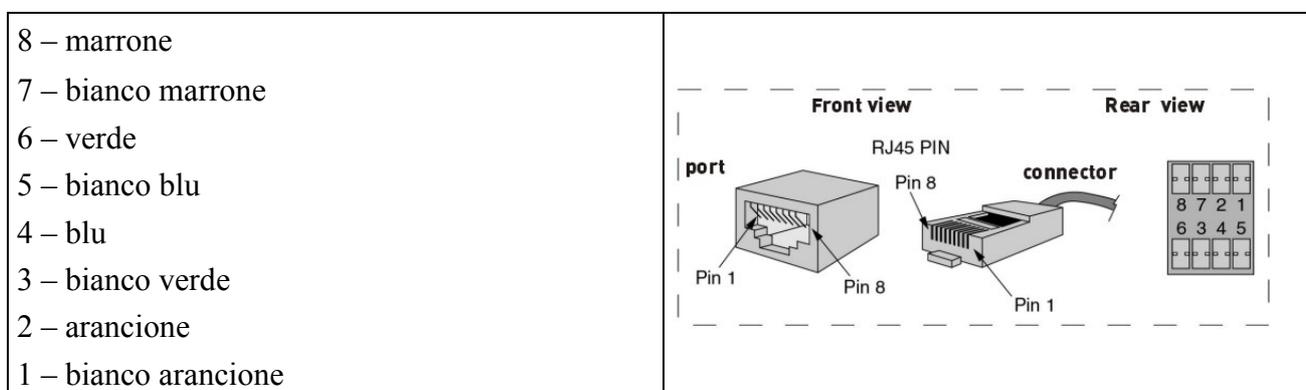
Se occorre collegare più di quattro PC allo Stargate, è necessario utilizzare un dispositivo esterno (es. hub o switch).

In tal caso, collegare il dispositivo esterno (es. hub o switch), utilizzando la porta n° 4 dopo averla configurata adeguatamente per questo tipo di collegamento (vedere paragrafo 5.3.5 o 7.1.4).



Per facilità riportiamo di seguito un esempio di collegamento dei connettori RJ45 ai cavi CAT5 per rete LAN:

! *Rispettate la sequenza dei colori per ottenere la corretta schermatura dei segnali (ed evitare errori di cablaggio. I connettori sono osservati di fronte (fili dietro).*

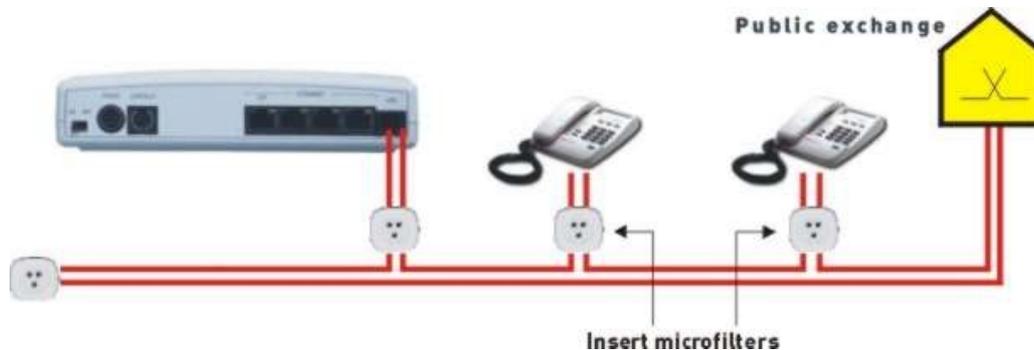


**NOTA:** I fili 1-2 devono essere appartenere alla medesima treccia, i fili 3-6 ad un'altra treccia.

### 3.3.2 Linea ADSL

Il collegamento alla linea ADSL si effettua con il cavetto in dotazione tra la porta con descrizione “LINE” e una delle vostre prese telefoniche.

Fate attenzione alla realizzazione dell'impianto telefonico interno in quanto questo deve essere di tipo “parallelo” e non “a spina”.



Se disponete di un impianto a spina, è indispensabile utilizzare gli appositi microfiltri<sup>1</sup> ADSL su TUTTE le prese sulle quali si intende utilizzare un telefono per rendere l'impianto di tipo parallelo.

Se l'impianto telefonico è collegato a PABX o apparati particolarmente sensibili al segnale ADSL, richiedete al vostro ISP l'installazione del POTS Splitter. Questo dispositivo, inserito all'ingresso della linea, separa il segnale telefonico tradizionale da quello ADSL evitando così l'interferenza reciproca delle due tipologie di servizio:



---

<sup>1</sup> E' sempre consigliabile installare gli appositi microfiltri ADSL in quanto qualche apparato tradizionale potrebbe ricevere disturbi in fonìa dal segnale ADSL.

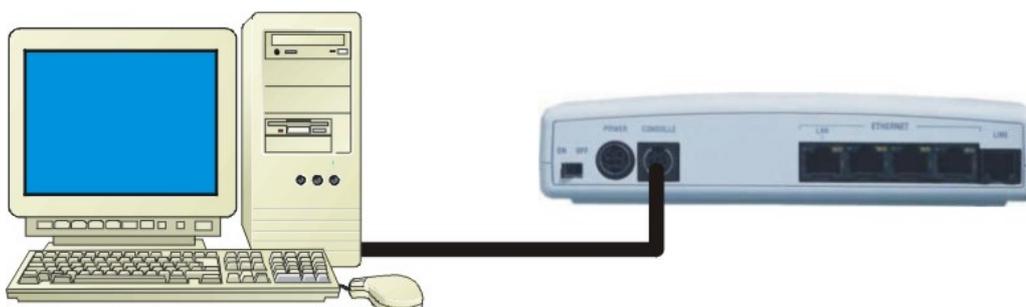
### 3.3.3 Alimentazione

Collegare l'alimentatore in dotazione nell'apposito attacco "PWR" e successivamente ad una presa elettrica con caratteristiche adeguate all'alimentatore in dotazione. *Per nessun motivo è possibile tagliare e collegare i cavi di alimentazione direttamente alla rete elettrica.*



### 3.3.4 Connessione alla porta console

Per collegare un PC o un qualsiasi altro sistema in grado di emulare un terminale start-stop, dovete utilizzare l'apposito adattatore fornito a corredo dello Stargate:



## CAPITOLO 4

### 4 Configurazione Stargate

#### 4.1 Informazioni Generali

Dopo aver realizzato le connessioni indicate nel capitolo 3 si può scegliere una delle modalità di configurazione qui elencate:

- ⇒ se dovete preconfigurare lo Stargate e non disponete di un PC con scheda LAN, potete utilizzare la porta console e l'applicativo StarFire, incluso nel CD fornito a corredo dell'apparato, come descritto nel paragrafo 4.3;
- ⇒ se disponete di un PC con scheda LAN, potete collegarlo direttamente ad una della porte Ethernet di Stargate e procedere con la configurazione da WEB browser, come indicato nel paragrafo 4.4.

**NOTA** Se dovete collegare lo Stargate ad una LAN già installata è probabile che si renda necessario cambiare l'indirizzo assegnato per default allo Stargate (10.0.0.1), per renderlo compatibile con gli indirizzi di sottorete in uso sulla vostra LAN. In questo caso, ***dopo aver effettuato la configurazione iniziale***, procedete come indicato nel paragrafo 4.6, ***prima di collegare Stargate alla LAN***.

Stargate consente di effettuare la configurazione mediante la Command Line Interface, secondo quanto descritto nel capitolo 5. Queste procedure sono però normalmente riservate ad utenti esperti o ad amministratori di sistema, per cui si consiglia di attenersi alle istruzioni che seguono per la prima configurazione, che vi permetterà la connessione ad Internet.

#### 4.2 Configurare la connessione ad Internet

Per accedere rapidamente a Internet con Stargate, occorre munirsi dei dati forniti dal proprio fornitore di servizio (Internet Service Provider) e seguire le istruzioni riportate di seguito. In particolare i dati che interessano sono:

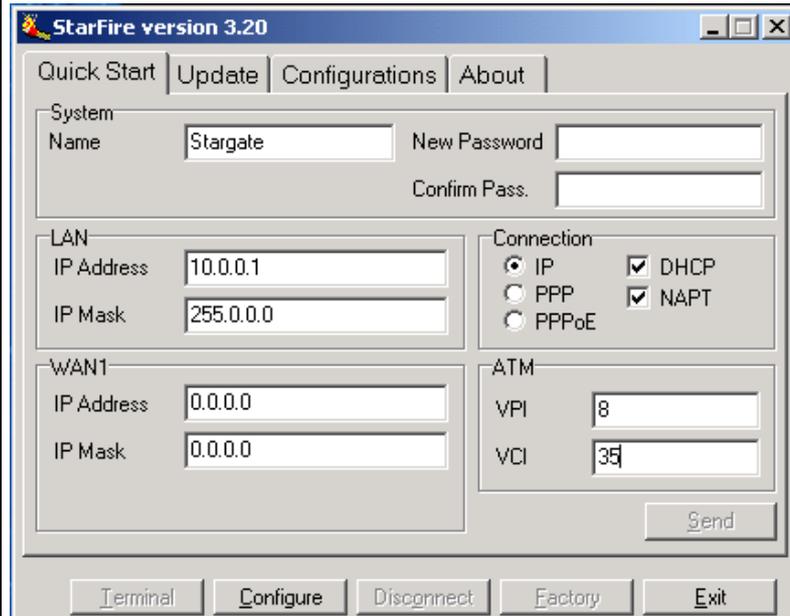
- valore VCI e VPI;
- tipo di incapsulamento adottato dal Provider (PPP over ATM o PPP over Ethernet o IP over ATM);
- Nome Utente e Password assegnata.

Una volta reperite queste informazioni siete pronti per effettuare in pochi istanti la configurazione dello Stargate.

### 4.3 Configurazione tramite StarFire

StarFire è un semplice programma di installazione che utilizza la porta console dello Stargate. Potete trovarlo nel CD fornito a corredo dell'apparato.

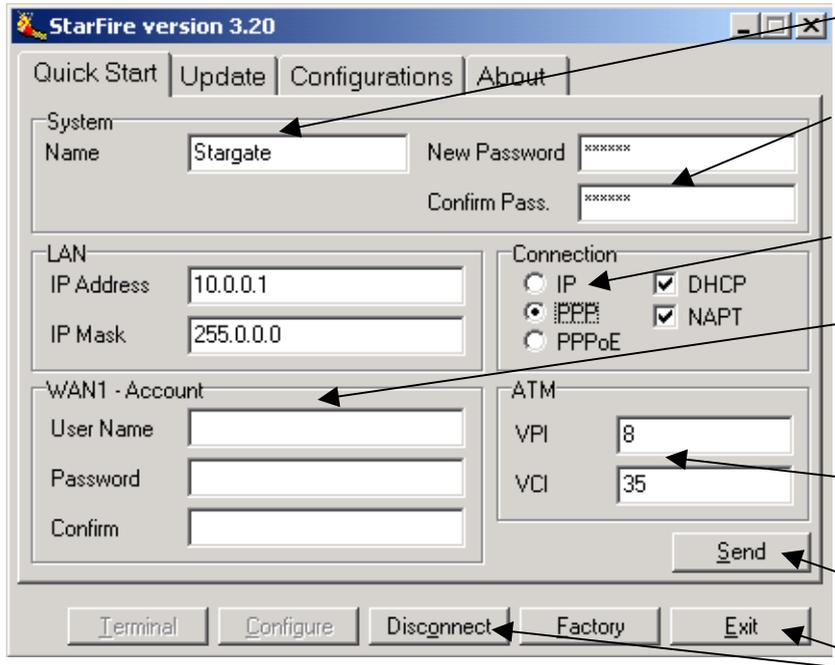
Procedete come indicato nel paragrafo 3.3.4 per collegare il vostro PC alla porta console di Stargate.

<ul style="list-style-type: none"> <li>▪ Avviate il programma Starfire (Starfire.exe);</li> <li>▪ spegnete lo Stargate, riaccendete e non appena il led RDY (fail) inizia a lampeggiare premete il bottone "Connect" ed apparirà il seguente menu'.</li> </ul>	
--	---

**NOTA** *Starfire è configurato per essere connesso alla COM1 di un PC, se utilizzate un'altra porta seriale è possibile configurare StarFire seguendo la procedura riportata di seguito.*

<ul style="list-style-type: none"> <li>▪ Scegliete l'opzione "Configure";</li> <li>▪ nella finestra "Serial" si ha la possibilità di scegliere una diversa porta seriale utilizzata dal PC dove è stato eseguito il programma Starfire;</li> <li>▪ chiudete la finestra con "Done".</li> </ul>	
--	--

A questo punto viene mostrata la configurazione corrente dei parametri visualizzati nello schermo e possono essere inserite tutte le informazioni relative al collegamento ad Internet come riportato nel seguente esempio.



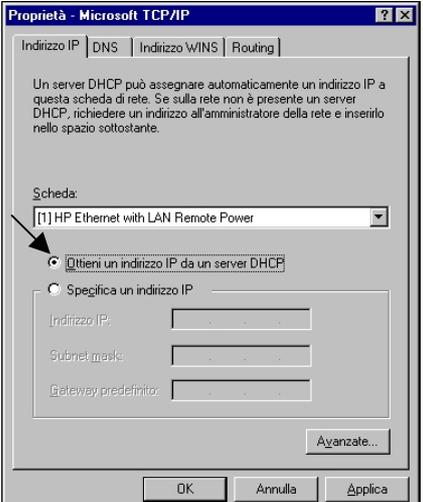
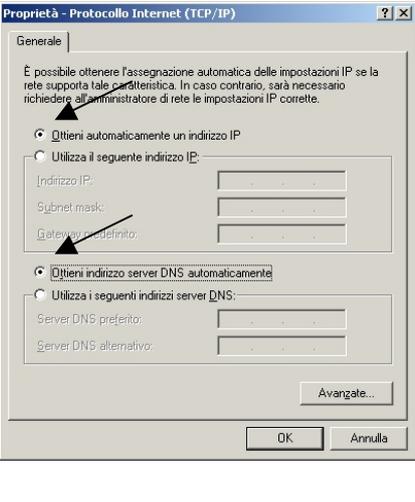
- Inserite il nome che volete assegnare allo Stargate;
- se volete modificare la password di amministratore del sistema compilate gli appositi campi;
- scegliete il tipo di incapsulamento adottato dal proprio ISP;
- con i dati ricevuti dal proprio ISP compilate i campi relativi all'account (UserName, Password e conferma Password);
- inserite i valori di VPI e VCI assegnati dall' ISP;
- premete il bottone "Send";
- uscite dal programma e attendere il riavvio di Stargate.

Seguendo questi pochi passi sarete in grado di accedere in pochi istanti ad Internet.

#### 4.4 Configurazione tramite il WEB server interno

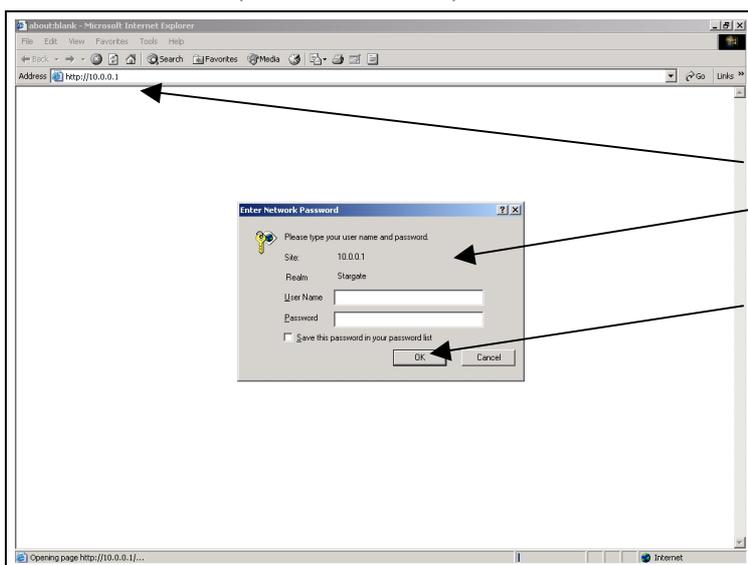
Collegate un PC dotato di interfaccia per LAN ad una della porte Ethernet di Stargate.

Sul PC, aprite il pannello di controllo "configurazione di rete" e configurate i parametri TCP/IP come riportato di seguito:

Windows 98	Windows NT	Windows 2000
		

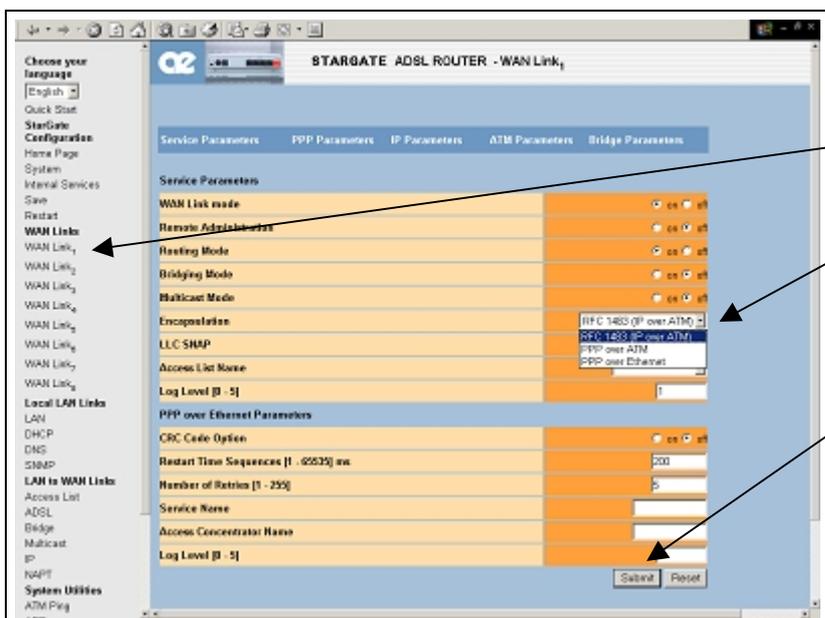
In questo modo, sfruttando i servizi DHCP per configurare automaticamente i parametri di rete dei PC sulla LAN (vedi approfondimenti in appendice B) si potrà da subito aprire il browser e digitare l'indirizzo IP locale assegnato allo Stargate (per default 10.0.0.1).

La prima schermata che Stargate propone è quella relativa all'autenticazione dell'ingresso in configurazione. Se non è stata cambiata, la password è vuota, è sufficiente quindi inserire soltanto un nome utente<sup>2</sup> (max 10 caratteri) e confermare.



- Aprire un WEB browser;
- digitare l'indirizzo 10.0.0.1 o in alternativa semplicemente "Stargate";
- inserire "nome Utente" e "Password" (vuota se non è stata mai modificata);
- confermare la scelta.

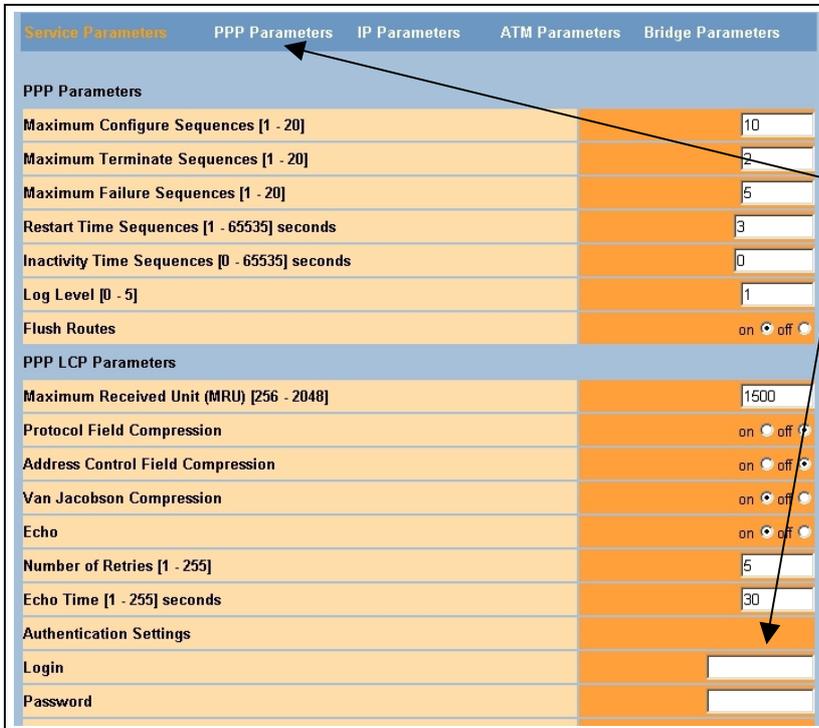
Dalla pagina principale che vi apparirà dopo il "login" effettuare la scelta WAN1 per poter inserire i dati che il Provider vi ha comunicato.



- Scelta Wan1;
- cambiare lo stato della Wan e scegliere il tipo di incapsulamento comunicato dal Provider;
- confermare la scelta.

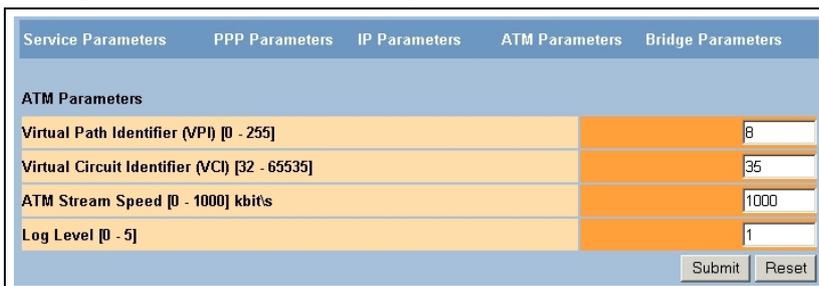
<sup>2</sup> Nel campo nome utente deve essere inserito almeno un carattere alfanumerico. Si consiglia di adottare ad esempio il cognome dell'operatore per avere traccia successivamente dei "logon" effettuati.

Effettuare la scelta “Parametri PPP” per inserire User Name e Password per Internet (comunicati dal Provider nel caso di incapsulamento PPP over ATM o PPP over Ethernet).



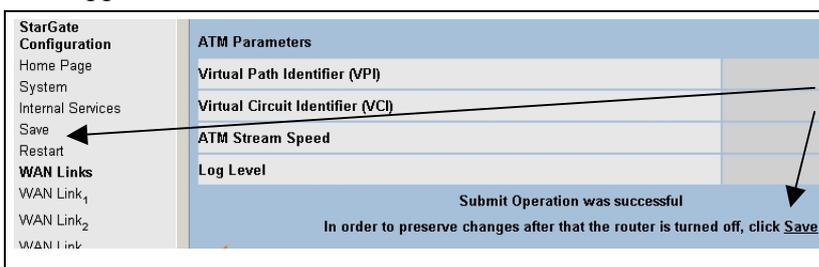
- Effettuare la scelta Parametri PPP;
- inserire User Name e Password;
- confermare la digitazione con il tasto “Submit”.

A questo punto scegliere “Parametri ATM” per poter inserire i dati ATM relativi al vostro collegamento (comunicati dal provider).



- Effettuare la scelta “Parametri ATM”;
- inserire i valori di VPI e VCI;
- confermare con il pulsante “Submit”.

L’ultima operazione da compiere è quella di **salvare** tutte le impostazioni effettuate in modo tale che Stargate memorizzi la configurazione e la renda operativa anche dopo uno spegnimento dell’apparato.



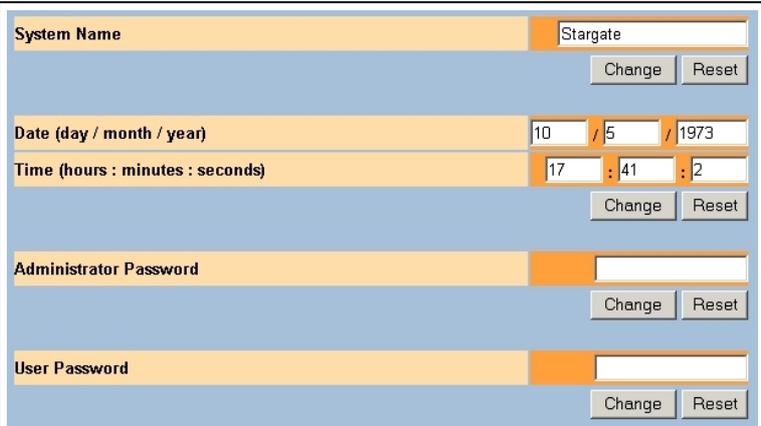
Si può salvare la configurazione sia con il pulsante posto sul frame di sinistra, sia con quello presente in ogni pagina successiva ad una conferma dei dati impostati.

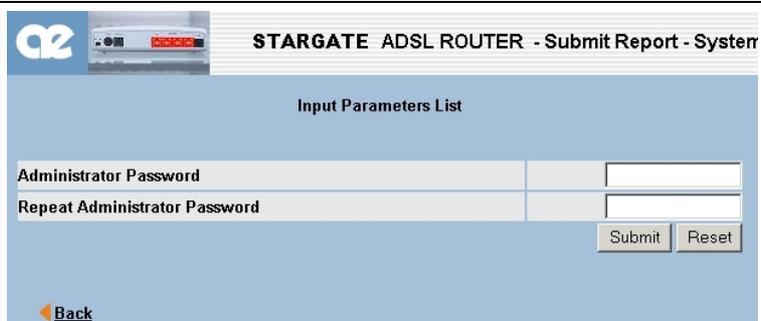
## 4.5 Cambiare la password di sistema

Stargate prevede due livelli di utenti:

- ⇒ Amministratore (Admin);
- ⇒ Utente (User).

Per poter discriminare il livello, occorre configurare due password distinte per i due utenti. Tale operazione è accessibile dalla pagina sistema come riportato di seguito:

	<ul style="list-style-type: none"> <li>▪ Scegliere “Sistema”;</li> <li>▪ cliccare il pulsante “Cambia” in base alla password che si vuole modificare dopo aver immesso la “vecchia password”.</li> </ul>
--	--

	<ul style="list-style-type: none"> <li>▪ Inserire la nuova password su entrambe le finestre;</li> <li>▪ confermare con il pulsante “Invia”.</li> </ul> <p><b>NOTA:</b> ricordarsi di effettuare il salvataggio tramite l'apposito link.</p>
---	---

## 4.6 Modificare l'indirizzo IP dello Stargate

Dopo aver effettuato la configurazione dei parametri essenziali, e prima di collegare lo Stargate ad una LAN esistente, dovete verificare che l'indirizzo IP di default dello Stargate (10.0.0.1) sia compatibile con gli indirizzi in uso sulla LAN.

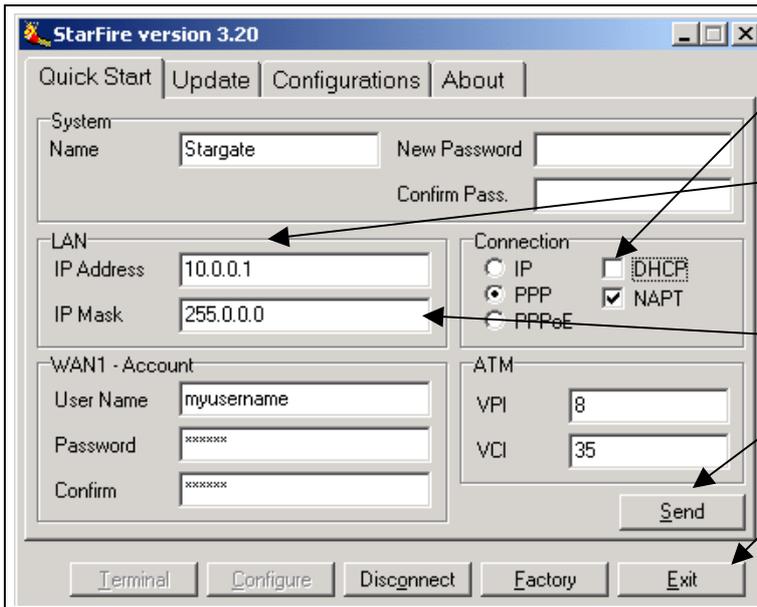
Nel caso in cui dobbiate modificarlo, seguite una di queste procedure.

Mediante browser WEB

<b>StarGate Configuration</b>	LAN Name	lan0
Home Page	Routing Mode	<input type="radio"/> on <input type="radio"/> off
System	Multicast Mode	<input type="radio"/> on <input type="radio"/> off
Internal Services	IP Address	192.168.118.254
Save	Net Mask	255.255.255.0
Restart	LAN Extension	<input type="radio"/> on <input type="radio"/> off
<b>WAN Links</b>	Access List Name	
WAN Link <sub>1</sub>	Log Level [0 - 5]	1
WAN Link <sub>2</sub>	<b>Bridge Parameters</b>	
WAN Link <sub>3</sub>	Bridging Mode	<input type="radio"/> on <input type="radio"/> off
WAN Link <sub>4</sub>	Bridge Select	Bridge1
WAN Link <sub>5</sub>	Bridge Cost [1 - 65535]	100
WAN Link <sub>6</sub>	Bridge Priority [0 - 65535]	128
WAN Link <sub>7</sub>		
WAN Link <sub>8</sub>		
<b>Local LAN Links</b>		
LAN		
DHCP		

- Effettuate la scelta “LAN”;
- inserite l’indirizzo IP e la relativa NET MASK;
- confermate con il pulsante “Invia”;
- salvate le modifiche con l’apposito pulsante;
- spegnere e riaccendere Stargate per rendere operative le modifiche.

