

Manuale Router Bintec



Il presente manuale fa riferimento a tutti gli apparati della serie Bintec R, RS, RT e TR.
In particolare: **R23xa(w)**, **R1200(w)**, **R3x00(w)**, **R4x00**, **Rxx02**, **TR200a(w)**, **RS120(wu)**,
RS230a(w), **RTxx02**

Definizione di Router:	3
Glossario:	4
Operazioni preliminari	7
Port separating	9
Configurazione DHCP Server	13
Configurazione WI-FI	17
NAT	23
Collegamento Internet	29
ETHERNET, ISDN, ADSL, HDSL, SHDSL, UMTS	29
Connessione Ethernet	30
Connessione ISDN.....	36
Connessione ADSL.....	40
Connessione UMTS tramite PCMCIA	57
Connessione UMTS tramite chiavetta USB	59
Connessione HDSL	62
Tunnel Privati Virtuali (VPN)	72
IPSec e PPTP	72
Premessa	73
Configurazione di un tunnel IPSEC.....	74
Configurazione di un tunnel PPTP	90
Configurazione DynDNS	99
Configurazione QoS (Quality of Service)	102
Backup di una connessione DialUp	114
Backup di una connessione ETHERNET	120
Aggiornamento Firmware di un router Bintec	124
Reset alle impostazioni di fabbrica	130

Definizione di Router:

Nella tecnologia delle [reti informatiche](#) un **router**, in inglese letteralmente *instradatore*, è un [dispositivo di rete](#) che si occupa di instradare [pacchetti](#) tra reti diverse ed eterogenee.

Un Router lavora al livello 3 ([rete](#)) del modello [OSI](#), ed è quindi in grado di interconnettere reti di livello 2 eterogenee, come ad esempio una [LAN ethernet](#) con un collegamento geografico in tecnologia [frame relay](#) o [ATM](#).

La funzione di [instradamento](#) è basata sugli indirizzi di livello 3 (rete) del modello OSI, a differenza dello [switch](#) che instrada sulla base degli indirizzi di livello 2 (collegamento). Gli elementi della tabella di instradamento non sono singoli calcolatori ma reti locali. Questo permette di interconnettere grandi reti senza crescita incontrollabili della tabella di instradamento.

Rispetto ai [bridge](#), infatti, i router operando a livello 3 non utilizzano il [MAC address](#) ma l'[indirizzo IP](#) per cui vanno configurati e non sono [plug and play](#).

Per garantire la massima affidabilità e lo sfruttamento ottimale dei collegamenti in caso di reti complesse costituite da molte sottoreti diverse e variamente interconnesse, i router si scambiano periodicamente fra loro informazioni su come raggiungere le varie reti che collegano l'un l'altro, che poi usano per ricavare ed aggiornare delle **tabelle di instradamento** interne da consultare ogni volta che devono smistare i pacchetti di dati in arrivo.

Rispetto ad un bridge, il router blocca le tempeste [broadcast](#) e razionalizza meglio le connessioni tra [host](#) posti su segmenti diversi.

Per fare questo sono stati messi a punto dei [protocolli di routing](#) appositi, come l'[OSPF](#) e il [BGP](#), attraverso i quali i router si scambiano informazioni sulle reti raggiungibili.

Alcuni router possiedono anche un [firewall](#) incorporato, poiché il punto di ingresso/uscita di una rete verso l'esterno è ovviamente il luogo migliore dove effettuare controlli sui pacchetti in transito.

Si vanno sempre più diffondendo router che incorporano la funzionalità di [access point](#) per [reti wireless](#).

I router possono essere normali computer che fanno girare un software apposito ([gateway](#)), o - sempre più spesso - apparati specializzati, dedicati a questo solo scopo. I router di fascia più alta sono basati su architetture hardware specializzate per ottenere prestazioni [wire speed](#), letteralmente alla velocità della linea. Questo significa che un router wire speed può inoltrare pacchetti alla massima velocità delle linee a cui è collegato.

[Fonte: www.wikipedia.org]

Glossario:

ADSL: Asymmetric digital subscriber line. Una delle quattro tecnologie DSL. L'ADSL trasmette con larghezza di banda più ampia in fase di ricezione che in quella di trasmissione.

ATM: Asynchronous Transfer Mode (modalità di trasferimento asincrono). Rete a commutazione di pacchetto caratterizzata da un'elevata ampiezza di banda e velocità di trasferimento dati che, con le fibre ottiche, può giungere fino a 622 Mbit/s. Questo tipo di rete permette di trasmettere su una linea telefonica contemporaneamente, ossia in parallelo, voce, dati ed immagini suddivisi in pacchetti (frame) di dimensione fissa che vengono ricomposti e decodificati una volta giunti a destinazione.

Broadcast: Pacchetto di dati che viene mandato a tutti i nodi di una rete. I pacchetti di dati sono identificati attraverso un indirizzo di broadcast

DHCP: Dynamic Host Configuration Protocol. È un protocollo che permette agli amministratori di rete di gestire centralmente ed in modo automatico l'assegnamento dell'indirizzo IP di ogni dispositivo connesso ad una rete (che deve risultare unico).

Dial-up: Canale di comunicazione telefonica che utilizza una connessione a "commutazione di circuito".

DNS: Acronimo di Domain Naming System. Si tratta del sistema di indirizzamento distribuito che traduce il nome del dominio (DN) nel corrispondente indirizzo IP.

Ethernet: La più diffusa tecnologia LAN inventata dalla Xerox Corporation che utilizza il protocollo CSMA/CS (Collision Detection) per spostare i pacchetti tra computer. Può operare ad una velocità di 10, 100 o 1000 Mbit/s.

Firewall: Software o apparato di rete hardware o software che filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della stessa. I router utilizzano firewall che implementano la sicurezza utilizzando filtri a livello di pacchetto come primo stadio di protezione della rete.

Gateway: Punto di collegamento tra due o più reti differenti, che quindi fa da ingresso. Spesso il gateway corrisponde ad un router, il quale sa in che direzione spedire i pacchetti ricevuti.

LAN: Local Area Network, ovvero la rete locale; generalmente si tratta di una rete privata i cui indirizzi sono del tipo 192.168.x.x oppure 10.x.x.x

Login: Operazione durante la quale vengono digitati lo username e la password, per avere accesso a risorse riservate.

Indirizzo IP: Indirizzo a 32 bit, assegnato agli hosts che utilizzano il protocollo TCP/IP, che identifica univocamente ogni computer collegato alla rete. L'indirizzo IP può appartenere alla classe A, B, C, D o E ed è visualizzato come una successione di 4 numeri decimali separati da un punto, ad esempio 192.168.2.1.

Interfaccia (interface): dispositivo in grado di far dialogare due sistemi di rete. Ogni interfaccia di rete è caratterizzata da un indirizzo MAC, ovvero un codice univoco che identifica l'hardware e da un indirizzo IP. Un'interfaccia viene definita "virtuale" quando utilizzano lo stesso indirizzo MAC di altre interfacce ma IP diverso.

IP: è l'acronimo di Internet Protocol. Esso rappresenta lo strato di rete nel protocollo TCP/IP. La funzione principale di tale protocollo è quello di instradare i pacchetti, attraverso le migliaia di reti che costituiscono Internet, affinché raggiungano correttamente la destinazione. A livello hardware sfrutta i router.

IPSec: Protocollo basato su IP che garantisce l'integrità e l'autenticità del traffico che transita su una rete condivisa non sicura.

ISDN: Acronimo di Integrated Services Digital Network: reti digitali di servizi integrati. Rete di comunicazione digitale mondiale che intende sostituire quelle attuali; il sistema, sincrono e full duplex, sarà in grado di trasmettere voce, immagini e dati contemporaneamente e sulla stessa linea.

ISP: Internet Service Provider. Società che gestisce gli accessi ad Internet. Collegando il proprio computer (via modem o router) al server dell'ISP, si entra in Internet.

MAC address: è un indirizzo univoco espresso in esadecimale e stampato sulla scheda di rete (NIC). Possiamo immaginarlo come un IP di livello più basso ed è attraverso questo indirizzo che il bridge e lo switch effettuano la consegna dei pacchetti all'interno di una LAN dopo che il MAC (Media Access Control) ha stabilito a chi assegnare la priorità di trasmissione.

NAT: Network Address Translation. Meccanismo sviluppato per ridurre il fabbisogno globale di indirizzi IP unici. Il NAT permette ad una organizzazione di utilizzare al suo interno indirizzi non unici, ovvero utilizzati anche da altre aziende. La connessione verso internet è possibile grazie ad una traslazione degli indirizzi privati in pubblici. Ad un unico indirizzo pubblico (risparmio degli indirizzi IP) possono corrispondere numerosi indirizzi privati.

Pacchetto: Rappresenta un blocco di dati che viene inoltrato sulla rete per raggiungere la destinazione opportuna. Il pacchetto che viene spedito, contiene alcune informazioni importanti come il mittente, il destinatario e informazioni per controllare eventuali errori dovuti alla trasmissione.

Ping: E' un programma che permette di controllare la connettività della rete. La verifica viene fatta inviando un pacchetto diagnostico a un nodo specifico della rete; quando tale pacchetto raggiungerà la destinazione, il nodo relativo dovrà riconoscere il pacchetto ricevuto e viene restituito anche il tempo necessario al pacchetto per raggiungere il nodo.

PPP: Acronimo di Point to Point Protocol: è un protocollo che permette a TCP/IP di funzionare su connessioni di linea seriale. PPP e SLIP, rappresentano i protocolli più comuni per supportare connessioni telefoniche a Internet.

PPTP: Point-To-Point Tunneling Protocol. Protocollo che permette l'implementazione di reti virtuali VPN in Internet o Intranet, consentendo di utilizzare protocolli diversi dal TCP/IP.

Protocollo: Insieme di regole e convenzioni seguite sia nel trasferimento che nella ricezione dei dati fra due computer. In particolare esso definisce il formato, la sincronizzazione, la sequenza e il controllo degli errori usati sulla rete.

QoS: Quality of Service - Qualità del Servizio. Nasce dall'idea che la velocità di trasmissione e il tasso di errori possono essere misurati, migliorati ed in alcuni casi bisogna garantirne una percentuale. QoS è particolarmente importante quando si trattano comunicazioni che includono video e voce o comunque informazioni di tipo multimediali, poiché questi tipi di dati devono essere gestiti in modo differenziato rispetto ai dati puri.

Scheda di rete: Si tratta di un dispositivo che permette al computer di colloquiare con la rete. Le schede di rete (NIC - Network Interface Card) sono generalmente installate all'interno del PC. Una scheda di rete è detta anche "interfaccia".

TCP: Transmission Control Protocol. E' un protocollo connection oriented del livello transport del modello OSI che trasmette i dati in maniera full-duplex ed è responsabile: della suddivisione dei dati che vengono trasmessi in segmenti, del rinvio dei segmenti non ricevuti, del riassettaggio dei dati.

TCP/IP: Transmission Control Protocol/Internet Protocol. È il protocollo utilizzato da Internet e da molte reti locali. In particolare, il TCP si occupa della suddivisione dei messaggi in "pacchetti", mentre l'IP pensa ad inviarli al corretto destinatario.

Telnet: Protocollo simile al TCP/IP che permette ad un utente di collegarsi in maniera interattiva ad un dispositivo in remoto; è un'applicazione client/server usata per interrogazioni di database o per usufruire di servizi specifici di alcuni server.

UDP: User Datagram Protocol. UDP è un protocollo di trasporto semplice, senza connessione, che si basa sul trasferimento di pacchetti di dati. Non è particolarmente affidabile: invia i pacchetti ma non garantisce che questi arrivino a destinazione. Sono quindi gli applicativi che lo utilizzano che devono preoccuparsi dell'affidabilità del servizio.

URL: Universal Resource Locator. L'indirizzo di una pagina web su Internet, cioè l'indirizzo completo da digitare per ricevere una pagina, in formato alfabetico. L'URL viene trasformata in indirizzo IP dal DNS.

VoIP: Voice Over IP. Tecnologia digitale che consente la trasmissione di pacchetti vocali attraverso reti Internet, Intranet, Extranet, e VPN. I pacchetti vengono trasportati secondo le specifiche H.323,

ossia lo standard ITU che costituisce la base per i servizi dati, audio, video e comunicazioni sulle reti di tipo IP.

VPN: Virtual Private Network. Rete privata virtuale che permette al traffico IP di viaggiare in modo sicuro su una rete TCP/IP pubblica (Internet, Intranet o Extranet) grazie alla codifica di tutto il traffico da una rete ad un'altra. La VPN utilizza il "tunneling" per codificare tutte le informazioni a livello IP e rappresenta l'alternativa economica alle più costose linee dedicate.

WAN: Wide Area Network; è una rete composta da due o più LAN. La WAN più comune è internet.

Wireless: Le tecnologie "wireless", sono quelle tecnologie che non utilizzano cavi per i collegamenti. Le LAN wireless (WLAN) sono reti locali senza cavi, interne a edifici, che comunicano utilizzando una tecnologia radio o a raggi infrarossi per collegare i computer.

xDSL: Acronimo generico che si riferisce all'intera famiglia delle tecnologie DSL. Vedi ADSL, HDSL, SDSL e VDSL.

ROUTER BINTEC

Operazioni preliminari

Esistono 3 modi diversi per accedere alla configurazione dei router Bintec:

Connessione seriale

Connessione IP

Connessione ISDN

Connessione Seriale:

Tutti i router Bintec dispongono di una porta seriale: in alcuni modelli si tratta di una mini-USB, in altri si utilizza la porta ethernet 1 alla quale si deve collegare il cavo seriale in dotazione.

Le impostazioni della porta seriale sono le seguenti:

Bit per Secondo: 9600

Bit di Dati: 8

Parità: Nessuno

Bit di Stop: 1

Controllo di Flusso: Nessuno

Connessione IP:

Per accedere attraverso il protocollo TCP/IP occorre collegarsi tramite cavo Ethernet alle porte delle switch oppure tramite wireless (solo per i modelli che supportano il wireless).

Per accedere al pannello di configurazione del router aprire il prompt di DOS e digitare il comando:

```
telnet <ip router>
```

L'indirizzo IP di default del router è 192.168.0.254.

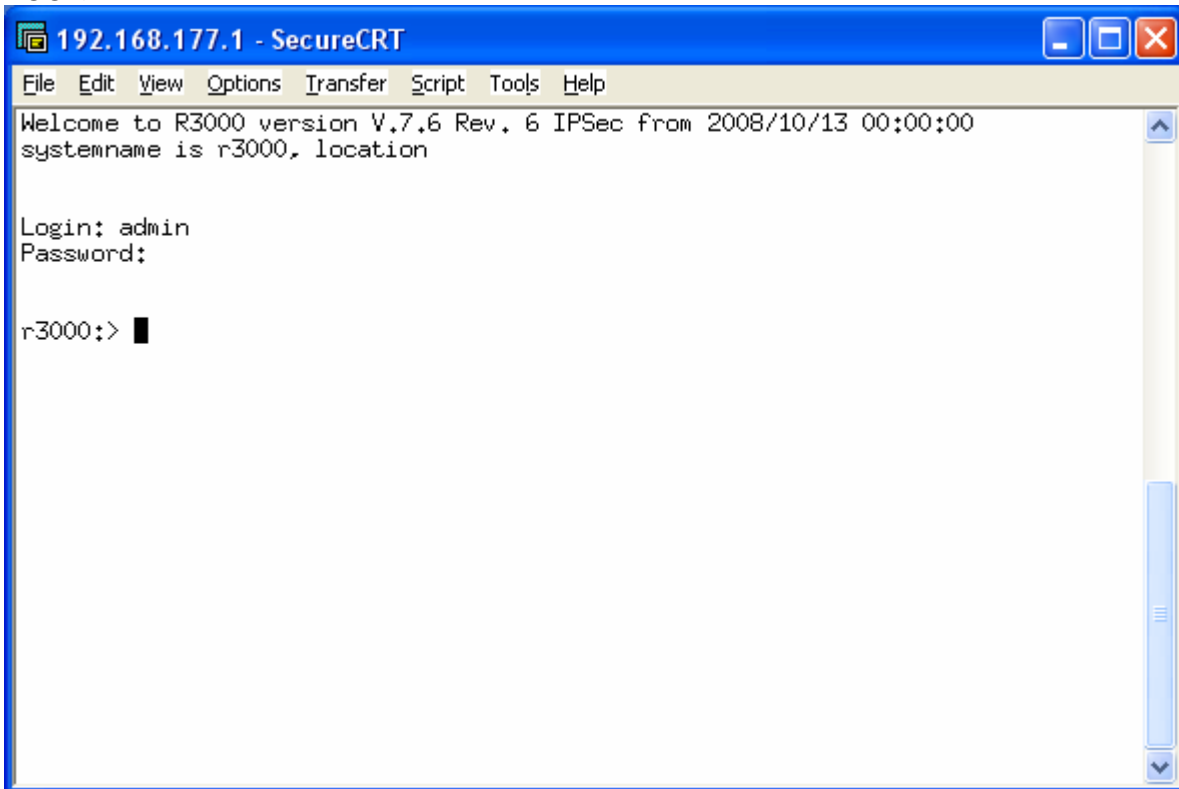
Connessione ISDN:

Tutti i router Bintec permettono l'accesso remoto tramite un protocollo proprietario chiamato ISDNLogin. In sostanza si tratta di collegare alla borchia ISDN il router remoto che vogliamo raggiungere; nella sede locale servirà un secondo router Bintec col quale effettuare la "chiamata" digitando il comando:

```
isdnlogin <numero telefonico>
```

Qualsiasi metodo si segua per l'accesso ci si troverà di fronte ad una schermata che ci chiede di effettuare il login (i parametri di default dalla serie "Bintec R" sono *user: admin password: funkwerk* mentre per i modelli precedenti (serie X) *user: admin password: bintec*)

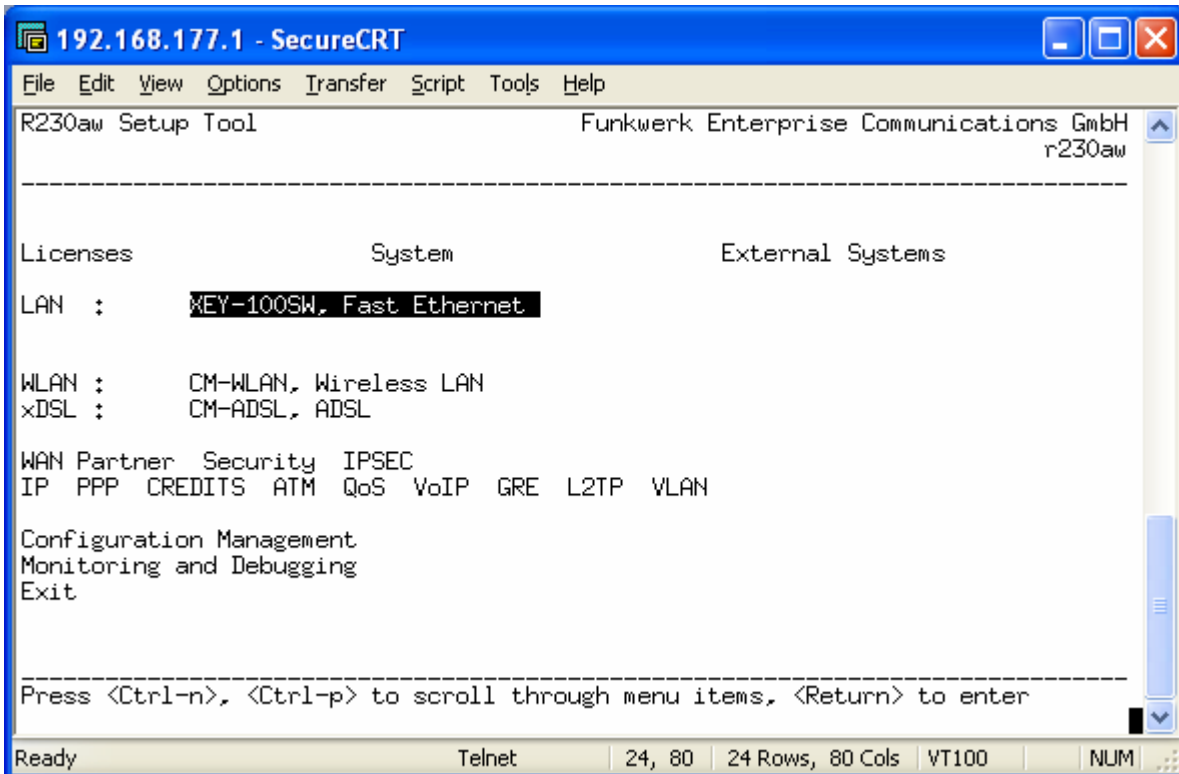
ROOT>



A questo punto si entra nel pannello attraverso il comando *setup*. Se a questo facciamo seguire l'opzione *-p* sarà possibile vedere le password in chiaro (utile per ricavare la password di login dell'[ADSL](#)).

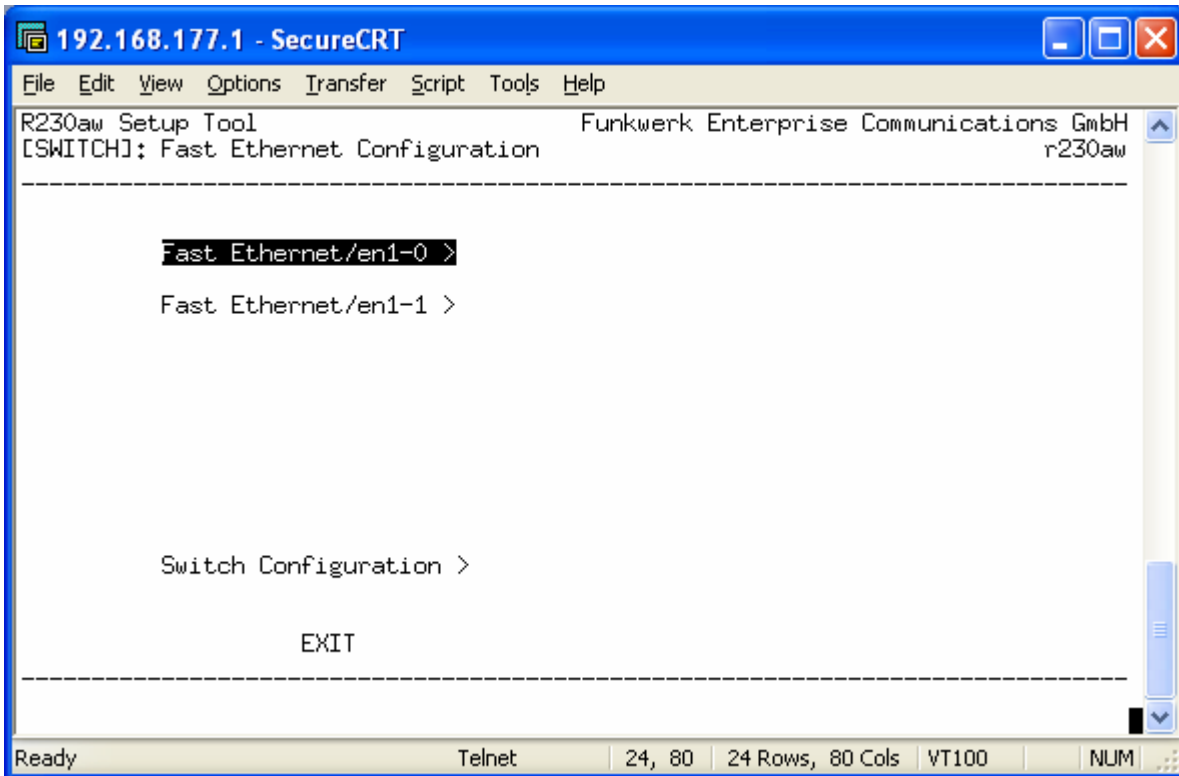
La schermata iniziale si presenta così:

ROOT> SETUP>



Port separating

Selezionando la voce *LAN: Fast Ethernet* si accede all'interfaccia ethernet del router. Da qui è possibile assegnare uno o più indirizzi (Primary Address e Secondary Address) alla parte LAN del router. Il secondo indirizzo risulta utile nel caso in cui si debba utilizzare un pool di indirizzi aggiuntivi come avviene per le ADSL di tipo RPoA.



```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool                               Funkwerk Enterprise Communications GmbH
[SWITCH]: Fast Ethernet Configuration           r230aw

-----

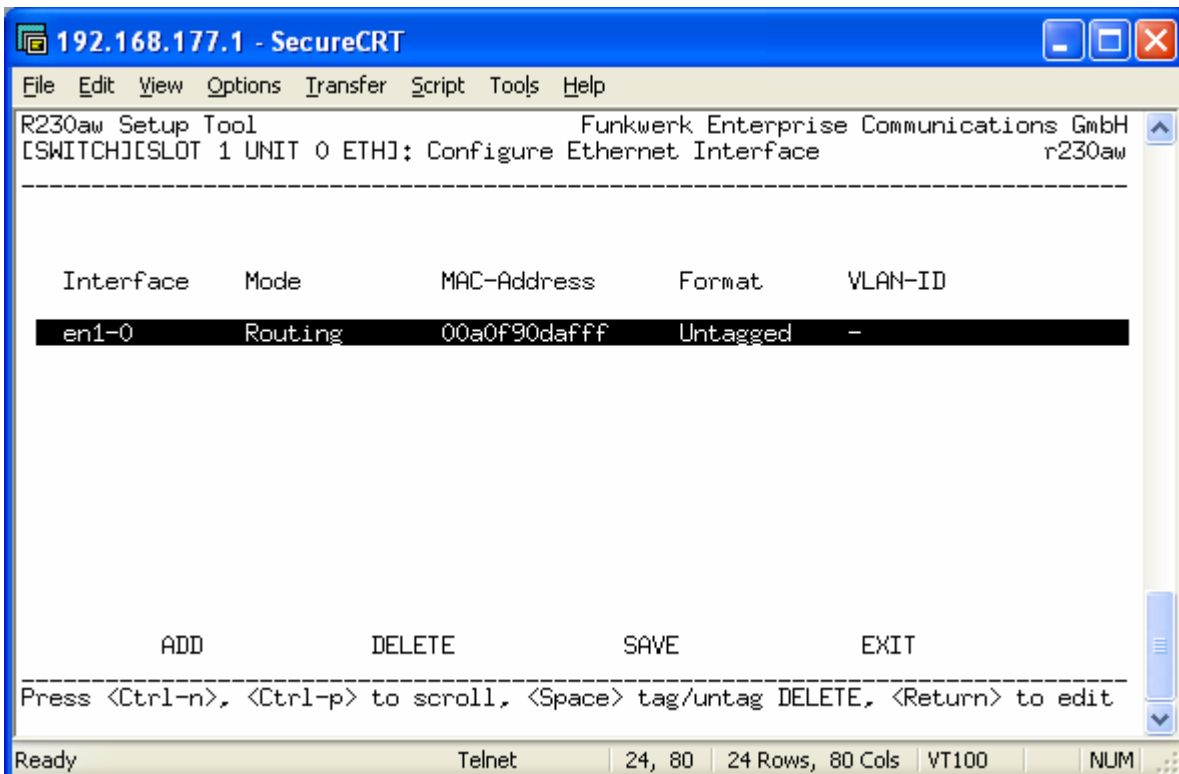
Fast Ethernet/en1-0 >
Fast Ethernet/en1-1 >

Switch Configuration >

EXIT

-----

Ready                               Telnet          24, 80   24 Rows, 80 Cols  VT100      NUM
```



```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool                               Funkwerk Enterprise Communications GmbH
[SWITCH][SLOT 1 UNIT 0 ETH]: Configure Ethernet Interface   r230aw

-----

Interface      Mode          MAC-Address    Format         VLAN-ID
-----
en1-0          Routing       00a0f90dafff  Untagged      -

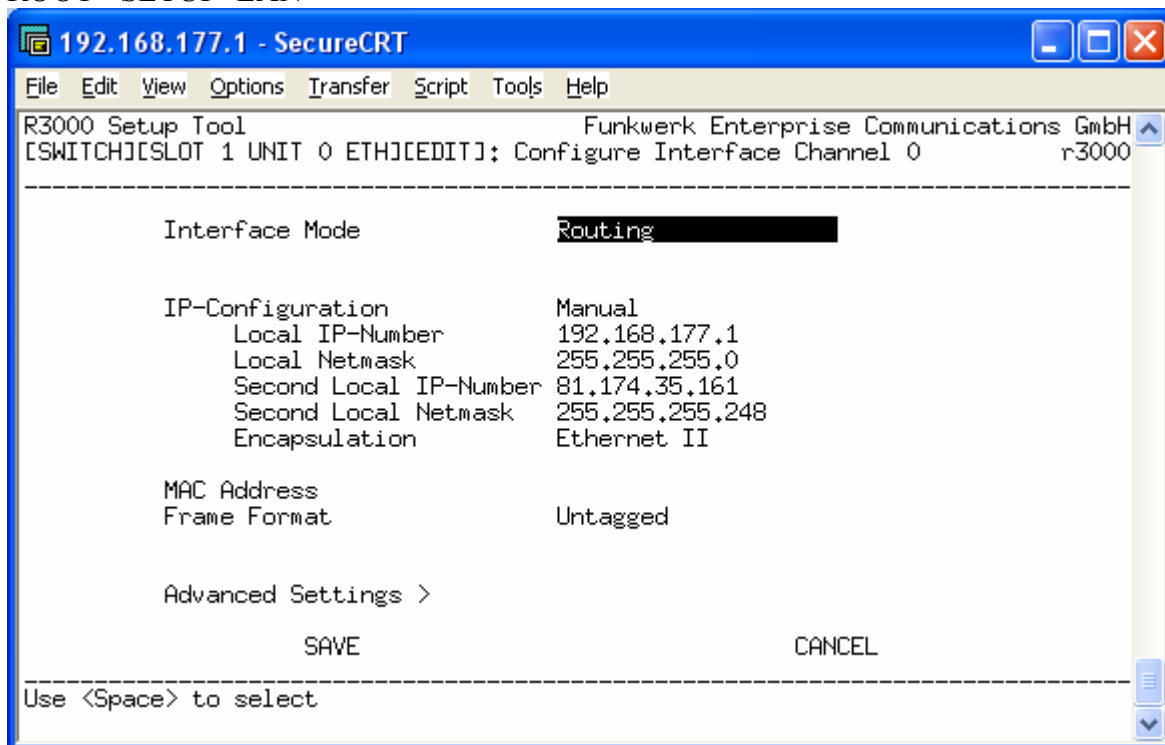
ADD            DELETE        SAVE           EXIT

-----
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit

Ready                               Telnet          24, 80   24 Rows, 80 Cols  VT100      NUM
```

Selezionando *Add* è possibile creare altre interfacce virtuali per applicazioni avanzate.

ROOT> SETUP>LAN>



Occorre fare attenzione alla differenza fra la modalità Routing (default) e la modalità Bridging: quando si specifica la modalità “Routing” significa che l’interfaccia possiede un indirizzo IP proprio, quando invece si specifica la modalità “Bridging” significa che l’interfaccia appartiene ad un bridge, ovvero appartiene ad una interfaccia virtuale (servono almeno 2 interfacce fisiche per fare un bridge!) e l’indirizzo IP viene assegnato al bridge, non all’interfaccia fisica. In sostanza si tratta di un indirizzo condiviso con un’altra interfaccia fisica.

Le porte ethernet del router fanno inizialmente parte della stessa interfaccia EN1-0. Se si vuol separare le porte dello switch 1-4 si entra nel menù LAN e in *switch configuration* si assegnano i nuovi nomi delle interfacce alle porte.

```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R3000 Setup Tool Funkwerk Enterprise Communications GmbH
[SWITCH]: Fast Ethernet Configuration r3000

-----

Fast Ethernet/en1-0 >
Fast Ethernet/en1-1 >

Fast Ethernet/en1-4 >

Switch Configuration >

EXIT

-----
```

```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R3000 Setup Tool Funkwerk Enterprise Communications GmbH
[SWITCH][ASSIGN]: Switch Interface Assignment r3000

-----

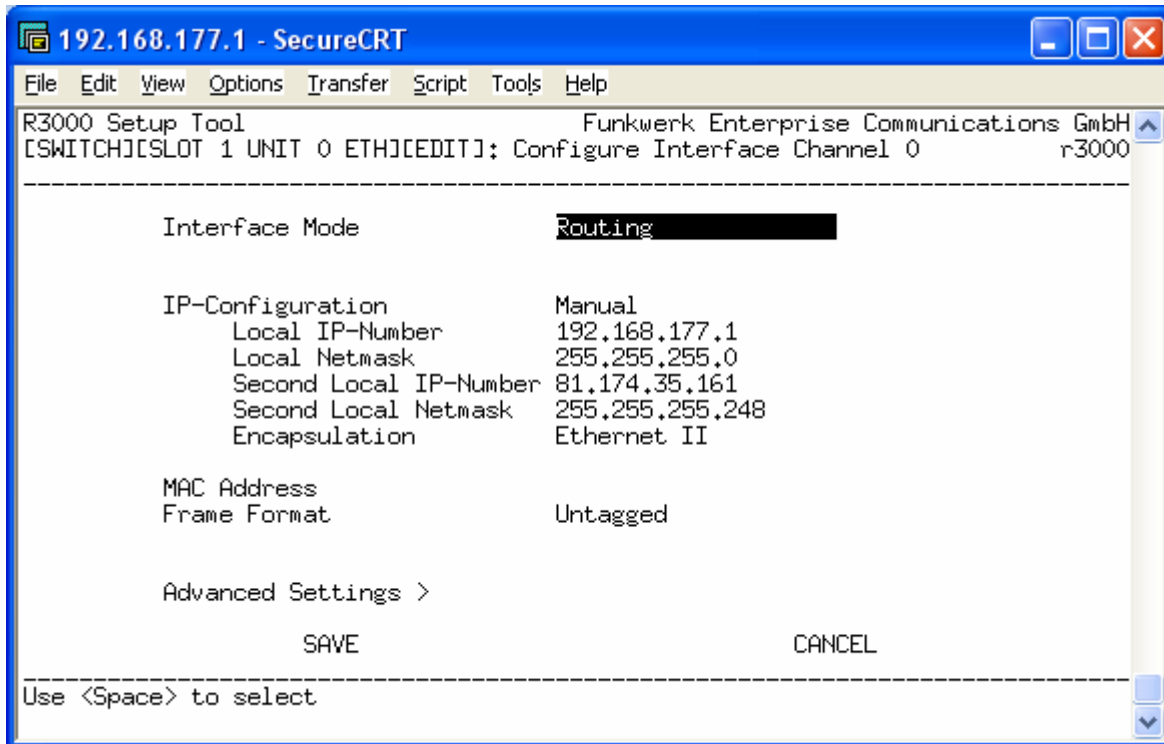
Switch Port    Assigned Interface    Switch Port Mode

Port 1         en1-0                 full autonegotiation
Port 2         en1-0                 full autonegotiation
Port 3         en1-0                 full autonegotiation
Port 4         en1-1                 full autonegotiation
Port 5         en1-4                 full autonegotiation

SAVE          CANCEL

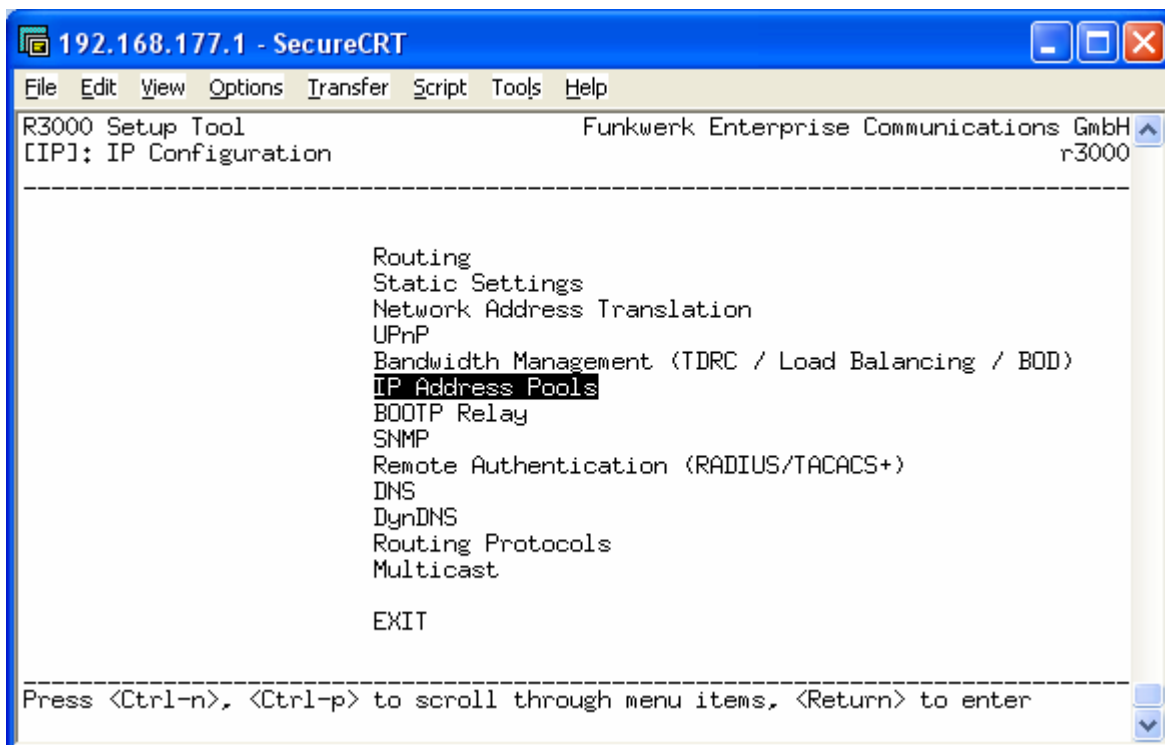
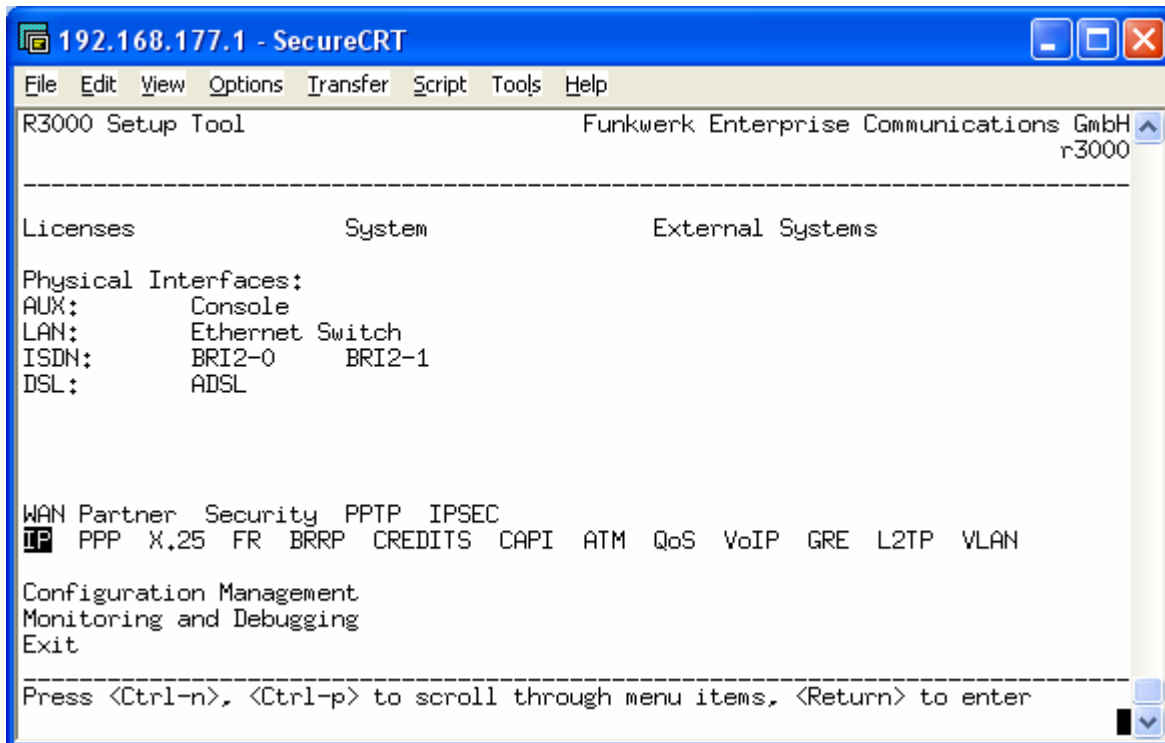
-----
Use <Space> to select
```

Successivamente dovremo configurare le nuove interfacce ottenute (EN1-X) assegnando loro un indirizzo IP ciascuna. Avendo 4 porte potremo ottenere 4 interfacce con indirizzi IP diversi ma pur sempre pingabili fra loro. Per separarle le reti a livello di IP è necessario operare con il Firewall.

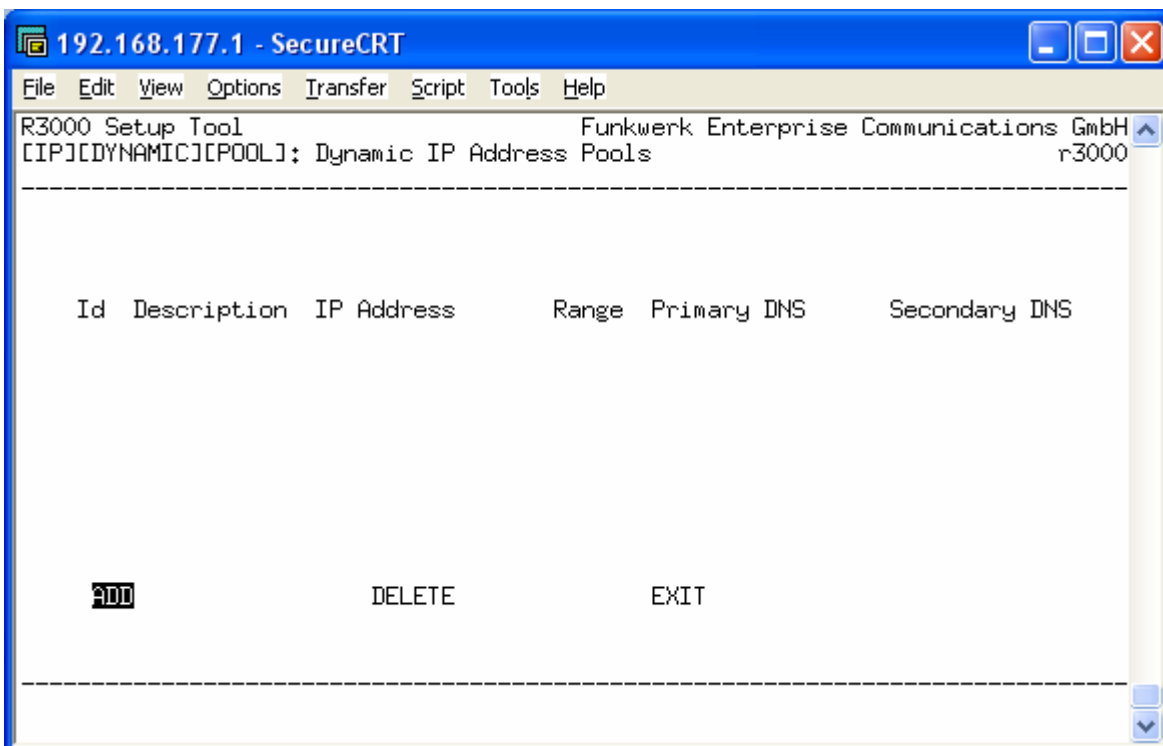
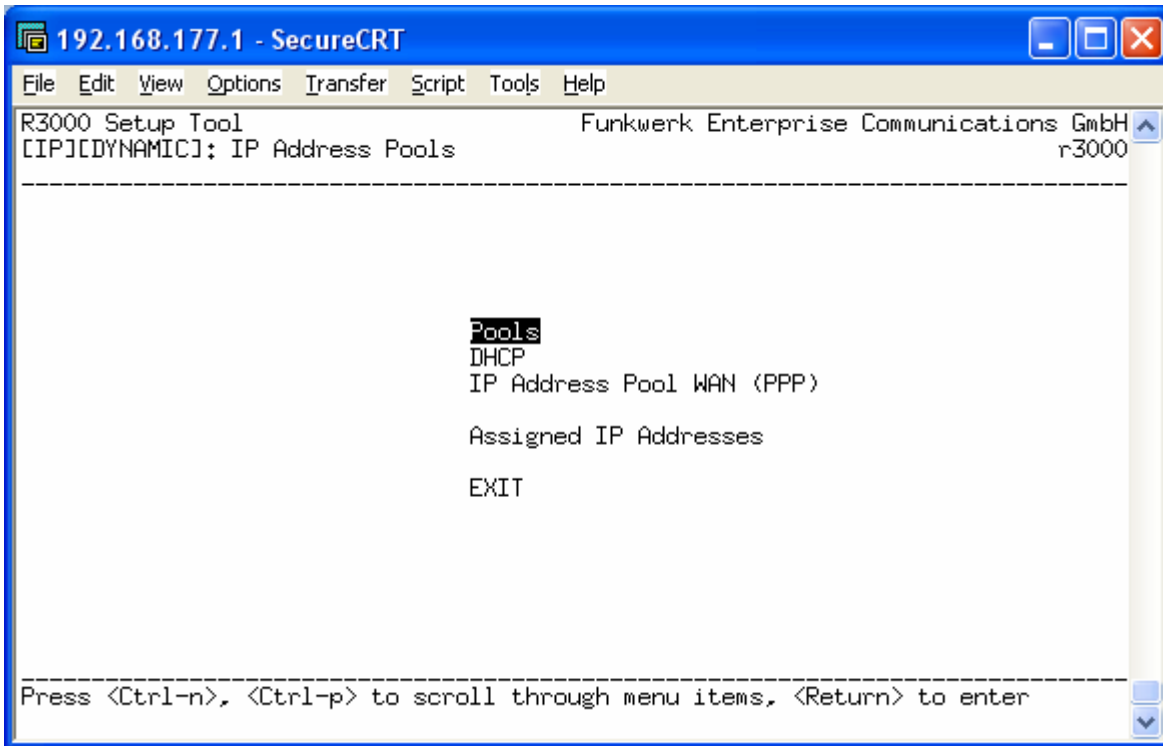


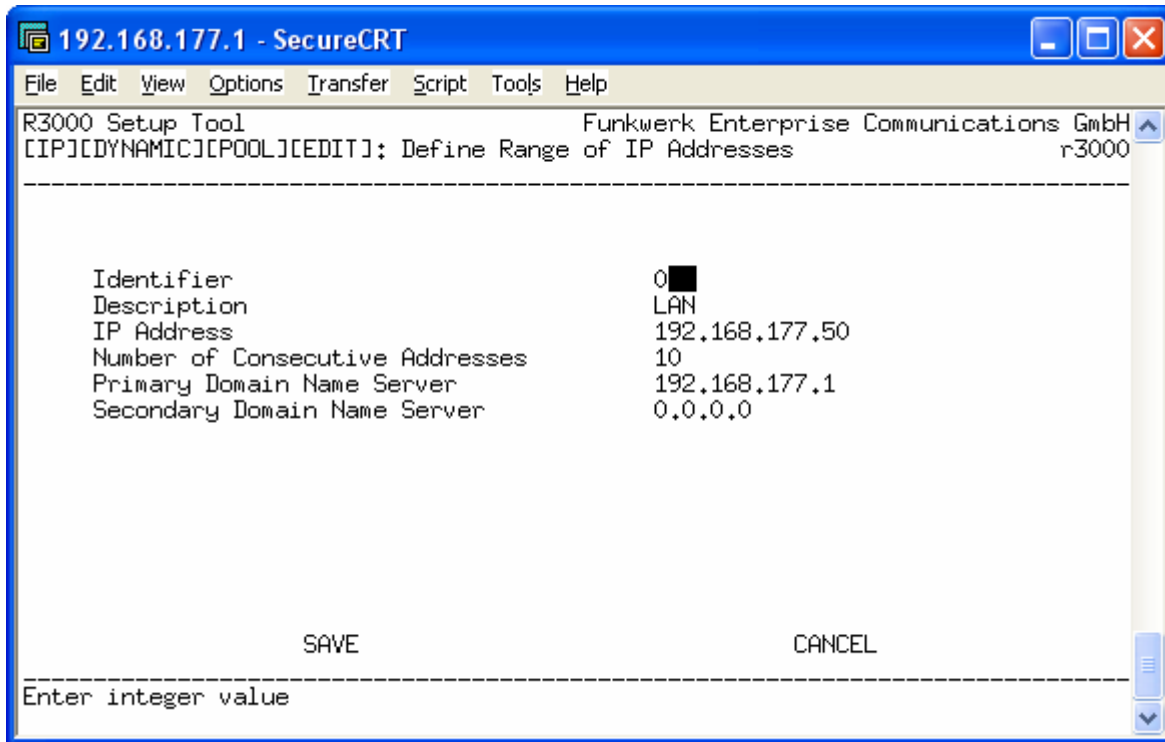
Configurazione DHCP Server

Per assegnare indirizzi IP attraverso le interfacce del router bisogna configurare il DHCP Server per ogni interfaccia che si intende utilizzare. Si accede al menù *IP* e quindi a *IP Address Pool*



Per prima cosa occorre creare i range di indirizzi da assegnare (*Pools*), poi occorre specificare su quali interfacce verranno distribuiti tali indirizzi (*DHCP*)





Identifier: identificativo del pool (deve essere diverso per ogni gruppo che si crea)

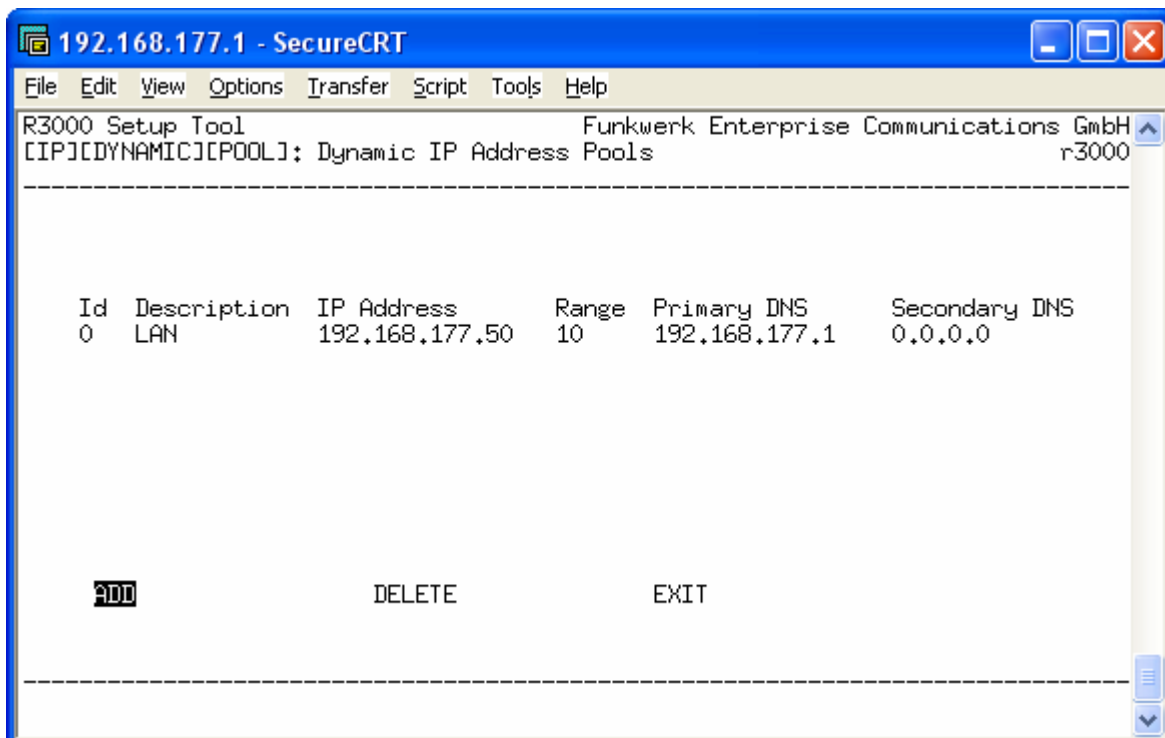
Description: descrizione del pool

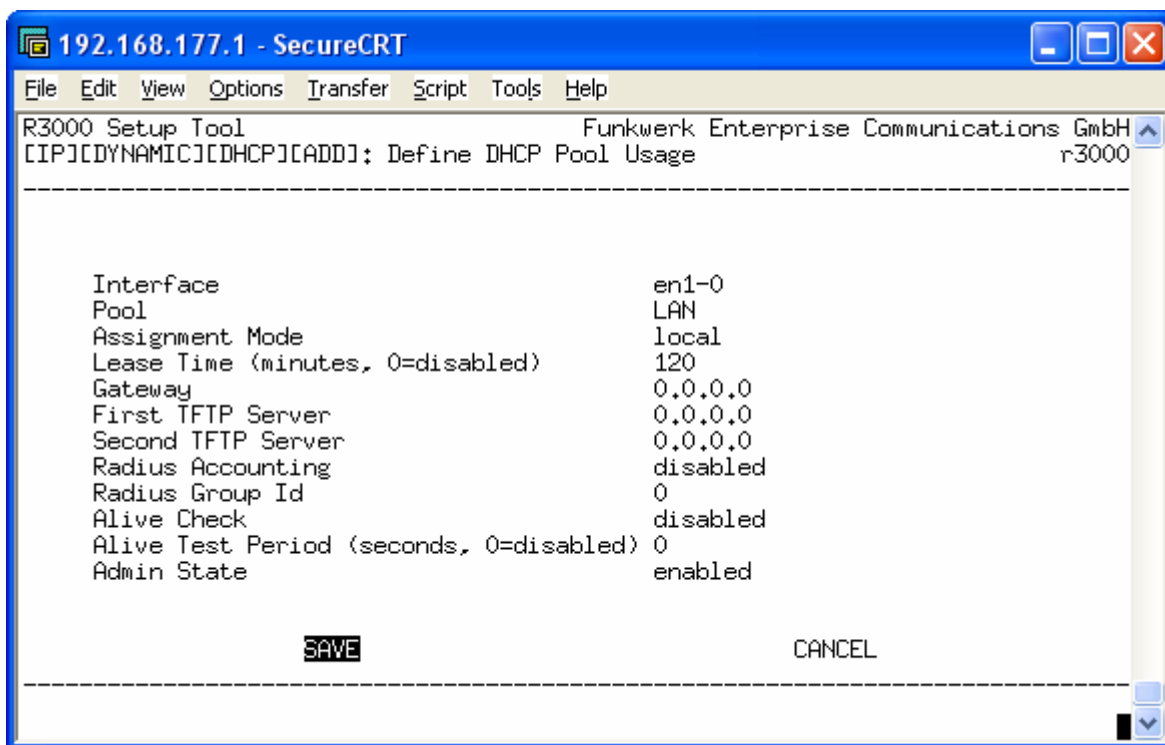
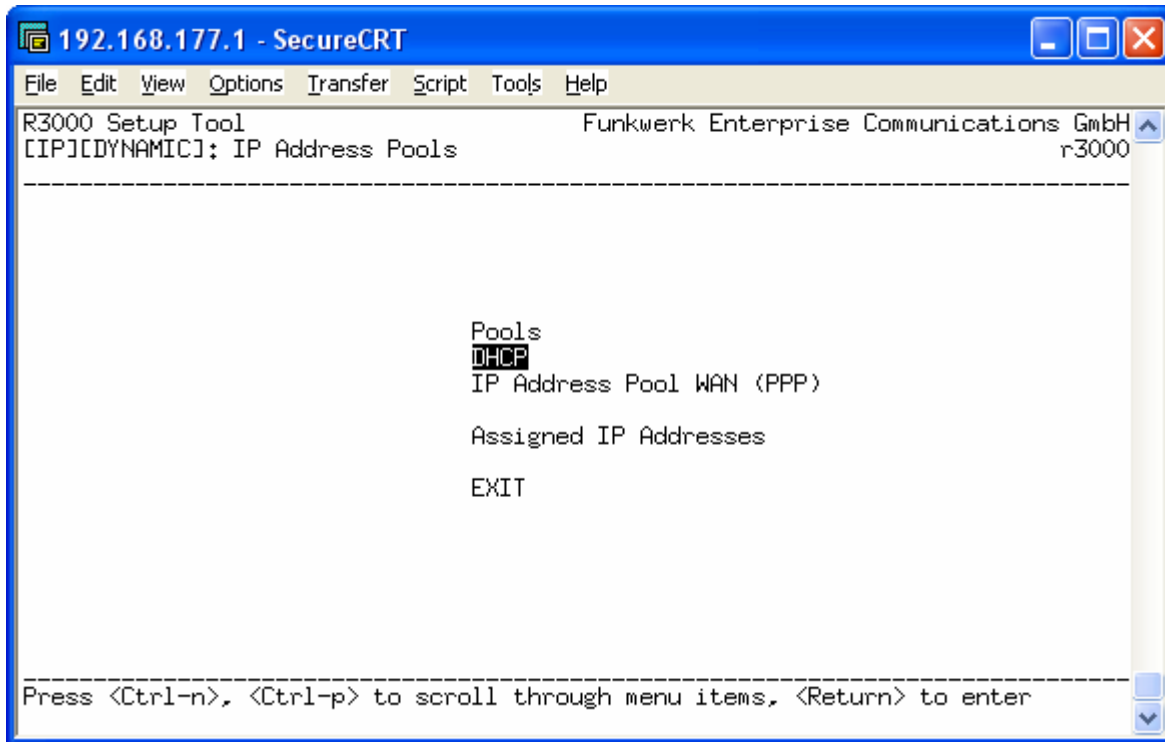
IP Address: primo indirizzo IP che verrà distribuito dal router

Number of Consecutive Addresses: numero massimo di indirizzi IP consecutivi che verranno distribuiti

Primary Domain Name Server: IP del resolver DNS principale

Secondary Domain Name Server: IP del revolver DNS secondario





Interface: indica l'interfaccia sulla quale distribuire gli indirizzi

Pool: nome del pool precedentemente creato

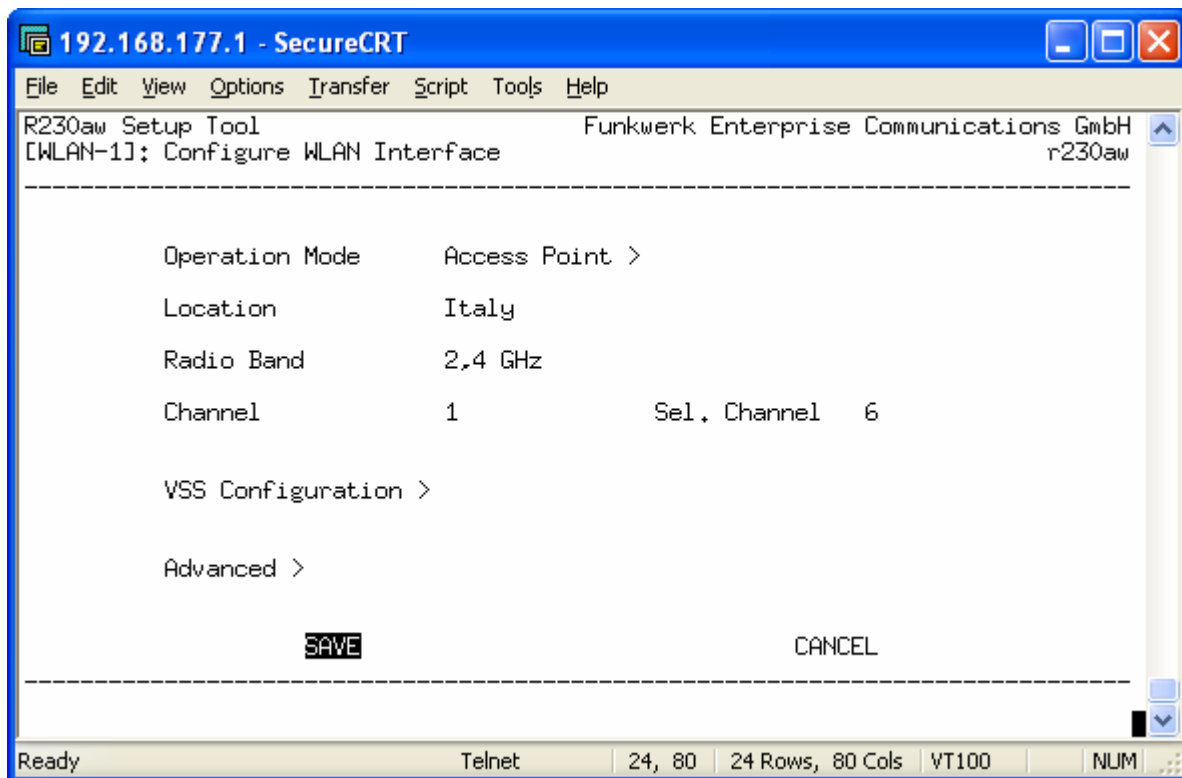
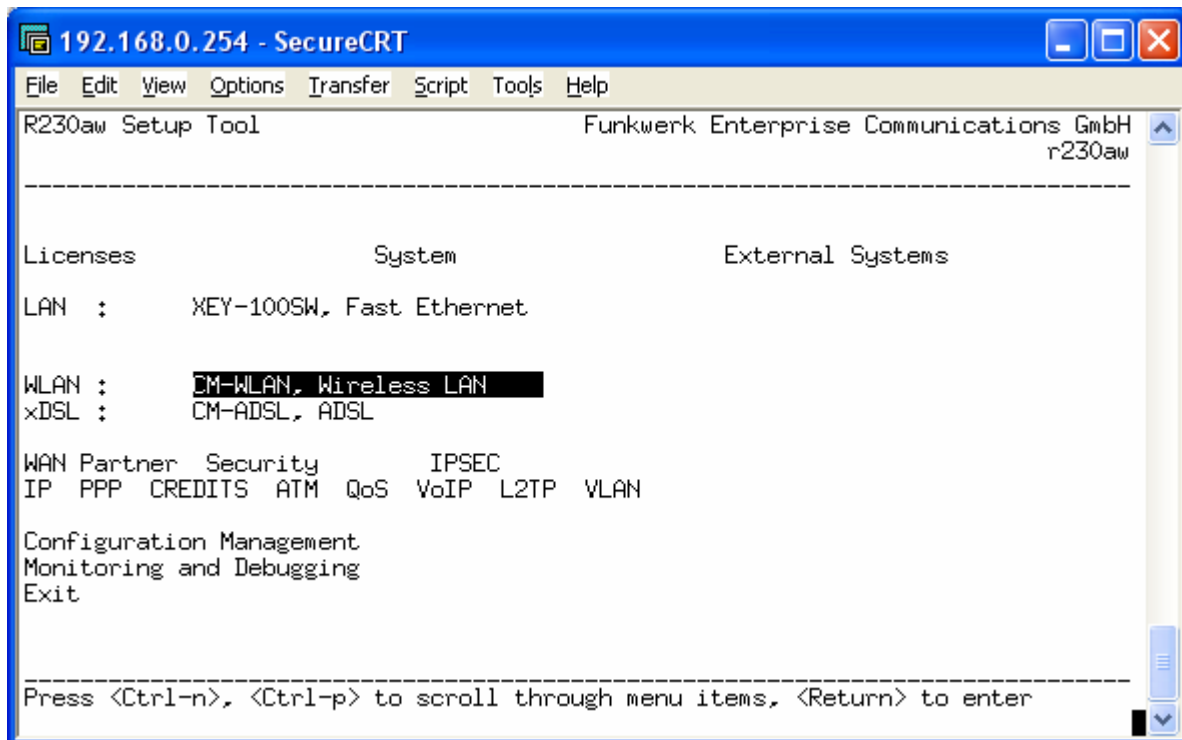
Assignment Mode: modalità di assegnamento (*local* significa che è il router che fa da DHCP server, *relay* significa che il router rigira le richieste di DHCP ad un altro server in rete)

Lease Time: tempo di rilascio degli indirizzo nel caso in cui l'host che ne ha fatto richiesta non sia più in rete

Gateway: permette di assegnare l'indirizzo IP del gateway di default; se non specificato viene assegnato l'indirizzo IP dell'interfaccia che ha provveduto all'assegnamento dell'indirizzo.

Configurazione WI-FI

Per accedere alla configurazione dell'interfaccia wireless entrare nel menù *Wireless LAN*.

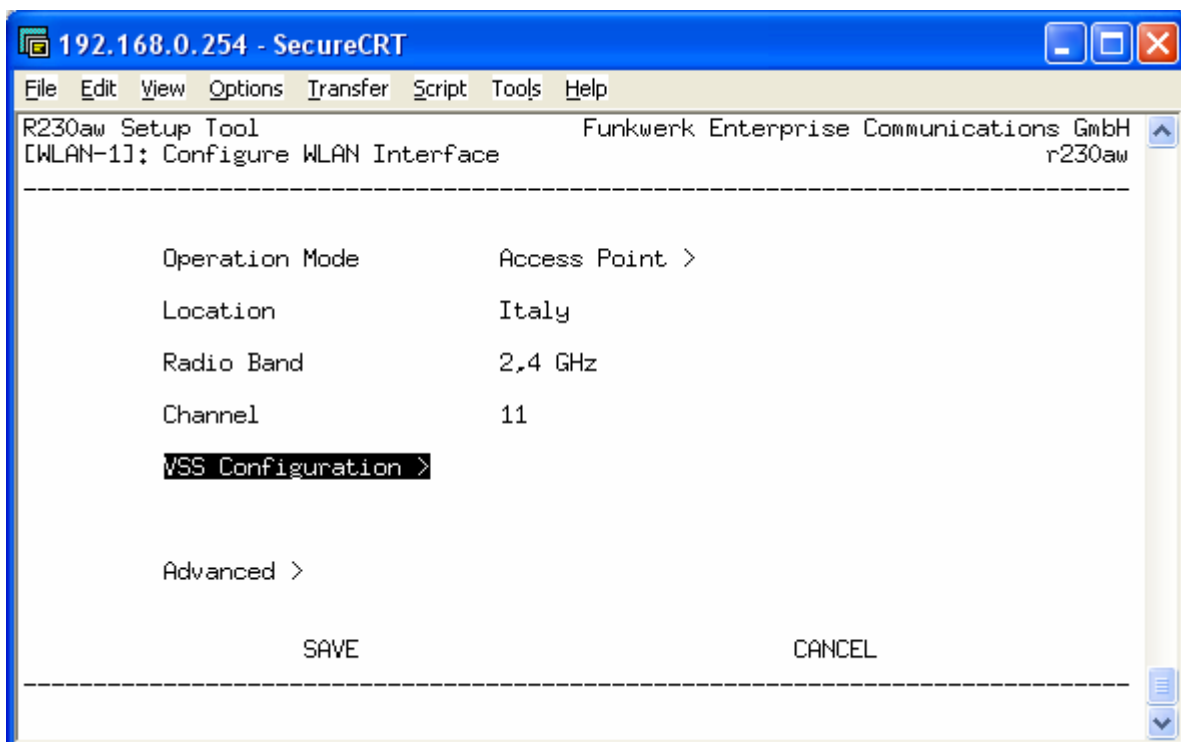
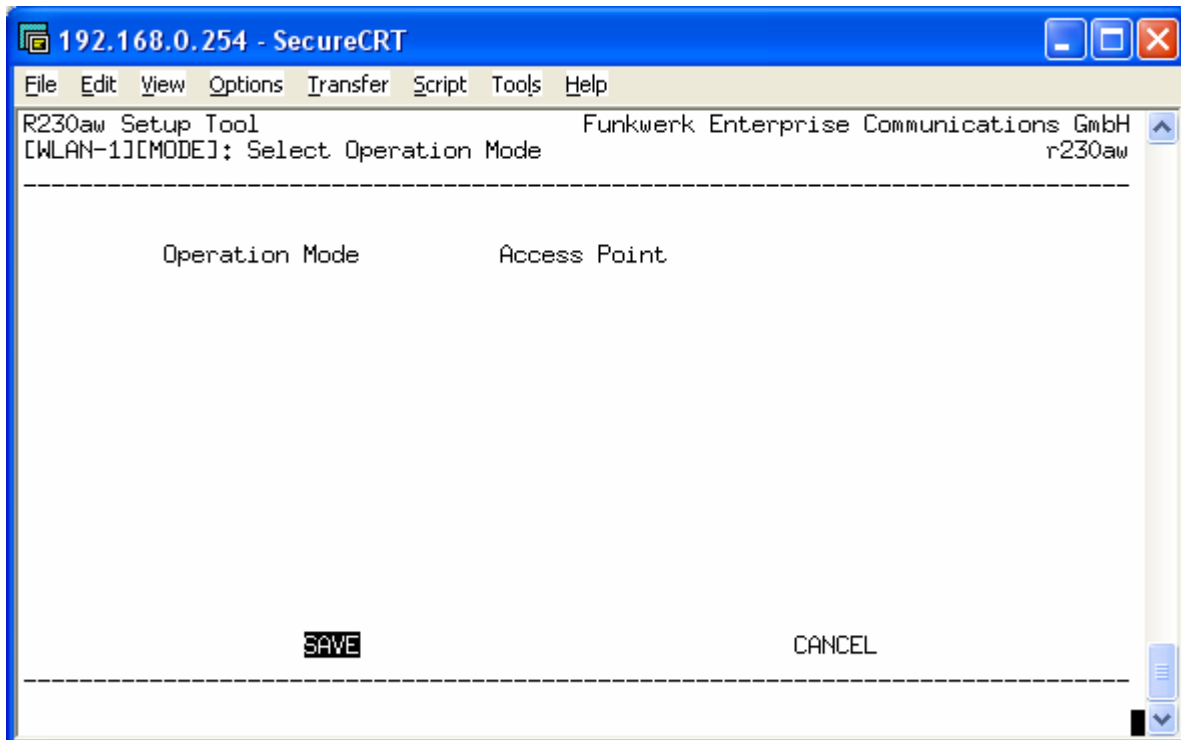


Operation Mode: i modelli R230aw, R232aw e TR200aw possono funzionare esclusivamente come Access Point a 2,4 GHz mentre i modelli R3000w, R1200w e R1200wu possono funzionare come Access Point e come Repeater a 2,4 GHz e a 5 GHz

Location: selezionare Italy. Serve a scegliere le frequenze legalmente concesse nel paese di utilizzo.

Radio Band: modificabile solo per gli apparati che possono lavorare sia a 2,4 GHz che a 5 GHz.
Channel: indica il canale sul quale verrà effettuata la trasmissione.

Dal menù Operation Mode settare la modalità Access Point



Entrando in *VSS Configuration* è possibile creare diverse interfacce wi-fi. Di default è già presente l'interfaccia Funkwerk-ec ma se ne possono aggiungere fino a 16.

```

192.168.0.254 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool Funkwerk Enterprise Communications GmbH
[WLAN-1][WIRELESS]: Interface List r230aw
-----
Network Name      Status  Security  ACL-Filter  interface
-----
*Funkwerk-ec     enable  NONE      disable     vss1-0

ADD                DELETE            EXIT

-----
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit

```

```

192.168.0.254 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool Funkwerk Enterprise Communications GmbH
[WLAN-1][WIRELESS][EDIT]: Wireless Interface <Funkwerk-ec> r230aw
-----
AdminStatus       enable
Network Name      Funkwerk-ec
Name is visible   yes
Local Communication enabled

Security Mode     NONE

IP and Bridging >
ACL Filter >
SAVE              CANCEL

-----
Use <Space> to select

```

Admin Status: permette di attivare o disattivare l'interfaccia

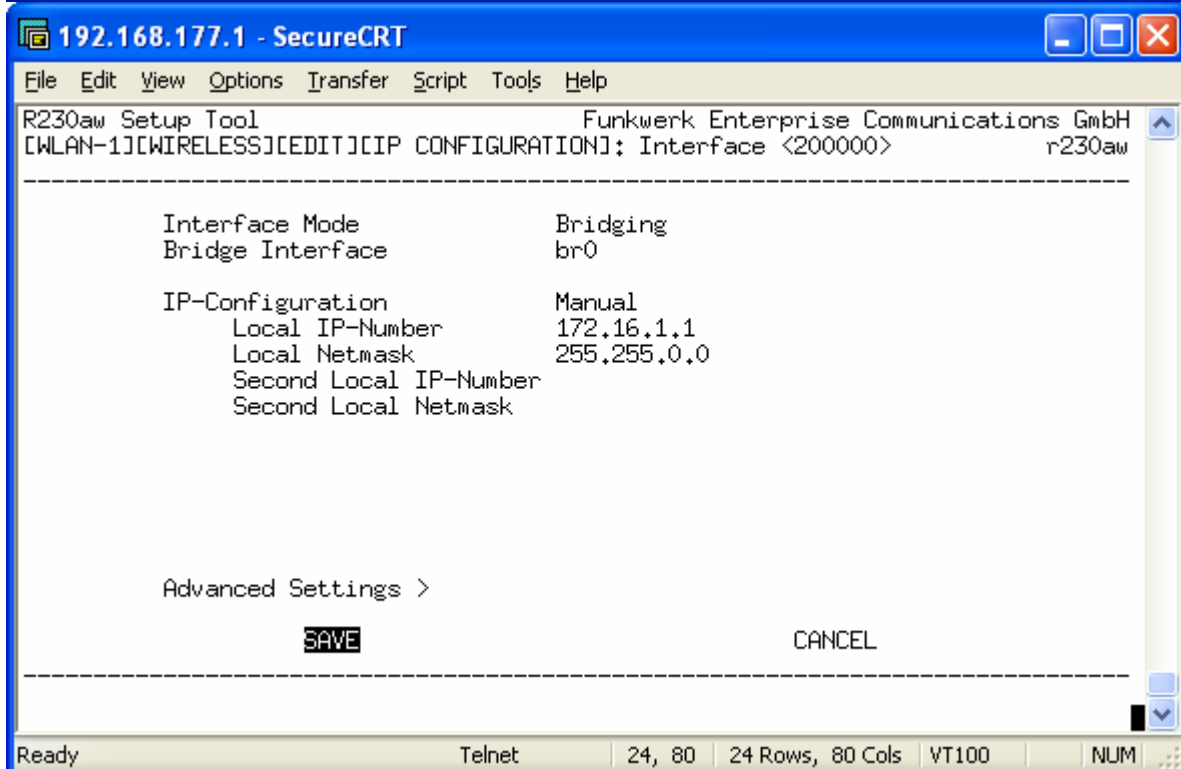
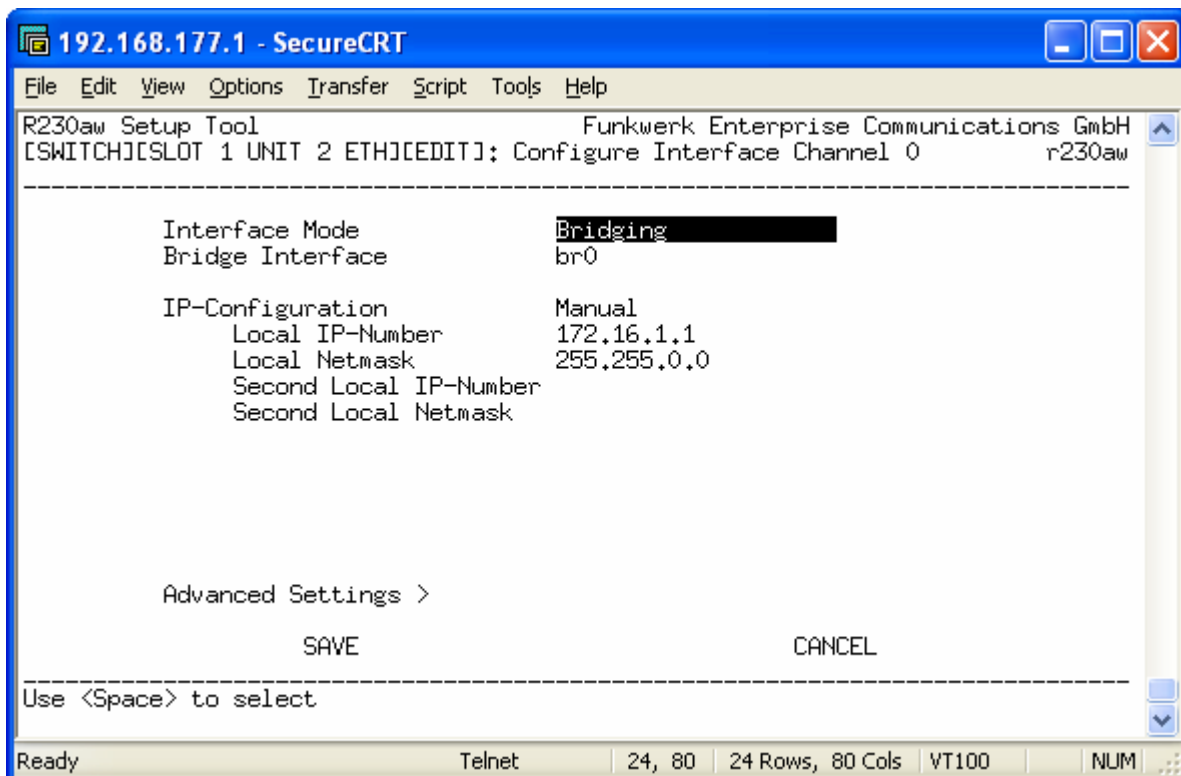
Network Name: è il nome identificativo della rete che verrà visualizzato dai client

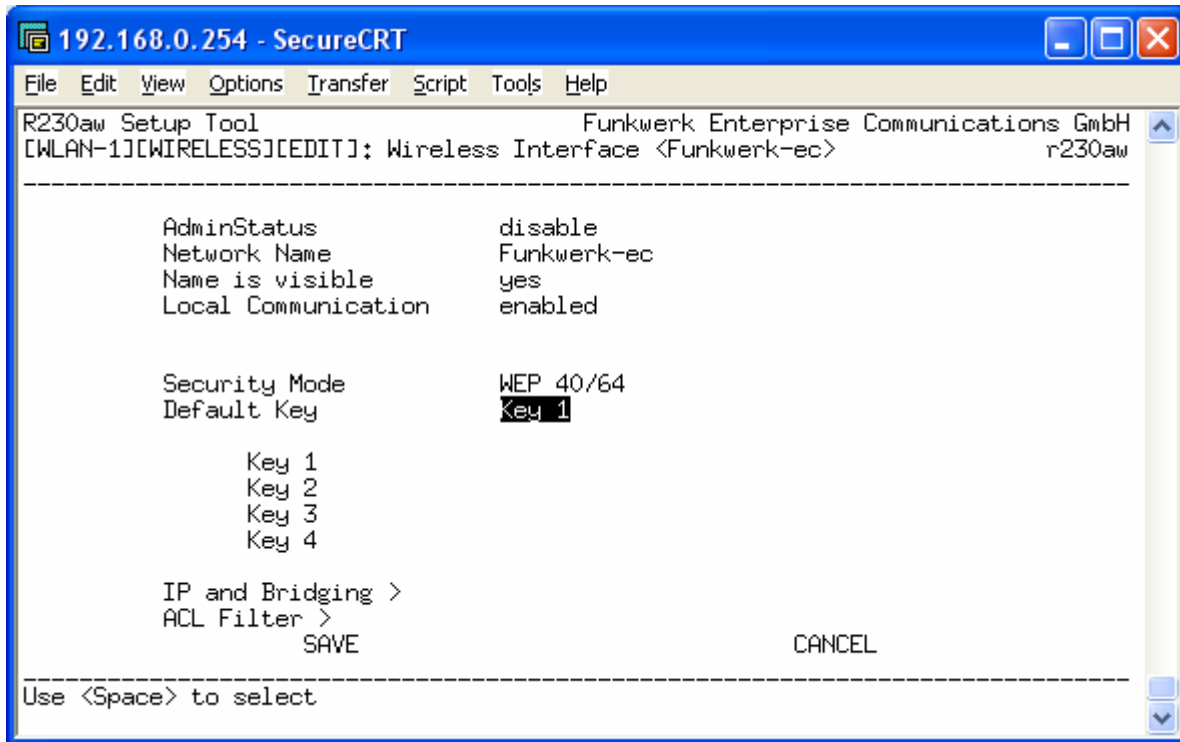
Name is visibile: permette di nascondere l'identificativo di rete quando i client effettuano una "Ricerca reti wireless a distanza di rilevamento". Solo gli host che conoscono il nome identificativo di rete possono linkarsi.

Local communication: permette di disabilitare la comunicazione fra gli host che si collegano all'Access Point.

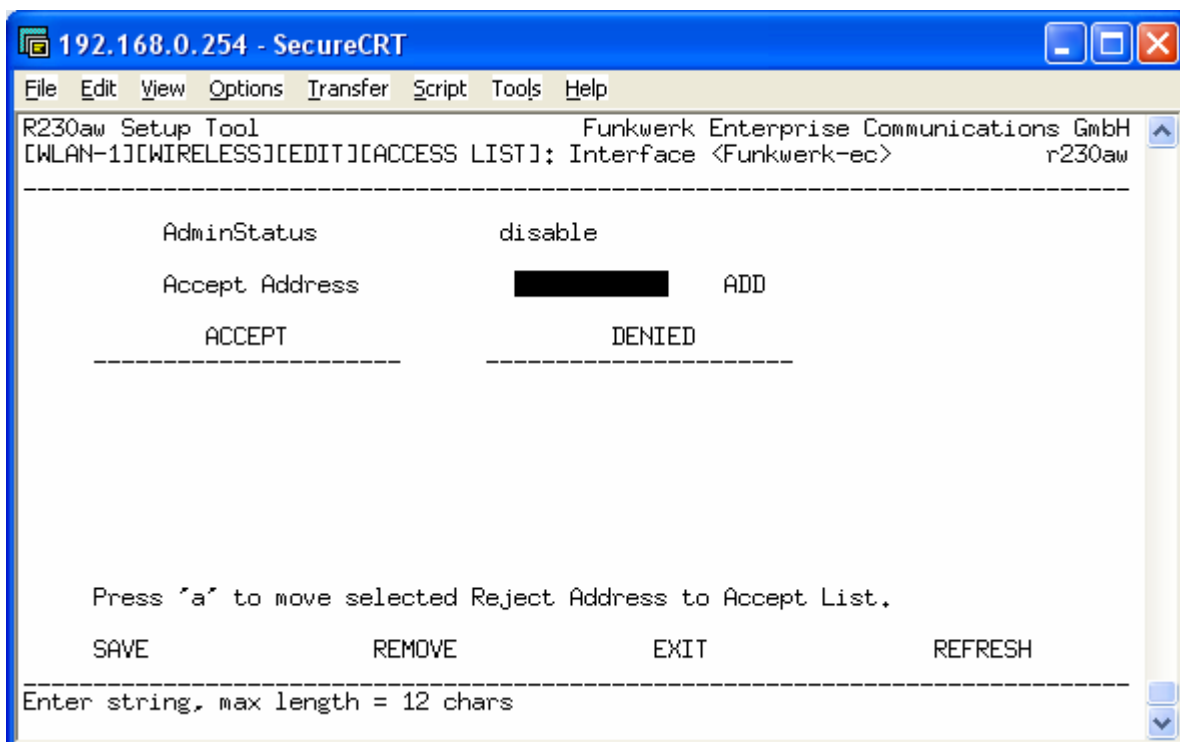
Security Mode: permette di inserire la crittografia per proteggere l'accesso alla rete e rendere sicure le comunicazioni fra gli host e l'Access Point. Sono disponibili le modalità WEP, WPA e WPA2. Dalla voce *IP and Bridging* è possibile assegnare un indirizzo IP alla WLAN. Se invece si vuole che la WLAN abbia lo stesso indirizzo della LAN bisogna assegnare entrambe le interfacce allo

stesso bridge (es. br0) come discusso nella sezione Port separating precedentemente affrontata. Come si vede dalle immagini che seguono entrambe le interfacce (Ethernet e Wireless) appartengono al bridge br0 e fanno capo quindi allo stesso indirizzo IP.

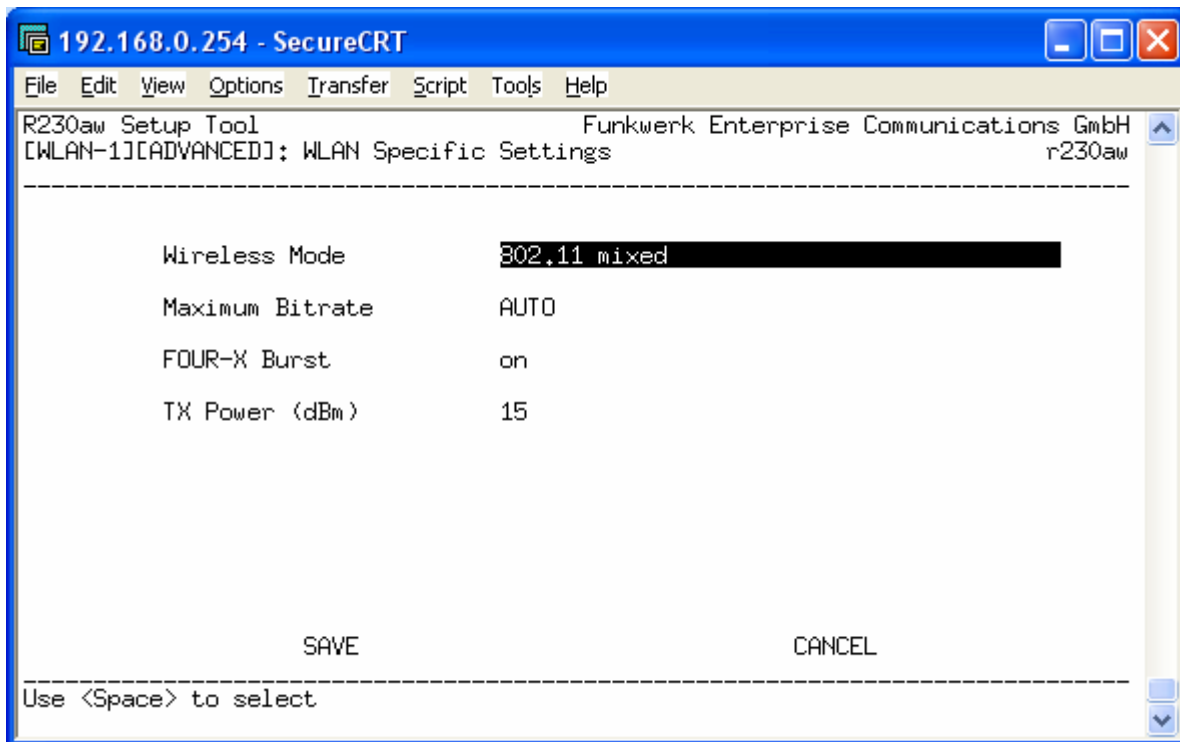
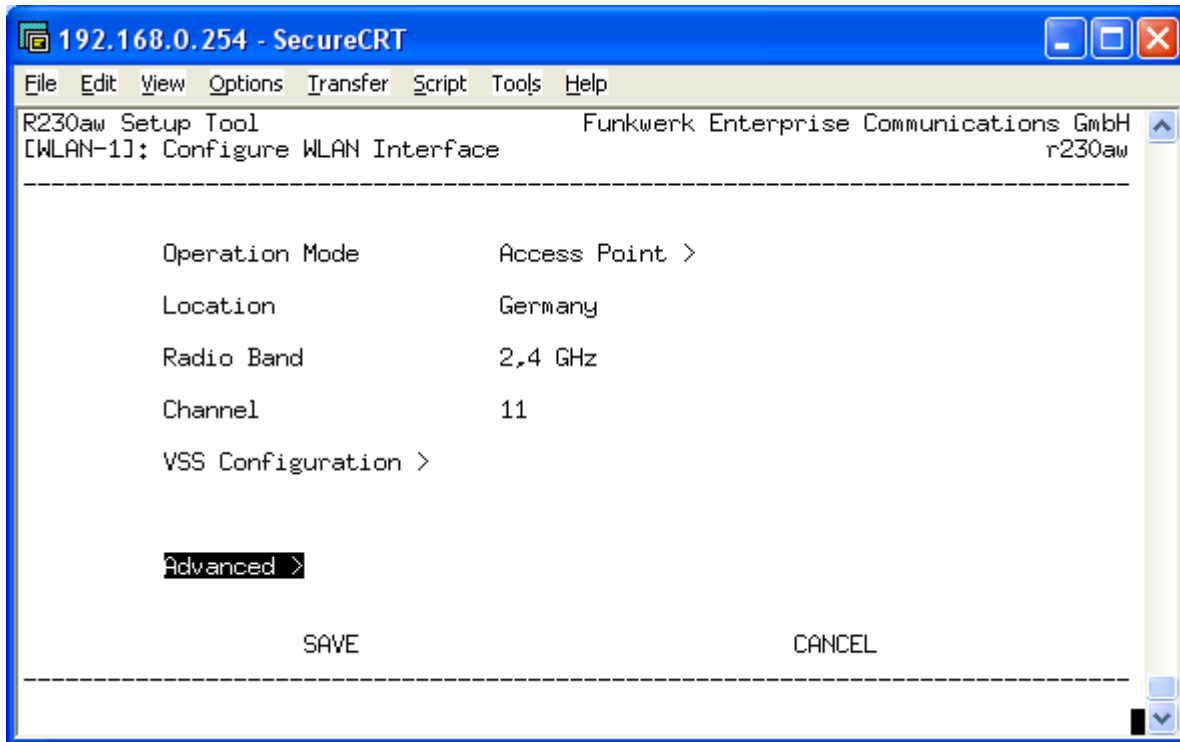




E' anche possibile negare l'accesso ad alcuni MAC ADDRESS abilitando l'ACL Filter. Ogni nuovo MAC che si collega al router viene messo per default nella lista REJECTED. Per abilitarlo è necessario spostarlo nella colonna ACCEPT con il tasto "a". Oppure si possono inserire anche a mano nella voce *Accept Address*.



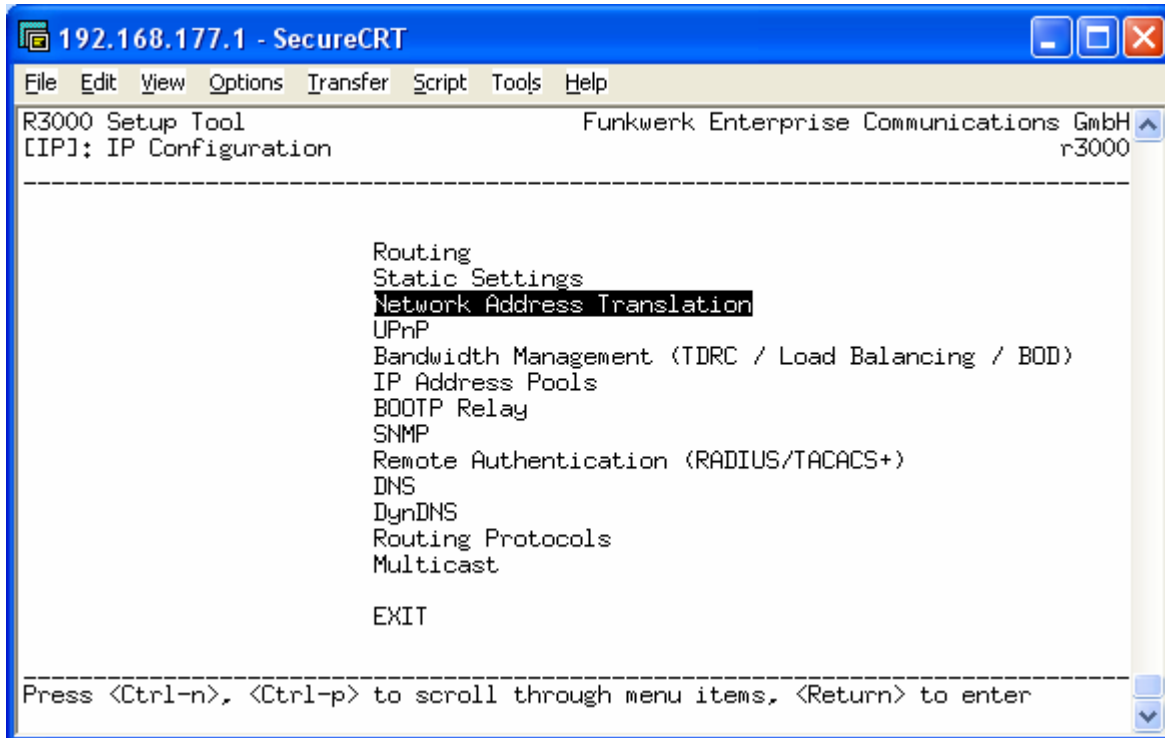
Infine, dal menù Advanced si può decidere di far lavorare l'Access Point in 802.11b, 802.11g, 802.11b/g mixed o 802.11a (solo su modelli R3000w, R1200w e R1200wu) . Per avere una maggior compatibilità con tutte le schede wireless è bene settare 802.11 mixed. In questo modo però verranno ridotte le prestazioni in quanto la banda massima si riduce notevolmente.



NAT

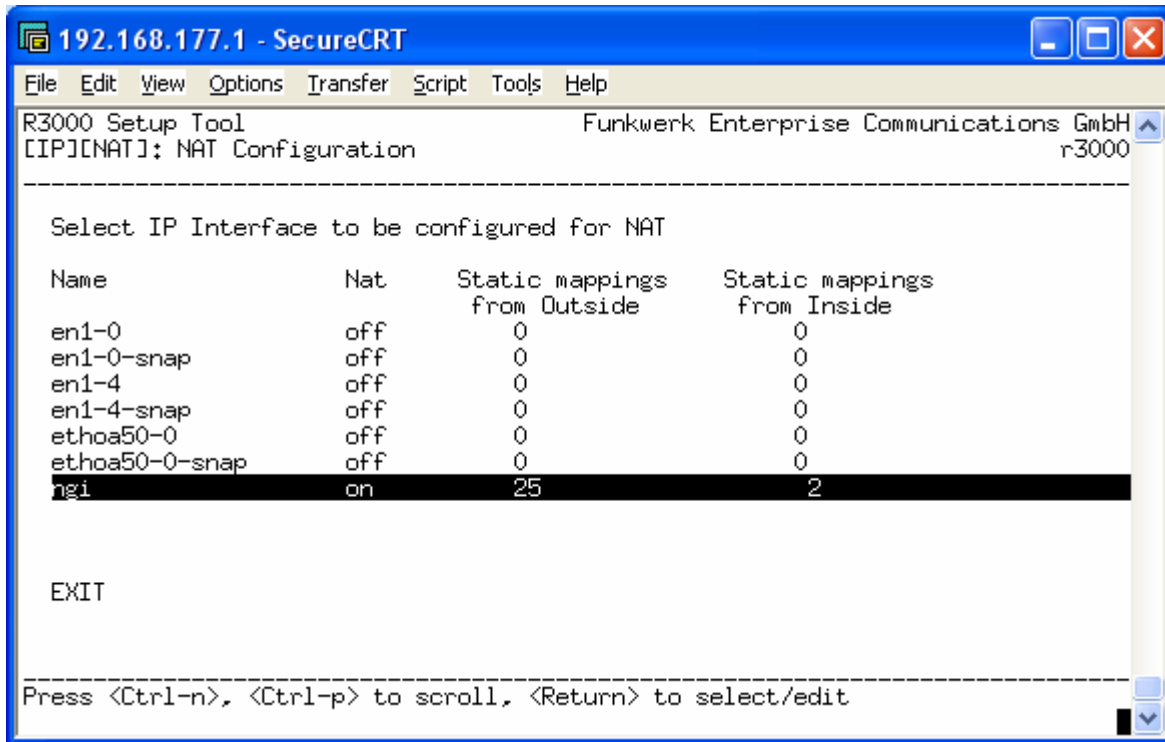
Attraverso il menù Network Address Translation è possibile impostare le regole del NAT per rendere accessibili da internet alcuni servizi in esecuzione sulla rete interna.

ROOT> SETUP>IP>



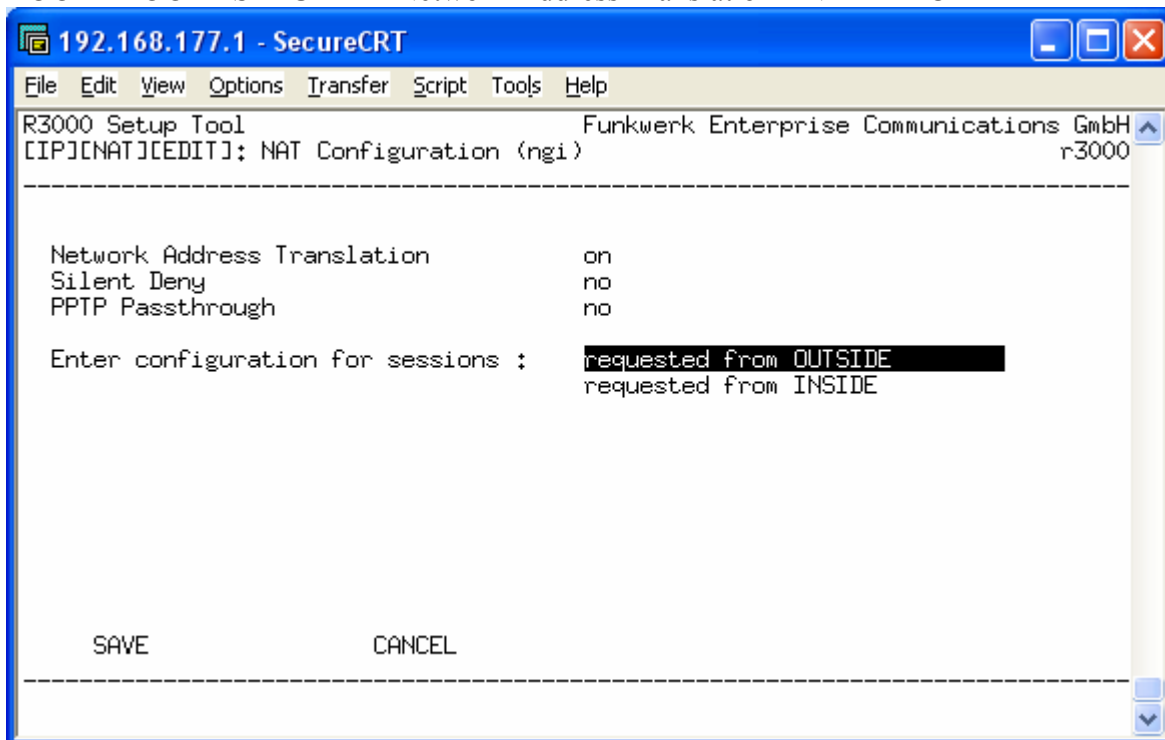
Prima di tutto si sceglie l'interfaccia sulla quale abilitare il NAT. Normalmente si tratta dell'interfaccia pubblica, quindi la WAN del router. L'abilitazione del NAT viene fatta durante la configurazione dell'interfaccia pubblica (vedi i punti precedenti).

ROOT> SETUP>IP>Network Address Translation>



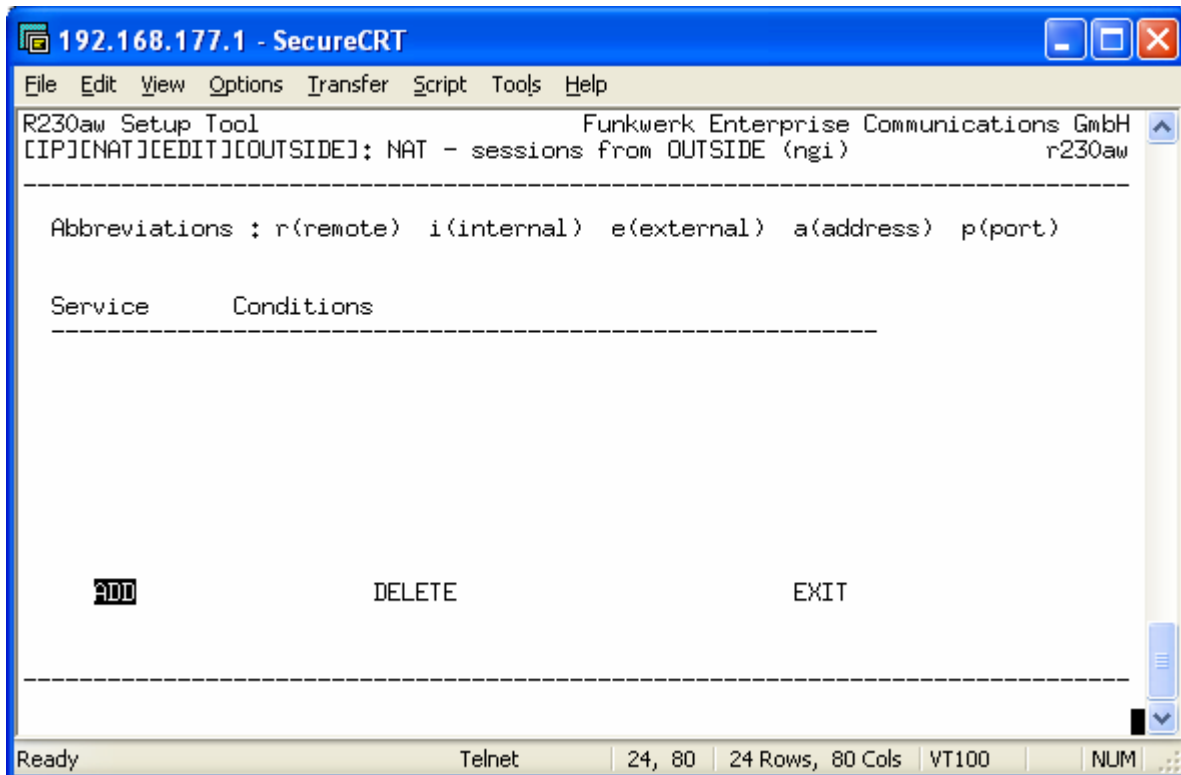
E' possibile fare NAT sia per le richieste che provengono dall'esterno (per pubblicare dei server su internet) ma anche per le richieste che provengono dall'interno della rete (per fare in modo che gli host interni si presentino su internet con un indirizzo IP pubblico specifico). Prendiamo in esame il caso più frequente, ovvero quando abbiamo degli host interni che devono essere raggiunti da remoto. ES: abbiamo un sever web, oppure un computer che deve essere gestito attraverso desktop remoto, oppure un centralino VoIP al quale dobbiamo registrare dei telefoni SIP, oppure ancora vogliamo semplicemente accedere alla configurazione del router da remoto.

ROOT> ROOT> SETUP>IP>Network Address Translation>INTERFACE>

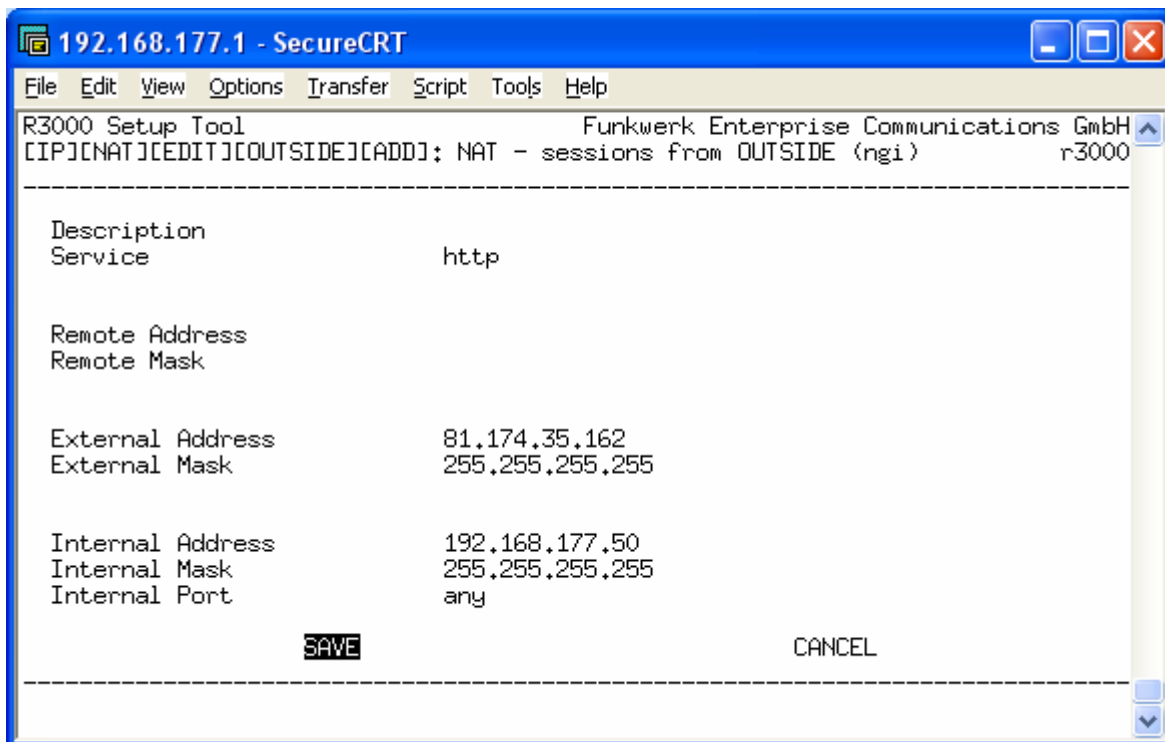


Il NAT, quando abilitato, blocca di default tutte le richieste provenienti dall'esterno (internet) verso l'intero (LAN). Dall'interno all'esterno invece è sempre tutto concesso.

Selezionando la voce “*Requested from OUTSIDE*” si visualizza l’elenco delle regole per le richieste provenienti dall’esterno.



Se è la prima volta che accediamo a questo menù troveremo vuota la tabella sopra riportata. Per creare una nuova regola occorre posizionarsi su “Add” e premere invio.



La voce *Service* indica il tipo di servizio da abilitare; alcuni sono pre-impostati, tutti gli altri si possono creare con l’opzione *User Defined* specificando anche il protocollo di comunicazione (TCP, UDP, ICMP, etc...). Ad esempio il PING non è presente nella lista dei servizi perciò bisogna definirlo come *USER DEFINED*, protocollo *ICMP*.

Remote Address serve a specificare l'indirizzo dell'host remoto abilitato ad utilizzare il servizio. Lasciando bianco questo campo non si effettua alcuna restrizione sul richiedente.

External Address rappresenta l'interfaccia esterna (pubblica) del router. Nel caso in cui abbiamo un solo indirizzo IP pubblico si può lasciare bianco questo campo, nel caso in cui si abbiano più indirizzi pubblici è possibile specificare l'indirizzo che intendiamo rendere disponibile per il servizio sopra indicato.

Internal Address è l'indirizzo IP dell'host sul quale è in esecuzione il servizio che si vuole rendere pubblico, ovvero è l'indirizzo IP dell'host interno al quale si vuole girare la richiesta.

Remote/External/Internal Mask deve essere 255.255.255.255 quando si fa riferimento ad un indirizzo IP specifico. Solo in casi particolari si utilizza una netmask differente.

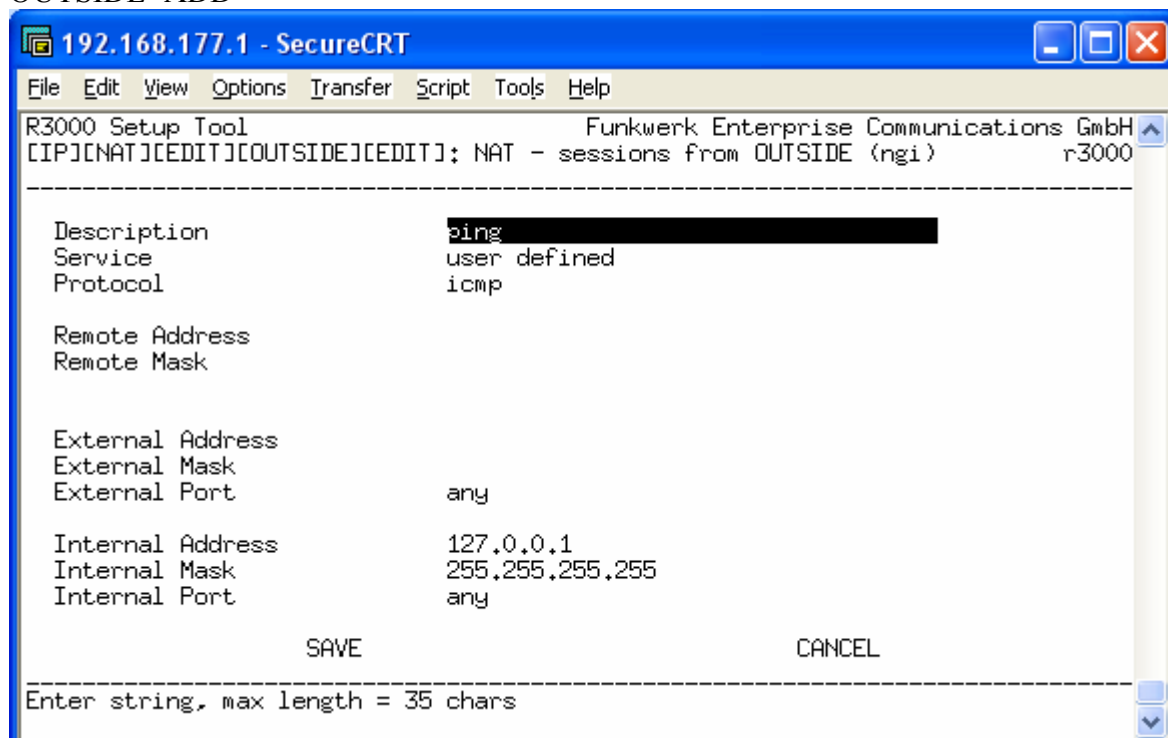
Suggerimento: le regole scritte sotto alla voce "*Requested from OUTSIDE*" vanno lette dall'alto verso il basso; il router modifica i campi "IP destination" e "Port destination" dei pacchetti provenienti dall'esterno.

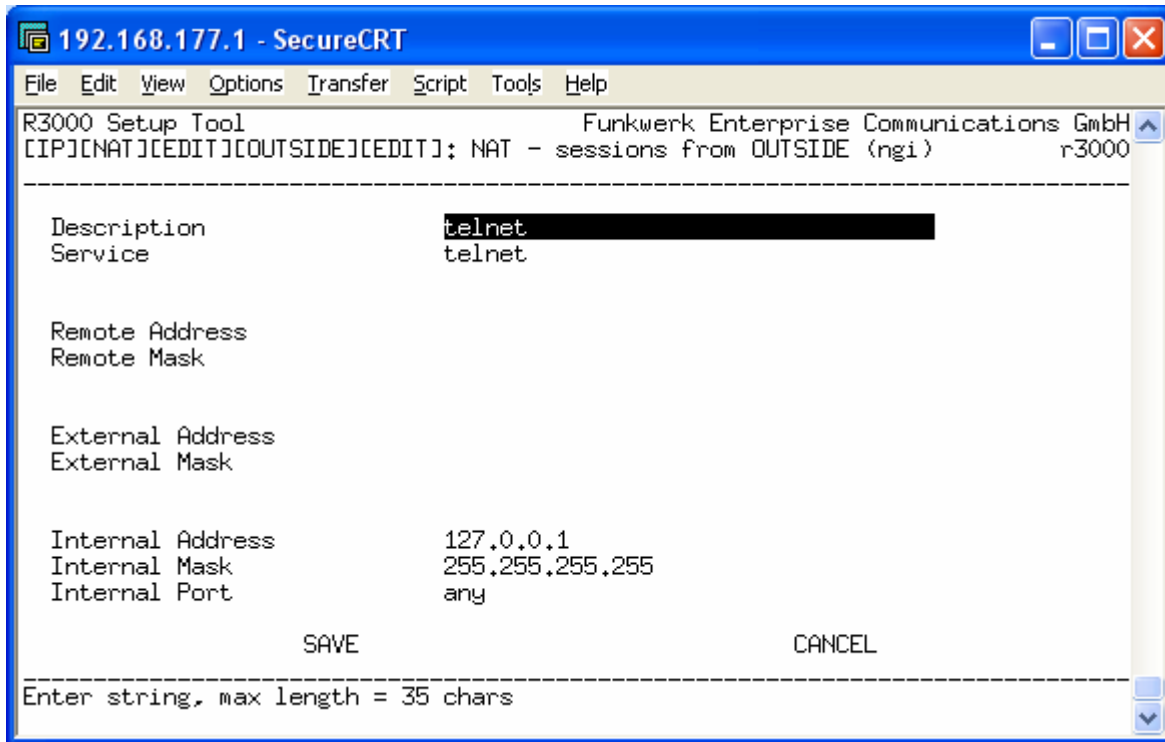
Se si vuole che sia il router a rispondere alle richieste occorre settare l'Internal Address a 127.0.0.1 (si tratta dell'interfaccia di loopback detta anche "localhost"); se invece si vuole rigirare la richiesta a un pc interno basta inserire l'indirizzo IP del pc. E' possibile inoltre specificare le porte sorgente e destinazione.

Se ho un server WEB interno e ho più indirizzi statici a disposizione posso assegnarne uno direttamente al server Web. Se invece ho solo un indirizzo pubblico possiamo assegnare al server Web un indirizzo privato e creare una regola di NAT per renderlo visibile dall'esterno.

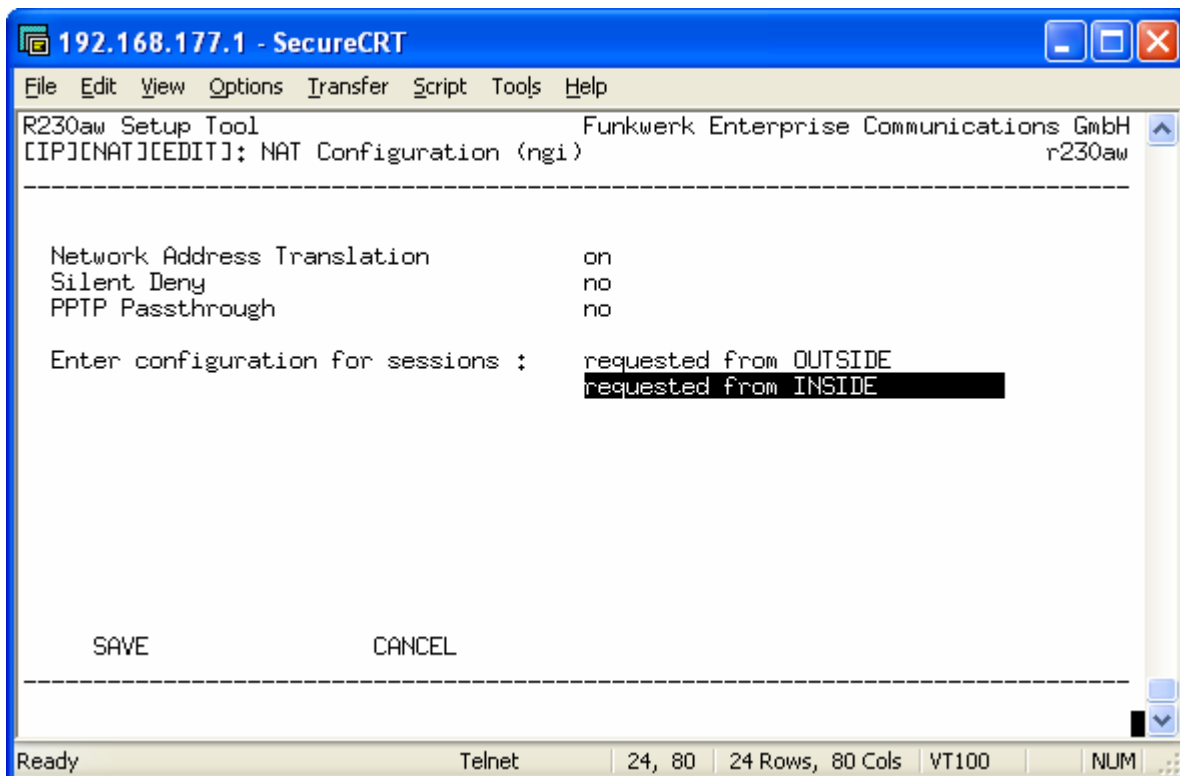
Riportiamo alcune regole di uso comune: il ping (per controllare da remoto se la connessione ADSL è attiva) e il telnet (per poter accedere alla configurazione del router da remoto). Come si nota dalle schermate che seguono le richieste sono state redirette verso l'indirizzo 127.0.0.1, ovvero verso il router stesso.

ROOT> ROOT> SETUP>IP>Network Address Translation>INTERFACE>Request from OUTSIDE>ADD>

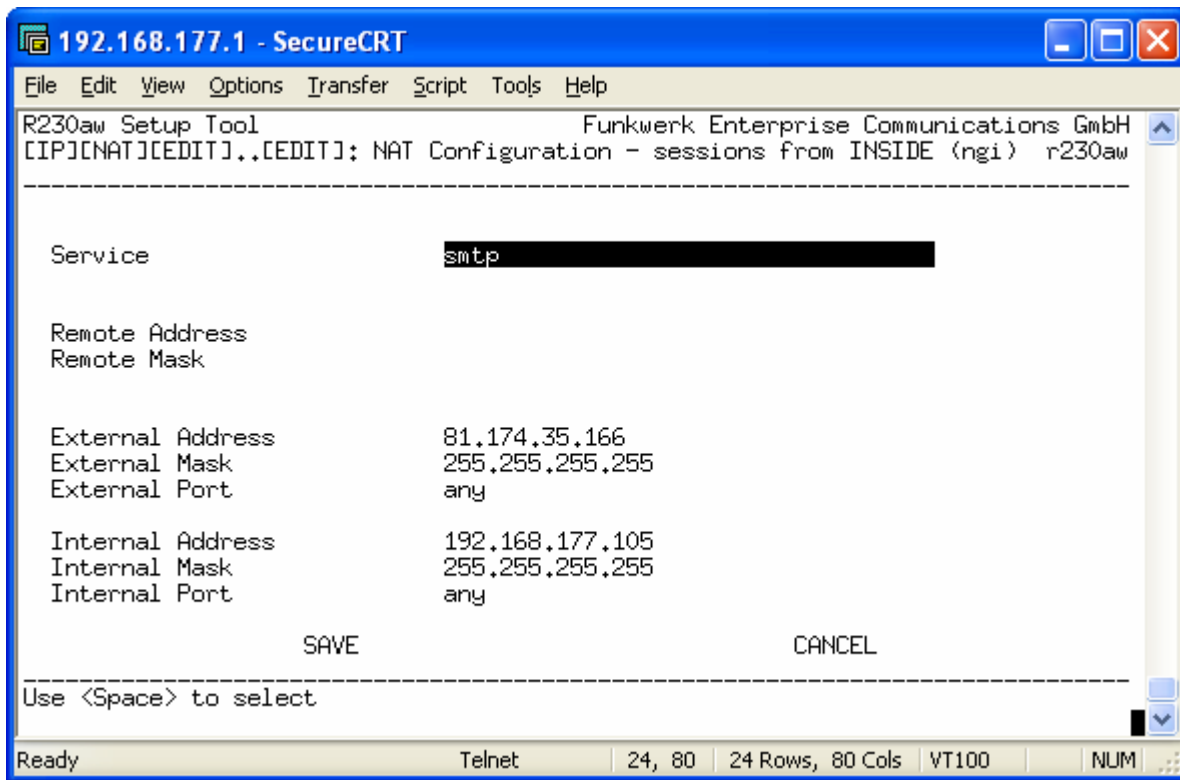




Quando invece vogliamo che un determinato host della rete privata (es, 192.168.177.105) esca utilizzando un determinato indirizzo IP pubblico (es. 81.174.35.166) dobbiamo creare una regola sotto alla voce “*Requested from INSIDE*”



Di seguito riportiamo un esempio di utilizzo; si vuole fare in modo che l’host interno 192.168.177.105 si presenti su internet utilizzando l’indirizzo 81.174.35.166 (uno degli IP aggiuntivi assegnatici dal Provider) solo nel caso in cui faccia uso del servizio SMTP (invio di posta elettronica)



Suggerimento: le regole scritte sotto alla voce “*Requested from INSIDE*” vanno lette dal basso verso l’alto; il router modifica i campi “IP source” e “Port source” dei pacchetti provenienti dall’interno della rete.

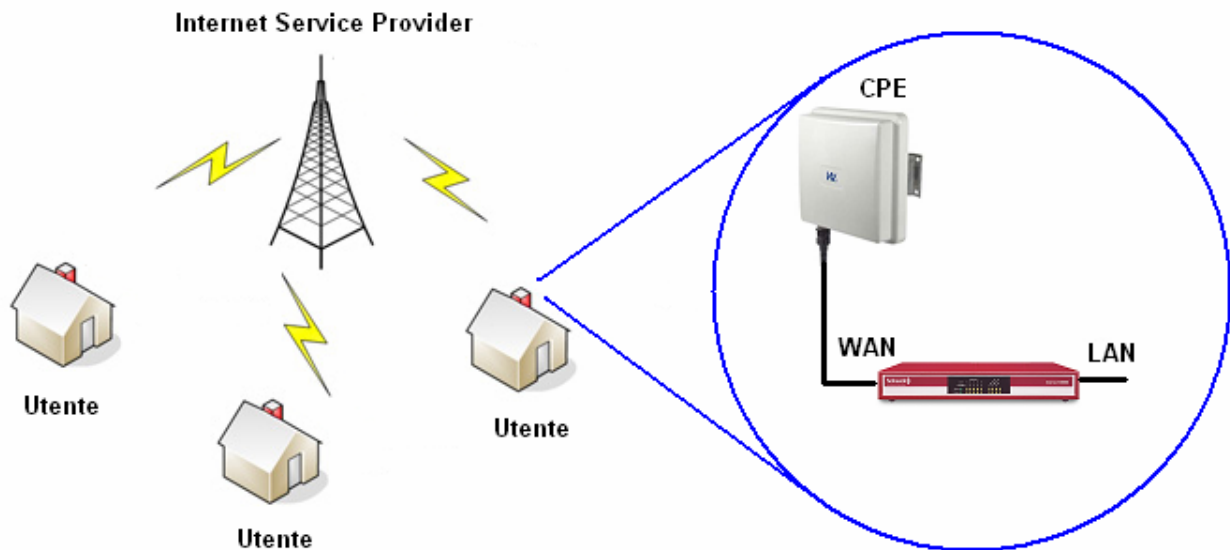
Se non specifichiamo nessuna regola sulla voce “*Requested from INSIDE*” il router farà uscire le richieste verso internet utilizzando l’indirizzo di Punto-Punto assegnato dal Provider (specificato sull’interfaccia WAN)

Collegamento Internet

ETHERNET, ISDN, ADSL, HDSL, SHDSL, UMTS

Connessione Ethernet

Capita spesso che i Service Internet Provider forniscano connessione attraverso modem ADSL o ponti radio: se non è possibile o non si intende sostituire il dispositivo fornito dall'ISP è opportuno collocare il router Bintec fra tale dispositivo e la rete interna. Questa soluzione ci permette di gestire in modo completo la connessione Internet evitando di doverci rivolgere al fornitore dei servizi ogni volta che vogliamo apportare una modifica alla configurazione della rete.



Per prima cosa dobbiamo separare una porta ethernet che verrà utilizzata come WAN (porta pubblica). Per farlo seguiamo la procedura del Port Separating precedentemente illustrata.