Mediante StarFire:



StarFire version 3.20

Quick Start | Update | Configurations | About

System  
Name: Stargate    New Password: \_\_\_\_\_  
Confirm Pass.: \_\_\_\_\_

LAN  
IP Address: 10.0.0.1  
IP Mask: 255.0.0.0

Connection  
 IP     DHCP  
 PPP     NAPT  
 PPPoE

WAN1 - Account  
User Name: myusername  
Password: \*\*\*\*\*  
Confirm: \*\*\*\*\*

ATM  
VPI: 8  
VCI: 35

Send

Terminal    Configure    Disconnect    Factory    Exit

- Togliete la funzionalità DHCP;
- inserite il nuovo indirizzo IP da assegnare allo Stargate;
- inserite la “Net Mask”;
- confermate le modifiche con il pulsante “Send”;
- uscite dal programma e attendere il riavvio dello Stargate.

## 4.7 Avviare la connessione ad Internet

Da questo momento in poi siete nel mondo di Internet con la Super Velocità di Stargate. Provate a digitare nella barra degli indirizzi del vostro browser [www.aethra.com](http://www.aethra.com) e sarete i benvenuti:



## CAPITOLO 5

### 5 Programmazione da Console CLI

#### 5.1 Introduzione

Collegando un PC o un terminale con interfaccia seriale RS232 alla porta "console", tramite il cavo in dotazione, si possono effettuare tutte le operazioni di configurazione e gestione dello Stargate.

Avviando un qualsiasi programma di emulazione di terminale, ad esempio il programma "Hyperterminal" di Windows, l'apparato richiederà di autenticarsi con una "username" e una "password", in base alla quale sarete abilitati alle programmazioni relative. Esistono due profili di utenti:

- *Amministratore* (Admin), abilitato a qualsiasi configurazione compresa quella della gestione della password utente;
- *Utente* (User), abilitato alla sola visualizzazione dei parametri configurati dall'amministratore del sistema.

Per mezzo della console potrete configurare lo Stargate anche se non conoscete i parametri relativi all' interfaccia LAN, come tipicamente avviene durante la prima installazione. Successivamente potrete configurare lo Stargate anche da uno dei PC connessi alle porte LAN.

La console utilizza un insieme di comandi di configurazione denominato "Command Line Interface" o, più brevemente, CLI.

I comandi disponibili con la CLI sono organizzati in una struttura gerarchica "ad albero", che organizza i parametri in gruppi funzionali, chiamati "*nodi*", con lo scopo di renderne più agevole la navigazione.

#### 5.1.1 Avvio della sessione CLI

Collegare un terminale come riportato nella seguente figura:

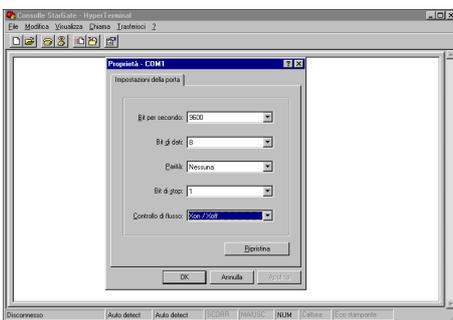


Avviare un programma "terminale" ad esempio Hyperterminal di Windows e scegliere le seguenti opzioni:



Immettere un nome per la connessione, scegliere la porta seriale da utilizzare, modificare le proprietà della connessione in:

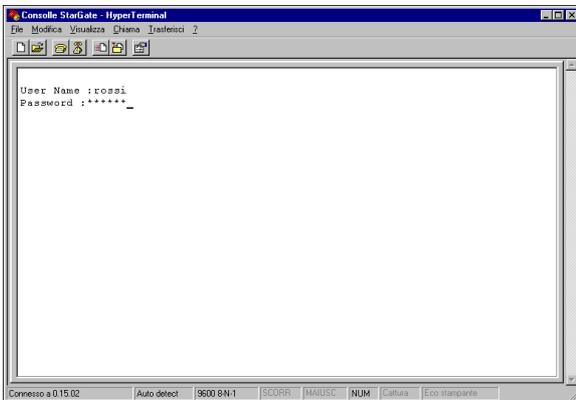
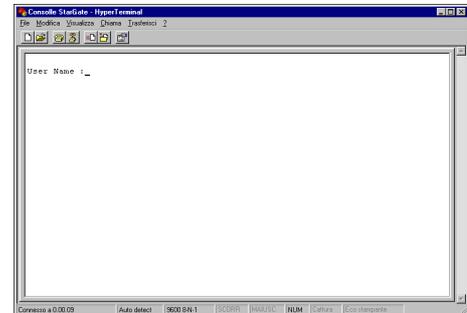
- ⇒ bit per secondo = 9600;
- ⇒ bit di dati = 8;
- ⇒ parità = nessuna;
- ⇒ bit di stop = 1;
- ⇒ flow control = Xon / Xoff.



Confermando la scelta e successivamente premendo il tasto “invio” comparirà l’invito alla digitazione della “user name”.

Questo campo, della lunghezza massima di 10 caratteri, non è rilevante per l’individuazione del profilo d’ingresso in quanto il controllo viene eseguito nella fase

successiva, alla digitazione della password.

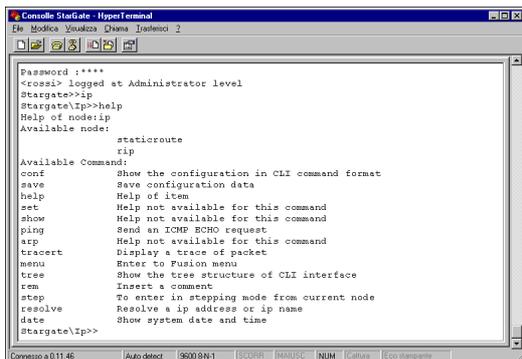


Si consiglia di digitare ad esempio il nome dell’operatore che sta effettuando l’autenticazione in modo da avere, come vedremo più avanti, la traccia di tutti gli ingressi al sistema.

Digitando la password (che per default è vuota) seguita dal tasto “invio”, si avrà dopo alcuni istanti il messaggio relativo al profilo riconosciuto dal sistema.

Se invece lo Stargate non riconosce la password digitata come valida, viene riproposto l’invito ad effettuare una nuova autenticazione.

## 5.1.2 Utilizzo della funzione di aiuto (help)



Quando siete in difficoltà e non sapete il comando da impartire o le opzioni che potete scegliere, digitando “help” saranno elencate le possibili scelte (nodi) e relativamente al nodo in cui vi trovate, i comandi accettati.

```
Stargate\System>>set ?
Command set:
Available node:
  password
Usage:
  DEFAULTS
  NAME <name>
  DATE <mm dd yyyy hh mm ss>
Stargate\System>>
```

Un altro aiuto è possibile ottenerlo digitando un comando seguito da uno “spazio” e dal punto interrogativo (?).

Se conoscete già l’intero percorso da digitare per cambiare un parametro ma non ricordate le possibili opzioni potete far seguire, come nel caso precedente, un punto

```
Stargate>>set system password ?
Command set:
Usage:
  <ADMIN|USER>
Stargate>>
```

interrogativo alla stringa digitata.

Se ricordate le prime lettere del comando, pigiando il tasto “tabulatore”, lo Stargate completa la parola per voi. Questo accorgimento facilita e velocizza l’immissione dei comandi. Inoltre con i tasti freccia in su (↑), freccia in giù (↓) è possibile richiamare gli ultimi 10 comandi impartiti nella sessione corrente.

### 5.1.3 Descrizione della sintassi utilizzata

La descrizione della sintassi utilizzata è la seguente:

- le lettere maiuscole identificano parole chiavi es SET , NETMASK .ecc.;
- <> identifica un parametro;
- <value> indica un parametro numerico 123, 23;
- <string> indica un parametro stringa di tipo alfanumerico;
- <ip add>indica un parametro di tipo ip address nel formato aaa.bbb.ccc.ddd es. 192.118.110.3;
- <ip name> indica un parametro di tipo ip nome, esempio www.xxx.ddd.com;
- il simbolo | indica un’alternativa sui parametri; es <value | TCP | UDP> il parametro può essere o un numero o la parola chiave TCP o la parola chiave UDP.

### 5.1.4 Salvataggio della configurazione

Le modifiche che di volta in volta vengono effettuate, vanno confermate con il comando SAVE. Il salvataggio può essere impartito da qualsiasi “nodo” vi troviate.

Le modifiche effettuate ma non salvate sono subito operative, se le condizioni di lavoro dello Stargate lo consentono, ma una volta spento l’apparato, verranno perse. Ad un successivo riavvio, lo Stargate caricherà l’ultima configurazione salvata.

```
Stargate>>save
Command executed
Stargate>>
```

## 5.2 Generalità sui comandi di configurazione

I comandi di configurazione sono di due tipi:

### Comandi relativi al nodo cui si è posizionati

Alcuni comandi sono eseguibili solo se si è posizionati nel nodo appropriato ad esempio il comando “download” si può impartire solamente se si è posizionati sul nodo principale (root) mentre non viene accettato negli altri nodi.

### Comandi disponibili su ogni nodo.

I comandi disponibili su ogni nodo sono i seguenti:

```
TRACERT <ip add|ip name> -w <timeout> -h <max hops> -d
```

Traccia l'elenco (indirizzo e, se disponibile, il nome) dei router incontrati ("route") per raggiungere l'host di destinazione.

- `<ip add|ip name>` contiene il nome dell'host da raggiungere o il suo indirizzo IP;
- `-w <timeout>` imposta il timeout di attesa/risposta per ogni tentativo ed è espresso in millisecondi (default 2000);
- `-h <max hops>` imposta il numero massimo di passaggi attraverso router che vengono tracciati sul percorso verso l'host di destinazione hops (default 30);
- `-d` con questa opzione, viene visualizzato solo l'elenco degli indirizzi.

Esempio di comando:

```
>>tracert www.aethra.com -w 3000 -h 50 -d ↵
```

(traccia www.aethra.com con un timeout di 3000 millisecondi, con un numero di hops pari a 50, disattivando la risoluzione degli ip address).

```
PING <ip add|ip name>-l<size>-n<packets>-i<TTL>-w<timeout>-f-t
```

Consente di verificare che un host può essere raggiunto. Stargate invia un particolare pacchetto (ICMP ECHO REQUEST) verso l'host di destinazione, il quale darà riscontro della ricezione con un pacchetto ICMP ECHO REPLY.

- `<ip add|ip name>` contiene il nome o l'indirizzo dell'host da raggiungere;
- `-l <size >` imposta la lunghezza del pacchetto da inviare (default 32);
- `-n < packets>` imposta il numero di richieste di eco (default 3);
- `-t` imposta come numero di richieste di eco ad infinito ed è in alternativa all'opzione `-n`. L'operazione viene conclusa quando si preme Ctrl-c;
- `-i <TTL>` imposta il parametro "time-to-live" (TTL) (default 64);
- `-w<timeout>` imposta il timeout di attesa/risposta per ogni tentativo in millisecondi (default 2000 msec);
- `-f` imposta a 1 il flag “Do Not Fragment” (default 0).

Esempio di comando:

```
>>ping www.aethra.com -l 64 -n 5 ↵
```

(esegue un ping verso l'indirizzo www.aethra.com con lunghezza del pacchetto di 64, per 5 volte).

#### ARP <ip add>

Risolve il MAC address dell'indirizzo IP digitato. Se si digita il comando ARP senza nessun indirizzo si visualizza la cache ARP.

Esempio di comando:

```
>>arp 192.168.110.228 ↵
```

#### ATMPING <vpi> <vci> {-e|-s} {-n<packets>|-t}

Consente di verificare l'integrità del collegamento sulla rete ATM. Lo Stargate invia una speciale cella di loopback sul VP e VC indicato che viene ritrasmessa dal destinatario.

**NOTA** *I valori degli indicativi VPI e VCI per la connessione ATM sono assegnati in modo permanente dal gestore della rete. Rivolgetevi al gestore della rete per avere indicazioni sui valori effettivamente in uso.*

- <vpi> = valore del VPI;
- <vci> = valore del VCI;
- -e la cella di loopback viene ritrasmessa dal punto terminale del collegamento ATM (end to end);
- -s imposta il ping segment-to-segment (default);
- -n <packets> imposta il numero di richieste di eco (default 5);
- -t imposta il numero di richieste di eco ad infinito ed è in alternativa all'opzione -n. L'operazione viene conclusa quando si preme Ctrl-C.

Esempio di comando:

```
>>atmping 8 35 -e -n12 ↵
```

(esegue un ping ATM verso il VPI 8 VCI 35 in modalità end to end).

#### RESOLVE <ip add | ip name>

Risolve un indirizzo IP in un nome di host, oppure risolve un nome di host in un indirizzo IP. Il parametro <ip add | ip name> può essere o l'indirizzo IP o il nome dell'host da risolvere.

Esempio di comando:

>>RESOLVE Stargate ↵

(verrà visualizzato l'indirizzo IP assegnato allo Stargate).

#### CONF

Mostra la configurazione di tutti i parametri dei vari nodi indipendentemente dal nodo in cui si sta operando.

#### SAVE

Salva la configurazione corrente. Tutte le modifiche apportate saranno memorizzate nell'apparato e rese operative quando le condizioni di lavoro dello Stargate lo permetteranno.

#### TREE

Visualizza i nodi disponibili a partire da quello corrente. Eseguito dal nodo principale (`root`), permette di visualizzare tutto l'albero dei nodi e quindi di individuare con facilità dove spostarsi per cambiare un determinato parametro.

#### HELP

Mostra i nodi disponibili a partire da quello corrente e i possibili comandi che si possono impartire per quel nodo.

#### SHOW CONF

Mostra parametri di configurazione del nodo corrente e dei "sottonodi" relativi. Se il nodo è configurabile ON/OFF e questo risulta essere OFF, i valori dei parametri del nodo non verranno visualizzati.

#### SHOW WORK

Mostra i parametri operativi del nodo corrente e dei "sottonodi" relativi. Se il nodo è configurabile ON/OFF e questo risulta essere OFF, i valori dei parametri del nodo non verranno visualizzati.

**NOTA** *I valori dei parametri operativi sono trasferiti nei rispettivi parametri di configurazione quando si esegue il comando SAVE .*

#### UP

E' il comando che permette di ritornare al nodo immediatamente superiore.

## TOP

E' il comando che permette di ritornare al nodo principale (`root`).

## QUIT o ^R

Sono i comandi per chiudere la sessione CLI (logout).

## STEP

E' il comando per eseguire la configurazione passo-passo. Il sistema propone in successione di "settare" tutti i parametri relativi al nodo in cui vi trovate e tutti i sottonodi relativi. Una volta proposto l'ultimo parametro di configurazione, viene richiesta la conferma o l'abbandono delle modifiche effettuate (yes/no). E' possibile uscire da questo modo di configurazione digitando ^U o saltare un nodo proposto digitando ^X.

Avviando il comando STEP dal nodo principale (`root`), vengono proposti in successione tutti i possibili parametri dello Stargate.

### 5.2.1 Prompt

Quando si utilizza la CLI per la configurazione, viene sempre visualizzato il simbolo del prompt (`>>`) preceduto dal nome assegnato allo Stargate e il percorso del nodo in cui siete. Nel caso in cui vi troviate nel nodo principale il prompt è preceduto semplicemente dal nome assegnato all'apparato.

Se ad esempio allo Stargate è stato assegnato il nome "AETHRA", il prompt viene visualizzato nel seguente modo:

```
AETHRA>>
```

Il simbolo del prompt indica la possibilità di digitare i comandi.

### 5.2.2 Gerarchia dei comandi

Per la configurazione dello Stargate, è stata scelta una struttura ad "albero" formata da un nodo principale (`root`) e da diversi sottonodi più o meno ramificati in base agli argomenti trattati. La "navigazione" tra i vari nodi è eseguibile digitando semplicemente l'intero percorso per raggiungere il nodo desiderato o in alternativa spostandosi di nodo in nodo fino a raggiungere quello voluto.

Per avere visione della struttura dell'albero basta digitare il comando TREE dal nodo principale:

```

Stargate>>tree ↵
Top system      password
  Napt          proxy
  accesslist
  wan1          ppp          lcp          echorequest
                authentication
                ipcp
                rip
                ip
                atm
                service      pppoe
  wan2          ppp          lcp          authentication
                ipcp
                rip
                ip
                atm
                service      pppoe
  ... ..
  wan8          ppp          lcp          echorequest
                authentication
                ipcp
                rip
                ip
                atm
                service      pppoe
  ip            Route
                rip
  lan0          ip          rip
                extension
  adsl
  dhcp
  dns
  intservices
  snmp
Stargate>>

```

Avendo individuato il percorso da effettuare per arrivare al sottonodo desiderato (ad esempio cambiare le password), si può digitare direttamente tutto il percorso:

```
Stargate>>system password ↵
```

Confermando con il tasto invio ci sposteremo direttamente sul sottonodo voluto:

```
Stargate\System>Password>>
```

A questo punto si può impartire il comando SET ADMIN o SET USER in base al cambio password da effettuare.

### 5.2.3 Visualizzazione della configurazione

Esistono diversi modi di visualizzare la configurazione dello Stargate.

## CONF

E' il comando che mostra tutti i parametri settati indipendentemente dal nodo in cui si opera:

```
Stargate>>conf ↵
```

## SHOW CONF

Mostra i parametri di configurazione del nodo corrente e dei “sottonodi” relativi:

```
Stargate\Lan0\Ip>>show conf ↵  
Show of Stargate Lan0 Ip  
Ip address      : 192.168.110.5  
Net mask       : 0.0.0.0  
Show of Stargate Lan0 Ip Rip  
RIP status    : off  
RIP version   : v1  
Stargate\Lan0\Ip>>
```

## SHOW WORK

Mostra i parametri operativi<sup>3</sup> del nodo corrente e dei “sottonodi” relativi:

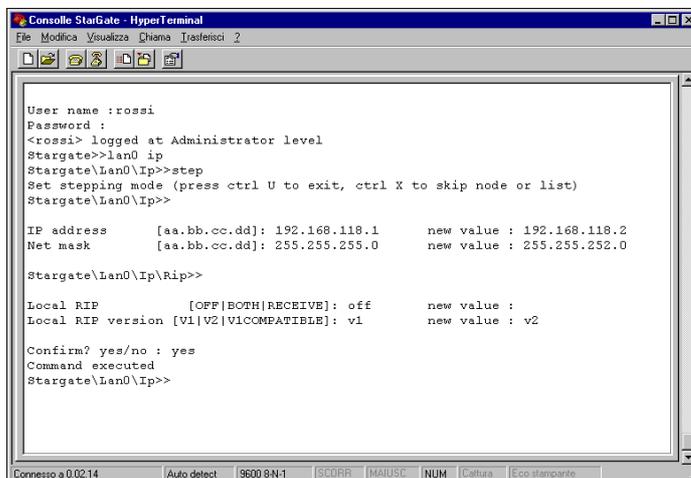
```
Stargate\Lan0\Ip>>show work ↵  
Show of Stargate Lan0 Ip  
Ip address      : 192.168.118.1  
Net mask       : 255.255.255.0  
Show of Stargate Lan0 Ip Rip  
RIP status    : off  
RIP version   : v1  
Stargate\Lan0\Ip>>
```

## 5.2.4 Configurazione passo-passo

### STEP

È il comando per eseguire la configurazione passo-passo. Il sistema propone in successione di settare tutti i parametri del nodo in cui vi trovate e tutti i sottonodi relativi. Una volta proposto l'ultimo parametro di configurazione, viene richiesta la conferma o l'abbandono delle modifiche effettuate (yes/no).

E' possibile uscire da questo modo di



<sup>3</sup> I parametri operativi differiscono da quelli di configurazione quando sono stati modificati alcuni parametri ma lo Stargate non può ancora renderli operativi per le condizioni di lavoro in cui si trova.

configurazione digitando ^U o saltare il nodo proposto digitando ^X.

Avviando il comando **STEP** dal nodo principale (`root`), vengono proposti in successione tutti i possibili parametri dello Stargate ad eccezione del nodo `SYSTEM`.

### 5.2.5 Salvataggio della configurazione

Le modifiche ai parametri di configurazione diventano immediatamente operative solo per alcuni parametri, mentre per gli altri questo non è possibile durante il normale funzionamento.

Il comando `SAVE` memorizza invece **TUTTE** le variazioni effettuate in un *file* di configurazione, mantenuto in una memoria non volatile. Questo *file* viene utilizzato al reboot, quando tutte le variazioni effettuate saranno rese operative.

### 5.2.6 Ripristino della configurazione di fabbrica

#### DELETE CONF

Per riportare lo Stargate nelle medesime condizioni iniziali in cui l'avete ricevuto dalla fabbrica, è sufficiente impartire il comando **DELETE CONF** da qualsiasi nodo.

Questo comando cancella il file di configurazione precedentemente creato o aggiornato da un comando **SAVE**. Al reboot, Stargate non troverà il file di configurazione ed userà per tutti i parametri i valori di default impostati in fabbrica.

- ! *Le password di accesso non vengono riportate al default.*
- ! *Per rendere completamente operativo il comando sarà necessario riavviare lo Stargate (reboot).*
- ! *Se avete inavvertitamente cancellato il file di configurazione potete recuperare la configurazione corrente eseguendo il comando `SAVE`.*

```
Stargate>>delete conf
Command executed
Stargate>>
```

## 5.3 Comandi di configurazione

Di seguito vengono descritte in dettaglio le operazioni da eseguire per la configurazione dello Stargate.

### 5.3.1 Configurazione di sistema

Digitando dal nodo principale il comando `SYSTEM` ci sposteremo nel relativo sottonodo:

```
Stargate>>system ↵
Stargate\System>>
```

In questo nodo si hanno a disposizione i seguenti comandi diretti:

#### LOGINS

Mostra gli eventi degli ultimi 10 ingressi di programmazione al sistema, sia come amministratori che come utenti. Fornisce l'indicazione del nome utente (NAME), livello dell'utente "loggato" (LEVEL), data e ora di ingresso (TIME(start login)), data e ora di uscita dalla programmazione (TIME(close login)) e la porta d'ingresso utilizzata (SOURCE) che può essere CONSOLE, Telnet oppure Server Web con il relativo indirizzo IP del terminale utilizzato:

```
Stargate\System>>logins ↵
LIST OF LOGS
NAME      LEVEL      TIME(start login)  TIME(close login)  SOURCE
Bianchi   Admin      01/02/2001 12:33:30  in progress        CONSOLE
Rossi     Admin      01/02/2001 10:37:04   01/02/2001 10:41:19  (192.168.118.72)
Verdi     User       01/02/2001 09:10:05   01/02/2001 09:40:25  (192.168.118.73)
```

#### SET NAME <string>

Permette di cambiare il nome del sistema (1-20 caratteri, default Stargate):

```
Stargate\System>>set name aethra ↵
Command executed
aethra\System>>
```

Quando il comando viene confermato, il nome del nodo principale assume quello scelto per il sistema.

#### SET DATE [mm gg yyyy hh mm ss]

Consente di modificare la data e l'ora interna dello Stargate (mese, giorno, anno, ore, minuti, secondi):

```
Stargate\System>>set date 01 02 2001 14 57 00 ↵
Command executed
Stargate\System>>
```

Per verificare la data e ora del sistema si può utilizzare il comando **DATE** da qualsiasi nodo:

```
Stargate>>date ↵
Date December 04 2000 Time 14:50:35
Stargate>>
```

Nel nodo SYSTEM è presente il sottonodo **PASSWORD**, che permette di modificare le impostazioni delle password di amministratore e di utente:

```
Stargate\System>>password ↵
Stargate\System>Password>>
```

In questo nodo si hanno a disposizione i seguenti comandi diretti:

#### SET ADMIN

Per modificare la password dell'amministratore (default vuota).

#### SET USER

Per cambiare la password dell'utente (default vuota):

```
Stargate\System>Password>>set admin ↵  
Old password : ↵  
New password :***** ↵  
Repeat new password :***** ↵  
Command executed  
Stargate\System>Password>>
```

Si consiglia di modificare entrambe le password impostandole con gli stessi canoni che si adottano per qualsiasi password di sistema.

### 5.3.2 Configurazione NAT

Lo Stargate supporta le funzionalità avanzate di NAT (Network Address Translation) e PAT (Port address Translation) le quali consentono di utilizzare sulla rete locale indirizzi IP assegnati liberamente, e di usare sulle porte WAN un indirizzo "pubblico" tipicamente fornito da un service provider .

Inoltre questa soluzione consente di utilizzare contemporaneamente più PC sulla LAN per accedere alle risorse esterne (es. Internet) pur avendo attivato con il vostro Service Provider un unico contratto.

Il nodo per la gestione delle sopra elencate funzionalità si chiama NAPT:

```
Stargate>>napt ↵  
Stargate\Napt>>
```

In questo nodo abbiamo le seguenti possibilità di configurazione:

#### SET <ON|OFF>

Per abilitare/disabilitare il NAT e il PAT su tutte le WAN (default ON).

Esempio di disabilitazione del NAPT:

```
Stargate\Napt>>set off ↵  
Command executed  
Stargate\Napt>>
```

#### SET TCPTIMEOUT <value>

Per modificare il timeout per il protocollo TCP (0-100 minuti, default 10).

**SET UDPTIMEOUT <value>**

Per modificare il timeout per il protocollo UDP (0-100 sec default 10).

Esempio per configurare il timeout per il protocollo TCP a 50 minuti:

```
Stargate\Napt>>set tcptimeout 50 ↵  
Command executed  
Stargate\Napt>>
```

**SET DEFAULTSERVER <ip add>**

Consente di assegnare l'IP address di un Server presente sulla LAN interna che soddisferà le richieste di connessione entranti dalle Wan (0.0.0.0 per disabilitare, valore di default).

Esempio di configurazione dell'Address Default Server:

```
Stargate\Napt>>set defaultserver 192.168.118.72 ↵  
Command executed  
Stargate\Napt>>
```

**SET CONNECTEDHOST <ON|OFF>**

Consente di abilitare/disabilitare una particolare funzionalità dello Stargate, che permette all'applicativo Microsoft<sup>®</sup> Netmeeting<sup>™</sup>, che utilizza la negoziazione della porta di comunicazione in banda (esempio per il protocollo H323), di funzionare correttamente (default OFF).

Esempio di abilitazione del connected host:

```
Stargate\Napt>>set connectedhost on ↵  
Command executed  
Stargate\Napt>>
```

**SET LOGLEVEL <0-5> [-s]**

Configura il livello di dettaglio con cui lo Stargate deve registrare gli eventi riferiti alle operazioni di NAT e PAT (default 1).

Nel nodo NAPT troviamo il sottonodo PROXY dove si ha la possibilità di aggiungere dei server proxy:

```
Stargate\Napt>>proxy ↵  
Stargate\Napt\Proxy>>
```

La funzione di proxy server consente di designare un host sulla LAN per rispondere alle richieste di servizio provenienti da una delle porte WAN.

I comandi disponibili in questo nodo sono:

**ADD <public port><priv ip addr><private port><"UDP" | "TCP" | value>**

per aggiungere un proxy (default lista vuota).

<public port>        Numero della porta pubblica che si vuole utilizzare<sup>4</sup> (0-65535).  
<priv ip addr >     Indirizzo IP privato dell'host che da utilizzare come proxy (aa.bb.cc.dd).  
<priv port>         Numero della porta privata che si vuole utilizzare (0-65535).  
<UDP|TCP|value>    Codice del protocollo da assegnare al proxy che si sta configurando (UDP,TCP, 0-65535).

Esempio di aggiunta di un proxy UDP su porta pubblica 10, indirizzo ip privato 192.168.118.70, porta privata 100:

```
Stargate\Napt\Proxy>>add 10 192.168.118.70 100 udp ↵  
Command executed  
Stargate\Napt\Proxy>>
```

**DEL <public port>**

Rimuove un proxy precedentemente creato con il comando ADD. Da notare che è sufficiente individuare il numero della porta pubblica assegnata al proxy per effettuare la cancellazione.

Esempio di cancellazione del proxy dell'esempio precedente:

```
Stargate\Napt\Proxy>>del 10 ↵  
Command executed  
Stargate\Napt\Proxy>>
```

**SET < public port> <"INIP"> <private addr>**

Modifica l'indirizzo ip privato del proxy precedentemente creato.

Esempio di modifica dell'indirizzo ip privato associato alla porta pubblica 10 precedentemente creata:

```
Stargate\Napt\Proxy>>set 10 inip 192.168.118.40 ↵  
Command executed  
Stargate\Napt\Proxy>>
```

**SET < public port> <"INPORT"> <priv port>**

Modifica la porta privata precedentemente assegnata ad un proxy.

Esempio di modifica della porta privata associata alla porta pubblica 10 precedentemente creata:

```
Stargate\Napt\Proxy>>set 10 inport 40 ↵  
Command executed  
Stargate\Napt\Proxy>>
```

---

<sup>4</sup> Questo numero diventerà la chiave di ricerca del proxy aggiunto.

```
SET < public port> <"PROTOCOL"><"UDP" | "TCP" | value>
```

Modifica il tipo di servizio precedentemente associato ad un proxy.

Esempio di modifica del codice protocollo associato alla porta pubblica 10 precedentemente creata:

```
Stargate\Napt\Proxy>>set 10 protocol TCP ↵  
Command executed  
Stargate\Napt\Proxy>>
```

### 5.3.3 Configurazione porte WAN

Lo Stargate permette la configurazione di otto diverse connessioni remote. Sottoscrivendo con il gestore del servizio più circuiti virtuali ATM, si possono effettuare contemporaneamente collegamenti verso destinazioni diverse, ognuna identificata da un valore di VPI/VCI.

Un esempio può essere quello di utilizzare una connessione per raggiungere il proprio Internet Service Provider ed un'altra per collegarsi da un sito periferico alla LAN aziendale. Nello Stargate, il nome attribuito alle otto possibili connessioni è WANx, dove x può assumere un valore da 1 (Wan1) a 8 (Wan8).

Per spostarsi nel sottonodo corrispondente alla WAN desiderata, digitare dalla root il nome della Wan da gestire.

Esempio per Wan1:

```
Stargate>>wan1 ↵  
Stargate\Wan1>>
```

I comandi disponibili in questo nodo sono:

```
SET <ON | OFF>
```

Per abilitare/disabilitare la WAN del nodo in cui si opera (default OFF).

Esempio di abilitazione Wan1:

```
Stargate\Wan1>>set on ↵  
Command executed  
Stargate\Wan1>>
```

```
SET REMOTEADMIN <ON | OFF>
```

Per abilitare/disabilitare la possibilità di entrare nella configurazione dello Stargate da un terminale collegato alla rete remota (default OFF).

Esempio:

```
Stargate\Wan1>>set remoteadmin on ↵  
Command executed  
Stargate\Wan1>>
```

**SET LOGLEVEL <0-5> [-S]**

Permette di indicare il livello di dettaglio sulle indicazioni generate da Stargate a seguito di errori relativi alle prestazioni offerte dal nodo Wan1 (default 1).

Esempio per innalzare il livello dei log per il nodo Wan1 a “3”

```
Stargate\Wan1>>set loglevel 3 ↵  
Command executed  
Stargate\Wan1>>
```

Per il trasporto dei dati, Stargate mette a disposizione tre tipi di incapsulamento: IP over ATM (RFC 2684 ex 1483), PPP over ATM (PPPoA, RFC2364) e PPP over Ethernet (PPPoE, RFC2516). La scelta va effettuata in base al tipo di protocollo supportato dal sistema a cui ci si collega.

Per poter effettuare la scelta desiderata si ha a disposizione il seguente comando nel sottonodo SERVICE:

**SET ENCAPSULATION <PPPOE|PPP|IP>**

Esempio per configurare l'incapsulamento di tipo PPP:

```
Stargate\Wan1\Service>>set encapsulation ppp ↵  
Command executed  
Stargate\Wan1\Service>>
```

Sempre nel nodo SERVICE si ha la possibilità di abilitare/disabilitare la funzione di incapsulamento LLC/SNAP.

Questa funzione permette, quando si trasmettono pacchetti di dati, di inserire un header che indica il tipo di incapsulamento che ha il payload che segue. La selezione del valore del parametro deve essere in accordo con la modalità di funzionamento del server a cui Stargate si collega:

**SET LLC SNAP <ON|OFF>**

Per default l'incapsulamento LLC/SNAP è disabilitato.

Esempio di abilitazione LLC/SNAP:

```
Stargate\Wan1\Service>>set llcsnap on ↵  
Command executed  
Stargate\Wan1\Service>>
```

Una volta scelto il tipo di incapsulamento, si hanno a disposizione tre sottonodi per la configurazione dei rispettivi parametri caratteristici.

### 5.3.3.1 Nodo PPP

Per il protocollo PPP si hanno a disposizione i seguenti comandi nel sottonodo PPP:

**SET MAXCONFIGURE <value>**

Numero massimo di richieste di instaurazione sessione PPP sulla WAN (CFG REQUEST), oltre il quale il tentativo è giudicato fallito (1- 20, default 10).

**SET MAXTERMINATE <value>**

Numero massimo di invio di richieste di abbattimento della connessione PPP (TERMINATE REQUEST) oltre il quale la connessione viene comunque abbattuta (1- 20, default 2).

**SET MAXFAILURE <value>**

Numero massimo di riscontri negativi durante la fase di negoziazione dei parametri della sessione PPP (CFG NAK) prima di inviare un accettazione (CFG ACK) (1- 20, default 5).

**SET RESTARTTIMER <value>**

Imposta il timeout tra un tentativo e il successivo per tutti i parametri sopra indicati (1- 30 secondi, default 3 sec.).

**SET FLUSHROUTES <ON | OFF>**

Per abilitare/disabilitare la cancellazione dalla tabella di routing delle routes dinamiche che partono dall'interfaccia WANx quando la sessione PPP viene terminata (default ON).

**SET INACTIVITYTIME <value>**

Per indicare il tempo oltre il quale, se non transitano più pacchetti di dati la sessione PPP viene abbattuta (0- 65535 secondi, default 0)

Esempio di modifica del timeout tra un tentativo e il successivo a 5 secondi:

```
Stargate\Wan1\Ppp>>set restarttimer 5 ↵  
Command executed  
Stargate\Wan1\Ppp>>
```

**SET LOGLEVEL <0-5> [-S]**

Permette di indicare il livello di dettaglio sulle indicazioni generate da Stargate a seguito di errori relativi alle prestazioni offerte dal sottonodo PPP (default 1):

Scendendo nel sottonodo LCP (Link Control Protocol) troviamo le seguenti configurazioni:

**SET MRU <value>**

Per configurare il valore espresso in bytes del parametro MRU (Max Receive Unit) (256-1500, default 1500).

**SET PFC <ON | OFF>**

Per attivare/disattivare la compressione del campo PID (default OFF).

**SET ACFC <ON | OFF>**

Per attivare/disattivare la compressione del campo Address e Control (default OFF).

**SET ECHO <ON | OFF>**

per abilitare/disabilitare lo Stargate all'invio di pacchetti PPP ECHO REQUEST per verificare lo stato del link PPP (default ON).

Esempio di abilitazione ACFC:

```
Stargate\Wan1\Ppp\Lcp>>set acfc on ↵  
Command executed  
Stargate\Wan1\Ppp\Lcp>>
```

Il sottonodo ECHOREQUEST mette a disposizione i seguenti parametri:

**SET MAXRETRIES <value>**

per inserire il numero massimo di richieste di ECHO oltre il quale, se non c'è stata risposta da parte del Server, viene terminato il link PPP (1...255, default 5).

**SET TIME <value>**

per configurare il timeout tra una richiesta di ECHO e la successiva (1...255 secondi, default 30 sec.).

Esempio configurazione numero richieste di ECHO:

```
Stargate\Wan1\Ppp\Lcp\EchoRequest>>set maxretries 10 ↵  
Command executed  
Stargate\Wan1\Ppp\Lcp\EchoRequest>>
```

Per accedere ad un Server PPP, normalmente viene richiesta l'autenticazione tramite un "nome utente" ed una "password". Inoltre, per il protocollo PPP viene specificata anche la modalità con cui verranno scambiate le informazioni relative all'autenticazione.

### 5.3.3.2 Parametri di Autenticazione

Per la configurazione di questi parametri si ha a disposizione il sottonodo AUTHENTICATION:

```
Stargate\Wan1\Ppp>>authentication ↵  
Stargate\Wan1\Ppp\Authentication>>
```

#### SET USERNAME <string>

Per inserire un “nome utente” per l’autenticazione (0-25 caratteri, default vuoto).

#### SET PASSWORD <string>

Per inserire la password di autenticazione (0- 15 caratteri, default vuoto).

Esempio per inserire il “nome utente” per la Wan1:

```
Stargate\Wan1\Ppp\Authentication>>set username abcdef ↵  
Command executed  
Stargate\Wan1\Ppp\Authentication>>
```

#### SET PAP <ON | OFF>

Per abilitare/disabilitare la modalità di autenticazione PAP (default ON).

#### SET CHAPMD5 <ON | OFF>

Per abilitare/disabilitare la modalità di autenticazione CHAP MD5 (default ON).

Per quanto riguarda la modalità di autenticazione, lo Stargate supporta sia quella di tipo PAP che di tipo CHAP MD5.

Se durante la fase di negoziazione del protocollo di autenticazione, Stargate riceve la richiesta di utilizzare un protocollo non supportato, viene indicato come alternativa il protocollo CHAPMD5 (a meno che non sia stato disabilitato), in quanto più sicuro per il modo con cui cripta l’invio della password.

Esempio per disabilitare la modalità CHAP MD5:

```
Stargate\Wan1\Ppp\Authentication>>set chapmd5 off ↵  
Command executed  
Stargate\Wan1\Ppp\Authentication>>
```

Il sottonodo IPCP contiene un parametro per abilitare la compressione Van Jacobson:

```
Stargate\Wan1\Ppp>>ipcp ↵  
Stargate\Wan1\Ppp\Ipcp>>
```

**SET VJCOMP <ON | OFF>**

Abilitando il parametro relativo, lo Stargate è in grado di ricevere dati dal remoto pacchetti compressi con la tecnica Van Jacobson (default ON).

### 5.3.3.3 Nodo PPPoE

Alcuni ISP utilizzano per gli accessi dei propri clienti, il protocollo PPP over Ethernet, il quale consente loro maggiore facilità di gestione degli account e monitoraggio del traffico svolto dai singoli utilizzatori. Questa tecnica prevede l'incapsulamento di trame Ethernet all'interno del link PPP.

Se il contratto sottoscritto con il Provider è del tipo sopra descritto, occorre scegliere questa modalità di incapsulamento (vedi paragrafo 5.3.3). Nel seguito il server PPPoE viene denominato anche "Access Concentrator".

Per i parametri specifici del protocollo PPP over Ethernet si ha a disposizione il sottonodo PPPOE:

```
Stargate\Wan1\Service>>pppoe ↵  
Stargate\Wan1\Service\PPPOE>>
```

**SET FCSPRESERVED <ON | OFF>**

Per abilitare/disabilitare l'opzione "Preserved CRC", che definisce se nei pacchetti inviati e ricevuti debba essere mantenuto il codice di rivelazione di errore (CRC-32) presente sulla trame Ethernet (default OFF)<sup>5</sup>.

**SET RESTARTTIMER <value>**

Per configurare il valore iniziale di un Timer utilizzato nella fase iniziale di *Discovery*, nella quale Stargate cerca di scoprire se un server PPPoE è raggiungibile. Il timer viene utilizzato per la prima ritrasmissione dei pacchetti "PADI" e "PADR", nel caso non si ottenga alcuna risposta. Il valore impostato viene poi raddoppiato ad ogni successiva ritrasmissione. (1-65535 msec., default 200 msec.).

**SET MAXRETRY <value>**

Per inserire il numero massimo di tentativi di ritrasmissione ad esempio di "PADI" (1-255, default 5).

---

<sup>5</sup> questo codice è ridondante in quanto già presente a livello AAL5

**SET SERVICENAME <string>**

Per inserire il nome di un determinato servizio richiesto ai Server in ascolto (max 32 caratteri, default vuoto di conseguenza Stargate accetta il primo proposto dall'Access Concentrator).

**SET ACNAME <string>**

Per inserire il nome di un "Access Concentrator" in cui si trova il servizio voluto (max 32 caratteri, default vuoto per cui Stargate accetta il primo che si presenta).

Esempio per modificare il tempo di Restart Timer a 100 msec.:

```
Stargate\Wan1\Service\PPPOE>>set restarttimer 100 ↵  
Command executed  
Stargate\Wan1\Service\PPPOE>>
```

Se non si conoscono né gli Access Concentrator né i servizi resi disponibili dal sistema remoto, lasciando i campi vuoti lo Stargate provvederà ad inserire nei messaggi di negoziazione della sessione PPPoE rispettivamente il primo Access Concentrator e il primo servizio che viene offerto. Per conoscere i parametri sopra descritti offerti dal sistema remoto si ha a disposizione il comando:

**QUERY**

Per visualizzare la lista degli Access Concentrator raggiungibili e i relativi servizi offerti.

Esempio:

```
Stargate\Wan1\Service\PPPOE>>query ↵
```

**NOTA** *User Name e Password si configurano nel nodo Wan1\Ppp\Authentication. (vedere paragrafo 5.3.3.2).*

**SET LOGLEVEL <0-5> [-S]**

Permette di indicare il livello del log che Stargate deve generare per errori relativi alle prestazioni offerte dal sottonodo PPPoE (default 1).

### 5.3.3.4 Nodo IP (Wan)

Questo nodo è riservato alla configurazione dei parametri relativi al protocollo IP sulla WAN che si sta configurando. Come abbiamo visto lo Stargate mette a disposizione otto possibili porte WAN e grazie a queste prestazioni si possono realizzare ad esempio collegamenti multipli ad esempio con più reti remote (sottoscrivendo il servizio presso il proprio gestore di telecomunicazioni).

Approdando nel sottonodo relativo si può accedere alla configurazione dei seguenti parametri:

**SET ADDRESS <ip add>**

Per assegnare l'indirizzo IP della porta WAN (default 0.0.0.0).

*Il valore configurato deve corrispondere esattamente all'indirizzo IP pubblico assegnato alla porta nel caso di incapsulamento IPoA. Negli altri casi (PPPoA e PPPoE), l'indirizzo assegnato viene negoziato con il server durante la fase di configurazione della sessione PPP, nella quale l'indirizzo può essere assegnato dinamicamente dal server PPP. Se l'indirizzo IP configurato viene modificato dal server d'accesso nella fase di configurazione PPP, la maschera di sottorete diviene quella corrispondente alla classe a cui appartiene l'indirizzo assegnato.*

Esempio per assegnare l'indirizzo IP proprio della Wan allo Stargate:

```
Stargate\Wan1\Ip>>set address 192.168.110.1 ↵  
Command executed  
Stargate\Wan1\Ip>>
```

**SET NETMASK <ip add>**

Per assegnare allo Stargate la maschera di sottorete della WAN (default 0.0.0.0, che ha il significato di assegnare la maschera di sottorete implicita nella classe dell'indirizzo IP assegnato).

**SET REMOTEADDRESS <ip add>**

Per indicare l'indirizzo IP del sistema connesso al lato remoto della WAN (default 0.0.0.0). Nel caso di connessione attraverso il PPP, questo indirizzo viene comunicato durante la fase di configurazione della sessione.

**SET ADDRESSVALIDATION <ON|OFF>**

Se abilitata (default OFF), la funzione permette di controllare se l'indirizzo IP sorgente contenuto in ogni pacchetto ricevuto dalla porta WAN è presente nelle tabelle di routing come indirizzo raggiungibile dalla medesima porta WAN. Se l'indirizzo è presente il pacchetto viene accettato, altrimenti viene scartato.

**SET NAPT <ON | OFF>**

Per abilitare/disabilitare la funzionalità di NAPT (configurata nel nodo corrispondente NAPT) nella Wan presa in esame (default ON).

**SET MTU <value>**

Per configurare il parametro MTU (Maximum Transmission Unit) (576-2048, default 1500).

Esempio per disabilitare il NAPT locale sulla Wan1:

```
Stargate\Wan1\Ip>>set napt off ↵  
Command executed  
Stargate\Wan1\Ip>>
```

**SET LOGLEVEL <0-5> [-s]**

Configura il livello di dettaglio con cui lo Stargate deve registrare gli eventi riferiti alle operazioni IP sulla WAN (default 1).

Se si vuole attivare la prestazione di RIP (Routing Information Protocol) in una Wan specifica, si può accedere al sottonodo relativo ed effettuare le configurazioni desiderate:

```
Stargate\Wan1\Ip>>rip ↵  
Stargate\Wan1\Ip\Rip>>
```

I comandi disponibili sono:

**SET <OFF | BOTH | RECEIVE>**

Per scegliere la modalità operativa del RIP (default BOTH):

- ⇒ con OFF l'uso del RIP è disabilitato;
- ⇒ con BOTH lo Stargate invia periodicamente il contenuto della propria tabella di routing su pacchetti RIP ed utilizza i pacchetti RIP ricevuti per aggiornare la sua tabella di routing (RIP attivo);
- ⇒ con RECEIVE lo Stargate utilizza i pacchetti RIP ricevuti per aggiornare la sua tabella di routing, senza inviare il contenuto della sua tabella di routing (RIP passivo).

**NOTA** *Per il funzionamento del RIP, è necessario che questo venga abilitato con il comando descritto nel paragrafo 5.3.4).*

Esempio per abilitare sulla Wan1 il RIP passivo:

```
Stargate\Wan1\Ip\Rip>>set receive ↵  
Command executed  
Stargate\Wan1\Ip\Rip>>
```

**SET VERSION <V1 | V2 | V1COMPATIBLE>**

Per configurare la versione di RIP utilizzata:

- ⇒ con V1 Stargate utilizza la versione 1 del protocollo;
- ⇒ con V2 Stargate utilizza la versione 1 del protocollo;

⇒ con V1COMPATIBLE lo Stargate utilizza la versione 2 del RIP, ma senza indirizzi di multicast, ed è quindi in grado di funzionare con altri router che supportano solo la versione 1.

Esempio per scegliere la versione V1COMPATIBLE:

```
Stargate\Wan1\Ip\Rip>>set version v1compatible ↵  
Command executed  
Stargate\Wan1\Ip\Rip>>
```

### 5.3.3.5 Nodo ATM (Wan)

Questo nodo è riservato alla configurazione dei parametri caratteristici di una connessione ATM. In particolare è di fondamentale importanza richiedere al gestore del servizio ADSL i valori di VPI e VCI assegnati. Per accedere alla configurazione di questi parametri spostarsi nel sottonodo relativo ATM:

```
Stargate\Wan1>>atm ↵  
Stargate\Wan1\Atm>>
```

#### SET VPI <value>

Indica il valore dell'identificativo del "virtual path" associato alla porta. I valori ammessi vanno da 1 a 255, il valore di default è 8.

#### SET VCI <value>

Indica il valore dell'identificativo del "virtual circuit" associato alla porta. I valori ammessi vanno da 32 a 65535, il valore di default è di 35 per WAN1, 36 per WAN2, fino a 42 per WAN8.

#### SET SPEED <value>

Per impostare la massima velocità nella direzione verso la rete (Upstream) . I valori vanno da 0 a 1000 Kbit/sec, con default di 1000 Kbit/sec. Se viene impostato il valore 0, viene comunque configurata una velocità Upstream di 32 Kbit/sec, che è la minima di funzionamento.

Esempio per configurare il VCI con un valore di 50:

```
Stargate\Wan1\Atm>>set vci 50 ↵  
Command executed  
Stargate\Wan1\Atm>>
```

#### SET LOGLEVEL <0-5> [-S]

Permette di indicare il livello del log che Stargate deve generare per errori relativi alle prestazioni offerte dal sottonodo ATM (default 1).

### 5.3.4 Configurazione RIP

Stargate, se opportunamente configurato è in grado di trasmettere informazioni relative alle proprie tabelle di routing, ma anche di riceverle dagli altri routers connessi sulla rete WAN o LAN.

Per far deve essere abilitato il protocollo RIP (Routing Information Protocol) in modo tale che il contenuto della tabella di routing interna allo Stargate venga periodicamente trasmetta agli altri router e che venga aggiornata con il contenuto dei pacchetti RIP ricevuti.

Queste abilitazioni sono disponibili nel seguente sottonodo:

```
Stargate>> ip rip ↓
Stargate\Ip\Rip>>
```

I comandi disponibili in questo sottonodo sono:

<b>SET &lt;ON   OFF&gt;</b>
-----------------------------

Per abilitare/disabilitare il RIP su tutte le WAN (default OFF)

Esempio per abilitare il RIP

```
Stargate\Ip\Rip>>set on ↓
Command executed
Stargate\Ip\Rip>>
```

<b>SET ROUTEADVICE&lt;ON   OFF&gt;</b>
--

Per abilitare/disabilitare la notifica in rete (route ICMP advertisement) da parte dello Stargate di essere un apparato router (default OFF)

```
Stargate\Ip\Rip>>set routeadvic on ↓
Command executed
Stargate\Ip\Rip>>
```

Quando il RIP è disabilitato o nei casi in cui si deve raggiungere una rete diversa da quella direttamente connessa alla Wan, si possono utilizzare delle rotte statiche (Static Route) configurate manualmente all'interno dello Stargate. Per aggiungere delle Static Route spostarsi nel seguente sottonodo:

```
Stargate>>ip route ↓
Stargate\Ip\Route>>
```

I comandi disponibili in questo sottonodo sono:

<b>ADD &lt;ip add dest&gt;&lt;ip add netmask&gt;&lt;ip add gateway&gt;&lt;value ifc&gt;&lt;value cost&gt;</b>
---

Per aggiungere una rotta statica alla lista delle Static Route (default lista vuota).

<ip add dest >	Indirizzo IP della rete finale che si vuole raggiungere.
<ip add netmask>	Valore di Subnet Mask della rete di destinazione.
<ip add gateway>	L'indirizzo IP del primo router sulla rotta indicata.
<value ifc>	Numero dell'interfaccia WAN da utilizzare. Ad esempio se si vuole utilizzare l'interfaccia WAN3, inserire in questo campo 3.

<value cost> Il parametro, che può assumere i valori da 1 a 15, fornisce l'indicazione del "costo" dell'instradamento in termini del numero di reti da attraversare (hops) .

Esempio per inserire una rotta statica per utilizzando la Wan3 (penultimo valore digitato):

```
Stargate\Ip\Route>>add 172.168.0.1 255.255.255.0 192.168.0.0 3 2 ↵
Command executed
Stargate\Ip\Route>>
```

Per eliminare una rotta precedentemente creata utilizzare l'apposito comando DEL:

**DEL <ip add dest ><ip add netmask>**

Per rimuovere una route dalla lista delle Static Route.

Esempio per rimuovere la rotta creata nell'esempio precedente:

```
Stargate\Ip\Route>>del 172.168.0.1 255.255.255.255 ↵
Command executed
Stargate\Ip\Route>>
```

Se si esegue il comando di visualizzazione della configurazione (SHOW CONF) quando non è stata ancora editata alcuna rotta si avrà il seguente risultato:

```
Stargate\Ip\Route>>show conf ↵
Show of Stargate Ip Route
LIST OF AVAILABLE INTERFACE
CODE  NAME  INTERFACE
0      LAN0
1      ATM_VC1      (corrispondente al canale virtuale impostato su Wan1)
2      ATM_VC2      (corrispondente al canale virtuale impostato su Wan2)
3      ATM_VC3      (corrispondente al canale virtuale impostato su Wan3)
4      ATM_VC4      (corrispondente al canale virtuale impostato su Wan4)
5      ATM_VC5      (corrispondente al canale virtuale impostato su Wan5)
6      ATM_VC6      (corrispondente al canale virtuale impostato su Wan6)
7      ATM_VC7      (corrispondente al canale virtuale impostato su Wan7)
8      ATM_VC8      (corrispondente al canale virtuale impostato su Wan8)

LIST OF STATIC ROUTE
DEST IP ADD      NET MASK      GATEWAY ADD      INTERFACE      COST      TYPE
192.168.3.0      255.255.255.0  0.0.0.0          Lan0           0         LOCAL
Stargate\Ip\Route>>
```

**!** *Si consiglia di non rimuovere dalla lista delle route, quella locale che ha un valore dipendente dall'indirizzo IP assegnato allo Stargate. Se ciò accadesse si potrebbero verificare dei malfunzionamenti della rete locale.*

### 5.3.5 Configurazione rete locale (LAN)

Partendo dal nodo principale (root), possiamo spostarci nei sottonodi relativi alla configurazione dei parametri della rete locale (LAN0):

```
SET NAME <string>
```

Per assegnare alla rete locale un nome diverso dal default (LAN0) il quale verrà utilizzato quando la configurazione di un parametro richiede il nome della LAN (max 16 caratteri non intervallati da spaziatura) ad esempio vedi paragrafo 5.3.4, nodo “\Ip\Route”:

```
Stargate\Lan0>>set mylan ↵  
Command executed  
Stargate\Lan0>>
```

Nel sottonodo IP avremo:

```
Stargate\Lan0\Ip>>
```

```
SET ADDRESS <ip add>
```

Per assegnare allo Stargate l’indirizzo IP sulla LAN (default 10.0.0.1):

```
Stargate\Lan0\Ip>>set address 192.168.118.1 ↵  
Command executed  
Stargate\Lan0\Ip>>
```

```
SET NETMASK <ip add>
```

Per assegnare allo Stargate la maschera di sottorete sulla LAN (default 255.0.0.0):

```
Stargate\Lan0\Ip>>set netmask 255.255.255.0 ↵  
Command executed  
Stargate\Lan0\Ip>>
```

Spostandosi nel seguente sottonodo RIP avremo:

```
Stargate\Lan0\Ip\Rip>>
```

```
SET <OFF | BOTH | RECEIVE>
```

Per abilitare il RIP sulla LAN (default OFF) con le modalità descritte nel paragrafo B.6:

```
Stargate\Lan0\Ip\Rip>>set receive ↵  
Command executed  
Stargate\Lan0\Ip\Rip>
```

```
SET VERSION <V1 | V2 | V1COMPATIBLE>
```

Per scegliere la versione RIP utilizzata localmente (default V1), con le modalità descritte nel paragrafo 5.3.4:

```
Stargate\Lan0\Ip\Rip>>set version v1compatible ↵  
Command executed  
Stargate\Lan0\Ip\Rip>>
```

Per poter ampliare la rete locale mediante ad esempio un ulteriore Hub, si può utilizzare la porta 4 (vedi paragrafo 3.3.1) avendo cura di effettuare la configurazione che segue spostandosi sul nodo opportuno:

```
Stargate\Lan0\Extension>>
```

**SET <ON|OFF>**

Per abilitare/disabilitare la porta Ethernet n° 4 per altra LAN o HUB (default OFF):

```
Stargate\Lan0\Extension>>set on ↵  
Command executed  
Stargate\Lan0\Extension>>
```

Una volta confermato il comando si udirà un klik interno all'apparato dovuto alla commutazione di un relè sulla porta Ethernet n°4.

### 5.3.6 Configurazione DHCP

**SET <ON|OFF>**

Per disabilitare/abilitare il server DHCP (default ON).

Esempio per disabilitare DHCP

```
Stargate\Dhcp>>set off ↵  
Command executed  
Stargate\Dhcp>>
```

**SET STARTADDRESS <IP ADD>**

Indica il primo degli indirizzi a disposizione del server DHCP per l'assegnazione agli host sulla LAN (default 10.0.0.2 ovvero l'indirizzo IP successivo a quello assegnato per default allo Stargate sulla LAN).

**SET ENDADDRESS <IP ADD>**

Indica l'ultimo indirizzo a disposizione del server DHCP per l'assegnazione agli host sulla LAN (default 10.0.0.50 corrispondente ad un pool di 49 indirizzi).

**NOTA** *Gli indirizzi del pool utilizzato dal server DHCP devono essere compatibili con quello assegnato allo Stargate.*

Esempio di inserimento primo indirizzo:

```
Stargate\Dhcp>>set startaddress 192.168.118.0 ↵  
Command executed  
Stargate\Dhcp>>
```

#### **SET HOSTNAME <string>**

Per configurare il nome base degli host (0-20 caratteri, default PC\_ ). Agli host che vengono configurati verrà assegnato un nome composto dal nome base seguito da due cifre decimali (es. PC\_01, PC\_02).

#### **SET DOMAINNAME <string>**

Per configurare il nome del dominio (0-23 caratteri, default DomName)

Esempio di configurazione del nome dominio:

```
Stargate\Dhcp>>set domainname aethra ↵  
Command executed  
Stargate\Dhcp>>
```

#### **SET DEFAULTROUTER <ip add>**

Per inserire l'indirizzo del router di default (default l'indirizzo assegnato allo Stargate sulla LAN). Questa informazione viene inclusa nella configurazione assegnata dal server DHCP agli host sulla LAN.

#### **SET DNS1 <ip add>**

Per configurare l'indirizzo del DNS primario (default l'indirizzo assegnato allo Stargate sulla LAN). Questa informazione viene inclusa nella configurazione assegnata dal server DHCP agli host sulla LAN.

#### **SET DNS2 <ip add>**

Per configurare l'indirizzo del DNS secondario (default 0.0.0.0). Questa informazione viene inclusa nella configurazione assegnata dal server DHCP agli host sulla LAN.

Esempio di configurazione del DNS secondario del DHCP:

```
Stargate\Dhcp>>set dns2 192.168.110.5 ↵  
Command executed  
Stargate\Dhcp>>
```

#### **SET WINS1 <ip add>**

Per configurare l'indirizzo del WINS primario (default 0.0.0.0). Questa informazione viene inclusa nella configurazione assegnata dal server DHCP agli host sulla LAN.

**SET WINS2 <ip add>**

Per configurare l'indirizzo del WINS secondario (default 0.0.0.0). Questa informazione viene inclusa nella configurazione assegnata dal server DHCP agli host sulla LAN.

**SET LEASETIME <value>**

Per programmare il tempo in secondi durante il quale viene garantito all'host l'uso dell'indirizzo assegnato.(0-32767 ,0=Disable, default 2000).

**SET LOGLEVEL <0-5> [-s]**

Configura il livello di dettaglio con cui lo Stargate deve registrare gli eventi riferiti alle operazioni DHCP (default 1).

### 5.3.7 Configurazione DNS

Stargate offre una funzionalità di server e forwarder DNS, allo scopo di rendere più semplice la configurazione e l'installazione dei PC sulla LAN. Quando la funzionalità di DNS server/forwarder è attiva, le richieste di risoluzione (queries) di un nome di host possono essere rivolte direttamente a Stargate.

Invece di inserire sui uno o più server DNS esterni, è sufficiente configurare l'indirizzo IP di Stargate sulla LAN come DNS server primario.

Le queries per un nome di host locale sono risolte da Stargate, mentre le queries per la risoluzione di un nome di host remoto sono ribattute da Stargate verso uno o più DNS esterni, i cui indirizzi sono configurati in una lista di server. Stargate supporta queries ricursive.

Una volta ottenuta la risposta finale, questa viene inviata verso il PC sulla rete locale che ha emesso la query e contemporaneamente viene registrata su una cache locale, in modo da poter essere utilizzata per risolvere localmente successive queries verso lo stesso nome.

**NOTA** *La cache DNS è mantenuta in una memoria non volatile, quindi le informazioni in essa contenute vengono perse quando l'apparato viene spento.*

**SET <ON | OFF >**

Per abilitare/disabilitare la funzionalità di DNS server/forwarder (default ON).

**SET DEFAULTHOST <ON|OFF>**

Abilita/disabilita la risoluzione del nome di sistema dello Stargate (cfr. paragrafo B.5) con l'indirizzo IP dello Stargate sulla LAN. Questo serve per poter indirizzare i servizi interni dello Stargate (Telnet, WEB server) da un PC sulla LAN facendo solamente riferimento al nome assegnato allo Stargate. (default ON).