Si sceglie per esempio la porta numero 4 e si cambia il nome dell'interfaccia (en1-1)

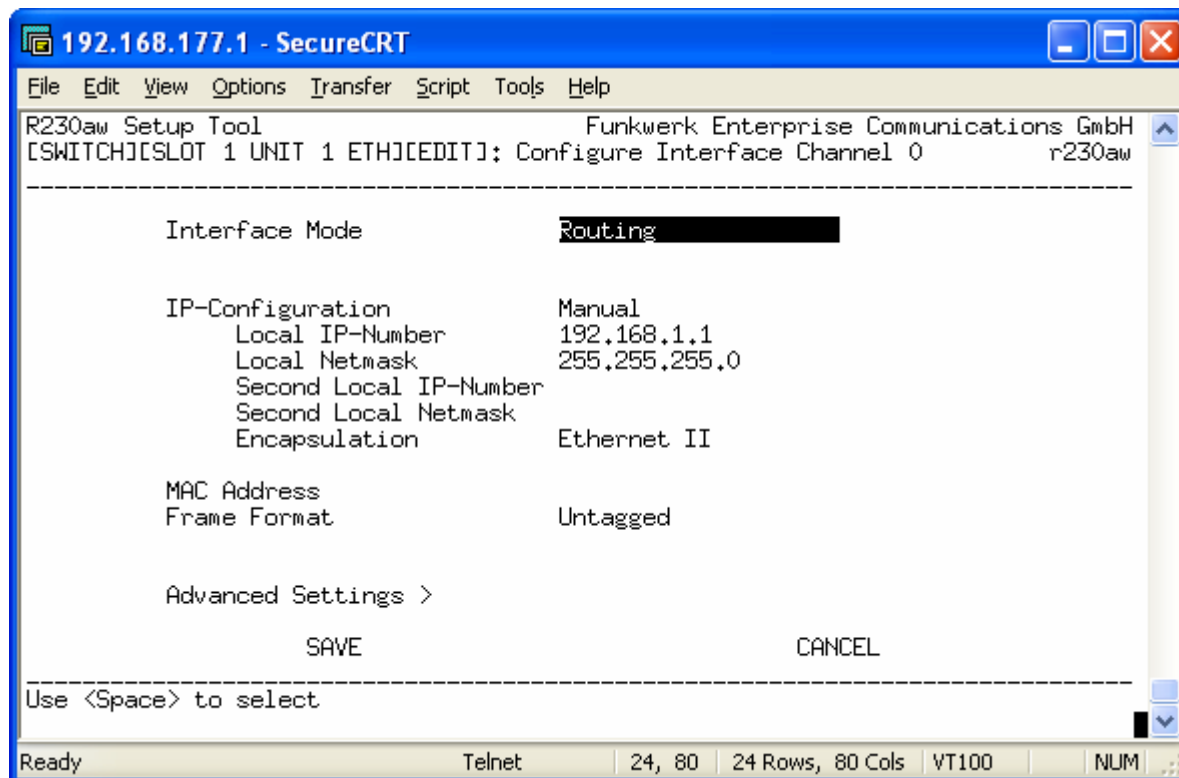
```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool                               Funkwerk Enterprise Communications GmbH
[SWITCH][ASSIGN]: Switch Interface Assignment      r230aw

-----
Switch Port   Assigned Interface   Switch Port Mode
Port 1        en1-0                full autonegotiation
Port 2        en1-0                full autonegotiation
Port 3        en1-0                full autonegotiation
Port 4        en1-1                full autonegotiation

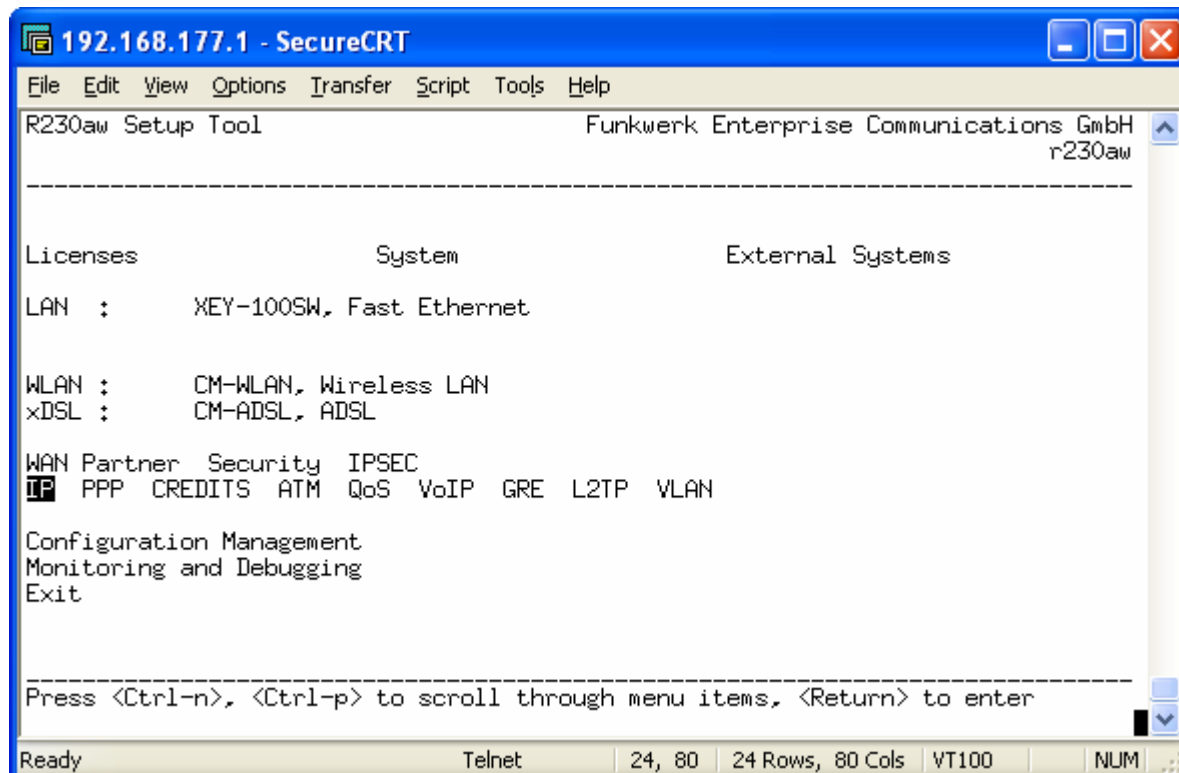
SAVE                                CANCEL
-----
Use <Space> to select

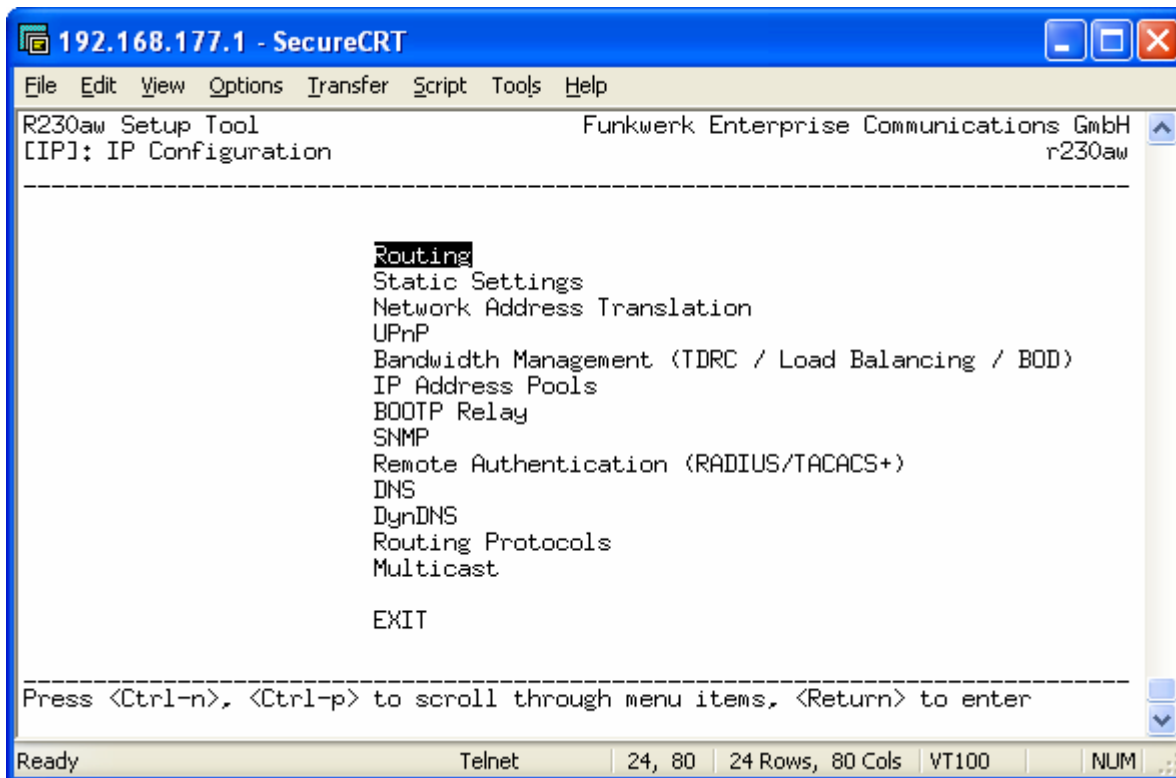
Ready                               Telnet    24, 80   24 Rows, 80 Cols  VT100    NUM
```

Si assegna all'interfaccia un indirizzo compatibile con il modem ADSL o il ponte radio al quale dobbiamo collegarlo. Ovviamente LAN e WAN del Bintec dovranno appartenere a classi di indirizzamento differente! (Es. LAN = 192.168.0.254 e WAN = 192.168.1.1)

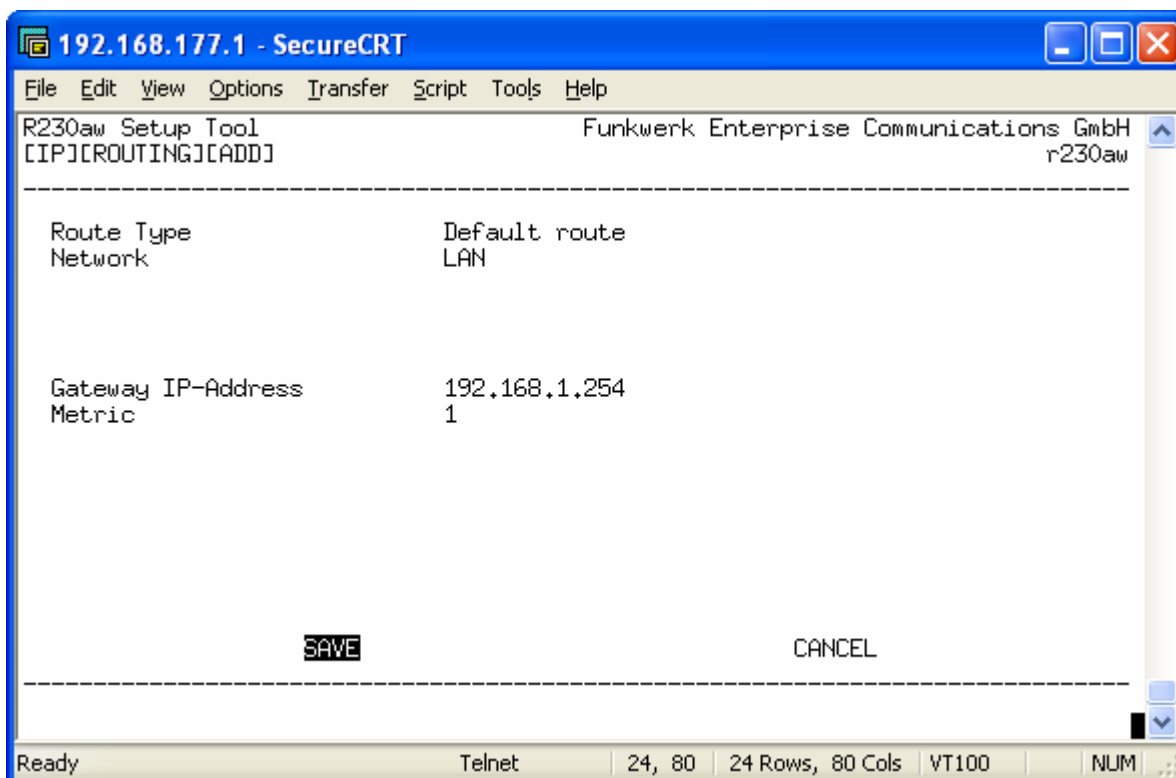


A questo punto non rimane che creare una regola nella tabella di routing per specificare qual è il gateway di default per tutte le richieste Internet. Il default gateway è rappresentato dal modem ADSL o del ponte radio al quale abbiamo collegato il router Bintec.





Si entra dentro alla tabella di routing e si aggiunge una regola selezionando "add".



Non rimane che abilitare il NAT sull'interfaccia WAN del Bintec (en1-1 in questo caso).


```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool                               Funkwerk Enterprise Communications GmbH
[IP]: IP Configuration                           r230aw

-----

Routing
Static Settings
Network Address Translation
UPnP
Bandwidth Management (TDRC / Load Balancing / BOD)
IP Address Pools
BOOTP Relay
SNMP
Remote Authentication (RADIUS/TACACS+)
DNS
DynDNS
Routing Protocols
Multicast

EXIT

-----
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter

Ready                               Telnet                               24, 80                               24 Rows, 80 Cols                               VT100                               NUM
```

```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool                               Funkwerk Enterprise Communications GmbH
[IP][NAT]: NAT Configuration                     r230aw

-----

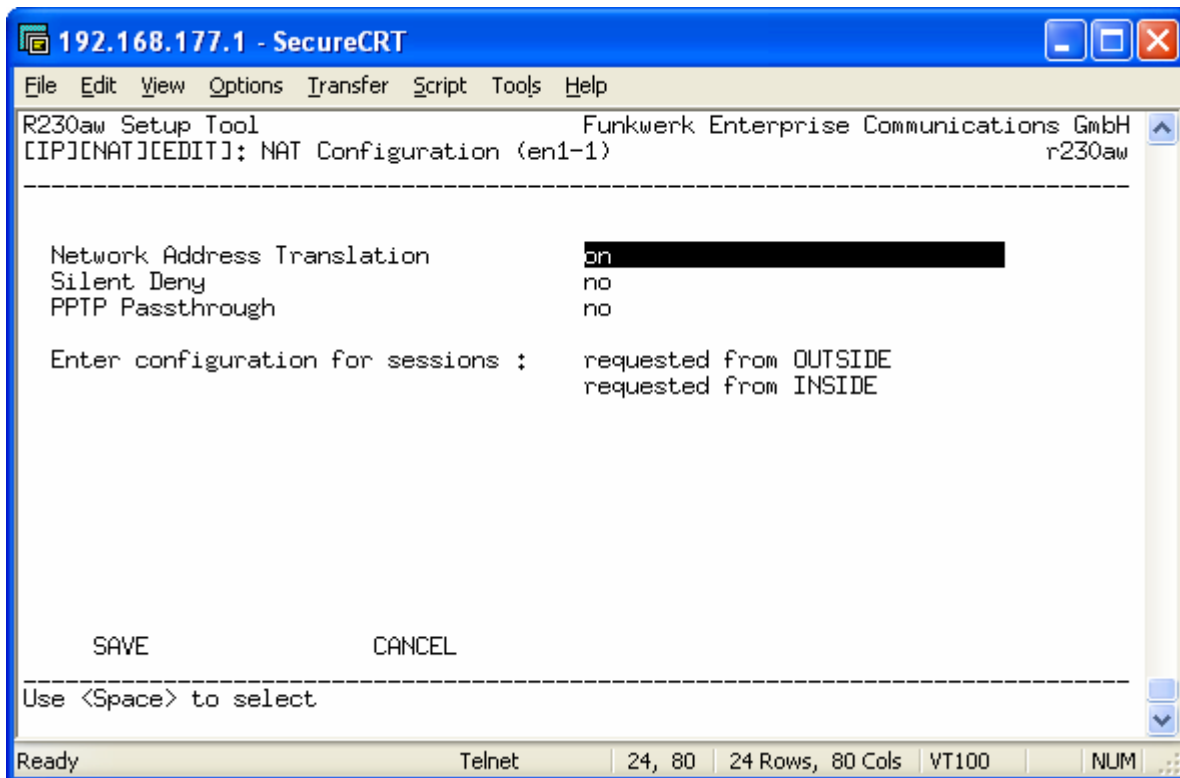
Select IP Interface to be configured for NAT

Name                Nat      Static mappings      Static mappings
                   from Outside      from Inside
en1-0                off      0                     0
en1-0-snap           off      0                     0
en1-1                off      0                     0
en1-1-snap           off      0                     0
ethoa50-0            off      0                     0
ethoa50-0-snap       off      0                     0
ngi                  on       21                    2
verso_rizzuti        off      0                     0

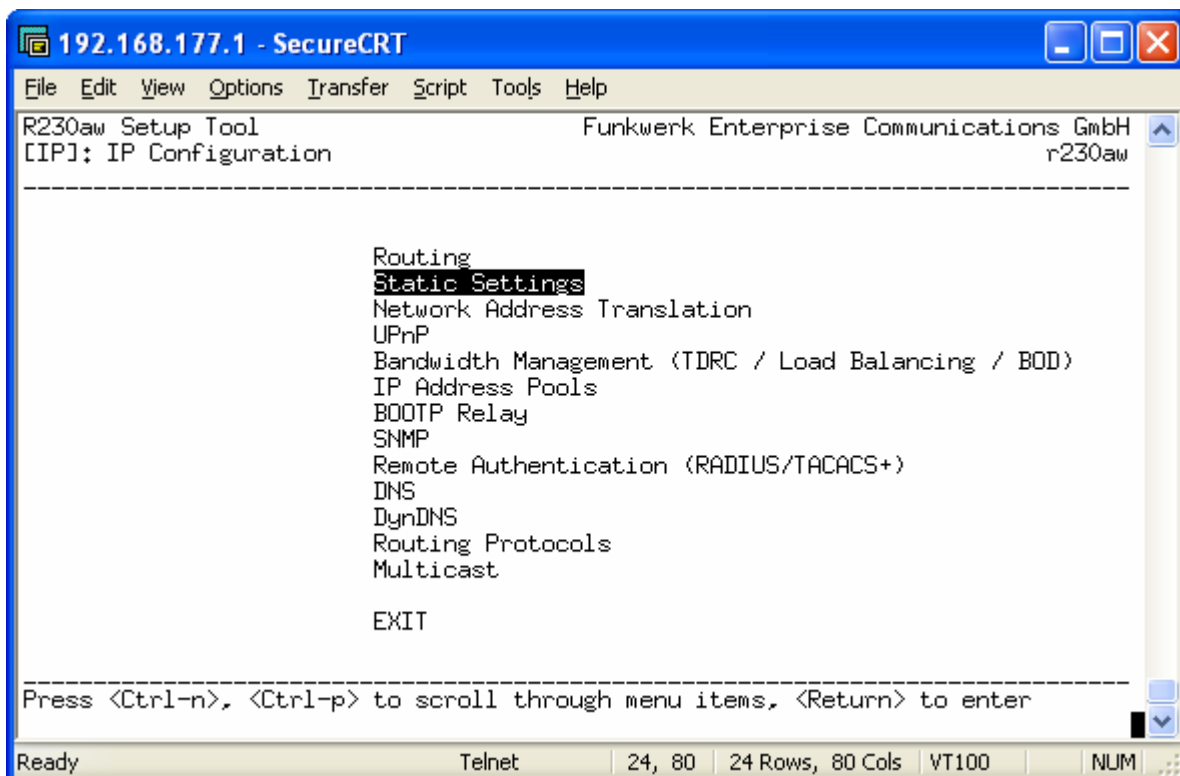
EXIT

-----
Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to select/edit

Ready                               Telnet                               24, 80                               24 Rows, 80 Cols                               VT100                               NUM
```



A questo punto la configurazione è completata. E' consigliabile inserire gli indirizzi dei server DNS (primario e secondario) sul router Bintec. Si entra nel menù *IP* → *Static Settings*



192.168.177.1 - SecureCRT

File Edit View Options Transfer Script Tools Help

R230aw Setup Tool Funkwerk Enterprise Communications GmbH
[IP][STATIC]: IP Static Settings r230aw

Domain Name	nextmedia.local
Primary Domain Name Server	151.99.125.3
Secondary Domain Name Server	151.99.125.1
Primary WINS	192.168.177.105
Secondary WINS	192.168.177.106
Remote CAPI Server TCP port	2662
Remote TRACE Server TCP port	7000
RIP UDP port	520

Unique Source IP Address	
HTTP TCP port	80

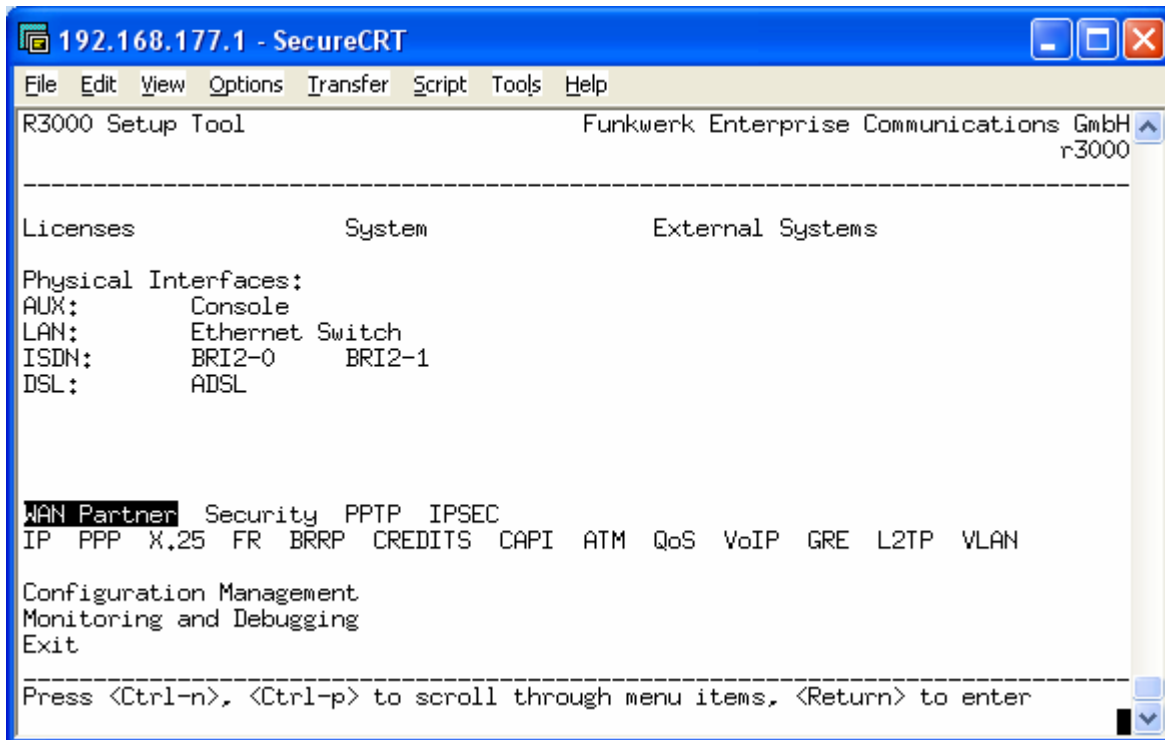
SAVE CANCEL

Enter IP address (a.b.c.d or resolvable hostname)

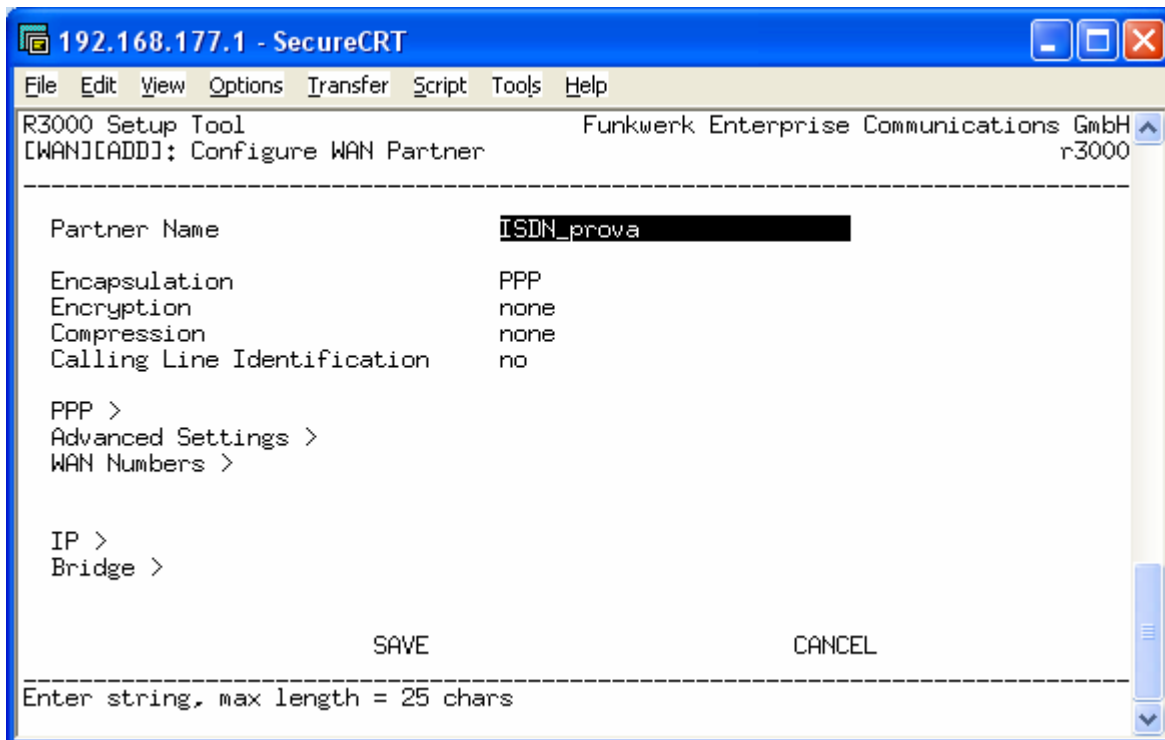
Ready Telnet 6, 43 24 Rows, 80 Cols VT100 NUM

Connessione ISDN

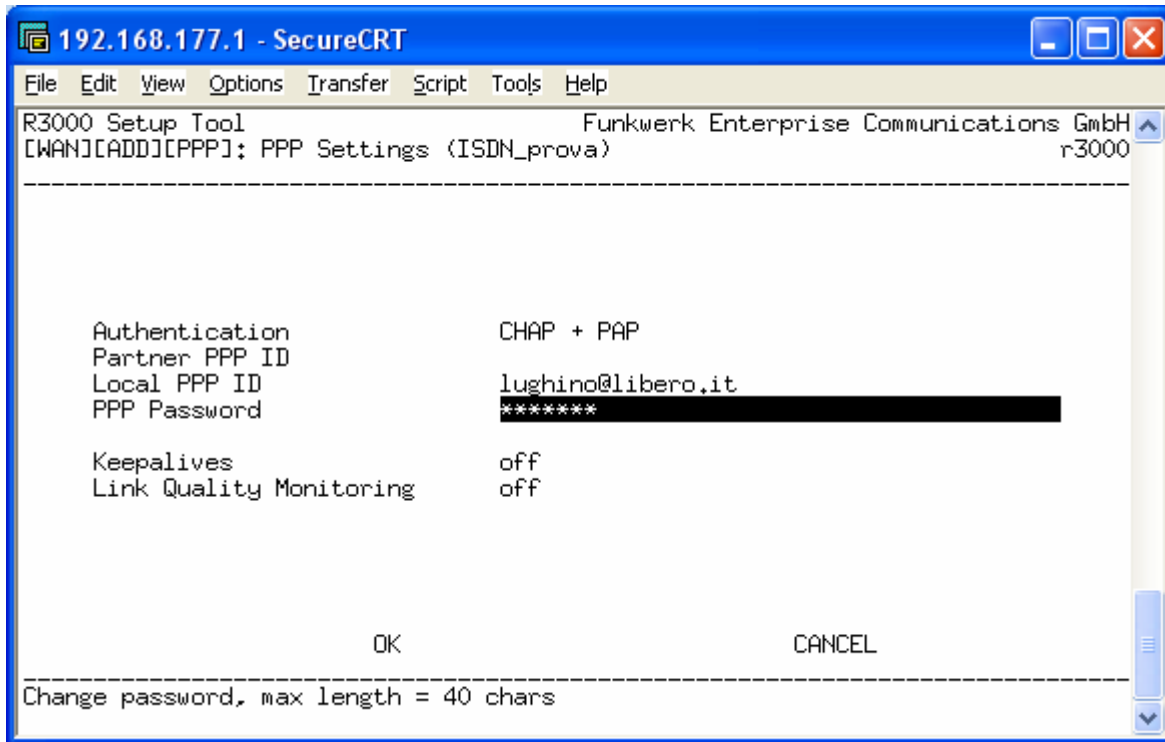
Per prima cosa accediamo al menù di Setup del router.



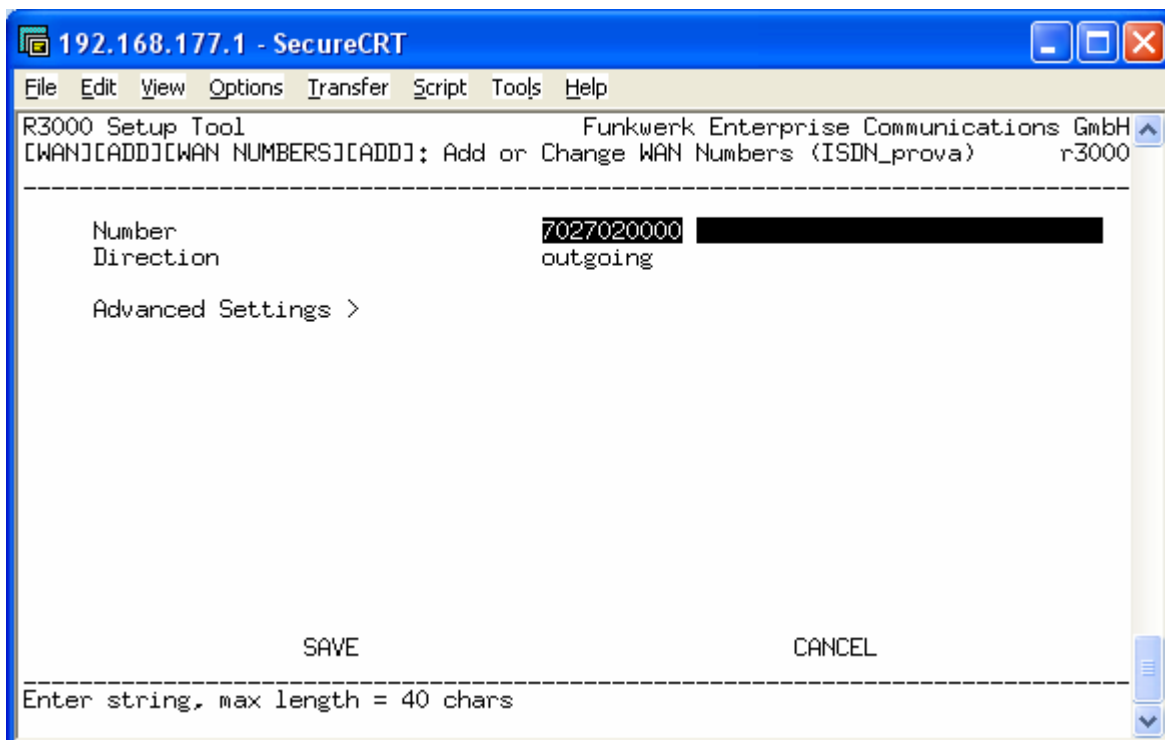
Nella sezione WAN Partner andiamo ad aggiungere una voce



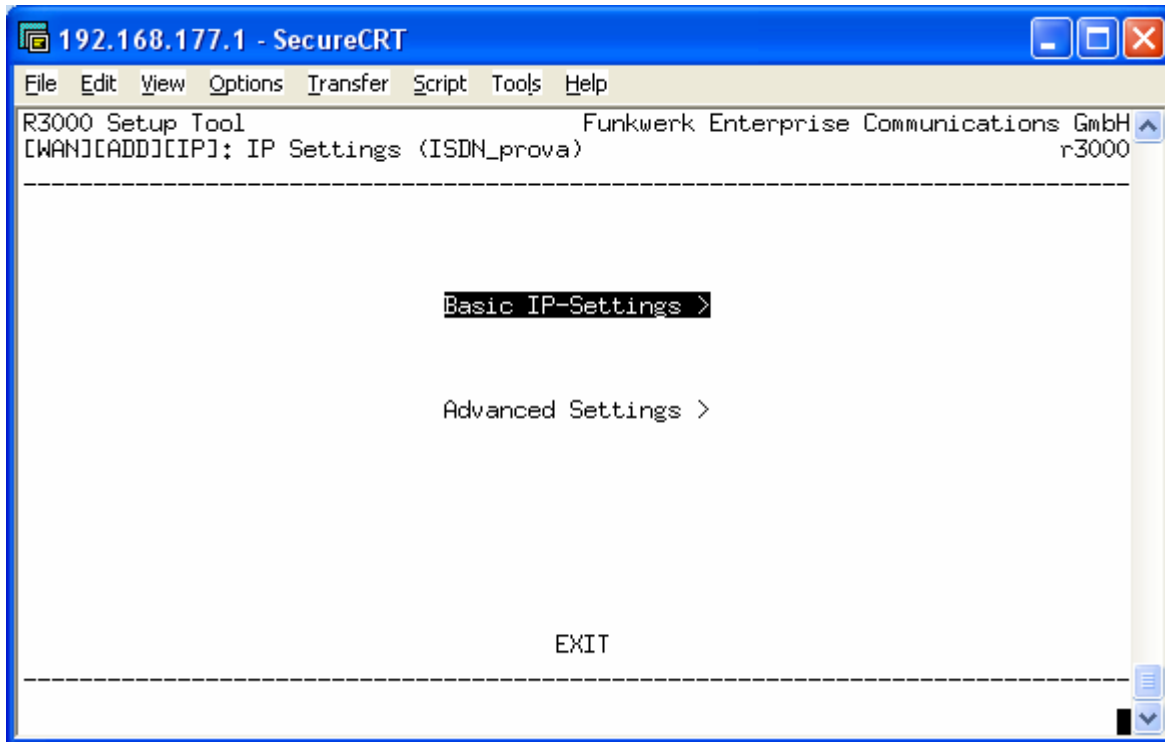
Nella sezione PPP andiamo ad inserire USER (*Local PPP ID*) e PASSWORD (*PPP Password*) della connessione internet. La modalità CHAP + PAP è quella utilizzata dalla maggior parte dei Provider italiani.



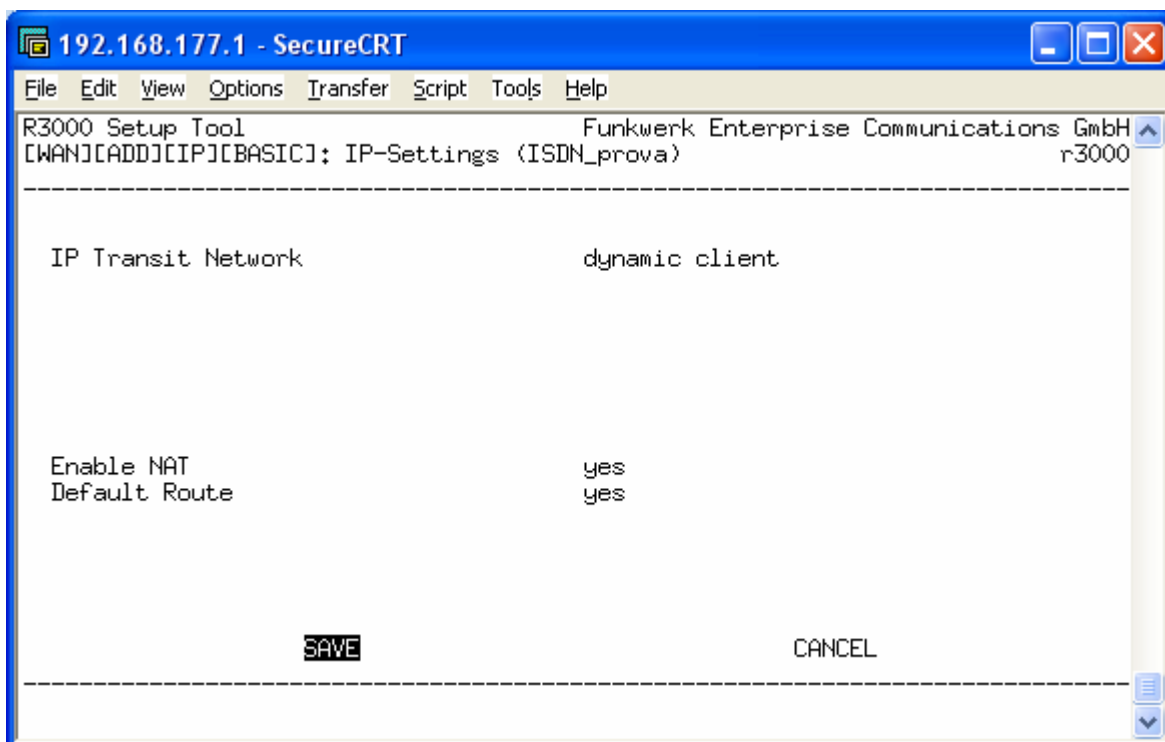
Nella sezione WAN Numbers aggiungiamo una voce ed andiamo ad inserire il numero di telefono del provider.



Nella sezione IP andiamo ad inserire una regola in Basic IP-Settings



Impostiamo “*dynamic client*” ed abilitiamo sia NAT che Default Route. Questo serve per fare in modo che il provider ci assegni un indirizzo IP e per abilitare automaticamente il NAT e la default route (indispensabili per navigare).



Ora non resta che attendere il collegamento. Per verificare che la connessione sia UP andiamo nel menù di Setup e scegliamo la voce Monitoring and Debugging.

```

192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool Funkwerk Enterprise Communications GmbH
[MONITOR]: Monitoring and Debugging r230aw

-----

ISDN Monitor          ATM/OAM
ISDN Credits          ADSL
xDSL Credits

Interfaces
Messages
Email Alert
TCP/IP                IP QoS
IPSec                 SSHD

EXIT

-----

Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM

```

```

192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool Funkwerk Enterprise Communications GmbH
[MONITOR][INTERFACE]: Interface Monitoring r230aw

-----

Interface Name      en1-0
Operational Status up
                    ngi
                    up

                    total      per second      total      per second

Received Packets    1005087      3      774807      1
Received Octets     716910750   192    459329586  102
Received Errors     0

Transmit Packets    875351      2      901018      0
Transmit Octets     491948540  231    670754345  0
Transmit Errors     0

Active Connections  N/A          1
Duration            N/A          50253

EXIT                EXTENDED    EXTENDED

-----

Use <Space> to select

Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM

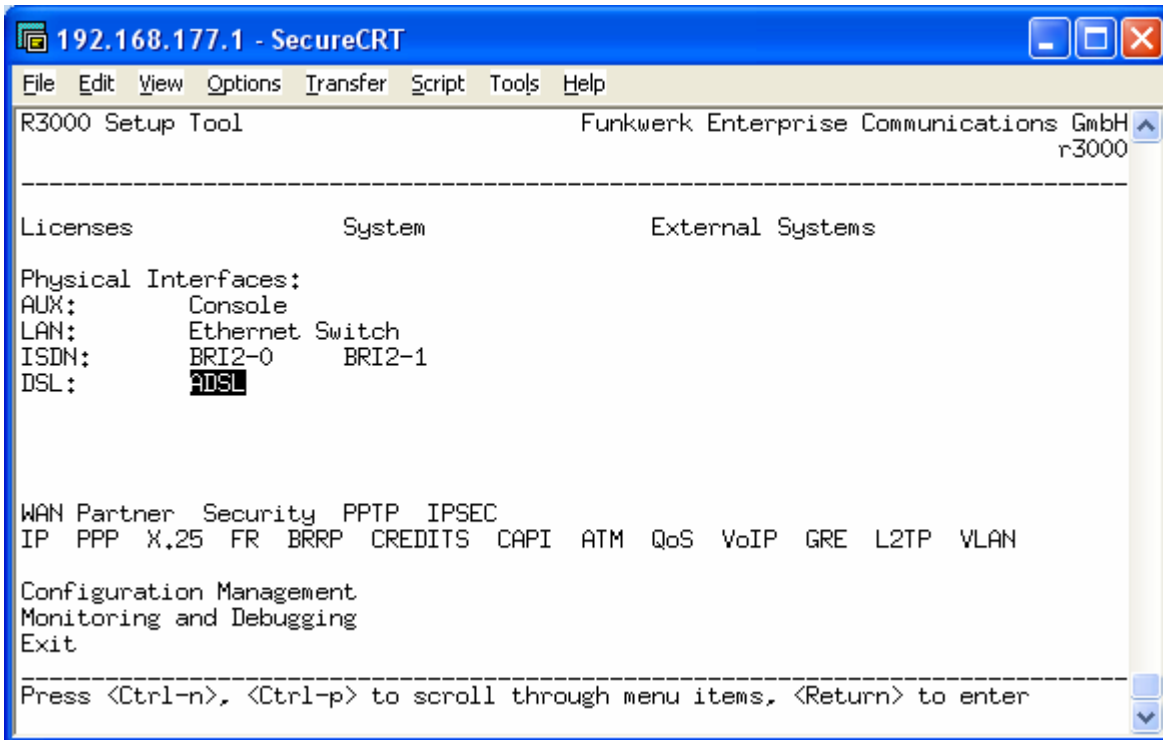
```

Connessione ADSL

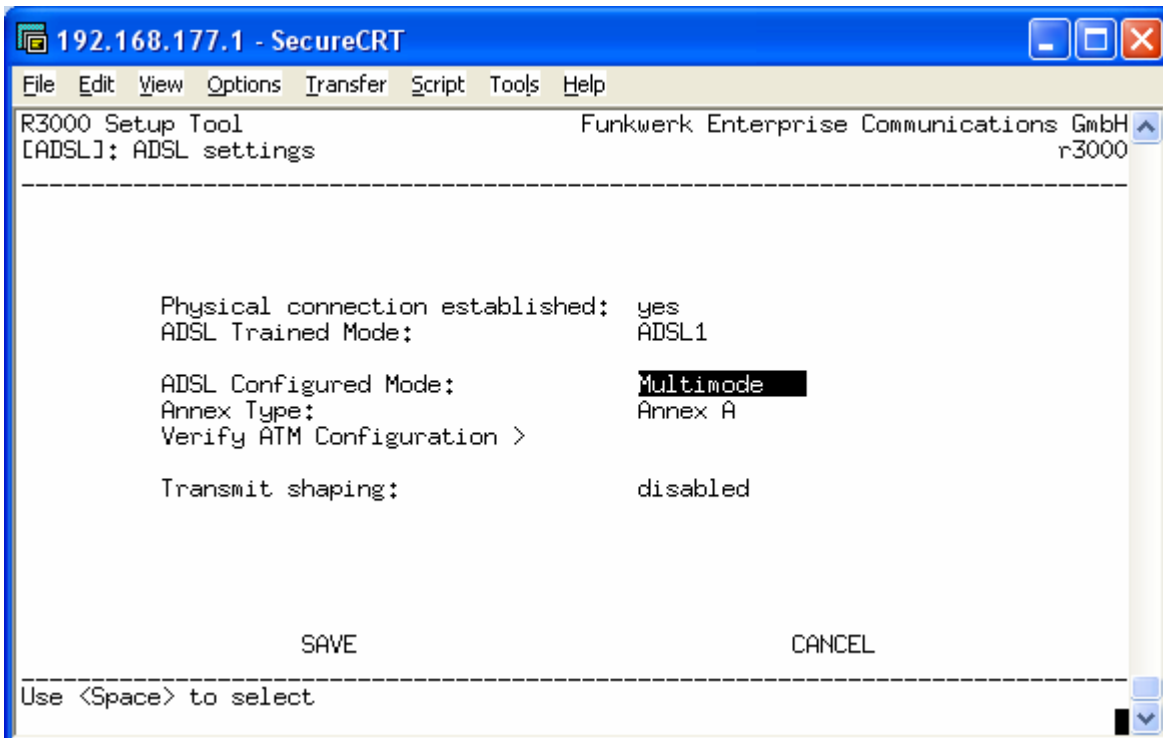
I router R230a(w), R232a(w) e R3000(w) hanno un modem ADSL integrato che supporta le seguenti tipologie di connessione: ADSL, ADSL2 e ADSL2+

Andare in **xDSL** e verificare che "*Physical Connection*" sia "yes" (significa che il doppino è collegato e c'è la portante della linea ADSL).

ROOT> SETUP>



ROOT> SETUP>xDSL>



E' consigliabile lasciare la modalità di connessione "Multimode" affinché venga concordata la tipologia migliore in base alla qualità della linea.

Suggerimento:

In Italia si usano generalmente due tipi di connessione:

PPPoA: prevede l'autenticazione tramite User Name e Password. A seguito di questa autenticazione il Provider può assegnarci un indirizzo IP statico o dinamico (in entrambe in casi la configurazione è esattamente la stessa). Dopo aver configurato la parte ATM è indispensabile configurare anche un WAN Partner.

RPoA: altrimenti detta **IPoA** o **RFC1483** non prevede autenticazione ed è legata al doppino fisico con il quale tentiamo di connetterci. L'indirizzo IP assegnato dal Provider può essere statico o dinamico ma spesso viene assegnato anche un pool di indirizzi aggiuntivi. Questa tipologia di collegamento non prevede la configurazione di un WAN Partner.

Quando si procede alla configurazione di una linea ADSL è importante capire a quale delle due tipologie sopra indicate appartiene. In linea generale la regola è questa:

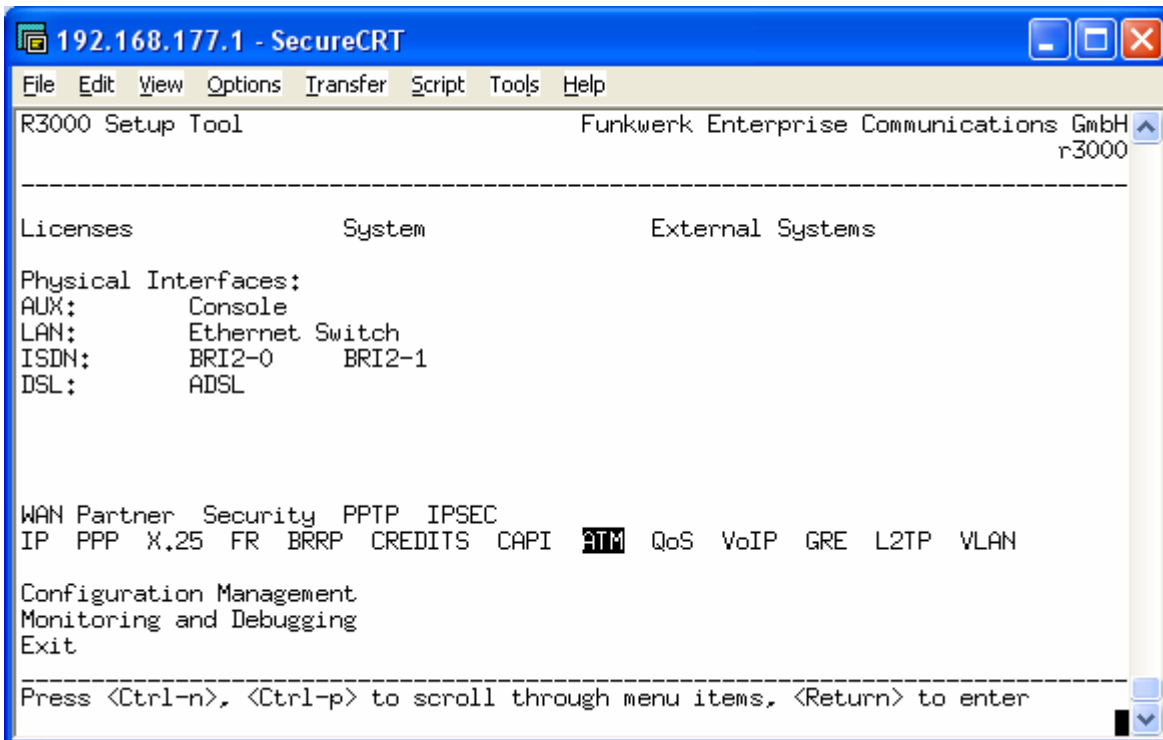
Il Provider mi ha fornito user name e password? Se SI' allora è una **PPPoA**, se NO vai al punto 2
E' una linea Telecom Alice Business? Se SI' allora è una **PPPoA** (user: *aliceadsl*, password: *aliceadsl*), se NO vai al punto 3

In tutto gli altri casi si tratta di una RPoA: nel contratto dovrebbe essere specificato un indirizzo IP di Default Gateway ed eventualmente un pool di indirizzi aggiuntivi. Quasi tutte le linee Business (ad eccezione di Alice Business) appartengono a questa tipologia.

Caso PPPoA:

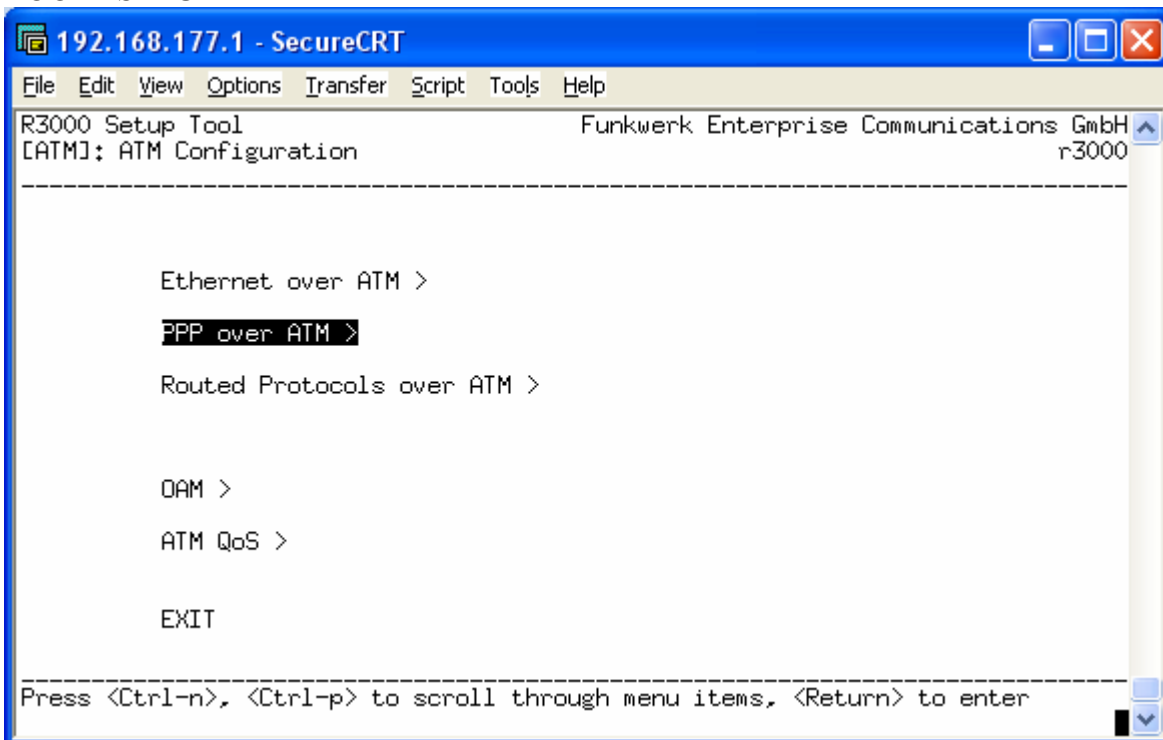
Dal menù Setup si va sul menù **ATM**: in questo sottomenù è possibile configurare la parte fisica (livello 1 - Physical) dell'ADSL.

ROOT> SETUP>

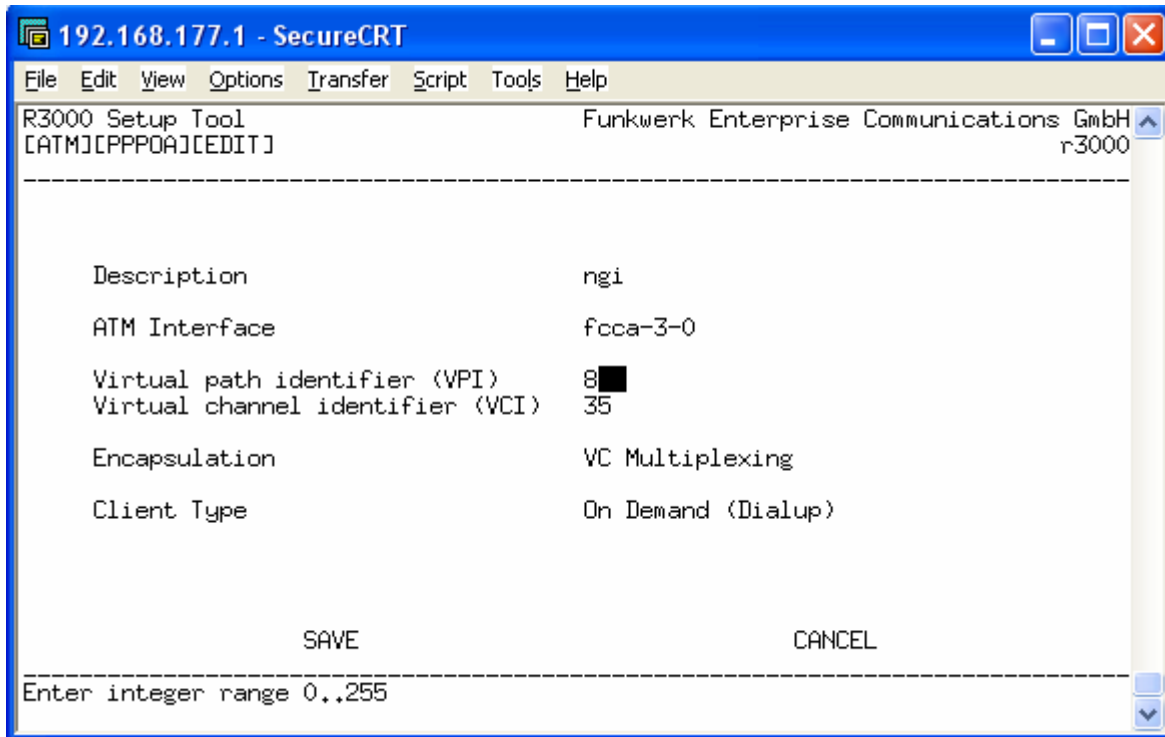


Entrando nel menù PPP over ATM è possibile aggiungere una connessione. I parametri per la configurazione vengono forniti dal provider e si trovano scritti sul contratto.

ROOT> SETUP>ATM>

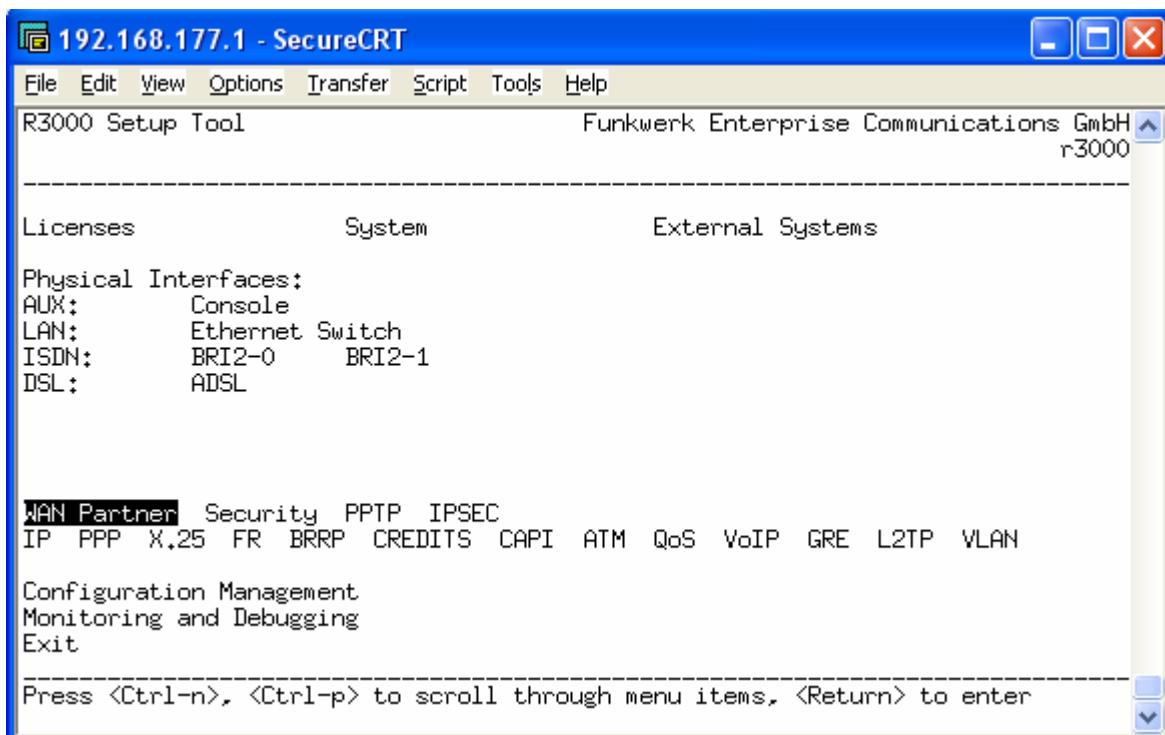


ROOT> SETUP>ATM>PPPoA>ADD>

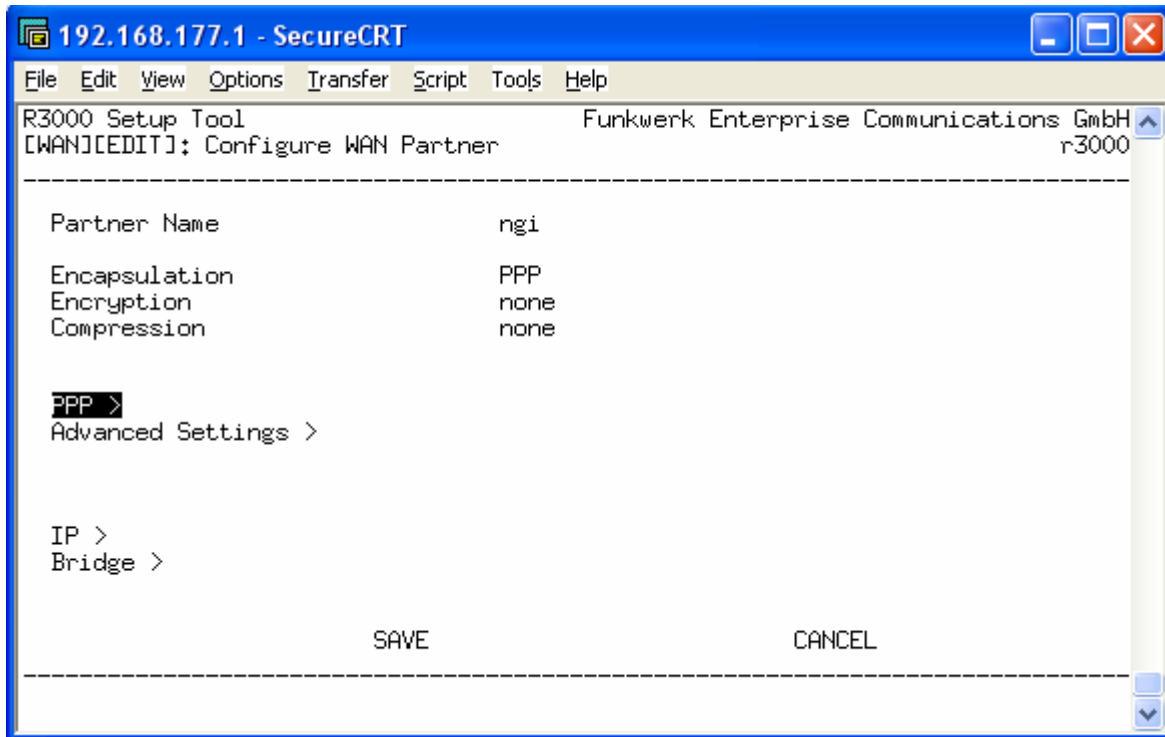


Il campo “Description” non è importante, serve solo per dare un nome all’interfaccia ADSL. VPI e VCI sono sempre 8 e 35 rispettivamente. “Client Type” è sempre "on demand (Dialup)".

Tornando alla schermata iniziale si accede al menù **WAN Partner**. Ogni volta che si configura un’ADSL di tipo PPPoA è necessario aggiungere una voce sotto a questo menù.

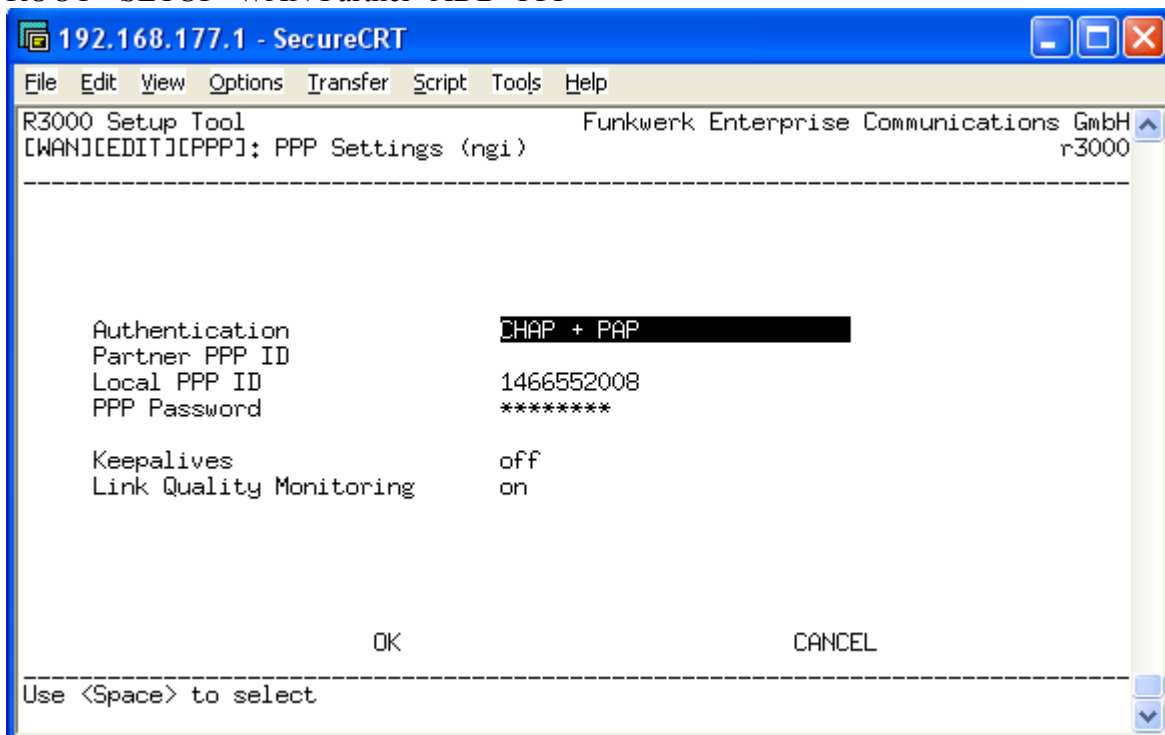


ROOT> SETUP>WAN Partner>ADD>

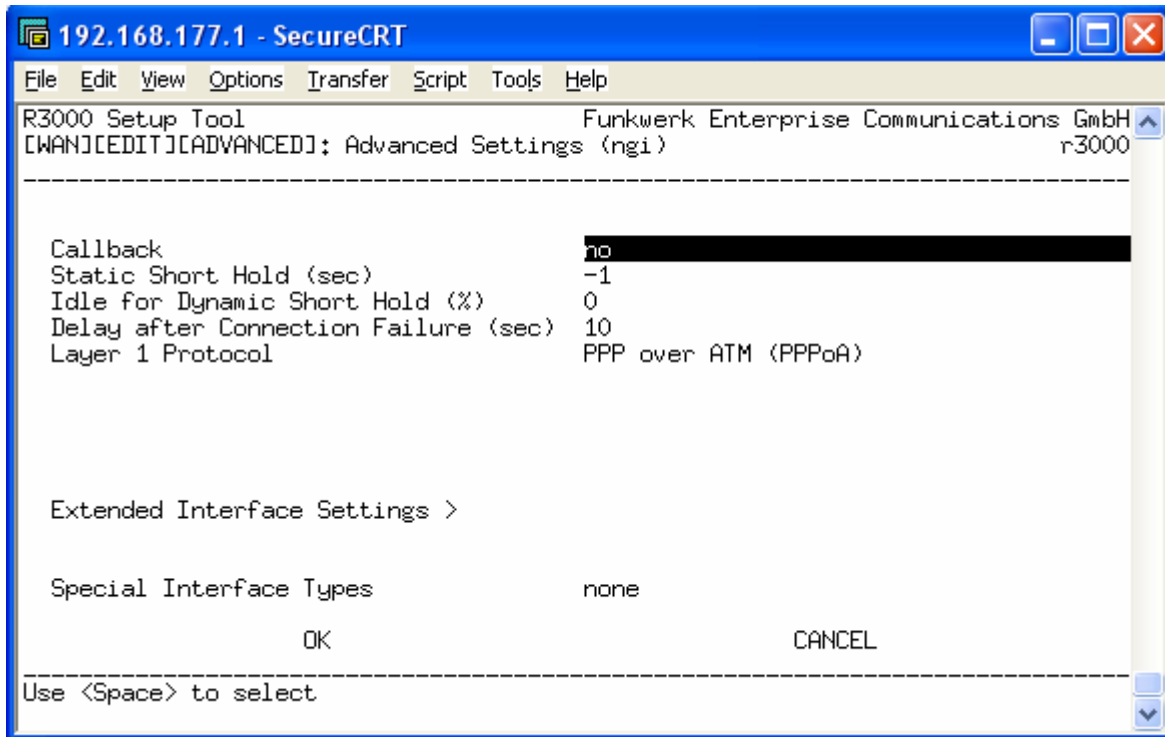


Dal menù PPP si impostano i dati relativi all'account (user e password) e il protocollo di autenticazione

ROOT> SETUP>WAN Partner>ADD>PPP>



Dal menu Advanced Settings invece si imposta il protocollo di livello 2 (data link)
 In questo caso dovremo specificare PPPoA (Point to Point Protocol over ATM).
 ROOT> SETUP>WAN Partner>ADD>Advanced Settings>



Callback: indica se si vuole che il provider o il server ci richiami (normalmente non utilizzato)

Static Short Hold: impostato a -1 indica che la connessione è sempre attiva; diversamente indica il tempo di inattività dell'ADSL prima che venga disconnessa.