Esempio di disabilitazione DNS:

```
Stargate\Dns>>set off ↵  
Command executed  
Stargate\Dns>>
```

**SET LOGLEVEL <0-5> [-S]**

Permette di indicare il livello del log per il nodo DNS (0-5, default 1).

**SET MAXRETRIES <value>**

Per configurare il massimo numero di tentativi effettuati verso lo stesso server.(0-255, default 3).

**SET TIMEOUT <value>**

Per configurare il tempo massimo di attesa di una risposta ad una query (0-65535, default 20 sec/10).

Esempio di modifica del Timeout ad un valore di 50 decimi di secondo:

```
Stargate\Dns>>set timeout 50  
Command executed  
Stargate\Dns>>
```

### 5.3.7.1 Inserimento dei server nella lista

È necessario specificare uno o più DNS esterni a cui Stargate possa rivolgere le query relative a nomi di host sconosciuti. Per aggiungere dei server DNS alla lista si hanno varie opzioni:

**ADD <string domain name> <ifc value>**

Questa opzione specifica che sull'interfaccia WAN(x) (<ifc value>), che deve essere configurata con incapsulamento PPP o PPPoE, si deve ricercare un server DNS (primario ed eventualmente secondario) che verrà comunicato dal server d'accesso (avente per dominio <string domain name>) durante la negoziazione IPCP. Lo stesso indirizzo verrà cancellato al termine della sessione PPP o PPPoE.

**ADD <string domain name><ip add primary>**

Questa opzione specifica l'indirizzo di un server DNS per il dominio indicato .

```
ADD <string domain name><ip add primary><ip add secondary>
```

Questa opzione specifica gli indirizzi di due server DNS per il dominio indicato

Quando il nome di dominio è rappresentato dalla stringa <any>, il relativo server DSN viene interrogato indipendentemente dal dominio a cui appartiene l'host name. Nell'elenco dei server interrogati, questo server sarà comunque l'ultimo.

**NOTA** È possibile inserire un solo server DNS con l'opzione <any>.

```
DEL <string domain name>
```

Rimuove dalla lista il server DNS relativo al dominio indicato . Se il nome di dominio è vuoto viene rimosso il server <any>.

### 5.3.8 Configurazione SNMP

Il protocollo SNMP (Simple Network Management Protocol) consente la gestione dello Stargate attraverso un manager SNMP remoto. Il software implementato è quello di un agent SNMP che permette di monitorare alcuni parametri (statistici) e di decidere, in base ai risultati visualizzati, se cambiare la configurazione dello Stargate. La versione implementata dallo Stargate è SNMPv1 (rfc.1157), la quale permette al manager remoto di gestire gli oggetti rappresentati nelle strutture definite nella MIB-2 (rfc.1155, rfc.1213).

Per consentire tale gestione, si ha a disposizione sotto il nodo SNMP i seguenti comandi:

```
SET <ON | OFF>
```

Per abilitare/disabilitare il servizio SNMP (default OFF).

```
SET READ_COMMUNITY_NAME <string>
```

Per inserire il nome della community abilitata alle operazioni di lettura dei parametri di gestione dello Stargate (default PUBLIC), max 32 caratteri.

```
SET WRITE_COMMUNITY_NAME <string>
```

Per inserire il nome della community abilitata alle operazioni di scrittura dei parametri di gestione dello Stargate (default NULL), max 32 caratteri.

**SET MANAGER <ip add>**

Per indicare l'indirizzo IP del Manager SNMP (default NULL).

**SET AUTHENTICATION\_TRAP <ON|OFF>**

Per abilitare/disabilitare i messaggi di *TRAP* authentication che l'Agent invia al Manager quando la procedura di autenticazione fallisce (default ON).

**SET SYSCONTACT <string>**

Per inserire il contatto del gestore dello Stargate: può essere utilizzato ad esempio un indirizzo e-mail o un l'indirizzo IP o un sito internet (default NULL), max 64 caratteri.

**SET SYSNAME <string>**

Per inserire il nome SNMP<sup>6</sup> allo Stargate (default Stargate), max 64 caratteri.

**SET SYSLOCATION <string>**

Per inserire la posizione geografica, in cui si trova lo Stargate (default NULL), max 64 caratteri.

**SET LOGLEVEL <0-5> [-s]**

Configura il livello di dettaglio con cui lo Stargate deve registrare gli eventi riferiti alle operazioni SNMP (default 1).

### 5.3.9 Configurazione porte di servizio

Accedendo al nodo `INTSERVICES` si ha la possibilità di configurare le porte per accedere ai servizi telnet e http interni.

**NOTA** *Questa operazione è necessaria quando si configura un server interno alla rete. In questo modo si possono distinguere le richieste di connessione ad un server interno, che tipicamente usa un numero di porta "wellknown" (23 per il servizio telnet e 80 per il servizio http).*

```
Stargate>>intservices ↵  
Stargate\InterServices>>
```

I comandi disponibili per questo nodo sono:

---

<sup>6</sup> il nome SNMP è inteso quello che Stargate utilizzerà solo per lo scambio di messaggi con il Manager SNMP

```
SET TELNET <0-65535>
```

per configurare la porta per applicazioni telnet (default 23).

```
SET HTTP <0-65535>
```

per configurare la porta per applicazioni HTTP (default 80).

Esempio per modificare la porta HTTP al valore 8080:

```
Stargate\InterServices>>set http 8080 ↵  
Command executed  
Stargate\InterServices>>
```

### 5.3.10 Visualizzazione degli eventi (Log)

Stargate è in grado di memorizzare una serie di informazioni per la risoluzione dei problemi che potrebbero nascere ad esempio per il cattivo funzionamento della linea ADSL, o di una errata configurazione di qualche parametro relativo alla connessione ATM o al protocollo utilizzato dal server d'accesso remoto. Il livello di log desiderato viene configurato su ogni singolo nodo. L'elenco degli eventi viene memorizzato su un *file* interno e può contemporaneamente essere visualizzato sulla porta console o collegandosi al server telnet interno.

I comandi di seguito elencati sono disponibili in qualsiasi posizione dei vari menù ad eccezione del comando SET LOGLEVEL il quale può essere impartito solo nei sottonodi abilitati:

```
LOG FILE
```

Attiva il salvataggio degli eventi anomali su file interno allo Stargate:

```
Stargate>>log file ↵  
Command executed  
Stargate>>
```

```
LOG CONSOLE
```

Attiva la visualizzazione degli eventi anomali sulla porta CONSOLE. Premendo un qualsiasi tasto si interrompe la visualizzazione, che può essere fatta ripartire con un nuovo comando LOG CONSOLE.

```
LOG FILE CONSOLE
```

Attiva sia l'acquisizione degli eventi anomali su file interno, sia la visualizzazione da CONSOLE. Premendo un qualsiasi tasto si ferma la visualizzazione su CONSOLE ma non l'acquisizione su file. Impartendo di il comando LOG CONSOLE fa ripartire la visualizzazione dei log su CONSOLE.

## LOG STOP

Ferma l'acquisizione degli eventi di log su file. Il file resta a disposizione per successive eventuali consultazioni fino a quando non verrà sovrascritto con altre acquisizioni:

```
Stargate>>log stop ↵  
Command executed  
Stargate>>
```

Se non è stata attivata precedentemente l'acquisizione si avrà invece il seguente messaggio:

```
Stargate>>log stop ↵  
Log not started  
Stargate>>
```

## LOG VIEW

Visualizza l'ultima acquisizione effettuata e quindi salvata su file. Se il file non contiene nessun elemento, lo Stargate risponderà nel seguente modo:

```
Stargate>>log view ↵  
Nothing to show  
Stargate>>
```

## SET LOGLEVEL <0-5> [-s]

Configura il livello di dettaglio con cui lo Stargate deve registrare gli eventi:

0 → nessun tipo di evento anomalo viene memorizzato;

1 → errori (es di protocollo);

2 → errori e warning di primo livello;

3 → errori e warning di primo e secondo livello;

4 → errori, warning di primo e secondo livello e segnalazioni di primo livello;

5 → errori, warning di primo e secondo livello e segnalazioni di primo e secondo livello;

-s → attivando questa opzione da un nodo, Stargate configura lo stesso livello di logs su quel nodo e su tutti i sottonodi a lui dipendenti. Non è possibile eseguire il comando dal nodo principale.

Esempio per configurare il nodo Wan1 e tutti i sottonodi dipendenti ad un valore di log pari a 3:

```
Stargate\Wan1>>set loglevel 3 -s ↵  
Command executed  
Stargate\Wan1>>
```

I nodi e sottonodi interessati alla generazione di "log" sono:

```

Top Napt
    Accesslist
    Wan(x)      ppp
                ip
                atm

                pppoe

    lan0        ip
    adsl
    dhcp
    dns
    snmp
  
```

E' possibile configurare il livello di log su un nodo con l'opzione "-s" in modo da avere per tutti i sottonodi dipendenti lo stesso dettaglio di log e di seguito modificare un singolo sottonodo per avere solo per quello, un livello di dettaglio differente.

### 5.3.11 Salvataggio e ripristino di un file di configurazione

Per permettere il salvataggio della configurazione corrente dello Stargate, al fine di avere la possibilità di ripristinare la stessa in caso di necessità, si ha a disposizione i seguenti comandi eseguiti dal nodo principale (root).

```
UPLOAD <string file name> <ip add >
```

Esegue il salvataggio del file di configurazione in un TFTP server specificato.

```
DOWNLOAD <string file name> <ip add> [-C | -AI | -AC]
```

Esegue il ripristino di un file di configurazione da un TFTP server, precedentemente salvato.

<string file name>	Nome del file con cui salvare la configurazione nel TFTP server o nome del file presente nel TFTP server da ripristinare.
<ip add>	Indirizzo IP del TFTP server dove salvare o prelevare il file di configurazione.
-C	Esegue il download firmware del codice Aethra dello Stargate.
-AI	Esegue il download del file di inizializzazione della sezione ADSL dello Stargate.
-AC	Esegue il download firmware del codice della sezione ADSL dello Stargate.

Esempio di Upload configurazione:

```

Stargate>>upload my_first_config 192.168.118.72 ↵
Command executed
Stargate>>
  
```

## CAPITOLO 6

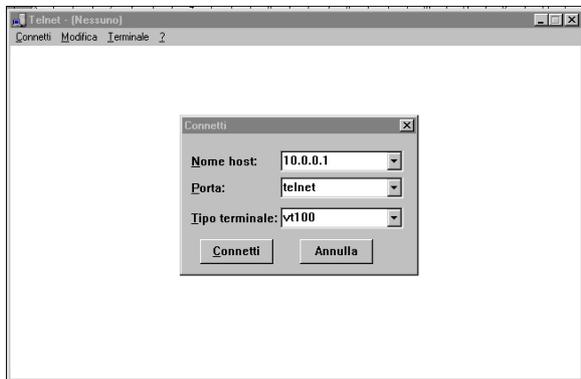
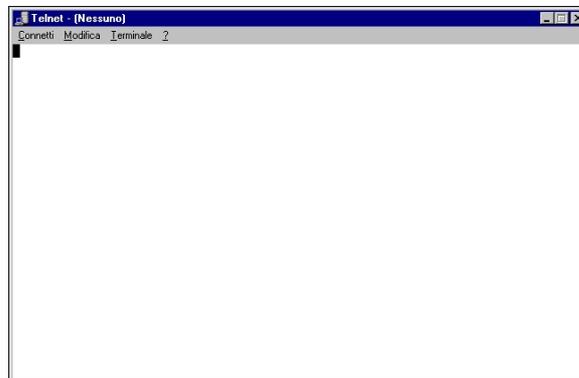
### 6 Configurazione via Telnet

Le configurazioni viste nel capitolo 5 possono essere eseguite anche attraverso un PC collegato sulla LAN di Stargate, avviando una sessione di Telnet.

A differenza della configurazione tramite porta seriale, in questo caso occorre conoscere preventivamente l'indirizzo IP locale assegnato allo Stargate (default 10.0.0.1).

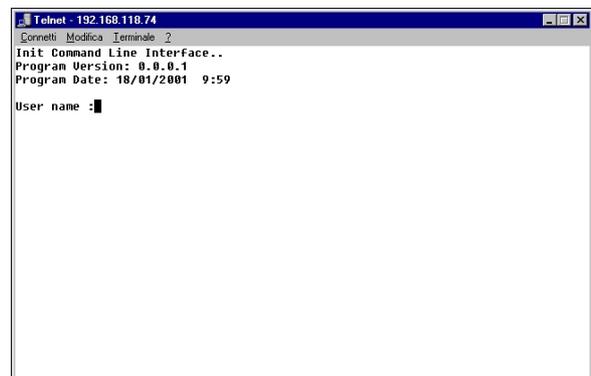
Per accedere alla configurazione via Telnet seguire i seguenti passi:

Aprire il programma Telnet;



da “Connetti” scegliere “Sistema remoto” e inserire nella finestra “Nome host” l'indirizzo IP assegnato allo Stargate e confermare con il pulsante “Connetti”;

a questo punto sarà possibile inserire la “User Name” e Password come descritto nel paragrafo 5.1.1. Le modalità di configurazione sono le stesse utilizzate dalla Console CLI.



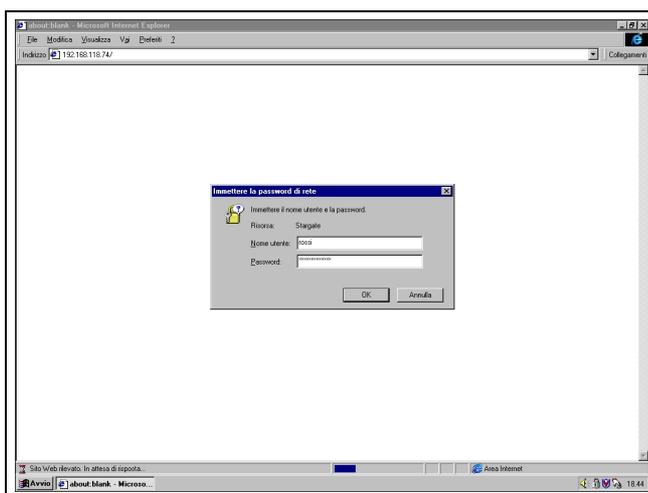
## CAPITOLO 7

### 7 Configurazione da WEB

Stargate include al suo interno un Web Server che facilita la configurazione e la gestione di tutti i parametri anche per utenti meno esperti.

Da qualsiasi PC collegato nella LAN dello Stargate e con l'ausilio di un programma browser (es. Microsoft Explorer o Netscape) si può accedere alle pagine di configurazione digitando l'indirizzo IP locale assegnato allo Stargate (default 10.0.0.1) o in alternativa digitando il nome assegnato all'apparato "Stargate". Se l'indirizzo assegnato a Stargate non è compatibile con la rete locale esistente, si può cambiare attraverso l'interfaccia CLI (vedi paragrafo 5.3.5 Configurazione locale LAN).

Se si sta costruendo invece una nuova LAN, è sufficiente collegare i PC in modo tale da ottenere tutti i parametri TCP/IP dallo Stargate. Infatti l'apparato ha le funzionalità di DHCP server abilitate di default.



- Aprire browser;
- digitare indirizzo ip locale Stargate (nell'esempio 192.168.118.74);
- inserire nome utente e password amministratore o utente. Se la PW non è stata cambiata basta digitare un nome utente qualsiasi, lasciare vuoto il campo Password e confermare con OK;
- Stargate non permette logon privi di nome utente.

Se la Password inserita è riconosciuta valida si accede alle pagine di configurazione, dove, in base al livello di autorizzazione (amministratore o utente), si possono effettuare le operazioni relative.

#### 7.1 Pagine di configurazione

Le pagine di configurazione sono accessibili attraverso i comodi links posti sulla sinistra dello schermo. In base alla scelta effettuata si avrà a disposizione la possibilità di visualizzare e/o modificare i parametri relativi. Occorre ricordare che tutte le modifiche effettuate vanno confermate con la funzione **Salva**. Il pulsante è disponibile sia sul lato sinistro dello schermo, sia quando si conferma una modifica di qualsiasi parametro.

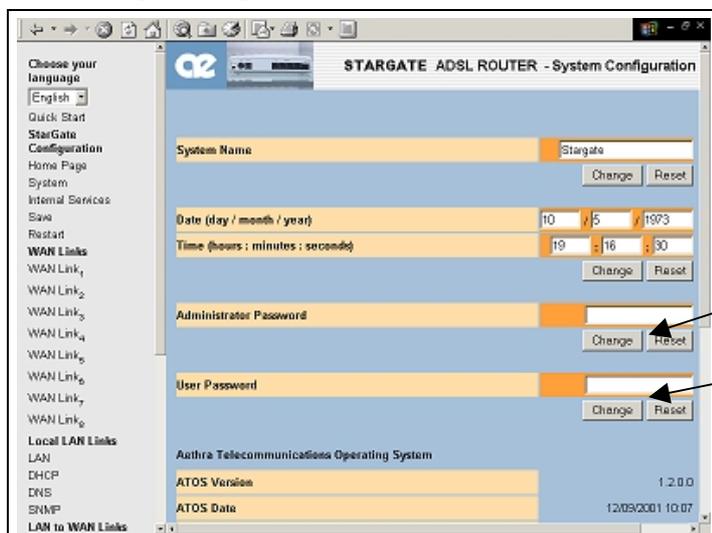
## 7.1.1 Pagina iniziale



- Effettuato il logon viene proposta la videata riportata a fianco;
- la prima finestra in alto permette di cambiare la lingua (italiano, inglese o spagnolo) con cui verranno visualizzati i vari menù;
- per accedere alla schermata dei parametri voluti fare un click con il mouse su uno dei possibili links posti sulla sinistra;
- per salvare le modifiche effettuate cliccare su Salva.

## 7.1.2 Sistema

Per configurare i parametri di sistema effettuare la scelta relativa:



- Per modificare il nome all'apparato, digitare il nome desiderato e premere il pulsante cambia fino alla conferma. Il tasto "Reset" serve per azzerare tutti i caratteri presenti nella finestra;
- per aggiornare data e ora interna allo Stargate e confermare con il pulsante cambia;
- per cambiare la PW amministratore;
- per cambiare PW utente.

Aethra Telecommunications Operating System	
ATOS Version	1.2.0.0
ATOS Date	12/09/2001 10:07
Boot Version	1.2.0.2
Boot Date	29/06/2001 15:09
Download ATOS from a TFTP Server	<input type="button" value="Download"/>
Download ADSL INIT from a TFTP Server	<input type="button" value="Download"/>
Download ADSL CODE from a TFTP Server	<input type="button" value="Download"/>
Download Configuration from a TFTP Server	<input type="button" value="Download"/>
Upload Configuration to a TFTP Server	<input type="button" value="Upload"/>
Restore default parameters	<input type="button" value="Restore"/>

- Per effettuare un Download di un firmware da un TFTP Server;
- per effettuare un Download di una configurazione da un TFTP Server precedentemente salvata;
- per salvare la configurazione in un TFTP server;
- per ripristinare tutti i parametri di configurazione a valore di fabbrica. **Si ricorda che le password di amministratore e utente non vengono riportate a default.**

### 7.1.3 L'interfaccia WAN

Lo Stargate ha la possibilità di utilizzare fino a 8 interfacce WAN. Per configurare una di esse effettuare la scelta opportuna e modificare i parametri alcuni dei quali devono essere comunicati dal gestore del servizio telefonico. Scegliendo ad esempio Wan1 si accede direttamente ai parametri di servizio della Wan.

Service Parameters	PPP Parameters	IP Parameters	ATM Parameters	Bridge Parameters
<b>Service Parameters</b>				
WAN Link mode			<input type="radio"/> on	<input type="radio"/> off
Remote Administration			<input type="radio"/> on	<input type="radio"/> off
Routing Mode			<input type="radio"/> on	<input type="radio"/> off
Bridging Mode			<input type="radio"/> on	<input type="radio"/> off
Multicast Mode			<input type="radio"/> on	<input type="radio"/> off
Encapsulation			RFC 1483 (IP over ATM)	
LLC SNAP			<input type="radio"/> on	<input type="radio"/> off
Access List Name				
Log Level [0 - 5]			1	
<b>PPP over Ethernet Parameters</b>				
CRC Code Option			<input type="radio"/> on	<input type="radio"/> off
Restart Time Sequences [1 - 65535] ms			200	
Number of Retries [1 - 255]			5	
Service Name				
Access Concentrator Name				
Log Level [0 - 5]			1	
<input type="button" value="Submit"/> <input type="button" value="Reset"/>				

- Scegliere Wan1;
- abilitare al funzionamento la Wan scelta. Nel menù a tendina si può scegliere la modalità di collegamento Wan tra IP (RFC 1483), PPP su AAL5 (RFC 2364) e PPP over Ethernet (RFC 2516). **La scelta deve essere effettuata in base alla modalità comunicata dal gestore del servizio;**
- abilitare/disabilitare la gestione remota di Stargate attraverso la Wan;
- scegliere il tipo di incapsulamento (LLC/SNAP o VC muxed) in accordo con la modalità del Server a cui si collega Stargate.

Proseguire la configurazione in base alla modalità di collegamento scelta.

#### 7.1.3.1 Modalità PPP su AAL5 (RFC 2364)

Effettuando la scelta "Parametri PPP" si otterrà la seguente schermata.

Service Parameters	PPP Parameters	IP Parameters	ATM Parameters	Bridge Parameters
<b>PPP Parameters</b>				
Maximum Configure Sequences [1 - 20]				10
Maximum Terminate Sequences [1 - 20]				2
Maximum Failure Sequences [1 - 20]				5
Restart Time Sequences [1 - 65535] seconds				3
Inactivity Time Sequences [0 - 65535] seconds				0
Log Level [0 - 5]				1
Flush Routes				on <input type="radio"/> off <input type="radio"/>
<b>PPP LCP Parameters</b>				
Maximum Received Unit (MRU) [256 - 2048]				1500
Protocol Field Compression				on <input type="radio"/> off <input type="radio"/>
Address Control Field Compression				on <input type="radio"/> off <input type="radio"/>
Van Jacobson Compression				on <input type="radio"/> off <input type="radio"/>
Echo				on <input type="radio"/> off <input type="radio"/>
Number of Retries [1 - 255]				5
Echo Time [1 - 255] seconds				30
<b>Authentication Settings</b>				
Login				
Password				
Password Authentication Protocol				on <input type="radio"/> off <input type="radio"/>

- Scegliere “Parametri PPP”;
- salvo particolari esigenze i parametri impostati sono adeguati a qualsiasi collegamento;
- inserire Nome Utente e Password comunicato dal Provider. Questi valori valgono anche per la modalità PPP over Ethernet;
- scegliere il tipo di autenticazione accettata dallo Stargate. La configurazione di default è normalmente consigliata;
- confermare con il pulsante “Invia”.

### 7.1.3.2 Modalità PPP over Ethernet (RFC 2516)

Se il Provider utilizza la modalità di incapsulamento PPPoE (RFC 2516) effettuare la scelta relativa per configurare adeguatamente i parametri.

PPP over Ethernet Parameters	
CRC Code Option	on <input type="radio"/> off <input type="radio"/>
Restart Time Sequences [1 - 65535] ms	200
Number of Retries [1 - 255]	5
Service Name	
Access Concentrator Name	
Log Level [0 - 5]	1
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Salvo particolari esigenze, tutti i parametri preconfigurati sono adeguati a tutti i tipi di connessione da effettuare.

### 7.1.3.3 Modalità IP (RFC 1483)

Questa modalità viene utilizzata principalmente nelle connessioni LAN to LAN o quando il Provider rende disponibile un indirizzo IP statico.

Service Parameters	PPP Parameters	IP Parameters	ATM Parameters	Bridge Parameters
<b>IP Parameters</b>				
IP Address		0.0.0.0		
Net Mask		0.0.0.0		
Remote IP Address		0.0.0.0		
Address Validation			<input type="radio"/> on <input type="radio"/> off	
NAPT			<input type="radio"/> on <input type="radio"/> off	
Maximum Transmission Unit (MTU) [256 - 2048]			1500	
Log Level [0 - 5]			1	
<b>RIP Messages</b>				
Mode			send and receive	
Version			version	
Submit Reset				

- Scegliere “Parametri IP”;
- inserire l’indirizzo IP pubblico dello Stargate (valore comunicato dal Provider o dall’amministratore della rete nel caso di connessione LAN to LAN)<sup>7</sup>;
- inserire il valore della Net Mask;
- inserire l’indirizzo IP che Stargate deve puntare per raggiungere la rete remota;
- pr abilitare/disabilitare la funzionalità di NAPT (configurata nella pagina corrispondente NAPT);
- per abilitare e scegliere la modalità RIP da utilizzare nella Wan.

### 7.1.3.4 Parametri ATM

Per configurare i parametri caratteristici di una connessione ATM utilizzare l’apposito link della Wan che si intende utilizzare. In particolare è di fondamentale importanza richiedere al gestore del servizio ADSL i valori di VPI e VCI assegnati.

Service Parameters	PPP Parameters	IP Parameters	ATM Parameters	Bridge Parameters
<b>ATM Parameters</b>				
Virtual Path Identifier (VPI) [0 - 255]			8	
Virtual Circuit Identifier (VCI) [32 - 65535]			35	
ATM Stream Speed [0 - 1000] kbit/s			1000	
Log Level [0 - 5]			1	
Submit Reset				

- Scegliere “Parametri ATM”;
- modificare i valori di VPI e VCI comunicati dal gestore del servizio ADSL;
- non modificare il valore della velocità massima del flusso ATM (Upstream) salvo specifiche esigenze.
- confermare con il pulsante “invia”.

### 7.1.4 L’interfaccia LAN

Per poter configurare i parametri TCP/IP della rete locale collegata a Stargate utilizzare l’apposito Link “LAN”. Nella stessa maschera è possibile abilitare la porta Ethernet in modo da poter collegare Stargate a valle di una rete esistente.

<sup>7</sup> Negli altri casi (PPPoA e PPPoE), l’indirizzo assegnato viene negoziato con il server durante la fase di configurazione della sessione PPP, nella quale l’indirizzo può essere assegnato dinamicamente dal server PPP. Se l’indirizzo IP configurato viene modificato dal server d’accesso nella fase di configurazione PPP, la maschera di sottorete diviene quella corrispondente alla classe a cui appartiene l’indirizzo assegnato.

<ul style="list-style-type: none"> <li>WAN Link<sub>0</sub></li> <li>WAN Link<sub>1</sub></li> <li>WAN Link<sub>2</sub></li> <li>Local LAN Links</li> <li>LAN</li> <li>DHCP</li> <li>DNS</li> <li>SNMP</li> <li>LAN to WAN Links</li> <li>Access List</li> <li>ADSL</li> <li>Bridge</li> <li>Multicast</li> <li>IP</li> <li>NAPT</li> <li>System Utilities</li> <li>ATM Ping</li> <li>ARP</li> <li>Log</li> <li>Logins</li> <li>Monitor</li> <li>Ping</li> <li>Resolve</li> <li>Tracert</li> </ul>	<table border="1"> <tr><td>LAN Name</td><td>lan0</td></tr> <tr><td>Routing Mode</td><td><input type="radio"/> on <input checked="" type="radio"/> off</td></tr> <tr><td>Multicast Mode</td><td><input type="radio"/> on <input checked="" type="radio"/> off</td></tr> <tr><td>IP Address</td><td>192.168.116.254</td></tr> <tr><td>Net Mask</td><td>255.255.255.0</td></tr> <tr><td>LAN Extension</td><td><input type="radio"/> on <input checked="" type="radio"/> off</td></tr> <tr><td>Access List Name</td><td></td></tr> <tr><td>Log Level [0 - 5]</td><td>1</td></tr> <tr><td colspan="2"><b>Bridge Parameters</b></td></tr> <tr><td>Bridging Mode</td><td><input type="radio"/> on <input checked="" type="radio"/> off</td></tr> <tr><td>Bridge Select</td><td>Bridge1</td></tr> <tr><td>Bridge Cost [1 - 65535]</td><td>100</td></tr> <tr><td>Bridge Priority [0 - 65535]</td><td>128</td></tr> <tr><td colspan="2"><b>RIP Messages</b></td></tr> <tr><td>Mode</td><td>none</td></tr> <tr><td>Version</td><td>version 1</td></tr> <tr><td colspan="2" style="text-align: right;">Submit Reset</td></tr> </table>	LAN Name	lan0	Routing Mode	<input type="radio"/> on <input checked="" type="radio"/> off	Multicast Mode	<input type="radio"/> on <input checked="" type="radio"/> off	IP Address	192.168.116.254	Net Mask	255.255.255.0	LAN Extension	<input type="radio"/> on <input checked="" type="radio"/> off	Access List Name		Log Level [0 - 5]	1	<b>Bridge Parameters</b>		Bridging Mode	<input type="radio"/> on <input checked="" type="radio"/> off	Bridge Select	Bridge1	Bridge Cost [1 - 65535]	100	Bridge Priority [0 - 65535]	128	<b>RIP Messages</b>		Mode	none	Version	version 1	Submit Reset		<ul style="list-style-type: none"> <li>▪ Scegliere con un click “LAN”;</li> <li>▪ inserire l’indirizzo IP locale con cui i PC vedranno lo Stargate e la relativa Net Mask;</li> <li>▪ abilitare la porta Ethernet n° 4, se necessario, al collegamento di un dispositivo tipo hub o switch Ethernet<sup>8</sup>;</li> <li>▪ se richiesto attivare il RIP con la modalità voluta;</li> <li>▪ confermare le scelte effettuate.</li> </ul>
LAN Name	lan0																																			
Routing Mode	<input type="radio"/> on <input checked="" type="radio"/> off																																			
Multicast Mode	<input type="radio"/> on <input checked="" type="radio"/> off																																			
IP Address	192.168.116.254																																			
Net Mask	255.255.255.0																																			
LAN Extension	<input type="radio"/> on <input checked="" type="radio"/> off																																			
Access List Name																																				
Log Level [0 - 5]	1																																			
<b>Bridge Parameters</b>																																				
Bridging Mode	<input type="radio"/> on <input checked="" type="radio"/> off																																			
Bridge Select	Bridge1																																			
Bridge Cost [1 - 65535]	100																																			
Bridge Priority [0 - 65535]	128																																			
<b>RIP Messages</b>																																				
Mode	none																																			
Version	version 1																																			
Submit Reset																																				

### 7.1.5 Parametri DHCP

Lo Stargate ha abilitato di default il server DHCP, il quale permette, ai dispositivi connessi alle sue porte Ethernet, di ottenere la configurazione TCP/IP nell’istante del “log on”. Questa funzionalità consente una facile gestione della rete da parte degli amministratori in quanto senza dover assegnare manualmente ad ogni PC tutti i parametri TCP/IP, si può adottare una configurazione uguale per tutti i dispositivi collegati.

<table border="1"> <tr><td>DHCP mode</td><td><input checked="" type="radio"/> on <input type="radio"/> off</td></tr> <tr><td>Start Address</td><td>10.0.0.2</td></tr> <tr><td>End Address</td><td>10.0.0.251</td></tr> <tr><td>Default Router</td><td>10.0.0.1</td></tr> <tr><td>WINS Primary</td><td>0.0.0.0</td></tr> <tr><td>WINS Secondary</td><td>0.0.0.0</td></tr> <tr><td>Primary DNS Address</td><td>10.0.0.1</td></tr> <tr><td>Secondary DNS Address</td><td>0.0.0.0</td></tr> <tr><td>Host Name</td><td>PC_</td></tr> <tr><td>Domain Name</td><td>DOMNAME</td></tr> <tr><td>Default Host LifeTime [0 - 32767] seconds</td><td>2000</td></tr> <tr><td>Log Level [0 - 5]</td><td>1</td></tr> <tr><td colspan="2" style="text-align: right;">Submit Reset</td></tr> </table>	DHCP mode	<input checked="" type="radio"/> on <input type="radio"/> off	Start Address	10.0.0.2	End Address	10.0.0.251	Default Router	10.0.0.1	WINS Primary	0.0.0.0	WINS Secondary	0.0.0.0	Primary DNS Address	10.0.0.1	Secondary DNS Address	0.0.0.0	Host Name	PC_	Domain Name	DOMNAME	Default Host LifeTime [0 - 32767] seconds	2000	Log Level [0 - 5]	1	Submit Reset		<ul style="list-style-type: none"> <li>▪ Scegliere “DHCP”;</li> <li>▪ per abilitare/disabilitare il DHCP;</li> <li>▪ primo e ultimo indirizzo IP che Stargate assegnerà agli Host;</li> <li>▪ modificare, se necessario il default router;</li> <li>▪ nome Host base con cui verranno assegnati i nomi agli Host (nell’esempio riportato a lato il primo PC che effettuerà il log on avrà nome host PC_1;</li> <li>▪ nome dominio che verrà assegnato agli host collegati;</li> <li>▪ per variare il tempo di vita degli Host.</li> </ul>
DHCP mode	<input checked="" type="radio"/> on <input type="radio"/> off																										
Start Address	10.0.0.2																										
End Address	10.0.0.251																										
Default Router	10.0.0.1																										
WINS Primary	0.0.0.0																										
WINS Secondary	0.0.0.0																										
Primary DNS Address	10.0.0.1																										
Secondary DNS Address	0.0.0.0																										
Host Name	PC_																										
Domain Name	DOMNAME																										
Default Host LifeTime [0 - 32767] seconds	2000																										
Log Level [0 - 5]	1																										
Submit Reset																											

### 7.1.6 Parametri DNS

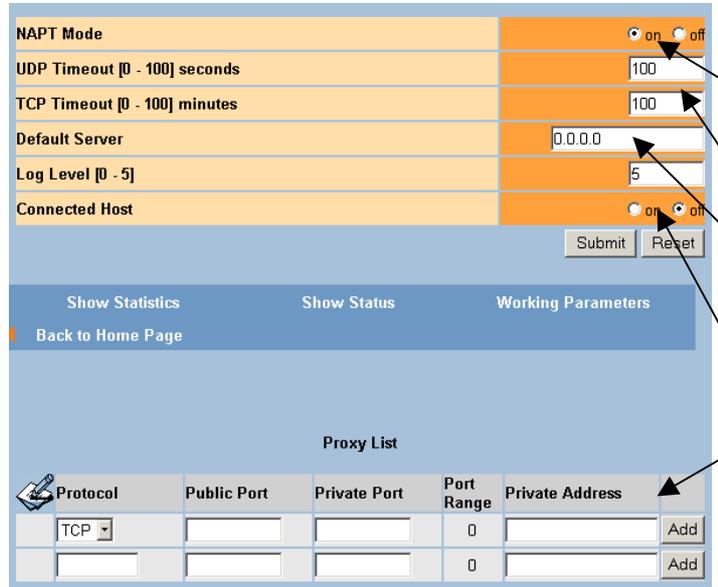
Stargate offre una funzionalità di server e forwarder DNS, allo scopo di rendere più semplice la configurazione e l’installazione dei PC sulla LAN. Quando la funzionalità di DNS server/forwarder è attiva, le richieste di risoluzione (queries) di un nome di host possono essere rivolte direttamente da Stargate.

<sup>8</sup> Non effettuare questa manovra da un PC collegato alla porta Ethernet n° 4 in quanto la commutazione interna dello Stargate renderà immediatamente inutilizzabile tale porta da un PC.

<p><b>DNS</b> <input checked="" type="radio"/> on <input type="radio"/> off</p> <p>Number of Retries [1 - 255] <input type="text" value="3"/></p> <p>Default Host <input checked="" type="radio"/> on <input type="radio"/> off</p> <p>DNS Timeout [0 - 65535] seconds <input type="text" value="20"/></p> <p>Log Level [0 - 5] <input type="text" value="1"/></p> <p style="text-align: right;">Submit Reset</p>	<ul style="list-style-type: none"> <li>▪ Per attivare / disattivare il DNS locale;</li> <li>- parametri da non modificare salvo esigenze particolari.</li> </ul>										
<p style="text-align: center;"><b>DNS Server List</b></p> <table border="1" style="width: 100%;"> <thead> <tr> <th>Domain Name</th> <th>Interface</th> <th>Primary DNS Address</th> <th>Secondary DNS Address</th> <th></th> </tr> </thead> <tbody> <tr> <td>Domain_Name</td> <td>1</td> <td></td> <td></td> <td style="text-align: right;">Delete</td> </tr> </tbody> </table> <p><b>Add new DNS Server from Interface</b></p> <p>Domain Name <input checked="" type="radio"/> New Name <input type="text" value="Domain Name"/> <input type="radio"/> any</p> <p>Interface <input type="text" value="ATM_VC1"/> <input type="button" value="Add"/></p> <p><b>Add new Static DNS Server</b></p> <p>Domain Name <input checked="" type="radio"/> New Name <input type="text" value="Domain Name"/> <input type="radio"/> any</p> <p>Primary DNS Address <input type="text"/></p> <p>Secondary DNS Address <input type="text"/></p> <p style="text-align: right;"><input type="button" value="Add"/></p>	Domain Name	Interface	Primary DNS Address	Secondary DNS Address		Domain_Name	1			Delete	<ul style="list-style-type: none"> <li>▪ Per cancellare eventuali DNS aggiunti;</li> <li>▪ per aggiungere un DNS da prelevare tramite un interfaccia Wan (da 1 per Wan1 a 8 per Wan8);</li> <li>▪ per aggiungere un DNS avendo a disposizione i relativi indirizzi IP.</li> </ul>
Domain Name	Interface	Primary DNS Address	Secondary DNS Address								
Domain_Name	1			Delete							

### 7.1.7 Parametri NAPT (LAN e WAN)

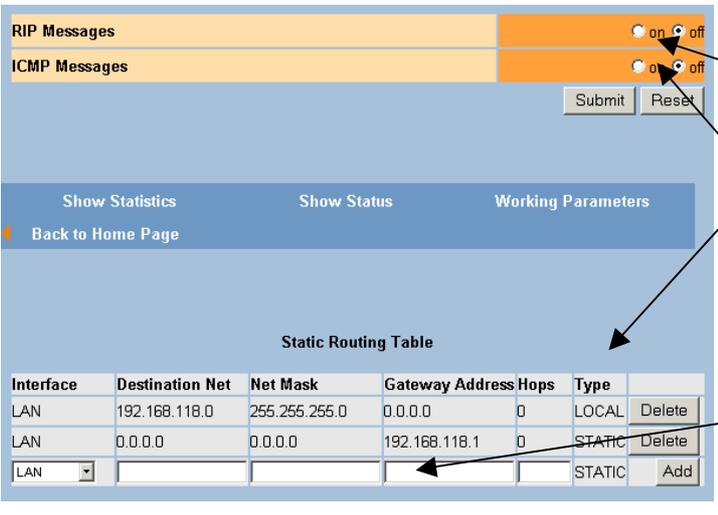
Come descritto in 5.3.2, Stargate supporta le funzionalità di NAT (Network Address Translation) e PAT Port Address Translation). Per poter accedere alla configurazione più opportuna tramite web seguire i passi indicati di seguito:



- Scegliere il link “NAPT”;
- per abilitare / disabilitare la funzionalità di NAPT;
- parametri da non modificare salvo particolari esigenze;
- inserire l’indirizzo IP del Server interno alla LAN che risponderà alle richieste di connessione entranti dalle WAN;
- abilitare solo se si usano applicativi particolari (esempio protocollo H323);
- per aggiungere Server Proxy specifici in base al servizio e alla porta del servizio indicato.

### 7.1.8 Parametri IP (LAN e WAN)

Stargate è in grado di ricevere e trasmettere informazioni relative alle tabelle di routing (RIP) verso altri routers connessi sia sulla LAN che sulle Wan. Per la configurazione dei parametri relativi effettuare la scelta “IP” presente nel frame di sinistra.



- Scegliere il link “IP”;
- per abilitare / disabilitare il RIP;
- per abilitare / disabilitare la notifica in Rete che Stargate è un router;
- **NOTA:** si consiglia di non rimuovere dalla lista delle route, quella locale. Se ciò avvenisse si potrebbero verificare malfunzionamenti sulla LAN.
- per aggiungere delle rotte statiche tramite le quali si possono raggiungere destinazioni da quelle conosciute dai router direttamente connessi sulle WAN.

## CAPITOLO 8

### 8 Configurazione delle Funzioni di Firewall

#### 8.1 Introduzione

Stargate fornisce un meccanismo potente e flessibile per proteggere la rete interna da intrusioni e da attacchi di vario tipo e per consentire la gestione dei diritti di accesso dei singoli host ai vari servizi esterni.

Ad esempio, è possibile far utilizzare la posta elettronica a delle postazioni e non ad altre, permettere la navigazione in Internet a determinati host e negarlo ad altri, consentire l'accesso alla programmazione dello Stargate soltanto alle postazioni configurate opportunamente.

**!** *La configurazione delle funzioni di firewall, in modo particolare se effettuata mediante la CLI, richiede una conoscenza specifica dei protocolli di rete ed è quindi riservata a personale esperto.*

Questo meccanismo si basa sulla formulazione di una serie di **regole**, che vengono utilizzate per filtrare il traffico uscente ed entrante. Queste **regole** sono raccolte in una o più **liste**, denominate appunto **Liste di Accesso**.

Ogni Lista di Accesso può essere assegnata ad una o più interfacce (LAN0, WAN1, ..., WAN8) ed è possibile associare più Liste di Accesso ad ogni interfaccia.

Assegnando una interfaccia ad una lista di accesso, ogni pacchetto entrante da quella interfaccia viene verificato in base alle regole contenute nella lista.

Ogni regola contiene una clausola di permesso (PERMIT) o di negazione (DENY). Si possono verificare tre casi:

- ⇒ il pacchetto soddisfa alle condizioni contenute nella regola, e la regola è del tipo DENY: il pacchetto viene immediatamente scartato;
- ⇒ il pacchetto soddisfa alle condizioni contenute nella regola, e la regola è del tipo PERMIT: il pacchetto viene inoltrato verso la funzione di routing, che provvede all'instradamento del pacchetto verso l'interfaccia di destinazione, senza essere sottoposto ad ulteriori verifiche;
- ⇒ il pacchetto non soddisfa alle condizioni contenute nella regola: il pacchetto viene sottoposto alla regola successiva presente nella lista di accesso.

Se non soddisfa a nessuna delle regole contenute nella lista, il pacchetto viene scartato.

**!** *Si consiglia quindi di creare le Liste di Accesso tenendo conto di tutti gli host presenti nella LAN.*

## 8.2 Creazione e gestione delle Liste di Accesso

Il processo di configurazione delle Liste di Accesso si svolge in due fasi:

- ⇒ si costruiscono una o più Liste di Accesso, specificando per ognuna una sequenza di regole;
- ⇒ le Liste di Accesso così costruite sono associate ad una (o più) interfacce (LAN o WAN).

Si possono definire fino a 40 *liste*, ciascuna con un numero teoricamente illimitato di *regole*.

Per creare una Lista di Accesso si entra nel nodo ACCESSLIST e si utilizza il comando ADD. Il medesimo comando ADD è anche usato per aggiungere regole ad una lista di accesso già esistente.

L'ordine di inserimento delle regole nella lista è importante, in quanto, durante la fase di esecuzione, le regole sono utilizzate nello stesso ordine con cui sono state inserite.

*Per rendere effettive la creazione o le modifiche ad una Lista di Accesso, è necessario operare un RESTART dello Stargate, salvando le modifiche apportate.*

**!** *Se ciò non avviene i parametri di lavoro (visualizzati con SHOW WORK) possono essere diversi da quelli configurati ma non ancora operativi (visualizzati con SHOW CONF).*

*Non è invece necessario operare un RESTART per rendere effettive le associazione delle Liste (quelle presenti nella SHOW WORK) alla LAN0 o alle WAN1..8.*

### 8.2.1 Creazione della lista ed editing delle regole

Il comando ADD, utilizzato per creare una nuova *regola*, ha uno dei seguenti formati:

#### per pacchetti che trasportano un payload TCP

```
ADD <name> <PERMIT|DENY> <TCP|6> <src-address> <dest-address> [<IP-option>] <src-port>  
<dest-port> [<tcp-flag>]
```

#### per pacchetti che trasportano un payload UDP

```
ADD <name> <PERMIT|DENY> <UDP|17> <src-address> <dest-address> [<IP-option>] <src-  
port> <dest-port>
```

#### per pacchetti che trasportano un payload ICMP

```
ADD <name> <PERMIT|DENY> <ICMP|1> <src-address> <dest-address> [<IP-option>] [icmp-  
type]
```

#### per pacchetti che trasportano un protocollo diverso dai precedenti

```
ADD <name> <PERMIT|DENY> <ANYPROT|0-255> <src-address> <dest-address> [<IP-option>]
```

dove:

<name>	è il nome della lista. Se si digita un comando ADD con un nome di lista non esistente, viene creata una nuova lista.
<PERMIT   DENY>	nel primo caso il pacchetto conforme alle regole viene accettato senza ulteriori controlli e viene inoltrato alla funzione di routing; nel secondo caso, il pacchetto viene immediatamente scartato;
<src-address>	il valore contro cui viene verificato l'indirizzo sorgente del pacchetto in esame;
<dest-address>	il valore contro cui viene verificato l'indirizzo di destinazione del pacchetto in esame;
<IP-option>	il valore contro cui viene verificato il campo opzioni IP del pacchetto in esame;
<icmp-type>	il valore contro cui viene verificato il campo icmp-type di un pacchetto ICMP;
<src-port>	il valore contro cui viene verificato il numero di porta sorgente di un pacchetto TCP o UDP;
<dest-port>	il valore contro cui viene verificato il numero di porta destinazione di un pacchetto TCP o UDP.

Di seguito sono riportate le descrizioni delle sintassi da utilizzare nei vari campi:

<name>	contiene il nome della lista, composto da un massimo di 32 caratteri. Si consiglia di utilizzare un nome che identifica facilmente il tipo di filtro che si vuol creare;
<PERMIT   DENY>	contiene la parola chiave PERMIT o la parola chiave DENY
<src-address> e <dest-address>	questi campi indicano i valori con cui confrontare rispettivamente i campi di indirizzo sorgente o destinazione contenuti nell'intestazione IP. Possono assumere le seguenti sintassi:

ANY	non viene effettuato alcun controllo sul campo;
ROUTER	l'indirizzo IP di Stargate sull'interfaccia (LAN o WAN) a cui viene assegnata la lista in cui è inserita questa regola;
LOCALHOSTS	uno indirizzo qualsiasi tra quelli assegnati agli host sulla LAN;
HOST<ip-address>	un host locale individuato con uno specifico indirizzo IP;
HOST<host-name>	un host locale individuato con un nome tra quelli assegnati dal servizio DHCP del router;
<ip-address><ip-wildmask>	un campo di indirizzi ottenuto combinando ip-address con ip-wildmask, che indica quali siano i bit di ip-address da includere nel confronto (un 1 in una posizione di ip-wildmask indica che il corrispondente bit in ip-address non deve essere verificato). ip-address ed ip-wildmask sono rappresentati in notazione decimale puntata (es. 192.168.110.231).

### <ip-option>

Questo parametro è opzionale e, se indicato, specifica valori presenti nel campo `datagram option` dell'header IP.

Si possono indicare i seguenti valori, che possono rappresentare anche più opzioni contemporanee:

ANY-OPTION	per specificare la presenza di una qualsiasi opzione;
SECURITY	indica la presenza dell'opzione Security (02);
LOOSEROUTING	indica la presenza dell'opzione Loose Source Routing (03);
TIMESTAMP	indica la presenza dell'opzione Internet Timestamp (40);
RECORDROUTE	indica la presenza dell'opzione Record Route (07);
STREAMID	indica la presenza dell'opzione Stream ID (08);
STRICTROUTING	indica la presenza dell'opzione Strict Source Routing (09);
SOURCEROUTING	indica la presenza dell'opzione Loose and Strict Source Routing (03 e 09).

### src-port e dest-port

Questi campi sono utilizzati per i pacchetti TCP e UDP. Essi specificano il valore del campo porta di sorgente o destinazione dell'instanziazione del pacchetto TCP o UDP e possono assumere una delle seguenti sintassi:

ANYPORT	qualsiasi porta;
EQU port-numer	una porta con valore numerico port tra 0 e 65535 ;
EQU port-name	una porta tra quelle elencate nella tabella seguente;
RANGE min-p max-p	un campo di valori compreso tra min-p e max-p (0...65535).

I valori mnemonici da usare con EQU sono:

DNS	Domain Name Service (53);
FTP	File Transfer Protocol (21);
FTP-DATA	FTP data connections ( 20);
POP2	Post Office Protocol v2 (109);
POP3	Post Office Protocol v3 (110);
SMTTP	Simple Mail Transport Protocol (25) ;
SNMPTRAP	SNMP Traps (162);
TELNET	Telnet (23);
HTTP	World Wide Web (http, 80);
TFTP	Trivial File Transfer Protocol (69).

### tcp-flag

Questo parametro è opzionale e, se specificato, indica valori presenti nel campo `flag` dell'header TCP.

La sintassi utilizzata è la seguente:

`flag-value flag-wildmask`

dove:

<code>flag-value</code>	indica il valore del campo <code>flag</code> (da 0 a 63)
<code>flag-wildmask</code>	indica quali siano i bit di <code>flag-value</code> da includere nel confronto (un 1 in una posizione indica che il corrispondente bit in <code>flag-value</code> non è verificato)

Il peso dei flag per compilare i due campi sono:

URG	32	RST	4
ACK	16	SYN	2
PSH	8	FIN	1

`icmp-type`

Questo parametro è opzionale e, se specificato, indica valori presenti nel campo `type` dell'header ICMP. Può assumere le seguenti sintassi:

<code>echo-request</code>	rappresenta un pacchetto ICMP di echo-request ( <code>icmp-type = 08</code> )
<code>echo-reply</code>	rappresenta un pacchetto di echo-reply ( <code>icmp-type = 00</code> )
<code>0-255</code>	un qualsiasi valore numerico compreso tra 0 e 255

### 8.2.2 Cancellazione di una lista di accesso

Per eliminare una lista di Access si utilizza il seguente comando:

```
DEL <name>
```

**!** *Non è consentita l'eliminazione di una singola regola da una Lista di Accesso.*

Di seguito sono riportati alcuni esempi esplicativi per la creazione di Access Lists di uso comune.

### 8.2.3 Esempi d'uso: blocco della Posta Elettronica

Per impedire l'utilizzo della posta elettronica, sia in entrata che in uscita, ad un host specifico, ad es. l'host 192.168.118.70, si può creare un Lista di Accesso, con le seguenti regole:

```
add nomail deny tcp host 192.168.118.70 any anyport equ smtp ↓  
add nomail deny tcp host 192.168.118.70 any anyport equ pop3 ↓  
add nomail permit anyprot host 192.168.118.70 any↓
```

Il primo comando crea la Lista d'Accesso "nomail" e definisce la seguente regola:  
scarta immediatamente (deny) un pacchetto che:

- ⇒ utilizza il protocollo tcp;
- ⇒ ha come indirizzo sorgente 192.168.118.70;
- ⇒ ha un valore qualunque dell'indirizzo di destinazione;
- ⇒ ha un valore qualunque della porta di sorgente;
- ⇒ ha come porta di destinazione quella riservata al servizio SMTP.

Il secondo comando aggiunge alla lista nomail una seconda regola:  
scarta immediatamente (deny) un pacchetto che:

- ⇒ utilizza il protocollo tcp;
- ⇒ ha come indirizzo sorgente 192.168.118.70;
- ⇒ ha un valore qualunque dell'indirizzo di destinazione;
- ⇒ ha un valore qualunque della porta di sorgente;
- ⇒ ha come porta di destinazione quella riservata al servizio POP3.

L'ultima regola permette l'inoltro dei pacchetti che:

- ⇒ utilizza un qualsiasi protocollo;
- ⇒ ha come indirizzo sorgente 192.168.118.70.

**!** *Quest'ultima regola è fondamentale per consentire a tutti i pacchetti che non sono utilizzati per la posta elettronica di essere correttamente instradati.  
In mancanza di questa regola, questi pacchetti sarebbero infatti scartati.*

Ad esempio, una regola del tipo:

```
add list-name permit anyprot any any ↓
```

aggiunta in ultima posizione nella lista, consente di inoltrare **tutti i pacchetti che non corrispondono a nessuna delle regole precedenti**.

#### 8.2.4 Verifica di una lista di accesso

Una volta creata la Access List "nomail" possiamo verificarla con il comando SHOW CONF:

```
Stargate\AccessList>>show conf ↓
```

```
ACCESS LIST nomail RULE N.1  
Access right and protocol .. deny tcp  
Source/dest address ..... <host 192.168.118.70><any>
```

```

IP option ..... none
Source/dest port ..... <anyport><equ smtp>
TCP flag (value/wildmask) .. none
ACCESS LIST nomail RULE N.2
Access right and protocol .. deny tcp
Source/dest address ..... <host 192.168.118.70><any>
IP option ..... none
Source/dest port ..... <anyport><equ pop3>
TCP flag (value/wildmask) .. none
ACCESS LIST nomail RULE N.3
Access right and protocol .. permit anyprot
Source/dest address ..... <host 192.168.118.70><any>
IP option ..... none

```

A questo punto, dopo aver effettuato un RESTART, posizionarsi nel nodo CLI LAN0 per associare la Access List “nomail” alla LAN con il seguente comando:

```

Stargate\Lan0>>set accesslistname nomail ↵
Command executed
Stargate\Lan0>>

```

## 8.2.5 Blocco dell'accesso ad Internet

Per bloccare l'utilizzo di internet agli hosts 192.168.118.70 e 192.168.118.71, creare una Access List impartendo i seguenti comandi:

```

add nointernet deny tcp 192.168.118.70 0.0.0.1 any anyport equ http
add nointernet permit anyprot 192.168.118.70 0.0.0.1 any

```

Con SHOW CONF si visualizzerà la seguente configurazione:

```

ACCESS LIST nointernet RULE N.1
Access right and protocol .. deny tcp
Source/dest address ..... <192.168.118.70 0.0.0.1><any>
IP option ..... none
Source/dest port ..... <anyport><equ http>
TCP flag (value/wildmask) .. none
ACCESS LIST nointernet RULE N.2
Access right and protocol .. permit anyprot
Source/dest address ..... <192.168.118.70 0.0.0.1><any>
IP option ..... none

```

## 8.2.6 Blocco del Management di Stargate

Per impedire il management da LAN (configurazione Web e Telnet), da parte dell' host “PC\_1”, si può creare una Access List impartendo i seguenti comandi:

```

add nomanagement deny TCP host PC_1 router anyport EQU HTTP
add nomanagement deny TCP host PC_1 router anyport EQU TELNET

```

Con SHOW CONF si visualizzerà la seguente configurazione:

```

ACCESS LIST nomanagement RULE N.1
Access right and protocol .. deny tcp
Source/dest address ..... <host PC_1><router>
IP option ..... none
Source/dest port ..... <anyport><equ http>
TCP flag (value/wildmask) .. none
ACCESS LIST nomanagement RULE N.2
Access right and protocol .. deny tcp
Source/dest address ..... <host PC_1><router>

```

```
IP option ..... none
Source/dest port ..... <anyport><equ telnet>
TCP flag (value/wildmask) .. none
ACCESS LIST nomangement RULE N.3
Access right and protocol .. permit anyprot
Source/dest address ..... <any><any>
IP option ..... none
```

### 8.3 Assegnazione lista d'accesso alla LAN e alle WANs

Una volta che le Liste di Accesso sono state create e rese operative con il RESTART di Stargate, si procede alla loro assegnazione.

In particolare se la Lista deve agire sulla LAN ci si sposta nel nodo CLI LAN0, o se deve agire su una WAN ci si porta nel nodo CLI WANx e si impartisce il comando:

```
SET ACCESSLISTNAME <list-name>
```

Per indicare quale lista d'accesso agisce.

Il comando

```
SET ACCESSLISTNAME
```

senza l'indicazione di un nome di lista rimuove tutte le associazioni relative alla LAN/WAN in esame. Quindi su questa interfaccia non agisce più alcuna lista d'accesso.

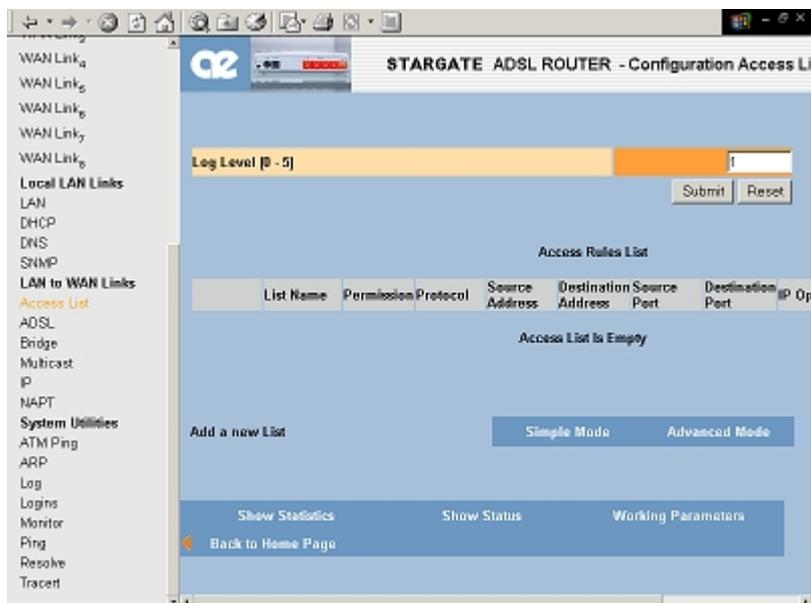
Esempio di assegnazione della Access List "internet" sulla LAN:

```
Stargate\Lan0>>set accesslistname internet
Command executed
Stargate\Lan0>>
```

### 8.4 Configurazione Access Lists da WEB

In questo capitolo viene illustrata la procedura per configurare le Liste di Accesso tramite il browser.

Dopo aver digitato da un browser qualsiasi l'indirizzo dello Stargate ed aver effettuato l'autenticazione:



- effettuare la scelta “Access List”;
- le liste già esistenti vengono elencate nella tabella, dove è possibile verificare le regole presenti;
- è’ possibile eliminare una intera lista ma non una singola regola;
- per aggiungere una Access List, scegliere tra Simple Mode (consigliata per i meno esperti) e Advanced Mode;
- per verificare le Access Lists operative effettuare la scelta “Working Parameters”.

### 8.4.1.1 Simple Mode

<b>List Name</b>	
<input checked="" type="radio"/> - New List	List Name
<input type="radio"/> - Existing List	
<b>Source Address:</b>	
<input checked="" type="radio"/> - Any Host	
<input type="radio"/> - IP Address	0.0.0.0
<input type="radio"/> - DHCP Host List	<empty>
<input type="radio"/> - DHCP Host Name	DHCP Host Name
<b>HTTP Web Browsing</b>	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
<b>Mail Services</b>	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
<b>Administration from LAN</b>	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Submit Reset	
<b>External Ping</b>	
<b>List Name</b>	List Name
<b>External Ping</b>	<input type="radio"/> Permit <input checked="" type="radio"/> Deny
Submit Reset	

- Scegliere se creare una nuova Lists o aggiungere una regola ad una Lists esistente;
- specificare il Source Address dell' host a cui deve essere applicato il test (tutti gli host, un indirizzo numerico di un host o il suo nome host nel caso di DHCP abilitato (default);
- scegliere il servizio da negare o permettere:
  - la navigazione in Internet;
  - il blocco della posta in arrivo ed in uscita;
  - la configurazione dello Stargate;
  - azionare “Submit” per confermare;
- per bloccare tentativi di ping esterni diretti a Stargate
  - scegliere il nome da dare alla Access List “External Ping”;
  - confermare con “Submit”.