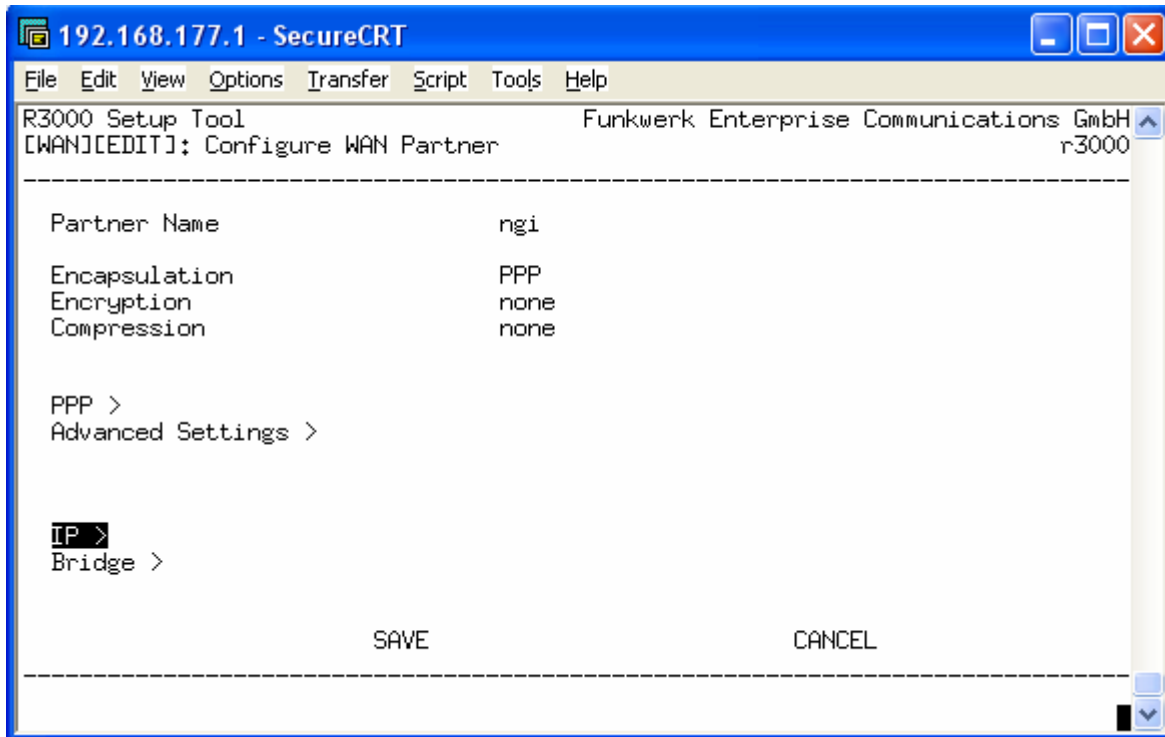
Idle for Dynamic Short Hold: indica un tempo dinamico di inattività in base alla durata della connessione. Per esempio se la connessione è attiva da 60 minuti e il parametro è impostato a 10% significa che il router effettuerà la disconnessione dopo 6 minuti di inattività.

Delay after Connection Failure: indica il tempo di attesa prima di un nuovo tentativo di connessione

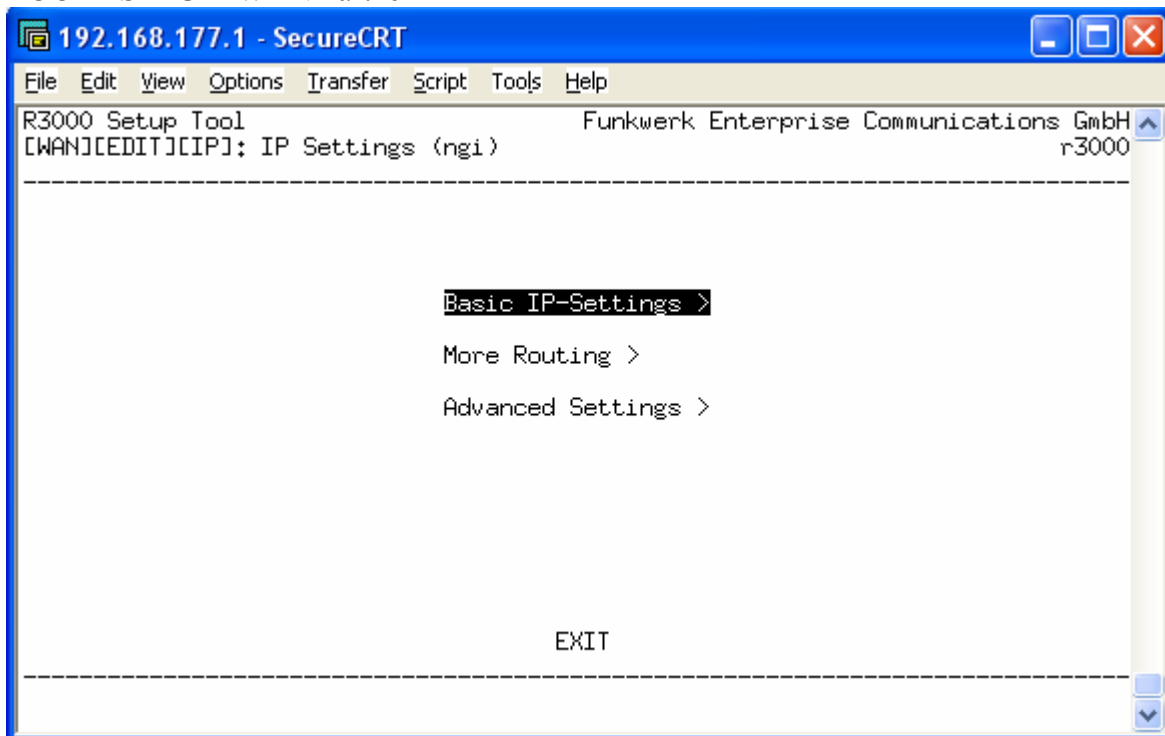
Layer 1 Protocol: indichiamo il tipo di ADSL precedentemente impostato nella sezione ATM. In sostanza il protocollo PPP (livello 2) si appoggia al protocollo ATM (livello 1)

Tornando al menù precedente andiamo nella sezione IP.

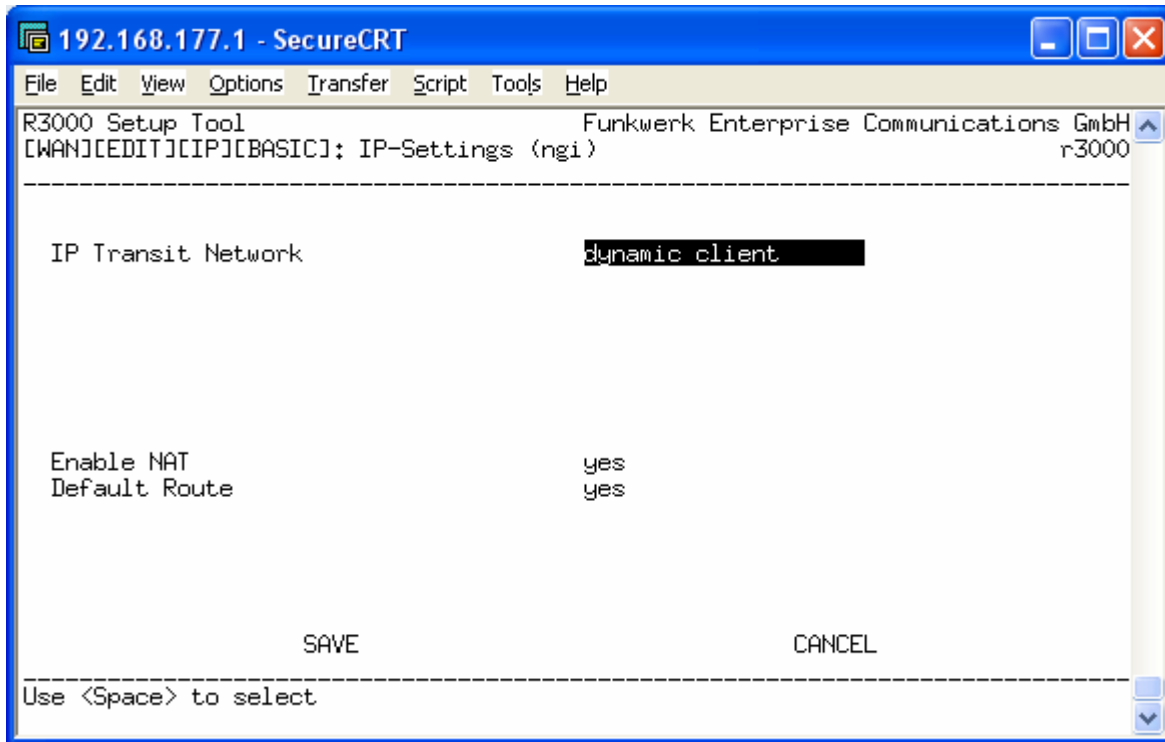
```
ROOT> SETUP>WAN Partner>ADD>
```



ROOT> SETUP>WAN Partner>ADD>IP>



ROOT>SETUP> WAN Partner>ADD>IP>BASIC IP-Settings>

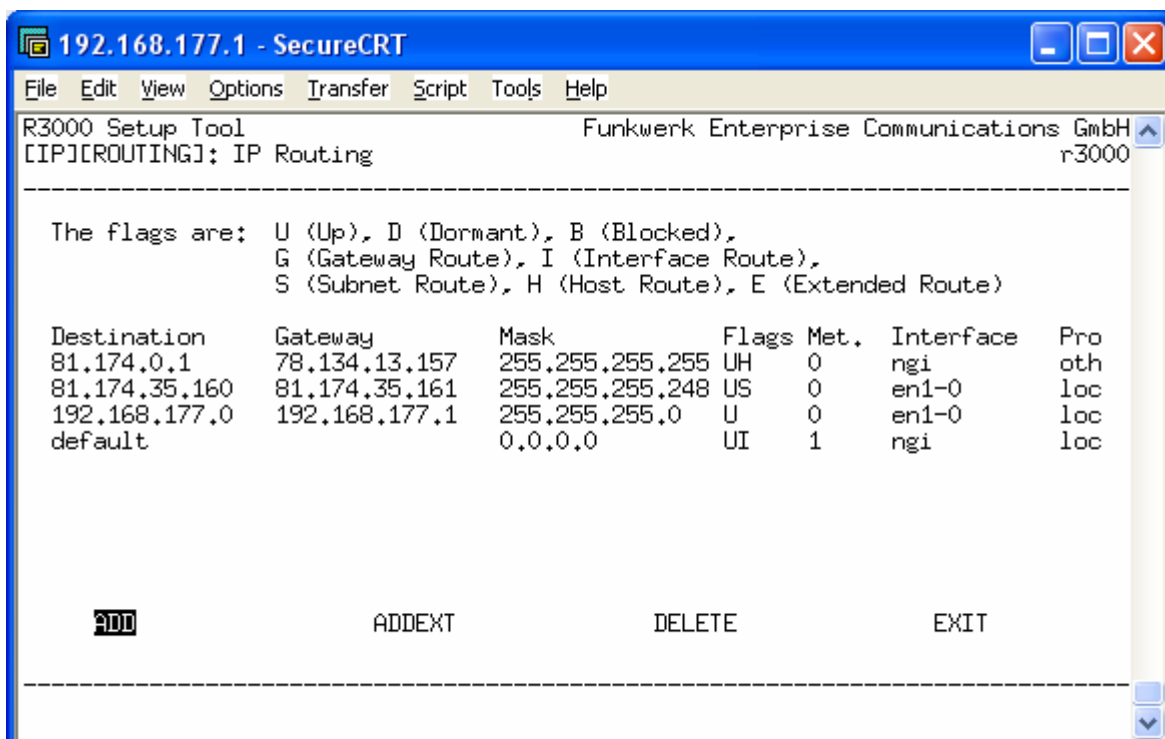


IP Transit Network: specifica il fatto che il nostro router è un client dinamico dunque riceverà un nuovo indirizzo dal provider ogni volta che tenterà di connettersi. In alcuni casi l'indirizzo assegnato dal Provider può essere statico.

Enable NAT: serve per abilitare il NAT sull'interfaccia WAN. Questa opzione ha effetto nella sezione ROOT>SETUP>IP>Network Address Translation nella quale è possibile impostare le regole.

Default Route: permette di aggiungere una entry nella tabella di routing per raggiungere tutti gli indirizzi che non rientrano nelle regole precedenti (es. tutte le destinazioni verso internet) cioè la destinazione di DEFAULT.

La tabella di routine apparirà circa così:



La prima riga mostra la connessione punto-punto (gateway) con il provider; in “destination” c’è l’indirizzo del provider stesso, in Gateway c’è l’indirizzo pubblico assegnato al router; questa riga è scritta automaticamente dal router quando si connette ad Internet. Nel caso di IP dinamico questo indirizzo cambia ad ogni riconnessione mentre nel caso di indirizzo statico è sempre lo stesso. La seconda riga è un indirizzo pubblico aggiuntivo (comprato dal Provider) ed è stato impostato come secondo indirizzo (fisico) della LAN.

La terza riga è stata scritta quando abbiamo assegnato all’interfaccia LAN del router l’indirizzo 192.168.177.1. Serve per raggiungere tutti gli host che appartengono alla rete 192.168.177.x

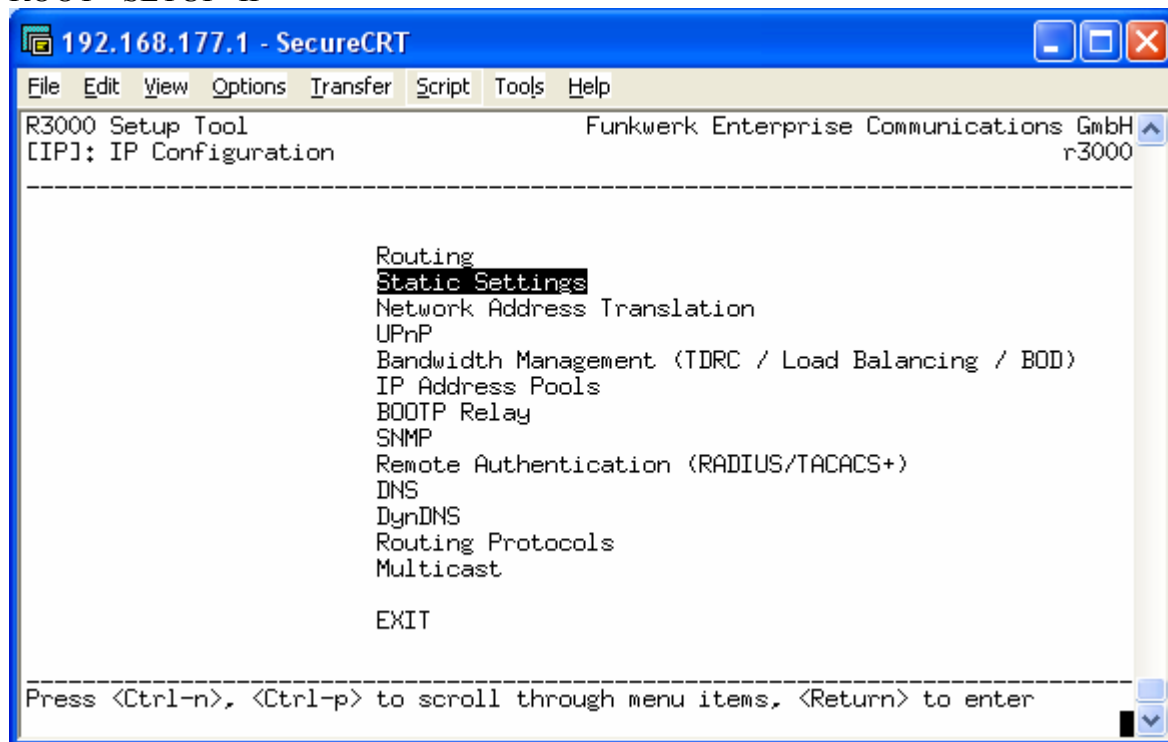
L’quarta riga è dovuta al campo “default route” messo a “yes” nella sezione ROOT>SETUP>WAN Partner>ADD>IP>BASIC IP-Settings>. Rappresenta la route di default, ovvero indica quale deve essere il gateway per tutte le destinazioni che non rientrano nelle righe precedenti, ovvero per tutte le richieste che hanno “internet” come destinazione. In questo caso il gateway è lo stesso utilizzato dall’interfaccia WAN (ngi) ed è proprio il router del provider.

Con queste tre righe appena descritte il ROUTER può navigare su internet.

NB: questo NON significa che anche un pc della LAN privata possa navigare!!! Per farlo è necessario abilitare il NAT e impostare sul pc il router come gateway predefinito!

Nella sezione Static Settings è possibile specificare il DNS per la risoluzione dei nomi. Normalmente gli indirizzi dei server DNS vengono specificati dal provider.

ROOT> SETUP>IP>

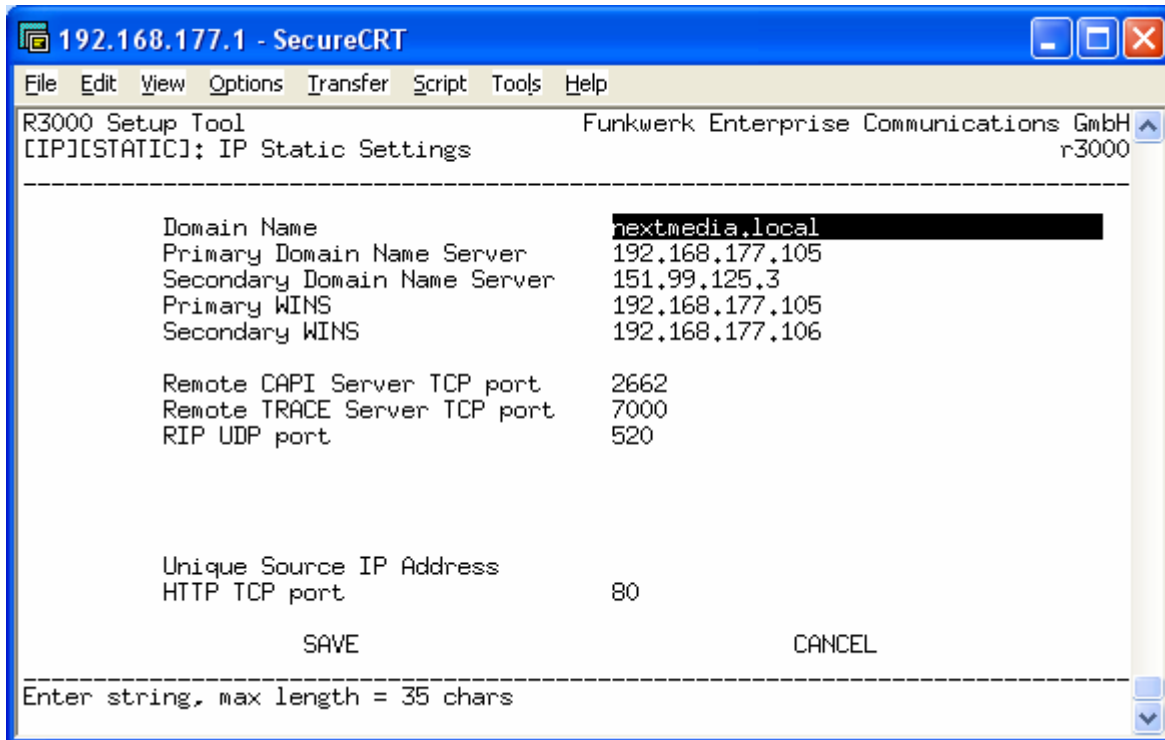


The screenshot shows a terminal window titled "192.168.177.1 - SecureCRT". The window contains the following text:

```
R3000 Setup Tool                               Funkwerk Enterprise Communications GmbH
[IP]: IP Configuration                           r3000
-----
                                Routing
                                Static Settings
                                Network Address Translation
                                UPnP
                                Bandwidth Management (TDRC / Load Balancing / BOD)
                                IP Address Pools
                                BOOTP Relay
                                SNMP
                                Remote Authentication (RADIUS/TACACS+)
                                DNS
                                DynDNS
                                Routing Protocols
                                Multicast

                                EXIT
-----
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```

ROOT> SETUP>IP>IP Static Settings>

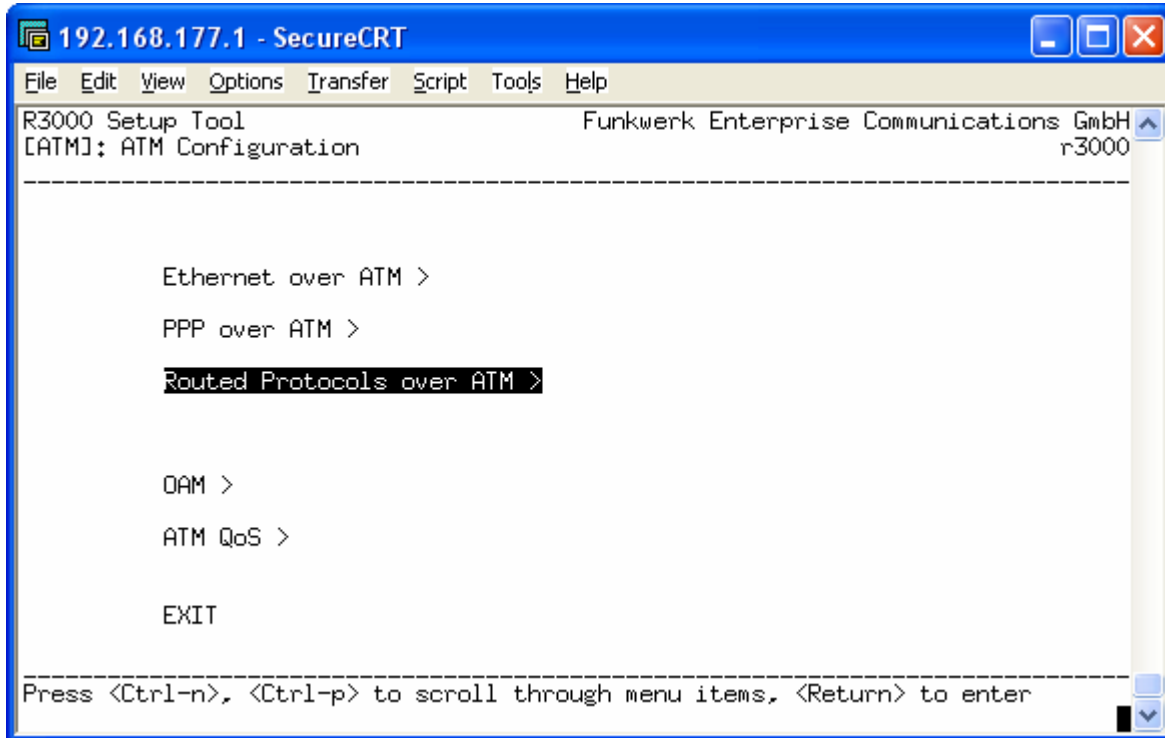


Caso IPoA (RFC 1483):

E' il caso in cui si ha a disposizione un IP statico senza User Name e Password. Non serve alcuna autenticazione: l'indirizzo IP viene assegnato dal provider solamente in relazione al doppino fisico che si utilizza per la connessione.

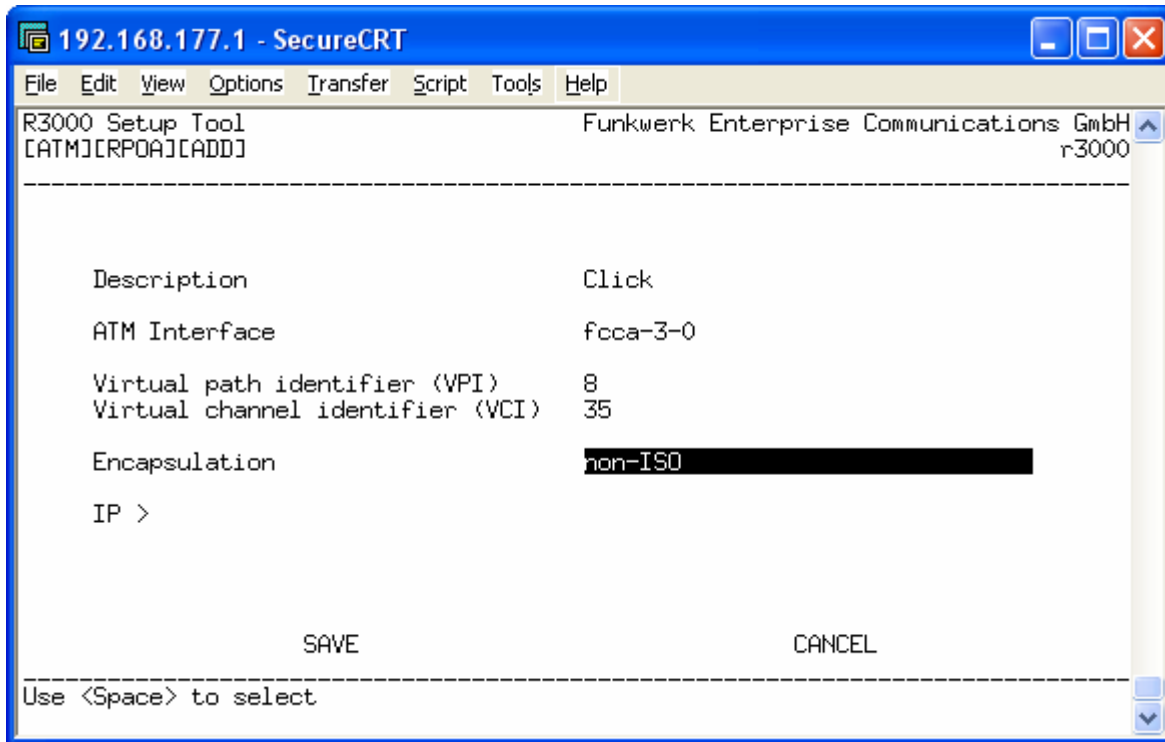
Dopo aver eseguito le operazioni preliminari (configurazione della parte LAN e verifica della connessione fisica del doppino telefonico) si entra nella sezione ATM.

ROOT> SETUP>ATM>



Entrando nel menù Routed Protocols over ATM è possibile aggiungere una connessione. I parametri per la configurazione vengono forniti dal provider e si trovano scritti sul contratto.

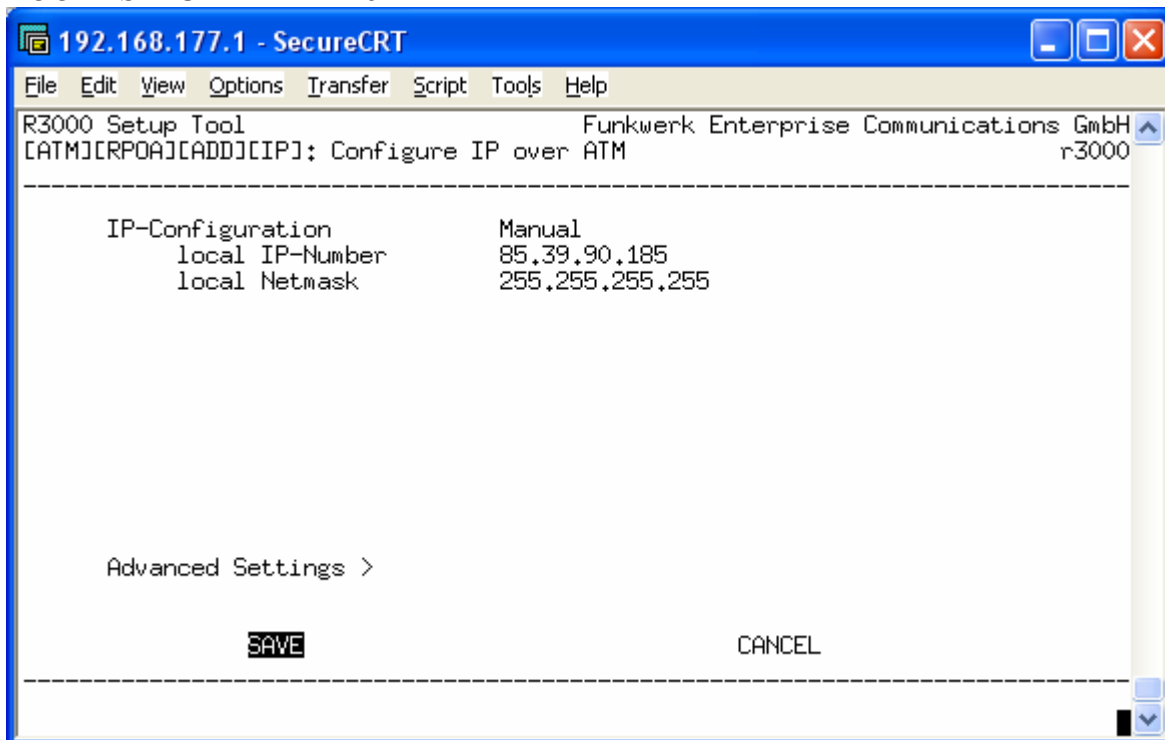
ROOT> SETUP>ATM>RPoA>ADD>



Il tipo di "Encapsulation" è sempre "non-ISO" mentre VPI e VCI sono sempre 8 e 35 rispettivamente.

Entrando nel sottomenù IP è possibile assegnare all'interfaccia WAN del router l'indirizzo pubblico (statico) che ci è stato fornito insieme al contratto. Si tratta dell'indirizzo Punto-Punto. Gli indirizzi aggiuntivi, quando presenti, vanno inseriti sull'interfaccia LAN.

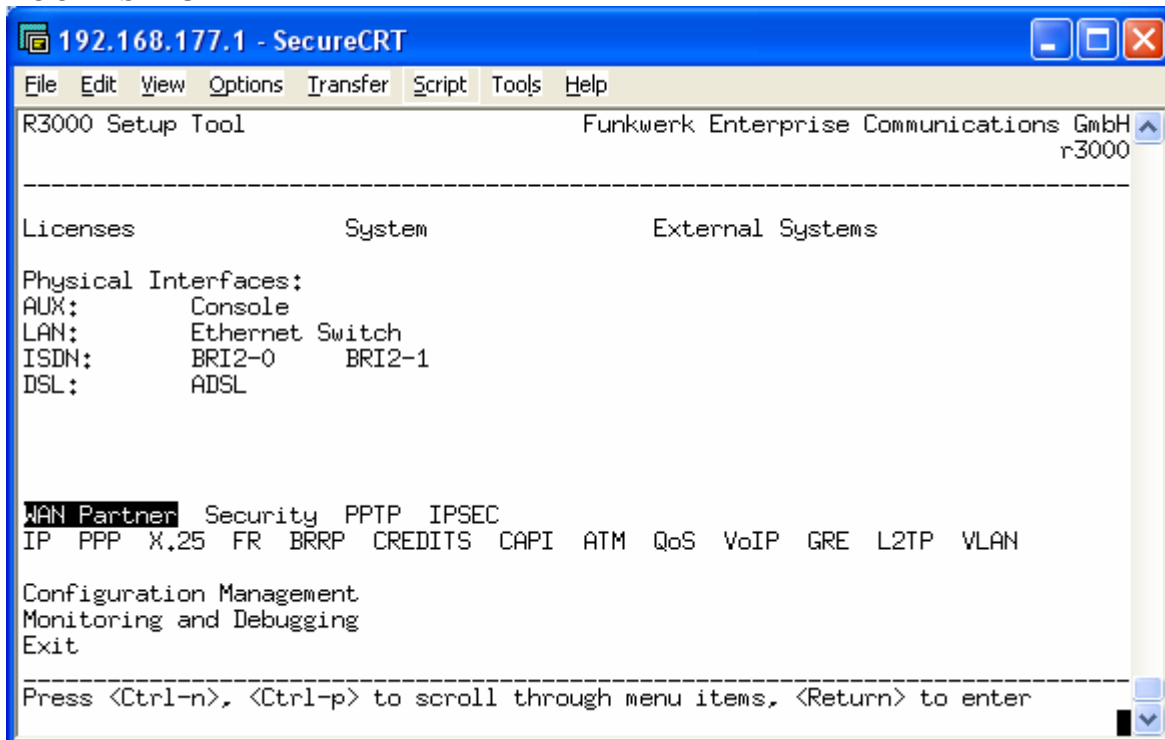
ROOT> SETUP>ATM>RPoA>ADD>IP>



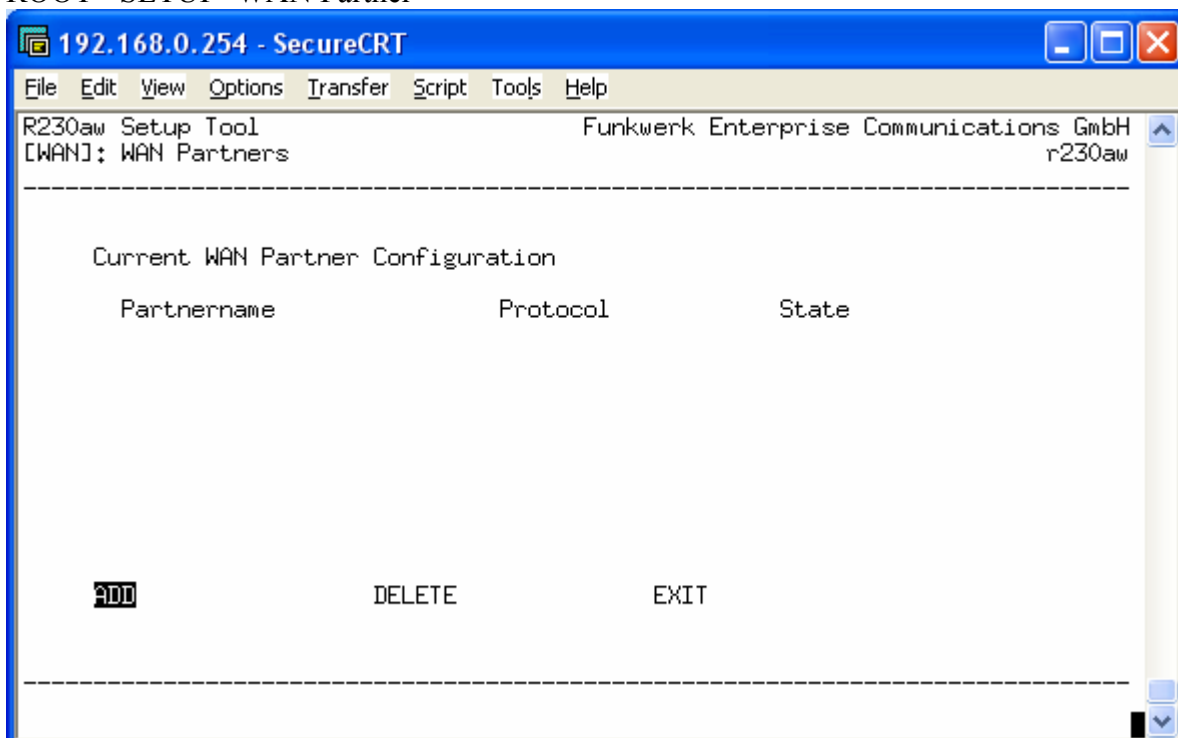
NB: Normalmente la netmask del punto-punto è 255.255.255.252 ma nulla vieta che possa essere più ampia come per es. 255.255.255.0. Altre volte è invece più piccola, es. 255.255.255.255.

Una volta salvato si torna alla schermata principale. Si entra nella sezione WAN Partner e si controlla che non ci siano voci nell'elenco. Come detto in precedenza la configurazione RPoA (o IPoA) NON prevede la configurazione di un WAN Partner.

ROOT> SETUP>

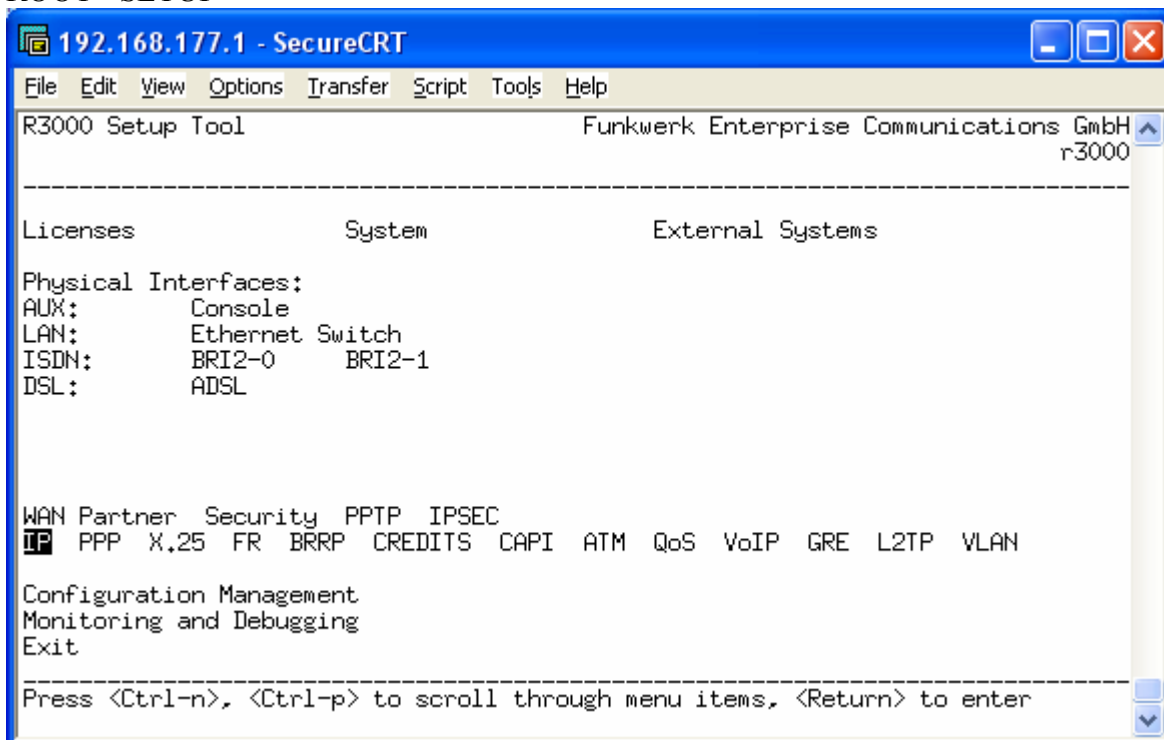


ROOT> SETUP>WAN Partner>

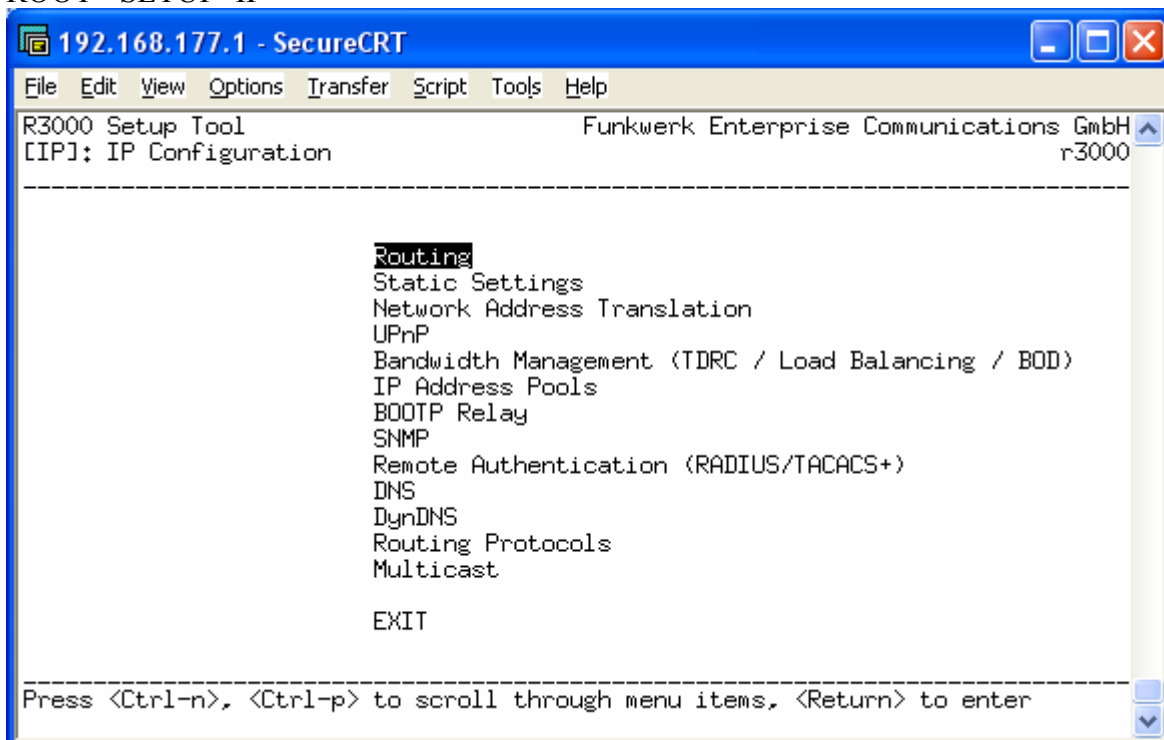


A questo punto si entra nella sezione IP → Routing:

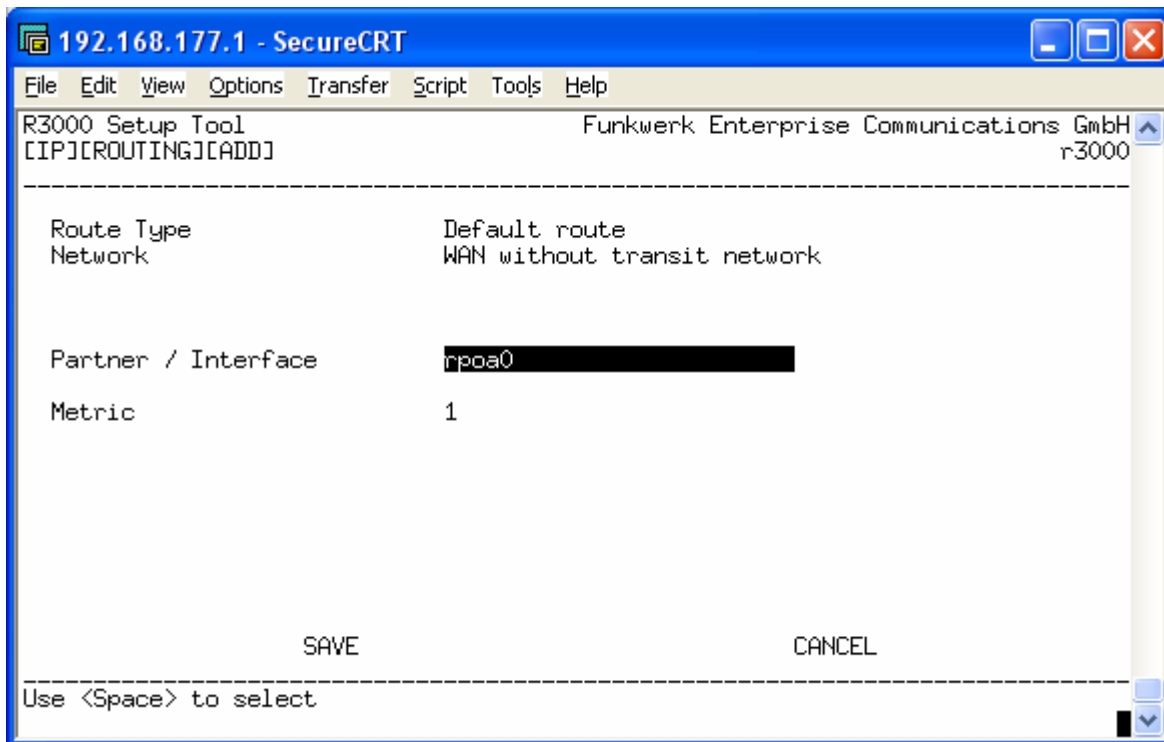
ROOT> SETUP>



ROOT> SETUP>IP>



All'interno della voce Routing troviamo la tabella di routing. Dobbiamo aggiungere manualmente la Default Route sfruttando l'interfaccia ADSL.

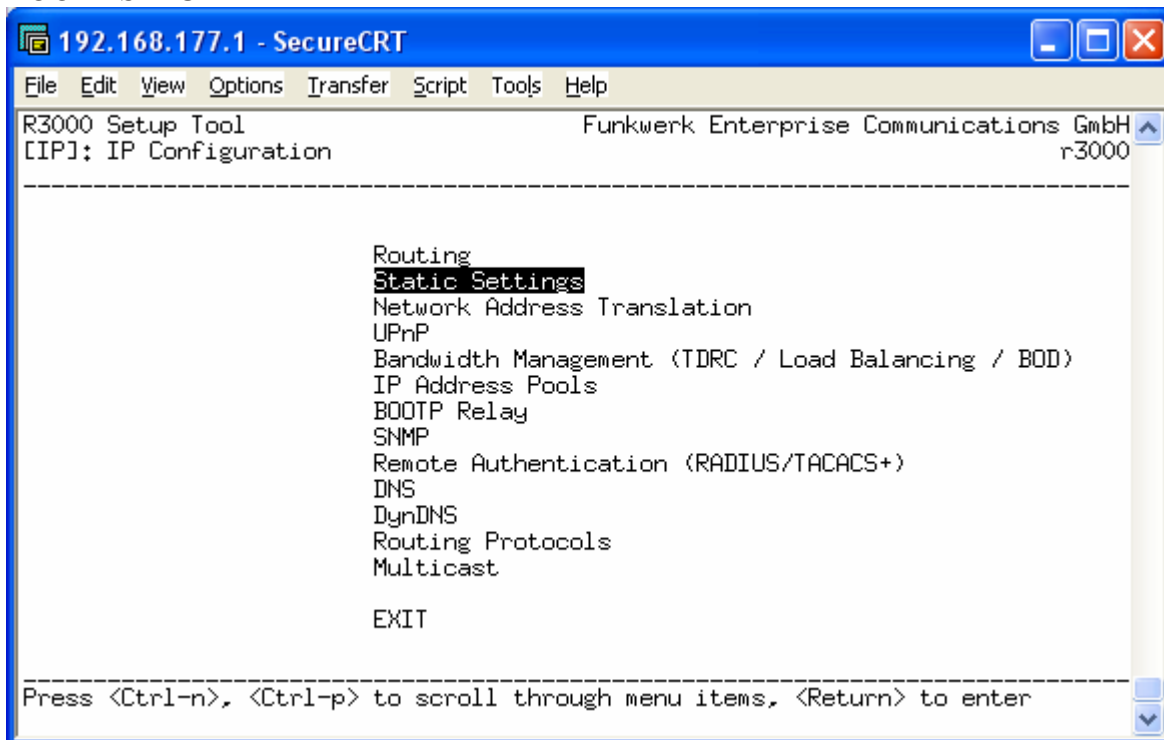


Come tipologia di route specifichiamo che si tratta di una “Default route” mentre come rete indichiamo “WAN without transit network”. Specifichiamo poi che l’interfaccia di riferimento per questa regola è proprio l’interfaccia RPoA0 creata in precedenza.

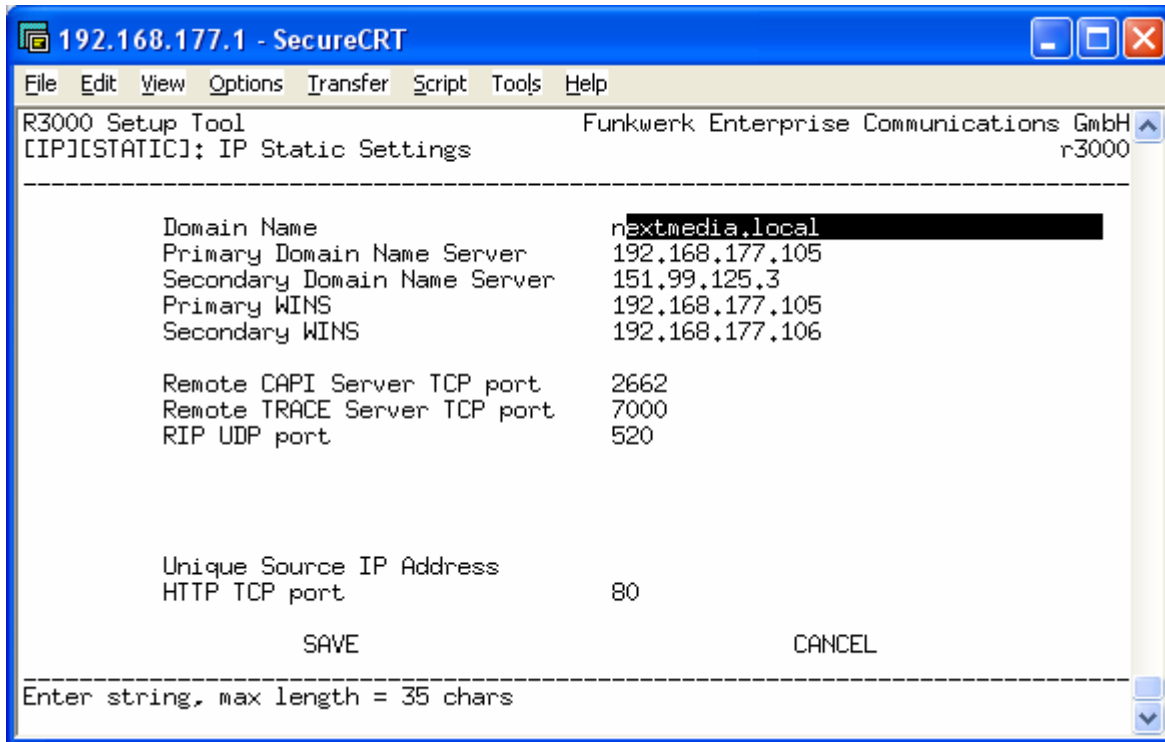
Nella sezione Static Settings è possibile specificare il DNS per la risoluzione dei nomi.

Normalmente gli indirizzi dei server DNS vengono forniti dal provider.

ROOT> SETUP>IP>

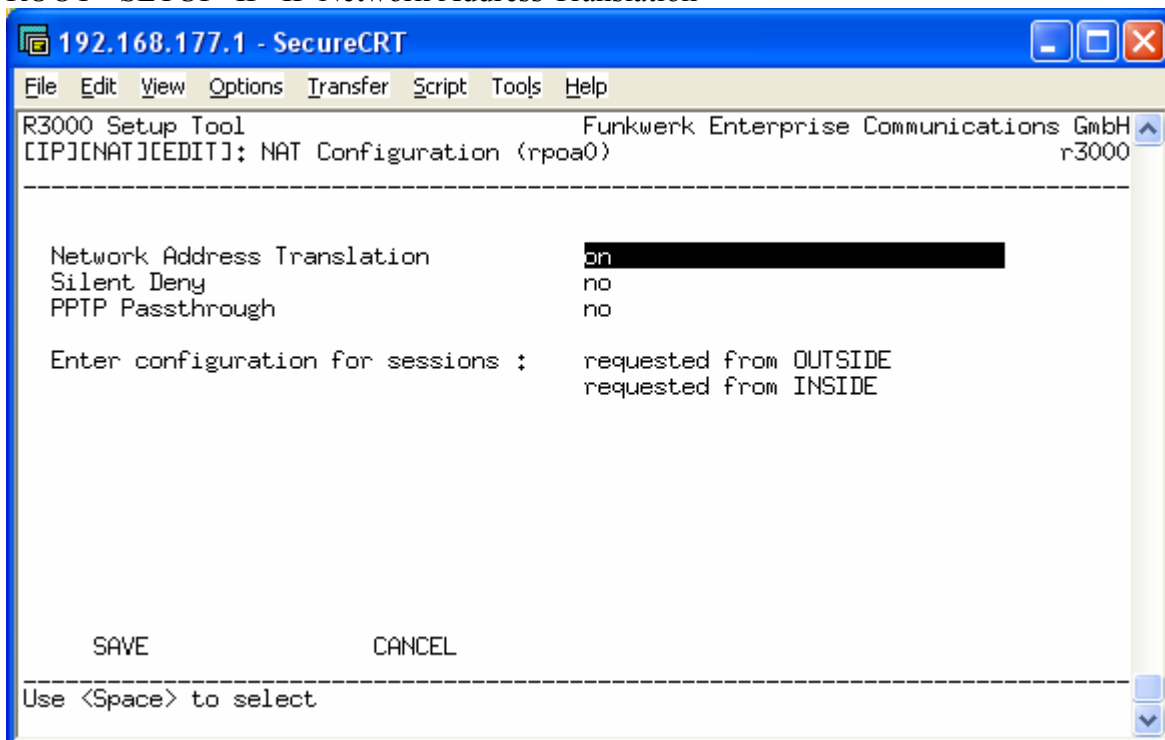


ROOT> SETUP>IP>IP Static Settings>

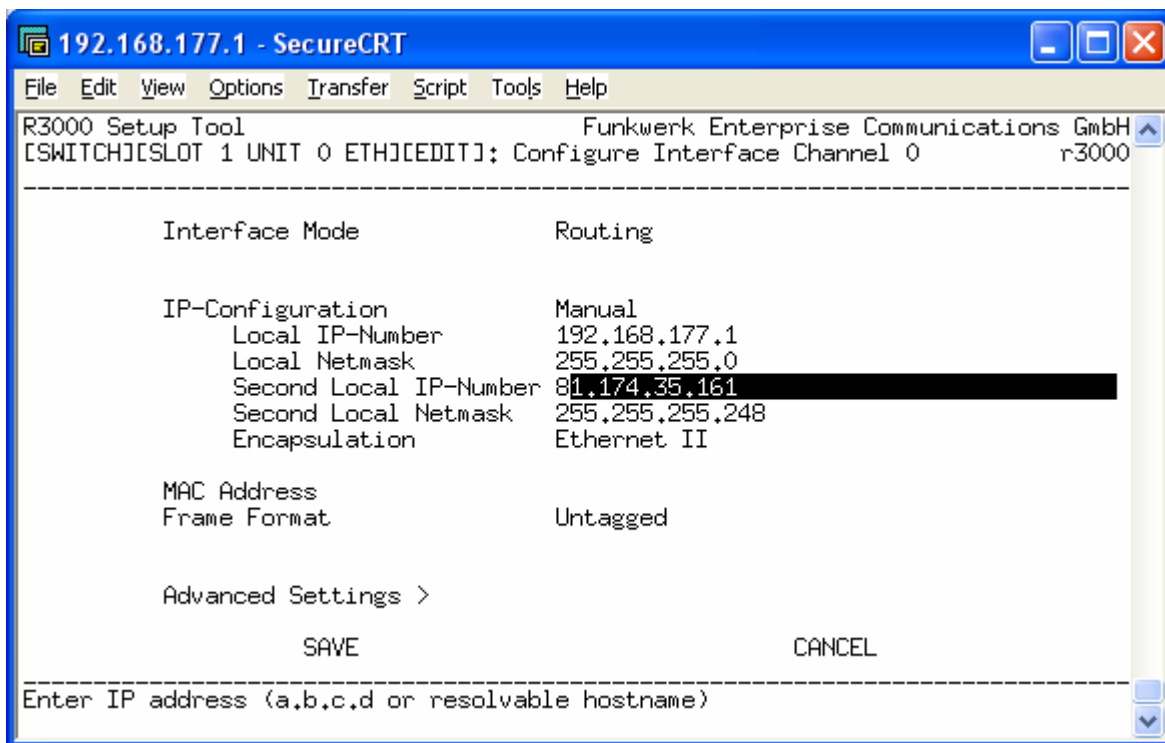


Dal menù Network Address Translation abilitare il NAT sull'interfaccia rpoa0.

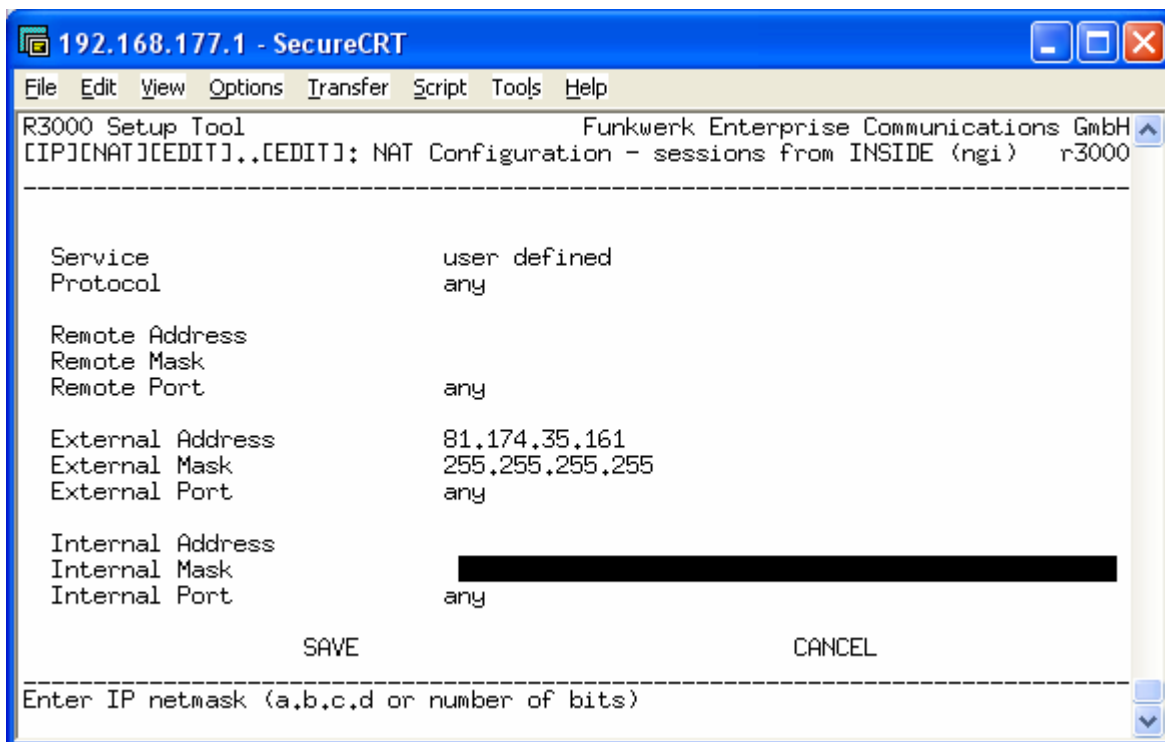
ROOT> SETUP>IP>IP Network Address Translation>



Nel caso in cui ci venga fornito un pool di indirizzi pubblici aggiuntivi dobbiamo assegnarli sull'interfaccia LAN (Second Local IP-Number, Second Local Netmask). In questo campo dobbiamo mettere il primo indirizzo valido del pool e la netmask specificata dal Provider.



A questo punto occorre tornare sulle impostazioni del NAT (precedentemente abilitato) e creare una regola sotto la voce "Requested From Inside" per fare in modo che tutte le richieste provenienti dalla LAN e dirette verso internet escano utilizzando l'indirizzo aggiuntivo assegnato al router sulla LAN. La regola da creare deve essere uguale a quella dell'immagine sottostante, l'unica cosa da modificare sarà l'indirizzo IP "External"



Connessione UMTS tramite PCMCIA

L'unico modello di router Bintec in grado di gestire connessioni GPRS/UMTS tramite PCMCIA è l'R1200wu. Per prima cosa dobbiamo assicurarci che la scheda PCMCIA sia compatibile con il router in questione. Per verificarlo fare riferimento a questo indirizzo: http://www.funkwerk-ec.com/prod_bintec_r1200wu_cards_en.75538,837.html (l'indirizzo potrebbe subire variazioni).

Verificata la compatibilità fra scheda e router si inserisce la SIM all'interno della scheda UMTS e si inserisce quest'ultima nello slot del router. Entrando nel menù UMTS dovrebbe essere possibile controllare la qualità del segnale e assegnare l'APN (Access Point Name).

Suggerimento: disabilitare il codice PIN dalla SIM card oppure inserire il codice PIN corretto nella schermata sottostante. Se si sbaglia ad inserire il codice PIN la SIM card andrà in blocco richiedendo il codice PUK!

```
R1200 Setup Tool                               Funkwerk Enterprise Communications GmbH
[UMTS]: Settings                               r1200

-----

UMTS Adminstatus      : enable
UMTS PIN              : ****

Additional Initstring  : ATX3E0
Access Point Name (APN): internet.t-mobile
Incoming call action  : isdnlogin

Current Modem Status  : up
UMTS Network Provider : T-Mobile D
UMTS Signal Quality   : -91 dB (low)
Last Modem Command    : AT+CSQ
Last Modem Answer     : OK

SAVE                                CANCEL

-----
```

Principali APN italiani:

Operatore	APN	Numero telefonico
Vodafone	web.omnitel.it	*99**1*1#
Tim	ibox.tim.it	*99***1#
Wind	internet.wind	*99**1*1#
Tre	tre.it	*99**1*1#

Ora occorre aggiungere un profilo sotto alla voce WAN Partner (si veda la configurazione ISDN, è praticamente identica, cambia solo il parametro *Layer 1 Protocol*). Alla voce Advanced Settings si specificano il tempo di disconnessione automatica in caso di inattività (Static Short Hold) e la tipologia di connessione (Layer 1 Protocol = GPRS/UMTS)

Callback	no
Static Short Hold (sec)	50
Idle for Dynamic Short Hold (%)	0
Delay after Connection Failure (sec)	10
Layer 1 Protocol	GPRS/UMTS
GPRS/UMTS Interface	Slot 6 Unit 0 UMTS

Extended Interface Settings (optional) >

Special Interface Types	none
-------------------------	------

OK

CANCEL

Connessione UMTS tramite chiavetta USB

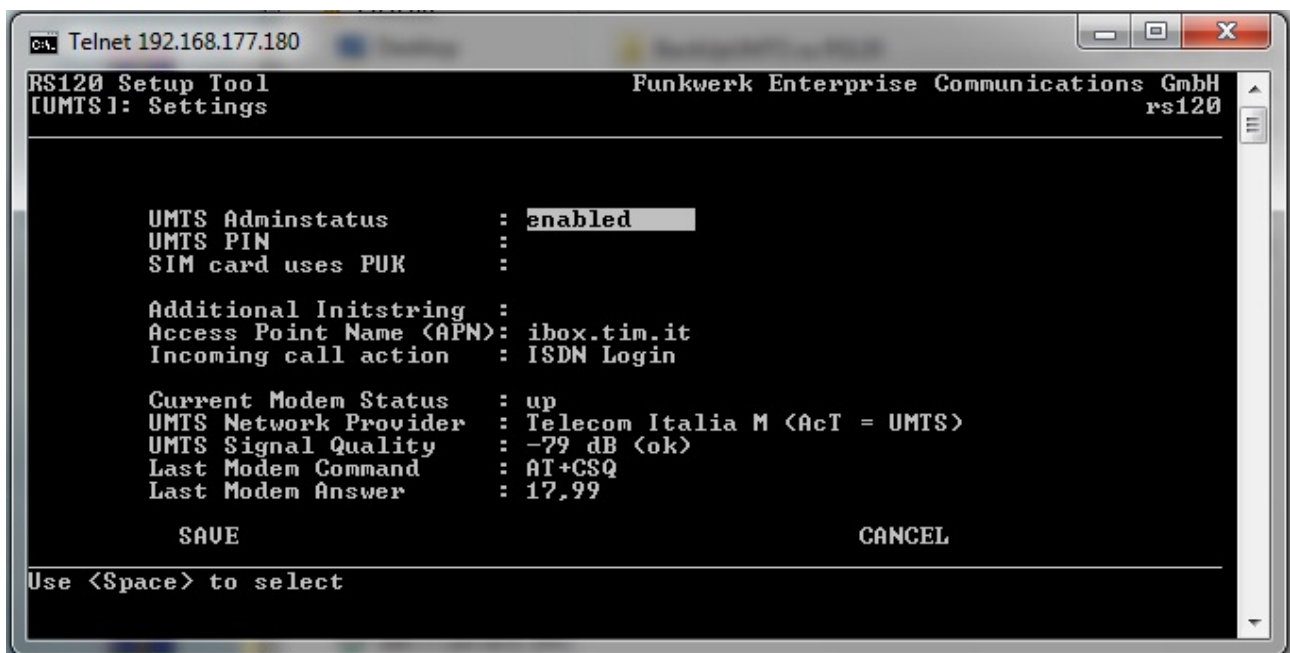
I router Bintec RS120(wu) e RS230a(w) hanno una porta USB sulla quale è possibile collegare una chiavetta UMTS.

L'elenco delle chiavette supportate è reperibile a questo indirizzo: [Chiavette supportate](#).

Collegare la chiavetta a router spento, una volta avviato il router, nel menù principale sotto alla voce **LAN Gigabit** dovrebbe apparire un'altra voce relativa all'UMTS; se il modello della vostra chiavetta non dovesse apparire è necessario riavviare il router una seconda volta.

A questo punto di fianco alla voce UMTS dovrebbe apparire il modello della vostra chiavetta.

Per configurare la connessione a internet tramite chiavetta entriamo sul menù UMTS e andiamo a impostare: PIN e PUK della SIM (se richiesti) e l'APN del provider.