**!** Effettuare un **RESTART** per attivare le funzioni così configurate.  
Le associazione delle Access List alla LAN o alle WAN sono invece subito operative.

### 8.4.1.2 Modalità Avanzate

Per impostare delle Liste di accesso con diritti e/o negazioni particolari occorre utilizzare la funzione “Modalità Avanzata”.

Any Protocol	TCP Protocol	UDP Protocol	ICMP Protocol
<b>Any Protocol</b>			
<b>List Name</b>			
<input checked="" type="radio"/> - New List		<input type="text" value="List Name"/>	
<input type="radio"/> - Existing List			
<b>Permission</b>		<input checked="" type="radio"/> Permit <input type="radio"/> Deny	
<b>Source Address:</b>			
<input type="radio"/> - IP Address , Wild Mask		<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="radio"/> - Host IP Address		<input type="text" value="0.0.0.0"/>	
<input checked="" type="radio"/> - Group		<input type="text" value="any"/>	
<input type="radio"/> - DHCP Host List		<input type="text" value="&lt;empty&gt;"/>	
<input type="radio"/> - DHCP Host Name		<input type="text" value="DHCP Host Name"/>	

In base al tipo di protocollo scelto (TCP o UDP o ICMP o ANY), Stargate proporrà dei campi congruenti al tipo di scelta effettuata. In ogni caso:

- scegliere se creare una nuova lista o se aggiungere ulteriori regole a una lista esistente;
- scegliere se la regola corrente è di PERMIT o DENY;
- indicare l'indirizzo sorgente a cui applicare il test specificando:
  - un pool di indirizzi IP, usando un indirizzo e una Wild-Mask;
  - un singolo indirizzo IP ;
  - un gruppo di host;
  - un nome host se è abilitato il server DHCP.

*Se la scelta effettuata è “ANY PROTOCOL”*

<b>Destination Address:</b>			
<input type="radio"/> - IP Address , Wild Mask		<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<input type="radio"/> - Host IP Address		<input type="text" value="0.0.0.0"/>	
<input checked="" type="radio"/> - Group		<input type="text" value="any"/>	
<input type="radio"/> - DHCP Host List		<input type="text" value="&lt;empty&gt;"/>	
<input type="radio"/> - DHCP Host Name		<input type="text" value="DHCP Host Name"/>	
<b>IP Options [Optional]:</b>			
<input type="checkbox"/> any option	<input type="checkbox"/> stream id		
<input type="checkbox"/> strict routing	<input type="checkbox"/> loose routing		
<input type="checkbox"/> record route	<input type="checkbox"/> time stamp		
<input type="checkbox"/> source routing	<input type="checkbox"/> security		
		<input type="button" value="Submit"/>	<input type="button" value="Reset"/>

- Effettuare le medesime scelte anche per l'indirizzo IP di destinazione;
- specificare le Opzioni IP .

Se si è selezionato il protocollo TCP

IP Options [Optional]:	
<input type="checkbox"/> any option	<input type="checkbox"/> stream id
<input type="checkbox"/> strict routing	<input type="checkbox"/> loose routing
<input type="checkbox"/> record route	<input type="checkbox"/> time stamp
<input type="checkbox"/> source routing	<input type="checkbox"/> security
Source Port:	
<input type="radio"/> - Port Number [0 - 65535]	<input type="text" value="255"/>
<input type="radio"/> - Port Type	<input type="text" value="dns"/>
<input type="radio"/> - Port Range [0 - 65535]	<input type="text" value="0"/> min - <input type="text" value="65535"/> max
<input checked="" type="radio"/> - Any Port	
Destination Port:	
<input type="radio"/> - Port Number [0 - 65535]	<input type="text" value="255"/>
<input type="radio"/> - Port Type	<input type="text" value="dns"/>
<input type="radio"/> - Port Range [0 - 65535]	<input type="text" value="0"/> min - <input type="text" value="65535"/> max
<input checked="" type="radio"/> - Any Port	
TCP Flag [Optional]:	
<input checked="" type="radio"/> - none	
<input type="radio"/> Value [0 - 65535] - Wild Mask [0 - 65535]	<input type="text" value="0"/> - <input type="text" value="0"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

- Specificare le condizioni relative alle opzioni IP e alle flag TCP;
- selezionare le condizioni relative alla porte di sorgente e destinazione sia indicando dei singoli valori numerici, sia utilizzando i valori mnemonici presenti nel menu a tendina “Port Type” o inserendo un campo di valori numerici;
- ad esempio se si vuole disabilitare solo l’invio della posta elettronica, selezionare in “Source Port” la porta SMTP presente nella finestra “Port Type”.

Se si è selezionato il protocollo UDP

IP Options [Optional]:	
<input type="checkbox"/> any option	<input type="checkbox"/> stream id
<input type="checkbox"/> strict routing	<input type="checkbox"/> loose routing
<input type="checkbox"/> record route	<input type="checkbox"/> time stamp
<input type="checkbox"/> source routing	<input type="checkbox"/> security
Source Port:	
<input type="radio"/> - Port Number [0 - 65535]	<input type="text" value="255"/>
<input type="radio"/> - Port Type	<input type="text" value="dns"/>
<input type="radio"/> - Port Range [0 - 65535]	<input type="text" value="0"/> min - <input type="text" value="65535"/> max
<input checked="" type="radio"/> - Any Port	
Destination Port:	
<input type="radio"/> - Port Number [0 - 65535]	<input type="text" value="255"/>
<input type="radio"/> - Port Type	<input type="text" value="dns"/>
<input type="radio"/> - Port Range [0 - 65535]	<input type="text" value="0"/> min - <input type="text" value="65535"/> max
<input checked="" type="radio"/> - Any Port	
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

- Specificare le condizioni relative alle opzioni IP;
- selezionare le condizioni relative alla porte di sorgente e destinazione sia indicando dei singoli valori numerici, sia utilizzando i valori mnemonici presenti nel menu a tendina “Port Type” o inserendo un campo di valori numerici;
- ad esempio se si vuole disabilitare l’uso del DNS, selezionare in “Source Port” la porta DNS presente nella finestra “Port Type”.

Se si è selezionato il protocollo ICMP

<b>IP Options [Optional]:</b>	
<input type="checkbox"/> any option	<input type="checkbox"/> stream id
<input type="checkbox"/> strict routing	<input type="checkbox"/> loose routing
<input type="checkbox"/> record route	<input type="checkbox"/> time stamp
<input type="checkbox"/> source routing	<input type="checkbox"/> security
<b>ICMP Type [Optional]:</b>	
<input type="radio"/> - none	
<input checked="" type="radio"/> - Value [0 - 255]	<input type="text" value="0"/>
<input type="radio"/> - Type	<input type="text" value="echo request"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

- Specificare le condizioni relative alle opzioni IP;
- specificare, se occorre, il campo ICMP-Type da controllare indicando un valore numerico o uno di quelli presentati nel menu a tendina;
- ad esempio se si vogliono bloccare le richieste di PING selezionare la voce “echo request” presente nella finestra “Type”.

### 8.4.2 Assegnazione liste d’accesso alla LAN e alle WANs

Una volta create le Access list, in modalità advanced o simple, rese operative con il salvataggio della configurazione e il restart dello Stargate, si può procedere alla loro associazione alla LAN o alle WAN

Per associare una Access List alla rete locale

<b>LAN Name</b>	<input type="text" value="lan0"/>
<b>Routing Mode</b>	<input checked="" type="radio"/> on <input type="radio"/> off
<b>Multicast Mode</b>	<input type="radio"/> on <input checked="" type="radio"/> off
<b>IP Address</b>	<input type="text" value="192.168.118.254"/>
<b>Net Mask</b>	<input type="text" value="255.255.255.0"/>
<b>LAN Extension</b>	<input checked="" type="radio"/> on <input type="radio"/> off
<b>Access List Name</b>	<input type="text" value="nomail"/>
<b>Log Level [0 - 5]</b>	<input type="text" value="1"/>

- Selezionare “LAN”;
- aprire la tendina “Access List Name” e selezionare il nome desiderato dalla lista (nell’esempio “nomail”);
- confermare la scelta con il pulsante “Submit”;
- Stargate chiederà la conferma del salvataggio della configurazione effettuata.

Per associare una Access List ad una interfaccia Wan

Service Parameters	
WAN Link mode	<input checked="" type="radio"/> on <input type="radio"/> off
Remote Administration	<input type="radio"/> on <input checked="" type="radio"/> off
Routing Mode	<input checked="" type="radio"/> on <input type="radio"/> off
Bridging Mode	<input type="radio"/> on <input checked="" type="radio"/> off
Multicast Mode	<input type="radio"/> on <input checked="" type="radio"/> off
Encapsulation	RFC 1483 (IP over ATM) ▾
LLC SNAP	<input type="radio"/> on <input checked="" type="radio"/> off
Access List Name	no_external_ping ▾
Log Level [0 - 5]	1

- Selezionare ad esempio “WAN Link1”;
- aprire la tendina “Access List Name” e selezionare il nome desiderato dalla lista (nell’esempio “no\_external\_ping”);
- confermare la scelta con il pulsante “Submit”;
- Stargate chiederà la conferma del salvataggio della configurazione effettuata.

*Le associazione delle Access List alla LAN o alle WAN sono immediatamente operative anche se la configurazione non è stata salvata.*

**!** *Se si deve effettuare un'associazione che comporta il blocco dell'accesso per configurazione da parte di un host o di un'interfaccia, è necessario farlo da un host o da un'interfaccia diversi da quelli per cui si sta attivando il blocco, altrimenti non risulterà possibile il salvataggio della configurazione.*

*Se si verifica questo inconveniente, occorre spegnere e riaccendere Stargate: in questo modo l'associazione, non essendo stata salvata, non è attiva al riavvio di Stargate.*

## CAPITOLO 9

### 9 Bridging

#### 9.1 Introduzione

La funzione di “bridge” collega tra loro due o più reti LAN Ethernet attraverso un mezzo trasmissivo, effettuando contemporaneamente un’azione selettiva sul traffico: il traffico appartenente alla stessa rete resta confinato su di essa e solo le trame scambiate, appartenenti a reti differenti, transitano attraverso il bridge.

Il bridge svolge quindi due azioni distinte:

1. l’inoltro dei pacchetti da una porta d’ingresso ad una o più porte d’uscita (processo di inoltro o forwarding);
2. l’apprendimento degli host connessi alle singole interfacce (processo di learning).

Per effettuare il processo di learning il bridge analizza l’intestazione (header) di ogni trama Ethernet ricevuta su una delle interfacce e memorizza l’indirizzo MAC di sorgente e l’identificativo dell’interfaccia da cui la trama proviene, aggiungendo un entry nella sua tabella di inoltro (filtering database).

Le informazioni che se ne ricavano servono per determinare la o le porte d’uscita di una trama durante il processo di forwarding.

Il filtering database contiene registrazioni (entry) dinamiche e entry statiche:

1. le entry statiche sono gestite dal livello di management e sono permanentemente memorizzate nel database;
2. le entry dinamiche sono gestite dal processo di learning: esse possono essere aggiunte, aggiornate o rimosse dal filtering database.

Un’ulteriore funzionalità svolta dal bridge è il processo di “spanning tree”. Questo processo trasforma periodicamente una rete contenente maglie chiuse (anelli) in un albero, in modo da eliminare eventuali percorsi circolari sui quali un bridge non opera in maniera corretta: una trama broadcast o multicast inviata su una rete contenente un anello continuerebbe ad essere indefinitamente inoltrato dai bridges sulla rete.

#### 9.2 Implementazione

Stargate può svolgere la funzione di bridge contemporaneamente a quella di router attraverso una selezione del traffico entrante sulle varie interfacce. È infatti possibile abilitare un’interfaccia (LAN o WAN) sia alla funzione di bridging che a quella di routing:

- se un’interfaccia è abilitata solamente alla funzione di routing, i pacchetti IP entranti verranno instradati sulla base del contenuto delle tabelle di routing;
- se un’interfaccia è abilitata solamente alla funzione di bridging, le trame Ethernet ricevute verranno instradate sulla base del contenuto delle tabelle di forwarding;

- se un'interfaccia è abilitata **contemporaneamente** alle funzioni di bridging e di routing, il traffico ricevuto su questa interfaccia viene instradato:
  - sulla base del contenuto delle tabelle di **routing se il traffico è di tipo IP**;
  - sulla base del contenuto delle tabelle di **forwarding se il traffico NON è di tipo IP**.

Stargate determina il tipo di traffico sulla base:

- del campo EtherType sulle trame ricevute dalla LAN;
- dell'intestazione LLC/SNAP sul traffico ricevuto dalle interfacce WAN.

Per questo motivo sulle interfacce WAN l'uso dell'incapsulamento LLC/SNAP viene forzato quando l'interfaccia è abilitata al servizio contemporaneo di bridging e routing.

Per motivi simili l'incapsulamento LLC/SNAP è necessario e viene forzato quando è abilitata la funzione di spanning tree.

Da un'interfaccia abilitata **solamente** alla funzione di bridge non è possibile accedere ai servizi IP interni al dispositivo (WEB server, telnet, ...).

**NOTA** *Se si accede al server WEB interno attraverso la LAN, e su questa è abilitata la sola funzione di "bridging" la connessione viene immediatamente interrotta. Sarà possibile ripristinare la connessione al server WEB solo attraverso la console locale, riabilitando la funzione di routing sulla LAN.*

## 9.3 Configurazione

L'aggiunta della funzionalità di bridging fa comparire i seguenti nodi sull'albero della CLI:

- un nodo BRIDGES, a cui sono collegati quattro sottonodi denominati bridge1, bridge2, bridge3, bridge4, ciascuno dotato di un ulteriore sottonodo spanningtreeprotocol;
- un comando set bridging <ON|OFF> per ciascun nodo WAN o LAN;
- un comando set routing <ON|OFF> per ciascun nodo WAN o LAN.

### 9.3.1 Parametri di configurazione del nodo BRIDGES

Stargate consente di definire fino a quattro tipologie (classi) di bridge. Ogni interfaccia LAN o WAN viene abilitata alla funzionalità di bridge associandola ad una delle classi di bridge.

È possibile configurare il sistema per funzionare da bridge tra la LAN e una o più interfacce WAN solamente tra più interfacce WAN.

```

Stargate\Bridges>>set bridge1 ?
Nodes available:
                                spanningtreeprotocol

Set command parameters:
  <ON|OFF>
  MAXENTRY           <1024|2048|4096|8192>
  AGEINGTIME         <value>
  SPANNINGTREE       <ON|OFF>
  LOGLEVEL           <value> [-s]

Stargate\Bridges>>set bridge1 spanningtreeprotocol ?

Nodes not available.

Set command parameters:
  BRIDGEPRIORITY     <value>
  HELLOTIME          <value>
  FORWARDDELAYTIME  <value>
  MAXAGE             <value>

Stargate\Bridges>>

```

dove:

MAXENTRY	definisce il numero massimo di entry statiche e dinamiche che il bridge è in grado di memorizzare nel suo database di filtering (i valori possibili sono 1024/2048/4096/8192, il valore di default è 1024);
AGEINGTIME	definisce il tempo, espresso in secondi, dopo il quale un'entry dinamica viene rimossa dal database (valori possibili 10~100 000, default 300 secondi);
SPANNINGTREE	abilita/disabilita il bridge alla gestione del protocollo di spanning tree (valori possibili ON/OFF, default OFF);
LOGLEVEL	livello di log per il debug (valori possibili 1~5, default 1).

Nel nodo `bridges` sono anche disponibili i comandi di `add` e di `del` per aggiungere e rimuovere entry statiche del filtering database. Possono essere aggiunte fino ad un massimo di 256 entry statiche. La sintassi prevede:

```
Stargate\Bridges\Bridge1>>add ?
```

```
add command parameters:
```

```
ADD <mac-address aa-bb-cc-dd-ee-ff><device-name string>
```

```
Stargate\Bridges\Bridge1>>del ?
```

```
del command parameters:
```

```
DEL <mac-address aa-bb-cc-dd-ee-ff><device-name string>
```

```
Stargate\Bridges\Bridge1>>
```

### 9.3.2 Parametri di configurazione del nodo SPANNINGTREEPROTOCOL

I parametri del nodo `spanningtreeprotocol` sono utilizzati dall'algoritmo di spanning tree nelle fasi decisionali per la determinazione della topologia ad albero.

<code>bridgepriority</code>	Priorità assegnata al bridge (valori possibili 0~65535, default 32768);
<code>hellotime</code>	periodicità, espressa in secondi, con cui vengono generati i pacchetti di "Configuration BPDU" (valori possibili 1~10, default 2 secondi);
<code>forwarddelaytimer</code>	tempo, espresso in secondi, utilizzato per ritardare alcuni cambiamenti di stato delle porte ( <code>listening</code> → <code>learning</code> , <code>learning</code> → <code>forwarding</code> ) o per forzare l' <code>ageing time</code> delle entry statiche del <code>filtering database</code> ad un valore inferiore quando si sono riscontrati cambiamenti di topologia (valori possibili 4~30, default 15 secondi);
<code>maxage</code>	tempo, espresso in secondi, intercorso dalla ricezione dell'ultima BPDU oltre il quale questa non è più ritenuta valida (valori possibili 6~40, default 20).

### 9.3.3 Parametri di configurazione dei nodi d'interfaccia

```
Stargate>>lan0
```

```
Stargate\Lan0>>set bridging ?
```

```
Bridging enable [ON|OFF]
```

```
Stargate\Lan0>>set bridgepar ?
```

```
Nodes not available.
```

```
Set command parameters:
```

```
<BRIDGE1 | BRIDGE2 | BRIDGE3 | BRIDGE4 >
```

```
PRIORITY <value>
```

```
COST <value>
```

```
Stargate>>
```

dove:

bridging	abilita/disabilita l'interfaccia ad appartenere ad una classe di bridge (valori possibili ON/OFF, default OFF).
----------	---

### 9.3.4 Parametri di configurazione del nodo BRIDGEPAR

bridgen	Definisce la classe di bridging a cui è associata l'interfaccia. I valori possibili sono BRIDGE1/BRIDGE2/BRIDGE3/BRIDGE4, il valore di default è BRIDGE1;
priority	definisce la priorità associata alla porta (valori ammessi 0~255, default 128);
cost	definisce il costo associato alla porta di un bridge (valori ammessi 0~65535, default 1000/velocità della linea di connessione).

## CAPITOLO 10

### 10 Multicasting

#### 10.1 Introduzione

ATOS è in grado di processare il traffico multicast in ingresso ad una interfaccia abilitata (al multicast) replicandolo su tutte le interfacce abilitate al multicast (eccetto quella di origine del traffico).

#### 10.2 Configurazione

I comandi di configurazione sono disponibili nel nodo principale, LAN0 e WANx:

1) l'abilitazione generale della funzionalità Multicast è ottenuta impartendo il comando `set multicast on` dal nodo principale:

```
Stargate>>set multicast ?
```

```
Nodes not available.  
Set command parameters:  
  <ON|OFF>  
  LOGLEVEL <value> [-s]
```

se tale parametro è ON, la ethernet lavorerà in modalità promiscua nel caso di almeno due interfacce abilitate al multicast (LAN0 e WANx);

2) una volta abilitato sul nodo principale, il multicast andrà abilitato anche sull'interfaccia su cui deve operare:

```
Stargate>>lan0
```

```
Stargate\Lan0>>set multicast ?
```

```
  Multicast enable          [ON|OFF]
```

```
Stargate>>wan1
```

```
Stargate\wan1>>set multicast ?
```

```
  Multicast enable          [ON|OFF]
```

## CAPITOLO 11

### 11 Monitor

Stargate permette la visualizzazione di statistiche relative alle varie interfacce e e ai protocolli utilizzati. La possibilità di monitorare i parametri caratteristici dei collegamenti LAN e WAN fornisce uno strumento anche di diagnostica per verificare il buon funzionamento dell'apparato.

#### 11.1 Visualizzazione stato dello Stargate

Per conoscere lo stato dello Stargate, ad esempio per controllare se la linea ADSL è funzionante, si ha a disposizione da Console CLI il comando:

```
SHOW STATUS [-s]
```

Il comando impartito su un determinato nodo, visualizza lo stato relativo al solo nodo in cui si è posizionati;

-s permette la visualizzazione dello stato anche dei parametri dei “sottonodi” dipendenti dal nodo in cui si è dato il comando.

Esempio:

```
Stargate\Adsl>>show status ↵  
Adsl Link Status: Up  
Command executed  
Stargate\Adsl>>
```

I nodi in cui è disponibile il comando di visualizzazione dello stato sono quelli interessati anche alla generazione dei “log” (riferimento paragrafo 5.3.10).

#### 11.2 Visualizzazione statistiche

Per visualizzare statistiche relative al funzionamento di Stargate, si può utilizzare il seguente comando nei nodi che prevedono la visualizzazione dei suddetti parametri. I nodi interessati alle statistiche sono gli stessi in cui è possibile generare dei “log” (riferimento paragrafo 5.3.10):

```
SHOW STATISTICS [-s]
```

Il comando impartito direttamente sotto un nodo, visualizza le statistiche relative al solo nodo in cui si è posizionati;

-s permette la visualizzazione delle statistiche anche dei “sottonodi” dipendenti dal nodo in cui si è dato il comando.

Si può decidere di azzerare le statistiche prodotte da Stargate impartendo il seguente comando:

**DELETE STATISTICS [-s]**

Il comando impartito direttamente sotto un nodo, azzerava le statistiche relative al solo nodo in cui si è posizionati;

-s permette l'azzeramento delle statistiche anche dei "sottonodi" dipendenti dal nodo in cui si è dato il comando.

### 11.2.1 Statistiche ADSL

Esempio:

```
Stargate\Adsl>>show statistics ↵
***** Adsl statistics *****

***** Downstream direction *****
Channel BitRate Interleaved: 8000 Kbps
Channel BitRate Fast: 0 Kbps
Relative Capacity Occupation: 88 %
Noise Margin: 8.0 dB
Output Power: 15.5 dBm
Attenuation: 3.0 dB

***** Upstream direction *****
Channel BitRate Interleaved: 928 Kbps
Channel BitRate Fast: 0 Kbps
Relative Capacity Occupation: 98 %
Noise Margin: 7.0 dB
Output Power: 12.0 dBm
Attenuation: 2.5 dB
Command executed
Stargate\Adsl>>
```

Channel BitRate Interleaved	Se il profilo del collegamento fornito dal gestore è "interleaved" fornisce il valore della velocità del collegamento. Se il profilo è di tipo "Fast" il valore è "0".
Channel BitRate Fast	Se il profilo del collegamento fornito dal gestore è "fast" fornisce il valore della velocità del collegamento. Se il profilo è di tipo "interleaved" il valore è "0".
Relative Capacity Occupation	Rapporto espresso in percentuale tra velocità del collegamento e la massima velocità potenziale raggiungibile da Stargate. Questa percentuale è condizionata dal tipo di contratto stipulato con il gestore.
Noise Margin	Margine di rumore ancora disponibile oltre il quale il sistema non garantisce un tasso d'errore di $10^{-7}$ .
Output Power	Potenza di uscita dal momem della centrale pubblica nel caso Downstream, potenza di uscita dello Stargate nel caso Upstream.
Attenuation	Attenuazione introdotta dalla linea telefonica.

## 11.2.2 Visualizzazione statistiche ATM

Le statistiche ATM sono disponibili sui nodi “\Wan(x)\Atm” e si riferiscono al traffico inviato e ricevuto sul singolo canale virtuale.

Esempio:

```
Stargate\Wan1\Atm>>show statistic ↵

Statistics of physical ATM_VC0 interface
***** Upstream direction *****
Frames : 20602
Errors : 0
Pool full errors : 0
Queue full errors : 0
***** Downstream direction *****
Frames : 48068
Bad CRC frames : 0
Too long frames : 0
Aborted frames : 0
Bad HEC frames : 0
CLP frames : 0
Congestion frames : 0
Bad length frames : 0
FIFO overflow : 0

Command executed
Stargate\Wan1\Atm>>
```

UPSTREAM DIRECTION	
Frames	Numero di pacchetti inviati sull'interfaccia.
Errors	Numero di pacchetti non trasmessi a causa di: errore a livello di driver AAL5 (API).
Pool full errors	Numero di pacchetti non trasmessi a causa della mancata disponibilità di un blocco di memoria nel pool dei buffers di trasmissione fisica (API).
Queue full errors	Numero di pacchetti non trasmessi a causa della mancata disponibilità di spazio nella coda di trasmissione fisica (API).

DOWNSTREAM DIRECTION	
Frames	Numero di pacchetti validi ricevuti sull'interfaccia.
Bad CRC frames	Numero di pacchetti con CRC-AAL5 errato ricevuti sull'interfaccia.
Too long frames	Numero di pacchetti ricevuti sull'interfaccia con payload AAL5 di lunghezza maggiore del valore di MRU negoziato o configurato più la dimensione delle eventuali intestazioni di incapsulamento.
Aborted frames	Numero di pacchetti abortiti ricevuti sull'interfaccia.

Bad HEC frames	Numero di pacchetti ricevuti sull'interfaccia con almeno una cella avente un HEC errato.
CLP frames	Numero di pacchetti ricevuti sull'interfaccia con almeno una cella con il bit CLP settato.
Congestion frames	Numero di pacchetti ricevuti sull'interfaccia con l'ultima cella con il bit PTI congestion settato
Bad length frames	Numero di pacchetti ricevuti sull'interfaccia con un numero di ottetti diverso dalla lunghezza indicata nel campo lunghezza della AAL5
FIFO overflow	Numero di pacchetti ricevuti sull'interfaccia che sono stati scartati a causa della mancanza di spazio nel FIFO di ricezione

### 11.2.3 Visualizzazione statistiche PPP

Queste statistiche sono disponibili sulle interfacce WAN(x) quando il parametro di configurazione "Wanx\Service\Encapsulation" è di tipo PPPoA o PPPoE.

Esempio:

```
Stargate\Wan1\PPP>>show statistic ↵

Statistics of PPP on ATM_VC0 interface
***** Upstream direction *****
Frames : 20601
***** Downstream direction *****
Frames : 48066
Invalid frames : 0
Unknown PID frames : 0
Discarded frames : 0

Command executed
Stargate\Wan1\PPP>>
```

<b>DIREZIONE UPSTREAM</b>	
Frames	Numero di pacchetti inviati sull'interfaccia.

<b>DIREZIONE DOWNSTREAM</b>	
Frames	Numero di pacchetti validi ricevuti sull'interfaccia.
Invalid frames	Numero di pacchetti ricevuti sull'interfaccia con uno dei seguenti errori: control o authentication protocol implementato con lunghezza inferiore alla dimensione dell'header del messaggio;

	control o authentication protocol implementato con lunghezza inferiore a quella specificata nell'header del messaggio.
Discarded frames	Numero di pacchetti ricevuti sull'interfaccia scartati per: Echo Request di formato invalido; pacchetto IP con IPCP layer non in stato opened; messaggio non atteso nello stato corrente del relativo protocollo.
Unknown PID frames	Numero di pacchetti ricevuti sull'interfaccia con protocollo non implementato

### 11.2.4 Visualizzazione statistiche PPPoE

Le statistiche PPPoE sono disponibili solo sulle interfacce WAN(x) quando il parametro di configurazione Wanx\Service\Encapsulation è di tipo PPPoE.

Esempio:

```
Stargate\Wan1\Service\PPPOE>>show statistic
```

```
Statistics of PPPoE on ATM_VC0 interface
```

```
***** Upstream direction *****
```

```
Frames : 50202
```

```
***** Downstream direction *****
```

```
Frames : 97302
```

```
Invalid frames : 0
```

```
Unknown ether-type frames : 0
```

```
Discarded frames : 0
```

```
Command executed
```

```
Stargate\Wan1\Service\PPPOE>>
```

<b>DIREZIONE UPSTREAM</b>	
Frames	Numero di pacchetti inviati sull'interfaccia

<b>DIREZIONE DOWNSTREAM</b>	
Frames	Numero di pacchetti validi ricevuti sull'interfaccia.
Invalid frames	Numero di pacchetti ricevuti sull'interfaccia con uno dei seguenti errori: dimensione minore dell'header ethernet più l'header PPPoE; payload PPPoE inferiore al campo Length dell'header PPPoE; pacchetto di Discovery con Code diverso da PADO, PADS o PADT; pacchetto PPP Stage con Code diverso da PPP (0x00); pacchetto PPP Stage con Session Id diverso da quello assegnato;

	<p>PADO o PADS con il campo length = 0;</p> <p>PADO con Session Id diverso da zero;</p> <p>PADS o PADT con Session Id uguale a zero;</p> <p>PADO o PADS con almeno un TAG invalido per: campi Type e Length incompleti; campo Length maggiore degli ottetti disponibili;</p> <p>PADO o PADS senza uno o più TAGs obbligatori.</p>
Discarded frames	<p>Numero di pacchetti ricevuti sull'interfaccia scartati per:</p> <p>PPPoE Version o Type non supportato;</p> <p>MAC destination address diverso da quello proprio;</p> <p>PADO dopo aver già selezionato un AC;</p> <p>PADS da un AC non selezionato;</p> <p>PADS in stato PPP_STAGE;</p> <p>PADT con Session Id diverso da quello in uso;</p> <p>PADT da un AC non selezionato;</p> <p>pacchetto PPP stage non in stato PPP_STAGE;</p> <p>pacchetto PPP stage da un AC non selezionato.</p>
Unknown ether-type frames	<p>Numero di pacchetti ricevuti sull'interfaccia con il campo ether-type diverso da 0x8863 o 0x8864.</p>

### 11.2.5 Visualizzazione statistiche DHCP

Esempio:

```
Stargate\Dhcp>>show statistic ↵
DHCP STATISTIC
```

```
Plain bootp requests received: 0
Plain bootp replys sent:      0
Discover packets received:    1
Offer packets sent:           1
Dhcp request packets received: 1
Declines received:           0
Releases received:           1
Aacks sent:                   1
Naks sent:                    0
Requests for other servers:   0
Protocol errors all types:    0
```

```
Command executed
Stargate\Dhcp>>
```

Plain bootp requests received:	Frame non DHCP ma di tipo BOOTP, viene trattata come la Discover del DHCP.
Plain bootp replys sent:	Frame non DHCP ma di tipo BOOTP, simile alla Offer del DHCP.
Discover packets received:	Frame originate dal host per ricercare DHCP server nella rete.
Offer packets sent:	Frame originata da Stargate, in risposta alla discover, per indicare quali parametri il DHCP server può offrire. Con questa il DHCP indica l'ip address che può offrire al host.
Dhcp request packets received:	Frame originata dal host per richiedere parametri di configurazione al DHCP server. Con questa l' host indica quale ip address desidera che gli venga assegnato.
Declines received:	Frame originata dal host, dopo la ricezione di ack. Con questa il l' host comunica che gli è stato assegnato un ip address già in uso.
Releases received:	Frame originata dal host, per indicare il rilascio dei parametri che gli sono stati assegnati. Con questa l' host segnala il rilascio del ip address assegnatogli.
Aacks sent:	Frame originato da Stargate in risposta alla request, per comunicare al host i parametri che gli sono stati assegnati. Con questa il DHCP comunica l'ip address assegnato al host.
Naks sent:	Frame originato da Stargate in risposta alla request, per comunicare al host quale parametro richiesto non riesce a soddisfare. Con questa il DHCP comunica se l'ip address richiesto con la request è fuori dal range.
Requests for other servers:	Frame DHCP o BOOTP indirizzate ad altri DHCP server.
Protocol errors all types:	Somma di errori in ricezioni che sono: - ricezione frame DHCP non prevista; - ricezione frame di risposta senza MAGIC COOKIE option.

### 11.2.6 Visualizzazione statistiche IP

Queste statistiche sono sempre disponibili su qualunque tipo d'interfaccia WAN(x) indipendentemente dal tipo di incapsulamento scelto. Il nodo in cui è possibile visualizzare dette statistiche è "\Wan(x)\Ip".

Esempio statistiche IP sulle Wan:

```
Stargate\Wan1\Ip>>show statistic ↵
```

```
Statistics of IP on ATM_VC0 interface
***** Upstream direction *****
Frames : 2598
Discarded frames : 0
Max frame size : 52
Min frame size : 40
```

```

Average frame size : 40
Average speed (bps) : 8800
***** Downstream direction *****
Frames : 4864
Unexpected TCPComp frames : 0
Invalid TCPComp frames : 0
Max frame size : 1500
Min frame size : 28
Average frame size : 1497
Average speed (bps) : 653600

```

```

Command executed
Stargate\Wan1\Ip>>

```

<b>DIREZIONE UPSTREAM</b>	
Frames	Numero di pacchetti inviati sull'interfaccia.
Discarded frames	Numero di pacchetti inviati che vengono scartati perché l'interfaccia non è aperta.
Max frame size	Dimensione massima dei pacchetti inviati.
Min frame size	Dimensione minima dei pacchetti inviati.
Average frame size	Dimensione media dei pacchetti inviati.
Average speed (bps)	Velocità media espressa in bits per secondo (non si tiene conto nel calcolo del tempo in cui l'interfaccia è chiusa).

<b>DIREZIONE DOWNSTREAM</b>	
Frames	Numero di pacchetti validi ricevuti sull'interfaccia.
Unexpected TCPComp frames	Numero di pacchetti ricevuti sull'interfaccia con header TCP/IP compresso quando non è stata negoziata la compressione (questo parametro è disponibile solo se l'incapsulamento è PPP o PPPoE).
Invalid TCPComp frames	Numero di pacchetti ricevuti sull'interfaccia con header TCP/IP compresso invalido (questo parametro è disponibile solo se l'incapsulamento è PPP o PPPoE).
Max frame size	Dimensione massima dei pacchetti ricevuti.
Min frame size	Dimensione minima dei pacchetti ricevuti.
Average frame size	Dimensione media dei pacchetti ricevuti.
Average speed (bps)	Velocità media espressa in bits per secondo (non si tiene conto nel calcolo del tempo in cui l'interfaccia è chiusa).

## CAPITOLO 12

### 12 Aggiornamento software

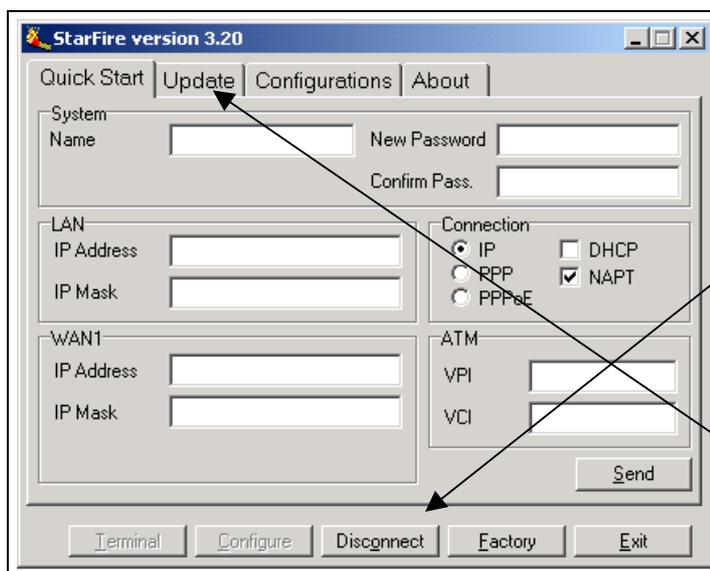
Lo Stargate permette di effettuare l'aggiornamento firmware in diversi modi a seconda dell'interfaccia di comunicazione che si sta utilizzando:

- Interfaccia Seriale, con il programma Aethra "Starfire" presente nel CD a corredo con lo Stargate;
- Interfaccia Ethernet (LAN), tramite il protocollo TFTP (Trivial File Transfer Protocol) usando un PC dotato di client sia Telnet che TFTP.

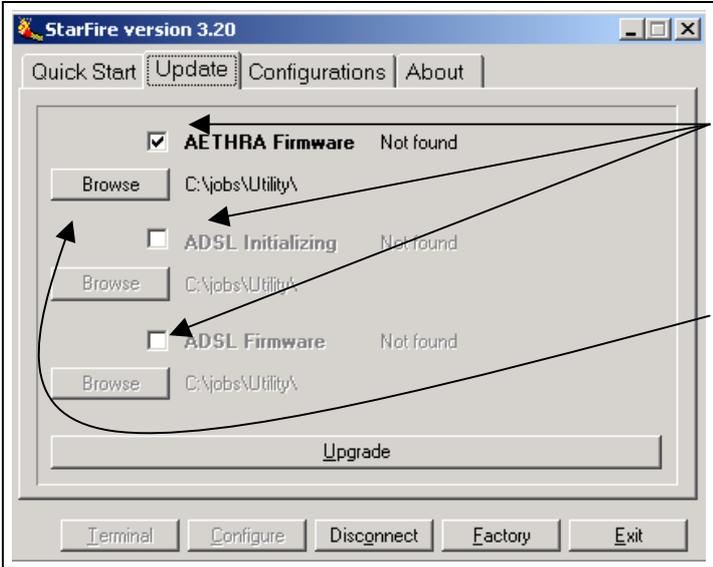
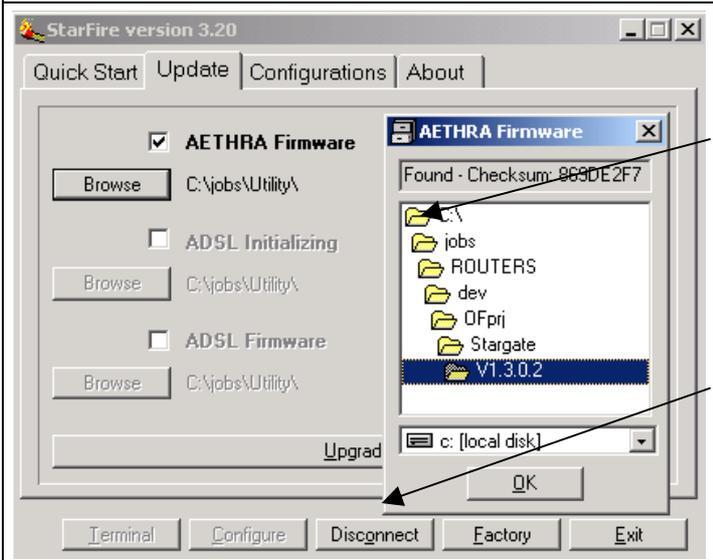
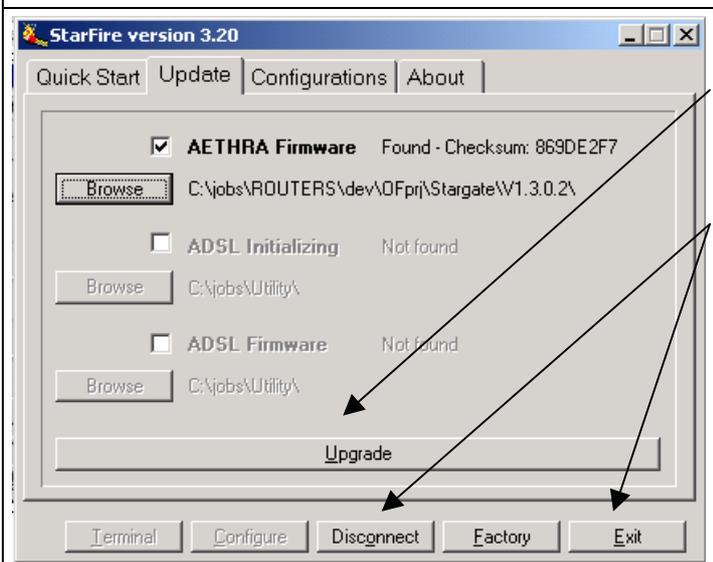
Le versioni aggiornate del firmware saranno pubblicate nell'indirizzo internet [www.aethra.com](http://www.aethra.com).

#### 12.1 Aggiornamento tramite interfaccia seriale

Per eseguire l'aggiornamento firmware tramite il programma Starfire, collegare un PC all'interfaccia seriale dello Stargate, avviare il programma e attenersi alle seguenti indicazioni:



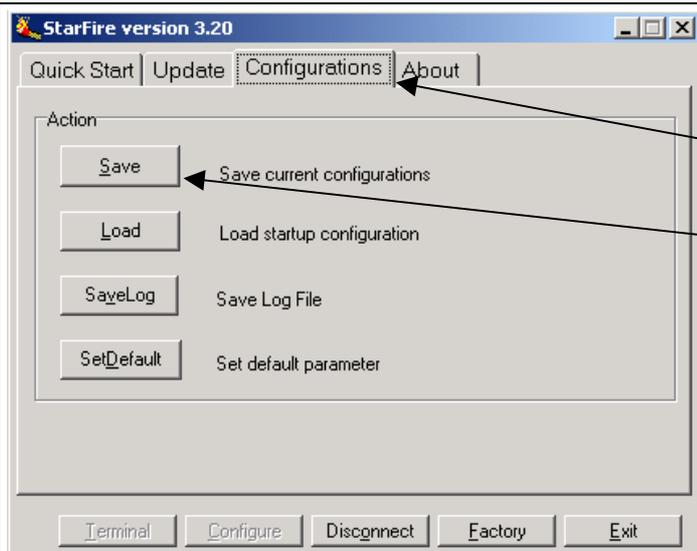
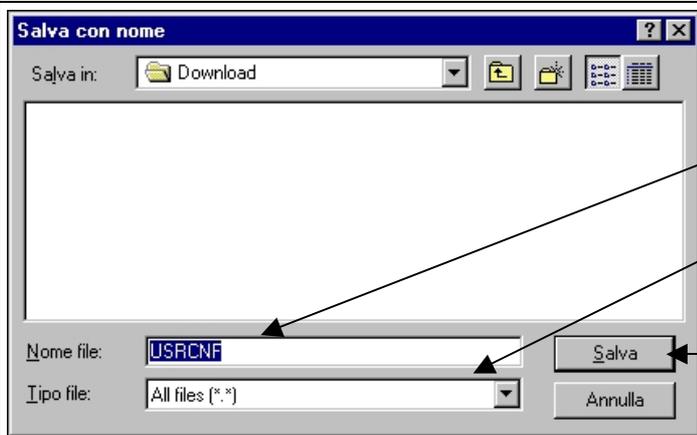
- Spegnere lo Stargate
- riaccendere lo Stargate e subito dopo (fase di inizializzazione) premere il pulsante "Connect";
- scegliere la cartella Update.

	<ul style="list-style-type: none"> <li>▪ Scegliere il tipo di aggiornamento da effettuare in base alle indicazioni riportate insieme al firmware;</li> <li>▪ premere il pulsante “Browse” per la ricerca della directory che contiene il file di Update.</li> </ul>
	<ul style="list-style-type: none"> <li>▪ Quando il programma rileva nella directory in cui vi trovate un file compatibile con l’aggiornamento da effettuare compare l’indicazione “Found” con la relativa checksum;</li> <li>▪ confermare la scelta con “Done”.</li> </ul>
	<ul style="list-style-type: none"> <li>▪ Premere il pulsante “Upgrade” e attendere il completamento del caricamento;</li> <li>▪ terminato l’Update premere in successione “Disconnect” e “Exit”;</li> <li>▪ lo Stargate effettuerà automaticamente il reboot e sarà in pochi istanti pronto al normale funzionamento.</li> </ul>

### 12.1.1 Salvataggio e ripristino file di configurazione con Starfire

Prima di compiere un aggiornamento firmware può risultare utile salvare i dati di configurazione correnti per poi ripristinarli all'occorrenza.

Starfire mette a disposizione l'utility "Configurations" per svolgere le sopra indicate operazioni:

	<ul style="list-style-type: none"> <li>▪ Scegliere la cartella "Configurations";</li> <li>▪ premere il pulsante "Save", lo Stargate richiederà la password di amministratore o nel caso sia ancora quella di default (vuota) vi presenterà direttamente le directory del vostro PC.</li> </ul>
	<ul style="list-style-type: none"> <li>▪ Spostarsi nella directory dove si intende salvare la configurazione;</li> <li>▪ il nome proposto è USRCNF ma si può cambiare con un qualsiasi altro nome;</li> <li>▪ non mettere nessuna estensione per "Tipo files";</li> <li>▪ confermare con "Save".</li> </ul>
	<ul style="list-style-type: none"> <li>▪ Nel caso di ripristino dati di configurazione precedentemente salvati è sufficiente effettuare la scelta "Load" e ricercare il file da ripristinare;</li> <li>▪ confermare la scelta con "Apri".</li> </ul>

## 12.2 Aggiornamento tramite LAN

Per effettuare un aggiornamento firmware dall'interfaccia Ethernet (LAN) è necessario avere installato nella postazione da cui si intende operare un client Telnet e avere a disposizione nella rete un Server TFTP attivo dove sono stati depositati i file relativi all'aggiornamento.

Una volta collegati con lo Stargate con la procedura riportata nel capitolo 6 eseguire il comando **DOWNLOAD** scegliendo l'opzione opportuna (vedi paragrafo 5.3.11), in base al tipo di aggiornamento che si intende effettuare.

Nell'esempio seguente si sta aggiornando il firmware Aethra dello Stargate in quale si chiama "newfirmware" e che risiede nel Server TFTP con indirizzo 192.168.118.72:

```
Stargate>>download newfirmware 192.168.118.72 -c ↵
```

```
.....  
Command executed  
Stargate>>
```

Il nuovo firmware sarà operativo solamente al reboot dell'apparato.

## APPENDICE A

### A Specifiche tecniche

#### A.1 Componenti

- Processore: RISC PowerPC 32bit 40 MHz
- Memoria: SDRAM 24Mbytes, Flash EPROM 4Mbytes

#### A.2 Interfacce

- 4 Ethernet 10Base-T (RJ45 100 ohm) 10Mbps
- 1 Ethernet AUI 10Mbps (solo versione **PLUS**)
- 1 ADSL
- 1 interfaccia seriale RS232 230Kbps (9600 bps per la programmazione da console CLI)

#### A.3 Alimentazione

Alimentatore Esterno:

- OUT<sup>1</sup>: 12V – 0,5A
- OUT<sup>2</sup>: 12V – 0,5A (integrato nello stesso connettore di OUT<sup>1</sup> per alimentazione interfaccia AUI, solo su versione **PLUS**)
- INPUT: 90 ÷ 250 VAC – 0,3A 50 ÷ 60Hz

#### A.4 Dimensioni

- Lunghezza 180 mm, larghezza 145 mm, altezza 40 mm
- Peso 450 gr

#### A.5 Standard Compatibili

- ADSL: G992.1 (G.dmt), ANSI T1.413 issue 2
- ATM: ITU-T – I.361, ITU-T I.363.5, ITU-T I.432, ITU-T I.610, ITU-T I.731

#### A.6 Protocolli supportati

- TCP, UDP, ICMP, IP, IGMP



- RIP V1, V2, V1 compatibile
- PAP CHAP-MD5
- DHCP, DNS, HTTP, TELNET, SNMP

### **A.7 Servizi di Rete supportati**

- IP over ATM (RFC 2684 ex 1483)
- PPP over ATM (RFC 2364)
- PPP over Ethernet (RFC 2516)
- LLC/SNAP o VC-Mux encapsulation

### **A.8 ADSL**

- Full rate ADSL over POTS
- Upstream: fino a 768 Kbps
- Downstream: fino a 8192 Kbps

### **A.9 ATM**

- 8 canali VC (VC<sub>s</sub>)
- Classe di servizio UBR
- Adattamento: AAL5

## APPENDICE B

### B Approfondimenti

#### B.1 Instradamento di Datagrammi

La funzione principale di Stargate è costituita dall'invio di datagrammi IP tra la LAN ed una connessione WAN. Per lo svolgimento di questa funzione Stargate utilizza delle tabelle di routing.

Ciascuna voce delle tabelle di routing si dirige ad una rete che può essere raggiunta tramite una delle interfacce e contiene inoltre il numero di reti intermedie che devono essere attraversate per raggiungere la destinazione finale.

Al ricevimento di un pacchetto dalla LAN o da una delle connessioni WAN, Stargate esamina l'indirizzo IP di destinazione contenuto nel pacchetto per vedere se corrisponde ad una o più reti contenute nelle tabelle di routing. In caso affermativo il pacchetto viene inviato alla porta appropriata (LAN o WAN) giungendo alla rete di destinazione con il minor numero possibile di reti da attraversare (hop).

Le tabelle di routing utilizzano tre tipi di voci:

- ⇒ **rotte statiche**, definite al momento della configurazione che restano invariate durante il funzionamento;
- ⇒ **rotte dinamiche**, aggiornate durante il funzionamento in base alle informazioni scambiate con i router vicini nelle estremità remote delle connessioni WAN mediante il Routing Information Protocol (RIP);
- ⇒ **rotte locali**, create per ciascuna interfaccia attiva, con una route alla rete direttamente collegata a quell'interfaccia.

Una delle rotte statiche può essere configurata in modo da dirigersi ad un gateway di default su una specifica porta WAN, in modo tale che i pacchetti che non potrebbero essere instradati altrimenti vengono inviati a quella specifica porta. Quando si utilizza una connessione WAN per collegarsi ad un Internet Service Provider, esso viene normalmente definito "gateway di default".

#### B.2 Network Address and Port Translation

Il meccanismo Network Address e Port Translation (NAPT) viene normalmente utilizzato per consentire agli host di una LAN interna di condividere un unico account ISP (vale a dire un indirizzo IP "pubblico" unico) durante la connessione a Internet. Dal punto di vista del Service Provider, viene collegata un'unica entità, anche se le richieste sono effettivamente originate da host diversi.

Il NAPT, inoltre, rende gli indirizzi IP utilizzati sulla LAN interna invisibili al mondo esterno. Questo comporta due principali vantaggi:

- ⇒ gli host nella LAN non devono utilizzare indirizzi IP registrati InterNic e possono utilizzare invece uno schema di indirizzamento "privato";

⇒ maggiore sicurezza in quanto gli host remoti non possono contattare direttamente gli host sulla LAN interna.

Stargate può essere configurato in modo tale da inviare traffico selezionato tra host remoti e host specifici sulla LAN. Questo consente all'utente di installare dei server nella LAN e offrire i relativi servizi a clienti remoti.

Dato che non è sensibile all'annuncio di indirizzi privati, Stargate non invia mai annunci RIP sulle connessioni WAN quando il NAPT è abilitato, anche se può comunque utilizzare gli annunci RIP ricevuti dalle connessioni WAN per costruire rotte per la tabella di routing dinamico.

Il NAPT può essere abilitato per ogni singola connessione WAN.

### **B.3 Servizi DHCP e DNS**

Stargate è in grado di fornire una configurazione dinamica agli host sulla LAN, utilizzando le funzionalità di server Dynamic Host Configuration Protocol (DHCP).

Quando un host cliente richiede informazioni di configurazione (indirizzo IP, nome dominio, nome host, indirizzi server DNS e server WINS, gateway di default), Stargate fornisce i dati richiesti utilizzando le informazioni configurate in un database locale.

Stargate fornisce inoltre funzionalità di server DNS agli host sulla LAN. È in grado di risolvere nomi sulla LAN interna (se sono stati assegnati dal server DHCP interno) o inviare la query DNS ad un server appropriato sulla LAN o su una delle connessioni WAN.

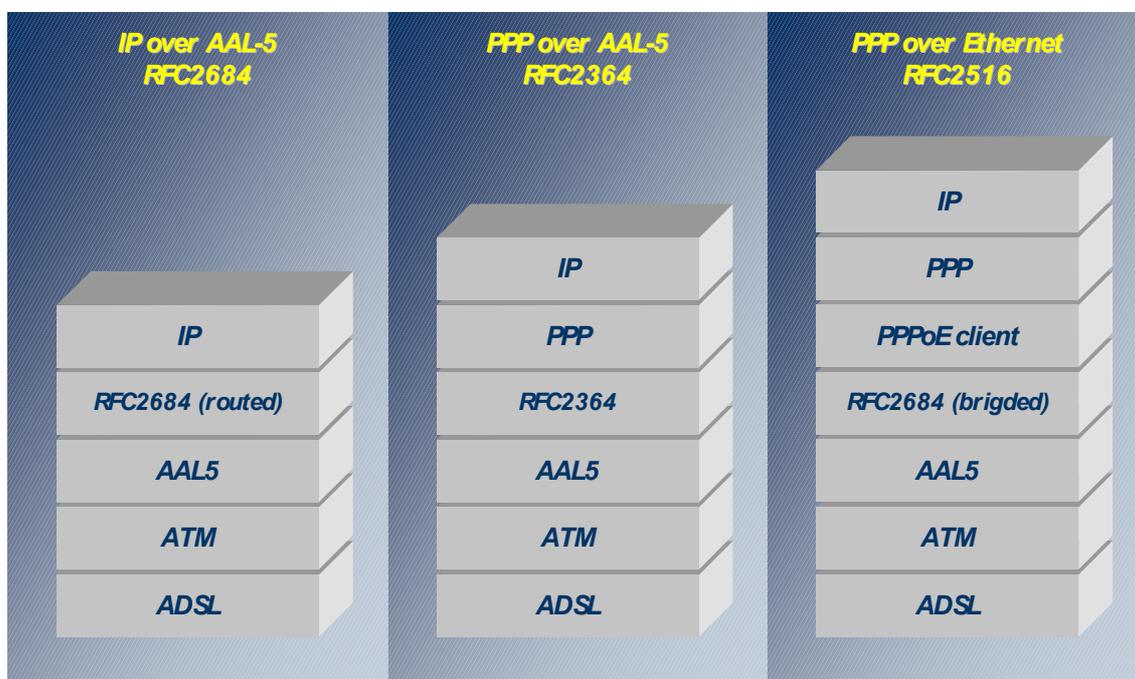
L'uso dei servizi NAPT, DHCP e DNS rende immediata la configurazione degli host sulla LAN interna: tutti gli hosts possono essere configurati nello stesso modo, in quanto ricevono le informazioni richieste (indirizzo IP, gateway di default, indirizzo server DNS, indirizzo server WINS, ecc.) direttamente da Stargate al momento dell'accensione.

### **B.4 Protocolli di Trasporto**

Ciascuna connessione WAN può essere configurata indipendentemente:

- ⇒ per trasportare traffico IP instradato "puro" in conformità a RFC2684, oppure
- ⇒ per utilizzare l'incapsulamento PPP in conformità a RFC2364 quando l'estremità remota della connessione WAN è un server di accesso PPP, oppure
- ⇒ per utilizzare RFC2516 conforme a incapsulamento PPPoE del traffico PPP quando l'estremità remota è un server di accesso abilitato PPPoE.

La figura che segue descrive gli stack di protocolli di trasporto implementati da Stargate.



### B.4.1 IP over ATM

L'instradamento RFC2684 IP viene utilizzato quando l'estremità remota della connessione WAN non supporta l'incapsulamento PPP e i servizi di autenticazione. Questo può verificarsi quando la connessione WAN è utilizzata per collegare la LAN interna ad una LAN aziendale remota.

### B.4.2 PPP over AAL-5

Quando l'estremità remota della connessione WAN supporta l'incapsulamento PPP, Stargate autentica il server di accesso ed utilizza le informazioni aggiuntive di configurazione fornite durante la fase di inizializzazione IP Control Protocol (IPCP): queste informazioni possono contenere l'indirizzo IP da utilizzare nella connessione WAN e l'indirizzo del server o dei server DNS disponibili al di là del server di accesso PPP.

### B.4.3 PPP over Ethernet

Inoltre, se il server remoto è un server abilitato PPPoE, Stargate incapsula ulteriormente i datagrammi PPP in trame di tipo Ethernet che vengono successivamente inviate all'estremità remota come PDU RFC2684 bridged.

Quando le trame PPPoE sono abilitate, Stargate inizia una Fase di **Discovery** per ottenere l'indirizzo o gli indirizzi MAC del server o dei server disponibili dalla porta WAN prima di tentare di stabilire una sessione PPPoE.

Durante la fase di discovery, Stargate trasmette un pacchetto di iniziazione (PADI). Il campo dell'indirizzo sorgente in questo pacchetto contiene l'indirizzo sorgente MAC di Stargate sulla porta LAN. Stargate attende quindi che un server risponda con un pacchetto di offerta (PADO). Questo pacchetto contiene l'indirizzo MAC del server che risponde. Se non riceve una risposta prima del time-out di un `restarttimer`, Stargate invia nuovamente il pacchetto PADI. Il valore iniziale del `restarttimer` viene raddoppiato ad ogni ritrasmissione del pacchetto PADI.

Una volta ricevuti i primi pacchetti PADO, Stargate trasmette un pacchetto Service Request (PADR) al server che restituisce un pacchetto di conferma sessione (PADS) con una ID di sessione unica, che sarà utilizzata durante tutta la sessione PPP. Anche in questo caso il valore iniziale del `restarttimer` viene raddoppiato ad ogni ritrasmissione del pacchetto PADR se non si ottiene una risposta PADS.

Dopo aver completato con successo la Fase di Discovery, Stargate formatta le trame di tipo Ethernet contenenti datagrammi PPP. Queste trame possono conservare gli FCS 32 bit presenti nella trama Ethernet oppure, in alternativa, il FCS può essere eliminato. Dato che la trama Ethernet viene trasportata su una PDU AAL-5, essa è in ogni caso protetta dal codice di rivelazione di errore CRC-32 incluso nel trailer PDU AAL-5.

## **LLC/SNAP vs. VC-mux**

RFC2684 e RFC2364 definiscono entrambi due modi di incapsulamento diversi, il Logical Link Control/Sub-network Access Protocol (LLC/SNAP) e il Virtual Circuit multiplexing (VC mux).

Il modo di incapsulamento LLC/SNAP è stato ideato per consentire al traffico multi-protocollo (come datagrammi IP, IPX e MAC bridging) di condividere la stessa Connessione Virtuale ATM. Il modo LLC/SNAP aggiunge un'intestazione a ciascun datagramma per identificare il protocollo che viene trasportato.

Il modo VC-mux, invece, considera che ciascuna VC viene utilizzata solamente per trasportare traffico per un unico protocollo e pertanto non richiede nessuna intestazione.

Il modo di incapsulamento è staticamente configurato per ciascuna connessione WAN dato che corrisponde al modo utilizzato dal server di accesso (o dal router remoto) nell'estremità remota e non può essere negoziato.

Inoltre, per il traffico PPPoE, le trame di tipo Ethernet che contengono datagrammi PPP possono essere inviate in modo trasparente sulla connessione ATM oppure il campo FCS 32 bit può essere "strippato" prima dell'invio e rigenerato al ricevimento da parte dell'estremità remota.

## **AAL-5**

L'ATM Adaptation Layer 5 (AAL-5) si occupa di tutte le operazioni richieste per segmentare il datagramma IP risultante IP o PPP incapsulato LLC/SNAP o VC-mux in celle ATM dalla lunghezza fissa e riassemblare le celle in datagrammi nella direzione opposta.

L'AAL-5 fornisce anche la delimitazione dei datagrammi e la rivelazione di errori con un codice CRC-32.

#### **B.4.4 Livello ATM**

Il livello ATM provvede a compiti di livello inferiore, come identificare le celle con Virtual Path Identifier (VPI) e Virtual Circuit Identifier (VCI), formare il traffico uscente ed eseguire alcune operazioni di Operation and Management (O&M).