```
Telnet 192.168.177.180
RS120 Setup Tool
[UMTS]: Settings
Funkwerk Enterprise Communications GmbH
rs120

UMTS Adminstatus      : enabled
UMTS PIN              :
SIM card uses PUK     :

Additional Initstring  :
Access Point Name (APN): ibox.tim.it
Incoming call action   : ISDN Login

Current Modem Status   : up
UMTS Network Provider : Telecom Italia M (AcT = UMTS)
UMTS Signal Quality    : -79 dB (ok)
Last Modem Command    : AT+CSQ
Last Modem Answer     : 17,99

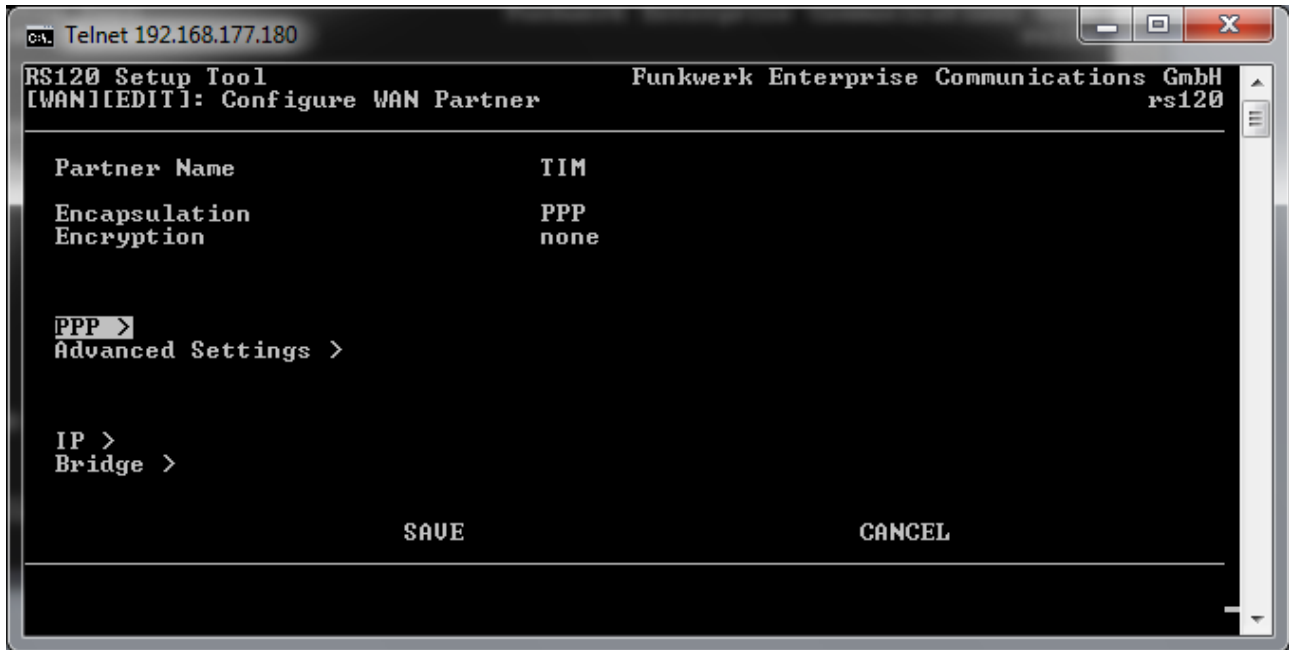
SAVE                  CANCEL

Use <Space> to select
```

Ricordiamo che gli APN dei provider italiani sono:

- TIM: ibox.tim.it
- Vodafone: web.omnitel.it oppure m2mbis.vodafone.it
- Wind: internet.wind
- H3G: tre.it

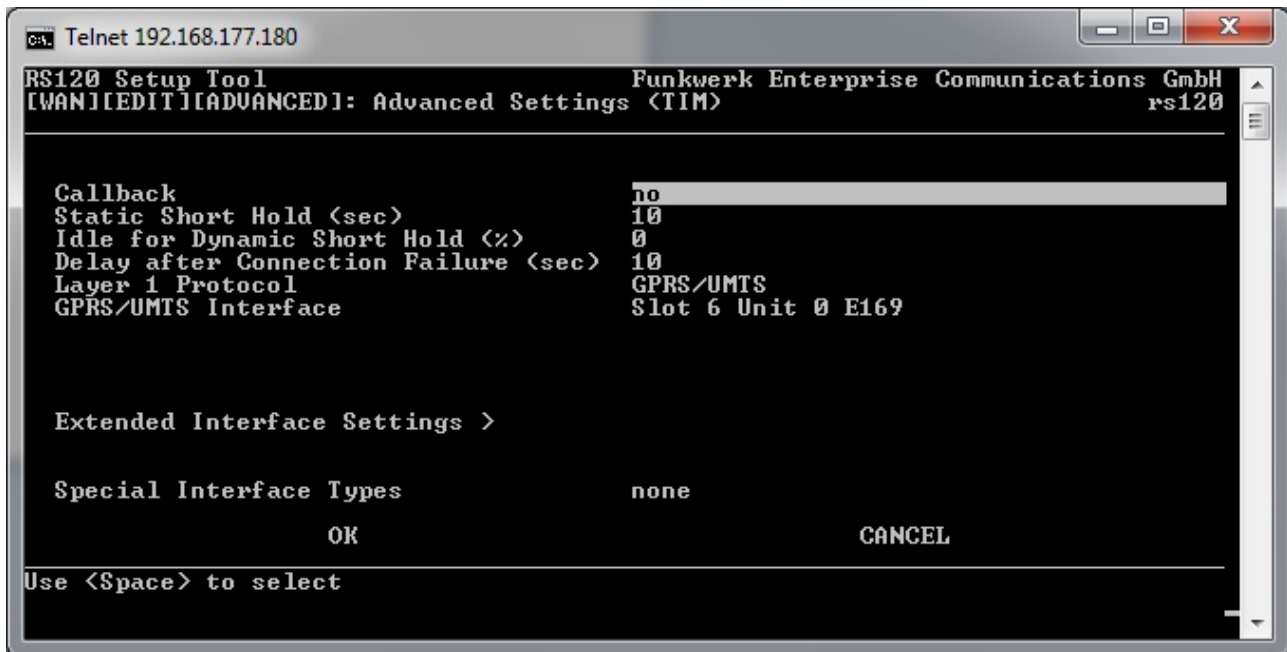
A questo punto salviamo e dal menù principale andiamo sulla voce **WAN PARTNERS**, clicchiamo su **ADD** e configuriamo come segue:



Andiamo poi sulla voce **PPP** e impostiamo il tipo di autenticazione; solitamente non è utilizzato alcun tipo di autenticazione per cui impostiamo come segue:

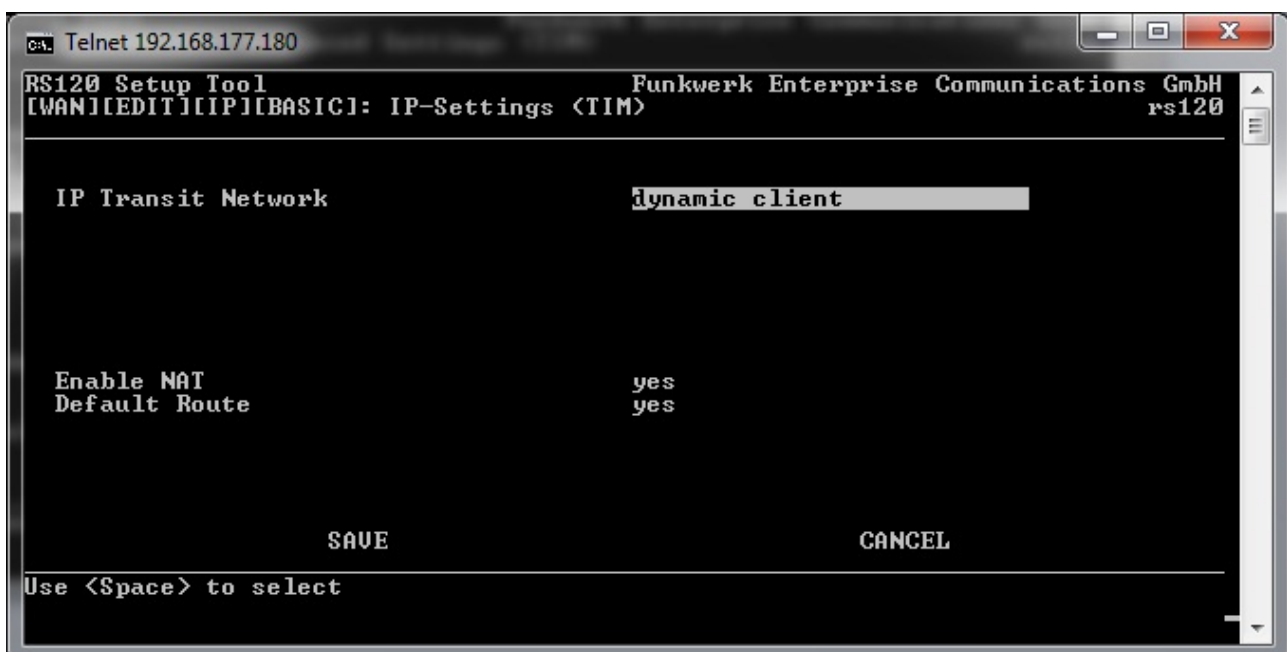


Clicchiamo su **Ok** e entriamo poi sulla voce **Advanced Settings**.



Callback: indica se si vuole che il provider o il server ci richiami (normalmente non utilizzato)
Static Short Hold: impostato a 10 indica il tempo di inattività della connessione prima che venga disconnessa. Se vogliamo che la connessione sia sempre attiva impostiamo questo parametro a -1
Idle for Dynamic Short Hold: indica un tempo dinamico di inattività in base alla durata della connessione. Per esempio se la connessione è attiva da 60 minuti e il parametro è impostato a 10% significa che il router effettuerà la disconnessione dopo 6 minuti di inattività.
Delay after Connection Failure: indica il tempo di attesa prima di un nuovo tentativo di connessione.
Layer 1 Protocol: indichiamo la voce GPRS/UMTS.
GPRS/UMTS Interface: Indica il modello di chiavetta utilizzata.

Clicchiamo su **OK** e andiamo poi alla voce **IP → Basic IP Settings** e impostiamo come segue:

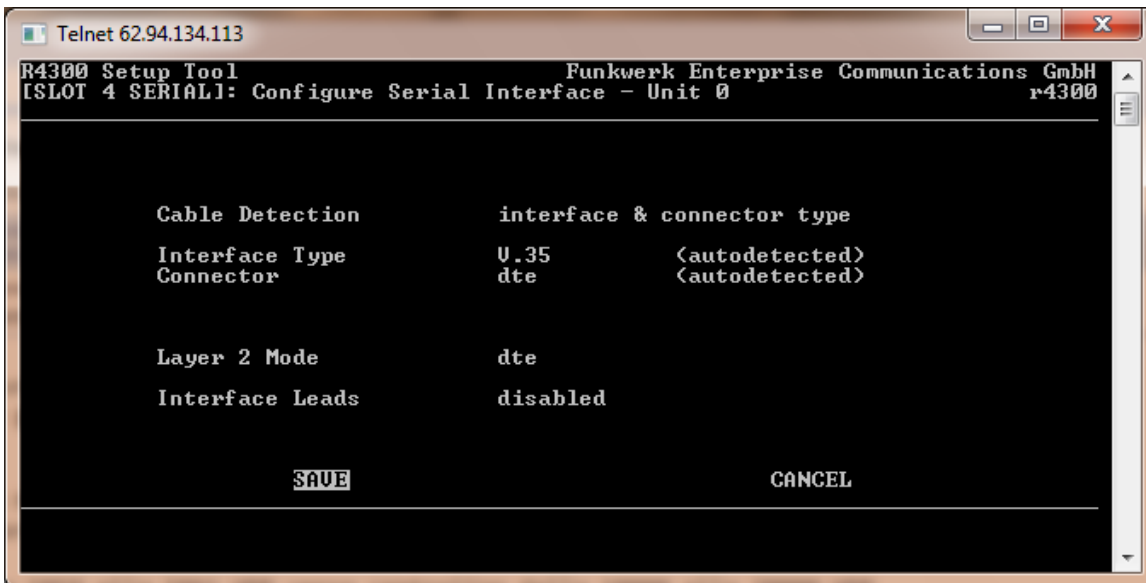
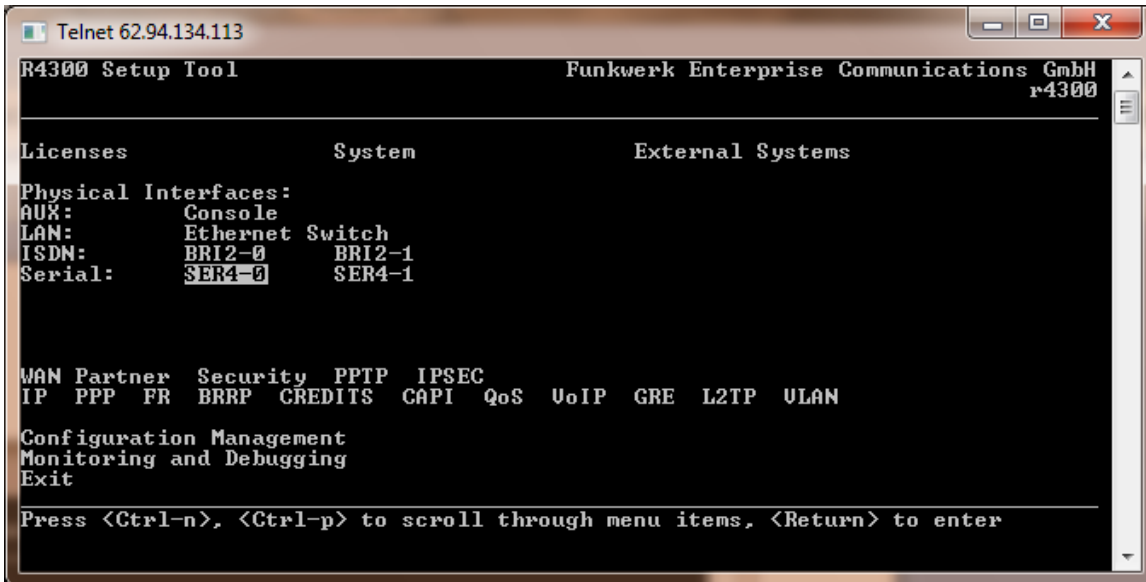


Non ci resta che salvare.
 A questo punto il router dovrebbe connettersi a internet automaticamente tramite UMTS.

Connessione HDSL

Per utilizzare una connessione HDSL è necessario un router R4300. Tale router dovrà essere connesso al modem fornito dal provider tramite un cavo seriale DTE v.35.

Per prima cosa impostiamo i parametri relativi alla seriale:



Ora creiamo il Wan Partner (attraverso il comando ADD) avendo cura di specificare il tipo di incapsulamento Frame Relay:

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
                                                r4300

Licenses                System                External Systems

Physical Interfaces:
AUX:      Console
LAN:      Ethernet Switch
ISDN:     BRI2-0   BRI2-1
Serial:   SER4-0   SER4-1

WAN Partner Security PPTP IPSEC
IP PPP FR BRRP CREDITS CAPI QoS UoIP GRE L2TP ULAN

Configuration Management
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
                                                r4300
[WAN]: WAN Partners

Current WAN Partner Configuration

Partnername      Protocol      State
-----
si4-0            frame_relay  up

ADD                DELETE          EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit
```

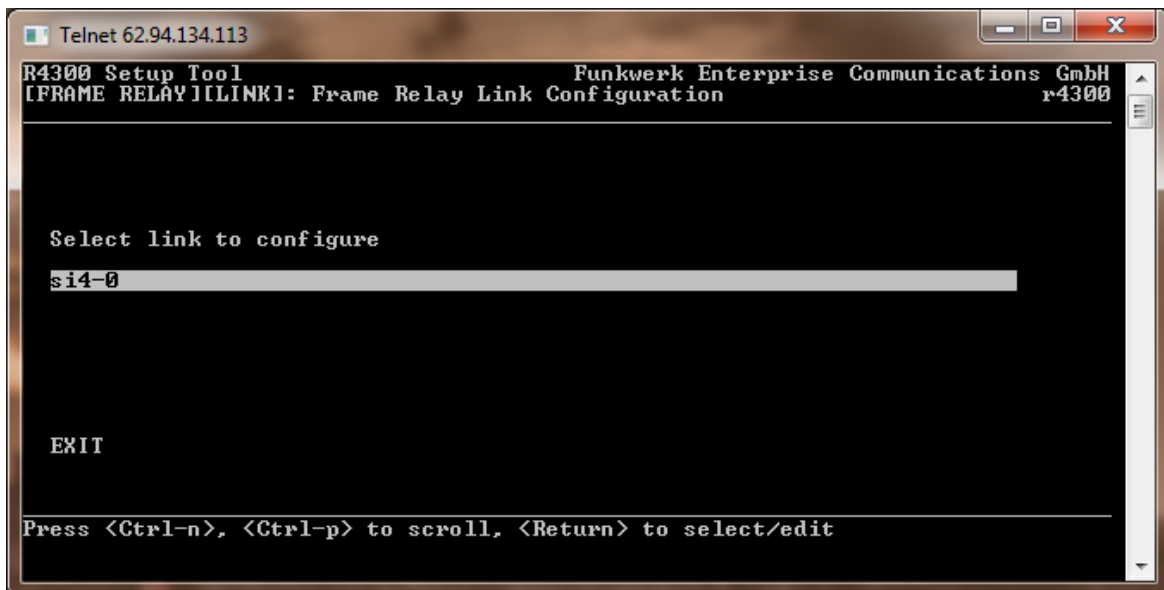
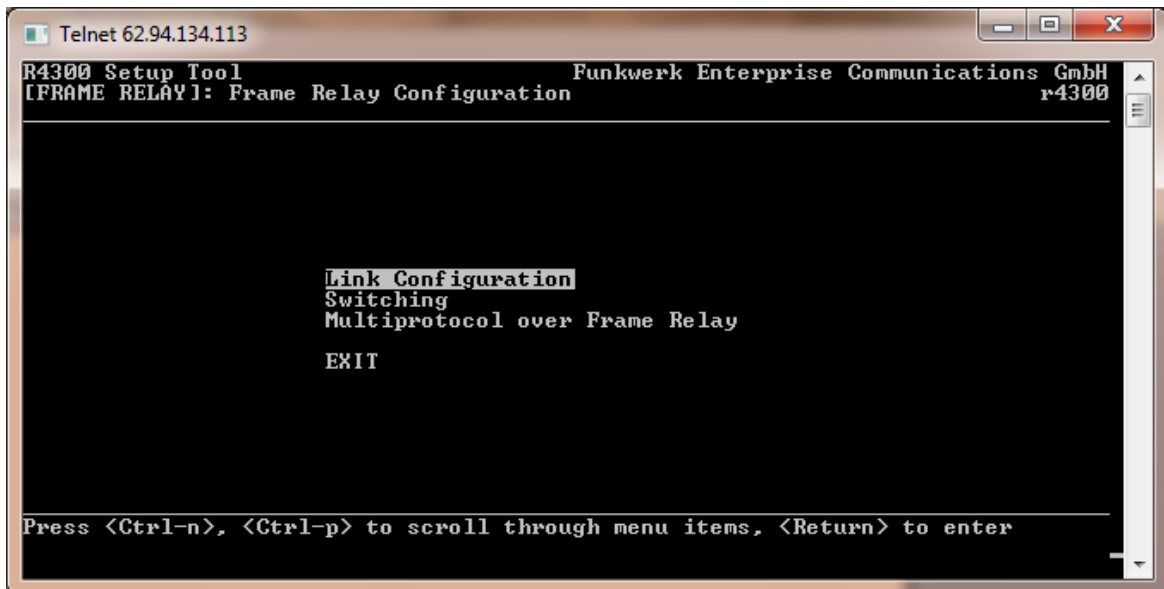
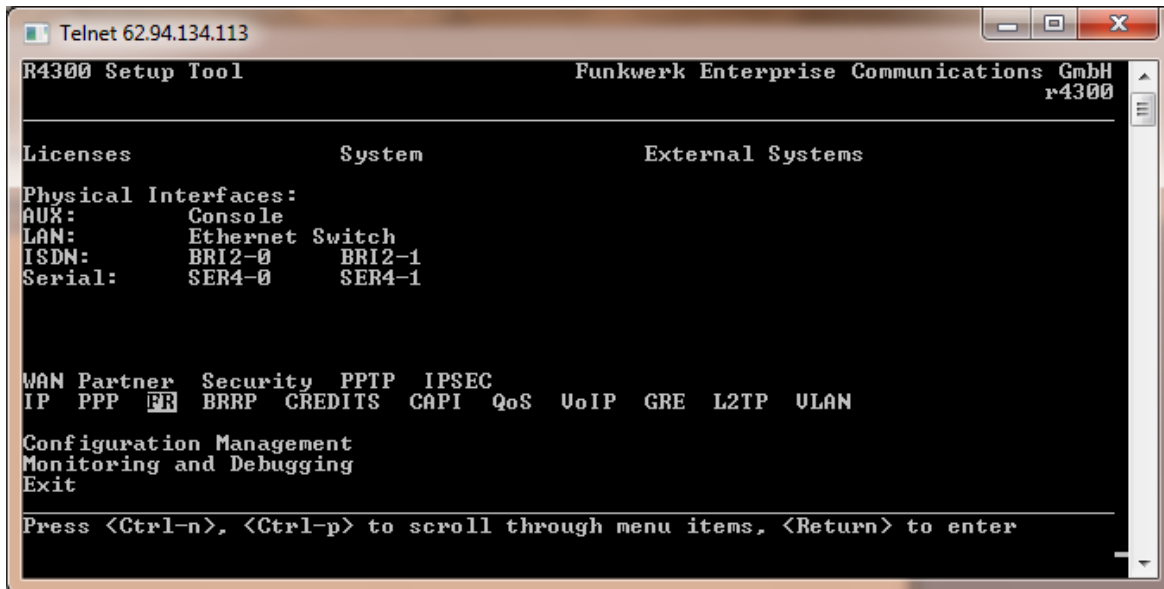
```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
                                                r4300
[WAN][EDIT]: Configure Synchronous Serial Leased Line

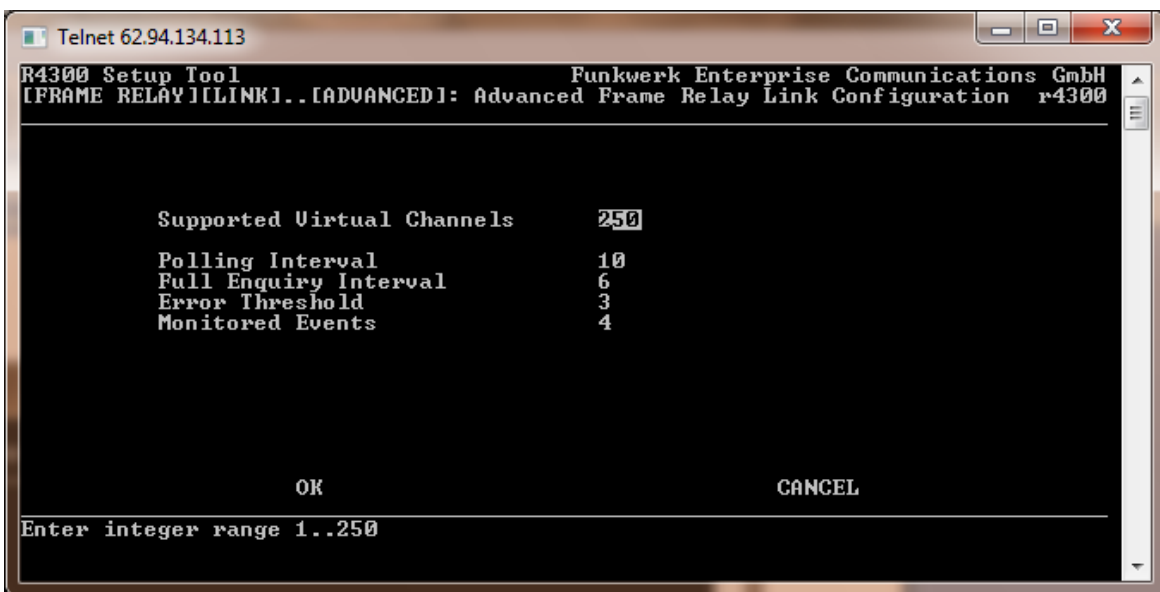
Partner Name      si4-0
Encapsulation     Frame Relay

SAVE                CANCEL

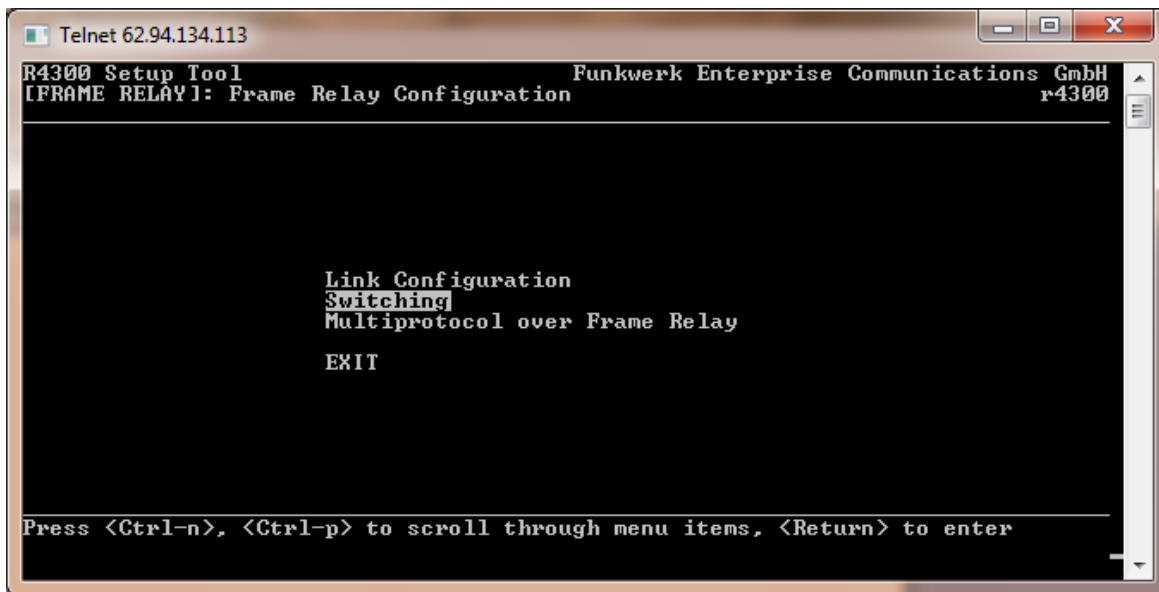
Enter string, max length = 25 chars
```

Ora impostiamo i parametri relativi al Frame Relay:





Torniamo alla schermata principale di FR...



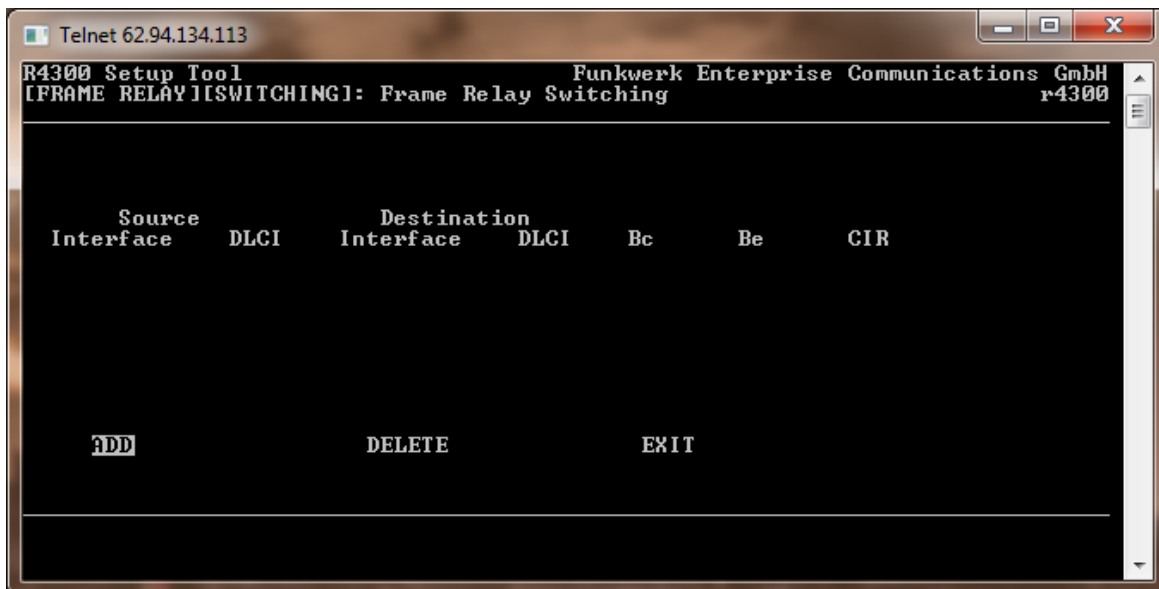
```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
[FRAME RELAY]: Frame Relay Configuration       r4300

Link Configuration
Switching
Multiprotocol over Frame Relay

EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```

Verifichiamo che il menù Switching sia vuoto.



```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
[FRAME RELAY][SWITCHING]: Frame Relay Switching r4300

Source      Destination
Interface   DLCI        Interface   DLCI        Bc         Be         CIR

ADD          DELETE      EXIT
```

Torniamo ancora alla schermata principale di FR...

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
[FRAME RELAY]: Frame Relay Configuration       r4300

Link Configuration
Switching
Multiprotocol over Frame Relay
EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
[FRAME RELAY][MPR]: Frame Relay Multiprotocol Routing       r4300

Interface Name      Type
-----
mpfr1               point to point

ADD                DELETE                EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit
```

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
[FRAME RELAY][MPR][EDIT]: Configure Frame Relay MPR Partner       r4300

Partner Name                mpfr1
Interface Type              point to point
Inverse Arp                 disabled

Virtual Circuits >
IP >
Bridge >

SAVE                CANCEL
```

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
[FRAME RELAY][MPR]..[SWITCHING]: Configure Frame Relay Virtual Circuits  r4300

Source      Destination
Interface   DLCI      Interface   DLCI      Bc      Be      CIR
si4-0       20                2048000  0         2048000

ADD                DELETE                EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit
```

Inseriamo il DLCI fornito dal provider e la velocità di connessione...

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
[FRAME RELAY][MPR][EDIT][SWITCHING][EDIT]  r4300

Source Interface      si4-0
Source DLCI           20

Burst committed <Bc>      2048000
Burst excess <Be>         0
Committed Information Rate <CIR> 2048000

OK                CANCEL

Use <Space> to select
```

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
[FRAME RELAY][MPR][EDIT]: Configure Frame Relay MPR Partner  r4300

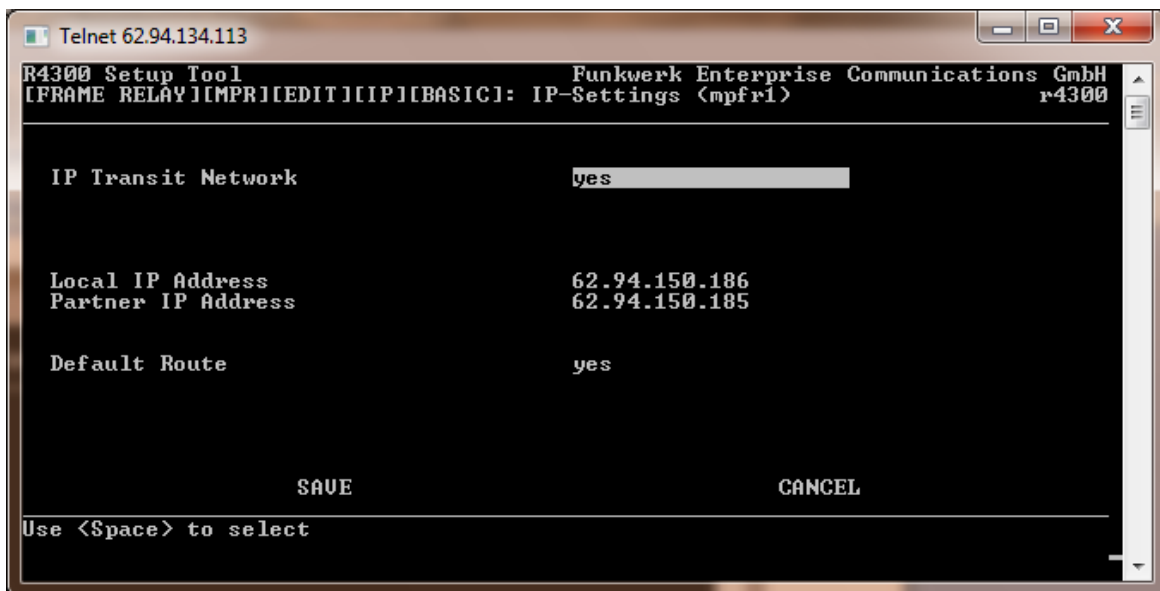
Partner Name              mpfr1
Interface Type            point to point
Inverse Arp               disabled

Virtual Circuits >
IP >
Bridge >

SAVE                CANCEL
```



Inseriamo l'indirizzo di punto-punto assegnatoci dal provider (Local IP è l'indirizzo del nostro router, Partner IP è invece l'indirizzo del router di centrale)



Ora non resta che abilitare il NAT sull'interfaccia mpfr1:

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
                                               r4300

Licenses          System          External Systems

Physical Interfaces:
AUX:      Console
LAN:      Ethernet Switch
ISDN:     BRI2-0   BRI2-1
Serial:   SER4-0   SER4-1

WAN Partner Security PPTP IPSEC
PPP FR BRRP CREDITS CAPI QoS UoIP GRE L2TP ULAN

Configuration Management
Monitoring and Debugging
Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
                                               r4300
IIP1: IP Configuration

Routing
Static Settings
Network Address Translation
UPnP
Bandwidth Management <TDRC / Load Balancing / BOD>
IP Address Pools
BOOTP Relay
SNMP
Remote Authentication <RADIUS/TACACS+>
DNS
DynDNS
Routing Protocols
Multicast

EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```

```
Telnet 62.94.134.113
R4300 Setup Tool                               Funkwerk Enterprise Communications GmbH
                                               r4300
IIP1I[NAT]: NAT Configuration

Select IP Interface to be configured for NAT

Name          Nat          Static mappings          Static mappings
              from Outside          from Inside
en1-0         off          0          0
en1-0-snap    off          0          0
en1-4         off          0          0
en1-4-snap    off          0          0
mpfr1         on           6          1

EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to select/edit
```


Tunnel Privati Virtuali (VPN)

IPSec e PPTP

Premessa

Per poter realizzare la sicurezza delle trasmissioni mediante una VPN esistono diversi protocolli appositamente progettati per permettere una trasmissione sicura a vari livelli nella rete. In sostanza è possibile realizzare una VPN praticamente su ogni livello della pila OSI. La scelta di utilizzare un protocollo piuttosto che un altro dipende dai requisiti di sicurezza delle applicazioni e dalle necessità di sicurezza dell'utente, il quale deve decidere a che livello della pila deve essere implementata la sicurezza nelle trasmissioni offerta da una VPN. In alcuni casi questi protocolli possono fornire una soluzione più adeguata alle esigenze dell'utente rispetto all'utilizzo di una VPN IPsec. In ogni caso questi protocolli, ognuno con la propria tecnologia di sicurezza, utilizzano tutti dei meccanismi di tunneling e cifratura che incapsulano il pacchetto di dati creandogli attorno una protezione durante la trasmissione e lo de-incapsulano in ricezione.

Esistono quattro principali protocolli di tunnel:

- IPsec (IP Security) tunnel mode
- PPTP (Point to Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- GRE (Cisco Generic Routing Encapsulation)

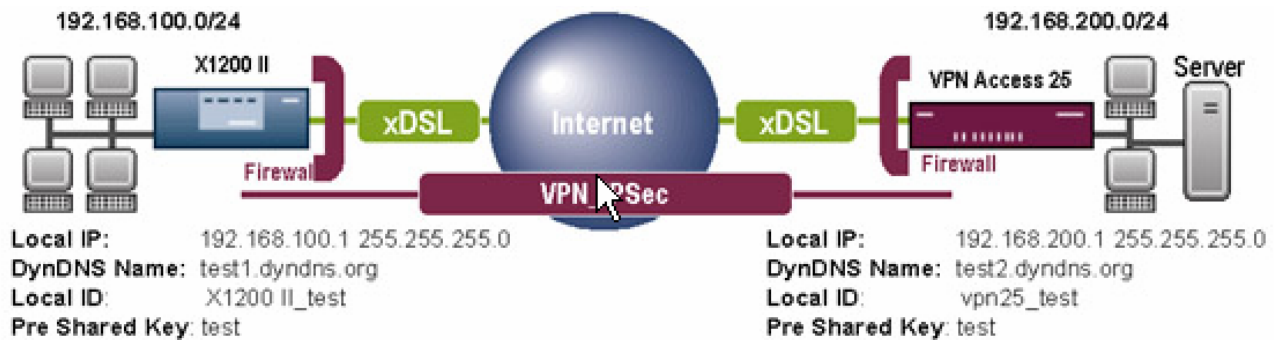
Prenderemo in esame solamente i primi due casi; nello specifico si utilizzano tunnel IPsec quando si vogliono stabilire connessioni permanenti fra due o più sedi, mentre si utilizzano tunnel PPTP quando si vuole connettere un computer portatile alla sede principale.

Prerequisito fondamentale per realizzare una VPN fra due router, o più in generale fra due END-POINT, è che gli end-points stessi siano collegati ad internet.

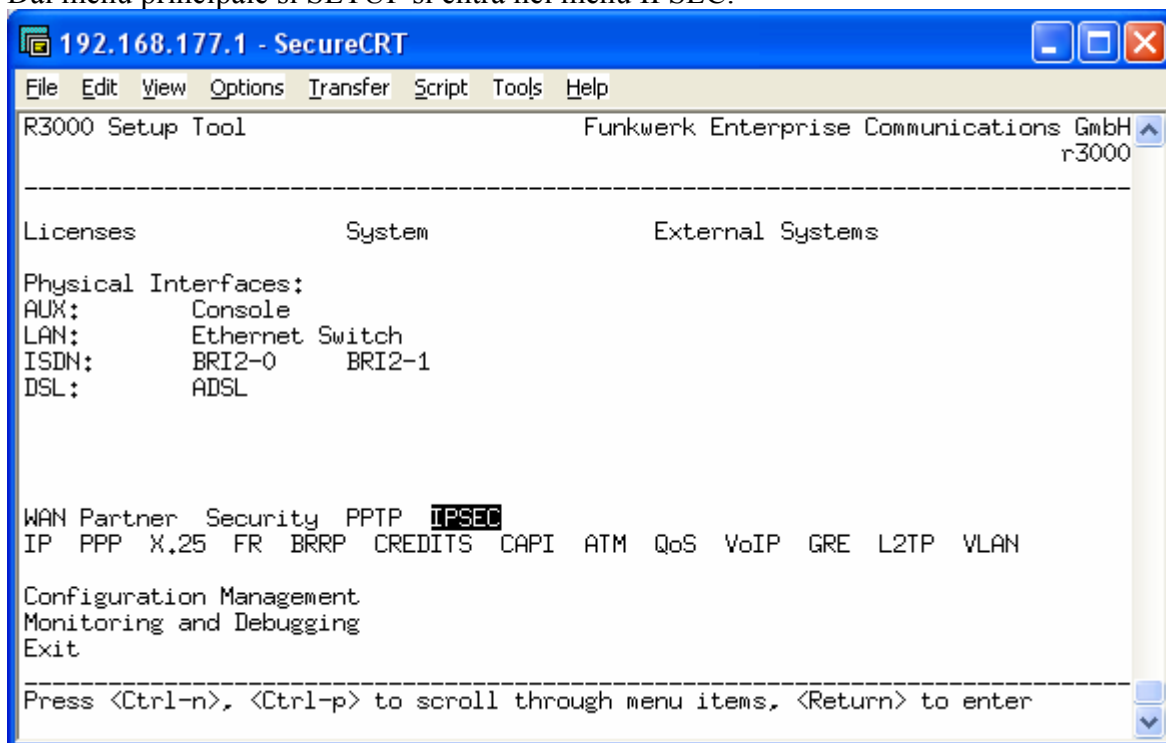
Configurazione di un tunnel IPSEC

Di fabbrica, nei router Bintec, sono presenti 5 licenze IPsec sui modelli R23x e 10 licenze su tutti gli altri apparati ma, nel caso non fossero sufficienti, è possibile comprarne altre aggiuntive.

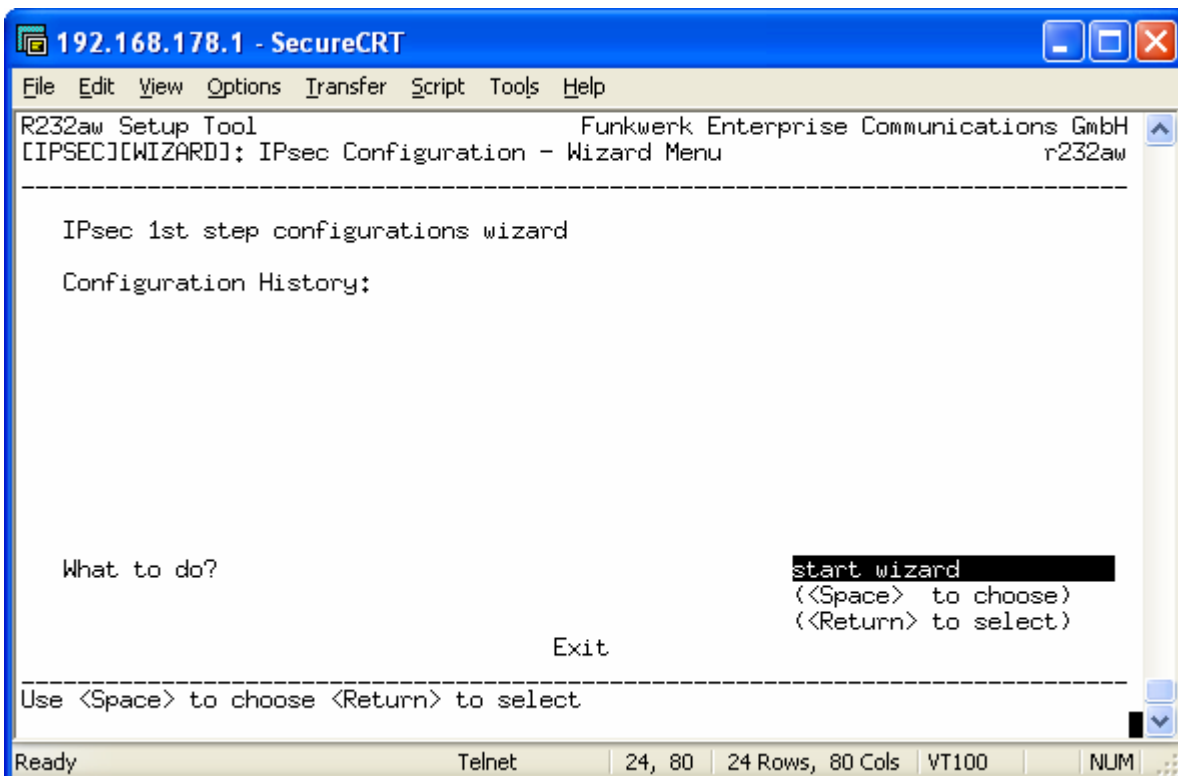
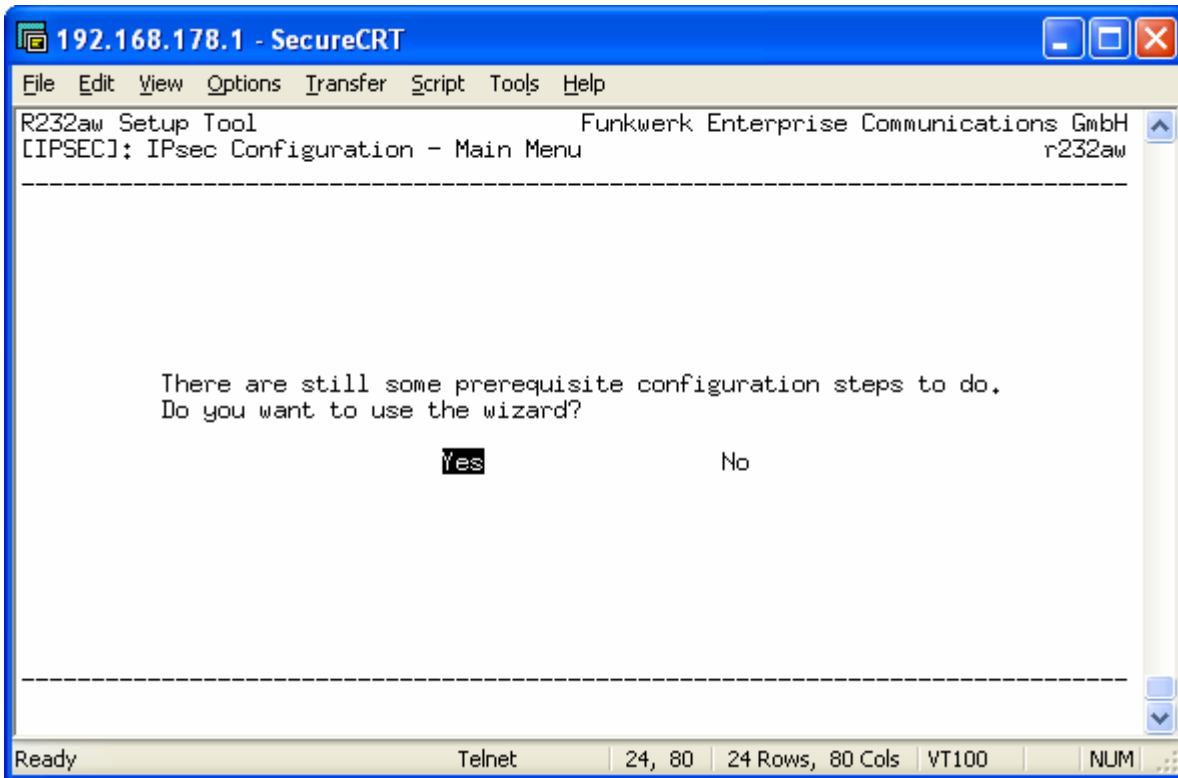
Ora vediamo l'esempio di una VPN con IPsec fra due router Bintec. Il disegno riassume la configurazione che andremo a realizzare.



Dal menù principale si SETUP si entra nel menù IPSEC.



Se è la prima volta che si configura una VPN sarà **necessario** eseguire il wizard il quale chiederà solo alcune informazioni, per altro modificabili in seguito. L'esecuzione del wizard è importante perché permette di creare i proposal e le regole di NAT. Vediamo come si presenta durante la configurazione del router della sede 1:



```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[IPSEC][WIZARD]: IPsec Configuration - Wizard Menu r232aw

-----

IPsec 1st step configurations wizard

Configuration History:
- for ESP: NULL AES Twofish Blowfish CAST DES DES3      ^
              MD5 SHA1 NOMAC                            |
- for AH:  SHA1 MD5                                     |
+ Check default IKE profile ...                          |
  default profile created                               |
+ Check default IPsec profile ...                        |
  default profile created                               |
+ Check IPSEC Default Authentication Method ...         |
  Currently set to "Pre Shared Keys"                   =

Use which Default IPSEC Authentication Method ?         current: PSK
                                                         (<Space> to choose)
                                                         (<Return> to select)

Exit

-----

Ready Telnet 18, 56 24 Rows, 80 Cols VT100 NUM
```

```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[IPSEC][WIZARD]: IPsec Configuration - Wizard Menu r232aw

-----

IPsec 1st step configurations wizard

Configuration History:
- for AH:  SHA1 MD5      ^
+ Check default IKE profile ... |
  default profile created |
+ Check default IPsec profile ... |
  default profile created |
+ Check IPSEC Default Authentication Method ... |
  Currently set to "Pre Shared Keys" |
+ Check IPSEC Default Local ID ... |
  Currently unconfigured |
                                                         =

Which Local ID should be used for IPsec ?             x1200 II_test
                                                         (<Space> to choose)
                                                         (<Return> to select)

Exit

-----

Ready Telnet 18, 69 24 Rows, 80 Cols VT100 NUM
```

```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[IPSEC][WIZARD]: IPsec Configuration - Wizard Menu r232aw

-----

IPsec 1st step configurations wizard

Configuration History:
+ Check pre- and post-IPsec rules ... ^
  Pre-IPsec rule list now initialised to rule for passing IKE Traffic |
+ Check Global Default Rule ... |
  Global Default Rule is changed to "pass" |
! CAUTION: |
  Brick now prepared for IPsec enabled standard router. |
  Further configuration is required for an IPsec only router! |
+ Check for Peer ... |
  IPSEC enabled =

Configure Peer ? start
                  (<Space> to choose)
                  (<Return> to select)

Exit

-----

Ready Telnet 18, 56 24 Rows, 80 Cols VT100 NUM
```

```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[IPSEC][WIZARD][PEER]: IPsec Wizard - Configure Peer r232aw

-----

Description: verso_sede_2
Admin Status: up

Peer Address: test2.dyndns.org
Peer IDs: vpn25_test
Pre Shared Key: ****

IPSec Callback: no

Virtual Interface: yes

SAVE CANCEL

-----

Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM
```

```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[IPSEC][WIZARD]: IPsec Configuration - Wizard Menu r232aw

-----

IPsec 1st step configurations wizard

Configuration History:
! CAUTION:
  Brick now prepared for IPsec enabled standard router.
  Further configuration is required for an IPsec only router!
+ Check for Peer ...
  IPSEC enabled
  Pre Shared Key now set
  IPSEC already enabled
+ Check for ISDN Callback configuration ...
+ Check for Peer Virtual interface ...

Configure Virtual interface ?
                                start
                                (<Space> to choose)
                                (<Return> to select)

                                Exit

-----
Use <Space> to select
```

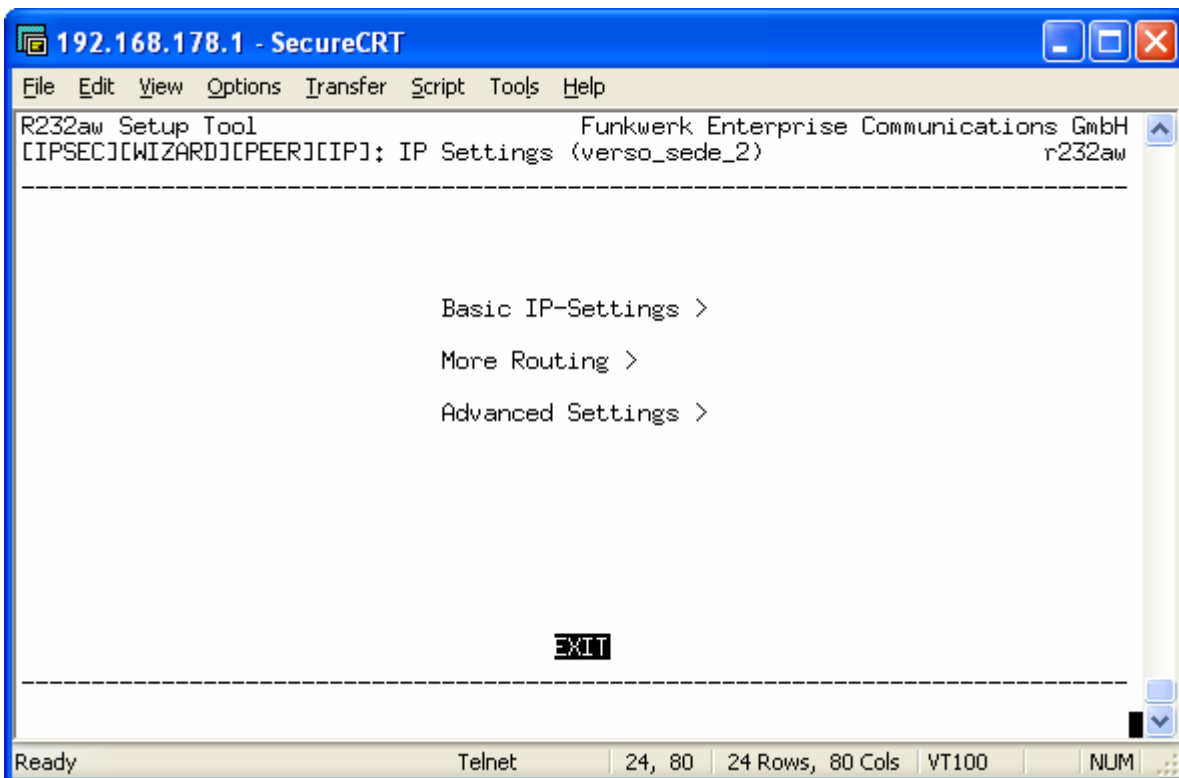
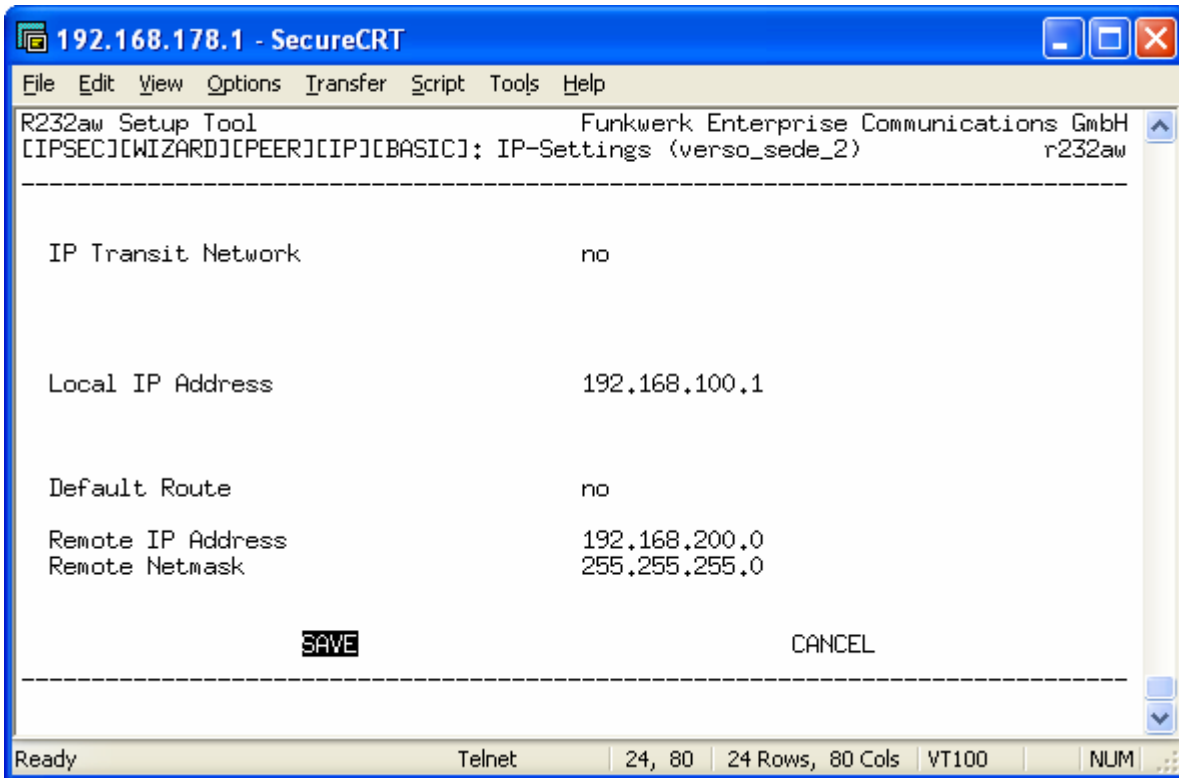
```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[IPSEC][WIZARD][PEER][IP]: IP Settings (verso_sede_2) r232aw

-----

Basic IP-Settings >
More Routing >
Advanced Settings >

EXIT

-----
```



```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[IPSEC][WIZARD]: IPsec Configuration - Wizard Menu r232aw

-----

IPsec 1st step configurations wizard

Configuration History:
+ Check for Peer ... ^
  IPSEC enabled |
  Pre Shared Key now set |
  IPSEC already enabled |
+ Check for ISDN Callback configuration ... |
+ Check for Peer Virtual interface ... |
  Virtual interface now configured |
+ Check for Peer Traffic ... |
= IPsec Wizard finished = =

What to do? clear config
(create syslog messages for configuration history) (<Space> to choose)
                                                    (<Return> to select)

Exit

-----
Use <Space> to choose <Return> to select
```

```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[IPSEC]: IPsec Configuration - Main Menu r232aw

-----

Enable IPsec : yes

Configure Peers >

IKE (Phase 1) Defaults *autogenerated* edit >
IPsec (Phase 2) Defaults *autogenerated* edit >
Certificate and Key Management >

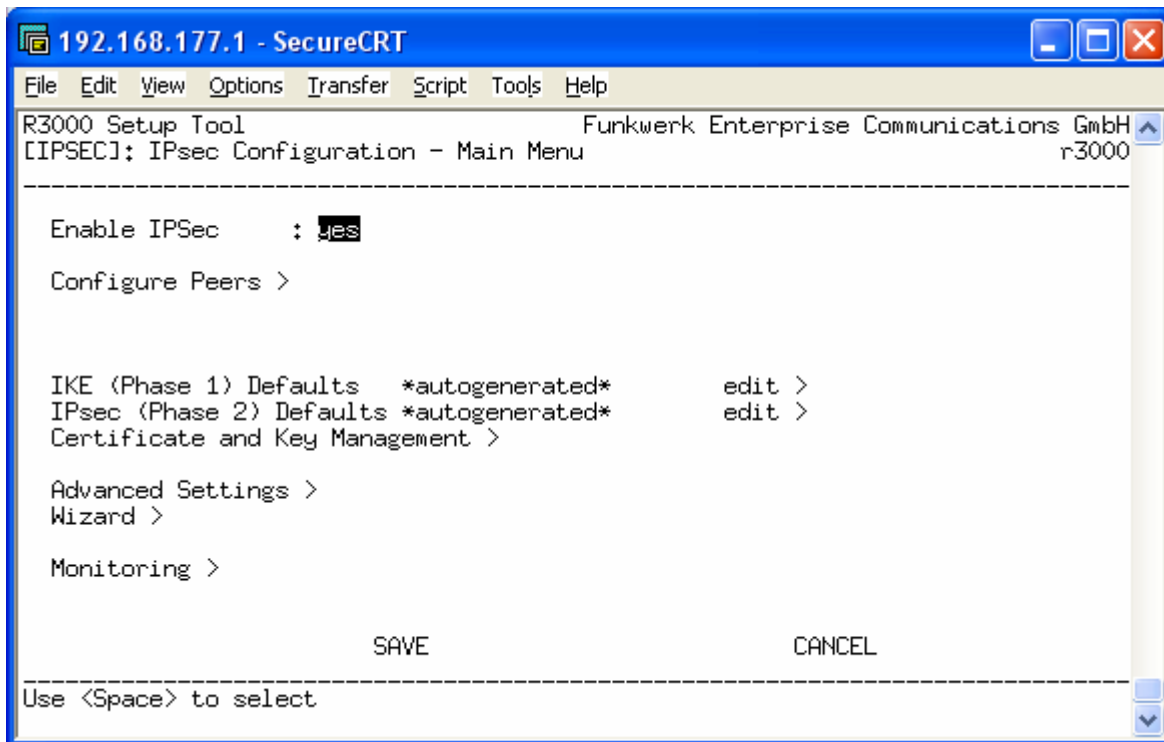
Advanced Settings >
Wizard >

Monitoring >

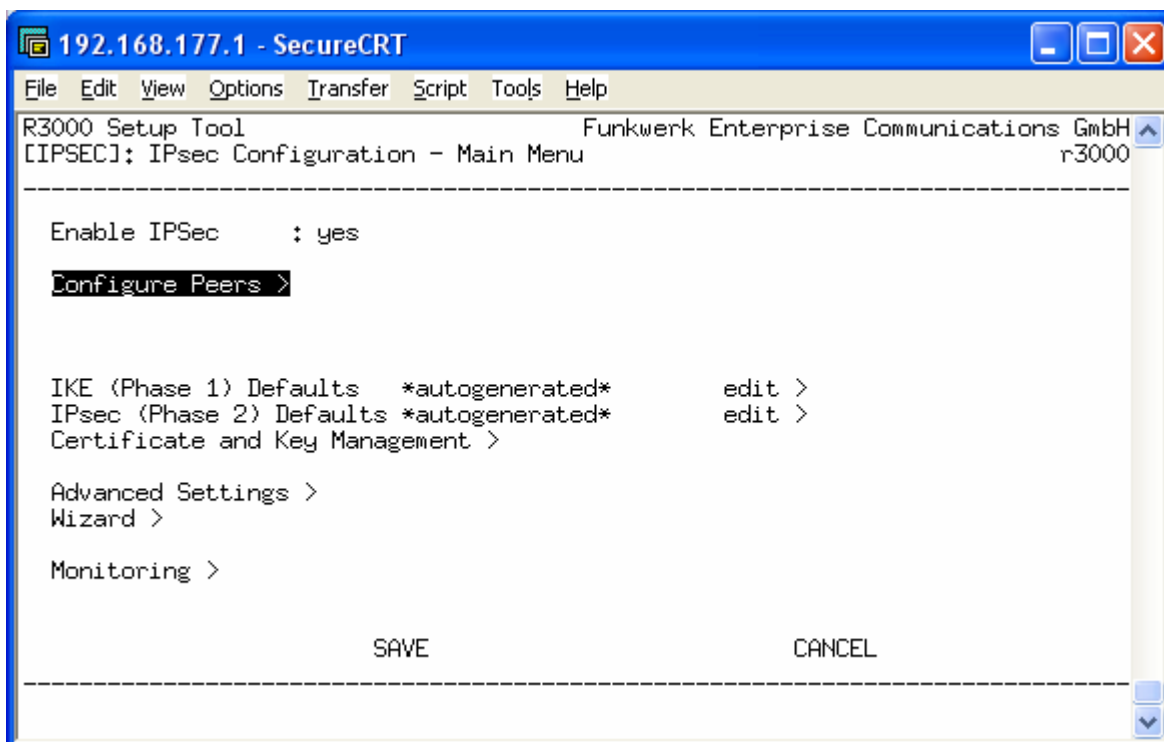
SAVE CANCEL

-----
```

Supponendo di aver già eseguito il wizard vediamo come deve essere impostata una VPN in modo dettagliato.



Come mostrato in figura è necessario abilitare l'IPSec. Dal menù Configure Peers è possibile impostare le caratteristiche dell'END-POINT remoto; sarà quindi possibile definirne l'IP pubblico, la rete privata e le fasi di autenticazione.



Il wizard avrà creato una entry nella tabella seguente. Questa riga indica una connessione VPN e lo stato della connessione stessa (in questo caso dormant). Editando questa connessione andiamo a modificarne i parametri.

```

192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[PEERS]: IPsec Configuration - Configure Peer List r232aw

-----
Highlight an entry and type "I" to insert new entry below,
"U"/"D" to move up/down, "M" to monitor, "PSCEAFT" to change sorting.

State desCription pEerid peerAddress proFile Traffic
dorm verso_sede_2 vpn25_test test2.dyndns.org 1 0

APPEND DELETE REORG EXIT

-----
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit
Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM

```

```

192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[PEERS][EDIT]: Configure Peer r232aw

-----
Description: verso_sede_2
Admin Status: up

Peer Address: test2.dyndns.org
Peer IDs: vpn25_test
Pre Shared Key: *

IPSec Callback >
Peer specific Settings >

Virtual Interface: yes
Interface IP Settings >

SAVE CANCEL

-----
Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM

```

Per prima cosa dobbiamo assegnare un nome identificativo alla connessione; questo nome non ha alcuna rilevanza ai fini del funzionamento ma serve a noi per distinguere le varie connessioni.

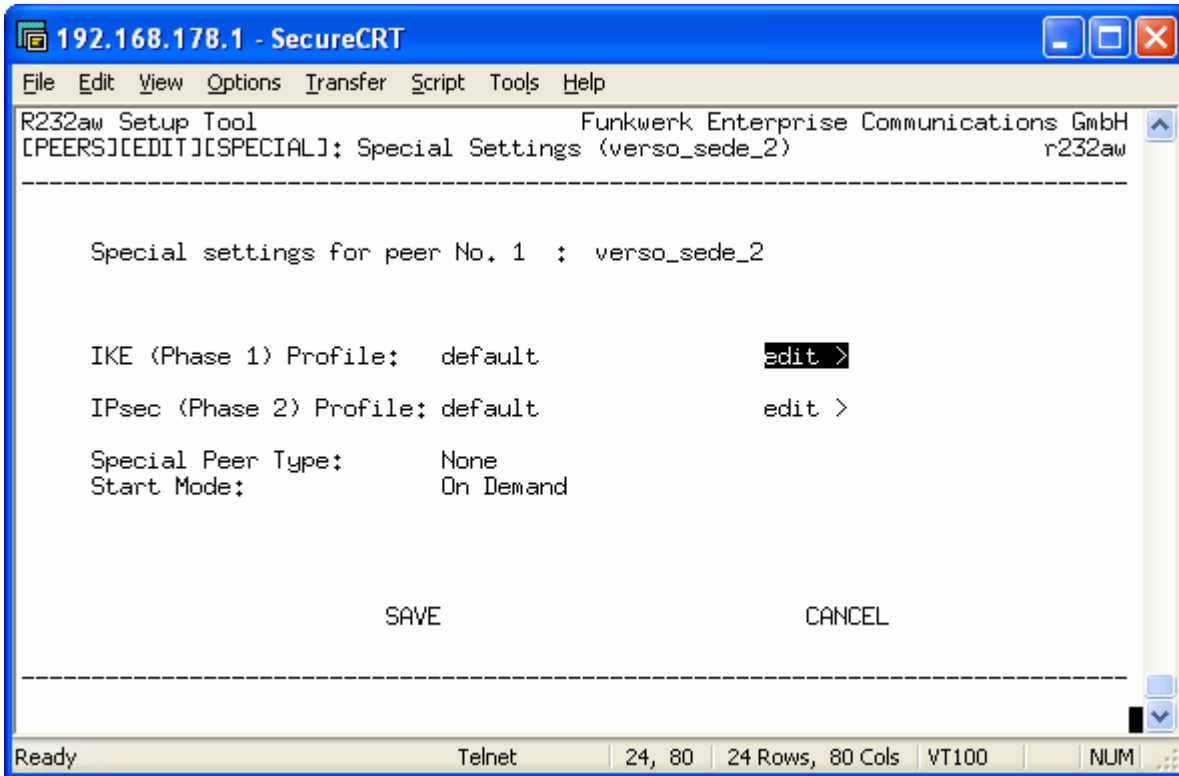
L'*Admin Status* deve essere impostato su *up*.

Il *Peer Address* non è altro che l'indirizzo pubblico dell'end-point remoto. Possiamo definire un indirizzo IP oppure un nome di dominio (es. nome.dyndnd.org).

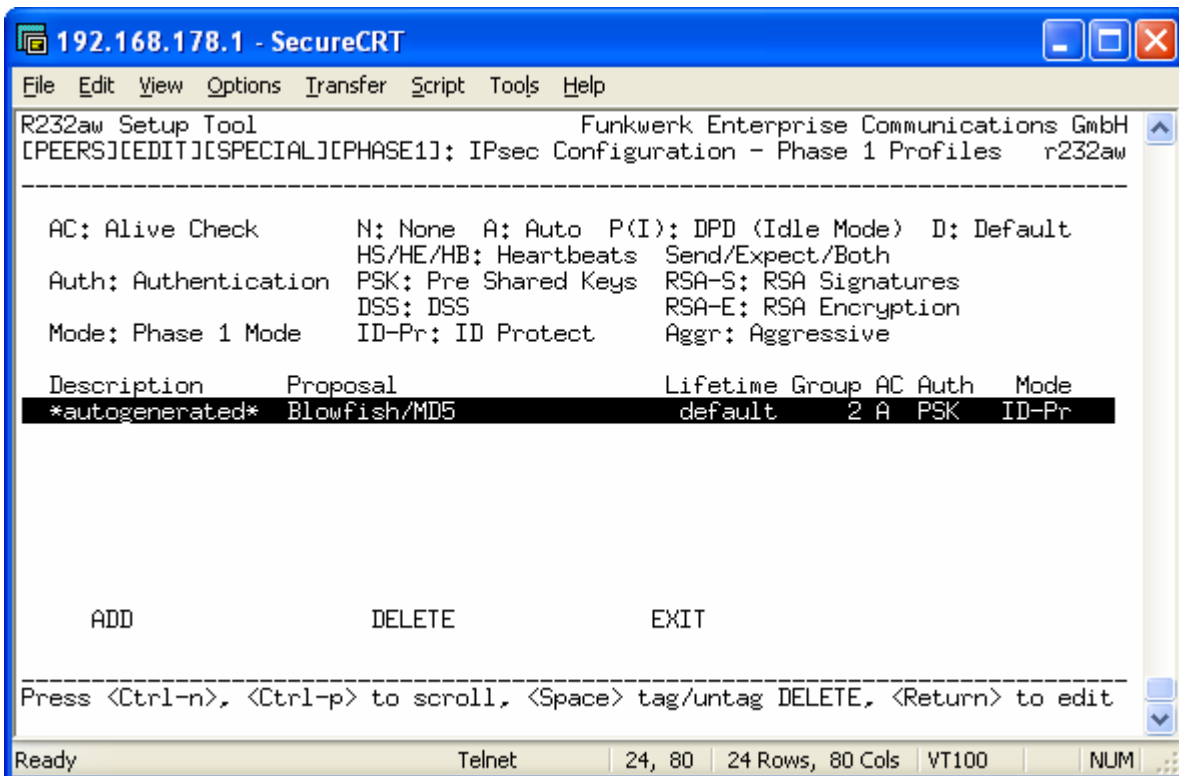
Il *Peer IDs* invece è il nome identificativo dell'end-point remoto; è importante scrivere in modo preciso questo nome in quanto sarà utilizzato dall'algorithmo crittografico per generare la chiave.

La *Pre Shared Key* invece è la password che i due end-points si scambieranno perciò deve essere uguale su entrambi gli end-point.

Entrando nel menù *Peer specific Settings* si possono impostare le fasi di autenticazione.



La prima fase (IKE) serve per l'autenticazione e lo scambio delle chiavi segrete. Editando la prima fase si ottiene una tabella nella quale sono riportate tutte le possibili modalità di autenticazione che abbiamo impostato.



Nel nostro caso dovrebbe esserci una sola riga chiamata "Default" oppure "*autogenerated*" creata dal wizard. Editando questa riga impostiamo i valori a seconda delle nostre esigenze:

```
R232aw Setup Tool                               Funkwerk Enterprise Communications GmbH
[PEERS][EDIT][SPECIAL][PHASE1][EDIT]          r232aw

-----
Description (Idx 1) :   *autogenerated*
Proposal               :   1 (Blowfish/MD5)
Lifetime Policy       :   Use default lifetime settings

Group                 :   2 (1024 bit MODP)
Authentication Method :   Pre Shared Keys
Mode                  :   id_protect
Alive Check           :   autodetect
Block Time            :   0
Local ID              :   X1200 II_test
Local Certificate     :   none
CA Certificates       :
Nat-Traversal         :   enabled

View Proposals >

                               SAVE                               CANCEL

-----
Enter string, max length = 255 chars

Ready                               Telnet                               5, 29   24 Rows, 80 Cols   VT100   NUM
```

Description: è un nome identificativo per riconoscere la modalità di autenticazione della prima fase.

Proposal: indica i protocolli utilizzati di cifratura; la lista completa de protocolli supportati è visualizzabile alla voce *View Proposals*

Lifetime Policy: permette di settare la durata e la lunghezza delle chiavi di autenticazione

Group: permette di settare la lunghezza in bit della cifratura

Authentication Method: permette di settare il metodo di scambio delle chiavi. Fra le varie possibilità esistono Pre Shared Key (PSK), RSA e DSA (certificati).

Mode: permette di decidere la modalità di autenticazione. Fra le possibili modalità vanno sottolineate l'Aggressive mode e l'ID-Protect mode (main mode). Il primo modo è più veloce ma meno sicuro; viene utilizzato quando si utilizzano indirizzi IP pubblici dinamici o DynDNS.

Alive Check: serve a verificare la presenza del peer.

Block Time: permette di specificare la durata di inattività della connessione. Scaduto questo tempo la connessione cade. Se si imposta il valore -1 si indica una connessione sempre attiva.

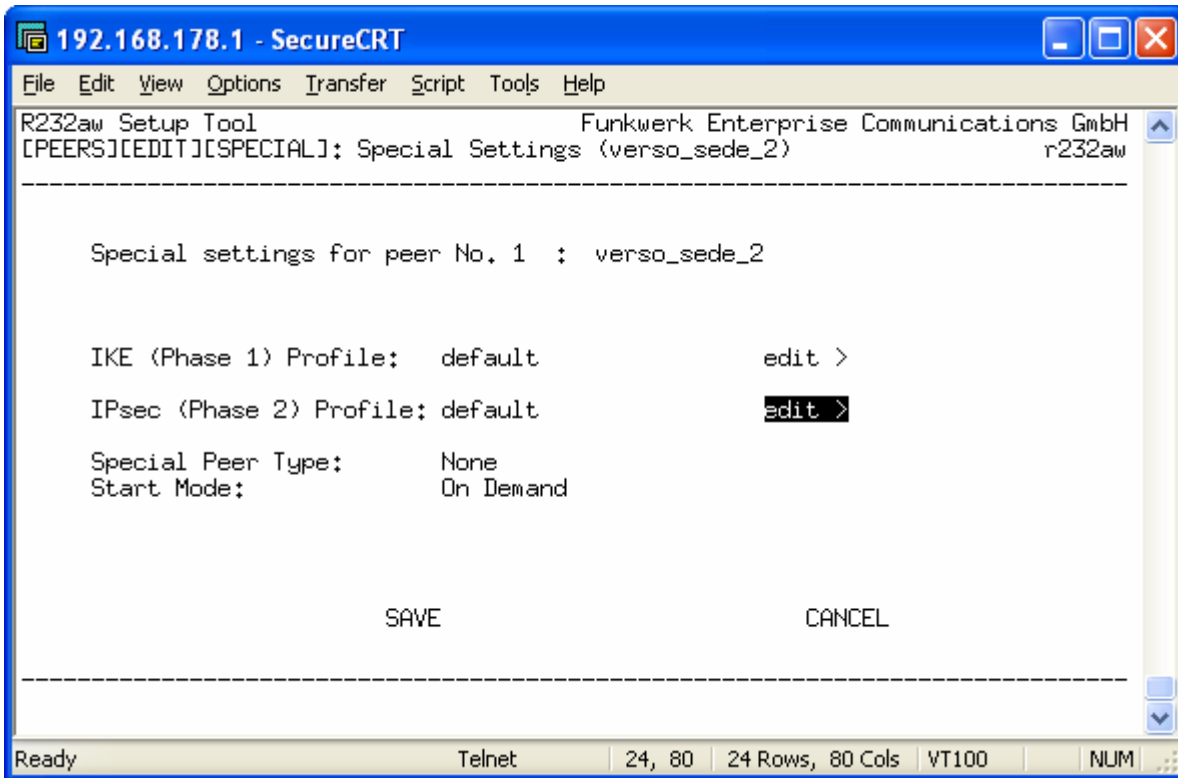
Local ID: rappresenta l'identificativo dell'END-POINT locale.

Local Certificate: permette di indicare il certificato per lo scambio delle chiavi

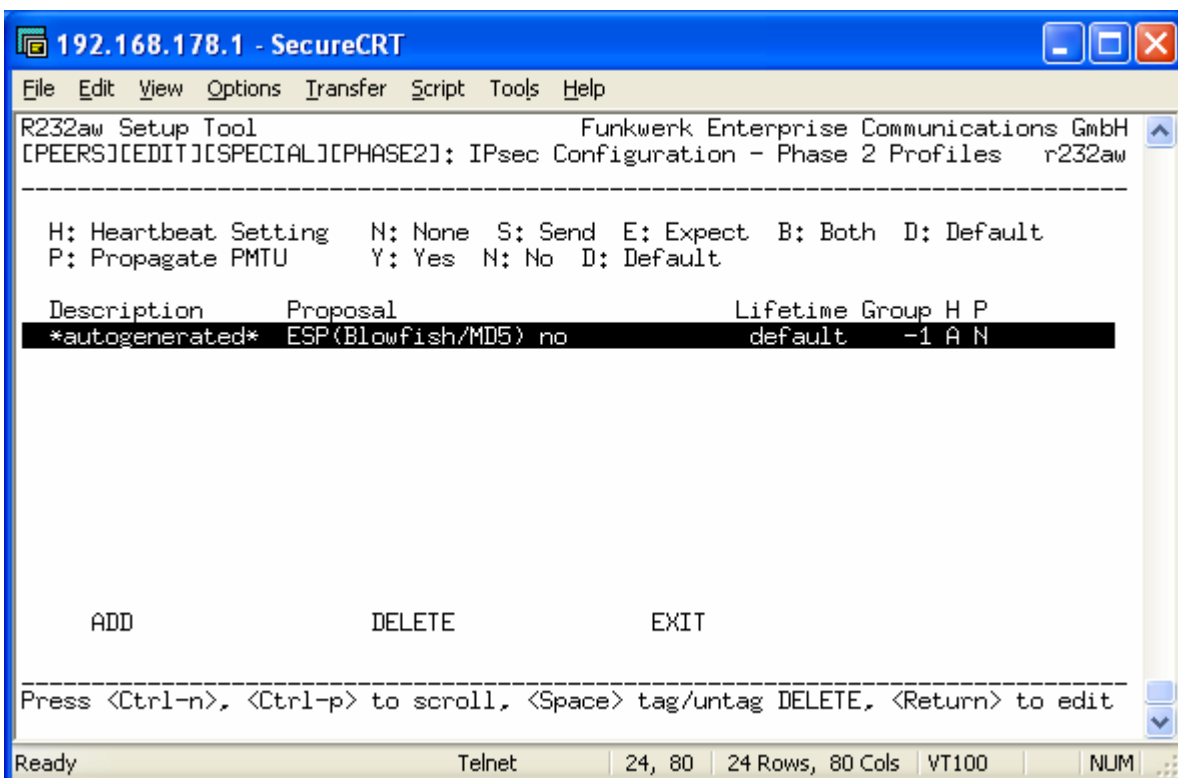
CA Certificates: è l'autorità che garantisce la veridicità del certificato

Nat-Traversal: da attivare nel caso in cui il router si trovi sotto al NAT di un altro apparato.

Passiamo ora alla fase 2.



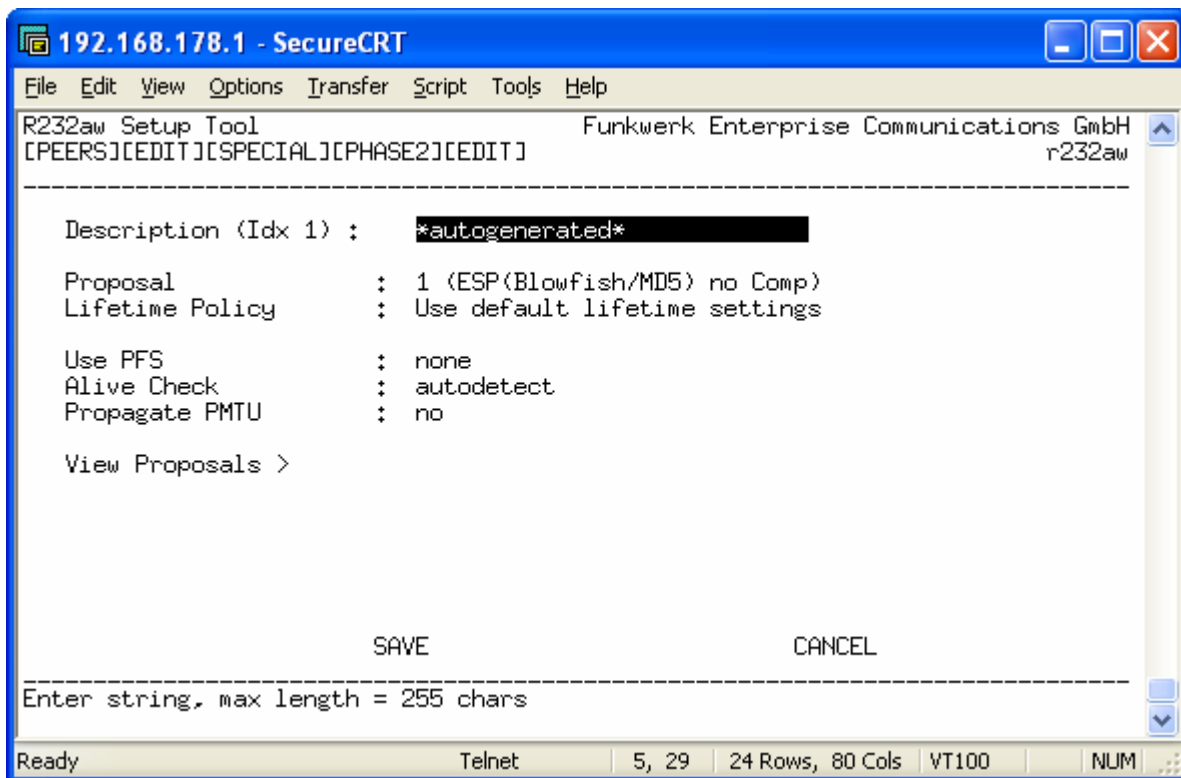
Anche in questo caso compare una tabella con una sola entry creata dal wizard. Editiamola.



La seconda fase (IPSec) serve per la cifratura dei dati al fine di rendere confidenziale lo scambio di informazioni. Esistono due protocolli di cifratura: AH e ESP.

AH protegge l'integrità del datagramma IP e calcola un HMAC del pacchetto in base ad una chiave segreta, al payload e le parti del header IP che non possono cambiare (ad esempio i campi con gli indirizzi IP). Quindi aggiunge l'header AH all'header del pacchetto.

Il protocollo ESP può garantire sia l'integrità di un pacchetto utilizzando HMAC sia la confidenzialità della trasmissione utilizzando la cifratura. Dopo aver cifrato il pacchetto e calcolato l'HMAC viene generato ed aggiunto l'header ESP.



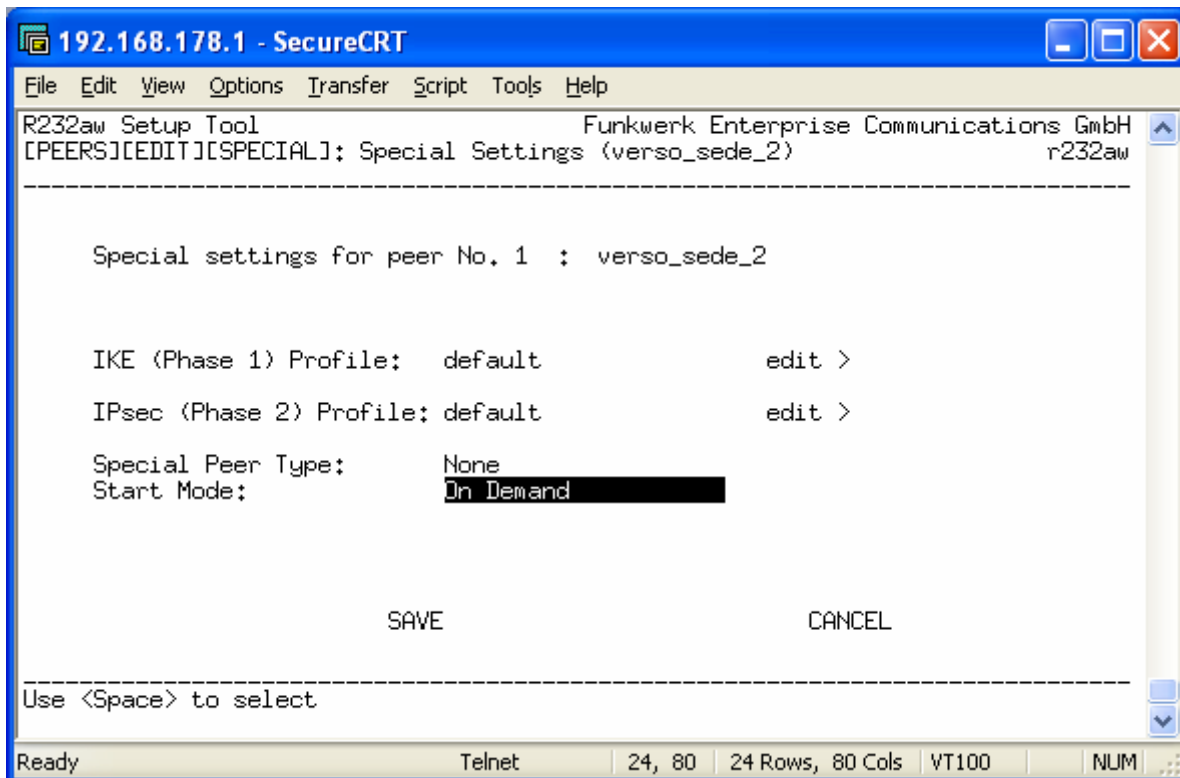
Description: è un nome identificativo per riconoscere la modalità di cifratura della seconda fase.

Proposal: indica la modalità di cifratura (ESP o AH) e l'eventuale supporto per la compressione
Lifetime Policy: indica il tempo di vita e la dimensione delle chiavi

Use PFS: indica la dimensione della sliding windows per proteggersi contro i *retry attacks*

Alive Check: serve a verificare la presenza del peer.

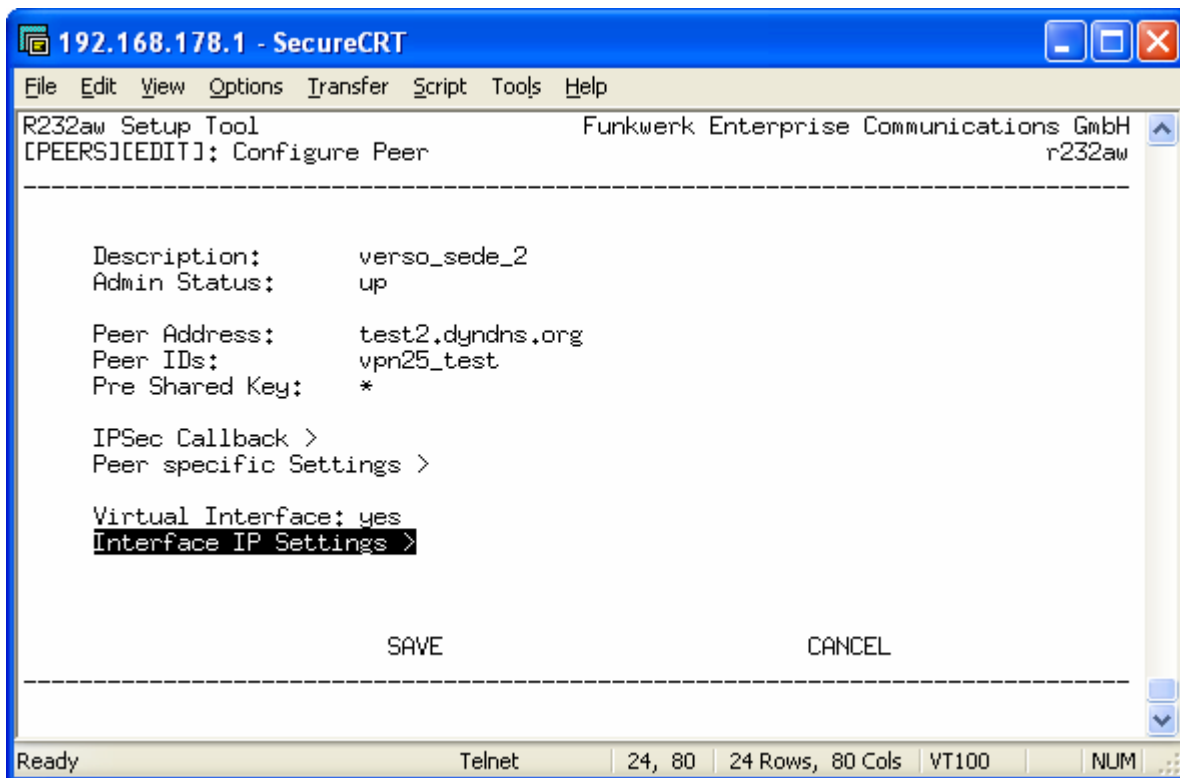
Propagate PMTU: il protocollo PMTU (Path MTU) serve per scoprire la grandezza massima dei pacchetti che possono transitare attraverso la VPN.

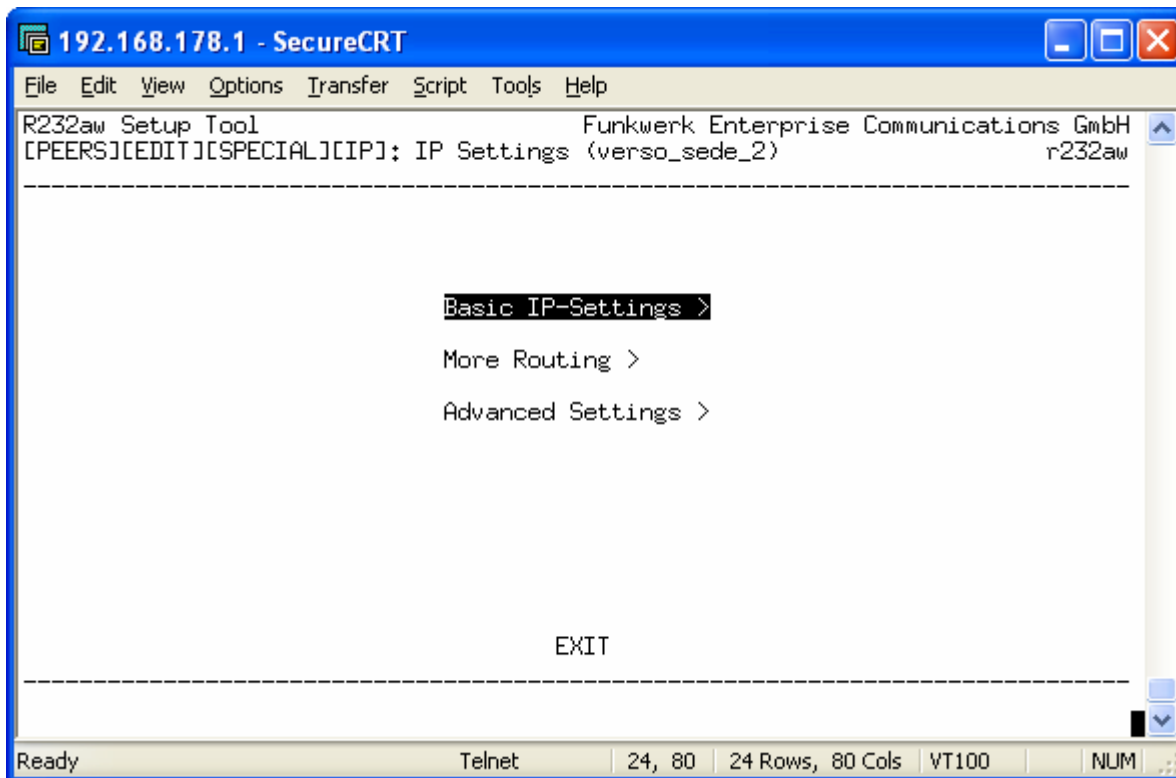


Special Peer Type: specificando Dynamic Client è possibile assegnare un indirizzo IP al client remoto; per poter assegnare un indirizzo è indispensabile aver creato prima il pool nel menù IP → IP Address Pool.

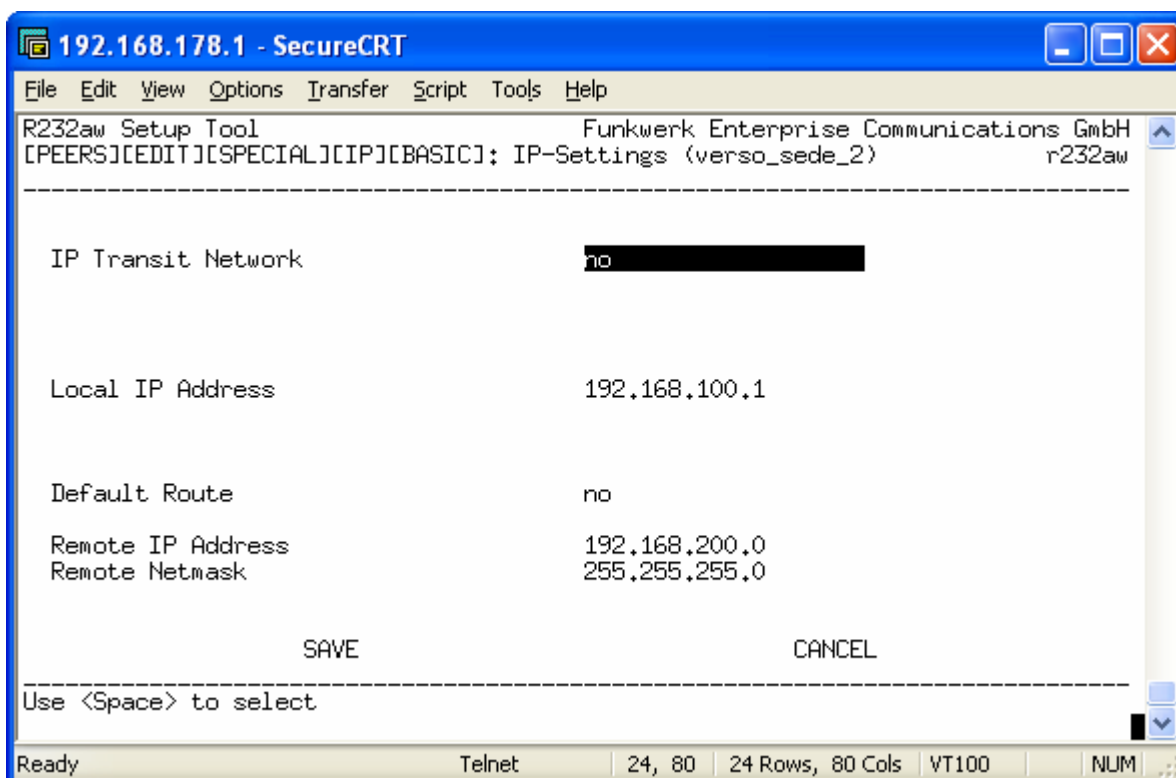
Start Mode: permette di specificare se creare il tunnel VPN solo in presenza di traffico tra le due sedi (On Demand) oppure in modo permanente (Always Up)

Alla voce *Virtual Interface* assegnamo il valore *yes* ed andiamo nel menù *Interface IP Setting*.





Dal menù *Basic IP-Settings* andiamo a configurare le reti private che devono essere collegate in VPN.



In questo caso il *Local IP Address* rappresenta l'indirizzo privato dell'END-POINT locale (router) mentre il *remote IP Address* rappresenta l'indirizzo della rete che si vuole raggiungere (es. 192.168.200.0/24). E' importante che le due reti private abbiano classi di indirizzamento diverse (es. 192.168.100.0 e 192.168.200.0).

Se impostiamo il valore di *Default Route* a *yes* significa che tutte le richieste verso una rete diversa da quella locale saranno inoltrate attraverso il tunnel VPN. Questa opzione è utile nel caso in cui vogliamo accedere ad internet sfruttando una connessione che si trova dall'altro lato del tunnel.

Ora la configurazione della sede 1 è completata. Configurando allo stesso modo il router remoto potremo avviare la connessione VPN. E' importante che le password (Pre Shared Key) e le fasi di autenticazione (IKE e IPSec) siano uguali nei due END-POINTS altrimenti non sarà possibile completare la fase di autenticazione.

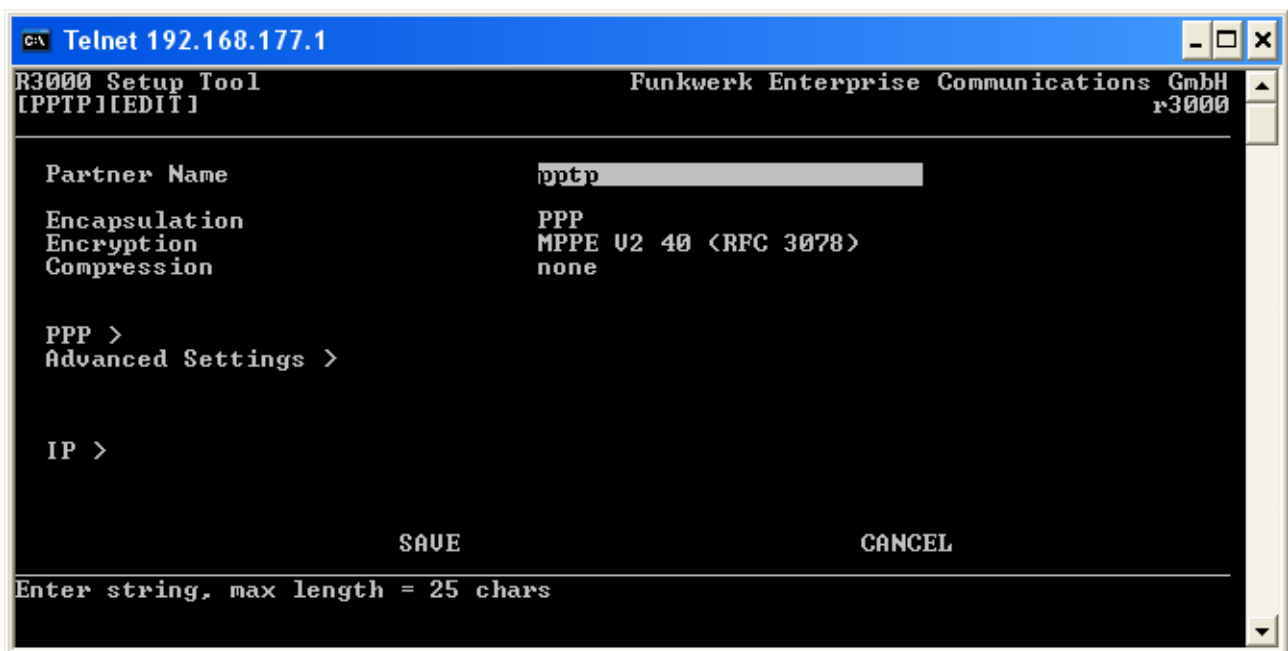
Nel caso di indirizzi pubblici dinamici bisogna ricordarsi di configurare l'account di DynDNS come descritto nel paragrafo seguente.

Configurazione di un tunnel PPTP

PPTP, acronimo di **Point to Point Tunneling Protocol**, è un protocollo di rete che attraverso la cifratura dei dati rende sicure la trasmissione in una rete privata, che utilizza VPN, su una rete pubblica. Il PPTP è stato sviluppato da Microsoft; assicura autenticazione, cifratura e compressione dei dati. Lavora in collaborazione al protocollo di livello trasporto GRE (Generic Routing Encapsulation).

I router Bintec che supportano questo protocollo sono: R23x(w), R1200(w), R1200wu, R3000(w), R3400, R3800, R4100, R4300.

Entrando in configurazione via telnet, accedere al menù di *setup* -> *PPTP* e creare una nuova configurazione con *ADD*.



Partner Name: specificare il nome della connessione

Encapsulation: PPP

Encryption: MPPE V2 40 (RFC 3078). L'importante è che sia specificato RFC 3078

Compression: none

Entrare nel menù *PPP*

```

c:\ Telnet 192.168.177.1
R3000 Setup Tool                               Funkwerk Enterprise Communications GmbH
[PPTP][EDIT][PPP]: PPP Settings <pptp>        r3000

Authentication                               MS-CHAP V2
Partner PPP ID                               prova_pptp
Local PPP ID                                 prova_pptp
PPP Password                                 *****
MS Domain
Keepalives                                   off
Link Quality Monitoring                       off

OK                                             CANCEL

Use <Space> to select

```

Authentication: MS-CHAP V2
Partner PPP ID: specificare un nominativo per il partner
Local PPP ID: non è indispensabile
PPP Password: specificare una password

In *Advanced Settings* specificare:

```

c:\ Telnet 62.123.203.199
R3000 Setup Tool                               Funkwerk Enterprise Communications GmbH
[PPTP][EDIT][ADVANCED]: Advanced Settings <Nord_Est 9000 PPTP> r3000

Callback                                     10
Static Short Hold <sec>                     -1

Delay after Connection Failure <sec>        10
PPTP Mode                                    PPTP PNS

Extended Interface Settings <optional> >

Special Interface Types                       none

OK                                             CANCEL

Use <Space> to select

```

Static Short Hold (sec): -1
PPTP Mode: PPTP PNS (in questo modo il router resta in attesa di una richiesta PPTP)

In *Basic IP Settings* specificare:

```

C:\ Telnet 62.123.203.199
R3000 Setup Tool                               Funkwerk Enterprise Communications GmbH
[PPTP][EDIT][IP][BASIC]: IP-Settings <Nord_Est 9000 PPTP>      r3000

Dynamic PPTP UPN                               no
Identification by IP Address                   no
PPTP UPN Partner's IP Address

IP Address Negotiation                         dynamic server

SAVE                                           CANCEL

Use <Space> to select

```

Dynamic PPTP VPN: no
IP Address Negotiation: dynamic server

Dal menù *setup* -> *IP* -> *IP Address pool* creare un nuovo pool di indirizzi.

```

C:\ Telnet 192.168.177.1
R3000 Setup Tool                               Funkwerk Enterprise Communications GmbH
[IP][DYNAMIC][POOL][EDIT]: Define Range of IP Addresses      r3000

Identifier                                     0
Description                                    WAN
IP Address                                     10.10.10.10
Number of Consecutive Addresses               3
Primary Domain Name Server                   0.0.0.0
Secondary Domain Name Server                 0.0.0.0

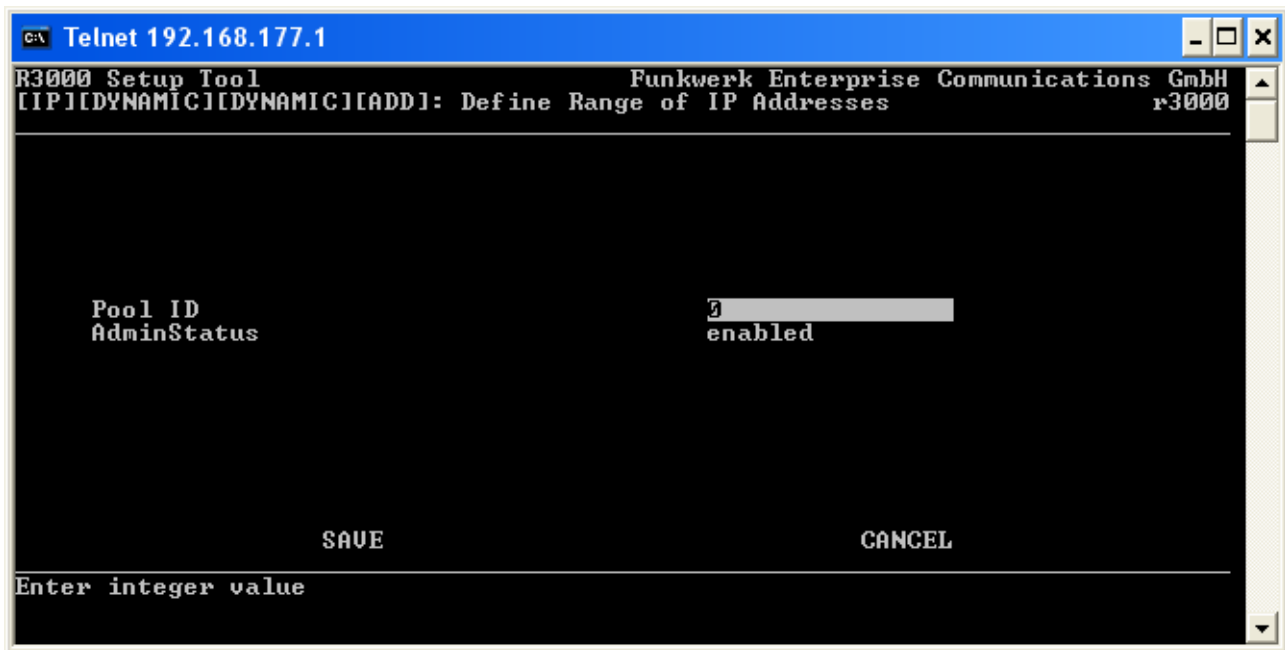
SAVE                                           CANCEL

Enter integer value

```

Pool ID: identificativo del pool di indirizzi
IP Address: indirizzo IP di partenza da assegnare dinamicamente (Importante: deve essere diverso da quello assegnato sulla parte LAN)
Number of consecutive addresses: numero massimo di indirizzi assegnabili consecutivamente a partire da quello di partenza.

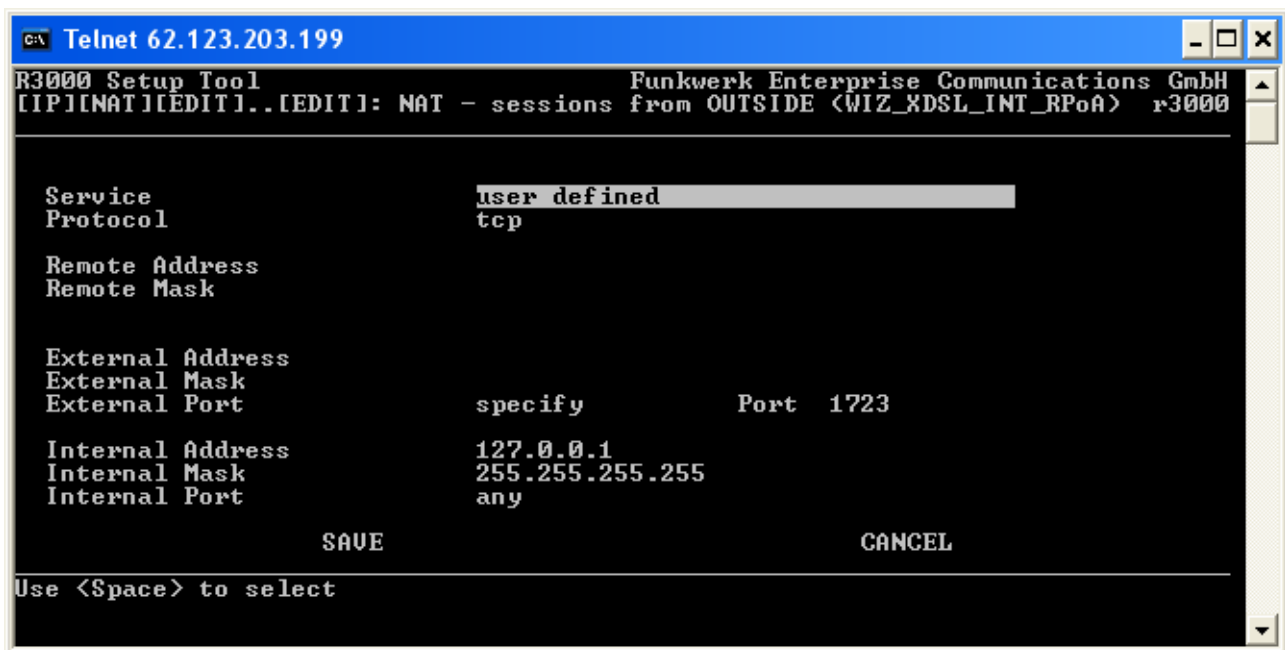
Dal menù *IP Address Pool WAN (PPP)* abilitare il pool creato. E' importante utilizzare l'ID impostato nel punto precedente (in questo esempio l'ID è 0).



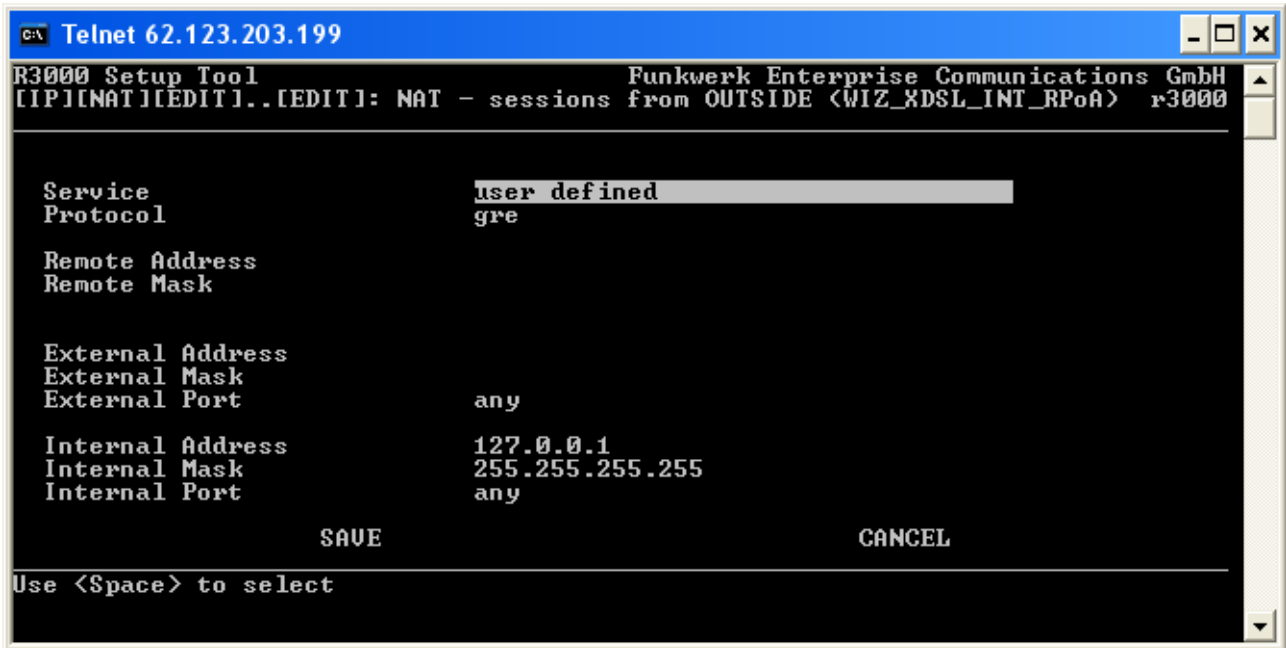
In questo modo la tabella di routing verrà aggiornata istantaneamente appena si stabilisce una connessione PPTP.

Dal *menù setup -> IP -> Network Address Translation* sull'interfaccia internet dobbiamo andare a specificare 2 nuove regole di NAT su *requested from OUTSIDE*.

abilitare la porta 1723 tcp (porta utilizzata per l'autenticazione)

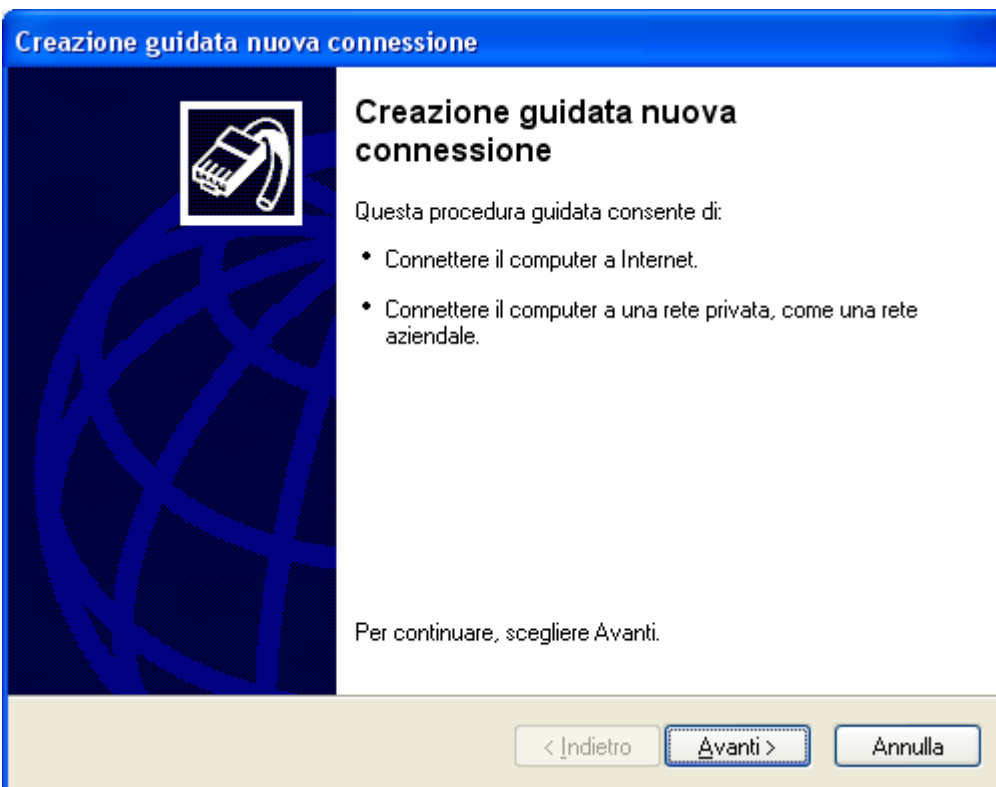


abilitare il protocollo GRE (protocollo per l'incapsulamento)

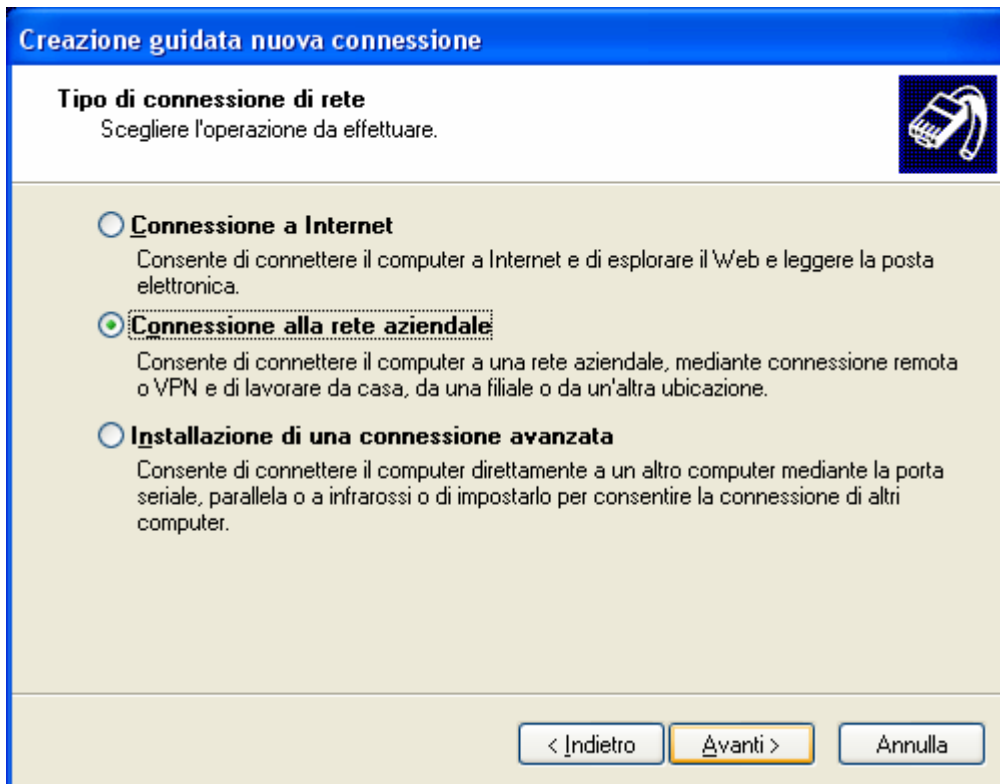


Per quanto riguarda il lato client dobbiamo eseguire le seguenti istruzioni da un PC Windows.

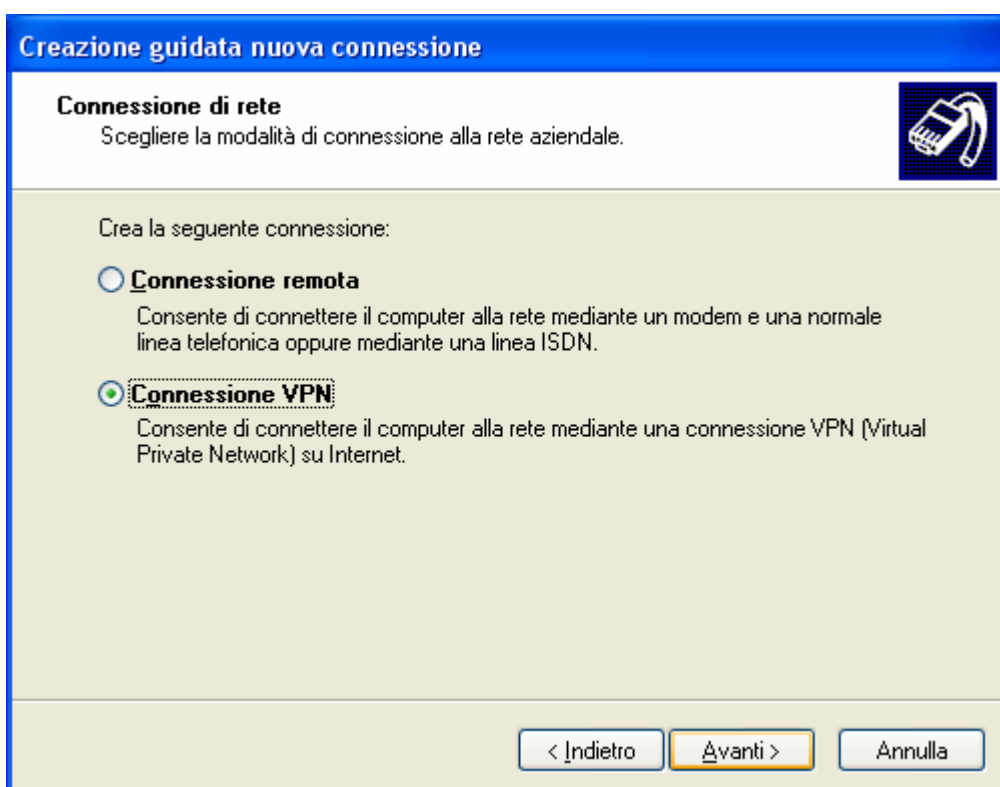
Dal menù *start* -> *connessione di rete* -> *crea una nuova connessione*



Selezionare *connessione alla rete aziendale*



Selezionare *Connessione VPN*



Specificare un nome da attribuire alla connessione

Creazione guidata nuova connessione

Nome connessione
Specificare un nome per la connessione alla rete aziendale.

Immettere un nome per la connessione nella seguente casella.

Nome società

Connessione_PPTP

Ad esempio, è possibile immettere il nome della rete aziendale o del server a cui si effettuerà la connessione.

< Indietro Avanti > Annulla

Specificare l'indirizzo IP pubblico

Creazione guidata nuova connessione

Selezione server VPN
Indicare il nome o l'indirizzo del server VPN.

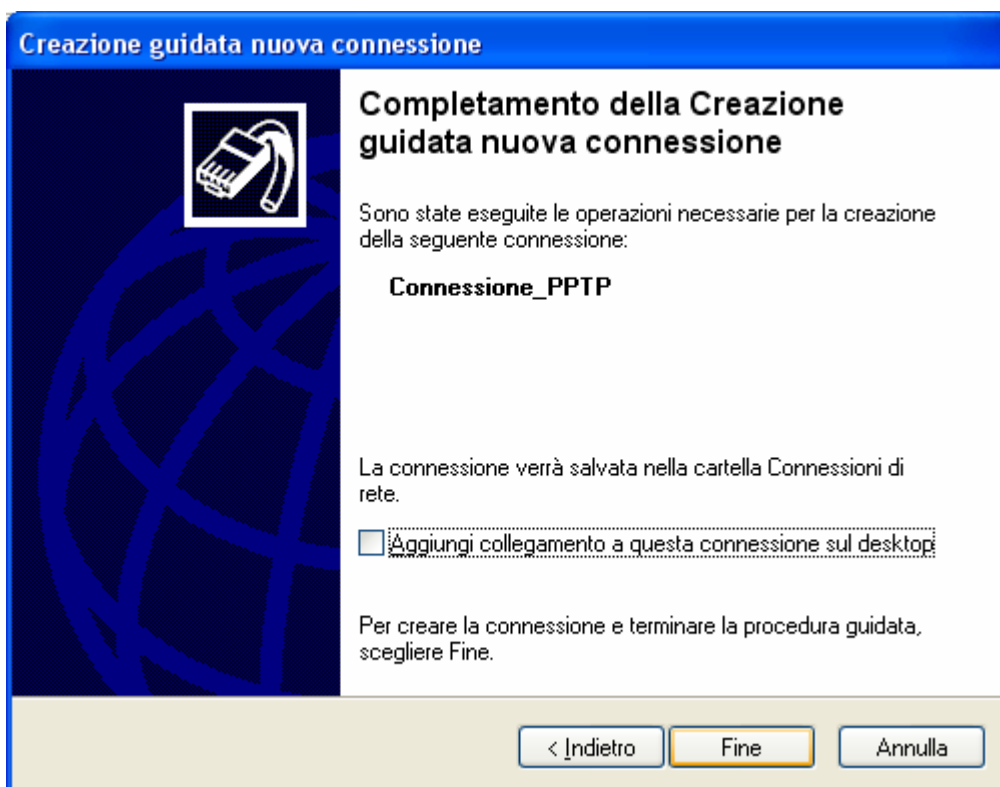
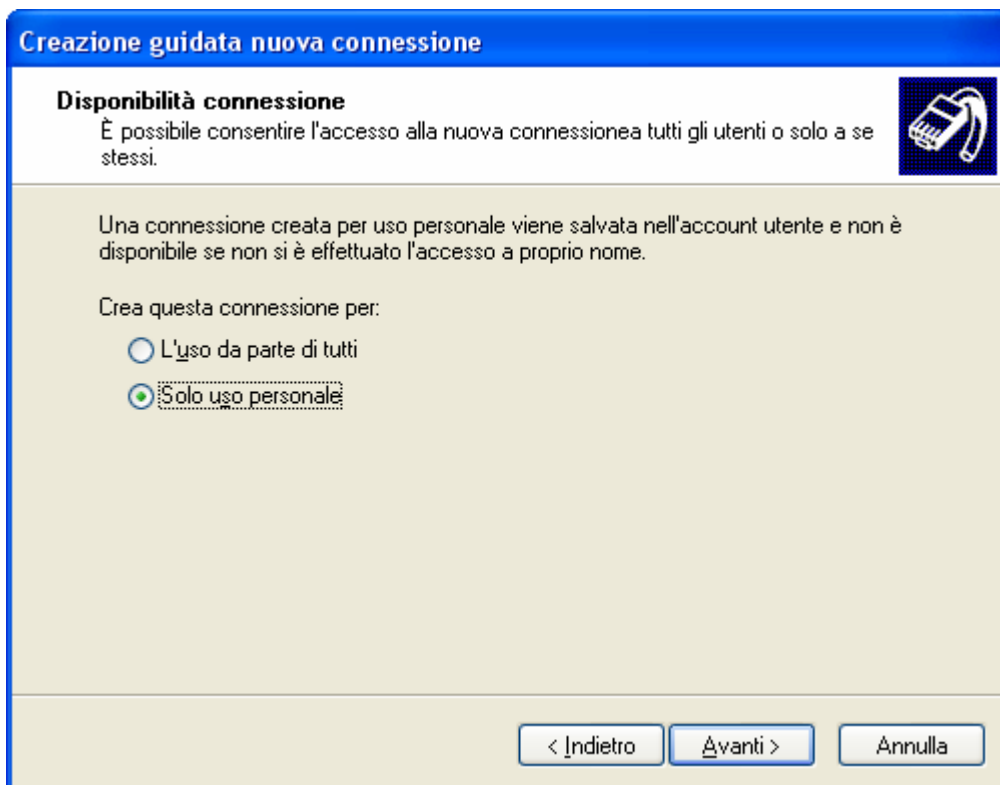
Digitare il nome host o l'indirizzo IP del protocollo internet del computer a cui si sta effettuando la connessione.

Nome host o indirizzo IP (ad esempio microsoft.com o 157.54.0.1):

88.26.35.154

< Indietro Avanti > Annulla

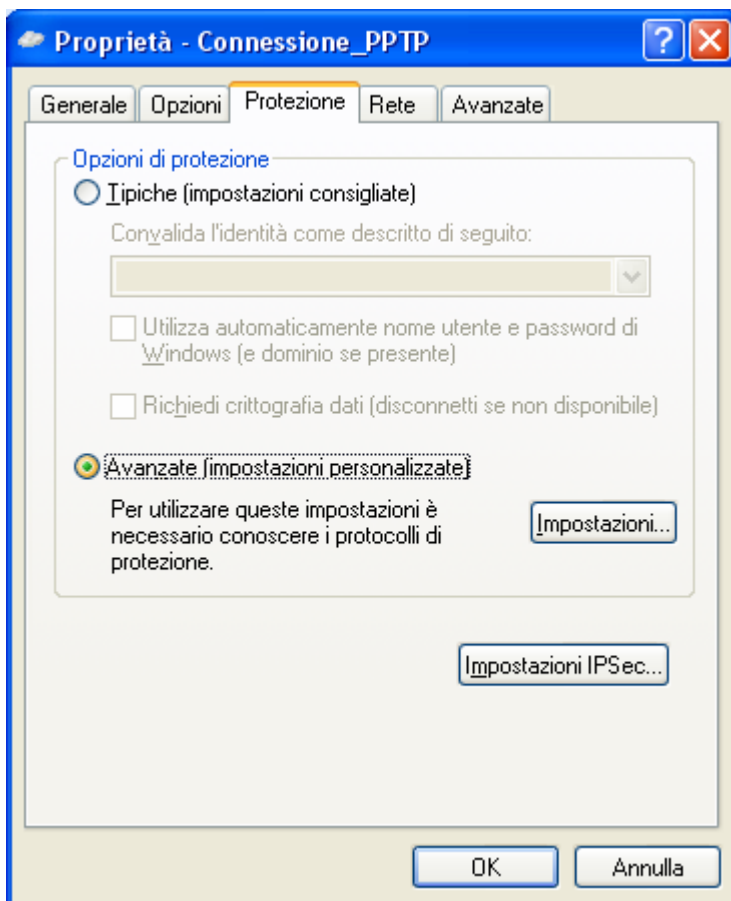
Selezionare Solo uso personale



Specificare User Name e Password indicati nel router.