#### **B.4.5 Livello ADSL**

Il modem ADSL integrato in Stargate fornisce un canale di trasmissione ad alta velocità.

I parametri individuali ADSL sono configurati nel Digital Subscriber Access Line Multiplexer (DSLAM) nel lato della centrale del canale ADSL.

Durante l'inizializzazione, il DSLAM dà istruzioni a Stargate sulla definizione di parametri, come le velocità nette dei bit per i canali upstream e downstream.

### **Informazioni di Riferimento**

#### **B.5 Server proxy DNS**

Stargate offre una funzionalità di server e forwarder DNS allo scopo di rendere più semplice la configurazione e l'installazione degli host sulla LAN.

Quando è abilitato il proxy DNS interno:

- ⇒ gli host locali devono essere configurati in modo tale da dirigersi a Stargate come server DNS primario (o unico), o manualmente o tramite la funzione server DHCP di Stargate. In quest'ultimo caso, il server DHCP deve essere configurato in modo tale da avere l'indirizzo IP locale di Stargate come "server DNS primario";
- ⇒ le queries DNS sono quindi indirizzate direttamente a Stargate. Le queries per nomi di host locale sono risolte localmente da Stargate, mentre le queries per nomi di host remoti vengono ribattute verso i server DNS esterni;
- ⇒ gli indirizzi dei server esterni sono configurati in una lista di server. Stargate supporta queries ricorsive ai server DNS esterni;
- ⇒ una volta ottenuta la risposta finale da uno dei server nella lista, questa viene restituita all'host che ha emesso la query sulla LAN e contemporaneamente viene registrata su una cache locale, in modo da poter essere usata per risolvere localmente successive queries verso lo stesso nome.

Quando il Proxy DNS è disabilitato:

- ⇒ gli host locali devono essere esplicitamente configurati con gli indirizzi di uno o due server DNS, essere immessi manualmente in ciascuna postazione o appresi da un server DHCP (Stargate stesso, se il servizio DHCP è abilitato), oppure da Server di Accesso PPP remoto;
- ⇒ le queries e le risposte DNS sono instradate in modo trasparente da Stargate tra host locali e server DNS sulla WAN.

## B.6 RIP

Stargate utilizza il Routing Information Protocol (RIP) per scambiare informazioni di instradamento con router vicini sulle connessioni WAN o sulla LAN.

Per ciascuna porta WAN o LAN Stargate può essere configurato in modo tale da:

- ⇒ ignorare il traffico RIP entrante ed evitare di inviare datagrammi RIP;
- ⇒ inviare e ricevere datagrammi RIP (RIP attivo);
- ⇒ ricevere solamente datagrammi RIP e acquisire così informazioni sulle tabelle di routing dei router vicini, senza inviare il contenuto della sua tabella di routing (RIP passivo).

**NOTA** *L'invio di datagrammi RIP non è consentito su connessioni con NAPT abilitato.*

Stargate può essere configurato in modo tale da utilizzare la versione 1 o la versione 2 del RIP. Inoltre può essere selezionato un modo compatibile con la versione 1 in cui l'RIP segue in linea generale la versione 2, senza utilizzare indirizzi multicast. Questo consente a Stargate di funzionare con router che supportano solo RIP V1.

Le informazioni ricevute dai router vicini vengono utilizzate per aggiornare le voci dinamiche della tabella di routing. Se una voce dinamica della tabella di routing non viene aggiornata con datagrammi RIP (tipicamente dopo 180 secondi), essa viene cancellata e la rete verso cui si dirige tale voce viene marcata come “non raggiungibile”.

Tuttavia, la voce non viene immediatamente rimossa dalla tabella di routing, in modo tale che il prossimo datagramma RIP inviato da Stargate propagherà questa informazione agli altri router. La voce viene cancellata dopo un certo periodo di tempo (tipicamente 30 secondi).

## B.7 PPP

Stargate supporta totalmente le funzionalità PPP, comprese le negoziazioni LCP e IPCP, le autenticazioni PAP e CHAP-MD5 e i controlli di continuità della connessione. Quando una sessione PPP ha termine o la connessione PPP viene comunque abbattuta, Stargate può essere configurato cancellare automaticamente tutte le route associate con quella connessione.

### B.7.1 Opzioni di Configurazione LCP

Stargate e il Server di Accesso PPP nell'estremità remota della connessione WAN negoziano una serie di parametri relativi alla connessione da usare durante la connessione con LCP. Si possono configurare le seguenti opzioni di configurazione:

- ⇒ **Maximum-Receive-Unit (MRU)**, che definisce il valore della opzione LCP corrispondente nelle Richieste di Configurazione iniziali. Rappresenta la lunghezza massima di datagrammi che Stargate è pronto a ricevere;

**NOTA** *In base a RFC2364, l'opzione MRU non deve essere configurata ad una dimensione maggiore della dimensione CPCS-SDU massima specificata nella direzione associata per il contratto di traffico della connessione virtuale (ove esistente).*

⇒ **flag Protocol Field Compression (PFC) e Address and Control Field Compression (ACFC)**, che consentono a Stargate di includere la relativa opzione LCP nelle Richieste di Configurazioni iniziali;

**NOTA** *In base a RFC2364, l'uso di PFC e/o ACFC non è raccomandato; inoltre le opzioni ACFC non devono essere incluse nelle Richieste di Configurazioni uscenti. Stargate, comunque, riconosce richieste di PFC e ACFC indipendentemente dalla definizione di questi flag.*

⇒ flag Echo request, che consente a Stargate di inviare puntualmente Richieste di Echo.

Stargate supporta l'opzione Magic Number, non richiede mai e rifiuta sempre le opzioni seguenti:

- ⇒ Field Check Sequence (FCS) Alternatives;
- ⇒ Asynchronous-Control-Character-Map (ACCM);
- ⇒ Quality Protocol;
- ⇒ Endpoint Identifier;
- ⇒ Multilink MRU.

## **B.7.2 Autenticazione**

La fase di autenticazione inizia immediatamente dopo la conclusione della fase di negoziazione LCP.

Stargate supporta i protocolli di autenticazione CHAP-MD5 e PAP sul lato cliente (cioè non è in grado di autenticare un'entità pari remota e non include nessuna Opzione di Configurazione del Protocollo di Autenticazione nelle Richieste di Configurazione uscenti).

Per ciascuna connessione WAN Stargate può essere configurato in modo tale da avere:

- ⇒ un **username** e una **password** (segreti), validi per tutti gli schemi di autenticazione supportati;
- ⇒ un flag che consente l'autenticazione CHAP-MD5;
- ⇒ un flag che consente l'autenticazione PAP.

Se uno di questi flag è definito, Stargate accetta di autenticarsi utilizzando il protocollo corrispondente. Il protocollo di autenticazione da utilizzare sarà indicato dal server di accesso.

Se il server di accesso richiede l'autenticazione usando un protocollo non supportato, Stargate risponderà alla richiesta con Configure-NAK, indicando uno dei protocolli supportati. Se entrambi i protocolli sono abilitati, CHAPMD5 verrà usato per primo nella Richiesta di Configurazione.

### B.7.3 Configurazione IPCP

IPCP parte immediatamente una volta autenticata la connessione. Esso viene usato principalmente per definire l'indirizzo IP da utilizzare sulla porta WAN. Stargate può essere configurato in modo tale da includere l'opzione protocollo di compressione *Van Jacobson* nelle sue Richieste di Configurazione uscenti. La stessa opzione viene sempre riconosciuta quando ricevuta nelle Richieste di Configurazione entranti.

Stargate include sempre nella richiesta di configurazione iniziale IPCP l'indirizzo IP programmato per la porta WAN. Stargate accetta tutti gli indirizzi indicati dal server di accesso PPP in una risposta Configure-NAK alle Richieste di Configurazione, ritornando una nuova Richiesta di Configurazione IPCP con l'opzione indirizzo definita all'indirizzo indicato.

Stargate può essere anche programmato in modo tale da ricevere gli indirizzi IP dei server DNS e WINS da una porta WAN<sup>9</sup>. Questi valori sono immessi come server DNS primario e secondario in una delle voci della lista Server Nomi Dominio. Queste informazioni vengono conservate fino al termine della sessione PPP.

## B.8 NAPT

### B.8.1 Sessioni

Il funzionamento NAPT si basa sul concetto di *sessione*. Una sessione include tutto il flusso di traffico tra due indirizzi di trasporto.

Un indirizzo di trasporto è la serie (indirizzo sorgente IP, numero porta sorgente, indirizzo di destinazione IP, numero porta destinazione) per una sessione TCP o UDP. Le sessioni di query ICMP sono invece identificate dalla serie (indirizzo sorgente IP, ID query ICMP, indirizzo di destinazione IP). Tutti gli altri tipi di sessione sono caratterizzati dalla serie (indirizzo sorgente IP, indirizzo di destinazione IP, protocollo IP).

Il primo pacchetto di una sessione uscente è un pacchetto uscente. Al contrario, una sessione entrante inizia con un pacchetto entrante.

NAPT normalmente gestisce sessioni uscenti (cioè sessioni iniziate da host interni). Le sessioni interne, come nel caso in cui un cliente sulla WAN tenti di raggiungere un host server sulla LAN interna, non sono consentite, a parte i casi particolari descritti più avanti.

Quando la sessione inizia, viene creata una voce nella tabella NAPT, in riferimento ai due indirizzi di trasporto che identificano la sessione. La voce viene quindi utilizzata per tradurre i pacchetti entranti ed uscenti appartenenti alla sessione.

### B.8.2 Inizio della sessione

L'inizio di un pacchetto TCP viene identificato facilmente, in quanto solo il primo pacchetto di una sessione TCP è autorizzato ad avere il ACK bit azzerato (anche il bit SYN è definito in questo

---

<sup>9</sup> Vedi RFC1877 "IPCP Name Server Options"

pacchetto). Tutti i pacchetti TCP, con eccezione del primo pacchetto, devono invece avere il bit ACK definito.

Tuttavia non esiste un modo deterministico per riconoscere l'inizio di una sessione UDP o non TCP. Una sessione non-TCP inizia non appena viene rilevato un pacchetto con una serie non mappata di indirizzi di trasporto.

### B.8.3 Fine della sessione

La fine di una sessione TCP può essere rilevata quando FIN è riconosciuto da entrambi gli estremi della sessione o quando una delle metà riceve un segmento con il bit RST nel campo flag TCP.

Quando viene rilevato questo pacchetto, il motore NAPT considera la sessione terminata e cancella la voce relativa nella tabella NAPT.

In realtà, la fine della sessione viene ritardata per consentire ad eventuali pacchetti ritrasmessi di passare attraverso il NAPT. Inoltre, la sessione TCP può terminare senza che il NAPT se ne renda conto (ad esempio nel caso in cui una o entrambe le entità pari effettuano un reboot). Di conseguenza, le connessioni TCP che sono rimaste inattive per un certo periodo di tempo sono considerate terminate, rimuovendo qualsiasi associazione dalle tabelle NAPT.

Non esiste un modo per determinare la fine di una sessione non TCP e pertanto il NAPT utilizza un meccanismo di time-out per cancellare le voci associate a sessioni non TCP.

### B.8.4 Gestione di pacchetti non richiesti

I pacchetti entranti che non appartengono ad una sessione esistente vengono normalmente scartati, eccetto nel caso in cui il motore NAPT abbia ricevuto istruzioni specifiche per:

- ⇒ consentire l'accesso ad un server nella lista di server interni (massima priorità): questo consente ai clienti remoti di accedere ai server interni sulla LAN (ad esempio un server Web). Questa lista viene definita *proxy list*;
- ⇒ inviare all'host che ha già una sessione esistente con l'host che ha emesso questo pacchetto<sup>10</sup>;
- ⇒ inviare a un *host di default* sulla LAN interna se configurato nella sezione NAPT del database di configurazione (minima priorità).

Le opzioni sono prioritarizzate, pertanto l'opzione con priorità più alta viene scelta in caso di abilitazione di varie opzioni.

### B.8.5 NAPT walk-through

Immaginiamo due connessioni WAN abilitate a pacchetti NAPT. La connessione WAN 1 ha come indirizzo 136.pp.qq.rr.ss, e la connessione WAN 2 ha come indirizzo 165.xx.yy.zz. Una terza connessione WAN non usa il NAPT e si collega ad una LAN remota.

---

<sup>10</sup> Questo modo può essere utilizzato per consentire agli host interni di stabilire sessioni di MS<sup>®</sup> Netmeeting verso estremità remote.

Sulla terza connessione WAN l'indirizzo assegnato a Stargate è un indirizzo privato 192.168.110.1. La LAN remota ha come indirizzo 192.168.111.00/24. Stargate ha una voce nella tabella di routing statico verso questa rete.

Viene ricevuto un pacchetto da un host sulla LAN e Stargate, in base alle tabelle di routing, decide che deve essere inviato alla connessione WAN 1 in cui è abilitato NAPT. Questo può essere ad esempio un pacchetto dall'host 192.168.110.134 con porta sorgente 2345 e diretto alla porta http nota di un server a 129.kk.mm.nn (un indirizzo "pubblico").

Il motore NAPT in Stargate cambia l'indirizzo sorgente IP nell'indirizzo assegnato alla connessione WAN 1 e modifica possibilmente il numero di porta sorgente per evitare ambiguità nel caso in cui lo stesso numero si utilizzato da più di un host locale:

	<i>ind. sorgente:porta</i>	<i>ind. dest :porta</i>
<i>prima NAPT</i>	192.168.110.101:1234	129.kk.mm.nn:80
	↓	
<i>dopo NAPT</i>	136.pp.qq.rr:2345	129.kk.mm.nn:80

Se non esistente, viene creata una voce nella tabella NAPT dinamico che associa l'indirizzo "privato" e il numero della porta originali (192.168.110.101:1234) all'indirizzo e al numero della porta "pubblici" (136.22.36.12:2345).

Viene ricevuto un pacchetto dall'host 192.168.110.102 sulla LAN alla porta server TELNET dell'host 134:ss.tt.uu e Stargate, in base alle sue tabelle di routing, decide che questo pacchetto deve essere inviato sulla connessione WAN 2.

	<i>ind. sorgente:porta</i>	<i>ind. dest.:porta</i>
<i>prima NAPT</i>	192.168.110.102:1234	134:ss.tt.uu:23
	↓	
<i>dopo NAPT</i>	165.xx.yy.zz:4567	134:ss.tt.uu:23

Viene ricevuto un terzo pacchetto dalla connessione WAN 3 destinato allo stesso server WEB 129.kk.mm.nn considerato in precedenza. In base all'indirizzo di destinazione Stargate invia questo pacchetto sulla connessione WAN 1:

	<i>ind. sorgente:porta</i>	<i>ind. dest.:porta</i>
<i>prima NAPT</i>	192.168.111.103:1234	129.kk.mm.nn:80
	↓	
<i>dopo NAPT</i>	136.pp.qq.rr:5678	129.kk.mm.nn:80

Ora il server Web attraverso la rete risponde con un pacchetto destinato a 136.pp.qq.rr:2345. Questo pacchetto arriva alla connessione WAN 1, sebbene questo non sia rilevante ai fini della trattazione che segue.

Dato che la connessione WAN 1 ha l'NAPT abilitato, il pacchetto viene prima passato al motore NAPT. Una ricerca nella tabella di mappatura degli indirizzi basata sul **numero porta di destinazione** contenuto nel pacchetto recupera le associazioni con l'indirizzo di host e con il numero di porta originale e inverte il processo di traduzione:

	<i>ind. sorgente:porta</i>	<i>ind. dest.:porta</i>
<i>prima NAPT</i>	129.kk.mm.nn:80	136.pp.qq.rr:2345
		↓
<i>dopo NAPT</i>	129.kk.mm.nn:80	192.168.110.101:1234

Ora l'indirizzo di destinazione reale è noto ed il pacchetto può essere instradato alla porta appropriata dell'host sulla LAN.

Quando il server TELNET risponde con un pacchetto destinato a 165.xx.yy.zz:4567, anche in questo caso viene effettuata una ricerca nella tabella di mappatura e viene recuperata la connessione originale a 192.168.110.102:1234.

	<i>ind. sorgente:porta</i>	<i>ind. dest.:porta</i>
<i>prima NAPT</i>	134.ss.tt.uu:23	165.xx.yy.zz:4567
		↓
<i>dopo NAPT</i>	134.ss.tt.uu:23	192.168.110.102:1234

Stargate ora instrada correttamente il pacchetto alla LAN.

Infine viene ricevuta la risposta al terzo pacchetto, viene effettuata la ricerca nella tabella di mappatura e viene rilevato l'indirizzo di destinazione:

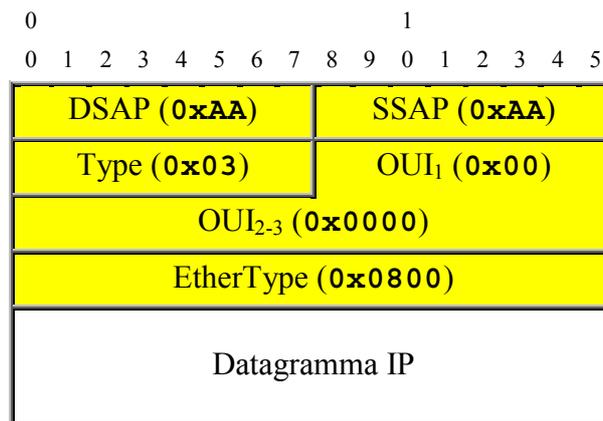
	<i>ind. sorgente:porta</i>	<i>ind. dest.:porta</i>
<i>prima NAPT</i>	129.kk.mm.nn:80	136.pp.qq.rr:5678
		↓
<i>dopo NAPT</i>	129.kk.mm.nn:80	192.168.111.103:1234

Il pacchetto viene quindi inviato alla connessione WAN 3.

## B.9 Incapsulamento LLC/SNAP

### B.9.1 Routed IP PDU

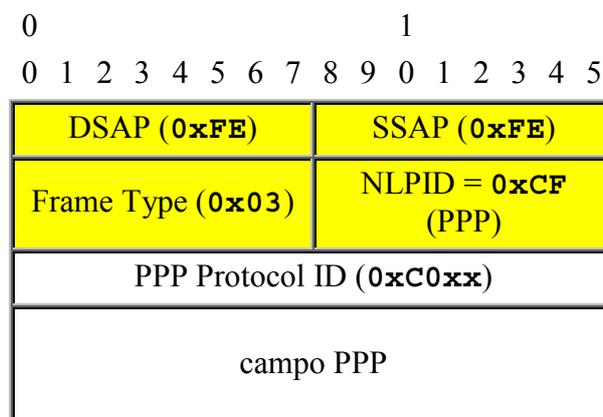
In base a RFC2684, i pacchetti scambiati su una connessione WAN configurata per traffico IP diretto utilizzando l'incapsulamento LLC/SNAP hanno un'intestazione prefissata al payload per indicare che il payload consiste in un datagramma IP:



Quando viene utilizzato l'incapsulamento VC-mux l'intestazione LLC/SNAP è omessa.

### B.9.2 Incapsulamento datagrammi PPP

In base a RFC2364 i pacchetti scambiati su una connessione WAN configurata per trasportare traffico PPP utilizzando l'incapsulamento LLC/SNAP hanno un'intestazione prefissata al payload per indicare che il payload consiste in un datagramma PPP:

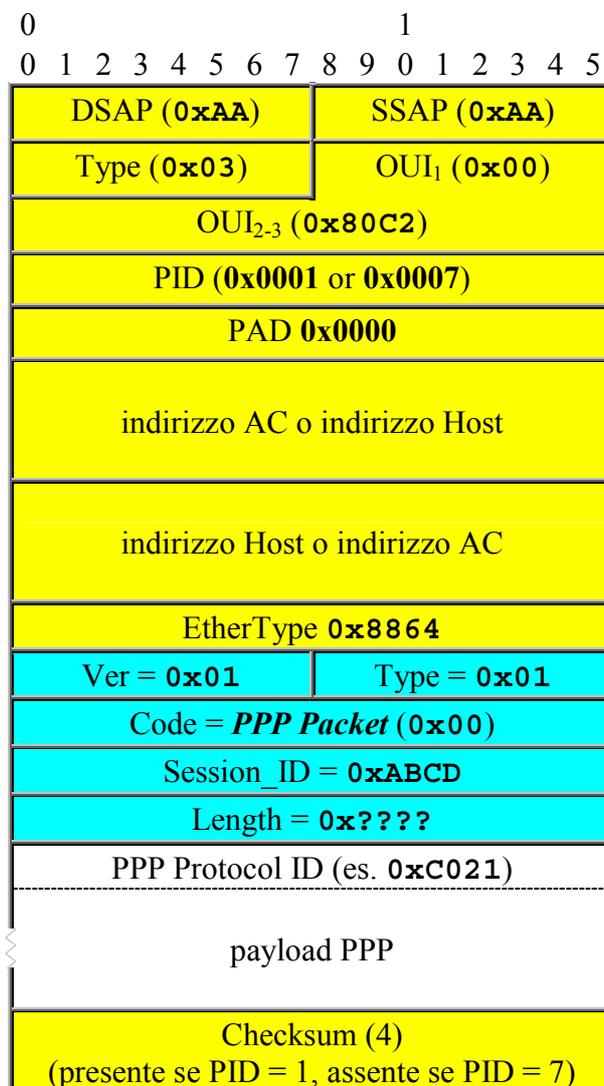


Quando viene utilizzato l'incapsulamento VC-mux l'intestazione LLC/SNAP è omessa.

### B.9.3 Incapsulamento PPPoE

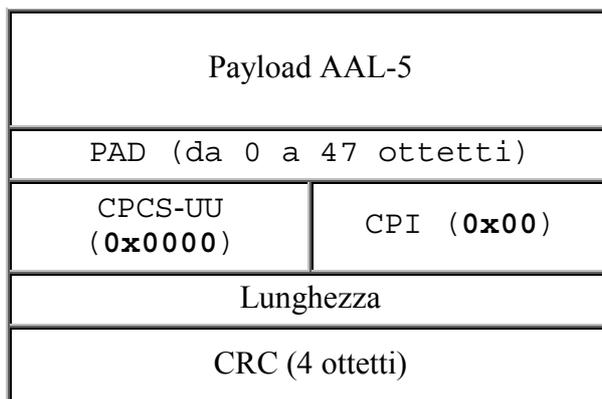
Quando è programmato il trasporto PPPoE, i pacchetti scambiati su una connessione WAN hanno intestazioni multiple:

- ⇒ un'intestazione LLC/SNAP per traffico Ethernet "bridged" (non utilizzato nel modo di incapsulamento VC);
- ⇒ un'intestazione Ethernet;
- ⇒ un'intestazione PPPoE.



## B.10 Funzionamento AAL-5

Stargate implementa l'ATM Adaptation Layer 5 in conformità a ITU-T-I.363.5. Il formato della AAL-5 Protocol Data Unit (PDU) viene descritto di seguito:



Il payload AAL-5 è il datagramma IP o PPP incapsulato (possibilmente LLC/SNAP). Il campo PAD contiene un numero di ottetti tale che la lunghezza totale della AAL-5 Protocol Data Unit (PDU) è un multiplo di 48. Questo garantisce che l'intera PDU AAL-5 entra in un numero intero di celle ATM.

Il campo CPCS-UU (indicazione User-to-User) non è utilizzato ed è configurato a 0x0000.

Il CPI è codificato a 0x00 e viene usato solamente per allineare il trailer CPCS-PDU a 64 bit.

Il campo Length indica la lunghezza, in ottetti, del campo Payload. Il valore massimo del campo Length è 65535 ottetti. Un campo Length codificato come 0x00 viene usato per la funzione abort.

Il campo CRC protegge l'intera CPCS-PDU tranne il campo CRC stesso.

Nel AAL-5-SAP vengono utilizzate le seguenti opzioni:

- ⇒ viene usato il modo messaggio e l'opzione consegna dati corrotti non viene utilizzata;
- ⇒ i parametri CPCS-LP, CPCS-CI e CPCS-UU sono fissati a "0" in direzione upstream e ignorati in direzione downstream.

## B.11 Segmentation and Reassembly (SAR)

Nella direzione di trasmissione, SAR segmenta le PDU AAL-5 in pezzi di dati da 48 ottetti. Ciascun pezzo entra nel campo payload di una cella ATM. Il SAR dà inoltre istruzioni al sottostante livello ATM di marcare la cella finale della PDU affinché l'entità SAR ricevente sia in grado di rilevare la fine della PDU.

## B.12 Livello ATM

A questo livello, l'utente deve specificare il Canale Virtuale da usare in questa connessione WAN. Un Canale Virtuale viene costituito usando un Virtual Path Identifier (VPI) e un Virtual Channel Identifier (VCI): entrambi devono essere forniti dal Service Provider.

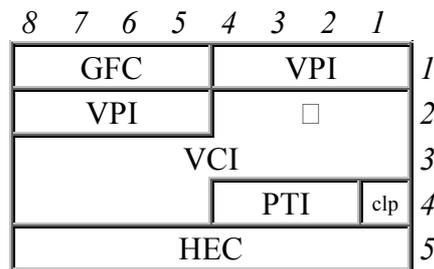
Stargate è un'estremità di connessione per un massimo di otto connessioni ATM Virtual Channel (VC).

Ciascuna VC può essere configurata separatamente a un throughput upstream massimo, che viene quindi tradotto internamente in Peak Cell Rate e usato per controllare la velocità dati.

Attualmente è supportata la Categoria di servizio UBR. Il supporto di categorie addizionali (VBR, ABR, CBR) potrà essere aggiunto in un secondo momento.

### B.12.1.1 Formato delle celle

Il formato dell'intestazione delle celle e la codifica/decodifica dell'intestazione sono conformi al formato UNI come specificato in ITU-T-I.361:



### B.12.1.2 Campo GFC

Il GFC di celle upstream è sempre fissato a zero. Non viene implementata nessuna azione in base al valore del campo GFC nelle celle downstream.

### B.12.1.3 Campo VPI

I valori VPI di ciascuna VC sono programmabili nella gamma 0...255. Il valore di default per il VPI è 8. Le celle con un VPI diverso sono scartate. Un VP/VC speciale è utilizzato per il loopback.

### B.12.1.4 Campo VCI

I valori VCI per ciascuna VC sono programmabili nella gamma 0...65535. Il valore di default per il VCI sono 35, 43, 51 e 59.

### **B.12.1.5 Campo PTI**

L'ultimo bit del campo PTI è utilizzato in entrambe le direzioni per marcare le celle finali per una PDU SAR. Tutti gli altri bit sono fissati a zero/ignorati.

### **B.12.1.6 Bit CLP**

Le celle upstream hanno sempre il bit CLP fissato a 0. I bit CLP delle celle downstream sono ignorati.

## **B.12.2 Supporto F4/F5**

Stargate è conforme ai requisiti di elaborazione Inserzione/estrazione OAM F4/F5 specificati in [ITU-T-I.610].

## **B.13 Livello Fisico**

### **B.13.1 Sublivello TC**

#### **B.13.1.1 Generazione HEC**

Il byte HEC è generato in conformità a ITU-T I.432, compresa l'addizione modulo 2 (XOR) del pattern  $01010101_2$  ai bit HEC .

#### **B.13.1.2 Cell payload scrambling**

Come da ITU-T I.432, il payload di celle upstream/downstream viene scramblato/descramblato utilizzando il polinomio  $X^{43}+1$ .

#### **B.13.1.3 Bit timing and ordering**

Le velocità dati del canale portante AS0 o AS1 devono essere multipli interi di 32 kbit/s. I byte di dati

ATM vengono prima inviati MSB.

#### **B.13.1.4 Cell Delineation**

Il meccanismo di cell delineation si basa sul rilevamento/verifica del campo HEC delle celle downstream.

### B.13.1.5 Cell Rate Decoupling

Stargate inserisce cellule inattive<sup>11</sup> per adattare la velocità delle celle upstream al bit rate upstream configurato dal DSLAM.

### B.13.1.6 Categoria di servizio

Stargate supporta la Categoria di Servizio Unspecified Bit Rate (UBR), secondo quanto specificato nello standard ATM Forum af-tm-0056\_0000.

## B.14 Trasporto ADSL di Traffico ATM

Il subsistema ADSL di Stargate supporta il modo latenza singola. Questo significa che i dati in entrambe le direzioni sono assegnati a un percorso a latenza singola (“fast” o “interleaved”), anche se possono essere utilizzati due percorsi diversi per le due direzioni.

In base alla raccomandazione ITU-T G.992.1 paragrafo 6.2, Stargate utilizza il canale portante AS0 nella direzione downstream e il LS0 nella direzione upstream<sup>12</sup>, con entrambi i canali assegnati indipendentemente al percorso di tipo fast o interleaved.

Sono supportati i bit rate seguenti:

<i>Canale portante</i>	<i>Downstream</i>	<i>Upstream</i>
AS0	da 32 a 6144 kbps, con incrementi da 32 kbps	non applicabile
LS0	0	da 32 a 640 kbps, con incrementi da 32 kbps

<sup>11</sup>

*Intestazione Cella*

*Cella Inattiva*

*Cella Non Assegnata*

<b>GFC</b>	<b>VPI</b>	<b>VPI</b>	<b>VCI</b>	<b>VCI</b>	<b>VCI</b>	<b>VCI</b>	<b>PTI</b>	<b>CLP</b>
0000	0000	0000	0000	0000	0000	0000	000	0
0000	0000	0000	0000	0000	0000	0000	XXX	1

<sup>12</sup> Il LS0 fornisce in principio comunicazione full duplex possibilmente con velocità diverse nelle due direzioni. Nell'applicazione ATM over ADSL la velocità downstream è zero.

**Diritti**

CopyRight 2000 Aethra Srl

Tutti i diritti riservati

Stampato in Italia

**Marchi**

Il marchio AETHRA è registrato da Aethra Srl. Ethernet è un marchio registrato da Xerox Corporation. Microsoft e Windows sono marchi registrati da Microsoft Corporation.