Entrare nel menù proprietà della connessione creata (tasto destro del mouse) e scegliere Avanzate



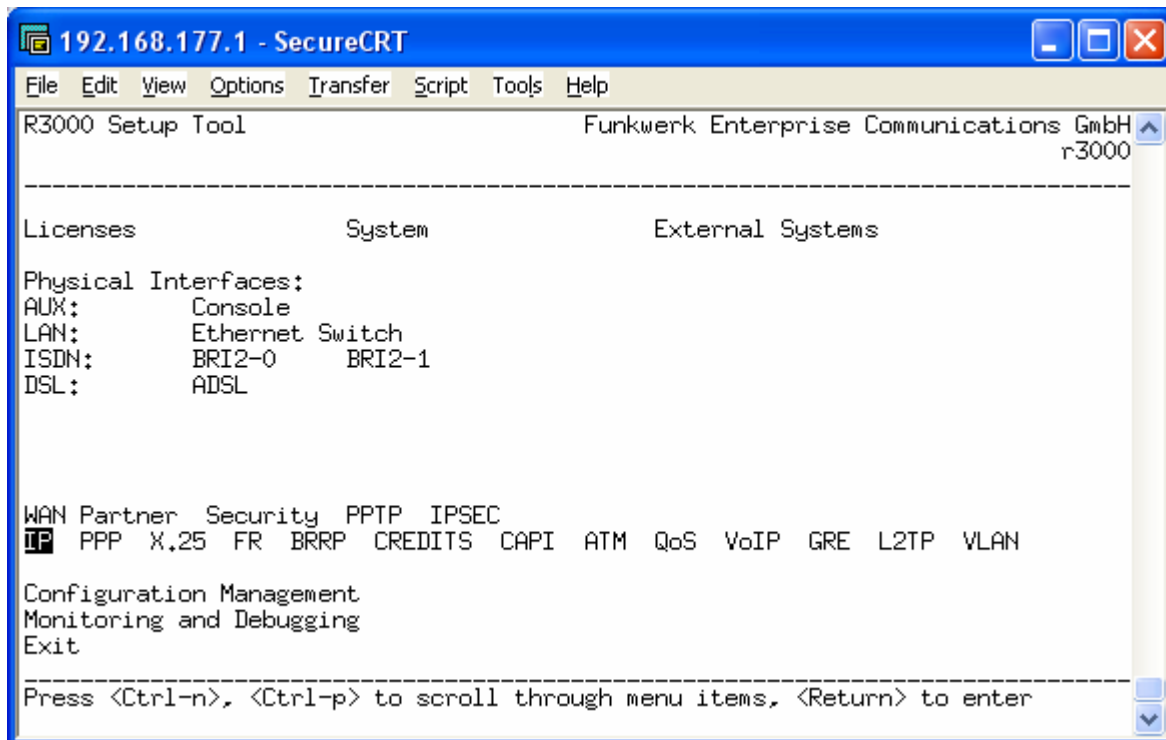
Confermare a avviare la connessione.

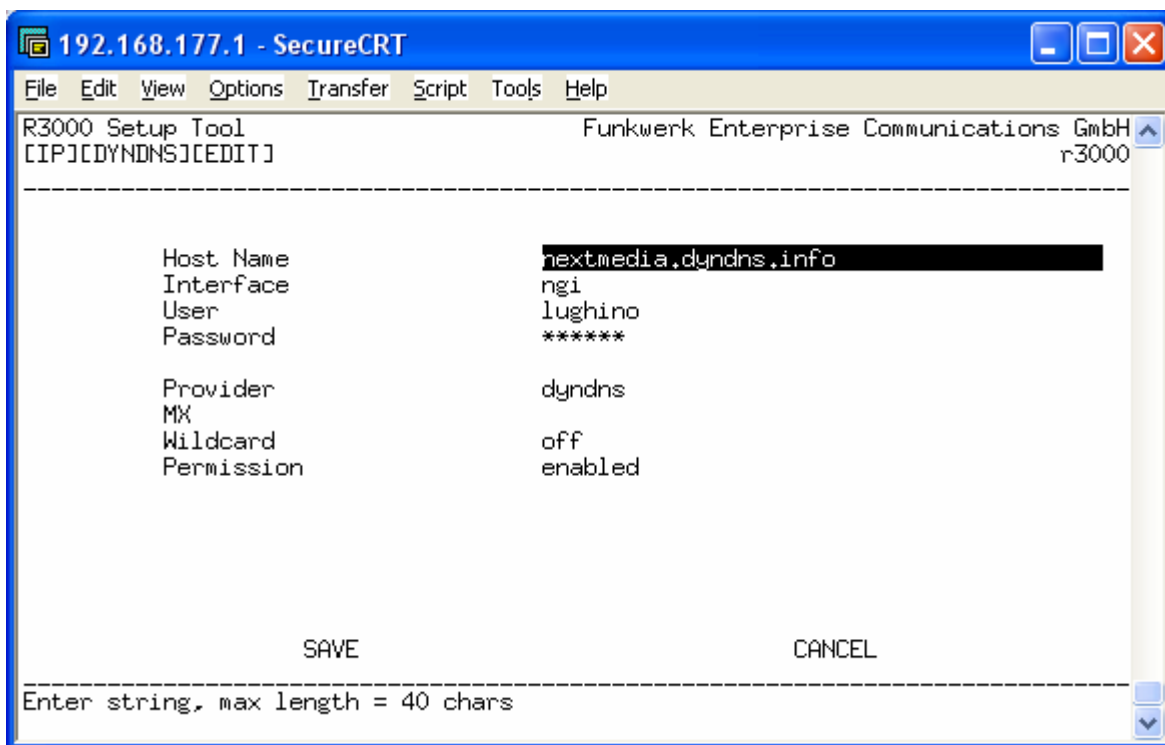
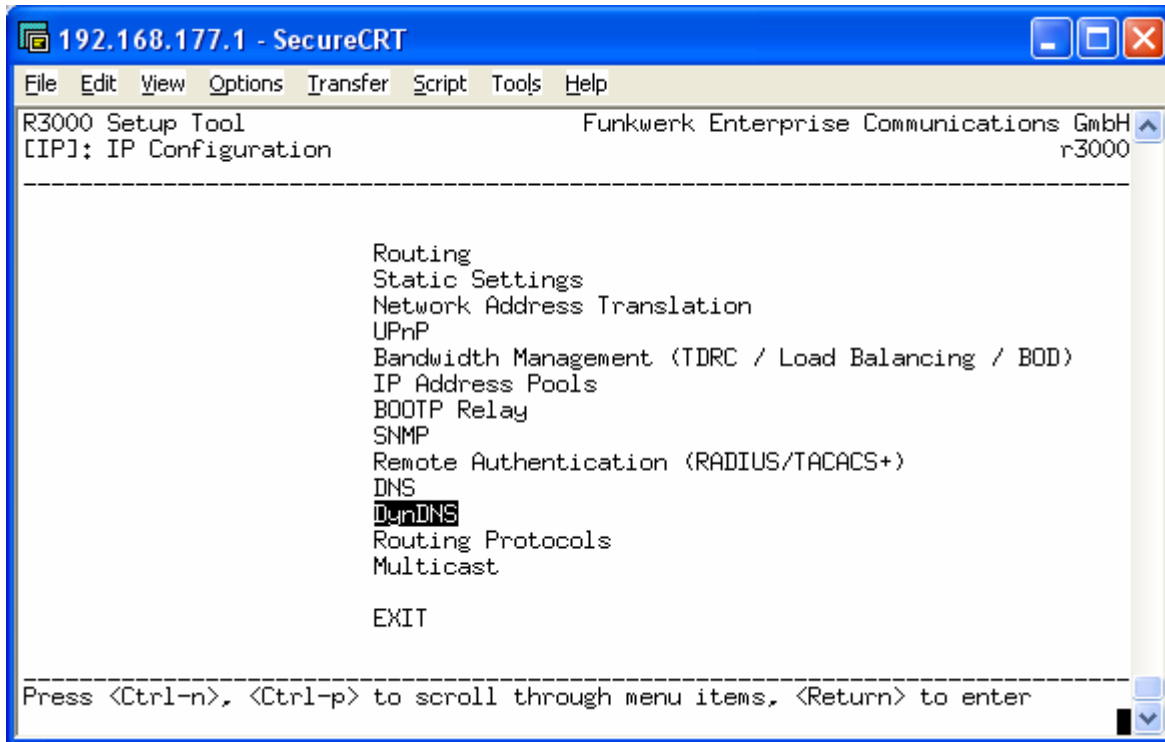
Configurazione DynDNS

Se il nostro Provider ADSL ci fornisce un indirizzo IP dinamico diventa difficile raggiungere il router da remoto perché ad ogni nuova connessione ADSL l'indirizzo pubblico sarà differente; è però possibile aggirare il problema sfruttando un account di DNS dinamico. Il router Bintec è in grado di aggiornare il nome di dominio registrato con i più importanti gestori di DNS dinamici. Per prima cosa occorre registrare un account presso uno dei seguenti gestori:

members.dyndns.org
update.ods.org
dup.hn.org
www.dyns.cx
www.orgdns.org
carol.selfhost.de
dnupdate.no-ip.com

A questo punto è possibile inserire nella maschera i dati relativi all'account appena registrato. Pennerà poi il router ad aggiornare il nome di dominio con l'indirizzo IP pubblico acquisito durante il collegamento ADSL.





Host Name: è il nome di dominio scelto in fase di registrazione

Interface: è l'interfaccia che dispone di un IP dinamico

User: è il nome utente scelto in fase di registrazione

Password: è la password scelta in fase di registrazione

Provider: è il provider che ci fornisce l'account

MX: se il provider ci fornisce anche un Mail eXchange possiamo configurarlo qui

Wildcard: se il nome di dominio che abbiamo scelto contiene caratteri speciali (_~\$%* etc...)

Permission: per consentire l'aggiornamento dell'indirizzo IP

```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R3000 Setup Tool Funkwerk Enterprise Communications GmbH
[CIP][DYNDNS]: Dynamic DNS Service r3000
-----
DynDNS Services:

Host Name          Interface      Permission    State
nextmedia.dyndns.info  ngi           enabled       up-to-date

DynDNS Provider List>
      ADD           DELETE        EXIT

-----
Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit
```

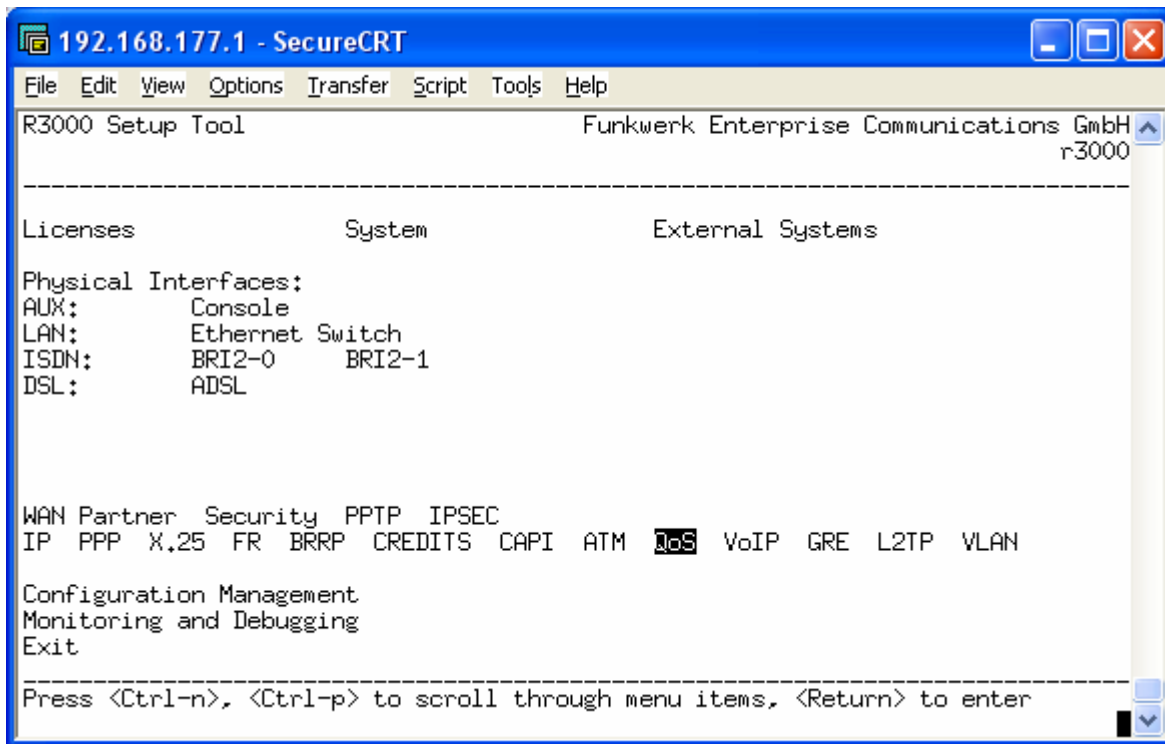
Configurazione QoS (Quality of Service)

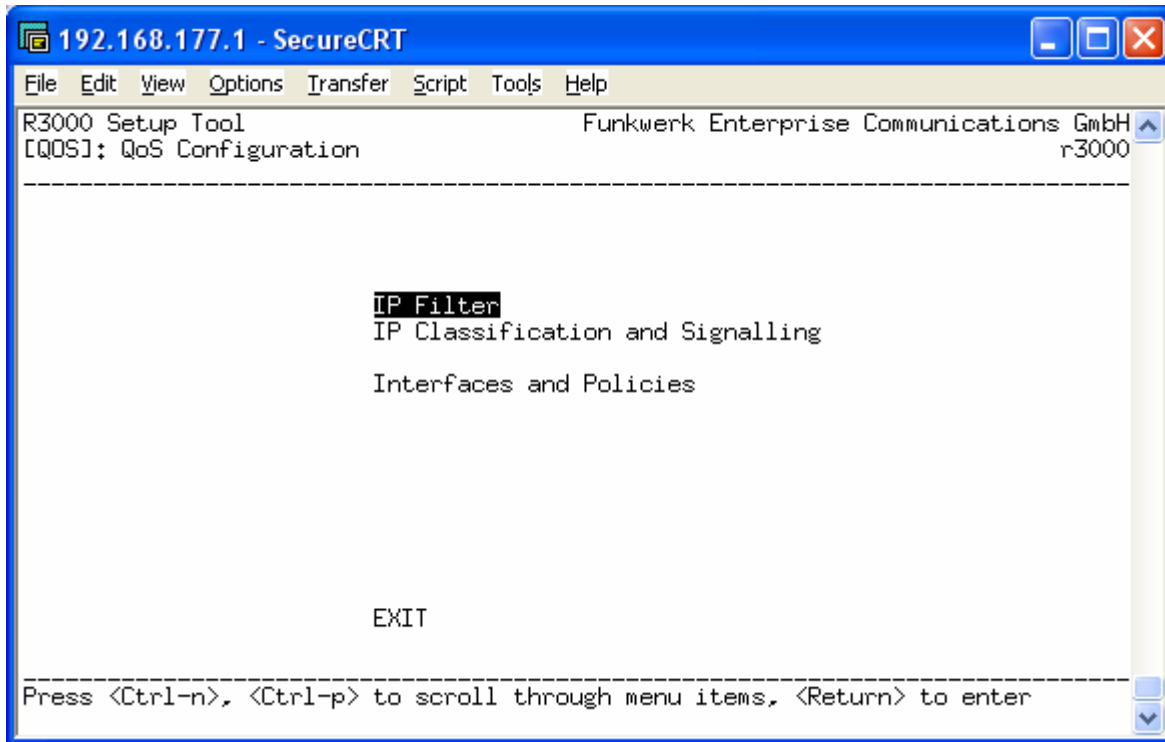
Ci sono diversi modi per fare QoS. Il più semplice è definito “High Priority” e consiste nell’individuare i pacchetti che devono essere trasmessi prima di tutti gli altri.

Per individuare i pacchetti prioritari possiamo effettuare un controllo sugli IP sorgenti/destinazione, sul protocollo oppure sul campo ToS (Type of Service).

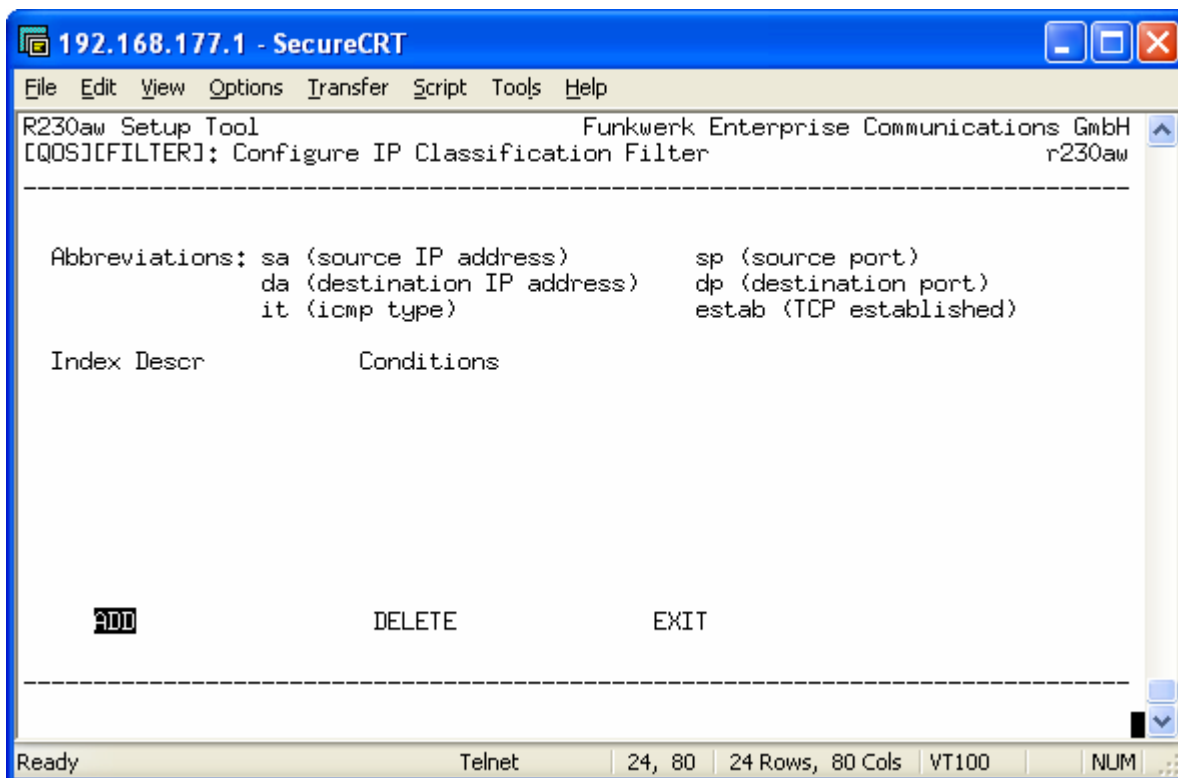
All’interno della nostra rete abbiamo la possibilità di settare alcune macchine (es. telefoni SIP) in modo da marcare tutti i pacchetti da esse generati con un valore prestabilito (es. 160). In questo modo il router che si vede recapitare i pacchetti ha la possibilità di riconoscerli e farli passare per primi.

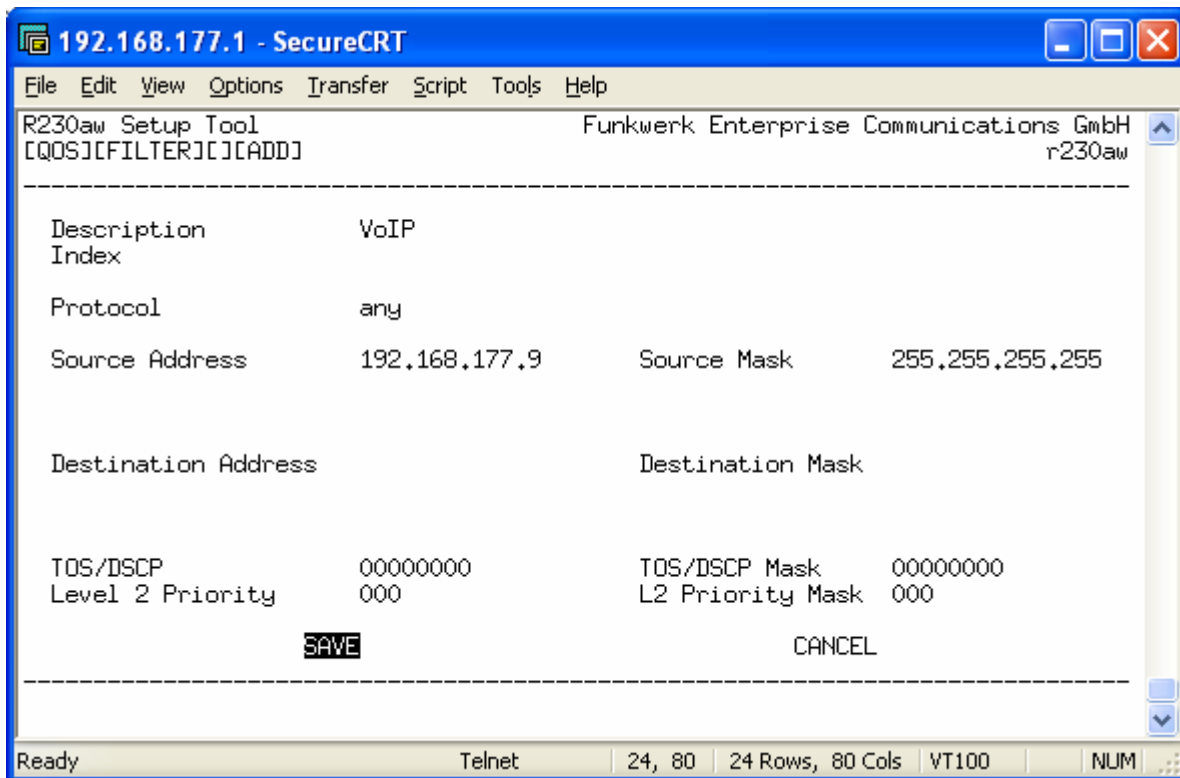
Si può anche effettuare il controllo sull’indirizzo IP sorgente; in questo esempio si va a settare la priorità ai pacchetti che hanno come sorgente l’indirizzo IP del centralino



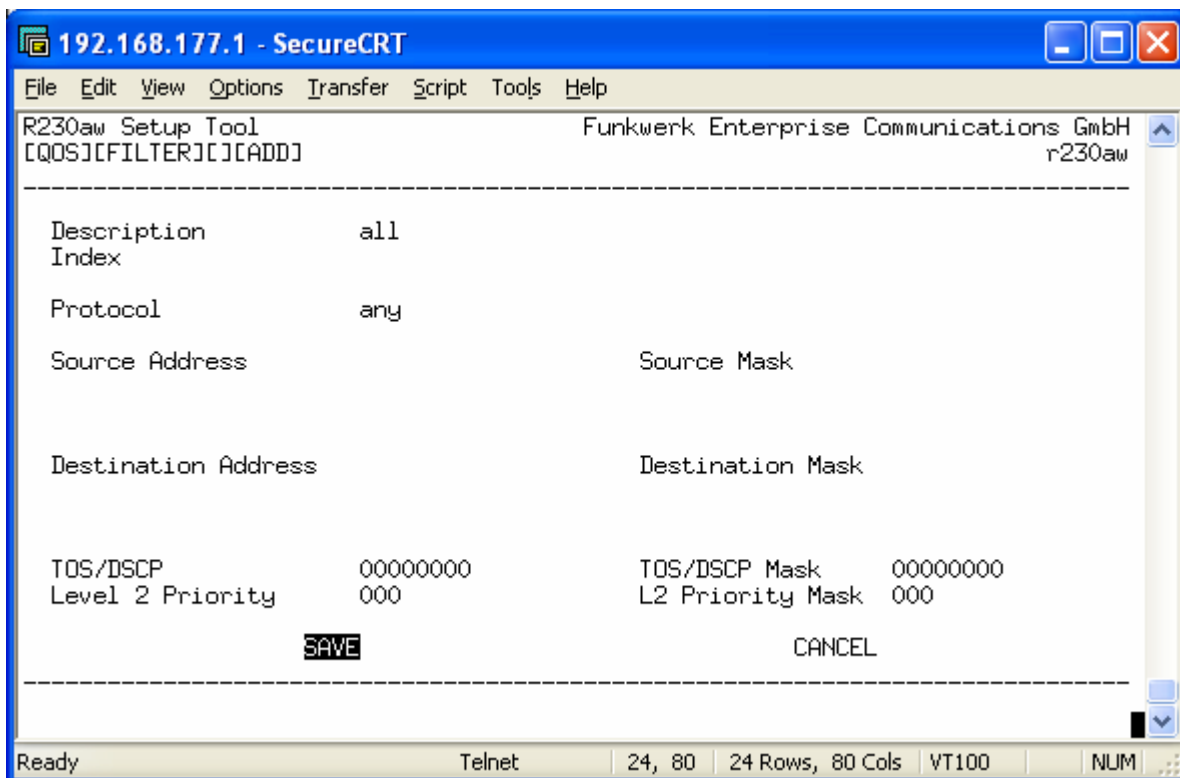


Aggiungiamo due nuove filtri: uno per trovare i pacchetti generati dal centralino e uno per tutti gli altri.





In questo caso abbiamo specificato come indirizzo IP sorgente solo quello del centralino 192.168.0.20



Il secondo filtro permette di intercettare tutti i pacchetti che non sono stati intercettati dal primo.


```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool                               Funkwerk Enterprise Communications GmbH
[QOS][FILTER]: Configure IP Classification Filter  r230aw

-----

Abbreviations: sa (source IP address)           sp (source port)
               da (destination IP address)      dp (destination port)
               it (icmp type)                  estab (TCP established)

Index  Descr          Conditions
  1     VoIP          sa 192.168.177.9/32
  2     all

ADD          DELETE          EXIT

-----

Ready                               Telnet    24, 80    24 Rows, 80 Cols  VT100    NUM
```

A questo punto, dal menù “*IP Classification and Signalling*” dobbiamo impostare la priorità ai pacchetti intercettati dai due filtri precedenti.

```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool                               Funkwerk Enterprise Communications GmbH
[QOS]: QoS Configuration                         r230aw

-----

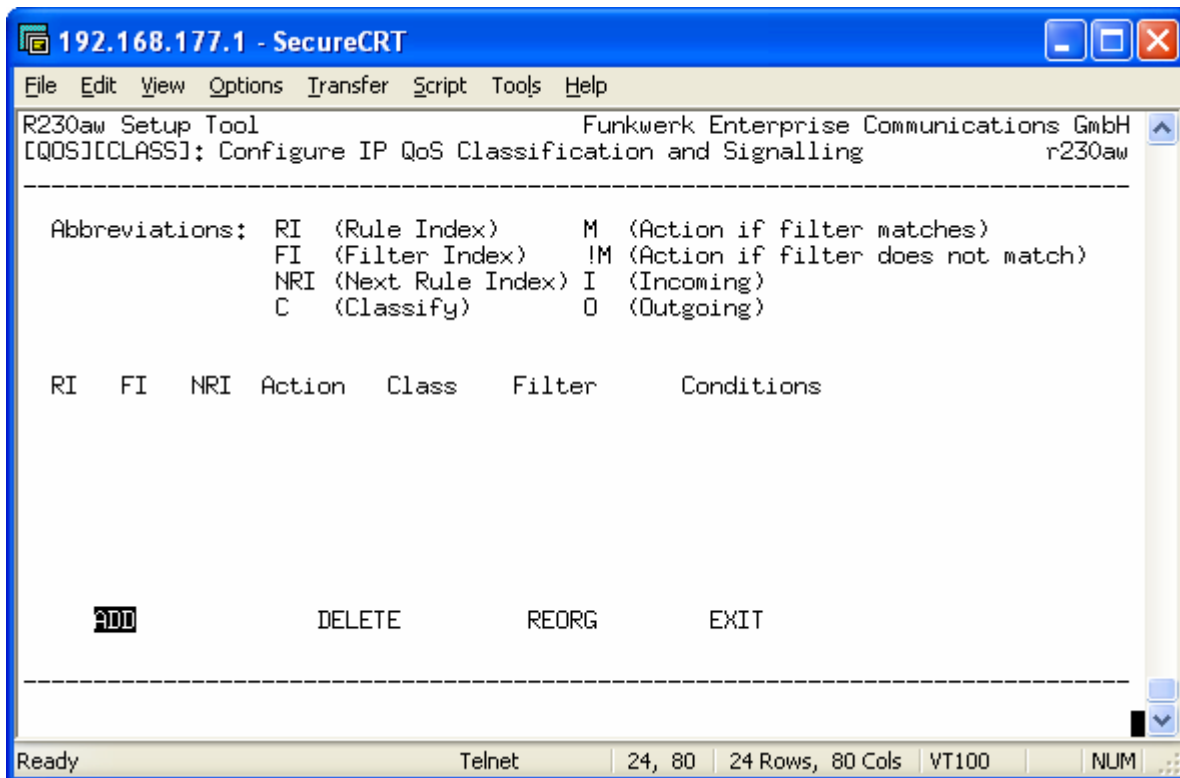
IP Filter
IP Classification and Signalling
Interfaces and Policies

EXIT

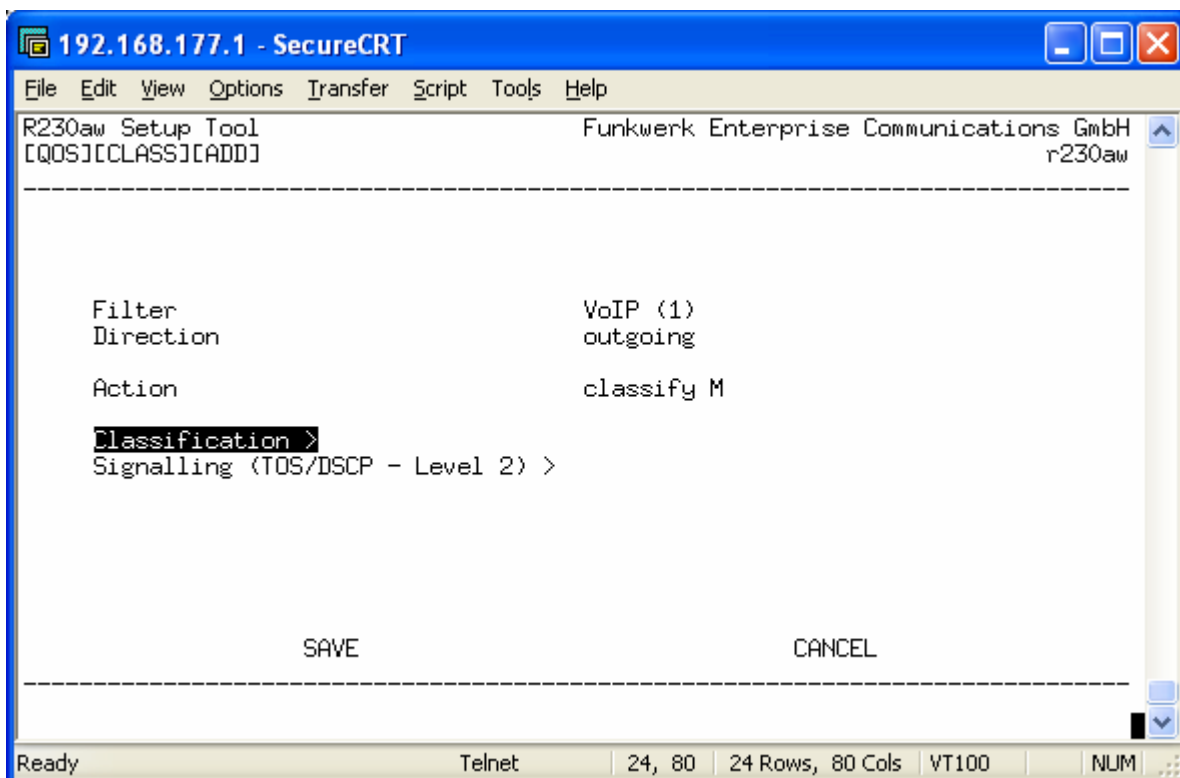
-----

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter

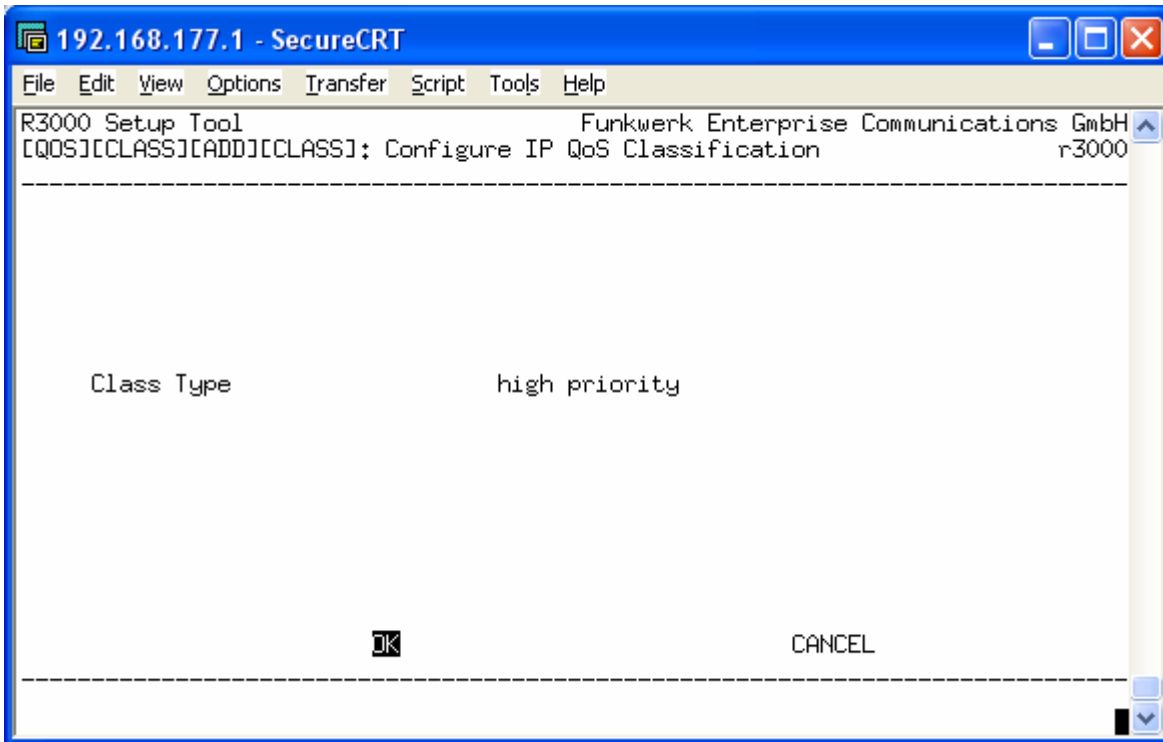
Ready                               Telnet    24, 80    24 Rows, 80 Cols  VT100    NUM
```



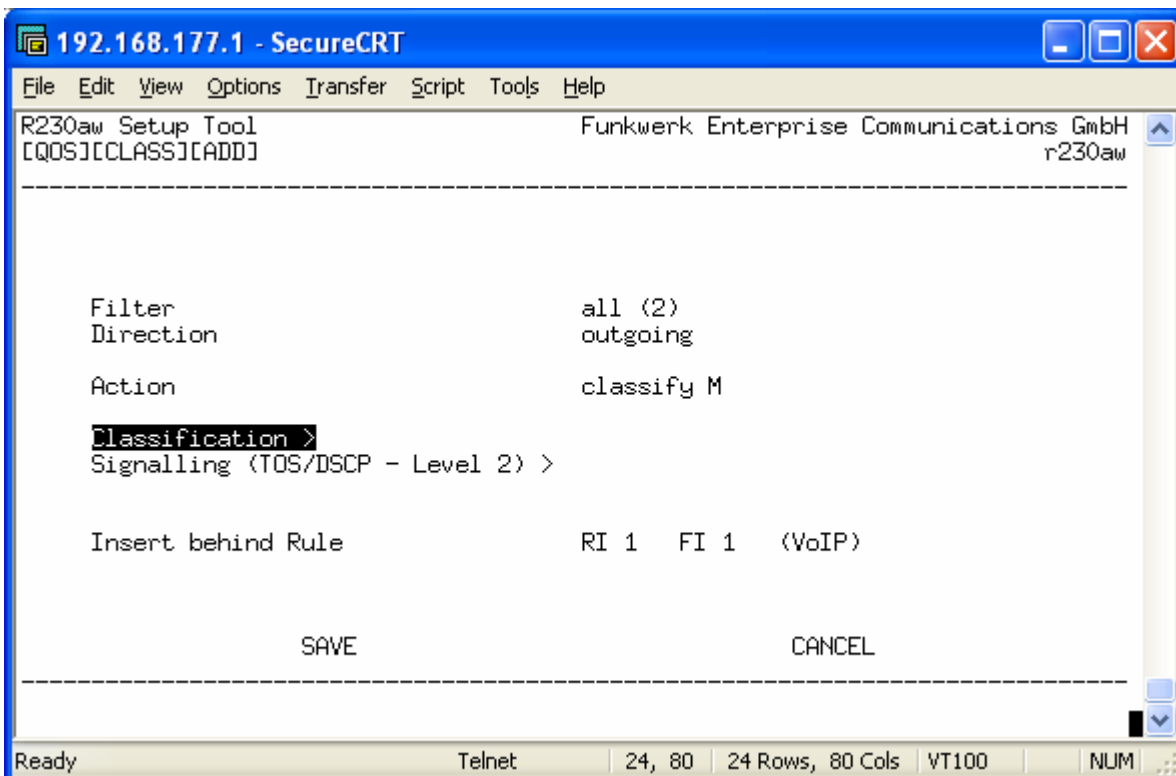
Creiamo quindi una catena composta da due regole:

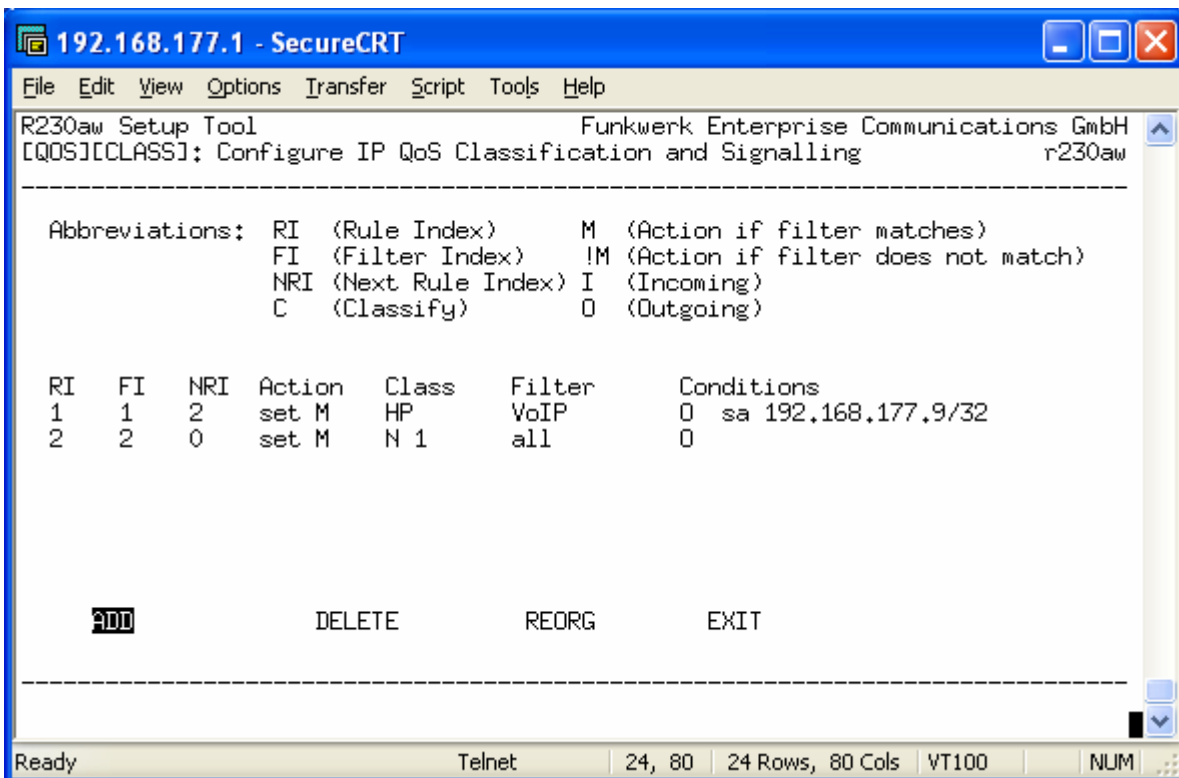
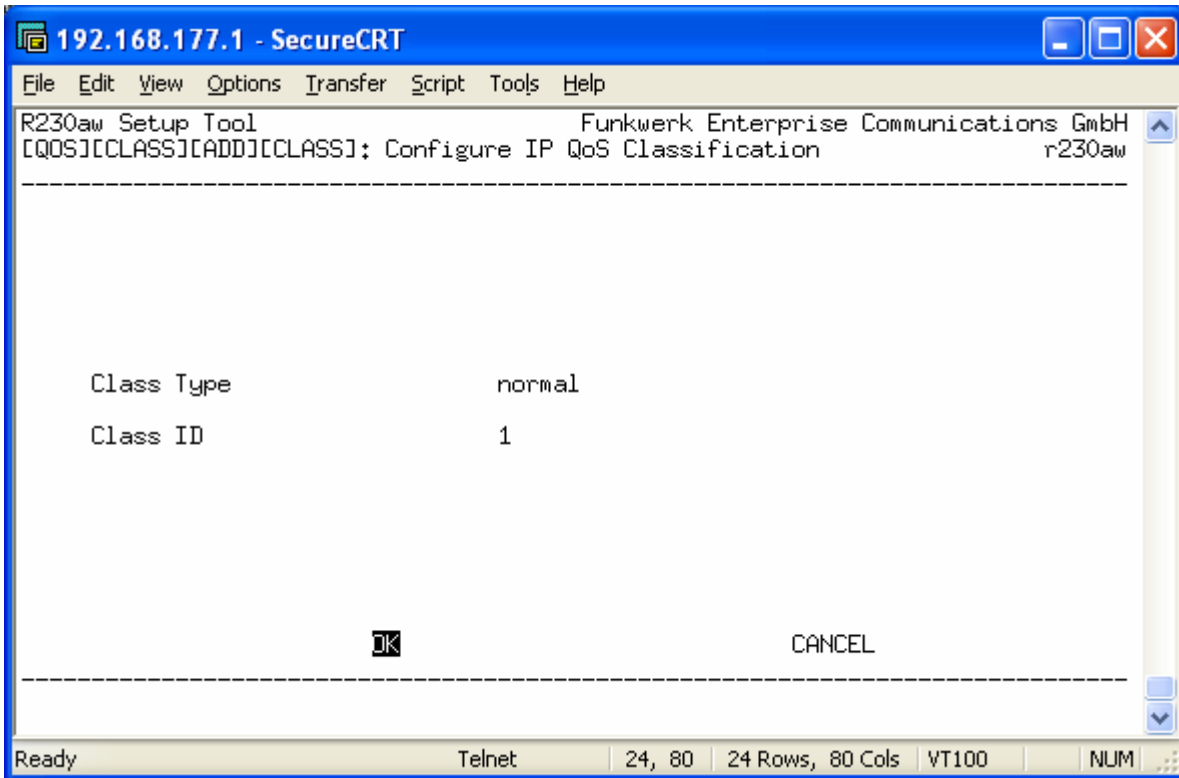


Il QoS va sempre fatto in direzione “outgoing” in quanto il collo di bottiglia è rappresentato dalla velocità della linea ADSL (es. LAN 100 Mb → WAN 512 Kb).



In questo modo tutti pacchetti che verificano il filtro verranno considerati come High Priority.



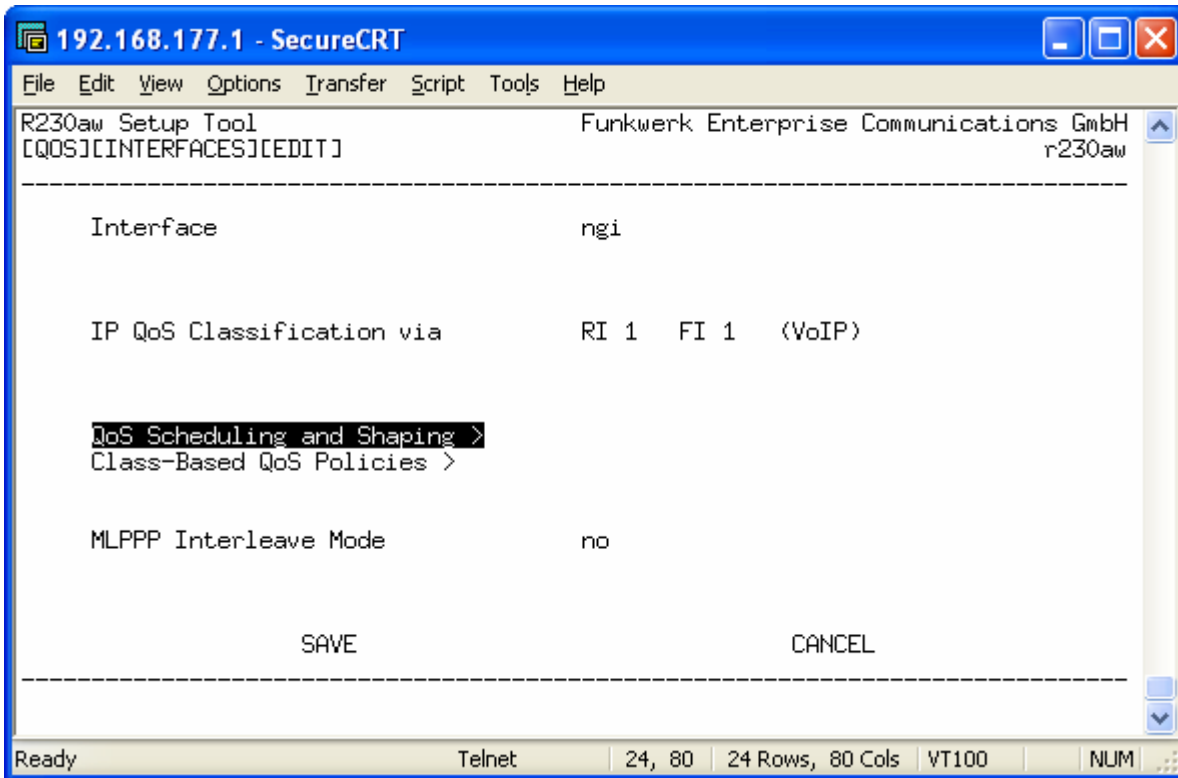


Non rimane che specificare la banda da assegnare alla categoria “High Priority” e alla categoria “default”. Si entra perciò nel menù “*Interfaces and Policies*”.

```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R3000 Setup Tool Funkwerk Enterprise Communications GmbH
[QOS]: QoS Configuration r3000
-----
IP Filter
IP Classification and Signalling
Interfaces and Policies
EXIT
-----
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```

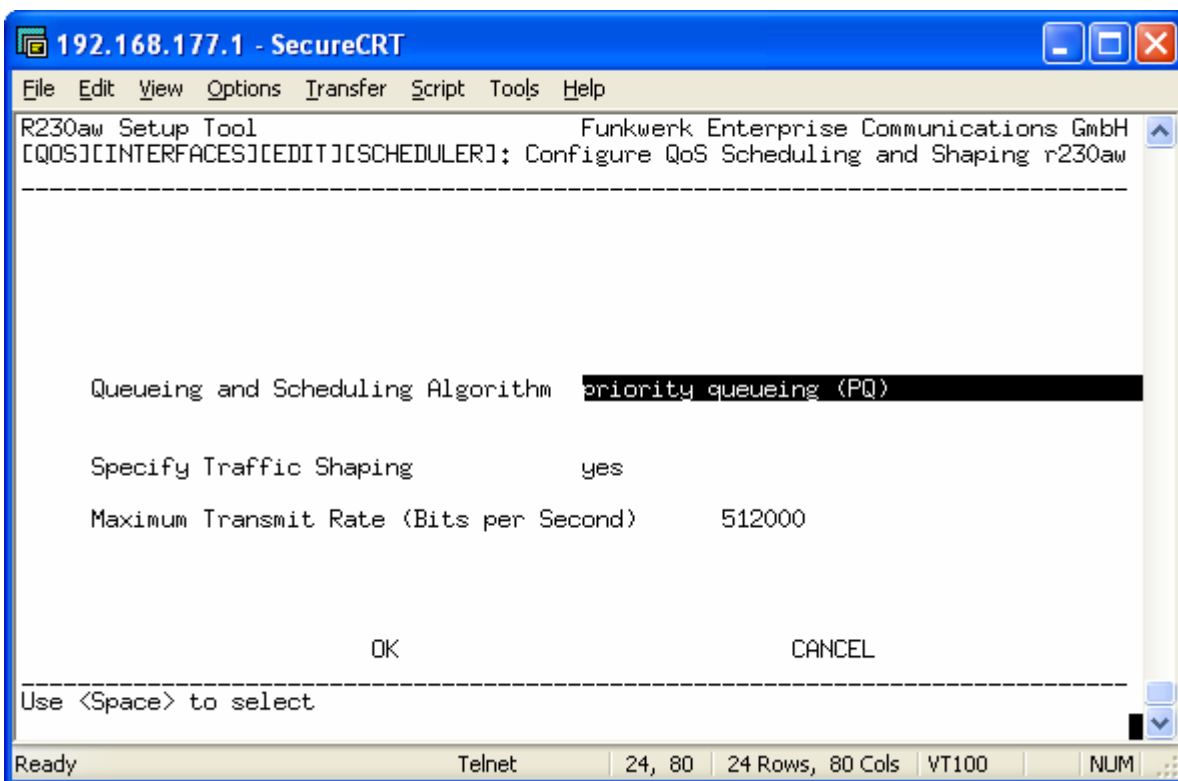
Ora bisogna specificare su quale interfaccia applicare la regola appena creata. Nel nostro caso sarà l'interfaccia ADSL.

```
192.168.177.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R230aw Setup Tool Funkwerk Enterprise Communications GmbH
[QOS][INTERFACES]: Enable IP QoS Classification and Policies r230aw
-----
Interface      First Rule      First Filter      Scheduler      TxRate Limit
en1-0           no IP QoS classification
en1-0-snap     no IP QoS classification
en1-1           no IP QoS classification
en1-1-snap     no IP QoS classification
ethoa50-0      no IP QoS classification
ethoa50-0-snap no IP QoS classification
ngi           no IP QoS classification
verso_casa     no IP QoS classification
verso_rizzuti  no IP QoS classification
vss1-0         no IP QoS classification
vss1-0-snap   no IP QoS classification
EXIT
-----
Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to select/edit
Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM
```

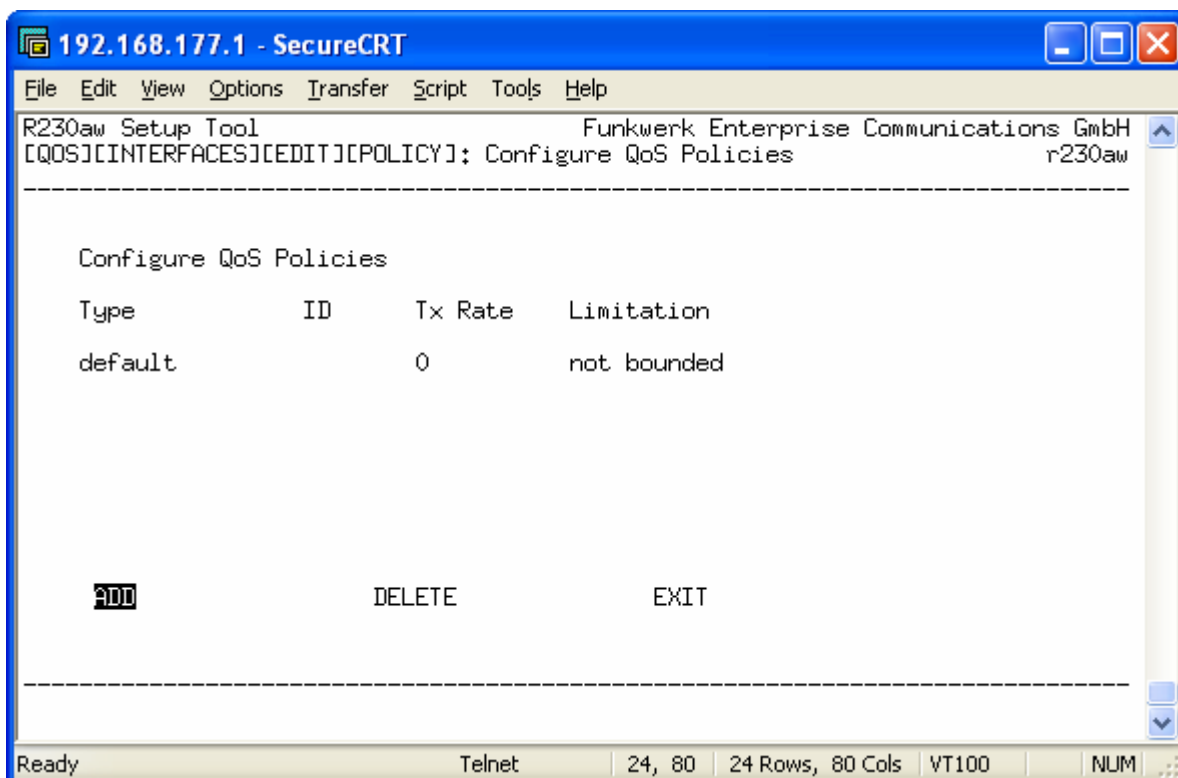
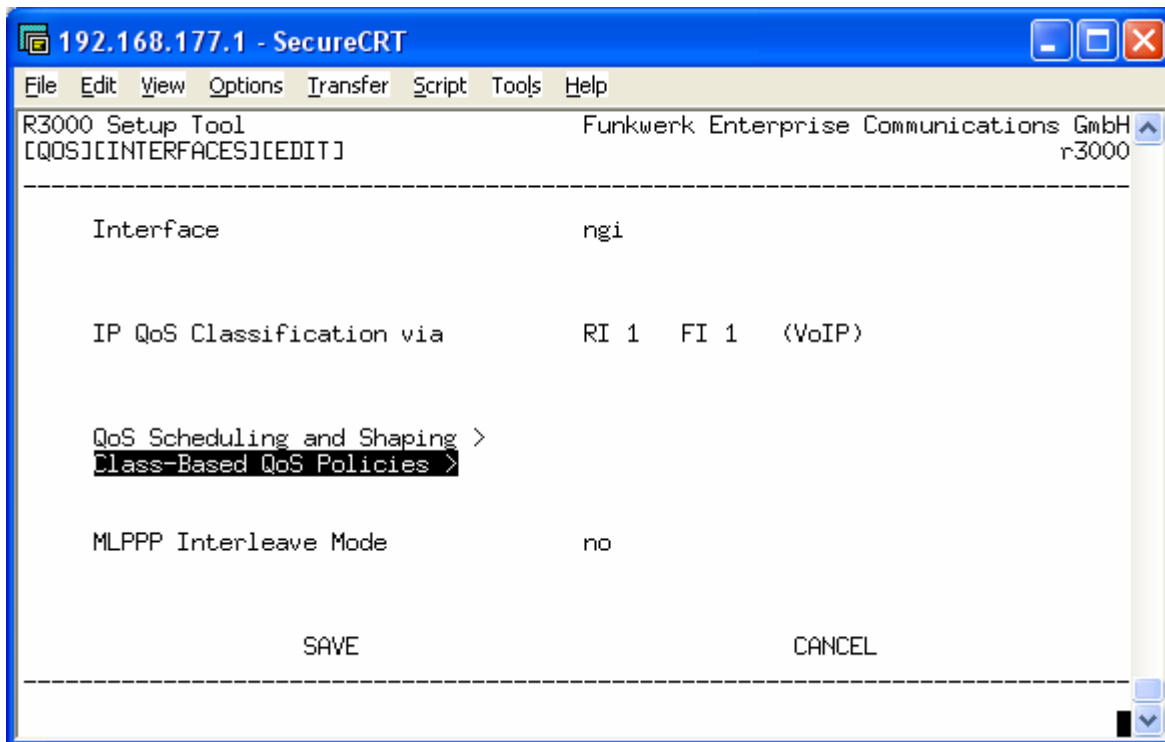


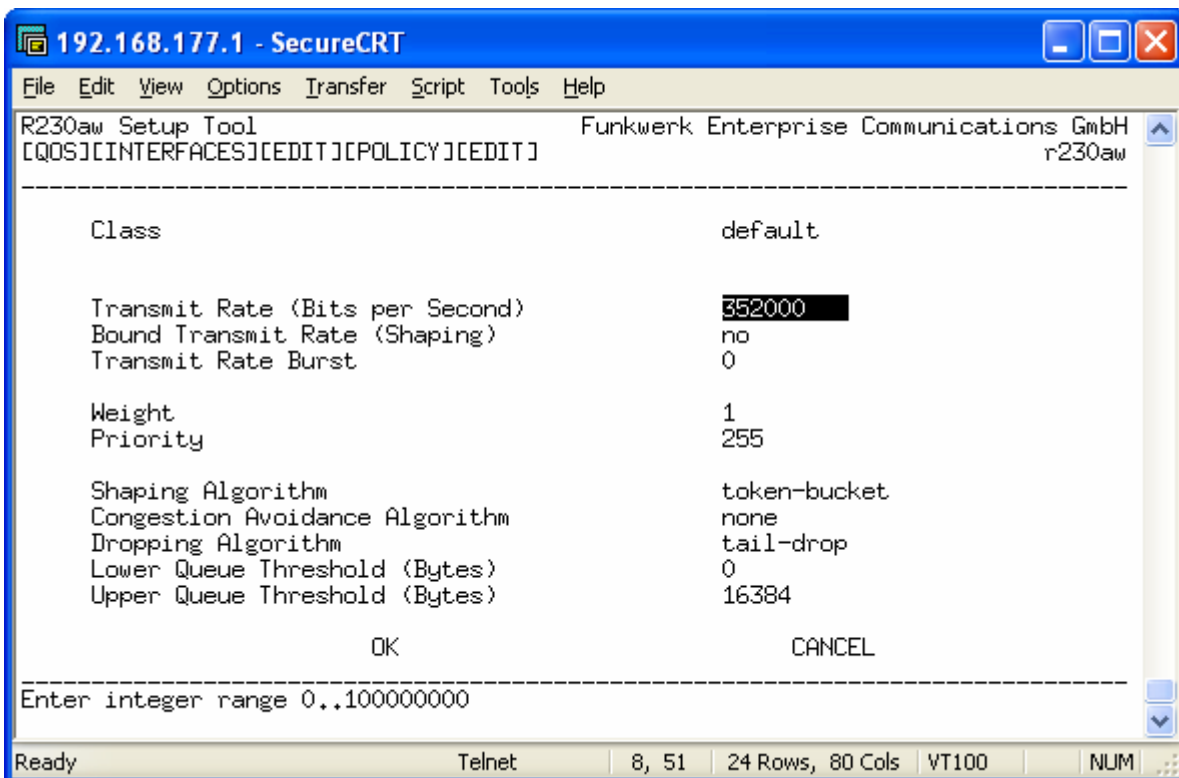
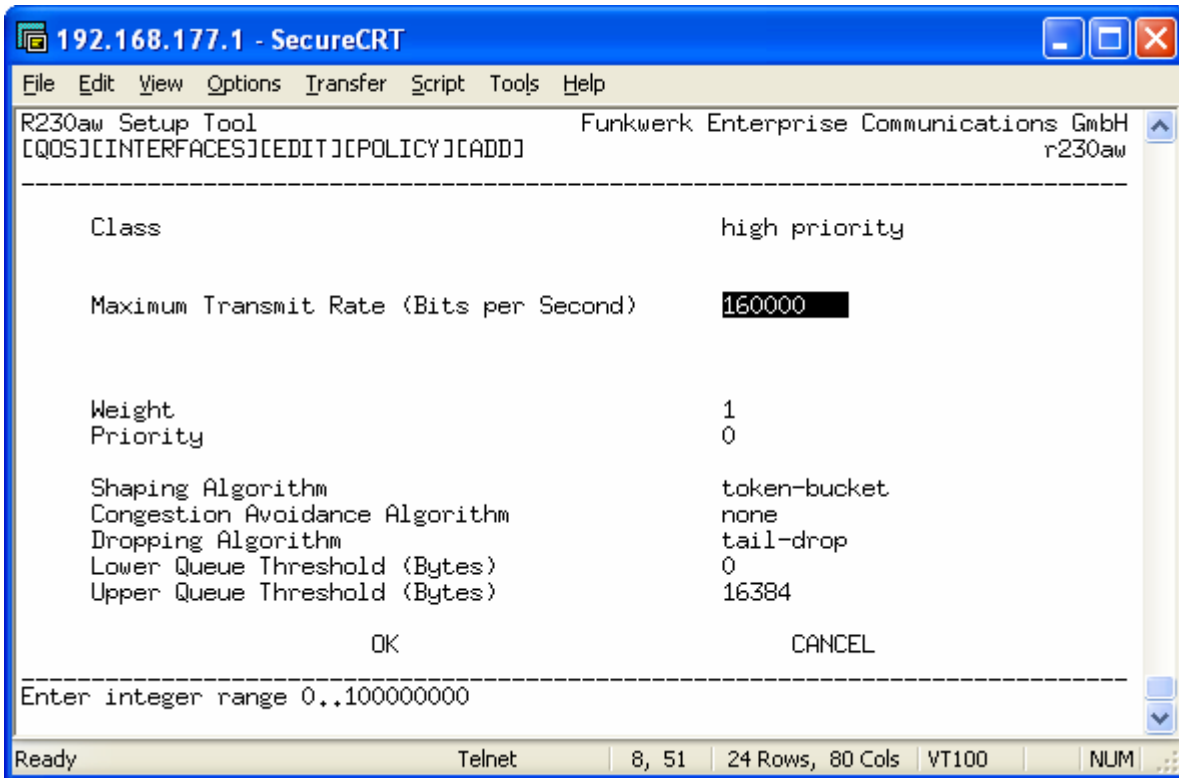
Il parametro “*IP QoS Classification via*” chiede di specificare quale regola della catena seguire per prima; nel nostro caso la prima regola è proprio VoIP.

Nel menù “*QoS Scheduling and Shaping*” specifichiamo qual è la banda in Uplink della linea ADSL (quella massima concordata col provider) e indichiamo l’algoritmo di accodamento.



Infine dobbiamo decidere quanta banda assegnare ai pacchetti prioritari. Dal menù “*Class-Based QoS Policies*”:





I pacchetti “High Priority” vedono garantirsi circa 160 Kb (limitati = bounded) di banda mentre i pacchetti “default” possono avere da 352 Kb (nel caso in cui i primi 160 Kb siano già occupati) a 512 Kb (nel caso in cui l’host 192.168.177.9 non stia trasmettendo pacchetti)

192.168.177.1 - SecureCRT

File Edit View Options Transfer Script Tools Help

R230aw Setup Tool Funkwerk Enterprise Communications GmbH
[QOS][INTERFACES][EDIT][POLICY]: Configure QoS Policies r230aw

Configure QoS Policies

Type	ID	Tx Rate	Limitation
default		352000	not bounded
high priority		160000	bounded

900 DELETE EXIT

Ready Telnet 24, 80 24 Rows, 80 Cols VT100 NUM

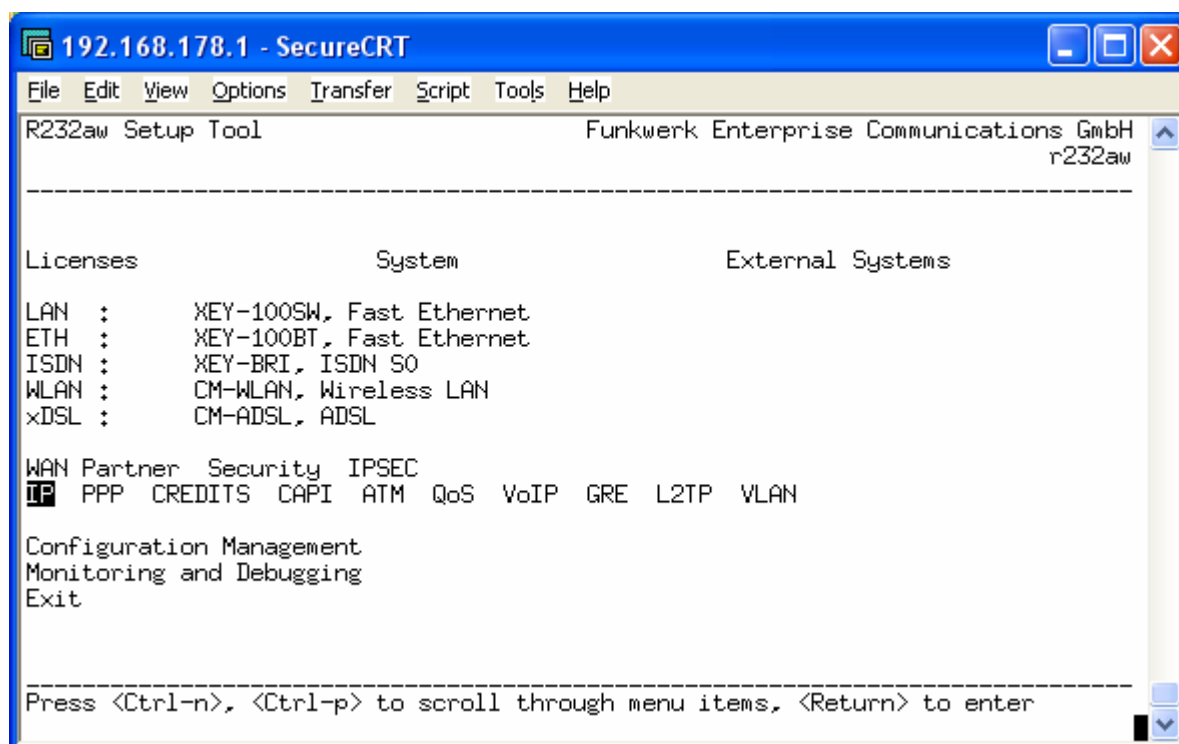
Backup di una connessione DialUp

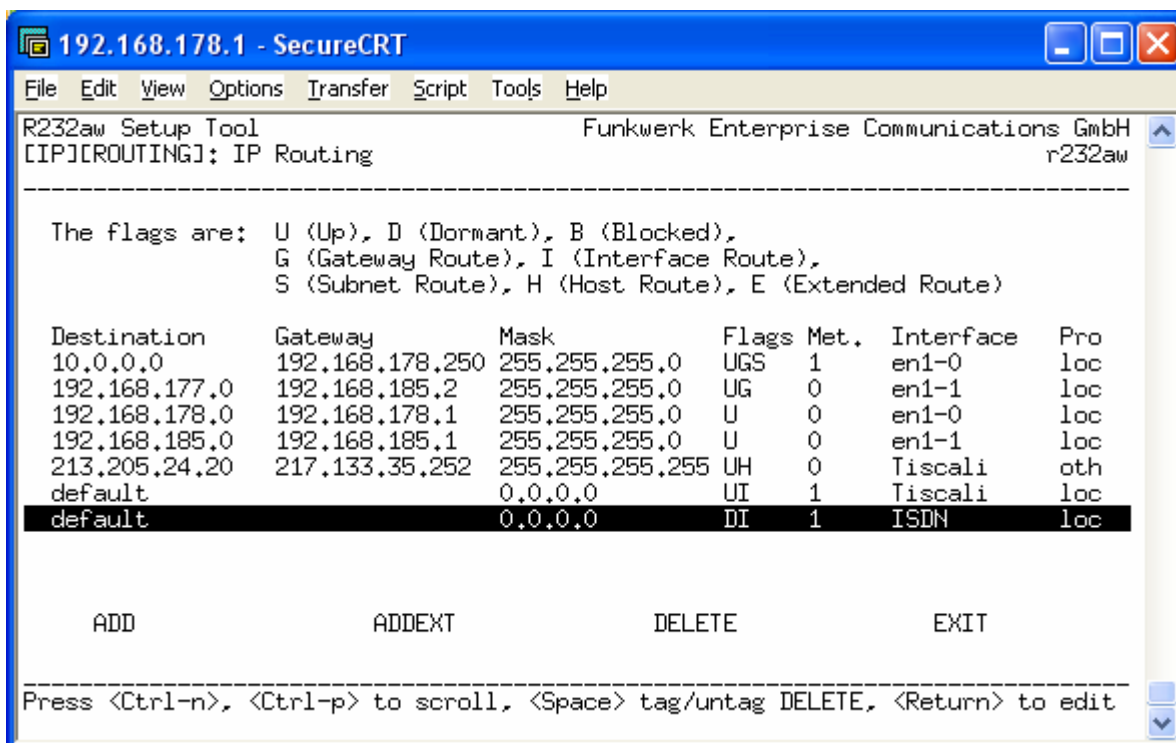
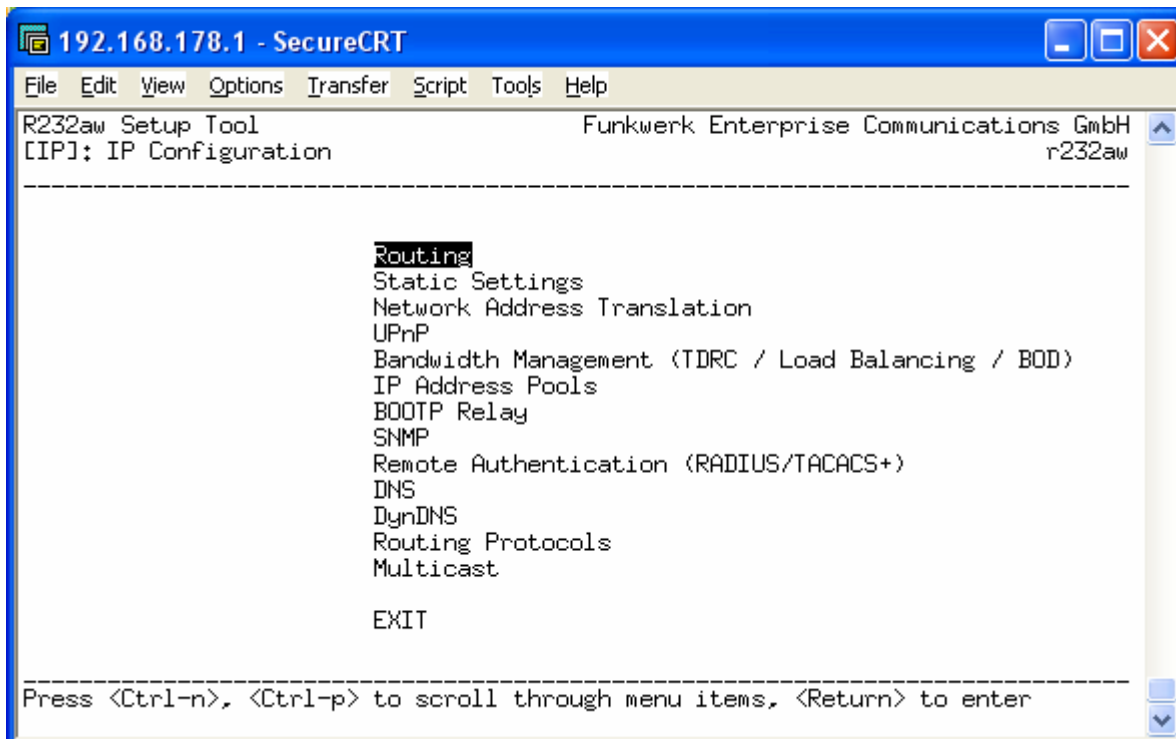
Può capitare di dover fornire una connessione di back-up che entri in funzione nel caso in cui la connessione principale sia fuori uso. Sui router che hanno la porta ISDN è possibile effettuare il backup ISDN.

Occorre quindi configurare due connessioni ad internet: la prima (per esempio) sarà un'ADSL mentre la seconda sarà un'ISDN (per la configurazione di ADSL e ISDN si vedano i paragrafi relativi alla connessione internet precedentemente decritti).

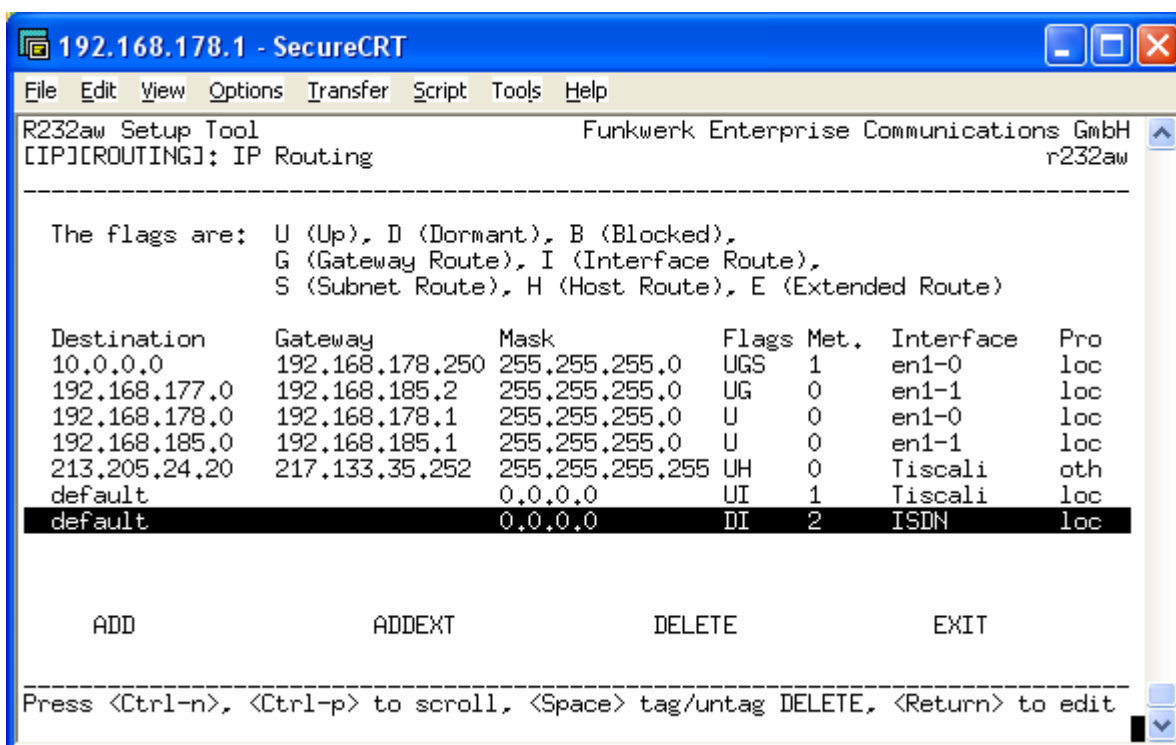
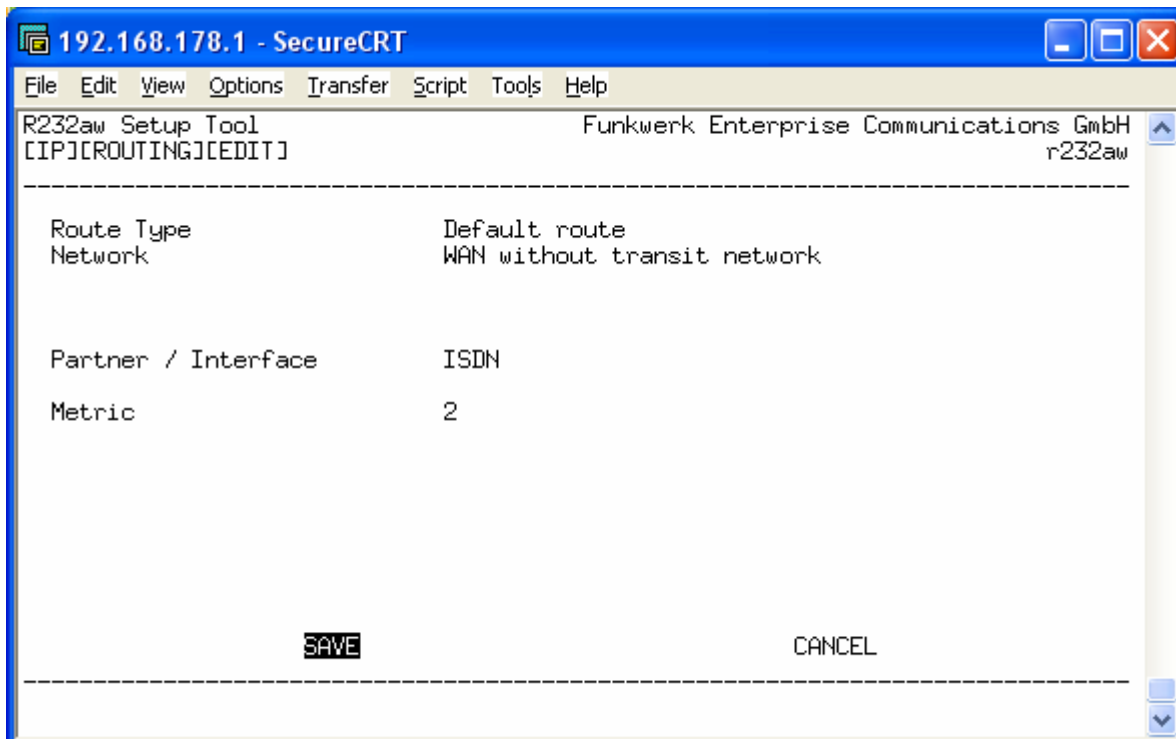
Ora, per indicare che la connessione ISDN è secondaria rispetto all'ADSL è necessario alzare la metrica sull'interfaccia ISDN, in modo che venga attivata solo quando va in down l'ADSL.

Dal menù IP → Routing





Si seleziona la default route relativa all'interfaccia ISDN e si imposta a 2 la metrica.



A questo punto occorre attivare un meccanismo intelligente per capire quando l'ADSL non funziona e permettere al back-up ISDN di entrare in funzione. Questo meccanismo è definito Keepalive.

Dal menù System → Schedule and Monitor → Keepalive Monitoring

```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
r232aw
-----
Licenses          System          External Systems
LAN : XEY-100SW, Fast Ethernet
ETH : XEY-100BT, Fast Ethernet
ISDN : XEY-BRI, ISDN SO
WLAN : CM-WLAN, Wireless LAN
xDSL : CM-ADSL, ADSL
WAN Partner Security IPSEC
IP PPP CREDITS CAPI ATM QoS VoIP GRE L2TP VLAN
Configuration Management
Monitoring and Debugging
Exit
-----
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```

```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
r232aw
[SYSTEM]: Change System Parameters
-----
System Name                r232aw
Local PPP ID (default)    r232aw_Tiscali
Location
Contact                    BINTEC

Syslog output on serial console  no
Message level for the syslog table  debug
Maximum Number of Syslog Entries  50
Maximum Number of Acctlog Entries  20
External Activity Monitor >
External System Logging >
Schedule & Monitor >
Password settings >
Time and Date >

SAVE                          CANCEL
-----
```

```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[SYSTEM][SCHEDMONJ]: Schedule & Monitor r232aw

-----

Keepalive Monitoring (Hosts & Ifc) >
Event Scheduler (Time & SNMP) >

EXIT

-----
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```

```
192.168.178.1 - SecureCRT
File Edit View Options Transfer Script Tools Help
R232aw Setup Tool Funkwerk Enterprise Communications GmbH
[SYSTEM][KEEPALIVE MONITORING][ADD]: Host Monitoring r232aw

-----

Group 0
IPAddress 151.1.1.1
Interval 10
Trials 3
Source IP 127.0.0.1
DownAction down
FirstIFIndex 10001
Range 0

SAVE CANCEL

-----
```

Attiviamo il keepalive sull'indirizzo 151.1.1.1 ogni 10sec.

In sostanza il router ogni 10 secondi manda un ping ad un indirizzo internet (es. 151.1.1.1). Per raggiungere questo indirizzo verrà utilizzata in prima battuta la default route con metrica più bassa, in questo caso si tratta della linea ADSL. Se l'host remoto non risponde al ping per 3 volte consecutive allora viene eseguita l'azione che abbiamo impostato sul parametro "DownAction": nell'esempio abbiamo scritto di mettere in down l'interfaccia ADSL (10001).

Per scoprire l'indice dell'interfaccia che deve essere messa in down basta digitare il comando:

```
ifstat
```

```

192.168.0.254 (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
192.168.0.254 (1)
Login: admin
Password:
Password not changed. Call "setup" for quick configuration.
r230aw:> ifstat
Index  Descr      Type Mtu  Speed St  Ipkts   Ies  opkts   Oes  PhyAddr/ChgTime
000000 REFUSE     othr 8192    0 up  0       0  0       0    0 00:00:00
000001 LOCAL     othr 8192    0 up  0       0  0       0    0 00:00:00
000002 IGNORE    othr 8192    0 up  0       0  0       0    0 00:00:00
001000 en1-0     eth 1500  100M up  82      0  31      0    00:a0:f9:20:e4:a3
001001 en1-0-llc eth 1496  100M up  0       0  0       0    00:a0:f9:20:e4:a3
001002 en1-0-snap eth 1492  100M up  0       0  0       0    00:a0:f9:20:e4:a3
200000 vss1-0    eth 1500   54M dn  0       0  0       0    00:00:00:00:00:00
200001 vss1-0-llc eth 1496   54M dn  0       0  0       0    00:00:00:00:00:00
200002 vss1-0-snap eth 1492   54M dn  0       0  0       0    00:00:00:00:00:00
001100 en1-1     eth 1500  100M dn 327     0  0       0    00:a0:f9:20:e4:a3
001101 en1-1-llc eth 1496  100M dn  0       0  0       0    00:a0:f9:20:e4:a3
001102 en1-1-snap eth 1492  100M dn  0       0  0       0    00:a0:f9:20:e4:a3
010001 Alice    ppp 1500   64K bk  0       0  0       0    0 01:06:02
total: 13
r230aw:>
Ready Telnet 24, 10 24 Rows, 80 Cols VT100 CAP NUM

```

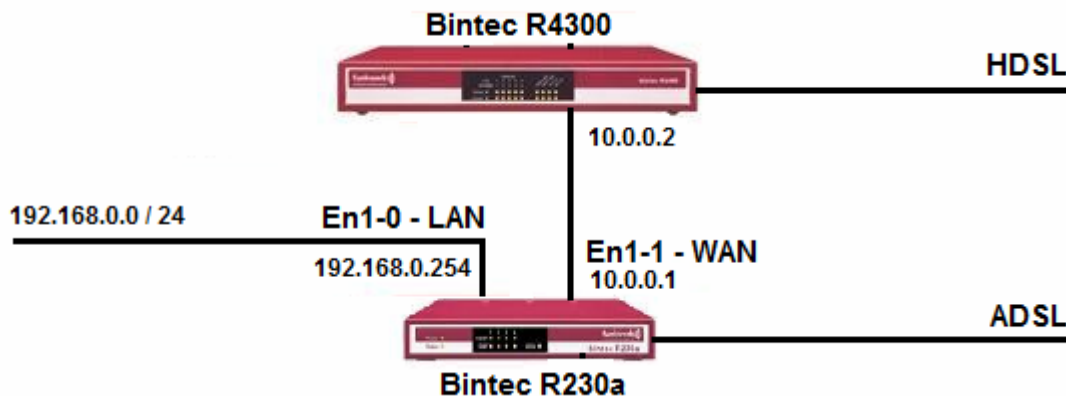
Questo fa in modo che il router utilizzi la default route con metrica 2, ovvero l'interfaccia ISDN. A questo punto il router invierà le richieste di keepalive attraverso l'interfaccia ISDN perché è l'unica che consente l'accesso ad internet: molto probabilmente l'host remoto tornerà a rispondere e di conseguenza il router compierà l'azione contraria a quella impostata sul parametro "DownAction", ovvero tenterà di rimettere in UP la linea ADSL. Se il tentativo va a buon fine il router continuerà ad utilizzare l'ADSL per uscire su internet e la linea ISDN verrà messa in stato di "Dormant" per inattività allo scadere del tempo impostato sul parametro "Static Short Hold". Se invece persistono i problemi alla linea ADSL verrà semplicemente ripetuto il ciclo descritto in precedenza. Il tutto verrà eseguito in modo del completamente trasparente dal router senza che l'utente finale si accorga di niente .

Suggerimento: ricordarsi di impostare il parametro "Static Short Hold" della connessione ISDN ad un valore ragionevolmente basso (20 – 30 secondi) per fare in modo che tale connessione venga disattivata (per inattività) quando l'ADSL torna a funzionare. Impostando "Static Short Hold" a -1 si avrà come risultato che l'ISDN rimarrà sempre attiva anche se non utilizzata!

Backup di una connessione ETHERNET

Nel capitolo precedente abbiamo visto come configurare un back-up nel caso in cui entrambe le connessioni (ADSL e ISDN) siano di tipo DialUp. Per DialUp intendiamo tutte quelle connessioni che richiedono un'autenticazione presso il provider.

Ora invece esaminiamo un altro caso: si presti attenzione all'esempio qui sotto.



In questo caso si vuole utilizzare la linea HDSL collegata al Bintec R4300 come principale e, in caso di guasto, si vuole utilizzare la linea ADSL collegata al Bintec R230a. Per prima cosa occorre configurare sull'R230a sia la linea ADSL che la linea Ethernet come descritto nei capitoli precedenti. Una volta terminata la configurazione si dovrebbe ottenere una tabella di routing che assomiglia a questa:

```
Router Bintec - HyperTerminal
File Modifica Visualizza Chiama Trasferimento ?
R230aw Setup Tool                               Funkwerk Enterprise Communications GmbH
[IP][ROUTING]: IP Routing                       r230aw

The flags are:  U (Up), D (Dormant), B (Blocked),
                 G (Gateway Route), I (Interface Route),
                 S (Subnet Route), H (Host Route), E (Extended Route)

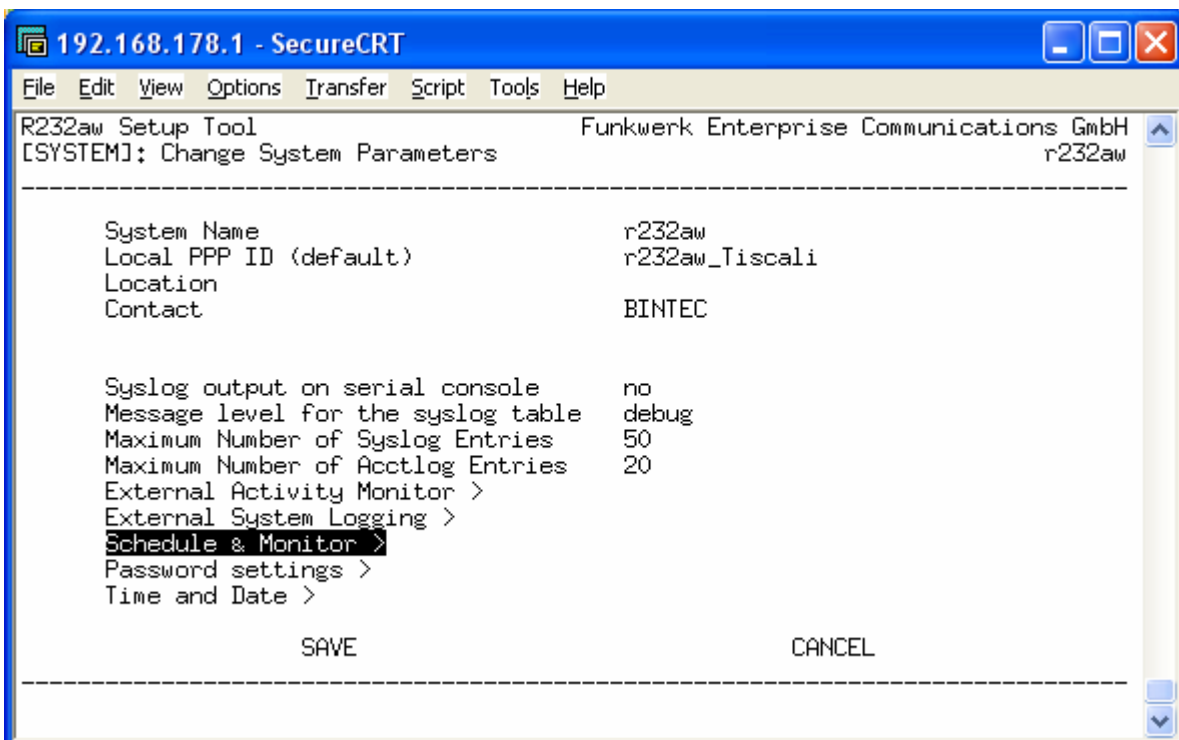
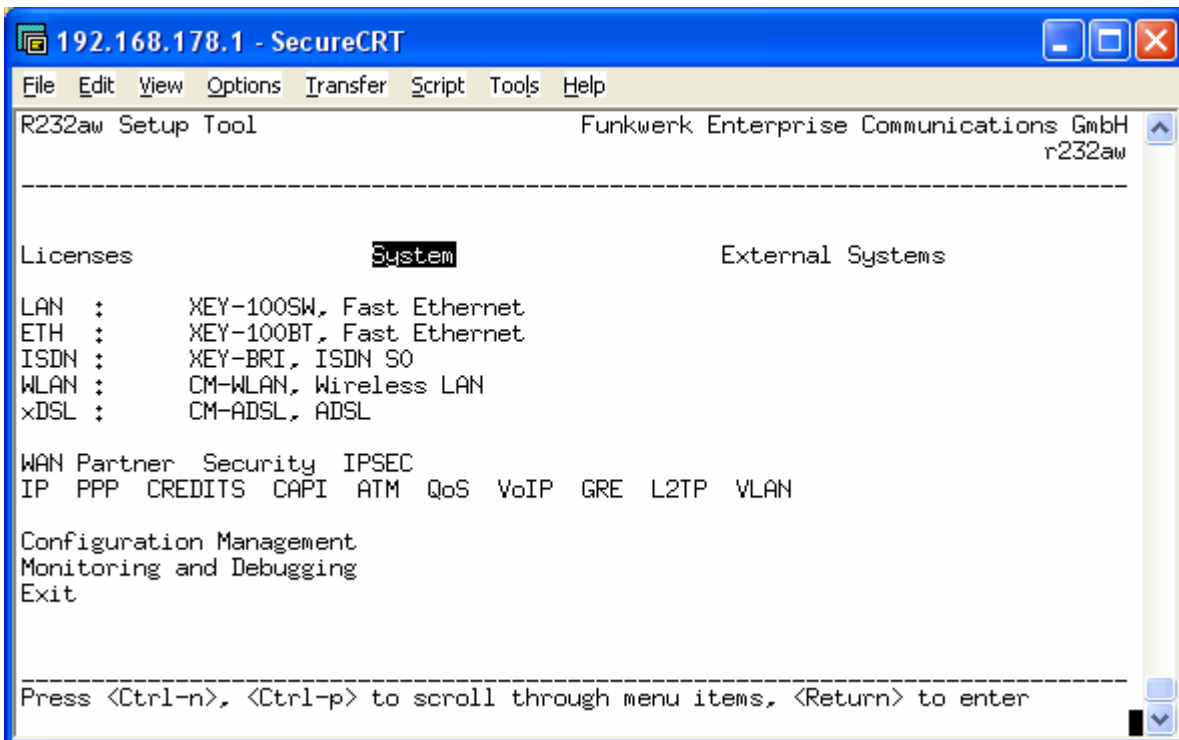
Destination   Gateway      Mask          Flags Met.  Interface  Pro
10.0.0.0      10.0.0.1    255.255.255.252 S    0    en1-1     loc
192.168.0.0  192.168.0.254 255.255.255.0  0    en1-0     loc
default      10.0.0.2    0.0.0.0      G    2    en1-1     loc
default      10.0.0.2    0.0.0.0      BI   1    Alice     loc

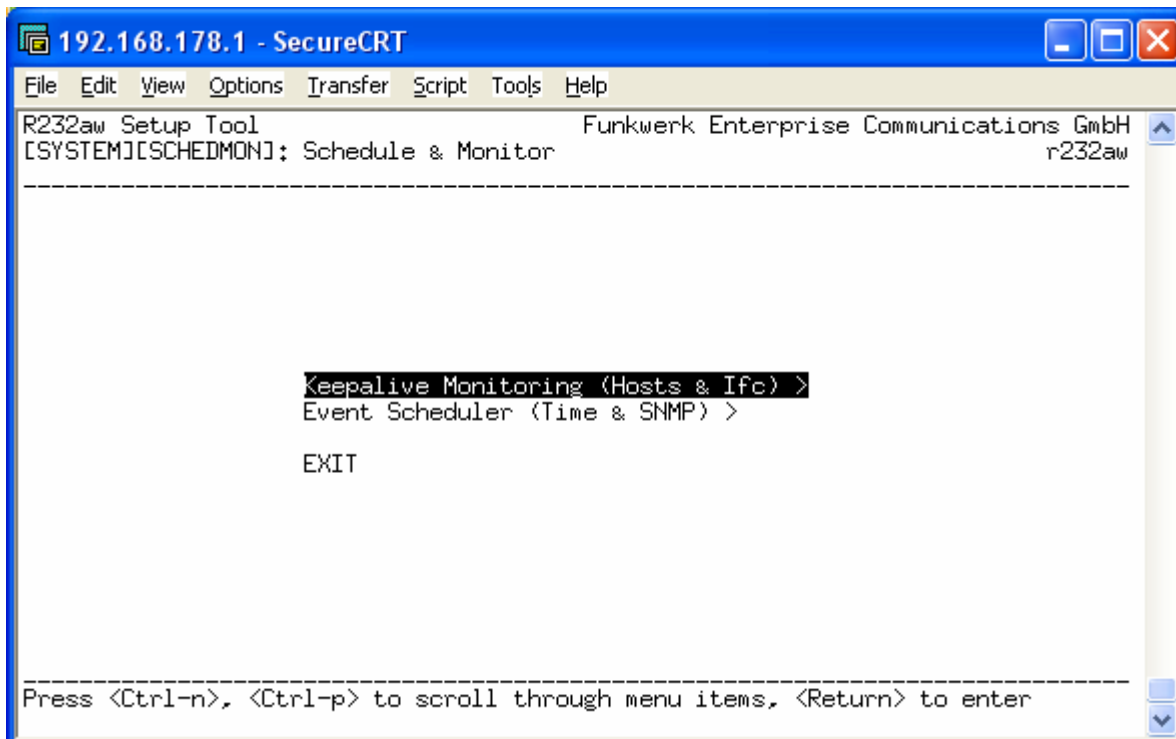
ADD          ADDEXT      DELETE      EXIT

Connesso a 0.35.18      Rilev. aut.      9600 8-N-1      SCORR      MAILJSC      NUM      Acquisisci      Eco stampante
```

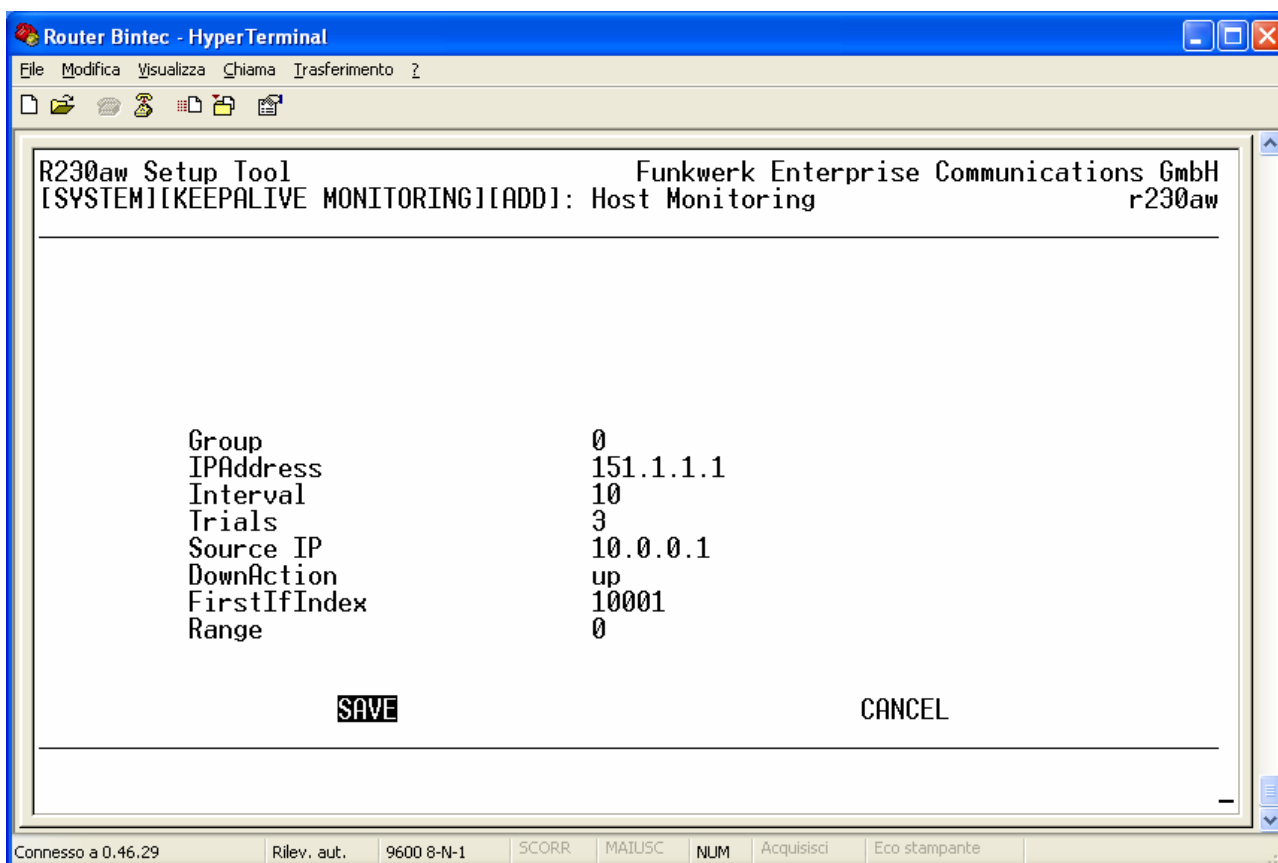

Se si fa bene attenzione alle metriche delle due default route si potrebbe pensare ad un errore in quanto risultano essere in disaccordo con quanto scritto precedentemente. In realtà la cosa è voluta e lo vedremo fra poco quando andremo a configurare il keepalive.

Dal menù System → Schedule and Monitor → Keepalive Monitoring

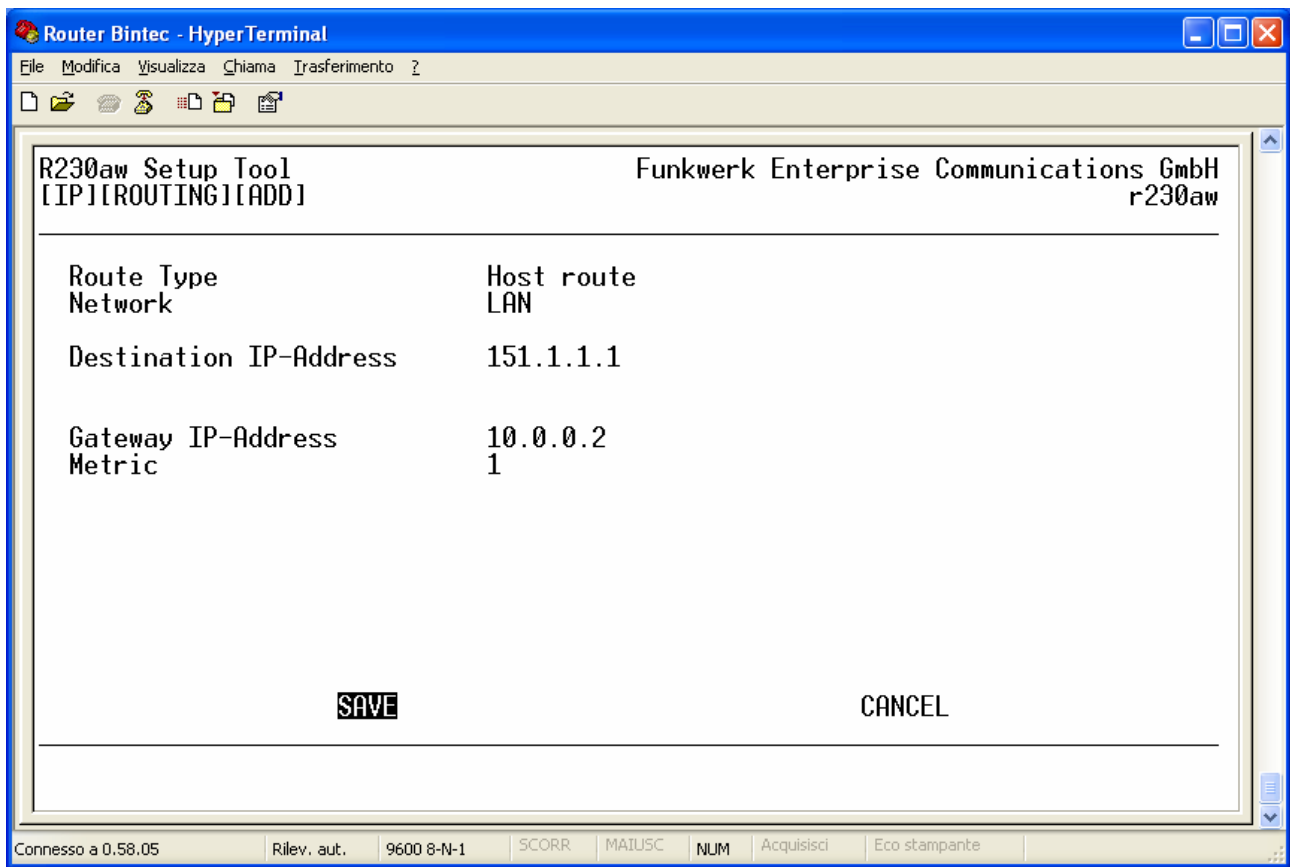




L'obiettivo è quello di controllare la presenza e quindi la raggiungibilità dell'host remoto attraverso l'interfaccia Ethernet En1-1. Nel caso in cui l'host non sia raggiungibile il router si impegnerà a mettere in UP l'interfaccia ADSL (indice 10001). Essendo la metrica dell'interfaccia ADSL prioritaria su quella della connessione Ethernet tutto il traffico diretto verso internet verrà dirottato su di essa. Facciamo notare come il router continui a verificare la presenza dell'host remoto attraverso l'interfaccia En1-1 indipendentemente dallo stato dell'ADSL. Non appena l'host torna ad essere raggiungibile il router eseguirà l'azione contraria mettendo in Down l'interfaccia ADSL. Verrà così utilizzata la default route con metrica 2, quindi la connessione HDSL.



Per essere sicuri che il router verifichi la presenza dell'host remoto attraverso l'interfaccia ethernet e non tramite l'interfaccia ADSL è possibile aggiungere una regola nella tabella di routing:



Aggiornamento Firmware di un router Bintec

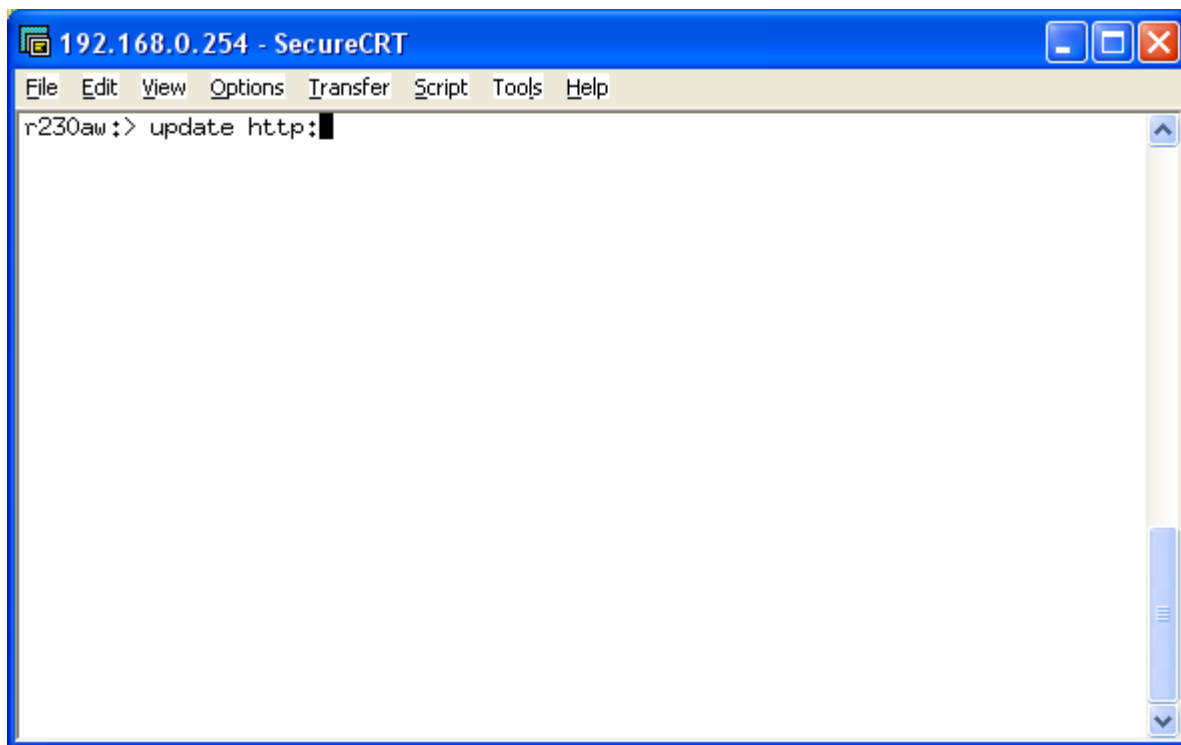
Vi sono tre metodi per effettuare l'aggiornamento al router.

METODO 1

Il più semplice è quello di farlo fare in automatico direttamente al router.

Ovviamente per questo metodo il router deve poter navigare e deve avere i DNS impostati.

Si entra in telnet sul router e si scrive *update http:*



In questo modo il router si collega direttamente al sito del produttore e si scarica l'ultimo firmware disponibile.

```
192.168.0.254 - SecureCRT
File Edit View Options Transfer Script Tools Help
r230aw:> update http;
retrieve current version from: http://www.funkwerk-ec.com/static/files/R230aw/R2
30aw-s_current
Starting HTTP File Transfer .....
```

```
192.168.0.254 - SecureCRT
File Edit View Options Transfer Script Tools Help
r230aw:> update http;
retrieve current version from: http://www.funkwerk-ec.com/static/files/R230aw/R2
30aw-s_current
Starting HTTP File Transfer ..... (139320+5778128 bytes)
List of files in this update (len 5778128):
  Version   Length  Name
7.6.1.106  4254565 Boss
7.6.1.106   798198 webpages.ez
7.6.1.106  433470 text_ger.ez
7.6.1.106   64812 CountryProfiles
7.6.1.106  130952 german.rey
7.6.1.106   96122 french.rey

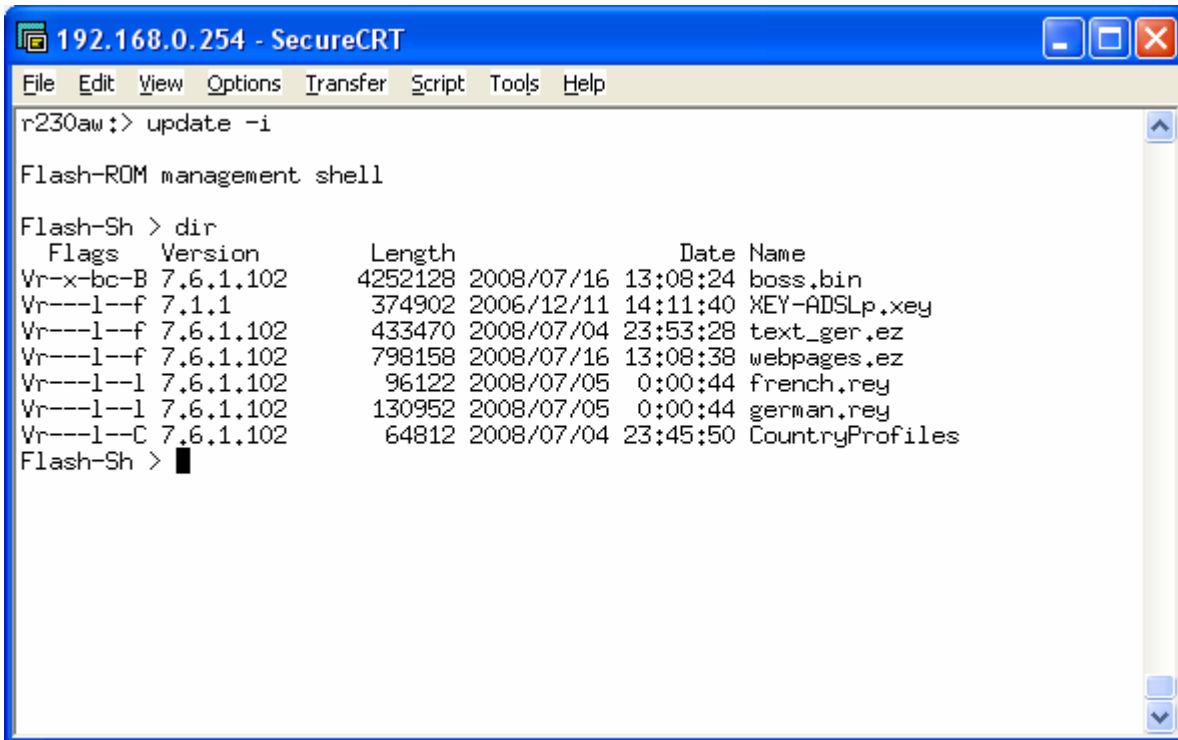
*** Don't power-off while the update takes place ***

Perform update (y or n) ? y
```

Poi il router va riavviato.

METODO 2

Attraverso il Telnet si entra nel router quindi si effettua il login; con i comandi *update -i* e *dir* si controlla la versione attuale dei firmware.

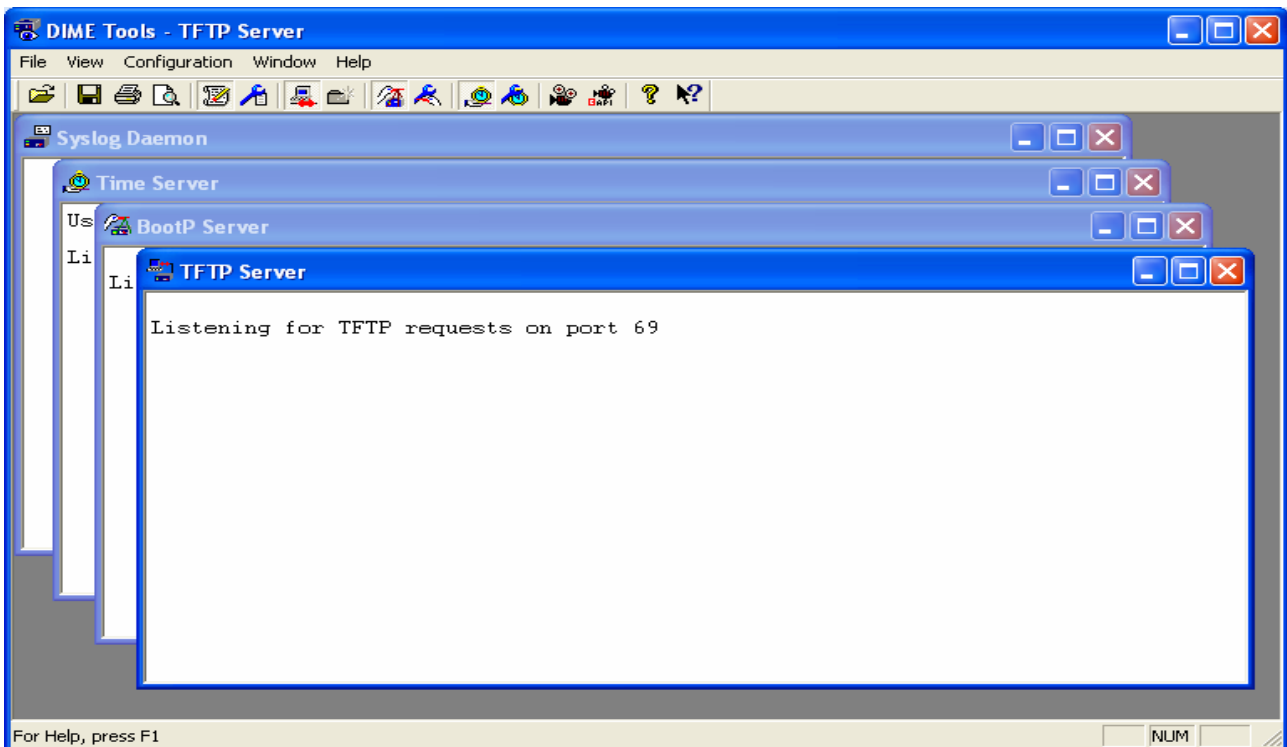


```
192.168.0.254 - SecureCRT
File Edit View Options Transfer Script Tools Help
r230aw:> update -i

Flash-ROM management shell

Flash-Sh > dir
  Flags  Version          Length      Date      Name
Vr-x-bc-B 7.6.1.102    4252128 2008/07/16 13:08:24 boss.bin
Vr---l--f 7.1.1        374902 2006/12/11 14:11:40 KEY-ADSLp.key
Vr---l--f 7.6.1.102    433470 2008/07/04 23:53:28 text_ger.ez
Vr---l--f 7.6.1.102    798158 2008/07/16 13:08:38 webpages.ez
Vr---l--l 7.6.1.102    96122 2008/07/05 0:00:44 french.rey
Vr---l--l 7.6.1.102   130952 2008/07/05 0:00:44 german.rey
Vr---l--C 7.6.1.102    64812 2008/07/04 23:45:50 CountryProfiles
Flash-Sh >
```

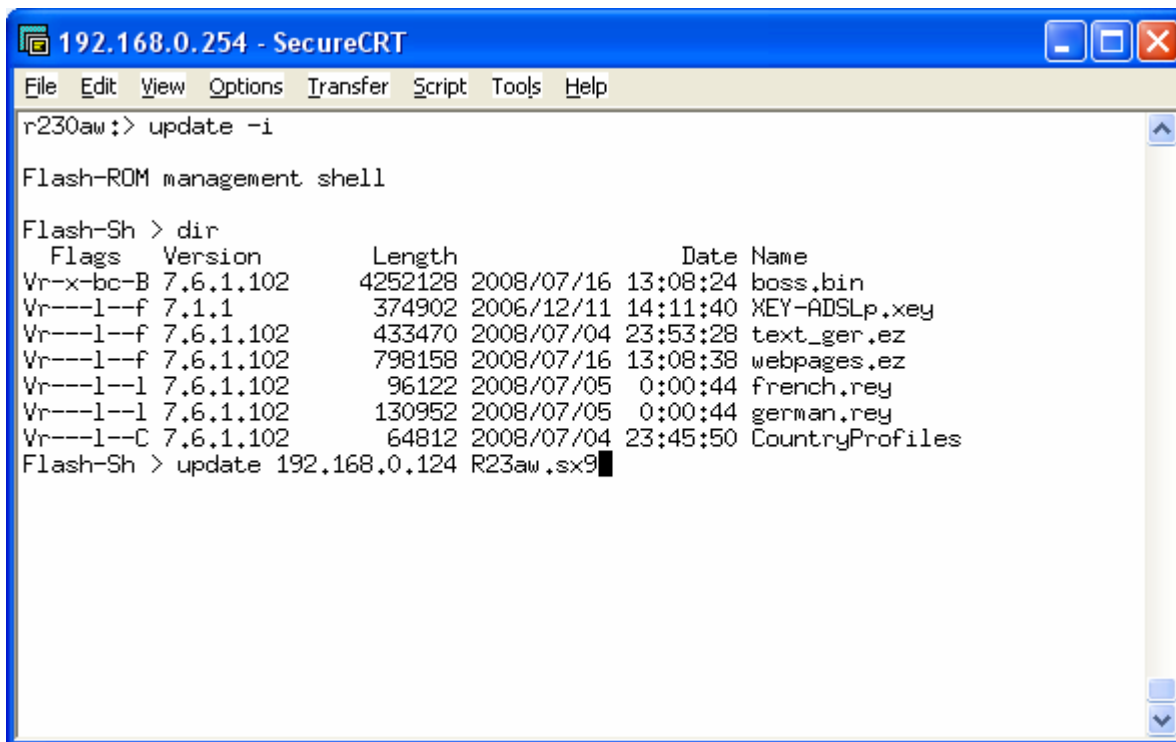
Durante la fase di update occorre tenere aperti gli strumenti DIME del software Brickware (in dotazione con tutti i router Bintec). Perciò occorre lanciare il programma DIME, cliccare su File, spuntare l'opzione TFTP Server. Cliccare su Configuration, quindi su TFTP Server... ed impostare la cartella nella quale è salvato il file che contiene il firmware nuovo. Ridurre a icona la finestra.



La prima cosa da fare è cancellare il firmware del modem ADSL tramite il comando *rm <nome file>*. Questo serve a liberare spazio sulla memoria.

Cancellando il firmware del modem non cade la connessione ADSL a meno che non si faccia un reboot.

Ora va caricato il firmware del router; la stringa da digitare è: *update <IP del pc che contiene il fw> <nome file fw>* (fare attenzione a digitare correttamente maiuscole e minuscole). Il file deve necessariamente essere contenuto nella cartella specificata all'interno dell'utility DIME.



```
192.168.0.254 - SecureCRT
File Edit View Options Transfer Script Tools Help
r230aw:> update -i

Flash-ROM management shell

Flash-Sh > dir
  Flags  Version      Length      Date Name
Vr-x-bc-B 7.6.1.102  4252128 2008/07/16 13:08:24 boss.bin
Vr---l--f 7.1.1      374902  2006/12/11 14:11:40 XEY-ADSLp.xey
Vr---l--f 7.6.1.102  433470  2008/07/04 23:53:28 text_ger.ez
Vr---l--f 7.6.1.102  798158  2008/07/16 13:08:38 webpages.ez
Vr---l--l 7.6.1.102   96122  2008/07/05 0:00:44 french.rey
Vr---l--l 7.6.1.102  130952  2008/07/05 0:00:44 german.rey
Vr---l--C 7.6.1.102   64812  2008/07/04 23:45:50 CountryProfiles
Flash-Sh > update 192.168.0.124 R23aw.sx9
```

Quando viene chiesto *Perform update <y o n> ?* digitare y e attendere. Una volta caricato il firmware bisogna fare un reboot. Ora bisogna ricaricare il firmware del modem ADSL digitando il comando *update <IP del pc che contiene il fw> <nome file fw>*

Ogni volta che si rimuove o si aggiunge un file è bene digitare il comando reorg per riorganizzare lo spazio libero all'interno della flash.

```
192.168.0.254 - SecureCRT
File Edit View Options Transfer Script Tools Help
update successfully finished
Updating text_ger.ez
*** delete text_ger.ez V. 7.5.1.100 (y or n) [y] ? y
Perform Flash-ROM update
Writing Flash-ROM ..... OK
Verify Flash-ROM ..... OK
update successfully finished
Updating webpages.ez
*** delete webpages.ez V. 7.5.1.100 (y or n) [y] ? y
Perform Flash-ROM update
Writing Flash-ROM ..... OK
Verify Flash-ROM ..... OK
update successfully finished
Rebooting... (y or n) [n] ? n
Flash-Sh > █
```


METODO 3

Si entra in configurazione tramite l'interfaccia HTTP e si va alla voce "Maintenance → Software & Configuration". Se il router è collegato ad internet è possibile scaricare direttamente l'ultima release sul sito del fornitore, altrimenti è possibile specificare il file locale precedentemente scaricato.

The screenshot shows the web interface of a bintec R230aw router. The browser window title is "bintec R230aw: Software & Configuration - Options - Microsoft Internet Explorer". The address bar shows the URL: "http://192.168.177.1/esi/7825/esi.cgi?page=status-index.xml&sessionID=3629612115".

The interface includes a navigation menu on the left with the following items: Save configuration, System Management, Physical Interfaces, LAN, Wireless LAN, Routing, WAN, VPN, Firewall, VoIP, Local Services, Maintenance (highlighted), Diagnostics, Software & Configuration (highlighted), Reboot, External Reporting, and Monitoring.

The main content area is titled "Options" and contains a table for "Currently Installed Software":

Currently Installed Software	
BOSS	V.7.8 Rev. 2 (Beta 5) IPSec from 2008/11/14 00:00:00
System Logic	1.2
ADSL Logic	6.2.1

Below the table, there are "Software and Configuration Options":

- Action: Update system software (dropdown menu)
- Source Location: Local File (dropdown menu)
- Filename: (input field) Sfoglia...

A "Go" button is located at the bottom of the options section.

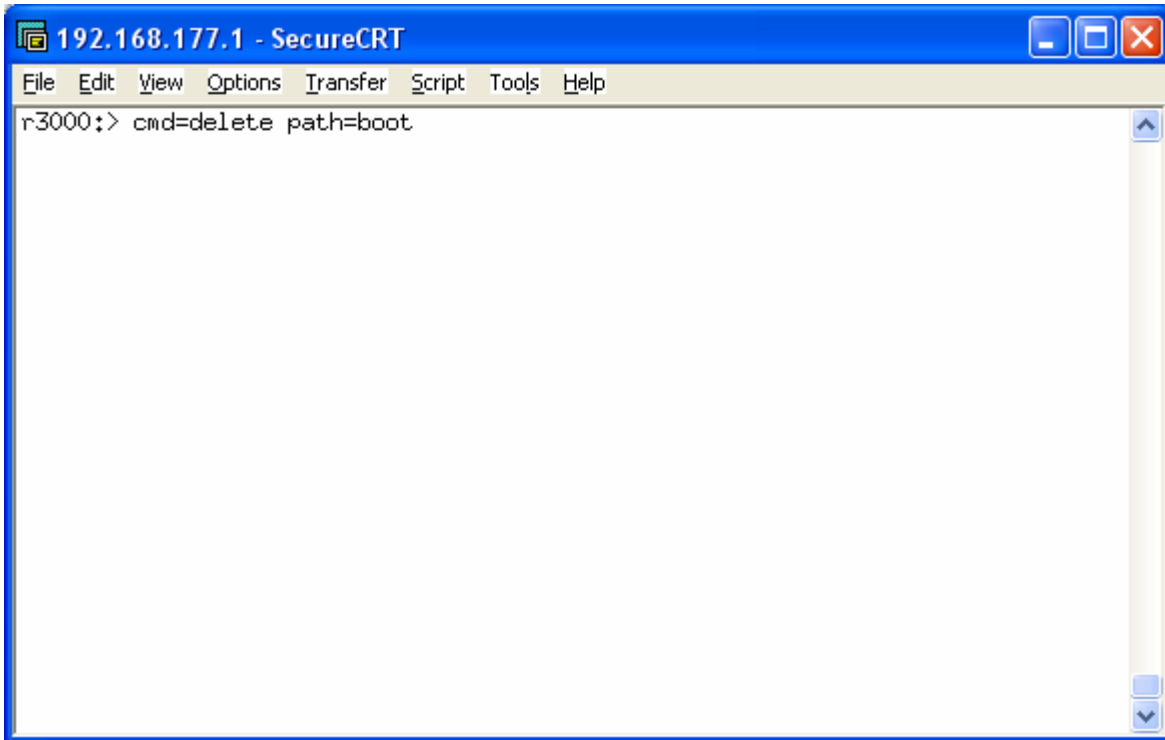
The status bar at the bottom of the browser window shows "Operazione completata" and "Internet".

Reset alle impostazioni di fabbrica

Ci sono 3 modi per riportare il router alle condizioni di fabbrica:

METODO 1: Utilizzando la porta Ethernet

Accedendo in Telnet è possibile effettuare il reset digitando il comando *cmd=delete path=boot* e successivo *halt* (per riavviare il router)



METODO 2: Utilizzando la porta seriale RS232

Connettere il router al pc attraverso la porta seriale.

Per visualizzare il menù con le varie voci (tra cui il reset) occorre RIAVVIARE il router e premere SPACE quando richiesto. Scegliendo l'opzione 4 l'apparato viene riportato ai valori di fabbrica.

METODO 3: Utilizzando il pulsante di reset o una sequenza di riavvio

Alcuni router sono dotati di un pulsante di reset posto sul retro dell'apparato; è sufficiente premere tale pulsante per alcuni secondi fino a quando tutti i led si accendono contemporaneamente. Questo indica che il router è tornato alle condizioni di fabbrica.

Altri router non hanno il pulsante di reset perciò occorre seguire una procedura di riavvio:

You can reset your gateway to the "factory reset" (ex works) state by means of a special reset sequence (switching on and off). This state corresponds to a booted gateway in the ex works state.

In the "factory reset" state, the default configuration is used and any existing boot configuration is ignored but not deleted.

Proceed as follows to reset your gateway to the "factory reset" state:

To protect your gateway against unauthorized access in the "factory reset" state, you need the password of the previously active boot configuration for logging in.

You can log in with this password, e.g. for loading, modifying and saving the boot configuration.

- If the gateway is in operation, switch it off and then on again. The gateway runs through the boot sequence.
- Observe the LEDs on the front of your gateway. After the gateway runs through the start mode, the block of eight LEDs on the right side lights up.
- Switch off the gateway while the block of eight LEDs on the right side are lit up. You have approx. four seconds for this.
- Repeat the on/off operation twice. Your gateway has now been switched on and off three times altogether.
- Switch on your gateway for the fourth time. If you do not interrupt the boot sequence this time, the gateway starts in the "factory reset" state. This state is indicated by the block of eight LEDs on the right side flashing three times.

As an option, you can enter "*erase bootconfig*" after the login prompt. This command deletes all the existing configurations and the gateway is rebooted.

You can create the same effect by switching the gateway on and off five times instead of only three times.

If you switch the gateway off and on again, it starts with the switch saved boot configuration.